**SSH**

|  |  |  |
| --- | --- | --- |
| **DESC** | | |
| Secure Shell : TCP port 22 | | |
| **FILES** | | |
| /etc/ssh/ | Ssh\_config |  |
|  | Sshd\_config | Configuration serveur |
| ~/.ssh/ | known\_hosts | Si première connexion SSH, la clef publique est ajoutée ici avec avertissement. |
|  | Authorized\_keys | Mettre les clefs publiques ici sur serveur si on peut pouvoir s’y authentifier sans mdp |
| /var/log/ | secure | Logs d’échec d’authentification |
|  | Auth.log |  |
| **QUICK START** | | |
| * Ssh login@host | | |

**Généralités :**

* Suite SSH comprend :
  + SSH : connexion shell sécurisé
  + SCP : Transfert fichier via SSH
  + SFTP
* Remplace la suite rxxx :
  + rlogin/telnet (remote login)
  + rsh/rexec (remote Shell, remote exec)
  + rcp (Copie à distance : remote copie)
  + ftp
* Authentification via :
  + Login/mdp via les clefs publiques connues dans known\_hosts
  + Via clés publiques dans authorized\_keys
* Agent SSH permet de stocker en mémoire les passphrases : Chiffrement symétrique d’une clef privée à partir d’une clef dérivée de la passphrase (via un hash). S’utilise dans le cas où la clef privée est compromise.
* SSH 2.0 utilise Diffie-Hellman pour l’échange d’une clef symétrique choisie par le client dans la liste proposée par le serveur

**Authentification par clef publique/privée :**

* Clef publique du client doit se trouver dans l’authorized\_keys du serveur
* Client doit avoir ses clefs publique/privée dans ~/.ssh/

**Fichier de configuration sshd :**

|  |  |
| --- | --- |
| **Directive** | **Comments** |
| Port |  |