

eoie-cntlm - Tâche #13533

Scénario # 13622 (Terminé (Sprint)): Faire fonctionner Cntlm en mode une carte

netmask et network non conforme dans dicos 61_cntlm.xml

12/10/2015 11:46 - Gaetan Mottier

Statut:	Fermé	Début:	12/10/2015
Priorité:	Normal	Echéance:	
Assigné à:	Joël Cuissinat	% réalisé:	100%
Version cible:	sprint 2017 1-3 Equipe MENSUR	Temps estimé:	2.00 heures
		Temps passé:	2.00 heures
Description			
<p>Le dictionnaire de cntlm ne possède pas les bonnes valeurs pour les règles iptables</p> <p>les lignes des interfaces inverses network et netmask : <ip interface='eth1' netmask='adresse_network_eth1' netmask_type='SymLinkOption' ip_type='SymLinkOption'>adresse_netmask_eth1</ip></p> <p>Celles des vlans ne possèdent que netmask comme valeurs : <ip interface='eth1' netmask='vlan_netmask_eth1' netmask_type='SymLinkOption' ip_type='SymLinkOption'>vlan_netmask_eth1</ip></p> <p>ce qui donne dans iptables ceci: ACCEPT tcp -- 10.14.222.0/10.14.222.0 anywhere tcp dpt:3127 flags:FIN,SYN,RST,ACK,SYN</p> <p>Je joins le dictionnaire tel que nous l'utilisons et auquel nous rajoutons aussi l'accès au "Réseaux supplémentaire autorisés a se connecter depuis cette interface", ce qui je pense est un manque dans le dictionnaire actuel.</p> <p>Ceci est valable en 2.4 et aussi sur la rc de la 2.5</p>			

Révisions associées

Révision 831e1de5 - 10/01/2017 11:52 - Joël Cuissinat

Correction des règles de pare-feu pour Cntlm

Ref: #13533 @2h

Historique

#1 - 12/10/2015 11:59 - Gaetan Mottier

Précision : lorsque je parle de la rc 2.5, je parle de la rc 2.5.1

Et le dictionnaire joint est celui repris de mes tests en 2.5.1, les modifications apportés sont les mêmes que sur 2.4.2, il s'agit des balises <service_restriction>

#2 - 12/10/2015 17:25 - Joël Cuissinat

- Tracker changé de Anomalie à Tâche
- Temps estimé mis à 3.00 h
- Tâche parente mis à #13526
- Restant à faire (heures) mis à 3.0
- Distribution changé de EOIE 2.4 à EOIE 2.5

Je confirme le bug sur ce dico.

Par contre, merci de créer un signalement dédié pour la demande d'évolution sur les réseaux supplémentaires.

NB : si celle-ci est implémenté nativement, nous devons faire évoluer les modèles ERA en conséquence.

#3 - 12/10/2015 17:28 - Joël Cuissinat

- *Tâche parente #13526 supprimé*

Après réflexion, cette demande n'est pas prioritaire car Amon n'utilise pas cette fonctionnalité (ERA power) et que le module "Eolebase + proxy" n'est pas stabilisé par ailleurs.

#4 - 12/10/2015 17:29 - Joël Cuissinat

- *Version cible Sprint 2015 42-44 - Équipe MENESR supprimé*

#5 - 12/10/2015 17:32 - Joël Cuissinat

- *Tracker changé de Tâche à Anomalie*

#6 - 16/10/2015 15:36 - Joël Cuissinat

- *Tracker changé de Anomalie à Tâche*

- *Temps estimé changé de 3.00 h à 2.00 h*

- *Tâche parente mis à #13622*

- *Restant à faire (heures) changé de 3.0 à 2.0*

#7 - 10/01/2017 11:17 - Joël Cuissinat

- *Statut changé de Nouveau à En cours*

#8 - 10/01/2017 11:52 - Joël Cuissinat

- *Assigné à mis à Joël Cuissinat*

#9 - 10/01/2017 11:57 - Joël Cuissinat

- *% réalisé changé de 0 à 100*

- *Restant à faire (heures) changé de 2.0 à 0.25*

Sur aca.eolebase + eole-proxy, la commande suivante **iptables-save | grep 3127** doit retourner :

- pour l'interface 0

```
-A eth0-root -s 192.168.0.0/24 -p tcp -m tcp --dport 3127 --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
```

- pour un VLAN déclaré dans l'interface de configuration du module

```
-A eth0-root -s <network_vlan>/24 -p tcp -m tcp --dport 3127 --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
```

#10 - 11/01/2017 09:38 - Scrum Master

- Statut changé de *En cours* à *Résolu*

#11 - 13/01/2017 15:59 - Philippe Caseiro

- Statut changé de *Résolu* à *Fermé*

- Restant à faire (heures) changé de 0.25 à 0.0

Fichiers

61_cntlm.xml

7,71 ko

12/10/2015

Gaetan Mottier