

Distribution EOLE - Tâche #36243

Scénario # 36163 (Terminé (Sprint)): Les clients de scribe n'utilisent pas l'heure de l'AD

Étude (complémentaire)

31/10/2024 10:04 - Benjamin Bohard

Statut:	Fermé	Début:	01/10/2022
Priorité:	Normal	Echéance:	
Assigné à:	Benjamin Bohard	% réalisé:	100%
Version cible:	Livraison Cadoles - MEN 31/12/2024 (100)	Temps estimé:	0.00 heure
		Temps passé:	0.00 heure
Description			

Historique

#1 - 31/10/2024 10:04 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#2 - 31/10/2024 10:16 - Benjamin Bohard

Cas actuel

Dans le cas nominal (pas de routage des paquets), on observe avec tcpdump, pour une requête sur le port 123 :

sur l'amon

```
10:12:36.145559 enp5s0 In IP (tos 0xb8, ttl 64, id 8331, offset 0, flags [DF], proto UDP (17), length 76)
  addc.dompedago.etbl.lan.ntp > ntp.altinea.fr.ntp: NTPv4, Client, length 48
    Leap indicator: clock unsynchronized (192), Stratum 0 (unspecified), poll 6 (64s), precision -23
    Root Delay: 0.000000, Root dispersion: 0.000000, Reference-ID: (unspec)
    Reference Timestamp: 0.000000000
    Originator Timestamp: 0.000000000
    Receive Timestamp: 0.000000000
    Transmit Timestamp: 3939354731.909824128 (2024-10-31T09:12:11Z)
      Originator - Receive Timestamp: 0.000000000
      Originator - Transmit Timestamp: 3939354731.909824128 (2024-10-31T09:12:11Z)
10:12:36.145644 enp2s0 Out IP (tos 0xb8, ttl 63, id 8331, offset 0, flags [DF], proto UDP (17), length 76)
  addc.dompedago.etbl.lan.ntp > ntp.altinea.fr.ntp: NTPv4, Client, length 48
    Leap indicator: clock unsynchronized (192), Stratum 0 (unspecified), poll 6 (64s), precision -23
    Root Delay: 0.000000, Root dispersion: 0.000000, Reference-ID: (unspec)
    Reference Timestamp: 0.000000000
    Originator Timestamp: 0.000000000
    Receive Timestamp: 0.000000000
    Transmit Timestamp: 3939354731.909824128 (2024-10-31T09:12:11Z)
      Originator - Receive Timestamp: 0.000000000
      Originator - Transmit Timestamp: 3939354731.909824128 (2024-10-31T09:12:11Z)
```

sur le Scribe (hôte)

```
10:12:11.909876 enp2s0 Out IP (tos 0xb8, ttl 64, id 8331, offset 0, flags [DF], proto UDP (17), length 76)
  addc.dompedago.etbl.lan.ntp > ntp.altinea.fr.ntp: NTPv4, Client, length 48
    Leap indicator: clock unsynchronized (192), Stratum 0 (unspecified), poll 6 (64s), precision -23
    Root Delay: 0.000000, Root dispersion: 0.000000, Reference-ID: (unspec)
    Reference Timestamp: 0.000000000
    Originator Timestamp: 0.000000000
    Receive Timestamp: 0.000000000
    Transmit Timestamp: 3939354731.909824128 (2024-10-31T09:12:11Z)
      Originator - Receive Timestamp: 0.000000000
      Originator - Transmit Timestamp: 3939354731.909824128 (2024-10-31T09:12:11Z)
```

sur le Scribe (conteneur addc)

```
10:12:11.909861 eth0 Out IP (tos 0xb8, ttl 64, id 8331, offset 0, flags [DF], proto UDP (17), length 76)
  addc.dompedago.etbl.lan.ntp > ntp.altinea.fr.ntp: NTPv4, Client, length 48
  Leap indicator: clock unsynchronized (192), Stratum 0 (unspecified), poll 6 (64s), precision -23
  Root Delay: 0.000000, Root dispersion: 0.000000, Reference-ID: (unspec)
  Reference Timestamp: 0.000000000
  Originator Timestamp: 0.000000000
  Receive Timestamp: 0.000000000
  Transmit Timestamp: 3939354731.909824128 (2024-10-31T09:12:11Z)
  Originator - Receive Timestamp: 0.000000000
  Originator - Transmit Timestamp: 3939354731.909824128 (2024-10-31T09:12:11Z)
```

La réponse du serveur NTP ne revient même pas sur l'Amon.

