Utiliser des certificats OpenSSH

Présentation

La connexion à distance à un serveur en SSH peut se faire avec des certificats dont le format est spécifique à OpenSSH.

Rappel : l'authentification sur le serveur en SSH consiste à renseigner votre clé publique dans le dossier .ssh/authorized_keys du compte existant sur le serveur.

Votre clé privée reste sur votre ordinateur client et ne doit pas être communiquée. Cette clé privée peut en plus être protégée par une passphrase.

Configuration du service SSH du serveur

Avec Debian, la configuration d'un serveur SSH se fait dans le fichier **/etc/ssh/sshd_config** :

- La directive **PasswordAuthentication** doit être fixée à **no** pour interdire l'authentification par mot de passe.
- dans le dossier **/etc/ssh** se trouve plusieurs types de clés privées, avec les clés publiques associées, générées automatiquement, que peut utiliser le serveur SSH : **ssh_host_ecdsa_key** (ssh_host_ecdsa_key.pub) , **ssh_host_rsa_key** (ssh_host_rsa_key.pub) et **ssh_host_ed25519_key** (ssh_host_ed25519_key.pub).

Pour **vérifier** le paramétrage du serveur SSH, lancez la commande suivante en mode debug :

```
$ sudo /usr/sbin/sshd -d
```

Génération du couple de clés privée / publique par le client

Utilisation de l'utilitaire **ssh-keygen** avec les options possibles suivantes :

- option **-t** : préciser le tp de clés : dsa, rsa, ecdsa ou ed25519 (valeur par défaut) ;
  - option **-b** : préciser la longueur de la clé (2048 par défaut).
  - option **-C** : préciser un commentaire pour identifier la clé publique : courriel, nom, etc..

```
$ ssh-keygen
```

Les clés privée et publique sont enregistrées dans le dossier **~/.ssh** : **id_ed25519** et **id_ed25519.pub**.

La passphrase de la clé privée peut être modifiée avec la commande suivante :

```
$ ssh-keygen -p -f .ssh/id_ed25519
```

La clé publique peut être affichée à partir de la clé privée :

```
$ ssh-keygen -y -f .ssh/id_ed25519
```

Paramètrage du compte du serveur avec votre clé publique

Sur le serveur distant, vous souhaitez permettre une authentification avec votre clé publique shh.

Pour cela, il suffit de **copier** le contenu de votre clé publique dans le fichier **~/.ssh/authorized_keys** du compte du serveur.

Exemple pour un compte appelé sio créé sur le serveur distant :

```
cat ~/.ssh/id_ed25519 | ssh sio@ipserveur cat
```