Configurer une authentification SSH avec certificat

Principes

L'utilisation de certificats permet de garantir l'identité du client et du serveur.

Le certificat présent par le client ou le serveur est signé par la clé privée d'une authorité de certification reconnue.

- **Intérêt pour le client** : la **clé publique de la CA** permet de vérifier le certificat présenté par le serveur. Il n'est pas nécessaire de renseigner le fichier **know_hosts**.
- **Intérêt pour le serveur** : la **clé publique du CA** permet de vérifier le certificat présenté par le client sans avoir à renseigner le fichier a**uthorized_keys**.

Les éléments nécessaires

- le certificat de la CA
- le certificat du client
- l'identité du client

Mise en place côté serveur

- Le serveur doit disposer de la clé publique du certificat du CA
- la clé publique est indiquée dans le fichier de configuration du serveur SSH **/etc/ssh/sshd_config** avec la directive **TrustedUserCAKeys** qui précise le nom du fichier contenant la liste des clef publique des CA

```
TrustedUserCAKeys /etc/ssh/ca.pub
```

> **IMPORTANT** : le certificat du client ne sera considéré que si sa liste de nom-clés (principal) contient le nom du compte auquel il tente de se connecter.
>
> SAUF si un fichier spécifique à chaque compte indique la liste des noms-clés acceptés. Directive **AuthorizedPrincipalsFile** dans sshd_config

Mise en place côté client

Le client doit faire signer sa clé publique pour obtenir un certificat qui doit être placé dans le même répertoire que sa clé privé et publique.

Lors d'une connexion avec la clé privée, le certificat sera automatiquement présenté au serveur.

Le client ssh doit seulement indique quelle clé privée utiliser avec l'option -i

```
ssh -i ~/.ssh/id_ed25519 nomDNSserveur
```

Ainsi même s'il n'y a pas de clé publique client dans authorized_keys, l'authentification se fait. L'option -v permet de voir l'utilisation du certificat

```
ssh -v -i ~/.ssh/id_ed25519 nomDNSserveur
```

Les commandes utiles

- obtenir la clé publique à partir de la clé privée d'une identité utilisateur au format openSSH

```
$ ssh-keygen -y -f utilisateur-identite.pem > id_rsa.pub
```

- Obtenir la clé publique à partir du certificat de l'utilisateur au format openSSH pour une connexion ssh
  - Extraire la clé publique du certificat de l'utilisteur

```
$ openssl x509 -in charles-cert.pem -pubkey –noout > id_rsa.pem
```

noout permet d'avoir uniquement la clé publique sans le certificat

- Convertir la clé publique du format PEM au format openssh

```
$ ssh-keygen -f id_rsa.pem -i –mPKCS8 > id_rsa.pub
```

- Obtenir la clé publique de la CA du certificat de la CA au format openSSH pour une connexion ssh
  - Extraire la clé publique du certificat du CA

```
$ openssl x509 -in pkicub-cert.pem -pubkey –noout > ca.pem
```

```
* Convertir la clé publique du format PEM au format openssh
```

```
$ ssh-keygen -f ca.pem > ca.pub
```