

BTS SIO1

# TP-ADMINA DISTANCE SSH

**Nicolas Debut** 





# Internet Qu'est ce que le ssh?

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé permettant entre autres de se connecter à un ordinateur à distance. SSH est indispensable pour l'administration de serveur sous Linux.

SSH

## Server with **public SSH** key

# Voyons comment le configurer

Tout d'abord nous allons effectuer la commande which ssh pour voir si le service n'est pas déjà installé en occurrence il l'est sinon effectuez un apt-get install ssh.

> root@nicolasserver:~# which ssh /usr/bin/ssh

### Une fois que vous l'aurez installé repérez votre adresse IP puis allez dans putty afin de tenter la connexion.

### root@nicolasserver:~# ip a

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
 inet 127.0.0.1/8 scope host lo
 valid\_lft forever preferred\_lft forever
 inet6 ::1/128 scope host noprefixroute
 valid\_lft forever preferred\_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000
 link/ether 9e:63:32:e8:f3:97 brd ff:ff:ff:ff:ff
 altname enp0s18
 inet 192.168.20.59/24 brd 192.168.20.255 scope global dynamic ens18
 valid\_lft 6826sec preferred\_lft 6826sec
 inet6 fe80::9c63:32ff:fee8:f397/64 scope link
 valid\_lft forever preferred\_lft forever

	PuTTY Security Alert	: -	0	8
The server's host key the server is the comp The server's ssh-ed25 ssh-ed25519 255 b2: If you trust this host, cache and carry on co If you want to carry o key to the cache, pres If you do not trust thi connection.	is not cached. You have uter you think it is. 519 key fingerprint is: 3c:b3:00:c3:66:5a:f6:67 press "Accept" to add t nnecting. n connecting just once, s "Connect Once". s host, press "Cancel" t	e no guarantee 7:de:4e:25:66:b the key to PuT , without addin to abandon the	d:41 TY's	: :50 e
<u>A</u> ccept	C <u>o</u> nnect Once	Cance	l	

PuTTY Configuration	- 🛛 😣
Basic options for your PuTTY sessi Specify the destination you want to connect to	on
Host Name (or IP address)	Port
192.168.20.59	22
Connection type: Raw <u>T</u> elnet Rlogin <u>S</u> SH	◯ Se <u>r</u> ial
Load, save or delete a stored session Sav <u>e</u> d Sessions	
Default Settings	Load
	Sa <u>v</u> e
	<u>D</u> elete
Close window on e <u>x</u> it: Always Never Only on clear	n exit
<u>O</u> pen	<u>C</u> ancel

Une fois connectez vous arriverez sur cette page. Vous devrez entrer des logins et mots de passe. Vous remarquerez que vous ne pouvez pas vous connecter en root mais nous y reviendrons plus tard.

	192.168.20.59 - PuTTY	-	ø 😣	Maxime_Fenetre@192.168
📌 login as: 📘				12-30) x86_64
				The programs included with the exact distribution ten individual files in /usr/:
				Debian GNU/Linux comes wi permitted by applicable l Maxime_Fenetre@nicolasser

.20.59's password: -17-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.1.69-1 (2023-

n the Debian GNU/Linux system are free software; rms for each program are described in the share/doc/\*/copyright.

th ABSOLUTELY NO WARRANTY, to the extent er:~\$ ∏

GNU nano 7.2

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:/usr/games

<sup>!</sup> 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

#AddressFamily any #ListenAddress 0.0.0.0 #ListenAddress ::

#HostKey /etc/ssh/ssh\_host\_rsa\_key #HostKey /etc/ssh/ssh\_host\_ecdsa\_key M∣ostKey /etc/ssh/ssh\_host\_ed25519\_key

≭ Ciphers and keying ≭RekeyLimit default none

¥ Logging ¥SyslogFacility AUTH ¥LogLevel INFO

/ Authentication:

#LoginGraceTime 2m #PermitRootLogin prohibit-password #StrictModes yes #MaxAuthTries 6 #MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized\_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized\_keys .ssh/authorized\_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none #AuthorizedKeysCommandUser nobody /etc/ssh/sshd\_config

Vous aurez remarqué que le port par défaut du ssh est le port 22 ainsi pour sécuriser un minimum votre connexion ici par exemple nous avons mis le port 2022.

