SSH

Le **S**ecure **SH**ell est un protocole permettant de ce connecter à distance à un équipement via une connexion sécurisée.

La version 1 à été créé par Tatu Ylönen en 1995

La version 2 à été définit par IETF en 2006, elle est décrite dans la RFC4251

SSH utilise le port 22 en TCP

SSH permet de s'authentifier via :

- un mot de passe
- une clefs

A la première connexion, il est demandé si la clefs du serveur est à accepter.
Une fois connecté il est possible :

- exécuter des tâches dans la limite de droits d'accès de l'utilisateur
- exécuter des scripts
- transférer des fichiers vers le serveur
- rapatrier des fichiers depuis le serveur

Pour une utilisation optimale :

- connexion par clefs
- si pas de clefs connexion par mot de passe
- certificats de la connexion connue
- limiter l'accès à la connexion SSH

Pour la configuration il faut éditer le fichier /etc/ssh/sshd_config
Il faut absolument configurer :

- **Port** 22 (par défaut)
- **ListenAddress** 0.0.0.0 (IPv4, adresse par défaut)
- **ListenAddress** : : (IPv6, adresse par défaut)
- **X11Forwarding** (yes, no)
- **PermitRootLogin prohibit-password** (prohibit-password, yes, no, forced-commands-only)

Les options supplémentaires à connaitre sont :

- **SyslogFacility** (définit le programme qui enregistre les logs)
- **LogLevel**
- **Banner** (message à la connexion)

Pour l'authentification par clefs

- **Cyphers** (cryptage autorisé)
- **PasswordAuthentication** (yes, no)
- **Hostkey** (chemin des clefs)
- **PublicHostKeyFile** (chemin de la clef publique)
- **PubkeyAuthentication** (yes, no)
- **AuthorizedKeysFile** (chemin des clefs autorisées)

Exemple :
Pour s'authentifier sur le serveur srv0 via clefs avec le compte adminsrv, il faut

- Générer une paire de clefs ssh : ssh-keygen -t ecdsa -b 256
- Transférer la clefs /home/user/.ssh/id_ecdsa.pub vers le serveur srv0
- Ajouter la clefs id_ecdsa.pub à /home/adminsrv/.ssh/authorized_keys

Connexion en ipv4 avec un autre port
ssh compte@adresseip -p port

Connexion en IPv6 avec un autre port
ssh -6 compte@adresseip -p port

Transférer un fichier
scp source utilisateur@ip :destination

Récupérer un fichier
scp utilisateur@ip :cheminsource destination

Transférer un fichier **scp -r repertoiresource utilisateurip :destination**

Récupérer un fichier
scp -r utilisateur@ip :repertoiresource repertoiredestination

Installer un serveur SSH sur Debian
apt install openssh-server

Configurer le serveur
nano /etc/ssh/sshd_config