Mise à niveau L3: ssh

Stefan Schwoon

DER Informatique, ENS Paris-Saclay

10 septembre 2024

Objectifs

ssh: Connection à distance

- se connecter d'une machine à une autre
- (ou depuis chez vous à la salle de machines)

git: gestionnaire de versions

- sauvegarde/archive des version de vos projets
- projets collaboratifs

Internet protocol (IP)

en très très bref → pour un traitement détaillé, voir cours de Réseau en M1

Adressage de machines

- IPv4: toute machine a une adresse de 4 octets (32 bits), p.ex. `138.231.36.60`
- IPv6: adresses de 16 octets (128 bits), p.ex. `fe80::5054:ff:fe46:7eb` (avec des 0 manquants)
- DNS: adresse textuelle (traduite en IP derrière les scènes), p.ex. `ssh.dptinfo.ens-cachan.fr`

Commandes utiles

- `/sbin/ifconfig` (trouver son adresse IP)
- `hostname -r` (trouver son nom DNS)

Les ports

- On se connecte sur une machine sur un port (entier entre 0 et 65535).
- Certains services attendent des connections sur des ports bien définis, p.ex. ssh (22), http (80).
- Une fois une connection établie, les deux parties échangent des données selon un protocôle préalablement défini (les RFC).
- L'usage des ports 0..1023 est réservé aux admins.

L'utilitaire SSH

Obtenir un shell sur une autre machine (à priori, port 22)

Syntax de ssh

ssh [-p port] [user@]nom_de_machine

Salle de machines

- passerelle (accessible depuis l'extérieur): `ssh.dptinfo.ens-cachan.fr`
- machines individuelles (accessible depuis passerelle): `01.dptinfo.ens-cachan.fr` etc

Exercices

- se connecter à `ssh.dptinfo.ens-cachan.fr` (la passerelle)
- depuis cette passerelle, se connecter à une autre machine
- créer de fichiers dans dossier de départ (partagé) et dans `/tmp` (stockage local)
- utiliser la commande `who`

Outil companion: scp

Copier des fichiers entre machine locale et distante

- locale $\rightarrow$ distante:
  `scp fichier.txt ssh.dptinfo.ens-cachan.fr:`
- distante $\rightarrow$ locale:
  `scp ssh.dptinfo.ens-cachan.fr:fichier.txt .`

Redirections

Local forwarding

- ssh -L localhost:[port]:01.dptinfo.ens-cachan.fr:22 [user]@ssh.dptinfo.ens-cachan.fr
- crée un port sur la machine locale
- toute connection SSH à ce port local sera redirigée vers la passerelle qui elle la redirige vers la machine 01

D'autres options

- ajouter -N pour ne pas avoir de shell
- option -J (dans des versions plus récentes)
- option -D pour redirection plus général

Cryptographie asymétrique

- paire de clés *publique* et *privée*
- ce qui est crypté par l'une est décrypté par l'autre
- on garde la clé privée secrète, mais on peut donner la clé publique à tout le monde
- toute personne peut encrypter ses message à vous avec votre clé publique (et seul vous pouvez les décrypter)
- vous pouvez signer un document avec votre clé privée (tout le monde peut vérifier que le document vient de vous en le décryptant avec votre clé publique)

Dépôt d'une clé publique

Générer une paire de clés

- ssh-keygen [-f .ssh/mon_cle]
- demande une phrase de passe
- génère une clé privée dans le fichier donné, une clé publique correspondante dans un fichier .pub

Installation

- sur sa machine : générer une paire de clés
- sur la machine distante : copier la clé publique dans `.ssh/authorized_keys`
- sur sa machine : `ssh -i .ssh/mon_cle user@machine_distante`

Fichier de configuration

Raccourci pour se connecter à la passerelle

- créer un alias sa `.ssh/config`, p.ex.

```
Host passerelle
  HostName ssh.dptinfo.ens-cachan.fr
  User [username]
  IdentityFile  /.ssh/mon_cle
```

- puis `ssh passerelle`

Connexion vers une machine derrière la passerelle

- ajouter un alias de plus:

```
Host m01
  HostName 01.dptinfo.ens-cachan.fr
  User [username]
  IdentityFile  /.ssh/id_man
  ProxyCommand ssh passerelle -W %h:%p
```