

Hanah SAHMOUNE



DÉPARTEMENT INFORMATIQUE

Installation de Services Réseau

Sommaire

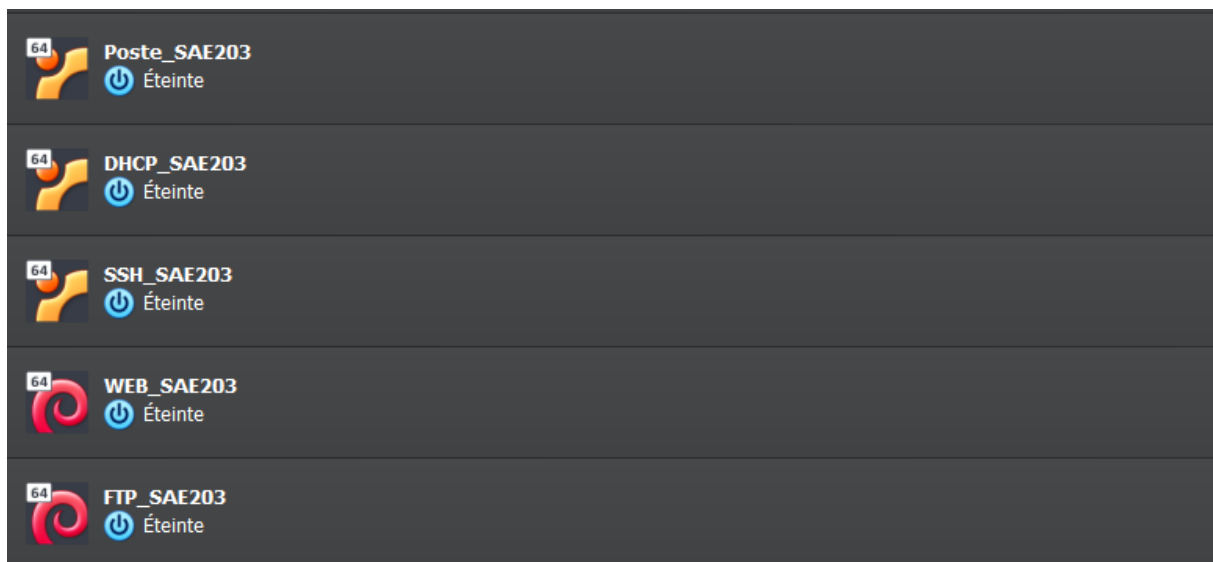
Table des matières

3 – Cahier des charges :	3
3.1 Généralités	3
3.2 Serveur DHCP	4
1/ Installation	5
3.3 Serveur SSH	8
Adressage IP dynamique et réservé	8
Admin peut se connecter en SSH via clef publique depuis l'extérieur	10
L'utilisateur admin a sa durée de connexion SSH.....	13
Invoquer la commande sudo sans mettre le mot de passe :	14
L'utilisateur « bastion » du SSH est le seul utilisateur pouvant se connecter aux autres VM.....	15
3.4 Serveur Web.....	16
Adresse IP dynamique et réservée :	16
Reprise du CDC de R2.05.....	16
Déploiement de la configuration sur une Debian CLI avec accès à internet.....	20
3.5 FTP	21
Adressage IP dynamique et réservé	21
Les utilisateurs peuvent se connecter avec leur identifiant	22
L'accès est en lecture/écriture sauf pour le compte « anonymous » qui est en lecture seule	22
Les utilisateurs peuvent déposer et télécharger leurs fichiers en SFTP sans taper leur mot de passe (authentification par clé publique)	23
3.6 Poste de travail	23