Pour le changer vous devrez modifié le fichier /etc/ssh/sshd\_config.

### Après avoir modifié cette ligne vous pourrez voir que vous ne pouvez plus vous connectez via le port 22. Essayons maintenant de nous connecter avec le port 2022.

		PuTTY Configuration
192.168.20.59 - PuTTY – 🔹 😢	Category:	Category: Basic options for your PuTTY see
	▼ Session	<ul> <li>Session</li> <li>Specify the destination you want to connect to</li> </ul>
	Logging	Logging Host <u>N</u> ame (or IP address)
	<ul> <li>Terminal</li> </ul>	• Terminal 192.168.20.59
	Keyboard	Keyboard Connection type:
	Bell	Bell ORaw O <u>T</u> elnet ORlog <u>i</u> n O <u>S</u> SH
DuTTV Estal Error	Features Window	Load, save or delete a stored session
Putty Facal Error - V 🐼		Appearance Sav <u>e</u> d Sessions
Connection refused	Behaviour	Behaviour
	Translation	Translation Default Settings
	Selection	Selection
	Colours	Colours
<u>O</u> K	Fonts	Fonts
	✓ Connection	<ul> <li>Connection</li> </ul>
	Daca	Data
	Telnet	Close window on exit:
	Rlogin	Rlogin
	► SSH	► SSH
	About	
	About	<u>A</u> bout <u>O</u> pen

### Et vous voilà de nouveau connectés via Putty

Maxime\_Fenetre@nicolasserver: ~

Iogin as: Maxime\_Fenetre Maxime\_Fenetre@192.168.20.59's password: Linux nicolasserver 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: Fri Feb 2 16:06:35 2024 from 192.168.20.123 Maxime\_Fenetre@nicolasserver:~\$



Comme nous l'avons vu précédemment il n'est pas possible de se connecter en root pour remédier à cela nous allons retourner dans le fichier configuration du ssh et modifier les lignes suivantes, qui, comme vous le verrez sont assez explicites. Il est important de réfléchir avant d'activer cette option surtout réfléchir à quoi va servir votre ssh veillez à ne pas activer cette option s'il n'y en a pas l'utilité. # Authent icat ion:

#LoginGraceTime 2m
PermitRootLogin yes\_
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# For this to work you will also need host keys in /etc/ssh/ssh\_known\_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known\_hosts for
# HostbasedAuthentication
# IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here! #PasswordAuthentication yes PermitEmptyPasswords no\_

# Change to yes to enable challenge-response passwords (beware issues with # some PAM modules and threads) KbdInteractiveAuthentication no

### Nous allons maintenant voir comment gérer les utilisateurs sur le serveur et sur le client.

root@nicolasserver:~# addgroup etudiant Ajout du groupe « etudiant » (GID 1015)... Fait. root@nicolasserver:~# addgroup ssh Ajout du groupe « ssh » (GID 1016)... Fait. root@nicolasserver:~# \_

root@nicolasserver:~# usermod -a -G etudiant user1 root@nicolasserver:~# usermod -a -G ssh user1 root@nicolasserver:~# usermod -a -G ssh user2 root@nicolasserver:~# usermod -a -G etudiant user3

Nous allons commencer par creer nos groupes et nos utilisateurs puis nous allons mettre les utilisateurs dans leurs groupes avec la commande usermod -a -G groupe utilisateur.

### root@nicolasserver:~# chpasswd user1:Password1 user2:Password1 user3:Password1 root@nicolasserver:~# \_

user1@nicolasserver: ~

12

₽ login as: user1 ₽ user10192.168.20.59's password: Linux nicolasserver 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@nicolasserver:~\$ Vous devrez ensuite modifier les mots de passes de vos utilisateurs avec la commande chpasswd, puis mettez

votre\_utilisateur:nouveau\_mdp autant de fois que d'utilisateur à modifier.

Vous pourrez ensuite voir que votre commande à fonctionner en essayant de vous reconnecter avec vos nouveau mots de passe.

