

Amon - Demande #19851

problème de génération des règles via era : template active_tags

23/03/2017 13:52 - CAMILLE JACTARD

Statut:	Classée sans suite	Début:	23/03/2017
Priorité:	Normal	Echéance:	
Assigné à:	Joël Cuissinat	% réalisé:	0%
Catégorie:		Temps estimé:	0.00 heure
Version cible:		Temps passé:	0.50 heure
Description Bonjour, Sur nos Amon 2.5 nous avons constaté un soucis dans un template (/usr/share/eole/creole/distrib/active_tags) qui ne prend pas en compte la valeur "distant" pour la variable activer_sso Ce qui empêche la bonne génération de règles iptables lors de ce type de configuration (tous nos établissement en ce qui nous concerne) Pour le moment nous allons contourner le problème, mais un futur correctif serait le bienvenu. Cordialement, Camille			

Historique

#1 - 29/03/2017 14:45 - Joël Cuissinat

- Statut changé de Nouveau à En attente d'informations
- Assigné à mis à Joël Cuissinat

Bonjour, peux-tu préciser la nature exacte des problèmes et l'infrastructure cible ?

Sur nos maquettes établissement, l'Amon est configuré avec activer_sso="distant" qui pointe sur le Scribe en DMZ avec le modèle "4zones" fourni par défaut et nous ne constatons pas de dysfonctionnement.

#2 - 31/03/2017 12:52 - CAMILLE JACTARD

Bonjour,

Donc pour compléter :

dans le script /usr/share/eole/creole/distrib/active_tags on a

```
%if %%getVar('activer_sso', 'non') == 'local'
eole_sso
%end if
```

Donc si je ne me trompe pas le cas activer_sso == distant ne donne pas le retour eole_sso dans le fichier d'active_tags.

Or dans le modele 4zones.xml (qui est le modèle père de tous nos modèles actuels) la directive eole_sso est une directive optionnelle cachée qui doit donc être présente dans le fichier active_tags pour être activée.

#3 - 31/03/2017 12:54 - CAMILLE JACTARD

Du coup pour le moment j'ai un patch qui modifie le template en remplaçant `%if %%getVar('activer_sso', 'non') == 'local' par %if %getVar('activer_sso', 'non') != 'non'` et cela semble plutôt bien fonctionner

#4 - 03/04/2017 14:36 - Joël Cuissinat

J'avais bien compris le problème "technique".

Le tag "eole_sso" est initialement prévu pour ouvrir les accès vers le service EoleSSO de l'Amon depuis toutes les interfaces et à ma connaissance fait ce travail correctement.

Le seul reproche qu'on pourrait lui faire c'est qu'il aurait du s'appeler "eole_sso_local".

À partir de ce constat, je suppose que dans ton infrastructure, c'est plutôt un nouveau tag (eole_sso_distant) qu'il faudrait ajouter ?

Quelles sont les règles que vous ajoutez dans ce cadre ?

#5 - 03/04/2017 15:20 - CAMILLE JACTARD

Dans le cadre de notre ENT on a des règles sur ERA entre notre DMZ et Amon sur le port eole_sso 8443 (pour Pronote)

Et sans le tag eole_sso aucune trace de 8443 sur la chaine dmz-bas dans le lance.firewall

#6 - 27/02/2018 15:35 - Gilles Grandgérard

Bonjour,

Est ce que ton patch est suffisant pour corriger le problème ? Si oui, pouvons nous fermer cette demande ?

#7 - 19/02/2019 15:52 - Gilles Grandgérard

- Statut changé de *En attente d'informations* à *Classée sans suite*