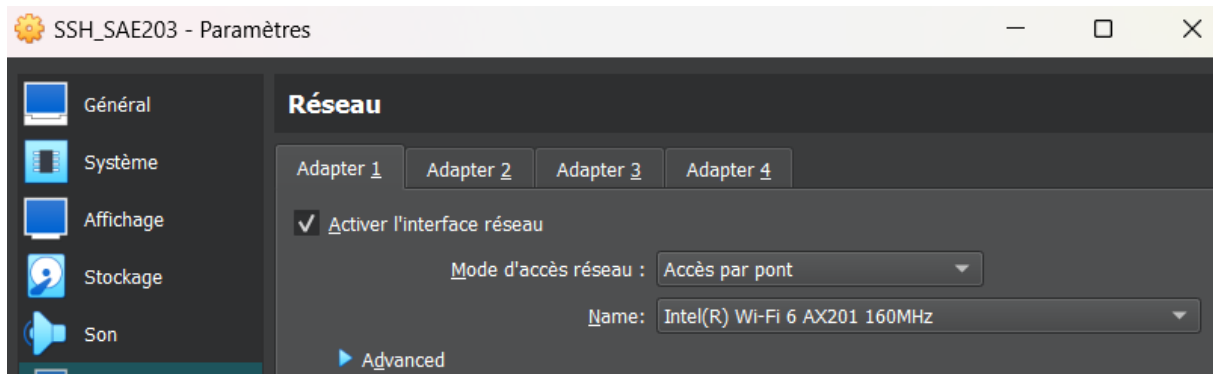
3 – Cahier des charges :

3.1 Généralités

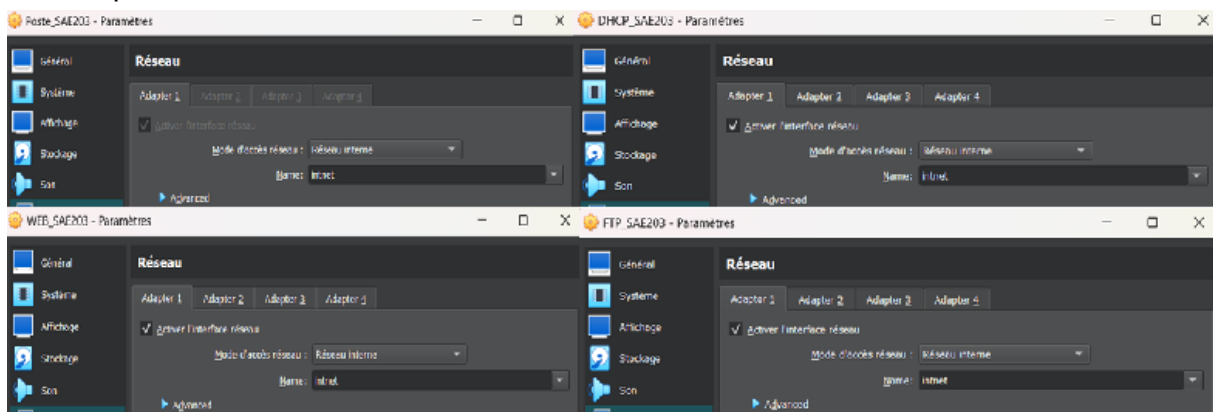
Tous les ordinateurs de la maquette sont bels et biens des Machines Virtuelles de VirtualBox :



Seul le serveur SSH a accès à internet grâce à l'accès par pont :



Tandis que tous les autres sont en mode d'accès réseau interne :



La première machine qui va être configuré sera le serveur DHCP car il devra permettre d'adresser les IP dynamiquement aux autres machines.

3.2 Serveur DHCP

Nous avons configuré le serveur DHCP pour qu'il ait une IP statique comme le montre le screen suivant :

```
GNU nano 6.2 /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      addresses:
        - 192.168.2.1/26
      dhcp4: false
      version: 2
```

Nous avons dû créer un nouveau fichier `etc/cloud/cloud.cfg.d/99-disable-network-config.cfg` car le fichier était supprimé et recréé à chaque reboot de la machine ce qui enlevait nos modifications.

```
GNU nano 6.2 /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg
network: {config: disabled}
```

Après ces modifications, on obtient :

```
administrateur@dhcp:~$ 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
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code1 state UP group default qlen 1000
    link/ether 08:00:27:d7:7a:0a brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.1/26 brd 192.168.2.63 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed7:7a0a/64 scope link
        valid_lft forever preferred_lft forever
administrateur@dhcp:~$
```

Nous allons installer dnsmasq :