### Nous allons maintenant voir comment gérer l'échange de clés publiques.

root@nicolasserver:/home# cd user1 root@nicolasserver:/home/user1# ls root@nicolasserver:/home/user1# mkdir .ssh mkdir: impossible de créer le répertoire « .ssh »: Le fichier existe root@nicolasserver:/home/user1# mkdir /home/user2/.ssh root@nicolasserver:/home/user1# mkdir /home/user3/.ssh root@nicolasserver:/home/user1# 📘

### Nous allons tout d'abord créer un dossier .ssh dans le dossier de chaque utilisateur.

root@nicolasserver:~# mkdir /home/.ssh

- root@nicolasserver:/home# chmod 0770 /home/user1/.ssh root@nicolasserver:/home# chmod 0770 /home/user2/.ssh root@nicolasserver:/home# chmod 0770 /home/user3/.ssh root@nicolasserver:/home# chmod 0770 /home/.ssh
- Nous allons ensuite faire en sorte que les propriétaires et les membres du groupe aient tous les droits sur leurs dossiers.



Nous allons ensuite générer une clé publique à destination du serveur pour chaque utillisateur avec la commande ssh-keygen -t dsa -f /home/utilisateur/.ssh/id\_dsa

user1@nicolasserver:~\$ cd /home/user1/.ssh user1@nicolasserver:~/.ssh\$ ls id\_dsa id\_dsa.pub

Vous verrez que dans votre dossier .ssh se situent 2 fichiers et lorsque nous regardons à quoi ressemblent ces fichiers:

### root@nicolasserver:~# cat /home/user1/.ssh/id\_dsa.pub

root@nicolasserver:~<mark>#</mark> cat /home/user1/.ssh/id\_dsa ----BEGIN OPENSSH PRIVATE KEY-----

b3B1bnNzaC1rZXktdjEAAAAACmF1czI1Ni1jdHIAAAAGYmNyeXBOAAAAGAAAABCR4Ppxzt 4EQREhA/cmTK/UAAAAEAAAAAEAAAGxAAAAB3NzaC1kc3MAAACBANC3ntagwUtzmLfno05p SkaBVDzDfAcaLVdcJLKxnsc67PaiJiem3p5HGzFQ61HPQp0mGqZtL0pUnVYen9q90A64Mn jK4MOzQsqGY1w1DIsz2GbMlyXTcIecvf2JxAbkvkOesCSixJ8Y1/X<u>EP46311RqUWAnhLUP</u> 8IK7fvbYeLRHAAAAFQDfypej5ops8Mhu5s1tyCAJYUtECwAAAIApCw2+I1e5ySvZvL/Z3N MpcBE1ZhJFfXbF30y7FoweEKBvggjKHpVkkTJjcGP9e+u5X0NaDsCX99GkMpbwMB6o3eya lv8WB+CEGmzy/FD/D+R2KukkfP8QPD1PHGffzfWkKXGoFzgrDa154V60/3SNPx7/DGXPdW 2M1gD9tEx2ZQAAAIApRbaBN+S8t4puDtNEJB5y4FxIiv5aDvKncmJco4XZ00om1M0Ce+YF 1AMY1HA8NOTt10XCB8JMsNJ7gTUMaCLvxJWoox290Ymd6cJZbYVL4h0U1S/ZL0bWsaKoZR KnjYv7VBq9u00z1k/bJnkLsKSJiN1urRMq90ZXb3N4GUAN+gAAAfBRVxYS257XGRY8eXnb 3059H2JcsEkUz7ZvW470bsN1qTaVkqKNIkUSzCUYM1EFL0ZD0yg5r0NPv1YsPngNkfL5xs 2X3ICeTpqHGMbKi5+YAruGjIIS5I10Id0HUMM1NFNj85QD3dKHQc5I3JPF09p5hwKNerV2 cGriHT6PUDTpGLUVODrJU3UPcC8D4dOCTi9f3Ug5ZP0TuiN0KGhD495RijSOWNJd9fczSm P+bAodLvCjBYx15UkimvwW7S1SoByHPDDDsS0zZ21S5cNS4YfCItkEo2UoKGQ6dHeKVAsM Qu8dU2n++MAoO8QH5R1vn9vrBat,jbVa04SMFFN7yYg6ppR30LN+UzRcLTqRZmGKim2MvZP DQqITDyy8VQTe7Rs7Pd3hwJggDgUvKprRaW98s65CrIGzyQxU1mH8s1fphMj8eeK31odzq XkYfxK4X/J9pki1Skb/GfY3sX4tyF9/QAjwJDid94kwNtnpZZLYYDQt92KzCbGrzX08fdi 8Fgon8HbCEUs4FTP0+Vhbd43DCQ8Y1bA/5kY1K0J/8D0HJ+7nBYhiBZ2fMmjwFvUM8851C 5c62bL/yatEZXcq2bfDyKHe76Ny9VZaHeVE3ikh5ixZ2UqZWESvYNNZ+eGEOPmYpmQAoQ+ (Cu+tmlOscha00

