RSA NetWitness Platform

Event Source Log Configuration Guide



Microsoft Windows

Last Modified: Tuesday, November 19, 2019

Event Source Product Information:

Vendor: Microsoft Event Source: Windows Versions:

- SNARE Enterprise: SNARE for Windows 4.x and earlier, 5.x and later and SNARE for Windows Vista 1.1.1
- SNARE Open Source 4.0.2
- NT, 2000, XP, 2003, Vista Business, Ultimate, and Enterprise
- Windows Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019
- Windows Server 2008 Enterprise with Hyper-V, Server 2008 R2 Standard, Enterprise, and Datacenter
- 7 Professional, Ultimate, and Enterprise
- Windows 8, 10
- Adiscon Event Reporter 8.1, 12.1, 15.x

Note: Microsoft Windows is supported via the third party tools InterSect Alliance SNARE and EventReporter

RSA Product Information::

Supported On: NetWitness Platform 10.0 and later

Collection Method: Syslog

Event Source Log Parser:

- Using third-party collection agent InterSect Alliance SNARE = winevent_snare
- Using third-party collection agent Adiscon Event Reporter = winevent_er

Event Source Class.Subclass: Host.Windows

Configure Microsoft Windows

To configure Syslog collection for Microsoft Windows you must:

- Configure NetWitness Platform for Syslog Collection
- Set up a Third-Party Collection Service

Configure NetWitness Platform

Configure NetWitness Virtual Log Collector

If the transport method from Snare is set to **tabs**, and you are sending information to a Virtual Log Collector, then you need to remove the tab-to-space setting from the VLC syslog configuration, or else the logs will not parse correctly.

Note: If you are sending logs to a log decoder, then no change necessary.

To remove the tab-to-space feature from a VLC:

- 1. Log onto RSA NetWitness Platform as an administrator.
- 2. In the NetWitness menu, select **ADMIN** > **Services**.
- 3. Select a Virtual Log Collector, then **View > Explore**.
- 4. From the left pane, select **logcollection** > **syslog** > **eventsources**.
- 5. Select your syslog configurations. You need to edit all of the syslog translations that you use:
 - syslog-tcp > tcp514
 - syslog-tcp > tcp6514
 - syslog-udp > udp514
- 6. Select the value for the receive_translations parameter, and remove TAB2SPACE:

RSA RESPOND INVESTIGA	TE MONITOR CONFIGURE ADMIN	
Hosts Services Event So	ources Health & Wellness System	Security
🚠 Change Service 🔰 🔟	Log Collector Explore ©	
🗏 pw111rc-vlc - Log Col	/logcollection/syslog/eventsources/syslog-tcp/tcp514	Log Collector
	enabled	true
snmptrap	event_filter	
	event_filter_debug	0
G destinations	inflight_published_log_threshold	0
eventsources	max_receivers	2
Syslog-tcp	name	tcp514
tcp514	node_type	workgroup
tcp6514	olling_interval	2
syslog-udp	port_number	514
🖾 🗁 stats	receive buffer size	2048
C workmanager	receive_translations	LF2SPACE,CR2SPACE,TAB2SPACE,NULL2SPACE
🖬 🗋 vmware	ssl_receiver	false
C windows	ssl_verify_mode	verify-none
Iogs	typespec_version	1.0
🖬 🗋 rest	use_header_ip	true
🖬 🗋 sdk	 use_header_time 	false
RSA NETWITNESS [®] PLATFORM		
RSA RESPOND INVESTIGATE	MONITOR CONFIGURE ADMIN	
Hosts Services Event Sour	۔ ces Health & Wellness System Secur	ity
Character in the second		
m change service		
≡nw111rc-vlc - Log Col <	nigcollection/systep/eventsources/systep/ccp/tcp314	- Log Conector
□ snmptrap	enabled	true
■ 🗁 syslog	event_inter	0
destinations	inflight published log threshold	0
eventsources	max_receivers	2
E 🕀 syslog-tcp	name	tcp514
C1 tcp514	node_type	workgroup
tcp6514	polling_interval	2
syslog-udp	port_number	514
tastats	receive_buffer_size	2048
	receive_translations	LF2SPACE, CR2SPACE, NULL2SPACE
a vmware	ssl_receiver	false
	ssi_verity_mode	verity-none
I Chrest	typespec_version	true
	use header time	false
1200 ¥		

Make sure to make this change for syslog-tcp/tcp514, syslog-tcp/tcp6514, and syslog-udp/udp514.

