

Distribution EOLE - Scénario #36163

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

10/09/2024 14:35 - Joël Cuissinat

Statut:	Terminé (Sprint)	Début:	01/10/2022
Priorité:	Normal	Echéance:	01/01/2026
Assigné à:	Benjamin Bohard	% réalisé:	100%
Catégorie:		Temps estimé:	0.00 heure
Version cible:	Livraison Cadoles - MEN 31/12/2024 (100)	Temps passé:	0.00 heure
Description			
Suite de la tâche #36118 :			
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).			
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).			
<pre>CreoleSet ad_local_default_bridge_via_internal_ip oui reconfigure</pre>			
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			
<pre>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</pre>			
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.			
<pre>iptables -A POSTROUTING -t nat --out enp2s0 -p udp --dport 123 -j SNAT --to-source 192.168.0.31</pre>			
Doit-on ajouter une règle similaire dans tous les Amon ?			
À faire			
- vérifier ce qu'il en est en 2.9.0 - ajouter la règle iptables dans le conteneur de façon en s'assurant qu'elle ne saute pas (<i>cas ad_local_default_bridge_via_internal_ip=non uniquement</i>) - faire le point sur les éventuels tests existants (jenkins/squash) et les adapter/en ajouter si nécessaire			
Sous-tâches:			
Tâche # 36243: Étude (complémentaire)			Fermé
Tâche # 36245: Installer iptables dans le conteneur			Fermé
Tâche # 36246: S'assurer que les paquets NTP prennent la bonne route.			Fermé
Tâche # 36254: Tester			Fermé

Tâche # 36334: Corriger le test Squash	Fermé
Tâche # 36340: Backporter le drop de CAP_SYS_TIME en 2.9 sur scribe	Fermé
Tâche # 36341: Configurer l'utilisation de ntpsigned en 2.9	Fermé
Tâche # 36357: Les règles ne sont pas (ré)appliquées au (re)démarrage du serveur	Fermé
Tâche # 36374: Supprimer la dépendance au service ssh	Fermé
Tâche # 36384: Messages d'erreur à vérifier/masquer lors de la mise à jour du paquet sc...	Fermé
Tâche # 36407: Le service addc-wait-running attend indéfiniment avant la création du co...	Fermé
Tâche # 36418: Modification non compatible avec le mode AD distant	Fermé
Tâche # 36448: Compléter un test squash pour Seth également	Fermé
Demandes liées:	
Lié à Distribution EOLE - Tâche #36118: Les clients de scribe n'utilisent pas...	Reporté 01/10/2022

Révisions associées

Révision 0e30143d - 07/01/2025 12:57 - Joël Cuissinat

Vérification des règles iptables dans le conteneur addc

Ref: #36163

Révision 0d92dea7 - 20/01/2025 16:49 - Joël Cuissinat

Vérifications des règles iptables sur EOLE $\geq$ 2.9.0 uniquement

Ref: #36163

Historique

#1 - 10/09/2024 14:38 - Joël Cuissinat

- Lié à Tâche #36118: Les clients de scribe n'utilisent pas l'heure de l'AD ajouté

#2 - 27/09/2024 16:39 - Joël Cuissinat

- Release changé de EOLE 2.9.0 à Carnet de produit Cadoles - MEN

#3 - 31/10/2024 08:28 - Benjamin Bohard

- Echéance mis à 01/01/2026

- Assigné à mis à Benjamin Bohard

- Version cible mis à Carnet Cadoles - MEN

- Début mis à 01/10/2022

#4 - 10/12/2024 12:21 - Joël Cuissinat

- Points de scénarios changé de 3.0 à 4.0

+1 pour correction test squash et portage en 2.9

#5 - 19/12/2024 11:13 - Joël Cuissinat

- Points de scénarios changé de 4.0 à 5.0

+1 pour règles au démarrage du serveur / conteneur

#6 - 07/01/2025 10:28 - Joël Cuissinat

- Points de scénarios changé de 5.0 à 6.0

#7 - 30/01/2025 12:31 - Joël Cuissinat

+1 pour vérifier le démarrage dans les tests Jenkins

#8 - 30/01/2025 12:31 - Joël Cuissinat

- *Points de scénarios changé de 6.0 à 7.0*

#9 - 18/02/2025 10:49 - Joël Cuissinat

- *Points de scénarios changé de 7.0 à 8.0*

+1 pour test squash

#10 - 05/05/2025 17:18 - Joël Cuissinat

- *Statut changé de Nouveau à Terminé (Sprint)*

- *Version cible changé de Carnet Cadoles - MEN à Livraison Cadoles - MEN 31/12/2024 (100)*

- *Release changé de Carnet de produit Cadoles - MEN à EOLE 2.9.0*