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

Comme vous pouvez le voir les deux clés sont différentes ce qui est normal la première est la clé publique qui sera partagée avec le serveur alors que la deuxième est une clé privée qui est une clé qui ne sera connue que par la machine qui l'a générée.

root@nicolasserver:/home/user1# cd Nous allons ensuite pour les root@nicolasserver:~# ssh-copy-id -i /home/user1/.ssh/id\_dsa.pub root@192.168.20.59 /usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user1/.ssh/id\_dsa.pub" The authenticity of host '192,168,20,59 (192,168,20,59)' can't be established. utilisateurs concernés envoyés une ED25519 key fingerprint is SHA256;e0CsetMLtOIeKKhFSEIuXeKG91180gVteoVLKDhrc68. This key is not known by any other names. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes copie de la clé publique au serveur /usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed /usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys root@192.168.20.59's password: ssh afin qu'il puisse nous Number of key(s) added: 1 Now try logging into the machine, with: "ssh 'root@192.168.20.59'" identifier avec la commande: and check to make sure that only the key(s) you wanted were added. root@nicolasserver:~# ssh-copy-id -i /home/user2/.ssh/id\_dsa.pub root@192.168.20.59 ssh-copy-id -i /usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user2/.ssh/id\_dsa.pub" /usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed /usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys /home/utilisateur/.ssh/id\_dsa.pub root@192.168.20.59's password: Pour finaliser cette étape on vous Number of key(s) added: 1 Now try logging into the machine, with: "ssh 'root@192.168.20.59'" and check to make sure that only the key(s) you wanted were added. demandera le mot de passe root de root@nicolasserver:~# [ la machine. root@nicolasserver:~# ssh root@192.168.20.59 root@192.168.20.59's password: Pour tester que vous avez bien une Linux nicolasserver 6.1.0-17-amd64 #1 SMP PREEMPT DYNAMIC Debian 6.1.69-1 (2023-12-30) x86 64 connexion entre votre client et votre The programs included with the Debian GNU/Linux system are free software; ssh vous pourrez utiliser la commande the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright. ssh utilisateur@adress\_ip\_serveur (-p Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent port (pas utile si laisser par défaut)) permitted by applicable law. Last login: Wed Feb 7 15:37:23 2024 from 192.168.60.75



Pour finir nous allons sécuriser un peu plus notre connexion en autorisant uniquement les groupes root et ssh à la connexion ainsi tout utilisateur ne faisant pas partis de ces groupes ne pourrons pas se connecter. To disable tunneled clear text passwords, change to no here!

PasswordAuthentication yes

#PermitEmptyPasswords no

Ensuite si vous souhaitez faire en sorte que l'authentification ne se fasse plus par mot de passe mais grâce à une clé alors modifier ce paramètre en no.



root@nicolasserver:~# ssh user2@192.168.20.59 user2@192.168.20.59's password: Linux nicolasserver 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.

Pour ensuite tester votre paramétrage essayez de vous connecter avec un utilisateur faisant partie d'un des deux groupes( ici user2 du groupe ssh) et un autre ne faisant partie d'aucun des deux groupes (ici user3 du groupe etudiant) et vous verrez que pour le deuxième la connexion

### est impossible.

user2@nicolasserver:~\$ ssh user3@192.168.20.59 hostkeys\_find\_by\_key\_hostfile: hostkeys\_foreach failed for /home/user2/.ssh/know n\_hosts: Permission denied The authenticity of host '192.168.20.59 (192.168.20.59)' can't be established. ED25519 key fingerprint is SHA256:e0CsetMLtOIeKKhFSEIuXeKG91180gVteoVLKDhrc68. This key is not known by any other names. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Failed to add the host to the list of known hosts (/home/user2/.ssh/known\_hosts). user3@192.168.20.59's password: Permission denied, please try again. user3@192.168.20.59's password:

# Voici votre ssh configuré !

