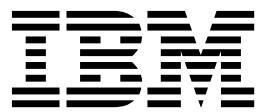


IBM Security QRadar

DSM Configuration Guide
March 2018



Note

Before using this information and the product that it supports, read the information in "Notices" on page 1003.

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This document applies to IBM QRadar Security Intelligence Platform V7.2.1 and subsequent releases unless superseded by an updated version of this document.

© Copyright IBM Corporation 2005, 2018.

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

Contents

About this DSM Configuration Guide	xix
Part 1. QRadar DSM installation and log source management	1
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
Part 2. Log sources	7
2 Introduction to log source management.	9
3 Adding a log source	11
Blue Coat Web Security Service REST API protocol configuration options	12
Cisco Firepower eStreamer protocol configuration options	13
Cisco NSEL protocol configuration options	13
EMC VMware protocol configuration options	14
Forwarded protocol configuration options	15
HTTP Receiver protocol configuration options	15
IBM BigFix SOAP protocol configuration options	15
JDBC protocol configuration options	16
JDBC SiteProtector configuration options	19
Juniper Networks NSM protocol configuration options	20
Juniper Security Binary Log Collector protocol configuration options	21
Log File protocol configuration options	21
Microsoft Azure Event Hubs protocol configuration options	22
Microsoft DHCP protocol configuration options	24
Microsoft Exchange protocol configuration options	25
Microsoft IIS protocol configuration options	26
Microsoft Security Event Log protocol configuration options	28
Microsoft Security Event Log over MSRPC Protocol	29
MQ protocol configuration options	31
Okta REST API protocol configuration options	32
OPSEC/LEA protocol configuration options	33
Oracle Database Listener protocol configuration options	34
PCAP Syslog Combination protocol configuration options	35
SDEE protocol configuration options	37
SMB Tail protocol configuration options	38
SNMPv2 protocol configuration options	39
SNMPv3 protocol configuration options	39
Seculert Protection REST API protocol configuration options	39
Sophos Enterprise Console JDBC protocol configuration options	40
Sourcefire Defense Center eStreamer protocol options	42
Syslog Redirect protocol overview	42
TCP multiline syslog protocol configuration options	43
TLS syslog protocol configuration options	47
Configuring multiple log sources over TLS syslog	48
UDP multiline syslog protocol configuration options	49
Configuring UDP multiline syslog for Cisco ACS appliances	51
VMware vCloud Director protocol configuration options	52
4 Adding bulk log sources	53
5 Adding a log source parsing order	55
6 Log source extensions	57
Examples of log source extensions on QRadar forum	57
Patterns in log source extension documents	58
Defining custom property by using a Regex or JSON expression	58
Match groups	59
Matcher (matcher)	60
JSON matcher (json-matcher)	63
Multi-event modifier (event-match-multiple)	66
Single-event modifier (event-match-single)	67
Extension document template	68
Creating a log source extensions document to get data into QRadar	70
Building a Universal DSM	71
Exporting the logs	71
Common regular expressions	73
Building regular expression patterns	74
Uploading extension documents to QRadar	75
Mapping unknown events	76
Parsing issues and examples	77
Parsing a CSV log format	79
Log Source Type IDs	80
7 Log source extension management	91
Adding a log source extension	91
Part 3. DSMs	93
8 3Com Switch 8800	95
Configuring your 3COM Switch 8800	95

9 AhnLab Policy Center	97
10 Akamai Kona.	99
11 Amazon AWS CloudTrail	101
Enabling communication between IBM Security QRadar and AWS CloudTrail	104
Verifying that Amazon AWS CloudTrail events are received	105
Troubleshooting Amazon AWS log source integrations	105
Configuring Amazon AWS CloudTrail to communicate with QRadar	107
12 Ambiron TrustWave ipAngel.	109
13 APC UPS	111
Configuring your APC UPS to forward syslog events	112
14 Apache HTTP Server	113
Configuring Apache HTTP Server with syslog	113
Configuring a Log Source in IBM Security QRadar	114
Configuring Apache HTTP Server with syslog- <i>ng</i>	114
Configuring a log source	115
15 Apple Mac OS X	117
Configuring a Mac OS X log source	117
Configuring syslog on your Apple Mac OS X	117
16 Application Security DbProtect	119
Installing the DbProtect LEEF Relay Module	120
Configuring the DbProtect LEEF Relay	120
Configuring DbProtect alerts	121
17 Arbor Networks	123
Arbor Networks Peakflow SP	123
Supported event types for Arbor Networks Peakflow SP	124
Configuring a remote syslog in Arbor Networks Peakflow SP	124
Configuring global notifications settings for alerts in Arbor Networks Peakflow SP	124
Configuring alert notification rules in Arbor Networks Peakflow SP	125
Configuring an Arbor Networks Peakflow SP log source	125
Arbor Networks Pravail	127
Configuring your Arbor Networks Pravail system to send events to IBM Security QRadar	127
18 Arpeggio SIFT-IT.	129
Configuring a SIFT-IT agent	129
Configuring a Arpeggio SIFT-IT log source	130
Additional information	131
19 Array Networks SSL VPN	133
Configuring a log source	133
20 Aruba Networks	135
Aruba ClearPass Policy Manager	135
Configuring Aruba ClearPass Policy Manager to communicate with QRadar	136
Aruba Introspect	136
Configuring Aruba Introspect to communicate with QRadar	138
Aruba Mobility Controllers.	139
Configuring your Aruba Mobility Controller	139
Configuring a log source	139
21 Avaya VPN Gateway	141
Avaya VPN Gateway DSM integration process	141
Configuring your Avaya VPN Gateway system for communication with IBM Security QRadar	141
Configuring an Avaya VPN Gateway log source in IBM Security QRadar.	142
22 BalaBit IT Security	143
BalaBit IT Security for Microsoft Windows Events	143
Configuring the Syslog- <i>ng</i> Agent event source	143
Configuring a syslog destination	144
Restarting the Syslog- <i>ng</i> Agent service	145
Configuring a log source	145
BalaBit IT Security for Microsoft ISA or TMG Events	145
Configure the BalaBit Syslog- <i>ng</i> Agent	146
Configuring the BalaBit Syslog- <i>ng</i> Agent file source	146
Configuring a BalaBit Syslog- <i>ng</i> Agent syslog destination	147
Filtering the log file for comment lines	147
Configuring a BalaBit Syslog- <i>ng</i> PE Relay	148
Configuring a log source	149
23 Barracuda	151
Barracuda Spam & Virus Firewall	151
Configuring syslog event forwarding	151
Configuring a log source	151
Barracuda Web Application Firewall.	152
Configuring Barracuda Web Application Firewall to send syslog events to QRadar	153
Configuring Barracuda Web Application Firewall to send syslog events to QRadar for devices that do not support LEEF	153
Barracuda Web Filter	154
Configuring syslog event forwarding	155
Configuring a log source	155
24 BeyondTrust PowerBroker	157
Configuring BeyondTrust PowerBroker to communicate with QRadar	158
BeyondTrust PowerBroker DSM specifications	159
Sample event messages	160
25 BlueCat Networks Adonis.	161
Supported event types	161
Event type format	161
Configuring BlueCat Adonis	162

Configuring a log source in IBM Security QRadar	162
26 Blue Coat	163
Blue Coat SG	163
Creating a custom event format	164
Creating a log facility.	165
Enabling access logging	165
Configuring Blue Coat SG for FTP uploads .	166
Configuring a Blue Coat SG Log Source . .	166
Configuring Blue Coat SG for syslog	169
Creating extra custom format key-value pairs	169
Blue Coat Web Security Service	170
Configuring Blue Coat Web Security Service to communicate with QRadar	171
27 Box	173
Configuring Box to communicate with QRadar .	174
28 Bridgewater.	177
Configuring Syslog for your Bridgewater Systems Device.	177
Configuring a log source	177
29 Brocade Fabric OS.	179
Configuring syslog for Brocade Fabric OS appliances	179
30 CA Technologies	181
CA ACF2.	181
Create a log source for near real-time event feed .	182
Creating a log source for Log File protocol . .	182
Integrate CA ACF2 with IBM Security QRadar by using audit scripts	185
Configuring CA ACF2 that uses audit scripts to integrate with IBM Security QRadar.	186
CA SiteMinder	189
Configuring a log source	189
Configuring Syslog-ng for CA SiteMinder. .	190
CA Top Secret	191
Creating a log source for Log File protocol .	192
Create a log source for near real-time event feed .	195
Integrate CA Top Secret with IBM Security QRadar by using audit scripts.	196
Configuring CA Top Secret that uses audit scripts to integrate with IBM Security QRadar .	196
31 Carbon Black	201
Carbon Black	201
Configuring Carbon Black to communicate with QRadar	202
Carbon Black Protection.	203
Configuring Carbon Black Protection to communicate with QRadar	204
Bit9 Parity	204
Configure a log source	205
Bit9 Security Platform	205
Configuring Bit9 Security Platform to communicate with QRadar	206
32 Centrify Infrastructure Services	207
Configuring WinCollect agent to collect event logs from Centrify Infrastructure Services	208
Configuring Centrify Infrastructure Services on a UNIX or Linux device to communicate with QRadar	210
Sample event messages	211
33 Check Point.	213
Check Point	213
Integration of Check Point by using OPSEC . .	213
Adding a Check Point Host	214
Creating an OPSEC Application Object	214
Locating the log source SIC.	215
Configuring an OPSEC/LEA log source in IBM Security QRadar	215
Edit your OPSEC communications configuration .	217
Updating your Check Point OPSEC log source .	217
Changing the default port for OPSEC LEA communication.	218
Configuring OPSEC LEA for unencrypted communications	218
Configuring IBM Security QRadar to receive events from a Check Point device	219
Integrate Check Point by using syslog	220
Configuring a log source	221
Integration of Check Point Firewall events from external syslog forwarders	222
Configuring a log source for Check Point forwarded events	222
Check Point Multi-Domain Management (Provider-1)	224
Integrating syslog for Check Point Multi-Domain Management (Provider-1)	224
Configuring a log source	225
Configuring OPSEC for Check Point Multi-Domain Management (Provider-1)	225
Configuring an OPSEC log source	226
34 Cilasoft QJRN/400	229
Configuring Cilasoft QJRN/400	229
Configuring a Cilasoft QJRN/400 log source . .	230
35 Cisco	233
Cisco ACE Firewall	233
Configuring Cisco ACE Firewall	233
Configuring a log source	233
Cisco Aironet	234
Configuring a log source	235
Cisco ACS	236
Configuring Syslog for Cisco ACS v5.x . . .	236
Creating a Remote Log Target	236
Configuring global logging categories	237
Configuring a log source	237
Configuring Syslog for Cisco ACS v4.x	238
Configuring syslog forwarding for Cisco ACS v4.x	238
Configuring a log source for Cisco ACS v4.x .	239
Configuring UDP multiline syslog for Cisco ACS appliances	239

Cisco ASA	240	Cisco Wireless Services Module	279
Integrate Cisco ASA Using Syslog	240	Configuring Cisco WiSM to forward events .	279
Configuring syslog forwarding	240	Configuring a log source	281
Configuring a log source	241	Cisco Wireless LAN Controllers	281
Integrate Cisco ASA for NetFlow by using NSEL .	242	Configuring syslog for Cisco Wireless LAN	
Configuring NetFlow Using NSEL	242	Controller	282
Configuring a log source	243	Configuring a syslog log source in IBM Security	
Cisco CallManager	244	QRadar	282
Configuring syslog forwarding	244	Configuring SNMPv2 for Cisco Wireless LAN	
Configuring a log source	245	Controller	283
Cisco CatOS for Catalyst Switches	245	Configuring a trap receiver for Cisco Wireless	
Configuring syslog	245	LAN Controller	284
Configuring a log source	246	Configuring a log source for the Cisco Wireless	
Cisco Cloud Web Security	247	LAN Controller that uses SNMPv2	284
Configuring Cloud Web Security to			
communicate with QRadar	249		
Cisco CSA	250	36 Citrix	287
Configuring syslog for Cisco CSA	250	Citrix NetScaler	287
Configuring a log source	250	Configuring a Citrix NetScaler log source . .	288
Cisco FireSIGHT Management Center	251	Citrix Access Gateway	288
Creating Cisco FireSIGHT Management Center		Configuring a Citrix Access Gateway log source	289
5.x and 6.x certificates	253		
Importing a Cisco FireSIGHT Management			
Center certificate in QRadar	255		
Configuring a log source for Cisco FireSIGHT			
Management Center events.	256		
Cisco FWSM	257	37 Cloudera Navigator	291
Configuring Cisco FWSM to forward syslog		Configuring Cloudera Navigator to communicate	
events	257	with QRadar	292
Configuring a log source	258		
Cisco IDS/IPS	258	38 CloudPassage Halo	293
Cisco IronPort	260	Configuring CloudPassage Halo for	
Configuring IronPort mail log	260	communication with QRadar	293
Configuring a log source	261	Configuring a CloudPassage Halo log source in	
IronPort web content filter	262	QRadar	295
Cisco IOS	262		
Configuring Cisco IOS to forward events .	262	39 CloudLock Cloud Security Fabric	297
Configuring a log source	263	Configuring CloudLock Cloud Security Fabric to	
Cisco Identity Services Engine	264	communicate with QRadar	298
Configuring a remote logging target in Cisco			
ISE	266	40 Correlog Agent for IBM z/OS	299
Configuring logging categories in Cisco ISE		Configuring your CorreLog Agent system for	
.	267	communication with QRadar	300
Cisco NAC	268		
Configuring Cisco NAC to forward events .	268	41 CrowdStrike Falcon Host	301
Configuring a log source	268	Configuring CrowdStrike Falcon Host to	
Cisco Nexus	269	communicate with QRadar	302
Configuring Cisco Nexus to forward events .	269		
Configuring a log source	269	42 CRYPTOCard CRYPTO-Shield	305
Cisco Pix	270	Configuring a log source	305
Configuring Cisco Pix to forward events .	270	Configuring syslog for CRYPTOCard	
Configuring a log source	271	CRYPTO-Shield	305
Cisco Stealthwatch	272		
Configuring Cisco Stealthwatch to communicate			
with QRadar	273		
Cisco Umbrella	274	43 CyberArk	307
Configure Cisco Umbrella to communicate with		CyberArk Privileged Threat Analytics	307
QRadar	276	Configuring CyberArk Privileged Threat	
Cisco Umbrella DSM specifications	277	Analytics to communicate with QRadar . .	308
Sample event messages	277	CyberArk Vault	308
Cisco VPN 3000 Concentrator	277	Configuring syslog for CyberArk Vault . .	308
Configuring a log source	278	Configuring a log source for CyberArk Vault	309

44 CyberGuard Firewall/VPN Appliance	311	Extreme NetSight Automatic Security Manager	340																																																																																												
Configuring syslog events	311	Extreme NAC	341																																																																																												
Configuring a log source	311	Configuring a log source	341																																																																																												
45 Damballa Failsafe	313	Extreme stackable and stand-alone switches	341																																																																																												
Configuring syslog for Damballa Failsafe	313	Extreme Networks ExtremeWare	343																																																																																												
Configuring a log source	313	Configuring a log source	343																																																																																												
46 DG Technology MEAS	315	Extreme XSR Security Router	343																																																																																												
Configuring your DG Technology MEAS system for communication with QRadar	315																																																																																														
47 Digital China Networks (DCN)	317																																																																																														
Configuring a log source	317																																																																																														
Configuring a DCN DCS/DCRS Series Switch	318																																																																																														
48 Enterprise-IT-Security.com SF-Sherlock	319																																																																																														
Configuring Enterprise-IT-Security.com SF-Sherlock to communicate with QRadar	320	F5 Networks BIG-IP AFM	345																																																																																												
		Configuring a logging pool	345																																																																																												
		Creating a high-speed log destination	346																																																																																												
		Creating a formatted log destination	346																																																																																												
		Creating a log publisher	346																																																																																												
		Creating a logging profile	347																																																																																												
		Associating the profile to a virtual server	347																																																																																												
		Configuring a log source	348																																																																																												
		F5 Networks BIG-IP APM	348																																																																																												
		Configuring Remote Syslog for F5 BIG-IP APM 11.x	348																																																																																												
		Configuring a Remote Syslog for F5 BIG-IP APM 10.x	349																																																																																												
		Configuring a log source	349																																																																																												
		Configuring F5 Networks BIG-IP ASM	350																																																																																												
		Configuring a log source	351																																																																																												
		F5 Networks BIG-IP LTM	351																																																																																												
		Configuring a log source	351																																																																																												
		Configuring syslog forwarding in BIG-IP LTM 11.x	352																																																																																												
		Configuring Remote Syslog for F5 BIG-IP LTM 10.x	352																																																																																												
		Configuring Remote Syslog for F5 BIG-IP LTM 9.4.2 to 9.4.8	353																																																																																												
		F5 Networks FirePass	353																																																																																												
		Configuring syslog forwarding for F5 FirePass	354																																																																																												
		Configuring a log source	354																																																																																												
49 Epic SIEM	321																																																																																														
Configuring Epic SIEM 2014 to communicate with QRadar	322	54 Fair Warning	357																																																																																												
Configuring Epic SIEM 2015 to communicate with QRadar	322	Configuring a log source	357	Configuring Epic SIEM 2017 to communicate with QRadar	324	50 ESET Remote Administrator	327			Configuring ESET Remote Administrator to communicate with QRadar	328	55 Fasoo Enterprise DRM	359	51 Exabeam	329	Configuring Fasoo Enterprise DRM to communicate with QRadar	361	Configuring Exabeam to communicate with QRadar	329			52 Extreme	331	56 Fidelis XPS	363	Extreme 800-Series Switch	331	Configuring Fidelis XPS	363	Configuring your Extreme 800-Series Switch	331	Configuring a log source	364	Configuring a log source	331	Extreme Dragon	332			Creating a Policy for Syslog	332	57 FireEye	365	Configuring a log source	334	Configuring your FireEye system for communication with QRadar	365	Configure the EMS to forward syslog messages	334	Configuring your FireEye HX system for communication with QRadar	366	Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later	334	Configuring a FireEye log source in QRadar	366	Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier	335			Extreme HiGuard Wireless IPS	335	58 FORCEPOINT	369	Configuring Enterasys HiGuard	336	FORCEPOINT Stonesoft Management Center	369	Configuring a log source	336			Extreme HiPath Wireless Controller	337			Configuring your HiPath Wireless Controller	337			Configuring a log source	337			Extreme Matrix Router	338			Configuring a FireEye log source in QRadar	366			Extreme Matrix K/N/S Series Switch	339		
Configuring a log source	357																																																																																														
Configuring Epic SIEM 2017 to communicate with QRadar	324	50 ESET Remote Administrator	327			Configuring ESET Remote Administrator to communicate with QRadar	328	55 Fasoo Enterprise DRM	359	51 Exabeam	329	Configuring Fasoo Enterprise DRM to communicate with QRadar	361	Configuring Exabeam to communicate with QRadar	329			52 Extreme	331	56 Fidelis XPS	363	Extreme 800-Series Switch	331	Configuring Fidelis XPS	363	Configuring your Extreme 800-Series Switch	331	Configuring a log source	364	Configuring a log source	331	Extreme Dragon	332			Creating a Policy for Syslog	332	57 FireEye	365	Configuring a log source	334	Configuring your FireEye system for communication with QRadar	365	Configure the EMS to forward syslog messages	334	Configuring your FireEye HX system for communication with QRadar	366	Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later	334	Configuring a FireEye log source in QRadar	366	Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier	335			Extreme HiGuard Wireless IPS	335	58 FORCEPOINT	369	Configuring Enterasys HiGuard	336	FORCEPOINT Stonesoft Management Center	369	Configuring a log source	336			Extreme HiPath Wireless Controller	337			Configuring your HiPath Wireless Controller	337			Configuring a log source	337			Extreme Matrix Router	338			Configuring a FireEye log source in QRadar	366			Extreme Matrix K/N/S Series Switch	339						
50 ESET Remote Administrator	327																																																																																														
Configuring ESET Remote Administrator to communicate with QRadar	328	55 Fasoo Enterprise DRM	359																																																																																												
51 Exabeam	329	Configuring Fasoo Enterprise DRM to communicate with QRadar	361																																																																																												
Configuring Exabeam to communicate with QRadar	329																																																																																														
52 Extreme	331	56 Fidelis XPS	363																																																																																												
Extreme 800-Series Switch	331	Configuring Fidelis XPS	363	Configuring your Extreme 800-Series Switch	331	Configuring a log source	364	Configuring a log source	331	Extreme Dragon	332			Creating a Policy for Syslog	332	57 FireEye	365	Configuring a log source	334	Configuring your FireEye system for communication with QRadar	365	Configure the EMS to forward syslog messages	334	Configuring your FireEye HX system for communication with QRadar	366	Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later	334	Configuring a FireEye log source in QRadar	366	Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier	335			Extreme HiGuard Wireless IPS	335	58 FORCEPOINT	369	Configuring Enterasys HiGuard	336	FORCEPOINT Stonesoft Management Center	369	Configuring a log source	336			Extreme HiPath Wireless Controller	337			Configuring your HiPath Wireless Controller	337			Configuring a log source	337			Extreme Matrix Router	338			Configuring a FireEye log source in QRadar	366			Extreme Matrix K/N/S Series Switch	339																												
Configuring Fidelis XPS	363																																																																																														
Configuring your Extreme 800-Series Switch	331	Configuring a log source	364	Configuring a log source	331	Extreme Dragon	332			Creating a Policy for Syslog	332	57 FireEye	365	Configuring a log source	334	Configuring your FireEye system for communication with QRadar	365	Configure the EMS to forward syslog messages	334	Configuring your FireEye HX system for communication with QRadar	366	Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later	334	Configuring a FireEye log source in QRadar	366	Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier	335			Extreme HiGuard Wireless IPS	335	58 FORCEPOINT	369	Configuring Enterasys HiGuard	336	FORCEPOINT Stonesoft Management Center	369	Configuring a log source	336			Extreme HiPath Wireless Controller	337			Configuring your HiPath Wireless Controller	337			Configuring a log source	337			Extreme Matrix Router	338			Configuring a FireEye log source in QRadar	366			Extreme Matrix K/N/S Series Switch	339																																
Configuring a log source	364																																																																																														
Configuring a log source	331	Extreme Dragon	332			Creating a Policy for Syslog	332	57 FireEye	365	Configuring a log source	334	Configuring your FireEye system for communication with QRadar	365	Configure the EMS to forward syslog messages	334	Configuring your FireEye HX system for communication with QRadar	366	Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later	334	Configuring a FireEye log source in QRadar	366	Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier	335			Extreme HiGuard Wireless IPS	335	58 FORCEPOINT	369	Configuring Enterasys HiGuard	336	FORCEPOINT Stonesoft Management Center	369	Configuring a log source	336			Extreme HiPath Wireless Controller	337			Configuring your HiPath Wireless Controller	337			Configuring a log source	337			Extreme Matrix Router	338			Configuring a FireEye log source in QRadar	366			Extreme Matrix K/N/S Series Switch	339																																				
Extreme Dragon	332																																																																																														
Creating a Policy for Syslog	332	57 FireEye	365																																																																																												
Configuring a log source	334	Configuring your FireEye system for communication with QRadar	365	Configure the EMS to forward syslog messages	334	Configuring your FireEye HX system for communication with QRadar	366	Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later	334	Configuring a FireEye log source in QRadar	366	Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier	335			Extreme HiGuard Wireless IPS	335	58 FORCEPOINT	369	Configuring Enterasys HiGuard	336	FORCEPOINT Stonesoft Management Center	369	Configuring a log source	336			Extreme HiPath Wireless Controller	337			Configuring your HiPath Wireless Controller	337			Configuring a log source	337			Extreme Matrix Router	338			Configuring a FireEye log source in QRadar	366			Extreme Matrix K/N/S Series Switch	339																																														
Configuring your FireEye system for communication with QRadar	365																																																																																														
Configure the EMS to forward syslog messages	334	Configuring your FireEye HX system for communication with QRadar	366	Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later	334	Configuring a FireEye log source in QRadar	366	Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier	335			Extreme HiGuard Wireless IPS	335	58 FORCEPOINT	369	Configuring Enterasys HiGuard	336	FORCEPOINT Stonesoft Management Center	369	Configuring a log source	336			Extreme HiPath Wireless Controller	337			Configuring your HiPath Wireless Controller	337			Configuring a log source	337			Extreme Matrix Router	338			Configuring a FireEye log source in QRadar	366			Extreme Matrix K/N/S Series Switch	339																																																		
Configuring your FireEye HX system for communication with QRadar	366																																																																																														
Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later	334	Configuring a FireEye log source in QRadar	366	Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier	335			Extreme HiGuard Wireless IPS	335	58 FORCEPOINT	369	Configuring Enterasys HiGuard	336	FORCEPOINT Stonesoft Management Center	369	Configuring a log source	336			Extreme HiPath Wireless Controller	337			Configuring your HiPath Wireless Controller	337			Configuring a log source	337			Extreme Matrix Router	338			Configuring a FireEye log source in QRadar	366			Extreme Matrix K/N/S Series Switch	339																																																						
Configuring a FireEye log source in QRadar	366																																																																																														
Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier	335																																																																																														
Extreme HiGuard Wireless IPS	335	58 FORCEPOINT	369																																																																																												
Configuring Enterasys HiGuard	336	FORCEPOINT Stonesoft Management Center	369	Configuring a log source	336			Extreme HiPath Wireless Controller	337			Configuring your HiPath Wireless Controller	337			Configuring a log source	337			Extreme Matrix Router	338			Configuring a FireEye log source in QRadar	366			Extreme Matrix K/N/S Series Switch	339																																																																		
FORCEPOINT Stonesoft Management Center	369																																																																																														
Configuring a log source	336																																																																																														
Extreme HiPath Wireless Controller	337																																																																																														
Configuring your HiPath Wireless Controller	337																																																																																														
Configuring a log source	337																																																																																														
Extreme Matrix Router	338																																																																																														
Configuring a FireEye log source in QRadar	366																																																																																														
Extreme Matrix K/N/S Series Switch	339																																																																																														

Configuring FORCEPOINT Stonesoft Management Center to communicate with QRadar	370
Configuring a syslog traffic rule for FORCEPOINT Stonesoft Management Center.	371
Forcepoint TRITON	372
Configuring syslog for Forcepoint TRITON	373
Configuring a log source for Forcepoint TRITON	373
Forcepoint V-Series Data Security Suite	374
Configuring syslog for Forcepoint V-Series Data Security Suite	374
Configuring a log source for Forcepoint V-Series Data Security Suite	375
Forcepoint V-Series Content Gateway	375
Configure syslog for Forcepoint V-Series Content Gateway	375
Configuring the Management Console for Forcepoint V-Series Content Gateway	376
Enabling Event Logging for Forcepoint V-Series Content Gateway	376
Configuring a log source for Forcepoint V-Series Content Gateway	377
Log file protocol for Forcepoint V-Series Content Gateway	377
Configuring the Content Management Console for Forcepoint V-Series Content Gateway	378
Configuring a log file protocol log source for Forcepoint V-Series Content Gateway	378
59 ForeScout CounterACT	379
Configuring a log source	379
Configuring the ForeScout CounterACT Plug-in	379
Configuring ForeScout CounterACT Policies	380
60 Fortinet FortiGate Security Gateway	383
Configuring a syslog destination on your Fortinet FortiGate Security Gateway device	384
Configuring a syslog destination on your Fortinet FortiAnalyzer device	384
61 Foundry FastIron	385
Configuring syslog for Foundry FastIron	385
Configuring a log source	385
62 FreeRADIUS	387
Configuring your FreeRADIUS device to communicate with QRadar	387
63 Generic	389
Generic Authorization Server	389
Configuring event properties	389
Configuring a log source	391
Generic Firewall	391
Configuring event properties	391
Configuring a log source	393
64 genua genugate	395
Configuring genua genugate to send events to QRadar	396
65 Great Bay Beacon	397
Configuring syslog for Great Bay Beacon	397
Configuring a log source	397
66 HBGary Active Defense	399
Configuring HBGary Active Defense	399
Configuring a log source	399
67 H3C Technologies	401
H3C Comware Platform	401
Configuring H3C Comware Platform to communicate with QRadar	402
68 Honeycomb Lexicon File Integrity Monitor (FIM)	403
Supported Honeycomb FIM event types logged by QRadar	403
Configuring the Lexicon mesh service	403
Configuring a Honeycomb Lexicon FIM log source in QRadar	404
69 Hewlett Packard (HP)	407
HP Network Automation	407
Configuring HP Network Automation Software to communicate with QRadar	408
HP ProCurve	409
Configuring a log source	409
HP Tandem	410
Hewlett Packard UNIX (HP-UX)	411
Configure a log source	411
70 Huawei	413
Huawei AR Series Router	413
Configuring a log source	413
Configuring Your Huawei AR Series Router	414
Huawei S Series Switch	414
Configuring a log source	415
Configuring Your Huawei S Series Switch	415
71 HyTrust CloudControl	417
Configuring HyTrust CloudControl to communicate with QRadar	418
72 IBM	419
IBM AIX	419
IBM AIX Server DSM overview	419
Configuring your IBM AIX Server device to send syslog events to QRadar	420
IBM AIX Audit DSM overview	420
Configuring IBM AIX Audit DSM to send syslog events to QRadar	422
Configuring IBM AIX Audit DSM to send log file protocol events to QRadar	423
IBM i	424

Configuring IBM i to integrate with IBM Security QRadar	425
Manually extracting journal entries for IBM i	427
Pulling Data Using Log File Protocol	428
Configuring Townsend Security Alliance LogAgent to integrate with QRadar	429
IBM BigFix	429
IBM BigFix Detect	431
Configuring IBM BigFix Detect to communicate with QRadar	432
IBM Bluemix Platform	434
Configuring Bluemix Platform to communicate with QRadar	434
Integrating Bluemix Platform with QRadar	435
Configuring a Bluemix log source to use Syslog	435
Configuring a Bluemix log source with TLS Syslog	435
IBM CICS	436
Create a log source for near real-time event feed	437
Creating a log source for Log File protocol	438
IBM DataPower	441
Configuring IBM DataPower to communicate with QRadar	441
IBM DB2	442
Create a log source for near real-time event feed	443
Creating a log source for Log File protocol	444
Integrating IBM DB2 Audit Events	447
Extracting audit data for DB2 v8.x to v9.4	447
Extracting audit data for DB2 v9.5	448
IBM Federated Directory Server	449
Configuring IBM Federated Directory Server to monitor security events	450
IBM Fiberlink MaaS360	450
Configuring an IBM Fiberlink MaaS360 log source in QRadar	451
IBM Guardium	452
Creating a syslog destination for events	453
Configuring policies to generate syslog events	453
Installing an IBM Guardium Policy	454
Configuring a log source	454
Creating an event map for IBM Guardium events	455
Modifying the event map	456
IBM IMS	456
Configuring IBM IMS	457
Configuring a log source	459
IBM Informix Audit	461
IBM Lotus Domino	462
Setting Up SNMP Services	462
Setting up SNMP in AIX	462
Starting the Domino Server Add-in Tasks	463
Configuring SNMP Services	463
Configuring your IBM Lotus Domino device to communicate with QRadar	464
IBM Privileged Session Recorder	465
Configuring IBM Privileged Session Recorder to communicate with QRadar	466
Configuring a log source for IBM Privileged Session Recorder	466
IBM Proventia	467
IBM Proventia Management SiteProtector	467
Configuring a log source	468
IBM ISS Proventia	470
IBM QRadar Packet Capture	470
Configuring IBM QRadar Packet Capture to communicate with QRadar	472
Configuring IBM QRadar Network Packet Capture to communicate with QRadar	473
IBM RACF	473
Creating a log source for Log File protocol	474
Create a log source for near real-time event feed	477
Integrate IBM RACF with IBM Security QRadar by using audit scripts	478
Configuring IBM RACF that uses audit scripts to integrate with IBM Security QRadar	478
IBM SAN Volume Controller	480
Configuring IBM SAN Volume Controller to communicate with QRadar	482
IBM Security Access Manager for Enterprise Single Sign-On	482
Configuring a log server type	483
Configuring syslog forwarding	483
Configuring a log source in IBM Security QRadar	483
IBM Security Access Manager for Mobile	484
Configuring IBM Security Access Manager for Mobile to communicate with QRadar	486
Configuring IBM IDaaS Platform to communicate with QRadar	487
Configuring an IBM IDaaS console to communicate with QRadar	487
IBM Security Directory Server	488
IBM Security Directory Server integration process	488
Configuring an IBM Security Directory Server log source in IBM Security QRadar	488
IBM Security Identity Governance	489
Configuring QRadar to communicate with your IBM Security Identity Governance database	490
IBM Security Identity Manager	491
IBM Security Network IPS (GX)	494
Configuring your IBM Security Network IPS (GX) appliance for communication with QRadar	495
Configuring an IBM Security Network IPS (GX) log source in QRadar	495
IBM QRadar Network Security XGS	496
Configuring IBM QRadar Network Security XGS Alerts	496
Configuring a Log Source in IBM Security QRadar	497
IBM Security Privileged Identity Manager	498
Configuring IBM Security Privileged Identity Manager	499
IBM Security Trusteer Apex Advanced Malware Protection	500
Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar	504
Configuring IBM Security Trusteer Apex Advanced Malware Protection to send TLS Syslog events to QRadar	504

Creating a TLS/SSL server certificate and private key	504	Configuring an agileSI log source	544
Creating Client Authentication certificates and keys for Apex Local Manager	505	79 Itron Smart Meter	547
Configuring the Apex Local Manager	505	80 Juniper Networks	549
Configuring the ALM instance	506	Juniper Networks AVT	549
Configuring a Flat File Feed service	506	Configuring IBM Security QRadar to receive events from a Juniper Networks AVT device	549
IBM Security Trusteer Apex Local Event Aggregator	507	Juniper Networks DDoS Secure	551
Configuring syslog for Trusteer Apex Local Event Aggregator	507	Juniper Networks DX Application Acceleration Platform	551
IBM Sense	508	Configuring IBM Security QRadar to receive events from a Juniper DX Application Acceleration Platform	552
Configuring IBM Sense to communicate with QRadar	509	Juniper Networks EX Series Ethernet Switch	552
IBM SmartCloud Orchestrator	509	Configuring IBM Security QRadar to receive events from a Juniper EX Series Ethernet Switch	553
Installing IBM SmartCloud Orchestrator	510	Juniper Networks IDP	553
Configuring an IBM SmartCloud Orchestrator log source in QRadar	510	Configure a log source	554
IBM Tivoli Access Manager for e-business	511	Juniper Networks Infranet Controller	555
Configure Tivoli Access Manager for e-business	511	Juniper Networks Firewall and VPN	555
Configuring a log source	512	Configuring IBM Security QRadar to receive events	555
IBM Tivoli Endpoint Manager	513	Juniper Networks Junos OS	556
IBM WebSphere Application Server	513	Configuring QRadar to receive events from a Juniper Junos OS Platform device	558
Configuring IBM WebSphere	513	Configure the PCAP Protocol	558
Customizing the Logging Option	513	Configuring a New Juniper Networks SRX Log Source with PCAP	559
Creating a log source	514	Juniper Networks Network and Security Manager	560
IBM WebSphere DataPower	517	Configuring Juniper Networks NSM to export logs to syslog	560
IBM z/OS	517	Configuring a log source for Juniper Networks NSM	560
Create a log source for near real-time event feed	518	Juniper Networks Secure Access	561
Creating a log source for Log File protocol	518	Juniper Networks Security Binary Log Collector	561
IBM zSecure Alert	521	Configuring the Juniper Networks Binary Log Format	561
73 ISC Bind	523	Configuring a log source	562
Configuring a log source	524	Juniper Networks Steel-Belted Radius	563
74 Illumio Adaptive Security Platform	527	Configuring Juniper Steel-Belted Radius for syslog	564
Configuring Illumio Adaptive Security Platform to communicate with QRadar	528	Juniper Networks vGW Virtual Gateway	564
Configuring Exporting Events to Syslog for Illumio PCE	528	Juniper Networks Junos WebApp Secure	565
Configuring Syslog Forwarding for Illumio PCE	529	Configuring syslog forwarding	566
75 Imperva Incapsula	531	Configuring event logging	566
Configuring Imperva Incapsula to communicate with QRadar	532	Configuring a log source	567
76 Imperva SecureSphere	535	Juniper Networks WLC Series Wireless LAN Controller	568
Configuring an alert action for Imperva SecureSphere	536	Configuring a syslog server from the Juniper WLC user interface	568
Configuring a system event action for Imperva SecureSphere	537	Configuring a syslog server with the command-line interface for Juniper WLC	569
Configuring Imperva SecureSphere V11.0 to send database audit records to QRadar	539		
77 Infoblox NIOS	541		
Configuring a log source	541		
78 iT-CUBE agileSI	543		
Configuring agileSI to forward events	543		
		81 Kaspersky	571
		Kaspersky Security Center	571
		Creating a Database View for Kaspersky Security Center	574
		Exporting syslog to QRadar from Kaspersky Security Center	575

Kaspersky Threat Feed Service	576	Configuring McAfee Firewall Enterprise to communicate with QRadar	614
Configuring Kaspersky Threat Feed Service to communicate with QRadar	577	McAfee Intrushield	615
Configuring QRadar to forward events to the Kaspersky Threat Feed Service	578	Configuring alert events for McAfee Intrushield V2.x - V5.x	615
82 Kisco Information Systems	581	Configuring alert events for McAfee Intrushield V6.x and V7.x	616
SafeNet/i	581	Configuring fault notification events for McAfee Intrushield V6.x and V7.x	617
Configuring Kisco Information Systems SafeNet/i to communicate with QRadar	582	McAfee Web Gateway	619
83 Lastline Enterprise.	585	McAfee Web Gateway DSM integration process	619
Configuring Lastline Enterprise to communicate with QRadar	586	Configuring McAfee Web Gateway to communicate with QRadar (syslog)	620
84 Lieberman Random Password Manager	587	Importing the Syslog Log Handler	620
85 LightCyber Magna	589	Configuring McAfee Web Gateway to communicate with IBM Security QRadar (log file protocol)	621
Configuring LightCyber Magna to communicate with QRadar	590	Pulling data by using the log file protocol	622
86 Linux	591	Creation of an event map for McAfee Web Gateway events	622
Linux DHCP	591	Discovering unknown events	622
Configuring a log source	591	Modifying the event map	623
Linux IPtables	591		
Configuring IPtables	592		
Configuring a log source	593		
Linux OS	593		
Configuring syslog on Linux OS	594		
Configuring syslog- <i>ng</i> on Linux OS	594		
Configuring Linux OS to send audit logs	595		
87 LOGbinder	597		
LOGbinder EX event collection from Microsoft Exchange Server	597		
Configuring your LOGbinder EX system to send Microsoft Exchange event logs to QRadar	598		
LOGbinder SP event collection from Microsoft SharePoint	598		
Configuring your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar	599		
LOGbinder SQL event collection from Microsoft SQL Server	600		
Configuring your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar	601		
88 McAfee	603		
McAfee Application / Change Control	603		
McAfee ePolicy Orchestrator	605		
Adding a registered server to McAfee ePolicy Orchestrator	611		
Configuring SNMP notifications on McAfee ePolicy Orchestrator	611		
Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator	613		
Installing the Java Cryptography Extension on QRadar	613		
McAfee Firewall Enterprise	614		
Configuring a log source for Microsoft Exchange	643		
Microsoft Hyper-V	645		
Microsoft Hyper-V DSM integration process	645		
Configuring a Microsoft Hyper-V log source in QRadar	646		
Microsoft IAS Server	646		

Microsoft IIS Server	647
Configuring Microsoft IIS by using the IIS Protocol	647
Configuring the Microsoft IIS Protocol in IBM Security QRadar	648
Configuring a Microsoft IIS log source	649
Microsoft ISA	650
Microsoft Office 365	650
Configuring Microsoft Office 365 to communicate with QRadar	653
Configuring Microsoft Office 365 to communicate with QRadar using the Classic Azure Management interface	654
Microsoft Operations Manager	655
Microsoft SharePoint	658
Configuring a database view to collect audit events	658
Configuring Microsoft SharePoint audit events	658
Creating a database view for Microsoft SharePoint	659
Creating read-only permissions for Microsoft SharePoint database users	660
Configuring a SharePoint log source for a database view	660
Configuring a SharePoint log source for predefined database queries	663
Microsoft SQL Server	665
Microsoft SQL Server preparation for communication with QRadar	666
Creating a Microsoft SQL Server auditing object	666
Creating a Microsoft SQL Server audit specification	666
Creating a Microsoft SQL Server database view	667
Configuring a Microsoft SQL Server log source	667
Microsoft System Center Operations Manager	670
Microsoft Windows Security Event Log	672
Verifying MSRPC Protocol	673
Verifying MSRPC protocol from the QRadar Console	673
Verifying MSRPC protocol from QRadar user interface	673
Restarting the Web Server	673
Installing the MSRPC protocol on the QRadar Console	674
Enabling MSRPC on Windows hosts	674
Diagnosing connection issues with the MSRPC test tool	677
Enabling WMI on Windows hosts	678
91 Motorola Symbol AP	683
Configuring a log source	683
Configure syslog events for Motorola Symbol AP	683
92 Name Value Pair	685
93 NCC Group DDoS Secure	689
Configuring NCC Group DDoS Secure to communicate with QRadar	690
94 NetApp Data ONTAP	691
95 Netskope Active	693
Configuring QRadar to collect events from your Netskope Active system	694
96 Niksun	695
Configuring a log source	695
97 Nokia Firewall	697
Integration with a Nokia Firewall by using syslog	697
Configuring IPtables	697
Configuring syslog	698
Configuring the logged events custom script	698
Configuring a log source	698
Integration with a Nokia Firewall by using OPSEC	699
Configuring a Nokia Firewall for OPSEC	699
Configuring an OPSEC log source	700
98 Nominum Vantio	703
Configure the Vantio LEEF Adapter	703
Configuring a log source	703
99 Nortel Networks	705
Nortel Multiprotocol Router	705
Nortel Application Switch	707
Nortel Contivity	708
Nortel Ethernet Routing Switch 2500/4500/5500	708
Nortel Ethernet Routing Switch 8300/8600	709
Nortel Secure Router	710
Nortel Secure Network Access Switch	711
Nortel Switched Firewall 5100	712
Integrating Nortel Switched Firewall by using syslog	712
Integrate Nortel Switched Firewall by using OPSEC	713
Configuring a log source	713
Nortel Switched Firewall 6000	713
Configuring syslog for Nortel Switched Firewalls	714
Configuring OPSEC for Nortel Switched Firewalls	714
Reconfiguring the Check Point SmartCenter Server	715
Nortel Threat Protection System (TPS)	715
Nortel VPN Gateway	716
100 Novell eDirectory	719
Configure XDASv2 to forward events	719
Load the XDASv2 Module	720
Loading the XDASv2 on a Linux Operating System	720
Loading the XDASv2 on a Windows Operating System	721
Configure event auditing using Novell iManager	721
Configure a log source	722

101 Observe IT JDBC	723	Oracle OS Audit	768
102 Okta	727	Configuring the log sources within QRadar for Oracle OS Audit	770
103 Onapsis Security Platform	731	109 OSSEC	771
Configuring Onapsis Security Platform to communicate with QRadar	732	Configuring OSSEC	771
104 OpenBSD	733	Configuring a log source	771
Configuring a log source	733	110 Palo Alto Networks	773
Configuring syslog for OpenBSD	733	Palo Alto Endpoint Security Manager	773
105 Open LDAP	735	Configuring Palo Alto Endpoint Security Manager to communicate with QRadar	774
Configuring a log source	735	Palo Alto Networks PA Series	775
Configuring IPtables for UDP Multiline Syslog events	736	Creating a syslog destination on your Palo Alto PA Series device	776
Configuring event forwarding for Open LDAP	738	Creating a forwarding policy on your Palo Alto PA Series device	780
106 Open Source SNORT	739	Creating ArcSight CEF formatted Syslog events on your Palo Alto PA Series Networks Firewall device	780
Configuring Open Source SNORT	739	111 Pirean Access: One	783
Configuring a log source	740	Configuring a log source	783
107 OpenStack	741	112 PostFix Mail Transfer Agent	787
Configuring OpenStack to communicate with QRadar	742	Configuring syslog for PostFix Mail Transfer Agent	787
108 Oracle	745	Configuring a PostFix MTA log source	787
Oracle Acme Packet Session Border Controller	745	Configuring IPtables for multiline UDP syslog events	788
Supported Oracle Acme Packet event types that are logged by IBM Security QRadar	745	113 ProFTPD	791
Configuring an Oracle Acme Packet SBC log source	745	Configuring ProFTPD	791
Configuring SNMP to syslog conversion on Oracle Acme Packet SBC	746	Configuring a log source	791
Enabling syslog settings on the media manager object	747	114 Proofpoint Enterprise Protection and Enterprise Privacy	793
Oracle Audit Vault	747	Configuring Proofpoint Enterprise Protection and Enterprise Privacy DSM to communicate with IBM Security QRadar	794
Configuring Oracle Audit Vault to communicate with QRadar	750	Configuring a Proofpoint Enterprise Protection and Enterprise Privacy log source	794
Oracle BEA WebLogic	750	115 Pulse Secure Pulse Connect Secure	799
Enabling event logs	751	Configuring a Pulse Secure Pulse Connect Secure device to send WebTrends Enhanced Log File (WELF) events to IBM Security QRadar	800
Configuring domain logging	751	Configuring a Pulse Secure Pulse Connect Secure device to send syslog events to QRadar	801
Configuring application logging	751	Sample event message	802
Configuring an audit provider	752	116 Radware	803
Configuring a log source	752	Radware AppWall	803
Oracle DB Audit	754	Configuring Radware AppWall to communicate with QRadar	804
Enabling Unified Auditing in Oracle 12c	758	Increasing the maximum TCP Syslog payload length for Radware AppWall	804
Configuring an Oracle database server to send syslog audit logs to QRadar	758	Radware DefensePro	805
Oracle DB Listener	760		
Collecting events by using the Oracle Database Listener Protocol	760		
Collecting Oracle database events by using Perl	762		
Configuring the Oracle Database Listener within QRadar	763		
Oracle Directory Server overview	764		
Oracle Enterprise Manager	764		
Oracle Fine Grained Auditing	765		
Configuring a log source	766		

Configuring a log source	806
117 Raz-Lee iSecurity	807
Configuring Raz-Lee iSecurity to communicate with QRadar	807
Configuring a log source for Raz-Lee iSecurity	809
118 Redback ASE	811
Configuring Redback ASE	811
Configuring a log source	811
119 Resolution1 CyberSecurity	813
Configuring your Resolution1 CyberSecurity device to communicate with QRadar	814
Resolution1 CyberSecurity log source on your QRadar Console	814
120 Riverbed	815
Riverbed SteelCentral NetProfiler (Cascade Profiler) Audit	815
Creating a Riverbed SteelCentral NetProfiler report template and generating an audit file	816
Riverbed SteelCentral NetProfiler (Cascade Profiler) Alert	817
Configuring your Riverbed SteelCentral NetProfiler system to enable communication with QRadar	818
121 RSA Authentication Manager	819
Configuration of syslog for RSA Authentication Manager 6.x, 7.x and 8.x	819
Configuring Linux	819
Configuring Windows	820
Configuring the log file protocol for RSA Authentication Manager 6.x and 7.x	820
Configuring RSA Authentication Manager 6.x	821
Configuring RSA Authentication Manager 7.x	821
122 SafeNet DataSecure	823
Configuring SafeNet DataSecure to communicate with QRadar	823
123 Salesforce	825
Salesforce Security Auditing	825
Downloading the Salesforce audit trail file	825
Configuring a Salesforce Security Auditing log source in QRadar	826
Salesforce Security Monitoring	826
Configuring the Salesforce Security Monitoring server to communicate with QRadar	827
Configuring a Salesforce Security Monitoring log source in QRadar	828
124 Samhain Labs	831
Configuring syslog to collect Samhain events	831
Configuring JDBC to collect Samhain events	832
125 Seculert	835
Obtaining an API key	836
126 Sentrigo Hedgehog	837
127 Skyhigh Networks Cloud Security Platform	839
Configuring Skyhigh Networks Cloud Security Platform to communicate with QRadar	840
128 SolarWinds Orion	841
Configuring SolarWinds Orion to communicate with QRadar	842
Configuring a SolarWinds Orion log source by using the SNMP protocol	844
Installing the Java Cryptography Extension on QRadar	846
129 SonicWALL	847
Configuring SonicWALL to forward syslog events	847
Configuring a log source	847
130 Sophos	849
Sophos Enterprise Console	849
Configuring QRadar using the Sophos Enterprise Console Protocol	849
Configure IBM Security QRadar by using the JDBC protocol	851
Configuring the database view	852
Configuring a JDBC log source in QRadar	852
Sophos PureMessage	854
Integrating QRadar with Sophos PureMessage for Microsoft Exchange	855
Configure a JDBC log source for Sophos PureMessage	855
Integrating QRadar with Sophos PureMessage for Linux	857
Configuring a log source for Sophos PureMessage for Microsoft Exchange	858
Sophos Astaro Security Gateway	860
Sophos Web Security Appliance	861
131 Splunk	863
Collect Windows events that are forwarded from Splunk appliances	863
Configuring a log source for Splunk forwarded events	863
132 Squid Web Proxy	867
Configuring syslog forwarding	867
Create a log source	868
133 SSH CryptoAuditor	869
Configuring an SSH CryptoAuditor appliance to communicate with QRadar	870
134 Starent Networks	871
135 STEALTHbits	875
STEALTHbits StealthINTERCEPT	875

Configuring a STEALTHbits StealthINTERCEPT log source in IBM Security QRadar	875
Configuring your STEALTHbits StealthINTERCEPT to communicate with QRadar	875
Configuring your STEALTHbits File Activity Monitor to communicate with QRadar	876
Configuring a log source for STEALTHbits File Activity Monitor in QRadar	876
STEALTHbits StealthINTERCEPT Alerts	878
Collecting alerts logs from STEALTHbits StealthINTERCEPT	879
STEALTHbits StealthINTERCEPT Analytics	880
Collecting analytics logs from STEALTHbits StealthINTERCEPT	881
136 Sun	883
Sun ONE LDAP	883
Enabling the event log for Sun ONE Directory Server	883
Configuring a log source for Sun ONE LDAP	884
Configuring a UDP Multiline Syslog log source	887
Sun Solaris DHCP	888
Configuring Sun Solaris DHCP	888
Configuring Sun Solaris	889
Sun Solaris Sendmail	889
Configuring a Sun Solaris Sendmail log source	890
Sun Solaris Basic Security Mode (BSM)	891
Enabling Basic Security Mode in Solaris 10	891
Enabling Basic Security Mode in Solaris 11	891
Converting Sun Solaris BSM audit logs	892
Creating a cron job	893
Configuring a log source for Sun Solaris BSM	893
137 Sybase ASE	897
Configuring IBM Security QRadar SIEM to receive events from a Sybase ASE device	898
138 Symantec	899
Symantec Critical System Protection	899
Symantec Data Loss Prevention (DLP)	900
Creating an SMTP response rule	900
Creating a None Of SMTP response rule	901
Configuring a log source	902
Event map creation for Symantec DLP events	902
Discovering unknown events	902
Modifying the event map	903
Symantec Endpoint Protection	904
Configuring Symantec Endpoint Protection to Communicate with QRadar	905
Symantec PGP Universal Server	906
Configuring syslog for PGP Universal Server	906
Configuring a log source	906
Symantec SGS	907
Symantec System Center	907
Configuring a database view for Symantec System Center	908
Configuring a log source	908
139 Sourcefire Intrusion Sensor	911
Configuring Sourcefire Intrusion Sensor	911
Configuring a log source for Cisco FireSIGHT Management Center events	911
140 ThreatGRID Malware Threat Intelligence Platform	913
Supported event collection protocols for ThreatGRID Malware Threat Intelligence	913
ThreatGRID Malware Threat Intelligence configuration overview	913
Configuring a ThreatGRID syslog log source	913
Configuring a ThreatGRID log file protocol log source	914
141 TippingPoint	919
Tipping Point Intrusion Prevention System	919
Configure remote syslog for SMS	919
Configuring notification contacts for LSM	920
Configuring an Action Set for LSM	920
Tipping Point X505/X506 Device	921
Configuring syslog	921
142 Top Layer IPS	923
143 Townsend Security LogAgent	925
Configuring Raz-Lee iSecurity	925
Configuring a log source	925
144 Trend Micro	927
Trend Micro Control Manager	927
Configuring a log source	927
Configuring SNMP traps	928
Trend Micro Deep Discovery Analyzer	928
Configuring your Trend Micro Deep Discovery Analyzer instance for communication with QRadar	929
Trend Micro Deep Discovery Email Inspector	930
Configuring Trend Micro Deep Discovery Email Inspector to communicate with QRadar	931
Trend Micro Deep Discovery Inspector	932
Configuring Trend Micro Deep Discovery Inspector V3.0 to send events to QRadar	933
Configuring Trend Micro Deep Discovery Inspector V3.8 to send Events to QRadar	933
Trend Micro Deep Security	934
Configuring Trend Micro Deep Security to communicate with QRadar	935
Trend Micro InterScan VirusWall	936
Trend Micro Office Scan	936
Integrating with Trend Micro Office Scan 8.x	936
Integrating with Trend Micro Office Scan 10.x	937
Configuring General Settings	937
Configure Standard Notifications	938
Configuring Outbreak Criteria and Alert Notifications	938
Integrating with Trend Micro OfficeScan XG	939
Configuring General Settings in OfficeScan XG	939

Configuring Administrator Notifications in OfficeScan XG	939
Configuring Outbreak Notifications in OfficeScan XG	940
145 Tripwire	941
146 Tropos Control	943
147 Universal	945
Universal CEF	945
Configuring event mapping for Universal CEF events	946
Universal LEEF	947
Configuring a Universal LEEF log source	947
Configuring the log file protocol to collect Universal LEEF events	948
Forwarding events to IBM Security QRadar	950
Universal LEEF event map creation	951
Discovering unknown events	951
Modifying an event map	951
148 Vectra Networks Vectra	953
Configuring Vectra Networks Vectra to communicate with QRadar	954
149 Venustech Venusense	955
Venusense configuration overview	955
Configuring a Venusense syslog server	955
Configuring Venusense event filtering	955
Configuring a Venusense log source	956
150 Verdasys Digital Guardian	957
Configuring IPtables	957
Configuring a data export	958
Configuring a log source	959
151 Vericept Content 360 DSM	961
152 VMWare	963
VMware ESX and ESXi	963
Configuring syslog on VMware ESX and ESXi servers	963
Enabling syslog firewall settings on vSphere Clients	964
Enabling syslog firewall settings on vSphere Clients by using the esxcli command	964
Configuring a syslog log source for VMware ESX or ESXi	964
Configuring the EMC VMWare protocol for ESX or ESXi servers	965
Creating an account for QRadar in ESX	965
Configuring read-only account permissions	966
Configuring a log source for the EMC VMWare protocol	966
VMware vCenter	967
Configuring a log source for the VMware vCenter	967
VMware vCloud Director	967
Configuring the vCloud REST API public address	968
Supported VMware vCloud Director event types logged by IBM Security QRadar	968
Configuring a VMware vCloud Director log source in IBM Security QRadar	969
VMware vShield	970
VMware vShield DSM integration process	970
Configuring your VMware vShield system for communication with IBM Security QRadar	971
Configuring a VMware vShield log source in IBM Security QRadar	971
153 Vormetric Data Security	973
Vormetric Data Security DSM integration process	973
Configuring your Vormetric Data Security systems for communication with IBM Security QRadar	974
Configuring Vormetric Data Firewall FS Agents to bypass Vormetric Data Security Manager	974
Configuring a Vormetric Data Security log source in IBM Security QRadar	975
154 WatchGuard Fireware OS	977
Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar	977
Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar	978
Configuring a WatchGuard Fireware OS log source in QRadar	979
155 Websense	981
156 Zscaler Nanolog Streaming Service	983
Configuring a syslog feed in Zscaler NSS	983
Configuring a Zscaler NSS log source	984
157 QRadar supported DSMs	987
Part 4. Appendixes	
Notices	1003
Trademarks	1004
Terms and conditions for product documentation	1005
IBM Online Privacy Statement	1005
Privacy policy considerations	1006
Glossary	1007
A	1007
B	1007
C	1007
D	1008
E	1008
F	1008
G	1009
H	1009

I	1009	R	1011
K	1009	S	1012
L	1009	T	1012
M	1010	V	1012
N	1010	W	1013
O	1010		
P	1011	Index	1015
Q	1011		

About this DSM Configuration Guide

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

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/knowledgecenter/SS42VS/welcome>).

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

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (<http://www.ibm.com/support/docview.wss?uid=swg21616144>).

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

1 Event collection from third-party devices

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

Log sources

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

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

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 Security 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 security devices that QRadar does not provide a corresponding DSM, you can use the Universal DSM. QRadar can integrate with most devices and any common protocol sources by using the *Universal DSM*.

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

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

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:

8, “3Com Switch 8800,” on page 95

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

10, “Akamai Kona,” on page 99

The IBM Security QRadar DSM for Akamai KONA collects event logs from your Akamai KONA servers.

Adding a log source

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

About this task

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

Table 1. Log source parameters

Parameter	Description
Log Source Identifier	<p>The IPv4 address or host name that identifies the log source.</p> <p>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.</p>
Enabled	When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
Credibility	Credibility is a representation of the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events or adjusted as a response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	<p>Specifies the QRadar Event Collector that polls the remote log source.</p> <p>Use this parameter in a distributed deployment to improve Console system performance by moving the polling task to an Event Collector.</p>
Coalescing Events	<p>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.</p> <p>When this check box is clear, events are viewed individually and events are not bundled.</p> <p>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.</p>

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:

8, "3Com Switch 8800," on page 95

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

10, "Akamai Kona," on page 99

The IBM Security QRadar DSM for Akamai KONA collects event logs from your Akamai KONA servers.

Adding bulk log sources

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

Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. From the **Bulk Actions** list, select **Bulk Add**.
4. Configure the parameters for the bulk log source.
 - File Upload - Upload a text file that has one host name or IP per line
 - Manual - Enter the host name or IP of the host that you wish to add
5. Click **Save**.
6. Click **Continue** to add the log sources.
7. On the **Admin** tab, click **Deploy Changes**.

Adding a log source parsing order

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

About this task

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

Procedure

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

Part 2. Log sources

2 Introduction to log source management

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

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

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

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

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

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

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

[“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](#)

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

3 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 2. Log source parameters

Parameter	Description
Log Source Identifier	<p>The IPv4 address or host name that identifies the log source.</p> <p>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.</p>
Enabled	When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
Credibility	Credibility is a representation of the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events or adjusted as a response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	<p>Specifies the QRadar Event Collector that polls the remote log source.</p> <p>Use this parameter in a distributed deployment to improve Console system performance by moving the polling task to an Event Collector.</p>
Coalescing Events	<p>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.</p> <p>When this check box is clear, events are viewed individually and events are not bundled.</p> <p>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.</p>

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:

8, “3Com Switch 8800,” on page 95

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

10, “Akamai Kona,” on page 99

The IBM Security QRadar DSM for Akamai KONA collects event logs from your Akamai KONA servers.

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 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 3. Blue Coat Web Security Service REST API protocol parameters

Parameter	Description
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	Confirmation of the Password field.
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)	If you select Yes from the list, QRadar downloads the certificate and begins trusting the target server.
Recurrence	You can specify when the log collects data. The format is M/H/D for Months/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.

Cisco Firepower eStreamer protocol configuration options

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

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

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

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

Table 4. Cisco Firepower eStreamer protocol parameters

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

Cisco NSEL protocol configuration options

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

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

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

Table 5. Cisco NSEL protocol parameters

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

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.

IBM Security 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 6. EMC VMware protocol parameters

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

Forwarded protocol configuration options

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

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

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 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 7. HTTP Receiver protocol parameters

Parameter	Description
Protocol Configuration	From the list, select HTTP Receiver .
Log Source Identifier	The IP address, host name, or any name to identify the device. Must be unique for the log source type.
Communication Type	Select HTTP , or HTTPs , or HTTPs and Client Authentication .
Client Certificate Path	If you select HTTPs and Client Authentication 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.
Listen Port	The port that is used by QRadar to accept incoming HTTP Receiver events. The default port is 12469.
Message Pattern	Denotes the start of each event.
EPS Throttle	The maximum number of events per second (EPS) that you do not want this protocol to exceed. The default is 5000.

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 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 8. IBM BigFix SOAP protocol parameters

Parameter	Description
Protocol Configuration	IBM BigFix SOAP

Table 8. IBM BigFix SOAP protocol parameters (continued)

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

JDBC protocol configuration options

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

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

Table 9. JDBC protocol parameters

Parameter	Description
Log Source Name	Type a unique name for the log source.
Log Source Description	Type a description for the log source.
Log Source Type	Select your Device Support Module (DSM) that uses the JDBC protocol from the Log Source Type list.
Protocol Configuration	JDBC
Log Source Identifier	The Log Source Identifier value must follow the <database name>@<ip or hostname> format. The <database name> must match the Database Name parameter value and <ip or hostname> must match the IP or Hostname parameter value. Note: If you have more than one JDBC log source of the same log source type that connects to the same database on the same host, the Log Source Identifier value must follow the <table name> <database name>@<ip or hostname> format. The <table name> must match the Table Name parameter value.
Database Type	Select the type of database that contains the events.
Database Name	The database name must match the database name that is specified in the Log Source Identifier field.
IP or Hostname	The IP address or host name of the database server.

Table 9. JDBC protocol parameters (continued)

Parameter	Description
Port	<p>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.</p> <p>The defaults are:</p> <ul style="list-style-type: none"> • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Sybase - 1521 • Oracle - 1521 • Informix® - 9088 • DB2® - 50000 <p>If a database instance is used with the MSDE database type, you must leave the Port field blank.</p>
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.
Authentication Domain (MSDE only)	The domain for MSDE databases that are a Windows domain. If your network does not use a domain, leave this field blank.
Database Instance (MSDE or Informix only)	<p>The database instance, if required. MSDE databases can include multiple SQL server instances on one server.</p> <p>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>
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 9. JDBC protocol parameters (continued)

Parameter	Description
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 The maximum polling interval is one week.
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.
Use Named Pipe Communication (MSDE only)	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.
Database Cluster Name (MSDE only)	This field appears if the Use Named Pipe Communication box is selected. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.
Use NTLMv2 (MSDE only)	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.
Use SSL (MSDE only)	Select this option if your connection supports SSL. This option appears only for MSDE.
Use Oracle Encryption	<i>Oracle Encryption and Data Integrity settings</i> is also known as <i>Oracle Advanced Security</i> . If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.
Database Locale (Informix only)	For multilingual installations, use this field to specify the language to use.
Code-Set (Informix only)	This field appears after you choose a language for multilingual installations. Use this field to specify the character set to use.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	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.
Target Event Collector	Select the Target Event Collector to use as the target for the log source.
Coalescing Events	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.
Store Event Payload	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.

Related information:

-  [Configuring JDBC Over SSL with a Self-signed Certificate](#)
-  [Configuring JDBC Over SSL with an Externally-signed Certificate](#)

JDBC SiteProtector configuration options

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

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

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

Table 10. JDBC - SiteProtector protocol parameters

Parameter	Description
Protocol Configuration	JDBC - SiteProtector
Database Type	From the list, select MSDE as the type of database to use for the event source.
Database Name	Type RealSecureDB the name of the database to which the protocol can connect.
IP or Hostname	The IP address or host name of the database server.
Port	The port number that is used by the database server. The JDBC SiteProtector configuration port must match the listener port of the database. The database must have incoming TCP connections enabled. If you define a Database Instance when with MSDE as the database type, you must leave the Port parameter blank in your log source configuration.
Username	If you want to track access to a database by the JDBC protocol, you can create a specific user for your QRadar system.
Authentication Domain	If you select MSDE and the database is configured for Windows, you must define a Windows domain. If your network does not use a domain, leave this field blank.
Database Instance	If you select MSDE and you have multiple SQL server instances on one server, define the instance to which you want to connect. If you use a non-standard port in your database configuration, or access is blocked to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Predefined Query	The predefined database query for your log source. Predefined database queries are only available for special log source connections.
Table Name	SensorData1
AVP View Name	SensorDataAVP
Response View Name	SensorDataResponse
Select List	Type * to include all fields from the table or view.
Compare Field	SensorDataRowID

Table 10. JDBC - SiteProtector protocol parameters (continued)

Parameter	Description
Use Prepared Statements	Prepared statements allow the JDBC protocol source to set up the SQL statement, and then execute the SQL statement numerous times with different parameters. For security and performance reasons, use prepared statements. You can clear this check box to use an alternative method of querying that does not use pre-compiled statements.
Include Audit Events	Specifies to collect audit events from IBM SiteProtector®.
Start Date and Time	Optional. A start date and time for when the protocol can start to poll the database.
Polling Interval	The amount of time between queries to the event table. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. Numeric values without an H or M designator poll in seconds.
EPS Throttle	The number of Events Per Second (EPS) that you do not want this protocol to exceed.
Database Locale	For multilingual installations, use the Database Locale field to specify the language to use.
Database Codeset	For multilingual installations, use the Codeset field to specify the character set to use.
Use Named Pipe Communication	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.
Database Cluster Name	The cluster name to ensure that named pipe communications function properly.
Use NTLMv2	Forces MSDE connections to use the NTLMv2 protocol with SQL servers that require NTLMv2 authentication. The Use NTLMv2 check box does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
Use SSL	Enables SSL encryption for the JDBC protocol.
Log Source Language	Select the language of the events that are generated by the log source. The log source language helps the system parse events from external appliances or operating systems that can create events in multiple languages.

Juniper Networks NSM protocol configuration options

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

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

Table 11. 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 12. Juniper Security Binary Log Collector protocol parameters

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

Log File protocol configuration options

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

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

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

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

Table 13. Log File protocol parameters

Parameter	Description
Protocol Configuration	Log File
Remote Port	If the remote host uses a non-standard port number, you must adjust the port value to retrieve events.
SSH Key File	The path to the SSH key, if the system is configured to use key authentication. When an SSH key file is used, the Remote Password field is ignored.
Remote Directory	For FTP, if the log files are in the remote user's home directory, you can leave the remote directory blank. A blank remote directory field supports systems where a change in the working directory (CWD) command is restricted.

Table 13. Log File protocol parameters (continued)

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

Microsoft Azure Event Hubs protocol configuration options

The Microsoft Azure Event Hubs 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 14. Microsoft Azure Event Hubs log source parameters

Parameter	Value
Log Source type	Microsoft Azure
Protocol Configuration	Microsoft Azure Event Hubs
Log Source Identifier	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.

Table 14. Microsoft Azure Event Hubs log source parameters (continued)

Parameter	Value
Use as a Gateway Log Source	Enable this check box to send all events through the QRadar Traffic Analysis Engine and automatically detect one or more appropriate log sources.
Use Event Hub Connection String	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.
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.
Namespace Name	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.
Event Hub Name	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.
SAS Key Name	The Shared Access Signature (SAS) Name identifies the event publisher.
SAS Key	The Shared Access Signature (SAS) Key authenticates the event publisher.
Consumer Group	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.
Use Storage Account Connection String	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 .
Storage Account Connection String	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.
Storage Account Name	The Storage Account Name is part of the authentication process that is required to access data in the Azure Storage Account.
Storage Account Key	The Storage Account Key is part of the authentication process that is required to access data in the Azure Storage Account.
Automatically Acquire Server Certificate(s)	Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.
EPS Throttle	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.

Microsoft DHCP protocol configuration options

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

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

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

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

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

Table 15. Microsoft DHCP protocol parameters

Parameter	Description
Protocol Configuration	Microsoft DHCP
Log Source Identifier	Type a unique hostname or other identifier unique to the log source.
Server Address	The IP address or host name of your Microsoft DHCP server.
Domain	Type the domain for your Microsoft DHCP server. This parameter is optional if your server is not in a domain.
Username	Type the user name that is required to access the DHCP server.
Password	Type the password that is required to access the DHCP server.
Confirm Password	Confirm the password that is required to access the server.
Folder Path	The directory path to the DHCP log files. The default is c\$/WINDOWS/system32/dhcp/
File Pattern	The regular expression (regex) that identifies event logs. The log files must contain a three-character abbreviation for a day of the week. Use one of the following file patterns: English: <ul style="list-style-type: none">IPv4 file pattern: DhcpSrvLog-(?:Sun Mon Tue Wed Thu Fri Sat)\.log.IPv6 file pattern: DhcpV6SrvLog-(?:Sun Mon Tue Wed Thu Fri Sat)\.log.Mixed IPv4 and IPv6 file pattern: Dhcp.*SrvLog-(?:Sun Mon Tue Thu Fri Sat)\.log. Polish: <ul style="list-style-type: none">IPv4 file pattern: DhcpSrvLog-(?:Pią Pon Sob Wto Śro Czw Nie)\.logIPv6 file pattern: DhcpV6SrvLog-(?:Pt Pon So Wt Śr Czw Nie)\.log
Recursive	Select this option if you want the file pattern to search the sub folders.

Table 15. Microsoft DHCP protocol parameters (continued)

Parameter	Description
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)	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.
Throttle events/sec	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.
File Encoding	The character encoding that is used by the events in your log file.
Enabled	When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
Credibility	Credibility is a representation of the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events or adjusted as a response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	Specifies the QRadar Event Collector that polls the remote log source. Use this parameter in a distributed deployment to improve Console system performance by moving the polling task to an Event Collector.
Coalescing Events	Increases the event count when the same event occurs multiple times within a short time interval. Coalesced events provide a way to view and determine the frequency with which a single event type occurs on the Log Activity tab. When this check box is clear, events are viewed individually and events are not bundled. New and automatically discovered log sources inherit the value of this check box from the System Settings configuration on the Admin tab. You can use this check box to override the default behavior of the system settings for an individual log source.

Microsoft Exchange protocol configuration options

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

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

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

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

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

Table 16. Microsoft Exchange protocol parameters

Parameter	Description
Protocol Configuration	Microsoft Exchange
Log Source Identifier	Type the IP address, host name, or name to identify your log source.
Server Address	The IP address or host name of your Microsoft Exchange server.
Domain	Type the domain for your Microsoft Exchange server. This parameter is optional if your server is not in a domain.
Username	Type the user name that is required to access your server.
Password	Type the password that is required to access your server.
Confirm Password	Confirm the password that is required to access the server.
SMTP Log Folder Path	When the folder path is clear, SMTP event collection is disabled.
OWA Log Folder Path	When the folder path is clear, OWA event collection is disabled.
MSGTRK Log Folder Path	Message tracking is available on Microsoft Exchange 2007 or 2010 servers assigned the Hub Transport, Mailbox, or Edge Transport server role.
File Pattern	The regular expression (regex) that identifies the event logs. The default is <code>.*\.(?:log LOG)</code> .
Force File Read	If the check box is cleared, the log file is read only when QRadar detects a change in the modified time or file size.
Recursive	If you want the file pattern to search sub folders, use this option. By default, the check box is selected.
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/Second	The maximum number of events the Exchange protocol can forward per second.
File Encoding	The character encoding that is used by the events in your log file.

Microsoft IIS protocol configuration options

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

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

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

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

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

Table 17. Microsoft IIS protocol parameters

Parameter	Description
Protocol Configuration	Microsoft IIS
Log Source Identifier	Type the IP address, host name, or name to identify your log source.
Server Address	The IP address or host name of your Microsoft IIS server.
Domain	Type the domain for your Microsoft IIS server. This parameter is optional if your server is not in a domain.
Username	Type the user name that is required to access your server.
Password	Type the password that is required to access your server.
Confirm Password	Confirm the password that is required to access the server.
Log Folder Path	The directory path to access the log files. For example, administrators can use the c\$/LogFiles/ directory for an administrative share, or the LogFiles/directory for a public share folder path. However, the c:/LogFiles directory is not a supported log folder path. If a log folder path contains an administrative share (C\$), users with NetBIOS access on the administrative share (C\$) have the privileges that are required to read the log files. Local system or domain administrator privileges are also sufficient to access a log files that are on an administrative share.
File Pattern	The regular expression (regex) that identifies the event logs.
Recursive	If you want the file pattern to search sub folders, use this option. By default, the check box is selected.
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/Second	The maximum number of events the IIS protocol can forward per second.
File Encoding	The character encoding that is used by the events in your log file.

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 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 18. Microsoft Security Event Log protocol parameters

Parameter	Description
Protocol Configuration	Windows Security Event Log

Microsoft Security Event Log over MSRPC Protocol

The Microsoft Security Event Log over MSRPC protocol (MSRPC) 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 19. Supported features of the MSRPC protocol

Features	Microsoft Security Event Log over MSRPC protocol
Manufacturer	Microsoft
Connection test tool	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 (http://www.ibm.com/support/docview.wss?uid=swg21959348)
Protocol type	<p>The operating system dependent type of the remote procedure protocol for collection of events.</p> <p>Select one of the following options from the Protocol Type list:</p> <p>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.</p> <p>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.</p> <p>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.</p>
Maximum EPS rate	100 EPS / Windows host
Maximum overall EPS rate of MSRPC	8500 EPS / IBM Security QRadar 16xx or 18xx appliance
Maximum number of supported log sources	500 log sources / QRadar 16xx or 18xx appliance
Bulk log source support	Yes
Encryption	Yes

Table 19. Supported features of the MSRPC protocol (continued)

Features	Microsoft Security Event Log over MSRPC protocol
Supported event types	Application System Security DNS Server File Replication Directory Service logs
Supported Windows Operating Systems	Windows Server 2012 (most recent) Windows Server 2008 (most recent) Windows 8.1 Windows 8 Windows 7 Windows Vista MSRPC is not supported on versions of Microsoft Windows with end of life status such as Windows 2003 and Windows XP.
Required permissions	<p>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.</p> <p>Windows XP and 2003 operating system users require read access to the following registry keys:</p> <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language • HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion <p>QRadar provides no support for Windows 2003 integrations because this operating system has reached its end of life.</p>
Required RPM files	PROTOCOL-WindowsEventRPC-QRadar_release-Build_number.noarch.rpm DSM-MicrosoftWindows-QRadar_release-Build_number.noarch.rpm DSM-DSMCommon-QRadar_release-Build_number.noarch.rpm

Table 19. Supported features of the MSRPC protocol (continued)

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

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

Table 20. Contrast between MSRPC and WMI/DCOM event rates

Name	Protocol type	Maximum event rate
Microsoft Security Event Log	WMI/DCOM	50EPS / Windows host
Microsoft Security Event Log over MSRPC	MSRPC	100EPS / Windows host

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 Security QRadar as **MQ JMS**.

IBM MQ is supported.

The MQ protocol 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 21. MQ protocol parameters

Parameter	Description
Protocol Name	MQ JMS
IP or Hostname	The IP address or host name of the primary queue manager.
Port	The default port that is used for communicating with the primary queue manager is 1414.
Standby IP or Hostname	The IP address or host name of the standby queue manager.
Standby Port	The port that is used to communicate with the standby queue manager.
Queue Manager	The name of the queue manager.
Channel	The channel through which the queue manager sends messages. The default channel is SYSTEM.DEF.SVRCONN.
Queue	The queue or list of queues to monitor. A list of queues is specified with a comma-separated list.
Username	The user name that is used for authenticating with the MQ service.
Password	Optional: The password that is used to authenticate with the MQ service.
Incoming Message Encoding	The character encoding that is used by incoming messages.
Process Computational Fields	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.
CopyBook File Name	The name of the CopyBook file to use for processing data. The CopyBook file must be placed in /store/ec/mqjms/*
Event Formatter	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.
Include JMS Message Header	Select this option to include a header in each generated event containing JMS message fields such as the JMSMessageID and JMSTimestamp.
EPS Throttle	The upper limit for the maximum number of events per second (EPS).

Related concepts:

“Creating a log source extensions document to get data into QRadar” on page 70

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 71

The first step in building a Universal DSM is to create the log source in IBM Security 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 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 22. Okta REST API protocol parameters

Parameter	Description
IP or Hostname	oktprise.okta.com
Authentication Token	A single authentication token that is generated by the Okta console and must be used for all API transactions.
Use Proxy	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.
Automatically Acquire Server Certificate(s)	If you select Yes from the list, QRadar downloads the certificate and begins trusting the target server.
Recurrence	You can specify when the log source collects data. The format is M/H/D for Months/Hours/Days. The default is 1 M.
EPS Throttle	The maximum limit for the number of events per second.

OPSEC/LEA protocol configuration options

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

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

Table 23. OPSEC/LEA protocol parameters

Parameter	Description
Protocol Configuration	OPSEC/LEA
Log Source Identifier	The IP address, host name, or any name to identify the device. Must be unique for the log source type.
Server IP	Type the IP address of the server.
Server Port	The port number that is used for OPSEC communication. The valid range is 0 - 65,536 and the default is 18184.
Use Server IP for Log Source	Select the Use Server IP for Log Source check box if you want to use the LEA server IP address instead of the managed device IP address for a log source. By default, the check box is selected.
Statistics Report Interval	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 interval is 600.
Authentication Type	From the list, select the Authentication Type 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.
OPSEC Application Object SIC Attribute (SIC Name)	The Secure Internal Communications (SIC) name is the distinguished name (DN) of the application; for example: CN=LEA, o=fwconsole..7psaxx.
Log Source SIC Attribute (Entity SIC Name)	The SIC name of the server, for example: cn=cp_mgmt, o=fwconsole..7psaxx.
Specify Certificate	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.

Table 23. OPSEC/LEA protocol parameters (continued)

Parameter	Description
Certificate Filename	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.
Certificate Authority IP	Type the Check Point Manager Server IP address.
Pull Certificate Password	Type the activation key password.
OPSEC Application	The name of the application that makes the certificate request.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	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.
Target Event Collector	From the list, select the Target Event Collector to use as the target for the log source.
Coalescing Events	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.
Store Event Payload	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.

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.

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 24. Oracle Database Listener protocol parameters

Parameter	Description
Protocol Configuration	Oracle Database Listener
Log Source Identifier	Type the IP address, host name, or name to identify your log source.

Table 24. Oracle Database Listener protocol parameters (continued)

Parameter	Description
Server Address	The IP address or host name of your Oracle Database Listener server.
Domain	Type the domain for your Oracle Database Learner server. This parameter is optional if your server is not in a domain.
Username	Type the user name that is required to access your server.
Password	Type the password that is required to access your server.
Confirm Password	Confirm the password that is required to access the server.
Log Folder Path	Type the directory path to access the Oracle Database Listener log files.
File Pattern	The regular expression (regex) that identifies the event logs.
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	If you want the file pattern to search sub folders, use this option. By default, the check box is selected.
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.

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 25. PCAP Syslog Combination protocol parameters

Parameter	Description
Log Source Name	Type a unique name of the log source.
Log Source Description	Optional. Type a description for the log source.
Log Source Type	From the list, you can select either Juniper SRX Series Services Gateway or Juniper Junos OS Platform .
Protocol Configuration	From the list, select PCAP Syslog Combination .
Log Source Identifier	<p>Type an IP address, host name, or name to identify the Juniper SRX Series Services Gateway or Juniper Junos OS Platform appliance.</p> <p>The log source identifier must be unique for the log source type.</p>
Incoming PCAP Port	<p>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.</p> <p>To edit the Incoming PCAP Port number, complete the following steps:</p> <ol style="list-style-type: none"> 1. Type the new port number for receiving PCAP data 2. Click Save. <p>The port update is complete and event collection starts on the new port number.</p>
Enabled	<p>Select this check box to enable the log source.</p> <p>When this check box is clear, the log source does not collect events and the log source is not counted in the license limit.</p>
Credibility	<p>Select the credibility of the log source. The range is 0 (lowest) - 10 (highest). The default credibility is 5.</p> <p>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.</p>
Target Event Collector	<p>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.</p> <p>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.</p>
Coalescing Events	<p>Select this check box to enable the log source to coalesce (bundle) events.</p> <p>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.</p> <p>When this check box is clear, the events are displayed individually and the information is not bundled.</p> <p>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.</p>

Table 25. PCAP Syslog Combination protocol parameters (continued)

Parameter	Description
Store Event Payload	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.
Log Source Extension	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).
Extension Use Condition	From the list box, select the use condition for the log source extension. The options include: <ul style="list-style-type: none"> 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.
Groups	Select one or more groups for the log source.

SDEE protocol configuration options

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

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

Table 26. SDEE protocol parameters

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

SMB Tail protocol configuration options

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

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

Table 27. SMB Tail protocol parameters

Parameter	Description
Protocol Configuration	SMB Tail
Server Address	The IP address or host name of your SMB Tail server.
Domain	Type the domain for your SMB Tail server. This parameter is optional if your server is not in a domain.
Username	Type the user name that is required to access your server.
Password	Type the password that is required to access your server.
Confirm Password	Confirm the password that is required to access the server.
Log Folder Path	The directory path to access the log files. For example, administrators can use the c\$/LogFiles/ directory for an administrative share, or the LogFiles/ directory for a public share folder path. However, the c:/LogFiles directory is not a supported log folder path. If a log folder path contains an administrative share (C\$), users with NetBIOS access on the administrative share (C\$) have the privileges that are required to read the log files. Local system or domain administrator privileges are also sufficient to access a log files that are on an administrative share.
File Pattern	The regular expression (regex) that identifies the event logs.
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.
Force File Read	If the check box is cleared, the log file is read only when QRadar detects a change in the modified time or file size.
Recursive	If you want the file pattern to search sub folders, use this option. 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 default is 10 seconds.
Throttle Events/Second	The maximum number of events the SMB Tail protocol forwards per second.
File Encoding	The character encoding that is used by the events in your log file.

SNMPv2 protocol configuration options

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

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

Table 28. SNMPv2 protocol parameters

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

SNMPv3 protocol configuration options

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

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

Table 29. SNMPv3 protocol parameters

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

Seculert Protection REST API protocol configuration options

To receive events from Seculert, configure a log source to use the Seculert Protection REST API 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 30. Seculert Protection REST API protocol parameters

Parameter	Description
Log Source Type	Seculert

Table 30. Seculert Protection REST API protocol parameters (continued)

Parameter	Description
Protocol Configuration	Seculert Protection REST API
Log Source Identifier	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.
API Key	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.
Use Proxy	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.
Automatically Acquire Server Certificate(s)	If you select Yes from the list, QRadar downloads the certificate and begins trusting the target server.
Recurrence	Specify when the log collects data. The format is M/H/D for Months/Hours/Days. The default is 1 M.
EPS Throttle	The upper limit for the maximum number of events per second (eps) for events that are received from the API.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	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.
Target Event Collector	Select the Target Event Collector to use as the target for the log source.
Coalescing Events	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.
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.

Sophos Enterprise Console JDBC protocol configuration options

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

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

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

Table 31. Sophos Enterprise Console JDBC protocol parameters

Parameter	Description
Protocol Configuration	Sophos Enterprise Console JDBC
Database Type	MSDE
Database Name	The database name must match the database name that is specified in the Log Source Identifier field.
Port	<p>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.</p> <p>If a Database Instance is used with the MSDE database type, you must leave the Port parameter blank.</p>
Authentication Domain	If your network does not use a domain, leave this field blank.
Database Instance	<p>The database instance, if required. MSDE databases can include multiple SQL server instances on one server.</p> <p>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.</p>
Table Name	vEventsCommonData
Select List	*
Compare Field	InsertedAt
Use Prepared Statements	Prepared statements enable the protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most configurations can use prepared statements. Clear this check box to use an alternative method of querying that do not use pre-compiled statements.
Start Date and Time	Optional. A start date and time for when the protocol can start to poll the database. If a start time is not defined, the protocol attempts to poll for events after the log source configuration is saved and deployed.
Polling Interval	The polling interval, which is the amount of time between queries to the database. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.
EPS Throttle	The number of Events Per Second (EPS) that you do not want this protocol to exceed.
Use Named Pipe Communication	<p>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.</p> <p>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.</p>
Database Cluster Name	If you use your SQL server in a cluster environment, define the cluster name to ensure that named pipe communications function properly.

Table 31. Sophos Enterprise Console JDBC protocol parameters (continued)

Parameter	Description
Use NTLMv2	Forces MSDE connections to use the NTLMv2 protocol with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. The Use NTLMv2 check box does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.

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 used as an alternative to the Syslog protocol. Use this protocol to override how QRadar determines the source of a syslog event.

The standard syslog protocol listener on port 514 automatically parses the host name or IP from a standard syslog header and recognizes it as the source value of the event. If an event does not have a standard header, the source IP of the packet it arrived on is used as the source value.

If events are sent to QRadar through an intermediary system, such as a syslog forwarder, aggregator, load balancer, third-party log management, or SIEM system, the packet IP is that of the intermediary. Syslog Redirect addresses this issue by determining the source value from elsewhere in the event payload.

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

Table 32. Syslog Redirect protocol parameters

Parameter	Description
Protocol Configuration	Syslog Redirect
Log Source Identifier Regex	Enter a regex (regular expression) to capture one or more values from event payloads that are handled by this protocol. These values are used with the Log Source Identifier Regex Format 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.
Log Source Identifier Regex Format 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: <ul style="list-style-type: none">• One or more capture groups from the Log Source Identifier Regex. To refer to a capture group, use \x notation where x is the index of a capture group from the Log Source Identifier 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 Log Source Identifier Regex Format String can be user-provided text. For example, if the Log Source Identifier Regex is 'hostname=(.?)' and you want to append hostname.com to the capture group 1 value, set the Log Source Identifier Regex Format 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.

Table 32. Syslog Redirect protocol parameters (continued)

Parameter	Description
Perform DNS Lookup On Regex Match	Select this check box to allow the protocol to perform DNS lookups on source values (as set by the Log Source Identifier Regex and Log Source Identifier Format String parameters) to convert host names into IP addresses. If left clear, the source value remains as-is. By default, the check box is not selected. Note: If you enable the Perform DNS Lookup on Regex Match option, it might slow the performance of the Syslog Redirect protocol.
Listen Port	517 is the default port. Any port can be used for listening, other than port 514 as it is used by the standard Syslog listener.
Protocol	You can select either UDP or TCP .

TCP multiline syslog protocol configuration options

You can configure a log source that uses the TCP multiline syslog protocol. This protocol uses regular expressions to identify the start and end pattern of multiline events.

The following example is a multiline event:

```
06/13/2012 08:15:15 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5156
EventType=0
TaskCategory=Filtering Platform Connection
Keywords=Audit Success
Message=The Windows Filtering Platform permitted a connection.
Process ID: 4
Application Name: System
Direction: Inbound
Source Address: <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 33. TCP multiline syslog protocol parameters

Parameter	Description
Protocol Configuration	TCP Multiline Syslog
Log Source Identifier	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 .
Listen Port	The default port is 12468.
Aggregation Method	The default is Start/End Matching . Use ID-Linked if you want to combine multiline events that are joined by a common identifier.

Table 33. TCP multiline syslog protocol parameters (continued)

Parameter	Description
Event Start Pattern	<p>This parameter is available when you set the Aggregation Method parameter to Start/End Matching.</p> <p>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>
Event End Pattern	<p>This parameter is available when you set the Aggregation Method parameter to Start/End Matching.</p> <p>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.</p>
Message ID Pattern	<p>This parameter is available when you set the Aggregation Method parameter to ID-Linked.</p> <p>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.</p>
Event Formatter	Use the Windows Multiline option for multiline events that are formatted specifically for Windows.
Show Advanced Options	The default is No . Select Yes if you want to customize the event data.
Use Custom Source Name	<p>This parameter is available when you set Show Advanced Options to Yes.</p> <p>Select the check box if you want to customize the source name with regex.</p>
Source Name Regex	<p>This parameter is available when you check Use Custom Source Name.</p> <p>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.</p>
Source Name Formatting String	<p>This parameter is available when you check Use Custom Source Name.</p> <p>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:</p> <ul style="list-style-type: none"> 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.

Table 33. TCP multiline syslog protocol parameters (continued)

Parameter	Description
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.

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.



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/host name 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.

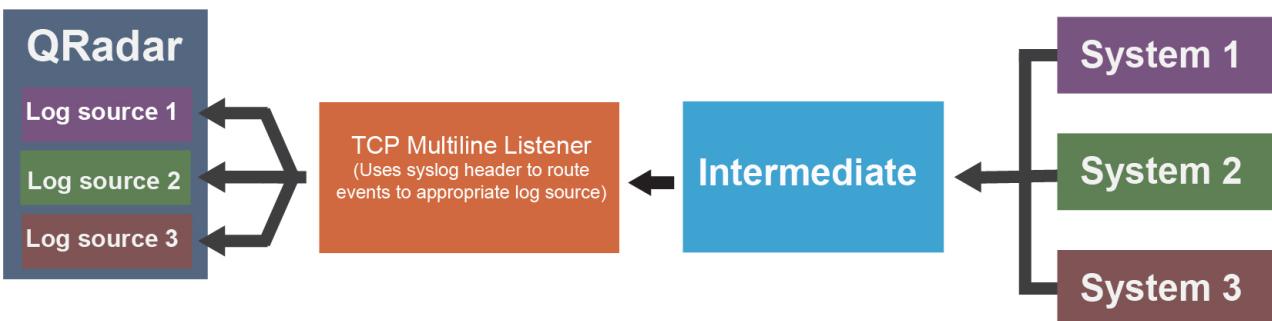


Figure 3. Separate QRadar log sources collect events sent from multiple systems and forwarded via an intermediate system to a TCP Multiline Listener, by using the syslog header.

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.

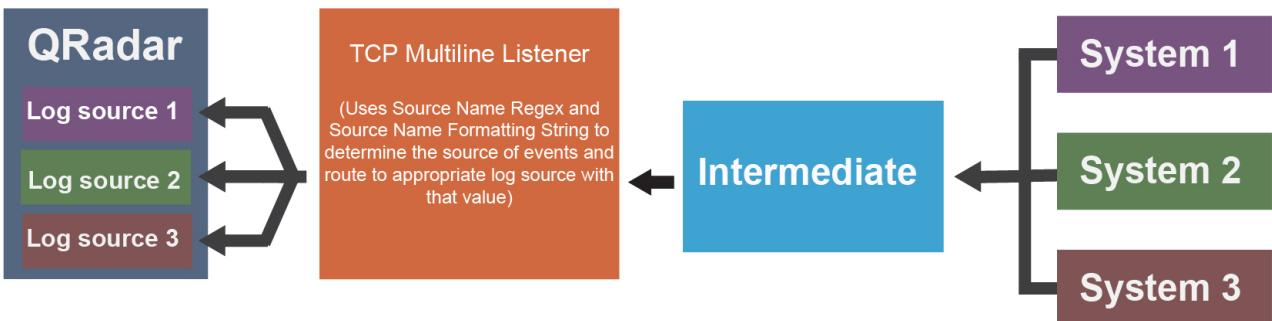


Figure 4. Separate QRadar log sources collect events sent from multiple systems and forwarded via an intermediate system to a TCP Multiline Listener, by using the Source Name Regex and Source Name Formatting String.

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 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 additional 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 34. TLS syslog protocol parameters

Parameter	Description
Protocol Configuration	TLS Syslog
TLS Listen Port	The default TLS listen port is 6514.
Authentication Mode	The mode by which your TLS connection is authenticated. If you select the TLS and Client Authentication option, you must configure the certificate parameters.
Client Certificate Path	The absolute path to the client-certificate on disk. The certificate must be stored on the Console or Event Collector for this log source.
Certificate Type	The type of certificate to use for authentication. If you select the Provide Certificate option, you must configure the file paths for the server certificate and the private key.
Provided Server Certificate Path	The absolute path to the server certificate.
Provided Private Key Path	The absolute path to the private key. Note: The corresponding private key must be a DER-encoded PKCS8 key. The configuration fails with any other key format.
Maximum Connections	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.

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 47

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 original multiline event must contain a value that repeats on each line in order for a regular expression to capture that value and identify and reassemble 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 35. UDP multiline syslog protocol parameters

Parameter	Description
Protocol Configuration	UDP Multiline Syslog
Listen Port	<p>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.</p> <p>To edit a saved configuration to use a new port number, complete the following steps:</p> <ol style="list-style-type: none">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. <p>The port update is complete and event collection starts on the new port number.</p>
Message ID Pattern	The regular expression (regex) required to filter the event payload messages. The UDP multiline event messages must contain a common identifying value that repeats on each line of the event message.
Event Formatter	<p>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.</p> <p>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.</p>
Show Advanced Options	The default is No . Select Yes if you want to configure advanced options.
Use Custom Source Name	Select the check box if you want to customize the source name with regex.

Table 35. UDP multiline syslog protocol parameters (continued)

Parameter	Description
Source Name Regex	<p>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.</p> <p>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.</p>
Source Name Formatting String	<p>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:</p> <ul style="list-style-type: none"> 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. <p>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.</p>
Use As A Gateway Log Source	<p>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.</p> <p>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.</p> <p>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.</p>
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.
Enabled	Select this check box to enable the log source.
Credibility	<p>Select the credibility of the log source. The range is 0 - 10.</p> <p>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.</p>
Target Event Collector	Select the Event Collector in your deployment that should host the UDP Multiline Syslog listener.

Table 35. UDP multiline syslog protocol parameters (continued)

Parameter	Description
Coalescing Events	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.
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.

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 36. Cisco ACS log source parameters

Parameter	Value
Log Source Identifier	Type the IP address, host name, or name to identify your Cisco ACS appliance.
Listen Port	<p>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.</p> <p>To edit a saved configuration to use a new port number, complete the following steps.</p> <ol style="list-style-type: none"> 1. In the Listen Port field, type the new port number for receiving UDP Multiline Syslog events. 2. Click Save. <p>The port update is complete and event collection starts on the new port number.</p>
Message ID Pattern	\s(\d{10})\s
Event Formatter	Select Cisco ACS Multiline from the list.

Related concepts:

"UDP multiline syslog protocol configuration options" on page 49

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

Table 37. VMware vCloud Director protocol parameters

Parameter	Description
Protocol Configuration	VMware vCloud Director
vCloud URL	The URL that is configured on the VMware vCloud appliance to access the REST API. The URL must match the address that is configured as the VCD public REST API base URL on the vCloud Server, for example, https://192.0.2.1 .
User Name	The user name that is required to remotely access the vCloud Server, for example, <code>console/user@organization</code> . To configure a read-only account to use with the vCloud Director protocol, a user must have Console Access Only permission.

4 Adding bulk log sources

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

Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. From the **Bulk Actions** list, select **Bulk Add**.
4. Configure the parameters for the bulk log source.
 - File Upload - Upload a text file that has one host name or IP per line
 - Manual - Enter the host name or IP of the host that you wish to add
5. Click **Save**.
6. Click **Continue** to add the log sources.
7. On the **Admin** tab, click **Deploy Changes**.

5 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**.

6 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:

```
<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.

