**Bachelier en informatique et Systèmes**

**Informatique industrielle**

**3ème année**



**Catégorie technique**

**Charleroi**

**Laboratoire de réseaux**

**SSH**

**2015 – 2016 Haveaux Valentin**

**Table des matières**

[1 Serveur SSH 4](#_Toc440962005)

[2 Fichier et dossier important 4](#_Toc440962006)

[3 Installer serveur SSH 4](#_Toc440962007)

[4 Lancer SSH en mode debug 4](#_Toc440962008)

[5 Générer une paire de clé SSH 4](#_Toc440962009)

[6 Se connecter à une autre machine/exécuter une commande/copier un fichier 5](#_Toc440962010)

[7 Générer/Vérifier une empreinte 5](#_Toc440962011)

[8 Vérifier la clé publique 5](#_Toc440962012)

[9 Régénérer une paire de clé SSH pour des machines clonés 5](#_Toc440962013)

[10 Visualisez les portes d'écoutes d'une connexion 5](#_Toc440962014)

[11 Fichier de configuration SSH 6](#_Toc440962015)

[12 Connexion par mot de passe 7](#_Toc440962016)

[12.1 Vérifiez qu'aucun coupe-feu ne tourne sur la machine 7](#_Toc440962017)

[12.2 Vérifiez sur la machine qu'un trousseau de clés existe 7](#_Toc440962018)

[12.3 Démarrer et configurer le service 7](#_Toc440962019)

[12.4 Se connecter d'une machine à l'autre 7](#_Toc440962020)

[12.5 Visualiser les ports d'écoutés 7](#_Toc440962021)

[12.6 Utilisez ssh et scp 7](#_Toc440962022)

[13 Connexion par clés 8](#_Toc440962023)

[13.1 Vérifier les clauses PubkeyAuthentication 8](#_Toc440962024)

[13.2 Générer un trousseau de clé et copier sa clé publique 8](#_Toc440962025)

[13.3 Attention aux permissions 8](#_Toc440962026)

[14 Port forwarding 9](#_Toc440962027)

[14.1 - vérifiez qu'aucun coupe-feu ne tourne sur aucune machine 9](#_Toc440962028)

[14.2 -N'oubliez pas d'activer l'ip forwarding sur MV2 9](#_Toc440962029)

[14.3 Stopper les services sshd sur MV1 et MV2 (s'ils tournent) 9](#_Toc440962030)

[14.4 Configurez un service sshd sur MV3 et relancez le service 9](#_Toc440962031)

[14.5 Vérifiez sur MV3 qu'un trousseau de clés existe 10](#_Toc440962032)

[14.6 Créez user3 sur MV3 10](#_Toc440962033)

[14.7 Configurez et testez un forwarding de port de MV1 vers MV3 en passant par MV2. 10](#_Toc440962034)

[15 Clé du serveur 11](#_Toc440962035)

[16 Clé du client 11](#_Toc440962036)

SSH

# Serveur SSH

**Daemon du serveur DHCP** : sshd

**Fichier de configuration** : /etc/ssh/sshd\_config

**Lancement/arrêt/redémarrage** : service sshd start/stop/restart

**Logs**: /var/log/message /var/log/secure

# Fichier et dossier important

**Clés publiques des serveurs consultés**: /home/jean/.ssh/known\_hosts

**La clé publique du serveur**: /etc/ssh/ssh\_host\_(rsa ou dsa)\_key.pub

**La clé privée du serveur:** /etc/ssh/ssh\_host\_(rsa ou dsa)\_key

**La clé publique du client**: ~/.ssh/id\_rsa

**La clé privée du client:**  ~/.ssh/id\_rsa.pub

**Fichier contenant la liste clés autorisée**: ~/.ssh/authorized\_keys

# Installer serveur SSH

Dans CentOS c'est déjà préinstaller☺.

# Lancer SSH en mode debug

/usr/sbin/sshd **-d**

# Générer une paire de clé SSH

ssh-keygen -t rsa **-b 1024**

# Se connecter à une autre machine/exécuter une commande/copier un fichier

ssh user2@10.0.0.2

ssh user2@10.0.0.2 'cat /etc/passwd'

scp /root/install.log user2@10.0.0.2:/tmp

# Générer/Vérifier une empreinte

sha1sum f1.txt > f1.txt.sha1 ou md5sum f1.txt > f1.txt.md5

sha1sum –c f1.txt.md5 ou md5sum -c f1.txt.md5

# Vérifier la clé publique

L'administrateur du serveur génère un 'fingerprint' (chaîne générée lors de la génération de la clé publique du serveur.

La commande 'sshkeygen –lf /etc/ssh/ssh\_host\_**rsa**\_key.pub' permet d'afficher cette empreinte.

