

SSH

Table des matières

SSH.....	1
Introduction au ssh	2
1) Qu'est-ce que c'est ?.....	2
2) Mise en garde sécurité	2
3) cryptographie.....	2
4) établissement d'une connexion SSH.....	3
II) installation et configuration.....	4
2) configuration.....	4
pour lancer le server : service sshd start	5
connexion du client : ssh login@machine.....	5
III) le teste	6
SCP	7
Tunnel SSH	7

Introduction au ssh

1) Qu'est-ce que c'est ?

SSH = secure Shell

Protocole qui permet des communications chiffrées entre un serveur et un client.

Il remplace les anciens protocoles telnet, rlogin, rsh.

Version 1 en 1995, aujourd'hui obsolète.

Version 2 en 2006

2) Mise en garde sécurité

SSH permet à un utilisateur d'accéder à un système à distance avec son identifiant.

Est son mot de passe.

Trois contraintes majeures de sécurité :

-avoir un serveur SSH à jour

-les mot de passe de l'utilisateur doivent être suffisamment complexe

-surveiller régulièrement les connexions dans les logs.

3) cryptographie

SSH utilise la cryptographie asymétrique et symétrique.

Cryptographie asymétrique (RSA de préférence > DSA)

Chaque personne dispose d'un couple de clef :

Une clef publique est une clef privée. La première peut être librement publiée

Alors que la deuxième doit rester secrète. La connaissance de la clef publique

Ne permet pas de connaître la clef privée

Si Alice veut envoyer un message privé à BOB elle doit le chiffrer avec la clef publique

De Bob. Seul Bob pourra déchiffrer le message avec sa clef privée

Cryptographie symétrique :

Si Alice et Bob veulent s'envoyer un message confidentiel, ils doivent d'abord

Posséder tous les deux la même clef secrète la même clef secrète

Les algorithmes de cryptage symétrique sont beaucoup moins gourmands en ressource

Processeur que ceux du cryptage asymétrique.

Mais leur problème est l'échange de la clef secrète

Dans le protocole SSL utilisé par SSH est le navigateur web, le cryptage

Asymétrique est utilisé au début pour échanger la clef secrète de manière sécuriser