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.

You can access log source extension examples (<https://www.ibm.com/developerworks/communityforums/html/topic?id=d15cac8d-b0fa-4461-bb1e-dc1b291de440&ps=25>) on the Discussion about DSM Extensions, Custom Properties and other REGEX related topics forum (<https://www.ibm.com/developerworks/community/forums/html/forum?id=1111111-0000-0000-000000003046&ps=25>).

The IBM Security 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” on page 70

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 38. Description of pattern parameters

Pattern	Type	Description
id (Required)	String	A regular string that is unique within the extension document.
case-insensitive (Optional)	Boolean	If true, the character case is ignored. For example, abc is the same as ABC. If not specified, this parameter defaults to false.
trim-whitespace (Optional)	Boolean	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.
use-default-pattern (Optional)	Boolean	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.

Defining custom property by using a Regex or JSON expression

You can define a custom property for an event payload by using a Regex or JSON expression.

About this task

Support for the JSON format was added in V7.3.1.

Procedure

1. Log in to QRadar and click the **Admin** tab.
2. From the Data Sources section, click **Custom Event Properties > Add**.
3. In the Property Type Selection section, select **Extraction Based**.
4. In the Test Field, enter the event payload that you want to use to test your custom property.
5. In the Property Definition section, complete the following steps:
 - a. If you're adding an expression to an existing property, select **Existing Property** and select a property from the list.

- b. If you're defining a new property, select **New Property** and enter the name of the property.
 - c. To use the property for rules, reports and searches, select the **Parse in advance for rules, reports, and searches** check box.
 - d. Select a **Field Type** for the property.
 - e. Enter a description for the property in the **Description** field.
6. In the Property Expression Definition section, complete the following steps:
- a. Select the **Enabled** check box to enable or clear the check box to disable the property.
 - b. From the **Log Source Type** list, select a log source type for the property.
 - c. If the expression is only evaluated against events for a specific log source, select a log source from the **Log Source** list. Otherwise, select **All**.
 - d. If the expression is only evaluated against events with a specific event name or QID, click the **Event Name** and browse for a QID to associate the expression with.
 - e. If the expression is evaluated against any event with a specific low-level category, select **Category**, and select the **High Level Category** and **Low Level Category** for the event.

Note: If the expression is evaluated for all events of the selected log source type and log source, ensure that you set the **Low Level Category** and **High Level Category** to **Any**.

- f. From the **Extraction using** field, select the extraction method that is used for the property.
- g. If the extraction method is **Regex**, enter the regex in the **Regex** field, and enter the capture group number in the **Capture Group** field.
- h. If the extraction method is **JsonKeypath**, enter the JSON expression in the **JsonKeypath** field.

Note: A valid JSON expression is in the form `"/<name of top-level field>"`.

For an event data in a nested JSON format, a valid JSON expression is in the form `"/<name of top-level field>/<name of sub-level field_1>.../<name of sub-level field_n>"`.

The following two examples show how to extract data from a JSON record:

- Simple case of an event for a flat JSON record: `{"action": "login", "user": "John Doe"}`
To extract the 'user' field, use this expression: `"/user"`.
 - Complex case of an event for a JSON record with nested objects: `{ "action": "login", "user": { "first_name": "John", "last_name": "Doe" } }`
To extract just the 'last_name' value from the 'user' subobject, use this expression:
`"/user"/"last_name"`.
- i. If you chose the **Numeric Field Type** in the Property Definition section, select a number format in the **Extracted Number Format** field in the Format section to define any digit group separators for the locale of the custom property.
 - j. If you chose the **Date/Time Field Type** in the Property Definition section, enter a format in the **Extracted Date/Time Format** and **Locale** fields in the Format section to define the date and time for the locale of the custom property.
 - k. Click **Test** to test the property expression definition.
7. Click **Save**.

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 39. Description of match group parameters

Parameter	Description
order (Required)	An integer greater than zero that defines the order in which the match groups are executed. It must be unique within the extension document.
description (Optional)	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.
device-type-id-override (Optional)	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. A list of log source type IDs is presented in Table 48 on page 80. If not specified, this parameter defaults to the log source type of the log source to which the extension is attached.

Match groups can have these entities:

- “Matcher (matcher)”
- “Single-event modifier (event-match-single)” on page 67
- “Multi-event modifier (event-match-multiple)” on page 66

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 40. Description of matcher parameters

Parameter	Description
field (Required)	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.
pattern-id (Required)	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 38 on page 58).
order (Required)	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.

Table 40. Description of matcher parameters (continued)

Parameter	Description
capture-group (Optional)	<p>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.</p> <p>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.</p> <p>This field has a dual purpose when combined with the enable-substitutions parameter.</p> <p>To see an example, review the extension document example.</p>
enable-substitutions (Optional)	<p>Boolean</p> <p>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.</p> <p>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:</p> <pre data-bbox="755 1227 1041 1256">capture-group="\1_\2@\1"</pre> <p>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:</p> <pre data-bbox="755 1417 1148 1446">capture-group="\1:\2:\3:\4:\5:\6"</pre> <p>If no groups are specified in the capture-group when substitutions are enabled, a direct text replacement occurs.</p> <p>Default is false.</p>
ext-data (Optional)	<p>An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension.</p> <p>The only field that uses this parameter is DeviceTime.</p> <p>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.</p>

The following table lists valid matcher field names.

Table 41. List of valid matcher field names

Field name	Description
EventName (Required)	<p>The event name to be retrieved from the QID to identify the event.</p> <p>Note: This parameter doesn't appear as a field in the Log Activity tab.</p>
EventCategory	<p>An event category for any event with a category not handled by an event-match-single entity or an event-match-multiple entity.</p> <p>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,</p> <pre><event-match-single event-name="Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity="OverrideAndNeverSend" /></pre> <p>The force-qidmap-lookup-on-fixup="true" is the flag override.</p> <p>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.
SourceIpPostNAT	The source IP address for the message after NAT occurs.
SourceMAC	The source MAC address for the message.
SourcePortPreNAT	The source port for the message before NAT occurs.
SourcePortPostNAT	The source port for the message after NAT occurs.
DestinationIp	The destination IP address for the message.
DestinationPort	The destination port for the message.
DestinationIpPreNAT	The destination IP address for the message before NAT occurs.
DestinationIpPostNAT	The destination IP address for the message after NAT occurs.
DestinationPortPreNAT	The destination port for the message before NAT occurs.
DestinationPortPostNAT	The destination port for the message after NAT occurs.
DestinationMAC	The destination MAC address for the message.

Table 41. List of valid matcher field names (continued)

Field name	Description
DeviceTime	<p>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.</p> <p>The following list contains examples of date and time stamp formats that you can use in the DeviceTime field:</p> <ul style="list-style-type: none"> • 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 <p>For more information about the possible values for the data and time stamp format, see the Joda-Time web page (http://www.joda.org/joda-time/key_format.html).</p> <p>DeviceTime is the only event field that uses the ext-data optional parameter.</p>
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.
DestinationIpv6	The IPv6 destination IP address for the message.

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 Security 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 42. Description of JSON matcher parameters

Parameter	Description
field (Required)	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.
pattern-id (Required)	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 38 on page 58)
order (Required)	<p>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.</p> <p>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.</p>
enable-substitutions (Optional)	<p>Boolean</p> <p>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.</p> <p>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 <code>{"/last_name"}, {"first_name"}</code>. The captured value for this expression is smith, john.</p> <p>Default is false.</p>
ext-data (Optional)	<p>An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension.</p> <p>The only field that uses this parameter is DeviceTime.</p> <p>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.</p>

The following table lists valid **JSON matcher** field names.

Table 43. List of valid JSON matcher field names

Field name	Description
EventName (Required)	<p>The event name to be retrieved from the QID to identify the event.</p> <p>Note: This parameter doesn't appear as a field in the Log Activity tab.</p>

Table 43. List of valid JSON matcher field names (continued)

Field name	Description
EventCategory	<p>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.</p> <p>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:</p> <pre><event-match-single event-name="Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity="OverrideAndNeverSend" /></pre> <p>The force-qidmap-lookup-on-fixup="true" is the flag override.</p> <p>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.
SourceIpPostNAT	The source IP address for the message after NAT occurs.
SourceMAC	The source MAC address for the message.
SourcePortPreNAT	The source port for the message before NAT occurs.
SourcePortPostNAT	The source port for the message after NAT occurs.
DestinationIp	The destination IP address for the message.
DestinationPort	The destination port for the message.
DestinationIpPreNAT	The destination IP address for the message before NAT occurs.
DestinationIpPostNAT	The destination IP address for the message after NAT occurs.
DestinationPortPreNAT	The destination port for the message before NAT occurs.
DestinationPortPostNAT	The destination port for the message after NAT occurs.
DestinationMAC	The destination MAC address for the message.

Table 43. List of valid JSON matcher field names (continued)

Field name	Description
DeviceTime	<p>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.</p> <p>The following list contains examples of date and time stamp formats that you can use in the DeviceTime field:</p> <ul style="list-style-type: none"> • 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 <p>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).</p> <p>DeviceTime is the only event field that uses the ext-data parameter.</p>
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.
DestinationIpv6	The IPv6 destination IP address for the message.

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 44. Description of single-event parameters

Parameter	Description
device-event-category	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.
severity	The severity of the event. This parameter must be an integer value 1 - 10. If a severity of less than 1 or greater than 10 is specified, the system defaults to 5. If not specified, the default is whatever is found in the QID.
send-identity	Specifies the sending of identity change information from the event. Choose one of the following options: <ul style="list-style-type: none">• 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.• 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.• OverrideAndAlwaysSend Ignores any identity event that is returned by the DSM and creates a new identity event, if there is enough information.• 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.

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 version="1.0" encoding="UTF-8"?>  
<device-extension xmlns="event_parsing/device_extension">  
<pattern id="EventNameFWSM_Pattern" xmlns=""><! [CDATA[%FWSM[a-zA-Z-]*\d-(\d{1,6})]]></pattern>  
<pattern id="SourceIp_Pattern" xmlns=""><! [CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/(\[\d{1,5}\])]></pattern>  
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><! [CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/(\[\d{1,5}\])]></pattern>  
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><! [CDATA[addr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/(\[\d{1,5}\])]></pattern>  
<pattern id="DestinationIp_Pattern" xmlns=""><! [CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/(\[\d{1,5}\])]></pattern>  
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><! [CDATA[(tcp|udp|icmp|gre)]]></pattern>  
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><! [CDATA[protocol=6]]></pattern>  
<pattern id="EventNameId_Pattern" xmlns=""><! [CDATA[(\d{1,6})]]></pattern>  
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">  
    <matcher field="EventName" order="1" pattern-id="EventNameFWSM_Pattern" capture-group="1"/>  
    <matcher field="SourceIp" order="1" pattern-id="SourceIp_Pattern" capture-group="1" />  
    <matcher field="SourcePort" order="1" pattern-id="SourcePort_Pattern" capture-group="2"/>  
    <matcher field="SourceIpPreNAT" order="1" pattern-id="SourceIpPreNAT_Pattern" capture-group="1" />  
    <matcher field="SourceIpPostNAT" order="1" pattern-id="SourceIpPostNAT_Pattern" capture-group="1" />  
    <matcher field="SourcePortPreNAT" order="1" pattern-id="SourcePortPreNAT_Pattern" capture-group="2" />  
    <matcher field="SourcePortPostNAT" order="1" pattern-id="SourcePortPostNAT_Pattern" capture-group="2" />  
    <matcher field="DestinationIp" order="1" pattern-id="DestinationIp_Pattern" capture-group="1" />  
    <matcher field="DestinationPort" order="1" pattern-id="DestinationIp_Pattern" capture-group="2" />  
    <matcher field="Protocol" order="1" pattern-id="Protocol_Pattern" capture-group="1" />  
    <matcher field="Protocol" order="2" pattern-id="Protocol_6_Pattern" capture-group="TCP" enable-substitutions=true/>  
    <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>  
</match-group>  
</device-extension>  
<?xml version="1.0" encoding="UTF-8"?>  
<device-extension xmlns="event_parsing/device_extension">  
!-- Do not remove the "allEventNames" value -->  
<pattern id="EventName-Fakeware_Pattern" xmlns=""><! [CDATA[]]></pattern>  
<pattern id="SourceIp-Fakeware_Pattern" xmlns=""><! [CDATA[]]></pattern>  
<pattern id="SourcePort-Fakeware_Pattern" xmlns=""><! [CDATA[]]></pattern>  
<pattern id="SourceMAC-Fakeware_Pattern" xmlns=""><! [CDATA[]]></pattern>  
<pattern id="DestinationIp-Fakeware_Pattern" xmlns=""><! [CDATA[]]></pattern>  
<pattern id="DestinationPort-Fakeware_Pattern" case-insensitive="true" xmlns=""><! [CDATA[]]></pattern>  
<pattern id="Protocol-Fakeware_Pattern" case-insensitive="true" xmlns=""><! [CDATA[]]></pattern>  
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">  
    <matcher field="EventName" order="1" pattern-id="EventName-Fakeware_Pattern" capture-group="1"/>  
    <matcher field="SourceIp" order="1" pattern-id="SourceIp-Fakeware_Pattern" capture-group="1" />  
    <matcher field="SourcePort" order="1" pattern-id="SourcePort-Fakeware_Pattern" capture-group="1" />  
    <matcher field="SourceMAC" order="1" pattern-id="SourceMAC-Fakeware_Pattern" capture-group="1" />  
    <matcher field="DestinationIp" order="1" pattern-id="DestinationIp-Fakeware_Pattern" capture-group="1" />  
    <matcher field="DestinationPort" order="1" pattern-id="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. For more information, see "Log Source Type IDs" on page 80).

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 Security 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 (\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.

```

<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 Security 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 Security 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 Security 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 Security 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:

“Extension document template” on page 68

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.

“Examples of log source extensions on QRadar forum” on page 57

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.

Related reference:

157, “QRadar supported DSMs,” on page 987

IBM Security QRadar can collect events from your security products by using a plugin file that is called a Device Support Module (DSM).

Building a Universal DSM

The first step in building a Universal DSM is to create the log source in IBM Security 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”

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.

The screenshot shows the 'Search Parameters' section of the QRadar Log Activity interface. It includes fields for Parameter (set to 'Log Source [Indexed]'), Operator (set to 'Equals'), Value (set to 'Log Source Group: Other'), Log Source Filter (containing 'Type to Filter'), and a Log Source text area. A 'Add Filter' button is visible to the right of the filter field.

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, la1 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)
```

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} (TCP|UDP|ICMP|GRE)
\w{3}\s\d{2}\s\d{2}:\d{2}:\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 45. Common regex expressions

Type	Expression
IP Address	\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}
MAC Address	(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}
Port Number	\d{1,5}
Protocol	(TCP UDP ICMP GRE)
Device Time	\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
Whitespace	\s
Tab	\t
Match Anything	.*?

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 Universal DSM, 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 "
- 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 46. Translating pseudo-code to regular expressions

Field	Pseudo-code	Regular expression
EventName	" kernel: VALUE "	\skernel\:\s.*?\s
SourceMAC	" MAC=VALUE "	\sMAC\=(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}\s

Table 46. Translating pseudo-code to regular expressions (continued)

Field	Pseudo-code	Regular expression
SourceIP	" SRC=VALUE "	\sSRC\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s
DestinationIp	" DST=VALUE "	\sDST\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s
Protocol	" PROTO=VALUE "	\sPROTO\=(TCP UDP ICMP GRE)\s
SourcePort	" SPT=VALUE "	\sSPT\=\d{1,5}\s
DestinationPort	" DPT=VALUE "	\sDPT\=\d{1,5}\s

6. 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 Security QRadar.

Insert parenthesis around the values you that you want capture:

Table 47. Mapping regular expressions to capture groups for event fields

Field	Regular expression	Capture group
EventName	\skernel\:\s.*?\s	\skernel\:\s.*?\s
SourceMAC	\sMAC\=(?:[0-9a-fA-F]{2}[:])[0-9a-fA-F]{2}\s	\sMAC\=((?:[0-9a-fA-F]{2}[:])[0-9a-fA-F]{2})\s
SourceIP	\sSRC\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s	\sSRC\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s
Destination IP	\sDST\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s	\sDST\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s
Protocol	\sPROTO\=(TCP UDP ICMP GRE)\s	\sPROTO\=((TCP UDP ICMP GRE))\s
SourcePort	\sSPT\=\d{1,5}\s	\sSPT\=(\d{1,5})\s
DestinationPort	\sDPT\=\d{1,5}\s	\sDPT\=(\d{1,5})\s

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.

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

Uploading extension documents to QRadar

You can create multiple extension documents and then upload them and associate 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 Security QRadar.

Procedure

- On the **Admin** tab, click **Log Source Extensions**.
- Click **Add**.
- Assign a name.
- 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. Optional: 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.

Mapping unknown events

Initially, all of the events from the Universal DSM appear as unknown in the **Log Activity** tab in QRadar. You must manually map all unknown events to their equivalents in the QID map.

Although the event names, such as DROP, DENY, and ACCEPT, might be understandable values when you see them in the log files, QRadar doesn't understand what these values represent. To QRadar, these values are strings of text that are not mapped to any known values. The values appear as expected and are treated as normalized events until you manually map them.

In some instances, such as an intrusion detection system (IDS) or an intrusion detection and prevention system (IDP) thousands of events exist and require mapping. In these situations, you can map a category as the event name instead of the itself. For example, in the following example, to reduce the number of mappings, instead of using the name field for the Event Name, use the category field instead. You can use a custom property to display the event name (Code Red v412):

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

Instead of using the name field for the Event Name, use the category field instead. The actual event name, for example Code Red v412, can be displayed using a custom property.

Before you begin

Ensure that you uploaded the log source extension document and applied it to the Universal DSM. For more information, see “Uploading extension documents to QRadar” on page 75.

Procedure

1. From the **Log Activity** tab, click **Search > Edit Search**
2. From the **Time Range** options, choose enough time, such as 15 minutes, from when the log source extension was applied to the Universal DSM.

3. Under **Search Parameters**, select **Log Source [Index]** from the **Parameter** list, **Equals** from the **Operator** list and then select the log source that you created from the **Log Source Group** and the **Log Source** lists.
4. Click **Search** to view the results.
All of the events appear as unknown.
5. Double-click an unknown entry to view the event details.
6. Click **Map Event** from the toolbar.
The value **Log Source Event ID** displays an **EventName** value, for example, **DROP**, **DENY**, or **ACCEPT**, from the log source extension. The value can't be blank. A blank value indicates that there is an error in the log source extension document.
7. Map the value that is displayed as the **Log Source Event ID** to the appropriate QID.
Use the **Browse By Category**, or **QID Search**, or both to find a value that best matches the **Log Source Event ID** value. For example, the value **DROP** can be mapped to the **QID Firewall Deny - Event CRE**.
Use the QID with the Event CRE in the name. Most events are specific to a particular log source type. For example, when you map to a random firewall, **Deny QID** is similar to mapping the Universal DSM to events from another log source type. The QID entries that contain the name Event CRE are generic and are not tied to a particular log source type.
8. Repeat these steps until all unknown events are mapped successfully.
From this point, any further events from the Universal DSM that contain that particular Log Source Event ID appear as the specified QID. Events that arrived before the QID mapping remain unknown. There is no supported method for mapping previous events to a current QID. This process must be repeated until all of the unknown event types are successfully mapped to a QID.

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:

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

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:

```
<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:

```
<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=12-34-56-78-90-AB is converted to a MAC address of 12:34:56:78:90:AB.

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:

```
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:

```
<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.

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

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

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

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:

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

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

Multiple Log Formats in a Single Log Source

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

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

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.

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

<pattern id="UserName_DDWRT-Auth1_Pattern" xmlns=""><! [CDATA[\\sfor\\s\\'(.*)\\'\\s]]></pattern>
<pattern id="UserName_DDWRT-Auth2_Pattern" xmlns=""><! [CDATA[\\safter\\sauth\\s\\'(.*)\\:\\]]></pattern>

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

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

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:

```
Event,User,Source IP,Source Port,Destination IP,Destination Port
Failed Login,<Username>,<Source IP_address>,1024,<Destination IP_address>,22
Successful Login,<Username>,<Source IP_address>,1743,<Destination IP_address>,110
Privilege Escalation,<Username>,<Source IP_address>,1028,<Destination IP_address>,23
```

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

5. Upload the log source extension.

6. Map the events.

Related tasks:

"Mapping unknown events" on page 76

Initially, all of the events from the Universal DSM appear as unknown in the **Log Activity** tab in QRadar. You must manually map all unknown events to their equivalents in the QID map.

Log Source Type IDs

IBM Security QRadar supports a number of log sources and each log source has an identifier. Use the Log Source Type IDs in a match-group statement:

The following table lists the supported log source type and their IDs.

Table 48. Log Source Type ID

ID	Log Source Type
2	Snort Open Source IDS
3	Check Point (formerly Firewall-1)
4	Configurable Firewall Filter
5	Juniper Networks Firewall and VPN
6	Cisco PIX Firewall
7	Configurable Authentication message filter
9	Extreme Dragon Network IPS
10	Apache HTTP Server

Table 48. Log Source Type ID (continued)

ID	Log Source Type
11	Linux OS
12	Microsoft Windows Security Event Log
13	Microsoft IIS
14	Linux iptables Firewall
15	IBM Proventia Network Intrusion Prevention System (IPS)
17	Juniper Networks Intrusion Detection and Prevention (IDP)
19	TippingPoint Intrusion Prevention System (IPS)
20	Cisco IOS
22	Nortel Multiprotocol Router
23	Cisco VPN 3000 Series Concentrator
24	Solaris Operating System Authentication Messages
25	McAfee IntruShield Network IPS Appliance
26	Cisco CSA
28	Extreme Matrix E1 Switch
29	Solaris Operating System Sendmail Logs
30	Cisco Intrusion Prevention System (IPS)
31	Cisco Firewall Services Module (FWSM)
33	IBM Proventia Management SiteProtector
35	CyberGuard TSP Firewall/VPN
36	Juniper Networks Secure Access (SA) SSL VPN
37	Nortel Contivity VPN Switch
38	Top Layer (IPS)
39	Universal DSM
40	Tripwire Enterprise
41	Cisco Adaptive Security Appliance (ASA)
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager
46	Squid Web Proxy
47	Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)
48	Oracle RDBMS Audit Record
49	F5 Networks BIG-IP LTM
50	Solaris Operating System DHCP Logs
55	Array Networks SSL VPN Access Gateways
56	Cisco CatOS for Catalyst Switches
57	ProFTPD Server
58	Linux DHCP Server
59	Juniper Networks Infranet Controller
64	Juniper Junos OS Platform

Table 48. Log Source Type ID (continued)

ID	Log Source Type
68	Extreme Matrix K/N/S Series Switch
70	Extreme Networks ExtremeWare Operating System (OS)
71	McAfee Firewall Enterprise
73	Fortinet FortiGate Security Gateway
78	SonicWALL SonicOS
79	Vericept Content 360
82	Symantec Gateway Security (SGS) Appliance
83	Juniper Steel-Belted Radius
85	IBM AIX Server
86	Metainfo MetaIP
87	Symantec System Center
90	Cisco ACS
91	Enterasys Sentinel DSM
92	ForeScout CounterACT
93	McAfee ePolicy Orchestrator
95	Cisco NAC Appliance
96	TippingPoint X Series Appliances
97	Microsoft DHCP Server
98	Microsoft IAS Server
99	Microsoft Exchange Server
100	Trend InterScan VirusWall
101	Microsoft SQL Server
102	MAC OS X
103	Blue Coat SG Appliance
104	Nortel Switched Firewall 6000
105	SIM Audit
106	3Com 8800 Series Switch
107	Nortel VPN Gateway
108	Nortel Threat Protection System (TPS) Intrusion Sensor
110	Nortel Application Switch
111	Juniper DX Application Acceleration Platform
112	SNARE Reflector Server
113	Cisco 12000 Series Routers
114	Cisco 6500 Series Switches
115	Cisco 7600 Series Routers
116	Cisco Carrier Routing System
117	Cisco Integrated Services Router
118	Juniper M Series Multiservice Edge Routing
120	Nortel Switched Firewall 5100
122	Juniper MX Series Ethernet Services Router

Table 48. Log Source Type ID (continued)

ID	Log Source Type
123	Juniper T Series Core Platform
134	Nortel Ethernet Routing Switch 8300/8600
135	Nortel Ethernet Routing Switch 2500/4500/5500
136	Nortel Secure Router
138	OpenBSD OS
139	Juniper Ex Series Ethernet Switch
140	Symark Power Broker
141	Oracle Database Listener
142	Samhain HIDS
143	Bridgewater Systems AAA Service Controller
144	Name Value Pair
145	Nortel Secure Network Access Switch (SNAS)
146	Starent Networks Home Agent (HA)
148	IBM AS/400 iSeries
149	Foundry Fastiron
150	Juniper SRX Series Services Gateway
153	CRYPTOCARD CRYPTOSHIELD
154	Imperva SecureSphere
155	Aruba Mobility Controller
156	Extreme NetsightASM
157	Extreme HiGuard
158	Motorola SymbolAP
159	Extreme HiPath
160	Symantec Endpoint Protection
161	IBM Resource Access Control Facility (RACF)
163	RSA Authentication Manager
164	Redback ASE
165	Trend Micro Office Scan
166	Extreme XSR Security Routers
167	Extreme Stackable and Standalone Switches
168	Juniper Networks AVT
170	Extreme A2-Series
171	Extreme B2-Series
172	Extreme B3-Series
173	Extreme C2-Series
174	Extreme C3-Series
175	Extreme D2-Series
176	Extreme G3-Series
177	Extreme I3-Series
178	Trend Micro Control Manager

Table 48. Log Source Type ID (continued)

ID	Log Source Type
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module (WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	HP Tandem
188	Sentrigo Hedgehog
189	Sybase ASE
191	Microsoft ISA
192	Juniper SRC
193	Radware DefensePro
194	Cisco ACE Firewall
195	IBM DB2
196	Oracle Audit Vault
197	Cisco FireSIGHT Management Center
198	Forcepoint V Series
199	Oracle RDBMS OS Audit Record
200	Risk Manager Default Question
206	Palo Alto PA Series
208	HP ProCurve
209	Microsoft Operations Manager
210	EMC VMWare
211	IBM WebSphere Application Server
212	Universal LEEF
213	F5 Networks BIG-IP ASM
214	FireEye
215	Fair Warning
216	IBM Informix Audit
217	CA Top Secret
218	Extreme NAC
219	Microsoft SCOM
220	McAfee Web Gateway
221	CA ACF2
222	McAfee Application / Change Control
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Cyber-Ark Vault

Table 48. Log Source Type ID (continued)

ID	Log Source Type
228	Itron Smart Meter
230	Bit9 Security Platform
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper vGW
236	Symantec DLP
237	Oracle Alert Logs
238	Solaris BSM
239	Oracle BEA WebLogic
240	Sophos Web Security Appliance
241	Sophos Astaro Security Gateway
242	Microsoft SQL Server Trace Log
243	Infoblox NIOS
244	Tropos Control
245	Novell eDirectory
247	VMware vShield
248	Cisco Wireless NCS
249	IBM Guardium
250	Cisco Nexus
251	Stonesoft Management Center
252	SolarWinds Orion
253	Microsoft Endpoint Protection
254	Great Bay Beacon
255	Damballa Failsafe
256	SecWorld X/G/F series
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI
262	CRE Event Response
263	DCN DCS/DCS Series
264	Juniper Security Binary Log Collector
265	Trend Micro Deep Discovery Inspector
266	IBM Tivoli Access Manager for e-business
268	Verdasys Digital Guardian
269	Hauwei S Series Switch
270	Citrix Access Gateway
271	HBGary Active Defense

Table 48. Log Source Type ID (continued)

ID	Log Source Type
272	APC UPS
273	Cisco Wireless LAN Controllers
274	Cisco Call Manager
275	CRE System
276	IBM Customer Information Control System (CICS)
278	Barracuda Spam & Virus Firewall
279	Open LDAP Software
280	Application Security DbProtect
281	Barracuda Web Application Firewall
282	OSSEC
283	Huawei AR Series Router
284	Sun ONE LDAP
285	BlueCat Networks Adonis
286	IBM AIX Audit
287	Symantec PGP Universal Server
288	Kaspersky Security Center
289	IBM BigFix
290	Juniper Junos WebApp Secure
291	Nominum Vantio
292	Extreme 800-Series Switch
293	IBM zSecure Alert
294	IBM Security Network Protection (XGS)
295	IBM Security Identity Manager
296	F5 Networks BIG-IP Advanced Firewall Manager (AFM)
297	IBM Security Network IPS (GX)
298	Fidelis XPS
299	Arpeggio SIFT-IT
300	Barracuda Web Filter
302	Brocade FabricOS
303	ThreatGRID Malware Threat Intelligence Platform
304	IBM Security Access Manager for Enterprise Single Sign-On
305	VmWare vCloud Director
306	Venustech Venusense Unified Threat Management
307	Venustech Venusense Firewall
308	Venustech Venusense Network Intrusion Prevention System
309	ObserveIT
311	Pirean Access: One
312	Venustech Venusense Security Platform

Table 48. Log Source Type ID (continued)

ID	Log Source Type
313	PostFix MailTransferAgent
314	Oracle Fine Grained Auditing
315	VMware vCenter
316	Cisco Identity Services Engine
317	Microsoft System Center Configuration Manager
318	Honeycomb Lexicon File Integrity Monitor
319	Oracle Acme Packet Session Border Controller (SBC)
320	Juniper WirelessLAN
321	Akamai KONA
330	Arbor Networks Peakflow SP
331	Zscaler NSS
332	Proofpoint Enterprise Protection/Enterprise Privacy
333	H3C Comware Platform
334	H3C Switches
335	H3C Routers
336	H3C Wireless LAN Devices
337	H3C IP Security Devices
338	Microsoft Hyper-V
339	Cilasoft QJRN/400
340	Vormetric Data Security
341	SafeNet DataSecure/KeySecure
342	OpenStack Ceilometer
343	STEALTHbits StealthINTERCEPT
344	Juniper DDoS Secure
345	Arbor Networks Pravail
346	IBM Security Trusteer Apex Advanced Walware Protection
347	Amazon AWS CloudTrail
348	IBM Security Directory Server
349	Extreme A4-Series
350	Extreme B5-Series
351	Extreme C5-Series
352	Salesforce Security Monitoring
353	Ahnlab Policy Center APC
354	Avaya VPN Gateway 3070
356	DG Technology MEAS
357	Salesforce Security Auditing
358	CloudPassage Halo
359	CorreLog Agent for IBM zOS
360	WatchGuard Fireware OS

Table 48. Log Source Type ID (continued)

ID	Log Source Type
361	IBM Fiberlink MaaS360
362	Trend Micro Deep Discovery Analyzer
363	Resolution 1 CyberSecurity
364	IBM Privileged Session Recorder
365	Bluemix Platform
366	IBM SmartCloud Orchestrator
367	Universal CEF
369	FreeRADIUS
370	Riverbed SteelCentral NetProfiler
371	Riverbed SteelCentral NetProfiler Audit
372	SSH CryptoAuditor
373	IBM WebSphere DataPower
374	Symantec Critical System Protection
375	Kisco Information Systems SafeNet/i
376	IBM Federated Directory Server
377	HyTrust CloudControl
378	Lastline Enterprise
379	genua genugate
380	IBM Security Privileged Identity Manager
381	Netskope Active
382	Okta Identity Management
383	Oracle Enterprise Manager
384	Microsoft DNS Debug
385	STEALTHbits StealthINTERCEPT Analytics
386	STEALTHbits StealthINTERCEPT Alerts
387	Universal SaaS
388	Cloudera Navigator
389	IBM Security Access Manager for Mobile
390	Skyhigh Networks Cloud Security Platlform
391	Aruba ClearPass Policy Manager
392	IBM Security Identity Governance
393	Seculert Seculert
394	Trend Micro Deep Security
395	Epic SIEM
396	Enterprise-IT-Security.com SF-Sherlock
397	Microsoft Office 365
398	Exabeam
399	Blue Coat Web Security Service
400	Carbon Black
401	Trend Micro Deep Discovery Email Inspector

Table 48. Log Source Type ID (continued)

ID	Log Source Type
402	Onapsis Inc. Onapsis Security Platform
403	CyberArk Privileged Threat Analytics
404	Palo Alto Networks Endpoint Security Manager
405	Box
406	Radware AppWall
407	CrowdStrike Falcon Host
408	IBM Sense
409	CloudLock Cloud Security Fabric
410	Vectra Networks Vectra
411	HP Network Automation
412	IBM QRadar Packet Capture
413	Microsoft Azure
414	Kaspersky Threat Feed Service
415	ESET Remote Administrator
416	Illumio Adaptive Security Platform
417	SecureAuth IdP
418	Aruba Introspect
419	Cisco Cloud Web Security
421	IBM SAN Volume Controller
422	LightCyber Magna
423	Fasoo Enterprise DRM
425	Imperva Incapsula
426	IBM BigFix EDR
427	Centrify Server Suite (DSM not released yet)
428	Carbon Black Protection
429	Cisco Stealthwatch
430	Amazon Virtual Private Cloud Flow Logs

7 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:

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

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

8 3Com Switch 8800

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

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

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

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

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

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

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“Configuring your 3COM Switch 8800”](#)

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

[“Adding a log source” on page 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 3COM Switch 8800

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

Procedure

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

9 AhnLab Policy Center

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

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

Table 49. AhnLab Policy Center DSM specifications

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

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

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

Tip: For more information, see your DB2 documentation.

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

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

Related tasks:

“Adding a DSM” on page 4

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

"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.

10 Akamai Kona

The IBM Security QRadar DSM for Akamai KONA collects event logs from your Akamai KONA servers.

The following table identifies the specifications for the Akamai KONA DSM:

Table 50. Akamai KONA DSM specifications

Specification	Value
Manufacturer	Akamai
Product	Kona
DSM RPM name	DSM-AkamaiKona-QRadar_Version-Build_Number.noarch.rpm
Protocol	HTTP Receiver
QRadar recorded events	Warn Rule Events Deny Rule Events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Akamai website (http://www.akamai.com/)

To send Akamai KONA events to QRadar, complete the following steps:

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.

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console:
 - DSMCommon RPM
 - HTTPReceiver Protocol RPM
 - Akamai KONA RPM
2. For each instance of Akamai KONA, 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 51. Akamai KONA log source parameters

Parameter	Description
Client Certificate Path	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 HTTPs and Client Authentication option from the Communication Type list, the Client Certificate Path parameter is required .
Listen Port	The destination port that is configured on the Akamai KONA system
Message Pattern	The Message Pattern '\{"type'

Related tasks:

"Adding a DSM" on page 4

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

"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.

11 Amazon AWS CloudTrail

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

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

Table 52. Amazon AWS CloudTrail DSM specifications

Specification	Value
Manufacturer	Amazon
DSM	Amazon AWS CloudTrail
RPM name	DSM-AmazonAWSCloudTrail-QRadar_version-Build_number.noarch.rpm
Supported versions	N/A
Protocol	Amazon AWS S3 REST API
QRadar recorded events	All version 1.0, 1.02, 1.03, and 1.04 events.
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Amazon website (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/whatisawscloudtrail.html)

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

1. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the **AmazonS3ReadOnlyAccess** policy.
2. Install the most recent version of the following RPMs on your QRadar Console.
 - Protocol Common
 - Amazon AWS REST API Protocol RPM
 - Amazon AWS CloudTrail DSM RPM
3. Click the **Admin** tab.
4. Click the **Log Sources** icon.
5. From the navigation menu, click **Add**.
6. Configure the Amazon AWS CloudTrail log source in QRadar.

Restriction:

A log source can retrieve data from only one region. Use a different log source for each region. Include the region folder name in the file path for the **Directory Prefix** value when you configure the log source.

The following table describes the parameters that require specific values to collect audit events from Amazon AWS CloudTrail:

Table 53. Amazon AWS CloudTrail log source parameters

Parameter	Description
Log Source Type	Amazon AWS CloudTrail
Protocol Configuration	Amazon AWS S3 REST API
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 AWS CloudTrail log source that is configured, you might want to identify the first log source as <i>awscloudtrail1</i> , the second log source as <i>awscloudtrail2</i> , and the third log source as <i>awscloudtrail3</i> .
Signature Version	Select AWSSIGNATUREV2 or AWSSIGNATURE4 . 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.
Region Name (Signature V4 only)	The region that is associated with the Amazon S3 bucket.
Bucket Name	The name of the AWS S3 bucket where the log files are stored.
Endpoint URL	https://s3.amazonaws.com
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 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 running within an AWS EC2 container.
Public Key	The public access key that is required to access the AWS S3 bucket. Note: This parameter is called Access Key ID in Amazon AWS Cloudtrail.
Access Key	The private access key that is required to access the AWS S3 bucket. Note: This parameter is called Secret Access Key in Amazon AWS Cloudtrail.
Directory Prefix	The root directory location on the AWS S3 bucket from which the CloudTrail logs are retrieved, for example, <code>AWSLogs/<AccountNumber>/CloudTrail/<RegionName>/</code>
File Pattern	The regular expression (regex) used to select files to process. The default is <code>.*?\.json\.\.gz</code>

Table 53. Amazon AWS CloudTrail log source parameters (continued)

Parameter	Description
Event Format	<p>Choose the format of the events contained within the files.</p> <p>AWS Cloud Trail JSON Files contain JSON formatted events for Amazon Cloudtrail (.gz files only).</p> <p>W3C For use with Cisco Cloud Web Services DSM (.gz files only).</p> <p>LINEBYLINE Files are raw log files that contain 1 record per line. Compression with gzip (.gz or .gzip) and zip (.zip) is supported and autodetected with the appropriate file extension.</p>
Use Proxy	<p>When a proxy is configured, all traffic for the log source travels through the proxy for QRadar to access the Amazon AWS S3 buckets.</p> <p>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.</p>
Automatically Acquire Server Certificate(s)	<p>If you select Yes, QRadar automatically downloads the server certificate and begins trusting the target server.</p> <p>This can be used to initialize a newly created log source and obtain certificates initially, or to replace expired certificates.</p>
Recurrence	<p>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.</p> <p>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.</p>

- To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

The following table provides a sample event message for the Amazon AWS CloudTrail DSM:

Table 54. Amazon AWS CloudTrail sample message supported by Amazon AWS CloudTrail.

Event name	Low-level category	Sample log message
Console Login	General Audit Event	{"eventVersion": "1.02", "userIdentity": {"type": "IAMUser", "principalId": "XXXXXXXXXXXXXXXXXXXX", "arn": "arn:aws:iam::<Account_number>:user/xx.xxxxxxId": "<Account_number>", "userName": "<Username>"}, "eventTime": "2016-05-04T14:10:58Z", "eventSource": "f.amazonaws.com", "eventName": "ConsoleLogin", "awsRegion": "us-east-1", "sourceIPAddress": "<Source_IP_address> Agent": "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.1125.102 Safari/537.36", "requestParameters": null, "responseElements": {"ConsoleLogin": "Success"}, "additionalEventData": {"LoginTo": "www.webpage.com", "MobileVersion": "No", "MFAUsed": "No"}, "eventID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "eventType": "AwsConsoleSignIn", "recipientAccountId": "<Account_ID>"}

Related tasks:

"Adding a DSM" on page 4

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

"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 communication between IBM Security QRadar and AWS CloudTrail"

A certificate is required for the HTTP connection between QRadar and Amazon AWS CloudTrail.

"Configuring Amazon AWS CloudTrail to communicate with QRadar" on page 107

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

Enabling communication between IBM Security QRadar and AWS CloudTrail

A certificate is required for the HTTP connection between QRadar and Amazon AWS CloudTrail.

Before you begin

The Automatic Certificate download option is available for the Amazon AWS CloudTrail log source. To download the certificate automatically, select **Yes** for the **Automatically Acquire Server Certificate(s)** option when you configure the log source.

If you want to download the certificate manually, complete the following steps.

Procedure

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 on which you plan to configure the log source.

Verifying that Amazon AWS CloudTrail events are received

You can verify that you are collecting event data from the Amazon AWS CloudTrail S3 bucket.

Procedure

1. Log in to QRadar as an administrator.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. Select **Log Source [Indexed] > Equals** and browse for the name of your Amazon AWS CloudTrail log source.
5. Click **Add Filter**.
6. From the **View** menu, select **Last 15 minutes** or **Last Interval**.

Results

If the log source parameters are correct, the Amazon AWS CloudTrail should display events retrieved from the Amazon AWS ecosystem.

Related information:

- ➡ Amazon AWS CloudTrail documentation (www.amazon.com)
- ➡ QRadar: Unable to integrate with Amazon AWS CloudTrail (www.ibm.com/support)
- ➡ QRadar: Troubleshooting Amazon AWS CloudTrail.

Troubleshooting Amazon AWS 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.web.SimpleRESTFileLister: [ERROR] [NOT:0000003000] [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.qc.a(qc.java:728)
```

Cause:

This error was probably caused by exporting the Amazon SSL certificate from the incorrect URL.

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. The customer must export the certificate for the following URL:

<https://<bucketname>.s3.amazonaws.com>

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 on the proper QRadar appliance and in the proper directory.

```
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.semsources.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.semsources.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.semsources.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.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -] The current certificate white list is:
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.semsources.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.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -] Subject = O=SyslogTLS_Server, CN=*
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -]
Subject = CN=s3-console-us-standard.console.aws.amazon.com,
O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -] To establish trust in this server certificate,
place a copy in /opt/qradar/conf/trusted_certificates
```

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.
2. Enable the Amazon AWS CloudTrail log source.

If you downloaded the certificate manually, you must move the .DER certificate file to the correctQRadar 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. Firefox can create the required certificate with the .DER extension.
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 that manages the Amazon AWS CloudTrail log source 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 Amazon AWS CloudTrail to communicate with QRadar

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

Note: Alternatively, instead of using the **AmazonS3ReadOnlyAccess** permission you can assign more granular permissions to the bucket. The minimum required permissions are **s3:listBucket** and **s3:getObject**.

For more information about permissions 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 Amazon AWS user interface as 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 pencil icon on the right side of the window.
 - f. Click **Advanced >>**.
 - g. Note the location path for the S3 bucket that is displayed below the **Log file prefix** field.

What to do next

The QRadar user is ready to 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.

12 Ambiron TrustWave ipAngel

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

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

Table 55. Ambiron TrustWave ipAngel DSM specifications

Specification	Value
Manufacturer	Ambiron
DSM name	Ambiron TrustWave ipAngel
RPM file name	DSM-AmbironTrustwaveIpAngel-QRadar_version-build_number.noarch.rpm
Supported versions	V4.0
Protocol	Syslog
Recorded event types	Snort-based events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Ambiron website (http://www.apache.org)

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

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

Table 56. Ambiron TrustWave ipAngel log source parameters

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

13 APC UPS

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

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

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

Table 57. APC UPS DSM specifications

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

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

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

Table 58. APC UPS log source parameters

Parameter	Value
Log Source type	APC UPS
Protocol Configuration	Syslog

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

Related tasks:

[“Adding a DSM” on page 4](#)

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

“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 APC UPS to forward syslog events”

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

Configuring your APC UPS to forward syslog events

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

Procedure

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

14 Apache HTTP Server

The Apache HTTP Server DSM for IBM Security 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”
- “Configuring Apache HTTP Server with syslog-*ng*” on page 114

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.”

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”.

- <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 113.
 - <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 Security QRadar

You can configure a log source manually for Apache HTTP Server events in IBM Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 59. 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 Apache installations.

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/>.

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 114.

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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 60. 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 Apache installations.

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/>.

15 Apple Mac OS X

The IBM Security 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 Security 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

You can configure syslog on systems that run Mac OS X operating systems.

Procedure

1. Using SSH, log in to your Mac OS X 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:
`*.* @QRadar_IP_address`
4. Save and exit the file.
5. Send a hang-up signal to the syslog daemon to make sure that all changes are enforced:
`sudo killall - HUP syslogd`

The syslog configuration is complete. Events that are forwarded to IBM Security QRadar by your Apple Mac OS X are displayed on the **Log Activity** tab.

For more information about Mac OS X configurations, see your Mac OS X vendor documentation.

16 Application Security DbProtect

The IBM Security 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 61. Application Security DbProtect DSM specifications

Specification	Value
Manufacturer	Application Security, Inc
DSM name	DbProtect
RPM file name	DSM-AppSecDbProtect-QRadar_version-build_number.noarch.rpm
Supported versions	v6.2 v6.3 v6.3sp1 v6.3.1 v6.4
Protocol	LEEF
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Application Security website (http://www.appsecinc.com/)

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 62. Application Security DbProtect log source parameters

Parameter	Value
Log Source type	Application Security DbProtect
Protocol Configuration	Syslog

Installing the DbProtect LEEF Relay Module

To enable DbProtect to communicate with IBM Security 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

1. Download the DbProtect LEEF Relay module for DbProtect from the Application Security, Inc. customer portal (<http://www.appsecinc.com>).
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”

Configuring the DbProtect LEEF Relay

After you install the DbProtect LEEF Relay module, configure the service to forward events to IBM Security 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:

Parameter	Description
<code>SyslogListenerPort</code>	The port number that the DbProtect LEEF Relay uses to listen for syslog messages from the DbProtect console.

Parameter	Description
SyslogDestinationHost	The IP address of your QRadar Console or Event Collector.
SyslogDestinationPort	514
LogFile Name	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"

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**.

17 Arbor Networks

Several Arbor Networks DSMs can be integrated with IBM Security QRadar.

This section provides information on the following DSMs:

- “Arbor Networks Peakflow SP”
- “Arbor Networks Pravail” on page 127

Arbor Networks Peakflow SP

IBM Security 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 63. Arbor Networks Peakflow SP log source parameters

Parameter	Value
Log Source type	Arbor Networks Peakflow SP
Protocol Configuration	Select Syslog or TLS Syslog
Log Source Identifier	Type a unique name for the log source.

Related concepts:

“TLS syslog protocol configuration options” on page 47

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

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

"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 Security 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 Security 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 Security 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 Security 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 64. Arbor Networks Peakflow SP notification rule parameters

Parameter	Description
Name	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.
Resource	Type a CIDR address or select a managed object from the list of Peakflow resources.
Importance	Select the Importance of the rule.
Notification Group	Select the Notification Group that you assigned to forward syslog events to QRadar.

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 Security 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 65. System parameters

Parameter	Description
Log Source Identifier	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.
Credibility	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.
Target Event Collector	The event collector to use as the target for the log source.
Coalescing Events	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.
Incoming Event Payload	The incoming payload encoder for parsing and storing the logs.
Store Event Payload	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.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

Arbor Networks Pravail

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

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

Table 66. Arbor Networks Pravail DSM specifications

Specification	Value
Manufacturer	Arbor Networks
DSM	Arbor Networks Pravail
RPM file name	DSM-ArbornetworksPravail-build_number.noarch.rpm
Protocol	Syslog
Recorded events	All relevant events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Arbor Networks website (www.arbornetworks.com)

To send Arbor Networks Pravail 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 67. Arbor Pravail parameters

Parameter	Value
Log Source Type	Arbor Networks Pravail
Protocol Configuration	Syslog

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“Configuring your Arbor Networks Pravail system to send events to IBM Security 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” 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 Arbor Networks Pravail system to send events to IBM Security 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 68. Syslog parameters

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

7. Click **Save**.

18 Arpeggio SIFT-IT

The IBM Security 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
jrmtIP=<SourceIP_address> jrmtPort=543 jSeqNo=4755 jPgm=QWTMCMNL 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 Security 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 47](#)

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 Security 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**.

Additional information

After you create your IBM Security 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.

19 Array Networks SSL VPN

The Array Networks SSL VPN DSM for IBM Security 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 Security 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.

20 Aruba Networks

Several Aruba DSMs can be integrated with IBM Security QRadar.

This section provides information on the following DSMs:

- “Aruba ClearPass Policy Manager”
- “Aruba Mobility Controllers” on page 139

Aruba ClearPass Policy Manager

The IBM Security 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 69. Aruba ClearPass Policy Manager DSM specifications

Specification	Value
Manufacturer	Aruba Networks
DSM name	ClearPass
RPM file name	DSM-ArubaClearPass-Qradar_version-build_number.noarch.rpm
Supported versions	6.5.0.71095 and later
Event format	LEEF
Recorded event types	Session Audit System Insight
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Aruba Networks website (http://www.arubanetworks.com/products/security/)

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 70. Aruba ClearPass Policy Manager log source parameters

Parameter	Value
Log Source type	Aruba ClearPass Policy Manager
Protocol Configuration	Syslog

Related tasks:

“Adding a DSM” on page 4

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

“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 Security QRadar DSM for Aruba Introspect collects events from an Aruba Introspect device.

The following table describes the specifications for the Aruba Introspect DSM:

Table 71. Aruba Introspect DSM specifications

Specification	Value
Manufacturer	Aruba
DSM name	Aruba Introspect
RPM file name	DSM-ArubaIntrospect-QRadar_version-build_number.noarch.rpm
Supported versions	1.6
Protocol	Syslog
Event format	Name-value pair (NVP)

Table 71. Aruba Introspect DSM specifications (continued)

Specification	Value
Recorded event types	Security System Internal Activity Exfiltration Infection Command & Control
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Aruba website (https://www.arubanetworks.com)

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 72. Aruba Introspect log source parameters

Parameter	Value
Log Source type	Aruba Introspect
Protocol Configuration	Syslog
Log Source Identifier	A unique identifier for the log source.

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 73. Aruba Introspect sample event message

Event name	Low level category	Sample log message
Cloud Exfiltration	Suspicious Activity	<pre> 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 xxxxxxxxxxxxxxxxxxxxxx_xxxxxxx xxxxxxxx_Large_DropBox_Upload </pre>

Related tasks:

"Adding a DSM" on page 4

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

"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 Security 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 74. Aruba Introspect Analyzer forwarding parameters

Parameter	Value
Syslog Destination	IP or host name of the QRadar Event Collector.
Protocol	TCP or UDP
Port	514

3. Configure notification.
 - a. Click **System Configuration > Security Alerts / Emails > Add New**.
 - b. Configure the following notification parameters:

Table 75. Aruba Introspect Analyzer notification parameters

Parameter	Value
Enable Alert Syslog Forwarding	Enable the Enable Alert Syslog Forwarding check box.
Sending Notification	As Alerts are produced. You can customize this setting to send in batches instead of a live stream.
TimeZone	Your local time zone.

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 Security 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 Security 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 Security 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**.

21 Avaya VPN Gateway

The IBM Security 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 76. Avaya VPN Gateway DSM specifications

Specification	Value
Manufacturer	Avaya Inc.
DSM	Avaya VPN Gateway
RPM file name	DSM-AvayaVPNGateway-7.1-799033.noarch.rpm DSM-AvayaVPNGateway-7.2-799036.noarch.rpm
Supported versions	9.0.7.2
Protocol	syslog
QRadar recorded events	OS, System Control Process, Traffic Processing, Startup, Configuration Reload, AAA Subsystem, IPsec Subsystem
Automatically discovered	Yes
Includes identity	Yes
More information	http://www.avaya.com

Avaya VPN Gateway DSM integration process

You can integrate Avaya VPN Gateway DSM with IBM Security 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 Security 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 Security 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**.

22 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 Security QRadar.

BalaBit IT Security for Microsoft Windows Events

The Microsoft Windows Security Event Log DSM in IBM Security 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 Security 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 Security 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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure one of the following parameters from the table:

Table 77. Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from the BalaBit Syslog- ng Agent.

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 Security 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 Security 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 Security 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 Security 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 Security 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_tmfw { tcp("QRadar_IP" port(QRadar_PORT) log_disk_fifo_size(10000000)
template(t_tmfw)); }; 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 Security 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 Security 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 78. Syslog Parameters

Parameter	Description
Log Source Identifier	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- <i>ng</i> Agent.

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.

23 Barracuda

IBM Security QRadar supports a range of Barracuda devices.

The devices QRadar supports are:

- “Barracuda Spam & Virus Firewall”
- “Barracuda Web Application Firewall” on page 152
- “Barracuda Web Filter” on page 154

Barracuda Spam & Virus Firewall

You can integrate Barracuda Spam & Virus Firewall with IBM Security 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 Security 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 Security QRadar DSM for Barracuda Web Application Firewall collects syslog LEEF and custom events from Barracuda Web Application Firewall devices.

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

Table 79. Barracuda Web Application Firewall DSM specifications

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

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

1. If automatic updates are not enabled, download the most recent version of the following RPMs on your QRadar Console:
 - Barracuda Web Application Firewall DSM RPM
 - DSMCommon RPM
2. Configure your Barracuda Web Application Firewall device to send syslog events to QRadar.

- 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 80. Barracuda Web Application Firewall log source parameters

Parameter	Value
Log Source type	Barracuda Web Application Firewall
Protocol Configuration	Syslog

Configuring Barracuda Web Application Firewall to send syslog events to QRadar

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

Before you begin

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

Procedure

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

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

- 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**.
- 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:

Option	Description
Web Firewall Logs Facility	Select a syslog facility between Local0 and Local7 .
Access Logs Facility	Select a syslog facility between Local0 and Local7 .
Audit Logs Facility	Select a syslog facility between Local0 and Local7 .
System Logs Facility	Select a syslog facility between Local0 and Local7 .

Setting a syslog unique facility for each log type allows the Barracuda Web Application Firewall to divide the logs in to 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 Security QRadar.

The Barracuda Web Filter DSM for IBM Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure one of the following parameters:

Table 81. 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 Barracuda Web Filter appliance.

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.

24 BeyondTrust PowerBroker

The IBM Security 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 82. Syslog log source parameters

Parameter	Description
Log Source Type	BeyondTrust PowerBroker
Protocol Configuration	Syslog
Log Source Identifier	Type a unique IP address or host name.
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 83. TLS syslog log source parameters

Parameter	Value
Log Source type	BeyondTrust PowerBroker
Protocol Configuration	TLS Syslog
Log Source Identifier	Type a unique IP address or host name.

For more information about TLS syslog log source parameters, see TLS syslog protocol configuration options.

Related concepts:

[“TLS syslog protocol configuration options” on page 47](#)

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 159](#)

The following table describes the specifications for the BeyondTrust PowerBroker DSM.

[“Sample event messages” on page 160](#)

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

Related tasks:

"Adding a DSM" on page 4

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

"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"

BeyondTrust *pblogs* must be reformatted by using a script and then forwarded to IBM Security 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 Security 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 84. Command parameters

Parameters	Description
<code>-h</code>	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.
<code>-t</code>	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 " <code>pblog -l -t</code> ".
<code>-p</code>	The <code>-p</code> parameter defines the TCP port to be used when forwarding events. If nothing is specified, the default is port 514.
<code>-H</code>	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.
<code>-r</code>	The <code>-r</code> parameter defines the directory name where you want to create the process ID (.pid) file. The default is <code>/var/run</code> . This parameter is ignored if <code>-D</code> is specified.
<code>-l</code>	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.

Table 84. Command parameters (continued)

Parameters	Description
-D	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.
-f	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, <code>user.info</code> is used.
-a	The -a parameter enables an AIX® compatible <code>ps</code> method. This command is only needed when you run BeyondTrust PowerBroker on AIX systems.
-d	The -d parameter enables debug logging.
-v	The -v parameter displays the script version information.

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 85. BeyondTrust PowerBroker DSM specifications

Specification	Value
Manufacturer	BeyondTrust
DSM name	BeyondTrust PowerBroker
RPM file name	DSM-BeyondTrustPowerBroker-QRadar_version-build_number.noarch.rpm
Supported versions	4.0
Protocol	Syslog, TLS syslog
Event format	System, Application
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	BeyondTrust web page (https://www.beyondtrust.com/products/powerbroker/)

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 86. BeyondTrust PowerBroker sample syslog message

Event name	Low level category	Sample log message
Finish pbrun terminated	Information	<14>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 = "Finish" exitdate = "2011/10/30" exitstatus = "pbrun terminated: signal 1 (Hangup) unknown signal code" exittime = "21:01:49" i18n_exitdate = "10/30/11" " i18n_exittime = "21:01:49" logpid = 22085786 uniqueid = "ac15208e4eaddfffb1BB002"

25 BlueCat Networks Adonis

The BlueCat Networks Adonis DSM for IBM Security 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 Security 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 Security 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 Security 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:
`/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 Security QRadar

IBM Security 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 87. 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 BlueCat Networks Adonis appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

26 Blue Coat

IBM Security QRadar supports a range of Blue Coat products.

Blue Coat SG

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

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

Table 88. Blue Coat SG DSM specifications

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

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

1. If automatic updates are not enabled, download and install the most recent version of the Blue Coat SG DSM RPM on your QRadar Console.
2. Configure your Blue Coat SG device to communicate with QRadar. Complete the following steps:
 - Create a custom event format.
 - Create a log facility.
 - Enable access logging.
 - Configure Blue Coat SG for 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 89. Blue Coat SG log source parameters

Parameter	Value
Log Source type	Blue Coat SG Appliance
Protocol Configuration	Select either Log File or Syslog

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

- Custom Format

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

Related concepts:

[“Creating extra custom format key-value pairs” on page 169](#)

Related tasks:

[“Creating a log facility” on page 165](#)

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

[“Enabling access logging” on page 165](#)

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

[“Configuring a Blue Coat SG Log Source” on page 166](#)

You can manually configure a Blue Coat SG log source in QRadar.

[“Configuring Blue Coat SG for FTP uploads” on page 166](#)

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” on page 169](#)

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

Creating a custom event format

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

Procedure

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

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

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

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

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

Note: The custom format for QRadar supports more key-value pairs by using the Blue Coat ELFF format. For more information, see “Creating extra custom format key-value pairs” on page 169.

What to do next

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

Related tasks:

“Creating a log facility”

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

Creating a log facility

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

Procedure

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

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

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

Related tasks:

“Enabling access logging”

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

Enabling access logging

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

Procedure

1. Select **Configuration > Access Logging > General**.
2. Select the **Enable Access Logging** check box.
3. Optional: If you use Blue Coat SGOS 6.2.11.2 Proxy Edition, complete the following steps:
 - a. Select **Config > Policy > 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" on page 169

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

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

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

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

Configuring 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 90. Blue Coat SG log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow QRadar to identify a log file to a unique event source.
Service Type	<p>From the list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP.</p> <p>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.</p>
Remote IP or Hostname	Type the IP address or host name of the device that stores your event log files.
Remote Port	<p>Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535.</p> <p>The options include:</p> <ul style="list-style-type: none"> • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 <p>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.</p>
Remote User	<p>Type the user name necessary to log in to the host that contains your event files.</p> <p>The user name can be up to 255 characters in length.</p>
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	<p>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.</p> <p>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.</p>
Recursive	<p>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.</p> <p>The Recursive option is ignored if you configure SCP as the Service Type.</p>
FTP File Pattern	<p>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.</p> <p>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:</p> <pre>.*\.\log</pre> <p>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/</p>

Table 90. Blue Coat SG log file protocol parameters (continued)

Parameter	Description
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.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	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.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. QRadar examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your QRadar system for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the Event Generator list, select LineByLine . The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

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 Security 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**.
11. Click **Apply**.

Creating extra custom format key-value pairs

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

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

For example:

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

Table 91. Custom Format examples

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

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

Blue Coat Web Security Service

The IBM Security 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 92. Blue Coat Web Security Service DSM specifications

Specification	Value
Manufacturer	Blue Coat
DSM name	Blue Coat Web Security Service
RPM file name	DSM-BlueCoatWebSecurityService-Qradar_version-build_number.noarch.rpm
Event format	Blue Coat ELFF
Recorded event types	Access
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Blue Coat website (https://www.bluecoat.com)

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 93. Blue Coat Web Security Service log source parameters

Parameter	Value
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.

Table 93. Blue Coat Web Security Service log source parameters (continued)

Parameter	Value
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](#)

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

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 Security 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.

27 Box

The IBM Security QRadar DSM for Box collects enterprise events from a Box enterprise account.

The following table describes the specifications for the Box DSM:

Table 94. Box DSM specifications

Specification	Value
Manufacturer	Box
DSM name	Box
RPM file name	DSM-BoxBox-Qradar_version-build_number.noarch.rpm
Supported versions	N/A
Protocol	Box REST API
Event format	JSON
Recorded event types	Administrator and enterprise events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Box website (https://www.box.com/)

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 95. Box log source parameters

Parameter	Value
Log Source type	Box
Protocol Configuration	Box REST API
Client ID	Generated in the OAuth2 parameters pane of the Box administrator configuration.
Client Secret	Generated in the OAuth2 parameters pane of the Box administrator configuration.
Key ID	Generated in the Public Key Management pane after you submit the public key.
Enterprise ID	Used for access token request.
Private Key File Name	The private key file name in the /opt/qradar/conf/trusted_certificates/box/ directory in QRadar.

Table 95. Box log source parameters (continued)

Parameter	Value
Use Proxy	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.
Automatically Acquire Server Certificate(s)	Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.
EPS Throttle	The maximum number of events per second. The default is 5000.
Recurrence	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.

The following table shows a sample event message for Box:

Table 96. Box enterprise sample event message

Event name	Low level category	Sample log message
LOGIN	User Login Success	{ "source": { "type": "user", "id": "<UserID>", "name": "UserName", "login": "username@example.com" }, "created_by": { "type": "user", "id": "<UserID>", "name": "UserName", "login": "username@example.com" }, "created_at": "2016-01-07T10:54:30-08:00", "event_id": "363714450", "event_type": "LOGIN", "ip_address": "<IP_address>", "type": "event", "session_id": null, "additional_details": null }

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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 Security 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:

```
openssl genrsa -out box_private_key.pem 2048
```

- For a public key, type the following command:

```
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:

```
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.

- Create a directory that is named box in the opt/qradar/conf/trusted_certificates/ directory in QRadar.
- 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.
- 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 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 a Box Application**.
 - b. Record the **client ID**, and the **client secret** in the OAuth2 parameters pane. The log source is configured by using the **client ID** and the **client secret**.
 - c. Select **Server Authentication (OAuth2.0 with JWT)**, and then select **All Users**.
 - d. Record the API key that is in the Backend parameters pane. The API key is required to authorize the new App.
 - e. In the OAuth2 parameters pane, from the **User Access Settings** list, select **All Users**, and then configure the following parameters.

Table 97. User Access Settings parameters

Parameter	Value
Authentication Type:	Server Authentication (OAuth2.0 with JWT)
User Access:	All Users

Table 97. User Access Settings parameters (continued)

Parameter	Value
Scopes:	<p>Content Read and write all files and folders stored in Box</p> <p>Enterprise Manage an enterprise's properties. Allows the application to view and edit enterprise attributes and reports; edit and delete device pinners.</p> <p>Important: If you do not select the correct scopes, Box API displays an error message.</p>

2. Submit the public key, and then generate the key ID.
 - a. In the Public Key Management pane, click **Add Public Key**.
 - b. 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.
 - c. Click **Verify**.
 - d. Click **Save**, and then record the key ID for the log source configuration.
 - 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 **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 **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**.
 - 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>).

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.

28 Bridgewater

The Bridgewater Systems DSM for IBM Security 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 Security 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 Security 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 98. 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 Bridgewater Systems appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

29 Brocade Fabric OS

IBM Security 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 Security 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.

30 CA Technologies

IBM Security 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 Security 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/smfp 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.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (<http://www-01.ibm.com/support/docview.wss?uid=pub1sc27277200>).

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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 99. Log source parameters

Parameter	Value
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Creating a log source for Log File protocol

The Log File protocol enables IBM Security 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 100. Log File protocol parameters

Parameter	Value
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 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.
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. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.

Table 100. Log File protocol parameters (continued)

Parameter	Value
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/)
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 100. Log File protocol parameters (continued)

Parameter	Value
Processor	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.
Ignore Previously Processed File(s)	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.
Change Local Directory?	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.
Event Generator	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.

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 Security 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 Security 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 Security QRadar

IBM Security 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 -zvxf 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)
 - trsmain sample 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 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 terced 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:

```

//TRSMAIN JOB (yourvalidjobcard),Q11abs,
// MSGCLASS=V
//DEL EXEC PGM=IEFBR14
//D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXACF2.LOAD.TRS
// UNIT=SYSDA,
// SPACE=(CYL,(10,10))
//TRSMAN EXEC PGM=TRSMAN,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 TRSMAN. 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:

```

//QEXACF2 JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=OM
//*
//**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=OM
//*
//**QEXACF2 JCL VERSION 1.0 OCTOBER, 2010
//*
//***** Change below dataset names to sites specific datasets names*
//*****
//SET1 SET SMFIN='MVS1.SMF.RECORDS(0)',
// QEXOUT='Q1JACK.QEXACF2.OUTPUT',
// SMFOUT='Q1JACK.ACF2.DATA'
//*****
// Delete old datasets *
//*****
//DEL EXEC PGM=IEFBR14
//DD1 DD DISP=(MOD,DELETE),DSN=&SMFOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//DD2 DD DISP=(MOD,DELETE),DSN=&QEXOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//*****
// Allocate new dataset *
//*****
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DISP=(NEW,CATLG),DSN=&QEXOUT,
// SPACE=(CYL,(100,100)),
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*****

```

```

/* Execute ACFRPTPP (Report Preprocessor GR0) to extract ACF2*
/* SMF records *
//*****PRESCAN EXEC PGM=ACFRPTPP
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//RECMAN1 DD DISP=SHR,DSN=&SMFIN
//SMFFLT DD DSN=&SMFOUT,SPACE=(CYL,(100,100)),DISP=(,CATLG),
// DCB=(RECFM=FB,LRECL=8192,BLKSIZE=40960),
// UNIT=SYSALLDA
//*****execute QEXACF2 *
//*****EXTRACT EXEC PGM=QEXACF2,DYNAMNBR=10,
// TIME=1440
//STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN DD DUMMY
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//CFG DD DUMMY
//ACFIN DD DISP=SHR,DSN=&SMFOUT
//ACFOUT DD DISP=SHR,DSN=&QEXOUT
//*****FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//*

```

- 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 '<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.

- 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 Security QRadar by using syslog-*ng*.

Configuring a log source

CA SiteMinder with IBM Security 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 101. Adding a syslog log source

Parameter	Description
Log Source Identifier	Type the IP address or host name for your CA SiteMinder appliance.

Table 101. Adding a syslog log source (continued)

Parameter	Description
Enabled	Select this check box to enable the log source. By default, this check box is selected.
Credibility	From the list, type the credibility value 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 device. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Target Event Collector to use as the target for the log source.
Coalescing Events	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 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 Security QRadar <i>Administration Guide</i> .
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. 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 Security QRadar <i>Administration Guide</i> .

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 Security 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 Security 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.
4. If you want to create a custom event property for CA Top Secret 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.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (<http://www-01.ibm.com/support/docview.wss?uid=pub1sc27277200>).

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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 102. Log File protocol parameters

Parameter	Value
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 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.
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. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.

Table 102. Log File protocol parameters (continued)

Parameter	Value
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/)
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.
Processor	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.

Table 102. Log File protocol parameters (continued)

Parameter	Value
Ignore Previously Processed File(s)	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.
Change Local Directory?	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.
Event Generator	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.

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 Security 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 103. Log source parameters

Parameter	Value
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Integrate CA Top Secret with IBM Security 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 Security 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 Security 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 -zvxf 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 terced 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),Q11abs,  
// MSGCLASS=V  
//DEL EXEC PGM=IEFBR14  
//D1 DD DISP=(MOD,DELETE),DSN=<yourh1q>.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=<yourh1q>.QEXTOPS.TRS  
//OUTFILE DD DISP=(NEW,CATLG,DELETE),  
// DSN=<yourh1q>.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  
//DD1 DD DISP=(MOD,DELETE),DSN=&TSSOUT,  
// UNIT=SYSDA,  
// SPACE=(CYL,(10,10)),  
// DCB=(RECFM=FB,LRECL=80)  
//DD2 DD DISP=(MOD,DELETE),DSN=&EARLOUT,  
// UNIT=SYSDA,  
// SPACE=(CYL,(10,10)),  
// DCB=(RECFM=FB,LRECL=80)  
//*****  
//** Allocate new dataset *  
//*****  
//ALLOC EXEC PGM=IEFBR14  
//DD1 DD DISP=(NEW,CATLG),DSN=&EARLOUT,  
// SPACE=(CYL,(100,100)),  
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)  
//*****  
//** Execute Top Secret TSSUTIL utility to extract smf records*  
//*****
```

```

//REPORT EXEC PGM=TSSUTIL
//SMFIN DD DISP=SHR,DSN=&SMFIN1
//SMFIN1 DD DISP=SHR,DSN=&SMFIN2
//UTILOUT DD DSN=&UTILOUT,
// DISP=(,CATLG),UNIT=SYSDA,SPACE=(CYL,(50,10),RLSE),
// DCB=(RECFM=FB,LRECL=133,BLKSIZE=0)
//EARLOUT DD DSN=&TSSOUT,
// DISP=(NEW,CATLG),UNIT=SYSDA,
// SPACE=(CYL,(200,100),RLSE),
// DCB=(RECFM=VB,LRECL=456,BLKSIZE=27816)
//UTILIN DD *
NOLEGEND
REPORT EVENT(ALL) END
/*
//*****+
//EXTRACT EXEC PGM=QEXTOPS,DYNAMNBR=10,
// TIME=1440
//STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSSIN DD DUMMY
//SYSTSPPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//CFG DD DUMMY
//EARLIN DD DISP=SHR,DSN=&TSSOUT
//EARLOUT DD DISP=SHR,DSN=&EARLOUT
//*****+
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*

```

- After the output file is created, schedule a job to a 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>/<EARLOUT>
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>/CA/QEXTOPS.OUTPUT.C320
```

<QEXTOUTDSN> 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.

- 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:

```
//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.

31 Carbon Black

Several Carbon Black DSMs can be integrated with IBM Security QRadar

Carbon Black

The IBM Security 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 104. Carbon Black DSM specifications

Specification	Value
Manufacturer	Carbon Black
DSM name	Carbon Black
RPM file name	DSM-CarbonBlackCarbonBlack-Qradar_version-build_number.noarch.rpm
Supported versions	5.1 and later
Protocol	Syslog
Recorded event types	Watchlist hits
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Carbon Black website (https://www.carbonblack.com/products/cb-response/)

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 105. Carbon Black log source parameters

Parameter	Value
Log Source type	Carbon Black
Protocol Configuration	Syslog

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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:

```
cd /etc/yum.repos.d
curl -o https://opensource.carbonblack.com/release/x86_64/CbOpenSource.repo
```
2. Install the RPM for cb-event-forwarder:

```
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: `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:
`/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 Security 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 106. Carbon Black Protection DSM Specifications

Specification	Value
Manufacturer	Carbon Black
DSM name	Carbon Black Protection
RPM filename	<code>DSM-CarbonBlackProtection-QRadar_version-build_number.noarch.rpm</code>
Supported versions	8.0.0, 8.1.0
Protocol	Syslog
Event format	LEEF
Recorded event types	Computer Management, Server Management, Session Management, Policy Management, Policy Enforcement, Internal Events, General Management, Discovery
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	https://www.carbonblack.com/products/carbon-black-enterprise-protection/

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 107. Carbon Black Protection log source parameters

Parameter	Value
Log source type	Carbon Black Protection
Log source identifier	IP address or host name for the log source
Protocol configuration	Syslog

4. Verify that Carbon Black Protection is configured correctly.

The following table provides a sample event message for the Carbon Black Protection DSM:

Table 108. Carbon Black Protection sample message supported by the Carbon Black Protection device

Event name	Low level category	Sample log message
Console user login	User login success	<pre> LEEF:1.0 Carbon_Black Protection 8.0.0.2141 Console_user_login cat=Session Management sev=4 devTime=Mar 09 2017 18:32:14.360 UTC msg=User '<Username>' logged in from <IP_address>. externalId=12345 src=<Source_IP_address> usrName=<Username> dstHostName=hostname receivedTime=Mar 09 2017 18:32:14.360 UTC </pre>

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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

- Access the Carbon Black Protection console by entering the Carbon Black Protection server URL in your browser.
- On the login screen, enter your username and password. You must use a Carbon Black Protection account with Administrator or Power User privileges.
- From the top console menu, select **System Configuration** in the Administration section.
- On the System Configuration page, click on the **Events** tab.
- 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.
- Change the Syslog format to LEEF (Q1Labs).
- Check **Syslog Enabled** for Syslog output.
- Click **Update** to confirm the changes.

Bit9 Parity

To collect events, you must configure your Bit9 Parity device to forward syslog events in Log Event Extended Format (LEEF).

Procedure

- Log in to the Bit9 Parity console with Administrator or PowerUser privileges.
 - From the navigation menu on the left side of the console, select **Administration > System Configuration**.
- The System Configuration window is displayed.
- 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 Security QRadar as Bit9 Parity events are automatically discovered. Events that are forwarded to QRadar by Bit9 Parity are displayed on the **Log Activity** tab of QRadar.

Configure a log source

IBM Security QRadar automatically discovers and creates a log source for syslog events from 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 109. 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 Bit9 Parity device.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

Bit9 Security Platform

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

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

Table 110. DSM specifications for Bit9 Security Platform

Specification	Value
Manufacturer	Carbon Black
DSM name	Bit9 Security Platform

Table 110. DSM specifications for Bit9 Security Platform (continued)

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

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

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

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

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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 Bit9 Security Platform to communicate with QRadar

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

Procedure

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

32 Centrify Infrastructure Services

The IBM Security 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 111. Centrify Infrastructure Services DSM specifications

Specification	Value
Manufacturer	Centrify
DSM name	Centrify Infrastructure Services
RPM file name	DSM-CentrifyInfrastructureServices-QRadar_version-build_number.noarch.rpm
Supported versions	Centrify Infrastructure Services 2017
Protocol	Syslog, TLS Syslog and WinCollect
Event format	name-value pair (NVP)
Recorded event types	Audit Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Centrify website (https://www.centrify.com/support/documentation/server-suite/)

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 112. Centrify Infrastructure Services log source parameters

Parameter	Value
Log Source type	Centrify Infrastructure Services
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the UNIX, Linux, or Windows device that sends Centrify Infrastructure Services events to QRadar.

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.

Table 113. Centrify Infrastructure Services TLS Syslog log source parameters

Parameter	Value
Log Source type	Centrify Infrastructure Services
Protocol Configuration	TLS Syslog
Log Source Identifier	Type a unique identifier for the log source.
TLS Protocols	Select the version of TLS that is installed on the client.

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.

Related concepts:

“TLS syslog protocol configuration options” on page 47

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

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

“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 Security 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 114. WinCollect log source parameters

Parameter	Value
Log Source type	Centrify Infrastructure Services
Protocol Configuration	WinCollect
Log Source Identifier	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.
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.

Table 114. WinCollect log source parameters (continued)

Parameter	Value
Event Rate Tuning Profile	<p>For the default polling interval of 3000 ms, the approximate Events per second (EPS) rates attainable are as follows:</p> <ul style="list-style-type: none"> Default (Endpoint): 33-50 EPS Typical Server: 166-250 EPS High Event Rate Server: 416-625 EPS <p>For a polling interval of 1000 ms, the approximate EPS rates are as follows:</p> <ul style="list-style-type: none"> Default (Endpoint): 100-150 EPS Typical Server: 500-750 EPS High Event Rate Server: 1250-1875 EPS <p>For more information about tuning WinCollect, go to the IBM Support website (http://www.ibm.com/support/docview.wss?uid=swg21672193).</p>
Polling Interval (ms)	The interval, in milliseconds, between times when WinCollect polls for new events.
Application or Service Log Type	Select None for the Application or Service Log Type .
Standard Log Types	<p>Do not enable the check box for any of the log types.</p> <p>Select No Filtering as the log filter type for the following log types: Security, System, Application, DNS Server, File Replication Service, and Directory Service.</p>
Event Types	You must select at least one event type.
XPath Query	<p>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.</p> <p>For more information about creating an XPath query, go to the Creating a custom view documentation on the IBM Support website (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.wincollect.doc/t_cg_wincollect_creating_customview.html).</p> <p>Important: When you create the custom view, ensure that the By Source option is selected. From the Event sources list, select the application name of the Centrify Audit Events.</p> <p>Example XPath query:</p> <pre><QueryList> <Query Id="0" Path="Application"> <SelectPath="Application">*[System[Provider[@Name='Centrify AuditTrailV2']]］</Select> </Query> </QueryList></pre>
Enable Active Directory Lookups	Do not select the check box.
WinCollectAgent	Select your WinCollect agent from the list.
Target Internal Destination	Use any managed host with an event processor component as an internal destination.

For more information about WinCollect log source parameters, go to the Common WinCollect log source parameters documentation on the IBM Support website (https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.wincollect.doc/r_ug_wincollect_comon_parameters.html).

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 Security 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:
`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:
`:msg, contains, "AUDIT_TRAIL" @@<QRadar Event Collector IP>:514`
Example: `: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 115. Centrify Infrastructure Services sample message

Event name	Low-level category	Sample log message
Remote login success	Remote Access Login Succeeded	<13>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: Remote login success Message: User successfully logged on remotely using role 'Windows Login/CentrifyTest'. May 09 16:58:41 centrifywindowsagent. centrify.lab dzagent[2008]: INFO AUDIT_TRAIL Centrify Suite DirectAuthorize - Windows 1.0 3 Remote login success 5 user=username userSid=domain \username sessionId=6 centrify EventID=6003 DAInst=N/A DASess ID=N/A role=Windows Login/ CentrifyTest desktopguid=7678b3 5e-00d0-4ddf-88f5-6626b8b1ec4b
The user logged in to the system successfully	User Login Success	<38>May 4 23:45:19 hostname adclient[1472]: INFO AUDIT _TRAIL Centrify Suite Centrify Commands 1.0 200 The user login to the system successfully 5 user =user pid=1234 utc=1493952319951 centrifyEventID=18200 DASessID= c6b7551c-31ea-8743-b870- cdef47393d07 DAInst=Default Installation status=SUCCESS service =sshd tty=/dev/pts/2

33 Check Point

Several Check Point products can be integrated with IBM Security 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 Security 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”
- “Integrate Check Point by using syslog” on page 220
- “Integration of Check Point Firewall events from external syslog forwarders” on page 222

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 Security 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 Security 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 Security 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 116. OPSEC Application Properties

Parameter	Value
Name	QRadar-OPSEC
Host	QRadar
Client Entities	LEA

- 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:

```
CN=QRadar=OPSEC,O=cpmodule..tdfaaz
```

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 Security 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 117. OPSEC/LEA protocol parameters

Parameter	Description
Log Source Identifier	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.
Server IP	Type the IP address of the Check Point host or Check Point Management Server IP.
Server Port	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.
Use Server IP for Log Source	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.
Statistics Report Interval	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.
Authentication Type	From the list, select the Authentication Type that you want for this LEA configuration. The options are as follows: <ul style="list-style-type: none">• 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.
OPSEC Application Object SIC Attribute (SIC Name)	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.
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.

Table 117. OPSEC/LEA protocol parameters (continued)

Parameter	Description
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 Security 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 Security 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 Security QRadar is complete.

Changing the default port for OPSEC LEA communication

Change the default port (18184) on which OPSEC LEA communicates.

Procedure

- At the command-line prompt of your Check Point SmartCenter Server, type the following command to stop the firewall services:
cpstop
- 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:

```
# 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 #
```

- Change the default **lea_server auth_port** from 18184 to another port number.
- Remove the hash (#) mark from that line.

Example:

```
lea_server auth_port 18888 # lea_server port 0
```

- Save and close the file.
- 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

- At the command-line prompt of your Check Point SmartCenter Server, stop the firewall services by typing the following command:
cpstop
- Depending on your Check Point SmartCenter Server operating system, open the following file:
 - Linux - \$FWDIR\conf\fwopsec.conf
 - Windows - %FWDIR%\conf\fwopsec.conf
- Change the default **lea_server auth_port** from 18184 to 0.
- Change the **default lea_server port** from 0 to 18184.
- Remove the hash (#) marks from both lines.

Example:

```
lea_server auth_port 0 lea_server port 18184
```

- Save and close the file.
- Type the following command to start the firewall services:
cpstart

Configuring IBM Security QRadar to receive events from a Check Point device

Configure IBM Security 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 118. OPSEC/LEA protocol parameters

Parameter	Description
Log Source Identifier	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.
Server IP	Type the IP address of the server.
Server Port	Type the port number that is used for OPSEC communication. The valid range is 0 - 65,536 and the default port used by QRadar is 18184.
Use Server IP for Log Source	Select the Use Server IP for Log Source check box if you want to use the LEA server IP address instead of the managed device IP address for a log source. By default, the check box is selected.
Statistics Report Interval	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.

Table 118. OPSEC/LEA protocol parameters (continued)

Parameter	Description
Authentication Type	<p>From the list, select the Authentication Type that you want to use for this LEA configuration. The options are <code>sslca</code> (default), <code>sslca_clear</code>, or <code>clear</code>. This value must match the authentication method that is used by the server. The following parameters appear if <code>sslca</code> or <code>sslca_clear</code> is selected as the authentication type:</p> <ul style="list-style-type: none"> • OPSEC Application Object SIC Attribute (SIC Name) - 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: <code>CN=LEA, o=fwconsole..7psasx</code>. The name can be up to 255 characters in length and is case-sensitive. • Log Source SIC Attribute (Entity SIC Name) - Type the SIC name of the server, for example: <code>cn=cp_mgmt, o=fwconsole..7psasx</code>. The name can be up to 255 characters in length and is case-sensitive. • Specify Certificate - 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. <p>If you select the Specify Certificate check box, the Certificate Filename parameter is displayed:</p> <ul style="list-style-type: none"> • Certificate Filename - 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 <code>/opt/qradar/conf/trusted_certificates/lea</code> directory. <p>If you clear the Specify Certificate check box, the following parameters appear:</p> <ul style="list-style-type: none"> • 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. The password can be up to 255 characters in length. • 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. <p>Important: Access to port 18210 is required for certificate pulls.</p>

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 Security QRadar Check Point DSMs accept Check Point events with syslog.

Before you configure IBM Security 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:
`expert`
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 Security 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 119. Syslog parameters

Parameter	Value
Log Source Identifier	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.

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 Security 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 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 Security 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 120. Syslog redirect protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for the Check Point Firewall events. The log source identifier must be unique value.
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. <code>orig=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})</code>
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.
Credibility	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.
Target Event Collector	From the list, select the Target Event Collector to use as the target for the log source.
Coalescing Events	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.
Incoming Event Payload	From the Incoming Event Payload list, select the incoming payload encoder for parsing and storing the logs.

Table 120. Syslog redirect protocol parameters (continued)

Parameter	Description
Store Event Payload	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.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

Check Point Multi-Domain Management (Provider-1)

You can configure IBM Security 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)”
- “Configuring OPSEC for Check Point Multi-Domain Management (Provider-1)” on page 225

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 Security 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 Security 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:

Table 121. 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 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 Security 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 *lepipe* 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 Security 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,0=cpmodule...tdfaaz, 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 33](#)

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

34 Cilasoft QJRN/400

IBM Security 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 Security 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 122. Cilasoft QJRN/400 output parameters

Parameter	Description
Format	Type *LEEF to configure the syslog output to write events in Log Extended Event Format (LEEF). LEEF is a special event format that is designed to for IBM Security QRadar.

Table 122. Cilasoft QJRN/400 output parameters (continued)

Parameter	Description
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 Security QRadar system. If an IP address for IBM Security 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 Security 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 Security QRadar.
Facility	This field is not used by IBM Security 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 <i>Cilasoft documentation</i> .

For more information on Cilasoft configuration parameters, see the *Cilasoft QJRN/400 User's Guide*.

Syslog events that are forwarded to IBM Security QRadar are viewable on the **Log Activity** tab.

Configuring a Cilasoft QJRN/400 log source

IBM Security 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 Security 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 123. Syslog protocol parameters

Parameter	Description
Log Source Identifier	Enter the IP address as an identifier for events from your Cilasoft QJRN/400 installation. The Log Source Identifier must be unique value.
Enabled	Select the Enabled check box to enable the log source. By default, the check box is selected.
Credibility	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.
Target Event Collector	Select the Target Event Collector to use as the target for the log source.
Coalescing Events	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 IBM Security 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.
Incoming Event Payload	From the list, select the Incoming Event Payload encoder for parsing and storing the logs.
Store Event Payload	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 IBM Security 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.

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

Related concepts:

["Log File protocol configuration options" on page 21](#)

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

35 Cisco

Several Cisco DSMs can be integrated with IBM Security QRadar.

Cisco ACE Firewall

The Cisco ACE firewall can be integrated with IBM Security 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 Security 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 Security 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 124. 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 ACE Firewalls.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
The configuration is complete.

Cisco Aironet

You can integrate Cisco Aironet devices with IBM Security 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 Security 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 125. 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 Aironet appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

Cisco ACS

The Cisco ACS DSM for IBM Security 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.”
- 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 238.
- Configure your Cisco ACS device to directly send UDP multiline syslog to QRadar. See “Configuring UDP multiline syslog for Cisco ACS appliances” on page 51

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 126. Remote target parameters

Parameter	Description
Name	Type a name for the remote syslog target.
Description	Type a description for the remote syslog target.
Type	Select Syslog .
IP address	Type the IP address of QRadar or your Event Collector.

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 Security 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 Security 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 127. Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for Cisco ACS events.

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 Security 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:
 - **Message-Type**
 - **User-Name**
 - **Nas-IP-Address**
 - **Authen-Failure-Code**
 - **Caller-ID**
 - **NAS-Port**
 - **Author-Data**
 - **Group-Name**
 - **Filter Information**
 - **Logged Remotely**
7. Configure the following syslog parameters:

Table 128. Syslog parameters

Parameter	Description
IP	Type the IP address of QRadar.
Port	Type the syslog port number of IBM Security QRadar. The default is port 514.
Max message length (Bytes) - Type	Type 1024 as the maximum syslog message length.

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 Security 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 129. Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for Cisco ACS events.

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 130. Cisco ACS log source parameters

Parameter	Value
Log Source Identifier	Type the IP address, host name, or name to identify your Cisco ACS appliance.
Listen Port	<p>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.</p> <p>To edit a saved configuration to use a new port number, complete the following steps.</p> <ol style="list-style-type: none">1. In the Listen Port field, type the new port number for receiving UDP Multiline Syslog events.2. Click Save. <p>The port update is complete and event collection starts on the new port number.</p>
Message ID Pattern	\s(\d{10})\s
Event Formatter	Select Cisco ACS Multiline from the list.

Related concepts:

"UDP multiline syslog protocol configuration options" on page 49

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 ASA

You can integrate a Cisco Adaptive Security Appliance (ASA) with IBM Security 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"
- Forward events to QRadar by using NetFlow (NSEL). See "Integrate Cisco ASA for NetFlow by using NSEL" on page 242

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"
- "Configuring a log source" on page 241

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 Security 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 Security 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 131. Syslog parameters*

| Parameter                    | Description                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your OSSEC installations. |

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”
- “Configuring a log source” on page 243

## 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 Security 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 242.

