

Distribution EOLE - Tâche #36118

Scénario # 35840 (Terminé (Sprint)): EOLE 2.10 : Mettre à niveau vers ntpsec et vérifier ntp_signd

Les clients de scribe n'utilisent pas l'heure de l'AD

29/07/2024 09:41 - Laurent Gourvenec

Statut:	Reporté	Début:	01/10/2022
Priorité:	Normal	Echéance:	
Assigné à:		% réalisé:	50%
Version cible:	Livraison Cadoles - MEN 30/06/2024 (60+18)	Temps estimé:	0.00 heure
		Temps passé:	0.00 heure
Description			
Vérifier le comportement en 2.9 et corriger si possible.			
Demandes liées:			
Lié à Distribution EOLE - Scénario #36163: Les clients de scribe n'utilisent ...		Terminé (Sprint)	01/10/2022 01/01/2026

Révisions associées

Révision 904f0c70 - 29/07/2024 15:56 - Benjamin Bohard

Pallier le problème entre apparmor et systemd en conteneur.

Ref #36112
Ref #36118

Révision afce5a8d - 28/08/2024 16:29 - Laurent Gourvenec

Bouger ntp.conf dans /etc/ntpsec/ sur scribe

ref #36118

Révision 70a9dabc - 29/08/2024 10:29 - Laurent Gourvenec

Re-Fix config sur scribe pour utiliser ntp_signd

ref #36118

Révision 71844169 - 12/12/2024 16:34 - Laurent Gourvenec

Fix config sur scribe pour utiliser ntp_signd

Ref #36341
Ref #36118

Historique

#1 - 29/07/2024 10:23 - Benjamin Bohard

Sur l'infrastructure de test etb1 en 2.9.0, un client windows ne semble pas récupérer l'heure du contrôleur de domaine non plus (serveur temporel : local CMOS clock)

#2 - 30/07/2024 09:59 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#3 - 29/08/2024 17:02 - Laurent Gourvenec

Il y a un dernier problème, un problème de routage. Dans le conteneur addc du scribe (contrairement à l'AmonEcole), la route par défaut est celle qui passe par l'IP publique de l'AD. Les requêtes NTP partent donc avec l'IP de l'adresse publique de l'AD. Aucune règle de routage coté scribe ou amon ne vient faire de NAT ensuite. Résultat : on sort sur internet avec une ip qui est interne et donc on ne reçoit jamais de réponse. Alors qu'en sortant avec l'ip du scribe, pas de soucis, l'Amon est configuré pour laisser sortir le scribe (et faire du NAT au passage).

```
CreoleSet ad_local_default_bridge_via_internal_ip oui  
reconfigure
```

résout bien le problème (les clients prennent l'heure de l'AD).

Une autre solution, peut-être, serait de faire du SNAT sur ce qui sort sur l'iface du scribe avec l'IP de l'AD et le port 123 en destination. Mais un essai avec

```
iptables -t nat -A POSTROUTING --out enp2s0 -s 10.1.3.11/32 -p udp --dport 123 -j SNAT --to-source 10.1.3.5
```

n'a pas fonctionné, sur l'amon les paquets arrivent encore avec l'ip de l'AD. Peut-être parce que l'interface eth0 du conteneur est un bridge sur enp2s0.

En revanche, sur l'Amon, faire du SNAT avec toutes les requêtes sortantes sur le port 123, ça fonctionne.

```
iptables -A POSTROUTING -t nat --out enp2s0 -p udp --dport 123 -j SNAT --to-source 192.168.0.31
```

Doit-on ajouter une règle similaire dans tous les Amon ?

#4 - 10/09/2024 14:37 - Joël Cuissinat

- Statut changé de En cours à Reporté

- % réalisé changé de 0 à 50

=> scénario dédié [#36163](#)

#5 - 10/09/2024 14:38 - Joël Cuissinat

- Lié à Scénario #36163: Les clients de scribe n'utilisent pas l'heure de l'AD ajouté