Nous utiliserons le tuto fourni par le wiki ubuntu officiel pour nous guider :

https://doc.ubuntu-fr.org/configuration_serveur_dns_dhcp

1/ Installation

La modification du fichier pour la résolution DNS:

```
GNU nano 6.2 /etc/systemd/resolved.conf *
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or modify it under the
# terms of the GNU Lesser General Public License as published by the Free
# Software Foundation; either version 2.1 of the License, or (at your option)
# any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file, or by creating "drop-ins" in
# the resolved.conf.d/ subdirectory. The latter is generally recommended.
# Defaults can be restored by simply deleting this file and all drop-ins.
#
# Use 'systemd-analyze cat-config systemd/resolved.conf' to display the full config.
#
# See resolved.conf(5) for details.

[Resolve]
# Some examples of DNS servers which may be used for DNS= and FallbackDNS=:
# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1#cloudflare-dns.com 2606:4700:4700::1111#cloudflare
# Google:      8.8.8.8#dns.google 8.8.4.4#dns.google 2001:4860:4860::8888#dns.google 2001:4860:4860:
# Quad9:       9.9.9.9#dns.quad9.net 149.112.112.112#dns.quad9.net 2620:fe::fe#dns.quad9.net 2620:fe
#DNS=
#FallbackDNS=
#Domains=
#DNSSEC=no
#DNSOverTLS=no
#MulticastDNS=no
#LLMNR=no
#Cache=no-negative
DNSStubListener=no
#DNSSEC=allow-downgrade
#QueryChosts=yes
```

Les commandes permettant l'installation :

```
administrateur@dhcp:~$ sudo systemctl restart systemd-resolved
administrateur@dhcp:~$ sudo apt-get install dnsmasq
```

2/ Configuration

Edition du fichier /etc/dnsmasq.conf :

```
GNU nano 6.2 /etc/dnsmasq.conf
domain-needed
bogus-priv
filterwin2k

localise-queries
local=/lan/
domain=local.lan
expand-hosts
no-negcache
resolv-file=/tmp/resolv.conf.auto

dhcp-authoritative
dhcp-leasefile=/tmp/dhcp.leases

read-ethers

dhcp-range=192.168.2.100,192.168.2.150,12h
dhcp-option=1,255.255.255.0
dhcp-option=3,192.168.2.254
```

Edition du fichier /etc/resolv.conf :

```
GNU nano 6.2 /etc/resolv.conf *
# This is /run/systemd/resolve/resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

# No DNS servers known.
domain local.lan
search local.lan
nameserver 195.238.2.21
nameserver 195.238.2.22
```

Edition du fichier /etc/hosts :

```
GNU nano 6.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 dhcp
192.168.2.1 mail
192.168.2.1 mail.local.lan_

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

On applique ensuite la nouvelle configuration :

