

Jérémie OBJOIS

Connexion entre un client et un serveur à l'aide de SSH

La présente procédure a pour but de montrer le processus de connexion entre un client et un serveur à l'aide du protocole SSH.

Table des matières

Section 1 : Mise en place de l'infrastructure	5
§1 : Mettre en place deux machines Debian 11 noms de code bullseye	5
§2 : Mettre à jour les deux machines debian11	5
§3 : Changer le nom des deux machines pour sshclient et sshserver	5
§4 : Installer le paquet openssh-client et openssh-server	5
A) Openssh-server sur le serveur sshserver	5
B) Openssh-client sur le serveur sshclient	6
§5 : Créer un utilisateur userserver sur le serveur sshserver et userclient sur le serveur sshclient	6
§6 : Exploration des fichiers de configuration	7
A) Sur le serveur ssh	7
B) Sur le serveur client	7
§7 : Connexion au serveur ssh, serveur client et Windows 10	7
A) Connexion au serveur ssh	7
B) Serveur Windows 2019, 2022 et Windows 10	8
1) Installer OpenSSH avec les Paramètres Windows	8
2) Démarrer et configurer OpenSSH Server	10
3) Connexion vers Windows 2019	11
4) Connexion vers serveur Linux	12
C) Votre machine physique Windows 10 (idem que Windows 2019)	12
Section 2 : création d'une identité numérique pour les comptes utilisateurs ssh en créant une paire de clés asymétrique	12
§1 : Création d'une identité numérique pour userclient en créant une paire de clés asymétrique sur sshclient	12
§2 : J'envoie la clé publique à userserver sur sshserver	13
§3 : Connexion au serveur ssh avec la Passphrase	14
Section 3 : Passphrase et agent SSH	14
§1 : Création d'une nouvelle instance bash	15
§2 : Charger la clé dans la mémoire de l'agent	15
§3 : Connexion ssh en utilisant l'agent ssh avec la Passphrase en mémoire	15
§4 : Autres options	16
Section 4 : Créations du fichier config	16
§1 : Créer le fichier config dans .ssh	16
§2 : Modifier le fichier config	16
§3 : Modifier le fichier hosts	17
Section 5 : La double authentification Google	17
Section 6 : Création d'une bannière	20
Section 7 : Connexion ssh avec une solution mobile	21





Introduction

(SSH) Secure Shell est un protocole de communication sécurisé. Ce protocole de connexion exige un échange de clés de chiffrement pour toutes connexions, tous les segments TCP sont **authentifiés et chiffrés**. Toute attaque de types *man-in-the-middle* (MITM)

Le protocole SSH a été conçu pour remplacer les différents protocoles non chiffrés comme rlogin, Telnet, rcp et rsh.

OpenSSH utilise la cryptographie* asymétrique comme mécanisme d'authentification. **OpenSSH gère les clés RSA**, les clés DSA et les clés DSA basées sur les courbes elliptiques. **OpenSSH reconnaît aussi les certificats X509** et les fichiers au format PKCS#12.

*La cryptographie sert principalement 3 objectifs :

- a- **La confidentialité**
- b- **L'authentification** (identification des partenaires, contrôle d'accès aux ressources et données, non-répudiation de l'origine de l'information)
- c- **L'intégrité des données** (données non altérées accidentellement ou frauduleusement lors du transfert ou sur place)

OpenSSH est, on l'a dit, une alternative à SSH. Il est également tout indiqué pour remplacer.

La principale différence entre OpenSSH et SSH est bien entendu le fait qu'OpenSSH soit libre. Il y a aussi quelques petites différences de configuration.

Modèle client/serveur :

- a- Comme tout protocole qui se respecte, OpenSSH est composé d'un serveur et d'un client
- b- Le serveur (sshd) écoute sur un port (22) par défaut. Pour une connexion entrante, il vérifie que c'est bien un client ssh qui est à l'autre bout, demande à l'utilisateur de s'identifier via une paire de clés asymétriques ou un mot de passe. Dans le premier cas, le serveur va lire un fichier de clés publiques (~/.ssh/authorized_keys) dans le répertoire home de l'utilisateur annoncé. S'il y trouve une clé ayant le même nom que celle proposée par le client, il va les vérifier par l'envoi d'un 'challenge' crypté avec la clé publique. Seule la clé privée pourra le décrypter, et elle renverra le challenge décrypté, prouvant que le client connaît la clé privée, mais sans jamais la dévoiler.

Dans le deuxième cas, le serveur vérifie que le mot de passe et le nom correspondent à un utilisateur de la machine. Cette méthode n'est utilisée que si la méthode par paire de clés a échoué. Le mot de passe étant lui-même crypté durant le transfert, il n'est pas possible de l'intercepter en clair. Si le client est autorisé, la machine locale est disponible en interactif, avec les droits de la personne entrée.

- c- Le client sert à se connecter au serveur. C'est lui qui choisit les algorithmes (et par là, la version du protocole). Si le serveur ne reconnaît pas l'algorithme demandé, c'est au client d'en proposer un autre.



- d- Certaines options peuvent être configurées des deux côtés, serveur et client. La règle qui prévaut alors est celle du 'Tout ce qui n'est pas interdit est autorisé'. Par exemple, le client autorisera les applications X-Windows à passer par le tunnel ssh, que si la configuration du serveur ne l'interdit pas expressément.



Section 1 : Mise en place de l'infrastructure

§1 : Mettre en place deux machines Debian 11 noms de code bullseye

Cloner deux machines à partir de la machine d'origine.

