Rsyslog et Winsyslog

Rsyslog et Winsyslog sont deux agents quasiment identiques(GUI similaire). Ils sont commercialisés par la même entreprise. Il y a quelques différences selon la licence. Vous pouvez voir la comparaison ici et ici.

1/8

Rsyslog et Winsyslog se configurent de la même façon.

note : Rsyslog et Winsyslog sont propriétaires et sous licence.

Installation

Fichier .exe à exécuter que vous pouvez télécharger ici (rsyslog) et/ou ici (winsyslog).

Créer une règle

Dans un premier temps il faut créer une règle. Une règle par défaut est déjà présente. Vous pouvez la supprimer.

Pour ajouter une règle cliquez droit sur **RuleSets > Add RuleSet**

Nommez votre règle et cochez uniquement « Add a single Rule including these Actions. » et « Syslog Forwading »

ast update: 2023/03/09 14:50	syslog:syslog_rsyslog_winsyslog_https://wiki.esia-sa.com/s	syslog/syslog	_rsyslog_winsysl
🤯 Add RuleSet	-		×
	Adding a new RuleSet	F	
Enter the N	lame of the new RuleSet	ОК	
ForwardSyslog		Cance	el
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			
Forwarding Actions			
Send RELP	Syslog Forwarding		
Internal Actions	2		
Call RuleSet	Compute Status Variable		
Discard	Normalize Event		
Set Property	Set Status		
Other Actions			

note: cette règle forward simplement les logs sans filtre particulier

La règle apparaît dans le menu latéral gauche.

3/8

_

 \times

🚏 RSyslog Windows Agent Configuration Client

File Tools Help		
Save Reset Changes Quit Verify Config	ration Connect Localhost Start Stop Restart Up Down DebugLog	
Service Events General General General Conse General Conse General Conse Cons	Comments <table-cell></table-cell>	
Status Trial period, days left 30	Connected	To: localhost

Développez l'arborescence jusqu'à l'action de la règle et cliquez sur celle-ci.

🚏 RSyslog Windows Agent Configuration C	lient				_		×
File Tools Help							
Save Reset Changes Quit Verify Config	uration Co	nnect Localhost Start	Stop Restart U	p Down DebugLog	_		
Service Events S General 	RuleSets >	ForwardSyslog > SingleRu	ile > Syslog Forward	ling 🔮 Enabled 🔹 🔻 🔞 Comments 📓 Sett	ings 🛃 Cor	nfirm	
	Protocol Ty	уре	UDP			~	
Gueue Manager Services Event Log Monitor V2 Services	Syslog Tar	get Options Syslog Message	UDP e Opt TCP (NOT RECO TCP (Persistent o TCP (Persistent o	DMMENDED, one message per connection) connection) connection, Octet based framing)			
Forward Syslog Single Rule Single Rule Single Filters	 Syslog S Use s 	end mode ingle syslog server with optior	RFC3195 Raw nal backup server				
"⊡	- Syslog Syslog	Receiver Options Server					
	Syslog	Port a this backup syslog server if f	514 first one fails.				
	Back	up Syslog Server					
	O Use n	ound robin (multiple syslog ser	vers)				
	Amount	of messages send to each sy	rslog server before loa	d balancing 1000			
	Syslog	Servers					
		Syslog Server	uor*	Syslog Port			
	•	Enter value for Syslog Sen	ver	Enter numvalue for Syslog Polt			×

Choisissez **UDP** Ou **TCP** selon votre préférence, entrez l'**adresse IP** du serveur Syslog et le port.

Pour terminer cliquez sur « Confirm » dans le coin supérieur droite.

Définir un serveur Syslog

Faites clique droit sur **Services > Add Service > Syslog Server**



🚏 RSyslog Windows Agent Configuration (Client			_		×
File Tools Help						
Save Reset Changes Quit Verify Config	guration Connect Localhost Start	Stop Restart Up Down DebugLog				
Service Events General Gener	Services > Syslog Server Enabled Test Syslog Server Internet Protocoltype Protocol Type IP Address Listener Port General Encoding UDP Options Resolve Hostnames Take source system from Syslog mes Save original source into property Propertyname: Escape control characters Enable RFC3164 Parsing Use original message timestamp (RF Try to parse year from message times Enable RFC5424 Parsing	Comments Settings Confirm Reset	©	Insert	······································)]]

Status Trial period, days left 30

Configurez le serveur à joindre en entrant :

- IPv4 ou IPv6
- Protocole
- Adresse IP
- Porte d'écoute

Ensuite tout en bas sélectionnez la règle qui vous avez créé au préalable.

