Infra Chapril - Demande #2436

Ipv6 sur l'infra

06/06/2017 16:09 - Quentin Gibeaux

Statut:	Fermé	**Début:**	06/06/2017
Priorité:	Normale	**Echéance:**	
Assigné à:	Quentin Gibeaux	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Mise en production Chapril		

Description

Il serait bon d'avoir de l'ipv6 sur l'infrastructure, cela faciliterait les choses (ne pas le désactiver là où il est activé par défaut).
La différence est qu'en ipv6 on fonctionne plus souvent sans réseau privé, mais qu'avec des adresses ip publiques… il faut donc déployer des pare-feux sur chaque machine !

Je pense qu'on peut configurer le réseau de maine/coon comme ceci (correspondance des terminaisons d'adresses ip) :

```
<network>
  <name>default</name>
  <uuid>cd3db10b-f4d7-4032-bb53-4cda1c7dc237</uuid>
  <forward mode='nat'/>
  <bridge name='virbr0' stp='on' delay='0'/>
  <mac address='52:54:00:54:b8:24'/>
  <ip address='192.168.1.4' netmask='255.255.255.0'>
    <dhcp>
      <range start='192.168.1.100' end='192.168.1.199'/>
      <host mac='52:54:00:02:e2:7a' name='dns' ip='192.168.1.53'/>
      <host mac='52:54:00:df:9f:7b' name='bastion' ip='192.168.1.93'/>
      <host mac='52:54:00:d6:6b:0a' name='mail' ip='192.168.1.57'/>
      <host mac='52:54:00:ad:15:d9' name='admin' ip='192.168.1.70'/>
      <host mac='52:54:00:61:f0:0f' name='pouet' ip='192.168.1.194'/>
    </dhcp>
  </ip>
  <ip family='ipv6' address='2a01:4f8:10b:c41::' prefix='64'>
    <dhcp>
      <range start='2a01:4f8:10b:c41:1:100' end='2a01:4f8:10b:c41:1:199'/>
      <host mac='52:54:00:02:e2:7a' name='dns' ip='2a01:4f8:10b:c41:1:53'/>
      <host mac='52:54:00:df:9f:7b' name='bastion' ip='2a01:4f8:10b:c41:1:93'/>
      <host mac='52:54:00:d6:6b:0a' name='mail' ip='2a01:4f8:10b:c41:1:57'/>
      <host mac='52:54:00:ad:15:d9' name='admin' ip='2a01:4f8:10b:c41:1:70'/>
      <host mac='52:54:00:61:f0:0f' name='pouet' ip='2a01:4f8:10b:c41:1:194'/>
    </dhcp>
  </ip>
</network>
```

Et derrière déployer des pare-feu iptables qui bloquent tout le traffic entrant sauf s'il vient de notre /64, ou si c'est un port autorisé (mail, ssh, http, https sur les vm idoines).

Demandes liées:

Duplique Infra Chapril - Demande #2402: IPV6 : finir la configuration du rout...	**Fermé**	**04/06/2017**

Historique

#1 - 06/06/2017 16:19 - Quentin Gibeaux

S'assurer que ça n'implique pas des communications externes à notre infrastructure entre deux vm internes : par exemple mastodon.cluster qui envoie un mail à mail.cluster, avec des paquets qui remontent en clair jusqu'au routeur Hetzner.

#2 - 06/06/2017 19:48 - Vincent-Xavier JUMEL

- Duplique Demande #2402: IPV6 : finir la configuration du routage IPv6 sur les machines virtuelles ajouté

#3 - 06/06/2017 19:49 - Vincent-Xavier JUMEL

- Statut changé de Nouveau à Fermé

#4 - 06/06/2017 20:06 - Quentin Gibeaux

- Statut changé de Fermé à En cours de traitement

#5 - 06/06/2017 20:45 - Quentin Gibeaux

j'ai créé le paquet firewall-chapril qui contient un script init chargé au démarrage : il charge les règles ip6tables (pour ipv6 donc) suivantes :

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [139:56229]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p ipv6-icmp -j ACCEPT
-A INPUT -s fe80::/10 -p udp -m udp --dport 546 -j ACCEPT
-A INPUT -s 2a01:4f8:10b:c41::/64 -j ACCEPT
-A INPUT -s 2a01:4f8:10b:c42::/64 -j ACCEPT
-A FORWARD -i lo -j ACCEPT
-A FORWARD -o lo -j ACCEPT
```

Et exécute pour compléter par configuration locale n'importe quel script contenant QUE des commandes iptables ou ip6tables ou commentaires ou lignes vides, se trouvant dans le dossier : /etc/firewall-chapril/local-rules.d/

#6 - 09/06/2017 00:46 - Quentin Gibeaux

J'ai fait quelques tests sur la soirée et j'ai appris plusieurs choses.

J'ai réussi à servir des adresses IPv6 via libvirt et une seconde conf réseau, avec la conf suivante :

