Rsyslog and Winsyslog

Rsyslog and Winsyslog are two almost identical agents (similar GUI). They are marketed by the same company. There are a few differences depending on the licence. You can see the comparison ici and ici.

Rsyslog and Winsyslog are configured in the same way.

note: Rsyslog and Winsyslog are proprietary and licensed.

Installation

File .exe which you can download ici (rsyslog) and/or ici (winsyslog).

Create a rule

The first step is to create a rule. A default rule already exists. You can delete it.

To add a rule, right-click on RuleSets > Add RuleSet

Name your rule and tick only ". Add a single Rule including these Actionsand " Syslog Forwading "

🙀 Add RuleSet		_	□ ×	
Adding a new RuleSet				
Enter the Name of the		ОК]	
ForwardSyslog			Cancel	
For example MyRuleSet or RuleSet1				
After the RuleSet has been added				
O Do not add a Rule yet.				
Add a single Rule including these Actions.				
Add a Rule for each of these Actions.				
Storing Actions				1
Forwarding Actions				
Send RELP	Syslog Forwarding			
Internal Actions	2			
Call RuleSet	Compute Status Variable			
Discard	Normalize Event			
Set Property	Set Status			
Other Actions				

 \times

note: this rule simply forwards logs without any particular filter

The rule appears in the left side menu.

🚏 RSyslog Windows Agent Configuration Client



Expand the tree to find the rule action and click on it.

2025/05/03 04:09

3/7

🚏 RSyslog Windows Agent Configuration	Client			- 🗆	×
File Tools Help	iguration Cor	a and the start stop Restart	Jp Down DebugLog		
Service Events General General General General General Queue Manager Services Forward Syslog Single Rule Filters Syslog Forwarding	RuleSets > Protocol Ty Syslog Targ Syslog Sel Image: Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Backu Backu	ForwardSyslog > SingleRule > Syslog ForwardSyslog > SingleRule > Syslog ForwardSyslog > SingleRule > Syslog ForwardSyslog Syslog Message Opt DP UDP et Options Syslog Message Opt TCP (NOT RECTCP (NOT RECTCP (NOT RECTCP (Persisten) TCP (Persisten) TCP (Persisten) TCP (Persisten) ngle syslog server with optional backup server Receiver Options Server Port 514 this backup syslog server p Syslog Server p Syslog Port 514	rding Image: Enabled Image: Enabled	ngs Confirm	
	Amount - Syslog	of messages send to each syslog server before lo Servers	ad balancing 1000		
		Syslog Server	Syslog Port		
	•	Enter value for Syslog Server	Enter numvalue for Syslog Port		

Choose **UDP** or **TCP** according to your preference, enter the**IP** address address of the Syslog server and the port.

To finish, click on **Confirm** "in the top right-hand corner.

Defining a Syslog server

Right-click on Services > Add Service > Syslog Server



Status Trial period, days left 30

Connected To: localhost

Configure the server to be reached by entering :

- IPv4 or IPv6
- Protocol

- IP address
- Listening port

Then, at the bottom, select the rule you created earlier.

🚏 RSyslog Windows Agent Configuration (Client		_		×
File Tools Help					
Save Reset Changes Quit Verify Config	guration Connect Localhost Star	rt Stop Restart Up Down DebugLog			
Service Events	Services > Syslog Server 🥝 Enab	oled 🔹 🔻 🚯 Comments 📓 Settings 🛛 😓 Confirm 🚑 Reset 🎯			
	Iake source system from Syslog n Save original source into property	message ,			^
Queue Manager	Propertyname:	sourceorig	Inser	t	
Services Services Event Log Monitor V2 Syslog Server	Escape control characters				
E	Enable RFC3164 Parsing				
idational for the second state of the second	Use original message timestamp	(RFC 3164) timestamp (RFC 3164)			
	✓ Enable RFC5424 Parsing				
	Append ProcessID to Syslogtag if available				
	RuleSet to use	Course 10 also		Defeat	
1		Forward Syslog	<u> </u>	Refresh	_
Status Trial period, days left 30			Connecter	d lo: local	host

Configure the Syslog agent

Right-click on Services > Add Service > EventLog V1 or V2 Monitor

Depending on OS version :