```
administrateur@dhcp:~$ sudo /etc/init.d/dnsmasq restart
Restarting dnsmasq (via systemctl): dnsmasq.service.
```

Maintenant que le DHCP est prêt nous allons donner une adresse IP au poste.

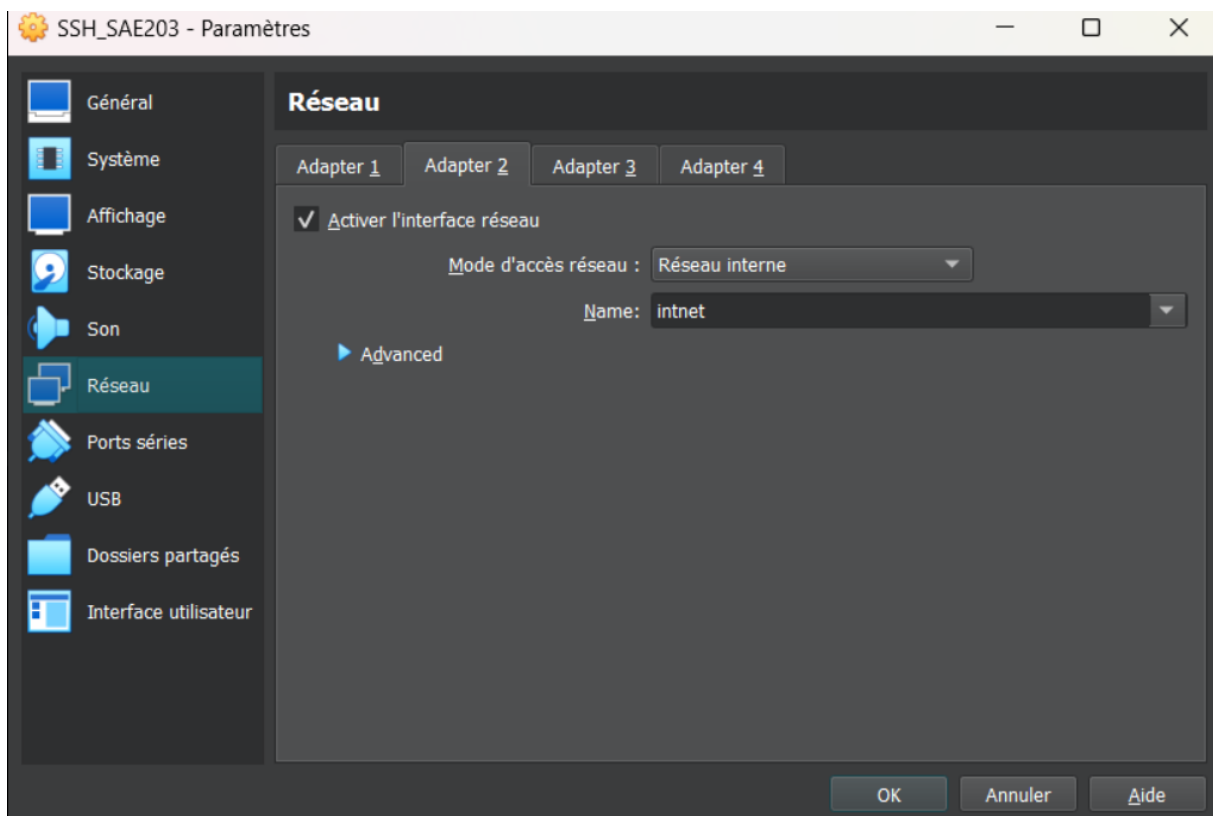
On a dû installer DHCLIENT avec "sudo apt install isc-dhcp-client"

```
administrateur@dhcp:~$ ping 192.168.2.20
PING 192.168.2.20 (192.168.2.20) 56(84) bytes of data.
64 bytes from 192.168.2.20: icmp_seq=1 ttl=64 time=0.677 ms
64 bytes from 192.168.2.20: icmp_seq=2 ttl=64 time=1.25 ms
64 bytes from 192.168.2.20: icmp_seq=3 ttl=64 time=2.81 ms
64 bytes from 192.168.2.20: icmp_seq=4 ttl=64 time=1.99 ms
^C
--- 192.168.2.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.677/1.680/2.812/0.801 ms
administrateur@dhcp:~$ _
```

3.3 Serveur SSH

Adressage IP dynamique et réservé

Adapter2 reçoit une adresse IP de manière dynamique :



On a installé DHCLIENT sur le serveur SSH

```

administrateur@ssh:~$ sudo apt install isc-dhcp-client
[sudo] password for administrateur:
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
isc-dhcp-client est déjà la version la plus récente (4.4.1-2.3ubuntu2.4).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 53 non mis à jour.
administrateur@ssh:~$

```

On modifie la réception de l'adresse IP de l'Adapter2 du SSH en mettant le dhcp sur True.

```

GNU nano 6.2 /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      dhcp4: true
  version: 2

```

On récupère l'adresse MAC de la carte réseau de l'Adapter2 qui est ceci :

```
link/ether 08:00:27:dd:e1:b2 brd ff:ff:ff:ff:ff:ff
```

On ajoute cette ligne dans le fichier /etc/dnsmasq.conf du serveur DHCP

```
dhcp-host=08:00:27:dd:e1:b2, 192.168.2.20
```

Nous avons bien un serveur SSH avec 2 adresses IP : Une qui a accès à internet, et l'autre qui peut communiquer avec le réseau interne.