```
<network ipv6='yes'>
  <name>default-ipv6</name>
  <uuid>7f46eb51-e1a5-41b2-8c11-aac06293b19c</uuid>
  <forward dev='enp0s31f6' mode='route'>
    <interface dev='enp0s31f6'/>
  </forward>
  <bridge name='virbr1' stp='on' delay='0'/>
  <mac address='52:54:00:f9:60:0e'/>
  <domain name='default-ipv6'/>
  <dns>
    <forwarder addr='2a01:4f8:0:a0a1::add:1010'/>
  </dns>
  <ip family='ipv6' address='2a01:4f8:10b:c41::2:1' prefix='112'>
    <dhcp>
      <host id='00:01:00:01:20:cc:6d:8e:52:54:00:40:2c:7c' name='test-ipv6' ip='2a01:4f8:10b:c41::2:199'/>
    </dhcp>
  </ip>
  <route family='ipv6' address='2a01:4f8:10b:c41::' prefix='64' gateway='2a01:4f8:10b:c41::2:1'/>
</network>
```

L'id associé à la vm test-ipv6 (créée pour l'occasion), est issue du scrutage des log de libvirtd et des négociations dhcp… c'est un id identifiant dérivé de l'adresse MAC.
Avec cela j'arrivais à pinger maine et coon, et test-ipv6 depuis maine, mais pas l'extérieur : des traces tcpdump montraient que l'extérieur ne me trouvait pas, mais recevait les pings.

En fait, mettre des adresses IPv6 fixes arbitraires est une mauvaise idée. *Il semblerait* que IPv6 trouve tout seul ses routes et cela fonctionne grace aux IP dynamiques attribuées, dérivées de l'adresse MAC (type préfix64::moitiéMAC:ff:ef:moitéMAC). En désactivant les baux, et laissant DHCPv6 attribuer les IPv6 c'était mieux, et j'arrivais à pinger l'extérieur. Mais pour ce faire, j'ai dû rattacher enp0s31f6 à l'interface bridge associée au réseau virtuel… et dès que j'ai fait ça, j'ai perdu la connectivité maine <-> coon, perdant de la même manière l'accès au DNS interne. Par contre j'arrivais à pinger l'extérieur (ping6 free.fr par exemple).

Donc pour résumer : actuellement, on obtient nos ipv6 dynamiquement via l'interface virbr0, mais celle-ci étant configurée en NAT, les VM n'accèdent pas à l'extéreur, et l'extérieur n'accède pas à elles. En passant par une seconde interface, configurée en ROUTE vers enp0s31f6 (<forward dev='enp0s31f6' mode='route'>), je n'ai pas réussi à obtenir une connectivité extérieur qu'en intégrant enp0s31f6 dans le bridge… ce qui a coupé, pour une raison obscure, le lien maine <-> coon.

#7 - 13/06/2017 11:46 - Quentin Gibeaux

- Version cible mis à Mise en production Chapril

#8 - 13/06/2017 17:17 - Quentin Gibeaux

Info utiles :
https://www.berrange.com/posts/2011/06/16/providing-ipv6-connectivity-to-virtual-guests-with-libvirt-and-kvm/
https://wiki.gentoo.org/wiki/QEMU/KVM_IPv6_Support

#9 - 13/06/2017 20:50 - Quentin Gibeaux

L'ipv6 fonctionne sur les VM \o/
J'ai ajouté une seconde interface réseau libvirt dédiée à l'ipv6, l'ai désactivée sur celle du réseau interne ipv4. Et pour chaque VM, il faut rajouter une règle ip -6 route pour faire pointer l'ipv6 de la vm vers virbr1 (iface virtuelle).

J'ai modifié le hook réseau pour qu'il applique ces règles, mais ça n'a pas l'air de se faire automatiquement, il faut investiguer ce point.

#10 - 13/06/2017 20:58 - Quentin Gibeaux

Voir également pour ajouter les entrées DNS idoines.
Il semblerait également qu'il manque une règle pour router le traffic entre les deux Hosts

#11 - 14/06/2017 00:57 - Quentin Gibeaux

> J'ai modifié le hook réseau pour qu'il applique ces règles, mais ça n'a pas l'air de se faire automatiquement, il faut investiguer ce point.

-> C'est bon, il fallait juste faire le ménage dans les vieux dnsmasq qui tournaient depuis le 4 juin

> Voir également pour ajouter les entrées DNS idoines.

IPV6 ajoutées pour toutes les VM en entrées AAAA, résolu que sur le réseau interne pour le moment.

> Il semblerait également qu'il manque une règle pour router le traffic entre les deux Hosts

Réglé par l'utilisation d'une adresse ipv6 dédiée pour l'iface virtuelle (prefix::1:2 pour maine et prefix::1:3 pour coon)

-> Tout fonctionne \o/

Il ne reste plus qu'à ajouter une "fip" ipv6 et un enregistrement AAAA pour router les mails/web/etc en ipv6

#12 - 14/06/2017 20:52 - Quentin Gibeaux

Il y avait en fait des problèmes de lifetime et de validité d'ip : au bout d'une heure les IP expiraient et n'étaient pas renouvelées.
Ça devrait marchait si le routeur de hetzner pouvait envoyer ses routes aux vm régulièrement, redonnant du temps aux adresses IP.
J'ai tenté de mettre le réseau ipv6 /64 exclusivement sur le bridge et de monter l'interface physique WAN sur le bridge, mais ça faisait tomber le réseau à cause du dnsmasq lancé automatiquement par libvirt.

Ne trouvant pas de solution, je me suis résolu à passer les IP en statique sur les VM…
J'ai également rajouté les champs AAAA idoines et maintenant l'infra chapril répond en IPv6 aux mails, au http/https et ssh.

#13 - 14/06/2017 20:53 - Quentin Gibeaux

- % réalisé changé de 0 à 90

#14 - 30/06/2017 22:36 - Quentin Gibeaux

- Statut changé de En cours de traitement à Résolu

- % réalisé changé de 90 à 100

Routage inter /64 via lien local fonctionnel, tout est ok !

#15 - 01/12/2019 04:03 - Christian P. Momon

- Assigné à mis à Quentin Gibeaux

#16 - 03/12/2019 10:35 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

#17 - 11/01/2020 06:26 - Christian P. Momon

- Projet changé de Chapril à Infra Chapril