SNAT dans le conteneur

Après installation du paquet iptables et ajout de la règle suivante :

```
iptables -t nat -A POSTROUTING --out eth0 -s 10.1.3.11/32 -p udp --dport 123 -j SNAT --to-source 10.1.3.5
```

Sur l'Amon

```
10:14:48.155857 enp5s0 In IP (tos 0xb8, ttl 64, id 64160, offset 0, flags [DF], proto UDP (17), length 76)
  scribe.etbl.lan.ntp > mwc339.ftth.cust.milkywan.net.ntp: NTPv4, Client, length 48
  Leap indicator: clock unsynchronized (192), Stratum 0 (unspecified), poll 6 (64s), precision -23
  Root Delay: 0.000000, Root dispersion: 0.000000, Reference-ID: (unspec)
  Reference Timestamp: 0.000000000
  Originator Timestamp: 0.000000000
  Receive Timestamp: 0.000000000
  Transmit Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
  Originator - Receive Timestamp: 0.000000000
  Originator - Transmit Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
10:14:48.155912 enp2s0 Out IP (tos 0xb8, ttl 63, id 64160, offset 0, flags [DF], proto UDP (17), length 76)
  amon.etbl.lan.ntp > mwc339.ftth.cust.milkywan.net.ntp: NTPv4, Client, length 48
  Leap indicator: clock unsynchronized (192), Stratum 0 (unspecified), poll 6 (64s), precision -23
  Root Delay: 0.000000, Root dispersion: 0.000000, Reference-ID: (unspec)
  Reference Timestamp: 0.000000000
  Originator Timestamp: 0.000000000
  Receive Timestamp: 0.000000000
  Transmit Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
  Originator - Receive Timestamp: 0.000000000
  Originator - Transmit Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
10:14:48.173175 enp2s0 In IP (tos 0x0, ttl 54, id 65380, offset 0, flags [DF], proto UDP (17), length 76)
  mwc339.ftth.cust.milkywan.net.ntp > amon.etbl.lan.ntp: NTPv4, Server, length 48
  Leap indicator: (0), Stratum 2 (secondary reference), poll 6 (64s), precision -25
  Root Delay: 0.001419, Root dispersion: 0.000701, Reference-ID: 0xe6e245b4
  Reference Timestamp: 3939354245.154001751 (2024-10-31T09:04:05Z)
  Originator Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
  Receive Timestamp: 3939354888.168305291 (2024-10-31T09:14:48Z)
  Transmit Timestamp: 3939354888.168326480 (2024-10-31T09:14:48Z)
  Originator - Receive Timestamp: +24.253345801
  Originator - Transmit Timestamp: +24.253366991
10:14:48.173188 enp5s0 Out IP (tos 0x0, ttl 53, id 65380, offset 0, flags [DF], proto UDP (17), length 76)
  mwc339.ftth.cust.milkywan.net.ntp > scribe.etbl.lan.ntp: NTPv4, Server, length 48
  Leap indicator: (0), Stratum 2 (secondary reference), poll 6 (64s), precision -25
  Root Delay: 0.001419, Root dispersion: 0.000701, Reference-ID: 0xe6e245b4
  Reference Timestamp: 3939354245.154001751 (2024-10-31T09:04:05Z)
  Originator Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
  Receive Timestamp: 3939354888.168305291 (2024-10-31T09:14:48Z)
  Transmit Timestamp: 3939354888.168326480 (2024-10-31T09:14:48Z)
  Originator - Receive Timestamp: +24.253345801
  Originator - Transmit Timestamp: +24.253366991
```

Sur le Scribe (hôte)

```
10:14:23.914985 enp2s0 Out IP (tos 0xb8, ttl 64, id 64160, offset 0, flags [DF], proto UDP (17), length 76)
  scribe.dompedago.etbl.lan.ntp > mwc339.ftth.cust.milkywan.net.ntp: NTPv4, Client, length 48
    Leap indicator: clock unsynchronized (192), Stratum 0 (unspecified), poll 6 (64s), precision -23
    Root Delay: 0.000000, Root dispersion: 0.000000, Reference-ID: (unspec)
    Reference Timestamp: 0.000000000
    Originator Timestamp: 0.000000000
    Receive Timestamp: 0.000000000
    Transmit Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
      Originator - Receive Timestamp: 0.000000000
      Originator - Transmit Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
10:14:23.932572 enp2s0 In IP (tos 0x0, ttl 53, id 65380, offset 0, flags [DF], proto UDP (17), length 76)
  mwc339.ftth.cust.milkywan.net.ntp > scribe.dompedago.etbl.lan.ntp: NTPv4, Server, length 48
    Leap indicator: (0), Stratum 2 (secondary reference), poll 6 (64s), precision -25
    Root Delay: 0.001419, Root dispersion: 0.000701, Reference-ID: 0xe6e245b4
    Reference Timestamp: 3939354245.154001751 (2024-10-31T09:04:05Z)
    Originator Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
    Receive Timestamp: 3939354888.168305291 (2024-10-31T09:14:48Z)
    Transmit Timestamp: 3939354888.168326480 (2024-10-31T09:14:48Z)
      Originator - Receive Timestamp: +24.253345801
      Originator - Transmit Timestamp: +24.253366991
```

