mumble.chapril.org - Demande #4437

L'interface Web de mumble n'est pas accessible en IPV6

24/04/2020 15:45 - Laurent POUJOULAT

Statut:	Rejeté	**Début:**	24/04/2020
Priorité:	Faible	**Echéance:**	
Assigné à:	Didier Clermonté	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Backlog		

Description

L'interface Web de mumble n'est pas accessible en IPV6. Toutes les requêtes arrivent en IPV4. Il y a probablement un problème de routage quelque part.
A noter que cela n'affecte que mumble.chapril.org et pas visio.chapril.org.

Cela n'affecte pas le fonctionnement du service.

Historique

#1 - 27/04/2020 17:05 - Laurent POUJOULAT

J'ai investigué un peu sur le sujet et il y a deux raisons empilées (au moins):

La première, c'est simplement que le NGinx de Allo n'écoute pas en IPV6 (!). Pour écouter in V4 et V6, il faut ajouter à la configuration:

```
listen [::]:80;
```

à la place de:

```
listen 80;
```

Il faut absolument mettre toutes les conf (visio et mumble) dans ce mode, sinon il se passe des choses étranges (mumble renvoie sur visio)

Mais ça ne suffit pas. Bastion transmet l'IP réelle via le proxy protocol. Pour récupérer l'IP réelle en IPV6, il faut donc aussi ajouter aussi:

```
set_real_ip_from 2a01:4f8:10b:c41::93;
```

Après ça, on voit bien les connexions en IPV6.

Mais ça ne suffit pas encore. Les logs montrent que l'IP transise par Bastion dans le header X-Real-IP via IPV6 est encore l'IP V4 du client !? La il y a encore un mystère, mais côté Bastion et/ou DNS.

J'ai laissé dans /root/tmp les fichiers de configuration NGinx de mes essais.

#2 - 27/04/2020 17:31 - Christian P. Momon

> La première, c'est simplement que le NGinx de Allo n'écoute pas en IPV6 (!).

Ha bah oui, bien vu ! :D

> Pour écouter in V4 et V6, il faut ajouter à la configuration:
> listen [::]:80;
> à la place de:
> listen 80;

Alors, pas vraiment « à la place de » mais en même temps :

```
    listen 80;
    listen [::]:80;
```

Là, ça devrait être bon :-)

#3 - 06/05/2020 08:08 - Laurent POUJOULAT

- Statut changé de Nouveau à Confirmé

#4 - 08/06/2020 18:29 - Christian P. Momon

Après analyse, la configuration DNS associait le domaine mumble.chapril.org à l'ipv6 de la vm allo :

```
=(^-^)=root@dns:/etc/bind# grep -R mumble
zones/masters/chapril.org:mumble          A       88.99.233.240
zones/masters/chapril.org-int:mumble            CNAME   allo.cluster
```

Donc c'était bien pour le flux 64738 mais pas pour les flux 80 et 443…

#5 - 08/06/2020 18:45 - Christian P. Momon

Un problème connexe à cette configuration bancale d'ipv6 :

- puisque le domaine avait une ipv6 définie dans le dns alors Letsencrypt cherchait à l'utiliser pour renouveler le certificat ;
- comme le site web n'était pas accessible alors le renouvellement du certificat HTTPS échouait…

Pour stabiliser la plateforme, j'ai tout remis en ipv4 seulement.

#6 - 08/06/2020 19:29 - Christian P. Momon

- Statut changé de Confirmé à En cours de traitement

Pour activer ipv6, deux possibilités :

- nat ipv6 par port :
  - mumble.chapril.org --nat----80--> vm bastion --proxy--> vm allo…,
  - mumble.chapril.org --nat---443--> vm bastion --proxy--> vm allo…,
  - mumble.chapril.org --nat-64738--> vm allo…
  - revient à donner des ipv6 privées aux vm donc un gros changement dans l'infra,

- utiliser 2 noms de domaines différents (solution suggérer par QGuLL) :
  - mumbleweb.chapril.org -----80--> vm bastion --proxy--> vm allo…,
  - mumbleweb.chapril.org ----443--> vm bastion --proxy--> vm allo…,
  - mumble.chapril.org -----80--> vm allo --302--> mumbleweb.chapril.org --proxy--> vm allo…,
  - mumble.chapril.org ----443--> vm allo --302--> mumbleweb.chapril.org --proxy--> vm allo…,
  - mumble.chapril.org --64738--> vm allo.

Une préférence ? Une autre idée ?

À noter que rester en ipv4 n'est pas nominal car implique que le domaine mumble.chapril.org ne soit pas CNAME de la fip.

#7 - 05/12/2021 15:39 - Didier Clermonté

- Statut changé de En cours de traitement à Rejeté

- Assigné à changé de Christian P. Momon à Didier Clermonté

A réétudier plus tard

#8 - 11/02/2022 18:52 - François Poulain

Une discussion avec quelqu'un qui fait de l'ip v6 m'indique qu'on pourrait avancer sur la question, pour les protocoles non proxyfiés, avec un nat pour changer l'ip de destination.
Ça permettrait d'être congruent entre la logique v6 et la logique v4.

```
Règle nftables pour réécrire l'IPv6 de destination :

nft add rule ip6 raw prerouting ip6 nexthdr tcp ip6 daddr set fe00::1
tcp dport set 10 notrack

nft add : ajoute une règle
ip6 : domaine IPv6
raw : table raw
prerouting chain prerouting
ip6 nexthdr tcp : protocole TCP
ip6 daddr set fe00::1 : écrase l'IPv6 de destination
dport set 10 : écrase le port de destination
notrack : désactive le suivi de connexion
```

Source : https://wiki.nftables.org/wiki-nftables/index.php/Performing_Network_Address_Translation_%28NAT%29