Ex. 2048 fe:91:17:91:c1:bd:ab:ae:5e:05:8b:70:40:1b:e8:c2 ( **RSA**)

• Le client demande le 'fingerprint' à l'administrateur.

• Le client compare le 'fingerprint' présenté lors du téléchargement à celui reçu de l'administrateur.

# Régénérer une paire de clé SSH pour des machines clonés

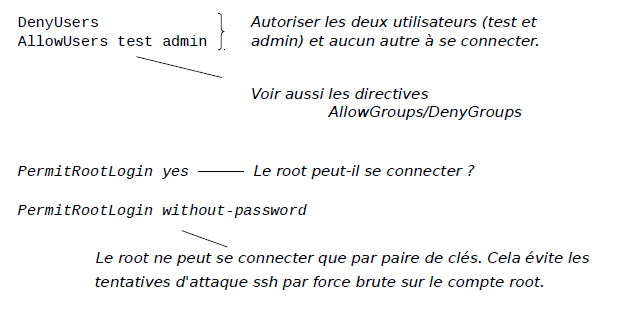
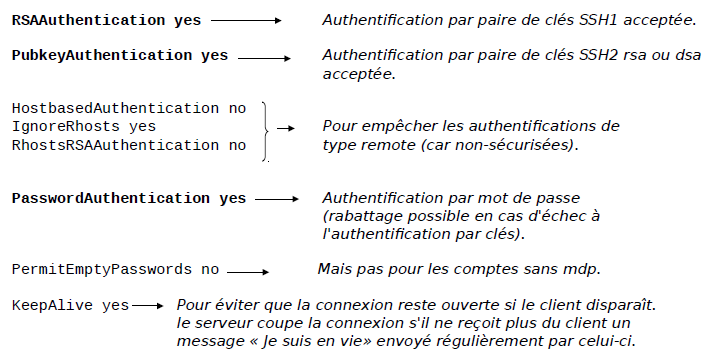
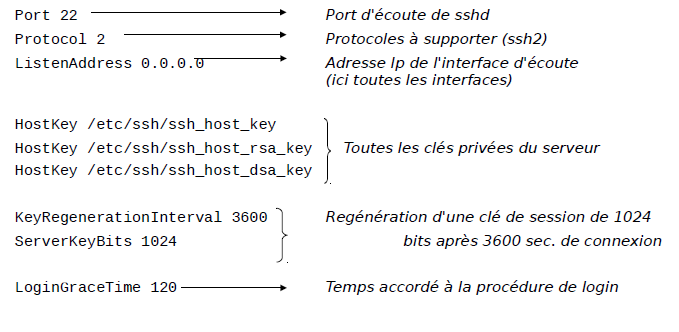
rm –f /etc/ssh\_host\*

service sshd restart

# Visualisez les portes d'écoutes d'une connexion

netstat –tn

# Fichier de configuration SSH



# Connexion par mot de passe

## Vérifiez qu'aucun coupe-feu ne tourne sur la machine

# iptables –L

# service iptables stop

# chkconfig --level 35 iptables off

## Vérifiez sur la machine qu'un trousseau de clés existe

#ls –l /etc/ssh

Régénérer une paire de clé SSH pour des machines clonées:

rm –f /etc/ssh\_host\*

service sshd restart

## Démarrer et configurer le service

Vérifiez que la directive PasswordAuthentication est à yes:

# cat /etc/ssh/sshd\_config | grep Password

Redémarrer le service et vérifier qu'il est bien relancé:

# service sshd restart

# ps ax | grep sshd

## Se connecter d'une machine à l'autre

ssh [user@10.0.0.1](mailto:user@10.0.0.1)

## Visualiser les ports d'écoutés

netstat –tn

## Utilisez ssh et scp

root@MV1# ssh user2@10.0.0.2 'cat /etc/passwd'

root@MV1# scp /root/install.log [user2@10.0.0.2:/tmp](mailto:user2@10.0.0.2:/tmp)

# Connexion par clés

## Vérifier les clauses PubkeyAuthentication

grep PubkeyAuthentication /etc/ssh/sshd\_config

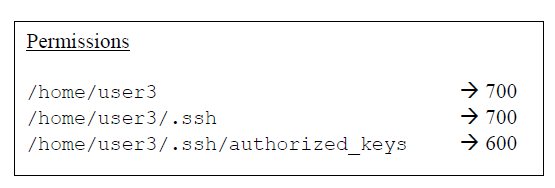
## Générer un trousseau de clé et copier sa clé publique

user1@MV1$ ssh-keygen –t rsa

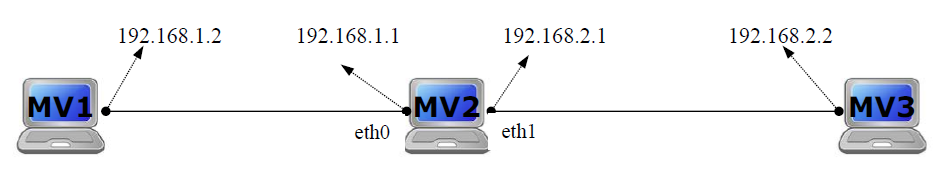
user1@MV1$ cd ~/.ssh

user1@MV1 .ssh$ ssh-copy-id –i id\_rsa.pub [user3@10.0.0.3](mailto:user3@10.0.0.3)