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 242 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 Security 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 132. Syslog parameters*

| Parameter                    | Description                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source.                                                                                                                                                                                                                                                                                                         |
| <b>Collector Port</b>        | <p>Type the UDP port number that is used by Cisco ASA to forward NSEL events. The valid range of the <b>Collector Port</b> parameter is 1-65535.</p> <p>QRadar typically uses port 2055 for NetFlow event data on the QRadar QFlow Collector. You must define a different UDP port on your Cisco Adaptive Security Appliance for NetFlow that uses NSEL.</p> |

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.

## Cisco CallManager

The Cisco CallManager DSM for IBM Security 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**.  
The Enterprise Parameters Configuration is displayed.
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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 133. 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 CallManager. |

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 Security 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 Security 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 Security 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 134. Syslog parameters

| Parameter                    | Description                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Cisco CatOS for Catalyst Switch appliance. |

11. Click **Save**.

12. On the Admin tab, click Deploy Changes.

The configuration is complete.

---

## Cisco Cloud Web Security

The IBM Security 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 135. Cisco Cloud Web Security DSM specifications*

| Specification               | Value                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------------|
| Manufacturer                | Cisco                                                                                                     |
| DSM name                    | Cisco Cloud Web Security                                                                                  |
| RPM file name               | DSM-CiscoCloudWebSecurity-QRadar_version-build_number.noarch.rpm                                          |
| Supported versions          | N/A                                                                                                       |
| Protocol                    | Amazon AWS S3 REST API                                                                                    |
| Event format                | W3C                                                                                                       |
| Recorded event types        | All web usage logs                                                                                        |
| Automatically discovered?   | No                                                                                                        |
| Includes identity?          | No                                                                                                        |
| Includes custom properties? | No                                                                                                        |
| More information            | Cisco CWS product information ( <a href="https://www.cisco.com/go/cws">https://www.cisco.com/go/cws</a> ) |

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 136. Cisco Cloud Web Security log source parameters*

| Parameter              | Value                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Source type        | Cisco Cloud Web Security                                                                                                                                                                                                                                                                                                                                                                         |
| Protocol Configuration | Amazon AWS S3 REST API                                                                                                                                                                                                                                                                                                                                                                           |
| Log Source Identifier  | The <b>Log Source Identifier</b> can be any valid value and does not need to reference a specific server. The <b>Log Source Identifier</b> can be the same value as the <b>Log Source Name</b> . If you configured more than one Cisco CWS log source, you might want to identify the first log source as ciscocws1, the second log source as ciscocws2, and the third log source as ciscocws13. |

Table 136. Cisco Cloud Web Security log source parameters (continued)

| Parameter                                          | Value                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Signature Version</b>                           | Select <b>Signature Version 2</b> .<br><br>If your Cisco CWS API is using <b>Signature Version 4</b> , contact your system administrator.                                                                                                                                                                                                                                                |
| <b>Region Name</b> (Signature V4 only)             | The region that is associated with the Amazon S3 bucket.                                                                                                                                                                                                                                                                                                                                 |
| <b>Service Name</b> (Signature V4 only)            | Type <code>s3</code> . The name of the Amazon Web Service.                                                                                                                                                                                                                                                                                                                               |
| <b>Bucket Name</b>                                 | The name of the Cisco CWS bucket where the log files are stored.                                                                                                                                                                                                                                                                                                                         |
| <b>Endpoint URL</b>                                | <code>https://vault.scansafe.com/</code>                                                                                                                                                                                                                                                                                                                                                 |
| <b>Public Key</b>                                  | The access key to enable log extraction from the Cisco CWS bucket.                                                                                                                                                                                                                                                                                                                       |
| <b>Access Key</b>                                  | The secret key to enable log extraction from the Cisco CWS bucket.                                                                                                                                                                                                                                                                                                                       |
| <b>Directory Prefix</b>                            | The location of the root directory on the Cisco CWS storage bucket from where the Cisco CWS logs are retrieved. For example, the root directory location might be <code>cws-logs/</code> .                                                                                                                                                                                               |
| <b>File Pattern</b>                                | <code>.*?\.\txt\.\gz</code>                                                                                                                                                                                                                                                                                                                                                              |
| <b>Event Format</b>                                | <b>W3C</b> . The log source retrieves W3C text formatted events.                                                                                                                                                                                                                                                                                                                         |
| <b>Use Proxy</b>                                   | When a proxy is configured, all traffic for the log source travels through the proxy so that QRadar can access the Amazon AWS S3 buckets.<br><br>Configure the <b>Proxy Server</b> , <b>Proxy Port</b> , <b>Proxy Username</b> , and <b>Proxy Password</b> fields. If the proxy does not require authentication, leave the <b>Proxy Username</b> and <b>Proxy Password</b> fields blank. |
| <b>Automatically Acquire Server Certificate(s)</b> | If you select <b>Yes</b> , QRadar downloads the certificate and begins trusting the target server.                                                                                                                                                                                                                                                                                       |
| <b>Recurrence</b>                                  | 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.<br><br>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.             |

The following table shows a sample event message from Cisco Cloud Web Security:

Table 137. Cisco Cloud Web Security sample message

| Event name     | Low level category | Sample log message                                                                                                                                                                                                                                                                                 |
|----------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| c:comp - block | Access Denied      | <pre>2016-08-22 18:22:34 GMT &lt;IP_address1&gt; &lt;IP_address1&gt; GET http www.example.com 80 / 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</pre> |

**Related tasks:**

“Adding a DSM” on page 4

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

“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 Security 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* on the Cisco website (<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 Security 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 Security 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 Security 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**.
  9. Using the **Protocol Configuration** list, select **Syslog**.

The syslog protocol configuration is displayed.

  10. Configure the following values:

*Table 138. Syslog parameters*

| Parameter                    | Description                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | 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 FireSIGHT Management Center

The IBM Security QRadar DSM for Cisco FireSIGHT Management Center collects FireSIGHT Management Center events by using the eStreamer API service.

Cisco FireSIGHT Management Center is formerly known as Sourcefire Defense Center.

QRadar supports FireSIGHT Management Center version 5.2 to version 6.2.0.1

### Configuration overview

To integrate with FireSIGHT Management Center, you must create certificates in the FireSIGHT Management Center interface, and then add the certificates to the QRadar appliances that receive eStreamer event data.

If your deployment includes multiple FireSIGHT 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 FireSIGHT 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 FireSIGHT Management Center, use the following steps:

1. Create the eStreamer certificate on your FireSIGHT Management Center appliance.
2. Import a Cisco FireSIGHT Management Center certificate in QRadar.
3. Configure a log source in QRadar for your FireSIGHT Management Center appliances.

### Supported event types

QRadar supports the following event types from FireSIGHT 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 FireSIGHT 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 FireSIGHT 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 FireSIGHT Management Center.

The following table provides sample event messages for the Cisco FireSIGHT Management Center DSM:

*Table 139. Cisco FireSIGHT Management Center sample messages supported by the Cisco FireSIGHT Management Center device.*

| Event name                | Low level category       | Sample log message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Login Change Event   | Computer Account Changed | <pre>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; MACAddres s=&lt;MAC_address&gt; hasIPv6=true eventSecond=1430491035 eve ntMicroSecond=0 eventType=USER_ LOGIN_INFORMATION fileNumber=00 000000 filePosition=00000000 ipV6Address=&lt;IPv6_address&gt; userLoginInformation.timestamp= 1430491035 userLoginInformati on.ipv4Address=&lt;IP_address&gt; userLog inInformation.userName=username userLoginInformation.userRef=0 userLoginInformation.protocol Ref=710 userLoginInformation.ema il= userLoginInformation.ipv6Ad dress=&lt;IP_address&gt; userLoginIn formation.loginType=0 userLogi nInformation.reportedBy=IPAddress"</pre> |
| User Removed Change Event | User Account Removed     | <pre>DeviceType=Estreamer DeviceAddress =&lt;IP_address&gt; CurrentTime=15077 43344985 netmapId=0 recordTyp e=USER_REMOVED_CHANGE_EVENT reco rdLength=191 timestamp=21 Sep 201 7 14:53:14 detectionEngineRef= 0 ipAddress=&lt;IP_address&gt; MACAddress =&lt;MAC_address&gt; hasIPv6=true eventSecond=1506016392 event MicroSecond=450775 eventType=DELE TE_USER_IDENTITY fileNumber=000 000 filePosition=00000000 ip V6Address=&lt;IPv6_address&gt; userIn formation.id=1 userInformatio n.userName=username userInformati on.protocol=710 userInformation .firstName=firstname userInformation .lastName=lastname userInformation .email=EmailAddress userInformation.department=R esearch userInformation.phone =000-000-0000</pre>                                                                                              |

*Table 139. Cisco FireSIGHT Management Center sample messages supported by the Cisco FireSIGHT Management Center device. (continued)*

| Event name                        | Low level category | Sample log message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| INTRUSION EVENT EXTRA DATA RECORD | Information        | DeviceType=Estreamer DeviceAddress=<IP_address> CurrentTime=1507740690263 netmapId=0 recordType=INTRUSION_EVENT_EXTRA_DATA_RECORD recordLength=49 timestamp=01 May 2015 15:32:53 eventExtraData.eventId=393275 eventExtraData.eventSecond=1430505172 eventExtraData.managedDevice.managedDeviceId=6 eventExtraData.managedDevice.name=manageddevice.e.<Server>.example.com eventExtraData.extraDataType.eventExtraDataType.type=10 eventExtraData.extraDataType.name=HTTP Hostname eventExtraData.extraDataType.eventExtraDataType.encoding=String eventExtraData.extraData.www.example.com |
| RUA User record                   | Information        | DeviceType=Estreamer DeviceAddress=<IP_address> CurrentTime=1507740603372 netmapId=0 recordType=RUA_USER_RECORD recordLength=21 timestamp=11 Oct 2017 13:50:02 userRef=2883 protocolRef=710 userName=UserName                                                                                                                                                                                                                                                                                                                                                                               |

#### Related tasks:

[“Creating Cisco FireSIGHT Management Center 5.x and 6.x certificates”](#)

IBM Security QRadar requires a certificate for every FireSIGHT 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 FireSIGHT Management Center certificate in QRadar” on page 255](#)

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 FireSIGHT Management Center pkcs12 certificate that you need to import to your QRadar Console or Event Collector.

[“Configuring a log source for Cisco FireSIGHT Management Center events” on page 256](#)

QRadar does not automatically discover Cisco FireSIGHT Management Center events. You must configure a log source in QRadar.

[“Adding a DSM” on page 4](#)

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

## Creating Cisco FireSIGHT Management Center 5.x and 6.x certificates

IBM Security QRadar requires a certificate for every FireSIGHT 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 FireSIGHT 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 FireSIGHT Management Center to send to QRadar, and then click **Save**.

The following image lists the types of events that FireSIGHT Management Center sends to QRadar.

The screenshot shows the 'eStreamer Event Configuration' section of the FireSIGHT Management Center. On the left, a sidebar lists various event types with checkboxes: Discovery Events, Correlation and White List Events, Impact Flag Alerts, Intrusion Events, Intrusion Event Packet Data, User Activity, Intrusion Event Extra Data, Malware Events, File Events, and Connection Events. At the bottom of this sidebar is a 'Save' button. To the right, a table titled 'Hostname' lists three entries: '1.2.3.4', '2.4.6.8', and 'testhost.host.com'. Each entry has a green pencil icon and a grey trash can icon to its right. At the top right of the main area is a 'Create Client' button.

Figure 5. FireSIGHT 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. Optional: 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 FireSIGHT Management Center certificate to your QRadar appliance.

### Related tasks:

"Importing a Cisco FireSIGHT Management Center certificate in QRadar" on page 255  
 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 FireSIGHT Management Center pkcs12 certificate that you need to import to your QRadar Console or Event Collector.

## Importing a Cisco FireSIGHT 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 FireSIGHT 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 FireSIGHT Management Center protocol.

The script converts and imports only 1 pkcs12 file at a time. You are required import a certificate only for the QRadar appliance that receives the FireSIGHT Management Center events. For example, after the FireSIGHT 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 FireSIGHT 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 FireSIGHT Management Center appliance to a temporary directory on the QRadar Event Collector.
3. Type the following command to import your pkcs12 file.

```
/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 140. Import script command parameters

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-f</code> | Identifies the file name of the pkcs12 files to import.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>-o</code> | Overrides the default eStreamer name for the keystore and truststore files. Use the <code>-o</code> parameter when you integrate multiple FireSIGHT Management Center devices. For example, <code>/opt/qradar/bin/estreamer-cert-import.pl -f &lt;file name&gt; -o &lt;IP_address&gt;</code><br><br>The import script creates the following files: <ul style="list-style-type: none"><li>• <code>/opt/qradar/conf/&lt;IP_address&gt;.keystore</code></li><li>• <code>/opt/qradar/conf/&lt;IP_address&gt;.truststore</code></li></ul> |
| <code>-d</code> | 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.                                                                                                                                                                                                                                                                                                                                                               |
| <code>-p</code> | Specifies a password if a password was provided when you generated the pkcs12 file.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <code>-v</code> | Displays the version information for the import script.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>-h</code> | Displays a help message about using the import script.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Results

The import script displays the location where the import files were copied.

**Example:**

```
[root@VM199-22 ~]# /opt/qradar/bin/estreamer-cert-import.pl -f yourCertificate.pcks12 -o 61estreamer
Successfully generated truststore file [/opt/qradar/conf/61estreamer.truststore].
Successfully generated keystore file [/opt/qradar/conf/61estreamer.keystore].
```

*Figure 6. Sample import script output*

## Configuring a log source for Cisco FireSIGHT Management Center events

QRadar does not automatically discover Cisco FireSIGHT 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 FireSIGHT Management Center**.
6. From the Protocol Configuration list, select **Cisco Firepower eStreamer**.
7. Configure the following parameters:

| Parameter                  | Description                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Server Address</b>      | The IP address or host name of the FireSIGHT Management Center device.                                                                                                                                                                                               |
| <b>Server Port</b>         | The port number that the FireSIGHT Management Center device is configured to accept connection requests on. The default port that QRadar uses for the FireSIGHT Management Center device is 8302.                                                                    |
| <b>Keystore Filename</b>   | 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                                                    |
| <b>Truststore Filename</b> | 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 |
| <b>Request Extra Data</b>  | Select this option to request intrusion event extra data from FireSIGHT Management Center. For example, extra data includes the original IP address of an event.                                                                                                     |

| Parameter     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domain</b> | <p><b>Note:</b> Domain Streaming Requests are only supported for eStreamer version 6.x. Leave the <b>Domain</b> field blank for eStreamer version 5.x.</p> <p>The domain where the events are streamed from.</p> <p>The value in the <b>Domain</b> 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.</p> <p>Example:</p> <p>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 <b>Domain</b> parameter:</p> <pre>Global \ B \ C</pre> |

- Click **Save**.

## Cisco FWSM

You can integrate Cisco Firewall Service Module (FWSM) with IBM Security 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 Security QRadar, you must configure your Cisco FWSM appliances to forward syslog events to QRadar.

#### About this task

To configure Cisco FWSM:

#### Procedure

- Using a console connection, telnet, or SSH, log in to the Cisco FWSM.

- Enable logging:

```
logging on
```

- 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).

- 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 Security 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)**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 141. Syslog parameters*

| Parameter                    | Description                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Cisco FWSM appliance. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

---

## Cisco IDS/IPS

The Cisco IDS/IPS DSM for IBM Security 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 142. SDEE parameters*

| Parameter                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type an IP address, host name, or name to identify the SDEE event source. IP addresses or host names allow QRadar to identify a log file to a unique event source.<br><br>The log source identifier must be unique for the log source type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>URL</b>                   | Type the URL address 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> . You must use an http or https in the URL.<br><br>Here are some options: <ul style="list-style-type: none"><li>• 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, <a href="https://www.example.com/cgi-bin/sdee-server">https://www.example.com/cgi-bin/sdee-server</a></li><li>• 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, <a href="https://www.example.com/cgi-bin/event-server">https://www.example.com/cgi-bin/event-server</a></li></ul> |
| <b>Username</b>              | Type the user name. This user name must match the SDEE URL user name that is used to access the SDEE URL. The user name can be up to 255 characters in length.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

*Table 142. SDEE parameters (continued)*

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Password</b>               | Type the user password. This password must match the SDEE URL password that is used to access the SDEE URL. The password can be up to 255 characters in length.                                                                                                                                                                       |
| <b>Events / Query</b>         | Type the maximum number of events to retrieve per query. The valid range is 0 - 501 and the default is 100.                                                                                                                                                                                                                           |
| <b>Force Subscription</b>     | Select this check box if you want to force a new SDEE subscription. By default, the check box is selected.<br><br>The check box forces the server to drop the least active connection and accept a new SDEE subscription connection for this log source.<br><br>Clearing the check box continues with any existing SDEE subscription. |
| <b>Severity Filter Low</b>    | Select this check box if you want to configure the severity level as low.<br><br>Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.                                                                                                                          |
| <b>Severity Filter Medium</b> | Select this check box if you want to configure the severity level as medium.<br><br>Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.                                                                                                                       |
| <b>Severity Filter High</b>   | Select this check box if you want to configure the severity level as high.<br><br>Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.                                                                                                                         |

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 IronPort

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

Before you configure QRadar to integrate with your Cisco IronPort device, you must select the log type to configure:

- To configure IronPort mail logs, see “Configuring IronPort mail log.”
- To configure IronPort content filtering logs, see “IronPort web content filter” on page 262.

### Configuring IronPort mail log

The IBM Security QRadar Cisco IronPort DSM accepts events by using syslog.

#### About this task

To configure your IronPort device to send syslog events to QRadar, take the following steps:

#### Procedure

1. Log in to your Cisco IronPort user interface.
2. Select **System Administration\Log Subscriptions**.
3. Click **Add Log Subscription**.

4. Configure the following values:
  - **Log Type** - Define a log subscription for both Ironport Text Mail Logs and System Logs.
  - **Log Name** - Type a log name.
  - **File Name** - Use the default configuration value.
  - **Maximum File Size** - Use the default configuration value.
  - **Log Level** - Select **Information** (Default).
  - **Retrieval Method** - Select **Syslog Push**.
  - **Hostname** - Type the IP address or server name of your QRadar system.
  - **Protocol** - Select **UDP**.
  - **Facility** - Use the default configuration value. This value depends on the configured Log Type.
5. Save the subscription.

You are now ready to configure the log source in QRadar.

## Configuring a log source

To integrate Cisco IronPort with IBM Security QRadar, you must manually create a log source to receive Cisco IronPort events. QRadar does not automatically discover or create log sources for syslog events from Cisco IronPort appliances.

### About this task

To create a log source for Cisco IronPort events, 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 IronPort**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 143. Syslog parameters*

| Parameter                    | Description                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Cisco IronPort appliance. |

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 IronPort are displayed on the **Log Activity** tab.

## IronPort web content filter

The Cisco IronPort DSM for IBM Security QRadar retrieves web content filtering events in W3C format from a remote source by using the log file protocol.

### About this task

Your system must be running the current version of log file protocol to integrate with a Cisco IronPort device. To configure your Cisco IronPort device 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 on configuring a log subscription, see your *Cisco IronPort documentation*.

You are now ready to configure the log source and protocol QRadar.

### Procedure

1. From the **Log Source Type** drop-down list box, select **Cisco IronPort**.
2. From the **Protocol Configuration** list, select **Log File** protocol option.
3. Select **W3C** as the **Event Generator** used to process the web content filter log files.
4. The **FTP File Pattern** parameter must use a regular expression that matches the log files that are generated by the web content filter logs.

#### Related concepts:

"Log File protocol configuration options" on page 21

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

---

## Cisco IOS

You can integrate Cisco IOS series devices with IBM Security 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 Security 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 Security 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.
- Configure the following values:

*Table 144. Syslog parameters*

| Parameter                    | Description                                                                                                       |
|------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Cisco IOS-based device. |

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

The configuration is complete.

---

## Cisco Identity Services Engine

The IBM Security 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 145. Cisco Identity Services Engine DSM specifications*

| Specification               | Value                                                                                                                                                                                                   |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manufacturer                | Cisco                                                                                                                                                                                                   |
| DSM name                    | Cisco Identity Services Engine                                                                                                                                                                          |
| RPM file name               | DSM-CiscoISE-QRadar_version-build_number.noarch.rpm                                                                                                                                                     |
| Supported versions          | 1.1 to 2.2                                                                                                                                                                                              |
| Protocol                    | UDP Multiline Syslog                                                                                                                                                                                    |
| Event format                | Syslog                                                                                                                                                                                                  |
| Recorded event types        | Device events                                                                                                                                                                                           |
| Automatically discovered?   | No                                                                                                                                                                                                      |
| Includes identity?          | Yes                                                                                                                                                                                                     |
| Includes custom properties? | No                                                                                                                                                                                                      |
| More information            | Cisco website ( <a href="https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html">https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html</a> ) |

To integrate Cisco ISE with QRadar, complete the following steps:

- 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>):
  - DSMCommon RPM
  - Cisco Identity Services Engine DSM RPM
- Configure your Cisco ISE appliance to send UDP Multiline Syslog events to QRadar.
- 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 146. Cisco Identity Services Engine log source parameters*

| Parameter                     | Value                         |
|-------------------------------|-------------------------------|
| <b>Log Source type</b>        | Cisco Identity Service Engine |
| <b>Protocol Configuration</b> | UDP Multiline Syslog          |

Table 146. Cisco Identity Services Engine log source parameters (continued)

| Parameter             | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Source Identifier | The IP address or host name of the Cisco Identity Service Engine device that sends UDP Multiline Syslog events to QRadar.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Listen Port           | <p>Type 517 as the port number used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65535.</p> <p><b>Note:</b> 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 <i>Common ports and servers used by QRadar</i> in the <i>IBM Security QRadar Administration Guide</i> or in the IBM Knowledge Center (<a href="https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_adm_ports_and_servers.html">https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_adm_ports_and_servers.html</a>).</p> <p>To edit a saved configuration to use a new port number, complete the following steps:</p> <ol style="list-style-type: none"> <li>In the <b>Listen Port</b> field, type the new port number for receiving UDP Multiline Syslog events.</li> <li>Click <b>Save</b>.</li> </ol> <p>The port update is complete and event collection starts on the new port number.</p> |
| Message ID Pattern    | <p>Type the following regular expression (regex) to filter the event payload messages:</p> <p>CISE_\S+ (\d{10})</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

- Configure a remote logging target on your Cisco ISE appliance.
- Configure the event logging categories on your Cisco ISE appliance.
- Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Cisco Identity Services Engine:

Table 147. Cisco Identity Services Engine sample message

| Event name    | Low level category     | Sample log message                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTHEN_PASSED | Admin Login Successful | <181>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 00 00008620 51001 NOTICE Administrator -Login: Administrator authentication succeeded, ConfigVersionId=84, AdminInterface=GUI, AdminIPAddress =x.x.x.x, AdminSession=0DE37 0E55527018DAA537F60AAAAAAA, Admin Name=adminUser, OperationMessage Text=Administrator authentication successful, |

Table 147. Cisco Identity Services Engine sample message (continued)

| Event name     | Low level category            | Sample log message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FAILED_ATTEMPT | General Authentication Failed | <181>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, User-Name=admin, NAS-Identifier=12782c2b-747a-4894-9689-000000000000, 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=15048, Step=15006, Step=15041, Step=15006, Step=15013, Step=24210, Step=24216, Step=22056, Step=22058, Step=22061, Step=11003 |

#### Related concepts:

“UDP multiline syslog protocol configuration options” on page 49

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

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

“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”

To forward syslog events to IBM Security QRadar, you must configure your Cisco ISE appliance with a remote logging target.

“Configuring logging categories in Cisco ISE” on page 267

The Cisco Identity Services Engine DSM for IBM Security 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 Security 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**.

- Click **Add**, and then configure the following parameters:

| Option         | Description                                                                               |
|----------------|-------------------------------------------------------------------------------------------|
| Name           | Type a unique name for the remote target system.                                          |
| Description    | You can uniquely identify the target system for users.                                    |
| IP Address     | Type the IP address of the QRadar Console or Event Collector.                             |
| Port           | Type 517 or use the port value that you specified in your Cisco ISE log source for QRadar |
| Facility Code  | From the <b>Facility Code</b> list, select the syslog facility to use for logging events. |
| Maximum Length | Type 1024 as the maximum packet length allowed for the UDP syslog message.                |

- 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 Security 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

- Log in to your Cisco ISE Administration Interface.
- From the navigation menu, select **Administration > System > Logging > Logging Categories**.  
The following list shows the supported event logging categories for the IBM Security 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 NAC

The Cisco NAC DSM for IBM Security 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 Security 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 Security 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 148. 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 Cisco NAC appliance. |

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 Security 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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 149. Syslog parameters*

| Parameter                    | Description                                                                                                       |
|------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Cisco Nexus appliances. |

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 Security 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 Security 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 Security 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 150. Syslog parameters*

| Parameter                    | Description                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Cisco Pix Firewall. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

## Cisco Stealthwatch

The IBM Security QRadar DSM for Cisco Stealthwatch receives events from a Cisco Stealthwatch device.

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

*Table 151. Cisco Stealthwatch DSM specifications*

| Specification               | Value                                                                                                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manufacturer                | Cisco                                                                                                                                                                        |
| DSM name                    | Cisco Stealthwatch                                                                                                                                                           |
| RPM file name               | DSM-CiscoStealthwatch-QRadar_version-build_number.noarch.rpm                                                                                                                 |
| Supported versions          | 6.8                                                                                                                                                                          |
| Protocol                    | Syslog                                                                                                                                                                       |
| Event format                | LEEF                                                                                                                                                                         |
| Recorded event types        | Anomaly, Data Hoarding, Exploitation, High Concern Index, High DDoS Source Index, High Target Index, Policy Violation, Recon, High DDoS Target Index, Data Exfiltration, C&C |
| Automatically discovered?   | Yes                                                                                                                                                                          |
| Includes identity?          | No                                                                                                                                                                           |
| Includes Custom properties? | No                                                                                                                                                                           |
| More information            | Cisco Stealthwatch website ( <a href="http://www.cisco.com">http://www.cisco.com</a> )                                                                                       |

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 152. Cisco Stealthwatch log source parameters*

| Parameter              | Value                                   |
|------------------------|-----------------------------------------|
| Log Source type        | Cisco Stealthwatch                      |
| Protocol Configuration | Syslog                                  |
| Log Source             | A unique identifier for the log source. |

The following table shows a sample syslog message that is supported by the Cisco Stealthwatch device:

Table 153. Cisco Stealthwatch sample syslog message

| Event name | Low-level category                 | Sample log message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16         | Network Threshold Policy Violation | <pre> May 5 18:11:01 127.0.0.1 May 05 18: 11:01 &lt;Server&gt; StealthWatch[3706]: LEEF:2.0 Lancope Stealthwatch 6.8  16 0x7C src=&lt;Source_IP_address&gt;  dst=&lt;Destination_IP_address&gt; dstP ort= proto= msg=The total traffic inbound + outbound exceeds the acc eptable total traffic values. fullm essage=Observed 3.95G bytes. Expect ed 2.22M bytes, tolerance of 50 all ows up to 1.92G bytes. start=2017- 05- 05T18:10:00Z end= cat=High Tot al Traffic alarmID=3L-1CR1- JI38-Q GNE-2 sourceHG=&lt;Country&gt; targetHG= Unknown sourc eHostSnapshot=https: //&lt;Server&gt;/ smc/getHostSnapshot?do mainid= 123&amp;hostip=&lt;Server_IP&gt;&amp;date =201 7-05- 05T18:10:00Z targetHost Snapsh ot=https://&lt;Server&gt;/smc/get Host Snapshot?domainid=123&amp;hostip =&lt;IP_address&gt;&amp;date=2017-05- 05T18 :10:00Z flowCollectorName =&lt;Server2&gt;  flowCollectorIP=&lt;IP_address2&gt; do main=example.com exporterName =  exporterIPAddress= exporterIn fo = targetUser= targetHostname=  sourceUser= alarmStatus=ACTIV E alarmSev=Major </pre> |

#### Related tasks:

“Adding a DSM” on page 4

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

“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:

| Parameter  | Value                                         |
|------------|-----------------------------------------------|
| Name       | The name for the syslog message action.       |
| Enabled    | This check box is enabled by default.         |
| IP Address | The IP address of the QRadar Event Collector. |
| Port       | The default port is port 514.                 |

| Parameter | Value                          |
|-----------|--------------------------------|
| Format    | Select <b>Syslog Formats</b> . |

5. Enter the following custom format:

```
LIEEEF:2.0|Lancope|Stealthwatch|6.8|{alarm_type_id}|0x7C|src={source_ip}
|dst={target_ip}|dstPort={port}|proto={protocol}|msg={alarm_type_description}|
fullMessage={details}|start={start_active_time}|end={end_active_time}|
|cat={alarm_category_name}|alarmID={alarm_id}|sourceHG={source_host_group_names}|
targetHG={target_host_group_names}|sourceHostSnapshot={source_url}|
targetHostSnapshot={target_url}|flowCollectorName={device_name}|
flowCollectorIP={device_ip}|domain={domain_name}|exporterName=
{exporter_hostname}|exporterIPAddress ={exporter_ip}|
exporterInfo={exporter_label}|targetUser={target_username}|
targetHostname={target_hostname}|sourceUser={source_username}|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 Security 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 154. Amazon AWS S3 REST API log source parameters*

| Parameter              | Value                  |
|------------------------|------------------------|
| Log Source type        | Cisco Umbrella         |
| Protocol Configuration | Amazon AWS S3 REST API |

Table 154. Amazon AWS S3 REST API log source parameters (continued)

| Parameter                              | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b>           | Type a unique name for the log source.<br><br>The <b>Log Source Identifier</b> can be any valid value and does not need to reference a specific server. The <b>Log Source Identifier</b> can be the same value as the <b>Log Source Name</b> . If you configured more than one Cisco Umbrella log source, you might want to identify the first log source as <code>ciscoumbrella1</code> , the second log source as <code>ciscoumbrella2</code> , and the third log source as <code>ciscoumbrella3</code> . |
| <b>Signature Version</b>               | Select <b>AWSSIGNATUREV2</b> or <b>AWSSIGNATURE4</b> .<br><br><b>AWSSIGNATUREV2</b> does not support all Amazon AWS regions. If you are using a region that supports only <b>AWSSIGNATUREV4</b> , you must choose <b>AWSSIGNATUREV4</b> from the list.<br><br><b>Note:</b> If you need to create a log source to retrieve events from multiple regions, you must choose <b>AWSSIGNATUREV4</b> .                                                                                                             |
| <b>Region Name</b> (Signature V4 only) | The region that is associated with the Amazon S3 bucket.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Bucket Name</b>                     | The name of the AWS S3 bucket where the log files are stored.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Endpoint URL</b>                    | <a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a><br><br>The Endpoint URL can be different depending on the device configurations.                                                                                                                                                                                                                                                                                                                                                            |
| <b>Authentication Method</b>           | <b>Access Key ID / Secret Key</b><br>Standard authentication that can be used from anywhere.<br><br><b>EC2 Instance IAM Role</b><br>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 <b>only</b> work for managed hosts that are running within an AWS EC2 container.                                                            |
| <b>Access Key ID</b>                   | The public access key that is required to access the AWS S3 bucket.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Secret Key</b>                      | The private access key that is required to access the AWS S3 bucket.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Directory Prefix</b>                | 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> .                                                                                                                                                                                                                                                                                                         |
| <b>File Pattern</b>                    | <code>.*?\.\csv\.\gz</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Event Format</b>                    | Select <b>Cisco Umbrella CSV</b> from the list. The log source retrieves CSV formatted events.                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 154. Amazon AWS S3 REST API log source parameters (continued)

| Parameter                                   | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use Proxy                                   | If QRadar accesses the Amazon Web Service by using a proxy, enable the check box.<br><br>If the proxy requires authentication, configure the <b>Proxy Server</b> , <b>Proxy Port</b> , <b>Proxy Username</b> , and <b>Proxy Password</b> fields. If the proxy does not require authentication, configure the <b>Proxy Username</b> and <b>Proxy Password</b> fields.                                                                                                                                                                                            |
| Automatically Acquire Server Certificate(s) | If you select <b>Yes</b> , 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.                                                                                                                                                                                                                                                                                                                 |
| Recurrence                                  | 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.<br><br>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. |
| EPS Throttle                                | The maximum number of events per second.<br><br>The default is 5000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

#### Related concepts:

“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.

“Cisco Umbrella DSM specifications” on page 277

The following table describes the specifications for the Cisco Umbrella DSM.

“Sample event messages” on page 277

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

#### Related tasks:

“Adding a DSM” on page 4

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

“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 Log Management in Amazon S3(<https://support.umbrella.com/hc/en-us/articles/231248448-Cisco-Umbrella-Log-Management-in-Amazon-S3>).

## Cisco Umbrella DSM specifications

The following table describes the specifications for the Cisco Umbrella DSM.

*Table 155. Cisco Umbrella DSM specifications*

| Specification               | Value                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------|
| Manufacturer                | Cisco                                                                                                           |
| DSM name                    | Cisco Umbrella                                                                                                  |
| RPM file name               | DSM-CiscoUmbrella-QRadar_version-build_number.noarch.rpm                                                        |
| Supported versions          | N/A                                                                                                             |
| Protocol                    | Amazon AWS S3 REST API                                                                                          |
| Event format                | Cisco Umbrella CSV                                                                                              |
| Recorded event types        | Audit                                                                                                           |
| Automatically discovered?   | No                                                                                                              |
| Includes identity?          | No                                                                                                              |
| Includes custom properties? | No                                                                                                              |
| More information            | Cisco Umbrella product information page ( <a href="https://umbrella.cisco.com">https://umbrella.cisco.com</a> ) |

## 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 156. Cisco Umbrella sample syslog message*

| Event name | Low level category      | Sample log message                                                                                                                                                                                                                                                                                                                                                                      |
|------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOERROR    | 18081 (DNS In Progress) | {"sourceFile": "test_2017-11-17-15-30-dcd8.csv.gz", "EventType": "DNSLog", "Timestamp": "2017-11-17 15:30:27", "MostGranularIdentity": "Test", "Identities": "Test", "InternalIp": "<IP_address>", "ExternalIp": "<External_IP_address>", "Action": "Allowed", "QueryType": "28(AAAA)", "ResponseCode": "NOERROR", "Domain": "abc.aws.amazon.com.", "Categories": "Ecommerce/Shopping"} |

*Table 157. Cisco Umbrella sample event message*

| Event name | Low level category      | Sample log message                                                                                                                                                                                                                             |
|------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOERROR    | 18081 (DNS In Progress) | "2015-01-16 17:48:41", "ActiveDirectoryUserName", "ActiveDirectoryUserName", "ADSite", "Network", "<IP_address1>", "<IP_address2>", "Allowed", "1 (A)", "NOERROR", "domain-visited.com.", "Chat, Photo Sharing, Social Networking, Allow List" |

## Cisco VPN 3000 Concentrator

The Cisco VPN 3000 Concentrator DSM for IBM Security 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 Security 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 158. Syslog parameters*

| Parameter                    | Description                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Cisco VPN 3000 Series Concentrators. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

---

## Cisco Wireless Services Module

You can integrate a Cisco Wireless Services Module (WiSM) device with IBM Security 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 Security 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
  - **Local Use 1** - Facility level 17
  - **Local Use 2** - Facility level 18
  - **Local Use 3** - Facility level 19
  - **Local Use 4** - Facility level 20
  - **Local Use 5** - Facility level 21
  - **Local Use 6** - Facility level 22
  - **Local Use 7** - Facility level 23
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 Security 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)**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 159. Syslog Protocol parameters*

| Parameter                    | Description                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Cisco WiSM appliance. |

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 Security 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 282
- “Configuring SNMPv2 for Cisco Wireless LAN Controller” on page 283

### 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 Security 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 Security 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 160. Syslog protocol parameters*

| Parameter                    | Description                                                                                                              |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Cisco Wireless LAN Controller. |
| <b>Enabled</b>               | Select the <b>Enabled</b> check box to enable the log source. By default, the check box is selected.                     |

Table 160. Syslog protocol parameters (continued)

| Parameter              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Credibility            | 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.                                                                                                                                                                                                                                                                        |
| Target Event Collector | From the list, select the <b>Target Event Collector</b> to use as the target for the log source.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Coalescing Events      | 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 <b>Coalescing Events</b> drop-down list in the QRadar Settings window on the <b>Admin</b> 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 on settings, see the <i>IBM Security QRadar Administration Guide</i> . |
| Incoming Event Payload | From the list, select the incoming payload encoder for parsing and storing the logs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 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 <b>Store Event Payload</b> drop-down list in the QRadar Settings window on the <b>Admin</b> 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.                                                                                                      |

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 Security 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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **SNMPv2**.
10. Configure the following values:

*Table 161. SNMPv2 protocol parameters*

| Parameter                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b>         | Type the IP address or host name for the log source as an identifier for events from your Cisco Wireless LAN Controller.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Community</b>                     | Type the SNMP community name that is needed to access the system that contains the SNMP events. The default is Public.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Include OIDs in Event Payload</b> | Select the <b>Include OIDs in Event Payload</b> check box.<br><br>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.                                                                                                                                                                                                                                                                      |
| <b>Enabled</b>                       | Select the <b>Enabled</b> check box to enable the log source. By default, the check box is selected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Credibility</b>                   | 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.                                                                                                                                                                                                                                                                      |
| <b>Target Event Collector</b>        | From the list, select the <b>Target Event Collector</b> to use as the target for the log source.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Coalescing Events</b>             | Select this check box to enable the log source to coalesce (bundle) events.<br><br>Automatically discovered log sources use the default value that is configured in the <b>Coalescing Events</b> drop-down in the QRadar Settings window on the <b>Admin</b> 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 <i>IBM Security QRadar Administration Guide</i> . |
| <b>Store Event Payload</b>           | Select this check box to enable or disable QRadar from storing the event payload.<br><br>Automatically discovered log sources use the default value from the <b>Store Event Payload</b> drop-down in the QRadar Settings window on the <b>Admin</b> 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.                                                                                                      |

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.



---

## 36 Citrix

Citrix NetScaler and Citrix Access Gateway DSMs.

The Citrix NetScaler DSM for IBM Security 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 Security 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
```
- 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> 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 Security QRadar automatically discovers and creates a log source for syslog events from Citrix NetScaler.

About this task

This procedure is optional.

Procedure

- Log in to QRadar.
- Click the **Admin** tab.
- On the navigation menu, click **Data Sources**.
- Click the **Log Sources** icon.
- Click **Add**.
- In the **Log Source Name** field, type a name for your log source.
- In the **Log Source Description** field, type a description for the log source.
- From the **Log Source Type** list, select **Citrix NetScaler**.
- Using the **Protocol Configuration** list, select **Syslog**.
- Configure the following values:

Table 162. 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.

- Click **Save**.
- 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

- Log in to your Citrix Access Gateway web interface.
- Click the **Access Gateway Cluster** tab.
- Select **Logging/Settings**.
- In the **Server** field, type the IP address of your QRadar Console or Event Collector.
- From the **Facility** list, select a syslog facility level.
- 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 Security 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 163. 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 Citrix Access Gateway appliance.

11. Click **Save**.
12. On the Admin tab, click **Deploy Changes**.

37 Cloudera Navigator

The IBM Security QRadar DSM for Cloudera Navigator collects events from Cloudera Navigator.

The following table identifies the specifications for the Cloudera Navigator DSM:

Table 164. Cloudera Navigator DSM specifications

Specification	Value
Manufacturer	Cloudera
DSM name	Cloudera Navigator
RPM file name	DSM-ClouderaNavigator-Qradar_version-build_number.noarch.rpm
Supported versions	v2.0
Protocol	Syslog
Recorded event types	Audit events for HDFS, HBase, Hive, Hue, Cloudera Impala, Sentry
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Cloudera Navigator website (www.cloudera.com)

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 165. Cloudera Navigator log source parameters

Parameter	Value
Log Source type	Cloudera Navigator
Protocol Configuration	Syslog
Log Source Identifier	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.

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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 Security 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.
3. Search for **Navigator Audit Server Logging Advanced Configuration Snippet**.
4. Depending on the format type, enter one of the following values in the **Value** field:
 - `log4j.logger.auditStream = TRACE,SYSLOG`
 - `log4j.appenders.SYSLOG = org.apache.log4j.net.SyslogAppender`
 - `log4j.appenders.SYSLOG.SyslogHost = <QRadar Hostname>`
 - `log4j.appenders.SYSLOG.Facility = Local2`
 - `log4j.appenders.SYSLOG.FacilityPrinting = true`
 - `log4j.additivity.auditStream = false`
5. Click **Save Changes**.

38 CloudPassage Halo

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

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

Table 166. CloudPassage Halo DSM Specifications

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

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

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

Configuring CloudPassage Halo for communication with QRadar

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

Before you begin

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

About this task

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

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

Procedure

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

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

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

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

 - - `rsyslog.conf`
 - `syslog-nginx.conf`
 - `syslog.conf`

```
        udp("qradar_hostname" port(514));  
};  
log {  
    source(s_src); destination(d_qradar);  
};
```

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

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

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

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

Configuring a CloudPassage Halo log source in QRadar

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

Procedure

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

39 CloudLock Cloud Security Fabric

The IBM Security 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 167. CloudLock Cloud Security Fabric DSM specifications

Specification	Value
Manufacturer	CloudLock
DSM name	CloudLock Cloud Security Fabric
RPM file name	DSM-CloudLockCloudSecurityFabric-Qradar_version-build_number.noarch.rpm
Supported versions	NA
Protocol	Syslog
Event format	Log Event Extended Format (LEEF)
Recorded event types	Incidents
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Cloud Cybersecurity (https://www.cloudlock.com/products/)

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 168. CloudLock Cloud Security Fabric log source parameters

Parameter	Value
Log Source type	CloudLock Cloud Security Fabric
Protocol Configuration	Syslog

The following table provides a sample event message for the CloudLock Cloud Security Fabric DSM:

Table 169. CloudLock Cloud Security Fabric sample message supported by the CloudLock Cloud Security Fabric service

Event name	Low level category	Sample log message
New Incident	Suspicious Activity	LEEF: 1.0 Cloudlock API v2 Incidents match_count=2 sev=1 entity_id=ebR4q6DxvA entity_origin_type=document group=None url=https://example.com/a/path/file/d/<File_path_ID/>view?usp=drivesdk CloudLockID=xxxxxxxxxx updated_at=2016-01-20T15:42:15.128356+0000 entity_owner_email=user@example.com cat=NEW entity_origin_id=<File_path_ID> entity_mime_type=text/plain devTime=2016-01-20T15:42:14.913178+0000 policy=Custom Regex resource=confidential.txt usrName=Admin Admin realm=domain policy_id=xxxxxxxxxx devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSSSZ

Related tasks:

“Adding a DSM” on page 4

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

“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

- 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.
- 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.

40 Correlog Agent for IBM z/OS

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

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

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

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

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

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

Related tasks:

“Adding a DSM” on page 4

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

“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 Security QRadar instructions**.

When you start the CorreLog agent, if QRadar does not collect z/OS events, see the **Troubleshooting topic in Section 3**.

- If you want to customize the optional CorreLog Agent parameter file, review QRadar normalized event attributes in **Appendix G: Fields**.

41 CrowdStrike Falcon Host

The IBM Security 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 170. CrowdStrike Falcon Host DSM specifications

Specification	Value
Manufacturer	CrowdStrike
DSM name	CrowdStrike Falcon Host
RPM file name	DSM-CrowdStrikeFalconHost-QRadar_version-build_number.noarch.rpm
Supported versions	N/A
Protocol	Syslog
Event format	LEEF
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 171. CrowdStrike Falcon Host log source parameters

Parameter	Value
Log Source type	CrowdStrike Falcon Host
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name where the Falcon SIEM Connector is installed.

The following table shows a sample event message from CrowdStrike Falcon Host:

Table 172. CrowdStrike Falcon Host sample message

Event name	Low level category	Sample log message
Suspicious Activity	Suspicious Activity	LEEF:1.0 CrowdStrike FalconHost 1.0 Suspicious Activity 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

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

“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 Security 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.
`rpm -Uvh /path/to/file/cs.falconhoseclient-<build_version>. <OS_version>.rpm`

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.leef.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 173. Key parameter values

Key	Description	Value
version	The version of authentication to be used. In this case, it is the API Key Authentication version.	2
api_url	The SIEM connector connects to this endpoint URL.	<code>https://firehose.crowdstrike.com/sensors/entities/datafeed/v1</code>
app_id	An arbitrary string identifier for connecting to Falcon Streaming API.	Any string. For example, FHAPI-LEEF
api_key	The API key is used as the credential for client verification.	Obtained at step 1
api_uuid	The UUID is used as the credential for client verification.	Obtained at step 1
send_to_syslog_server	To enable or disable syslog push to syslog server, set the flag to true or false.	true
host	The IP or host name of the SIEM.	The QRadar SIEM IP or host name where the Connector is forwarding the LEEF events.
header_delim	Header prefix and fields are delimited by this value.	The value must be a pipe ().
field_delim	The delimiter value that is used to separate key-value pairs.	The value must be a tab (\t).
time_fields	This datetime field value is converted to specified time format.	The default field is devTime (device time). If a custom LEEF key is used for setting device time, use a different field name .

4. Start the SIEM Connector service by typing the following command:

```
service cs.falconhoseclient 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.

42 CRYPTOCard CRYPTO-Shield

The IBM Security 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 Security 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 174. 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 CRYPTOCard CRYPTO-Shield device.

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.appenders.<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.appenders.<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 Security QRadar host to which you want to send logs.

Specify the *IP address* parameter after the log4j.appenders.<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.

43 CyberArk

IBM Security QRadar supports several CyberArk DSMs.

CyberArk Privileged Threat Analytics

The IBM Security 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 175. CyberArk Privileged Threat Analytics DSM specifications

Specification	Value
Manufacturer	CyberArk
DSM name	CyberArk Privileged Threat Analytics
RPM file name	DSM-CyberArkPrivilegedThreatAnalytics-Qradar_version-build_number.noarch.rpm
Supported versions	V3.1
Protocol	Syslog
Recorded event types	Detected security events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	CyberArk website (http://www.cyberark.com)

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 176. CyberArk Privileged Threat Analytics log source parameters

Parameter	Value
Log Source type	CyberArk Privileged Threat Analytics
Protocol Configuration	Syslog

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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:

Parameter	Value
Host	The host name or IP address of the QRadar system.
Port	514
Protocol	UDP
Format	QRadar

Example: The following is an example of the `syslog_outbound` property:

```
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:

```
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 Security 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 Security QRadar:

Procedure

1. Log in to your CyberArk device.
2. Edit the DBParm.ini file.
3. Configure the following parameters:

Table 177. Syslog parameters

Parameter	Description
SyslogServerIP	Type the IP address of QRadar.
SyslogServerPort	Type the UDP port that is used to connect to QRadar. The default value is 514.
SyslogMessageCodeFilter	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. Example: To define a message code of 1,2,3,30 and 5-10, you must type: 1,2,3,5-10,30.
SyslogTranslatorFile	Type the file path to the LEEF.xls translator file. The translator file is used to parse CyberArk audit records data in the syslog protocol.

4. Copy LEEF.xls 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 178. 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 CyberArk Vault appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

44 CyberGuard Firewall/VPN Appliance

The CyberGuard Firewall VPN Appliance DSM for IBM Security 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.
3. Under **System Log**, select **Enable Remote Logging**.
4. Type the IP address of IBM Security 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 Security 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**.

45 Damballa Failsafe

The Failsafe DSM for IBM Security 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 Security 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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 179. 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 Damballa Failsafe devices.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

46 DG Technology MEAS

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

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

Table 180. DSM Specifications for DG Technology MEAS

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

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

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

Related tasks:

“Adding a DSM” on page 4

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

“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 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.

47 Digital China Networks (DCN)

The Digital China Networks (DCN) DCS/DCRS Series DSM for IBM Security QRadar can accept events from Digital China Networks (DCN) switches by using syslog.

IBM Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following value:

Table 181. Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address, host name, or name for the log source for use as an identifier of your DCN DCS/DCRS Series switch. Each log source that you create for your DCN DCS/DCRS Series switch includes a unique identifier, such as an IP address or host name.

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 Security 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.

48 Enterprise-IT-Security.com SF-Sherlock

The IBM Security 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 182. Enterprise-IT-Security.com SF-Sherlock DSM specifications

Specification	Value
Manufacturer	Enterprise-IT-Security.com
DSM name	Enterprise-IT-Security.com SF-Sherlock
RPM file name	DSM-EnterpriseITSecuritySFSherlock-Qradar_version-build_number.noarch.rpm
Supported versions	v8.1 and later
Event format	Log Event Extended Format (LEEF)
Recorded event types	All_Checks, DB2_Security_Configuration, JES_Configuration, Job_Entry_System_Attack, Network_Parameter, Network_Security, No_Policy, Resource_Access_Viol, Resource_Allocation, Resource_Protection, Running_System_Change, Running_System_Security, Running_System_Status, Security_Dbase_Scan, Security_Dbase_Specialty, Security_Dbase_Status, Security_Parm_Change, Security_System_Attack, Security_System_Software, Security_System_Status, SF-Sherlock, Sherlock_Diverse, Sherlock_Diverse, Sherlock_Information, Sherlock_Specialties, Storage_Management, Subsystem_Scan, Sysplex_Security, Sysplex_Status, System_Catalog, System_File_Change, System_File_Security, System_File_Specialty, System_Log_Monitoring, System_Module_Security, System_Process_Security, System_Residence, System_Tampering, System_Volumes, TSO_Status, UNIX_OMVS_Security, UNIX_OMVS_System, User Defined_Monitoring, xx_Resource_Proto_Templ
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Enterprise-IT-Security website (http://www.enterprise-it-security.com)

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 183. Enterprise-IT-Security.com SF-Sherlock log source parameters

Parameter	Value
Log Source type	Enterprise-IT-Security.com SF-Sherlock

Table 183. Enterprise-IT-Security.com SF-Sherlock log source parameters (continued)

Parameter	Value
Protocol Configuration	Syslog

Related tasks:

“Adding a DSM” on page 4

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

“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.

49 Epic SIEM

The IBM Security 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 184. Epic SIEM DSM specifications

Specification	Value
Manufacturer	Epic
DSM name	Epic SIEM
RPM file name	DSM-EpicSIEM-QRadar_version-build_number.noarch.rpm
Supported versions	Epic 2014, Epic 2015, Epic 2017
Event format	LEEF
Recorded event types	Audit Authentication
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Epic website (http://www.epic.com/)

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 185. Epic SIEM log source parameters

Parameter	Value
Log Source type	Epic SIEM
Protocol Configuration	Syslog

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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:

Parameter	Description
SIEM Host	The host name or IP address of the QRadar appliance.
SIEM Port	514
SIEM Format	LEEF (Log Event Extended Format).

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 Security 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 186. Queue values for EMPSYNC prompts

Prompt	Value
Queue ID	Type an ID for the queue.
Queue Name	EMPSYNC
Descriptor	EMPSYNC
Run on Node	Press the Enter key. The value is automatically populated.

Table 186. Queue values for EMPSYNC prompts (continued)

Prompt	Value
IC Servers	Press the Enter key, without typing a value.
Edit advanced settings for this queue?	Yes
Does this queue handle synchronous outgoing messages?	Yes
Associate this descriptor with a queue type for outgoing communication?	Yes
Queue Type	EMP

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 187. Queue values for EMPASYNC prompts

Prompt	Value
Queue ID	Type an ID for the queue.
Queue Name	EMPASYNC
Descriptor	EMPASYNC
Run on Node	Press the Enter key. The value is automatically populated.
IC Servers	Press the Enter key, without typing a value.
Edit advanced settings for this queue?	Yes
Does this queue handle synchronous outgoing messages?	No
Associate this descriptor with a queue type for outgoing communication?	Yes
Queue Type	EMP

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:

Parameter	Value
SIEM Host	Your QRadar Event Collector host name or IP address.
SIEM Port	514
SIEM Format	LEEF (Log Event Extended Format)
Check Application Layer Response	Disable

14. Return to the **SIEM Syslog Settings Menu**.

- 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**.

Configuring Epic SIEM 2017 to communicate with QRadar

To collect events in IBM Security QRadar, you must configure the messaging queue values on your Epic SIEM 2017 system.

Procedure

- From the command line, select **Interconnect Administrator's Menu > Messaging Queues Setup**.
- Type an asterisk (*) to create the EMPSYNC queue.
- Enter the queue values identified in the following table for each of the prompts.

Table 188. Queue values for EMPSYNC prompts

Prompt	Value
Queue ID	Type an ID for the queue.
Queue Name	EMPSYNC
Descriptor	EMPSYNC
Run on Node	Press the Enter key. The value is automatically populated.
IC Servers	Press the Enter key, without typing a value.
Edit advanced settings for this queue?	Yes
Does this queue handle synchronous outgoing messages?	Yes
Associate this descriptor with a queue type for outgoing communication?	Yes
Queue Type	EMP

- Type an asterisk (*) to create the EMPASYNC queue.
- Enter the queue values identified in the following table for each of the prompts.

Table 189. Queue values for EMPASYNC prompts

Prompt	Value
Queue ID	Type an ID for the queue.
Queue Name	EMPASYNC
Descriptor	EMPASYNC
Run on Node	Press the Enter key. The value is automatically populated.
IC Servers	Press the Enter key, without typing a value.
Edit advanced settings for this queue?	Yes
Does this queue handle synchronous outgoing messages?	No
Associate this descriptor with a queue type for outgoing communication?	Yes
Queue Type	EMP

- 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:

Parameter	Value
SIEM Host	Your QRadar Event Collector host name or IP address.
SIEM Port	514
SIEM Format	LEEF (Log Event Extended Format)
Check Application Layer Response	Disable

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**.

50 ESET Remote Administrator

The IBM Security 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 190. ESET Remote Administrator DSM specifications

Specification	Value
Manufacturer	ESET
DSM name	ESET Remote Administrator
RPM file name	DSM-ESETRemoteAdministrator-QRadar_version-build_number.noarch.rpm
Supported versions	6.4.270
Protocol	Syslog
Event format	Log Extended Event Format (LEEF)
Recorded event types	Threat Firewall aggregated Host Intrusion Protection System (HIPS) aggregated Audit
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	ESET website (https://www.eset.com/us/support/download/business/remote-administrator-6)

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 191. ESET Remote Administrator log source parameters

Parameter	Value
Log Source type	ESET Remote Administrator
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the ESET Remote Administration server.

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 192. ESET Remote Administrator sample message

Event name	Low level category	Sample log message
Native user login	User Login Success	<14>1 2016-08-15T14:52:31.888Z hostname ERAserver 28021 - - △LEEF:1.0 ESET RemoteAdministrator <Version> Native user login cat= ESET RA Audit Event sev=2 devTime =Aug 15 2016 14:52:31 devTime Format=MMM dd yyyy HH:mm:ss src= <Source_IP_address> domain=Native user action=Login attempt target= username detail=Native user 'username' attempted to authenticate. result=Success

Related tasks:

"Adding a DSM" on page 4

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

"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 Security 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**.

51 Exabeam

The IBM Security QRadar DSM for Exabeam collects events from an Exabeam device.

The following table describes the specifications for the Exabeam DSM:

Table 193. Exabeam DSM specifications

Specification	Value
Manufacturer	Exabeam
DSM name	Exabeam
RPM file name	DSM-ExabeamExabeam-Qradar_version-build_number.noarch.rpm
Supported versions	v1.7 and v2.0
Recorded event types	Critical Anomalous
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Exabeam website (http://www.exabeam.com)

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 194. Exabeam log source parameters

Parameter	Value
Log Source type	Exabeam
Protocol Configuration	Syslog

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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

1. Log in to your Exabeam user interface (https://<Exabeam_IP>:8484).
2. Select https://<Exabeam_IP>:8484/#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.

Parameter	Description
IP Address or Hostname	The IP address of the QRadar Event Collector .
Protocol	TCP
Port	514
Syslog Severity Level	Emergency

52 Extreme

IBM Security QRadar accepts events from a range of Extreme DSMs.

Extreme 800-Series Switch

The Extreme 800-Series Switch DSM for IBM Security 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. Optional: 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 Security 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 195. 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 Extreme 800-Series Switch.

11. Click **Save**.
 12. On the **Admin** tab, click **Deploy Changes**.
- The configuration is complete.

Extreme Dragon

The Extreme Dragon DSM for IBM Security 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.”
2. Configure the log source within QRadar. See “Configuring a log source” on page 334.
3. Configure Dragon Enterprise Management Server (EMS) to forward syslog messages. See “Configure the EMS to forward syslog messages” on page 334.

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 Security 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 Security 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 Security 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.”
- 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 335.

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 Security 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 syslod 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 syslod for forwarding events to a Security and Information Manager such as IBM Security 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:
`local1.notice @<IP address>`
Where:
`<IP address>` is the IP address of the QRadar system.
3. Save the file and restart syslod.
`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 Security 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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 196. 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 Extreme HiGuard.

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 Security 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 Security 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**.
6. Using the **Wireless AP Log Level** list, select **Major**.
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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 197. 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 Extreme HiPath.

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 Security 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:

```
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 Security 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
 - r. set logging application LACP level 8
 - s. set logging application RtrNat level 8
 - t. set logging application RtrTwcb level 8
 - u. set logging application HostDoS level 8
 - v. set policy syslog extended-format enable
- 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 Security 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 Security 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 Security 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 198. 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 Extreme NAC appliances.

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 Security 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 Security 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 Security 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)**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 199. 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 ExtremeWare appliance.

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 Security 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:

```
logging <IP address> low
```

Where: <IP address> is the IP address of your QRadar.

4. Exit from config mode.

```
exit
```

5. Save the configuration:

```
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.

53 F5 Networks

IBM Security 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 Security 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."
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 **Finished**.

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 345 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" 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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 200. 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 F5 BIG-IP AFM appliance.

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 Security 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 11.x”
- “Configuring a Remote Syslog for F5 BIG-IP APM 10.x” on page 349

Configuring Remote Syslog for F5 BIG-IP APM 11.x

You can configure syslog for F5 BIG-IP APM 11.x.

About this task

To configure a remote syslog for F5 BIG-IP APM 11.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:

```
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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

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 F5 Networks BIG-IP APM appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
The configuration is complete.

Configuring F5 Networks BIG-IP ASM

The IBM Security 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 Security 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:

Table 201. 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 F5 Networks BIG-IP ASM appliance.

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 Security 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 Security 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 202. 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 BIG-IP LTM appliance.

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 11.x”
- “Configuring Remote Syslog for F5 BIG-IP LTM 10.x” on page 353
- “Configuring Remote Syslog for F5 BIG-IP LTM 9.4.2 to 9.4.8” on page 353

Configuring Remote Syslog for F5 BIG-IP LTM 11.x

You can configure syslog for F5 BIG-IP LTM 11.x.

About this task

To configure syslog for F5 BIG-IP LTM 11.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:
`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 Security QRadar.
For example,

```
modify /sys syslog remote-servers add {BIGIPsyslog {host 192.0.2.1 remote-port 514}}
```

4. Save the configuration changes:

```
save /sys config
```

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 10.x

You can configure syslog for F5 BIG-IP LTM 10.x.

About this task

To configure syslog for F5 BIG-IP LTM 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 LTM syslog source.
 - <IP_address> is the IP address of IBM Security 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>.

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 9.4.2 to 9.4.8

You can configure syslog for F5 BIG-IP LTM 9.4.2 to 9.4.8.

About this task

To configure syslog for F5 BIG-IP LTM 9.4.2 to 9.4.8 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 Security 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 Security 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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 203. 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 F5 Networks FirePass appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

54 Fair Warning

The Fair Warning DSM for IBM Security 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 Security 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**.
14. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete. For more information on full parameters for the log file protocol, see the *IBM Security 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.

55 Fasoo Enterprise DRM

The IBM Security 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 204. Fasoo Enterprise DRM DSM specifications

Specification	Value
Manufacturer	Fasoo
DSM name	Fasoo Enterprise DRM
RPM file name	DSM-FasooFED-QRadar_version-build_number.noarch.rpm
Supported versions	5.0
Protocol	JDBC
Event format	name-value pair (NVP)
Recorded event types	Usage events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Fasoo website (http://en.fasoo.com/Fasoo-Enterprise-DRM)

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 205. Fasoo Enterprise DRM log source parameters

Parameter	Value
Log Source type	Fasoo Enterprise DRM
Protocol Configuration	JDBC
Log Source Identifier	Since the protocol is JDBC, you need to use a specific format. For example, for Fasoo Enterprise DRM, use the following format: <Fasoo_Enterprise_DRM_Database>@ <Fasoo_Enterprise_DRM_Database_Server_IP_or_Host_Name> You must use the values of the Fasoo Enterprise DRM database and the database Server IP address or host name.
Database Type	From the list, select the type of the Fasoo Enterprise DRM database.

Table 205. Fasoo Enterprise DRM log source parameters (continued)

Parameter	Value
Database Name	The name of the Fasoo Enterprise DRM database. The database name must match the database name that is specified in the Log Source Identifier field.
IP or Hostname	The IP address or host name of the Fasoo Enterprise DRM database server.
Port	The port number that is used by the database server.
Username	The user name that is required to connect to the database.
Password	The password that is required to connect to the database. The password can be up to 255 characters in length.
Confirm Password	The confirmation password must be identical to the password that you typed for the Password parameter.
Authentication Domain	If you selected MSDE for the Database Type and the database is configured for Windows, define a Window Authentication Domain . Otherwise, leave this field blank.
Database Instance	If you selected MSDE for the Database Type and you have multiple SQL server instances, type the database instance. If you use a non-standard port for the database or access is blocked to port 1434 for SQL database resolution, the Database Instance parameter must be left blank in the log source configuration.
Table Name	view_fut_log The name of the view that includes the event records.
Select List	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.
Compare Field	log_date The Compare Field is used to identify new events that are added between queries to the table.
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.
Use Prepared Statements	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.
Polling Interval	The amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values that are entered without an H or M poll in seconds.
EPS Throttle	The number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.

- Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Fasoo Enterprise DRM:

Table 206. Fasoo Enterprise DRM sample message

Event name	Low level category	Sample log message
Edit - successful	Update Activity Succeeded	<pre>log_id: "xxxxxxxxxxxxxxxxxxxxxx" log_date: "2016-03-21 14:17:36.000" log_type: "1" product: "1" purpose: "16" usage_result: "1" license_status: "0" ip: "<Numeric>" user_code: "usercode" user_name: "username" user_dept_code: "xxxxxxxxxxxxxxxxxxxxx" user_dept_name: "userdeptname" position_code: "P001" position_name: "Employee" content_code: "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" current_content_name: "New Microsoft PowerPoint Presentation.pptx" content_name: "New Microsoft PowerPoint Presentation.pptx" sec_level_code: "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" sec_level_name: "Basic" system_code: "NULL" system_name: "NULL" owner_code: "ownercode" owner_name: "ownername" owner_dept_code: "xxxxxxxxxxxxxxxxxxxxx" owner_dept_name: "ownerdeptname" content_create-date: "2016-03-21 03:41:28.000" entry_date: "2016-03-21 13:18:26.670"</pre>

Related concepts:

["JDBC protocol configuration options" on page 16](#)

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

Related tasks:

["Adding a DSM" on page 4](#)

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

["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 Security 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,
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_content.content_create_date,
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
```

56 Fidelis XPS

The Fidelis XPS DSM for IBM Security 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 Security 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 363.

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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 207. 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 Fidelis XPS appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

57 FireEye

The IBM Security 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 208. FireEye DSM specifications

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

To integrate FireEye with QRadar, use the following procedures:

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

Related tasks:

[“Configuring your FireEye HX system for communication with QRadar” on page 366](#)

To enable FireEye HX to communicate with IBM Security QRadar, configure your FireEye HX appliance to forward syslog events.

[“Configuring your FireEye system for communication with QRadar”](#)

To enable FireEye to communicate with IBM Security QRadar, configure your FireEye appliance to forward syslog events.

[“Adding a DSM” on page 4](#)

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

[“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 Security 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”](#)

To enable FireEye HX to communicate with IBM Security 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 Security 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
```

Configuring a FireEye log source in QRadar

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

About this task

Procedure

1. Log in to QRadar
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.

4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **FireEye**.
7. Using the **Protocol Configuration** list, select **Syslog**.
8. In the **Log Source Identifier** field, type the IP address or host name of the FireEye appliance.
9. Configure the remaining parameters.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

58 FORCEPOINT

IBM Security QRadar supports a range of FORCEPOINT DSMs.

FORCEPOINT is formerly known as Websense.

Related concepts:

155, “Websense,” on page 981

QRadar supports a range of Websense DSMs.

FORCEPOINT Stonesoft Management Center

The IBM Security 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 209. Stonesoft Management Center DSM specifications

Specification	Value
Manufacturer	FORCEPOINT
DSM name	Stonesoft Management Center
RPM file name	DSM-StonesoftManagementCenter-QRadar_version-build_number.noarch.rpm
Supported versions	5.4 to 6.1
Protocol	Syslog
Event format	LEEF
Recorded event types	Management Center, IPS, Firewall, and VPN events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	FORCEPOINT website (https://www.forcepoint.com)

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:
 - DSMCommon RPM
 - 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 210. Stonesoft Management Center log source parameters

Parameter	Value
Log Source type	Stonesoft Management Center
Protocol Configuration	Syslog

Table 210. Stonesoft Management Center log source parameters (continued)

Parameter	Value
Log Source Identifier	Type a unique name for the log source.

4. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Stonesoft Management Center:

Table 211. Stonesoft Management Center sample message

Event name	Low level category	Sample log message
Generic_UDP-Rugged-Director-Denial-Of-Service	Misc DoS	LEEF:1.0 FORCEPOINT IPS 5.8.5 Generic_UDP-Rugged-Director-Denial-Of-Service dev TimeFormat=MMM dd yyyy HH:mm:ss srcMAC=00:00:00:00:00:00 sev=2 dstMAC=00:00:00:00:00:00 devTime=Feb 23 2017 10:13:58 proto=17 dstPort=00000 srcPort=00000 dst=127.0.0.1 src=127.0.0.1 action=Permit logicalInterface=NY2-1302-DMZ_IPS_ASA_Primary sender="username" Sensor

Related tasks:

"Adding a DSM" on page 4

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

"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 212. Log server configuration options

Parameter	Value	Description
SYSLOG_EXPORT_FORMAT	LEEF	Type LEEF as the export format to use for syslog.

Table 212. Log server configuration options (continued)

Parameter	Value	Description
SYSLOG_EXPORT_ALERT	YES NO	Type one of the following values: <ul style="list-style-type: none">• Yes - Exports alert entries to QRadar by using the syslog protocol.• No - Alert entries are not exported.
SYSLOG_EXPORT_FW	YES NO	Type one of the following values: <ul style="list-style-type: none">• 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 NO	Type one of the following values: <ul style="list-style-type: none">• 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.

6. Save the LogServerConfiguration.txt file.
 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:

Parameter	Value
Source	Type the IPv4 address of your Stonesoft Management Center Log server.
Destination	Type the IPv4 address of your QRadar Console or Event Collector.
Service	Select Syslog (UDP) .
Action	Select Allow .
Logging	Select None .

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*.

- 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 TRITON

The Forcepoint V-Series Content Gateway DSM for IBM Security QRadar supports events for web content from several Forcepoint TRITON solutions, including Web Security, Web Security Gateway, Web Security Gateway Anywhere, and V-Series appliances.

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

- 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>.
 - 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>.
 For information on adding a Forcepoint Multiplexer to software installations, see your *Forcepoint Security Information Event Management (SIEM) Solutions* documentation.
- Enable the Forcepoint Multiplexer on a V-Series appliance that is configured as a full policy source or user directory and filtering appliance:
 - Log in to your Forcepoint TRITON Web Security Console or V-Series appliance.
- 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 372 and “Forcepoint TRITON” on page 372 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 Security 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 213. Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from Forcepoint TRITON or V-Series appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
The log source is added to QRadar.

Forcepoint V-Series Data Security Suite

The Forcepoint V-Series Data Security Suite DSM for IBM Security QRadar supports Forcepoint V-Series appliances and the Data Security Suite (DSS) software.

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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 214. 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 Forcepoint V-Series Data Security Suite DSM

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 Security 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 Security 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=%<chi> devTime=%<cqtn>
devTimeFormat=dd/MMM/yyyy:HH:mm:ss Z
http-username=%<caun> url=%<cquc>
method=%<cqhm> httpversion=%<cqhv>
cachedcode=%<crc>dstBytes=%<sscl> dst=%<pqsi>
srcBytes=%<pscl> proxy-status-code=%<pssc>
server-status-code=%<sssc> usrName=%<wui>
duration=%<ttms>"/>
</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 Security QRadar.

- To start logging immediately, type the following command:

```
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 376 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

- Log in to QRadar.
- Click the **Admin** tab.
- On the navigation menu, click **Data Sources**.
- Click the **Log Sources** icon.
- Click **Add**.
- In the **Log Source Name** field, type a name for your log source.
- In the **Log Source Description** field, type a description for the log source.
- From the **Log Source Type** list, select **Forcepoint V Series**.
- Using the **Protocol Configuration** list, select **Syslog**.
- Configure the following values:

Table 215. 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 Forcepoint V-Series Content Gateway appliance.

- Click **Save**.
- 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 Security 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.
3. Select **Subsystems > Logging**.
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.
12. In the **Remote Directory** field, type /opt/WCG/logs.
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."
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.

59 ForeScout CounterACT

The ForeScout CounterACT DSM for IBM Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 216. 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 ForeScout CounterACT appliance.

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 Security 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 Security 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.

60 Fortinet FortiGate Security Gateway

The IBM Security 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 217. Fortinet FortiGate Security Gateway DSM specifications

Specification	Value
Manufacturer	Fortinet
DSM name	Fortinet FortiGate Security Gateway
RPM file name	DSM-FortinetFortiGate-QRadar_version-build_number.noarch.rpm
Supported versions	FortiOS V5.6 and earlier
Protocol	Syslog Syslog Redirect
Recorded event types	All events
Auto discovered?	Yes
Includes identity?	Yes
Includes custom properties?	Yes
More information	Fortinet website (http://www.fortinet.com)

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:

Parameter	Value
Log Source Identifier Regex	<code>devname=(\w-+)</code>
Listen Port	517
Protocol	UDP

Related tasks:

“Adding a DSM” on page 4

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

"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 syslog destination on your Fortinet FortiGate Security Gateway device"

To forward Fortinet FortiGate Security Gateway events to IBM Security QRadar, you must configure a syslog destination.

"Configuring a syslog destination on your Fortinet FortiAnalyzer device"

To forward Fortinet FortiAnalyzer events to IBM Security QRadar, you must configure a syslog destination.

Configuring a syslog destination on your Fortinet FortiGate Security Gateway device

To forward Fortinet FortiGate Security Gateway events to IBM Security 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 Security 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:

Parameter	Description
Port	The default port is 514.

5. Click **OK**.

61 Foundry FastIron

You can integrate a Foundry FastIron device with IBM Security 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 Security 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.
9. Using the Protocol Configuration list, select **Syslog**.
10. Configure the following values:

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 Foundry FastIron appliance.

11. Click Save.
12. On the Admin tab, click Deploy Changes.
The configuration is complete.

62 FreeRADIUS

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

The following table lists the specifications for the FreeRADIUS DSM:

Table 218. FreeRADIUS DSM specifications

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

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

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

Table 219. FreeRADIUS log source parameters

Parameter	Value
Log Source type	FreeRADIUS
Protocol Configuration	Syslog

Configuring your FreeRADIUS device to communicate with QRadar

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

Before you begin

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

About this task

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

Procedure

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

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

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

```
# .=notice logs authentication messages (L_AUTH).
# <facility_name>.=notice @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>
# .=err logs module errors for FreeRADIUS.
#<facility_name>.=err @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>
# .* logs messages to the same target.
# <facility_name>.* @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>
```

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

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

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

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

7. Add the following options to the FreeRADIUS startup script:

- -l syslog
- -g <facility_name>

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

8. Restart FreeRADIUS.

63 Generic

IBM Security QRadar supports a range of Generic DSMs.

Generic Authorization Server

The generic authorization server DSM for IBM Security 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 Security 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:

`login_success_pattern=<login success pattern>`

Where: <login success pattern> is the pattern that is determined in “Configuring event properties” on page 389.

For example:

```
login_success_pattern=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:

```
Jun 27 12:58:33 expo sshd[20627]: Failed password for root from <IP_address> port 1849 ssh2
```

The pattern for login failures is Failed password.

8. Add the following to the file:

```
login_failed_pattern=<login failure pattern>
```

Where: <login failure pattern> is the pattern that is determined for login failure.

For example:

```
login_failed_pattern=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:

```
Jun 27 13:00:01 expo su(<Username>)[22723]: session closed for user genuser
```

The pattern for logout is session closed.

10. Add the following to the genericAuthServer.conf file:

```
logout_pattern=<logout pattern>
```

Where: <logout pattern> is the pattern that is determined for logout in “Configuring event properties” on page 389.

For example:

```
logout_pattern=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:

```
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 from and the pattern for source port is port.

12. Add an entry to the file for source IP address and source port:

```
source_ip_pattern=<source IP pattern>
```

```
source_port_pattern=<source port pattern>
```

Where: <source IP pattern> and <source port pattern> are the patterns that are identified in “Configuring event properties” on page 389 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 Security 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.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 220. 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 generic authorization appliance.

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 Security 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 Security 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 391. 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:

```
Aug. 5, 2005 08:30:00 Packet denied. Source IP: <Source_IP_address> Source Port: 21  
Destination IP: <Destination_IP_address> Destination Port: 21 Protocol: tcp
```

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 391.

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:

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 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 391.

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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
The syslog protocol configuration is displayed.
10. Configure the following values:

Table 221. 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 generic firewall appliance.

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.

64 genua genugate

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

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

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

Table 222. genua genugate DSM specifications

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

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

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
 - DSMCommon RPM
 - genua genugate DSM RPM

2. Configure your genua genugate device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a genua genugate log source on the QRadar Console. Configure all required parameters and use the following table to identify specific values for genua genugate:

Table 223. genua genugate log source parameters

Parameter	Value
Log Source type	genua genugate
Protocol Configuration	Syslog

Related tasks:

“Adding a DSM” on page 4

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

“Configuring genua genugate to send events to QRadar”

Configure genua genugate to send events to IBM Security QRadar.

“Adding a log source” on page 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 genua genugate to send events to QRadar

Configure genua genugate to send events to IBM Security QRadar.

Procedure

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

65 Great Bay Beacon

The Great Bay Beacon DSM for IBM Security 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” to configure all of the events that you want to monitor in IBM Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 224. 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 Great Bay Beacon appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

66 HBGary Active Defense

The HBGary Active Defense DSM for IBM Security 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 Security 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 225. HBGary Active Defense syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for your HBGary Active Defense device. The IP address or host name identifies your HBGary Active Defense device as a unique event source in QRadar.

11. Click **Save**.

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

The HBGary Active Defense configuration is complete.

67 H3C Technologies

IBM Security QRadar accepts events from a range of H3C Technologies DSMs.

H3C Comware Platform

The IBM Security 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 226. H3C Comware Platform DSM specifications

Specification	Value
Manufacturer	H3C Technologies Co., Limited
DSM name	H3C Comware Platform, H3C Switches, H3C Routers, H3C Wireless LAN Devices, and H3C IP Security Devices.
RPM file name	DSM-H3CComware-QRadar_version-build_number.noarch.rpm
Supported versions	V7
Protocol	Syslog
Event format	NVP
Recorded event types	System
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	H3C Technologies (http://www.h3c.com)

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 227. H3C Comware Platform log source parameters

Parameter	Value
Log Source type	H3C Comware Platform
Protocol Configuration	Syslog

The following table provides a sample syslog event message for the H3C Comware Platform DSM:

Table 228. H3C Comware Platform sample syslog message

Event name	Low level category	Sample log message
A user's AAA request is rejected	AAA Session Denied	<188>Jun 14 17:11:11 2013 HP %%10AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain =domain1-Service=login- UserName=cwf@system; AAA is failed.

Related tasks:

“Adding a DSM” on page 4

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

“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.

68 Honeycomb Lexicon File Integrity Monitor (FIM)

You can use the Honeycomb Lexicon File Integrity Monitor (FIM) DSM with IBM Security 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 Security 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 Security 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 Security 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 229. 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 Honeycomb Lexicon FIM installation. The Log Source Identifier must be unique value.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	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.
Target Event Collector	From the list, select the Target Event Collector to use as the target for the log source.

Table 229. Syslog protocol parameters (continued)

Parameter	Description
Coalescing Events	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.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
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.

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.

69 Hewlett Packard (HP)

IBM Security QRadar can be integrated with several Hewlett Packard (HP) DSMs.

HP Network Automation

The IBM Security 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 230. HP Network Automation DSM specifications

Specification	Value
Manufacturer	Hewlett Packard
DSM name	HP Network Automation
RPM file name	DSM-HPNetworkAutomation-QRadar_version-build_number.noarch.rpm
Supported versions	V10.11
Protocol	Syslog
Event format	LEEF
Recorded event types	All operational and configuration network events.
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Hewlett Packard Network Automation (http://www.hpe.com/software/na)

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 231. HP Network Automation log source parameters

Parameter	Value
Log Source type	HP Network Automation
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the device from where QRadar collects HP Network Automation events.

The following table shows a sample LEEF message from the HP Network Automation DSM:

Table 232. HP Network Automation sample message supported by the HP Network Automation software

Event name	Low level category	Sample log message
Device Snapshot	Information	LEEF:1.0 HP Network Automation v10 Device Snapshot devTime=Wed Jul 06 08:26:45 UTC 2016 devTimeFormat=EEE MMM dd HH:mm:ss Z yyyy src=<Source_IP_address> eventId=11111111 userName=UserName eventText=Snapshot of configuration taken

Related tasks:

"Adding a DSM" on page 4

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

"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 Security 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**.
3. Click **New Event Notification & Response Rule**.
4. Configure the parameters for HP Network Automation.

The following table describes the parameter values to send LEEF events to QRadar:

Parameter	Value
Add Email and Event Rule named	You can use any string. For example, QRadar_logs.
To take this action	Select Send Syslog Message from the list.
When the following events occur	<ol style="list-style-type: none"> 1. Select all of the events. 2. Enable the of any importance button. 3. To take action for For Policy No-Compliance events, enable the for all policies button.
Rule Status	Enable the Active button.
Syslog Hostname	QRadar host name or IP address.
Syslog Port	514

Parameter	Value
Syslog Message	<pre>LEEF:1.0 HP Network Automation v10 \$EventType\$ devTime= \$EventDate\$ devTimeFormat=EE E MMM dd HH:mm:ss Z yyyy src=\$IPAddress\$ eventId=\$EventID\$ userName=\$EventUserName\$ eventText= \$EventText\$</pre> <p>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.</p> <p>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.</p>

- Click **Save**.

HP ProCurve

You can integrate an HP ProCurve device with IBM Security 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

- Log into the HP ProCurve device.
- Type the following command to make global configuration level changes.

```
config
```

If successful, the CLI will change to the following prompt:

```
ProCurve(config)#
```
- Type the following command:

```
logging <syslog-ip-addr>
```

Where: <syslog-ip-addr> is the IP address of QRadar.
- To exit config mode, press CTRL+Z.
- 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 Security 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 233. HP ProCurve syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for your HP ProCurve device.

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 Security 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:

Annnnnnn

The single alphabet character A is followed by a seven-digit decimal integer nnnnnnn, 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.

Hewlett Packard UNIX (HP-UX)

You can integrate an HP-UX device with IBM Security QRadar. An HP-UX DSM accepts events by using syslog.

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.
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.

You are now ready to configure the log source in QRadar.

Configure a log source

IBM Security QRadar automatically discovers and creates a log source for syslog events forwarded from HP-UX.

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 **Hewlett Packard UniX**.
9. From the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 234. HP-UX syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for your Hewlett Packard UniX device.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

70 Huawei

IBM Security QRadar can integrate with several Huawei DSMs.

Huawei AR Series Router

The Huawei AR Series Router DSM for IBM Security 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 Security 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:

Syslog protocol parameters

Parameter	Description
Log Source Identifier	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.

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 Security 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 Security 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 Security 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 235. Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address, host name, or name for the log source as an identifier for your Huawei S Series switch. Each log source that you create for your Huawei S Series switch must include a unique identifier, such as an IP address or host name.

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 Security 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.

71 HyTrust CloudControl

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

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

Table 236. HyTrust CloudControl DSM specifications

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

To collect HyTrust CloudControl events, complete the following steps:

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

Table 237. HyTrust CloudControl log source parameters

Parameter	Value
Log Source type	HyTrust CloudControl
Protocol Configuration	Syslog

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“Configuring HyTrust CloudControl to communicate with QRadar” on page 418](#)

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

[“Adding a log source” on page 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 HyTrust CloudControl to communicate with QRadar

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

Procedure

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

72 IBM

IBM Security QRadar supports a number of IBM DSMs.

IBM AIX

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

IBM AIX Server DSM overview

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

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

Table 238. IBM AIX Server DSM specifications

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

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

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

Parameter	Description
Log Source Type	IBM AIX Server
Protocol Configuration	Syslog

Related tasks:

“Adding a DSM” on page 4

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

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

"Adding a log source" on page 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 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 239. IBM AIX Audit DSM specifications

Specification	Value
Manufacturer	IBM
DSM names	IBM AIX Audit
RPM file names	DSM-IBMAIXAudit-QRadar_version-build_number.noarch.rpm
Supported versions	V6.1 and V7.1
Protocol type	Syslog Log File Protocol
QRadar recorded event types	Audit events
Automatically discovered?	Yes
Includes identity?	No
More information	IBM website (http://www.ibm.com/)

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

1. Download the latest version of the IBM AIX Audit DSM.

2. For syslog events, complete the following steps:
 - a. Configure your IBM AIX Audit device to send syslog events to QRadar. See “Configuring IBM AIX Audit DSM to send syslog events to QRadar” on page 422.
 - b. If QRadar does not automatically discover the log source, add an IBM AIX Audit log source. Use the following IBM AIX Audit-specific values in the log source configuration:

Parameter	Value
Log Source Type	IBM AIX Audit
Protocol Configuration	Syslog

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

Parameter	Value
Log Source Type	IBM AIX Audit
Protocol Configuration	Log File
Service Type	The protocol to retrieve log files from a remote server. Important: If you select the SCP and SFTP service type, ensure that the server that is specified in the Remote IP or Hostname parameter has the SFTP subsystem enabled.
Remote Port	If the host for your event files uses a non-standard port number for FTP, SFTP, or SCP, adjust the port value.
SSH Key File	If you select SCP or SFTP as the Service Type, use this parameter to define an SSH private key file. When you provide an SSH Key File, the Remote Password parameter is ignored.
Remote Directory	The directory location on the remote host where the files are retrieved. Specify the location relative to the user account you are using to log in. Restriction: For FTP only. If your log files are in a remote user home directory, leave the remote directory blank to support operating systems where a change in the working directory (CWD) command is restricted.
FTP File Pattern	The FTP file pattern must match the name that you assigned to your AIX audit files with the -n parameter in the audit script. For example, to collect files that start with AIX_AUDIT and end with your time stamp value, type AIX_Audit_* .
FTP Transfer Mode	ASCII is required for text event logs that are retrieved by the log file protocol by using FTP.
Processor	NONE
Change Local Directory?	Leave this check box clear.
Event Generator	LineByLine The Event Generator applies more processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks:

"Adding a DSM" on page 4

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

"Configuring IBM AIX Audit DSM to send syslog events to QRadar"

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

"Configuring IBM AIX Audit DSM to send log file protocol events to QRadar" on page 423

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

"Adding a log source" on page 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 AIX Audit DSM to send syslog events to QRadar

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

About this task

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

Procedure

1. Log in to your IBM AIX appliance.
2. Open the audit configuration file:
`/etc/security/audit/config`
3. Edit the Start section to disable the **binmode** element and enable the **streammode** element:
`binmode = off`
`streammode = on`
4. Edit the Classes section to specify which classes to audit.
5. Save the configuration changes.
6. Open the streamcmds file:
`/etc/security/audit/streamcmds`
7. Add the following line to the file:
`/usr/sbin/auditstream | /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:

```
trail = /audit/trail
bin1 = /audit/bin1
bin2 = /audit/bin2
binsize = 10240
cmds = /etc/security/audit/bincmds
```

In most cases, you do not have to edit the binary file in the bin1 and bin2 directories.
 - d. In the Classes section, edit the configuration to determine which classes are audited. For information on configuring classes, see your IBM AIX documentation.
 - e. Save the configuration changes.
3. Start auditing on your IBM AIX system:

```
audit start
```

4. Install the audit script:

a. Access the IBM Support website (<http://www.ibm.com/support>).

b. Download the audit.pl.gz file.

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

d. Extract the file:

```
tar -zxvf audit.pl.gz
```

e. Start the audit script:

```
./audit.pl
```

You can add the following parameters to modify the command:

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

What to do next

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

IBM i

The IBM Security 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 240. IBM i DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM i

Table 240. IBM i DSM specifications (continued)

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

To collect events from IBM 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 241. IBM i log source parameters

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

Related tasks:

“Configuring IBM i to integrate with IBM Security QRadar”

You can integrate IBM i with IBM Security QRadar.

“Adding a DSM” on page 4

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

“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 Townsend Security Alliance LogAgent to integrate with QRadar” on page 429

You can collect all audit logs and system events from Townsend Security Alliance LogAgent. You must configure Alliance LogAgent for the IBM Security QRadar LEEF and configure a destination that specifies QRadar as the syslog server.

Configuring IBM i to integrate with IBM Security QRadar

You can integrate IBM i with IBM Security 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
1cd 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/AUDITRN 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.

```
DSPJRN JRN(QSYS/QAUDJRN) RCVRNG(AUDRCV0001 AUDRCV0003)
JRNCDE((T)) ENTTYP(*ALL)
OUTPUT(*OUTFILE) OUTFILFMT(*TYPE5) OUTFILE(QTEMP/AUDITJRN)
ENTDTALEN(*VARLEN 16000 100)
```

3. To set the **Date Time** to use outfile *OUTF support, run the **AJLIB/DATETIME** command.

```
DSPJRN Start and End Times

F3 EXIT Without Update
ENTER Exit With Update

Blank End Date and/or Time will use current Date and/or Time

Start Date *OUTF
Start Time 113109
End Date
End Time

F3=Exit
```

Figure 7. DSPJRN Start and End Times

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 Security 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 Security 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:: **addlib 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.

Parameter	Description
Interface version	4=IBM QRadar LEEF
Transmit	1=Yes
Data queue control	1=Yes
Format	4=IBM QRadar LEEF

6. From the configuration menu, select **Work With TCP Clients**.
7. Select option 2 to change the **SYSLOGD** client and configure the following parameters.

