

ERA - Anomalie #3900

Le port 20514 n'est pas ouvert automatiquement si on autorise la réception de logs de machines distantes

17/08/2012 12:20 - Benjamin Bohard

Statut:	Fermé	Début:	17/08/2012
Priorité:	Normal	Echéance:	
Assigné à:	Benjamin Bohard	% réalisé:	100%
Catégorie:		Temps estimé:	0.00 heure
Version cible:	Mises à jour 2.3.6 RC	Temps passé:	0.67 heure
Distribution:	EOLE 2.3		
Description			
il faudrait ajouter des règles templatisées :			
- dans un fichier 00_root_rsyslog.fw			
- dans les modèles era pour amon/amonecole			
Cette demande traite le volet era.			
Demandes liées:			
Lié à eole-common - Anomalie #3621: Le port 20514 n'est pas ouvert automatiqu...		Fermé	12/06/2012
Lié à conf-amon - Anomalie #3904: Ajout de tags pour prendre en charge les di...		Fermé	20/08/2012

Révisions associées

Révision 5995cbcc - 17/08/2012 17:16 - Benjamin Bohard

Correction des règles.

- templates/subtmpl/rsyslog.xml : suppression des règles descendantes.

Fixes #3900

Révision 965a5bef - 20/08/2012 10:04 - Benjamin Bohard

Utilisation du mécanisme de directives optionnelles cachées.

- templates/subtmpl/rsyslog.xml : suppression des conditions au profit de tags et du changement de valeur d'attribut (de 0 à 17).

Fixes #3900

Historique

#1 - 17/08/2012 12:22 - Benjamin Bohard

Commits [1a9878422e7d78507abdf130ceadaae4079626cf](#) et [47f5a539e0538ca302680614b3dd6697286d6b1b](#)

#2 - 17/08/2012 13:48 - Joël Cuissinat

- Assigné à mis à Benjamin Bohard

- Version cible mis à Mises à jour 2.3.6 RC

#3 - 18/08/2012 12:14 - Benjamin Bohard

- Statut changé de Nouveau à Résolu

- % réalisé changé de 0 à 100

Appliqué par commit [5995cbccdba5ede2ea56595acd84788070f234a4](#).

#4 - 19/08/2012 16:20 - Emmanuel GARETTE

- Statut changé de Résolu à À valider

Il ne faut pas faire comme ça, mais utiliser les directives cachés (si tu écoutes gwen maintenant ...).

#5 - 20/08/2012 11:50 - Benjamin Bohard

- Statut changé de À valider à Résolu

Appliqué par commit [965a5bef67861440e55026c14270e09d0c1d5659](#).

#6 - 28/08/2012 14:12 - Joël Cuissinat

- Statut changé de Résolu à Fermé

Test sur AmonEcole (avec Era + modèle *2zones-amonecole-nginx*) :

```
root@amonecole:~# echo -e "UDP : \$adresses_ip_clients_logs_udp\nTCP: \$adresses_ip_clients_logs_tcp\nRELP: \$adresses_ip_clients_logs_relp"
UDP : 1.1.1.4
TCP: 1.1.1.3
RELP: 1.1.1.2
root@amonecole:~# iptables-save | grep "1.1.1"
:PREROUTING ACCEPT [695:111012]
-A ext-bas -s 1.1.1.2/32 -d 192.168.230.201/32 -i eth0 -p tcp -m state --state NEW -m tcp --dport 20514 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A ext-bas -s 1.1.1.3/32 -d 192.168.230.201/32 -i eth0 -p tcp -m state --state NEW -m tcp --dport 10514 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A ext-bas -s 1.1.1.4/32 -d 192.168.230.201/32 -i eth0 -p udp -m state --state NEW -m udp --dport 514 -j ACCEPT
T
```