§2 : Mettre à jour les deux machines debian11

```
root@debian:~# apt update
root@debian:~# apt upgrade
```

§3 : Changer le nom des deux machines pour sshclient et sshserver

```
root@debian:~# hostnamectl set-hostname sshclient
root@debian:~# hostnamectl set-hostname sshserver
```

§4 : Installer le paquet openssh-client et openssh-server

A) Openssh-server sur le serveur sshserver

```
root@sshserver:~# apt install openssh-server -y
```

Vérification : on constate que le paquet openssh est installé

```
root@sshclient:~# dpkg -l openssh*
Souhait=inconnU/Installé/suppRimé/Purgé/H=à garder
| État=Non/Installé/fichier-Config/dépaqUeté/échec-config/H=semi-installé/W=attend-traitement-déclenchements
|/ Err?=(aucune)/besoin Réinstallation (État,Err: majuscule=mauvais)
||/ Nom Version Architecture Description
+++=-----+-----+-----+-----+
ii openssh-client 1:8.4p1-5 amd64 secure shell (SSH) client, for secure access to remote machines
un openssh-server <aucune> <aucune> (aucune description n'est disponible)
ii openssh-sftp-server 1:8.4p1-5 amd64 secure shell (SSH) sftp server module, for SFTP access from remote ma
un openssh-sk-helper <aucune> <aucune> (aucune description n'est disponible)
lines 1-9/9 (END)
```



B) Openssh-client sur le serveur sshclient

```
root@sshclient:~# apt install openssh-client -y
```

Vérification : on constate que le paquet openssh est installé

```
root@sshclient:~# dpkg -l openssh*
Souhait=inconnU/Installé/suppRimé/Purgé/H=à garder
| État=Non/Installé/fichier-Config/dépaqueté/échec-conFig/H=semi-installé/W=attend-traitement-déclenchements
|/ Err?=(aucune)/besoin Réinstallation (État,Err: majuscule=mauvais)
||/ Nom                Version             Architecture Description
+++=-----+-----+-----+-----+
ii openssh-client      1:8.4p1-5          amd64        secure shell (SSH) client, for secure access to remote machines
un openssh-server      <aucune>            <aucune>      (aucune description n'est disponible)
un openssh-sk-helper   <aucune>            <aucune>      (aucune description n'est disponible)
root@sshclient:~#
```

On vérifie que le service ssh est bien démarré

```
root@sshserver:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enable)
   Active: active (running) since Sat 2021-09-25 21:15:40 CEST; 18s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 2603 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 2604 (sshd)
    Tasks: 1 (limit: 2303)
   Memory: 1.1M
      CPU: 24ms
   CGroup: /system.slice/ssh.service
           └─2604 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

sept. 25 21:15:40 sshserver systemd[1]: Starting OpenBSD Secure Shell server...
sept. 25 21:15:40 sshserver sshd[2604]: Server listening on 0.0.0.0 port 22.
sept. 25 21:15:40 sshserver sshd[2604]: Server listening on :: port 22.
sept. 25 21:15:40 sshserver systemd[1]: Started OpenBSD Secure Shell server.
```

§5 : Créer un utilisateur userserver sur le serveur sshserver et userclient sur le serveur sshclient



§6 : Exploration des fichiers de configuration

A) Sur le serveur ssh

```
root@sshserver:~# ls -l /etc/ssh
total 608
-rw-r--r-- 1 root root 577771 13 mars 2021 moduli
-rw-r--r-- 1 root root 1650 13 mars 2021 ssh_config
drwxr-xr-x 2 root root 4096 13 mars 2021 ssh_config.d
-rw-r--r-- 1 root root 3289 13 mars 2021 sshd_config
drwxr-xr-x 2 root root 4096 13 mars 2021 sshd_config.d
-rw----- 1 root root 505 25 sept. 21:15 ssh_host_ecdsa_key
-rw-r--r-- 1 root root 176 25 sept. 21:15 ssh_host_ecdsa_key.pub
-rw----- 1 root root 411 25 sept. 21:15 ssh_host_ed25519_key
-rw-r--r-- 1 root root 96 25 sept. 21:15 ssh_host_ed25519_key.pub
-rw----- 1 root root 2602 25 sept. 21:15 ssh_host_rsa_key
-rw-r--r-- 1 root root 568 25 sept. 21:15 ssh_host_rsa_key.pub
```

Sshd_config : paire de clés identifiées

- **RSA** basé sur la factorisation des nombres premiers
- **ecdsa**
- **ed25519** basés sur les courbes elliptiques

```
#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
```

B) Sur le serveur client

On remarque qu'il existe juste un fichier et un répertoire

```
root@sshclient:~# ls /etc/ssh
ssh_config  ssh_config.d
root@sshclient:~#
```

§7 : Connexion au serveur ssh, serveur client et Windows 10

A) Connexion au serveur ssh

On se connecte toujours avec les comptes hébergés sur le serveur ssh et non les comptes locaux. Depuis le client sshclient on va établir une connexion ssh au serveur ssh.

```
root@sshclient:/etc/ssh# ssh userserver@192.168.44.152
The authenticity of host '192.168.44.152 (192.168.44.152)' can't be established.
ECDSA key fingerprint is SHA256:izZkTe4Q0Low872yX0Zf8e0S0W05behllq9fIj1S11g.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```



Le serveur ssh envoie sa clé publique ainsi que l'empreinte de cette clé

(On peut vérifier cette empreinte sur le serveur ssh avant d'accepter cette clé publique, après comparaison on remarque que les deux empreintes correspondent)

```
# ssh-keygen -l -E sha256 -f ssh_host_ecdsa_key.pub
root@sshserver: /etc/ssh# ssh-keygen -lv -f sha256 -f ssh_host_ecdsa_key.pub
256 SHA256:izZkTe4Q0Low872yX0Zf8e0S0W05behllq9fIj1S11g root@sshserver (ECDSA)
+---[ECDSA 256]---+
|
| ..
| ..
| .. . . +E|
| + . = o.**|
| = o+ S . *oX|
| oo.= o . + O.|
| +.= , o * +|
| ...+ o =.|
| .+ . ...|
+---[SHA256]-----+
```

On trouve cette clé dans le fichier `/root/.ssh/known_hosts` on peut afficher cette clé