```

administrateur@ssh:~$ 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
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cc:33:37 brd ff:ff:ff:ff:ff:ff
    inet 10.10.2.74/17 metric 100 brd 10.10.127.255 scope global dynamic enp0s3
        valid_lft 83867sec preferred_lft 83867sec
    inet6 fe80::a00:27ff:fecc:3337/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:dd:e1:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.20/26 metric 100 brd 192.168.2.63 scope global dynamic enp0s8
        valid_lft 42955sec preferred_lft 42955sec
    inet6 fe80::a00:27ff:fedd:e1b2/64 scope link
        valid_lft forever preferred_lft forever

```

Admin peut se connecter en SSH via clef publique depuis l'extérieur

Nous utiliser la commande « ssh-keygen -t rsa » pour générer une clef publique. Nous mettons ensuite le fichier dans lequel celle-ci sera stockée puis une phrase secrète (dans notre cas : vitrygr).

```
administrateur@ssh:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/administrateur/.ssh/id_rsa): /home/administrateur/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/administrateur/.ssh/id_rsa
Your public key has been saved in /home/administrateur/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:xPC18iU7Yony15ky7hQLBvwKyzT6c2IpJEC7XSS+iug administrateur@ssh
The key's randomart image is:
+---[RSA 3072]-----+
| . . . . .
|..0 0 + 0
|..0. . . * .
|. 000. = +
|0=.0= = S
|000B 0 = +
|*0* 0 * +
|.0 + + 0
| E. .0
+----[SHA256]-----+
administrateur@ssh:~$ _
```

Nous récupérons ensuite la clef publique grâce à la commande « cat ~/.ssh/id_rsa.pub », nous donnant l'affichage suivant :

```
administrateur@ssh:~$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDPXWZCCURXxpqW35cJK1kYxyWgMg1991fvf0RxB9LnV9fb3/dTUmkujcEHzditt7C/eaUI63m2f0DLnQ60Qad89eB7QFP9h12uW6HnG+pb1LdMacZuFDUm1ppbEIOl iLuGDj7WJyo01LNxp0J18NHsofI6ANpQ97IK3yr30BrDdx/d/hS7F0mT2B5KvKAvAN7iyNHpG8kRUo8waH+d9Afk0g9ehuFSXhYij4kWP9q/j1UQNehe7ypbF6LzaRyKqSafK/xCvk01mH/JcvAmcFHHmoFSc7QSFerzKhnvWr1/OXWXk6MhzazsF5VUrxQ8cPrsr9+c88NO0ECjaz/oFXvXKNksxevVGHMcsaouhM3xGJ1n7+Hb69sUhpQE6Ops9YrFUzdG68XhdkdJSXDFPMcKH0yvxmpM0u9d4Fsns8XiY5jam25rq4Nurk6blbr7Ov9dN0WRk0JdyugcCrojsuwi5ixghzfs2sS4gU+3i5c5LD6Hs4cdTfyYh0Mt18c= administrateur@ssh
administrateur@ssh:~$
```

Ainsi, la clef publique est : « ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQgQDPXWZCCURXxpqW35cJK1kYxygkM1991vf0RxB9LnV9fb3/dTUmkujcEHzditt7C/eul63mZdfOLnQ6ODad9Be70FP9hL2u6HK6n+pb1dMaczUfDml1ppbE0L1LucGDi7HWyo0L1LNxp0J18NHsofI6ANp09TiX3yr30BrDdx/d/h5rF0MT2B5VqkNA7njYhJ6GkkRUo8waH+d9Afk0g9ehuFSXhYij4kWP9q/j1UQNehe7ypbF6LzaRyKqSafK/xCvk01mH/cvvmFcHHNmoFSc7Q5FEzKnxhv1r/OXWXk6MhzazsF5VUrxQ8cPrsr9+c88NO0ECjaz/oFXvXKNksxevVGHMcsaouhM3xGJ1n7+Hb69sUhpQE6Ops9YrFUzdG68XhdkdJSXDFPMcKH0yvxmpM0u9d4Fsns8XiY5jam25rq4Nurk6blbr7Ov9dN0WRk0JdyugcCrojsuwi5ixghzfs2sS4gU+3i5c5LD6Hs4cdTfyYh0Mt18c= administrateur@ssh »

Notons qu'il y avait une erreur lorsque je regardais le status du SSH sur mon serveur, il n'était pas activé et j'étais empêché de me connecter à mon serveur SSH, que ce soit avec ou sans mot de passe :

