

TP-SSH

KALETA MAXIME

#### SSH c'est quoi ?

SSH, OU SECURE SOCKET SHELL, EST UN PROTOCOLE RÉSEAU QUI **PERMET AUX ADMINISTRATEURS D'ACCÉDER À DISTANCE À UN ORDINATEUR, EN TOUTE SÉCURITÉ**. SSH

#### Commande "Which SSH"

root@debian:∼# which ssh ∕usr/bin/ssh

NOUS OBTENONS LE CHEMIN VERS LE DOSSIER SSH

## Connexion SSH avec Putty

#### 🧬 maxime@debian: ~

g<sup>R</sup> login as: maxime g<sup>R</sup> maxime@192.168.20.167's password: Linux debian 6.1.0-17-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.1.69-1 (2023-12-30) x86\_64

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

#### CONNEXION À DISTANCE

-

## Ouverture du dossier de configuration du SSH

GRÂCE À LA COMMANDE "NANO /ETC/SSH/SSHD\_CONFIG

ON NE PEUT PAS SE CONNECTER AVEC LE "USER" CAR IL N'EST PAS ADMIN



# Changement port 22 en 2022

# This is the sshd server system-wide configuration file. See # sshd\_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd\_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd\_config.d/\*.conf

Port 2022

DANS LE FICHIER VU PRÉCÉDEMMENT, CONFIGURATION DU PORT D'ÉCOUTE

#### connexion

SI L'ON SE RECONNECTE ON VA POUVOIR CAR LES MODIFICATIONS NE SONT PAS PRISES EN COMPTE ENCORE CEPENDANT APRÈS UN REDÉMARRAGE DE LA MACHINE LE PORT AURA OFFICIELLEMENT CHANGÉ

### Pour quoi faire ?

CHANGER DE PORT PERMET DE PAS SAVOIR QUE C'EST UN SSH ETANT DONNÉ QUE LE PORT 22 EST SOUVENT ASSOCIÉ AU SSH

# Connexion en changeant le port

🖉 maxime@debian: ~	<u></u>	
g <sup>R</sup> login as: maxime g <sup>R</sup> maxime@192.168.20.167's password: Linux debian 6.1.0-17-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.69-1 x86_64	(2023	3-12-
The programs included with the Debian GNU/Linux system are free so the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.	ftware	a *
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.		

maxime@debian:~\$

DANS PUTTY J'AI SAISI LE LE PORT 2022 ET JE ME SUIS CONNÉCTÉ

# Changement pour ajout du root

#LoginGraceTime 2m permitRootLogin without-password

POURQUOI EST-CE QUE LA PERMISSION DONNÉE (OU PAS) À ROOT EST-ELLE IMPORTANTE À MAITRISER ?

C'EST IMPORTANT CAR LA MOINDRE PERSONNE QUI ARRIVE À SE CONNECTER EN ROOT PEUT FAIRE CE QU'IL VEUT C'EST POUR CELA QU'IL FAUT SAVOIR L'UTILISER

#### Permis empty passwords no

CETTE OPTION PERMET D'AUTORISER OU NON DES CONNEXIONS AVEC UN COUPLE IDENTIFIANT/MOT DE PASSE MAIS EN AUTORISANT QUE LE MOT DE PASSE SOIT VIDE. CECI EST UNE ABERRATION DU POINT DE VUE SÉCURITÉ. PAR DÉFAUT, CETTE OPTION EST SUR « NO ».