```
root@sshclient: ~/.ssh# cat known_hosts
|1|dkwRRR3fLLuNpbFHD3Agg0kiPc=|h0ifiUKMM0sHr5/fskD66sVJtAY= ecdsa-sha2-nistp256 AA
AAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBmDcokbIMrWStT4pMdxzfzJJet+Xkindg
MubfqLVEO782dAZGDNF7d+YqzLoEGWqTE231QRmTRC/4VJUCuQNYzi=
```

- B) Serveur Windows 2019, 2022 et Windows 10
- 1) Installer OpenSSH avec les Paramètres Windows

Les deux composants OpenSSH client et serveur doivent être installés.

- a) Pour installer les composants OpenSSH graphiquement
 1. Ouvrez **Paramètres**, sélectionnez **Applications > Applications et fonctionnalités**, puis **Fonctionnalités facultatives**.
 2. Parcourez la liste pour voir si OpenSSH est déjà installé. Si ce n'est pas le cas, sélectionnez **ajouter une fonctionnalité** en haut de la page, puis :
 - Recherchez **OpenSSH Client** et cliquez sur **Installer**.
 - Recherchez **OpenSSH Server** et cliquez sur **Installer**.

Une fois l'installation terminée, revenez à **Applications > Applications et fonctionnalités** et **Fonctionnalités facultatives**. Vous devriez voir OpenSSH dans la liste.



	Client OpenSSH	5,05 Mo
	Serveur OpenSSH	4,71 Mo

On peut installer ssh en ligne de commande sur un power shell

b) Installation d'OpenSSH en ligne de commande

Ouvrez le PowerShell en tant qu'administrateur. Pour s'assurer qu'OpenSSH est disponible, exécutez l'applet de commande suivante :

`Get-WindowsCapability -Online | ? Name -like 'OpenSSH*'`

Installation des composants serveur ou client :

```
# Install the OpenSSH Client
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0

# Install the OpenSSH Server
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

Quel que soit le composant, la sortie suivante devrait être retournée :



2) Démarrer et configurer OpenSSH Server

Pour la première utilisation de ssh, ouvrez PowerShell en tant qu'administrateur, il faut exécuter les commandes suivantes pour démarre

démarrer le service sshd

Start-Service sshd

configurer un démarrage automatique du service sshd:

Set-Service -Name sshd -StartupType 'Automatic'

Il faut désactiver le firewall ou il faut le configurer pour le configurer il faut suivre les étapes suivantes

autorisez ssh sur le firewall.

Get-NetFirewallRule -Name *ssh*

la règle suivante doit être activée "OpenSSH-Server-In-TCP", si cette règle n'existe pas il faut la créer

New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22

On vérifie l'installation, on remarque les mêmes fichiers que sur Linux

```
PS C:\> cd .\ProgramData\ssh\
PS C:\ProgramData\ssh> dir

Répertoire : C:\ProgramData\ssh

Mode                LastWriteTime         Length Name
----                -
d-----          26/09/2021      11:21             logs
-a-----          26/09/2021      11:21              6 sshd.pid
-a-----          05/09/2018      15:07      2253 sshd_config
-a-----          26/09/2021      11:21      668 ssh_host_dsa_key
-a-----          26/09/2021      11:21      622 ssh_host_dsa_key.pub
-a-----          26/09/2021      11:21      227 ssh_host_ecdsa_key
-a-----          26/09/2021      11:21      194 ssh_host_ecdsa_key.pub
-a-----          26/09/2021      11:21      432 ssh_host_ed25519_key
-a-----          26/09/2021      11:21      114 ssh_host_ed25519_key.pub
-a-----          26/09/2021      11:21      1675 ssh_host_rsa_key
-a-----          26/09/2021      11:21      414 ssh_host_rsa_key.pub
```

Dans system32 le dossier openssh regroupe toutes les commandes ssh

```
PS C:\Windows\System32\OpenSSH> ls

Répertoire : C:\Windows\System32\OpenSSH

Mode                LastWriteTime         Length Name
----                -
-a-----          05/09/2018      17:07      322560 scp.exe
-a-----          05/09/2018      15:07      322048 sftp-server.exe
-a-----          05/09/2018      17:07      390144 sftp.exe
-a-----          05/09/2018      17:07      491520 ssh-add.exe
-a-----          05/09/2018      17:07      384512 ssh-agent.exe
-a-----          05/09/2018      17:07      637952 ssh-keygen.exe
-a-----          05/09/2018      17:07      530432 ssh-keyscan.exe
-a-----          05/09/2018      15:07      149504 ssh-shellhost.exe
-a-----          05/09/2018      17:07      882688 ssh.exe
-a-----          05/09/2018      15:07      974336 sshd.exe
-a-----          05/09/2018      15:07      2253 sshd_config_default
```



3) Connexion vers Windows 2019

Avant il faut créer un utilisateur **userw19** avec **Azerty123** comme mot de passe.

Nom	Nom complet	Description
Administrat...		Compte d'utilisateur d'administra...
bendi		
DefaultAcco...		Compte utilisateur géré par le syst...
Invité		Compte d'utilisateur invité
sshd	sshd	
userw19	userw19	

```
root@sshclient:~# ssh userw19@192.168.44.145
The authenticity of host '192.168.44.145 (192.168.44.145)' can't be established.
ECDSA key fingerprint is SHA256:D4axPeJ5a0v10T0+hIQnJUVZotXaJxYFsdWbvcA0hXQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

On peut lancer une console powershell à partir de cet endroit :

```
userw19@SSH-W-2019 C:\Users\userw19>
```

On peut vérifier comme auparavant l'envoi de la clé publique par le serveur ssh Windows au serveur Linux sshclient

Sur sshclient

