Nftables

Cheatsheet

Example de commandes:

- Lister toutes les règles : `nft list ruleset`
- Lister la table filter de famille inet : `nft list table inet filter`
- Lister les règles en incluant les positions : `nft list table inet filter -a`
- Inserer une règle (ouvire le port 8080 tcp) a une position dans la table filter de famille inet après la règle à la position 5: `nft add rule inet filter input position 5 tcp dport 8080 accept`
- Supprimer la règle à la position 22: `nft delete rule inet filter input handle 22`
- Pour seulement supprimer les tables gérées dans le fichier de config, remplacer `flush ruleset` par `table inet filter; delete table inet filter` au début du ficher. La première instruction s'assure que la table existe avec de la supprimer pour de pas avoir d'erreur lors de la première exécution.

Le fichier de configuration est /etc/sysconfig/nftables.conf, pour recharger les règles après modification il peut être directement exécuté, ce qui est équivalent à nft -f /etc/sysconfig/nftables.conf. Pour ne pas affecter les règles gérer par podman il ne faut pas recharger le service nftables, cela écraserait toute autre règle rendant les containers injoignables.

Liens utiles

- https://wiki.archlinux.org/index.php/nftables
- https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes
- https://wiki.nftables.org/wiki-nftables/index.php/Scripting
- https://wiki.nftables.org/wiki-nftables/index.php/Performing_Network_Address_Translation_(NAT)

Révision #3
Créé 2020-12-12 16:33:39 UTC par Admin
Mis à jour 2020-12-12 16:47:59 UTC par Admin