#### Permisrootaccess withoutpassword

PERMET DE SE CONNECTER AVEC MOT DE PASSE MAIS UNIQUEMENT AVEC LA MACHINE ORIGINELLE SUR

# Création des utilisateurs :



ADDUSER (NOM UTILISATEUR)

LES UTILISATEURS : USER1, USER2, USER3

#### Création des groupes :

ADDGROUP (NOM GROUPE)

LES GROUPES : ETUDIANTS, SSH



# Ajouter un utilisateur à un groupe

COMMANDE : USERMOD -G (GROUPE) (UTILISATEUR) POUR ATTRIBUER DEUX GROUPES AU USER1: USERMOD -G ETUDIANTS,SSH USER1

### Mot de passe utilisateurs :



CHPASSWD (TAPEZ ENTRÉE)

USER1: PASSWORD1 (TAPEZ ENTRÉE)

USER2: PASSWORD1 (TAPEZ ENTRÉE)

USER3: PASSWORD1 (TAPEZ ENTRÉE)

(TAPEZ CTRL-D)

root@debian:/home# chpasswd user1:Password1 user2:Password1 user3:password1

#### Connexion au ssh via le client

debian12@debian:~\$ ssh 192.168.1.33

debian12@192.168.1.33's password: Linux debian 6.1.0-17-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.1.69-1 (2023-12-30) x86\_64

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Sun Feb 4 13:49:25 2024 from 192.168.1.33

#### Droits d'accès

ÉTANT DONNÉ QUE L'ACCÈS AUX RÉPERTOIRE DES UTILISATEURS EST IMPOSSIBLE NOUZS ALLONS DEVOIR DONNER LES DROITS AUX UTILISATEURS POUR POUVOIR CREER LES SOUS-RÉPERTOIRE ".SSH"

debian12@debian:/home\$ cd user2
-bash: cd: user2: Permission non accordée

root@debiar root@debiar	n:/∤ n:/∤	nome# chmo nome# ls ·	od 777 use -l	er1						
total 20					~ .					
drwx	16	debian12	debian12	4096	31	janv.	15:30	debian12		
drwx	5	maxime	maxime	4096	2	fêvr.	16:22	maxime		
drwxrwxrwx	2	user1	user1	4096	4	févr.	12:28	user1		
drwx	2	user2	user2	4096	4	févr.	12:28	user2		
drwx	2	user3	user3	4096	4	févr.	12:31	user3		
root@debian:/home# chmod 777 user2										
root@debian:/home# chmod 777 user3										
root@debiar	h:∕ł	nome#ls ·	-1							
total 20										
drwx	16	debian12	debian12	4096	31	janv.	15:30	debian12		
drwx	5	maxime	maxime	4096	2	févr.	16:22	maxime		
drwxrwxrwx	3	user1	user1	4096	4	févr.	13:50	user1		
drwxrwxrwx	З	user2	user2	4096	4	févr.	13:52	user2		
drwxrwxrwx	3	user3	user3	4096	4	févr.	13:52	user3		

Désormais l'accès aux répertoires est possible je vais donc creer les repertoire ".ssh"

debian12@debian:/home\$ ls
debian12 maxime user1 user2 user3
debian12@debian:/home\$ cd user2
debian12@debian:/home/user2\$ mkdir .ssh
debian12@debian:/home\$ cd user3
debian12@debian:/home/user3\$ mkdir .ssh
debian12@debian:/home/user3\$

### Création du fichier .ssh dans le /home de root

root@debian:~# cd /home root@debian:/home# mkdir .ssh

# On donne les droits sur le fichier .ssh

#### COMMANDE CHM (root@debian:/home/user2# cd /home/user3 cd /home/user3# cd /home/user3# chmod 0770 ~/.ssh

root@debian:~# cd /home/user1 root@debian:/home/user1# ls root@debian:/home/user1# chmod 0770 ~/.ssh root@debian:/home/user1# cd /home/user2 root@debian:/home/user2# chmod 0770 ~/.ssh root@debian:/home/user2# cd /home/user3 root@debian:/home/user3# chmod 0770 ~/.ssh

#### Génération d'une clé :

maxime@debian:~\$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/maxime/.ssh/id\_rsa):
Created directory '/home/maxime/.ssh'.
Enter passphrase (empty for no passphrase):

PASSPHRASE : AZERTY59

## Generation des clé sur comptes clients

COMMANDE :

"SSH-KEYGEN -T DSA -F (CHEMIN VERS LE COMPTE)/.SSH/ID\_DSA"

