

SAE203 – PRESENTATION ET INSTALLATION

Présentation du projet

Une entreprise disposant de plusieurs réseaux souhaite centraliser sur un même serveur la gestion des serveurs DHCP opérant sur chacun de ses réseaux. Sur chacun des réseaux de l'entreprise :

- Un unique serveur DHCP distribue des adresses IPv4 aux clients reliés au réseau physique.
- Seules les machines dont l'adresse MAC (fixe) est enregistrée par le service Réseau & Système peuvent récupérer une adresse IPv4 auprès du serveur DHCP.

1 – Solution a un problème

L'entreprise souhaite gérer ses différents serveurs DHCP sur un unique serveur central. La solution à ce problème va donc d'être de lancer des commandes, python dans mon cas, sur le serveur central qui auront un accès sur les différents serveurs DHCP.

Mon produit va donc servir à se connecter à distance sur les serveurs DHCP via SSH, une connexion dite sécurisée et d'exécuter plusieurs actions sur ces mêmes serveurs.

2 – Quels actions ?

2.1 – Ajout d'un couple mac/IP

Une commande permettant de rajouter une association mac/IP au serveur DHCP, pour attribuer à une machine présente sur le réseau DHCP concernée une adresse IP fixe.

2.2 – Suppression d'un couple MAC/IP

Une commande permettant de supprimer une association MAC/IP au serveur DHCP, pour plus que la machine n'ait d'adresse fixe.

2.3 – Vérification du DHCP

Une commande permettant de vérifier l'intégrité de la configuration DHCP d'un serveur défini lors de l'appel de la commande. Et optionnellement la corriger

2.4 – Liste de la configuration DHCP

Une commande permettant l'affichage formaté d'une ou des configurations DHCP suivant quel paramètre est émis avec la commande.

Installation du projet

Prérequis technique

Architecture de réseau minimal

Afin de pouvoir utiliser correctement sans encombre mon produit il faut :

- 1 machine centrale, supervisant les serveurs DHCP des réseaux de l'entreprise
- 1 machine servant de DHCP
- 1 machine servant de client au serveur DHCP

Toutes ces machines fonctionnant sur Debian 11. Chaque serveur DHCP sera situé dans un vlan différent.

Procédure d'installation de la solution technique

Installation des paquets SSH sur tous les serveurs DHCP et le serveur central.

⇒ `sudo apt install openssh`

Installation du paquet dnsmasq sur les serveurs DHCP.

⇒ `sudo apt install dnsmasq`

Création d'un utilisateur responsable de l'administration des serveurs DHCP, appelé et configuré en 'superv' :

- sur le serveur central
 - ⇒ `sudo useradd -u 2001 -d /home/superv -s /bin/bash -m superv`
 - ⇒ `sudo -u superv mkdir /home/superv/bin /home/superv/.ssh`
 - ⇒ `sudo chmod 700 /home/superv/.ssh`
 - ⇒ `sudo passwd superv`
- sur chaque serveurs DHCP
 - ⇒ `sudo useradd -u 2001 -d /home/superv -s /bin/bash -m superv`
 - ⇒ `sudo -u superv mkdir /home/superv/bin /home/superv/.ssh`
 - ⇒ `sudo chmod 700 /home/superv/.ssh`
 - ⇒ `sudo passwd superv`

Création de clés SSH sur le serveur central et envoi des clés publiques à chacun des serveurs DHCP

- ⇒ `sudo login superv`
- ⇒ `ssh-keygen -t rsa -b 2048 -f ~/.ssh/superkey`
- ⇒ `scp ~/.ssh/superkey.pub superv@<dhcp server ip>:~/.ssh/authorized_keys`
- ⇒ `chmod 600 /home/superv/.ssh/superv`

Création d'un fichier de configuration SSH sur le serveur central pour l'utilisateur responsable de l'administration des serveurs DHCP :

```
nano /home/superv/.ssh/config
```

```
Match User superv
```

```
IdentityFile ~/.ssh/superkey
```

Restriction de l'authentification SSH sur les serveurs DHCP :

```
⇒ sudo nano /etc/ssh/sshd_config
```

```
PasswordAuthentication no
```

Procédure relative à l'exécution des commandes

Le projet se trouve sur mon GitHub a l'adresse : <https://github.com/crastiflette/SAE-203>

Il faut tout d'abord télécharger tous les fichiers dans le répertoire utilisateur de superv sur le serveur central.

Ensuite il faut installer les paquets et les modules nécessaire au bon fonctionnement des commandes :

```
⇒ sudo apt install python3-pip
```

```
⇒ sudo login superv
```

```
⇒ pip3 install fabric pyaml
```

Il faut ensuite créer un fichier de supervision yaml que j'ai personnellement mis dans /etc/supervisor.yaml et qui devrait ressembler a ca :

```
dhcp_hosts_cfg : /etc/dnsmasq.d/hosts.conf
user : sae203
dhcp-servers :
  192.168.122.101: 192.168.122.0/24
```

Avec en dhcp_hosts_cfg le chemin vers le fichier contenant les associations MAC/IP sur les serveurs DHCP, user le nom d'utilisateur devant être utilisé pour se connecter a distances sur les serveurs et dhcp-servers les adresses et les réseaux des différents serveurs DHCP.

Maintenant il faut créer le fichier contenant les associations dans chaque serveurs DHCP.

Il faudra créer sur chacun des serveurs DHCP configurés le fichier de configuration dnsmasq enregistrant les associations des adresses IPv4 fixées par DHCP. Sans cela, les commandes de supervision échoueront.

Configuration des filtrages des commandes sur les servers DHCP

Création du script Bash responsable du filtrage des commandes exécutées par SSH :

```
⇒ sudo nano /home/gatekeeping/ssh-limiter.sh
#!/bin/bash
# Liste des commandes autorisees
allowed_commands=("grep -i" "sudo sed -i" "sudo systemctl restart dnsmasq.service")
# Recuperation de la commande executee
command=$SSH_ORIGINAL_COMMAND
# Verifications des commandes
command_allowed=false
for allowed_cmd in ${allowed_commands[@]}; do
    # Verification de la commande entrée
    if [[ $command == $allowed_cmd* ]]; then
        command_allowed=true
        # Verification des caracteres spéciaux
        if echo $command | grep -q '[:&|]'; then
            command_allowed=false
        fi
        break
    fi
done
# Execution de la commande si elle est autorisee
if $command_allowed; then
    eval $command
else
    echo "Unauthorized command"
fi

sudo chmod 755 /home/gatekeeping/bin/ssh-limiter.sh
```

Après l'application du filtrage SSH, seules les commandes de supervision du serveur central pourront ouvrir une connexion SSH vers les serveurs DHCP. Aucune autre connexion SSH ne sera possible.