Sur le Scribe (conteneur addc)

```
10:14:23.914982 eth0 Out IP (tos 0xb8, ttl 64, id 64160, offset 0, flags [DF], proto UDP (17), length 76)
  10.1.3.5.ntp > mwc339.ftth.cust.milkywan.net.ntp: NTPv4, Client, length 48
    Leap indicator: clock unsynchronized (192), Stratum 0 (unspecified), poll 6 (64s), precision -23
    Root Delay: 0.000000, Root dispersion: 0.000000, Reference-ID: (unspec)
    Reference Timestamp: 0.000000000
    Originator Timestamp: 0.000000000
    Receive Timestamp: 0.000000000
    Transmit Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
      Originator - Receive Timestamp: 0.000000000
      Originator - Transmit Timestamp: 3939354863.914959489 (2024-10-31T09:14:23Z)
```

La réponse du serveur NTP revient bien au Scribe, le paquet d'origine étant bien associé à l'IP 10.1.3.5.
Par contre, elle ne parvient pas au conteneur addc.

#3 - 31/10/2024 11:13 - Benjamin Bohard

Mon hypothèse est que le paquet n'arrive pas sur la bonne interface sur le Scribe, pour que le paquet soit routé vers l'émetteur originel. D'après ce que je comprends du fonctionnement du réseau type macvlan utilisé pour le conteneur addc, c'est le comportement normal. L'interface réseau est divisée en deux sous-interfaces totalement indépendantes.

#4 - 31/10/2024 11:58 - Benjamin Bohard

SNAT dans le conteneur (mais avec d'autres règles)

Pour les deux règles suivantes (remplaçant celle précédemment testée), on retombe dans le cas 1 : pas de réponse reçue par l'Amon mais avec une différence dans l'IP source

```
iptables -t nat -A POSTROUTING --out eth0 -s 10.1.3.11/32 -p udp --dport 123 -j SNAT --to-source 192.0.2.2
```

La source est bien modifiée en 192.0.2.2

```
iptables -t nat -A POSTROUTING --out containers -s 10.1.3.11/32 -p udp --dport 123 -j SNAT --to-source 192.0.2.2
```

```
iptables -t nat -A POSTROUTING --out containers -p udp --dport 123 -j SNAT --to-source 192.0.2.2
```

La source n'est pas modifiée (et donc la route retour cherche 10.1.3.11, retour à la case départ).

Il semble que l'un des problèmes vient du fait que le client NTP envoie ses paquets sur l'interface eth0.

#5 - 31/10/2024 13:29 - Benjamin Bohard

L'idée serait donc de s'assurer que les paquets correspondants aux requêtes NTP s'orientent vers la bonne interface.

On peut les marquer et indiquer une route par défaut pour ces paquets marqués (via l'association à une table) :

```
iptables -t nat -A POSTROUTING --out containers -s 10.1.3.11/32 -p udp --dport 123 -j SNAT --to-source 192.0.2.2
```

```
iptables -t mangle -A OUTPUT -p udp --dport 123 -j MARK --set-mark <mark_number>
```

```
ip rule add fwmark <mark_number> table <table_number>
```

```
ip route add default via 192.0.2.1 table <table_number>
```

À voir si on ne peut pas obtenir un résultat semblable avec des règles iptables uniquement.

#6 - 04/11/2024 16:47 - Benjamin Bohard

- Statut changé de *En cours* à *À valider*

#7 - 16/12/2024 10:26 - Benjamin Bohard

- Statut changé de *À valider* à *Résolu*

#8 - 17/12/2024 15:51 - Joël Cuissinat

- Statut changé de *Résolu* à *Fermé*

- % réalisé changé de 0 à 100

- *Restant à faire (heures)* mis à 0.0