🚏 RSyslog Windows Agent Configuration (Client		_		\times
File Tools Help					
Save Reset Changes Quit Verify Confi	guration Connect Localhost St.	▶ I I I I I I I I I I			
General	Services > Syslog Server 🥝 Ena	ibled 🔹 🔞 Comments 📓 Settings 🛛 😓 Confirm 🚑 Reset 🥥			
	Iake source system from Syslog Save original source into propert	i message ty			^
Queue Manager	Propertyname:	sourceorig	Insert		
Systog Server	Escape control characters				
ia	Enable RFC3164 Parsing				1.
T¥ Filters Actions 	Use original message timestamp Try to parse year from message	p (RFC 3164) : timestamp (RFC 3164)			
a of old g f of harding	Enable RFC5424 Parsing				
	Append ProcessID to Syslogtag	g if available			
					_
	RuleSet to use	ForwardSyslog	l}∼	Refresh	•
Status Trial period, days left 30			Connected	lo: local	host .:

Configurer l'agent Syslog

Faites clique droit sur Services > Add Service > Moniteur EventLog V1 ou V2

Selon la version de l'OS :

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

note : pour les versions serveurs se référer au noyau (ex : microsoft server 2019 = windows 10) Services > Add Service > Eventlog Monitor V1/2

Cliquez sur l'onglet « Event Channels »

7/8

🊏 RSyslog Windows Agent Configuration	Client	-	- 🗆	×
File Tools Help				
Save Reset Changes Quit Verify Con	figuration Connect Localhost St	art Stop Restart Up Down DebugLog		
General	Services > Eventlog Monitor V2	🔮 Enabled 🔹 🔻 🔞 Comments 📓 Settings 🔚 Confirm 🖓 Reset 🥥		
	General Options Event Caching	Event Channels		î
Queue Manager	Overrun Prevention Delay (ms)	5 villisecond	s	
Syslog Server	Select MessageFormat	Predefined Event Format	~	
Eventlog Monitor V2	Copy Format into Property			
E Sorward Syslog	Select MessageFormat	Disabled	\sim	
⊡ SingleRule	store into Property	msgcopy In	sert	
Actions	Syslog Tag Value	EvntSLog		
🦾 🧠 Syslog Forwarding	Eventpolling related Options			
	Sleep Time(ms)	1 Minute v		
	Subscription related Options			
	Wait time after action failure	15 seconds 🗸		
	Emulate %Param% properties fro	m old EventLog Monitor		
	Include optional Event Parameter	ers as properties?		
	Convert to EventLog Monitor V	1 compatible Events		
	Process unknown/unconfigured	l Eventlog Channels		
	Enable remote EventLog monito	ring		
	Monitor Eventlog from this host:			
	Verify Connection			
Status Trial period, days left 30		Conner	ted To: Loc:	alhost

À partir de là vous pouvez sélectionner les eventslog à forward. N'oubliez pas de sélectionner la bonne règle au bas de la fenêtre. (si il y en a plusieurs) et d'enregistrer avant de quitter.

🚏 RSyslog Windows Agent Configuration C	-		×		
File Tools Help					
Save Reset Changes Quit Verify Config	uration Connect Localhost Start Stop Restart Up Down DebugLog				
	🗄 Services > Eventlog Monitor V2 🤡 Enabled 🛛 👻 🔞 Comments 📓 Settings 🛛 😓 Confirm Reset	0			
- Seneral - Seneral - Seneral	Select All Deleselect All Select All Reload All LastRecords			^	
	Enable Eventlog Channel				
Grow Gueue Manager	Microsoft-Management-UI/Admin Do NOT process existing entries				
Syslog Server	Microsoft-Rdms-UI/Admin	t Names			
Eventlog Monitor V2	Microsoft-Rdms-UI/Operational Facility Local 0		\sim		
Error Rule Sets	Microsoft-ServerCore-ShellLauncher/Admin Last Record 0	🚷 Re:	set		
SingleRule	Microsoft-System-Diagnostics-DiagnosticI Processing Mode Eventlog Subscription (R	ealtime)	\sim		
	Microsoft-User Experience Virtualization-A Eventpolling related Options				
Syslog Forwarding	Microsoft-User Experience Virtualization-A				
-,,	Microsoft-User Experience Virtualization-I				
	Microsoft-User Experience Virtualization-S File Path Name	Browse			
	Microsoft-Windows-AAD/Operational				
	Microsoft-Windows-AllJoyn/Operational Verbose				
	Microsoft-Windows-All-User-Install-Agent/	~			
	Microsoft-Windows-AppHost/Admin	~			
	Microsoft-Windows-AppID/Operational Warning Warning	~	1		
	Microsoft-Windows-ApplicabilityEngine/O	~			
	Microsoft-Windows-Application Server-Ap	~			
			-		
	RuleSet to use ForwardSyslog	~	Refresh	~	
Status Trial period, days left 30	N3	Connected	To: loca	lhost	

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

Démarrer le service

Cliquer sur start pour démarrer le service. Après la configuration et le démarrage du service vous pouvez fermer le programme.

🚏 RSyslog Windows Agent Configuration Client			Х
File Tools Help			
Save Reset Changes Quit Verify Configuration Connect Localhost Start Stop Restart Up Down DebugLog			
Service Events General Conse			
status i inal period, days left 30	Connected	io: local	nost 🔡

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

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



Last update: 2023/03/09 14:50