7. Restart the Virtual log Collector service for your changes to take effect.

Configure NetWitness Platform for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

- 1. In the **NetWitness** menu, select **ADMIN** > **Services**.
- In the Services grid, select a Log Decoder, and from the Actions menu, choose View > System.
- 3. Depending on the icon you see, do one of the following:
 - If you see ^{Start Capture}, click the icon to start capturing Syslog.
 - If you see [•] Stop Capture</sup>, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

- 1. In the NetWitness menu, select ADMIN > Services.
- In the Services grid, select a Remote Log Collector, and from the Actions menu, choose View > Config > Event Sources.
- 3. Select Syslog/Config from the drop-down menu.

The Event Categories panel displays the Syslog event sources that are configured, if any.

4. In the Event Categories panel toolbar, click +.

The Available Event Source Types dialog is displayed.

- 5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
- 6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

The Add Source dialog is displayed.

7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

After you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Set Up Third-Party Collection Services

RSA NetWitness Platform supports Windows logs collected by InterSect Alliance SNARE BackLog, InterSect Alliance SNARE for Windows, and Adiscon EventReporter. You can set up collection by any of the following:

- Set Up InterSect Alliance SNARE BackLog
- InterSect Alliance Snare:
 - Set Up InterSect Alliance SNARE 5.x and Later
 - Set Up InterSect Alliance SNARE Version 4.x and Earlier
 - <u>Collect Sysmon Logs using SNARE</u>
 - <u>Collect Heartbeat Messages using SNARE</u>
- Set Up Adiscon EventReporter

Note: If you install the SNARE agent on a Windows Vista or Server 2008 system, you must use SNARE for Windows Vista version 1.1.1.

Set Up InterSect Alliance SNARE BackLog

To set up InterSect Alliance SNARE BackLog:

- 1. Set the Target Host to the hostname of the RSA NetWitness Platform Log Decoder or RSA NetWitness Platform Remote Log Collector collecting the events.
- 2. Set the Syslog Category to Syslog Debug.
- 3. Set the Delimiter to **Tab**.

Note: If you set these incorrectly, you can run **configurator.exe**, located in the installation directory (the default installation directory is **C:\Program Files\Backlog**).

Set Up InterSect Alliance SNARE 5.x and Later

To install and set up InterSect Alliance SNARE on Windows Server 2008 Server Core:

- Click My Computer > Tools > Map Network Drive, and follow these steps to map a drive:
 - a. From the Drive drop-down list, select the drive which you want to map.
 - b. In the Folder field, enter the IP address of the drive to be mapped.

For example, if the IP address of the core server machine is 1.1.1.1 and the drive to be mapped is C:, enter (1.1.1)c in the Folder field.

- c. Select Reconnect at logon.
- d. Select **Connect using a different user name option**, and enter the logon credentials for the Server Core machine.
- 2. Create a new directory on Server Core, such as C:\files.
- 3. Go to https://www.snaresolutions.com/products/snare-agents/ and download the latest agent.
- 4. Copy the SNARE installation file to the directory that you created in step 2.
- 5. Follow these steps to install SNARE on the Server Core installation:
 - a. Open a command shell, and change directories to the directory that you created in step 2.
 - b. To install SNARE, type:

C:\files\SnareSetupVista-1.1.1-MultiArch.exe

Note: When installing the SNARE agent on a Server 2008 Server Core installation, you must set the **Remote Control Interface** setting to **YES** – **with password**. If this option is not selected, the SNARE agent can only be configured through the registry.

6. To configure the settings through the Internet, open a web browser to localhost:6161.

Note: If a firewall prevents the connection, to make a rule that allows connection to the web interface, you can run the command:

```
C:\ netsh advfirewall set all profiles firewallpolicy allowinbound, allowoutbound
```

- 7. Configure Destination settings as follows
 - a. Set the Destination Snare Server Address to the IP address of the RSA NetWitness Platform Log Decoder or RSA NetWitness Platform Remote Log Collector collecting the events.
 - b. Set protocol, format to syslog RFC3164
 - c. Set delimeter=tab
 - d. Set Syslog facility =syslog
 - e. Set Syslog priority = debug
 - f. Update destinations.