Parameter	Description
Status	1=Active
Autostart client	1=Yes
Remote IP address	IP address of QRadar
Remote port number	514

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:

```
/* 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 Security QRadar accepts system events in Log Extended Event Format (LEEF) retrieved from IBM BigFix.

IBM BigFix is formerly known as IBM Tivoli® Endpoiont 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:

IBM BigFix SOAP protocol configuration

Parameter	Description
Log Source Identifier	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.
Port	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.
Use HTTPS	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: <code>/opt/qradar/conf/trusted_certificates</code> 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.
Username	Type the user name that is required to access your IBM BigFix.
Password	Type the password that is required to access your IBM BigFix.
Confirm Password	Confirm the password necessary to access your IBM BigFix.

For more information about configuring QRadar to import IBM BigFix vulnerabilities assessment information, see the *IBM Security QRadar Vulnerability Assessment Guide*.

Click **Save**.

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

Related concepts:

"IBM BigFix SOAP protocol configuration options" on page 15

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 Security 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 242. IBM BigFix Detect DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM BigFix Detect
RPM file name	DSM-IBMBigFixDetect-QRadar_version-build_number.noarch.rpm
Supported versions	V9.5
Protocol	IBM BigFix EDR REST API Protocol
Event format	LEEF
Recorded event types	IOC and IOA alerts
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	IBM BigFix website (http://www-03.ibm.com/security/bigfix/index.html)

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 243. IBM BigFix Detect log source parameters

Parameter	Value
Log Source type	IBM BigFix Detect
Protocol Configuration	IBM BigFix EDR REST API
API Hostname or IP	The host name or IP address of the BigFix EDR API
API Port	The port number that is used to access the API. The default is 443.

Table 243. IBM BigFix Detect log source parameters (continued)

Parameter	Value
Client Certificate Filename	The PKCS12 certificate file name in the /opt/qradar/conf/trusted_certificates/ibmbigfixedr directory in QRadar.
Client Certificate Password	The password that you used for the Client Certificate .
Use Proxy	If QRadar accesses the BigFix EDR API 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.
Automatically Acquire Server Certificate(s)	Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.
EPS Throttle	The maximum number of events per second. The default is 5000.

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 244. IBM BigFix Detect sample LEEF message

Event name	Low level category	Sample log message
IOC Detected	Suspicious Activity	LEEF:1.0 IBM IBM BigFix Detect BF-Detect.9.5 blue.static alert_id =xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx xx event_id=xxxxxxxxxxxx ak=00000000000000000000000000000000 0962AA560FD9E45E5270557BB9DA801E resource=12587632 bf_ endpoint_name=xxxxxxxxxxxx det ected_ioc=urn:xxx.xxx.example.com:origi n.bigfixqaedr//example:Indicator-xxx xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx /ver/1 devTime=Feb 09 2017 06: 11:32.000 UTC detection_descri ption=IOC 00_jw-mo_File name and pa th detected. detection_mechani sm=blue.static risk=medium sev=5 confidence=low devTimeFormat=MMM dd yyyy HH: mm:ss.SSS z

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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:

Parameter	Description
private_key_filename	The Private key that you obtained from the BigFix administrator.
certificate_filename	The corresponding certificate that you obtained from the BigFix administrator.
PKCS#12_filename	The output keystore file name. For example, <code>bigfix_client_certificate.pkcs12</code>

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 Security QRadar DSM for the IBM Bluemix Platform collects events logs from your Bluemix Platform.

The following table identifies the specifications for the Bluemix Platform DSM:

Table 245. Bluemix Platform DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	Bluemix Platform
RPM file name	DSM-IBMBluemixPlatform-7.x-xxxxxx.noarch.rpm
Supported versions	N/A
Protocol	Syslog, TLS Syslog
Recorded event types	All System (Cloud Foundry) events, some application events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	IBM website for Bluemix (IBM website for Bluemix)

To integrate 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 Bluemix Platform DSM RPM on your QRadar Console:
2. Configure your Bluemix Platform device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Bluemix Platform log source on the QRadar Console.

Related tasks:

"Adding a DSM" on page 4

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

"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 Bluemix Platform to communicate with QRadar

To collect 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 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:
`cf cups drain_name -l syslog://QRadar_IP_Address:514`

Alternatively, use the following command:

```
cf cups drain_name -l syslog-tls://QRadar_IP_Address:1513  
1513 is the port that is used to communicate with QRadar.
```

- Bind the service instance with the following command:

```
cf bind-service BusinessApp_name drain_name
```

Integrating 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

- 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.
- 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.
- Download and install the latest 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 Bluemix log source in QRadar by using Syslog or Syslog TLS.

Configuring a Bluemix log source to use Syslog

You can configure a Bluemix log source in IBM Security QRadar.

Procedure

- Log in to QRadar to use **Syslog**.
- On the **Admin** tab, click **Data Sources > Log Sources > Add**.
- From the **Log Source Type** list, select **Bluemix Platform**.
- From the **Protocol Configuration** list, select **Syslog**.
- 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, 192.0.2.1:1234.

- Configure the remaining fields in the Log Sources window as required and click **Save**.

- On the **Admin** tab toolbar, click **Deploy Changes**.

Related tasks:

“Adding a DSM” on page 4

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

“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 Bluemix log source with TLS Syslog

You can configure a Bluemix log source in IBM Security QRadar to use TLS Syslog.

Procedure

- Log in to QRadar.
- On the **Admin** tab, click **Data Sources > Log Sources > Add**.

3. From the **Log Source Type** list, select **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

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

"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 Security 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.
4. If you want to create a custom event property for IBM CICS 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.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (<http://www-01.ibm.com/support/docview.wss?uid=pub1sc27277200>).

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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 246. Log source parameters

Parameter	Value
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Creating a log source for Log File protocol

The Log File protocol enables IBM Security 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 247. Log File protocol parameters

Parameter	Value
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 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.
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. <ul style="list-style-type: none">• 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.

Table 247. Log File protocol parameters (continued)

Parameter	Value
Remote Port	<p>Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535.</p> <p>The options include ports:</p> <ul style="list-style-type: none"> • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 <p>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.</p>
Remote User	<p>Type the user name or user ID necessary to log in to the system that contains your event files.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>If you configure SCP as the Service Type, the Recursive option is ignored.</p>
FTP File Pattern	<p>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.</p> <p>The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <code><product_name>.<timestamp>.gz</code></p> <p>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>z0S</code> and end with <code>.gz</code>, type the following code:</p> <pre><code>z0S.*\.gz</code></pre> <p>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/)</p>
FTP Transfer Mode	<p>This option displays only if you select FTP as the Service Type. From the list, select Binary.</p> <p>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.</p>
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.

Table 247. Log File protocol parameters (continued)

Parameter	Value
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.
Processor	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.
Ignore Previously Processed File(s)	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.
Change Local Directory?	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.
Event Generator	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.

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 Security 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 248. IBM DataPower DSM specifications

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

To send events from IBM 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:

Parameter	Value
Log Source Type	IBM DataPower
Protocol Configuration	Syslog

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“Configuring IBM DataPower to communicate with QRadar”](#)

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

Configuring IBM DataPower to communicate with QRadar

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

Before you begin

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

Procedure

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

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

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

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 Security 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.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (<http://www-01.ibm.com/support/docview.wss?uid=pub1sc27277200>).

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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 249. Log source parameters

Parameter	Value
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Creating a log source for Log File protocol

The Log File protocol enables IBM Security 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 250. Log File protocol parameters

Parameter	Value
Log Source Identifier	<p>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.</p> <p>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.</p>

Table 250. Log File protocol parameters (continued)

Parameter	Value
Service Type	<p>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.</p> <ul style="list-style-type: none"> • SFTP - SSH File Transfer Protocol • FTP - File Transfer Protocol • SCP - Secure Copy <p>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>
Remote IP or Hostname	Type the IP address or host name of the device that stores your event log files.
Remote Port	<p>Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535.</p> <p>The options include ports:</p> <ul style="list-style-type: none"> • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 <p>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.</p>
Remote User	<p>Type the user name or user ID necessary to log in to the system that contains your event files.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>If you configure SCP as the Service Type, the Recursive option is ignored.</p>
FTP File Pattern	<p>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.</p> <p>The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <code><product_name>.<timestamp>.gz</code></p> <p>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 z0S and end with .gz, type the following code:</p> <pre>z0S.*\.gz</pre> <p>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/)</p>

Table 250. Log File protocol parameters (continued)

Parameter	Value
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.
Processor	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.
Ignore Previously Processed File(s)	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.
Change Local Directory?	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.
Event Generator	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.

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 Security 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”

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 448

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:

```
db2audit start
```

For example, the start command response might resemble the following output:

```
AUD00001 Operation succeeded.
```

3. Move the audit records from the instance to the audit log:

```
db2audit flush
```

For example, the flush command response might resemble the following output:

```
AUD00001 Operation succeeded.
```

4. Extract the data from the archived audit log and write the data to .del files:

```
db2audit extract delasc
```

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. Remove non-active records:

```
db2audit prune all
```

6. Move the .del files to a storage location where IBM Security 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.

Extracting audit data for DB2 v9.5

You can extract audit data when you are using IBM DB2 v9.5.

Procedure

1. Log in to a DB2 account with SYSADMIN privilege.
2. Move the audit records from the database instance to the audit log:

```
db2audit flush
```

For example, the flush command response might resemble the following output:
AUD00001 Operation succeeded.

3. Archive and move the active instance to a new location for future extraction:

```
db2audit archive
```

For example, an archive command response might resemble the following output:

```
Node AUD Archived or Interim Log File Message
```

```
-----
```

```
- 0 AUD00001 dbsaudit.instance.log.0.20091217125028 AUD00001 Operation succeeded.
```

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

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

Table 251. IBM Federated Directory Server DSM specifications

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

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

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

Table 252. IBM Federated Directory Serve log source parameters

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

Related tasks:

“Adding a DSM” on page 4

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

“Configuring IBM Federated Directory Server to monitor security events” on page 450

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

“Adding a log source” on page 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 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 Security QRadar can collect event logs from the Fiberlink MaaS360 console.

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

Table 253. IBM Fiberlink MaaS360 DSM Specification

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

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

1. If automatic updates are not enabled, download the latest versions of the following RPMs:
 - DSMCommon RPM
 - IBM Fiberlink REST API Protocol RPM
 - IBM Fiberlink MaaS360 RPM

- Configure your Fiberlink MaaS360 instance to enable communication with QRadar.
- Add an IBM Fiberlink MaaS360 log source on the QRadar Console.

Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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

- Log in to QRadar.
- Click the **Admin** tab.
- In the navigation menu, click **Data Sources**.
- Click the **Log Sources** icon.
- Click **Add**.
- From the Log Source Type list, select **IBM Fiberlink MaaS360**.
- From the Protocol Configuration list, select **IBM Fiberlink REST API**.
- Configure the following IBM Fiberlink REST API parameters:

Parameter	Description
Log Source Identifier	Type a unique identifier for the log source. The Log Source Identifier can be set to any valid value and does not need to reference a specific server. You can set the Log Source Identifier 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 <i>fiberlink1</i> , the second log source as <i>fiberlink2</i> , and the third log source as <i>fiberlink3</i> .
Login URL	The URL for the Fiberlink MaaS360 REST server.
Username	The user name that is used to access the MaaS360 APIs. Users with the following administrator roles can access the APIs: <ul style="list-style-type: none"> • Service Administrator • Administrator • Administrator-Level 2
Password	The password that is used to access your MaaS360 APIs.
Secret Key	The secret key that is provided by Fiberlink Customer Service when you enabled the REST API.
App ID	The App ID that was provided by Fiberlink Customer Service when you enabled the REST API.

Parameter	Description
Billing ID	The Billing ID for your Fiberlink MaaS360 account.
Platform	The platform version of the Fiberlink MaaS360 console.
App Version	The App Version of the application that corresponds to your REST API account.
Use Proxy	If QRadar accesses the Fiberlink MaaS360 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
Automatically Acquire Server Certificate(s)	QRadar automatically downloads the server certificate and begins trusting the target server when the Yes option is selected.

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 Security QRadar collects informational, error, alert, and warnings from IBM Guardium by using syslog. IBM Security 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 453.
2. Configure your existing policies to generate syslog events. For more information, see “Configuring policies to generate syslog events” on page 453.
3. Install the policy on IBM Guardium. For more information, see “Installing an IBM Guardium Policy” on page 454.
4. Configure the log source in QRadar. For more information, see “Configuring a log source” on page 454.
5. Identify and map unknown policy events in QRadar. For more information, see “Creating an event map for IBM Guardium events” on page 455.

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 Security 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 Security 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 453 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 453.
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 Security QRadar.

Configuring a log source

IBM Security 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 254. IBM Guardium syslog configuration

Parameter	Description
Log Source Identifier	Type the IP address or host name for the IBM InfoSphere Guardium appliance.

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 Security 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 Security 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 Security 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 (IMSTM) DSM for IBM Security 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 -zvxf 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 terced 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,BLKSIZE=12901,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=OM /* //**QEXIMS JCL VERSION 1.0 FEBRUARY 2011
/*
//***** Change dataset names to site specific dataset names *
//*****SET1 SET IMSOUT='Q1JACK.QEXIMS.OUTPUT',
// IMSIN='Q1JACK.QEXIMS.INPUT.DATA'
//***** Delete old datasets *
//***** DEL EXEC PGM=IEFBR14 //DD1 DD DISP=(MOD,DELETE),DSN=&IMSOUT,
// UNIT=SYSDA, // SPACE=(CYL,(10,10)), // DCB=(RECFM=FB,LRECL=80)
//***** Allocate new dataset
//***** ALLOC EXEC PGM=IEFBR14 //DD1 DD DISP=(NEW,CATLG),DSN=&IMSOUT,
// SPACE=(CYL,(21,2)),
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//EXTRACT EXEC PGM=QEXIMS,DYNAMNBR=10,
// TIME=1440 //STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN DD DUMMY
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=/* //IMSIN DD DISP=SHR,DSN=&IMSIN
//IMSOUT DD DISP=SHR,DSN=&IMSOUT
//*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=*
//*

```

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:

```

//*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:

```
/*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 Security 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 255. Log file protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source. The log source identifier must be unique for the log source type.
Service Type	From the list, select the protocol that you want to use when retrieving log files from a remove server. The default is SFTP. <ul style="list-style-type: none">• SFTP - SSH File Transfer Protocol• FTP - File Transfer Protocol• SCP - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service types requires that the server specified in the Remote IP or Hostname field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the IBM IMS system.

Table 255. Log file protocol parameters (continued)

Parameter	Description
Remote Port	Type the TCP port on the remote host that is running the selected Service Type . If you configure the Service Type as FTP , the default is 21. If you configure the Service Type as SFTP or SCP , the default is 22. The valid range is 1 - 65535.
Remote User	Type the user name necessary to log in to your IBM IMS system. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to your IBM IMS system.
Confirm Password	Confirm the Remote Password to log in to your IBM IMS system.
SSH Key File	If you select SCP or SFTP from the Service Type field you can define a directory path to an SSH private key file. The SSH Private Key File gives the option to ignore the Remote Password field.
Remote Directory	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.
Recursive	Select this check box if you want the file pattern to also search sub folders. The Recursive parameter is not used if you configure SCP as the Service Type . By default, the check box is clear.
FTP File Pattern	If you select SFTP or FTP as the Service Type , this gives the option to configure the regular expression (regex) used 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 <starttime>.<endtime>.<hostname>.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: 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 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: <ul style="list-style-type: none"> 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 ASCII is used 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.

Table 255. Log file protocol parameters (continued)

Parameter	Description
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 the contents to be processed.
Ignore Previously Processed File(s)	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.
Change Local Directory?	Select this check box to define the local directory on your QRadar system that you want to use for storing downloaded files during processing. We recommend that you leave the check box clear. When the check box is selected, the Local Directory field is displayed, which gives the option to configure the local directory to use for storing files.
Event Generator	From the Event Generator list, select LineByLine .

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 Security 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 21

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 Security 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 Security 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:
`1nsnmp.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:

- ```
linsnmp.sh start
```
7. Create a link to the LNSNMP script

```
ln -f -s /opt/ibm/lotus/notes/latest/ibmpow/linsnmp.sh /etc/linsnmp.rc
```
  8. Configure LNSNMP service to start during the system restart. Add the following line to the end of `/etc/rc.tcpip`  
`/etc/linsnmp.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 Security QRadar.

## Configuring your IBM Lotus Domino device to communicate with QRadar

IBM Security 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 256. SNMPv2 protocol parameters*

| Parameter                            | Description                                                                                                                                                                                         |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b>         | Type an IP address, host name, or name to identify the SNMPv2 event source.<br><br>IP addresses or host names are recommended as they allow QRadar to identify a log file to a unique event source. |
| <b>Community</b>                     | Type the SNMP community name required to access the system containing SNMP events.                                                                                                                  |
| <b>Include OIDs in Event Payload</b> | Clear the value from this check box.<br><br>When selected, this option constructs SNMP events with name-value pairs instead of the standard event payload format.                                   |

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

## IBM Privileged Session Recorder

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

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

*Table 257. IBM Privileged Session Recorder specifications*

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

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 258. IBM Privileged Session Recorder log source parameters*

| Parameter               | Description                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------|
| Log Source Type         | IBM Privileged Session Recorder                                                                            |
| Protocol Configuration  | JDBC                                                                                                       |
| Log Source Identifier   | DATABASE@HOSTNAME                                                                                          |
| Database Type           | DB2                                                                                                        |
| Database Name           | The Session Recorder data store name that you configured on the IBM Privileged Identity Manager dashboard. |
| IP or Hostname          | The Session Recorder database server address.                                                              |
| Port                    | The port that is specified on IBM Privileged Identity Manager dashboard.                                   |
| Username                | The DB2 database user name                                                                                 |
| Password                | The DB2 database password                                                                                  |
| Predefined Query        | IBM Privileged Session Recorder                                                                            |
| Use Prepared Statements | This option must be selected.                                                                              |
| Start Date and Time     | The initial date and time for the JDBC retrieval.                                                          |

#### **Related tasks:**

“Adding a DSM” on page 4

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

“Configuring IBM Privileged Session Recorder to communicate with QRadar”

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

“Adding a log source” on page 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 Privileged Session Recorder to communicate with QRadar**

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

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

#### **Procedure**

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

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

## **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 “JDBC protocol configuration options” on page 16.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

**Related concepts:**

“JDBC protocol configuration options” on page 16

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

---

## IBM Proventia

IBM Security 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 Security 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 Security 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

You can configure IBM Security QRadar to poll for IBM SiteProtector 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 **IBM Proventia Management SiteProtector**.
6. Using the **Protocol Configuration** list, select **JDBC - SiteProtector**.
7. Configure the following values:

*Table 259. JDBC - SiteProtector protocol parameters*

| Parameter                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the identifier for the log source. The log source identifier must be defined in the following format:<br><br><i>&lt;database&gt;@&lt;hostname&gt;</i><br><br>Where: <ul style="list-style-type: none"><li>• <i>&lt;database&gt;</i> is the database name, as defined in the <b>Database Name</b> parameter. The database name is required.</li><li>• <i>&lt;hostname&gt;</i> is the host name or IP address for the log source as defined in the <b>IP or Hostname</b> parameter. The host name is required.</li></ul> The log source identifier must be unique for the log source type.                                                                                                                                                                            |
| <b>Database Type</b>         | From the list, select <b>MSDE</b> as the type of database to use for the event source.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Database Name</b>         | Type the name of the database to which you want to connect. The default database name is <b>RealSecureDB</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>IP or Hostname</b>        | Type the IP address or host name of the database server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Port</b>                  | Type the port number that is used by the database server. The default that is displayed depends on the selected <b>Database Type</b> . The valid range is 0 - 65536. The default for MSDE is port 1433.<br><br>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.<br><br>The default port number for all options includes the following ports: <ul style="list-style-type: none"><li>• MSDE - 1433</li><li>• Postgres - 5432</li><li>• MySQL - 3306</li><li>• Oracle - 1521</li><li>• Sybase - 1521</li></ul> If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration. |
| <b>Username</b>              | Type the database user name. The user name can be up to 255 alphanumeric characters in length. The user name can also include underscores (_).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Password</b>              | Type the database password.<br><br>The password can be up to 255 characters in length.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Confirm Password</b>      | Confirm the password to access the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 259. JDBC - SiteProtector protocol parameters (continued)

| Parameter                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Domain</b>        | If you select <b>MSDE</b> as the <b>Database Type</b> and the database is configured for Windows, you must define a Windows Authentication Domain. Otherwise, leave this field blank.<br><br>The authentication domain must contain alphanumeric characters. The domain can include the following special characters: underscore (_), en dash (-), and period(.).                                                                                                                          |
| <b>Database Instance</b>            | If you select <b>MSDE</b> as the <b>Database Type</b> and you have multiple SQL server instances on one server, define the instance to which you want to connect.<br><br>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 <b>Database Instance</b> parameter blank in your configuration.                                                                                                     |
| <b>Table Name</b>                   | Type the name of the view that includes the event records. The default table name is SensorData1.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>AVP View Name</b>                | Type the name of the view that includes the event attributes. The default table name is SensorDataAVP.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Response View Name</b>           | Type the name of the view that includes the response events. The default table name is SensorDataResponse.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Select List</b>                  | Type * to include all fields from the table or view.<br><br>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 <b>Compare Field</b> 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(.). |
| <b>Compare Field</b>                | Type SensorDataRowID to identify new events added between queries to the table.                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Polling Interval</b>             | Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds.<br><br>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.                                                                                                             |
| <b>Use Named Pipe Communication</b> | If you select <b>MSDE</b> as the <b>Database Type</b> , select this check box to use an alternative method to a TCP/IP port connection.<br><br>When a Named Pipe connection is used, 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.                                                                                                              |
| <b>Database Cluster Name</b>        | If you select the <b>Use Named Pipe Communication</b> check box, the <b>Database Cluster Name</b> 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.                                                                                                                                                                                                                      |
| <b>Include Audit Events</b>         | Select this check box to collect audit events from IBM SiteProtector.<br><br>By default, this check box is clear.                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Use NTLMv2</b>                   | Select the <b>Use NTLMv2</b> check box to force 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.<br><br>If the <b>Use NTLMv2</b> check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.                                                                                                                |

*Table 259. JDBC - SiteProtector protocol parameters (continued)*

| Parameter           | Description                                                          |
|---------------------|----------------------------------------------------------------------|
| Use SSL             | Select this check box if your connection supports SSL communication. |
| Log Source Language | Select the language of the log source events.                        |

8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

## IBM ISS Proventia

The IBM Integrated Systems Solutions® (ISS) Proventia DSM for IBM Security 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**.
3. Select **Services**.  
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 39

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

“SNMPv3 protocol configuration options” on page 39

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

---

## IBM QRadar Packet Capture

The IBM Security 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 260. IBM QRadar Packet Capture DSM specifications*

| Specification | Value                                                             |
|---------------|-------------------------------------------------------------------|
| Manufacturer  | IBM                                                               |
| DSM name      | IBM QRadar Packet Capture                                         |
| RPM file name | DSM-IBMQRadarPacketCapture-QRadar_version-build_number.noarch.rpm |

*Table 260. IBM QRadar Packet Capture DSM specifications (continued)*

| Specification               | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supported versions          | IBM QRadar Packet Capture V7.2.3 to V7.2.7<br>IBM QRadar Network Packet Capture V7.3.0                                                                                                                                                                                                                                                                                                                                                                                      |
| Protocol                    | Syslog                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Event format                | LEEF                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Recorded event types        | All events                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Automatically discovered?   | Yes                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Includes identity?          | No                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Includes custom properties? | No                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| More information            | IBM website ( <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/c_pcap_introduction.html">http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/c_pcap_introduction.html</a> )<br>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> ) |

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
  - IBM QRadar Packet Capture DSM 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 261. IBM QRadar Packet Capture log source parameters*

| Parameter              | Value                     |
|------------------------|---------------------------|
| Log Source type        | IBM QRadar Packet Capture |
| Protocol Configuration | Syslog                    |

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 262. IBM QRadar Packet Capture sample message*

| Event name | Low level category | Sample log message                                                                                                                            |
|------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| User Added | User Account Added | May 10 00:01:04 <Server><br>LEEF: 2.0 IBM QRadar Packet<br>Capture 7.2.7.255-1G<br> UserAdded cat=Admin msg=User<br><Username> has been added |

The following table shows a sample event message from IBM QRadar Network Packet Capture:

Table 263. IBM QRadar Network Packet Capture sample message

| Event name                | Low level category | Sample log message                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packet Capture Statistics | Information        | <14>Mar 1 20:39:41 <Server> LEEF: 2.0 IBM Packet Capture 7.3.0 1 ^  captured_packets=8844869^captured_packets_udp=4077106^captured_bytes_udp=379169082^total_packets=9090561^captured_bytes=27938019 18^captured_bytes_tcp=2379568101 ^compression_ratio=27.4^captured_packets_tcp=4356387^oldest_packet=2017-03-01T20:39:41.915555490Z^ total_bytes=2853950159 |

#### Related tasks:

"Adding a DSM" on page 4

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

"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 Security 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](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](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.
4. If you want to create a custom event property for IBM RACF 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](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](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.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (<http://www-01.ibm.com/support/docview.wss?uid=pub1sc27277200>).

#### **Related tasks:**

“Adding a DSM” on page 4

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

“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 Security 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 264. Log File protocol parameters*

| Parameter                    | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | 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.<br><br>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. |
| <b>Service Type</b>          | From the <b>Service Type</b> list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. <ul style="list-style-type: none"> <li>• SFTP - SSH File Transfer Protocol</li> <li>• FTP - File Transfer Protocol</li> <li>• SCP - Secure Copy</li> </ul> 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 <b>Remote IP or Hostname</b> field has the SFTP subsystem enabled.                                                                                  |
| <b>Remote IP or Hostname</b> | Type the IP address or host name of the device that stores your event log files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Remote Port</b>           | Type the TCP port on the remote host that is running the selected <b>Service Type</b> . The valid range is 1 - 65535.<br><br>The options include ports: <ul style="list-style-type: none"> <li>• FTP - TCP Port 21</li> <li>• SFTP - TCP Port 22</li> <li>• SCP - TCP Port 22</li> </ul> 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.                                                                                                                                                                                           |
| <b>Remote User</b>           | Type the user name or user ID necessary to log in to the system that contains your event files. <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>                                                                                                                           |
| <b>Remote Password</b>       | Type the password necessary to log in to the host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Confirm Password</b>      | Confirm the password necessary to log in to the host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>SSH Key File</b>          | If you select <b>SCP</b> or <b>SFTP</b> as the <b>Service Type</b> , this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the <b>Remote Password</b> field is ignored.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Remote Directory</b>      | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Recursive</b>             | 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.<br><br>If you configure SCP as the Service Type, the Recursive option is ignored.                                                                                                                                                                                                                                                                                                                                                                                       |

Table 264. Log File protocol parameters (continued)

| Parameter                | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FTP File Pattern</b>  | If you select <b>SFTP</b> or <b>FTP</b> as the <b>Service Type</b> , you can configure the regular expression (regex) needed to filter the list of files that are specified in the <b>Remote Directory</b> . All matching files are included in the processing.<br><br>The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <product_name>.<timestamp>.gz<br><br>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:<br><br>zOS.*\.gz<br><br>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> ) |
| <b>FTP Transfer Mode</b> | This option displays only if you select <b>FTP</b> as the <b>Service Type</b> . From the list, select <b>Binary</b> .<br><br>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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>SCP Remote File</b>   | If you select <b>SCP</b> as the <b>Service Type</b> you must type the file name of the remote file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Start Time</b>        | 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.<br><br>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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Recurrence</b>        | 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).<br><br>For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Run On Save</b>       | If you want the Log File protocol to run immediately after you click <b>Save</b> , select this check box.<br><br>After the <b>Run On Save</b> completes, the Log File protocol follows your configured start time and recurrence schedule.<br><br>Selecting <b>Run On Save</b> clears the list of previously processed files for the Ignore Previously Processed File parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>EPS Throttle</b>      | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Processor</b>         | From the list, select <b>gzip</b> .<br><br>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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Table 264. Log File protocol parameters (continued)

| Parameter                           | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ignore Previously Processed File(s) | Select this check box to track and ignore files that are already processed by the Log File protocol.<br><br>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.<br><br>This option applies only to FTP and SFTP service types. |
| Change Local Directory?             | Select this check box to define a local directory on your QRadar for storing downloaded files during processing.<br><br>It is suggested that you leave this check box clear. When this check box is selected, the <b>Local Directory</b> field is displayed, which gives you the option to configure the local directory to use for storing files.                                                                                                                                      |
| Event Generator                     | From the <b>Event Generator</b> list, select <b>LineByLine</b> .<br><br>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.                                                                                                                                                                                                                             |

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](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 Security 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 265. Log source parameters

| Parameter              | Value                                        |
|------------------------|----------------------------------------------|
| Log Source type        | Select your DSM name from the list.          |
| Protocol Configuration | Syslog                                       |
| Log Source Identifier  | Type a unique identifier for the log source. |

## Integrate IBM RACF with IBM Security 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 processes this file.

## Configuring IBM RACF that uses audit scripts to integrate with IBM Security QRadar

IBM Security 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:  

```
tar -zvxf 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 terced 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:

```

//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.

```

//QEXRACF JOB (<your valid jobcard>),Q1LABS,
// MSGCLASS=P, // REGION=0M /*
//**QEXRACF JCL version 1.0 April 2009 /**
//*****
//** Change below dataset names to sites specific datasets names *
//*****
//SET1 SET SMFOUT='<your hlq>.CUSTNAME.IRRADU00.OUTPUT',
// SMFIN='<your SMF dump ouput dataset>',
// QRACFOUT='<your hlq>.QEXRACF.OUTPUT'
//*****
//** Delete old datasets *
//*****
//DEL EXEC PGM=IEFBR14 //DD1 DD DISP=(MOD,DELETE),DSN=&QRACFOUT,
// UNIT=SYSDA, // SPACE=(TRK,(1,1)), // DCB=(RECFM=FB,LRECL=80)
//*****
//** Allocate new dataset *
//*****
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DISP=(NEW,CATLG),DSN=&QRACFOUT,
// SPACE=(CYL,(1,10)),UNIT=SYSDA,
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*****
//** Execute IBM IRRADU00 utility to extract RACF smf records *
//*****
//IRRADU00 EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//ADUPRINT DD SYSOUT=*
//OUTDD DD DSN=&SMFOUT,SPACE=(CYL,(100,100)),DISP=(,CATLG),
// DCB=(RECFM=FB,LRECL=8192,BLKSIZE=40960),
// UNIT=SYSALLDA
//SMFDATA DD DISP=SHR,DSN=&SMFIN
//SMFOUT DD DUMMY
//SYSIN DD *INDD(SMFDATA,OPTIONS(DUMP))
OUTDD(SMFOUT,TYPE(30:83)) ABEND(NORETRY)
USER2(IRRADU00) USER3(IRRADU86) /*
//EXTRACT EXEC PGM=QEXRACF,DYNAMNBR=10,
// TIME=1440
//STEPLIB DD DISP=SHR,DSN=
<the loadlib containing the QEXRACF program if not in LINKLST>

```

```

//SYSTSIN DD DUMMY //SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//RACIN DD DISP=SHR,DSN=&SMFOUT
//RACOUT DD DISP=SHR,DSN=&QRACFOUT //

/* FTP Output file from C program (Qexracf) to an FTP server *
/* QRadar will go to that FTP Server to get file *
/* Note you need to replace <user>, <password>,<serveripaddr>*
/* <THEIPOFTHEMAINFRAMEDEVICE> and <QEXRACFOUTDSN> *

//*FTP EXEC PGM=FTP,REGION=3800K /*INPUT DD *
//*<FTPSERVERIPADDR>
//*<USER>
//*<PASSWORD>
//*ASCII /*PUT '<QEXRACFOUTDSN>'
/<THEIPOFTHEMAINFRAMEDEVICE>/<QEXRACFOUTDSN>
//*QUIT /*OUTPUT DD SYSOUT=*
//*SYSPRINT DD SYSOUT=* /* */

```

8. After the output file is created, you must send this file to an FTP server. This 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 Security 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 266. IBM SAN Volume Controller DSM specifications*

| Specification               | Value                                                                                                                                                                                        |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manufacturer                | IBM                                                                                                                                                                                          |
| DSM name                    | IBM SAN Volume Controller                                                                                                                                                                    |
| RPM file name               | DSM-IBMSANVolumeController-QRadar_version-build_number.noarch.rpm                                                                                                                            |
| Supported versions          | N/A                                                                                                                                                                                          |
| Protocol                    | Syslog                                                                                                                                                                                       |
| Event format                | CADF                                                                                                                                                                                         |
| Recorded event types        | Activity, Control, and Monitor audit events                                                                                                                                                  |
| Automatically discovered?   | Yes                                                                                                                                                                                          |
| Includes identity?          | No                                                                                                                                                                                           |
| Includes custom properties? | No                                                                                                                                                                                           |
| More information            | IBM SAN Volume Controller website<br>( <a href="http://www-03.ibm.com/systems/storage/software/virtualization/svc/">http://www-03.ibm.com/systems/storage/software/virtualization/svc/</a> ) |

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

- Configure your IBM SAN Volume Controller server to send syslog events to QRadar.
- 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 267. IBM SAN Volume Controller log source parameters*

| Parameter              | Value                                                                |
|------------------------|----------------------------------------------------------------------|
| Log Source type        | IBM SAN Volume Controller                                            |
| Protocol Configuration | Syslog                                                               |
| Log Source Identifier  | The IP address or host name of the IBM SAN Volume Controller server. |

- 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 268. IBM SAN Volume Controller sample message*

| Event name        | Low level category        | Sample log message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup Successful | Backup Activity Succeeded | <pre>Oct 12 20:02:33 Cluster_&lt;IP_address&gt; 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": "&lt;IP_address&gt;"}, "attachments": [{"content": "6005076400C8010E5000000000000000000", "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": "xxxxxxxxxx-xxxxxxxxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxx"}</pre> |

#### Related tasks:

"Adding a DSM" on page 4

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

"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
```

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 Security 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

1. Log in to the IMS Configuration Utility for IBM Security Access Manager for Enterprise Single Sign-On.  
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 Server > Logging > Syslog**.
2. Configure the following options:

*Table 269. Syslog parameters*

| Field                   | Description                                                                                                                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable syslog           | From the <b>Available Tables</b> list, you must select the following tables, and click <b>Add</b> . <ul style="list-style-type: none"><li>• <b>logUserService</b></li><li>• <b>logUserActivity</b></li><li>• <b>logUserAdminActivity</b></li></ul> |
| 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 <b>##</b> as the characters used to separate name-value pair entries in the syslog payload.                                                                                                                                                   |

3. Click **Update** to save the configuration.
4. Restart your IBM Security Access Manager for Enterprise Single Sign-On appliance.

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 Security 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 270. Syslog parameters*

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b>  | 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.                                                                                                                                                                                                                             |
| <b>Enabled</b>                | Select this check box to enable the log source.<br><br>By default, the check box is selected.                                                                                                                                                                                                                                                                                              |
| <b>Credibility</b>            | Select the <b>Credibility</b> of the log source. The range is 0 - 10.<br><br>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.                                                                                            |
| <b>Target Event Collector</b> | Select the <b>Event Collector</b> to use as the target for the log source.                                                                                                                                                                                                                                                                                                                 |
| <b>Coalescing Events</b>      | Select this check box to enable the log source to coalesce (bundle) events.<br><br>By default, automatically discovered log sources inherit the value of the <b>Coalescing Events</b> 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.          |
| <b>Incoming Event Payload</b> | From the <b>Incoming Event Payload</b> list, select the incoming payload encoder for parsing and storing the logs.                                                                                                                                                                                                                                                                         |
| <b>Store Event Payload</b>    | Select this check box to enable the log source to store event payload information.<br><br>By default, automatically discovered log sources inherit the value of the <b>Store Event Payload</b> 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**.

---

## IBM Security Access Manager for Mobile

The IBM Security 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 271. IBM Security Access Manager for Mobile DSM specifications*

| Specification | Value                                  |
|---------------|----------------------------------------|
| Manufacturer  | IBM                                    |
| DSM name      | IBM Security Access Manager for Mobile |

Table 271. IBM Security Access Manager for Mobile DSM specifications (continued)

| Specification               | Value                                                                                                                                                                                                                                                                     |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RPM file name               | DSM-IBMSecurityAccessManagerForMobile-7.x<br>-Qradar_version-Buildbuild_number.noarch.rpm                                                                                                                                                                                 |
| Supported versions          | IBM Security Access Manager for Mobile v8.0.0<br>IBM IDaaS v2.0                                                                                                                                                                                                           |
| Event Format                | Common Base Event Format<br>Log Event Extended Format (LEEF)                                                                                                                                                                                                              |
| Recorded event types        | IBM_SECURITY_AUTHN<br>IBM_SECURITY_TRUST<br>IBM_SECURITY_RUNTIME<br>IBM_SECURITY_CBA_AUDIT_MGMT<br>IBM_SECURITY_CBA_AUDIT RTE<br>IBM_SECURITY_RTSS_AUDIT_AUTHZ<br>IBM_SECURITY_SIGNING<br>CloudOE<br>Operations<br>Usage<br>IDaaS Appliance Audit<br>IDaaS Platform Audit |
| Automatically discovered?   | Yes                                                                                                                                                                                                                                                                       |
| Includes identity?          | No                                                                                                                                                                                                                                                                        |
| Includes custom properties? | No                                                                                                                                                                                                                                                                        |
| More information            | <a href="http://www.ibm.com/software">www.ibm.com/software</a> ( <a href="http://www-03.ibm.com/software/products/en/access-mgr-mobile">http://www-03.ibm.com/software/products/en/access-mgr-mobile</a> ).                                                               |

To integrate IBM Security Access Manager for Mobile with QRadar, complete the following steps:

- 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
- Configure your IBM Security Access Manager for Mobile device to send syslog events to QRadar.
- 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:

Table 272. 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 |

Table 272. IBM Security Access Manager for Mobile log source parameters (continued)

| Parameter              | Value                                                                                                                                          |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol Configuration | TLS Syslog                                                                                                                                     |
| Log Source Identifier  | 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. |
| TLS Listen Port        | Type the port number to accept incoming TLS Syslog Event.                                                                                      |

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 Security 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.

| Field                                    | Value                                                                                                                                                            |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable audit log                         | Click <b>Enable audit log</b> .                                                                                                                                  |
| Enable verbose audit events              | Click <b>Enable verbose audit events</b> .<br><br>Audit events that are not verbose do not contain the JSON payload, which contains details of user activity.    |
| Location of syslog server                | Select <b>On a remote server</b>                                                                                                                                 |
| Host                                     | The QRadar server host name or IP.                                                                                                                               |
| Port                                     | The port number that you want to use for QRadar to accept incoming TLS syslog events.                                                                            |
| Protocol                                 | Select <b>TLS</b>                                                                                                                                                |
| Certificate database (truststore)        | The truststore that validates the syslog server certificate.                                                                                                     |
| Enable client certificate authentication | Click <b>Enable client certificate authentication</b> .<br><br>The client can do client certificate authentication during the SSL handshake upon server request. |
| Certificate database (keystore)          | The keystore for client certificate authentication.                                                                                                              |
| Certificate label                        | The personal certificate for client certificate authentication                                                                                                   |
| Enable disk failover                     | Clear <b>Enable disk failover</b> .                                                                                                                              |

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:

| Property                             | Description                                           |
|--------------------------------------|-------------------------------------------------------|
| <b>audit.enabled=true</b>            | Audit property is enabled.                            |
| audit.syslog.message.format=leef     | Valid type is LEEF.                                   |
| audit.syslog.server=<IP_address>     |                                                       |
| audit.syslog.transport=TRANSPORT_UDP | Transport values are TRANSPORT_UDP and TRANSPORT_TLS. |
| audit.syslog.server.port=514         |                                                       |

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 IBM Security QRadar DSM for IBM Security Directory Server can collect event logs from your IBM Security Directory Server.

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

*Table 273. IBM Security Directory Server DSM specifications*

| Specification            | Value                                                                 |
|--------------------------|-----------------------------------------------------------------------|
| Manufacturer             | IBM                                                                   |
| DSM                      | IBM Security Directory Server                                         |
| RPM file name            | DSM-IBMSecurityDirectoryServer-build_number.noarch.rpm                |
| Supported version        | 6.3.1 and later                                                       |
| Protocol                 | Syslog (LEEF)                                                         |
| QRadar recorded events   | All relevant events                                                   |
| Automatically discovered | Yes                                                                   |
| Includes identity        | Yes                                                                   |
| For more information     | IBM website ( <a href="https://www.ibm.com">https://www.ibm.com</a> ) |

## IBM Security Directory Server integration process

You can integrate IBM Security Directory Server with IBM Security 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 an IBM Security Directory Server log source in IBM Security 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 Security 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 274. IBM Security Identity Governance (ISIG) DSM specifications*

| Specification               | Value                                                                    |
|-----------------------------|--------------------------------------------------------------------------|
| Manufacturer                | IBM                                                                      |
| DSM name                    | IBM Security Identity Governance                                         |
| RPM file name               | DSM-IBMSecurityIdentityGovernance-Qradar_version-build_number.noarch.rpm |
| Supported versions          | IBM Security Identity Governance v5.1.1                                  |
| Protocol                    | JDBC                                                                     |
| Event format                | NVP                                                                      |
| Recorded event types        | Audit                                                                    |
| Automatically discovered?   | No                                                                       |
| Includes identity?          | No                                                                       |
| Includes custom properties? | No                                                                       |
| More information            | IBM website ( <a href="http://www.ibm.com">http://www.ibm.com</a> )      |

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
  - JDBC Protocol 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 275. IBM Security Identity Governance DSM log source parameters

| Parameter               | Value                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Source type         | IBM Security Identity Governance                                                                                                                                                       |
| Protocol Configuration  | JDBC                                                                                                                                                                                   |
| Log Source Identifier   | DATABASE@HOSTNAME                                                                                                                                                                      |
| Database Type           | Select <b>Oracle</b> or <b>DB2</b> for the database that you want to use as the event source.                                                                                          |
| Database Name           | The name of the IBM Security Identity Governance database. It must be the same as the <i>DATABASE</i> name for the <b>Log Source Identifier</b> .                                      |
| IP or Hostname          | The IP address or host name of the IBM Security Governance database. It must be the same as the <i>HOSTNAME</i> of <b>Log Source Identifier</b> .                                      |
| Port                    | The port number that is used by the database server. The defaults are <b>Oracle: 1521</b> and <b>DB2: 50000</b> . The default that is displayed depends on the selected database type. |
| Username                | The database user name.                                                                                                                                                                |
| Password                | The database password.                                                                                                                                                                 |
| Predefined Query        | The default is <b>none</b> .                                                                                                                                                           |
| Table Name              | AUDIT_LOG                                                                                                                                                                              |
| Select List             | *                                                                                                                                                                                      |
| Compare Field           | ID                                                                                                                                                                                     |
| Use Prepared Statements | Enable the check box.                                                                                                                                                                  |
| Start Date and Time     | The initial date and time for database polling.                                                                                                                                        |
| Polling interval        | The amount of time, in seconds, between queries to the database table. The default polling interval is 10 seconds.                                                                     |
| EPS Throttle            | The number of events per second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.                                                                    |

#### Related tasks:

"Adding a DSM" on page 4

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

"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 Security 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 Security 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 276. IBM Security Identity Manager JDBC parameters

| Parameter                    | Description                                                                                                                                                                                                                                                                                                           |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the identifier for the log source. The log source identifier must be defined in the following format:<br><br>ITIMDB@<hostname><br><br>Where <hostname> is the IP address or host name for your IBM Security Identity Manager appliance.<br><br>The log source identifier must be unique for the log source type. |

*Table 276. IBM Security Identity Manager JDBC parameters (continued)*

| Parameter               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Database Type</b>    | <p>From the <b>Database Type</b> list, select a database to use for the event source.</p> <p>The options include the following databases:</p> <ul style="list-style-type: none"> <li>• DB2 - Select this option if DB2 is the database type on your IBM Security Identity Manager appliance. DB2 is the default database type.</li> <li>• MSDE - Select this option if MSDE is the database type on your IBM Security Identity Manager appliance.</li> <li>• Oracle - Select this option if Oracle is the database type on your IBM Security Identity Manager appliance.</li> </ul>                                                                                                                                        |
| <b>Database Name</b>    | <p>Type the name of the database to connect to. The default database name is <b>ITIMDB</b>.</p> <p>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(.)</p>                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>IP or Hostname</b>   | Type the IP address or host name of the IBM Security Identity Manager appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Port</b>             | <p>Type the port number that is used by the database server. The default that is displayed depends on the selected <b>Database Type</b>. The valid range is 0 - 65536. The default for DB2 is port 50000.</p> <p>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.</p> <p>The default port number for all options include:</p> <ul style="list-style-type: none"> <li>• DB2 - 50000</li> <li>• MSDE - 1433</li> <li>• Oracle - 1521</li> </ul> <p>If you define a database Instance when you use MSDE as the database type, you must leave the <b>Port</b> parameter blank in your configuration.</p> |
| <b>Username</b>         | Type the database user name. The user name can be up to 255 alphanumeric characters in length. The user name can also include underscores (_).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Password</b>         | <p>Type the database password.</p> <p>The password can be up to 255 characters in length.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Confirm Password</b> | Confirm the password to access the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Schema Name</b>      | Type ISIMUSER in the <b>Schema Name</b> field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Table Name</b>       | <p>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.</p> <p>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(.)</p>                                                                                                                                                                                                                                                             |

Table 276. IBM Security Identity Manager JDBC parameters (continued)

| Parameter                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select List                  | <p>Type * to include all fields from the table or view.</p> <p>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 <b>Compare Field</b> 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(.)</p> |
| Compare Field                | <p>Type TIMESTAMP to identify new events added between queries to the table by their time stamp.</p> <p>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(.)</p>                                                                                                                                                                                     |
| Start Date and Time          | <p>Optional. Configure the start date and time for database polling.</p> <p>The <b>Start Date and Time</b> 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.</p>                                                                                                                                                                         |
| Polling Interval             | <p>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.</p> <p>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.</p>                                                                                              |
| EPS Throttle                 | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.                                                                                                                                                                                                                                                                                                                                                                         |
| Authentication Domain        | <p>If you select <b>MSDE</b> as the <b>Database Type</b>, the <b>Authentication Domain</b> 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.</p> <p>The authentication domain must contain alphanumeric characters. The domain can include the following special characters: underscore (_), en dash (-), and period(.)</p>                                       |
| Database Instance            | <p>If you select <b>MSDE</b> as the <b>Database Type</b>, the <b>Database Instance</b> field is displayed.</p> <p>Type the instance to which you want to connect, if you have multiple SQL server instances on one server.</p> <p>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 <b>Database Instance</b> parameter blank in your configuration.</p>                                           |
| Use Named Pipe Communication | <p>If you select <b>MSDE</b> as the <b>Database Type</b>, the <b>Use Named Pipe Communication</b> check box is displayed. By default, this check box is clear.</p> <p>Select this check box to use an alternative method to a TCP/IP port connection.</p> <p>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.</p>    |

*Table 276. IBM Security Identity Manager JDBC parameters (continued)*

| Parameter                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Use NTLMv2</b>            | If you select <b>MSDE</b> as the <b>Database Type</b> , the <b>Use NTLMv2</b> check box is displayed. Select the <b>Use NTLMv2</b> 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 <b>Use NTLMv2</b> check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication. |
| <b>Database Cluster Name</b> | If you select the <b>Use Named Pipe Communication</b> check box, the <b>Database Cluster Name</b> 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.                                                                                                                                                                                                       |

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:

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

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

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

“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:

| Parameter                     | Description                                                                                                                                                                                      |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b>  | The IP address or host name for the log source as an identifier for events from your IBM Security Network IPS (GX) appliance.                                                                    |
| <b>Credibility</b>            | 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. |
| <b>Coalescing Events</b>      | Enables the log source to coalesce (bundle) events.                                                                                                                                              |
| <b>Incoming Event Payload</b> | The incoming payload encoder for parsing and storing the logs.                                                                                                                                   |

8. Click **Save**.

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

## 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 Security QRadar to record all relevant events.

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

*Table 277. IBM QRadar Network Security XGS specifications*

| Specification            | Value                                                                                                                                                                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manufacturer             | IBM                                                                                                                                                                                                                                                                                                |
| DSM                      | QRadar Network Security XGS                                                                                                                                                                                                                                                                        |
| RPM file name            | DSM-IBMQRadarNetworkSecurityXGS-QRadar_version-build_number.noarch,rpm                                                                                                                                                                                                                             |
| Supported versions       | v5.0 with fixpack 7 to v5.4                                                                                                                                                                                                                                                                        |
| Protocol                 | Syslog                                                                                                                                                                                                                                                                                             |
| Event format             | LEEF                                                                                                                                                                                                                                                                                               |
| QRadar recorded events   | All relevant system, access, and security events                                                                                                                                                                                                                                                   |
| Automatically discovered | Yes                                                                                                                                                                                                                                                                                                |
| Includes identity        | No                                                                                                                                                                                                                                                                                                 |
| More information         | IBM QRadar Network Security (XGS) Knowledge Center ( <a href="https://www.ibm.com/support/knowledgecenter/SSHLHV_5.4.0/com.ibm.alps.doc/alps_collateral/alps_dochome_stg.htm">https://www.ibm.com/support/knowledgecenter/SSHLHV_5.4.0/com.ibm.alps.doc/alps_collateral/alps_dochome_stg.htm</a> ) |

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 Security 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

1. Click **New > Alert > Remote Syslog**.
2. Select an existing remote syslog alert object, and then click **Edit**.
3. Configure the following options:

*Table 278. Syslog configuration parameters*

| Option                              | Description                                                                                                                                                                                                                                      |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                         | Type a name for the syslog alert configuration.                                                                                                                                                                                                  |
| <b>Remote Syslog Collector</b>      | Type the IP address of your QRadar Console or Event Collector.                                                                                                                                                                                   |
| <b>Remote Syslog Collector Port</b> | Type 514 for the <b>Remote Syslog Collector Port</b> .                                                                                                                                                                                           |
| <b>Remote LEEF Enabled</b>          | Select this check box to enable LEEF formatted events. This is a required field.<br><br>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. |
| <b>Comment</b>                      | Typing a comment for the syslog configuration is optional.                                                                                                                                                                                       |

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 Security 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 279. Syslog parameters*

| Parameter                    | Description                                                                                                                |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your IBM QRadar Network Security XGS. |

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

---

## IBM Security Privileged Identity Manager

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

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

*Table 280. IBM Security Privileged Identity Manager DSM specifications*

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

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

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

Table 281. IBM Security Privileged Identity Manager log source parameters

| Parameter               | Value                                                                                                                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Source type         | IBM Security Privileged Identity Manager                                                                                                                                                             |
| Protocol Configuration  | JDBC                                                                                                                                                                                                 |
| Log Source Identifier   | <DATABASE@HOSTNAME>                                                                                                                                                                                  |
| Database Type           | DB2                                                                                                                                                                                                  |
| Database Name           | Must match the value in the <b>Database name</b> field in IBM Security Privileged Identity Manager.                                                                                                  |
| IP or Hostname          | Must match the value in the <b>Hostname</b> field in IBM Security Privileged Identity Manager.                                                                                                       |
| Port                    | Must match the value in the <b>Port</b> field in IBM Security Privileged Identity Manager.                                                                                                           |
| Username                | Must match the value in the <b>Database administrator ID</b> field in IBM Security Privileged Identity Manager.                                                                                      |
| Predefined Query        | None                                                                                                                                                                                                 |
| Table Name              | <p>DB2ADMIN.V_PIM_AUDIT_EVENT</p> <p>Replace DB2ADMIN with the actual database schema name as identified in the Database Administrator ID parameter in IBM Security Privileged Identity Manager.</p> |
| Select List             | *                                                                                                                                                                                                    |
| Compare Field           | TIMESTAMP                                                                                                                                                                                            |
| Use Prepared Statements | Select this check box.                                                                                                                                                                               |
| Start Date and Time     | Initial date/time for the JDBC retrieval.                                                                                                                                                            |
| Polling Interval        | 10                                                                                                                                                                                                   |
| EPS Throttle            | 20000                                                                                                                                                                                                |

## Configuring IBM Security Privileged Identity Manager

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

### Before you begin

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

### Procedure

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

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

```

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

```

## What to do next

“Adding a log source” on page 4

---

## 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 Security 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 282. IBM Security Trusteer Apex Advanced Malware Protection DSM specifications*

| Specification      | Value                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------|
| Manufacturer       | IBM                                                                                                           |
| DSM name           | IBM Security Trusteer Apex Advanced Malware Protection                                                        |
| RPM file name      | DSM-TrusteerApex-QRadar_version-build_number.noarch.rpm                                                       |
| Supported versions | Syslog/LEEF event collection: Apex Local Manager 2.0.45<br>LEEF: ver_1303.1<br>Flat File Feed: v1, v3, and v4 |
| Protocol           | Syslog<br>Log File<br>TLS Syslog                                                                              |

Table 282. IBM Security Trusteer Apex Advanced Malware Protection DSM specifications (continued)

| Specification               | Value                                                                                                                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recorded event types        | Malware Detection<br>Exploit Detection<br>Data Exfiltration Detection<br>Lockdown for Java Event<br>File Inspection Event<br>Apex Stopped Event<br>Apex Uninstalled Event<br>Policy Changed Event<br>ASLR Violation Event<br>ASLR Enforcement Event<br>Password Protection Event |
| Automatically discovered?   | Yes                                                                                                                                                                                                                                                                              |
| Includes identity?          | No                                                                                                                                                                                                                                                                               |
| Includes custom properties? | No                                                                                                                                                                                                                                                                               |
| More information            | IBM Security Trusteer Apex Advanced Malware Protection website ( <a href="http://www-03.ibm.com/software/products/en/trusteer-apex-adv-malware">http://www-03.ibm.com/software/products/en/trusteer-apex-adv-malware</a> )                                                       |

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 504.
  - 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 504
  - 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 506.
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 283. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Syslog protocol*

| Parameter                     | Value                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source type</b>        | IBM Security Trusteer Apex Advanced Malware Protection                                                                                             |
| <b>Protocol Configuration</b> | <b>Syslog</b>                                                                                                                                      |
| <b>Log Source Identifier</b>  | 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. |

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

*Table 284. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for TLS Syslog protocol*

| Parameter                               | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Type</b>                  | IBM Security Trusteer Apex Advanced Malware Protection                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Protocol Configuration</b>           | <b>TLS Syslog</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Log Source Identifier</b>            | 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.                                                                                                                                                                                                                                                                                                                                                         |
| <b>TLS Listen Port</b>                  | The default port is 6514.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Authentication Mode</b>              | TLS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Certificate Type</b>                 | Select the <b>Provide Certificate</b> option from the list.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Maximum Connections</b>              | 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.<br><b>Note:</b> 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. |
| <b>TLS Protocols</b>                    | Select the version of TLS installed on the client from the drop down list.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Provided Server Certificate Path</b> | Absolute path of server certificate. For example, /opt/qradar/conf/trusted_certificates/apex-alm-tls.cert                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Provided Private Key Path</b>        | Absolute path of PKCS#8 private key. For example, /etc/pki/tls/private/apex-alm-tls.pk8                                                                                                                                                                                                                                                                                                                                                                                                                   |

**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 285. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Log File Protocol*

| Parameter                     | Value                                                  |
|-------------------------------|--------------------------------------------------------|
| <b>Log Source Type</b>        | IBM Security Trusteer Apex Advanced Malware Protection |
| <b>Protocol Configuration</b> | <b>Log File</b>                                        |

*Table 285. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Log File Protocol (continued)*

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

#### Related concepts:

"Configuring IBM Security Trusteer Apex Advanced Malware Protection to send TLS Syslog events to QRadar" on page 504

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 Security QRadar.

#### Related tasks:

"Adding a DSM" on page 4

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

"Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar" on page 504

You can configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to IBM Security QRadar.

"Configuring a Flat File Feed service" on page 506

For IBM Security 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.

"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 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 Security QRadar.

### Before you begin

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

For more information about configuring your IBM Security Trusteer Apex Advanced Malware Protection to communicate with QRadar, 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 Security 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:  

```
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
```
3. Convert the private key to the required DER encode PKCS#8 format:

```
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.

**Note:** 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,

```
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:

```
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 286. Apex Local Manager SIEM/Syslog server setting parameters

| Parameter           | Description                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------------------|
| Type                | IBM Security Q-Radar SIEM (LEEF)                                                                                    |
| Hostname            | <fqdn of the Qradar appliance>                                                                                      |
| Port                | Default is 6514.                                                                                                    |
| Protocol            | TCP with SSL/TLS                                                                                                    |
| PKCS#12 Upload File | Upload the local PKCS#12 file                                                                                       |
| Encryption Password | The password that was entered during the creation of the client authentication certificates for Apex Local Manager. |

*Table 286. Apex Local Manager SIEM/Syslog server setting parameters (continued)*

| Parameter                         | Description                                                   |
|-----------------------------------|---------------------------------------------------------------|
| <b>CA Certificate Upload File</b> | Upload local certificate file. For example, apex-alm-tls.cert |

7. Click **Next**.
8. From the System Events Setting page, provide a value for the following parameters:

*Table 287. System events setting parameters*

| Parameter                         | Description                                                                                                         |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Hostname</b>                   | <QRadar FQDN or IP Address>                                                                                         |
| <b>Port</b>                       | Default is 6514                                                                                                     |
| <b>Protocol</b>                   | <b>Syslog with SSL/TLS</b>                                                                                          |
| <b>PKCS#12 Upload File</b>        | Upload the local PKCS#12 file. For example, alm-client-syslog.tls.p12                                               |
| <b>Encryption Password</b>        | The password that was entered during the creation of the client authentication certificates for Apex Local Manager. |
| <b>CA Certificate Upload File</b> | Upload local certificate file. For example, apex-alm-tls.cert                                                       |

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””

### 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 Security 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 Security 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.

- From the `syslog.event_targets` section, add the following information:

```
{
 host": "<QRadar IP address>", "port": "514", "proto": "tcp"
}
```

- Save the configuration file.

- From the navigation menu, select **Configuration**.

- Click **Choose file** and select the new configuration file that contains the event target IP address.

- 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 Security 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 288. IBM Sense DSM specifications*

| Specification               | Value                                                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Manufacturer                | IBM                                                                                                                          |
| DSM name                    | IBM Sense                                                                                                                    |
| RPM file name               | DSM-IBMSense-Qradar_version-build_number.noarch.rpm                                                                          |
| Supported versions          | 1                                                                                                                            |
| Protocol                    | Syslog                                                                                                                       |
| Event format                | LEEF                                                                                                                         |
| Recorded event types        | User Behavior<br>User Geography<br>User Time<br>User Access<br>User Privilege<br>User Risk<br>Sense Offense<br>Resource Risk |
| Automatically discovered?   | Yes                                                                                                                          |
| Includes identity?          | No                                                                                                                           |
| Includes custom properties? | No                                                                                                                           |
| More information            | IBM website ( <a href="http://www.ibm.com">http://www.ibm.com</a> )                                                          |

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 289. IBM Sense sample message.*

| Event name      | Low level category | Sample log message                                                                                                                                                                                                                                                                                                                               |
|-----------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behavior Change | User Behavior      | LEEF:2.0 IBM Sense 1.0 Behavior<br>Change cat=User Behavior description= score=<br>scoreType= confidence= primaryEntity=<br>primaryEntityType= additionalEntity=<br>additionalEntityType= beginningTimestamp=<br>endTimestamp= sensorDomain= referenceId1=<br>referenceId2= referenceId3= referenceId4=<br>referenceURL= originalSenseEventName= |

**Related tasks:**

“Adding a DSM” on page 4

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

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

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

*Table 290. IBM SmartCloud Orchestrator specifications*

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

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

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

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

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

#### Related tasks:

“Adding a DSM” on page 4

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

“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 Security QRadar

### Procedure

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

## Configuring an IBM SmartCloud Orchestrator log source in QRadar

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

### Procedure

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

| Option         | Description                                                   |
|----------------|---------------------------------------------------------------|
| IP or Hostname | The IP address or server name of the SmartCloud Orchestrator. |

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

## IBM Tivoli Access Manager for e-business

The IBM Tivoli Access Manager for e-business DSM for IBM Security 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 Tivoli Access Manager WebSEAL overview ([http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1359-00/en\\_US/HTML/am51\\_webseal\\_guide10.htm#j1031993](http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1359-00/en_US/HTML/am51_webseal_guide10.htm#j1031993)).

## Configure Tivoli Access Manager for e-business

You can configure syslog on your Tivoli Access Manager for e-business to forward events.

### 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.
- 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=%P|request-method=%m|response-status=%s|url=%U|bytes=%b|remote-host=%h|request=%r
  - Click **Submit**.

The **Deploy** button is displayed in the navigation menu.

- From the navigation menu, click **Deploy**.

- Click **Deploy**.

You must restart the reverse proxy instance to continue.

- From the **Instance** column, select your instance configuration.

- 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 Security 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

- 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 **IBM Tivoli Access Manager for e-business**.
- From the **Protocol Configuration** list, select **Syslog**.
- Configure the following values:

*Table 291. IBM Tivoli Access Manager for e-business syslog configuration*

| Parameter                    | Description                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for your IBM Tivoli Access Manager for e-business appliance.<br><br>The IP address or host name identifies your IBM Tivoli Access Manager for e-business as a unique event source in QRadar. |

- Click **Save**.
- 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 429](#)

The IBM BigFix DSM for IBM Security QRadar accepts system events in Log Extended Event Format (LEEF) retrieved from IBM BigFix.

---

## IBM WebSphere Application Server

The IBM WebSphere® Application Server DSM for IBM Security 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 Security 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” 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 Security QRadar using the log file protocol.

## Creating a log source

The log file protocol allows IBM Security 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 292. Log file parameters*

| Parameter                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | 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.<br><br>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. |
| <b>Service Type</b>          | From the list, select the protocol that you want to use when retrieving log files from a remove server. The default is SFTP. <ul style="list-style-type: none"> <li>• <b>SFTP - SSH File Transfer Protocol</b></li> <li>• <b>FTP - File Transfer Protocol</b></li> <li>• <b>SCP - Secure Copy</b></li> </ul> The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server specified in the <b>Remote IP or Hostname</b> field has the SFTP subsystem enabled.                                                      |

Table 292. Log file parameters (continued)

| Parameter                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote IP or Hostname</b> | Type the IP address or host name of your IBM WebSphere Application Server storing your event log files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Remote Port</b>           | <p>Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535.</p> <p>The options include FTP ports:</p> <ul style="list-style-type: none"> <li>• <b>FTP</b> - TCP Port 21</li> <li>• <b>SFTP</b> - TCP Port 22</li> <li>• <b>SCP</b> - TCP Port 22</li> </ul> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                        |
| <b>Remote User</b>           | <p>Type the user name necessary to log in to the host that contains your event files.</p> <p>The user name can be up to 255 characters in length.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Remote Password</b>       | Type the password necessary to log in to the host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Confirm Password</b>      | Confirm the password necessary to log in to the host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>SSH Key File</b>          | <p>If you select <b>SCP</b> or <b>SFTP</b> as the <b>Service Type</b>, this parameter allows for the definition of an SSH private key file.</p> <p>The <b>Remote Password</b> field is ignored when you provide an SSH Key File.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Remote Directory</b>      | <p>Type the directory location on the remote host to the cell and file path you specified in "Configuring IBM WebSphere" on page 513. This is the directory that you created containing your IBM WebSphere Application Server event files.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                 |
| <b>Recursive</b>             | <p>Select this check box if you want the file pattern to search sub folders. By default, the check box is clear.</p> <p>The <b>Recursive</b> option is ignored if you configure <b>SCP</b> as the <b>Service Type</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>FTP File Pattern</b>      | <p>If you select <b>SFTP</b> or <b>FTP</b> as the <b>Service Type</b>, this option allows for the configuration of the regular expression (regex) to filter the list of files that are specified in the <b>Remote Directory</b>. All matching files are included in the processing.</p> <p>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 513. For example, to collect system logs, type the following code:</p> <pre>System.*\.log</pre> <p>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></p> |

Table 292. Log file parameters (continued)

| Parameter                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FTP Transfer Mode</b>                   | <p>This option appears only if you select <b>FTP</b> as the <b>Service Type</b>. The <b>FTP Transfer Mode</b> parameter allows for the definition of the file transfer mode when log files are retrieved over FTP.</p> <p>From the list, select the transfer mode that you want to apply to this log source:</p> <ul style="list-style-type: none"> <li>• <b>Binary</b> - Select <b>Binary</b> for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files.</li> <li>• <b>ASCII</b> - Select <b>ASCII</b> for log sources that require an ASCII FTP file transfer.</li> </ul> <p>You must select <b>None</b> for the <b>Processor</b> parameter and <b>LINEBYLINE</b> the <b>Event Generator</b> parameter when you use <b>ASCII</b> as the <b>FTP Transfer Mode</b>.</p> |
| <b>SCP Remote File</b>                     | If you select <b>SCP</b> as the <b>Service Type</b> you must type the file name of the remote file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Start Time</b>                          | Type the time of day you want the processing to begin. This parameter functions with the <b>Recurrence</b> value to establish when and how often the <b>Remote Directory</b> is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Recurrence</b>                          | <p>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.</p> <p>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.</p>                                                                                                                                                                                                                           |
| <b>Run On Save</b>                         | <p>Select this check box if you want the log file protocol to run immediately after you click <b>Save</b>. After the <b>Run On Save</b> completes, the log file protocol follows your configured start time and recurrence schedule.</p> <p>Selecting <b>Run On Save</b> clears the list of previously processed files for the <b>Ignore Previously Processed File(s)</b> parameter.</p>                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>EPS Throttle</b>                        | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Processor</b>                           | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Ignore Previously Processed File(s)</b> | <p>Select this check box to track files that are processed. Files that are previously processed are not processed a second time.</p> <p>This check box applies only to <b>FTP</b> and <b>SFTP</b> Service Types.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Change Local Directory?</b>             | 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 <b>Local Directory</b> field is displayed, which gives the option of configuring the local directory to use for storing files.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Event Generator</b>                     | <p>From the <b>Event Generator</b> list, select <b>WebSphere Application Server</b>.</p> <p>The Event Generator applies more processing, which is specific to retrieved event files for IBM WebSphere Application Server events.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

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" on page 441](#)

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

---

## 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 Security 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](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](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](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](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.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (<http://www-01.ibm.com/support/docview.wss?uid=pub1sc27277200>).

#### Related tasks:

["Adding a DSM" on page 4](#)

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

["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 Security 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 293. Log source parameters*

| Parameter              | Value                                        |
|------------------------|----------------------------------------------|
| Log Source type        | Select your DSM name from the list.          |
| Protocol Configuration | Syslog                                       |
| Log Source Identifier  | Type a unique identifier for the log source. |

## Creating a log source for Log File protocol

The Log File protocol enables IBM Security 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 294. Log File protocol parameters*

| Parameter                    | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | 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.<br><br>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. |
| <b>Service Type</b>          | From the <b>Service Type</b> list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. <ul style="list-style-type: none"> <li>• SFTP - SSH File Transfer Protocol</li> <li>• FTP - File Transfer Protocol</li> <li>• SCP - Secure Copy</li> </ul> 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 <b>Remote IP or Hostname</b> field has the SFTP subsystem enabled.                                                                                  |
| <b>Remote IP or Hostname</b> | Type the IP address or host name of the device that stores your event log files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Remote Port</b>           | Type the TCP port on the remote host that is running the selected <b>Service Type</b> . The valid range is 1 - 65535.<br><br>The options include ports: <ul style="list-style-type: none"> <li>• FTP - TCP Port 21</li> <li>• SFTP - TCP Port 22</li> <li>• SCP - TCP Port 22</li> </ul> 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.                                                                                                                                                                                           |
| <b>Remote User</b>           | Type the user name or user ID necessary to log in to the system that contains your event files. <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>                                                                                                                           |

Table 294. Log File protocol parameters (continued)

| Parameter                | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote Password</b>   | Type the password necessary to log in to the host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Confirm Password</b>  | Confirm the password necessary to log in to the host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>SSH Key File</b>      | If you select <b>SCP</b> or <b>SFTP</b> as the <b>Service Type</b> , this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the <b>Remote Password</b> field is ignored.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Remote Directory</b>  | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Recursive</b>         | 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.<br><br>If you configure SCP as the Service Type, the Recursive option is ignored.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>FTP File Pattern</b>  | If you select <b>SFTP</b> or <b>FTP</b> as the <b>Service Type</b> , you can configure the regular expression (regex) needed to filter the list of files that are specified in the <b>Remote Directory</b> . All matching files are included in the processing.<br><br>The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <product_name>.<timestamp>.gz<br><br>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:<br><br>zOS.*\.gz<br><br>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> ) |
| <b>FTP Transfer Mode</b> | This option displays only if you select <b>FTP</b> as the <b>Service Type</b> . From the list, select <b>Binary</b> .<br><br>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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>SCP Remote File</b>   | If you select <b>SCP</b> as the <b>Service Type</b> you must type the file name of the remote file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Start Time</b>        | 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.<br><br>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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Recurrence</b>        | 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).<br><br>For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Run On Save</b>       | If you want the Log File protocol to run immediately after you click <b>Save</b> , select this check box.<br><br>After the <b>Run On Save</b> completes, the Log File protocol follows your configured start time and recurrence schedule.<br><br>Selecting <b>Run On Save</b> clears the list of previously processed files for the Ignore Previously Processed File parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 294. Log File protocol parameters (continued)

| Parameter                                  | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>EPS Throttle</b>                        | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Processor</b>                           | From the list, select <b>gzip</b> .<br><br>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 <b>zip</b> , <b>gzip</b> , <b>tar</b> , or <b>tar+gzip</b> archive format.                                                                                                                                                                                  |
| <b>Ignore Previously Processed File(s)</b> | Select this check box to track and ignore files that are already processed by the Log File protocol.<br><br>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.<br><br>This option applies only to FTP and SFTP service types. |
| <b>Change Local Directory?</b>             | Select this check box to define a local directory on your QRadar for storing downloaded files during processing.<br><br>It is suggested that you leave this check box clear. When this check box is selected, the <b>Local Directory</b> field is displayed, which gives you the option to configure the local directory to use for storing files.                                                                                                                                      |
| <b>Event Generator</b>                     | From the <b>Event Generator</b> list, select <b>LineByLine</b> .<br><br>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.                                                                                                                                                                                                                             |

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](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 Security 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 295. Syslog parameters*

| Parameter                    | Description                                                                                                  |
|------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your IBM zSecure Alert. |

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

The configuration is complete.

---

## 73 ISC Bind

You can integrate an Internet System Consortium (ISC) BIND device with IBM Security 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;
 };
 category queries {
 QRadar;
 };
 category notify {
```

```
QRadar;
};

category network {
QRadar;
};

category client {
QRadar;
};
};
```

3. Save and exit the file.
4. Edit the syslog configuration to log to your QRadar using the facility you selected in 73, "ISC Bind," on page 523:

```
<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 Security 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 296. Syslog protocol parameters*

| Parameter                    | Description                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your ISC BIND appliance. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.



---

## 74 Illumio Adaptive Security Platform

The IBM Security 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 297. Illumio Adaptive Security Platform DSM specifications*

| Specification               | Value                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Manufacturer                | Illumio                                                                                                               |
| DSM name                    | Illumio Adaptive Security Platform                                                                                    |
| RPM file name               | DSM-IllumioAdaptiveSecurityPlatform-QRadar_version-build_number.noarch.rpm                                            |
| Supported versions          | N/A                                                                                                                   |
| Protocol                    | Syslog                                                                                                                |
| Event format                | Log Event Extended Format (LEEF)                                                                                      |
| Recorded event types        | Audit<br>Traffic                                                                                                      |
| Automatically discovered?   | Yes                                                                                                                   |
| Includes identity?          | No                                                                                                                    |
| Includes custom properties? | No                                                                                                                    |
| More information            | <a href="https://www.illumio.com">Illumio website (<a href="https://www.illumio.com">https://www.illumio.com</a>)</a> |

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 298. Illumio Adaptive Security Platform log source parameters*

| Parameter              | Value                                   |
|------------------------|-----------------------------------------|
| Log Source type        | Illumio Adaptive Security Platform      |
| Protocol Configuration | Syslog                                  |
| Log Source Identifier  | A unique identifier for the log source. |

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:

Table 299. Illumio Adaptive Security Platform sample message

| Event name   | Low level category | Sample log message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| flow_allowed | Firewall Permit    | <14>1 2016-08-08T22:18:24.000+00:00<br>hostname1<br>illumio_pce/collector 5458 --<br>sec=694704.253 sev=INFO pid=5458<br>tid=14554040 rid=0 LEEF:2.0 Illumio<br> PCE 16.6.0 flow_allowed cat=flow<br>_summary devTime=2016-08-08T15<br>:20:55-07:00 devTimeFormat=<br>yyyy-MM-dd'T'HH:mm:ssX<br>proto=udp sev=1<br>src=<Source_IP_address> dst=<Destin<br>ation_IP_address> dstPort=14000<br>srcBytes=0 dstBytes=15936<br>count=1 dir=I hostname=<br>hostname2 intervalSec=3180<br>state=T workloadUUID=xxxxxxxx-xxxx<br>-xxxx-xxxx-xxxxxxxxxxxx |

#### Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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”

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 529

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 \
and $syslogtag startswith 'illumio_pce/collector[' \
and $msg contains 'LEEF:' \
and $msg contains '|Illumio|PCE|' \
and $msg contains 'cat=flow_summary' \
then @@<QRadar Event Collector IP>:514

if $syslogseverity <= 6 \
and $syslogtag startswith 'illumio_pce/' \
and $msg contains 'LEEF:' \
and $msg contains '|Illumio|PCE|' \
and $msg contains 'audit_events' \
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:[^T]+\\|Illumio\\|PCE\\|')
 and message('cat=flow_summary');
};

filter audit_events {
 level(info..emerg)
 and program("^illumio_pce/")
 and message('LEEF:[^T]+\\|Illumio\\|PCE\\|')
 and message('cat=[^ #]*audit_events');
};
```
  - b. Restart the syslog-ng service.

```
service syslog-nginx restart
```

---

## 75 Imperva Incapsula

The IBM Security QRadar DSM for Imperva Incapsula collects logs from an Imperva Incapsula service.

The following table describes the specifications for the Imperva Incapsula DSM:

*Table 300. Imperva Incapsula DSM specifications*

| Specification               | Value                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------------|
| Manufacturer                | Imperva                                                                                           |
| DSM name                    | Imperva Incapsula                                                                                 |
| RPM file name               | DSM-ImpervaIncapsula-QRadar_version-build_number.noarch.rpm                                       |
| Supported versions          | N/A                                                                                               |
| Protocol                    | Syslog                                                                                            |
| Event format                | LEEF                                                                                              |
| Recorded event types        | Access events and Security alerts                                                                 |
| Automatically discovered?   | Yes                                                                                               |
| Includes identity?          | No                                                                                                |
| Includes custom properties? | No                                                                                                |
| More information            | Imperva Incapsula website ( <a href="https://www.incapsula.com/">https://www.incapsula.com/</a> ) |

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 301. Imperva Incapsula log source parameters*

| Parameter              | Value             |
|------------------------|-------------------|
| Log Source type        | Imperva Incapsula |
| Protocol Configuration | Syslog            |

4. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Imperva Incapsula:

Table 302. Imperva Incapsula sample message

| Event name | Low level category | Sample log message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ_PASSED | Information        | <pre> LEEF:1.0  Incapsula  SIEMintegration  1.0 Normal  fileId=fid sourceServiceName =ssname siteid=siteid suid=suid requestClientAppl ication=reqcliapp cs2=true cs2Label=Javascri pt Support cs3=true cs3Label=C0 Support src=&lt;Source_IP_address&gt; cs1=NA cs1Label=Cap Support cs5Label=clappsig dproc=Browser cs6=Internet Explorer cs6Label=clapp calCountryOrRegion=[XX] cs7=xx.xx cs7Label=latitude cs8=xx.xx cs8Label=longitude Customer=customer start=start requestMethod=GET cn1=200 proto=HTTP cat=REQ_PASSED </pre> |

#### Related tasks:

“Adding a DSM” on page 4

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

“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 following dependencies might require additional modules, depending on your operating system:
  - M2Crypto
  - loggerglue

- crypto.cipher
- To collect log events, run the script.
    - 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>).
    - Configure the parameter values for the Settings.Config configuration file.

*Table 303. Parameter values for the Settings.Config configuration file*

| Parameter          | Value                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APIID              | Your API ID.                                                                                                                                                              |
| APIKEY             | Your API key.                                                                                                                                                             |
| SAVE_LOCALLY       | 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.<br><br>The default is YES.  |
| PROCESS_DIR        | The directory where Incapsula automatically saves the logs after extracting them.<br><br>The default is /tmp/processed/                                                   |
| BASEURL            | The URL of your logs repository in the Incapsula cloud. This URL is displayed in the Incapsula Administration Console Settings window as the <b>Log Server URL</b> field. |
| USEPROXY           | Specify YES to use a proxy to download the files.<br><br>The default is NO.                                                                                               |
| PROXYSERVER        | If you choose to use a proxy server, when you type the proxy URL, use the < <a href="https://192.0.2.1:8080">https://192.0.2.1:8080</a> > format.                         |
| SYSLOG_ENABLE      | Type YES.<br><br>A Yes or No value that instructs Incapsula about whether to send the files by using syslog.<br><br>The default is YES.                                   |
| SYSLOG_ADDRESS     | The IP address for QRadar                                                                                                                                                 |
| SYSLOG_PORT        | 514                                                                                                                                                                       |
| USE_CUSTOM_CA_FILE | In case the service's certificate is not in the bundle, the default is NO.                                                                                                |
| CUSTOM_CA_FILE     | The file path for the custom certificate file.                                                                                                                            |

- 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 304. LogsDownloader.py parameter values*

| Parameter               | Value                                            |
|-------------------------|--------------------------------------------------|
| <path_to_config_folder> | The default is<br><br>/etc/incapsula/logs/config |

Table 304. LogsDownloader.py parameter values (continued)

| Parameter                    | Value                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <path_to_system_logs_folder> | The <path_to_system_logs_folder> is the folder where the LogsDownloader.py script output log file is stored. This parameter does not refer to your Incapsula logs.<br>The default is /var/log/incapsula/logsDownloader/ |
| <system_logs_level>          | The logging level for the script output log. Supported values are info, debug, and error.<br>The default value is info.                                                                                                 |

**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.

---

## 76 Imperva SecureSphere

The IBM Security 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 305. Imperva SecureSphere DSM*

| Specification               | Value                                                                           |
|-----------------------------|---------------------------------------------------------------------------------|
| Manufacturer                | Imperva                                                                         |
| DSM name                    | SecureSphere                                                                    |
| RPM file name               | DSM-ImpervaSecuresphere-QRadar-version-Build_number.noarch.rpm                  |
| Supported versions          | v6.2 and v7.x Release Enterprise Edition (syslog)<br>v9.5 to v11.5 (LEEF)       |
| Event format                | syslog<br>LEEF                                                                  |
| QRadar recorded event types | Firewall policy events                                                          |
| Automatically discovered?   | Yes                                                                             |
| Includes identity?          | Yes                                                                             |
| Includes custom properties? | No                                                                              |
| More information            | Imperva website ( <a href="http://www.imperva.com">http://www.imperva.com</a> ) |

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 306. Imperva SecureSphere log source parameters*

| Parameter              | Description          |
|------------------------|----------------------|
| Log Source Type        | Imperva SecureSphere |
| Protocol Configuration | Syslog               |

### Related tasks:

[“Configuring an alert action for Imperva SecureSphere” on page 536](#)

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 537](#)

Configure your Imperva SecureSphere appliance to forward syslog system policy events to QRadar.

“Configuring Imperva SecureSphere V11.0 to send database audit records to QRadar” on page 539  
To send database audit records from Imperva SecureSphere V11.0 to IBM Security QRadar, create a custom action set, add an action interface, and then configure an audit policy.

“Adding a DSM” on page 4

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

“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” on page 537

Configure your Imperva SecureSphere appliance to forward syslog system policy events to 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.

---

## 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 to v11.5)

```
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 Description=${Alert.description}|
Severity=${Alert.severity}|Immediate Action=${Alert.immediateAction}|
SecureSphere Version=${SecureSphereVersion}
```

#### File server alerts (v9.5 to v11.5)

```
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=${Event.destInfo.serverIp}|
Alert Description=${Alert.description}|Severity=${Alert.severity}|
Immediate Action=${Alert.immediateAction} |SecureSphere
Version=${SecureSphereVersion}
```

#### Web application firewall alerts (v9.5 to v11.5)

```
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=${Alert.description}|
Severity=${Alert.severity}|Simulation Mode=${Alert.simulationMode}|
Immediate Action=${Alert.immediateAction}
```

#### All alerts (v6.2 and v7.x 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 to v11.5)

```
L0EF: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 to v11.5)

```
L0EF: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.user.user}|User Group=${Event.struct.userGroup}
|Authenticated=${Event.struct.user.authenticated}|App User=$
{Event.struct.applicationUser}|src=${Event.sourceInfo.sourceIp}
|Application=${Event.struct.application.application}|OS User=
${Event.struct.osUser.osUser}|Host=${Event.struct.host.host}
|Service Type=${Event.struct.serviceType}|dst=$
{Event.destInfo.serverIp}|Event Type=${Event.struct.eventType}
|Operation=${Event.struct.operations.name}|Operation type=
${Event.struct.operations.operationType}|Object name=$
{Event.struct.operations.objects.name}|Object type=$
{Event.struct.operations.objectType}|Subject=
${Event.struct.operations.subjects.name}|Database=$
{Event.struct.databases.databaseName}|Schema=
${Event.struct.databases.schemaName}|Table Group=$
{Event.struct.tableGroups.displayName}|Sensitive=
${Event.struct.tableGroups.sensitive}|Privileged=$
{Event.struct.operations.privileged}|Stored Proc=$
{Event.struct.operations.storedProcedure}|Completed Successfully
= ${Event.struct.complete.completeSuccessful}|Parsed Query=$
{Event.struct.query.parsedQuery}|Bind Variables=$
{Event.struct.rawQuery.bindVariables}|Error=$
{Event.struct.complete.errorValue}|Response Size=$
{Event.struct.complete.responseSize}|Response Time=$
{Event.struct.complete.responseTime}|Affected Rows=
${Event.struct.query.affectedRows}| devTimeFormat=[see note]
|devTime=${Event.createTime}
```

## All alerts (v6.2 and v7.x Release Enterprise Edition)

```
DeviceType=ImpervaSecuresphere Event|et=$!{Event.eventType}
|dc=Securesphere System Event|sp=$!{Event.sourceInfo.sourcePort}
|s=$!{Event.sourceInfo.sourceIp}|d=$!{Event.destInfo.serverIp}
|dp=$!{Event.destInfo.serverPort}|u=$!{Event.username}|t=$!
{Event.createTime}|sev=$!{Event.severity}|m=$!{Event.message}
```

**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 send database audit records to QRadar

To send database audit records from Imperva SecureSphere V11.0 to IBM Security 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:

| Parameter        | Value                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------|
| Name             | Type the name that you created for the action set. For example, <b>QRadar SIEM</b> .            |
| Protocol         | Select <b>UDP</b> .                                                                             |
| Host             | Type the IP address or the host name of the QRadar appliance for which you want to send events. |
| Port             | 514                                                                                             |
| Syslog Log Level | Info                                                                                            |
| Facility         | syslog                                                                                          |

| Parameter | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message   | <p><b>Attention:</b> 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 <b>Message</b> field.</p> <pre>L3EF: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}</pre> |

- a. Select the **Run on Every Event** check box.
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.

---

## 77 Infoblox NIOS

The Infoblox NIOS DSM for IBM Security QRadar accepts events by using syslog, which enables QRadar to record all relevant events from an Infoblox NIOS device.

**Note:** If you send Infoblox NIOS syslog events to QRadar without first creating an Infoblox NIOS log source, the following log sources are automatically discovered:

- ISC Bind
- Linux DHCP
- Linux Server
- Apache

To avoid creating extra log sources, manually create the Infoblox NIOS log source before you configure your Infoblox NIOS device to send syslog events to QRadar. For more information on configuring logs on your Infoblox NIOS device, see your *Infoblox NIOS* vendor documentation.

The following table identifies the specifications for the Infoblox NIOS DSM:

Infoblox NIOS DSM specifications

| Specification          | Value                                                                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Manufacturer           | Infoblox                                                                                                                                            |
| DSM                    | NIOS                                                                                                                                                |
| Version                | v6.x                                                                                                                                                |
| Events accepted        | Syslog                                                                                                                                              |
| QRadar recorded events | <ul style="list-style-type: none"><li>• ISC Bind events</li><li>• Linux DHCP events</li><li>• Linux Server events</li><li>• Apache events</li></ul> |
| Option in QRadar       | Infoblox NIOS                                                                                                                                       |
| Auto discovered        | No                                                                                                                                                  |
| Includes identity      | Yes                                                                                                                                                 |
| For more information   | <a href="http://www.infoblox.com">http://www.infoblox.com</a>                                                                                       |

---

## Configuring a log source

IBM Security QRadar does not automatically discover or create log sources for syslog events from Infoblox NIOS appliances. To integrate Infoblox NIOS appliances with QRadar, you must manually create a log source to receive Infoblox NIOS 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 **Infoblox NIOS**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the remaining parameters.
11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

---

## 78 iT-CUBE agileSI

The iT-CUBE agileSI DSM for IBM Security 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 Security 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.

For example, `http://<sap-system-url:port>/sap/bc/webdynpro/itcube/ ccf?sap-client=<client>&sap-language=EN`

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."

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 Security 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 307. SMB Tail protocol parameters*

| Parameter                    | Description                                                                                                                                                                                            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address, host name, or name for the log source as an identifier for your <i>iT-CUBE</i> agileSI events.                                                                                    |
| <b>Server Address</b>        | Type the IP address of your <i>iT-CUBE</i> agileSI server.                                                                                                                                             |
| <b>Domain</b>                | Type the domain for your <i>iT-CUBE</i> agileSI server.<br>This parameter is optional if your server is not in a domain.                                                                               |
| <b>Username</b>              | Type the user name that is required to access your <i>iT-CUBE</i> agileSI server.<br>The user name and password you specify must be able to read to the LEEFYYYYDDMM.txt file for your agileSI events. |
| <b>Password</b>              | Type the password that is required to access your <i>iT-CUBE</i> agileSI server.                                                                                                                       |
| <b>Confirm Password</b>      | Confirm the password that is required to access your <i>iT-CUBE</i> agileSI server.                                                                                                                    |

Table 307. SMB Tail protocol parameters (continued)

| Parameter                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Folder Path</b>               | Type the directory path to access the LEEFYYYYDDMM.txt file.<br><br>Parameters that support file paths gives 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.<br><br>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 required to read the log files. Local or domain administrators have sufficient privileges to access log files that are on administrative shares. |
| <b>File Pattern</b>                  | Type the regular expression (regex) required to filter the file names. All matching files are included for processing when QRadar polls for events.<br><br>For example, if you want to list all files that end with txt, use the following entry: .*\.txt. 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>                                                                                                                    |
| <b>Force File Read</b>               | Select this check box to force the protocol to read the log file. By default, the check box is selected.<br><br>If the check box is clear the event file is read when QRadar detects a change in the modified time or file size.                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Recursive</b>                     | Select this check box if you want the file pattern to search sub folders. By default, the check box is selected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Polling Interval (in seconds)</b> | Type the polling interval, which is the number of seconds between queries to the event file to check for new data.<br><br>The minimum polling interval is 10 seconds, with a maximum polling interval of 3,600 seconds. The default is 10 seconds.                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Throttle Events/Sec</b>           | Type the maximum number of events the SMB Tail protocol forwards per second.<br><br>The minimum value is 100 EPS and the maximum is 20,000 EPS. The default is 100 EPS.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

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.



---

## 79 Itron Smart Meter

The Itron Smart Meter DSM for IBM Security 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 *Ittron 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 **Ittron Smart Meter**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

*Table 308. 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 Itron Openway Smart Meter installation. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.



---

## 80 Juniper Networks

IBM Security QRadar supports the a range of Juniper Networks DSMs.

---

### Juniper Networks AVT

The Juniper Networks Application Volume Tracking (AVT) DSM for IBM Security 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:  
`/var/netscreen/DevSvr/pgsql/data/pg_hba.conf` file
3. Add the following line to the end of the file:  
`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:  
`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:  
`create view strm_avt_view as SELECT a.name, a.category, v.srcip,v.dstip,v.dstport, v."last", u.name as userinfo, v.id, v.device, v.vlan,v.sessionid, v.bytecnt,v.pktcnt, v."first" FROM avt_part v JOIN app a ON v.app =a.id  
JOIN userinfo u ON v.userinfo = u.id;`

The view is created.

You are now ready to configure the log source in QRadar.

### Configuring IBM Security 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. On the navigation menu, click **Data Sources**.
3. Click the **Log Sources** icon.
4. Click **Add Log Source**.
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 **Juniper Networks AVT**.
8. Configure the JDBC protocol for the log source. The following table describes the parameter values for the JDBC protocol:

*Table 309. JDBC log source parameters*

| Parameter                      | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Type</b>         | Juniper Networks AVT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Protocol Configuration</b>  | JDBC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Log Source Identifier</b>   | <p>Type the identifier for the log source. Type the log source identifier in the following format:</p> <p><i>&lt;Database&gt;@&lt;Database Server IP or Host Name&gt;</i></p> <p>Where:</p> <ul style="list-style-type: none"> <li>• <i>&lt;Database&gt;</i> is the database name, as entered in the <b>Database Name</b> parameter.</li> <li>• <i>&lt;Database Server IP or Host Name&gt;</i> is the host name or IP address for this log source, as entered in the <b>IP or Hostname</b> parameter.</li> </ul> |
| <b>Database Type</b>           | <b>Postgres</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Database Name</b>           | <b>profilerDb</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>IP or Hostname</b>          | The IP address or host name of the SQL server that hosts the Juniper Networks AVT database.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Port</b>                    | <p>Type the port number that is used by the database server. The default port for Postgres is 5432.</p> <p>The JDBC configuration port must match the listener port of the Juniper Networks AVT database. The Juniper Networks AVT database must have incoming TCP connections that are enabled to communicate with QRadar.</p>                                                                                                                                                                                  |
| <b>Username</b>                | Type the user name the log source can use to access the Juniper Networks AVT database.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Password</b>                | <p>Type the password the log source can use to access the Juniper Networks AVT database.</p> <p>The password can be up to 255 characters in length.</p>                                                                                                                                                                                                                                                                                                                                                          |
| <b>Confirm Password</b>        | Confirm the password that is used to access the database. The confirmation password must be identical to the password entered in the <b>Password</b> field.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Predefined Query</b>        | From the list, select <b>Juniper Networks AVT</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Use Prepared Statements</b> | The <b>Use Prepared Statements</b> check box must be clear. The Juniper Networks AVT DSM does not support prepared statements.                                                                                                                                                                                                                                                                                                                                                                                   |

Table 309. JDBC log source parameters (continued)

| Parameter                  | Value                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Start Date and Time</b> | <p>Optional. Type the start date and time for database polling.</p> <p>The <b>Start Date and Time</b> 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.</p>                                                                             |
| <b>Polling Interval</b>    | <p>Type the polling interval, which is the amount of time between queries to the view you created. The default polling interval is 10 seconds.</p> <p>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.</p> |
| <b>EPS Throttle</b>        | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.                                                                                                                                                                                                                                                                         |

**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.

#### Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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:

[93, “NCC Group DDoS Secure,” on page 689](#)

The IBM Security 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 Security 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 Security 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](#)

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

[“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 Security 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:

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 310.

Table 310. Juniper Networks EX Series switch options

| Option               | Description                |
|----------------------|----------------------------|
| <b>any</b>           | All facilities             |
| <b>authorization</b> | Authorization system       |
| <b>change-log</b>    | Configuration change log   |
| <b>conflict-log</b>  | Configuration conflict log |

Table 310. Juniper Networks EX Series switch options (continued)

| Option                      | Description                                     |
|-----------------------------|-------------------------------------------------|
| <b>daemon</b>               | Various system processes                        |
| <b>dfc</b>                  | Dynamic flow capture                            |
| <b>explicit-priority</b>    | Include priority and facility in messages       |
| <b>external</b>             | Local external applications                     |
| <b>facility-override</b>    | Alternative facility for logging to remote host |
| <b>firewall</b>             | Firewall filtering system                       |
| <b>ftp</b>                  | FTP process                                     |
| <b>interactive-commands</b> | Commands run by the UI                          |
| <b>kernel</b>               | Kernel                                          |
| <b>log-prefix</b>           | Prefix for all logging to this host             |
| <b>match</b>                | Regular expression for lines to be logged       |
| <b>pfe</b>                  | Packet Forwarding Engine                        |
| <b>user</b>                 | User processes                                  |

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 Security 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

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

“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 Security 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>, <dstzone>, <dst interface>,
<dst addr>, <dst port>, <nat dst addr>,
<nat dst port>, <protocol>, <rule domain>,
<rule domainVersion>, <policyname>, <rulebase>,
<rulenumber>, <action>, <severity>,
<is alert>, <elapsed>, <bytes in>,
<bytes out>, <bytestotal>, <packet in>,
<packet out>, <packet total>, <repeatCount>,
<hasPacketData>, <varData Enum>, <misc-str>,
<user str>, <application str>, <uri str>
```

See the following syslog example:

```
[syslog@juniper.net dayId="20061012" recordId="0"
timeRecv="2006/10/12 21:52:21"
timeGen="2006/10/12 21:52:21" domain="" devDomVer2="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 Security 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

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

“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 Security 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 Security QRadar Managing Log Sources Guide*.

---

## Juniper Networks Firewall and VPN

The Juniper Networks Firewall and VPN DSM for IBM Security 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.
2. Select **Configuration > Report Settings > Syslog**.
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

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

“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 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 Security 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 558.

**Note:** For more information about structured-data syslog, see RFC 5424 at the Internet Engineering Task Force: <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.

