|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **SSH** | | | | |
| **DESC** | | |  | | |
| **FILES** | | | | | |
| **/etc/ssh/** | | | coté serveur | | |
| **~/.ssh/** | | | coté client | | |
| **~/.ssh/known\_hosts** | | | Clefs publiques connues | | |
| **CLI** | | | | | |
| **CONNEXION** | | | | | |
| **ssh** | | login@IP [commande] | |  | |
|  | |  | | -l login |  |
| **GENERATION CLEF** | | | | | |
| **Ssh-keygen** | |  | | Génère clef publique + privée | |
|  | | -t rsa | | Type de clef | |
|  | | -b 4096 | | Taille de la clef | |
|  | | -l –f clef | | Génère hash de la clef  -f pour préciser la clef | |
| **AGENT** | | | | | |
| **Ssh-agent** | |  | | Charge les clefs privées en mémoire | |
| **Ssh-add [Opts] <clef>** | |  | | Ajout d’une clef à l’agent | |
|  | | -d | | Supprime la clef de l’agent | |
| **Comments :**  Authentification asymétrique puis canal symétrique  Authentification par clefs :   * Coté client : clef publique et privée dans ~/.ssh * Coté serveur : clef publique du client dans authorized\_keys de .ssh   établissement :   * serveur envoie sa clef publique asymetrique * client chiffre sa clef avec la clef publique du serveur * serveur dechiffre puis connexion symetrique * si authentification par clef, serveur envoie un challenge crypté avec la clef publique du client * le client decode et renvoie le challenge * auth accepte | | | | | |