ON LE FAIT POUR TOUT LES UTILISATEURS

root@debian:~# ssh-keygen -t dsa -f /home/user2/.ssh/id\_dsa Generating public/private dsa key pair. Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in /home/user2/.ssh/id\_dsa Your public key has been saved in /home/user2/.ssh/id\_dsa.pub The key fingerprint is:

SHA256:im8VTBkLkjJiLHLd7c4pRvxeFe3FlC6+NmikoQwciJ4 root@debiar The key's randomart image is:

+---[DSA 1024]----+

#### Deux fichiers sont créé

#### SUITE AU "NANO ID\_DSA"

----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAzDmyDdr h3NpGCEJ7HQFrRAAAAEAAAAAAAAAAAGzAAAAB3NzaC1kc3MAAACBAO+NTKkacIDmMAF/28+X hprh6p+pgry3eDxgGNe1K2wHLXWXgQOMgHs/mcJsIoNhMSU92MHApLHUEceLGo1KMkHaAF 0cnwyuMnm7FL5+eM128d8F13aKWXI7dSDoh0Jn0IrDe982w0MrxwKMpbAZNnwzWVW5qZV0 vZ7j1a+bIeKXAAAAFQDBjPbMFhZ8f2itKCcddDkhvL4kbQAAAIEA0jW2+b3KPuM/M5P4Hk k8GrWx0SkD/94f7gfcCwGHaMM8AFdaG4xnKx7gkggB0I+3ETd3Sy6M2GxRwRUE8+B7pfmF y7bxqqwBq9VQ4iFkDXHE484vyTSZn09V4rf25cuXj8Q5SUoLYBtT0Ecc1NZdoaum3Vfy1Y VaPULaM/mSvR4AAACBAMvST7w0Ld529jYC6Ha0m/8QNvnMzz6bRe2Qe2WdNpzgFK2Fa2Fi mP7FZVTmJm6xb14Goqri+nHb5uDHG6J9bfW9SlCk31jenM3E+a30nvHsYAvdqqaWHGuBMQ 4IJbDZ9Gxq26BvRwjzqSrToHj9le+/sPwuTZ+3Yj4xTIeyM4kZAAAB8Mx14SN90BP5WdLc 2ZNJebxy19CtXbaVgGTJeBQNdYYlnPJ6friiWznRoRFS2uH5D0yRVDr5tVHoYM3n+3i/y1 kH28+zYdCDSVFHk3ZtSQ77pno/UenziGP9ECKikmCsi0m5SWZP3wkYxYmriCyCcU4CmCBw BAcBLCXSUu0kU4lsEnVVQwfARMIhyFbZ1K9jbDn92HwuqwUu3C3dJP3fZ6TDWz5rMTVHNC U44RVgcaIlC3RHFv8X3YyyAYl2vD9447x+9babKgZ6NgW1fgltkVxRvTEgeS6ZMF2L9wGs 8GCalS8YLZEFJUieiZUPxbTto7jQbaqqwrHsmY2XyzbtGRTAqZ3xyMrYiz20M3qT4xvCrA pZkU9S6aDy/aHqqdADn+rdoRihCJdh4t16T/K8fYn8Byb0KzQEtBDDkfK8Potyptjidk9x S8dH/etkS6d3e0BtnpYFzHkbSFnyMfsjXdLKkiPH219msvom4rto0bvxEMvcVMn3lLdeYr YFf5dtBHM09hs+8eTfVect0npanF3YdJe26z04szzltt56GEhE6NuDvsBlIIchCCK6nLSI 4GqCM+dC56loUstLJuIZSmn2B5NhA1TC67IIqtmsDjrfzSTpCJ2t0tGtVci8ITrLskfkap qhvRhGpL55doF90ps=