4) établissement d'une connexion SSH

Un serveur SSH possède un couple de clef attachée dans le dossier /etc/ssh

ssh_host_rsa_key contient la clef privée

Avec les permissions 600

```
pi@raspberrypi:/etc/ssh $ sudo cat ssh_host_rsa_key
-----BEGIN OPENSSH PRIVATE KEY-----
o3B1bnNzC1rZXkttdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlAAAAadz2gtc
NhAAAAAEAAQAAAYEAw18hsOkQ0dtsGDgG+eDCYrVi7tXrLP8Yn8fhEOx9kAGmT4GmkIc
rN1+gDIzR2Ahacz4uvZQwKITdRA9vK00nH18/WUAQU+/NFU9d1ntMnZSrrZKDe1MGeLxS
oD0yDU8bG7KybRSikozJ2ABbzrepQ2164ATssQ1PvD37YiI+2wbZFbi1RoITTKI:qZENk
yJSTI2Aw2MXNzrF1GfruyvVNI0aeMD4E9ddk1zudy4CinHw/ku4/HxaZgcwItVR32bps
WbjZhh/J2iJmRgBSbwUGfRICT9PMNZ3pQ0AkUT1NTdmhwUqHb0UQbLmVYab9r0rgmQ1/0
IEytHR+w5mMo8/RAPuv1XLH0pRxxgZGe36Cz6e1Djp0npTV5ahNYehWkr1rbFTczx7vYf
Njv80TAQZxhkn99jwq6I0U73vT5sHDwZX63MRmeSHqxwHaEY7C+ihzwbvHxnojuZeMM0
DUIdGWhS06mEw1o6ErhRFsyFT7hvgKxCmQP9HZrJAAAFiCGB4Z0hgeGdAAAAAB3NzaC1yc
EAAAGBAMJfIbDpEnHbbBg4BvngwmK1Yu7V6yz/6J/H4RDsfZABpk+8ppCHD6zZfoAyM0d
IwnM+Lr2UMCiE3UQpbytnJx5fP11AEFPvzRVPXZ7TJ2Uq62Sg3tT8ni8UjqAzsg1PGxu
sm0UopKMydgAw863qUNpeuAE7LEJ7w9+2IiPtsG2RW4tUaIk0yiMamRDZJMiUkyNgMNj
lzc6xZrn67sr1TYtGnjA+BPXZJc7ncuAopx8P5LuPx8WmMCMVUd9m6bJfGy2YYfydo
ZkYAUm8F8Bn64gk/TzDwd6UDGJFE5U3ZocFKh29FEgy51cmm/a9K4Jk3f9NyBMR0fs0Z
KPP0QD7r9YyxUcYGRnt+gs+ntQ46dJ6U1eWoTWHoVq5K9a2xU3M8e72BYzY7/DkwKkG
4ZJ/fY8KuINFO970+bBw8GV+tzEZnkh6sVh2hgOwvooc8G7x8Z6I7mXjDNHglCHR1oUju
mMNaOhK4URbMhU+4bxiSqpKd/R2ayQAAAAMBAEAAAGAFZsnjpfJw9o1Q0fxdpNSaFCLZ
s1skHF8fXAdmX94sHZq0dy9EHoAopMqzh4FxCOpWLTJUM0UxUMD2a+PBBmfGyhARIDF
XqoTA/XpFQPsGvmub6/iFrqQYa+Jnmf+48MC8EAHYbwDigMz+09QKbcr/nhcFmYiOL1nv
VZB4G5cp2uo0GLpzdYD1pj6VwCoxsNMvuC+eOx1NaccJjepEANQKEJEoONJjjoVR0
MSKLTGK0bfS0w+impCicG5nkvB4F0VV4uAFrd+eguIePxfPqQhZB iPMp2tA5rnLqHP
xSNqZV0QhUc8Vwe02/Vi0UDuRQDBV7seuueq/Xp6yRpDuxo3tixdUILxtOwDxM6wn4xic
4T+PM9Kf5Wg5AC0SrwUkzhv2isp+iAXd/11UCKO9biOw+XQe59i5+rWbYH1SgPPNAf9
CuY9+SpkEUpIQYx3wYtGaB2aFmgED9WKLMB9Ch4tkqHtV9wK8Z7VRgZov7fL0bzyBAA
wC1gbQildgpo9cXS2UelmpaZqa7t7kPDI181DCgYnBU3RYWtm3oxsSds9mDkOtH23Ht
QRc+f93EKau+QkdbCSCDL2RKL1+6MZbLkSUdeUjsN9o+LHPUkwH0H2L4UJ1pi+pBUK8BY
AkV662zTmcniN9G8RQ1zg6Vcz2F7mFRIHuaRkz/6NfMp3awWPPCmr8gx9bHSVST3Eyzv3
n00FJ+0oaFGtA2i2c28nPMGsOypppsOFmmbGH+oEddj5R9AAAAEAA/YiKLP7UR7MZw1h
DSIFrCw8TRp5NsJGImrVXxvRkSjyFDxybU1qhMAMH17hQHPn0GXyZ6x4k7VNUPUx9B55
MM+zQ+P5PDMmo9fffkBqmpPUqRcomqsshwgz14vG3ZznqUsj5c3jW1W6zDTsR//EbHgw0
NFayM1oEtmhZBRjp4dJvLs+1JKtsZhiHd1WAF3Jpb16hQrIcrF5ZxHQ/N4C6NU/o/BTPf
MtjgzXVq4dq7UBfZaUblfcsIwa+ghZAAAwQDEQz3Co10gULQMNPH0yS0cgHczhHkKjG
9A3U10h6F4Bw9xak4yyXctu18r6J61cpIXOVHagY01D5yWLR/2e+XwU/S01tMan4HGnr8B
FzyyJ3wL13KLWYRHdoj/skGHBjT52+DHj2YctygbyjNwOwaZaEGStWZzZqcuIpcM3q+R
gLS/yGQLNokYIN+oSshUKRTMQD1h8AATMnyAPK4cXQ72j4q94uNq3J+vxAm8STpCmtjT
Hh57F2V1h1/EAAAAQcm9vdEByYXNwYVYcnlwaQECAw==
-----END OPENSSH PRIVATE KEY-----
```