List of Syslog Configuration Setting Variables

| Parameter   | Description                                                          |
|-------------|----------------------------------------------------------------------|
| <b>host</b> | Type the IP address or the fully qualified host name of your QRadar. |

## List of Syslog Configuration Setting Variables

| Parameter              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Facility</b>        | <p>Define the severity of the messages that belong to the named facility with which it is paired. Valid severity levels are:</p> <ul style="list-style-type: none"> <li>• Any</li> <li>• None</li> <li>• Emergency</li> <li>• Alert</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notice</li> <li>• Info</li> </ul> <p>Messages with the specified severity level and higher are logged. The levels from emergency through info are in order from highest severity to lowest.</p> |
| <b>Source-address</b>  | <p>Type a valid IP address configured on one of the router interfaces for system logging purposes.</p> <p>The source-address is recorded as the source of the syslog message send to QRadar. This IP address is specified in the <code>host</code> host name statement set <code>system syslog</code> hierarchy level; however, this is not for messages directed to the other routing engine, or to the TX Matrix platform in a routing matrix.</p>                                                   |
| <b>structured-data</b> | Inserts structured-data syslog into the data.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

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 47](#)

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](#)

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

[“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 receive events from a Juniper Junos OS Platform device

You can manually configure IBM Security 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

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

“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 the PCAP Protocol

The Juniper SRX Series appliance supports forwarding of packet capture (PCAP) and syslog data to IBM Security 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 559

The Juniper Networks SRX Series appliance is automatically discovered by IBM Security 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 Security 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

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

“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 Security 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”
- “Configuring a log source for Juniper Networks NSM”

### 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.
6. Select **Syslog Enable** for **Category**, **Severity**, and **Action**.

You are now ready to configure the log source in IBM Security QRadar.

### Configuring a log source for Juniper Networks NSM

You can configure a log source in IBM Security 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 311. Juniper NSM protocol parameters*

| Parameter             | Description                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Log Source Identifier | Type the IP address or host name for the log source.<br><br>The <b>Log Source Identifier</b> must be unique for the log source type. |

*Table 311. Juniper NSM protocol parameters (continued)*

| Parameter                             | Description                                                                                                                                            |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP</b>                             | Type the IP address or host name of the Juniper Networks NSM server.                                                                                   |
| <b>Inbound Port</b>                   | Type the <b>Inbound Port</b> to which the Juniper Networks NSM sends communications. The valid range is 0 - 65536. The default is 514.                 |
| <b>Redirection Listen Port</b>        | Type the port to which traffic is forwarded. The valid range is 0 - 65,536. The default is 516.                                                        |
| <b>Use NSM Address for Log Source</b> | 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. |

**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:

115, "Pulse Secure Pulse Connect Secure," on page 799

The IBM Security QRadar DSM for Pulse Secure Pulse Connect Secure collects syslog and WebTrends Enhanced Log File (WELF) formatted events from Pulse Secure Pulse Connect Secure mobile VPN devices.

---

## Juniper Networks Security Binary Log Collector

The Juniper Security Binary Log Collector DSM for IBM Security 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"
- "Configuring a log source" on page 562

## Configuring the Juniper Networks Binary Log Format

The binary log format from Juniper SRX or J Series appliances are streamed to IBM Security 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 Security 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 561.
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 Security 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**.
9. Using the **Protocol Configuration** list, select **Juniper Security Binary Log Collector**.
10. Configure the following values:

*Table 312. Juniper Security Binary Log Collector protocol parameters*

| Parameter                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b>      | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Binary Collector Port</b>      | <p>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 “Configuring the Juniper Networks Binary Log Format” on page 561, “Configuring the Juniper Networks Binary Log Format” on page 561.</p> <p>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 <b>Binary Collector Port</b> parameter in QRadar.</p> <p>To edit the port:</p> <ol style="list-style-type: none"> <li>1. In the <b>Binary Collector Port</b> field, type the new port number for receiving binary event data.</li> <li>2. Click <b>Save</b>.</li> </ol> <p>The port update is complete and event collection starts on the new port number.</p> |
| <b>XML Template File Location</b> | <p>Type the path to the XML file used to decode the binary stream from your Juniper SRX or Juniper J Series appliance.</p> <p>By default, QRadar includes an XML template file for decoding the binary stream in the following directory:</p> <p>/opt/qradar/conf/security_log.xml</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

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 Security QRadar accepts syslog events from clients that run the WinCollect agent.

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, see the *IBM Security QRadar WinCollect User Guide*.
- Configure Juniper Steel-Belted Radius by using syslog on Linux-based operating systems. For more information, see “Configuring Juniper Steel-Belted Radius for syslog” on page 564.

### Related tasks:

“Adding a DSM” on page 4

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

“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 Steel-Belted Radius for syslog

You can integrate a Juniper Steel-Belted Radius DSM with IBM Security QRadar by using syslog on a Linux-based operating system.

### 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`

6. You can now configure the log source in QRadar.

To configure QRadar to receive events from Juniper Steel-Belted Radius:

From the **Log Source Type** list, select the **Juniper Steel-Belted Radius** option.

For more information on configuring your Steel-Belted Radius server 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.

---

## Juniper Networks vGW Virtual Gateway

The Juniper Networks vGW Virtual Gateway DSM for IBM Security 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 313. Syslog parameters*

| Parameter          | Description                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syslog Server      | Type the IP address of your vGW management server if you selected to <b>Send Syslog from vGW management server</b> . Or, type the IP address of QRadar if you selected <b>Send Syslog from Firewalls</b> . |
| Syslog Server Port | Type the port address for syslog. This port is typically port 514.                                                                                                                                         |

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 314. Netflow parameters*

| Parameter                 | Description                             |
|---------------------------|-----------------------------------------|
| NetFlow collector address | Type the IP address of QRadar.          |
| Syslog Server Port        | Type a port address for NetFlow events. |

**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

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

“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 Security 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 Security 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 315. Juniper Junos WebApp Secure logging parameters

| Parameter                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access logging: Log Level</b>                                     | <p>Click this option to configure the level of information that is logged when access logging is enabled.</p> <p>The options include the following levels:</p> <ul style="list-style-type: none"> <li>• <b>0</b> - Access logging is disabled.</li> <li>• <b>1</b> - Basic logging.</li> <li>• <b>2</b> - Basic logging with headers.</li> <li>• <b>3</b> - Basic logging with headers and body.</li> </ul> <p><b>Note:</b> Access logging is disabled by default. It is suggested that you enable access logging only for debugging purposes. For more information, see your <i>Juniper Junos WebApp Secure documentation</i>.</p>                                                                            |
| <b>Access logging: Log requests before processing</b>                | Click this option and select <b>True</b> to log the request before it is processed, then forward the event to QRadar.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Access logging: Log requests to access log after processing</b>   | Click this option and select <b>True</b> to log the request after it is processed. After Juniper Junos WebApp Secure processes the event, then it is forwarded to QRadar.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Access logging: Log responses to access log after processing</b>  | Click this option and select <b>True</b> to log the response after it is processed. After Juniper Junos WebApp Secure processes the event, then the event is forwarded to QRadar.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Access logging: Log responses to access log before processing</b> | Click this option and select <b>True</b> to log the response before it is processed, then forward the event to QRadar.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Incident severity log level</b>                                   | <p>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.</p> <p>The options include the following levels:</p> <ul style="list-style-type: none"> <li>• <b>0</b> - Informational level and later incident events are logged and forwarded.</li> <li>• <b>1</b> - Suspicious level and later incident events are logged and forwarded.</li> <li>• <b>2</b> - Low level and later incident events are logged and forwarded.</li> <li>• <b>3</b> - Medium level and later incident events are logged and forwarded.</li> <li>• <b>4</b> - High level and later incident events are logged and forwarded.</li> </ul> |
| <b>Log incidents to the syslog</b>                                   | Click this option and select <b>Yes</b> to enable syslog forwarding to QRadar.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

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 Security 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 Security 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 316. Syslog protocol parameters*

| Parameter                    | Description                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Identifier</b> | Type the IP address or host name for the log source as an identifier for events from your Juniper Junos WebApp Secure appliance. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

## Juniper Networks WLC Series Wireless LAN Controller

IBM Security 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.”
  - 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 569.
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 Security 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 Security 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:
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.



---

## 81 Kaspersky

IBM Security QRadar supports a range of Kaspersky DSMs.

### Kaspersky Security Center

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

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

*Table 317. Kaspersky Security Center DSM specifications*

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

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:

*Table 318. Kaspersky Security Center syslog log source parameters*

| Parameter                     | Value                                                                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source type</b>        | Kaspersky Security Center                                                                                                                         |
| <b>Protocol Configuration</b> | Syslog                                                                                                                                            |
| <b>Log Source Identifier</b>  | 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:

*Table 319. Kaspersky Security Center JDBC log source parameters*

| Parameter                     | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source type</b>        | Kaspersky Security Center                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Protocol Configuration</b> | JDBC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Log Source Identifier</b>  | <p>Use the following format:<br/> <i>&lt;Kaspersky_Database&gt;@&lt;Server_Address&gt;</i></p> <p>Where the <i>&lt;Server_Address&gt;</i> is the IP address or host name of the Kaspersky Security Center database server.</p>                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Database Type</b>          | MSDE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Database Name</b>          | KAV                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>IP or Hostname</b>         | The IP address or host name of the SQL server that hosts the Kaspersky Security Center database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Port</b>                   | <p>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 <b>Port</b> field.</p> <p>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.</p> <p>If you define a database instance that uses MSDE as the database type, you must leave the <b>Port</b> parameter blank in your configuration.</p> |
| <b>Username</b>               | Type the user name the log source can use to access the Kaspersky Security Center database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Password</b>               | <p>Type the password the log source can use to access the Kaspersky Security Center database.</p> <p>The password can be up to 255 characters in length.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Confirm Password</b>       | Confirm the password that is used to access the database. The confirmation password must be identical to the password entered in the <b>Password</b> field.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Authentication Domain</b>  | If you select <b>MSDE</b> as the <b>Database Type</b> and the database is configured for Windows Authentication, you must populate the <b>Authentication Domain</b> field. Otherwise, leave this field blank.                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 319. Kaspersky Security Center JDBC log source parameters (continued)

| Parameter                           | Value                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Database Instance</b>            | If you have multiple SQL server instances on your database server, type the database instance.<br><br>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 <b>Database Instance</b> parameter blank in your configuration.                                                                                                                             |
| <b>Predefined Query</b>             | From the list, select <b>Kaspersky Security Center</b> .                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Use Prepared Statements</b>      | Select the <b>Use Prepared Statements</b> check box.<br><br>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.<br><br>Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements. |
| <b>Start Date and Time</b>          | Optional. Type the start date and time for database polling.<br><br>The <b>Start Date and Time</b> 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.                                                                                                                                 |
| <b>Polling Interval</b>             | Type the polling interval, which is the amount of time between queries to the view you created. The default polling interval is 10 seconds.<br><br>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.                                                     |
| <b>EPS Throttle</b>                 | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.                                                                                                                                                                                                                                                                                                                      |
| <b>Use Named Pipe Communication</b> | 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.                                                                                                                                                                                                                                                               |
| <b>Database Cluster Name</b>        | If you select the <b>Use Named Pipe Communication</b> check box, the <b>Database Cluster Name</b> 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.                                                                                                                                                                         |

Table 319. Kaspersky Security Center JDBC log source parameters (continued)

| Parameter  | Value                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use NTLMv2 | Select the <b>Use NTLMv2</b> check box.<br><br>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.<br><br>If the <b>Use NTLMv2</b> check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication. |
| Use SSL    | If your connection supports SSL communication, select <b>Use SSL</b> . This option requires extra configuration on your Kaspersky Security Center database and also requires administrators to configure certificates on both appliances.                                                                                                                                                      |

**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.

#### Related concepts:

“JDBC protocol configuration options” on page 16

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

#### Related tasks:

“Adding a DSM” on page 4

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

“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

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

“Exporting syslog to QRadar from Kaspersky Security Center” on page 575

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

“Creating a Database View for Kaspersky Security Center”

To collect audit event data, you must create a database view on your Kaspersky server that is accessible to IBM Security 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.

## 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 Security QRadar.

### About this task

To create a database view, you can download the `k1sql2.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 `k1sql2.zip` file:  
<http://support.kaspersky.com/9284>
2. Copy `k1sql2.zip` to your Kaspersky Security Center Administration Server.
3. Extract `k1sql2.zip` to a directory.
4. The following files are included:
  - `k1sql2.exe`
  - `src.sql`
  - `start.cmd`
5. In any text editor, edit the `src.sql` file.
6. Clear the contents of the `src.sql` file.
7. Type the following Transact-SQL statement to create the `dbo.events` database view:

```
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 `k1sql2` files.
10. Type the following command to create the view on your Kaspersky Security Center appliance:  
`k1sql2 -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 Security QRadar Console or Event Collector.

### About this task

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

## Procedure

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

## Kaspersky Threat Feed Service

The IBM Security QRadar DSM for Kaspersky Threat Feed Service collects events from Kaspersky Feed Service.

The following table describes the specifications for the Kaspersky Threat Feed Service DSM:

*Table 320. Kaspersky Threat Feed Service DSM specifications*

| Specification               | Value                                                                                   |
|-----------------------------|-----------------------------------------------------------------------------------------|
| Manufacturer                | Kaspersky Lab                                                                           |
| DSM name                    | KasperskyThreatFeedService                                                              |
| RPM file name               | DSM-KasperskyThreatFeedService-QRadar_version-build_number.noarch.rpm                   |
| Supported versions          | 2.0                                                                                     |
| Protocol                    | Syslog                                                                                  |
| Event format                | LEEF                                                                                    |
| Recorded event types        | Detect, Status, Evaluation                                                              |
| Automatically discovered?   | Yes                                                                                     |
| Includes identity?          | No                                                                                      |
| Includes custom properties? | No                                                                                      |
| More information            | Kaspersky website ( <a href="http://www.kaspersky.com/">http://www.kaspersky.com/</a> ) |

To integrate Kaspersky Threat Feed 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, in the order that they are listed:
  - DSMCommon RPM
  - Kaspersky Threat Feed Service DSM RPM
2. Configure Kaspersky Threat Feed Service to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Kaspersky Threat Feed Service log source on the desired event collector. The following table describes the parameters that require specific values for Kaspersky Threat Feed Service event collection:

*Table 321. Kaspersky Threat Feed Service log source parameters*

| Parameter              | Value                         |
|------------------------|-------------------------------|
| Log Source type        | Kaspersky Threat Feed Service |
| Protocol Configuration | Syslog                        |
| Log Source Identifier  | KL_Threat_Feed_Service_V2     |

The following table provides a sample event message for Kaspersky Threat Feed Service.

Table 322. Kaspersky Threat Feed Service sample event message

| Event name              | Low level category | Sample log message                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KL_Mobile_BotnetCnc_URL | Botnet address     | <pre>Jul 10 10:10:14 KL_Threat_Feed_Service_v2 LEEF:1.0 Kaspersky Lab Threat Feed Service  2.0 KL_Mobile BotnetCnc_URL - url=example.com/ xxxxxxxxxxxxxx/xxx md5=- sha1=- sha256=- usrName= TestUser mask= xxxxxxxxxxxx.xxxx type=2 first_seen=04.01.2016 16:40 last_seen=27.01.2016 10:46 popularity=5</pre> |

#### Related tasks:

“Adding a DSM” on page 4

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

“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 Threat Feed Service to communicate with QRadar

### Before you begin

Before you install the Threat Feed Service on a device, ensure that your device meets the hardware and software requirements. The requirements are specified in the Kaspersky Threat Feed Service for QRadar distribution kit documentation.

### Procedure

1. Unpack the contents of the installation archive, `Kaspersky_Threat_Feed_Service-Linux-x86_64-2.0.x.y-Release_for_Qradar.tar.gz`, to any directory on the computer that you want to use for running the service.

**Note:** The installation directory is denoted by the variable `<service_dir>` in the following configuration steps.

2. Configure the Threat Feed Service.
  - a. Edit `<service_dir>/etc/k1_feed_service.conf`
  - b. Modify the `ConnectionString` element nested within the `InputSettings` element to specify the IP and Port where the Threat Feed Service listens for events from QRadar:

The IP address is from the server that the Threat Feed Service runs from.

```
<InputSettings>
 ...
 <ConnectionString>Server_IP:Port</ConnectionString>
</InputSettings>
```

The following table identifies the Input Settings parameters that need to be modified in the `k1_feed_service.conf` file.

Table 323. Input Settings parameters

Parameter	Value
QRadar_IP	The IP address of the system the Threat Feed Service is running on.
Port	An available port where the Threat Feed Service listens for events from QRadar. The default is 9995.

- c. Modify the ConnectionString element nested within the OutputSettings element to specify the QRadar event collector IP and Port that the threat Feed Service sends events to.

```
<OutputSettings>
 ...
 <ConnectionString>QRadar_IP:Port</ConnectionString>
</OutputSettings>
```

The following table identifies the Output Settings parameters that need to be modified in the k1\_feed\_service.conf file.

Table 324. Output Settings parameters

Parameter	Value
QRadar_IP	The IP address of the QRadar Event Collector.
Port	514

3. Save the changes.
4. Type the following command from the <service\_dir> directory to start the Threat Feed Service.

```
etc/init.d/k1_feed_service start
```

The following message is displayed when the Threat Feed Service starts.

```
Starting k1_feed_service: Config file: .../etc/k1_feed_service.conf
```

```
[OK]
```

**Note:** If the configuration file is missing or if its contents do not conform to the specified rules, the feed service does not start and an error message appears.

**Note:** To stop the Feed Service, type the following command from the <service\_dir> directory.

```
etc/init.d/k1_feed_service stop
```

5. Verify the communication between the Threat Feed Service and QRadar is working by sending a set of test events by entering the following command:

```
/usr/bin/python <service_dir>/tools/tcp_client.py -a <QRadar_IP> -p 514 <service_dir>/integration/sample_initiallog.txt
```

**Note:** The <QRadar\_IP> test parameter is the IP address of your QRadar Event Collector.

## Configuring QRadar to forward events to the Kaspersky Threat Feed Service

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 325. Forwarding Destination parameters.

Parameter	Value
Name	An identifier for the destination. For example, KL Threat Feed Service v2
Destination Address	IP address of the host that runs the Threat Feed Service.
Event Format	JSON
Destination Port	The port that is specified in <code>k1_feed_service.conf InputSetting &gt; ConnectionString.</code> The default value is 9995.
Protocol	TCP
Profile	Default profile

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 326. Routing Rules parameters

Parameter	Value
Name	An identifier for the rule name. For example, KL Threat Feed Service v2 Rule.
Description	Create a description for the routing rule that you are creating.
Mode	Online
Forwarding Event Collector	Select the event collector that is used to forward events to the Threat Feed Service.
Data Source	Events
Event Filters	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.
Routing Options	Enable <b>Forward</b> , and then select the <code>&lt;forwarding_destination&gt;</code> that you created in Step 1.

9. Click **Save**.



---

## 82 Kisco Information Systems SafeNet/i

The IBM Security 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 327. Kisco Information Systems SafeNet/i DSM specifications*

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

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 328. Kisco Information Systems SafeNet/i log source parameters*

Parameter	Value
Log Source type	Kisco Information Systems SafeNet/i
Protocol Configuration	Log File
Service Type	FTP
Remote IP or Hostname	The IP or host name of Kisco Information systems SafeNet/i device.
Remote Port	21
Remote User	The IBM i User ID that you created for QRadar in Kisco Information Systems SafeNet/i.
Remote Directory	Leave this field empty.
FTP File Pattern	.*

*Table 328. Kisco Information Systems SafeNet/i log source parameters (continued)*

Parameter	Value
FTP Transfer Mode	BINARY
Processor	NONE
Event Generator	LINEBYLINE
File Encoding	US-ASCII

**Related tasks:**

“Adding a DSM” on page 4

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

“Configuring Kisco Information Systems SafeNet/i to communicate with QRadar”

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

“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 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 329. FTP access settings*

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

### Procedure

1. Create an IFS directory on your IBM 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 329 on page 582.
  - h. Press F3 and select **Work with User to Long Paths**.
  - i. Press F6 and provide the path to the IFS directory.  
Ensure that the path is followed by an asterisk, for example, /SafeNet/QRadar/\*
  - j. Type X under the **R** column.
  - k. Press F3 to exit.
3. Type CHGRDRSET and then press F4.
4. Configure the following parameters:

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

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

Parameter	Value
Alert Notification Status	On
Summarized Alerts?	Yes



---

## 83 Lastline Enterprise

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

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

*Table 330. Lastline Enterprise DSM specifications*

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

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 331. Lastline Enterprise log source parameters*

Parameter	Value
Log Source type	Lastline Enterprise
Protocol Configuration	Syslog

### Related tasks:

[“Adding a DSM” on page 4](#)

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

[“Configuring Lastline Enterprise to communicate with QRadar” on page 586](#)

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

[“Adding a log source” on page 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 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**.

---

## 84 Lieberman Random Password Manager

The Lieberman Random Password Manager DSM gives the option to integrate IBM Security 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](#)

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

[“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.



---

## 85 LightCyber Magna

The IBM Security QRadar DSM for LightCyber Magna collects events from a LightCyber Magna device.

The following table describes the specifications for the LightCyber Magna DSM:

*Table 332. LightCyber Magna DSM specifications*

Specification	Value
Manufacturer	LightCyber
DSM name	LightCyber Magna
RPM file name	DSM-LightCyberMagna-QRadar_version-build_number.noarch.rpm
Supported versions	3.9
Protocol	Syslog
Event format	LEEF
Recorded event types	C&C Exfilt Lateral Malware Recon
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	LightCyber website ( <a href="https://www.lightcyber.com">https://www.lightcyber.com</a> )

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 333. LightCyber Magna log source parameters*

Parameter	Value
Log Source type	LightCyber Magna
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

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 334. LightCyber Magna sample message

Event name	Low level category	Sample log message
Suspicious Riskware	Misc Malware	LEEF:2.0 LightCyber Magna  3.7.3.0 New indicator type=Riskware sev=7 devTime=Sep 18 2016 08:26 :08 devTimeFormat=MMM dd yyyy HH:mm:ss devTimeEnd=Sep 29 2016 15:26:47 devTimeEndFormat=MMM dd yyyy HH:mm:ss msg=Riskware alert (0 ) app= dstPort= userName= shostId=xxxxxxxx- xxxx-xxxx-xxxx-xxxxxxxxxxxx shost=PC04 src=<Source_IP_address> srcMAC=<Source_MAC_address> status=Suspicious filePath=c:\program files\ galaxy must\galaxy must.exe malwareName=W32.HfsAutoB.3DF2 fileHash=d836433d538d864d21a4e 0f7d66e30d2 externalId=16100 sdeviceExternalId=32373337 -3938-5A43-4A35-313030303336

**Related tasks:**

“Adding a DSM” on page 4

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

“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 335. LightCyber Magna configuration parameters

Parameter	Value
Host	The IP address or host name of the QRadar Event Collector.
Port	514
Protocol	TCP
Format	LEEF

5. Click **Save**.

---

## 86 Linux

IBM Security QRadar supports the a range of Linux DSMs.

---

### Linux DHCP

The Linux DHCP Server DSM for IBM Security 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 Security 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 336. Syslog parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source as an identifier for events from your Linux DHCP Server.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

---

### Linux IPTables

The Linux IPTables DSM for IBM Security 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 Security 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. For example:

```
-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. IPtable events that are forwarded from Linux Servers are automatically discovered and displayed in the **Log Activity** tab of QRadar.

## Configuring a log source

IBM Security QRadar automatically discovers and creates log sources for IPtables 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 337. Syslog protocol parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source as an identifier for IPtables events that are forwarded from your Linux Server.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete. IPtables events that are forwarded from Linux Servers are automatically discovered and displayed in the **Log Activity** tab of QRadar.

For more information about configuring IPtables on Linux Servers, consult the man pages or your associated Linux documentation.

---

## Linux OS

The Linux OS DSM for IBM Security 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 594
- “Configuring syslog-ng on Linux OS” on page 594

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 595.

## 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](#)

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

[“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 Security 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(<Source name>);
filter(auth_filter);
destination(auth_destination);
};
```

Where:

- <IP address> is the IP address of the IBM Security 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.

---

## 87 LOGbinder

Configure your LOGbinder system to send event logs to IBM Security 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 Security QRadar DSM for Microsoft Exchange Server can collect LOGbinder EX V2.0 events.

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

*Table 338. LOGbinder for Microsoft Exchange Server*

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

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

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

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

*Table 339. Microsoft Exchange Server log source parameters for LOGbinder event collection*

Parameter	Value
Log Source type	Microsoft Exchange Server
Protocol Configuration	Syslog

**Related tasks:**

“Adding a DSM” on page 4

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

“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 EX system to send Microsoft Exchange event logs to QRadar

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

### Before you begin

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

### Procedure

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

---

## LOGbinder SP event collection from Microsoft SharePoint

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

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

*Table 340. LOGbinder for Microsoft SharePoint specifications*

Specification	Value
Manufacturer	Microsoft
DSM name	Microsoft SharePoint

Table 340. LOGbinder for Microsoft SharePoint specifications (continued)

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

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 341. Microsoft SharePoint log source parameters for LOGbinder event collection

Parameter	Value
Log Source type	Microsoft SharePoint
Protocol Configuration	Syslog

#### Related tasks:

“Adding a DSM” on page 4

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

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

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

“Adding a log source” on page 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 SP system to send Microsoft SharePoint event logs to QRadar

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

## Procedure

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

---

## LOGbinder SQL event collection from Microsoft SQL Server

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

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

*Table 342. LOGbinder for Microsoft SQL Server specifications*

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

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.

- 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 343. Microsoft SQL Server log source parameters for LOGbinder event collection*

Parameter	Value
Log Source type	Microsoft SQL Server
Protocol Configuration	Syslog

#### Related tasks:

"Adding a DSM" on page 4

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

"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 Security QRadar.

### Before you begin

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

### Procedure

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



---

## 88 McAfee

IBM Security QRadar supports a range of McAfee products.

### McAfee Application / Change Control

The McAfee Application / Change Control DSM for IBM Security 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**.
5. From the **Log Source Type** list, select **McAfee Application / Change Control**.
6. From the **Protocol Configuration** list, select **JDBC**.

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.

7. Configure the following values:

Table 344. McAfee Application / Change Control JDBC protocol parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the identifier for the log source. Type the log source identifier in the following format:  <i>&lt;McAfee Change Control Database&gt;@&lt;Change Control Database Server IP or Host Name&gt;</i>  Where: <ul style="list-style-type: none"><li>• <i>&lt;McAfee Change Control Database&gt;</i> is the database name, as entered in the <b>Database Name</b> parameter.</li><li>• <i>&lt;Change Control Database Server IP or Host Name&gt;</i> is the host name or IP address for this log source, as entered in the <b>IP or Hostname</b> parameter.</li></ul> When you define a name for your <b>Log Source Identifier</b> , you must use the values of the McAfee Change Control Database and Database Server IP address or host name from the ePO Management Console.
<b>Database Type</b>	From the list, select <b>MSDE</b> .
<b>Database Name</b>	Type the exact name of the McAfee Application / Change Control database.
<b>IP or Hostname</b>	Type the IP address or host name of the McAfee Application / Change Control SQL Server.

Table 344. McAfee Application / Change Control JDBC protocol parameters (continued)

Parameter	Description
<b>Port</b>	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 <b>Database Instance</b> when you use MSDE as the database type, you must leave the <b>Port</b> parameter blank in your configuration.
<b>Username</b>	Type the user name required to access the database.
<b>Password</b>	Type the password required to access the database. The password can be up to 255 characters in length.
<b>Confirm Password</b>	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the <b>Password</b> parameter.
<b>Authentication Domain</b>	If you select <b>MSDE</b> as the <b>Database Type</b> and the database is configured for Windows, you must define the Windows <b>Authentication Domain</b> . Otherwise, leave this field blank.
<b>Database Instance</b>	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 <b>Database Instance</b> parameter blank in your configuration.
<b>Table Name</b>	Type SCOR_EVENTS as the name of the table or view that includes the event records.
<b>Select List</b>	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 <b>Compare Field</b> 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(.)
<b>Compare Field</b>	Type AutoID as the compare field. The compare field is used to identify new events added between queries to the table.
<b>Start Date and Time</b>	Optional. Type the start date and time for database polling.  The <b>Start Date and Time</b> 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.

*Table 344. McAfee Application / Change Control JDBC protocol parameters (continued)*

Parameter	Description
<b>Use Prepared Statements</b>	Select this check box to use prepared statements.  Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is better to use prepared statements.  Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
<b>Polling Interval</b>	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.
<b>EPS Throttle</b>	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
<b>Use Named Pipe Communication</b>	Clear the <b>Use Named Pipe Communications</b> 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.
<b>Database Cluster Name</b>	If you select the <b>Use Named Pipe Communication</b> check box, the <b>Database Cluster Name</b> 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.

**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.

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

#### Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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 345. McAfee ePolicy Orchestrator*

Specification	Value
Manufacturer	McAfee

*Table 345. McAfee ePolicy Orchestrator (continued)*

Specification	Value
DSM name	McAfee ePolicy Orchestrator
RPM file name	DSM-McAfeeEpo-QRadar_version-build_number.noarch.rpm
Supported versions	V3.5 to V5.x
Protocol	JDBC SNMPv1 SNMPv2 SNMPv3
Recorded event types	AntiVirus events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	McAfee website ( <a href="http://www.mcafee.com/usproducts/epolicy-orchestrator.aspx">http://www.mcafee.com/usproducts/epolicy-orchestrator.aspx</a> )

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
  - 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.
  - 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, and JDBC protocol log source parameters that require specific values to collect events from McAfee ePolicy Orchestrator.

*Table 346. McAfee ePolicy Orchestrator SNMPv1 log source parameters*

Parameter	Value
Log Source type	McAfee ePolicy Orchestrator
Protocol Configuration	SNMPv1
Log Source Identifier	Type a unique identifier for the log source.

*Table 347. McAfee ePolicy Orchestrator SNMPv2 log source parameters*

Parameter	Value
Log Source type	McAfee ePolicy Orchestrator
Protocol Configuration	SNMPv2

Table 347. McAfee ePolicy Orchestrator SNMPv2 log source parameters (continued)

Parameter	Value
Log Source Identifier	Type a unique identifier for the log source.
Community	The SNMP community string for the SNMPv2 protocol, such as Public.
Include OIDs in Event Payload	<p>To allow the McAfee ePolicy Orchestrator event payloads to be constructed as name-value pairs instead of the standard event payload format, enable the <b>Include OIDs in Event Payload</b> check box.</p> <p><b>Important:</b> You must include OIDs in the event payload for processing SNMPv2 events for McAfee ePolicy Orchestrator.</p>

Table 348. McAfee ePolicy Orchestrator SNMPv3 log source parameters

Parameter	Value
Log Source type	McAfee ePolicy Orchestrator
Protocol Configuration	SNMPv3
Log Source Identifier	Type a unique identifier for the log source.
Authentication Protocol	<p>The algorithm that you want to use to authenticate SNMPv3 traps:</p> <ul style="list-style-type: none"> <li>• <b>SHA</b> uses Secure Hash Algorithm (SHA) as your authentication protocol.</li> <li>• <b>MD5</b> uses Message Digest 5 (MD5) as your authentication protocol.</li> </ul>
Authentication Password	The password to authenticate SNMPv3. Your authentication password must include a minimum of 8 characters.
Decryption Protocol	<p>Select the algorithm that you want to use to decrypt the SNMPv3 traps.</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> </ul> <p><b>Note:</b> 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 <a href="#">Installing the Java Cryptography Extension</a>.</p>
Decryption Password	The password to decrypt SNMPv3 traps. Your decryption password must include a minimum of 8 characters.
User	The user name that was used to configure SNMPv3 on your McAfee ePO appliance.
Include OIDs in Event Payload	<p>To allow the McAfee ePolicy Orchestrator event payloads to be constructed as name-value pairs instead of the standard event payload format, select the <b>Include OIDs in Event Payload</b> check box.</p> <p><b>Important:</b> You must include OIDs in the event payload for processing SNMPv3 events for McAfee ePolicy Orchestrator.</p>

Table 349. McAfee ePolicy Orchestrator JDBC log source parameters

Parameter	Value
<b>Log Source type</b>	McAfee ePolicy Orchestrator
<b>Protocol Configuration</b>	JDBC
<b>Log Source Identifier</b>	<p>Use the following format:</p> <pre>&lt;McAfee_ePO_Database&gt;@&lt;McAfee_ePO_Database_Server_IP_or_Host_Name&gt;</pre> <p>You must use the values of the McAfee ePolicy Orchestrator database and database server IP address or host name of the McAfee ePolicy Orchestrator Management Console.</p>
<b>Database Type</b>	Select <b>MSDE</b> from the list.
<b>Database Name</b>	The name of the McAfee ePolicy Orchestrator database.
<b>IP or Hostname</b>	The IP address or host name of the McAfee ePolicy Orchestrator SQL Server.
<b>Port</b>	<p>The port number that the database server uses. The port must match the listener port of the McAfee ePolicy Orchestrator database. The incoming TCP connections on the McAfee ePolicy Orchestrator database must be enabled to communicate with QRadar.</p> <p>The default port for MSDE databases is port 1433.</p>
<b>Username</b>	<p>The user name can be up to 255 alphanumeric characters in length and can include underscore (_) characters.</p> <p>To track database access for audit purposes, create a specific user on the database for QRadar.</p>
<b>Password</b>	The password can be up to 255 characters in length.
<b>Authentication Domain</b>	If you select <b>MSDE</b> from the <b>Database Type</b> list and the database is configured for Windows authentication, you must define this parameter. Otherwise, leave this parameter blank.
<b>Database Instance</b>	MDSE 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 <b>Database Instance</b> parameter must be blank in the log source configuration.
<b>Predefined Query</b>	Select a predefined query for the log source. If a predefined query is not available for the log source type, administrators can select <b>none</b> .
<b>Table Name</b>	<p>A table or view that includes the event records as follows:</p> <ul style="list-style-type: none"> <li>• For ePolicy Orchestrator 3.x, type Events.</li> <li>• For ePolicy Orchestrator 4.x, type EPOEvents.</li> <li>• For ePolicy Orchestrator 5.x, type EPOEvents</li> </ul>
<b>Select List</b>	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 <b>Compare Field</b> .
<b>Compare Field</b>	To identify new events added between queries to the table, type AutoID.

Table 349. McAfee ePolicy Orchestrator JDBC log source parameters (continued)

Parameter	Value
<b>Use Prepared Statements</b>	Allows the JDBC protocol source to set up the SQL statement once, and then run the SQL statement many times with different parameters. For security and performance reasons, use prepared statements. If you clear this check box, use an alternative query method that does not use pre-compiled statements.
<b>Start Date and Time</b>	Type the start date and time for database polling in the following format: yyyy-MM-dd HH:mm. Use a 24-hour clock to specify HH. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
<b>Polling Interval</b>	The amount of time between queries to the event table. The default polling interval is 10 seconds. To define a longer polling interval, append H for hours or M for minutes to the numeric value. The maximum polling interval is one week in any time format. Numeric values that are entered without an H or M poll in seconds.
<b>EPS Throttle</b>	The number of events per second (EPS) that you do not want this protocol to exceed.
<b>Use Named Pipe Communication</b>	<p>Clear the <b>Use Named Pipe Communication</b> check box.</p> <p>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.</p>
<b>Database Cluster Name</b>	<p>The <b>Database Cluster Name</b> parameter displays when the <b>Use Named Pipe Communication</b> parameter is enabled.</p> <p>If you are running your SQL server in a cluster environment, define the cluster name to ensure that named pipe communication functions properly.</p>
<b>Use NTLMv2</b>	If you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication, select this option. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
<b>Use SSL</b>	You must enable this parameter if your connection supports SSL, even if your connection does not require it. This option requires extra configuration on your database and requires you to configure certificates on both appliances.

- Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from McAfee ePolicy Orchestrator:

Table 350. McAfee ePolicy Orchestrator sample message

Event name	Low level category	Sample log message
Device Unplug	Information	<pre> AutoID: "41210078" AutoGUID: "B3B25537-38F2-4F88-9D62-FD1620159C 75" ServerID:&lt;Server&gt;" ReceivedUT C: "2016-04-11 20:34:09.913" Detecte dUTC: "2016-04-11 17:18:02.0" Agent GUID: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxx xxxxxx" Analyzer: "DATALOSS2000" AnalyzerName: "Data Loss Prevention" AnalyzerVersion: "9.3.500.15" Analyz erHostName: "&lt;Server&gt;" AnalyzerIPV4 : "&lt;IP_address&gt;" AnalyzerIPV6: "&lt;IPv6_address&gt;" AnalyzerMAC: "null" AnalyzerDATVersion: "null" AnalyzerEngineVers ion: "null" AnalyzerDetection Method: "null" SourceHostName: "xxxx-xx-c-xxx" SourceIPV4: "&lt;Source_IP_address&gt;" SourceIPV6: "&lt;IPv6_address&gt;" SourceMAC: "&lt;Source_MAC_address&gt;" Source UserName: "&lt;Username&gt;\&lt;Domain&gt;" SourceProcessName: "" SourceURL: "null" TargetHostName: "xxxx-xx -x-x" TargetIPV4: "&lt;IP_ad dress&gt;" TargetIPV6: "&lt;IPv6_ _address&gt;" TargetMAC: "&lt;MAC_ address&gt;" TargetUserName: "&lt;Username&gt;" TargetPort: "null" " TargetProtocol: "null" TargetPro cessName: "" TargetFileName: "null" " ThreatCategory: "policy" Threat EventID: "19116" ThreatSeverity: "5" ThreatName: "Politica 1: Audi tar USB de Almacenamiento" Threat Type: "DEVICE_UNPLUG" Threat ActionTaken: "MON ON" ThreatHandled : "null" TheTimestamp: "[B@cd76718a " TenantId: "1"</pre>

#### Related concepts:

["SNMPv2 protocol configuration options" on page 39](#)

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

["SNMPv3 protocol configuration options" on page 39](#)

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

["JDBC protocol configuration options" on page 16](#)

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

#### 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](#)

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

["Configuring SNMP notifications on McAfee ePolicy Orchestrator" on page 611](#)

To send SNMP events from McAfee ePolicy Orchestrator to IBM Security QRadar, you must configure SNMP notifications on your McAfee ePolicy Orchestrator device.

“Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator” on page 613  
The Java™ Cryptography Extension (JCE) is a Java framework that is required for IBM Security 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”

To send SNMP events from McAfee ePolicy Orchestrator to IBM Security 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 Security 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:

Available Types	Selected Types	ePolicy Orchestrator Version
Detected UTC	{listOfDetectedUTC}	4.5, 5.1
Received UTC	{listOfReceivedUTC}	4.5, 5.1
Detecting Product IPv4 Address	{listOfAnalyzerIPV4}	4.5, 5.1
Detecting Product IPv6 Address	{listOfAnalyzerIPV6}	4.5, 5.1
Detecting Product MAC Address	{listOfAnalyzerMAC}	4.5, 5.1
Source IPv4 Address	{listOfSourceIPV4}	4.5, 5.1
Source IPv6 Address	{listOfSourceIPV6}	4.5, 5.1
Source MAC Address	{listOfSourceMAC}	4.5, 5.1
Source User Name	{listOfSourceUserName}	4.5, 5.1
Target IPv4 Address	{listOfTargetIPV4}	4.5, 5.1
Target IPv6 Address	{listOfTargetIPV6}	4.5, 5.1
Target MAC	{listOfTargetMAC}	4.5, 5.1
Target Port	{listOfTargetPort}	4.5, 5.1
Threat Event ID	{listOfThreatEventID}	4.5, 5.1
Threat Event ID	{listOfThreatEventID}	4.5, 5.1
Threat Severity	{listOfThreatSeverity}	4.5, 5.1
SourceComputers		4.0
AffectedComputerIPs		4.0
EventIDs		4.0
TimeNotificationSent		4.0

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”

The Java™ Cryptography Extension (JCE) is a Java framework that is required for IBM Security 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 QRadar”

The Java™ Cryptography Extension (JCE) is a Java framework that is required for IBM Security 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 McAfee ePolicy Orchestrator

The Java™ Cryptography Extension (JCE) is a Java framework that is required for IBM Security 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.

### Procedure

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

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

The JavaTM Cryptography Extension version must match the version of the Java™ installed on your McAfee ePO 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 Security QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your QRadar appliance.

### Procedure

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

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

The JavaTM Cryptography Extension version must match the version of the Java™ installed on QRadar.

2. Extract the JCE file.

The following Java archive (JAR) files are included in the JCE download:

- local\_policy.jar
- US\_export\_policy.jar

3. Log in to your QRadar Console or QRadar Event Collector as a root user.

4. Copy the JCE JAR files to the following directory on your QRadar Console or Event Collector:

/usr/java/j2sdk/jre/lib/

**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.

## McAfee Firewall Enterprise

McAfee Firewall Enterprise is formerly known as Secure Computing Sidewinder. The IBM Security QRadar DSM for McAfee Firewall Enterprise collects logs from a McAfee Firewall Enterprise device.

The following table describes the specifications for the McAfee Firewall Enterprise DSM:

*Table 351. McAfee Firewall Enterprise DSM specifications*

Specification	Value
Manufacturer	McAfee
DSM name	McAfee Firewall Enterprise
RPM file name	DSM-McAfeeFirewallEnterprise-Qradar_version-build_number.noarch.rpm
Supported versions	v6.1
Event format	Syslog
Recorded event types	Firewall Enterprise events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	McAfee website ( <a href="https://www.McAfee.com">https://www.McAfee.com</a> )

To integrate McAfee Firewall Enterprise with QRadar, complete the following steps:

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

*Table 352. McAfee Firewall Enterprise log source parameters*

Parameter	Value
Log Source type	McAfee Firewall Enterprise
Protocol Configuration	Syslog

### Related tasks:

“Adding a DSM” on page 4

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

“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 Firewall Enterprise to communicate with QRadar

The IBM Security QRadar DSM for McAfee Firewall Enterprise collects events by using syslog.

### About this task

Before you configure QRadar SIEM to integrate with a Firewall Enterprise device, you must configure syslog within your McAfee Firewall Enterprise device. When you configure the McAfee Firewall

Enterprise device to forward syslog events to QRadar SIEM, export the logs in Sidewinder Export Format (SEF).

## Procedure

See your vendor documentation for information about configuring McAfee Firewall Enterprise.

## What to do next

After you configure syslog to forward events to QRadar SIEM, you are ready to configure the log source in QRadar SIEM.

---

## McAfee Intrushield

A IBM Security QRadar McAfee Intrushield DSM accepts events that use syslog. QRadar records all relevant events.

Before you configure QRadar to integrate with a McAfee Intrushield device, you must configure your McAfee Intrushield device to send events to QRadar.

- To collect alert events from McAfee Intrushield V2.x - V5.x, see “Configuring alert events for McAfee Intrushield V2.x - V5.x.”
- To collect alert events from McAfee Intrushield V6.x - V7.x, see “Configuring alert events for McAfee Intrushield V6.x and V7.x” on page 616.
- To collect fault notification events from McAfee Intrushield V6.x - V7.x, see “Configuring fault notification events for McAfee Intrushield V6.x and V7.x” on page 617.

## 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 Security 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 353. McAfee Intrushield V2.x - V5.x custom message formats*

Parameter	Description
Unpatched McAfee Intrushield V2.x systems	\$ALERT_ID\$ \$ALERT_TYPE\$ \$ATTACK_TIME\$ "\$ATTACK_NAME" \$ATTACK_ID\$ \$ATTACK_SEVERITY\$ \$ATTACK_SIGNATURE\$ \$ATTACK_CONFIDENCE\$ \$ADMIN_DOMAIN\$ \$SENSOR_NAME\$ \$INTERFACE\$ \$SOURCE_IP\$ \$SOURCE_PORT\$ \$DESTINATION_IP\$ \$DESTINATION_PORT\$

Table 353. McAfee Intrushield V2.x - V5.x custom message formats (continued)

Parameter	Description
McAfee Intrushield that has patches applied to update to V3.x - V5.x	\$IV_ALERT_ID \$IV_ALERT_TYPE \$IV_ATTACK_TIME\$ "\$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 Intrushield V6.x and V7.x

To collect alert notification events from McAfee Intrushield, administrators must configure a syslog forwarder to send events to IBM Security QRadar

#### Procedure

1. Log in to the McAfee Intrushield 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 354. McAfee Intrushield v6.x & 7.x alert notification parameters

Parameter	Description
<b>Enable Syslog Notification</b>	Select <b>Yes</b> to enable syslog notifications for McAfee Intrushield. You must enable this option to forward events to QRadar.
<b>Admin Domain</b>	Select any of the following options: <ul style="list-style-type: none"> <li>• <b>Current</b> - Select this check box to send syslog notifications for alerts in the current domain. This option is selected by default.</li> <li>• <b>Children</b> - Select this check box to send syslog notifications for alerts in any child domains within the current domain.</li> </ul>
<b>Server Name or IP Address</b>	Type the IP address of your QRadar Console or Event Collector. This field supports both IPv4 and IPv6 addresses.
<b>UDP Port</b>	Type 514 as the UDP port for syslog events.

Table 354. McAfee Intrushield v6.x & 7.x alert notification parameters (continued)

Parameter	Description
Facility	Select a syslog facility value.
Severity Mappings	Select a value to map the <b>informational</b> , <b>low</b> , <b>medium</b> , and <b>high</b> alert notification level to a syslog severity.  The options include the following levels: <ul style="list-style-type: none"><li>• <b>Emergency</b> - The system is down or unusable.</li><li>• <b>Alert</b> - The system requires immediate user input or intervention.</li><li>• <b>Critical</b> - The system should be corrected for a critical condition.</li><li>• <b>Error</b> - The system has non-urgent failures.</li><li>• <b>Warning</b> - The system has a warning message that indicates an imminent error.</li><li>• <b>Notice</b> - The system has notifications, no immediate action required.</li><li>• <b>Informational</b> - Normal operating messages.</li></ul>
Send Notification If	Select the following check boxes: <ul style="list-style-type: none"><li>• <b>The attack definition has this notification option explicitly enabled</b></li><li>• <b>The following notification filter is matched</b>, and From the list, select <b>Severity Informational and later</b>.</li></ul>
Notify on IPS Quarantine Alert	Select <b>No</b> as the notify on IPS quarantine option.
Message Preference	Select the <b>Customized</b> option.

- From the **Message Preference** field, click **Edit** to add a custom message filter.
- To ensure that alert notifications are formatted correctly, type the following message string:

```
IV_ALERT_ID|IV_ALERT_TYPE|IV_ATTACK_TIME
"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
$IV_DESTINATION_IP$|$IV_DESTINATION_PORT$|$IV_DIRECTION$
$IV_SUB_CATEGORY$
```

**Note:** The custom message string must be entered as a single line without carriage returns or spaces. 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.

You might require a text editor to properly format the custom message string as a single line.

- Click **Save**.

As alert events are generated by McAfee Intrushield, they are forwarded to the syslog destination 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 fault notification events for McAfee Intrushield V6.x and V7.x

To integrate fault notifications with McAfee Intrushield, you must configure your McAfee Intrushield to forward fault notification events.

## Procedure

1. Log in to the McAfee Intrushield 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 355. McAfee Intrushield V6.x - V7.x fault notification parameters

Parameter	Description
<b>Enable Syslog Notification</b>	Select <b>Yes</b> to enable syslog notifications for McAfee Intrushield. You must enable this option to forward events to QRadar.
<b>Admin Domain</b>	Select any of the following options: <ul style="list-style-type: none"><li>• <b>Current</b> - Select this check box to send syslog notifications for alerts in the current domain. This option is selected by default.</li><li>• <b>Children</b> - Select this check box to send syslog notifications for alerts in any child domains within the current domain.</li></ul>
<b>Server Name or IP Address</b>	Type the IP address of your QRadar Console or Event Collector. This field supports both IPv4 and IPv6 addresses.
<b>Port</b>	Type <b>514</b> as the port for syslog events.
<b>Facilities</b>	Select a syslog facility value.
<b>Severity Mappings</b>	Select a value to map the <b>informational</b> , <b>low</b> , <b>medium</b> , and <b>high</b> alert notification level to a syslog severity.  The options include the following levels: <ul style="list-style-type: none"><li>• <b>Emergency</b> - The system is down or unusable.</li><li>• <b>Alert</b> - The system requires immediate user input or intervention.</li><li>• <b>Critical</b> - The system should be corrected for a critical condition.</li><li>• <b>Error</b> - The system has non-urgent failures.</li><li>• <b>Warning</b> - The system has a warning message that indicates an imminent error.</li><li>• <b>Notice</b> - The system has notifications, no immediate action required.</li><li>• <b>Informational</b> - Normal operating messages.</li></ul>
<b>Forward Faults with severity level</b>	Select <b>Informational and later</b> .
<b>Message Preference</b>	Select the <b>Customized</b> 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 Intrushield 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 Intrushield, 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 Intrushield appliance.

---

## McAfee Web Gateway

You can configure McAfee Web Gateway to integrate with IBM Security QRadar.

Use one of the following methods:

- “Configuring McAfee Web Gateway to communicate with QRadar (syslog)” on page 620
- “Configuring McAfee Web Gateway to communicate with IBM Security QRadar (log file protocol)” on page 621

**Note:** McAfee Web Gateway is formerly known as McAfee WebWasher.

The following table identifies the specifications for the McAfee Web Gateway DSM:

*Table 356. McAfee Web Gateway DSM specifications*

Specification	Value
Manufacturer	McAfee
DSM	McAfee Web Gateway
RPM file name	DSM-McAfeeWebGateway-qradarversion-buildnumber.noarch
Supported versions	v6.0.0 and later
Protocol	Syslog, log file protocol
QRadar recorded events	All relevant events
Automatically discovered	Yes
Includes identity	No
More information	McAfee website ( <a href="http://www.mcafee.com">http://www.mcafee.com</a> )

## McAfee Web Gateway DSM integration process

You can integrate McAfee Web Gateway DSM with IBM Security 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 620

“Configuring McAfee Web Gateway to communicate with IBM Security QRadar (log file protocol)” on page 621

"Creation of an event map for McAfee Web Gateway events" on page 622

## Configuring McAfee Web Gateway to communicate with QRadar (syslog)

To collect all events from McAfee Web Gateway, you must specify IBM Security 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."

## 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 357. McAfee Web Gateway required log handler file

Version	Required XML file
McAfee Web Gateway V7.0	syslog_loghandler_70.xml
McAfee Web Gateway V7.3	syslog_loghandler_73.xml

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 Security 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.”

## Pulling data by using the log file protocol

A log file protocol source allows IBM Security 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 required for all events that are collected from McAfee Web Gateway v7.0.0 and later.

You can individually map each event for your device to an event category in IBM Security 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.

---

## 89 MetaInfo MetaIP

The MetaInfo MetaIP DSM for IBM Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 358. Syslog parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source as an identifier for events from your MetaInfo MetaIP appliances.

11. Click **Save**.
12. On the Admin tab, click **Deploy Changes**.  
The configuration is complete.



---

## 90 Microsoft

IBM Security QRadar supports a range of Microsoft products.

### Microsoft Azure

The IBM Security 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.
  - Protocol Common RPM
  - Microsoft Azure Event Hubs Protocol 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:

*Note:* QRadar 7.2.8 Patch 7 and later is required for Microsoft Azure Event Hubs Protocol RPM.

  - DSMCommon RPM
  - Microsoft Azure DSM RPM

*Table 359. Syslog log source parameters*

Parameter	Value
Log Source type	Microsoft Azure
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the device that sends Microsoft Azure events to QRadar.

3. Optional: Configure the Microsoft Azure Event Hubs Protocol. QRadar does not automatically detect the Microsoft Azure Event Hubs Protocol. For more information about configuring the protocol, see the Microsoft Azure Event Hubs protocol configuration options topic in the IBM Knowledge Center. ([https://www.ibm.com/support/knowledgecenter/SS42VS\\_DSM/c\\_logsource\\_Microsoft\\_Azure\\_Event\\_Hubs\\_protocol.html?cp=SS42VS\\_7.3.0](https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_logsource_Microsoft_Azure_Event_Hubs_protocol.html?cp=SS42VS_7.3.0))

#### Related concepts:

“Microsoft Azure Event Hubs protocol configuration options” on page 22

The Microsoft Azure Event Hubs protocol for IBM Security QRadar collects events from Microsoft Azure Event Hubs.

#### Related tasks:

“Adding a DSM” on page 4

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

“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**.
2. Obtain and install the Microsoft Azure Log Integration service (`AzureLogIntegration.msi`) from the Microsoft website (<https://azure.microsoft.com/en-us/documentation/articles/security-azure-log-integration-get-started/>).
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].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.

### 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 **Default keys** 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];core.windows.net
```

**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 Hub. 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 Hub** 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 a log source to collect events from Microsoft Azure Event Hubs

Follow these steps to configure and create a log source that collects events from Microsoft Azure Event Hubs.

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 Azure**.
7. From the **Protocol Configuration** list, select **Microsoft Azure Event Hubs**.
8. Complete the procedure on “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628.
9. Configure the parameters that are based on the following table:

*Table 360. Configuring a log source in Microsoft Azure Event Hubs*

Parameter	Description
<b>Log Source Identifier</b>	Enter an identifiable name or IP address for the log source. When <b>Use as Gateway Log Source</b> is selected, the <b>Log Source Identifier</b> is not used.
<b>Use as Gateway Log Source</b>	Set this option to <b>Enabled</b> for the collected events to go through the QRadar Traffic Analysis Engine and automatically detect the appropriate log source or log sources.
<b>Use Event Hub Connection String</b>	Enable this check box to use an <b>Event Hub Connection String</b> . Clear this check box to manually enter the <b>Event Hub Connection String</b> , <b>Namespace Name</b> , <b>Event Hub Name</b> , <b>SAS Name</b> , and <b>SAS Key</b> .
<b>Event Hub Connection String</b>	This option is only available if <b>Use Event Hub Connection String</b> is enabled. Enter the <b>Connection string-primary key</b> that you obtained during step 2 in “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628.
<b>Namespace Name</b>	This option is only available if the <b>Use Event Hub Connection String</b> check box is cleared. Enter the <b>Namespace Name</b> obtained during step 2 in “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628.
<b>Event Hub Name</b>	This option is only available if the <b>Use Event Hub Connection String</b> check box is cleared. Enter the <b>Event Hub Name</b> obtained during step 2 in “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628.
<b>SAS Key Name</b>	This option is only available if the <b>Use Event Hub Connection String</b> check box is cleared. Enter the <b>SAS Key Name</b> obtained during step 2 in “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628.
<b>SAS Key</b>	This option is only available if the <b>Use Event Hub Connection String</b> check box is cleared. Enter the <b>Primary key</b> obtained during step 2 in “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628.
<b>Consumer Group</b>	Enter the <b>Consumer Group</b> obtained during step 3 of “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628.

Table 360. Configuring a log source in Microsoft Azure Event Hubs (continued)

Parameter	Description
<b>Use Storage Account Connection String</b>	Enable this check box to use a <b>Storage Account Connection String</b> . Clear this check box to manually enter the <b>Storage Account Name</b> and <b>Storage Account Key</b> .
<b>Storage Account Connection String</b>	This option is only available if the <b>Use Storage Account Connection String</b> check box is enabled. Enter the <b>CONNECTION STRING</b> obtained during step 1 in “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628.
<b>Storage Account Name</b>	This option is only available if the <b>Use Storage Account Connection String</b> check box is cleared. Enter the <b>Storage Account Name</b> obtained during step 1 in “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628.
<b>Storage Account Key</b>	This option is only available if the <b>Use Storage Account Connection String</b> check box is cleared. Enter the <b>KEY</b> obtained during step 1 in “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 628
<b>Automatically Acquire Server Certificates</b>	If you choose <b>Yes</b> from the drop-down list, QRadar automatically downloads the certificate and begins trusting the target server.
<b>EPS Throttle</b>	Type the maximum number of events the Microsoft Azure Event Hubs Protocol forwards per second. The minimum value is 100 EPS and the maximum is 10,000 EPS. The default is 5000 EPS.

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

## Microsoft Azure DSM specifications

The following table describes the specifications for the Microsoft Azure DSM.

Table 361. Microsoft Azure DSM specifications

Specification	Value
Manufacturer	Microsoft
DSM name	Microsoft Azure
RPM file name	DSM-MicrosoftAzure-QRadar_version-build_number.noarch.rpm
Supported versions	N/A
Protocol	Syslog Microsoft Azure Event Hubs
Event format	LIEF JSON

*Table 361. Microsoft Azure DSM specifications (continued)*

Specification	Value
Recorded event types	Network Security Group (NSG) Flow logs, Network Security Group (NSG) Logs, Authorization, Classic Compute, Classic Storage, Compute, Insights, KeyVault, SQL, Storage, Automation, Cache, CDN, Devices, Event Hub, HDInsight, Recovery Services, AppService, Batch, Bing Maps, Certificate Registration, Cognitive Services, Container Service, Content Moderator, Data Catalog, Data Factory, Data Lake Analytics, Data Lake Store, Domain Registration, Dynamics LCS, Features, Logic, Media, Notification Hubs, Search, Servicebus, Support, Web, Scheduler, Resources, Resource Health, Operation Insights, Market Place Ordering, API Management, AD Hybrid Health Service, Server Management
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	<a href="https://azure.microsoft.com/en-us/services/event-hubs">Microsoft Azure Information page (https://azure.microsoft.com/en-us/services/event-hubs)</a> <a href="https://portal.azure.com">Microsoft Azure Portal (https://portal.azure.com)</a>

## 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 362. Microsoft Azure sample syslog message*

Event name	Low level category	Sample log message
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= <IP_address> usrName =name@example.com sev=4 resource= testvm resourceGroup=Test Resource Group description =Restart a Virtual Machine

Table 363. Microsoft Azure Event Hubs sample event messages

Event name	Low level category	Sample log message
microsoft.operation alinsights/ workspaces/listkeys/ action	Read Activity Attempted	<pre>{"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": "&lt;IP_address&gt;", "correlationId": "", "identity": {"authorization": {"scope": "/subscriptions//resourceGroups//providers/Microsoft.Storage/storageAccounts//", "action": "Microsoft.Storage/storageAccounts/listKeys/action", "evidence": {"role": "Insights Management Service Role", "roleAssignmentScope": "/subscriptions//", "roleAssignmentId": "", "roleDefinitionId": "", "principalId": "", "principalType": "ServicePrincipal"}, "claims": {"aud": "https://management.azure.com//", "iss": "https://sts.windows.net//", "iat": "", "nbf": "", "exp": "", "aio": "==", "appid": "", "appidacr": "2", "e_exp": "262800", "http://schemas.microsoft.com/identity/claims/identityprovider": "https://sts.windows.net//", "http://schemas.microsoft.com/identity/claims/objectidentifier": "", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier": "", "http://schemas.microsoft.com/identity/claims/tenantid": "", "uti": "WjPain_x0WJEqtFGqMEAA", "ver": "1.0"}}, "level": "Information", "location": "global"}, {"time": "2017-09-14T11:47:36.3237658Z", "resourceId": "/SUBSCRIPTIONS//RESOURCEGROUPS//PROVIDERS/MICROSOFT.STORAGE/STORAGEACCOUNTS//", "operationName": "MICROSOFT.STORAGE/STORAGEACCOUNTS/LISTKEYS/ACTION", "category": "Action", "resultType": "Success", "resultSignature": "Succeeded.OK", "durationMs": 125, "callerIpAddress": "&lt;IP_address&gt;", "correlationId": "", "identity": {"authorization": {"scope": "/subscriptions//resourceGroups//providers/Microsoft.Storage/storageAccounts//", "action": "Microsoft.Storage/storageAccounts/listKeys/action", "evidence": {"role": "Insights Management Service Role", "roleAssignmentScope": "/subscriptions//", "roleAssignmentId": "", "roleDefinitionId": "", "principalId": "", "principalType": "ServicePrincipal"}, "claims": {"aud": "https://management.azure.com//", "iss": "https://sts.windows.net/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx//", "iat": "1505389356", "nbf": "1505389356", "exp": "1505393256", "aio": "Y2VgYBBQE5y0vTd4PVnSpSp9qVwAA==", "appid": "", "appidacr": "2", "e_exp": "262800", "http://schemas.microso</pre>

Table 363. Microsoft Azure Event Hubs sample event messages (continued)

Event name	Low level category	Sample log message
microsoft.operation alinsights/ workspaces/listkeys/ action (Continued)		ft.com/identity/claims/identityprovider":"https://sts.windows.net//","http://schemas.microsoft.com/identity/claims/objectidentifier":","http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier":","http://schemas.microsoft.com/identity/claims/tenantid":","uti":"xxxxxx_xxxxxxxxxxxx","ver":"1.0"}}, "level": "Information", "location": "global", "properties": {"statusCode": "OK", "serviceRequestId": ""}}]]}"
SecretGet	Read Activity Attempted	"{"records": [{"time": "2016-03-02T04:31:28.6127743Z", "resourceId": "/SUBSCRIPTIONS//RESOURCEGROUPS//PROVIDERS/MICROSOFT.KEYVAULT/VAULTS/AZLOGTEST", "operationName": "SecretGet", "operationVersion": "2015-06-01", "category": "AuditEvent", "resultType": "Success", "resultSignature": "OK", "resultDescription": "", "durationMs": "187", "callerIpAddress": "", "correlationId": "", "identity": {"claim": {"http://schemas.microsoft.com/identity/claims/objectidentifier": "", "appid": "", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn": ""}}, "properties": {"clientInfo": "", "requestUri": "", "id": "https://vault.azure.net/secrets/testsecret/", "httpStatusCode": 200} }]}"
Failed Password	SSH Login Failed	"{"time": "2017-05-11T21:58:37.000000Z", "resourceId": "/subscriptions//resourceGroups//providers/Microsoft.Compute/virtualMachines/", "properties": {"host": "", "ident": "sshd", "pid": "", "Ignore": "syslog", "Facility": "auth", "Severity": "info", "EventTime": "2017-05-11T21:58:37+0000", "SendingHost": "", "Msg": "Failed password for root from <IP_address> port 1111 ssh2", "hostname": "", "FluentdIngestTimestamp": "2017-05-11T21:58:37Z"}, "category": "auth", "level": "info"}}"

## Microsoft DHCP Server

The Microsoft DHCP Server DSM for IBM Security 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.

- Click the **General** tab.

The General pane is displayed.

- 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 364. Microsoft DHCP log file examples*

Log Type	Example
IPv4	DhcpSrvLog-Mon.log
IPv6	DhcpV6SrvLog-Wed.log

By default Microsoft DHCP is configured to write audit logs to the %WINDIR%\system32\dhcp\ directory.

- Restart the DHCP service.

- 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 Security QRadar WinCollect User Guide*.

#### Related concepts:

“Microsoft DHCP protocol configuration options” on page 24

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 Security 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 365. Microsoft DNS Debug DSM specifications*

Specification	Value
Manufacturer	Microsoft
DSM name	Microsoft DNS Debug
RPM file name	DSM-MicrosoftDNS-QRadar_version-build_number.noarch.rpm
Supported versions	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016

Table 365. Microsoft DNS Debug DSM specifications (continued)

Specification	Value
Protocol	WinCollect Microsoft DNS Debug
Event format	LEEF
Recorded event types	All operational and configuration network events.
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	<a href="http://www.microsoft.com">http://www.microsoft.com</a>

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
2. Configure WinCollect to forward Microsoft DNS Debug events to QRadar. For more information, go to Log Sources for WinCollect agents in the *IBM Security QRadar WinCollect User Guide*. ([https://www.ibm.com/support/knowledgecenter/SS42VS\\_7.2.8/com.ibm.wincollect.doc/c\\_ug\\_wincollect\\_log\\_sources.html](https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.wincollect.doc/c_ug_wincollect_log_sources.html)).
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

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

“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 Security 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. On the navigation menu, click **Data Sources**.
3. Click the **Log Sources** icon.
4. Click **Add Log Source**.
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 **Microsoft Endpoint Protection**.
8. From the **Protocol Configuration** list, select **JDBC**.
9. Configure the following values:

Table 366. Microsoft Endpoint Protection JDBC parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the identifier for the log source. Type the log source identifier in the following format:  <i>&lt;Database&gt;@&lt;Database Server IP or Host Name&gt;</i>  Where: <ul style="list-style-type: none"> <li>• <i>&lt;Database&gt;</i> is the database name, as entered in the <b>Database Name</b> parameter.</li> <li>• <i>&lt;Database Server IP or Host Name&gt;</i> is the host name or IP address for this log source, as entered in the <b>IP or Hostname</b> parameter.</li> </ul>
<b>Database Type</b>	From the list, select <b>MSDE</b> .
<b>Database Name</b>	Type the name of the Microsoft Endpoint Protection database.
<b>IP or Hostname</b>	Type the IP address or host name of the Microsoft Endpoint Protection SQL Server.
<b>Port</b>	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 Endpoint Protection database. The Microsoft Endpoint Protection database must have incoming TCP connections that are enabled to communicate with QRadar.  If you define a <b>Database Instance</b> when MSDE is used as the database type, you must leave the Port parameter blank in your configuration.
<b>Username</b>	Type the user name the log source can use to access the Microsoft Endpoint Protection database.
<b>Password</b>	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.
<b>Confirm Password</b>	Confirm the password that is used to access the database. The confirmation password must be identical to the password entered in the <b>Password</b> field.
<b>Authentication Domain</b>	If you select <b>MSDE</b> as the <b>Database Type</b> and the database is configured for Windows Authentication, you must populate the <b>Authentication Domain</b> field. Otherwise, leave this field blank.
<b>Database Instance</b>	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 <b>Database Instance</b> parameter blank in your configuration.
<b>Predefined Query</b>	From the list, select <b>Microsoft Endpoint Protection</b> .
<b>Use Prepared Statements</b>	Select the <b>Use Prepared Statements</b> 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.
<b>Start Date and Time</b>	Optional. Type the start date and time for database polling.  The <b>Start Date and Time</b> 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.

Table 366. Microsoft Endpoint Protection JDBC parameters (continued)

Parameter	Description
<b>Polling Interval</b>	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.
<b>EPS Throttle</b>	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
<b>Use Named Pipe Communication</b>	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.
<b>Database Cluster Name</b>	If you select the Use Named Pipe Communication check box, the <b>Database Cluster Name</b> 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.
<b>Use NTLMv2</b>	Select the <b>Use NTLMv2</b> 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 <b>Use NTLMv2</b> check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
<b>Use SSL</b>	If your connection supports SSL communication, select <b>Use SSL</b> . This option requires extra configuration on your Endpoint Protection database and also requires administrators to configure certificates on both appliances.

**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.

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

## Microsoft Exchange Server

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

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

Table 367. Microsoft Exchange Server

Specification	Value
Manufacturer	Microsoft
DSM name	Exchange Server
RPM file name	DSM-MicrosoftExchange-QRadar_version-build_number.noarch.rpm

Table 367. Microsoft Exchange Server (continued)

Specification	Value
Supported versions	Microsoft Exchange 2003 Microsoft Exchange 2007 Microsoft Exchange 2010 Microsoft Exchange 2013 Microsoft Exchange 2016
Protocol type	WinCollect for Microsoft Exchange 2003 Microsoft Exchange protocol for Microsoft Exchange 2007, 2010, 2013, and 2016.
QRadar recorded event types	Outlook Web Access events (OWA) Simple Mail Transfer Protocol events (SMTP) Message Tracking Protocol events (MSGTRK)
Automatically discovered?	No
Included identity?	No
More information	Microsoft website ( <a href="http://www.microsoft.com">http://www.microsoft.com</a> )

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](#)

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

[“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 Security QRadar, configure Outlook Web Access (OWA) event logs.

## **Procedure**

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

## **Procedure**

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

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

## **Enabling SMTP logs on your Microsoft Exchange Server 2013, and 2016**

To prepare your Microsoft Exchange Server 2013 and 2016 to communicate with IBM Security 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:

Parameter	Description
<b>Enable message tracking log</b>	Enable or disable message tracking on the server.
<b>Message tracking log path</b>	The value that you specify must be on the local Exchange server. If the folder does not exist, it is created when you click <b>Save</b> .

6. Click **Save**.

## Configuring a log source for Microsoft Exchange

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

### Before you begin

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

### About this task

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

Directory paths can be specified in the following formats:

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

### Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **Log Sources** icon.
4. In the **Log Source Name** field, type a name for the log source.

5. In the **Log Source Description** field, type a description for the log source.
6. From the **Log Source Type** list, select **Microsoft Exchange Server**.
7. From the **Protocol Configuration** list, select **Microsoft Exchange**.
8. Configure the log source parameters.

**Learn more about Microsoft Exchange log source parameters:**

Parameter	Description
Log Source Identifier	The IP address or host name to identify the Windows Exchange event source in the QRadar user interface.
Server Address	The IP address of the Microsoft Exchange server.
SMTP Log Folder Path	<p>The directory path to access the SMTP log files. Use one of the following directory paths:</p> <ul style="list-style-type: none"> <li>• For Microsoft Exchange 2003, use c\$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/ .</li> <li>• For Microsoft Exchange 2007, use c\$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/.</li> <li>• For Microsoft Exchange 2010, use c\$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/ProtocolLog/.</li> <li>• For Microsoft Exchange 2013, use c\$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/ProtocolLog/.</li> <li>• For Microsoft Exchange 2016, use c\$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/ProtocolLog/.</li> </ul>
OWA Log Folder Path	<p>The directory path to access the OWA log files. Use one of the following directory paths:</p> <ul style="list-style-type: none"> <li>• For Microsoft Exchange 2003, use c\$/WINDOWS/system32/LogFiles/W3SVC1/.</li> <li>• For Microsoft Exchange 2007, use c\$/WINDOWS/system32/LogFiles/W3SVC1/.</li> <li>• For Microsoft Exchange 2010, use c\$/inetpub/logs/LogFiles/W3SVC1/.</li> <li>• For Microsoft Exchange 2013, use c\$/inetpub/logs/LogFiles/W3SVC1/.</li> <li>• For Microsoft Exchange 2016, use c\$/inetpub/logs/LogFiles/W3SVC1/.</li> </ul>

Parameter	Description
MSGTRK Log Folder Path	The directory path to access message tracking log files. Message tracking is only available on Microsoft Exchange 2007 servers assigned the Hub Transport, Mailbox, or Edge Transport server role. Use one of the following directory paths: <ul style="list-style-type: none"> <li>For Microsoft Exchange 2007, use c\$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/MessageTracking/.</li> <li>For Microsoft Exchange 2010, use c\$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/MessageTracking/.</li> <li>For Microsoft Exchange 2013, use c\$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/MessageTracking/.</li> <li>For Microsoft Exchange 2016, use c\$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/MessageTracking/.</li> </ul>
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 Security 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 368. Microsoft Hyper-V DSM specifications*

Specification	Value
Manufacturer	Microsoft
DSM	Microsoft Hyper-V
RPM file name	DSM-MicrosoftHyperV-build_number.rpm
Supported versions	v2008 and v2012
Protocol	WinCollect
QRadar recorded events	All relevant events
Automatically discovered	No
Includes identity	No
More information	<a href="http://technet.microsoft.com/en-us/windowsserver/dd448604.aspx">http://technet.microsoft.com/en-us/windowsserver/dd448604.aspx</a>

## Microsoft Hyper-V DSM integration process

You can integrate Microsoft Hyper-V DSM with IBM Security 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 Security 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”

## Configuring a Microsoft Hyper-V log source in QRadar

To collect Microsoft Hyper-V events, configure a log source in IBM Security 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 Security QRadar accepts RADIUS events by using syslog.

## About this task

You can integrate Internet Authentication Service (IAS) or Network Policy Server (NPS<sup>®</sup>) logs with QRadar by using WinCollect. For more information, see the *IBM Security 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 Security 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.”
- Configure WinCollect to forward IIS events to QRadar. For more information, go to Log Sources for WinCollect agents in the *IBM Security QRadar WinCollect User Guide*. ([https://www.ibm.com/support/knowledgecenter/SS42VS\\_7.2.8/com.ibm.wincollect.doc/c\\_ug\\_wincollect\\_log\\_sources.html](https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.wincollect.doc/c_ug_wincollect_log_sources.html)).

*Table 369. Supported log types for Microsoft IIS 6.0 - IIS 10.0*

Method of Import	Supported Log Type
IIS Protocol	HTTP
WinCollect	SMTP, NNTP, FTP, HTTP

## 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 Security 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

- Log in to your Microsoft Information Services (IIS) Manager.
- Expand **IIS Manager > Local Computer > Sites**.
- Select **Web Site**.
- Double-click the **Logging** icon.
- Select **W3C** as the log file format from the Log File window.
- Click the **Select Fields** push button.
- From the list of properties, select check boxes for the following W3C properties:

Table 370. Required Properties for IIS event logs

IIS 6.0 Required Properties	IIS 7.0/7.5 Required Properties	IIS 8.0/8.5 Required Properties	IIS 10 Required Properties
Date (date)	Date (date)	Date (date)	Date (date)
Time (time)	Time (time)	Time (time)	Time (time)
Client IP Address (c-ip)	Client IP Address (c-ip)	Client IP Address (c-ip)	Client IP Address (c-ip)
User Name (cs-username)	User Name (cs-username)	User Name (cs-username)	User Name (cs-username)
Server IP Address (s-ip)	Server IP Address (s-ip)	Server IP Address (s-ip)	Server IP Address (s-ip)
Server Port (s-port)	Server Port (s-port)	Server Port (s-port)	Server Port (s-port)
Method (cs-method)	Method (cs-method)	Method (cs-method)	Method (cs-method)
URI Stem (cs-uri-stem)	URI Stem (cs-uri-stem)	URI Stem (cs-uri-stem)	URI Stem (cs-uri-stem)
URI Query (cs-uri-query)	URI Query (cs-uri-query)	URI Query (cs-uri-query)	URI Query (cs-uri-query)
Protocol Status (sc-status)	Protocol Status (sc-status)	Protocol Status (sc-status)	Protocol Status (sc-status)
Protocol Version (cs-version)	User Agent (cs(User-Agent))	User Agent (cs(User-Agent))	User Agent (cs(User-Agent))
User Agent (cs(User-Agent))			

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 Security 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 371. Microsoft IIS protocol parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source.
<b>Server Address</b>	Type the IP address of the Microsoft IIS server.
<b>Username</b>	Type the user name that is required to access the Microsoft IIS server.
<b>Password</b>	Type the password that is required to access the Microsoft IIS server.

Table 371. Microsoft IIS protocol parameters (continued)

Parameter	Description
<b>Confirm Password</b>	Confirm the password that is required to access the Microsoft IIS server.
<b>Domain</b>	Type the domain that is required to access the Microsoft IIS server.
<b>Folder Path</b>	<p>Type the directory path to access the IIS log files. The default is /WINDOWS/system32/LogFiles/W3SVC1/</p> <p>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.</p> <p>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.</p>
<b>File Pattern</b>	<p>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 LOG)</p> <p>For example, 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: <a href="http://download.oracle.com/javase/tutorial/essential/regex/">http://download.oracle.com/javase/tutorial/essential/regex/</a></p>
<b>Recursive</b>	Select this check box if you want the file pattern to search sub folders. By default, the check box is selected.
<b>Polling Interval (s)</b>	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.

9. Click **Save**.
10. The Microsoft IIS protocol configuration is complete.

## Configuring a Microsoft IIS log source

IBM Security 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 372. Microsoft IIS syslog configuration*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source.

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 Security QRadar accepts events by using syslog.

You can integrate Microsoft ISA Server with QRadar by using WinCollect. For more information, see the *IBM Security QRadar WinCollect User Guide*.

**Note:** The Microsoft ISA DSM also supports events from Microsoft Threat Management Gateway by using WinCollect.

---

## Microsoft Office 365

The IBM Security 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 373. Microsoft Office 365 DSM specifications*

Specification	Value
Manufacturer	Microsoft
DSM name	Microsoft Office 365
RPM file name	DSM-MicrosoftOffice365-Qradar_version-build_number.noarch.rpm
Supported versions	N/A
Protocol	Office 365 REST API
Event format	JSON
Recorded event types	Exchange Audit, SharePoint Audit, Azure Active Directory Audit, Service Communications
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Microsoft website ( <a href="https://www.microsoft.com">https://www.microsoft.com</a> )

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 on your QRadar Console:
  - Protocol Common RPM
  - Office 365 REST API Protocol RPM
  - Microsoft Office 365 DSM RPM
2. Register an application in Azure Active Directory.

3. Add a Microsoft Office 365 log source on the QRadar Console. The following table describes the parameters that require specific values for Microsoft Office 365 event collection:

*Table 374. Microsoft Office 365 log source parameters*

Parameter	Value
Log Source type	Microsoft Office 365
Protocol Configuration	Office 365 REST API
Log Source Identifier	<p>A unique identifier for the log source.</p> <p>The <b>Log Source Identifier</b> can be any valid value and does not need to reference a specific server. The <b>Log Source Identifier</b> can be the same value as the <b>Log Source Name</b>. If you have 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.</p>
Client ID	In your application configuration of Azure Active Directory, this parameter is under <b>Client ID</b> .
Client Secret	In your application configuration of Azure Active Directory, this parameter is under <b>Keys</b> .
Tenant ID	Used for Azure AD authentication.
Event Filter	<p>The type of audit events to retrieve from Microsoft Office.</p> <ul style="list-style-type: none"> <li>• Azure Active Directory</li> <li>• Exchange</li> <li>• SharePoint</li> <li>• Service Communications</li> </ul>
Use Proxy	<p>For QRadar to access the Office 365 Management APIs, all traffic for the log source travels through configured proxies.</p> <p>Configure the <b>Proxy Server</b>, <b>Proxy Port</b>, <b>Proxy Username</b>, and <b>Proxy Password</b> fields.</p> <p>If the proxy does not require authentication, keep the <b>Proxy Username</b> and <b>Proxy Password</b> fields empty.</p>
Automatically Acquire Server Certificate(s)	<p>Automatically downloads the server certificates and begins trusting the target server when selected. You can disable this parameter and manually download server certificates.</p> <p><b>Note:</b> When manually downloading certificates for Microsoft Office 365, you must download certificates from both <code>manage.office.com</code> and <code>login.windows.net</code>.</p>
EPS Throttle	<p>The maximum number of events per second.</p> <p>The default is 5000.</p>

The following table provides a sample event message for the Microsoft Office 365 DSM:

Table 375. Microsoft Office 365 sample message supported by the Microsoft Office 365 service

Event name	Low level category	Sample log message
Update user-fail	Update Activity Failed	<pre>{"CreationTime": "2016-05-05T08:53:46", "Id": "xxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "Operation": "Update user.", "OrganizationId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxx", "RecordType": 8, "ResultStatus": "fail", "UserKey": "Not Available", "UserType": 6, "Workload": "AzureActiveDirectory", "ObjectId": "xxxxxxxxxxxxxx", "UserId": "xxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "AzureActiveDirectoryEventType": 1, "ExtendedProperties": [{"Name": "MethodExecutionResult.", "Value": "Microsoft.Online.Workflows.ValidationException"}], "Actor": [{"ID": "x-xxxx-xxxx-xxxx-xxxxxx", "Type": 4}, {"ID": "xxxxxx_xxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxx", "Type": 2}], "ActorContextId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxx", "InterSystemsId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxx", "IntraSystemId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "Target": [{"ID": "x-xxxx-xxxx-xxxxxx", "Type": 2}, {"ID": "username@example.com", "Type": 1}, {"ID": "1706BDBF", "Type": 3}], "TargetContextId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"}</pre>
Site permissions modified	Update Activity Succeeded	<pre>{"CreationTime": "2015-10-20T15:54:05", "Id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "Operation": "SitePermissionsModified", "OrganizationId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxx", "RecordType": 4, "UserKey": "(empty)", "UserType": 0, "Workload": "SharePoint", "ClientIP": "&lt;IP_address&gt;", "ObjectId": "https://example.com/url", "UserId": "SHAREPOINT\\system", "EventSource": "SharePoint", "ItemType": "Web", "Site": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "UserAgent": "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0"}</pre>

#### Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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 Office 365 to communicate with QRadar

## Procedure

1. Run the Azure Active Directory PowerShell cmdlet. For more information, go to How to install and configure Azure PowerShell (<https://azure.microsoft.com/en-us/documentation/articles/powershell-install-configure/>).

**Tip:** The following table shows specific parameters that contain the same values in both QRadar and Microsoft.

Table 376. QRadar log source parameters and Microsoft parameters

QRadar log source parameter name	Microsoft parameter name
Client ID	Application ID
Client Secret	Key value
Tenant ID	Tenant ID

2. To obtain the **Tenant ID** of the tenant that is subscribed to Microsoft Office 365, type the following commands:

```
import-module MSOnline
$userCredential = Get-Credential
Connect-MsolService -Credential $userCredential
Get-MsolAccountSku | % {$_.AccountObjectID}
```

3. Use Azure Management Portal to register an application in Azure Active Directory. Sign in with the credentials of the tenant that is subscribed to Microsoft Office 365.

- a. Click **Active Directory**.
- b. Select **App registrations** and click **Add**.
- c. Select the **Create** blade.
- d. Enter a name for the application.
- e. For the Application type, select **Web app / API**.
- f. For the **Sign-on URL** field, type the following address: <http://localhost> (<http://localhost>)
- g. Click **Create**.
- h. Select the newly created application in Azure AD.

4. Configure the application properties.

- a. In the Settings blade, select **Properties**.
- b. Verify that **Multi-Tenanted** is set to NO.
- c. Copy and store the **Application ID** for future use. Use this value for the **Client ID** when you configure a log source.
- d. Save the configuration.

5. Generate a client secret for the application.

- a. In the Settings blade, select **Keys**.
- b. Enter a value for the key description.
- c. Click **Duration** and choose either **In 1 year**, **In 2 years**, or **Never expires**.
- d. Save the configuration. The client secret displays after the configuration is saved.
- e. Copy and store the **Key value**, as it cannot be retrieved later. Use this value for the **Client Secret** when you configure a log source.

6. Specify the permissions that the application requires to access Office 365 Management APIs.

- a. In the Settings blade, select **Required permissions**.
- b. Click **Add**.

- c. In the Add API Access blade, click **Select an API**.
- d. Select **Office 365 Management APIs**. The Enable Access blade is displayed.
- e. Under Application Permissions, select the following options:
  - 1) **Read Activity data for your organization**
  - 2) **Read service health information for your organization**
- f. Under Delegated Permissions, select the following options:
  - 1) **Read Activity data for your organization**
  - 2) **Read service health information for your organization**
- g. Click **Save**.
- h. In the Required permissions blade, click **Grant Permissions**, and then select **Yes**.

## Configuring Microsoft Office 365 to communicate with QRadar using the Classic Azure Management interface

Before you can configure a log source for Microsoft Office 365, you might need to request that Microsoft enables content subscriptions for your **Tenant ID**. By enabling content subscription, QRadar can retrieve data from management activity APIs.

### Before you begin

The **Tenant ID**, **Client ID**, and **Client Secret** are required.

### Procedure

1. Run 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. To obtain the **Tenant ID** of the tenant that is subscribed to Microsoft Office 365, type the following commands:
 

```
import-module MSOnline
$userCredential = Get-Credential
Connect-MsolService -Credential $userCredential
Get-MsolAccountSku | % {$_.AccountObjectID}
```
3. Use Azure Management Portal to register an application in Azure Active Directory.
  - a. To sign in Azure Management Portal, use the credentials of the tenant that is subscribed to Microsoft Office 365
  - b. Click **Active Directory**.
  - c. Select the directory name where the new application is registered under.
  - d. On the directory page, select **Applications**.
  - e. Click **Add**.
  - f. Select **Add an application my organization is developing**.
  - g. Enter a name for the application.
  - h. For the type, select **Web application and/or web API**.
  - i. For the **Sign-on URL** field, type the following:  
`http://localhost`
  - j. For the **App ID URL**, enter a unique identifier in the form of a URL for the application. An example of a unique identifier is the following URL: `http://company_name.onmicrosoft.com/QRadarApp`.
4. Configure the application properties.
  - a. Select the newly created application in Azure AD.

- b. Select **Configure**.
  - c. Verify that the **Application is Multi-Tenant** option is set to **NO**.
  - d. Copy the client ID for future use.
  - e. Save the configuration.
5. Generate a client secret for the application.
    - a. Under **Keys**, click **Select Duration**.
    - b. Choose either 1 year or 2 years.
    - c. Save the configuration.

The client secret displays after the configuration is saved. Copy and store the client secret because it appears only once and cannot be retrieved.

6. Specify the permissions that the application requires to access Office 365 Management APIs.
  - a. Under **Permissions to other applications**, select **Add application**.
  - b. Select **Office 365 Management APIs**.
  - c. Click the check mark to save the selection.
  - d. Under **Application Permissions and Delegated Permissions**, select the following options:
    - **Read Activity data for your organization**
    - **Read service health information for your organization**
    - **Read activity reports for your organization**
  - e. Save the configuration.

The application configuration in Azure AD is complete. You can create a log source for Microsoft Office 365 in QRadar. For more information, see Getting started with Office 365 Management APIs (<https://msdn.microsoft.com/EN-US/library/office/dn707383.aspx>).

---

## Microsoft Operations Manager

The Microsoft Operations Manager DSM for IBM Security 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:

### 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. From the **Log Source Type** list, select Microsoft Operations Manager.

- From the **Protocol Configuration** list, select **JDBC**.

The JDBC protocol parameters appear.

- Configure the following values:

*Table 377. Microsoft Operations Manager JDBC parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the identifier for the log source. Type the log source identifier in the following format:  <i>&lt;MOM Database&gt;@&lt;MOM Database Server IP or Host Name&gt;</i>  Where: <ul style="list-style-type: none"> <li>• <i>&lt;MOM Database&gt;</i> is the database name, as entered in the Database Name parameter.</li> <li>• <i>&lt;MOM Database Server IP or Host Name&gt;</i> is the host name or IP address for this log source, as entered in the IP or Host name parameter.</li> </ul>
<b>Database Type</b>	From the list, select <b>MSDE</b> .
<b>Database Name</b>	Type <b>OnePoint</b> as the name of the Microsoft Operations Manager database.
<b>IP or Hostname</b>	Type the IP address or host name of the Microsoft Operations Manager SQL Server.
<b>Port</b>	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 <b>Database Instance</b> when MSDE is used as the database type, you must leave the <b>Port</b> parameter blank in your configuration.
<b>Username</b>	Type the user name that is required to access the database.
<b>Password</b>	Type the password that is required to access the database. The password can be up to 255 characters in length.
<b>Confirm Password</b>	Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the <b>Password</b> parameter.
<b>Authentication Domain</b>	If you select <b>MSDE</b> as the <b>Database Type</b> and the database is configured for Windows, you must define the Window Authentication Domain. Otherwise, leave this field blank.
<b>Database Instance</b>	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 <b>Database Instance</b> parameter blank in your configuration.
<b>Table Name</b>	Type <b>SDKEventView</b> as the name of the table or view that includes the event records.

Table 377. Microsoft Operations Manager JDBC parameters (continued)

Parameter	Description
Select List	Type * for all fields from the table or view.  You can use a comma-separated list to define specific fields from tables or views, if you need it for your configuration. The list must contain the field that is defined in the <b>Compare Field</b> 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 TimeStored as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling.  The <b>Start Date and Time</b> parameter must be formatted as yyyy-MM-dd HH:mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select this check box to use prepared statements.  Prepared statements allow the JDBC protocol source to set up the SQL statement 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.
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 that are entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the <b>Use Named Pipe Communications</b> 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.
Database Cluster Name	If you select the <b>Use Named Pipe Communication</b> check box, the <b>Database Cluster Name</b> 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.

**Note:** 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.

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

**Related tasks:**

“Adding a DSM” on page 4

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

“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 Security 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.”
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 663.