- EventLog V1 monitor: 2000, XP, 2003
- EventLog V2 Monitor: Vista, 2008, 7, 10

note: for server versions, refer to the kernel (e.g. microsoft server 2019 = windows 10) Services > Add Service > Eventlog Monitor V1/2

Click on the " Event Channels "

🚏 RSyslog Windows Agent Configuration Cl	ient		_		×
File Tools Help					
Save Reset Changes Quit Verify Configu	uration Connect Localhost Sta	rt Stop Restart Up Down DebugLog			
Service Events	Services > Eventlog Monitor V2	🔰 Enabled 🛛 👻 🔯 Comments 📓 Settings 🛛 😓 Confirm 🧔 Reset	2		
General Gen	General Options Event Caching E Overrun Prevention Delay (ms) Select MessageFormat Copy Format into Property Select MessageFormat store into Property Syslog Tag Value Eventpolling related Options	5 Predefined Event Format Disabled msgcopy EvrntSLog	milliseconds	>	^
	Sleep Time(ms)	1 Minute V			
	Wait time after action failure	15 seconds 🗸			
	Emulate %Param% properties from Include optional Event Parameter Convert to EventLog Monitor V1	n old EventLog Monitor rs as properties? compatible Events			
	Process unknown/unconfigured Enable remote EventLog monitori	Eventlog Channels ng			
	Monitor Eventlog from this host: Verify Connection			~	~
Status Trial period, days left 30			Connected 1	fo: local	host .:

From here you can select the eventslog to be forwarded. Don't forget to select the right rule at the bottom of the window (if there are several) and save before exiting.

🚏 RSyslog Windows Agent Configuration C	- 🗆 ×			
File Tools Help				
Save Reset Changes Quit Verify Configu	ration Connect Localhost Start Stop	Restart Up Down DebugLog		
···· Service Events □···· Service Events □···· Service Events ···· S	Services > Eventlog Monitor V2 Senable	ed Comments Settings Reload All LastRecords Evention Channels Figure 1 and Channels	Records	
Queue Manager	Enable Eventiog Channel		s existing entries	
Services	Microsoft-Management-01/A	Try to convert S	ecurity IDs (SID) to Object Names	
Syslog Server		Facility	Local 0 V	
⊟ 💑 RuleSets	Microsoft-ServerCore-Shell	auncher/Admin Last Record	0 🙌 Reset	
Konserver Single Bule	Microsoft-System-Diagnostic	cs-DiagnosticI Processing Mode	Evention Subscription (Realtime)	
	Microsoft-User Experience \	√irtualization-A Eventpolling relate	ed Options	
	Microsoft-User Experience \	√itualization-A Read Eventlog	from File	
Sysiog Forwarding	Microsoft-User Experience V	√irtualization-l		
	Microsoft-User Experience V	Virtualization-S File Path Name	Browse	
	Microsoft-Windows-AAD/Op	perational Evention Types to		
	Microsoft-Windows-AllJoyn	Operational Verbose	Netter	
	Microsoft-Windows-All-User-	-Install-Agent/	Notice	
	Microsoft-Windows-AppHos	t/Admin	Information ~	
	Microsoft-Windows-AppID/0	Operational Warning	Warning ~	
	Microsoft-Windows-Applicab	pilityEngine/O	Error ~	
	Microsoft-Windows-Applicati	ion Server-Ap Critical	Critical ~	
	RuleSet to use	orwardSyslog	V Refresh V	
Status Trial period, days left 30	Status Trial period, days left 30			

Start the service

Click on start to start the service. Once the service has been configured and started, you can close the program.

😤 RSyslog Windows Agent Configuration Client	_		×
File Tools Help			
Save Reset Changes Quit Verify Configuration Connect Localhost Start Stop Restart Up Down DebugLog			
Service Events General Connect Conne			
Status Trial period, days left 30	Connected 1	local	nost 🚲

From: https://wiki.esia-sa.com/ - Esia Wiki

Permanent link: https://wiki.esia-sa.com/en/syslog/syslog_rsyslog_winsyslog



Last update: 2023/11/09 18:07