```
root@sshclient:~/.ssh# cat known_hosts
|1|/dkwRRR3fLLuNpbFHd3Agq0kiPc=|h0ifiUKMM0sHr5/fskD66sVJtAY= ecdsa-sha2-nistp256 AA
AAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBMDcokbIMrWStT4pMdxFzjJet+xkindg
MUbfaLVE078ZdAZGDNF7d+YqzLoEGWqTE231ORmTRC/4VJUCuONYzI=
|1|iAnhWgWTAzd4hKvO6uLmstOu+kY=|Vz8CyJFgZF4n8RvT6UjNPuweDXk= ecdsa-sha2-nistp256 AA
AAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBANG/HxgTba9d/+4POe+vMDGuxnQWcxrX
G5w0HF3gK1AEuGwWksXddyKVT62bWagS6VPzoeY5LbRqgduos/FYhY=
root@sshclient:~/.ssh#
```

Sur w2019

```
PS C:\ProgramData\ssh> cat .\ssh_host_ecdsa_key.pub
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBANG/HxgTba9d/+4POe+
vMDGuxnQWcxrXG5w0HF3gK1AEuGwWksXddyKVT62bWagS6VPzoeY5LbRqgduos/FYhY= autorite nt\systÃme@ss
h-w-2019
PS C:\ProgramData\ssh>
```

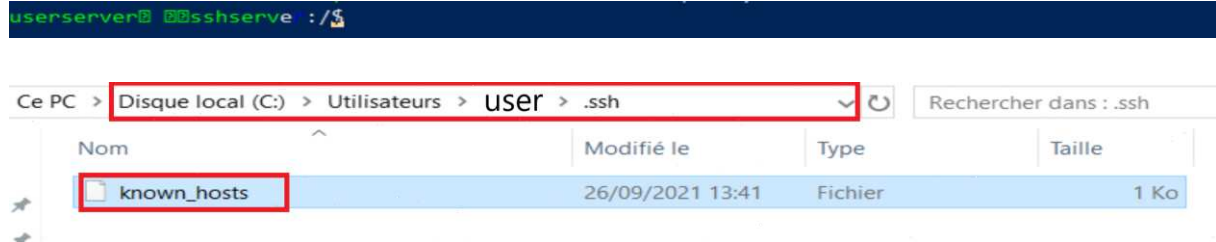
On remarque que c'est la même clé.



4) Connexion vers serveur Linux

```
Windows PowerShell
PS C:\> ssh userserver@192.168.44.152
The authenticity of host '192.168.44.152 (192.168.44.152)' can't be established.
ECDSA key fingerprint is SHA256:PuHV+MhVrRqd1E2AzJ2jDB0ThrkUXpQwbEpPKrWniAU.
Are you sure you want to continue connecting (yes/no)?
```

Le serveur ssh a envoyé sa clé publique



C) Votre machine physique Windows 10 (idem que Windows 2019)

Section 2 : Création d'une identité numérique pour les comptes utilisateurs ssh en créant une paire de clés asymétrique

§1 : Création d'une identité numérique pour userclient en créant une paire de clés asymétrique sur sshclient

Création d'une paire de clés asymétrique la clé **privée** est protégée par un **mot de passe**

```
root@sshclient:~# ssh-keygen -t rsa -b 1024 -f /home/userclient/uc_rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/userclient/uc_rsa
Your public key has been saved in /home/userclient/uc_rsa.pub
The key fingerprint is:
SHA256:EZiQntPh2rpv4Wg5ytNSaQb0zQFao4FFaLGFNhk0qAI root@sshclient
The key's randomart image is:
+---[RSA 1024]-----+
|+XB=. .|.
|EBO o...|
|*+0000..|
|o.=.+o .|
|...*. S|
|. =o|
|==|
|.0*.o|
|.++=|
+---[SHA256]-----+
```



Je vérifie la création de la paire de clés

```
root@sshclient:~# ls /home/userclient/
uc_rsa  uc_rsa.pub
```

J'affiche la clé privée

```
userclient@sshclient:~$ cat uc_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDZelRmg2
KxpLKVuOER+WsEAAAAEAAAAEAAACXAAAB3NzaC1yc2EAAAADAQABAAQgQDdKVWtmNOC
WpBq4oMLbEqsFAES+ZDvDhdBHzYXW1vUT+U/Xg5RgrjSJKFH3GZ3Ie9MHznwZv4uXzRGg9
hcrvzMtIdJbDpZpjK8Z6pPhW71W9u8NJqERfidoh//7M6+v/f0XDxkrIJtT3yXnuGHuLf8
OSYJRrXmNa3YP+J2SgFwQwAAAhDg3VDRhbrbrup/AA/LnrLjuhQjinpG0JxRPK4ZLo8u9k
NakQbtanU62cd7QicFxnNYPjofSyKCTZRCC/6vrxaQL0yuWw+YU0jd9qpZSF5Q+4D6dANj
or1VOQ0ptwxwEWA98YpfJOxWpgQsNPWx+tXyK1zgX40ZxRxrUuQLHX6oKSDXAVcjkI+YHf
HPuPVarH59QEYqBzep06HQxdhjteZnN1hFGsaJobT9BF2LbXr+mIBY/Gdgb+TOyLPtzzcK
YASH7imzyc7xL9ufnVZ4h5FK9chxbrz2Q9mZb25CyF5ryJpqtB7cRDdnEA1ID8MLgqyAZV
0mrOhLD3LS9Dx7FJqiTY1ewqTpp3JvDGGVlWdZ0PVPwVSG45hPNk01Fqp6rmmZeeRGg3ny
pNTk+ftXAaZN0Z8DcjIGKmZLz7zpCooPuZw8b390ZI44YuhH/1EehXuZGq80DzoEjY01ch
27IHRFshpBzeJIKs1+Y4zfVGAkKLnP/w9cmjicodXS60sPx1277UTWT9tOCqND02G7wpv2
hjtZ7uIleJ8N7Uw9ZtmBHM/v7NXX4pDXauxLzMMUlyW8+84suinWpAKaNIjcx5kpz1t28t
S5yMZVlsakrhka+2fG52T0d0/9GwmKtsjY3Q4H0T8/UCyeYdvkgqmpHayy6+p3s3hrdbe5
ck9xBYCfPBCIXJkDhfnrFbCHCcPrhpq=
-----END OPENSSH PRIVATE KEY-----
```

J'affiche la clé publique