> Network Destinati	ons					
Multiple destinations	per protoco	ol may be confi	igured to send the events to y	our SIEM.		
Domain / IP	Port	Protocol	Format	Delimiter Character		
100 100 100 10	514	UDF -	SYSLOG (RFC3164)	Tab	-	

- 8. Apply the configuration and restart the snare service:
 - a. To stop the service, at the command prompt, type:

C:/sc stop snare

b. To start the service, type:

C:/sc start snare

c. To verify that the SNARE service is running, type:

C:/sc query snare

Set Up InterSect Alliance SNARE Version 4.x and Earlier

Note the following:

- RSA NetWitness Platform supports Open Source and Enterprise SNARE.
- DNS server logs are not supported by SNARE for Windows Vista 1.1.1 on Windows Server 2008.

To set up InterSect Alliance SNARE version 4.x:

Note: RSA recommends and supports Tab delimited logs by default. If you select tabdelimited logs, and are sending logs to a Virtual Log Collector, see <u>Configure NetWitness</u> <u>Virtual Log Collector</u> for configuration details.

- Set the Destination Snare Server Address to the IP address of the RSA NetWitness Platform Log Decoder or RSA NetWitness Platform Remote Log Collector collecting the events.
- 2. Set the Destination Port to **514**.
- 3. If you use SNARE for Windows 4.0.0.2 and later, ensure that the following options are selected:

Note: If you use an earlier version of SNARE for Windows, skip this step.

- Allow SNARE to automatically set audit configuration.
- Allow SNARE to automatically set file audit configuration.
- 4. Set the Syslog facility to **Syslog**.
- 5. Set the Syslog Priority to Debug.
- 6. Ensure that Enable Syslog Header is selected.

7. Ensure that Use Alternate Header is cleared, as shown here:

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	
Destination Snare Server address (Multiple destinations available in the enterprise version)	192.168.
Destination Port	514
Allow SNARE to automatically set event log max size (Enterprise version only)	Π
Event Log Cache Size (Note that if you wish to shrink the size of the cache, you will need to clear each event log) <u>(Enterprise version only)</u>	Ома
Use UDP or TCP (Enterprise version only)	© UDP © TCP © TLS/SSL
Encrypt Messages (Requires Snare Server 4.2 and above, <u>enterprise version only</u>)	Π
Perform a scan of ALL objectives, and display the maximum criticality?	
Allow SNARE to automatically set audit configuration?	v
Allow SNARE to automatically set file audit configuration?	v
Export Snare Log data to a file?	Ε
Use Coordinated Universal Time (UTC)? (Enterprise version only)	п
Use Dynamic DNS Names? (Enterprise version only)	п
Custom Event Log? (Enterprise version only)	п
Enable active USB auditing? (This option requires the service to be fully restarted)	
Enable SYSLOG Header?	v
EVELOG Espility	(Use alternate header?)
STOLOG Faulty	
SYSLUG Priority	

- 8. Press Change Configuration.
- 9. Restart the SNARE service.

To install and set up InterSect Alliance SNARE on Windows Server 2008 Server Core:

- Click My Computer > Tools > Map Network Drive, and follow these steps to map a drive:
 - a. From the **Drive** drop-down list, select the drive which you want to map.
 - b. In the Folder field, enter the IP address of the drive to be mapped.

For example, if the IP address of the core server machine is 1.1.1.1 and the drive to be mapped is C:, enter 1.1.1.1 in the Folder field.

- c. Select Reconnect at logon.
- d. Select **Connect using a different user name option**, and enter the logon credentials for the Server Core machine.
- 2. Create a new directory on Server Core, such as C:\files.
- Copy the SNARE installation file (downloaded from http://www.intersectalliance.com/projects/SnareWindows/index.html#Dow to the local machine) to the directory that you created in step 2.
- 4. Follow these steps to install SNARE on the Server Core installation:

- a. Open a command shell, and change directories to the directory that you created in step 2.
- b. To install SNARE, type:

C:\files\SnareSetupVista-1.1.1-MultiArch.exe

Note: When installing the SNARE agent on a Server 2008 Server Core installation, you must set the **Remote Control Interface** setting to **YES – with password**. If this option is not selected, the SNARE agent can only be configured through the registry.