ssh_host_rsa_key.pub contient la clef publique avec les permissions 644.

```
pi@raspberrypi:/etc/ssh $ sudo cat ssh_host_rsa_key.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQCXyGw6RDR22wY0AB54MjItWLuless/xifx+EQ7H2QAAZPgaaQhw+s2X6AMjNHYCFpzPi6
91DAohN1ED28rTScexZ9ZQBBT780VT12We0ydlKutkoN7UwZ4vF16gM7INTxsbsrJtFKKSjMnYAFvOt61DaXrgB0yxCU+8PftiIj7bBtkVuL
VGiJNMojGpkQ2STI1JmJYDDYxdc30sWUZ+u7K5U2LRp4wPgT112SX053LgKKcFd+S7j8FFpmBzAi1VHfZumyRYGNmGH8naImZGAFJvBQZ+uI
DP08w1ne1A4CRR0U1N2aHBSodvRR8suZXJpv2vSuCZCX/TcgTK0JH7DmYyJz9EA+6/VcsfS1HGBkZ7FoLPp7U00nSe1NX1qE1h6FauSvWtsV
NzPHu9gW20/w5MCpBleGSf32PCroJRTve9PmwcPB1frcxGZ5IerFYdoRjsL6KHPBu8fGei0514wzR4NQh0ZaFI7qYTDWj0SuFEWzIVPuG8Y
rEKZA/0dmk= root@raspberrypi
```

Etapes :

- 1) le serveur envoie sa clef publique au client qui vérifie si la déjà reçu
- 2) le client génère une clef secrète est l'envoi au serveur en la cryptant avec la clef publique du serveur
- 3) pour le prouver au client le serveur chiffre un message standard avec la clef secrète et l'envoi au client qui le déchiffre avec sa clef secrète donc c'est le bon serveur
- 4) une fois la clef secrète échanger, le client et le serveur peuvent donc établir

un canal sécurisé grâce à la clef secrète commune, on passe en cryptage symétriques

5)le client peu maintenant envoyer son id et mot de passe au serveur en toute sécurité

II) installation et configuration

1) on utilise la version openssh

-la partie client est normalement installer par défaut : paquet openssh-client

-pour installer le serveur paquet openssh-server

2)configuration

-client : /etc/ssh/ssh_config

```
pi@raspberrypi:/etc/ssh $ cat ssh_config

# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information. This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
# 1. command line options
# 2. user-specific file
# 3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options. For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Include /etc/ssh/ssh_config.d/*.conf

Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
# Port 22
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
# UserKnownHostsFile ~/.ssh/known_hosts.d/%k
# SendEnv LANG LC_*
# HashKnownHosts yes
# GSSAPIAuthentication yes
```

-serveur : /etc/ssh/sshd_config

```
pi@raspberrypi:~$ cat /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

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

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

# 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 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```

repérer :

- port 22 port d'écoute par défaut
- permitRootLogin yes/no permet de se connecter directement en root (à déconseiller)
- X11Forwarding yes : pour autoriser les transmissions graphiques

pour lancer le serveur : service sshd start

connexion du client : ssh login@machine

```
PS C:\Windows\system32> ssh pi@10.100.30.47
pi@10.100.30.47's password:
Linux raspberrypi 5.10.63+ #1488 Thu Nov 18 16:14:04 GMT 2021 armv6l