```
userclient@sshclient:~$ cat uc_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDdKVWtmNOCWpBq4oMLbEqsFAES+ZDvDhdBHzYXW1vUT+U/Xg5RgrjSJKFH3GZ3Ie9
MHznwZv4uXzRGg9hcrvzMtIdJbDpZpjK8Z6pPhW71W9u8NJqERfidoh//7M6+v/f0XDxkrIJtT3yXnuGHuLf8OSYJRrXmNa3YP+J2Sg
FwQw== userclient@sshclient
userclient@sshclient:~$
```

Je vérifie l'empreinte numérique de ma clé publique

```
root@sshclient:~# ssh-keygen -l -E sha256 -f /home/userclient/uc_rsa.pub
1024 SHA256:EZIQntPh2rpv4Wg5ytNSaQb0zQFao4FFaLGFNhk0qAI root@sshclient (RSA)
```

§2 : J'envoie la clé publique à userserver sur sshserver

```
userclient@sshclient:~$ ssh-copy-id -i uc_rsa.pub userserver@192.168.44.152
```

```
userclient@sshclient:~$ ssh-copy-id -i uc_rsa.pub userserver@192.168.44.152
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "uc_rsa.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
userserver@192.168.44.152's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'userserver@192.168.44.152'"
and check to make sure that only the key(s) you wanted were added.
```



On vérifie sur le serveur sshserver si la clé publique est envoyée, elle doit être stocker dans le répertoire personnel de l'utilisateur userserver.

```
userserver@sshserver:~$ pwd
/home/userserver
userserver@sshserver:~$ ls -a
. . . .bash_aliases .bash_history .bash_logout .bashrc .config .profile .ssh .viminfo
userserver@sshserver:~$ ls .ssh
authorized_keys
userserver@sshserver:~$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDdKVWtmNOCWpBq4oMLbEqsFAES+ZDvDhdBHzyXW1vUT+U/Xg5RgrjSJKFH3GZ3Ie9
MHznwZv4uXzRGg9hcrvzMtIdJbDpZpjK8Z6pPhW71W9u8NJqeRfidoh//7M6+v/f0XDxkrIJtT3yXnuGHuLf80SYJRrXmNa3YP+J2Sg
FwQw== userclient@sshclient
userserver@sshserver:~$
```

On remarque qu'elle correspond à celle affichée précédemment sur le serveur sshclient.

§3 : Connexion au serveur ssh avec la Passphrase

Je me connecte en ssh sur sshserver avec le compte sshserver ; la machine distante va remarquer qu'elle possède la clé publique attachée à mon compte elle va m'envoyer un message chiffré (challenge) je le déchiffre le message et je l'envoie je prouve que j'ai en ma possession la clé privée donc je certifie mon identité dans le cas contraire je ne pourrais pas me connecter

```
userclient@sshclient:~$ ssh -i uc_rsa userserver@192.168.44.152
Enter passphrase for key 'uc_rsa': useruc
```

Section 3 : Passphrase et agent SSH

Ssh-agent est un outil coté client ; **Ssh-agent** permet de **rajouter dans la mémoire** de mon agent ma clé privée tout en-déverrouillant-la clé privée pendant un certain temps.
La commande ssh-add permet de charger la clé privée en mémoire.

```
root@server1:~# man ssh-add
```

SSH-ADD(1)	BSD General Commands Manual	SSH-ADD(1)
NAME		
ssh-add - adds private key identities to the OpenSSH authentication agent		
SYNOPSIS		
ssh-add [-cDdKkLlqvXx] [-E fingerprint_hash]		
[-S provider] [-t life] [file ...]		
ssh-add -s pkcs11		
ssh-add -e pkcs11		
ssh-add -T pubkey ...		

L' **agent** est un programme qui garde les clés en mémoire afin de les déverrouiller *qu'une seule fois*.



Il y'a deux méthodes pour démarrer *ssh-agent* :

- a- **eval `ssh-agent`**- cela exécute l'agent en arrière-plan et définit les variables d'environnement appropriées pour l'instance de shell *actuelle* .
- b- **exec ssh-agent bash**- démarre une *nouvelle* instance du bashshell, en remplaçant l'actuelle.

La deuxième méthode est parfois préférée, car elle arrête automatiquement *ssh-agent* lorsqu'on arrête la session.

Après il faut utiliser *ssh-add* , pour déverrouiller les clés et les associés à l'agent, les connexions *ssh*, *scp*, *sftp* ... pourront tirer profit de cette méthode afin de simplifier les connexions.

§1 : Création d'une nouvelle instance bash

exec *ssh-agent bash*- démarre une *nouvelle* instance du bashshell, en remplaçant l'actuelle.

```
userclient@sshclient:~$ exec ssh-agent bash
```

§2 : Charger la clé dans la mémoire de l'agent

Utiliser *ssh-add* , déverrouille les clés (généralement *~/.ssh/id_**) et les charge dans l'agent, les rendant accessibles aux connexions *ssh* ou *sftp* .

```
userclient@sshclient:~$ ssh-add uc_rsa
Enter passphrase for uc_rsa: useruc
Identity added: uc_rsa (userclient@sshclient)
userclient@sshclient:~$
```

Pour vérifier, on peut lister les clés en mémoire.