5. To configure the settings through the Internet, connect to the interface through a web browser.

For example if the IP address of the Server Core host is 1.1.1.1, go to http://1.1.1.16161/

Note: If a firewall prevents the connection, to make a rule that allows connection to the web interface, you can run the command:

```
\texttt{C:}\ netsh advfirewall set all profiles firewall
policy allowinbound, allowoutbound
```

6. To configure the settings, follow steps 1 to 6 of the preceding SNARE setup procedure.

Follow these steps to restart the SNARE service:

1. To stop the service, at the command prompt, type:

C:/sc stop snare

2. To start the service, type:

C:/sc start snare

3. To verify that the SNARE service is running, type:

```
C:/sc query snare
```

Collect Sysmon Logs using SNARE

Use this procedure to collect Sysmon messages.

- 1. After you set up SNARE to collect syslog on the Log Decoder, open the Intersect Alliance SNARE Agent for Windows admin console.
- 2. In the left navigation pane, select Objectives Configuration.
- 3. Add the Microsoft-Windows-Sysmon channel.

The following figure shows an example where the **Microsoft-Windows-Sysmon** channel has been added:

	SNARE Agent for Windows									
Latest Events Network Configuration Remote Control Configuration	The following filtering of	bjectives of t	SNARE Fi	iltering	Obje	ctives (Configuration			
Upjectives Configuration	Action Required	Criticality	Event ID Include /Evolude	Event ID Match	Licor Match	Conoral Match	Course Match	Boturn	Event Fre	Order
Versites and rules toy Were Audit Service Status Apply the Latest Audit Configuration Local users and once Members bomain Group Members	Delete Modify	Critical	Include	*	Include: *	Include: *	Include: Microsoft-Windows-Sysmon	Success Failure Error Information Warning ActivityTracing Critical Verbose	Custom	
	Select this button to add a new objective. Add (SGP) = Super Group Policy, (ACP) = Agent Group Policy, (LR) = Local Registry, (D) = Default Value SGP and AGP settings are read-only and can only be edited by group policy administrator (c) Intersect Alliance Phy Ltd 1999-2016. This site is powered by <u>SMARE for Windows</u> .									

Collect Heartbeat Messages using SNARE

Use this procedure to collect Heartbeat messages.

- 1. After you set up SNARE to collect syslog on the Log Decoder, open the Intersect Alliance SNARE Agent for Windows admin console.
- 2. In the left navigation pane, select HeartBeat and Agent Log.

The Snare HeartBeat and Agent Log Configuration page opens.

	SNARE Enterprise Agent for Windows				
Latest Events Network Configuration	Snare HeartBeat	and Agent Log C	Configuration		
Remote Control Configuration Objectives Configuration	The following general configuration parameters of the Sn	are agent are set to the following values:			
HeartBeat and Agent Log View Audit Service Status	Agent Logging Options	Service logs (LR)			
Apply the Latest Audit Configuration	Agent Heartbeat Frequency	15 mins + (LR)			
Local overs Domain Users Local Group Members Domain Group Members	Change Configuration Reset Form (SGP) = Super Group Policy, (AGP) = Agent Group Policy, (LI	i) = Local Registry, (D) = Default Value			
	SGP and AGP settings are read-only and can only be edited by group	o policy administrator			
	(c) <u>Intersect Alliance</u> F	ty Ltd 1999-2016. This site is powered by SNARE for V	Vindows.		

- 3. Select the following Agent Logging Options:
 - Service logs
 - Trace logs
- 4. From the Agent Heartbeat Frequency drop-down menu, choose 15 minutes.

- 5. Click Change configuration.
- 6. From the left pane, click Apply the Latest Audit Configuration.
- 7. From the right pane, click **Reload Settings**.

Set Up Adiscon EventReporter

RSA NetWitness Platform supports EventReporter 8.1, 12.1, and 15.x.

Note: By default, DNS server logging is not selected.

Note: The **Default EventLog Monitor Service** is compatible only with Windows Server 2008 Enterprise Edition. The service is not compatible with Windows Server 2008 Standard Edition and is therefore not supported by RSA NetWitness Platform.