**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 Security 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 Security 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 Security 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:  
`ssms`
  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:
- ```
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 **dbo_datareader** 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 for a database view

IBM Security 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. 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 378. Microsoft SharePoint JDBC parameters

| Parameter | Description |
|------------------------------|--|
| Log Source Identifier | Type the identifier for the log source. Type the log source identifier in the following format:

<i><SharePoint Database>@<SharePoint Database Server IP or Host Name></i>

Where: <ul style="list-style-type: none">• <i><SharePoint Database></i> is the database name, as entered in the Database Name parameter.• <i><SharePoint Database Server IP or Host Name></i> is the host name or IP address for this log source, as entered in the IP or Hostname parameter. |
| Database Type | From the list, select MSDE . |
| Database Name | Type 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. |
| Port | Type the port number that is used by the database server. The default port for MSDE is 1433.

The JDBC configuration port must match the listener port of the Microsoft 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. |
| Username | Type the user name the log source can use to access the Microsoft SharePoint database. |
| Password | Type the password the log source can use to access the Microsoft SharePoint 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 select MSDE as the Database Type and the database is configured for Windows, you must define the Window Authentication Domain. Otherwise, leave this field blank. |
| Database Instance | 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 you block access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration. |
| Table Name | Type AuditEvent as the name of the table or view that includes the event records. |

Table 378. Microsoft SharePoint JDBC parameters (continued)

| Parameter | Description |
|-------------------------------------|--|
| Select List | Type * for all fields from the table or view.

You can use a comma-separated list to define specific fields from tables or views, if 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(.) |
| Compare Field | Type EventTime as the compare field. The compare field is used to identify new events added between queries to the table. |
| Start Date and Time | Optional. Type the start date and time for database polling.

The Start Date and Time parameter must be formatted as yyyy-MM-dd HH: mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval. |
| Use Prepared Statements | Select the Use Prepared Statements 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. |
| Polling Interval | 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. |
| EPS Throttle | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS. |
| Use Named Pipe Communication | 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. |
| Use NTLMv2 | Select the Use NTLMv2 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 Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication. |
| Use SSL | 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. |
| Database Cluster Name | If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly. |

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**.

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 379. Microsoft SharePoint JDBC parameters

| Parameter | Description |
|------------------------------|---|
| Log Source Identifier | Type the identifier for the log source. Type the log source identifier in the following format:

<i><SharePoint Database>@<SharePoint Database Server IP or Host Name></i>

Where: <ul style="list-style-type: none"> • <i><SharePoint Database></i> is the database name, as entered in the Database Name parameter. • <i><SharePoint Database Server IP or Host Name></i> is the host name or IP address for this log source, as entered in the IP or Hostname parameter. |
| Database Type | From the list, select MSDE . |
| Database Name | Type 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. |
| Port | Type the port number that is used by the database server. The default port for MSDE is 1433.

The JDBC configuration port must match the listener port of the Microsoft SharePoint database. The Microsoft SharePoint database must have incoming TCP connections that are enabled to communicate with IBM Security 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. |
| Username | Type the user name the log source can use to access the Microsoft SharePoint database. |
| Password | Type the password the log source can use to access the Microsoft SharePoint database.

The password can be up to 255 characters in length. |

Table 379. Microsoft SharePoint JDBC parameters (continued)

| Parameter | Description |
|-------------------------------------|---|
| 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 select MSDE as the Database Type and the database is configured for Windows Authentication, you must specify the Windows Authentication Domain. Otherwise, leave this field blank. |
| Database Instance | 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. |
| Predefined Query | From the list, select Microsoft SharePoint . |
| Use Prepared Statements | Select the Use Prepared Statements 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. |
| Start Date and Time | 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. |
| Polling Interval | 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. |
| EPS Throttle | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS. |
| Use Named Pipe Communication | 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. |
| Use NTLMv2 | 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. |
| Use SSL | 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. |
| Database Cluster Name | If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly. |

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

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

Table 380. Microsoft SQL Server DSM

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

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

Syslog

The IBM Security 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, and 2014 Enterprise.

WinCollect

You can integrate Microsoft SQL Server 2000, 2005, 2008, 2012, and 2014 with QRadar by using WinCollect to collect ERRORLOG messages from the databases that are managed by your Microsoft SQL Server. For more information about WinCollect, go to the IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.wincollect.doc/c_wincollect_overview_new.html).

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 600

The IBM Security 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 601

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

“Adding a DSM” on page 4

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

“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.”

About this task

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

Procedure

1. From the Microsoft SQL Server Management Studio navigation menu, select one of the following options:
 - **Security > Server Audit Specifications**
 - **<Database> > Security > Database Audit Specifications**
2. Right-click **Server Audit Specifications**, and then select one of the following options:
 - **New Server Audit Specifications**
 - **New Database Audit Specifications**

3. In the **Name** field, type a name for the new audit file.
4. From the **Audit** list, select the audit object that you created.
5. In the **Actions** pane, add actions and objects to the server audit.
6. Click **OK**.
7. Right-click your server audit specification and select one of the following options:
 - **Enable Server Audit Specification**
 - **Enable Database Audit Specification**

Creating a Microsoft SQL Server database view

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

Procedure

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

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

For example:

```
create view dbo.AuditData as
  SELECT * FROM sys.fn_get_audit_file
  ('C:\inetpub\logs\SQLAudits*',default,default);
GO
```

3. From the Standard toolbar, click **Execute**.

Configuring a Microsoft SQL Server log source

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

Procedure

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

| Parameter | Description |
|------------------------------|--|
| Log Source Identifier | <p>Type the identifier for the log source in the following format:</p> <p><SQL Database>@<SQL DB Server IP or Host Name></p> <p>Where:</p> <p><SQL Database> is the database name, as entered in the Database Name parameter.</p> <p><SQL DB Server IP or Host Name> is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.</p> |
| Database Type | From the list, select MSDE . |
| Database Name | Type Master as the name of the Microsoft SQL database. |
| IP or Hostname | Type the IP address or host name of the Microsoft SQL server. |
| Port | <p>Type the port number that is used by the database server. The default port for MSDE is 1433.</p> <p>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.</p> <p>Important: If you define a Database Instance when you are using MSDE as the Database Type, you must leave the Port parameter blank in your configuration.</p> |
| Username | Type the user name to access the SQL database. |
| Password | Type the password to access the SQL database. |
| Confirm Password | Type the password to access the SQL database. |
| Authentication Domain | If you select MSDE as the Database Type and the database is configured for Windows, you must define a Window Authentication Domain . Otherwise, leave this field blank. |
| Database Instance | <p>Optional: If you have multiple SQL server instances on your database server, type the database instance.</p> <p>Important: If you have a non-standard port in your database configuration, or access is blocked to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank.</p> |
| Table Name | Type dbo.AuditData as the name of the table or view that includes the audit event records. |

| Parameter | Description |
|-------------------------------------|--|
| Select List | <p>Type * for all fields from the table or view.</p> <p>You can use a comma-separated list to define specific fields from tables or views. The list must contain the field that is defined in the Compare Field parameter. The comma-separated list can be a maximum of 255 characters. You can include the special characters, dollar sign (\$), number sign (#), underscore (_), en dash (-), and period (.).</p> |
| Compare Field | <p>Type event_time in the Compare Field parameter. The Compare Field identifies new events that are added between queries, in the table.</p> |
| Start Date and Time | <p>Optional: Type the start date and time for database polling.</p> <p>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.</p> |
| Use Prepared Statements | <p>Select this check box to use prepared statements</p> <p>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.</p> <p>Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</p> |
| Polling Interval | <p>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.</p> <p>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.</p> |
| EPS Throttle | <p>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</p> |
| Use Named Pipe Communication | <p>Clear the Use Named Pipe Communications check box.</p> <p>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.</p> |

| Parameter | Description |
|------------------------------|---|
| Database Cluster Name | If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name. |

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

Microsoft System Center Operations Manager

A QRadar Microsoft System Center Operations Manager (SCOM) DSM accepts SCOM events by polling the OperationsManager 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 OperationsManager 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. 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. From the **Log Source Type** list, select Microsoft SCOM.
5. From the **Protocol Configuration** list, select **JDBC**.
The JDBC protocol is displayed.
6. Configure the following values:

Table 381. Microsoft SCOM JDBC parameters

| Parameter | Description |
|------------------------------|---|
| Log Source Identifier | Type the identifier for the log source. Type the log source identifier in the following format:

<code><SCOM Database>@<SCOM Database Server IP or Host Name></code>

Where: <ul style="list-style-type: none"> • <code><SCOM Database></code> is the database name, as entered in the Database Name parameter. • <code><SCOM Database Server IP or Host Name></code> is the host name or IP address for this log source, as entered in the IP or Hostname parameter. |

Table 381. Microsoft SCOM JDBC parameters (continued)

| Parameter | Description |
|--------------------------------|--|
| Database Type | From the list, select MSDE . |
| Database Name | Type OperationsManager as the name of the Microsoft SCOM database. |
| IP or Hostname | Type the IP address or host name of the Microsoft SCOM SQL Server. |
| Port | <p>Type the port number that is used by the database server. The default port for MSDE is 1433.</p> <p>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.</p> <p>If you define a Database Instance when MSDE is used as the database type, you must leave the Port parameter blank in your configuration.</p> |
| 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 parameter. |
| Authentication Domain | If you select MSDE as the Database Type and the database is configured for Windows, you must define a Window Authentication Domain. Otherwise, leave this field blank. |
| Database Instance | <p>Optional. Type the database instance, if you have multiple SQL server instances on your database server.</p> <p>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.</p> |
| Table Name | Type EventView as the name of the table or view that includes the event records. |
| Select List | <p>Type * for all fields from the table or view.</p> <p>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(.)</p> |
| Compare Field | Type TimeAdded as the compare field. The compare field is used to identify new events added between queries to the table. |
| Start Date and Time | <p>Optional. Type the start date and time for database polling.</p> <p>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.</p> |
| Use Prepared Statements | <p>Select this check box to use prepared statements.</p> <p>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.</p> <p>Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</p> |

Table 381. Microsoft SCOM JDBC parameters (continued)

| Parameter | Description |
|-------------------------------------|--|
| 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 that are entered without an H or M poll in seconds. |
| EPS Throttle | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS. |
| Use Named Pipe Communication | 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. |
| Database Cluster Name | If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly. |

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.

7. Click **Save**.

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

Related tasks:

“Adding a DSM” on page 4

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

“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 Security Event Log

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

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

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

All events, including Sysmon, are supported.

Related tasks:

“Enabling MSRPC on Windows hosts” on page 674

To enable communication between your Windows host and IBM Security 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” on page 678

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

Verifying MSRPC Protocol

For most users, the Microsoft Security Event Log over MSRPC protocol is provided automatically to the IBM Security 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”

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 Security QRadar over MSRPC, configure the Remote Procedure Calls (RPC) settings on the Windows host for the Microsoft Remote Procedure Calls (MSRPC) protocol.

Before you begin

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

About this task

Based on performance tests on an IBM Security QRadar 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.

| Specification | Value |
|---------------|-----------|
| Manufacturer | Microsoft |

| Specification | Value |
|---|---|
| Protocol type | <p>The operating system dependant type of the remote procedure protocol for collection of events.</p> <p>Select one of the following options from the Protocol Type list:</p> <p>MS-EVEN6
The default protocol type for new log sources.</p> <p>The protocol type that is used by QRadar to communicate with Windows Vista and Windows Server 2008 and later.</p> <p>MS-EVEN (for Windows XP/2003)
The protocol type that is used by QRadar to communicate with Windows XP and Windows Server 2003.</p> <p>Windows XP and Windows Server 2003 are not supported by Microsoft. The use of this option might not be successful.</p> <p>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.</p> <p>Upgrade to the MS_EVEN6 or the MS-EVEN (for Windows XP/2003) protocol type.</p> |
| Supported versions | <p>Windows Server 2016</p> <p>Windows Server 2012 (most recent)</p> <p>Windows Server 2012 Core</p> <p>Windows Server 2008 (most recent)</p> <p>Windows Server 2008 Core</p> <p>Windows 10 (most recent)</p> <p>Windows 8 (most recent)</p> <p>Windows 7 (most recent)</p> <p>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 |
| Special features | Supports encrypted events by default. |

| Specification | Value |
|------------------------------|--|
| Required permissions | <p>The log source user must be a member of the Event Log Readers group. If this group is not configured, then domain admin privileges are required in most cases to poll a Windows event log across a domain. In some cases, the Backup operators group can also be used depending on how Microsoft Group Policy Objects are configured.</p> <p>Windows XP and 2003 operating system users require read access to the following registry keys:</p> <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language • HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion |
| Supported event types | <p>Application</p> <p>System</p> <p>Security</p> <p>DNS Server</p> <p>File Replication</p> <p>Directory Service logs</p> |
| Windows service requirements | <p>For Windows Server 2008 and Windows Vista, use the following services:</p> <ul style="list-style-type: none"> • Remote Procedure Call (RPC) • RPC Endpoint Mapper <p>For Windows 2003, use the Remote Registry and Server.</p> |
| Windows port requirements | <p>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:</p> <p>For Windows Server 2008 and Windows Vista, use the following ports:</p> <ul style="list-style-type: none"> • TCP port 135 • TCP port that is dynamically allocated for RPC, above 49152 <p>For Windows 2003, use the following ports:</p> <ul style="list-style-type: none"> • TCP port 445 • TCP port 139 |
| Automatically discovered? | No |
| Includes identity? | Yes |
| Includes custom properties? | A security content pack with Windows custom event properties is available on IBM Fix Central. |

| Specification | Value |
|--------------------------------|--|
| Required RPM files | PROTOCOL-WindowsEventRPC-QRadar_release-
Build_number.noarch.rpm

DSM-MicrosoftWindows-QRadar_release-
Build_number.noarch.rpm

DSM-DSMCommon-QRadar_release-Build_number.noarch.rpm |
| More information | Microsoft support (http://support.microsoft.com/) |
| Troubleshooting tool available | 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 |

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 Security 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 382. *MSRPC test tool flags*

| Flags | Description |
|------------------|--|
| -? or --help | Displays the help and usage information for the MSRPC tool. |
| -b | Displays debugging information, if available. |
| -d <domain> | Active Directory Domain, or hostname if in a workgroup. |
| -e <protocol> | EventLog Remoting protocol.
Values: MSEVEN, MSEVEN6, and AUTO
Default: AUTO |
| -h <hostname/ip> | Hostname or IP address of the Windows host. |
| -p <password> | Password |
| -u <username> | Username |
| -w <poll> | Polling mode. Specify one or more event log channels.
Values: Security, System, Application, DNS Server, File Replication Service, Directory Service
Separate multiple values by comma. Example: Application, Security.
Default: Security |

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 Security QRadar, you can use Windows Management Instrumentation (WMI).

Before you begin

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

About this task

The Microsoft Security Event Log protocol (WMI) is not recommended for event collection where more than 50 EPS is required or for servers over slow network connections, such as satellite or slow WAN

networks. Network delays that are created by slow connections decrease the EPS throughput available to remote servers. Faster connections can use MSRPC as an alternative. If it is not possible to decrease your network round-trip delay time, we recommend that you use an agent, such as WinCollect.

| Specification | Value |
|------------------------------------|--|
| Manufacturer | Microsoft |
| DSM name | Windows Security Event Log |
| Supported versions | Windows Server 2003 (most recent)
Windows Server 2008 (most recent)
Windows 2012 (most recent)
Windows 7
Windows 8 (64-bit versions)
Windows Vista
Windows XP |
| Special features | Supports encrypted events by default. |
| Intended application | Agentless event collection for Windows operating systems over WMI that is capable of 50 EPS per log source.
Important: This is a legacy protocol. In most cases, new log sources should be configured by using the Microsoft Security Event Log over MSRPC protocol. |
| Special configuration instructions | Configuring DCOM and WMI to Remotely Retrieve Windows 7 Events (http://www.ibm.com/support/docview.wss?uid=swg21678809)
Configuring DCOM and WMI to Remotely Retrieve Windows 8 and Windows 2012 Events (http://www.ibm.com/support/docview.wss?uid=swg21681046) |
| Windows port requirements | You must ensure that external firewalls between the Windows host and the QRadar appliance are configured to allow incoming and outgoing TCP connections on the following ports:
<ul style="list-style-type: none"> • TCP port 135 (all operating system versions) • TCP port that is dynamically allocated above 49152 (required for Vista and above operating systems) • TCP port that is dynamically allocated above 1024 (required for Windows XP & 2003) • TCP port 445 (required for Windows XP & 2003) • TCP port 139 (required for Windows XP & 2003) |
| Windows service requirements | The following services must be configured to start automatically: <ul style="list-style-type: none"> • Remote Procedure Call (RPC) • Remote Procedure Call (RPC) Locator • RPC Endpoint Mapper • Remote Registry • Server • Windows Management Instrumentation |

| Specification | Value |
|---------------------------------|--|
| Log source permissions | <p>The log source user must be a member of the Event Log Readers group. If this group is not configured, then domain admin privileges are required in most cases to poll a Windows event log across a domain. In some cases, the Backup operators group can also be used depending on how Microsoft Group Policy Objects are configured.</p> <p>The log source user must have access to following components:</p> <ul style="list-style-type: none"> • Window event log protocol DCOM components • Windows event log protocol name space • Appropriate access to the remote registry keys |
| Supported event types | <p>Application</p> <p>System</p> <p>Security</p> <p>DNS Server</p> <p>File Replication</p> <p>Directory Service logs</p> |
| Automatically discovered? | No, manual log source creation is required |
| Includes identity? | Yes |
| Includes custom properties? | A security content pack with Windows custom event properties is available on IBM Fix Central. |
| Required RPM files | <p>PROTOCOL-WinCollectWindowsEventLog-QRadar_release-
Build_number.noarch.rpm</p> <p>DSM-MicrosoftWindows-QRadar_release-
Build_number.noarch.rpm</p> <p>DSM-DSMCommon-QRadar_release-Build_number.noarch.rpm</p> |
| More information | Microsoft support (support.microsoft.com/) |
| Troubleshooting tools available | Yes, a WMI test tool is available in /opt/qradar/jars. |

Procedure

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

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

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

91 Motorola Symbol AP

The Motorola Symbol AP DSM for IBM Security QRadar records all relevant events forwarded from Motorola Symbol AP devices using syslog.

Configuring a log source

To integrate Motorola SymbolAP with IBM Security 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 SymbolAP 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 SymbolAP**.
9. Using the **Protocol Configuration** list, select **Syslog**.
The syslog protocol configuration is displayed.
10. Configure the following values:

Table 383. 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 Motorola SymbolAP appliance. |

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 Security 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.

92 Name Value Pair

The Name Value Pair DSM gives you the option to integrate IBM Security 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 384. Name Value Pair log format tags

| Tag | Description |
|--------------------------|---|
| DeviceType | Type NVP as the DeviceType . 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. |
| EventName | 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 <i>IBM Security QRadar User Guide</i> .
This is a required parameter. |
| EventCategory | 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. |
| SourceIp | Type the source IP address for the message. |
| SourcePort | Type the source port for the message. |
| SourceIpPreNAT | Type the source IP address for the message before Network Address Translation (NAT) occurred. |
| SourceIpPostNAT | Type the source IP address for the message after NAT occurs. |
| SourceMAC | Type the source MAC address for the message. |
| SourcePortPreNAT | Type the source port for the message before NAT occurs. |
| SourcePortPostNAT | Type the source port for the message after NAT occurs. |

Table 384. Name Value Pair log format tags (continued)

| Tag | Description |
|-------------------------------|---|
| DestinationIp | Type the destination IP address for the message. |
| DestinationPort | Type the destination port for the message. |
| DestinationIpPreNAT | Type the destination IP address for the message before NAT occurs. |
| DestinationIpPostNAT | Type the IP address for the message after NAT occurs. |
| DestinationPortPreNAT | Type the destination port for the message before NAT occurs. |
| DestinationPortPostNAT | Type the destination port for the message after NAT occurs. |
| DestinationMAC | Type the destination MAC address for the message. |
| DeviceTime | 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. |
| UserName | Type the user name that is associated with the event. |
| HostName | Type the host name that is associated with the event. Typically, this parameter is only associated with identity events. |
| GroupName | Type the group name that is associated with the event. Typically, this parameter is only associated with identity events. |
| NetBIOSName | Type the NetBIOS name that is associated with the event. Typically, this parameter is only associated with identity events. |
| Identity | 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 . |
| IdentityUseSrcIp | 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. |

Example 1

The following example parses all fields:

```
DeviceType=NVP EventName=Test
DestinationIpPostNAT=<IP_address>
DeviceTime=2007/12/14 09:53:49
SourcePort=1111 Identity=FALSE SourcePortPostNAT=3333
DestinationPortPostNAT=6666 HostName=testhost
DestinationIpPreNAT=<IP_address> SourcePortPreNAT=2222
DestinationPortPreNAT=5555 SourceMAC=<MAC_address>
SourceIp=<IP_address> SourceIpPostNAT=<IP_address>
NetBIOSName=<BIOS_name> DestinationMAC=<MAC_address>
EventCategory=Accept DestinationPort=4444
GroupName=testgroup SourceIpPreNAT=<IP_address>
UserName=<Username> DestinationIp=<IP_address>
```

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>
```

93 NCC Group DDoS Secure

The IBM Security 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 385. NCC Group DDoS Secure DSM specifications

| Specification | Value |
|-----------------------------|---|
| Manufacturer | NCC Group |
| DSM name | NCC Group DDoS Secure |
| RPM file name | DSM-NCCGroupDDoSSecure-QRadar_version-build_number.noarch.rpm |
| Supported versions | 5.13.1-2s to 5.16.1-0 |
| Protocol | Syslog |
| Event format | LEEF |
| Recorded event types | All events |
| Automatically discovered? | Yes |
| Includes identity? | No |
| Includes custom properties? | No |
| More information | NCC Group website (https://www.nccgroup.trust/uk/) |

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 386. NCC Group DDoS Secure log source parameters

| Parameter | Value |
|------------------------|-----------------------|
| Log Source type | NCC Group DDoS Secure |
| Protocol Configuration | Syslog |

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 387. NCC Group DDoS Secure sample message

| Event name | Low level category | Sample log message |
|------------------------------|--------------------|--|
| TCP Attack - Port Scan - END | Host Port Scan | <134>LEEF:1.0 NCCGroup DDoS Secure 5.16.2-1 4078 desc=TCP Attack - Port Scan sev=4 myip=<IP_address> proto=TCP scrPort =0 dstPort=0 src=<Source_IP_address> dst=<Destination_IP_address> cat= END devTime=2017-06-05 11: 26:00 devTimeFormat=yyyy-MM -dd HH:mm:ss end=2017-06-05 11:34:33 CurrentPps=0 PeakPps=14 totalPackets=243 realm=<Domain> action=DROP |

Related tasks:

"Adding a DSM" on page 4

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

"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 Security 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 Bandwidth** field, specify the expected normal peak bandwidth of the appliance.

94 NetApp Data ONTAP

IBM Security 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 Security QRadar WinCollect User Guide*.

95 Netskope Active

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

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

Table 388. Netskope Active DSM specifications

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

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

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

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

Table 389. Netskope Active log source parameters

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

Related tasks:

“Adding a DSM” on page 4

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

“Configuring QRadar to collect events from your Netskope Active system” on page 694

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 390. Netskope Active DSM log source parameters

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

Procedure

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

96 Niksun

The Niksun DSM for IBM Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
The syslog protocol configuration is displayed.
10. Configure the following values:

Table 391. 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 Niksun appliance. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
The log source is added to QRadar.

97 Nokia Firewall

The Check Point Firewall-1 DSM allows IBM Security 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 Security QRadar to integrate with a Nokia Firewall device, take the following steps:

1. Configure iptables on yourQRadar 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.
4. Optional. Configure a log source in QRadar.

Configuring IPtables

Nokia Firewalls require a TCP reset (rst) or a TCP acknowledge (ack) from IBM Security 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 Security 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 Security 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:

#### Syslog protocol parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source as an identifier for events from your Nokia Firewall appliance.

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 Security QRadar.

---

## Integration with a Nokia Firewall by using OPSEC

IBM Security 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.”
2. Configure a log source in QRadar for your Nokia Firewall using the OPSEC LEA protocol, see “Configuring an OPSEC log source” on page 700.

## Configuring a Nokia Firewall for OPSEC

You can configure Nokia Firewall by using OPSEC.

### Procedure

1. To create a host object for your IBM Security 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.”
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 Security 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 392. OPSEC/LEA protocol parameters*

Parameter	Description
<b>Log Source Identifier</b>	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.
<b>Server IP</b>	Type the IP address of the server.
<b>Server Port</b>	Type the port that is used for OPSEC communication. The valid range is 0 - 65,536 and the default is 18184.
<b>Use Server IP for Log Source</b>	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.
<b>Statistics Report Interval</b>	Type the interval, in seconds, during which syslog events are recorded in the <code>qradar.log</code> file.  The valid range is 4 - 2,147,483,648 and the default is 600.

Table 392. OPSEC/LEA protocol parameters (continued)

Parameter	Description
Authentication Type	<p>From the list, select the authentication type that you want to use for this LEA configuration. The options are <b>sslca</b> (default), <b>sslca_clear</b>, or <b>clear</b>. This value must match the authentication method that is used by the server. The following parameters appear if <b>sslca</b> or <b>sslca_clear</b> is selected as the authentication type:</p> <ul style="list-style-type: none"> <li>• <b>OPSEC Application Object SIC Attribute (SIC Name)</b> - 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=xxxxxxxx..xxxxxx. The name can be up to 255 characters in length and is case-sensitive.</li> <li>• <b>Log Source SIC Attribute (Entity SIC Name)</b> - Type the SIC name of the server, for example: cn=cp_mgmt,o=xxxxxxxx..xxxxxx. The name can be up to 255 characters in length and is case-sensitive.</li> <li>• <b>Specify Certificate</b> - 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.</li> </ul> <p>If you select the <b>Specify Certificate</b> check box, the <b>Certificate Filename</b> parameter is displayed:</p> <ul style="list-style-type: none"> <li>• <b>Certificate Filename</b> - This option appears only if <b>Specify Certificate</b> 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.</li> </ul> <p>If you clear the <b>Specify Certificate</b> check box, the following parameters appear:</p> <ul style="list-style-type: none"> <li>• <b>Certificate Authority IP</b> - Type the IP address of the SmartCenter server from which you want to pull your certificate.</li> <li>• <b>Pull Certificate Password</b> - Type the password that you want to use when a certificate is requested. The password can be up to 255 characters in length.</li> <li>• <b>OPSEC Application</b> - 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.</li> </ul>

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.



---

## 98 Nominum Vantio

The Nominum Vantio DSM for IBM Security 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. For more information about configuring LVP, see the *Vantio Administrator's Manual*.

Before you can integrate Nominum Vantio events with QRadar, you must install and configure the Vantio LEEF adapter. To obtain the Vantio LEEF adapter or request additional information, email Nominum at the following address: leefadapter@nominum.com.

---

## Configure the Vantio LEEF Adapter

You can install and configure your Vantio LEEF Adapter.

### Procedure

1. Use SSH to log in to your Vantio engine server.
  2. Install the Vantio LEEF Adapter:  

```
sudo yum install VantioLEEFAdapter-0.1-a.x86_64.rpm
```
  3. Edit the Vantio LEEF Adapter configuration file.  

```
usr/local/nom/sbin/VantioLEEFAdapter
```
  4. Configure the Vantio LEEF Adapter configuration to forward LEEF events to IBM Security QRadar:  

```
-qradar-dest-addr=<IP Address>
```

Where <IP Address> is the IP address of your QRadar Console or Event Collector.
  5. Save the Vantio LEEF configuration file.
  6. Type the following command to start the Vantio Adapter:  

```
usr/local/nom/sbin/VantioLEEFAdapter &
```
- The configuration is complete. The log source is added to QRadar as Nominum Vantio events are automatically discovered. Events forwarded to QRadar by the Vantio LEEF Adapter are displayed on the **Log Activity** tab of QRadar.

---

## Configuring a log source

IBM Security QRadar automatically discovers and creates a log source for syslog events from the Vantio LEEF Adapter. The following configuration steps are optional.

### About this task

To manually configure a log source for Nominum Vantio:

### 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 **Nominum Vantio**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

#### Syslog Parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source as an identifier for events from Nominum Vantio.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

---

## 99 Nortel Networks

Several Nortel Networks DSMs can be integrated with IBM Security QRadar.

---

### Nortel Multiprotocol Router

The Nortel Multiprotocol Router DSM for IBM Security 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” 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
```

- 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.

- Configure the level of syslog messages you want to send to your QRadar.

```
severity-mask all
```

- 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
```

- 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]
```

*Table 393. Syslog filters*

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

- 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 394. Syslog host log*

Host IP address	Configured State	Operational State	Time Sequencing	UDP Port	Facility Code	#Messages Sent
<IP_address1>	enabled	up	disabled	514	local0	1402

Table 394. Syslog host log (continued)

Host IP address	Configured State	Operational State	Time Sequencing	UDP Port	Facility Code	#Messages Sent
<IP_address2>	enabled	up	disabled	514	local0	131

15. Exit the command line interface:

a. Exit the current command line to return to the bcc command line:

```
exit
```

16. Exit the bcc 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

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

“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 Security 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

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

“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 Security 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

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

“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 Security 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 709.

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 709.

7. Enable the ability to send syslog messages:

```
state enable
```

8. Verify the syslog configuration for the host:

```
syslog 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 Security 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
system: info
fr: warning
ppp: warning
ipmux: warning
bundle: warning
qos: warning
hdlc: warning
local7: warning
vpn: warning
firewall: 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 Security 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.
3. Select **Secure Access Domain and Syslog** from the Navigation pane.  
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

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

“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 Security 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”
- “Integrate Nortel Switched Firewall by using OPSEC” on page 713

### Integrating Nortel Switched Firewall by using syslog

This method ensures the IBM Security 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](#)

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

[“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 Security 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 33](#)

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 Security 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 714](#)
- [“Configuring OPSEC for Nortel Switched Firewalls” on page 714](#)

## Configuring syslog for Nortel Switched Firewalls

This method ensures the IBM Security 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-local17): 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 Security 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 715.
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 33

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 Security QRadar system. The *lepipe* 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.  
The name that you type must be different from the name in “Reconfiguring the Check Point SmartCenter Server.”
7. From the **Host** drop-down menu, select the host object that you have created in “Reconfiguring the Check Point SmartCenter Server.”
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 Security 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**.  
The Detection & Prevention window is displayed.
3. Click **Edit** next to the intrusion policy you want to configure alerting option.  
The Edit Policy window is displayed.
4. Click **Alerting**.  
The Alerting window is displayed.
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

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

"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 Security 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

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

“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.



---

## 100 Novell eDirectory

The Novell eDirectory DSM for IBM Security 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](#)

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

[“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\xdasconfig.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.appenders.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.appenders.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.appenders.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.appenders.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.”
- To load the XDASv2 in Windows, see “Loading the XDASv2 on a Windows Operating System” on page 721.

**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 721.

---

## 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 721.

---

## 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**.
10. Close the Novell eDirectory Services window.

### 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."

---

## 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.
7. 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 Security 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 Security 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.

---

## 101 Observe IT JDBC

The IBM Security QRadar DSM for ObserveIT JDBC collects JDBC events from ObserveIT.

The following table identifies the specifications for the ObserveIT JDBC DSM:

*Table 395. ObserveIT JDBC DSM specifications*

Specification	Value
Manufacturer	ObserveIT
Product	ObserveIT JDBC
DSM RPM name	DSM-ObserveIT-QRadar_Version-Build_Number.noarch.rpm
Supported versions	v5.7 and later
Protocol	ObserveIT JDBC Log File Protocol
QRadar recorded events	The following event types are supported by ObserveIT JDBC: <ul style="list-style-type: none"><li>• Alerts</li><li>• User Activity</li><li>• System Events</li><li>• Session Activity</li><li>• DBA Activity</li></ul> The Log File Protocol supports User activity in LEEF logs.
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	ObserveIT website ( <a href="http://www.observeit-sys.com">http://www.observeit-sys.com</a> )

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 396. ObserveIT JDBC log source parameters*

Parameter	Description
Log Source type	ObserveIT

*Table 396. ObserveIT JDBC log source parameters (continued)*

Parameter	Description
Protocol Configuration	<b>DATABASE@HOSTNAME</b> where <b>DATABASE</b> must be a string that matches the text that was entered into the <b>Database Name</b> field and must not contain the @ character, and <b>HOSTNAME</b> must be a string that matches the text that was entered into the <b>IP or Hostname</b> field and must not contain the @ character.
Database name	ObserveIT
IP or Hostname	The IP address or host name of the ObserveIT system.
Port	The port on the ObserveIT host. The default is 1433.
Username	The user name that is required to connect to the ObserveIT MS SQL database
Password	The password that is required to connect to the ObserveIT MS SQL database.
Start Date and Time	Use the yyyy-MM-dd HH: mm format.
Polling Interval	The frequency by which to poll the database.
EPS Throttle	The event rate throttle in events per second.

*Table 397. Log file protocol parameters*

Parameter	Description
Protocol Configuration	Log file
Log Source Identifier	The IP address for the log source. This value must match the value that is configured in the <b>Server IP</b> parameter. The <b>log source identifier</b> must be unique for the log source type.
Service Type	From the list, select the protocol that you want to use when retrieving log files from a 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 <b>Remote IP or Hostname</b> field has the SFTP subsystem enabled.
Remote IP or Hostname	The IP address or host name of the device that stores your event log files.
Remote Port	If the remote host uses a non-standard port number, you must adjust the port value to retrieve events.
Remote User	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.
Remote Password	The password that is necessary to log in to the host.
Confirm Password	Confirmation of the password that is necessary to log in to the host.

Table 397. Log file protocol parameters (continued)

Parameter	Description
SSH Key File	The path to the SSH key, if the system is configured to use key authentication. When an SSH key file is used, the <b>Remote Password</b> field is ignored.
Remote Directory	For FTP, if the log files are in the remote user's home directory, you can leave the remote directory blank. A blank <b>remote directory</b> field supports systems where a change in the working directory (CWD) command is restricted.
SCP Remote File	If you selected <b>SCP</b> as the <b>Service Type</b> , you must type the file name of the remote file.
Recursive	This option is ignored for SCP file transfers.
FTP File Pattern	The regular expression (regex) required to identify the files to download from the remote host.
FTP Transfer Mode	For ASCII transfers over FTP, you must select <b>NONE</b> in the <b>Processor</b> field and <b>LINEBYLINE</b> in the <b>Event Generator</b> field.
Start Time	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 <b>Recurrence</b> value to establish when and how often the <b>Remote Directory</b> is scanned for files. Type the <b>start time</b> , based on a 12-hour clock, in the following format: HH:MM <AM/PM>.
Recurrence	The time interval to determine how frequently the remote directory is scanned for new event log files. The time interval can include values in hours (H), minutes (M), or days (D). For example, a recurrence of 2H scans the remote directory every 2 hours.
Run On Save	Starts the log file import immediately after you save the log source configuration. When selected, this check box clears the list of previously downloaded and processed files. After the first file import, the log file protocol follows the start time and recurrence schedule that is defined by the administrator.
EPS Throttle	The number of Events Per Second (EPS) that the protocol cannot exceed.
Processor	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.
Ignore Previously Processed File(s)	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.
Change Local Directory?	Changes the local directory on the Target Event Collector to store event logs before they are processed.

*Table 397. Log file protocol parameters (continued)*

Parameter	Description
Local Directory	The local directory on the Target Event Collector. The directory must exist before the log file protocol attempts to retrieve events.
File Encoding	The character encoding that is used by the events in your log file.
Folder Separator	The character that is used to separate folders for your operating system. Most configurations can use the default value in <b>Folder Separator</b> 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](#)

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

[“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.

---

## 102 Okta

The IBM Security QRadar DSM for Okta collects events by using the Okta REST API.

The following table identifies the specifications for the Okta DSM:

*Table 398. Okta DSM specifications*

Specification	Value
Manufacturer	Okta
DSM name	Okta
RPM file name	DSM-OktaIdentityManagement-QRadar_version-build_number.noarch.rpm
Protocol	Okta REST API
Event format	JSON
Recorded event types	All
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Okta website ( <a href="https://www.okta.com/">https://www.okta.com/</a> )

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 RPMIf 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 399. Okta DSM log source parameters*

Parameter	Value
Log Source type	Okta
Protocol Configuration	Okta REST API
IP or Hostname	Your personal Okta host name. <b>Example:</b> example.okta.com
Authentication Token	A single authentication token that is generated by the Okta console and must be used for all API transactions.
Use Proxy	When a proxy is configured, all traffic for the log source travels through the proxy for QRadar to access Okta.  Configure the <b>Proxy IP or Hostname</b> , <b>Proxy Port</b> , <b>Proxy Username</b> , and <b>Proxy Password</b> fields. If the proxy does not require authentication, you can leave the <b>Proxy Username</b> and <b>Proxy Password</b> fields blank.

*Table 399. Okta DSM log source parameters (continued)*

Parameter	Value
Automatically Acquire Server Certificate(s)	If you select <b>Yes</b> from the list, QRadar downloads the certificate and begins trusting the target server.
Recurrence	You can specify when the log source collects data. The format is M/H/D for Months/Hours/Days. The default is 1 M.
EPS Throttle	The maximum limit for the number of events per second.

The following table provides a sample event message for the Okta DSM:

*Table 400. Okta sample message supported by the Okta device*

Event name	Low level category	Sample log message
Core-User Auth-Login Success	User Login Success	<pre>{"eventId": "xxxxxxxxxxxxxxxxxxxx", "sessionId": "xxxxxxxxxxxxxxxxxxxx", "requestId": "xxxxxx", "published": "2016-04-06T16:16:40.000Z", "action": {   "message": "Sign-in successful",   "categories": [     "Sign-in Success"   ],   "objectType": "core.user_auth.login_success",   "requestUri": "/api/v1/authn" }, "actors": [   {     "id": "xxxxxxxxxxxxxxxxxxxx",     "displayName": "User",     "login": "username@example.com",     "objectType": "User"   } ], "targets": [   {     "id": "xxxxxxxxxxxxxxxxxxxx",     "displayName": "User",     "login": "username@example.com",     "objectType": "User"   } ]</pre>
Core-User Auth-Login Failed	User Login Failure	<pre>{"eventId": "xxxxxxxxxxxxxxxxxxxx_xxxxxxxxxxxxxxxxxxxxx", "sessionId": "", "requestId": "xxxxxxxxxxxxxxxxxxxx", "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": "&lt;IP_address&gt;",     "objectType": "Client"   } ], "targets": [   {     "id": "",     "objectType": "User"   } ]</pre>

**Related concepts:**

“Okta REST API protocol configuration options” on page 32

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

**Related tasks:**

“Adding a DSM” on page 4

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

“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.



---

## 103 Onapsis Security Platform

The IBM Security 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 401. Onapsis Security Platform DSM specifications*

Specification	Value
Manufacturer	Onapsis
DSM name	Onapsis Security Platform
RPM file name	DSM-OnapsisIncOnapsisSecurityPlatform-Qradar_version-build_number.noarch.rpm
Supported versions	1.5.8 and later
Event format	Log Event Extended Format (LEEF)
Recorded event types	Assessment Attack signature Correlation Compliance
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Onapsis website ( <a href="https://www.onapsis.com">https://www.onapsis.com</a> )

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 402. Onapsis Security Platform log source parameters*

Parameter	Value
Log Source type	Onapsis Security Platform
Protocol Configuration	Syslog

**Related tasks:**

“Adding a DSM” on page 4

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

“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.

---

## 104 OpenBSD

The OpenBSD DSM for IBM Security 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 Security 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:

*Table 403. Syslog parameters*

Parameter	Description
<b>Log Source Identifier</b>	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 SSH, 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 Security 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.

---

## 105 Open LDAP

The Open LDAP DSM for IBM Security 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 Security 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](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 49

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

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

"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 Security 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 404. UDP Multiline protocol configuration*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source as an identifier for events from your Open LDAP server.
<b>Listen Port</b>	<p>Type the port number that is used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65536.</p> <p>The default UDP Multiline Syslog listen port is 517.</p> <p>If you do not see the <b>Listen Port</b> field, you must restart Tomcat on QRadar.</p> <p>To edit the <b>Listen Port</b> number:</p> <p>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.”</p> <ol style="list-style-type: none"> <li>1. In the <b>Listen Port</b> field, type the new port number for receiving UDP Multiline Syslog events.</li> <li>2. Click <b>Save</b>.</li> </ol> <p>The port update is complete and event collection starts on the new port number.</p>
<b>Message ID Pattern</b>	<p>Type the regular expression (regex) that is needed to filter the event payload messages. All matching events are included when processing Open LDAP events.</p> <p>The following regular expression is suggested for Open LDAP events:</p> <pre>conn=(\d+)</pre> <p>For example, Open LDAP starts connection messages with the word <i>conn</i>, 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:  <a href="http://download.oracle.com/javase/tutorial/essential/regex/">http://download.oracle.com/javase/tutorial/essential/regex/</a></p>

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 Security 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.

---

## 106 Open Source SNORT

The Open Source SNORT DSM for IBM Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 405. Syslog parameters*

Parameter	Description
<b>Log Source Identifier</b>	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/>.

---

## 107 OpenStack

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

The following table identifies the specifications for the OpenStack DSM:

*Table 406. OpenStack DSM specifications*

Specification	Value
Manufacturer	OpenStack
DSM name	OpenStack
RPM file name	DSM-OpenStackCeilometer-Qradar_version-build_number.noarch.rpm
Supported versions	v 2015.1
Protocol	HTTP Receiver
Recorded event types	Audit event
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	OpenStack website ( <a href="http://www.openstack.org/">http://www.openstack.org/</a> )

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 407. OpenStack log source parameters*

Parameter	Value
Log Source type	OpenStack
Log Source Identifier	The IP address of the OpenStack server, and not the host name.
Protocol Configuration	HTTPReceiver
Communication Type	HTTP
Listen Port	The port number that OpenStack uses to communicate with QRadar. <b>Important:</b> Use a non-standard port. Make note of this port because it is required to configure your OpenStack device.
Message Pattern	<code>^\\{"typeURI</code>

3. Configure your OpenStack device to communicate with QRadar.

The following table provides a sample event message for the OpenStack DSM:

*Table 408. OpenStack sample message supported by the OpenStack device*

#### **Related tasks:**

## “Configuring OpenStack to communicate with QRadar”

To collect OpenStack events, you must configure your OpenStack device to allow connections from 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.

“Adding a DSM” on page 4

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

# Configuring OpenStack to communicate with QRadar

To collect OpenStack events, you must configure your OpenStack device to allow connections from QRadar.

**Important:** OpenStack is an open source product with many different distributions that can be set up on many different operating systems. This procedure might vary in your environment.

## Procedure

1. Log in to your OpenStack device.
  2. Edit the `/etc/nova/api-paste.ini` file.
  3. At the end of the file, add the following text:

```
[filter:audit]
paste.filter_factory = pycadf.middleware.audit:AuditMiddleware.factory
audit_map_file = /etc/nova/api_audit_map.conf
```

4. Review the [composite:openstack\_compute\_api\_v2] settings and verify that the values match the following sample:

```
[composite:openstack_compute_api_v2]
use = call:nova.api.auth:pipeline_factory
noauth = faultwrap sizelimit noauth ratelimit osapi_compute_app_v2
keystone = faultwrap sizelimit authtoken keystonecontext ratelimit audit osapi_compute_app_v2
keystone_nolimit = faultwrap sizelimit authtoken keystonecontext audit osapi_compute_app_v2
```

5. Copy the api\_audit\_map.conf file to the /etc/nova/ directory.
6. Restart the api service.

The command to restart the API service depends on what operating system your OpenStack node is hosted on. On Redhat Enterprise Linux systems, the command is service openstack-nova-api restart.

7. Open the entry\_points.txt file in the egg-info subdirectory of your OpenStack installation directory.

For PackStack installations, the file path resembles the following path: /usr/lib/python2.7/site-packages/ceilometer-2014.2-py2.7.egg-info/entry\_points.txt.

8. Add the http dispatcher to the [ceilometer.dispatcher] section.

```
[ceilometer.dispatcher]
file = ceilometer.dispatcher.file:FileDispatcher
database = ceilometer.dispatcher.database:DatabaseDispatcher
http = ceilometer.dispatcher.http:HttpDispatcher
```

9. Copy the supplied http.py script to the dispatcher subdirectory of the Ceilometer installation directory.

The exact location depends on your operating system and OpenStack distribution. On the Redhat Enterprise Linux Distribution of OpenStack, the directory is /usr/lib/python2.7/site-packages/ceilometer/dispatcher/.

10. Edit the /etc/ceilometer/ceilometer.conf file.
11. Under the [default] section, add dispatcher=http.
12. At the bottom of the file, add this section:

```
[dispatcher_http]
target = http://<QRadar-IP>:<QRadar-Port>
cadf_only = True
```

Use the port that you configured for OpenStack when you created the log source on your QRadar system.

13. Restart the ceilometer collector and notification services.

The command to restart the ceilometer collector and notification services depends on what operating system your OpenStack device is hosted on. On devices that use the Redhat Enterprise Linux operating system, use the following commands:

```
service openstack-ceilometer-collector restart
service openstack-ceilometer-notification restart
```



---

## 108 Oracle

IBM Security QRadar supports a number of Oracle DSMs.

---

### Oracle Acme Packet Session Border Controller

You can use IBM Security 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 Security 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 Security 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 409. Syslog protocol parameters

Parameter	Description
<b>Log Source Identifier</b>	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.
<b>Enabled</b>	Select this check box to enable the log source. By default, the check box is selected.
<b>Credibility</b>	Select the <b>Credibility</b> 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.
<b>Target Event Collector</b>	Select the <b>Event Collector</b> to use as the target for the log source.
<b>Coalescing Events</b>	Select this check box to enable the log source to coalesce (bundle) events.  By default, automatically discovered log sources inherit the value of the <b>Coalescing Events</b> 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.
<b>Incoming Event Payload</b>	From the list, select the incoming payload encoder for parsing and storing the logs.
<b>Store Event Payload</b>	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 <b>Store Event Payload</b> 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.

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 Security 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
```

- 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

- 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.
```

- 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.
```

- 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
```

- 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
```

- 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
```

- Type the following commands to return to configuration mode:

```
(media-manager-config)# done (media-manager-config)#
exit (media-manager)#
exit (configure)#
exit
```

- Type the following commands to save and activate the configuration:

```
save Save complete # activate
```

- Type reboot to restart your Oracle Acme Packet SBC installation.

After the system restarts, events are forwarded to IBM Security QRadar and displayed on the **Log Activity** tab.

## Oracle Audit Vault

The IBM Security 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 410. Oracle Audit Vault DSM specifications*

Specification	Value
Manufacturer	Oracle
DSM name	Oracle Audit Vault

*Table 410. Oracle Audit Vault DSM specifications (continued)*

Specification	Value
RPM file name	DSM-OracleAuditVault-QRadar_version-build_number.noarch.rpm
Supported versions	10.3 and 12.2
Protocol	JDBC
Event format	name-value pair (NVP)
Recorded event types	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.
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Oracle website ( <a href="https://www.oracle.com/index.html">https://www.oracle.com/index.html</a> )

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 411. Oracle Audit Vault log source parameters*

Parameter	Value
<b>Log Source type</b>	Oracle Audit Vault
<b>Protocol Configuration</b>	JDBC
<b>Log Source Identifier</b>	<DATABASE>@<HOSTNAME>
<b>Database Type</b>	Oracle
<b>Database Name</b>	The name of the Oracle Audit Vault database.
<b>IP or Hostname</b>	The IP address or host name of the Oracle Audit Vault server.
<b>Port</b>	The port from where the Oracle Audit Vault database is listening.
<b>Username</b>	Any user with the AV_AUDITOR permission. For example, AVAUDITOR.
<b>Password</b>	The password for the database user.
<b>Predefined Query</b>	None

*Table 411. Oracle Audit Vault log source parameters (continued)*

Parameter	Value
<b>Table Name</b>	For Oracle Audit Vault Version 10.3, the <b>Table Name</b> value is AVSYS.AV\$ALERT_STORE. For Oracle Audit Vault Version 12.2, the <b>Table Name</b> value is AVSYS.AV_ALERT_STORE_V.
<b>Compare Field</b>	For Oracle Audit Vault Version 10.3, the <b>Compare Field</b> value is ALERT_SEQUENCE For Oracle Audit Vault Version 12.2, the <b>Compare Field</b> value is RECORD_ID.
<b>Use Prepared Statements</b>	You must select the <b>Use Prepared Statements</b> option.
<b>Start Date and Time</b>	The initial date and time for the JDBC retrieval.

- Verify that QRadar is configured correctly.

The following table shows a sample parsed audit event message from Oracle Audit Vault:

*Table 412. Oracle Audit Vault sample message*

Event name	Low level category	Sample log message
LOGON-success	3075	<pre> ALERT_SEQUENCE: "25" AV_ALERT_TIME: "2010-01- 11 13:02:13.30702" ACTUAL_ALERT_TIME: "2010-01-11 12:19:36.0" TIME_CLEARED: "null" ALERT_NAME: "testing2" TARGET_OWNER: "null" TARGET_OBJECT: "null" ASSOCIATED_OBJECT_OW NER: "null" ASSOCIATED_OBJECT_NA ME: "null" ALERT_SEVERITY: "1" CLIENT_HOST: "host.domain.lab" CLIENT_HOSTIP: "&lt;client_host_IP_address&gt;" SOURCE_HOST: "&lt;source_host_IP_address&gt;" SOURCE_HOSTIP: "&lt;source_host_IP_address&gt;" PROCESS#: "3428" OSUSER_NAME: "null" USERNAME: "&lt;os_user_name&gt;" INSTANCE_NAME: "null" INSTANCE_NUMBER: "null" EVENT_STATUS: "0" CONTEXTID: "1561" SUB_CONTEXTID: "null" PARENT_CONTEXTID: "null" SOURCE_NAME: "XE" RECORD_ID: "23960" MSG_NUMBER: "0" CAT_ID: "2" EVENT_ID: "95" MSG_ARG_1: "null" MSG_ARG2: "null" MSG_ARG3: "null" MSG_ARG4: "null" MSG_ARG5: "null" </pre>

**Related concepts:**

“JDBC protocol configuration options” on page 16

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

#### Related tasks:

“Adding a DSM” on page 4

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

“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”

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 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.

### 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:

```
create or replace view AVSYS.AV12_EVENT_LOG_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 e1 where
e1.alert_raised = 1;
```

3. To allow a user that has AV\_AUDITOR permission to read the view that you created, type the following query:

```
grant select on AVSYS.AV_ALERT_STORE_V to AV_AUDITOR;
```

---

## Oracle BEA WebLogic

The Oracle BEA WebLogic DSM allows IBM Security 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.”
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 Security QRadar to pull log files from Oracle BEA WebLogic.

## Configuring a log source

You can configure IBM Security 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**.
6. Using the **Protocol Configuration** list, select **Log File**.
7. Configure the following parameters:

*Table 413. Log file parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source. This value must match the value that is configured in the <b>Remote Host IP or Hostname</b> parameter.  The log source identifier must be unique for the log source type.
<b>Service Type</b>	From the list, select the <b>File Transfer Protocol (FTP)</b> you want to use for retrieving files. You can choose: <b>SSH File Transfer Protocol (SFTP)</b> , <b>File Transfer Protocol (FTP)</b> , or <b>Secure Copy (SCP)</b> . The default is <b>SFTP</b> .
<b>Remote IP or Hostname</b>	Type the IP address or host name of the host from which you want to receive files.
<b>Remote Port</b>	Type the TCP port on the remote host that is running the selected <b>Service Type</b> . If you configure the <b>Service Type</b> as <b>FTP</b> , the default is 21. If you configure the <b>Service Type</b> as <b>SFTP</b> or <b>SCP</b> , the default is 22.  The valid range is 1 - 65535.

Table 413. Log file parameters (continued)

Parameter	Description
<b>Remote User</b>	Type the user name necessary to log in to the host that runs the selected <b>Service Type</b> .  The user name can be up to 255 characters in length.
<b>Remote Password</b>	Type the password necessary to log in to the host that runs the selected <b>Service Type</b> .
<b>Confirm Password</b>	Confirm the <b>Remote Password</b> to log in to the host that runs the selected <b>Service Type</b> .
<b>SSH Key File</b>	If you select <b>SCP</b> or <b>SFTP</b> as the <b>Service Type</b> , this parameter gives the option to define an SSH private key file. Also, when you provide an SSH Key File, the <b>Remote Password</b> option is ignored.
<b>Remote Directory</b>	Type the directory location on the remote host from which the files are retrieved.
<b>Recursive</b>	Select this check box if you want the file pattern to also search sub folders. The <b>Recursive</b> parameter is not used if you configure <b>SCP</b> as the <b>Service Type</b> . By default, the check box is clear.
<b>FTP File Pattern</b>	If you select <b>SFTP</b> or <b>FTP</b> as the <b>Service Type</b> , this gives the option to configure the regular expression (regex) that is needed to filter the list of files that are specified in the <b>Remote Directory</b> . 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 .log, use the following entry: server[0-9]+\.\log. 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>
<b>FTP Transfer Mode</b>	This option appears only if you select <b>FTP</b> as the <b>Service Type</b> . The <b>FTP Transfer Mode</b> 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: <ul style="list-style-type: none"> <li><b>Binary</b> - Select a binary FTP transfer mode for log sources that require binary data files or compressed .zip, .gzip, .tar, or .tar+gz archive files.</li> <li><b>ASCII</b> - Select <b>ASCII</b> for log sources that require an ASCII FTP file transfer. You must select <b>None</b> for the Processor parameter and <b>LineByLine</b> the <b>Event Generator</b> parameter when you use <b>ASCII</b> as the FTP Transfer Mode.</li> </ul>
<b>SCP Remote File</b>	If you select <b>SCP</b> as the <b>Service Type</b> you must type the file name of the remote file.
<b>Start Time</b>	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.
<b>Recurrence</b>	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.
<b>Run On Save</b>	Select this check box if you want the log file protocol to run immediately after you click Save. After the <b>Run On Save</b> completes, the log file protocol follows your configured start time and recurrence schedule.  Selecting <b>Run On Save</b> clears the list of previously processed files for the <b>Ignore Previously Processed File(s)</b> parameter.
<b>EPS Throttle</b>	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.

*Table 413. Log file parameters (continued)*

Parameter	Description
<b>Processor</b>	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.
<b>Ignore Previously Processed File(s)</b>	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.
<b>Change Local Directory?</b>	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 <b>Local Directory</b> field is displayed, and this gives you the option to configure the local directory for storing files.
<b>Event Generator</b>	From the <b>Event Generator</b> list, select <b>Oracle BEA WebLogic</b> .

8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

---

## Oracle DB Audit

The IBM Security 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 414. Oracle DB Audit DSM specifications*

Specification	Value
Manufacturer	Oracle
DSM name	Oracle DB Audit
RPM file name	DSM-OracleDbAudit-QRadar_version-build_number.noarch.rpm
Supported versions	9i, 10g, 11g, 12c (includes unified auditing)
Protocol	JDBC, Syslog
Event format	Name-Value Pair
Recorded event types	Audit records
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Oracle website ( <a href="https://www.oracle.com">https://www.oracle.com</a> )

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.

- 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 415. Oracle DB Audit Syslog log source parameters*

Parameter	Value
<b>Log Source type</b>	Oracle RDBMS Audit Record
<b>Protocol Configuration</b>	Syslog
<b>Log Source Identifier</b>	Type a unique identifier for the log source.

*Table 416. Oracle DB Audit JDBC log source parameters*

Parameter	Value
<b>Log Source type</b>	Oracle RDBMS Audit Record
<b>Protocol Configuration</b>	JDBC
<b>Log Source Identifier</b>	<p>Enter the value in &lt;DATABASE&gt;@&lt;HOSTNAME&gt; format.</p> <p>The &lt;DATABASE&gt; value must match the database name that is specified in the <b>Database name</b> field. The &lt;HOSTNAME&gt; value must match the IP or host name that is specified in the <b>IP or Hostname</b> field.</p>
<b>Database Type</b>	Oracle
<b>Database Name</b>	The name of the database from where you collect audit logs.
<b>IP or Hostname</b>	The IP or host name of the Oracle database.
<b>Port</b>	The JDBC port. The JDBC port must match the listen port that is configured on the remote database.
<b>Username</b>	The user name of the user to connect to the database. The user must have AUDIT_ADMIN or AUDIT_VIEWER permissions.
<b>Password</b>	The password of the user to connect to the database.
<b>Table name</b>	The name of the table that contains the audit records that you want to collect.
<b>Compare Field</b>	<p>For Oracle 9i or Oracle 10g Release 1, type <code>Qradar_time</code>.</p> <p>For Oracle 10g Release 2, Oracle 11g, or Oracle 12c (non-unified auditing), type <code>extended_timestamp</code>.</p> <p>For Oracle 12c (unified auditing), type <code>event_timestamp</code>.</p>

- Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Oracle Db Audit:

Table 417. Oracle Db Audit sample message

Event name	Low level category	Sample log message
SELECT succeeded	System Action Allow	<pre> 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_LREAD: "null" LOGOFF_PREAD: "null" LOGOFF_ LWRITE: "null" LOGOFF_DLOCK: "null" COMMENT_TEXT: "null" SESSIONID: "xxxxxx" ENTRYID: "2" STATEMENTID: "2" RETURNCODE: "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"</pre>

*Table 417. Oracle Db Audit sample message (continued)*

### **Related concepts:**

[“JDBC protocol configuration options” on page 16](#)

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

several database types.

**Related tasks:**

“Adding a DSM” on page 4

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

“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 Security 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:  
 `${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora`
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(dbा_audit_trail.timestamp AS TIMESTAMP)
AS qradar_time, dbа_audit_trail.* FROM dbа_audit_trail;
```

If you are using the JDBC protocol, when you configure the JDBC protocol within QRadar, use the following specific parameters:

Table 418. Configuring log source parameters

Parameter Name	Oracle v9i or 10g Release 1 Values	Oracle v10g Release 2 and v11g Values
Table Name	QRadar_audit_view	dbа_audit_trail
Select List	*	*
Compare Field	QRadar_time	extended_timestamp
Database Name	For all supported versions of Oracle, the <b>Database Name</b> must be the exact service name that is used by the Oracle <i>listener</i> . You can view the available service names by running the following command on the Oracle host: <code>lsnrctl status</code>	

**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 concepts:**

“JDBC protocol configuration options” on page 16

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

**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 Security QRadar with Oracle DB Listener, select one of the following methods for event collection:

- “Collecting events by using the Oracle Database Listener Protocol”
- “Collecting Oracle database events by using Perl” on page 762

**Related tasks:**

“Adding a DSM” on page 4

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

“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 Security 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 419. Oracle Database Listener parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source.
<b>Server Address</b>	Type the IP address of the Oracle Database Listener.
<b>Domain</b>	Type the domain that is required to access the Oracle Database Listener. This parameter is optional.
<b>Username</b>	Type the user name that is required to access the host that runs the Oracle Database Listener.
<b>Password</b>	Type the password that is required to access the host that runs the Oracle Database Listener.
<b>Confirm Password</b>	Confirm the password that is required to access the Oracle Database Listener.
<b>Log Folder Path</b>	Type the directory path to access the Oracle Database Listener log files.
<b>File Pattern</b>	<p>Type the regular expression (regex) that is needed to filter the file names. All matching files are included in the processing. The default is <code>listener\.\log</code></p> <p>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 <code>log</code>, followed by one or more digits and ending with <code>.tar.gz</code>, use the following entry: <code>log[0-9]+\.\tar\.\gz</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></p>
<b>Force File Read</b>	<p>Select this check box to force the protocol to read the log file when the timing of the polling interval specifies.</p> <p>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.</p> <p>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.</p>
<b>Recursive</b>	Select this check box if you want the file pattern to also search sub folders. By default, the check box is selected.
<b>Polling Interval (in seconds)</b>	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.
<b>Throttle Events/Sec</b>	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 Security 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 in to 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.
6. Select the **Installed Version** of QRadar.
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 420. Command parameters

Parameters	Description
<code>-D</code>	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.

Table 420. Command parameters (continued)

Parameters	Description
<b>-t</b>	The <b>-t</b> 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: <install_directory>/product/9.2/network/log/listener.log Oracle 10g: <install_directory>/product/10.2.0/db_1/network/log /listener.log Oracle 11g: <install_directory>/diag/tnslnsr/qoracle11/listener /trace/listener.log
<b>-f</b>	The <b>-f</b> parameter defines the <b>syslog facility.priority</b> to be included at the beginning of the log. If nothing is specified, <b>user.info</b> is used.
<b>-g</b>	The <b>-g</b> parameter defines the language pack file. For example, .oracle_dblistener_fwdr.pl -h <IP_address> -g /root/OracleDBListener/languagepacks/localization.french -t "tail -f /root/smbtest/listener_vali.log"  This parameter is optional.
<b>-H</b>	The <b>-H</b> 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.
<b>-h</b>	The <b>-h</b> parameter defines the receiving syslog host (the Event Collector host name or IP address that is used to receive the logs).
<b>-p</b>	The <b>-p</b> parameter defines the receiving UDP syslog port.  If a port is not specified, 514 is used.
<b>-r</b>	The <b>-r</b> parameter defines the directory name where you want to create the .pid file. The default is /var/run. This parameter is ignored if <b>-D</b> is specified.
<b>-l</b>	The <b>-l</b> parameter defines the directory name where you want to create the lock file. The default is /var/lock. This parameter is ignored if <b>-D</b> is specified.

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:

```
<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=qoraq
```

**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.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 Security 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 762.  
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 883

The Sun ONE LDAP DSM for QRadar accepts multiline UDP access and LDAP events from Sun ONE Directory Servers.

---

## Oracle Enterprise Manager

The IBM Security QRadar DSM for Oracle Enterprise Manager collects events from an Oracle Enterprise Manager device. The Real-time Monitoring Compliance feature of Oracle Enterprise Manager generates the events.

The following table lists the specifications for the Oracle Enterprise Manager DSM:

*Table 421. Oracle Enterprise Manager DSM specifications*

Specification	Value
Manufacturer	Oracle
DSM name	Oracle Enterprise Manager
RPM file name	DSM-OracleEnterpriseManager-Qradar_version-Buildbuild_number.noarch.rpm
Supported versions	Oracle Enterprise Manager Cloud Control 12c
Protocol	JDBC
Recorded event types	Audit Compliance
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Oracle Enterprise Manager ( <a href="http://www.oracle.com/us/products/enterprise-manager/index.html">http://www.oracle.com/us/products/enterprise-manager/index.html</a> )  The original format of the events are rows in an Oracle Enterprise Manager database view ( <code>sysman.mgmt\$ccc_all_observations</code> ). QRadar polls this view for new rows and uses them to generate events. For more information, see Compliance Views ( <a href="http://docs.oracle.com/cd/E24628_01/doc.121/e57277/ch5_complianceviews.htm#BABBIAA">http://docs.oracle.com/cd/E24628_01/doc.121/e57277/ch5_complianceviews.htm#BABBIAA</a> )

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 422. Oracle Enterprise Manager log source parameters*

Parameter	Description
Log Source type	Oracle Enterprise Manager
Protocol Configuration	JDBC
Database Type	Oracle
Database Name	<p>The Service Name of Oracle Enterprise Manager database.</p> <p>To view the available service names, run the <code>lsnrctl status</code> command on the Oracle host.</p>
IP or Hostname	The IP address or host name of host for Oracle Enterprise Manager database.
Port	The port that is used by the Oracle Enterprise Manager database.
Username	The user name of the account that has right to access the <code>sysman.mgmt\$ccc_all_observations</code> table.
Predefined Query	none
Table Name	<code>sysman.mgmt\$ccc_all_observations</code>
Select List	*
Compare Field	<code>ACTION_TIME</code>
Use Prepared Statements	True

#### Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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 an 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.

- Verify that the events polled are collected and displayed on the **Log Activity** tab of IBM Security QRadar.

## Configuring a log source

After the database administrator has configured database policies, you can configure a log source to access the Oracle database with the JDBC protocol.

### Procedure

- Log in to QRadar.
- Click the **Admin** tab.
- On the navigation menu, click **Data Sources**.
- Click the **Log Sources** icon.
- Click **Add**.
- Using the **Log Source Type** list, select **Oracle Fine Grained Auditing**.
- From the **Protocol Configuration** list, select **JDBC**.
- Configure the following values:

*Table 423. Oracle Fine Grained Auditing JDBC parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the log source identifier in the following format:  <code>&lt;database&gt;@&lt;hostname&gt;</code> or  <code>&lt;table name&gt;   &lt;database&gt;@&lt;hostname&gt;</code>  Where: <ul style="list-style-type: none"> <li><code>&lt;table name&gt;</code> is the name of the table or view of the database that contains the event records. This parameter is optional. If you include the table name, you must include a pipe ( ) character and the table name must match the <i>Table Name</i> parameter.</li> <li><code>&lt;database&gt;</code> is the database name, as defined in the <b>Database Name</b> parameter. The database name is a required parameter.</li> <li><code>&lt;hostname&gt;</code> is the host name or IP address for this log source, as defined in the <b>IP or Hostname</b> parameter. The host name is a required parameter.</li> </ul> The log source identifier must be unique for the log source type.
<b>Database Type</b>	Select <b>MSDE</b> as the database type.
<b>Database Name</b>	Type the name of the database to which you want to connect.  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(.).
<b>IP or Hostname</b>	Type the IP address or host name of the database.

Table 423. Oracle Fine Grained Auditing JDBC parameters (continued)

Parameter	Description
<b>Port</b>	<p>Type the port number that is used by the database server. The default that is displayed depends on the selected <b>Database Type</b>. The valid range is 0 - 65536.</p> <p>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.</p> <p>The default port number for all options includes the following ports:</p> <ul style="list-style-type: none"> <li>• DB2 - 50000</li> <li>• MSDE - 1433</li> <li>• Oracle - 1521</li> </ul> <p>If you define a <b>Database Instance</b> when MSDE is used as the database type, you must leave the Port parameter blank in your configuration.</p>
<b>Username</b>	<p>Type the database user name.</p> <p>The user name can be up to 255 alphanumeric characters in length. The user name can also include underscores (_).</p>
<b>Password</b>	<p>Type the database password.</p> <p>The password can be up to 255 characters in length.</p>
<b>Confirm Password</b>	Confirm the password to access the database.
<b>Authentication Domain</b>	<p>If you select <b>MSDE</b> as the Database Type, the <b>Authentication Domain</b> 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.</p> <p>The authentication domain must contain alphanumeric characters. The domain can include the following special characters: underscore (_), en dash (-), and period(.)</p>
<b>Database Instance</b>	<p>If you select <b>MSDE</b> as the Database Type, the <b>Database Instance</b> field is displayed.</p> <p>Type the type the instance to which you want to connect, if you have multiple SQL server instances on one server.</p> <p>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 <b>Database Instance</b> parameter blank in your configuration.</p>
<b>Predefined Query</b>	From the list, select <b>None</b> .
<b>Table Name</b>	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.
<b>Select List</b>	<p>Type * to include all fields from the table or view.</p> <p>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 <b>Compare Field</b> 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(.)</p>
<b>Compare Field</b>	Type extended_timestamp to identify new events added between queries to the table by their time stamp.

Table 423. Oracle Fine Grained Auditing JDBC parameters (continued)

Parameter	Description
<b>Use Prepared Statements</b>	Select the <b>Use Prepared Statements</b> 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.
<b>Start Date and Time</b>	Optional. Configure the start date and time for database polling.
<b>Polling Interval</b>	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.
<b>EPS Throttle</b>	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
<b>Use Named Pipe Communication</b>	If you select <b>MSDE</b> as the <b>Database Type</b> , the <b>Use Named Pipe Communications</b> 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 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.
<b>Use NTLMv2</b>	If you select <b>MSDE</b> as the <b>Database Type</b> , the <b>Use NTLMv2</b> check box is displayed.  Select the <b>Use NTLMv2</b> check box to force 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 <b>Use NTLMv2</b> check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
<b>Use SSL</b>	Select this check box if your connection supports SSL communication. This option requires more configuration on your SharePoint database and also requires administrators to configure certificates on both appliances.
<b>Database Cluster Name</b>	If you select the <b>Use Named Pipe Communication</b> check box, the <b>Database Cluster Name</b> parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure that Named Pipe communication functions properly.

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

## Oracle OS Audit

The Oracle OS Audit DSM for IBM Security 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 in to 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:  
<http://www.ibm.com/support>
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.

**Note:** Perl 5.8 must be installed on the device that hosts the Oracle server. If you do not have Perl 5.8 installed, you might be prompted that library files are missing when you attempt to start the Oracle OS Audit script. It is suggested that you verify that Perl 5.8 is installed before you continue.

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 424. Oracle OS Audit command parameters

Parameters	Description
<b>-t</b>	The <b>-t</b> parameter defines the remote host that receives the audit log files.
<b>-d</b>	The <b>-d</b> 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.
<b>-H</b>	The <b>-H</b> parameter defines the host name or IP address for the syslog header. It is suggested that it is the IP address of the Oracle server on which the script is running.
<b>-D</b>	The <b>-D</b> 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.

Table 424. Oracle OS Audit command parameters (continued)

Parameters	Description
<b>-n</b>	The <b>-n</b> parameter processes new logs, and monitors existing log files for changes to be processed. If the <b>-n</b> option string is absent all existing log files are processed during script execution.
<b>-u</b>	The <b>-u</b> parameter defines UDP.
<b>-f</b>	The <b>-f</b> parameter defines the <b>syslog facility.priority</b> to be included at the beginning of the log. If you do not type a value, <b>user.info</b> is used.
<b>-r</b>	The <b>-r</b> parameter defines the directory name where you want to create the .pid file. The default is /var/run. This parameter is ignored if <b>-D</b> is specified.
<b>-l</b>	The <b>-l</b> parameter defines the directory name where you want to create the lock file. The default is /var/lock. This parameter is ignored if <b>-D</b> is specified.
<b>-h</b>	The <b>-h</b> parameter displays the help message.
<b>-v</b>	The <b>-v</b> 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

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

“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 Security QRadar.

### Procedure

- From the **Log Source Type** list, select **Oracle RDBMS OS Audit Record**.
- From the **Protocol Configuration** list, select **syslog**.
- From the **Log Source Identifier** field, type the address that is specified by using the **-H** option in “Oracle OS Audit” on page 768.

For more information about your Oracle Audit Record, see your vendor documentation.

---

## 109 OSSEC

The OSSEC DSM for IBM Security 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>
```

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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 425. Syslog parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source as an identifier for events from your OSSEC installation.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

---

## 110 Palo Alto Networks

IBM Security QRadar supports a range of Palo Alto Network devices.

### Palo Alto Endpoint Security Manager

The IBM Security 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 426. Palo Alto Endpoint Security Manager DSM specifications*

Specification	Value
Manufacturer	Palo Alto Networks
DSM name	Palo Alto Endpoint Security Manager
RPM file name	DSM-PaloAltoEndpointSecurityManager-QRadar_version-build_number.noarch.rpm
Supported versions	3.4.2.17401
Protocol	Syslog
Event format	Log Event Extended Format (LEEF) Common Event Format (CEF)
Recorded event types	Agent Config Policy System Threat
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Palo Alto Networks website ( <a href="https://www.paloaltonetworks.com">https://www.paloaltonetworks.com</a> )

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 427. Palo Alto Endpoint Security Manager log source parameters*

Parameter	Value
Log Source type	Palo Alto Endpoint Security Manager
Protocol Configuration	Syslog
Log Source Identifier	A unique identifier for the log source.

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 428. Palo Alto Endpoint Security Manager sample message*

Event name	Low level category	Sample log message
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 src=<Source_IP_address> shost=hostname suser= fileHash=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxx NewVerdict=Benign msg>New hash added sev=6

#### Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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:

Parameter	Value
Syslog Server	Host name or IP address of the QRadar server.
Syslog Port	514
Syslog Protocol	LEEF
Keep-alive-timeout	0
Send reports interval	Frequency (in minutes), in which Traps sends logs from the endpoint. The default is 10. The range is 1 - 2,147,483,647.

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 Security QRadar DSM for Palo Alto PA Series to collect events from Palo Alto PA Series devices.

The following table identifies the specifications for the Palo Alto PA Series DSM:

*Table 429. DSM specifications for Palo Alto PA Series*

Specification	Value
Manufacturer	Palo Alto Networks
DSM name	Palo Alto PA Series
RPM file name	DSM-PaloAltoPaSeries-QRadar_version-build_number.noarch.rpm
Supported versions	PAN-OS v3.0 to v8.0
Event format	LEEF for PAN-OS v3.0 to v8.0 CEF for PAN-OS v4.0 to v6.1
QRadar recorded log types	Traffic Threat Config System HIP Match Data WildFire Authentication Tunnel Inspection Correlation URL Filtering User-ID
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Palo Alto Networks website ( <a href="http://www.paloaltonetworks.com">http://www.paloaltonetworks.com</a> )

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/fxcentral>).
2. Configure your Palo Alto PA Series device to communicate with QRadar. You must create a syslog destination and forwarding policy on the Palo Alto PA Series device.
3. If QRadar does not automatically detect Palo Alto PA Series as a log source, create a Palo Alto PA Series log source on the QRadar Console. Use the following Palo Alto values to configure the log source parameters:

Parameter	Description
Log Source Identifier	The IP address or host name of the Palo Alto PA Series device.
Log Source Type	Palo Alto PA Series
Protocol Configuration	Syslog

## Creating a syslog destination on your Palo Alto PA Series device

To send Palo Alto PA Series events to IBM Security QRadar, create a syslog destination on the Palo Alto PA Series device.

### Procedure

1. Log in to the Palo Alto Networks interface.
2. Click the **Device** tab.
3. Click **Server Profiles > Syslog**.
4. Click **Add**.
5. Create a syslog destination:
  - a. In the **Syslog Server Profile** dialog box, click **Add**.
  - b. Specify the name, server IP address, port, and facility of the QRadar system that you want to use as a syslog server.
  - c. Click **OK**.
6. Configure LEEF events:

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

- a. Click the **Custom Log Format** tab.
- b. Copy the following text and paste it in the **Custom Format** column for the **Config** log type.

#### PAN-OS v3.0 - v6.1

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$result|cat=$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|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|devTime=$cef-formatted-receive_time|src=$host|VirtualSystem=$vsys|msg=$cmd|usrName=$admin|client=$client|Result=$result|ConfigurationPath=$path|sequence=$seqno|ActionFlags=$actionFlags|BeforeChangeDetail=$before-change-detail|AfterChangeDetail=$after-change-detail|DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|vsrcName=$sys_name|DeviceName=$device_name
```

- c. Copy the following text and paste it in the **Custom Format** column 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=
$module|sev=$number-of-severity|Severity=$severity|msg=$opaque|sequence=$seqno|
ActionFlags=$actionflags|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
```

- d. Copy the following text and paste it in the **Custom Format** column 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=$flags|URLCategory=$category|sev=$severity|Severity=$number-of-severity
|Direction=$direction|ContentType=$contenttype|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=$repeatcnt|srcPort=
=$sport|dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=
$flags|proto=$proto|action=$action|Miscellaneous=$misc|ThreatID=$threatid|
URLCategory=$category|sev=$number-of-severity|Severity=$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=$reportid|DeviceGroupHierarchyL1=$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
```

## 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|sev=$number-of-severity|Severity=$severity|
Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=$srcloc|
DestinationLocation=$dstloc|ContentType=$contenttype|PCAP_ID=$pcap_id|FileDigest=$filedigest|
Cloud=$cloud|URLIndex=$url_idx|RequestMethod=$http_method|Subject=$subject|
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|SrcUUID=$src_uuid|DstUUID=$dst_uuid|
TunnelID=$tunnelid|MonitorTag=$monitorTag|ParentSessionID=$parent_session_id|
ParentStartTime=$parent_start_time|TunnelType=$tunnel|ThreatCategory=$thr_category|
ContentVer=$contentver
```

- e. Copy the following text and paste it in the **Custom Format** column 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|srcPort=$sport|dstPort=$dport|proto=$proto|usrName=$srcuser| SerialNumber=
$serial|Type=$type|Subtype=$subtype|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=
$rule|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app| VirtualSystem=
$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if
|EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=$flags
|totalBytes=$bytes|totalPackets=$packets|ElapsedTime=$elapsed|URLCategory=$category
|dstBytes=$bytes_received|srcBytes=$bytes_sent|action=$action
```

## PAN-OS v7.1

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender
_sw_version|$action|cat=$type|ReceiveTime=$receive_time|SerialNumber=$serial|Type=
$type|Subtype=$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|totalBytes=$bytes|dstBytes=$bytes_received|
|srcBytes=$bytes_sent|totalPackets=$packets|StartTime=$start|ElapsedTime=$elapsed|
URLCategory=$category|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=
$srcloc|DestinationLocation=$dstloc|dstPackets=$pkts_received|srcPackets=$pkts_-
```

```

sent|SessionEndReason=$session_end_reason|DeviceGroupHierarchyL1=$dg_hier_level_1
|DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|
ActionSource=$action_source

```

### PAN-OS v8.0

```

LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$action|cat=$type|
ReceiveTime=$receive_time|SerialNumber=$serial|Type=$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|
totalBytes=$bytes|dstBytes=$bytes_received|srcBytes=$bytes_sent|totalPackets=$packets|StartTime=$start|
ElapsedTime=$elapsed|URLCategory=$category|sequence=$seqno|ActionFlags=$actionflags|
SourceLocation=$srcloc|DestinationLocation=$dstloc|dstPackets=$pkts_received|srcPackets=$pkts_sent|
SessionEndReason=$session_end_reason|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|
ActionSource=$action_source|SrcUUID=$src_uuid|DstUUID=$dst_uuid|TunnelID=$tunnelid|
MonitorTag=$monitortag|ParentSessionID=$parent_session_id|ParentStartTime=$parent_start_time|
TunnelType=$tunnel

```

- f. Copy the following text and paste it in the **Custom Format** column 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|$sender_sw_version|$matchname|
$matchname|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|
|Subtype=$subtype|devTime=$cef-formatted-receive_time|usrName=$srcuser|
VirtualSystem=$vsys|identHostName=$machinename|OS=$os|identSrc=$src|HIP=$matchname|
|RepeatCount=$repeatcnt|H IPType=$matchtype|sequence=$seqno|ActionFlags=$actionflags|
|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

```

### PAN-OS v8.0

```

LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$matchname|
ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive_
time|usrName=$srcuser|VirtualSystem=$vsys|identHostName=$machinename|OS=$os|identsrc=$src|
HIP=$matchname|RepeatCount=$repeatcnt|H IPType=$matchtype|sequence=$seqno|ActionFlags=$actionflags|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|VirtualSystemID=$vsys_id|srcipv6=$srcipv6|
startTime=$cef-formatted-time_generated

```

- 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=$cef-formatted-receive_
time|src=$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|sev=$number-of-severity|Severity=$severity|
Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=$srcloc|
DestinationLocation=$dstloc|ContentType=$contenttype|PCAP_ID=$pcap_id|FileDigest=$filedigest|
Cloud=$cloud|URLIndex=$url_idx|RequestMethod=$http_method|UserAgent=$user_agent|identSrc=$xff|
Referer=$referer|Subject=$subject|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|
SrcUUID=$src_uuid|DstUUID=$dst_uuid|TunnelID=$tunnelid|MonitorTag=$monitortag|
ParentSessionID=$parent_session_id|ParentStartTime=$parent_start_time|TunnelType=$tunnel|
ThreatCategory=$thr_category|ContentVer=$contentver

```

- 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|sev=$number-of-severity|Severity=$severity|
Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=$srcloc|
DestinationLocation=$dstloc|ContentType=$contenttype|PCAP_ID=$pcap_id|FileDigest=$filedigest|
Cloud=$cloud|URLIndex=$url_idx|RequestMethod=$http_method|Subject=$subject|

```

```

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|SrcUUID=$src_uuid|DstUUID=$dst_uuid|
TunnelID=$tunnelid|MonitorTag=$monitortag|ParentSessionID=$parent_session_id|
ParentStartTime=$parent_start_time|TunnelType=$tunnel|ThreatCategory=$thr_category|
ContentVer=$contentver

```

- 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|sev=$number-of-severity|Severity=$severity|
Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=$srcloc|
DestinationLocation=$dstloc|ContentType=$contenttype|PCAP_ID=$pcap_id|FileDigest=$filedigest|
Cloud=$cloud|URLIndex=$url_idx|RequestMethod=$http_method|FileType=$filetype|Sender=$sender|
Subject=$subject|Recipient=$recipient|ReportID=$reportid|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|
SrcUUID=$src_uuid|DstUUID=$dst_uuid|TunnelID=$tunnelid|MonitorTag=$monitortag|
ParentSessionID=$parent_session_id|ParentStartTime=$parent_start_time|TunnelType=$tunnel|
ThreatCategory=$thr_category|ContentVer=$contentver

```

- 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=$normalize_user|ObjectName=$object|
FactorNumber=$factorno|AuthenticationID=$authid|src=$ip|RepeatCount=$repeatcnt|usrName=$user|
Vendor=$vendor|msg=$event|sequence=$seqno|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|
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|
ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive_
time|FactorType=$factorytype|VirtualSystem=$vsys|DataSourceName=$datasourcename|
DataSource=$datasource|DataSourceType=$datasourcetype|FactorNumber=$factorno|VirtualSystemID=$vsys_id|
TimeoutThreshold=$timeout|src=$ip|srcPort=$beginport|dstPort=$endport|RepeatCount=$repeatcnt|
usrName=$user|sequence=$seqno|EventID=$eventid|FactorCompletionTime=$factorcompletiontime|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|ActionFlags=$actionflags

```

- 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|$sender_sw_version|$action|
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=$action|
sequence=$seqno|ActionFlags=$actionflags|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|
TunnelID=$tunnelid|MonitorTag=$monitortag|ParentSessionID=$parent_session_id|
ParentStartTime=$parent_start_time|TunnelType=$tunnel|totalBytes=$bytes|dstBytes=$bytes_received|
srcBytes=$bytes_sent|totalPackets=$packets|dstPackets=$pkts_received|srcPackets=$pkts_sent|
MaximumEncapsulation=$max_encap|UnknownProtocol=$unknown_proto|StrictChecking=$strict_check|
TunnelFragment=$tunnel_fragment|SessionsCreated=$sessions_created|SessionsClosed=$sessions_closed|
SessionEndReason=$session_end_reason|ActionSource=$action_source|startTime=$start|ElapsedTime=$elapsed

```

- m. Copy the following text and paste it in the **Custom Format** column for the **Correlation** log type.

## PAN-OS v8.0

```
L0EF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|8.0|$category|ReceiveTime=$receive_time|
SerialNumber=$serial|cat=$type|devTime=$cef-formatted-receive_time|startTime=$cef-formatted-time_
generated|Severity=$severity|VirtualSystem=$vsys|VirtualSystemID=$vsys_id|src=$src|
SourceUser=$srcuser|msg=$evidence|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|
ObjectName=$object_name|ObjectID=$object_id
```

7. Click **OK**.
8. Specify the severity of events that are contained in the syslog messages.
  - a. Click **Log Setting > System** and then click **Edit**.
  - b. Select the check box for each event severity level that you want contained in the syslog message.
  - c. Type the name of the syslog destination.
  - d. Click **OK**.
9. Click the **Device** tab and then click **Commit**.

## What to do next

To allow communication between your Palo Alto Networks device and QRadar, create a forwarding policy. See “Creating a forwarding policy on your Palo Alto PA Series device.”

## Creating a forwarding policy on your Palo Alto PA Series device

If your IBM Security QRadar Console or Event Collector is in a different security zone than your Palo Alto PA Series device, create a forwarding policy rule.

### Procedure

1. Log in to Palo Alto Networks.
2. On the dashboard, click the **Policies** tab.
3. Click **Policies > Policy Based Forwarding**.
4. Click **New**.
5. Configure the parameters. For descriptions of the policy-based forwarding values, see your *Palo Alto Networks Administrator’s Guide*.

## Creating ArcSight CEF formatted Syslog events on your Palo Alto PA Series Networks Firewall device

You can configure your Palo Alto Networks firewall to send ArcSight CEF formatted Syslog events to IBM Security QRadar.

### Procedure

1. Log in to the Palo Alto Networks interface.
2. Select **Panorama/Device > Setup > Management**, to configure the device to include its IP Address in the header of Syslog messages.
3. In the **Logging and Reporting Settings** section, click **Edit**.
4. In the **Syslog HOSTNAME Format** list, select **ipv4-address** or **ipv6-address**, and then click **OK**.
5. Select **Device > Server Profiles > Syslog**, and then click **Add**.
6. Specify the **Name** and **Location**. Location refers to a virtual system if the device is enabled for virtual systems.
7. On the **Servers** tab, click **Add**.
8. Specify the name, server IP address, port, and facility of the QRadar system that you want to use as a syslog server:
  - a. **Name** is Syslog server name.

- b. **Syslog Server** is the IP address for the Syslog server.
  - c. The **Transport/Port** default is **514**.
  - d. The **Faculty** default is **LOG\_USER**.
9. 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**.
10. 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:
- 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**.
- 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=$rule suser=$srcuser duser
=$dstuser app=$app 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
suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual
System cs3=$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
```

### System

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$type|
$number-of-severity|rt=$cef-formatted-receive_time
deviceExternalId=$serial cs3Label=Virtual System cs3=$vsys
fname=$object flexString2Label=Module flexString2=$module
msg=$opaque externalId=$seqno cat=$eventid
```

### HIP Match

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$matchtype|$type|1|
rt=$cef-formatted-receive_time deviceExternalId=$serial
suser=$srcuser cs3Label=Virtual System cs3=$vsys shost=$machinename
src=$src cnt=$repeatcnt externalId=$seqno cat=$matchname
cs2Label=Operating System cs2=$os
```

## 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>).

---

## 111 Pirean Access: One

The Pirean Access: One DSM for IBM Security 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

To collect events, you must configure a log source in IBM Security QRadar to poll your Access: One installation database with the JDBC protocol.

#### 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 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 **Pirean Access: One**.
8. Using the **Protocol Configuration** list, select **JDBC**.
9. Configure the following values:

Table 430. Pirean Access: One log source parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the identifier for the log source. The log source identifier must be defined in the following format:  <code>&lt;database&gt;@&lt;hostname&gt;</code>  Where:  <code>&lt;database&gt;</code> is the database name, as defined in the <b>Database Name</b> parameter. The database name is a required parameter.  <code>&lt;hostname&gt;</code> is the host name or IP address for the log source as defined in the <b>IP or Hostname</b> parameter. The host name is a required parameter.  The log source identifier must be unique for the log source type.
<b>Database Type</b>	From the list, select DB2 as the type of database to use for the event source.
<b>Database Name</b>	Type the name of the database to which you want to connect. The default database name is LOGINAUD.
<b>IP or Hostname</b>	Type the IP address or host name of the database server.
<b>Port</b>	Type the TCP port number that is used by the audit database DB2 instance.  Your DB2 administrator can provide you with the TCP port that is needed for this field.
<b>Username</b>	Type a user name that has access to the DB2 database server and audit table.  The user name can be up to 255 alphanumeric characters in length. The user name can also include underscores (_).
<b>Password</b>	Type the database password.  The password can be up to 255 characters in length.
<b>Confirm Password</b>	Confirm the password to access the database.
<b>Table Name</b>	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(.) .
<b>Select List</b>	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 <b>Compare Field</b> 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(.) .
<b>Compare Field</b>	Type <b>TIMESTAMP</b> 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(.) .
<b>Use Prepared Statements</b>	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.

*Table 430. Pirean Access: One log source parameters (continued)*

Parameter	Description
<b>Start Date and Time</b>	Optional. Configure the start date and time for database polling.  The <b>Start Date and Time</b> 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.
<b>Polling Interval</b>	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.
<b>EPS Throttle</b>	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
<b>Enabled</b>	Select this check box to enable the Pirean Access: One log source.

10. Click **Save**.

11. 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.



---

## 112 PostFix Mail Transfer Agent

IBM Security 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 Security 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 values:

*Table 431. PostFix MTA log source parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address, host name, or name to identify your PostFix MTA installation.
<b>Listen Port</b>	<p>Type <b>517</b> as the port number used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65535.</p> <p>To edit a saved configuration to use a new port number:</p> <ol style="list-style-type: none"> <li>1. In the <b>Listen Port</b> field, type the new port number for receiving UDP Multiline Syslog events.</li> <li>2. Click <b>Save</b>.</li> </ol> <p>The port update is complete and event collection starts on the new port number.</p>
<b>Message ID Pattern</b>	<p>Type the following regular expression (regex) needed to filter the event payload messages.</p> <pre>postfix/.*?[ \[]\d+[ \]](?:- -  : )([A-Z0-9]{8,10})</pre>
<b>Enabled</b>	Select this check box to enable the log source.
<b>Credibility</b>	<p>Select the credibility of the log source. The range is 0 - 10.</p> <p>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.</p>
<b>Target Event Collector</b>	Select the <b>Target Event Collector</b> to use as the target for the log source.
<b>Coalescing Events</b>	<p>Select this check box to enable the log source to coalesce (bundle) events.</p> <p>By default, automatically discovered log sources inherit the value of the <b>Coalescing Events</b> 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.</p>
<b>Store Event Payload</b>	<p>Select this check box to enable the log source to store event payload information.</p> <p>By default, automatically discovered log sources inherit the value of the <b>Store Event Payload</b> 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.</p>

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 Security QRadar as the root user.
2. To edit the IPtables file, type the following command:  
`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:  
`-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:

```
-A PREROUTING -p udp --dport 514 -j
REDIRECT --to-port 517 -s <IP_address1> -A PREROUTING -p udp --dport 514 -j
REDIRECT --to-port 517 -s <IP_address2> -A PREROUTING -p udp --dport 514 -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:

```
vi /opt/qradar/conf/iptables.post
```

6. Type the following command to instruct QRadar to allow communication from your PostFix MTA installations:

```
-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:

```
-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:

```
./opt/qradar/bin/iptables_update.pl
```



---

## 113 ProFTPD

IBM Security 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/proftpd.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.” 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 432. 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 ProFTPD installation.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

---

## 114 Proofpoint Enterprise Protection and Enterprise Privacy

The IBM Security 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 433. Proofpoint Enterprise Protection and Enterprise Privacy DSM specifications*

Specification	Value
Manufacturer	Proofpoint
DSM name	Proofpoint Enterprise Protection/Enterprise Privacy
RPM file name	DSM-Proofpoint_Enterprise_Protection/_Enterprise_PrivacyQradar_version-build_number.noarch.rpm
Supported versions	V7.02 V7.1 V7.2 V7.5 V8.0
Protocol	Syslog Log File
Recorded event types	System Email security threat classification Email audit and encryption
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Proofpoint website ( <a href="https://www.proofpoint.com/us/solutions/products/enterprise-protection">https://www.proofpoint.com/us/solutions/products/enterprise-protection</a> )

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. If QRadar does not automatically discover the Proofpoint Enterprise Protection and Enterprise Privacy log source, create a log source for each instance of Proofpoint Enterprise and Enterprise Privacy DSM on your network.

**Related tasks:**

"Adding a DSM" on page 4

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

"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 Proofpoint Enterprise Protection and Enterprise Privacy DSM to communicate with IBM Security 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 Security 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

IBM Security QRadar automatically discovers and creates a log source for syslog events from Proofpoint Enterprise Protection and Enterprise Privacy appliances. You can also manually configure a log source.

### About this task

The following configuration steps are optional. To manually configure a syslog log source for Proofpoint Enterprise Protection and Enterprise Privacy, complete 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 **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 434. Syslog parameters*

Parameter	Description
Log Source Identifier	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

**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 435. Log file parameters*

Parameter	Description
Log Source Identifier	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.
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. <ul style="list-style-type: none"> <li>• SFTP - SSH File Transfer Protocol</li> <li>• FTP - File Transfer Protocol</li> <li>• SCP - Secure Copy</li> </ul> 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 <b>Remote IP or Hostname</b> field has the SFTP subsystem enabled.
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.
Remote User	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.
Remote Password	Type the password necessary to log in to your Proofpoint Enterprise Protection and Enterprise Privacy system.
Confirm Password	Confirm the Remote Password to log in to your Proofpoint Enterprise Protection and Enterprise Privacy system.

Table 435. Log file parameters (continued)

Parameter	Description
SSH Key File	If you select SCP or SFTP from the <b>Service Type</b> field you can define a directory path to an SSH private key file. The SSH Private Key File allows you to ignore the <b>Remote Password</b> field.
Remote Directory	Type the directory location on the remote host from which the files are retrieved.
Recursive	Select this check box if you want the file pattern to also search sub folders. The Recursive parameter is not used if you configure SCP as the Service Type. By default, the check box is clear.
FTP File Pattern	<p>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.</p> <p>Another example, if you want to retrieve all syslog files with the keyword "_filter" in the file name, use the following entry: <code>.*_filter.*\syslog</code>.</p> <p>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></p>
FTP Transfer Mode	<p>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.</p> <p>From the list, select the transfer mode that you want to apply to this log source:</p> <ul style="list-style-type: none"> <li>• Binary - Select Binary for log sources that require binary data files or compressed .zip, .gzip, .tar, or .tar+gzip archive files.</li> <li>• ASCII - Select ASCII for log sources that require an ASCII FTP file transfer. You must select <b>NONE</b> for the <b>Processor</b> field and <b>LINEBYLINE</b> the <b>Event Generator</b> field when you are using ASCII as the transfer mode.</li> </ul>
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	<p>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).</p> <p>For example, type 2H if you want the directory to be scanned every 2 hours. The default is 1H.</p>

Table 435. Log file parameters (continued)

Parameter	Description
Run On Save	Select this check box if you want the log file protocol to run immediately after you click Save. After the <b>Run On Save</b> completes, the log file protocol follows your configured start time and recurrence schedule.  Selecting <b>Run On Save</b> clears the list of previously processed files for the <b>Ignore Previously Processed File(s)</b> parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.
Processor	If the files on the remote host are stored in a .zip, .gzip, .tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents that are processed.
Ignore Previously Processed File(s)	Select this check box to track files that have already been processed and you do not want the files to be processed a second time. This applies to FTP and SFTP Service Types only.
Change Local Directory?	Select this check box to define the local directory on your QRadar system that you want to use for storing downloaded files during processing. We recommend that you leave the check box clear. When the check box is selected, the <b>Local Directory</b> field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the <b>Event Generator</b> list, select <b>LINEBYLINE</b> .