```
userclient@sshclient:~$ ssh-add -l
1024 SHA256:sJNv70kVxqI2+m1pZagLgQsJaeOtE2ZoAtujOMQOmFg userclient@sshclient (RSA)
```

§3 : Connexion ssh en utilisant l'agent ssh avec la Passphrase en mémoire

Je me connecte en ssh on me demande plus la clé passphrase

```
userclient@sshclient:~$ ssh -i uc_rsa userserver@192.168.44.152
```



§4 : Autres options

Si je veux effacer des clés en mémoire de l'agent ssh

```
userclient@sshclient:~$ ssh-add -d uc_rsa  
Identity removed: uc_rsa RSA (userclient@sshclient)  
userclient@sshclient:~$ ssh-add -l  
The agent has no identities.  
userclient@sshclient:~$
```

Mémoriser la clé pour une durée limitée

```
userclient@sshclient:~$ ssh-add -t 60 uc_rsa  
Enter passphrase for uc_rsa:  
Identity added: uc_rsa (userclient@sshclient)  
Lifetime set to 60 seconds  
userclient@sshclient:~$
```

Après 60 secondes la clé est effacée de la mémoire de l'agent

```
userclient@sshclient:~$ ssh-add -l  
The agent has no identities.
```

Section 4 : Créations du fichier config

§1 : Créer le fichier config dans .ssh

```
userclient@sshclient:~$ cd .ssh  
userclient@sshclient:~/.ssh$ touch config  
userclient@sshclient:~/.ssh$ ls  
config known_hosts
```

§2 : Modifier le fichier config

```
userclient@sshclient:~/.ssh$ vim config |  
  
host sshserver  
    user userserver  
    port 22  
    identityfile /home/userserver/uc_rsa
```



§3 : Modifier le fichier hosts

```
root@sshclient:~# vim /etc/hosts
127.0.0.1    localhost
127.0.1.1    sshclient
192.168.44.152 sshserver

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

Maintenant on peut se connecter sur notre serveur

```
userclient@sshclient:/root$ ssh sshserver
```

Section 5 : La double authentification Google

On commence par installer le paquet **libpam-google-authenticator** sur le serveur ssh.

```
root@sshserver:~# apt install libpam-google-authenticator
```

On modifie le fichier sshd dans le dossier /etc/pam.d/

```
root@sshserver:~# vim /etc/pam.d/sshd
#Authentication Google
auth required pam_google_authenticator.so
```

On modifie aussi le fichier sshd_config dans /etc/ssh/

```
root@sshserver:/etc/ssh# vim sshd_config
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication yes
```

On redémarre le service sshd.

En même temps on vérifie si le service a bien redémarré.



```
root@sshserver: /etc/ssh# service sshd restart
root@sshserver: /etc/ssh# service sshd status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-09-26 20:24:22 CEST; 13s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 6911 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 6912 (sshd)
    Tasks: 1 (limit: 2303)
   Memory: 1.1M
      CPU: 29ms
   CGroup: /system.slice/ssh.service
           └─6912 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

sept. 26 20:24:22 sshserver systemd[1]: Starting OpenBSD Secure Shell server...
sept. 26 20:24:22 sshserver sshd[6912]: Server listening on 0.0.0.0 port 22.
sept. 26 20:24:22 sshserver sshd[6912]: Server listening on :: port 22.
sept. 26 20:24:22 sshserver systemd[1]: Started OpenBSD Secure Shell server.
```

On lance google-authenticator

```
root@sshserver: /etc/ssh# google-authenticator
Do you want authentication tokens to be time-based (y/n) y|
```





Sur le smartphone il faut télécharger sur le store l'application



Authenticator

Synchronisation automatique

Il faut d'abord installer les paquets ntp et ntpdate avec la commande suivante

```
root@server1:~# apt install ntp ntpdate
```

Il faut configurer NTP, on peut utiliser :

- Serveurs NTP du projet **pool.ntp.org** (pour la France, les serveurs NTP à utiliser sont : **server 0.fr.pool.ntp.org server 1.fr.pool.ntp.org server 2.fr.pool.ntp.org**)

Donc on va modifier le fichier /etc/ntp.conf et de remplacer les lignes correspondantes aux adresses des serveurs NTP par celles ci-dessus.

On peut régler l'heure manuellement avec la commande suivante :



```
root@server1:~# ntpdate pool.ntp.org
8 Oct 18:45:44 ntpdate[1920]: adjust time server 45.33.84.208 offset -0.021789 sec
```

On vérifie si le service ntp est démarré

```

root@server1:~# service ntp status
● ntp.service - Network Time Service
   Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-10-08 18:49:03 CEST; 27s ago
     Docs: man:ntpd(8)
  Process: 1930 ExecStart=/usr/lib/ntp/ntp-systemd-wrapper (code=exited, status=0/SUCCESS)
    Main PID: 1936 (ntpd)
      Tasks: 2 (limit: 2303)
     Memory: 948.0K
        CPU: 41ms
    CGroup: /system.slice/ntp.service
            └─1936 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 106:112

oct. 08 18:49:05 server1 ntpd[1936]: Soliciting pool server 95.81.173.155
oct. 08 18:49:05 server1 ntpd[1936]: Soliciting pool server 37.187.105.73
oct. 08 18:49:06 server1 ntpd[1936]: Soliciting pool server 129.250.35.251
oct. 08 18:49:06 server1 ntpd[1936]: Soliciting pool server 162.159.200.1
oct. 08 18:49:07 server1 ntpd[1936]: Soliciting pool server 212.83.179.156
oct. 08 18:49:07 server1 ntpd[1936]: Soliciting pool server 162.159.200.123
oct. 08 18:49:07 server1 ntpd[1936]: Soliciting pool server 80.74.64.2
oct. 08 18:49:08 server1 ntpd[1936]: Soliciting pool server 51.255.197.148
oct. 08 18:49:09 server1 ntpd[1936]: Soliciting pool server 78.196.167.192
oct. 08 18:49:10 server1 ntpd[1936]: Soliciting pool server 92.243.6.5
root@server1:~#

```

Section 6 : Création d'une bannière

Le but est d'avoir une bannière d'accueil au cours de notre connexion Ssh

Pour réaliser cette bannière, il faut :

- a- Créer un fichier qui va présenter cette bannière on peut lui donner le nom qu'on veut dans notre cas je lui ai donné le nom de banner

[illegible]

- b- Il faut renseigner le chemin du fichier banner dans `sshd_config`

```
root@server1:/etc/ssh# vim sshd_config
```

```
# no default banner path
Banner /root/banner
```



Section 7 : Connexion ssh avec une solution mobile

Maintenant on va essayer d'accéder à notre serveur ssh à partir de l'extérieur en utilisant notre adresse publique.