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: Thu Dec  9 14:21:24 2021

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~$
```

III) le teste

Cette commande passe dans le Shell, ou PowerShell

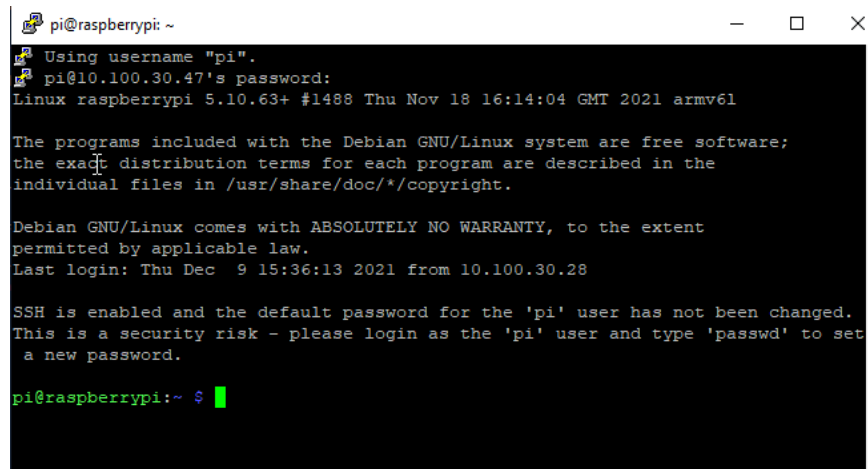
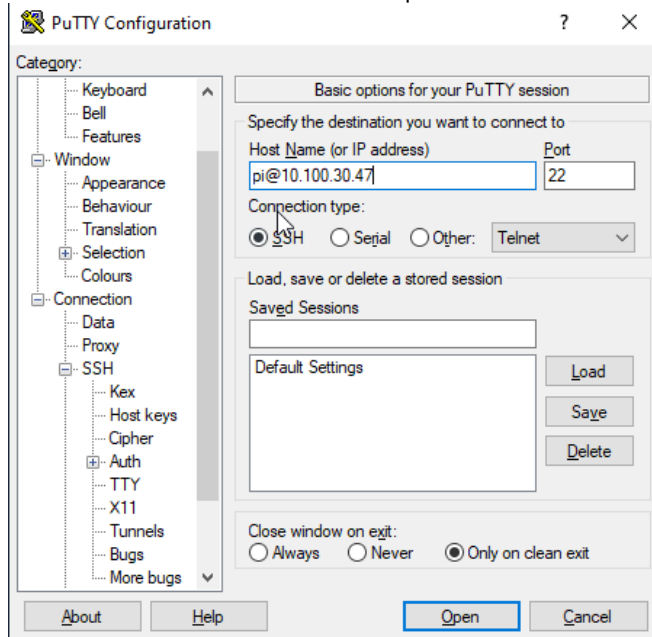
ssh pi@10.100.30.47

pour ouvrir le ssh en mode normal (Shell)

ssh -XC pi@10.100.30.47

pour ouvrir le ssh en mode graphique + (Shell)

connexion ssh depuis PuTTY



ensuite « yes »

Et pour finir entres votre mot de passe

sudo apt install ufw pour ajouter un fire-wall ➔ il bloquera les connexions suivre tuto fire-wall (bientôt)

Tester le transport de fichier par SSH

cp [options] [source] [destination]

cp /etc/ssh/mathias.html /var/www/html/

copie le fichier mathias.html qui se trouve dans /etc/ssh/ dans le dossier /var/www/html/

mv [source] [destination]

mv /etc/ssh/mathias.html /var/www/html

déplace le fichier mathias.html qui se trouve dans /etc/ssh/ dans le dossier /var/www/html/

SCP

- transfère de fichier
- récupérer tout un dossier
- transférer tout un dossier

scp [autres options] [nom d'utilisateur source@IP]:/[dossier et nom de fichier] [nom d'utilisateur de destination@IP]:/[dossier de destination]

en réel ça donne ça

-scp C:\Users\Mathias\Desktop\01.png vraica@192.168.0.63:/home/vraica/

Tunnel SSH

Il sert à chiffrer toutes les communications entre les deux machines

Exemple pour créer un tunnel ssh pour une connexion http du port 2021 au port 80

-ssh -L 2021 :IP_serveur :80 vraica@ip_serveur

Dans votre Navigateur : <http://localhost:2021>