You must complete the following tasks to set up Adiscon EventReporter:

- 1. Configure EventReporter based on your version:
 - Set Up Adiscon EventReporter Version 15.x, or
 - Set Up Adiscon EventReporter Version 8.1 and 12.1
- 2. (Optional) Set Up Hyper-V and Powershell Operational Logs

Set Up Adiscon EventReporter Version 15.x

EventReporter 15.x automatically installs the Event Log Monitor V2 service. However, in order to generate log records in the appropriate RSA NetWitness format for the v20_winevent_ermsg.xml parser, the Eventlog Monitor V1 service must be added.

To add the Eventlog Monitor V1 service:

- 1. Launch the EventReporter Configuration Client.
- 2. Right click Services.
- 3. Select Add Service > Eventlog Monitor V1.

The General tab is displayed.

4. Make sure that all of the options in the screenshot below are selected.

Ele Tools Help Save Reset Change Qut Verify Configuration Connect Localhost Star Stop Restart Up Down Name: Eventlog Monitor VI © Enabled * © Enabled (I * © Comments © Settings © Confirm @ Reset © General General Options Event Channels Seep Time(ms) Overnun Prevention Delay (ms) Prefered Inguage Compress Spaces and Remove Control Characters Compress Spaces and Remove Cont	Ele Tools: Help Save RestChanges: Qut Verly Configuration: Connect Localhost: Stat: Stop: Restat: Up Down Service Events Connect Conn
Save Reset Changes Quit Verify Configuration Connect Locabaet Sate Stop Restat Up Down Service Reset Changes Quit Verify Configuration Connect Locabaet Sate Stop Restat Up Down Service Services General Debug Service Services Service S	Stree Reet Changes Out Verty Configuration Connect Localitiest State Stop Returt Up Down Street Changes Out Name: Eventlog Monitor VI © Enabled • © Enabled (T • © Comments © Settings © Confirm @ Reset ©) Street Changes Out Name: Eventlog Monitor VI © Enabled • © Enabled (T • © Comments © Settings © Confirm @ Reset ©) Peters Log Monter VI Enable • © Enabled • © Enabled • © Infine © © Comments © Settings © Confirm @ Reset ©) Peters Log Monter VI Enable • © Compress State ©) Peters Log Monter VI Enable • © Enable • © Infine © © © © © © © © © © © © © © © © © © ©
Service Everts General Corneral Services Corneral Options Evertlog Monitor V1 Corneral System	Image: Service Events Image:
Save atter amount of entries 100	

5. Select the **Event Channels** tab and verify that the options in the screenshot below have been selected.

Note: At a minimum, select Security and System.

Tools Help	
🔇 📲 🔍 📓 🌚 📗	
Reset Changes Quit Verify Configuration Connect Localhost Si	art Stop Restart Up Down
Service Events Name: Eventlog Monitor V1 🤡 Enabled	🔹 🕫 Enabled (T 🔹 🔞 Comments 📓 Settings 🛛 😓 Confirm ಿ Reset 🎯
😵 License	
General General Ontions Event Channels	
Pengine	
🚱 Queue Manager 🛛 🔛 Select All 🛄 Deleselect All 🧯	Reload All LastRecords 🛛 🛞 Reset All LastRecords
Event Log Monitor V2 Enable Eventlog Channel	Eventlog Channels
Eventlog Monitor V1 Application	Report Truncated Log
Default RuleSet	Do NOT process existing entries
ForwardSyslog Internet Explorer	Iny to convert Security IDs (SID) to Object Names
Key Management Service	Use Checksum to verify the last processed event
ForwardSyslog	
System	Always search for the last processed Event using the Checksum
windows Powersneii	Syslog Facility Local 0 V
	Last Record 0 Reset
	Read Eventlog from File
	File_Path Name Browse
	Type of Eventlog Application
	Enable date replacement characters (See manual for more)
	Office tile second to
	- Processed file remarties
	Last Record
	A Deat
	43 LICOCI
	Eventlogtypes to Log
	Success Information
	Information
	Warning Warning
	Error Fron
	Audit Success Notice
	Audit Failure Warning
	- vvormig V

- 6. Select Rule Sets > Default Rule Set > ForwardSyslog > Actions > ForwardSyslog
- 7. For **Syslog Server**, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector, and verify that the options in the screenshot below have been selected:

EventReporter Configuration Clie	ant		>
File Tools Help	an		
1 🐴 🚛			
Save Reset Changes Quit Verify	y Configuration Connect Localhost	Start Stop Restart Up Down	
Service Events	Name: ForwardSyslog 🥝 Enabled	🝷 🔞 Comments 📓 Settings 🛛 😓 Confirm 🧔 Reset 🎯 🗐 Config	gure for 🕶
	Protocol Type		
	Syslog Receiver Options	ODF	*
Queue Manager	Syslog Server	Netwitness Log Decoder IP Addre	ss.
Event Log Monitor V2	Syslog Port	514	
	Use this backup syslog server if first or	ne fails.	
E- Contract Rule Set			
ForwardSyslog Fiters	Backup Syslog Server		
Actions	Backup Syslog Port	514	
IIIII 🤹 Forward Syslog	Session Timeout	30 minutes	~
	Syslog Message Options SSL/TLS relat	ted Options TCP related Options UDP related Options	
	Use Custom Syslog Header	<%syslognfac%>%syslogver% %imereported.::date-frc3339% %source% %syslogappname% %syslogprocid% %syslogmsgid% %syslogstructdata%	↑ Insert
	Output Encoding		*
	Include UTF8 BOM in message	System Derault	~
	Use XML to Report		
	Forward as MWAgent XML represent	ation code	
	Use CEE enhanced Syslog Format		
	Message Format	%msg%	∧ Insert
	🗆 Add Cales Course when forwards a	te etter Curles secure	¥
	Use zLib Compression to compress th	ie data.	
	Compression Level	Best Compression	\sim

Set Up Adiscon EventReporter Version 8.1 and 12.1

To set up Adiscon EventReporter 8.1 or 12.1:

- From the Windows Start menu, click Programs > EventReporter > EventReporterConfiguration.
- 2. In the left-hand panel, double-click Configured Services, and follow these steps:
 - a. Click **Default EventLog Monitor** > **Advanced Options.**
 - b. Select Use Legacy Format.

- c. Select only Add Facilitystring, Add Username, and Add Logtype.
- d. Click Save.
- 3. Follow these steps to configure syslog forwarding:
 - a. In the left-hand panel, double-click Rule Sets > Default RuleSet > Forward Syslog > Actions.
 - b. Select Forward Syslog.
 - c. In the **Syslog Server** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector collecting the events.
 - d. Clear Add Syslog Source when forwarding to other Syslog servers.
 - e. Ensure that the Message Format is %msg%.
 - f. Leave all other options at the default settings.
- 4. Restart the EventReporter service.

(Optional) Set Up Hyper-V and Powershell Operational Logs

This procedure is optional. Follow these steps only if you are configuring Hyper-V and Powershell.

To configure Hyper-V and Powershell:

Note: EventReporter 11.1, 12.1, or higher is required to configure Hyper-V/Powershell support.

- From the Windows Start menu, click Programs > EventReporter > EventReporterConfiguration.
- 2. To create a rule set, follow these steps:
 - a. In the left-hand panel, right-click Rule Sets, and select Add Rule Set.
 - b. Name the rule set, and click Next.
 - c. Select Forward Syslog, and accept all other defaults to add the rule set.
 - d. Select your rule set from RuleSets, and click Forward Syslog > Actions > Forward Syslog.
 - e. Accept all defaults, and complete the fields as follows:

- Syslog Server: the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
- Message format: [%level%] %timegenerated%: %user%/%source%/%sourceproc% (%id%) - "%msg%"

Note: If you cut and paste the message format string, ensure that the string does not contain any line or paragraph breaks.



- 3. To configure a service to use the rule set, follow these steps:
 - a. Right-click Configured Services, and click Add Service > Event Log Monitor V2.
 - b. Accept all defaults, and click Next.
 - c. Click Finish.
 - d. Click the new service.
 - e. By default, all items are selected. Clear all items except those that start with the string Microsoft-Windows-Hyper-V or Microsoft-Windows-Powershell/Operational.

Note: The Hyper-V and Powershell items are under **New EventLog** - **Serviced Channels** > **Microsoft** > **Windows**.

- f. In the Rule Set to Use field, select your rule set.
- g. Click Save.
- 4. Restart the EventReporter service.

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.