Tout d'abord :

Attention mettez votre machine en bridge au lieu du Nat

- 1- Il faut accéder à la boxe internet et ouvrir le port 22 en créant une redirection de port

Service	Adresse IP du serveur	Protocole	Ports externes	Ports internes	Activer la règle
Utilisateur					
SSH	192.168.1.250	TCP/UDP	22 • 22	22 • 22	on
Activer UPnP <input type="checkbox"/>					
Règles actives UPnP v4 2					
NAT for STB 6035C0EBE710 port STBCONTROL	192.168.1.150	TCP	1290 • 1290	8000 • 8000	on
NAT for STB 6035C0EBE6D4 port STBCONTROL	192.168.1.137	TCP	1291 • 1291	8000 • 8000	on

- 2- Ensuite il faut déterminer notre adresse publique soit à partir de la boxe ou un site internet <http://www.whatismyip.com>

- 3- Après sur notre smartphone on télécharge un client ssh sur  google store **Juicessh**



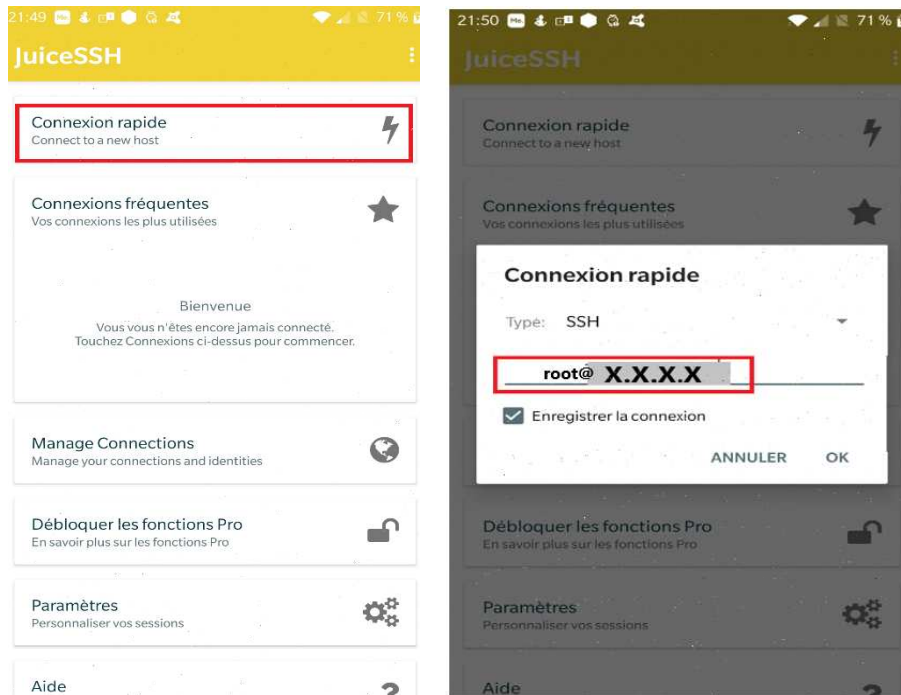
JuiceSSH - SSH Client

- 4- Sur notre smartphone il faut qu'on se mette en 4G et non en wifi.
On peut effectuer cette procédure en wifi sur notre smartphone et non en 4G.
- 5- On ouvre l'application et on commence à établir notre connexion ssh

On sélectionne connexion rapide

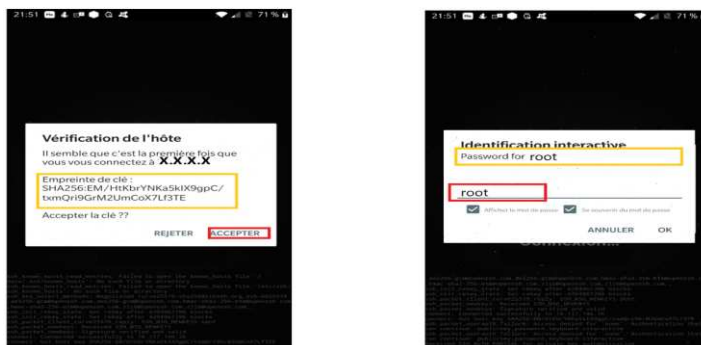
ssh root@ adresse publique





Le serveur nous envoie l'empreinte de sa clé publique
On constate que c'est la même que celle qu'on a calculée
Sur le serveur

EM/HtKbrYNKa5kIX9gpC/txmQri9GrM2UmCoX7Lf3TE rentre le mot de
passe root



Après on tombe sur notre console VMWare



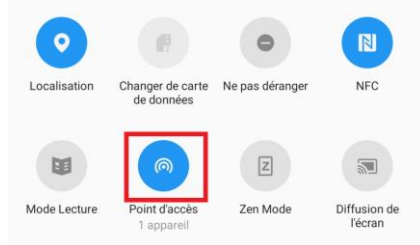
```

16:23
root@server:~# ip ad
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
        valid_lft forever preferred_lft forever
2: ens13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f7:2e:20 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.136/24 brd 192.168.1.255 scope global dynamic ens33
        valid_lft 60792sec preferred_lft 60792sec
    inet6 fe80::20c:29ff:fe77:2e20/64 scope link
        valid_lft forever preferred_lft forever
root@server:~#

```

a- Connexion avec un partage de connexion 4G

- Faites un partage de connexion à partir de votre smartphone



- Connectez-vous en wifi sur votre machine physique en utilisant le wifi correspondant au partage de connexion de votre smartphone
- Mettez votre serveur SSH en Bridge pour avoir une adresse IP du même réseau que la machine physique et le smartphone
- Installez un terminal sur le smartphone :

Exemple de terminal :