----END OPENSSH PRIVATE KEY-----

#### SUITE AU"ID\_DSA.PUB"

GNU nano 7.2 sh-dss AAAAB3NzaC1kc3MAAACBAO+NTKkacIDmMAF/28+Xhprh6p+pgry3eDxqGNe1K2wHLXWXqQOMqHs/mcJsIoNhMSU92MHApLHUEceLGo1>

Les deux fichiers sont differents car l'un est la clé d'identification et l'autre clé public

## Copie de la clé sur le serveur pour le root

maxime@debian:-\$ ssh-copy-id -i ~/.ssh/id\_dsa.pub root@192.168.20.167
/usr/bin/ssh-copy-id: INF0: Source of key(s) to be installed: "/home/maxime/.ssh/id\_dsa.pub"
The authenticity of host '192.168.20.167 (192.168.20.167)' can't be established.
ED25519 key fingerprint is SHA256:j4GydC3+KMpSg+dsyKaWFuo0hh/YKezRgF073wJ7stI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INF0: attempting to log in with the new key(s), to filter out any that are already install
ed
/usr/bin/ssh-copy-id: INF0: 1 key(s) remain to be installed -- if you are prompted now it is to install the new
keys
root@192.168.20.167's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@192.168.20.167'" and check to make sure that only the key(s) you wanted were added.

FAIRE LA MÊME COMMANDE POUR LES AUTRES UTILISATEURS GRÂCE AU CHEMIN D'ACCÈS À LA PLACE DU "~"

#### Pour voir les clé autorisée

Commande : "(nano ~/.ssh/authorized\_keys)"

ssh-dss AAAAB3NzaC1kc3MAAACBAM2qafQA0XV37cakn7XU6Gu9PlRwelTVDN9FBvHm9JCIDZGLgvQqZBjFIrjmciyGDAadDdsiMMIAuUiojUE<mark>> <</mark>2WCvUNrNGWZ29nHONgvi9QrYQAAAIEAkNaEml/eC9FFENEtV8zWjgsYsS<mark>7</mark>rq+Lv0/R0mrLAlQPdmAE1sdHc6e90LC40I6YwkdAZmMqQW873abF ssh-dss AAAAB3NzaC1kc3MAAACBALdhS9FeMp9tiQcUHE5Se4lp5BulGt2HhE1Db+ksKeit2uFx7ogbXLZgSsGqAMSL0zkxmzw4p/6zXGnmAm6> ssh-dss AAAAB3NzaC1kc3MAAACBALdhS9FeMp9tiQcUHE5Se4lp5BulGt2HhE1Db+ksKeit2uFx7ogbXLZgSsGqAMSL0zkxmzw4p/6zXGnmAm6>

# Connexion à partir du client

root@maxime-HP-ZBook-15-G5:/home/maxime# ssh user1@192.168.60.80 The authenticity of host '192.168.60.80 (192.168.60.80)' can't be established. ED25519 key fingerprint is SHA256:j4Gydc3+KMpSg+dsyKaWFuo0hh/YKezRgFQr3wJ7stI. This key is not known by any other names Are you sure you want to continue connecting (yes/no/[fingerprint])? YES Warning: Permanently added '192.168.60.80' (ED25519) to the list of known hosts user1@192.168.60.80's password: pASPermission denied, please try again. user1@192.168.60.80's password: Permission denied, please try again. user1@192.168.60.80's password: Linux debian 6.1.0-17-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.1.69-1 (2023-12-30) x86\_64

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. user1@debian:~\$

### Apres config du fichier de ssh

#LoginGraceTime 2m AllowGroups root, ssh #popmitDrotyDecowords ro

AUTORISATION AU PERSONNES DU GROUPE SSH ET ROOT À ACCEDER AU PC EN SSH

### Connexion au compte qui n'est pas dans le groupe root ou ssh

## En revanche avec l'utilisateur 2

naxime@maxime-HP-ZBook-15-G5:~\$ ssh user2@192.168.60.80
Jser2@192.168.60.80's password:
\_inux debian 6.1.0-17-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.1.69-1 (2023-12-30)
<86 64</pre>

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Jser2@debian:~\$