

eoie-common - Anomalie #3359

les logs iptables sont dans kernel, le logrotate pour iptables.*.log est en échec

04/20/2012 10:09 AM - Benjamin Bohard

Status:	Fermé	Start date:	04/20/2012
Priority:	Normal	Due date:	
Assigned To:	Benjamin Bohard	% Done:	100%
Category:		Estimated time:	0.00 hour
Target version:	Mises à jour 2.3.5 RC	Spent time:	0.00 hour
Distribution:	EOLE 2.3		

Description

Il y a une incohérence entre la répartition des logs (pas de filtre spécifique pour iptables) et les règles de rotation.

La solution proposée est l'ajout de la règle manquante pour rsyslog.

Associated revisions

Revision 0d003f5e - 04/20/2012 10:17 AM - Benjamin Bohard

absence de règle pour filtrer iptables (fixes #3359)

- `tmpl/80-iptables.conf` : règle filtrant les messages concernant iptables et supprimant les messages de la chaîne après.
- `dicos/01_log.xml` : ajout de la directive `file` pour la nouvelle règle.

Revision 6d6d1708 - 04/20/2012 11:11 AM - Benjamin Bohard

le filtre n'est pas adapté (fixes #3359)

- `tmpl/80-iptables.conf` : révision du filtre pour différencier les sources de messages locales et externes.

History

#1 - 04/20/2012 10:22 AM - Benjamin Bohard

- Status changed from *Nouveau* to *Résolu*

- % Done changed from 0 to 100

Appliqué par commit [0d003f5e82c6636c6f38dad237b3df9e8254c2d5](#).

#2 - 04/20/2012 10:27 AM - Benjamin Bohard

- Status changed from *Résolu* to *Nouveau*

le commit précédent ne prend pas en charge la différence entre `loacl` et `distant`

#3 - 04/20/2012 11:24 AM - Benjamin Bohard

- Status changed from *Nouveau* to *Résolu*

Appliqué par commit [6d6d17087a8c2b5426ff9af7b32812cde878d8c7](#).

#4 - 04/20/2012 04:18 PM - Joël Cuissinat

- *Assigned To set to Benjamin Bohard*

- *Target version set to Mises à jour 2.3.5 RC*

#5 - 06/12/2012 04:55 PM - Bruno Boiget

- *Status changed from Résolu to Fermé*

templates ok, testé en local et distant entre un amonecole et seshat.

pour la réception des logs d'une machine distante il manque l'ouverture du port 20514 depuis les ips autorisées (cf demande liée).