- Relevez l'adresse IP smartphone, machine physique et la VM serveur SSH

IP du smartphone : 192.168.43.234 /24

```

12:25
$ ip ad
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
        valid_lft forever preferred_lft forever
26: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 3000
    link/ether da:7e:ff:f6:a7:79 brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.234/24 brd 192.168.43.255 scope global wlan0
        valid_lft forever preferred_lft forever
    inet6 fe80::d87e:ffff:fef6:a779/64 scope link
        valid_lft forever preferred_lft forever

```

IP de la machine physique : 192.168.43.197 /24

```

(root@ETANIUM)-[~]
# ip ad

```




```
22: wifio: <BROADCAST,MULTICAST,UP> mtu 1500 group default qlen 1
    link/ieee802.11 f8:16:54:2b:40:f8
    inet 192.168.43.197/24 brd 192.168.43.255 scope global dynamic
        valid_lft 2341sec preferred_lft 2341sec
    inet6 fe80::3410:fa32:28b6:999a/64 scope link dynamic
        valid_lft forever preferred_lft forever

22: wifio: <BROADCAST,MULTICAST,UP> mtu 1500 group default qlen 1
    link/ieee802.11 f8:16:54:2b:40:f8
    inet 192.168.43.197/24 brd 192.168.43.255 scope global dynamic
        valid_lft 2341sec preferred_lft 2341sec
    inet6 fe80::3410:fa32:28b6:999a/64 scope link dynamic
        valid_lft forever preferred_lft forever
```

IP de la machine VM serveur SSH : 192.168.43.122 /24

```
root@server1:~# ip ad
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
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f7:2e:20 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.43.122/24 brd 192.168.43.255 scope global dynamic ens33
        valid_lft 3207sec preferred_lft 3207sec
    inet6 fe80::20c:29ff:fef7:2e20/64 scope link
        valid_lft forever preferred_lft forever
```

- Faite un test de ping entre smartphones, machine physique et la VM serveur SSH
Smartphone à Machine physique

```
13:40 $ ping 192.168.43.197
PING 192.168.43.197 (192.168.43.197) 56(84) bytes of data:
64 bytes from 192.168.43.197: icmp_seq=1 ttl=128 time=15.8 ms
64 bytes from 192.168.43.197: icmp_seq=2 ttl=128 time=5.17 ms
```

Smartphone à Serveur SSH

```
13:37 $ ping 192.168.43.122
PING 192.168.43.122 (192.168.43.122) 56(84) bytes of data:
64 bytes from 192.168.43.122: icmp_seq=1 ttl=64 time=5.11 ms
64 bytes from 192.168.43.122: icmp_seq=2 ttl=64 time=14.5 ms
```

- Utilisez maintenant votre application client SSH sur votre smartphone pour se connecter la VM serveur SSH, avec IP ad on vérifie bien qu'on est sur le serveur ssh



```

15:20 [system icons] 35%
root@server:~# ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noque
ue 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
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 150
0 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f7:2e:20 brd ff:ff:ff:ff:ff:ff
    ff
    altname enp2s1
    inet 192.168.43.122/24 brd 192.168.43.255 scope
global dynamic ens33
        valid_lft 3180sec preferred_lft 3180sec
    inet6 fe80::20c:29ff:fef7:2e20/64 scope link
        valid_lft forever preferred_lft forever
root@server:~#

```

B- Les Ports de communication:

Un numéro de port est codé sur 16 bits, ce qui fait qu'il existe un maximum de 2^{16} , soit **65 536** ports distincts par machine. Ces ports sont classés en 3 catégories en fonction de leur numéro:

- Les numéros de port de 0 à 1 023 correspondent aux ports "bien connus" (**well-known ports**), utilisés pour les services réseau les plus courants.
- sous Windows, ce fichier est dans **C:\Windows\System32\drivers\etc**

Disque local (C:) > Windows > System32 > drivers > etc

Nom	Modifié le	Type	Taille
hosts	09/10/2021 22:20	Fichier	2 Ko
hosts	16/10/2021 15:13	Fichier iCalendar	1 Ko
lmhosts.sam	07/12/2019 10:12	Fichier SAM	4 Ko
networks	29/09/2017 15:44	Fichier	1 Ko
protocol	29/09/2017 15:44	Fichier	2 Ko
services	29/09/2017 15:44	Fichier	18 Ko

- Sous Linux le fichier `services` indiquant la liste des services dits well-known, est dans `/etc` ;

```
root@server1:/etc# ls services
services
```

- les numéros de ports de 1 024 à 49 151 correspondent aux ports enregistrés (registered ports), assignés par l'IANA
- les numéros de ports de 49 152 à 65 535 correspondent aux ports dynamiques, utilisables pour tout type de requêtes TCP ou UDP autres que celle citée précédemment.

Lorsqu'un logiciel client veut dialoguer avec un logiciel serveur, aussi appelé service, il a besoin de connaître le port écouté par ce dernier. Les ports utilisés par les services devant être connus par les clients, les principaux types de services utilisent des ports qui sont dits réservés. Par convention, ce sont tous ceux compris entre 0 et 1 023 inclus et leur utilisation par un logiciel



serveur nécessite souvent que celui-ci s'exécute avec des droits d'accès particuliers. Les services utilisant ces ports sont appelés les services bien connus ("Well-Known Services").

Le fichier services indique la liste de ces services dits well-known. Sous UNIX, ce fichier est directement dans /etc ; sous Windows, ce fichier est par défaut dans C:\Windows\System32\drivers\etc. Les services les plus utilisés sont :

Toutefois, ces conventions ci-dessus peuvent ne pas être respectées pourvu que le client et le serveur soient cohérents entre eux et que le nouveau numéro choisi ne soit pas déjà utilisé. Pour afficher les ports on utilise netstat

```
#netstat -paunt
```

- -a : Tous les ports
- -t : Tous les ports TCP
- -u : Tous les ports UDP
- -l : Tous les ports en écoute
- -n : Affiche directement les IP. Pas de résolution de nom.
- -p : Affiche le nom du programme et le PID associés.

