eole-common - Scénario #9965

Création redondante de ligne d'autorisation d'IP dans host.allow et IP indûment présentes

05/12/2014 17:11 - Thierry Jambou

Statut:	Terminé (Sprint)	**Début:**	05/12/2014
Priorité:	Normal	**Echéance:**	22/01/2015
Assigné à:		**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	sprint 2015 2-4	**Temps passé:**	7.50 heures

Description

Lors de l'utilisation de tcpwrapper sur les services d'un essl dans era, plusieurs lignes d'autorisation pour une même IP sur un même service sont créées dans le host.allow

Copie d'un host.allow pour les services sshd et gen_config :

```
root@ssl24-pne-02:~# cat /etc/eole/hosts.allow
##### begin: this file is generated by Era - do not edit #####
gen_config:192.168.250.0/255.255.255.224
sshd:192.168.250.0/255.255.255.224
gen_config:172.26.46.240/255.255.255.240Extrait
gen_config:172.20.41.38
gen_config:172.20.45.38
gen_config:172.20.46.38
gen_config:172.20.41.192
gen_config:172.20.41.157
gen_config:172.20.42.157
gen_config:172.20.43.157
gen_config:172.20.44.157
gen_config:172.20.41.1
gen_config:172.20.42.1
gen_config:172.20.43.1
gen_config:172.20.44.1
gen_config:172.20.41.69
gen_config:172.20.42.69
gen_config:172.20.43.69
gen_config:172.20.44.69
sshd:172.26.46.240/255.255.255.240Extrait
sshd:172.20.41.38
sshd:172.20.45.38
sshd:172.20.46.38
sshd:172.20.41.192
sshd:172.20.41.157
sshd:172.20.42.157
sshd:172.20.43.157
sshd:172.20.44.157
sshd:172.20.41.1
sshd:172.20.42.1
sshd:172.20.43.1
sshd:172.20.44.1
sshd:172.20.41.69
sshd:172.20.42.69
sshd:172.20.43.69
sshd:172.20.44.69
sshd:172.26.32.0/255.255.240.0
gen_config:172.26.32.0/255.255.240.0
gen_config:192.168.250.0/255.255.255.224
gen_config:172.26.46.240/255.255.255.240
gen_config:172.20.41.38
gen_config:172.20.45.38
gen_config:172.20.46.38
gen_config:172.20.41.192
gen_config:172.20.41.157
```

```
gen_config:172.20.42.157
gen_config:172.20.43.157
gen_config:172.20.44.157
gen_config:172.20.41.1
gen_config:172.20.42.1
gen_config:172.20.43.1
gen_config:172.20.44.1
gen_config:172.20.41.69
gen_config:172.20.42.69
gen_config:172.20.43.69
gen_config:172.20.44.69
gen_config:172.28.10.19
gen_config:172.28.10.25
gen_config:172.28.10.66
sshd:192.168.250.0/255.255.255.224
sshd:172.26.46.240/255.255.255.240
sshd:172.20.41.38
sshd:172.20.45.38
sshd:172.20.46.38
sshd:172.20.41.192
sshd:172.20.41.157
sshd:172.20.42.157
sshd:172.20.43.157
sshd:172.20.44.157
sshd:172.20.41.1
sshd:172.20.42.1
sshd:172.20.43.1
sshd:172.20.44.1
sshd:172.20.41.69
sshd:172.20.42.69
sshd:172.20.43.69
sshd:172.20.44.69
sshd:172.28.10.19
sshd:172.28.10.25
sshd:172.28.10.66
sshd:172.26.62.0/255.255.254.0
gen_config:172.26.62.0/255.255.254.0
```

Il semble qu'on rajoute des lignes pour chaque directive qui utilise le service pour une même extrémité

Plus délicat, on trouve des IPs qui n'ont rien à faire dans le host.allow semble t'il ... je m'explique :

- nous avons une directive qui autorise notre réseau (le PNESR) à accéder au bastion en ssh, donc on apparaît
- nous avons une autre directive qui autorise le même réseau à accéder au LAN du service, on réapparaît à nouveau, jusqu'ici cette redondance n'est pas gênante ...
- par-contre, il y a une directive qui autorise un autre réseau (le PNE environnement de travail) à accéder en ssh au Lan et seulement au Lan, le réseau apparaît aussi dans le host.allow et là c'est plus embêtant car ça veut dire que ce réseau peut au moins essayer de rentrer sur le bastion en ssh ... Il ne peut pas à cause (ou plutôt grâce) aux règles Iptables mais quand même ;-)

Merci d'avance

Sous-tâches:

Tâche # 10191: Prendre contact avec Thierry Jambou, pour plus de précisions sur leur mo...	**Fermé**

Révisions associées

Révision c59955fd - 09/01/2015 11:19 - Gwenael Remond

Era pollue le hosts.allow en cas de directive qui n'est pas de type input

fixes #9965 @7h

Historique

#1 - 08/12/2014 14:02 - Joël Cuissinat

- Temps estimé mis à 3.00 h

- Tâche parente mis à #9969

- Restant à faire (heures) mis à 3.0

#2 - 05/01/2015 11:13 - Joël Cuissinat

- Description mis à jour

#3 - 05/01/2015 11:21 - Joël Cuissinat

- Tâche parente #9969 supprimé

#4 - 05/01/2015 11:23 - Joël Cuissinat

- Version cible sprint 2014 50-51 Eq 1 supprimé

#5 - 05/01/2015 11:50 - Luc Bourdot

- Tracker changé de Tâche à Scénario

- Echéance mis à 22/01/2015

- Version cible mis à sprint 2015 2-4

#6 - 05/01/2015 16:39 - Klaas TJEBBES

- Points de scénarios mis à 3.0

#7 - 09/01/2015 11:21 - Gwenael Remond

- Statut changé de Nouveau à Résolu

- % réalisé changé de 0 à 100

Appliqué par commit era:c59955fd35327b0cb35bf43b631a14520acc6651.

#8 - 09/01/2015 11:23 - Gwenael Remond

- Assigné à mis à Gwenael Remond

#9 - 09/01/2015 11:33 - Joël Cuissinat

- Statut changé de Résolu à Terminé (Sprint)

- Assigné à Gwenael Remond supprimé

#10 - 09/01/2015 11:33 - Joël Cuissinat

- Statut changé de Terminé (Sprint) à En cours

#11 - 12/01/2015 10:11 - Joël Cuissinat

- Statut changé de En cours à Terminé (Sprint)