**SSH**

|  |  |  |
| --- | --- | --- |
| **DESC** | | |
| Secure Shell : TCP port 22 | | |
| **FILES** | | |
| /etc/ssh/ | Ssh\_config |  |
|  | Sshd\_config | Configuration serveur |
| ~/.ssh/  Rwx pour owner uniquement | known\_hosts | Clefs publiques connues |
|  | authorized\_keys | Clefs publiques utilisables pour l’authentification par clefs |
| /var/log/ | secure | Logs d’échec d’authentification sous CentOS |
|  | Auth.log | Sous Debian |
| \* | Sshd –f <path> : ce fichier de configuration est utilisé  Utile quand on démarre plusieurs sshd sur différents ports | |
| **QUICK START** | | |
| * Ssh login@host | | |

**Généralités :**

* Démon sshd, fork un nouveau démon lors de chaque connexion
* 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
* 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
* Fonctionnalités natives :
  + Authentification par login/passwd via les clefs publiques connues dans known\_hosts
  + Par clef publique (2048 octets de base) dans authorized\_keys
  + Par LDAP qui va rapatrier les clefs publiques ?
  + Par Kerberos
  + Liste d’utilisateurs autorisés
  + Couplage avec PAM
* Sshd ne démarrera pas si les clefs sont accessibles par quelqu’un d’autre que le propriétaire.

**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 value

|  |  |  |  |
| --- | --- | --- | --- |
| **Directive** | **Comments** | | |
| **GENERALE** | | | |
| Port <X> |  | | |
| Protocol <X> | 1|2|2,1  Utiliser 2 : 1 pose des problèmes de sécurité | | |
| Hostkey <path> | Clefs privées utilisées par sshd  Sshd refuse d’utiliser un fichier accessible au groupe et others | | |
| **LOGIN** | | | |
| LoginGraceTime <X> | Sshd se déconnecte après X secondes si l’utilisateur ne s’est pas connecté | | |
| StrictModes | Yes|no  Si oui, sshd check owner+permissions du /home de l’utilisateur en train de se connecter | | |
| **SECURITE** | | | |
| UsePrivilegeSeparation | Yes|no  Si yes, sshd fork un fils non privilégié avant de prendre en charge la connexion entrante | | |
| PermitRootLogin | Yes|without-password|forced-commands-only|no | | |
| PermitEmptyPasswords | Yes|no  Si on autorise l’utilisateur à avoir le mdp "" | | |
| UsePAM |  | | |
| AllowUsers <user1> [<user2>] | | |  |
| AllowGroups |  | | |
| DenyUsers |  | | |
| DenyGroups |  | | |
| **AUTHENTIFICATION** | | | |
| RSAAuthentication | | **Obsolète** | |
| PubKeyAuthentication | | Yes|no  Spécifie si on autorise l’authentification par clefs publiques  S’applique uniquement à la version 2 | |
| AuthorizedKeysFile <path> | | Clefs publiques pour l’authentification utilisateur   * %h : home directory * %u : utilisateur | |
| AuthenticationMethods | | publickey[,password][,keyboard-interactive] | |
| **LOG** | | | |
| SyslogFacility | DAEMON|AUTH|LOCAL0-7 | | |
| LogLevel | Niveau de verbosité de sshd dans les logs | | |
| PrintLastLog | Spécifie si on affiche la date-heure de la dernière connexion utilisateur | | |
| **GRAPHIQUE** | | | |
| X11Forwarding | Yes|no | | |