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.



---

## 115 Pulse Secure Pulse Connect Secure

The IBM Security QRadar DSM for Pulse Secure Pulse Connect Secure collects syslog and WebTrends Enhanced Log File (WELF) formatted events from Pulse Secure Pulse Connect Secure mobile VPN devices.

The following table describes the specifications for the Pulse Secure Pulse Connect Secure DSM:

*Table 436. Pulse Secure Pulse Connect Secure DSM specifications*

Specification	Value
Manufacturer	Pulse Secure
DSM name	Pulse Secure Pulse Connect Secure
RPM file name	DSM-PulseSecurePulseConnectSecure-QRadar_version-build_number.noarch.rpm
Supported versions	8.2R5
Protocol	Syslog, TLS Syslog
Event format	Admin Authentication System Network Error
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	Yes
More information	Pulse Secure website ( <a href="https://www.pulsesecure.net">https://www.pulsesecure.net</a> )

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 437. Pulse Secure Pulse Connect Secure Syslog log source parameters*

Parameter	Value
Log Source type	Pulse Secure Pulse Connect Secure
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

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 438. Pulse Secure Pulse Connect Secure TLS Syslog log source parameters*

Parameter	Value
Log Source type	Pulse Secure Pulse Connect Secure
Protocol Configuration	TLS Syslog
Log Source Identifier	Type a unique identifier for the log source.
TLS Protocols	Select the version of TLS that is installed on the client.

#### Related concepts:

“TLS syslog protocol configuration options” on page 47

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

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

“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 Security 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](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](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 439. Pulse Secure Pulse Connect Secure sample message*

Event name	Low level category	Sample log message
VlanAssigned	Information	<pre>id=firewall time= "2009-10-01 22:26:39" pri=6 fw= &lt;IP_address&gt; vpn=ic user=user realm=&lt;Domain&gt; roles="Employee, Remediation" proto= src=&lt;Source_IP_address&gt; dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="EAM24459: User assigned to vlan (VLAN='16')"</pre>

---

## 116 Radware

IBM Security QRadar supports a range of Radware devices.

### Radware AppWall

The IBM Security QRadar DSM for Radware AppWall collects logs from a Radware AppWall appliance.

The following table describes the specifications for the Radware AppWall DSM:

*Table 440. Radware AppWall DSM specifications*

Specification	Value
Manufacturer	Radware
DSM name	Radware AppWall
RPM file name	DSM-RadwareAppWall-Qradar_version-build_number.noarch.rpm
Supported versions	V6.5.2 V8.2
Protocol	Syslog
Event format	Vision Log
Recorded event types	Administration Audit Learning Security System
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Radware website ( <a href="http://www.radware.com">http://www.radware.com</a> )

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 441. Radware AppWall log source parameters*

Parameter	Value
Log Source type	Radware AppWall
Protocol Configuration	Syslog

**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

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

“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”

Configure your Radware AppWall device to send logs to IBM Security QRadar. You integrate AppWall logs with QRadar by using the Vision Log event format.

“Increasing the maximum TCP Syslog payload length for Radware AppWall”

Increase the maximum TCP Syslog payload length for your RadWare AppWall appliance in IBM Security QRadar.

## Configuring Radware AppWall to communicate with QRadar

Configure your Radware AppWall device to send logs to IBM Security 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:

Parameter	Value
<b>Address</b>	The IP address for the QRadar Console.
<b>Port</b>	514
<b>Version</b>	Select the most recent version from the list. It is the last item in the list.

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 Security 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/pluggableresources/` 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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 442. Syslog parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source as an identifier for events from your Radware DefensePro installation.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

---

## 117 Raz-Lee iSecurity

IBM Security 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 443. IBM i DSM specifications for Raz-Lee iSecurity*

Specification	Value
Manufacturer	IBM
DSM name	IBM i
RPM file name	DSM-IBMi-QRadar_version-build_number.noarch.rpm
Supported versions	iSecurity Firewall V15.7 iSecurity Audit V11.7
Protocol	Syslog
Event format	LEEF
Recorded event types	All security, compliance, and audit events.
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	IBM website ( <a href="http://www.ibm.com">http://www.ibm.com</a> )

---

## 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 Security 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 444. 32.SIEM 1 parameter values*

Parameter	Value
SIEM 1 name	Type QRadar.
Port	Type the port that is used to send syslog messages. The default port is 514, which is the syslog standard.
SYSLOG type	Type 1 for UDP.

*Table 444. 32.SIEM 1 parameter values (continued)*

Parameter	Value
Destination address	Type the IP address for QRadar.
Severity range to auto send	Type a severity message level in the range of 0 - 7. For example, type 7 to send all syslog messages.
Facility to use	Type a syslog facility level in the range of 0 - 23.
Message structure	Type *LEEF.
Convert data to CCSID	Type 0 in the <b>Convert data to CCSID</b> field. This is the default character conversion.
Maximum length	Type 1024.

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 445. 31. Main Control parameter values*

Parameter	Value
Run rules before sending	To process the events that you want to send, type Y. To send all events, type N.
SIEM 1: QRadar	Type Y.
Send JSON messages (for DAM)	Type N.
As only operation	Type N.

8. From the command line, to configure the **Firewall** options, type STRFW to access the menu options.
9. From the **Firewall** menu, select **81. System Configuration**.
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 446. 72.SIEM 1 parameter values*

Parameter	Value
SIEM 1 name	Type QRadar.
Port	Type the port that is used to send syslog messages. The default port is 514, which is the Syslog standard.
SYSLOG type	Type 1 for UDP syslog type.
Send in FYI mode	Type N.
Destination address	Type the IP address for the QRadar console.
Severity range to auto send	Type a severity level in the range 0 - 7.
Facility to use	Type a facility level.
Message structure	Type *LEEF.
Convert data to CCSID	Type 0.
Maximum length	Type 1024.

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 447. 71. Main Control parameter values*

Parameter	Value
SIEM 1: QRadar	Type 2.
Send JSON messages (for DAM)	Type 0.

## 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 Security 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 448. Syslog protocol parameters*

Parameter	Description
<b>Log Source Identifier</b>	The IP address or host name of the log source that sends events from the Raz-Lee iSecurity device.
<b>Enabled</b>	By default, the check box is selected.
<b>Credibility</b>	The <b>Credibility</b> 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.
<b>Coalescing Events</b>	By default, automatically discovered log sources inherit the value of the <b>Coalescing Events</b> 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.

*Table 448. Syslog protocol parameters (continued)*

Parameter	Description
<b>Incoming Payload Encoding</b>	Select <b>Incoming Payload Encoder</b> for parsing and storing the logs.
<b>Store Event Payload</b>	By default, automatically discovered log sources inherit the value of the <b>Store Event Payload</b> list from the <b>System Settings</b> 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.

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

---

## 118 Redback ASE

The Redback ASE DSM for IBM Security 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 Security 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 Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.  
The syslog protocol configuration is displayed.
10. Configure the following values:

*Table 449. Syslog parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address or host name for the log source as an identifier for events from your Redback ASE appliance.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.  
The configuration is complete.

---

## 119 Resolution1 CyberSecurity

Resolution1 CyberSecurity is formerly known as AccessData InSight. The Resolution1 CyberSecurity DSM for IBM Security QRadar collects event logs from your Resolution1 CyberSecurity device.

The following table identifies the specifications for the Resolution1 CyberSecurity DSM:

*Table 450. Resolution1 CyberSecurity DSM specifications*

Specification	Value
Manufacturer	Resolution1
DSM name	Resolution1 CyberSecurity
RPM file name	DSM-Resolution1CyberSecurity-Qradar_version-build_number.noarch.rpm
Supported versions	V2
Event format	Log file
QRadar recorded event types	Volatile Data Memory Analysis Data Memory Acquisition Data Collection Data Software Inventory Process Dump Data Threat Scan Data Agent Remediation Data
Automatically discovered?	No
Included identity?	No

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” on page 4

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

“Configuring your Resolution1 CyberSecurity device to communicate with QRadar” on page 814

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” on page 814

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:

```
<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**.

---

## 120 Riverbed

IBM Security QRadar supports a number of Riverbed DSMs:

### Riverbed SteelCentral NetProfiler (Cascade Profiler) Audit

The IBM Security 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 451. Riverbed SteelCentral NetProfiler specifications*

Specification	Value
Manufacturer	Riverbed
DSM name	SteelCentral NetProfiler Audit
RPM file name	DSM-RiverbedSteelCentralNetProfilerAudit-Qradar_version-build_number.noarch.rpm
Event format	Log file protocol
Recorded event types	Audit Events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Riverbed website ( <a href="http://www.riverbed.com/">http://www.riverbed.com/</a> )

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 816.
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 452. Riverbed SteelCentral NetProfiler log source parameters*

Parameter	Description
Log Source Type	Riverbed SteelCentral NetProfiler Audit
Protocol Configuration	LogFile
Remote IP or Hostname	The IP address or host name of the third-party host that stores the generated audit file
Remote User	The user name for the account that can access the host.
Remote Password	The password for the user account.
Remote Directory	The absolute file path on the third-party host that contains the generated audit file.
FTP File Pattern	A regex pattern that matches the name of the audit file.
Recurrence	Ensure that recurrence matches the frequency at which the SteelScript for Python SDK script is run on the remote host.

Table 452. Riverbed SteelCentral NetProfiler log source parameters (continued)

Parameter	Description
Event Generator	Line Matcher
Line Matcher RegEx	<code>^\d+/\d+/\d+ \d+:\d+,</code>

**Related tasks:**

“Adding a DSM” on page 4

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

“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 Security QRadar DSM for Riverbed SteelCentral NetProfiler collects alert logs from your Riverbed SteelCentral NetProfiler system. This product is also known as *Cascade Profiler*.

The following table identifies the specifications for the Riverbed SteelCentral NetProfiler DSM:

*Table 453. Riverbed SteelCentral NetProfiler specifications*

Specification	Value
Manufacturer	Riverbed
DSM name	SteelCentral NetProfiler
RPM file name	DSM-RiverbedSteelCentralNetProfiler-Qradar_version-build_number.noarch.rpm
Event format	JDBC
Recorded event types	Alert Events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Riverbed website ( <a href="http://www.riverbed.com/">http://www.riverbed.com/</a> )

To integrate Riverbed SteelCentral NetProfiler with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console.
  - Protocol-JDBC RPM
  - Riverbed SteelCentral NetProfiler RPM
2. Configure your Riverbed SteelCentral NetProfiler system to enable communication with QRadar.
3. Create a log source on the QRadar Console. Use the following table to define the Riverbed-specific parameters:

*Table 454. Riverbed SteelCentral NetProfiler log source parameters*

Parameter	Description
Log Source Type	Riverbed SteelCentral NetProfiler
Protocol Configuration	JDBC
Database Name	You must type the actual name of the Riverbed database. For most configurations, the database name is <code>mazu</code> . <b>Tip:</b> Confirm the actual name of the Riverbed database.
Table Name	<code>events.export_csv_view</code>
Username	The user name for the account that is configured to access the PostgreSQL database on the Riverbed SteelCentral NetProfiler system.
Comparable Field	<code>start_time</code>
Polling Interval	<code>5M</code>

### Related tasks:

“Adding a DSM” on page 4

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

“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.

---

## 121 RSA Authentication Manager

You can use an RSA Authentication Manager DSM to integrate IBM Security 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”
- “Configuring the log file protocol for RSA Authentication Manager 6.x and 7.x” on page 820

**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

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

“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.”

If you are using RSA Authentication Manager on Windows, see “Configuring Windows” on page 820.

---

## 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:

```
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 IBM Security 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/RSA Security/RSA Authentication Manager/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 Security 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 821.

- If you are using RSA Authentication Manager v7.x, see “Configuring RSA Authentication Manager 7.x.”

---

## 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.
6. Select the **Enable Automatic Audit Log Maintenance** check box.
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 Security 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 21](#)

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.

---

## 122 SafeNet DataSecure

The IBM Security 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 detects 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

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

“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 can 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:

Parameter	Description
Syslog Server #1 IP	The IP address or host name of the target QRadar Event Collector.
Syslog Server #1 Port	The listening port for QRadar. Use Port 514.
Syslog Server #1 Proto	QRadar can receive syslog messages by using either UDP or TCP.

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**.

---

## 123 Salesforce

IBM Security QRadar supports a range of Salesforce DSMs.

### Salesforce Security Auditing

The IBM Security QRadar DSM for Salesforce Security Auditing can collect Salesforce Security Auditing audit trail logs that you copy from the cloud to a location that QRadar can access.

The following table identifies the specifications for the Salesforce Security Auditing DSM:

*Table 455. Salesforce Security Auditing DSM specifications*

Specification	Value
Manufacturer	Salesforce
DSM	Salesforce Security Auditing
RPM file name	DSM-SalesforceSecurityAuditing-QRadar_Version-Build_Number.noarch.rpm
Protocol	Log File
QRadar recorded events	Setup Audit Records
Automatically discovered	No
Includes identity	No
More information	Salesforce web site ( <a href="http://www.salesforce.com/">http://www.salesforce.com/</a> )

### Salesforce Security Auditing DSM integration process

To integrate Salesforce Security Auditing DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console:
  - Log File Protocol RPM
  - Salesforce Security Auditing RPM
2. Download the Salesforce audit trail file to a remote host that QRadar can access.
3. For each instance of Salesforce Security Auditing, create a log source on the QRadar Console.

### Downloading the Salesforce audit trail file

To collect Salesforce Security Auditing events, you must download the Salesforce audit trail file to a remote host that QRadar can access.

#### About this task

You must use this procedure each time that you want to import an updated set of audit data into QRadar. When you download the audit trail file, you can overwrite the previous audit trail CSV file. When QRadar retrieves data from the audit trail file, QRadar processes only audit records that were not imported before.

#### Procedure

1. Log in to your Salesforce Security Auditing server.
2. Go to the **Setup** section.

3. Click **Security Controls**.
4. Click **View Setup Audit Trail**.
5. Click **Download setup audit trail for last six months (Excel.csv file)**.
6. Copy the downloaded file to a location that QRadar can reach by using Log File Protocol.

## Configuring a Salesforce Security Auditing log source in QRadar

To collect Salesforce Security Auditing events, configure a log source in QRadar.

### Procedure

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

Parameter	Description
Event Generator	RegEx Based Multiline
Start Pattern	(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} \w+)
End Pattern	Ensure that this parameter remains empty.
Date Time RegEx	(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} \w+)
Date Time Format	dd/MM/yyyy hh:mm:ss z

**Attention:** These values are based on the Winter 2015 version of Salesforce Security Auditing. For previous versions, use the following regex statements:

- For the **Start Pattern** parameter, use the following statement:  
(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} [AM] {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**.

---

## Salesforce Security Monitoring

The IBM Security QRadar DSM for Salesforce Security Monitoring can collect event logs from your Salesforce console by using a RESTful API in the cloud.

The following table identifies the specifications for the Salesforce Security Monitoring DSM:

*Table 456. Salesforce Security Monitoring DSM specifications*

Specification	Value
Manufacturer	Salesforce
DSM	Salesforce Security Monitoring

Table 456. Salesforce Security Monitoring DSM specifications (continued)

Specification	Value
RPM file name	DSM-SalesforceSecurityMonitoring-QRadar_Version-Build_Number.noarch.rpm
Protocol	Salesforce REST API Protocol
QRadar recorded events	Login History, Account History, Case History, Entitlement History, Service Contract History, Contract Line Item History, Contract History, Contact History, Lead History, Opportunity History, Solution History
Automatically discovered	No
Includes identity	Yes
More information	Salesforce website ( <a href="http://www.salesforce.com/">http://www.salesforce.com/</a> )

## Salesforce Security Monitoring DSM integration process

To integrate Salesforce Security Monitoring DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console.
  - DSMCommon RPM
  - SalesforceRESTAPI Protocol RPM
  - Salesforce Security Monitoring RPM
2. Configure the Salesforce Security Monitoring server to communicate with QRadar.
3. Obtain and install a certificate to enable communication between Salesforce Security Monitoring and QRadar. The certificate must be in the /opt/QRadar/conf/trusted\_certificates/ folder and be in .DER format.
4. For each instance of Salesforce Security Monitoring, create a log source on the QRadar Console.

## Configuring the Salesforce Security Monitoring server to communicate with QRadar

To allow QRadar communication, you need to configure Connected App on the Salesforce console and collect information that the Connected App generates. This information is required for when you configure the QRadar log source.

### Before you begin

If the RESTful API is not enabled on your Salesforce server, contact Salesforce support.

### Procedure

1. Log in to your Salesforce Security Monitoring server.
2. From the **Setup** menu, click **Create > Apps > New**.
3. Type the name of your application.
4. Type the contact email information.
5. Select **Enable OAuth Settings**.
6. From the **Selected OAuth Scopes** list, select **Full Access**.
7. In the **Info URL** field, type a URL where the user can go for more information about your application.
8. Configure the remaining optional parameters.
9. Click **Save**.

## What to do next

The Connected App generates the information that is required for when you to configure a log source on QRadar. Record the following information:

### Consumer Key

Use the **Consumer Key** value to configure the **Client ID** parameter for the QRadar log source.

### Consumer Secret

You can click the link to reveal the consumer secret. Use the **Consumer Secret** value to configure the **Secret ID** parameter for the QRadar log source.

**Important:** The **Consumer Secret** value is confidential. Do not store the consumer secret as plain text.

### Security token

A security token is sent by email to the email address that you configured as the contact email.

## Configuring a Salesforce Security Monitoring log source in QRadar

To collect Salesforce Security Monitoring events, configure a log source in QRadar.

### Before you begin

When you configured a Connected App on the Salesforce Security Monitoring server, the following information was generated:

- Consumer Key
- Consumer Secret
- Security token

This information is required to configure a Salesforce Security Monitoring log source in QRadar.

Ensure that the trusted certificate from the Salesforce Security Monitoring instance is copied to the /opt/qradar/conf/trusted\_certificates/ folder in .DER format on QRadar system.

### Procedure

1. Log in toQRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **Salesforce Security Monitoring**.
7. From the **Protocol Configuration** list, select **Salesforce Rest API**.
8. Configure the following values:

Parameter	Description
<b>Login URL</b>	The URL of the Salesforce security console.
<b>Username</b>	The user name of the Salesforce security console.
<b>Security Token</b>	The security token that was sent to the email address configured as the contact email for the Connected App on the Salesforce security console.
<b>Client ID</b>	The Consumer Key that was generated when you configured the Connected App on the Salesforce security console.

Parameter	Description
<b>Secret ID</b>	The Consumer Secret that was generated when you configured the Connected App on the Salesforce security console.
Use Proxy	<p>When a proxy is configured, all traffic for the log source travels through the proxy for QRadar to access the Salesforce Security buckets.</p> <p>Configure the <b>Proxy Server</b>, <b>Proxy Port</b>, <b>Proxy Username</b>, and <b>Proxy Password</b> fields. If the proxy does not require authentication, you can leave the <b>Proxy Username</b> and <b>Proxy Password</b> fields blank.</p>

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



---

## 124 Samhain Labs

The Samhain Labs Host-Based Intrusion Detection System (HIDS) monitors changes to files on the system.

The Samhain HIDS DSM for IBM Security 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 concepts:**

“JDBC protocol configuration options” on page 16

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

**Related tasks:**

“Adding a DSM” on page 4

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

“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 Security 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. To configure QRadar to receive events from Samhain:

- 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 JDBC to collect Samhain events

You can configure Samhain HIDS to send log alerts to a database. Oracle, PostgreSQL, and MySQL are natively supported by Samhain.

### About this task

You can also configure IBM Security QRadar to collect events from these databases by using the JDBC protocol.

**Note:** IBM Security 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/>.

### Procedure

- Log into QRadar.
  - Click the **Admin** tab.
  - On the navigation menu, click **Data Sources**.
  - Click the **Log Sources** icon.
  - Click **Add**.
  - From the **Log Source Type** list, select the **Samhain HIDS** option.
  - Using the **Protocol Configuration** list, select **JDBC**.
  - Update the JDBC configuration to include the following values:
    - Database Type:** <Samhain Database Type>
    - Database Name:** <Samhain SetDBName>
    - Table Name:** <Samhain SetDBTable>
    - Select List:** \*
    - Compare Field:** log\_index
    - IP or Hostname:** <Samhain SetDBHost>
    - Port:** <Default Port>
    - Username:** <Samhain SetDBUser>
    - Password:** <Samhain SetDBPassword>
    - Polling Interval:** <Default Interval>
- 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.

9. You can now configure the log source in QRadar. To configure QRadar to receive events from Samhain: From the **Log Source Type** list, select the **Samhain HIDS** option.

For more information about Samhain, see <http://www.la-samhna.de/samhain/manual>.

**Related concepts:**

“JDBC protocol configuration options” on page 16

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

**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.



---

## 125 Seculert

The IBM Security QRadar DSM for Seculert collects events from the Seculert cloud service.

The following table describes the specifications for the Seculert DSM:

*Table 457. Seculert DSM specifications*

Specification	Value
Manufacturer	Seculert
DSM name	Seculert
RPM file name	DSM-SeculertSeculert-Qradar_version-build_number.noarch.rpm
Supported versions	v1
Protocol	Seculert Protection REST API Protocol
Recorded event types	All malware communication events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Seculert website ( <a href="https://www.seculert.com">https://www.seculert.com</a> )

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 458. Seculert log source parameters*

Parameter	Value
Log Source type	Seculert
Protocol Configuration	Seculert Protection REST API
API Key	32 character UUID For more information about obtaining an API key, see <a href="#">Obtaining an API key</a> .

### Related tasks:

[“Adding a DSM” on page 4](#)

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

[“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.

---

## 126 Sentrigo Hedgehog

You can integrate a Sentrigo Hedgehog device with IBM Security 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=osUser:20$|duser=$execUser:20$|
severity=$severity$|identHostName=$sourceHost$|src=$sourceIP$|
dst=$agent.ip$|devTime=$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|$serverVersion$|$rules.name:150$|
log.format.header.escaping.custom=\\|
log.format.header.separator.custom=,
log.format.header.escape.char.custom=\\
log.format.body.escaping.custom=\=
log.format.body.escape.char.custom=\\
log.format.body.separator.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

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

“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.



---

## 127 Skyhigh Networks Cloud Security Platform

The IBM Security QRadar DSM for Skyhigh Networks Cloud Security Platform DSM collects logs from a Skyhigh Networks Cloud Security Platform.

The following table identifies the specifications for the Skyhigh Networks Cloud Security Platform DSM:

*Table 459. Skyhigh Networks Cloud Security Platform DSM specifications*

Specification	Value
Manufacturer	Skyhigh Networks
DSM name	Skyhigh Networks Cloud Security Platform
RPM file name	DSM-SkyhighNetworksCloudSecurityPlatform-QRadar_version-build_number.noarch.rpm
Supported versions	2.4 and 3.3
Protocol	Syslog
Event format	LEEF
Recorded event types	Privilege Access, Insider Threat, Compromised Account, Access, Admin, Data, Policy, and Audit
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Skyhigh Networks website ( <a href="http://www.skyhighnetworks.com/">www.skyhighnetworks.com/</a> )

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 460. Skyhigh Networks Cloud Security Platform log source parameters*

Parameter	Value
Log Source type	Skyhigh Networks Cloud Security Platform
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the Skyhigh Networks Cloud Security Platform that sends events to QRadar.

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 461. Skyhigh Networks Cloud Security Platform sample message

Event name	Low level category	Sample log message
Login Success	User Login Success	<14>Mar 16 18:51:10 hostname LEEF:1.0 Skyhigh Anomalies 3.3.3.1  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 threshold Duration=daily thresholdValue=30 updatedOn=Jan 30 2017 07:08:05. 906 UTC

#### Related tasks:

"Adding a DSM" on page 4

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

"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:

Parameter	Value
SIEM server	ON
Format	Log Event Extended Format (LEEF)
Syslog Protocol	TCP
Syslog Server	<QRadar IP or hostname>
Syslog Port	514
Send to SIEM	new anomalies only

4. Click **Save**.

---

## 128 SolarWinds Orion

The IBM Security QRadar DSM for SolarWinds Orion collects events from a SolarWinds Orion appliance.

The following table describes the specifications for the SolarWinds Orion DSM:

*Table 462. SolarWinds Orion DSM specifications*

Specification	Value
Manufacturer	SolarWinds
DSM name	SolarWinds Orion
RPM file name	DSM-SolarWindsOrion-QRadar_version-build_number.noarch.rpm
Supported versions	2013.2.0
Protocol	SNMPv2 SNMPv3
Event format	name-value pair (NVP)
Recorded event types	All events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	SolarWinds website ( <a href="http://www.solarwinds.com/orion">http://www.solarwinds.com/orion</a> )

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 463. SolarWinds Orion sample message

Event name	Low level category	Sample log message
Domain controller UnManaged	Warning	<pre>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 1.3.6.1.6.3.1.1.4.3. 0=1.3.6.1.4.1.11307 1.3.6.1.4.1.1 1307.10.2=hostname 1.3.6.1.4.1.11 307.10.3=127.0.0.1 1.3.6.1.4.1.11 307.10.4=2466 1.3.6.1.4.1.11307.1 0.5=hostname 1.3.6.1.4.1.11307.10 .6=Node 1.3.6.1.4.1.11307.10.7=24 66 1.3.6.1.4.1.11307.10.1=InfoSec - EMAIL ONLY - Domain Controller Un Managed - hostname - Status = Un known 1.3.6.1.4.1.11307.10. 8=InfoSec -EMAIL ONLY - Domain Cont roller UnManaged hostname is Unknown.</pre>

#### Related tasks:

"Adding a DSM" on page 4

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

"Configuring a SolarWinds Orion log source by using the SNMP protocol" on page 844

Configure IBM Security QRadar to access your SolarWinds Orion appliance by using the SNMP protocol.

## Configuring SolarWinds Orion to communicate with QRadar

To collect events in IBM Security 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.

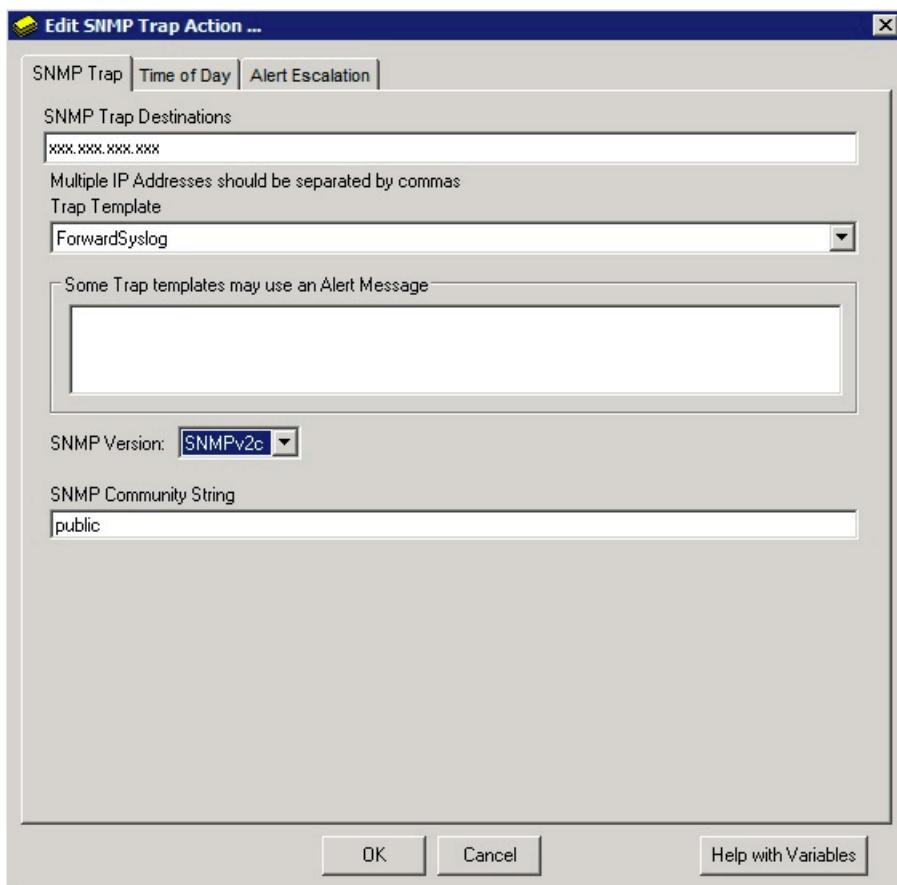


Figure 8. Edit SNMP Trap Action configuration for SNMPv2c

**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.

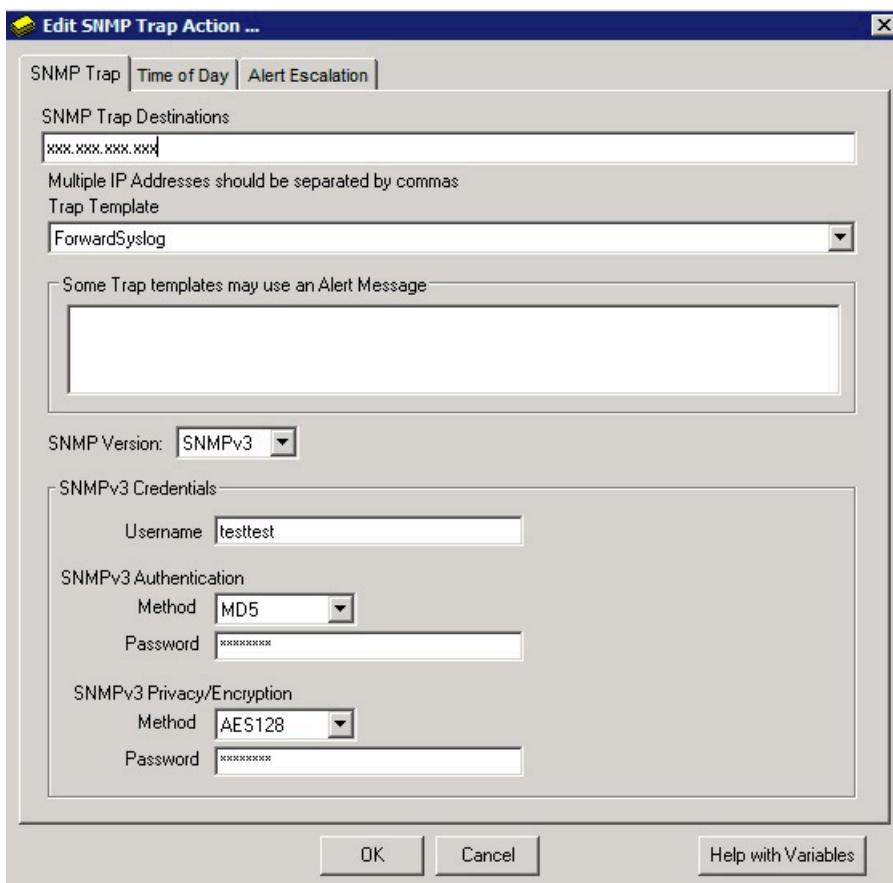


Figure 9. Edit SNMP Trap Action configuration for SNMPv3

**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

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

“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 Security 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 464. SNMPv2 log source parameters*

Parameter	Value
<b>Log Source Identifier</b>	Type the IP address or the host name of your SolarWinds Orion appliance to use as the identifier.
<b>Community</b>	Type the SNMP community name that was used when SNMP was configured on your SolarWinds Orion appliance.
<b>Include OIDs in Event Payload</b>	<p>To allow the SolarWinds Orion event payloads to be constructed as name-value pairs instead of the standard event payload format, select the <b>Include OIDs in Event Payload</b> check box.</p> <p><b>Important:</b> You must include OIDs in the event payload for processing SNMPv2 or SNMPv3 events for SolarWinds Orion.</p>

7. Optional: If you selected **SNMPv3**, configure the following specific log source parameters:

*Table 465. SNMPv3 log source parameters*

Parameter	Value
<b>Log Source Identifier</b>	Type the IP address or the host name of your SolarWinds Orion appliance to use as the identifier.
<b>Authentication Protocol</b>	<p>The algorithm that was used when SNMP was configured on your SolarWinds Orion appliance:</p> <ul style="list-style-type: none"> <li>• <b>MD5</b> uses Message Digest 5 (MD5) as your authentication protocol.</li> <li>• <b>SHA</b> uses Secure Hash Algorithm (SHA) as your authentication protocol.</li> </ul>
<b>Authentication Password</b>	The password that was used when SNMP was configured on your SolarWinds Orion appliance. Your authentication password must include a minimum of 8 characters.
<b>Decryption Protocol</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> </ul> <p><b>Note:</b> If you select AES192 or AES256 as your decryption algorithm, you must install the Java Cryptography Extension.</p>
<b>Decryption Password</b>	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.

Table 465. SNMPv3 log source parameters (continued)

Parameter	Value
User	The user name that was used when SNMP was configured on your SolarWinds Orion appliance.
Include OIDs in Event Payload	To allow the SolarWinds Orion event payloads to be constructed as name-value pairs instead of the standard event payload format, select the <b>Include OIDs in Event Payload</b> check box.  <b>Important:</b> You must include OIDs in the event payload for processing SNMPv2 or SNMPv3 events for SolarWinds Orion.

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

**Related tasks:**

“Installing the Java Cryptography Extension on QRadar” on page 613

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

### Procedure

1. Download the latest version of the JavaTM Cryptography Extension from the following website:  
<https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk>  
The JavaTM Cryptography Extension version must match the version of the Java™ installed on QRadar.
  2. Extract the JCE file.  
The following Java archive (JAR) files are included in the JCE download:
    - local\_policy.jar
    - US\_export\_policy.jar
  3. Log in to your QRadar Console or QRadar Event Collector as a root user.
  4. Copy the JCE JAR files to the following directory on your QRadar Console or Event Collector:  
`/usr/java/j2sdk/jre/lib/`
- 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`.

---

## 129 SonicWALL

The SonicWALL SonicOS DSM accepts events by using syslog.

IBM Security 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 Security 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 466. Syslog parameters

Parameter	Description
<b>Log Source Identifier</b>	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.

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 Security QRadar User Guide*.

---

## 130 Sophos

IBM Security QRadar supports a number of Sophos DSMs.

---

### Sophos Enterprise Console

IBM Security 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”
- “Configure IBM Security QRadar by using the JDBC protocol” on page 851

**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 concepts:**

“JDBC protocol configuration options” on page 16

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

**Related tasks:**

“Adding a DSM” on page 4

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

“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 using the Sophos Enterprise Console Protocol

The Sophos Enterprise Console DSM for IBM Security 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 467. Sophos Enterprise Console JDBC parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the identifier for the log source. Type the log source identifier in the following format:  <i>&lt;Sophos Database&gt;@&lt;Sophos Database Server IP or Host Name&gt;</i>  Where: <ul style="list-style-type: none"> <li>• <i>&lt;Sophos Database&gt;</i> is the database name, as entered in the <b>Database Name</b> parameter.</li> <li>• <i>&lt;Sophos Database Server IP or Host Name&gt;</i> is the host name or IP address for this log source, as entered in the <b>IP or Hostname</b> parameter.</li> </ul> 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.
<b>Database Type</b>	From the list, select <b>MSDE</b> .
<b>Database Name</b>	Type the exact name of the Sophos database.
<b>IP or Hostname</b>	Type the IP address or host name of the Sophos SQL Server.
<b>Port</b>	Type the port number that is used by the database server. The default port for <b>MSDE</b> 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 enabled to communicate with QRadar.  If you define a <b>Database Instance</b> when you use <b>MSDE</b> as the database type, you must leave the <b>Port</b> parameter blank in your configuration.
<b>Username</b>	Type the user name that is required to access the database.
<b>Password</b>	Type the password that is required to access the database. The password can be up to 255 characters in length.
<b>Confirm Password</b>	Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the <b>Password</b> parameter.
<b>Authentication Domain</b>	If you select <b>MSDE</b> as the <b>Database Type</b> and the database is configured for Windows, you must define a Window Authentication Domain. Otherwise, leave this field blank.
<b>Database Instance</b>	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 <b>Database Instance</b> parameter blank in your configuration.
<b>Table Name</b>	Type <i>vEventsCommonData</i> as the name of the table or view that includes the event records.

Table 467. Sophos Enterprise Console JDBC parameters (continued)

Parameter	Description
Select List	Type * for all fields from the table or view.  You can use a comma-separated list to define specific fields from tables or views, if this is needed for your configuration. The list must contain the field that is defined in the <b>Compare Field</b> 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 InsertedAt as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling.  The <b>Start Date and Time</b> 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.
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 that are entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the <b>Use Named Pipe Communications</b> 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.
Database Cluster Name	If you select the <b>Use Named Pipe Communication</b> check box, the <b>Database Cluster Name</b> 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.
Use NTLMv2	If you select MSDE as the <b>Database Type</b> , the <b>Use NTLMv2</b> check box is displayed.  Select the <b>Use NTLMv2</b> 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 <b>Use NTLMv2</b> check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.

**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.

9. Click **Save**.
10. On the Admin tab, click **Deploy Changes**.  
The configuration is complete.

## Configure IBM Security QRadar by using the JDBC protocol

The Sophos Enterprise Console DSM for IBM Security 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 Security 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:

```
CREATE VIEW threats_view AS SELECT t.ThreatInstanceID,
t.ThreatType, t.FirstDetectedAt, c.Name, c.LastLoggedOnUser,
c.IPAddress, c.DomainName, c.OperatingSystem, c.ServicePack,
t.ThreatSubType, t.Priority, t.ThreatLocalID,
t.ThreatLocalIDSource, t.ThreatName, t.FullFilePathCheckSum,
t.FullFilePath, t.FileNameOffset, tFileVersion, t.CheckSum,
t.ActionSubmittedAt, t.DealtWithAt, t.CleanUpable, t.IsFragment,
t.IsRebootRequired, t.Outstanding, t.Status, InsertedAt
FROM <Database Name>.dbo.ThreatInstancesAll
t, <Database Name>.dbo.Computers c
WHERE t.ComputerID = c.ID;
```

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.”

## Configuring a JDBC log source in QRadar

You can configure IBM Security QRadar to access the Sophos 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 Enterprise Console**.
7. From the Protocol Configuration list, select **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 DSM in QRadar.

8. Configure the following values:

Table 468. Sophos Enterprise Console JDBC parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the identifier for the log source. Type the log source identifier in the following format:  <i>&lt;Sophos Database&gt;@&lt;Sophos Database Server IP or Host Name&gt;</i>  Where: <ul style="list-style-type: none"> <li>• <i>&lt;Sophos Database&gt;</i> is the database name, as entered in the Database Name parameter.</li> <li>• <i>&lt;Sophos Database Server IP or Host Name&gt;</i> is the host name or IP address for this log source, as entered in the <b>IP or Hostname</b> parameter.</li> </ul> When defining 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.
<b>Database Type</b>	From the list, select <b>MSDE</b> .
<b>Database Name</b>	Type the exact name of the Sophos database.
<b>IP or Hostname</b>	Type the IP address or host name of the Sophos SQL Server.
<b>Port</b>	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 Sophos database. The Sophos database must have incoming TCP connections that are enabled to communicate with QRadar.  If you define a <b>Database Instance</b> when you use MSDE as the database type, you must leave the <b>Port</b> parameter blank in your configuration.
<b>Username</b>	Type the user name that is required to access the database.
<b>Password</b>	Type the password that is required to access the database. The password can be up to 255 characters in length.
<b>Confirm Password</b>	Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the <b>Password</b> parameter.
<b>Authentication Domain</b>	If you select <b>MSDE</b> as the <b>Database Type</b> and the database is configured for Windows, you must define a Window Authentication Domain. Otherwise, leave this field blank.
<b>Database Instance</b>	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 <b>Database Instance</b> parameter blank in your configuration.
<b>Table Name</b>	Type <code>threats_view</code> as the name of the table or view that includes the event records.
<b>Select List</b>	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 <b>Compare Field</b> 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(.)
<b>Compare Field</b>	Type <code>ThreatInstanceID</code> as the compare field. The compare field is used to identify new events added between queries to the table.

Table 468. Sophos Enterprise Console JDBC parameters (continued)

Parameter	Description
<b>Start Date and Time</b>	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.
<b>Use Prepared Statements</b>	Select this check box to use prepared statements.  Prepared statements give the JDBC protocol source the option 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.
<b>Polling Interval</b>	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.
<b>EPS Throttle</b>	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
<b>Use Named Pipe Communication</b>	Clear the <b>Use Named Pipe Communication</b> 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.
<b>Database Cluster Name</b>	If you select the <b>Use Named Pipe Communication</b> check box, the <b>Database Cluster Name</b> 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.

**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.

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

## Sophos PureMessage

The Sophos PureMessage DSM for IBM Security 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”
- “Integrating QRadar with Sophos PureMessage for Linux” on page 857

**Related concepts:**

“JDBC protocol configuration options” on page 16

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

**Related tasks:**

“Adding a DSM” on page 4

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

“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 “Configure a JDBC log source for Sophos PureMessage.”

## Configure a JDBC log source for Sophos PureMessage

You can configure QRadar to access the Sophos PureMessage for Microsoft Exchange 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 database configuration settings on your Sophos PureMessage device to define the parameters required to configure the Sophos PureMessage DSM in QRadar.

8. Configure the following values:

Table 469. Sophos PureMessage JDBC parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the identifier for the log source. Type the log source identifier in the following format:  <i>&lt;Sophos PureMessage Database&gt;@&lt;Sophos PureMessage Database Server IP or Host Name&gt;</i>  Where: <ul style="list-style-type: none"> <li>• <i>&lt;Sophos PureMessage Database&gt;</i> is the database name, as entered in the <b>Database Name</b> parameter.</li> <li>• <i>&lt;Sophos PureMessage Database Server IP or Host Name&gt;</i> is the host name or IP address for this log source, as entered in the <b>IP or Hostname</b> parameter.</li> </ul> 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.
<b>Database Type</b>	From the list, select <b>MSDE</b> .
<b>Database Name</b>	Type <b>savexquar</b> .
<b>IP or Hostname</b>	Type the IP address or host name of the Sophos PureMessage server.
<b>Port</b>	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 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 <b>Database Instance</b> parameter, you must leave the <b>Port</b> 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.
<b>Username</b>	Type the user name required to access the database.
<b>Password</b>	Type the password required to access the database. The password can be up to 255 characters in length.
<b>Confirm Password</b>	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the <b>Password</b> parameter.
<b>Authentication Domain</b>	If you select <b>MSDE</b> as the Database Type and the database is configured for Windows, you must define a Window Authentication Domain. Otherwise, leave this field blank.
<b>Database Instance</b>	Optional. Type the database instance, if you have multiple SQL server instances on your database server.  If you define a port number other than the default in the <b>Port</b> parameter, or block access to port 1434 for SQL database resolution, you must leave the <b>Database Instance</b> parameter blank.
<b>Table Name</b>	Type <b>siem_view</b> as the name of the table or view that includes the event records.

Table 469. Sophos PureMessage JDBC parameters (continued)

Parameter	Description
<b>Select List</b>	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 <b>Compare Field</b> 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(.)�.
<b>Compare Field</b>	Type ID. The Compare Field parameter is used to identify new events added between queries to the table.
<b>Use Prepared Statements</b>	Select this check box to use prepared statements.  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.  Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
<b>Start Date and Time</b>	Optional. Type the start date and time for database polling.  The <b>Start Date and Time</b> parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24-hour clock. If the <b>Start Date and Time</b> parameter is clear, polling begins immediately and repeats at the specified polling interval.
<b>Polling Interval</b>	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.
<b>Use Named Pipe Communication</b>	Clear the <b>Use Named Pipe Communication</b> check box.  When using a Named Pipe connection, the user name and password must be the appropriate Windows authentication username and password and not the database user name and password. Also, you must use the default Named Pipe.
<b>Database Cluster Name</b>	If you select the <b>Use Named Pipe Communication</b> check box, the <b>Database Cluster Name</b> 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.

**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**.

## Integrating QRadar with Sophos PureMessage for Linux

You can integrate IBM Security 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:

```

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 Security 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:

#### Sophos PureMessage JDBC parameters

Parameter	Description
<b>Log Source Identifier</b>	Type the identifier for the log source. Type the log source identifier in the following format:  <i>&lt;Sophos PureMessage Database&gt;@&lt;Sophos PureMessage Database Server IP or Host Name&gt;</i>  Where: <ul style="list-style-type: none"> <li>• <i>&lt;Sophos PureMessage Database&gt;</i> is the database name, as entered in the Database Name parameter.</li> <li>• <i>&lt;Sophos PureMessage Database Server IP or Host Name&gt;</i> is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.</li> </ul> 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.
<b>Database Type</b>	From the list, select <b>Postgres</b> .
<b>Database Name</b>	Type pmx_quarantine.

### Sophos PureMessage JDBC parameters

Parameter	Description
<b>IP or Hostname</b>	Type the IP address or host name of the Sophos PureMessage server.
<b>Port</b>	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.
<b>Username</b>	Type the user name required to access the database.
<b>Password</b>	Type the password required to access the database. The password can be up to 255 characters in length.
<b>Confirm Password</b>	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the <b>Password</b> parameter.
<b>Database Instance</b>	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 have blocked access to port 1434 for SQL database resolution, you must leave the <b>Database Instance</b> parameter blank in your configuration.
<b>Table Name</b>	Type <code>siem_view</code> as the name of the table or view that includes the event records.
<b>Select List</b>	Type <code>*</code> for all fields from the table or view.  You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the <b>Compare Field</b> 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(.)
<b>Compare Field</b>	Type ID.  The <b>Compare Field</b> parameter is used to identify new events added between queries to the table.
<b>Use Prepared Statements</b>	Select this check box to use prepared statements.  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.  Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
<b>Start Date and Time</b>	Optional. Type the start date and time for database polling.  The <b>Start Date and Time</b> parameter must be formatted as yyyy-MM-dd HH: mm with HH specified by using a 24-hour clock. If the <b>Start Date and Time</b> parameter is clear, polling begins immediately and repeats at the specified polling interval.
<b>Polling Interval</b>	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.

**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.

- Click **Save**.

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

---

## Sophos Astaro Security Gateway

The Sophos Astaro Security Gateway DSM for IBM Security QRadar accepts events by using syslog, enabling QRadar to 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

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

“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 Security 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

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

“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.



---

## 131 Splunk

IBM Security QRadar accepts and parses multiple event types that are forwarded from Splunk appliances.

For Check Point events that are forwarded from Splunk, see 33, "Check Point," on page 213.

---

### Collect Windows events that are forwarded from Splunk appliances

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 suggested. 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 Security 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:

*Table 470. TCP multiline syslog protocol parameters*

Parameter	Description
Protocol Configuration	<b>TCP Multiline Syslog</b>
Log Source Identifier	<p>Type the IP address or host name for the log source as an identifier for events from your Splunk appliance.</p> <p>The log source identifier must be unique value.</p>
Listen Port	<p>Type the port number that is used by QRadar to accept incoming TCP multi-line syslog events from Splunk.</p> <p>The default listen port is 12468.</p> <p><b>Important:</b> Do not use listen port 514.</p> <p>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.</p> <p>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.</p>
Aggregation Method	The default is <b>Start/End Matching</b> . If you want to combine multiline events that are joined by a common identifier, use <b>ID-Linked</b> .
Event Start Pattern	<p>Type the following regular expression (regex) to identify the start of your Splunk windows event:</p> <pre>(?:&lt;(\d+)&gt;\s?(\w{3} \d{2} \d{2}:\d{2}:\d{2}) (\S+) )?(\d{2}/\d{2}/\d{4} \d{2}:\d{2}:\d{2}:\d{2} [AP]M)</pre> <p>This parameter is available when you set the Aggregation Method parameter to <b>Start/End Matching</b>.</p> <p>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>
Event End Pattern	<p>This parameter is available when you set the Aggregation Method parameter to <b>Start/End Matching</b>.</p> <p>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.</p>

Table 470. TCP multiline syslog protocol parameters (continued)

Parameter	Description
Message ID Pattern	<p>This parameter is available when you set the <b>Aggregation Method</b> parameter to <b>ID-Linked</b>.</p> <p>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.</p>
Event Formatter	Use the <b>Windows Multiline</b> option for multiline events that are formatted specifically for Windows.
Show Advanced Options	The default is <b>No</b> . If you want to customize the event data, select <b>Yes</b> .
Use Custom Source Name	<p>This parameter is available when you set <b>Show Advanced Options</b> to <b>Yes</b>.</p> <p>Select the check box if you want to customize the source name with regex.</p>
Source Name Regex	<p>This parameter is available when you check <b>Use Custom Source Name</b>.</p> <p>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 <b>Source Name Formatting String</b> 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.</p>
Source Name Formatting String	<p>This parameter is available when you check <b>Use Custom Source Name</b>.</p> <p>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:</p> <ul style="list-style-type: none"> <li>One or more capture groups from the <b>Source Name Regex</b>. To refer to a capture group, use \x notation where x is the index of a capture group from the <b>Source Name Regex</b>.</li> <li>The IP address where the event data originated from. To refer to the packet IP, use the token \$PIP\$.</li> <li>Literal text characters. The entire <b>Source Name Formatting String</b> can be user-provided text. For example, if the <b>Source Name Regex</b> is 'hostname=(.*?)' and you want to append hostname.com to the capture group 1 value, set the <b>Source Name Formatting String</b> 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 <b>Log Source Identifier</b>.</li> </ul>
Use as a Gateway Log Source	<p>This parameter is available when you set <b>Show Advanced Options</b> to <b>Yes</b>.</p> <p>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.</p> <p>When this option is not selected and <b>Use Custom Source Name</b> is not checked, incoming events are tagged with a source name that corresponds to the <b>Log Source Identifier</b> parameter.</p>
Flatten Multiline Events into Single Line	This parameter is available when you set <b>Show Advanced Options</b> to <b>Yes</b> . Shows an event in one single line or multiple lines.
Retain Entire Lines during Event Aggregation	<p>This parameter is available when you set <b>Show Advanced Options</b> to <b>Yes</b>.</p> <p>If you set the <b>Aggregation Method</b> parameter to <b>ID-Linked</b>, you can enable <b>Retain Entire Lines during Event Aggregation</b> to either discard or keep the part of the events that comes before <b>Message ID Pattern</b> when events are concatenated with the same ID pattern together.</p>

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.

---

## 132 Squid Web Proxy

The Squid Web Proxy DSM for IBM Security 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:

`access_log /path/to/access.log common`

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 Security 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:

*Table 471. Syslog parameters*

Parameter	Description
<b>Log Source Identifier</b>	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.

---

## 133 SSH CryptoAuditor

The IBM Security QRadar DSM for SSH CryptoAuditor collects logs from an SSH CryptoAuditor.

The following table identifies the specifications for the SSH CryptoAuditor DSM.

*Table 472. SSH CryptoAuditor DSM specifications*

Specification	Value
Manufacturer	SSH Communications Security
Product	CryptoAuditor
DSM Name	SSH CryptoAuditor
RPM filename	DSM-SSHCryptoAuditor-QRadar_release-Build_number.noarch.rpm
Supported versions	1.4.0 or later
Event format	Syslog
QRadar recorded event types	Audit, Forensics
Log source type in QRadar UI	SSH CryptoAuditor
Auto discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	SSH Communications Security website ( <a href="http://www.ssh.com/">http://www.ssh.com/</a> )

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

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
  - DSMCommon RPM
  - SSH CryptoAuditor RPM
2. For each instance of SSH CryptoAuditor, configure your SSH CryptoAuditor system to communicate with QRadar.
3. If QRadar does not automatically discover SSH CryptoAuditor, create a log source on the QRadar Console for each instance of SSH CryptoAuditor. Use the following SSH CryptoAuditor specific parameters:

Parameter	Value
Log Source Type	SSH CryptoAuditor
Protocol Configuration	Syslog

**Related tasks:**

[“Configuring an SSH CryptoAuditor appliance to communicate with QRadar” on page 870](#)

To collect SSH CryptoAuditor events, you must configure your third-party appliance to send events to IBM Security QRadar.

[“Adding a DSM” on page 4](#)

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

---

## Configuring an SSH CryptoAuditor appliance to communicate with QRadar

To collect SSH CryptoAuditor events, you must configure your third-party appliance to send events to IBM Security QRadar.

### Procedure

1. Log in to SSH CryptoAuditor.
2. Go to the syslog settings in **Settings > External Services > External Syslog Servers**.
3. To create server settings for QRadar, click **Add Syslog Server**.
4. Type the QRadar server settings: address (IP address or FQDN) and port in which QRadar collects log messages.
5. To set the syslog format to Universal LEEF, select the **Leef format** check box.
6. To save the configuration, click **Save**.
7. Configure SSH CryptoAuditor alerts in **Settings > Alerts**. The SSH CryptoAuditor alert configuration defines which events are sent to external systems (email or SIEM/syslog).
  - a. Select an existing alert group, or create new alert group by clicking **Add alert group**.
  - b. Select the QRadar server that you defined earlier in the **External Syslog Server** drop box.
  - c. If you created a new alert group, click **Save**. Save the group before binding alerts to the group.
  - d. Define which alerts are sent to QRadar by binding alerts to the alert group. Click **[+]** next to the alert that you want to collect in QRadar, and select the alert group that has QRadar as external syslog server. Repeat this step for each alert that you want to collect in QRadar.
  - e. Click **Save**.
8. Apply the pending configuration changes. The saved configuration changes do not take effect until you apply them from pending state.

---

## 134 Starent Networks

The Starent Networks DSM for IBM Security 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 473. Syslog server parameters

Parameter	Description
syslog <IP address>	Type the IP address of your QRadar
facility <facilities>	Type the local facility for which the logging options are applied. The options are as follows: <ul style="list-style-type: none"><li>• local0</li><li>• local1</li><li>• local2</li><li>• local3</li><li>• local4</li><li>• local5</li><li>• local6</li><li>• local7</li></ul> The default is local7.
rate value	Type the rate that you want log entries to be sent to the system log server. This value must be an integer 0 - 100000. The default is 1000 events per second.
pdu-verbosity <pdu-level>	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.
pdu-data <format>	Type the output format for the PDU when logged as one of following formats: <ul style="list-style-type: none"><li>• none - Displays results in raw or unformatted text.</li><li>• hex - Displays results in hexadecimal format.</li><li>• hex-ascii - Displays results in hexadecimal and ASCII format similar to a main frame dump.</li></ul>

Table 473. Syslog server parameters (continued)

Parameter	Description
event-verbosity <event_level>	Type the level of detail you want to use in logging of events, that includes: <ul style="list-style-type: none"><li>• min - Provides minimal information about the event, such as, event name, facility, event ID, severity level, data, and time.</li><li>• concise - Provides detailed information about the event, but does not provide the event source.</li><li>• full - Provides detailed information about the event and includes the source information that identifies the task or subsystem that generated the event.</li></ul>

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 474. Trace log parameters

Parameter	Description
callid <call_id>	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.
ipaddr <IP address>	Indicates a trace log is generated for a session that is identified by the specified IP address.
msid <ms_id>	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.
name <username>	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.

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 475. Active log parameters

Parameter	Description
facility <facility>	<p>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:</p> <ul style="list-style-type: none"> <li>• local0</li> <li>• local1</li> <li>• local2</li> <li>• local3</li> <li>• local4</li> <li>• local5</li> <li>• local6</li> <li>• local7</li> </ul> <p>The default is local7.</p>
level <report_level>	<p>Type the log severity level, including:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• warning - Logs events that can indicate a potential problem. This level also logs events with a higher severity level.</li> <li>• unusual - Logs events that are unusual and might need to be investigated. This level also logs events with a higher severity level.</li> <li>• info - Logs informational events and events with a higher severity level.</li> <li>• debug - Logs all events regardless of the severity.</li> </ul> <p>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.</p>
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 476. Monitor log parameters

Parameter	Description
msid <md_id>	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.

*Table 476. Monitor log parameters (continued)*

Parameter	Description
username <username>	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.

7. You are now ready to configure the log source in QRadar.

To configure QRadar to receive events from a Starent device:

- 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](#)

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

[“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.

---

## 135 STEALTHbits

IBM Security QRadar supports a range of STEALTHbits DSMs.

### STEALTHbits StealthINTERCEPT

The IBM Security 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 477. STEALTHbits StealthINTERCEPT DSM specifications*

Specification	Value
Manufacturer	STEALTHbits Technologies
DSM	STEALTHbits StealthINTERCEPT
RPM file name	DSM-STEALTHbitsStealthINTERCEPT-QRadar_Version-build_number.noarch.rpm
Supported versions	3.3
Protocol	Syslog
Event format	LEEF
QRadar recorded events	Active Directory Audit Events, File Activity Monitor Events
Automatically discovered	Yes
Includes identity	No
More information	<a href="http://www.stealthbits.com/resources">http://www.stealthbits.com/resources</a>

### Configuring a STEALTHbits StealthINTERCEPT log source in IBM Security 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 Security QRadar as the syslog server and configure the message format.

## Procedure

1. Log in to your STEALTHbits StealthINTERCEPT server.
2. Start the Administration Console.
3. Click **Configuration > Syslog Server**.
4. Configure the following parameters:

Table 478. Syslog parameters

Parameter	Description
Host Address	The IP address of the QRadar Console
Port	514

5. Click **Import mapping file**.
6. Select the `SyslogLeefTemplate.txt` file and press Enter.
7. Click **Save**.
8. On the Administration Console, click **Actions**.
9. Select the mapping file that you imported, and then select the **Send to Syslog** check box.  
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 Security 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:

Parameter	Description
Bulk Syslog server in SERVER[:PORT] format	<QRadar event collector IP address>:514  Example: 192.0.2.1:514  <qradarhostname>:514
Syslog message template file path	<code>SyslogLeefTemplate.txt</code>  The template is stored in the STEALTHbits File Activity Monitor Install Directory

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 479. STEALTHbits StealthINTERCEPT and STEALTHbits File Activity Monitor sample event message supported by the STEALTHbits StealthINTERCEPT DSM*

Event name	Low level category	Sample log message
Active Directory Group Created	Group Added	LEEF:1.0 STEALTHbits StealthINTERCEPT <IP_address> Active Directorygroup Object AddedTrueFalse cat=Object Added devTimeFormat=yyyy-MM-dd HH:mm:ss.SSS devTime=2013-10-24 15:41:38.387 SettingName=A11 AD Changes domain=<Domain> usrName=CN=Administrator, CN=Users, DC=<Domain_controller>, DC=com src=LDAP: [<Source_IPv6_address>]:60843 DistinguishedName= cn=asdfasfasdf, OU=<City>, OU=<State>, DC=<Domain_controller>, DC=com ClassName=group OrigServer=<Server> Success=True Blocked=False AttNames= AttNewValues= AttOldValues=

*Table 479. STEALTHbits StealthINTERCEPT and STEALTHbits File Activity Monitor sample event message supported by the STEALTHbits StealthINTERCEPT DSM (continued)*

Event name	Low level category	Sample log message
Windows File System Folder or File Delete	File Deleted	<pre>L00F:1.0 STEALTHbits  STEALTHbits Technologies File Monitoring  2,3,0,402 Windows File SystemDeleteTrueFalse  cat=Delete devTimeFormat=yyyy-MM-dd HH:mm:ss.SSS devTime=2016-04-19 13:15:12.000 SettingName=FileMonitor domain=&lt;Domain&gt; usrName=&lt;Domain&gt;\&lt;Username&gt; src=&lt;IP_address&gt; DistinguishedName=C:\Share1_CIFS_volume\1(2) - Copy ClassName= OrigServer=&lt;Server&gt; Success=True Blocked=False AttrName= AttrNewValue= AttrOldValue= Operation=</pre>

## STEALTHbits StealthINTERCEPT Alerts

IBM Security QRadar collects alerts logs from a STEALTHbits StealthINTERCEPT server by using STEALTHbits StealthINTERCEPT Alerts DSM

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT Alerts DSM:

*Table 480. STEALTHbits StealthINTERCEPT Alerts DSM specifications*

Specification	Value
Manufacturer	STEALTHbits Technologies
DSM name	STEALTHbits StealthINTERCEPT Alerts
RPM file name	DSM-STEALTHbitsStealthINTERCEPTAlerts-Qradar_version-build_number.noarch.rpm
Supported versions	3.3
Protocol	Syslog L00F
Recorded event types	Active Directory Alerts Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	<a href="http://www.stealthbits.com/products/stealthintercept">StealthINTERCEPT</a> ( <a href="http://www.stealthbits.com/products/stealthintercept">http://www.stealthbits.com/products/stealthintercept</a> )

To integrate STEALTHbits StealthINTERCEPT with QRadar, complete the following steps:

- 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
- Configure your STEALTHbits StealthINTERCEPT device to send syslog events to QRadar.
- 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 481. STEALTHbits StealthINTERCEPT Alerts log source parameters*

Parameter	Value
Log Source type	STEALTHbits StealthINTERCEPT Alerts
Protocol Configuration	Syslog

#### Related tasks:

“Adding a DSM” on page 4

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

“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 Security QRadar as the syslog server and configure the message format.

### Procedure

- Log in to your STEALTHbits StealthINTERCEPT server.
- Start the Administration Console.
- Click **Configuration > Syslog Server**.
- Configure the following parameters:

Parameter	Description
Host Address	The IP address of the QRadar Console
Port	514

- Click **Import mapping file**.
- Select the **SyslogLeefTemplate.txt** file and press Enter.
- Click **Save**.
- On the Administration Console, click **Actions**.
- 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.

- Click **Add**.

## STEALTHbits StealthINTERCEPT Analytics

IBM Security QRadar collects analytics logs from a STEALTHbits StealthINTERCEPT server by using STEALTHbits StealthINTERCEPT Analytics DSM.

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT Analytics DSM:

*Table 482. STEALTHbits StealthINTERCEPT Analytics DSM specifications*

Specification	Value
Manufacturer	STEALTHbits Technologies
DSM name	STEALTHbits StealthINTERCEPT Analytics
RPM file name	DSM-STEALTHbitsStealthINTERCEPTAnalytics-Qradar_version-build_number.noarch.rpm
Supported versions	3.3
Protocol	Syslog LEEF
Recorded event types	Active Directory Analytics Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	StealthINTERCEPT ( <a href="http://www.stealthbits.com/products/stealthintercept">http://www.stealthbits.com/products/stealthintercept</a> )

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 483. STEALTHbits StealthINTERCEPT Analytics log source parameters*

Parameter	Value
Log Source type	STEALTHbits StealthINTERCEPT Analytics
Protocol Configuration	Syslog

### Related tasks:

“Adding a DSM” on page 4

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

“Collecting analytics logs from STEALTHbits StealthINTERCEPT” on page 881

To collect all analytics logs from STEALTHbits StealthINTERCEPT, you must specify IBM Security QRadar as the syslog server and configure the message format.

“Adding a log source” on page 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 Security QRadar as the syslog server and configure the message format.

### Procedure

1. Log in to your STEALTHbits StealthINTERCEPT server.
2. Start the Administration Console.
3. Click **Configuration > Syslog Server**.
4. Configure the following parameters:

Parameter	Description
Host Address	The IP address of the QRadar Console
Port	514

5. Click **Import mapping file**.
6. Select the **SyslogLeafTemplate.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**.



---

## 136 Sun

IBM Security 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 49](#)

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](#)

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

[“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:

Parameter	Description
<b>Log Source Identifier</b>	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.
<b>Service Type</b>	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535. The options include:  <b>FTP</b> TCP Port 21. <b>SFTP</b> TCP Port 22. <b>SCP</b> TCP Port 22. <b>Important:</b> 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.
<b>Remote User</b>	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.
<b>Confirm Password</b>	Confirm the password necessary to log in to the host.

Parameter	Description
<b>SSH Key File</b>	If you select SCP or SFTP as the <b>Service Type</b> , this parameter enables you to define an SSH private key file. When you provide an SSH Key File, the <b>Remote Password</b> field is ignored.
<b>Remote Directory</b>	<p>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.</p> <p><b>Important:</b> 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.</p>
<b>Recursive</b>	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 <b>Recursive</b> option is not available for SCP connections.
<b>FTP File Pattern</b>	<p>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.</p> <p>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>)</p>
<b>FTP Transfer Mode</b>	<p>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.</p> <p>From the list box, select the transfer mode that you want to apply to this log source:</p> <ul style="list-style-type: none"> <li><b>Binary</b> Select <b>Binary</b> for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files.</li> <li><b>ASCII</b> Select <b>ASCII</b> for log sources that require an ASCII FTP file transfer.</li> </ul> <p><b>Important:</b> You must select <b>NONE</b> for the <b>Processor</b> parameter and <b>LINEBYLINE</b> the <b>Event Generator</b> parameter when you use ASCII as the FTP Transfer Mode.</p>
<b>SCP Remote File</b>	If you select SCP as the <b>Service Type</b> you must type the file name of the remote file.
<b>Start Time</b>	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.

Parameter	Description
<b>Recurrence</b>	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.
<b>Run On Save</b>	<p>Select this check box if you want the log file protocol to run immediately after you click <b>Save</b>. After the <b>Run On Save</b> completes, the log file protocol follows your configured start time and recurrence schedule.</p> <p>Selecting <b>Run On Save</b> clears the list of previously processed files for the <b>Ignore Previously Processed File</b> parameter.</p>
<b>EPS Throttle</b>	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.
<b>Processor</b>	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.
<b>Ignore Previously Processed File(s)</b>	<p>Select this check box to track files that were processed and you do not want the files to be processed a second time.</p> <p>This only applies to FTP and SFTP Service Types.</p>
<b>Change Local Directory?</b>	<p>Select this check box to define the local directory on your QRadar that you want to use for storing downloaded files during processing.</p> <p>Most configurations can leave this check box clear. When you select the check box, the <b>Local Directory</b> field is displayed, which enables you to configure a local directory to use for temporarily storing files.</p>
<b>Event Generator</b>	<p>Select <b>ID-Linked Multiline</b> to process to the retrieved event log as multiline events.</p> <p>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 <b>Message ID Pattern</b> field that uses regex to identify and reassemble the multiline event in to single event payload.</p>
<b>Folder Separator</b>	<p>Type the character that is used to separate folders for your operating system. The default value is /.</p> <p>Most configurations can use the default value in the <b>Folder Separator</b> 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.</p>

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 484. Sun ONE LDAP UDP Multiline Syslog log source parameters*

Parameter	Description
<b>Log Source Identifier</b>	Type the IP address, host name, or name to identify your Sun ONE LDAP installation.
<b>Listen Port</b>	Type 517 as the port number used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65535.  To edit a saved configuration to use a new port number complete the following steps. 1. In the <b>Listen Port</b> field, type the new port number for receiving UDP Multiline Syslog events. 2. Click <b>Save</b> .  The port update is complete and event collection starts on the new port number.
<b>Message ID Pattern</b>	Type the following regular expression (regex) needed to filter the event payload messages.  conn=(\d+)
<b>Enabled</b>	Select this check box to enable the log source.
<b>Credibility</b>	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.
<b>Target Event Collector</b>	Select the <b>Target Event Collector</b> to use as the target for the log source.
<b>Coalescing Events</b>	Select this check box to enable the log source to coalesce (bundle) events.  By default, automatically discovered log sources inherit the value of the <b>Coalescing Events</b> 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.
<b>Store Event Payload</b>	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 <b>Store Event Payload</b> 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**.

## Sun Solaris DHCP

IBM Security 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**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

*Table 485. Syslog parameters*

Parameter	Description
<b>Log Source Identifier</b>	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.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The log source is added to IBM Security 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 Security 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 888.

<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 Security 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 Security 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;auth.notice;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 Security 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 Security QRadar automatically discovers and creates a log source for syslog events from Sun Solaris Sendmail appliances.

### About this task

The following configuration steps are optional.

## 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 486. Syslog parameters

Parameter	Description
<b>Log Source Identifier</b>	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.

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 Security 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:  
`/etc/security/bsmconv`  
The bsmconv script enables Solaris Basic Security Mode and starts the auditing service audittd.
4. Type the following command to open the audit control log for editing:  
`vi /etc/security/audit_control`
5. Edit the audit control file to contain the following information:  
`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 audittd.
7. Type the following command to verify that audittd starts :  
`/usr/sbin/auditconfig -getcond`  
If the audittd process is started, the following string is returned:  
`audit condition = auditing`

#### **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 audidd process is started, the following string is returned:

```
audit condition = auditing
```

Converting Sun Solaris BSM audit logs

IBM Security 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:

```
#!/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 $AUDIT_DIR # in case it is a link #
Get a listing of the files based on creation date that are not current in use
FILES=$(ls -lrt | tr -s " " | cut -d" " -f9 | grep -v "not_terminated")
# We just created a new audit log by doing 'audit -n',
so we can # be sure that the last file in the list will be the
latest # archived binary log file.
lastFile="" for file in $FILES; do
    lastFile=$file
done
# Extract a human-readable file from the binary log file
echo "Beginning praudit of $lastFile"
praudit -l $lastFile > "$LOG_DIR$lastFile.log" echo "Done praudit,
creating log file at: $LOG_DIR$lastFile.log"
/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 891.
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 Security 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 Security 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**.
6. Using the **Protocol Configuration** list, select **Log File**.
7. Configure the following parameters:

Table 487. Log file parameters

| Parameter | Description |
|------------------------------|--|
| Log Source Identifier | Type the IP address or host name for the log source. The log source identifier must be unique for the log source type. |

Table 487. Log file parameters (continued)

| Parameter | Description |
|------------------------------|--|
| Service Type | <p>From the list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP.</p> <ul style="list-style-type: none"> SFTP - SSH File Transfer Protocol FTP - File Transfer Protocol SCP - Secure Copy <p>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.</p> |
| Remote IP or Hostname | Type the IP address or host name of the Sun Solaris BSM system. |
| Remote Port | <p>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.</p> <p>The valid range is 1 - 65535.</p> |
| Remote User | <p>Type the user name necessary to log in to your Sun Solaris system.</p> <p>The user name can be up to 255 characters in length.</p> |
| Remote Password | Type the password necessary to log in to your Sun Solaris system. |
| Confirm Password | Confirm the Remote Password to log in to your Sun Solaris system. |
| SSH Key File | If you select SCP or SFTP from the Service Type field you can define a directory path to an SSH private key file. The SSH Private Key File gives the option to ignore the Remote Password field. |
| Remote Directory | 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. |
| Recursive | Select this check box if you want the file pattern to also search sub folders. The Recursive parameter is not used if you configure SCP as the Service Type. By default, the check box is clear. |
| FTP File Pattern | <p>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.</p> <p>For example, if you want to retrieve all files in the <starttime>.<endtime>.<hostname>.log format, use the following entry:
 <code>\d+\.\d+\.\w+\.\log</code>.</p> <p>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/</p> |
| FTP Transfer Mode | <p>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.</p> <p>From the list, select the transfer mode that you want to apply to this log source:</p> <ul style="list-style-type: none"> 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 use the 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. |

Table 487. Log file parameters (continued)

| Parameter | Description |
|--|---|
| 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 processed. |
| Ignore Previously Processed File(s) | 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. |
| Change Local Directory? | Select this check box to define the local directory on your QRadar system that you want to use for storing downloaded files during processing. 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. |
| Event Generator | From the Event Generator list, select LINEBYLINE . |

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.

137 Sybase ASE

You can integrate a Sybase Adaptive Server Enterprise (ASE) device with IBM Security 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:

```
isql -Usa -P<password>
```

Where <password> is the password necessary to access the database.

3. Switch to the security database:

- use sybsecurity
- go

4. Create a view for IBM Security QRadar SIEM.

- create view audit_view
- as
- select audit_event_name(event) as event_name, * from <audit_table_1>
- union
- select audit_event_name(event) as event_name, * from <audit_table_2>
- go

5. For each additional audit table in the audit configuration, make sure that the **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:

- create view audit_view as select audit_event_name(event) as event_name, * from sysaudits_01
- union select audit_event_name(event) as event_name, * from sysaudits_02,
- union select audit_event_name(event) as event_name, * from sysaudits_03,
- union select audit_event_name(event) as event_name, * from sysaudits_04

What to do next

You can now configure the log source IBM Security QRadar SIEM.

Related concepts:

“JDBC protocol configuration options” on page 16

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

Related tasks:

“Adding a DSM” on page 4

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

"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 QRadar SIEM to receive events from a Sybase ASE device

You can configure QRadar SIEM to receive events from a Sybase ASE device:

Procedure

1. Log in to QRadar SIEM.
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 the **Sybase ASE** option.
7. Using the **Protocol Configuration** list, select **JDBC**.
The JDBC protocol configuration is displayed.
8. Update the JDBC configuration to include the following values:
 - **Database Name:** **sybsecurity**
 - **Port:** **5000 (Default)**
 - **Username:** **sa**
 - **Table Name:** **audit_view**
 - **Compare Field:** **eventtime**

The **Database Name** and **Table Name** parameters are case-sensitive.

For more information about the Sybase ASE device, see your vendor documentation.

138 Symantec

IBM Security QRadar supports a number of Symantec DSMs.

Symantec Critical System Protection

The IBM Security QRadar DSM for Symantec Critical System Protection can collect event logs from Symantec Critical System Protection systems.

The following table identifies the specifications for the Symantec Critical System Protection DSM.

Table 488. Symantec Critical System Protection DSM specifications

| Specification | Value |
|------------------------------|---|
| Manufacturer | Symantec |
| DSM Name | Critical System Protection |
| RPM file name | DSM-SymantecCriticalSystemProtection-Qradar_version_build_number.noarch.rpm |
| Supported versions | 5.1.1 |
| Event format | DB Entries |
| QRadar recorded event types | All events from the 'CSPEVENT_VW' view |
| Log source type in QRadar UI | Symantec Critical System Protection |
| Auto discovered? | No |
| Includes identity? | No |
| Includes custom properties | No |
| For more information | Symantec Web Page (http://www.symantec.com/) |

To integrate Symantec Critical System Protection with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most current version of the following RPMs on your QRadar Console:
 - Protocol-JDBC RPM
 - Symantec Critical System Protection RPM
2. For each Symantec Critical System Protection instance, configure Symantec Critical System Protection to enable communication with QRadar.
Ensure that QRadar can poll the database for events by using TCP port 1433 or the port that is configured for your log source. Protocol connections are often disabled on databases and extra configuration steps are required in certain situations to allow connections for event polling. Configure firewalls that are located between Symantec Critical System Protection and QRadar to allow traffic for event polling.
3. If QRadar does not automatically discover Symantec Critical System Protection, create a log source for each Symantec Critical System Protection instance on the QRadar Console. Use the following values for the required log source parameters:

| Parameter | Description |
|------------------------|-------------------------------------|
| Log Source Type | Symantec Critical System Protection |
| Protocol Configuration | JDBC |
| Database Type | MSDE |

| Parameter | Description |
|---------------|-------------|
| Instance | SCSP |
| Database Name | SCSPDB |
| Table Name | CSPEVENT_VW |
| Compare Field | EVENT_ID |

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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**.
Configure the following values:
 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:
- Host** - Type the IP address of your IBM Security QRadar.
13. **Port** - Type 514 as the syslog port.
14. **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=$INCIDENT_SNAPSHOT$  
|subject=$SUBJECT$|fileName=$FILE_NAME$|parentPath=$PARENT_PATH$  
|path=$PATH$|quarantineParentPath=$QUARANTINE_PARENT_PATH$  
|scan=$SCAN$|target=$TARGET$
```

15. **Level** - From this list, select **6 - Informational**.
16. 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

- From the menu, select the **Manage > Policies > Response Rules**.
- Click **Add Response Rule**.
- 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.
- Click **Next**.
Configure the following values:
 - 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
 - Description** - Optional. Type a description for the rule you are creating.
- Click **Add Condition**.
- 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**.
- On the Actions pane, click **Add Action**.
- From the **Actions** list, select **All: Log to a Syslog Server**.
- Configure the following options:
 - Host** - Type the IP address of your QRadar.
- 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 Security QRadar.

Configuring a log source

You can configure the log source in IBM Security 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 Security 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 Security 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 Security 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 Security 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 489. Symantec Endpoint Protection DSM specifications

| Specification | Value |
|-----------------------------|--|
| Manufacturer | Symantec |
| DSM name | Symantec Endpoint Protection |
| RPM file name | DSM-SymantecEndpointProtection-QRadar_version-build_number.noarch.rpm |
| Supported versions | Endpoint Protection V11, V12, and V14 |
| Protocol | Syslog |
| Event format | Syslog |
| Recorded event types | All Audit and Security Logs |
| Automatically discovered? | Yes |
| Includes identity? | No |
| Includes custom properties? | No |
| More information | Symantec website (https://www.symantec.com) |

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:

Table 490. Symantec Endpoint Protection log source parameters

| Parameter | Value |
|------------------------|--|
| Log Source type | Symantec Endpoint Protection |
| Protocol Configuration | Syslog |
| Log Source Identifier | Type a unique identifier for the log source. |

4. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Symantec Endpoint Protection:

Table 491. Symantec Endpoint Protection sample message

| Event name | Low level category | Sample log message |
|------------|--------------------|---|
| Blocked | Access Denied | <51>Mar 3 13:52:13 <Server> SymantecServer: USER,<IP_address>, Blocked,[AC13-1.5] Block from loading other DLLs - Caller MD5=xxxxxx xxxxxxxxxxxxxxxxxxxxxxxx,Load D1 1,Begin: 2017-03-03 13:48:18,End: 2 017-03-03 13:48:18,Rule: Corp Endpoint - Brower Restrictions [AC13-1.5] Block from loading other DLLs, 6804,C:/Program Files (x86)/Microsoft Office/Office14/WINPROJ.EXE,0,N o Module Name,C:/Users/USER/AppData/Local/assembly/d13/DMD7K 4QX.8GW/WQ9LV1W4.8HL/e705c114/00 6fef9d_f364d101/ProjectPublisher 2010.DLL,User: USER,Domain : LAB,Action Type: ,File size (bytes): 4216832,Device ID: SCSI\Disk&Ven_ATA&Prod_SAMSUNG_SSD_PM83\4&27c82505&0&000000 |

Related tasks:

“Adding a DSM” on page 4

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

“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

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

"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 PGP Universal Server

The PGP Universal Server DSM for IBM Security QRadar accepts syslog events from PGP Universal Servers.

QRadar accepts 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 PGP Universal Server events with QRadar, you must enable and configure PGP Universal Server to forward syslog events to QRadar.

Configuring syslog for PGP Universal Server

You can enable external logging to forward syslog events to IBM Security QRadar.

Procedure

1. In a web browser, log in to your PGP server's administrative interface.

`https://<PGP 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 PGP Universal Server events are automatically discovered. Events that are forwarded to QRadar by the PGP Universal Servers are displayed on the **Log Activity** tab of QRadar.

Configuring a log source

IBM Security QRadar automatically discovers and creates a log source for syslog events from PGP Universal Servers.

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 **PGP Universal Server**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 492. 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 PGP Universal Server. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

Symantec SGS

The Symantec Gateway Security (SGS) Appliance DSM for IBM Security 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

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

“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 Security 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 Security 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,
- dbo.inventory.Computer AS computer_name,
- dbo.virus.Virusname AS virus_name,
- dbo.alerts.Filepath AS filepath,
- dbo.alerts.NoOfViruses AS no_of_virus,
- dbo.actualaction.Actualaction AS [action],
- dbo.alerts.Alertdatetime AS [date],
- dbo.clientuser.Clientuser AS user_name FROM
- dbo.alerts INNER JOIN
- dbo.virus ON dbo.alerts.Virusname_Idx = dbo.virus.Virusname_Idx INNER JOIN
- dbo.inventory ON dbo.alerts.Computer_Idx = dbo.inventory.Computer_Idx INNER JOIN
- dbo.actualaction ON dbo.alerts.Actualaction_Idx =
- dbo.actualaction.Actualaction_Idx INNER JOIN
- dbo.clientuser ON dbo.alerts.Clientuser_Idx = dbo.clientuser.Clientuser_Idx

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

You can configure IBM Security QRadar to access the SSC 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**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. Using the **Log Source Type** list, select **Symantec System Center**.
7. Using the **Protocol Configuration** list, select **JDBC**.
8. Configure the following parameters:

Table 493. Symantec System Center JDBC parameters

| Parameter | Description |
|------------------------------|---|
| Log Source Identifier | Type the identifier for the log source. Type the log source identifier in the following format:

<i><SSC Database>@<SSC Database Server IP or Host Name></i>

Where: <ul style="list-style-type: none"> • <i><SSC Database></i> is the database name, as entered in the Database Name parameter. • <i><SSC Database Server IP or Host Name></i> is the host name or IP address for this log source, as entered in the IP or Hostname parameter. |
| Database Type | From the list, select MSDE . |
| Database Name | Type 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 parameter 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 parameter. |
| Authentication Domain | If you select MSDE as the Database Type and the database is configured for Windows, you must define a Windows Authentication Domain. Otherwise, leave this field blank. |
| Database Instance | 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. |
| Table Name | Type vw_qradar as the name of the table or view that includes the event records. |
| Select List | Type * 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(.). |
| Compare Field | Type idx as the compare field. The compare field is used to identify new events added between queries to the table. |
| Start Date and Time | Optional. Type the start date and time for database polling.

The Start Date and Time parameter must be formatted as yyyy-MM-dd HH: mm with HH specified you use a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval. |

Table 493. Symantec System Center JDBC parameters (continued)

| Parameter | Description |
|-------------------------------------|--|
| Use Prepared Statements | 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. |
| 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 that are entered without an H or M poll in seconds. |
| EPS Throttle | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS. |
| Use Named Pipe Communication | Clear the Use Named Pipe Communication check box.

When using a Named Pipe connection, the user name and password must be the appropriate Windows authentication user name and password and not the database user name and password. Also, you must use the default Named Pipe. |
| Database Cluster Name | If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly. |

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.

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

The configuration is complete.

139 Sourcefire Intrusion Sensor

The Sourcefire Intrusion Sensor DSM for IBM Security QRadar accepts Snort based intrusion and prevention syslog events from Sourcefire devices.

Configuring Sourcefire Intrusion Sensor

To configure your Sourcefire Intrusion Sensor, you must enable policy alerts and configure your appliance to forward the event to QRadar.

Procedure

1. Log in to your Sourcefire user interface.
2. On the navigation menu, select **Intrusion Sensor > Detection Policy > Edit**.
3. Select an active policy and click **Edit**.
4. Click **Alerting**.
5. In the **State** field, select on to enable the syslog alert for your policy.
6. From the Facility list, select **Alert**.
7. From the Priority list, select **Alert**.
8. In the **Logging Host** field, type the IP address of the QRadar Console or Event Collector.
9. Click **Save**.
10. On the navigation menu, select **Intrusion Sensor > Detection Policy > Apply**.
11. Click **Apply**.

What to do next

You are now ready to configure the log source in QRadar.

Configuring a log source for Cisco FireSIGHT Management Center events

QRadar does not automatically discover Cisco FireSIGHT 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 FireSIGHT Management Center**.
6. From the Protocol Configuration list, select **Cisco Firepower eStreamer**.
7. Configure the following parameters:

| Parameter | Description |
|----------------|--|
| Server Address | The IP address or host name of the FireSIGHT Management Center device. |

| Parameter | Description |
|----------------------------|---|
| Server Port | The port number that the FireSIGHT Management Center device is configured to accept connection requests on. The default port that QRadar uses for the FireSIGHT Management Center device is 8302. |
| Keystore Filename | The directory path and file name for the keystore private key and associated certificate. By default, the import script creates the keystore file in the following directory: /opt/qradar/conf/estreamer.keystore |
| Truststore Filename | 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 |
| Request Extra Data | Select this option to request intrusion event extra data from FireSIGHT Management Center. For example, extra data includes the original IP address of an event. |
| Domain | <p>Note: Domain Streaming Requests are only supported for eStreamer version 6.x. Leave the Domain field blank for eStreamer version 5.x.</p> <p>The domain where the events are streamed from.</p> <p>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.</p> <p>Example:</p> <p>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:</p> <pre>Global \ B \ C</pre> |

8. Click **Save**.

140 ThreatGRID Malware Threat Intelligence Platform

The ThreatGRID Malware Threat Intelligence Platform DSM for IBM Security 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 Security 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 Security 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 Security 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 494. 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 ThreatGRID Malware Intelligence Platform.

The log source identifier must be unique for the log source type. |
| Enabled | Select this check box to enable the log source. By default, the check box is selected. |
| Credibility | 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. |
| Target Event Collector | From the list, select the Target Event Collector to use as the target for the log source. |
| Coalescing Events | 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. |
| Incoming Event Payload | From the list, select the incoming payload encoder for parsing and storing the logs. |
| 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. |

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 Security 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 495. Log file protocol parameters

| Parameter | Description |
|------------------------------|--|
| Log Source Identifier | 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. |
| Service Type | From the list, select the protocol that you want to use to retrieve log files from a remote server. The default is SFTP. <ul style="list-style-type: none"> • SFTP - SSH File Transfer Protocol • FTP - File Transfer Protocol • SCP - Secure Copy Protocol
The SCP and SFTP service type requires that the host server 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 ThreatGRID server that contains your event log files. |
| Remote Port | 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.

The list of default service type port numbers: <ul style="list-style-type: none"> • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 |
| Remote User | 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. |
| Remote Password | Type the password to log in to your ThreatGRID server. |
| Confirm Password | Confirm the password to log in to your ThreatGRID server |
| SSH Key File | If you select SCP or SFTP as the Service Type , use this parameter to define an SSH private key file. When you provide an SSH Key File , the Remote Password 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.

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 Remote Directory field support systems that have operating systems where a change in the working directory (CWD) command is restricted. |
| Recursive | Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear.

The Recursive parameter is ignored if you configure SCP as the Service Type . |

Table 495. Log file protocol parameters (continued)

| Parameter | Description |
|--|--|
| FTP File Pattern | <p>Type the regular expression (regex) required to filter the list of files that are specified in the Remote Directory. All files that match the regular expression are retrieved and processed.</p> <p>The FTP file pattern must match the name that you assigned to your ThreatGRID event log. For example, to collect files that start with leef or LEEF and ends with a text file extension, type the following value:</p> <pre>(leef LEEF)+.*\..txt</pre> <p>Use of this parameter requires knowledge of regular expressions (regex). This parameter applies to log sources that are configured to use FTP or SFTP.</p> |
| FTP Transfer Mode | <p>If you select FTP as the Service Type, from the list, select ASCII.</p> <p>ASCII is required for text-based event logs.</p> |
| SCP Remote File | If you select SCP as the Service Type , type the file name of the remote file. |
| Start Time | <p>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.</p> <p>For example, type 00:00 to schedule the Log File protocol to collect event files at midnight.</p> <p>This parameter functions with the Recurrence field value to establish when your ThreatGRID server is polled for new event log files.</p> |
| Recurrence | <p>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).</p> <p>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.</p> |
| Run On Save | <p>Select this check box if you want the log file protocol to run immediately after you click Save.</p> <p>After the save action completes, the log file protocol follows your configured start time and recurrence schedule.</p> <p>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 - 5000. |
| Processor | <p>From the list, select NONE.</p> <p>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.</p> |
| Ignore Previously Processed File(s) | <p>Select this check box to track and ignore files that are already processed.</p> <p>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.</p> <p>This option applies to FTP and SFTP service types.</p> |

Table 495. Log file protocol parameters (continued)

| Parameter | Description |
|-------------------------|---|
| Change Local Directory? | Select this check box to define a local directory on your QRadar appliance to store event log files during processing.

In most scenarios, you can leave this check box not selected. When this check box is selected, the Local Directory 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. |
| Event Generator | From the Event Generator list, select LineByLine .

The Event Generator 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. |

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.

141 TippingPoint

IBM Security QRadar supports a range of Tipping Point DSMs.

Tipping Point Intrusion Prevention System

The Tipping Point Intrusion Prevention System (IPS) DSM for IBM Security 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.”
- If you are using an LMS, see “Configuring notification contacts for LSM” on page 920.

Related tasks:

“Adding a DSM” on page 4

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

“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.
2. On the **Admin** Navigation menu, select **Server Properties**.
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.
4. In the Contacts List, click Remote System Log.
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.”

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 that 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 Security 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 Security 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.

142 Top Layer IPS

The Top Layer IPS DSM for IBM Security 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

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

“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.

143 Townsend Security LogAgent

IBM Security 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 Security 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 Security QRadar automatically discovers and creates a log source for syslog events forwarded from Raz-Lee i Security. 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 496. 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 IBM i system with Raz-Lee iSecurity. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

144 Trend Micro

IBM Security QRadar supports several Trend Micro DSMs.

Trend Micro Control Manager

You can integrate a Trend Micro Control Manager device with IBM Security 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 Security 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 497. SNMPv2 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 Trend Micro Control Manager appliance. |
| Community | Type the SNMP community name required to access the system containing SNMP events. The default is Public. |
| Include OIDs in Event Payload | <p>Clear the Include OIDs in Event Payload check box, if selected.</p> <p>This options allows the SNMP event payload to be constructed using <i>name-value pairs</i> instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs.</p> |

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, 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 Security 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" 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 Security 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 498. Trend Micro Deep Discovery Analyzer DSM specifications

| Specification | Value |
|-----------------------------|--|
| Manufacturer | Trend Micro |
| DSM name | Trend Micro Deep Discovery Analyzer |
| RPM file name | DSM-TrendMicroDeepDiscoveryAnalyzer-QRadar_version-build_number.noarch.rpm |
| Supported versions | 5.0, 5.5, 5.8 and 6.0 |
| Event format | LEEF |
| QRadar recorded event types | All events |

Table 498. Trend Micro Deep Discovery Analyzer DSM specifications (continued)

| Specification | Value |
|-----------------------------|--|
| Automatically discovered? | Yes |
| Includes identity? | No |
| Includes custom properties? | No |
| More information | Trend Micro website (www.trendmicro.com) |

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 499. Trend Micro Deep Discovery Analyzer log source parameters

| Parameter | Value |
|------------------------|-------------------------------------|
| Log Source type | Trend Micro Deep Discovery Analyzer |
| Protocol Configuration | Syslog |

Related tasks:

“Adding a DSM” on page 4

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

“Configuring your Trend Micro Deep Discovery Analyzer instance for communication with QRadar”

To collect Trend Micro Deep Discovery Analyzer events, configure your third-party instance to enable logging.

“Adding a log source” on page 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 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 Email Inspector

The IBM Security 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 500. Trend Micro Deep Discovery Email Inspector DSM specifications

| Specification | Value |
|-----------------------------|---|
| Manufacturer | Trend Micro |
| DSM name | Trend Micro Deep Discovery Email Inspector |
| RPM file name | DSM-TrendMicroDeepDiscoveryEmailInspector-Qradar_version-build_number.noarch.rpm |
| Supported versions | V3.0 |
| Event format | Log Event Extended Format (LEEF) |
| Recorded event types | Detections
Virtual analyzer analysis logs
System events
Alert events |
| Automatically discovered? | Yes |
| Includes identity? | No |
| Includes custom properties? | No |
| More information | Trend Micro website (http://www.trendmicro.ca) |

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:

Table 501. Trend Micro Deep Discovery Email Inspector log source parameters

| Parameter | Description |
|------------------------|--|
| Log Source type | Trend Micro Deep Discovery Email Inspector |
| Protocol Configuration | Syslog |

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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:

| Parameter | Description |
|---------------|---|
| Profile name | Specify a name for the profile. |
| Syslog server | The host name or IP of the QRadar server. |
| Port | 514 |
| Log format | LEEE |

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 Security 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 502. Trend Micro Deep Discovery Inspector DSM specifications

| Specification | Value |
|-----------------------------|---|
| Manufacturer | Trend Micro |
| DSM name | Trend Micro Deep Discovery Inspector |
| RPM file name | DSM-TrendMicroDeepDiscovery-QRadar_version-build_number.noarch.rpm |
| Supported versions | V3.0 to V3.8 |
| Event format | LEEF |
| QRadar recorded event types | Malicious content
Malicious behavior
Suspicious behavior
Exploit
Grayware
Web reputation
Disruptive application
Sandbox
Correlation
System
Update |
| Automatically discovered? | Yes |
| Included identity? | No |
| Includes custom properties? | No |
| More information | Trend Micro website (www.trendmicro.com/DeepDiscovery) |

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. Configure all required parameters and use the following table to determine specific values that are required for Trend Micro Deep Discovery Inspector event collection:

Table 503. Trend Micro Deep Discovery Inspector log source parameters

| Parameter | Value |
|------------------------|--------------------------------------|
| Log Source type | Trend Micro Deep Discovery Inspector |
| Protocol Configuration | Syslog |

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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:

| Parameter | Description |
|-----------------|---|
| IP address | The IP address of your QRadar Console or Event Collector. |
| Port | 514 |
| Syslog facility | The local facility, for example, local 3 . |
| Syslog severity | The minimum severity level that you want to include. |
| Syslog format | LEEF |

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 to send Events to QRadar

To collect Trend Micro Deep Discovery Inspector events, configure the device to send events to IBM Security 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:

| Parameter | Description |
|---------------------------|---|
| Server Name or IP address | The IP address of your QRadar Console or Event Collector. |

| Parameter | Description |
|-----------------------|---|
| Port | <ul style="list-style-type: none"> Default is UDP/514 TCP/601 SSL/6514 |
| Protocol | UDP/TCP/SSL |
| Facility level | Select a facility level that specifies the source of a message. |
| Severity level | Select a severity level of the type of messages to be sent to the syslog server. |
| Log format | LEEF |

- In the Detections pane, select the check boxes for the events that you want to forward to QRadar.
- Select **Connect through a proxy server** if you need proxy servers for your connections. The device uses the settings that are configured in the **Administrator > System Settings > Proxy** screen.

Note: Select this option if you require the use of proxy servers for intranet connections.

- Click **Save**.

Trend Micro Deep Security

The IBM Security QRadar DSM for Trend Micro Deep Security can collect logs from your Trend Micro Deep Security server.

The following table identifies the specifications for the Trend Micro Deep Security DSM:

Table 504. Trend Micro Deep Security DSM specifications

| Specification | Value |
|---------------------------|--|
| Manufacturer | Trend Micro |
| DSM name | Trend Micro Deep Security |
| RPM file name | DSM-TrendMicroDeepSecurity-Qradar_version-build_number.noarch.rpm |
| Supported versions | V9.6.1532
V10.0.1962
V10.1 |
| Event format | Log Event Extended Format |
| Recorded event types | Anti-Malware
Deep Security
Firewall
Integrity Monitor
Intrusion Prevention
Log Inspection
System
Web Reputation |
| Automatically discovered? | Yes |

Table 504. Trend Micro Deep Security DSM specifications (continued)

| Specification | Value |
|-----------------------------|---|
| Includes identity? | No |
| Includes custom properties? | No |
| More information | Trend Micro website (https://www.trendmicro.com/us/) |

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 505. Trend Micro Deep Security DSM log source parameters

| Parameter | Value |
|------------------------|---------------------------|
| Log Source type | Trend Micro Deep Security |
| Protocol Configuration | Syslog |

Related tasks:

“Adding a DSM” on page 4

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

“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 Security QRadar as the syslog server and configure the syslog format.

Before you begin

Ensure that your Deep Security Manager is installed and configured.

Procedure

1. Click the **Administration > System Settings > SIEM** tab.
2. From the **System Event Notification (from the Manager)** area, set 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.
6. Select **LEEF** for the **Syslog Format**.

Note: Deep Security can only send events in LEEF format from the **Manager**. If you select the **Direct forward** option on the **SIEM** tab, you cannot select **Log Event Extended Format 2.0** for the **Syslog Format**.

Trend Micro InterScan VirusWall

The Trend Micro InterScan VirusWall DSM for IBM Security 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 506.

| Parameter | Description |
|------------------------|--|
| Log Source Type | Trend InterScan VirusWall |
| Log Source Identifier | IP address or host name for the log source |
| Protocol Configuration | Syslog |

For more information about your Trend Micro InterScan VirusWall device, see your vendor documentation.

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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”
- “Integrating with Trend Micro Office Scan 10.x” on page 937
- “Integrating with Trend Micro OfficeScan XG” on page 939

Related concepts:

“SNMPv2 protocol configuration options” on page 39

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

Related tasks:

“Adding a DSM” on page 4

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

“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 Security 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 Security 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 Security 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

1. Select **Notifications > Administrator Notifications > Standard Notifications**.
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.
4. Select **Shared Folder Session Link** and enable Office Scan to monitor for firewall violations and shared folder sessions.

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 Security 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: %CNRISKLEVEL% 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.

145 Tripwire

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**.
9. Repeat 145, “Tripwire” to 145, “Tripwire” for each rule you want to monitor. 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

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

“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.

146 Tropos Control

The Tropos Control DSM for IBM Security 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

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

“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.

147 Universal

IBM Security 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:

6, "Log source extensions," on page 57

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 Security QRadar DSM for Universal CEF accepts events from any device that produces events in the Common Event Format (CEF).

The following table identifies the specifications for the Universal CEF DSM:

Table 507. Universal CEF DSM specifications

| Specification | Value |
|---------------------------|---|
| DSM name | Universal CEF |
| RPM file name | DSM-UniversalCEF-Qradar_version-build_number.noarch.rpm |
| Protocol | Syslog
Log File |
| Recorded event types | CEF-formatted events |
| Automatically discovered? | No |

Table 507. Universal CEF DSM specifications (continued)

| Specification | Value |
|-----------------------------|-------|
| Includes identity? | No |
| Includes custom properties? | No |

To send events from a device that generates CEF-formatted events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
 - DSMCommon RPM
 - Universal CEF RPM
2. Add a Universal CEF log source on the QRadar Console. Use the following values that are specific to Universal CEF:

| Parameter | Description |
|------------------------|--------------------|
| Log Source Type | Universal CEF |
| Protocol Configuration | Syslog or Log File |

3. Configure your third-party device to send events to QRadar. For more information about how to configure your third-party device, see your vendor documentation.
4. Configure event mapping for Universal CEF events.

Configuring event mapping for Universal CEF events

Universal CEF events do not contain a predefined QRadar Identifier (QID) map to categorize security events. You must search for unknown events from the Universal CEF log source and map them to high and low-level categories.

Before you begin

Ensure that you installed the Universal CEF DSM and added log source for it in QRadar.

About this task

By default, the Universal CEF DSM categorizes all events as unknown. All Universal CEF events display a value of **unknown** in the **Event Name** and **Low Level Category** columns on the **Log Activity** tab. You must modify the QID map to individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track events from your network devices.

For more information about event mapping, see the *IBM Security QRadar 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 Security 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 Security 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 Security 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 508. Syslog protocol parameters

| Parameter | Description |
|-----------------------|---|
| Log Source Identifier | Type the IP address or host name for the log source as an identifier for Universal LEEF events. |

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 Security 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 509. Log file protocol parameters

| Parameter | Description |
|-----------------------|--|
| Log Source Identifier | Type the IP address or host name for your Universal LEEF log source. This value must match the value configured in the Remote Host IP or Hostname parameter.

The log source identifier must be unique for the log source type. |

Table 509. Log file protocol parameters (continued)

| Parameter | Description |
|-----------------------|--|
| Service Type | <p>From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP.</p> <ul style="list-style-type: none"> • SFTP - SSH File Transfer Protocol • FTP - File Transfer Protocol • SCP - Secure Copy <p>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.</p> |
| 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 | <p>Type the directory location on the remote host from which the files are retrieved.</p> <p>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.</p> |
| Recursive | <p>Select this check box if you want the file pattern to search sub folders. By default, the check box is clear.</p> <p>The Recursive parameter is not used if you configure SCP as the Service Type.</p> |
| FTP File Pattern | <p>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.</p> <p>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:
 <code>log[0-9]+\.\tar\.\gz</code>. 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/</p> |
| FTP Transfer Mode | <p>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.</p> <p>From the list, select the transfer mode you want to apply to this log source:</p> <ul style="list-style-type: none"> • 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. <p>You must select NONE as the Processor and LINEBYLINE as the Event Generator when using ASCII as the FTP Transfer Mode.</p> |
| SCP Remote File | If you select SCP as the Service Type you must type the file name of the remote file. |

Table 509. Log file protocol parameters (continued)

| Parameter | Description |
|-------------------------------------|--|
| Start Time | 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. |
| 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 parameter. |
| EPS Throttle | Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000. |
| Processor | 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. |
| Ignore Previously Processed File(s) | 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. |
| Change Local Directory? | Select this check box to define the local directory on your QRadar system that you want to use for storing downloaded files during processing.

We recommend that you leave 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. |
| Event Generator | 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. |

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 Security 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 951.

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 Security 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 Security 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 Security 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 Security 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.

148 Vectra Networks Vectra

The IBM Security 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 510. Vectra Networks Vectra DSM specifications

| Specification | Value |
|-----------------------------|---|
| Manufacturer | Vectra Networks |
| DSM name | Vectra Networks Vectra |
| RPM file name | DSM-VectraNetworksVectra-QRadar_version-build_number.noarch.rpm |
| Supported versions | V2.2 |
| Protocol | Syslog |
| Event Format | Common Event Format |
| Recorded event types | Host scoring, command and control, botnet activity, reconnaissance, lateral movement, exfiltration |
| Automatically discovered? | Yes |
| Includes identity? | No |
| Includes custom properties? | No |
| More information | Vectra Networks Website (http://www.vectranetworks.com) |

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 511. Vectra Networks Vectra log source parameters

| Parameter | Value |
|------------------------|---|
| Log Source type | Vectra Networks Vectra |
| Protocol Configuration | Syslog |
| Log Source Identifier | A unique identifier for the log source. |

The following table provides a sample event message for the Vectra Networks Vectra DSM:

Table 512. Vectra Networks Vectra sample message.

| Event Name | Low level category | Sample log message |
|--------------|--------------------|---|
| Host Scoring | Backdoor Detected | <pre><13>Dec 22 16:38:53 <Server> - -: CEF:0 Vectra Networks Vectra 2.3 HSC Host Score Change 3 externalId =283 cat=HOST SCORING shost=IP-<IP_address> src= <Source_IP_address> flexNumber1=26 flexNumber1Label=threat flexNumber2=60 flexNumber 2Label=certainty cs4=https: //<IP_address>/hosts/283 cs4Label=URL start= 1450831133169 end= 1450831133169</pre> |

Related tasks:

“Adding a DSM” on page 4

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

“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:

| Option | Description |
|-------------|--|
| Destination | The QRadar Event Collector IP address. |
| Port | 514 |
| Protocol | UDP |
| Format | CEF |

149 Venustech Venusense

The Venustech Venusense DSM for IBM Security 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
- Venusense Unified Threat Management (UTM)
- Venusense Firewall
- Venusense Network Intrusion Prevention System (NIPS)

Venusense configuration overview

IBM Security 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 Security 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 Security 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.

3. From the list, select a syslog facility for the event log you enabled.
4. Repeat “Configuring Venusense event filtering” on page 955 and “Configuring Venusense event filtering” on page 955 to configure any additional syslog event filters.
5. Click **OK**.

What to do next

You can now configure a log source for your Venusense appliance in QRadar. QRadar does not automatically discover or create log sources for syslog events from Venusense appliances.

Configuring a Venusense log source

To integrate Venusense syslog events, you must manually create a log source in IBM Security QRadar as Venusense 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 Venusense appliance.
The type of log source that you select is determined by the event filter that is configured on your Venusense appliance. The options include the following types:
 - **Venustech Venusense Security Platform** - Select this option if you enabled all event filter options.
 - **Venustech Venusense UTM** - Select this option if you enabled unified filtering events.
 - **Venustech Venusense Firewall** - Select this option if you enabled filtering for firewall events.
 - **Venustech Venusense 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 Venusense appliance.
11. Click **Save**.
12. On the Admin tab, click **Deploy Changes**.

The configuration is complete. Events that are forwarded to QRadar by your Venusense appliance are displayed on the **Log Activity** tab.

150 Verdasys Digital Guardian

The Verdasys Digital Guardian DSM for IBM Security 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:

| Specification | Value |
|-----------------------------|--|
| Manufacturer | Verdasys Digital Guardian |
| DSM name | Verdasys Digital Guardian |
| RPM file name | DSM-VerdasysDigitalGuardian-QRadar_version-Build_number.noarch.rpm |
| Supported versions | V6.1.x and V7.2.1.0248 with the QRadar LEEF format
V6.0x with the Syslog event format |
| Protocol | Syslog, LEEF |
| Event format | Syslog |
| Recorded event types | All events |
| Automatically discovered? | Yes |
| Includes identity? | No |
| Includes custom properties? | No |
| More information | Digital Guardian website (https://digitalguardian.com) |

Configuring IPtables

Before you configure your Verdasys Digital Guardian to forward events, you must configure IPtables in IBM Security 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:

```
[root@Qradar bin]# iptables --list --line-numbers  
Chain QChain (1 references)  
num  target  prot      opt          source        destination  
1    ACCEPT  icmp     --  <IP address>  anywhere     icmp echo-reply  
2    ACCEPT  icmp     --  <IP address>  anywhere     icmp echo-request  
3    ACCEPT  tcp      --  anywhere    anywhere     state NEW tcp dpt:https  
4    ACCEPT  tcp      --  anywhere    anywhere     state NEW tcp dpt:http
```

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 Security 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 Security 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.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

Table 513. Syslog parameters

| Parameter | Description |
|------------------------------|---|
| Log Source Identifier | Type the IP address or host name for the log source as an identifier for events from Verdasys Digital Guardian appliance. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The log source is added to QRadar.

151 Vericept Content 360 DSM

The Vericept Content 360 DSM for IBM Security 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

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

“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.

152 VMWare

IBM Security QRadar supports a range of VMWare products.

VMware ESX and ESXi

The EMC VMware DSM for IBM Security 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”
- “Configuring the EMC VMWare protocol for ESX or ESXi servers” on page 965

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 Security 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 514. VMware syslog protocol parameters

| Parameter | ESX version | Description |
|----------------------------|--------------------------|---|
| Syslog.Local.DatastorePath | ESX or ESXi 3.5.x or 4.x | Type the directory path for the local syslog messages on your ESXi server.
The default directory path is [] /scratch/log/messages. |
| Syslog.Remote.Hostname | ESX or ESXi 3.5.x or 4.x | Type the IP address or host name of QRadar. |
| Syslog.Remote.Port | ESX or ESXi 3.5.x or 4.x | Type the port number the ESXi server uses to forward syslog data.
The default is port 514. |
| Syslog.global.logHost | ESXi v5.x or ESXi v6.x | Type the URL and port number that the ESXi server uses to forward syslog data.
Examples:
udp://<QRadar IP address>:514
tcp://<QRadar IP address>:514 |

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:

```
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 Security 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 515. 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 EMC VMware server. |
| Enabled | Select this check box to enable the log source. By default, the check box is selected. |
| Credibility | 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. |

Table 515. Syslog protocol parameters (continued)

| Parameter | Description |
|------------------------|--|
| Target Event Collector | From the list, select the Target Event Collector to use as the target for the log source. |
| Coalescing Events | 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. |
| Incoming Event Payload | From the list, select the incoming payload encoder for parsing and storing the logs. |
| 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 Security 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 Security 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 Security 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 516. VMWare protocol parameters

| Parameter | Description |
|------------------------------|---|
| Log Source Identifier | Type the IP address or host name for the log source. This value must match the value that is configured in the ESX IP field. |
| ESX IP | Type the IP address of the VMWare ESX or ESXi server.

The VMware protocol <i>prepends</i> the IP address of your VMWare ESX or ESXi server with HTTPS before the protocol requests event data. |
| User Name | Type the user name that is required to access the VMWare server. |
| Password | Type the password that is required to access the VMWare server. |

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

VMware vCenter

The VMware vCenter DSM for IBM Security 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 Security 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 517. EMC VMWare protocol parameters

| Parameter | Description |
|------------------------------|--|
| Log Source Identifier | Type the IP address or host name for the log source. This value must match the value that is configured in the ESX IP field. |
| ESX IP | Type the IP address of the VMWare vCenter server.
The EMC VMWare protocol prepends the IP address of your VMware vCenter server with HTTPS before the protocol requests event data. |
| User Name | Type the user name that is required to access the VMWare vCenter server. |
| Password | Type the password that is required to access the VMWare vCenter server. |

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

VMware vCloud Director

You can use the VMware vCloud Director DSM and the vCloud protocol for IBM Security 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 Security 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 Security 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 Security 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 518. VMware vCloud Director log source parameters

| Parameter | Description |
|-------------------------------|---|
| Log Source Identifier | Type the IP address, host name, or name that identifies the vCloud appliance events to QRadar. |
| vCloud URL | Type the URL configured on your vCloud appliance to access the REST API.

The URL you type must match the address that you configured in the VCD public REST API base URL field on your vCloud Server. |
| User Name | Type the user name that is required to remotely access the vCloud Server.

For example, <code>console/user@organization</code> .

If you want to configure a read-only account to use with QRadar, you can create a vCloud user in your organization who has the Console Access Only permission. |
| Password | Type the password that is required to remotely access the vCloud Server. |
| Confirm Password | Confirm the password that is required to remotely access the vCloud Server. |
| Polling Interval | Type a polling interval, which is the amount of time between queries to the vCloud Server for new events.

The default polling interval is 10 seconds. |
| Enabled | Select this check box to enable the log source. By default, the check box is selected. |
| Credibility | 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. |
| Target Event Collector | From the list, select the Target Event Collector to use as the target for the log source. |
| Coalescing Events | 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. |
| Incoming Event Payload | From the list, select the incoming payload encoder for parsing and storing the logs. |

Table 518. VMware vCloud Director log source parameters (continued)

| Parameter | Description |
|----------------------------|---|
| 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. |

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 Security 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 519. VMware vShield DSM specifications

| Specification | Value |
|--------------------------|---|
| Manufacturer | VMware |
| DSM | vShield |
| RPM file name | DSM-VMwarevShield-build_number.noarch.rpm |
| Supported versions | |
| Protocol | Syslog |
| QRadar recorded events | All events |
| Automatically discovered | Yes |
| Includes identity | No |
| More information | http://www.vmware.com/ |

VMware vShield DSM integration process

You can integrate VMware vShield DSM with IBM Security 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 Security QRadar" on page 971

"Configuring a VMware vShield log source in IBM Security QRadar" on page 971

Configuring your VMware vShield system for communication with IBM Security 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 Security 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 Security 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**.

153 Vormetric Data Security

The Vormetric Data Security DSM for IBM Security QRadar can collect event logs from your Vormetric Data Security servers.

The following table identifies the specifications for the Vormetric Data Security DSM:

Vormetric Data Security DSM specifications

| Specification | Value |
|------------------------|---|
| Manufacturer | Vormetric, Inc. |
| DSM | Vormetric Data Security |
| RPM file name | DSM-VormetricDataSecurity-7.1-804377.noarch.rpm
DSM-VormetricDataSecurity-7.2-804381.noarch.rpm |
| Supported versions | Vormetric Data Security Manager v5.1.3 and later
Vormetric Data Firewall FS Agent v5.2 and later |
| Protocol | Syslog (LEEF) |
| QRadar recorded events | Audit, Alarm, Warn, Learn Mode, System |
| Auto discovered | Yes |
| Includes identity | No |
| More information | Vormetric website (http://www.vormetric.com) |

Vormetric Data Security DSM integration process

You can integrate Vormetric Data Security DSM with IBM Security 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:
 2.
 - 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
3. For each instance of Vormetric Data Security, configure your Vormetric Data Security system to enable communication with QRadar.
4. 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 Security QRadar" on page 974

"Configuring a Vormetric Data Security log source in IBM Security QRadar" on page 975

Configuring your Vormetric Data Security systems for communication with IBM Security 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"

Configuring Vormetric Data Firewall FS Agents to bypass Vormetric Data Security Manager

When the Vormetric Data Security Manager is enabled to communicate with IBM Security 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.
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 Security QRadar

To collect Vormetric Data Security events, configure a log source in IBM Security QRadar.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **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**.

154 WatchGuard Fireware OS

The IBM Security QRadar DSM for WatchGuard Fireware OS can collect event logs from your WatchGuard Fireware OS.

The following table identifies the specifications for the WatchGuard Fireware OS DSM:

Table 520. WatchGuard Fireware DSM specifications

| Specification | Value |
|-----------------------------|--|
| Manufacturer | WatchGuard |
| DSM name | WatchGuard Fireware OS |
| RPM file name | DSM-WatchGuardFirewareOS-QRadar-version-
Build_number.noarch.rpm |
| Supported versions | Fireware XTM OS v11.9 and later |
| Event format | syslog |
| QRadar recorded event types | All events |
| Automatically discovered? | Yes |
| Includes identity? | No |
| More information | WatchGuard Website (http://www.watchguard.com/) |

To integrate the WatchGuard Fireware OS with QRadar, use the following steps:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console.
 - DSMCommon RPM
 - WatchGuard Fireware OS RPM
2. For each instance of WatchGuard Fireware OS, configure your WatchGuard Fireware OS appliance to enable communication with QRadar. You can use one of the following procedures:
 - “Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar”
 - “Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar” on page 978
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

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

“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**.

155 Websense

Websense is now known as Forcepoint.

Related concepts:

58, "FORCEPOINT," on page 369

IBM Security QRadar supports a range of FORCEPOINT DSMs.

156 Zscaler Nanolog Streaming Service

IBM Security 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 log feed on your Zscaler NSS to forward syslog events to IBM Security 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|%s{reason}|cat=%s{action}  
\tdevTime=%s{mon} %02d{dd} %d{yy} %02d{hh}:  
%02d{mm}:%02d{ss} %s{tz}\tdevTimeFormat=MMM dd yyyy HH:mm:ss  
\tdst=%s{sip}\tsrcPostNAT=%s{cintip}  
\trealm=%s{location}\tusrName=%s{login}\tsrcBytes=%d{reqsize}  
\tdstBytes=%d{respsize}  
\trole=%s{dept}\tpolicy=%s{reason}\turl=%s{eurl}  
\trecordid=%d{recordid}  
\tbwthrottle=%s{bwthrottle}\tuseragent=%s{ua}  
\treferer=%s{referrer}\thostname=%s{ehost}  
\tappproto=%s{proto}\turlcategory=%s{urlcat}  
\turlsupercategory=%s{urlsupercat}
```

```

\turlclass=%s{urlclass}\tappclass=%s{appclass}\tappname=%s{appname}
\tmalwaretype=%s{malwarecat}
\tmalwareclass=%s{malwareclass}\tthreatname=%s{threatname}
\triskscore=%d{riskscore}
\tdlpdict=%s{dlpdict}\tdlpeng=%s{dlpeng}\tfileclass=%s{fileclass}
\tfiletype=%s{filetype}
\treqmethod=%s{reqmethod}\trespcode=%s{respcode}\t%s{bamd5}\n

```

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 Security 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 521. Syslog protocol parameters

| Parameter | Description |
|-------------------------------|---|
| Log Source Identifier | Type the IP address as an identifier for events from your Zscaler NSS installation.

The log source identifier must be unique value. |
| Enabled | Select this check box to enable the log source.

By default, the check box is selected. |
| Credibility | 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. |
| Target Event Collector | Select the Target Event Collector to use as the target for the log source. |
| Coalescing Events | 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. |
| Incoming Event Payload | From the list, select the Incoming Payload Encoder for parsing and storing the logs. |

Table 521. Syslog protocol parameters (continued)

| Parameter | Description |
|----------------------------|---|
| 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. |
| Log Source Language | Select the language of the events that are generated by zScaler NSS. |

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

157 QRadar supported DSMs

IBM Security QRadar can collect events from your security products by using a plugin file that is called a Device Support Module (DSM).

The following table lists supported DSMs for third-party and IBM Security QRadar solutions.

Table 522. QRadar Supported DSMs

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|----------------------------|---|----------------------------|---|------------------|--------------------|-----------------------------|
| 3Com | 8800 Series Switch V3.01.30 | Syslog | Status and network condition events | Yes | No | No |
| AhnLab | AhnLab Policy Center | AhnLabPolicy
CenterJdbc | Spyware detection

Virus detection

Audit | No | Yes | No |
| Akamai | Akamai KONA | HTTP Receiver | Warn Rule Events

Deny Rule Events | No | No | No |
| Amazon | Amazon AWS CloudTrail | Amazon AWS S3 REST API | All version 1.0, 1.02, 1.03, and 1.04 events. | No | No | No |
| Ambiron | TrustWave ipAngel V4.0 | Syslog | Snort-based events | No | No | No |
| Apache | HTTP Server V1.3+ | Syslog | HTTP status | Yes | No | No |
| APC | UPS | Syslog | Smart-UPS series events | No | No | No |
| Apple | Mac OS X (10) | Syslog | Firewall, web server (access/error), privilege, and information events | No | Yes | No |
| Application Security, Inc. | DbProtect V6.2, V6.3, V6.3sp1, V6.3.1, and v6.4 | Syslog | All events | Yes | No | No |
| Arbor Networks | Arbor Networks Pravail APS V3.1+ | Syslog, TLS Syslog | All events | Yes | No | No |
| Arbor Networks | Arbor Networks Peakflow SP V5.8 to V8.1.2 | Syslog, TLS Syslog | Denial of Service (DoS)

Authentication

Exploit

Suspicious activity

System | Yes | No | No |
| Arpeggio Software | SIFT-IT V3.1+ | Syslog | All events configured in the SIFT-IT rule set | Yes | No | No |
| Array Networks | SSL VPN ArraySP V7.3 | Syslog | All events | No | Yes | Yes |
| Aruba Networks | Aruba Introspect V1.6 | Syslog | Security

System

Internal Activity

Exfiltration

Infection

Command & Control | Yes | No | No |
| Aruba Networks | ClearPass Policy Manager V6.5.0.71095 and above | Syslog | LIEEEF | Yes | Yes | No |
| Aruba Networks | Mobility Controllers V2.5 + | Syslog | All events | Yes | No | No |
| Avaya Inc. | Avaya VPN Gateway V9.0.7.2 | Syslog | All events | Yes | Yes | No |
| BalaBit IT Security | MicrosoftWindows Security Event Log V4.x | Syslog | Microsoft Event Log events | Yes | Yes | No |
| BalaBit IT Security | Microsoft ISA V4.x | Syslog | Microsoft Event Log vents | Yes | Yes | No |
| Barracuda Networks | Spam & Virus Firewall V5.x and later | Syslog | All events | Yes | No | No |
| Barracuda Networks | Web Application Firewall V7.0.x | Syslog | System, web firewall, access, and audit events | Yes | No | No |
| Barracuda Networks | Web Filter V6.0.x+ | Syslog | Web traffic and web interface events | Yes | No | No |
| BeyondTrust | BeyondTrust PowerBroker V4.0 | Syslog, TLS syslog | All events | Yes | No | No |
| Bit9 | Carbon Black V5.1 and later | Syslog | Watchlist hits | Yes | No | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|---------------------|---|---------------------------|--|------------------|--------------------|-----------------------------|
| Bit9 | Carbon Black Protection V8.0.0, V8.1.0 | Syslog | LEEF

Computer Management

Server Management

Session Management

Policy Management,

Policy Enforcement

Internal Events

General Management

Discovery | Yes | Yes | No |
| Bit9 | Bit9 Parity | Syslog | LEEF | Yes | | No |
| Bit9 | Security Platform V6.0.2 and later | Syslog | All events | Yes | Yes | No |
| BlueCat Networks | Adonis V6.7.1-P2+ | Syslog | DNS and DHCP events | Yes | No | No |
| Blue Coat | SG V4.x+ | Syslog, Log File Protocol | All events | No | No | Yes |
| Blue Coat | Web Security Service | | Blue Coat ELFF, Access | No | No | No |
| Box | Box | Box REST API | JSON

Administrator and enterprise events | No | Yes | No |
| Bridgewater Systems | AAA V8.2c1 | Syslog | All events | Yes | Yes | No |
| Brocade | Fabric OS V7.x | Syslog | System and audit events | Yes | No | No |
| CA | Access Control Facility V12 to V15 | Log File Protocol | All events | No | No | Yes |
| CA | SiteMinder | Syslog | All events | No | No | No |
| CA | Top Secret V12 to V15 | Log File Protocol | All events | No | No | Yes |
| Centrify | Centrify Infrastructure Services 2017 | Syslog and WinCollect | WinCollect logs, Audit events | Yes | No | No |
| Check Point | Check Point versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R75, R77, R80, and NGX | Syslog or OPSEC LEA | All events | Yes | Yes | Yes |
| Check Point | VPN-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, and NGX | Syslog or OPSEC LEA | All events | Yes | Yes | No |
| Check Point | Check Point Multi-Domain Management (Provider-1) versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, and NGX | Syslog or OPSEC LEA | All events | Yes | Yes | No |
| Cilasoft | Cilasoft QJRN/400 V5.14.K+ | Syslog | IBM audit events | Yes | Yes | No |
| Cisco | 4400 Series Wireless LAN Controller V7.2 | Syslog or SNMPv2 | All events | No | No | No |
| Cisco | CallManager V8.x | Syslog | Application events | Yes | No | No |
| Cisco | ACS V4.1 and later if directly from ACS V3.x and later if using ALE | Syslog | Failed Access Attempts | Yes | Yes | No |
| Cisco | Aironet V4.x+ | Syslog | Cisco Emblem Format | Yes | No | No |
| Cisco | ACE Firewall V12.2 | Syslog | All events | Yes | Yes | No |
| Cisco | ASA V7.x and later | Syslog | All events | Yes | Yes | No |
| Cisco | ASA V7.x+ | NSEL Protocol | All events | No | No | No |
| Cisco | CSA V4.x, V5.x and V6.x | Syslog SNMPv1 SNMPv2 | All events | Yes | Yes | No |
| Cisco | CatOS for catalyst systems V7.3+ | Syslog | All events | Yes | Yes | No |
| Cisco | Cloud Web Security (CWS) | Amazon AWS S3 REST API | W3C

All web usage logs | No | No | No |
| Cisco | Cisco Stealthwatch V6.8 | Syslog | Event format: LEEF

Event types: Anomaly, Data Hoarding, Exploitation, High Concern, Index, High DDoS Source Index, High Target Index, Policy Violation, Recon, High DDoS Target Index, Data Exfiltration, C&C | Yes | No | No |
| Cisco | IPS V7.1.10 and later, V7.2.x, V7.3.x | SDEE | All events | No | No | No |
| Cisco | Cisco IronPort V5.5, V6.5, V7.1, V7.5 (adds support for access logs), V10.0 | Syslog, Log File protocol | Event format: All events

Recorded event types:

Mail (syslog)

System (syslog)

Access (syslog)

Web content filtering (Log File) | No | No | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|------------------------|---|------------------------------------|---|------------------|--------------------|-----------------------------|
| Cisco | FireSIGHT Management Center V5.2 to V6.2.0.1

(formerly known as Sourcefire Defense Center) | Cisco Firepower eStreamer protocol | 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 | No | No | No |
| Cisco | Firewall Service Module (FWSM) v2.1+ | Syslog | All events | Yes | Yes | Yes |
| Cisco | Catalyst Switch IOS, 12.2, 12.5+ | Syslog | All events | Yes | Yes | No |
| Cisco | NAC Appliance v4.x + | Syslog | Audit, error, failure, quarantine, and infected events | No | No | No |
| Cisco | Nexus v6.x | Syslog | Nexus-OS events | Yes | No | No |
| Cisco | PIX Firewall v5.x, v6.3+ | Syslog | Cisco PIX events | Yes | Yes | Yes |
| Cisco | Identity Services Engine V1.1 and V1.2 | UDP Multiline Syslog | Event format: Syslog

Event types: Device events | No | Yes | No |
| Cisco | IOS 12.2, 12.5+ | Syslog | All events | Yes | Yes | No |
| Cisco | Cisco Umbrella | Amazon AWS S3 REST API | Event format: Cisco Umbrella CSV

Event type: Audit | No | No | No |
| Cisco | VPN 3000 Concentrator versions VPN 3005, 4.1.7.H | Syslog | All events | Yes | Yes | Yes |
| Cisco | Wireless Services Modules (WiSM) V 5.1+ | Syslog | All events | Yes | No | No |
| Citrix | NetScaler V9.3 to V10.0 | Syslog | All events | Yes | Yes | No |
| Citrix | Access Gateway V4.5 | Syslog | Access, audit, and diagnostic events | Yes | No | No |
| Cloudera | Cloudera Navigator | Syslog | Audit events for HDFS, HBase, Hive, Hue, Cloudera Impala, Sentry | Yes | No | No |
| CloudPassage | CloudPassage Halo | Syslog, Log file | All events | Yes | No | No |
| CrowdStrike | Falcon Host V1.0 | Syslog

LEEF | Falcon Host Detection Summary

Falcon Host Authentication Log

Falcon Host Detect Status Update Logs

Customer IOC Detect Event

Hash Spreading Event | Yes | No | No |
| CorreLog | CorreLog Agent for IBM z/OS | Syslog LEEF | All events | Yes | No | No |
| CRYPTOCard | CRYPTO- Shield V6.3 | Syslog | All events | No | No | No |
| CyberArk | CyberArk Privileged Threat Analytics V3.1 | Syslog | Detected security events | Yes | No | No |
| CyberArk | CyberArk Vault V6.x | Syslog | All events | Yes | Yes | No |
| CyberGuard | Firewall/VPN KS1000 V5.1 | Syslog | CyberGuard events | Yes | No | No |
| Damballa | Failsafe V5.0.2+ | Syslog | All events | Yes | No | No |
| Digital China Networks | DCS and DCRS Series switches V1.8.7 | Syslog | DCS and DCRS IPv4 events | No | No | No |
| DG Technology | DG Technology MEAS | Syslog LEEF | Mainframe events | Yes | No | No |
| ESET | ESET Remote Administrator V6.4.270 | Syslog

LEEF | Threat events

Firewall Aggregated Event

HIPS Aggregated Event

Audit events | Yes | Yes | No |
| Extreme | Dragon V5.0, V6.x, V7.1, V7.2, V7.3, and V7.4 | Syslog SNMPv1 SNMPv3 | All relevant Extreme Dragon events | Yes | No | No |
| Extreme | 800-Series Switch | Syslog | All events | Yes | No | No |
| Extreme | Matrix Router V3.5 | Syslog SNMPv1 SNMPv2 SNMPv3 | SNMP and syslog login, logout, and login failed events | Yes | No | No |
| Extreme | NetSight Automatic Security Manager V3.1.2 | Syslog | All events | Yes | No | No |
| Extreme | Matrix N/K/S Series Switch V6.x, V7.x | Syslog | All relevant Matrix K-Series, N-Series and S-Series device events | Yes | No | No |
| Extreme | Stackable and Standalone Switches | Syslog | All events | Yes | Yes | No |
| Extreme | XSR Security Router V7.6.14.0002 | Syslog | All events | Yes | No | No |
| Extreme | HiGuard Wireless IPS V2R2.0.30 | Syslog | All events | Yes | No | No |
| Extreme | HiPath Wireless Controller V2R2.0.30 | Syslog | All events | Yes | No | No |
| Extreme | NAC V3.2 and V3.3 | Syslog | All events | Yes | No | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|--|---|-------------------------------|--|------------------|--------------------|-----------------------------|
| Enterprise-IT-Security.com | SF-Sherlock V8.1 and later | LEEF | All_Checks,
DB2_Security_Configuration,
JES_Configuration,
Job_Entry_System_Attack,
Network_Parameter_Network_Security,
No_Policy_Resource_Access_Viol,
Resource_Allocation,
Resource_Protection,
Running_System_Change,
Running_System_Security,
Running_System_Status,
Security_Dbase_Scan,
Security_Dbase_Specialty,
Security_Dbase_Status,
Security_Parm_Change,
Security_System_Attack,
Security_System_Software,
Security_System_Status_SF-Sherlock,
Sherlock_Diverse_Sherlock_Diverse,
Sherlock_Information,
Sherlock_Specialties,
Storage_Management_Subsystem_Scan,
Sysplex_Security_Sysplex_Status,
System_Catalog_System_File_Change,
System_File_Security,
System_File_Specialty,
System_Log_Monitoring,
System_Module_Security,
System_Process_Security,
System_Residence_System_Tampering,
System_Volumes_TSO_Status,
UNIX_OMVS_Security,
UNIX_OMVS_System,
User Defined_Monitoring,
xx_Resource_Proto_Templ | Yes | No | No |
| Epic | Epic SIEM, Versions Epic 2014, Epic 2015, and Epic 2017 | LEEF | Audit, Authentication | Yes | Yes | No |
| Exabeam | Exabeam V1.7 and V2.0 | not applicable | Critical, Anomalous | Yes | No | No |
| Extreme Networks | Extreme Ware V7.7 and XOS V12.4.1.x | Syslog | All events | No | Yes | No |
| F5 Networks | BIG-IP AFM V11.3 | Syslog | Network, network DoS, protocol security, DNS, and DNS DoS events | Yes | No | No |
| F5 Networks | BIG-IP LTM V4.5, V9.x to V11.x | Syslog | All events | No | Yes | No |
| F5 Networks | BIG-IP ASM V10.1 to V13.0.0 | Syslog | All events

Common Event Format (CEF) formatted messages | No | Yes | No |
| F5 Networks | BIG-IP APM V10.x, and V11.x | Syslog | All events | Yes | No | No |
| F5 Networks | FirePass V7.0 | Syslog | All events | Yes | Yes | No |
| Fair Warning | Fair Warning V2.9.2 | Log File Protocol | All events | No | No | No |
| Fasoo | Fasoo Enterprise DRM V5.0 | JDBC | NVP event format

Usage events | No | No | No |
| Fidelis Security Systems | Fidelis XPS V7.3.x | Syslog | Alert events | Yes | No | No |
| FireEye | FireEye CMS, MPS, EX, AX, NX, FX, and HX | Syslog | All relevant events

Common Event Format (CEF) formatted messages

Log Event Extended Format (LEEF) | No | Yes | No |
| FreeRADIUS | FreeRADIUS V2.x | Syslog | All events | Yes | Yes | No |
| FORCEPOINT | Stonesoft Management Center V5.4 to 6.1 | Syslog | Event format: LEEF

Event types: Management Center, IPS, Firewall, and VPN events | Yes | No | No |
| FORCEPOINT

(formerly known as Websense) | TRITON V7.7, and V8.2 | Syslog | All events | Yes | No | No |
| FORCEPOINT

(formerly known as Websense) | V-Series Data Security Suite (DSS) V7.1x | Syslog | All events | Yes | Yes | Yes |
| FORCEPOINT

(formerly known as Websense) | V-Series Content Gateway V7.1x | Log File Protocol | All events | No | No | No |
| ForeScout | CounterACT V7.x and later | Syslog | Denial of Service, system, exploit, authentication, and suspicious events | No | No | No |
| Fortinet | FortiGate Security Gateway FortiOS V5.6 and earlier | Syslog

Syslog Redirect | All events | Yes | Yes | Yes |
| Foundry | FastIron V3.x.x and V4.x.x | Syslog | All events | Yes | Yes | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|------------------------|---|----------------------------------|---|------------------|--------------------|-----------------------------|
| genua | genugate V8.2+ | Syslog | General error messages
High availability
General relay messages
Relay-specific messages
genua programs/daemons
EPSI Accounting Daemon - gg/src/acctd
Configfw FWConfig
ROFWConfig
User-Interface
Webserver | Yes | Yes | No |
| Great Bay | Beacon | Syslog | All events | Yes | Yes | No |
| H3C Technologies | H3C Comware Platform, H3C Switches, H3C Routers, H3C Wireless LAN Devices, and H3C IP Security Devices

V7 is supported | Syslog | NVP

System | No | No | No |
| HBCGary | Active Defense V1.2 and later | Syslog | All events | Yes | No | No |
| HP | Network Automation V10.11 | Syslog

LEEF | All operational and configuration network events. | Yes | Yes | No |
| HP | ProCurve K.14.52 | Syslog | All events | Yes | No | No |
| HP | Tandem | Log File Protocol | Safe Guard Audit file events | No | No | No |
| HP | UX V11.x and later | Syslog | All events | No | Yes | No |
| Honeycomb Technologies | Lexicon File Integrity Monitor mesh service V3.1 and later | Syslog | integrity events | Yes | No | No |
| Huawei | S Series Switch S5700, S7700, and S9700 using V200R001C00 | Syslog | IPv4 events from S5700, S7700, and S9700 Switches | No | No | No |
| Huawei | AR Series Router (AR150, AR200, AR1200, AR2200, and AR3200 routers using V200R002C00) | Syslog | IPv4 events | No | No | No |
| IBM | AIX V6.1 and V7.1 | Syslog, Log File Protocol | Configured audit events | Yes | No | No |
| IBM | AIX 5.x, 6.x, and v7.x | Syslog | Authentication and operating system events | Yes | Yes | No |
| IBM | BigFixV8.2.x to 9.5.2

(formerly known as Tivoli EndPoint Manager) | IBM BigFix SOAP Protocol | Server events | No | Yes | No |
| IBM | IBM BigFix Detect | IBM BigFix EDR REST API Protocol | LEEF, IOC and IOA alerts | No | No | No |
| IBM | Bluemix® Platform | Syslog, TLS Syslog | All System (Cloud Foundry) events, some application events | Yes | No | No |
| IBM | Federated Directory Server V7.2.0.2 and later | LEEF | FDS Audit | Yes | No | No |
| IBM | InfoSphere 8.2p45 | Syslog | Policy builder events | No | No | No |
| IBM | IBM i DSM V5R4 and later

(formerly known as AS/400Series) | Log File Protocol | All events | No | Yes | No |
| IBM | IBM i - Robert Townsend Security Solutions V5R1 and later

(formerly known as AS/400Series) | Syslog | CEF formatted messages | Yes | Yes | No |
| IBM | IBM i - Powertech Interact V5R1 and later

(formerly known as AS/400Series) | Syslog | CEF formatted messages | Yes | Yes | No |
| IBM | ISS Proventia M10 v2.1_2004.1122_15.13.53 | SNMP | All events | No | No | No |
| IBM | Lotus Domino v8.5 | SNMP | All events | No | No | No |
| IBM | Proventia Management SiteProtector v2.0 and v2.9 | JDBC | IPS and audit events | No | No | No |
| IBM | RACF v1.9 to v1.13 | Log File Protocol | All events | No | No | Yes |
| IBM | CICS v3.1 to v4.2 | Log File Protocol | All events | No | No | Yes |
| IBM | DB2 v8.1 to v10.1 | Log File Protocol | All events | No | No | Yes |
| IBM | IBM DataPower FirmwareV6 and V7

(formerly known as WebSphere DataPower) | Syslog | All events | Yes | No | No |
| IBM | IBM Fiberlink MaaS360 | LEEF | Compliance rule events

Device enrollment events

Action history events | No | Yes | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|--------------|---|--------------------------------------|--|------------------|--------------------|-----------------------------|
| IBM | IBM QRadar Packet Capture | Syslog, LEEF | All events | Yes | No | No |
| | IBM QRadar Packet Capture V7.2.3 to V7.2.8 | | | | | |
| | IBM QRadar Network Packet Capture V7.3.0 | | | | | |
| IBM | IBM SAN Volume Controller | Syslog | CADF event format
Activity, Control, and Monitor audit events | Yes | No | No |
| IBM | z/OS v1.9 to v1.13 | Log File Protocol | All events | No | No | Yes |
| IBM | Informix v11 | Log File Protocol | All events | No | No | No |
| IBM | IMS | Log File Protocol | All events | No | No | No |
| IBM | Security Access Manager for Mobile (ISAM) | TLS Syslog | 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 | Yes | No | No |
| IBM | Security Identity Governance (ISIG) | JDBC | NVP event format
Audit event type | No | No | No |
| IBM | QRadar Network Security XGS v5.0 with fixpack 7 to v5.4 | Syslog | System, access, and security events | Yes | No | No |
| IBM | Security Network IPS (GX) v4.6 and later | Syslog | Security, health, and system events | Yes | No | No |
| IBM | Security Identity Manager 6.0.x and later | JDBC | Audit and recertification events | No | Yes | No |
| IBM | IBM Security Trusteer Apex Advanced Malware Protection | Syslog/LEEF
Log File Protocol | Malware Detection

Exploit Detection

Data Exfiltration Detection

Lockdown for Java Event

File Inspection Event

Apex Stopped Event

Apex Uninstalled Event

Policy Changed Event

ASLR Violation Event

ASLR Enforcement Event

Password Protection Event | Yes | Yes | No |
| IBM | IBM Sense v1 | Syslog | LEEF | Yes | No | No |
| IBM | IBM SmartCloud Orchestrator v2.3 FPI and later | IBM SmartCloud Orchestrator REST API | Audit Records | No | Yes | No |
| IBM | Tivoli Access Manager IBM Web Security Gateway v7.x | Syslog | audit, access, and HTTP events | Yes | Yes | No |
| IBM | Tivoli Endpoint Manager

(now known as IBM BigFix) | | | | | |
| IBM | WebSphere Application Server v5.0 to v8.5 | Log File Protocol | All events | No | Yes | No |
| IBM | WebSphere DataPower

(now known as DataPower)WebSphere DataPower | | | | | |
| IBM | zSecure Alert v1.13.x and later | UNIX syslog | Alert events | Yes | Yes | No |
| IBM | Security Access Manager v8.1 and v8.2 | Syslog | Audit, system, and authentication events | Yes | No | No |
| IBM | Security Directory v6.3.1 and later | Syslog LEEF | All events | Yes | Yes | No |
| Imperva | Incapsula | LEEF | Access events and Security alerts | Yes | No | No |
| Imperva | SecureSphere v6.2 and v7.x Release Enterprise Edition (Syslog)

SecureSphere v9.5 to v11.5 (LEEF) | Syslog

LEEF | All events | Yes | No | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|-----------------------------------|---|------------------------------|--|------------------|--------------------|-----------------------------|
| Illumio | Illumio Adaptive Security Platform | Syslog | Audit | Yes | No | No |
| | | LEEF | Traffic | | | |
| Internet Systems Consortium (ISC) | BIND v9.9, v9.11 | Syslog | All events | Yes | No | No |
| Intersect Alliance | SNARE Enterprise Windows Agent | Syslog | Microsoft Event Logs | Yes | Yes | No |
| iT-CUBE | agileSI v1.x | SMB Tail | AgileSI SAP events | No | Yes | No |
| Itron | Openway Smart Meter | Syslog | All events | Yes | No | No |
| Juniper Networks | AVT | JDBC | All events | No | No | Yes |
| Juniper Networks | DDoS Secure | | | | No | No |
| | Juniper Networks DDoS Secure is now known as NCC Group DDoS Secure. | | | | | |
| Juniper Networks | DX | Syslog | Status and network condition events | Yes | No | Yes |
| Juniper Networks* | Infranet Controller v2.1, v3.1 & v4.0 | Syslog | All events | No | Yes | Yes |
| Juniper Networks | Firewall and VPN v5.5r3 and later | Syslog | NetScreen Firewall events | Yes | Yes | Yes |
| Juniper Networks | Junos WebApp Secure v4.2.x | Syslog | Incident and access events | Yes | No | No |
| Juniper Networks | IDP v4.0, v4.1 & v5.0 | Syslog | NetScreen IDP events | Yes | No | Yes |
| Juniper Networks | Network and Security Manager (NSM) and Juniper SSG v2007.1r2 to 2007.2r2, 2008.r1, 2009r1.1, 2010.x | Syslog | NetScreen NSM events | Yes | No | Yes |
| Juniper Networks | Junos OS v7.x to v10.x Ex Series | Syslog or PCAP Syslog*** | All events | Yes** | Yes | Yes |
| | Ethernet Switch DSM only supports v9.0 to v10.x | | | | | |
| Juniper Networks | Secure Access | | | | | Yes |
| | Juniper Networks Secure Access is now known as Pulse Secure Pulse Connect Secure. | | | | | |
| Juniper Networks | Juniper Security Binary Log Collector | Binary | Audit, system, firewall, and IPS events | No | No | Yes |
| | SRX or J Series appliances at v12.1 or above | | | | | |
| Juniper Networks | Steel-Belted Radius v5.x | Log File | All events | Yes | Yes | Yes |
| Juniper Networks | vGW Virtual Gateway v4.5 | Syslog | Firewall, admin, policy and IDS Log events | Yes | No | No |
| Juniper Networks | Wireless LAN Controller | Syslog | All events | Yes | No | No |
| | Wireless LAN devices with Mobility System Software (MSS) V7.6 and later | | | | | |
| Kaspersky | Security Center v9.2 | JDBC, LEEF | Antivirus, server, and audit events | No | Yes | No |
| Kaspersky | Threat Feed Service | Syslog | Detect, Status, Evaluation | Yes | No | No |
| Kisco | Kisco Information Systems SafeNet/i V10.11 | Log File | All events | No | No | No |
| Lastline | Lastline Enterprise 6.0 | LEEF | Anti-malware | Yes | No | No |
| Lieberman | Random Password Manager v4.8x | Syslog | All events | Yes | No | No |
| LightCyber | LightCyber Magna V3.9 | Syslog, LEEF | C&C, exfilt, lateral, malware and recon | Yes | No | No |
| Linux | Open Source Linux OS v2.4 and later | Syslog | Operating system events | Yes | Yes | No |
| Linux | DHCP Server v2.4 and later | Syslog | All events from a DHCP server | Yes | Yes | No |
| Linux | IPTables kernel v2.4 and later | Syslog | Accept, Drop, or Reject events | Yes | No | No |
| McAfee | Application / Change Control v4.5.x | JDBC | Change management events | No | Yes | No |
| McAfee | ePolicy Orchestrator V3.5 to v5.x | JDBC, SNMPv1, SNMPv2, SNMPv3 | AntiVirus events | No | No | No |
| McAfee | Firewall Enterprise v6.1 | Syslog | Firewall Enterprise events | Yes | No | No |
| McAfee | Intrushield v2.x - v5.x | Syslog | Alert notification events | Yes | No | No |
| McAfee | Intrushield v6.x - v7.x | Syslog | Alert and fault notification events | Yes | No | No |
| | | | | | | |
| McAfee | Web v6.0 and later | Syslog, Log File Protocol | All events | Yes | No | No |
| MetaInfo | MetaIP v5.7.00-6059 and later | Syslog | All events | Yes | Yes | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|--------------|---|--|--|------------------|--------------------|-----------------------------|
| Microsoft | Azure | Syslog

Microsoft Azure Event Hubs | Event formats: LEEF, JSON

Recorded event types:

Network Security Group (NSG) Flow logs, Network Security Group (NSG) Logs, Authorization, Classic Compute, Classic Storage, Compute, Insights, KeyVault, SQL, Storage, Automation, Cache, CDN, Devices, Event Hub, HDInsight, Recovery Services, Recovery Services, AppService, Batch, Bing Maps, Certificate Registration, Cognitive Services, Container Service, Content Moderator, Data Catalog, Data Factory™, Data Lake Analytics, Data Lake Store, Domain Registration, Dynamics LCS, Features, Logic, Media, Notification Hubs, Search, Servicebus, Support, Web, Scheduler, Resources, Resource Health, Operation Insights, Market Place Ordering, API Management, AD Hybrid Health Service, Server Management | Yes | No | No |
| Microsoft | DNS Debug

Supported versions:

Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2 | WinCollect Microsoft DNS Debug | LEEF | Yes | Yes | No |
| Microsoft | IIS v6.0, 7.0 and 8.x | Syslog | HTTP status code events | Yes | No | No |
| Microsoft | Internet and Acceleration (ISA) Server or Threat Management Gateway 2006 | Syslog | ISA or TMG events | Yes | No | No |
| Microsoft | Exchange Server 2003, 2007, 2010, 2013, and 2016 | Windows Exchange Protocol | Outlook Web Access events (OWA)

Simple Mail Transfer Protocol events (SMTP)

Message Tracking Protocol events (MSGTRK) | No | No | No |
| Microsoft | Endpoint Protection 2012 | JDBC | Malware detection events | No | No | No |
| Microsoft | Hyper V v2008 and v2012 | WinCollect | All events | No | No | No |
| Microsoft | IAS Server

v2000, 2003, and 2008 | Syslog | All events | Yes | No | No |
| Microsoft | Microsoft Windows Event Security Log v2000, 2003, 2008, XP, Vista, and Windows 7 (32 or 64-bit systems supported) | Syslog

non-Syslog

Microsoft Windows Event Log Protocol Source

Common Event Format (CEF) format,

Log Event Extended Format (LEEF) | All events, including Sysmon | Yes | Yes | Yes |
| Microsoft | SQL Server 2008, 2012, and 2014 | JDBC | SQL Audit events | No | No | No |
| Microsoft | SharePoint 2010 and 2013 | JDBC | SharePoint audit, site, and file events | No | No | No |
| Microsoft | DHCP Server 2000/2003 | Syslog | All events | Yes | Yes | No |
| Microsoft | Microsoft Office 365 | Office 365 REST API | JSON | No | No | No |
| Microsoft | Operations Manager 2005 | JDBC | All events | No | No | No |
| Microsoft | System Center Operations Manager 2007 | JDBC | All events | No | No | No |
| Motorola | Symbol AP firmware v1.1 to 2.1 | Syslog | All events | No | No | No |
| NCC Group | NCC Group DDos V15.1.2s to 516.1-0 | Syslog | Event format: LEEF

Event types: All events | Yes | No | No |
| NetApp | Data ONTAP | Syslog | CIFS events | Yes | Yes | No |
| Netskope | Netskope Active | Netskope Active REST API | Alert, All events | No | Yes | No |
| Niksun | NetVCR 2005 v3.x | Syslog | Niksun events | No | No | No |
| Nokia | Firewall NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and later | Syslog or OPSEC LEA | All events | Yes | Yes | No |
| Nokia | VPN-1 NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and later | Syslog or OPSEC LEA | All events | Yes | Yes | No |
| Nominum | Vantio v5.3 | Syslog | All events | Yes | No | No |
| Nortel | Contivity | Syslog | All events | Yes | No | No |
| Nortel | Application Switch v3.2 and later | Syslog | Status and network condition events | No | Yes | No |
| Nortel | ARN v15.5 | Syslog | All events | Yes | No | No |
| Nortel* | Ethernet Routing Switch 2500 v4.1 | Syslog | All events | No | Yes | No |
| Nortel* | Ethernet Routing Switch 4500 v5.1 | Syslog | All events | No | Yes | No |
| Nortel* | Ethernet Routing Switch 5500 v5.1 | Syslog | All events | No | Yes | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|----------------------|--|---|--|------------------|--------------------|-----------------------------|
| Nortel | Ethernet Routing Switch 8300 v4.1 | Syslog | All events | No | Yes | No |
| Nortel | Ethernet Routing Switch 8600 v5.0 | Syslog | All events | No | Yes | No |
| Nortel | VPN Gateway v6.0, 7.0.1 and later, v8.x | Syslog | All events | Yes | Yes | No |
| Nortel | Secure Router v9.3, v10.1 | Syslog | All events | Yes | Yes | No |
| Nortel | Secure Network Access Switch v1.6 and v2.0 | Syslog | All events | Yes | Yes | No |
| Nortel | Switched Firewall 5100 v2.4 | Syslog or OPSEC | All events | Yes | Yes | No |
| Nortel | Switched Firewall 6000 v4.2 | Syslog or OPSEC | All events | Yes | Yes | No |
| Nortel | Threat Protection System v4.6 and v4.7 | Syslog | All events | No | No | No |
| Novell | eDirectory v2.7 | Syslog | All events | Yes | No | No |
| ObserveIT | ObserveIT 5.7.x and later | JDBC | Alerts

User Activity

System Events

Session Activity

DBA Activity | No | Yes | No |
| Okta | Okta Identity Management | Okta REST API | JSON | No | Yes | No |
| Onapsis | Onapsis Security Platform v1.5.8 and later | Log Event Extended Format (LEEFD) | Assessment

Attack signature

Correlation

Compliance | Yes | No | No |
| OpenBSD Project | OpenBSD v4.2 and later | Syslog | All events | No | Yes | No |
| Open LDAP Foundation | Open LDAP 2.4.x | UDP Multiline Syslog | All events | No | No | No |
| Open Source | SNORT v2.x | Syslog | All events | Yes | No | No |
| OpenStack | OpenStack v2015.1 | HTTP Reciever | Audit events | No | No | No |
| Oracle | Oracle DB Audit versions 9i, 10g, 11g, 12c (includes unified auditing)

136787 | JDBC, Syslog | Event format: Name-Value Pair

Recorded event types: Audit records | No | Yes | No |
| Oracle | Audit Vault V10.3 and V12.2 | JDBC | 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. | No | Yes | No |
| Oracle | OS Audit v9i, v10g, and v11g | Syslog | Oracle events | Yes | Yes | No |
| Oracle | BEA WebLogic v10.3.x | Log File Protocol | Oracle events | No | No | No |
| Oracle | Database Listener v9i, v10g, and v11g | Syslog | Oracle events | Yes | No | No |
| Oracle | Directory Server

(Formerly known as Sun ONE LDAP). | | | | | |
| Oracle | Fine Grained Auditing v9i and v10g | JDBC | Select, insert, delete, or update events for tables configured with a policy | No | No | No |
| OSSEC | OSSEC v2.6 and later | Syslog | All relevant | Yes | No | No |
| Palo Alto Networks | Palo Alto PA Series PanOS v3.0 to v8.0 | LEEF for PAN-OS v3.0 to v8.0

CEF for PAN-OS v4.0 to v6.1 | Traffic

Threat

URL Filtering

Data

WildFire

Config

System

HIP Match

Authentication

User-ID

Tunnel Inspection

Correlation | Yes | Yes | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|--------------------|---|--|---|------------------|--------------------|-----------------------------|
| Palo Alto Networks | Palo Alto Endpoint Security Manager V3.4.2.17401 | Syslog | Agent | Yes | No | No |
| | | LEEF | Config | | | |
| | | CEF | Policy | | | |
| | | | System | | | |
| | | | Threat | | | |
| Pirean | Access: One v2.2 with DB2 v9.7 | JDBC | Access management and authentication events | No | No | No |
| PostFix | Mail Transfer Agent v2.6.6 and later | UDP Multiline Protocol or Syslog | Mail events | No | No | No |
| ProFTPd | ProFTPD v1.2.x, v1.3.x | Syslog | All events | Yes | Yes | No |
| Proofpoint | Proofpoint Enterprise Protection and Enterprise Privacy versions 7.0.2, 7.1, or 7.2 | Syslog | System, email audit, email encryption, and email security threat classification events | No | No | No |
| Pulse Secure | Pulse Secure Pulse Connect Secure V8.2R5 | Syslog | Event formats: | Yes | Yes | Yes |
| | | TLS Syslog | Admin, Authentication, System, Network, Error | | | |
| | | | Event types: | | | |
| | | | All events | | | |
| Radware | AppWall V6.5.2 and V8.2 | Syslog | Event format: Vision Log | Yes | No | No |
| | | | Recorded event types: | | | |
| | | | Administration | | | |
| | | | Audit | | | |
| | | | Learning | | | |
| | | | Security | | | |
| | | | System | | | |
| Radware | DefensePro v4.23, 5.01, 6.x and 7.x | Syslog | All events | Yes | No | No |
| Raz-Lee iSecurity | IBM i Firewall 15.7 and Audit 11.7 | Syslog | Security and audit events | Yes | Yes | No |
| Redback Networks | ASE v6.1.5 | Syslog | All events | Yes | No | No |
| Resolution1 | Resolution1 CyberSecurity

Formerly known as AccessData InSightResolution1 CyberSecurity. | Log file | Volatile Data, Memory Analysis Data, Memory Acquisition Data, Collection Data, Software Inventory, Process Dump Data, Threat Scan Data, Agent Remediation Data | No | No | No |
| Riverbed | SteelCentral NetProfiler | JDBC | Alert events | No | No | No |
| Riverbed | SteelCentral NetProfiler Audit | Log file protocol | Audit events | No | Yes | No |
| RSA | Authentication Manager v6.x, v7.x, and v8.x | v6.x and v7.x use Syslog or Log File Protocol

v8.x uses Syslog only | All events | No | No | No |
| SafeNet | DataSecure v6.3.0 and later | Syslog | All events | Yes | No | No |
| Salesforce | Security Auditing | Log File | Setup Audit Records | No | No | No |
| Salesforce | Security Monitoring | Salesforce REST API Protocol | Login History

Account History

Case History

Entitlement History

Service Contract History

Contract Line Item History

Contract History

Contact History

Lead History

Opportunity History

Solution History | No | Yes | No |
| Samhain Labs | HIDS v2.4 | Syslog

JDBC | All events | Yes | No | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|--------------------------|--|--|---|------------------|--------------------|-----------------------------|
| Seculert | Seculert v1 | Seculert Protection REST API Protocol | All malware communication events | No | No | No |
| Seculert | Seculert | Seculert protection REST API Protoco | All malware communication events | No | No | No |
| SentriGo | Hedgehog v2.5.3 | Syslog | All events | Yes | No | No |
| Skyhigh Networks | Skyhigh Networks Cloud Security Platform 2.4 and 3.3 | Syslog | Event format:

Log Event Extended Format (LEEF)

Recorded event types:

Privilege Access, Insider Threat, Compromised Account, Access, Admin, Data, Policy, and AuditAnomaly events | Yes | No | No |
| SolarWinds | SolarWinds Orion v2011.2 | Syslog | All events | No | No | No |
| SonicWALL | UTM/Firewall/VPN Appliance v3.x and later | Syslog | All events | Yes | No | No |
| Sophos | Astaro v8.x | Syslog | All events | Yes | No | No |
| Sophos | Enterprise Console v4.5.1 and v5.1 | Sophos Enterprise Console protocol

JDBC | All events | No | No | No |
| Sophos | PureMessage v3.1.0.0 and later for Microsoft Exchange v5.6.0 for Linux | JDBC | Quarantined email events | No | No | No |
| Sophos | Web Security Appliance v3.x | Syslog | Transaction log events | Yes | No | No |
| Sourcefire | Intrusion Sensor IS 500, v2.x, 3.x, 4.x | Syslog | All events | Yes | No | No |
| Sourcefire | Defense Center

(Now known as Cisco FireSIGHT Management Center) | | | | | |
| Splunk | MicrosoftWindows Security Event Log | Windows-based event provided by Splunk Forwarders | All events | No | Yes | No |
| Squid | Web Proxy v2.5 and later | Syslog | All cache and access log events | Yes | No | No |
| Startent Networks | Startent Networks | Syslog | All events | Yes | No | No |
| STEALTHbits Technologies | STEALTHbits File Activity Monitor | Syslog LEEF | File Activity Monitor Events | | | |
| STEALTHbits Technologies | StealthINTERCEPT | Syslog LEEF | Active Directory Audit Events | Yes | No | No |
| STEALTHbits Technologies | STEALTHbits StealthINTERCEPT Alerts | Syslog LEEF | Active Directory Alerts Events | Yes | No | No |
| STEALTHbits Technologies | STEALTHbits StealthINTERCEPT Analytics | Syslog LEEF | Active Directory Analytics Events | Yes | No | No |
| Sun | Solaris v5.8, v5.9, Sun OS v5.8, v5.9 | Syslog | All events | Yes | Yes | No |
| Sun | Solaris DHCP v2.8 | Syslog | All events | Yes | Yes | No |
| Sun | Solaris Sendmail v2.x | Syslog

Log File Protocol

Proofpoint 7.5 and 8.0 Sendmail log | All events | Yes | No | No |
| Sun | Solaris Basic Security Mode (BSM) v5.10 and v5.11 | Log File Protocol | All events | No | Yes | No |
| Sun | ONE LDAP v11.1

(Known as Oracle Directory Server) | Log File Protocol

UDP Multiline Syslog | All relevant access and LDAP events | No | No | No |
| Sybase | ASE v15.0 and later | JDBC | All events | No | No | No |
| Symantec | Endpoint Protection V11, V12, and V14 | Syslog | All Audit and Security Logs | Yes | No | Yes |
| Symantec | SGS Appliance v3.x and later | Syslog | All events | Yes | No | Yes |
| Symantec | SSC v10.1 | JDBC | All events | Yes | No | No |
| Symantec | Data Loss Prevention (DLP) v8.x and later | Syslog | All events | No | No | No |
| Symantec | PGP Universal Server 3.0.x | Syslog | All events | Yes | No | No |
| ThreatGRID | Malware Threat Intelligence Platform v2.0 | Log file protocol

Syslog | Malware events | No | No | No |
| TippingPoint | Intrusion Prevention System (IPS) v1.4.2 to v3.2.x | Syslog | All events | No | No | No |
| TippingPoint | X505/X506 v2.5 and later | Syslog | All events | Yes | Yes | No |
| Top Layer | IPS 5500 v4.1 and later | Syslog | All events | Yes | No | No |
| Trend Micro | Control Manager v5.0 or v5.5 with hotfix 1697 or hotfix 1713 after SP1 Patch 1 | SNMPv1

SNMPv2

SNMPv3 | All events | Yes | No | No |
| Trend Micro | Deep Discovery Analyzer V5.0, V5.5, V5.8 and V6.0 | LEEF | All events | Yes | No | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|-----------------|---|----------------------------------|---|------------------|--------------------|-----------------------------|
| Trend Micro | Deep Discovery Email Inspector V3.0 | Log Event Extended Format (LEEF) | Detections, Virtual Analyzer Analysis logs, System events, Alert events | Yes | No | No |
| Trend Micro | Deep Discovery Inspector V3.0 to V3.8 | Log Event Extended Format (LEEF) | Malicious content
Malicious behavior
Suspicious behavior
Exploit
Grayware
Web reputation
Disruptive application
Sandbox
Correlation
System
Update | Yes | No | No |
| Trend Micro | Deep Security V9.6.1532, V10.0.1962 and V10.1 | Log Event Extended Format (LEEF) | Anti-Malware
Deep Security
Firewall
Integrity Monitor
Intrusion Prevention
Log Inspection
System
Web Reputation | Yes | No | No |
| Trend Micro | InterScan VirusWall v6.0 and later | Syslog | All events | Yes | No | No |
| Trend Micro | Office Scan v8.x and v10.x | SNMPv2 | All events | No | No | No |
| Tripwire | Enterprise Manager v5.2 and later | Syslog | Resource additions, removal, and modification events | Yes | No | No |
| Tropos Networks | Tropos Control v7.7 | Syslog | Fault management, login/logout, provision, and device image upload events | No | No | No |
| Trusteer | Apex Local Event Aggregator v1304.x and later | Syslog | Malware, exploit, and data exfiltration detection events | Yes | No | No |
| Universal | Syslog and SNMP | Syslog
SNMP
SDEE | All events | No | Yes | No |
| Universal | Syslog | Syslog
Log File Protocol | All events | No | Yes | No |
| Universal | Authentication Server | Syslog | All events | No | Yes | No |
| Universal | Firewall | Syslog | All events | No | No | No |
| Vectra Networks | Vectra Networks Vectra v2.2 | Syslog
Common Event Format | Host scoring, command and control, botnet activity, reconnaissance, lateral movement, exfiltration | Yes | No | No |
| Verdasys | Digital Guardian V6.0.x (Syslog only)
Digital Guardian V6.1.1 and V7.2 (LEEF only) | Syslog
LEEF | All events | Yes | No | No |
| Vericept | Content 360 up to v8.0 | Syslog | All events | Yes | No | No |

Table 522. QRadar Supported DSMs (continued)

| Manufacturer | Device name and version | Protocol | Recorded events and formats | Auto discovered? | Includes identity? | Includes custom properties? |
|---------------------------------------|--|---------------------------------|---|------------------|--------------------|-----------------------------|
| VMware | VMware ESX or ESXi 3.x, 4.x, 5.x and 6.x | Syslog
EMC VMware protocol | Account Information
Notice
Warning
Error
System Informational
System Configuration
System Error
User Login
Misc Suspicious Event
Access Denied
License Expired
Information
Authentication
Session Tracking | Yes if syslog | No | No |
| VMware | VMware vCenter v5.x | EMC VMware protocol | Account Information
Notice
Warning
Error
System Informational
System Configuration
System Error
User Login
Misc Suspicious Event
Access Denied
License Expired
Information
Authentication
Session Tracking | No | No | No |
| VMware | VMware vCloud Director v5.1 | VMware vCloud Director protocol | All events | No | Yes | No |
| VMware | VMWare vShield | Syslog | All events | Yes | No | No |
| Vormetric, Inc. | Vormetric Data Security | Syslog (LEEF) | Audit
Alarm
Warn
Learn Mode
System | Yes | No | No |
| Watchguard | WatchGuard Fireware OS | Syslog | All events | Yes | No | No |
| Websense
(now known as Forcepoint) | | | | | | |
| Zscaler | Zscaler NSS v4.1 | Syslog | Web log events | Yes | No | No |

Part 4. Appendixes

Notices

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

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

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

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

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

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

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

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

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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

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, NON-INFRINGEMENT, 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.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Privacy policy considerations

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Glossary

This glossary provides terms and definitions for the IBM Security 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.

C

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.

console

A display station from which an operator can control and observe the system operation.

content capture

A process that captures a configurable amount of payload and then stores the data in a flow log.

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.

D

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.

H**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.

I**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.

K**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 | See Lightweight Directory Access Protocol. |
| 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.

S

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

See Simple Network Management Protocol.

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.

T

TCP See Transmission Control Protocol.

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.

V

violation

An act that bypasses or contravenes corporate policy.

vulnerability

A security exposure in an operating system, system software, or application software component.

W

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 95

A

About this guide xix
Access Manager for Mobile 484
Action Set for LSM 920
Advanced Firewall Manager
 Logging profile 347
agile 543
agileSI 543
agileSI log source 544
AhnLab Policy Center 97
Akamai Kona 99
Amazon AWS CloudTrail 104, 108
 overview 101
Ambiron TrustWave ipAngel 109
Apache HTTP Server 113, 114, 115
 syslog 113
 syslog-*ng* 114
APC UPS 111
Apple Mac OS
 Apple Mac OS X 117
Apple Mac OS X
 syslog 117
Application Security DbProtect 119
Arbor 123
Arbor Networks Peakflow 123
 Supported event types 124
Arbor Networks Peakflow SP
 Configure a log source 126
 Configuring global notifications
 settings 124
 Configuring remote syslog 124
Arbor Networks PeakFlow SP
 Configuring alert notification
 rules 125
Arbor Networks Pravail 127, 128
Arpeggio SIFT-IT 129, 130
 Additional information 131
Array Networks 133
 SSL VPN 133
Aruba 135
Aruba Mobility Controller 139
Aruba Mobility Controllers 139, 140
automatic updates 3
Avaya VPN Gateway 141, 142
 DSM integration 141
AWS CloudTrail
 overview 101

B

Balabit
 Filtering log file 147
BalaBit 143
 Configuring a log source 149
 PE Relay 148
 Syslog 144

BalaBit (*continued*)
 Syslog-*ng* Agent 146, 147
BalaBit
 IT Security 143
BalaBit IT Security
 Microsoft ISA and TMG Events 146
BalaBit Syslog-*ng* 146
Barracuda 151
 Log source 151
 Syslog 151
Barracuda Web Filter 154
 Log source 155
 Syslog 155
Basic Security Mode 891
BIG-IP
 Log publisher 346
BIG-IP AFM
 High-speed logging destination 346
BIG-IP LTM 352
Bit9 Parity 204, 205
Blue Coat 163, 166, 169
Blue Coat SG 163, 166
BlueCat 161
 Adonis 161
 Event type 161
 Log source 162
BlueCat Adonis 162
Bluemix 435
Bridgewater 177
Bridgewater Systems 177
 Log source 177
Brocade Fabric OS 179
 Syslog 179
bulk add 6, 53

C

CA ACF2 181
CA SiteMinder 189
 Log source 189
 Syslog-*ng* 190
Carbon Black 201
Cascade Profiler 815, 817
Check Point 213, 219
 Add a host 214
 Log source 221, 222
 Log Source SIC 215
 OPSEC 213, 217
 OPSEC Application Object 214
 OPSEC LEA 218
 OPSEC log source 226
 OPSEC/LEA 215
Check Point Firewall
 Syslog forwarders 222
Check Point Multi-Domain Management
 (Provider-1) 224
 OPSEC 226
 Syslog 224
 Syslog events 225
Check Point SmartCenter Server 715
Check Point Syslog 220
Cilasoft QJRN/400 229
 Log source 230
 Syslog 229
Cisco ACE 233
 Log source 233
Cisco ACE Firewall 233
Cisco ACS 236
 Global logging categories 237
 Remote log 236
 v5.x 236
Cisco ACS v4.x
 Log source 239
 Syslog 238
Cisco ACS v5.x
 Log source 237
Cisco Aironet 234
 Log Source 235
Cisco ASA 240, 242
 Log source 241
 Log Source 243
 Syslog 240
Cisco ASASyslog 240
Cisco CallManager 244
 Log Source 245
 Syslog 244
Cisco CatOS
 Catalyst switches 245
 Log source 246
 Syslog 245
Cisco CSA 250
 Log Source 250
 Syslog 250
Cisco FWSM 257
 Log source 258
 Syslog 257
Cisco IDS/IPS 258
Cisco IOS 262
 Log source 263
Cisco IOSForwarding events 262
Cisco IronPort 260
 Log source 261
Cisco ISE
 Logging categories 267
 Syslog events 266
Cisco NAC 268
 Syslog events 268
Cisco Nexus
 Log source 269
 NX-OS 269
 Syslog 269
Cisco NSEL 13
Cisco Pix 270
 Forwarding events 270
Cisco PixSyslog 271
Cisco VPN 3000
 Log source 278
Cisco VPN 3000 Concentrator 278
Cisco Wireless LAN Controller
 Log source 282
 SNMPv2 283, 284
 Syslog 282

Cisco Wireless LAN Controller
(continued)
 Trap receiver 284
Cisco Wireless LAN Controllers 281
Cisco Wireless Services Module
 WiSM 279
Cisco WiSM
 Log source 281
 Syslog 279
Citrix 287
Citrix Access Gateway 289
Citrix NetScaler 287
 Log source 288
CloudTrail 101
Configuring a log source 145
configuring IBM AIX Audit for
 syslog 422
Configuring syslog forwarding 566
Content Gateway Manager 376
Content Management Console 378
cron 893
CRYPTOCARD CRYPTO-Shield 305
 Log source 305
CRYPTOCARD CRYPTO-
 ShieldSyslog 305
CyberArk 307
CyberArk Vault 308
 Log source 309
 Syslog 309
CyberGuard
 Firewall/VPN Appliance 311
 Log source 311
 Syslog 311

D

Damballa Failsafe 313
 Log source 313
 Syslog 313
DbProtect alerts 121
DbProtect LEEF Relay 120
DbProtect LEEF Relay Module 120
Digital China Networks
 DCN DCS/DCRS 318
 DCS/DCRS Series Switch 317
 Log source 317
Domino
 SNMP 463
Domino Server
 Add-in Tasks 463
Dragon Enterprise Management Server
 (EMS) v7.4.0 334

E

EMC VMWare 965
EMC VMware protocol 14
extension documents
 troubleshooting 77
Extreme 331
Extreme 800-Series Switch 331
Extreme 800-Series Switches
 Log source 331
Extreme Dragon 332
 Log source 334

Extreme Dragon EMS
 Alarm tool policy
 Syslog 332
Extreme Dragon EMS v7.4.0
 Syslog 334
Extreme HiGuard Wireless IPS 335
Extreme HiPath Wireless Controller 337
Extreme Matrix K/N/S Series
 Switch 339
Extreme Matrix Router
 version 3.5 338
Extreme NAC 341
 Log source 341
Extreme NetSight Automatic Security
 Manager 340
Extreme Networks ExtremeWare 343
Extreme stackable and stand-alone
 switches 341

F

F5 BIG-IP APM 10.x
 Remote syslog 349
F5 BIG-IP APM 11.x
 Remote syslog 348
F5 BIG-IP LTM
 9.4.2 to 9.4.8 353
 Log source 351
F5 BIG-IP LTM 10.x
 Remote syslog 353
F5 BIG-IP LTM 11.x
 Remote syslog 352
F5 FirePass
 Syslog 354
F5 Networks BIG-IP AFM 345, 347
 Log source 348
F5 Networks BIG-IP APM
 Log source 349
 Remote syslog 348
F5 Networks BIG-IP ASM 350
 Log source 351
F5 Networks BIG-IP LTM 351
F5 Networks FirePass 354
 Log source 354
Fair Warning 357
 Log source 357
Fidelis XPS 363
 Log source 364
 Syslog 363
Firewall Enterprise 614
Forcepoint 981
Forcepoint Technical Support 376
Forcepoint TRITON 372, 373
Forcepoint TRITON and V-Series 373
Forcepoint V-Series 378
Forcepoint V-Series Content
 Gateway 375
Forcepoint V-Series Data Security
 Suite 374, 375
Forcepoint V-Series DSS 374
ForeScout CounterACT 379
 Log source 379
 Plug-in 380
 Policies 380
Fortinet FortiAnalyzer 384
Fortinet FortiGate 384
Fortinet FortiGate Security Gateway 383

forwarded protocol 15
forwarding events 950
Foundry FastIron 385
FreeRADIUS 387
FW 5100 713

G

Generic 389
Generic authorization
 Log source 391
Generic authorization events 389
Generic authorization Server 389
Generic Firewall 391
 Configuring event properties 391
 Log source 393
genua genugate 395
glossary 1007
Great Bay Beacon 397
 Syslog 397

H

H3C Technologies 401
HBGary Active Defense 399
 Log source 399
 Syslog 399
Hewlett Packard UniX
 Logsource 411
Hewlett Packard UNIX (HP-UX)
 Syslog 411
Honeycomb FIM
 Events 403
Honeycomb Lexicon File Integrity
 Monitor 403
Honeycomb Lexicon FIM
 Log source 404
HP 407
HP ProCurve
 Log source 410
 Syslog 409
HP Tandem 410
HTTP Receiver protocol 15
Huawei 413
Huawei AR Series 414
 Log source 464
Huawei AR Series Router 413
Huawei AR Series Routers 413
Huawei S Series
 Log source 415
Huawei S Series Switch 415
 Syslog 416
HyTrust CloudControl 417

I

IBM 419
IBM AIX Audit, configuring for
 syslog 422
IBM AS/400 425
IBM AS/400 iSeries 428
IBM BigFix 429
IBM BigFix protocol 15
IBM CICS 436
IBM Guardium 452
 event map 456

IBM Guardium (*continued*)
 Event maps 455
 Policy 454
 Syslog events 453
 IBM i 427
 IBM IMS 456, 457
 Log source 459
 IBM Informix
 audit 461
 IBM iSeries 425
 IBM ISS Proventia 470
 IBM Lotus Domino 462
 SNMP Services 462
 IBM Network Security (XGS)
 Log source 497
 IBM Proventia Management
 SiteProtector 467
 IBM Proventia® Management
 SiteProtector® 19
 IBM Security Access Manager for Enterprise Single Sign-On 483
 version 8.1 or 8.2 482
 IBM Security Access Manager for Mobile 484
 IBM Security Directory Server 488
 Log source 488
 IBM Security Identity Manager 491
 IBM Security Network Protection (XGS)
 Alerts 497
 LEEF 496
 IBM Security Trusteer Apex Advanced Malware Protection 500
 IBM SiteProtector
 Log source 468
 IBM Tivoli Access Manager e-business 511, 512
 IBM Tivoli Endpoint Manager 513
 IBM WebSphere 513
 IBM WebSphere Application Server 513
 Log source 514
 IBM zSecure Alert 521
 Infoblox NIOS 541
 Internet System Consortium (ISC) Bind 523
 IPTables 592, 697
 IPTables syslog
 log source 593
 IronPort
 Mail log 260
 web content filter 262
 ISC Bind 523
 ISC BIND 524
 Itron Smart Meter
 Array Networks SSL VPN 547

J

JDBC
 Samhain events 832
 JDBC protocol 16
 JDBC SiteProtector protocol 19
 Juniper DX Application Acceleration Platform 551
 Juniper EX Series Ethernet Switch 552, 553
 Juniper IDP
 syslog 553

Juniper Infranet Controller 555
 Juniper Junos OS 556
 Juniper Junos OS Platform device 558
 Juniper Junos WebApp Secure 565
 event logging 566
 Juniper Networks 549
 Juniper Secure Services Gateway (SSG) 560
 Juniper Networks AVT 549
 Juniper Networks AVT device 549
 Juniper Networks Binary Log Format 561
 Juniper Networks Firewall and VPN 555
 Juniper Networks Firewall and VPN device
 events 555
 Juniper Networks NSM
 export to syslog 560
 Juniper Networks NSM protocol 20
 Juniper Networks SRX
 log source 559
 Juniper Networks vGW Virtual Gateway 564
 Juniper Networks WLC Series 568
 Juniper NSM 554
 Juniper Security Binary Log Collector 561, 562
 Juniper Security Binary Log Collector protocol 21
 Juniper Steel-Belted Radius 563
 syslog 564
 Juniper WLC
 syslog 569
 Juniper WLC user interface
 syslog 568

K

Kaspersky 571
 Kaspersky Security Center 571
 database view 574
 Kisco Information Systems SafeNet/i 581

L

Lastline Enterprise 585
 Lexicon mesh service 404
 Lieberman Random Password Manager 587
 Linux 591
 Linux DHCP 591
 Linux DHCP Servers
 log source 591
 Linux IPTables 591
 Linux OS 593
 syslog 594
 log source
 status 5, 11
 log source extension
 disable extension 91
 enable extension 91
 log source extensions 91
 log sources 9
 LOGbinder 597
 Logging pool 345

LSM notification contacts 920

M

Mac OS X log source 117
 manage 91
 McAfee 603
 McAfee Application / Change Control 603
 McAfee Intrushield 615
 McAfee Intrushield V2.x - V5.x 615
 McAfee Intrushield V6.x and V7.x 616
 fault notification events 618
 McAfee Web Gateway 619, 620
 DSM integration 619
 event map 622, 623
 log file protocol 621, 622
 unknown events 623
 media-manager object 747
 MetaInfo MetaIP 625
 Microsoft 627
 Microsoft DHCP protocol 24
 Microsoft DHCP Server 634
 Microsoft Endpoint Protection 637
 log source 637
 Microsoft Exchange protocol 25
 Microsoft Hyper-V 645
 log source 646
 Microsoft IAS
 LOGbinder EX event collection 646
 Microsoft IIS
 IIS Protocol 647
 log source 648, 649
 Microsoft IIS protocol 26
 Microsoft IIS Server
 IIS Protocol 647
 Microsoft Internet and Acceleration (ISA) 650
 Microsoft Operations Manager
 log source 655
 Microsoft Security Event Log protocol 28
 Microsoft SharePoint 658
 audit events 659
 database view 659
 events 658
 log source 660, 663
 Microsoft System Center Operations Manager 670
 Motorola Symbol AP 683
 Motorola SymbolAP 683
 MSGTRK logs 642, 643

N

Name Value Pair 685
 NCC Group DDoS Secure 690
 Niksun NetVCR 2005 695
 Nokia Firewall 697
 custom script 698
 log source 698
 OPSEC 699
 OPSEC/LEA 699
 syslog 697
 Nominum Vantio 703
 None Of SMTP response rule 901

Nortel Application Switch 707
 Nortel Contivity 708
 Nortel Ethernet Routing Switch 2500/4500/5500 708
 Nortel Ethernet Routing Switch 8300/8600 709
 Nortel Multiprotocol Router 705
 Nortel Networks 705
 Nortel Secure Network Access Switch 711
 Nortel Secure Router 710
 Nortel Switched Firewall OPSEC 713
 syslog 712
 Nortel Switched Firewall 5100 712
 Nortel Switched Firewall 6000 713
 Nortel Switched Firewalls OPSEC 714
 syslog 714
 Nortel Threat Protection System 715
 Nortel VPN Gateway 716
 Novell eDirectory 719

O

Observe IT JDBC 723
 ObserveIT 723
 Open LDAP 735
 event forwarding 738
 log source 735
 syslog 737
 Open Source SNORT 739
 syslog 740
 OpenBSD 733
 log source 733
 syslog 734
 ophos Astaro Security Gateway 860
 OPSEC log source 700
 OPSEC/LEA protocol 33
 Oracle 745
 Oracle Acme
 event types 745
 Oracle Acme Packet SBC
 log source 745
 SNMP to syslog conversion 746
 Oracle Acme Packet Session Border Controller 745
 Oracle audit logs 759
 Oracle BEA WebLogic 750
 application logging 751
 audit provider 752
 domain logging 751
 event logs 751
 log source 752
 Oracle database Perl 762
 Oracle Database Listener 764
 Oracle Database Listener protocol 34
 Oracle DB Listener 760
 Oracle Enterprise Manager 764
 Oracle Fine Grained Auditing 765
 Oracle OS Audit 768, 770
 OSSEC 771
 syslog 771
 Outbreak Criteria and Alert Notifications 938
 overview 9, 101

P

parsing order 6, 55
 PCAP Protocol 558
 PCAP Syslog Combination protocol 35
 PGP Universal Server 906
 PGP Universal Servers 906
 Pirean Access: One 783
 log source 783
 PostFix Mail Transfer Agent 787
 PostFix MTA
 log source 787
 multiline UDP syslog events 789
 ProFTPD 791
 Proventia 467

R

Radware DefensePro 803, 805, 806
 Raz-Lee i Security 926
 log source 809
 Raz-Lee iSecurity 807, 925
 Red Hat Enterprise Linux v6 operating systems 595
 Redback ASE 811
 Riverbed 815
 Riverbed SteelCentral NetProfiler 815, 817
 RSA Authentication Manager 819
 Linux 819
 log file protocol 820
 syslog 819
 Windows 820
 RSA Authentication Manager 6.x 821

S

S3 bucket 104, 108
 Samhain HIDS 831
 Samhain Labs 831
 SDEE protocol 37
 Sentrigo Hedgehog 837
 SIFT-IT 129
 SMB Tail protocol 38
 SNMPv2 protocol 39
 SonicWALL
 log source 847
 SonicWALL 847
 Sophos 849
 Sophos database 852
 Sophos Enterprise Console 849, 852
 JDBC 851
 Sophos Enterprise Console JDBC protocol 40
 Sophos Enterprise Console Protocol 849
 Sophos PureMessage 854, 855
 Microsoft Exchange 858
 Sophos PureMessage for Linux 857
 Sophos Web Security Appliance 861
 Spam and Virus Firewall 151
 Splunk 863
 Splunk appliances 863
 Splunk forwarded events 863
 Squid Web Proxy 867, 868
 Standard Notifications 938, 939, 940
 Starent Networks 871
 STEALTHbits 825, 875

STEALTHbits StealthINTERCEPT 875, 876
 log source 875, 877
 Stonesoft Management Center 369, 370, 371
 Sun 883
 Sun ONE LDAP
 log source 887
 Sun Solaris 889
 Sun Solaris Basic Security Mode (BSM) 891
 Sun Solaris BSM 893
 Sun Solaris BSM audit logs 892
 Sun Solaris DHCP 888
 Sun Solaris Sendmail 889, 890
 Sybase ASE 897
 Sybase ASE device 898
 Symantec 899
 Symantec Data Loss Prevention (DLP) 900
 Symantec Endpoint Protection 905
 Symantec SGS 907
 Symantec System Center 908
 Symark PowerBroker 158
 syslog firewall settings on vSphere Clients 964
 Syslog Redirect protocol 42
 Syslog-ng Agent 143, 145

T

TCP multiline syslog protocol 43
 third-party event collection overview 3
 ThreatGRID log file protocol 914
 ThreatGRID Malware Threat Intelligence 913
 ThreatGRID syslog 913
 Tipping Point for SMS 919
 Tipping Point Intrusion Prevention System 919
 Tipping Point x505
 Tipping Point x506 921
 Tipping Point X505/X506 Device 921
 TippingPoint 919
 Tivoli Access Manager
 Configure e-business 511
 TLS syslog protocol 47
 Top Layer IPS 923
 Townsend Security LogAgent 925
 Trend Micro 927
 Trend Micro Control Manager 927, 928
 Trend Micro InterScan VirusWall 936
 Trend Micro Office Scan 936
 Trend Micro Office Scan 10.x 937
 Trend Micro Office Scan 8.x 936
 Trend Micro OfficeScan XG 939
 Tripwire 941
 Tropos Control 943
 Trusteer Apex Local Event Aggregator 507

U

UDP multiline syslog protocol 49
 Universal LEEF 947

Universal DSM 945
unknown events 902, 951

V

Vantio LEEF Adapter 703
log source 703
vCloud Director protocol 52
vCloud event types 968
vCloud log source 969
vCloud REST API 968
Venusense configuration 955
Venusense event filtering 955
Venusense log source 956
Venusense syslog server 955
Venustech Venusense 955
Verdasys Digital Guardian 957, 958, 959
 IPtables 958
Vericrypt Content 360 DSM 961
VMWare 963
VMware ESX and ESXi servers 963
VMware ESX or ESXi 964
VMWare protocol
 read-only account permissions 966
VMWare Protocol 966
VMware protocol for ESX or ESXi
 servers 965
VMware vCenter 967
VMWare vCenter 967
VMware vCloud Director 967
VMware vShield 970, 971
VMware vShield log source 971
Vormetric Data Firewall 974
Vormetric Data Security 973, 975
Vormetric Data Security systems 974

W

WebSphere
 JVM logs 513

X

XML examples 77

Z

Zscaler Nanolog Streaming Service 983
Zscaler NSS 983, 984

IBM[®]

Printed in USA