## Attention aux permissions



# Port forwarding



## - vérifiez qu'aucun coupe-feu ne tourne sur aucune machine

*Sur chaque station:*

# iptables –L

# service iptables stop

# chkconfig --level 35 iptables off

## -N'oubliez pas d'activer l'ip forwarding sur MV2

# mcedit /etc/sysctl.conf

Ip\_forward=1

#sysctl -p

## Stopper les services sshd sur MV1 et MV2 (s'ils tournent)

MV1# service sshd stop

MV2# service sshd stop

## Configurez un service sshd sur MV3 et relancez le service

*(bien vérifiez que la directive 'PasswordAuthentication' est à yes)*

# cat /etc/ssh/sshd\_config | grep Password

# service sshd restart

# ps ax | grep sshd

## Vérifiez sur MV3 qu'un trousseau de clés existe

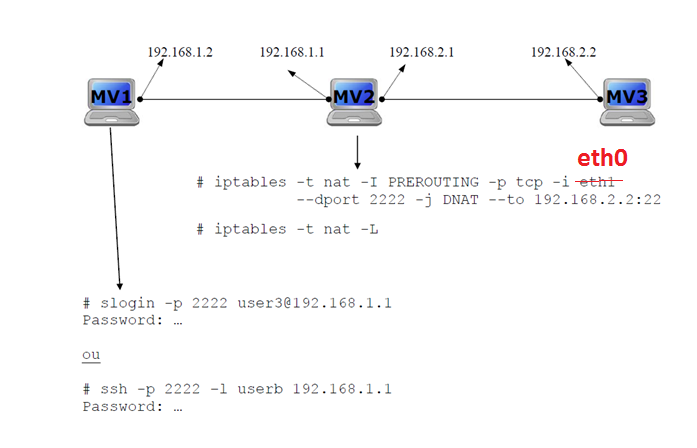
MV3# ls –l /etc/ssh

## Créez user3 sur MV3

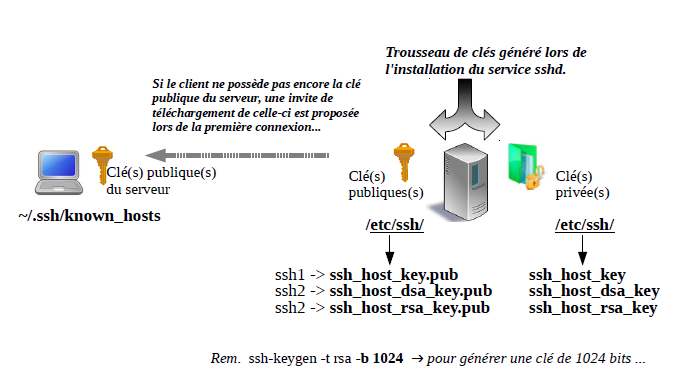
root@MV3# adduser user3

root@MV3# passwd user3

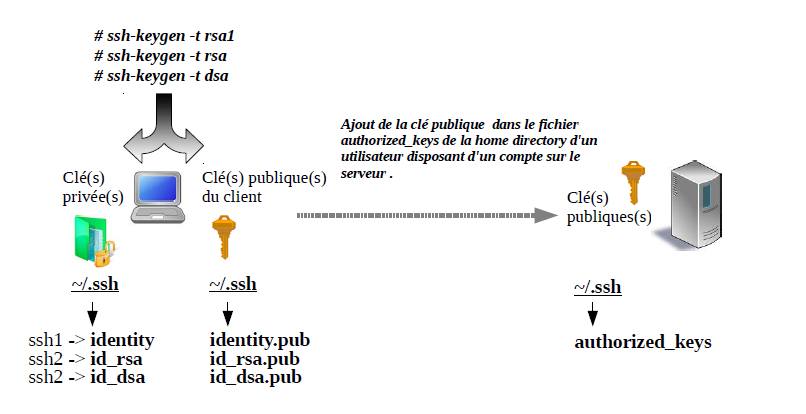
## Configurez et testez un forwarding de port de MV1 vers MV3 en passant par MV2.



# Clé du serveur



# Clé du client



ssh-copy-id *username*@*adresse* copie sa clé publique dans l'authorized\_keys de l'autre user.