```
administrateur@ssh:~$ systemctl status ssh.service
* ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Wed 2025-04-30 09:57:26 UTC; 10s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 1115 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=1/FAILURE)
      CPU: 7ms

avril 30 09:57:26 ssh systemd[1]: ssh.service: Control process exited, code=exited, status=1/FAILURE
avril 30 09:57:26 ssh systemd[1]: ssh.service: Failed with result 'exit-code'.
avril 30 09:57:26 ssh systemd[1]: Failed to start OpenBSD Secure Shell server.
avril 30 09:57:26 ssh systemd[1]: ssh.service: Scheduled restart job, restart counter is at 5.
avril 30 09:57:26 ssh systemd[1]: Stopped OpenBSD Secure Shell server.
avril 30 09:57:26 ssh systemd[1]: ssh.service: Start request repeated too quickly.
avril 30 09:57:26 ssh systemd[1]: ssh.service: Failed with result 'exit-code'.
avril 30 09:57:26 ssh systemd[1]: Failed to start OpenBSD Secure Shell server.

The unit ssh.service has entered the 'failed' state with result 'exit-code'.
avril 30 10:02:34 ssh systemd[1]: Failed to start OpenBSD Secure Shell server.
   Subject: L'unité (unit) ssh.service a échoué
   Defined-By: systemd
   Support: http://www.ubuntu.com/support

L'unité (unit) ssh.service a échoué, avec le résultat failed.
avril 30 10:02:34 ssh systemd[1]: ssh.service: Scheduled restart job, restart counter is at 5.
   Subject: Le redémarrage automatique d'une unité (unit) a été planifié
   Defined-By: systemd
   Support: http://www.ubuntu.com/support

Le redémarrage automatique de l'unité (unit) ssh.service a été planifié, en
raison de sa configuration avec le paramètre Restart=.
avril 30 10:02:34 ssh systemd[1]: Stopped OpenBSD Secure Shell server.
   Subject: L'unité (unit) ssh.service a terminé son arrêt
   Defined-By: systemd
   Support: http://www.ubuntu.com/support

L'unité (unit) ssh.service a terminé son arrêt.
avril 30 10:02:34 ssh systemd[1]: ssh.service: Start request repeated too quickly.
avril 30 10:02:34 ssh systemd[1]: ssh.service: Failed with result 'exit-code'.
   Subject: Unit failed
   Defined-By: systemd
   Support: http://www.ubuntu.com/support

The unit ssh.service has entered the 'failed' state with result 'exit-code'.
avril 30 10:02:34 ssh systemd[1]: Failed to start OpenBSD Secure Shell server.
   Subject: L'unité (unit) ssh.service a échoué
   Defined-By: systemd
   Support: http://www.ubuntu.com/support

L'unité (unit) ssh.service a échoué, avec le résultat failed.
```

Pour y remédier, j'ai fait quelques recherches qui m'ont menées à savoir qu'il manquait les clefs hôtes, j'ai donc fait « sudo ssh-keygen -A » afin de les créer, ce qui a permis d'activer mon SSH

```
administrateur@ssh:~$ sudo sshd -t
sshd: no hostkeys available -- exiting.
administrateur@ssh:~$ sudo ssh-keygen -A
ssh-keygen: generating new host keys: RSA DSA ECDSA ED25519
administrateur@ssh:~$ sudo systemctl restart ssh
administrateur@ssh:~$ sudo systemctl status ssh
* ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-04-30 10:15:34 UTC; 6s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 2351 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 2352 (sshd)
     Tasks: 1 (limit: 9165)
    Memory: 1.7M
       CPU: 16ms
   CGroup: /system.slice/ssh.service
           └─2352 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

avril 30 10:15:34 ssh systemd[1]: Starting OpenBSD Secure Shell server...
avril 30 10:15:34 ssh sshd[2352]: Server listening on 0.0.0.0 port 22.
avril 30 10:15:34 ssh sshd[2352]: Server listening on :: port 22.
avril 30 10:15:34 ssh systemd[1]: Started OpenBSD Secure Shell server.
administrateur@ssh:~$
```

Pour ensuite pouvoir me connecter en SSH sans mot de passe sur le serveur SSH, j'ai dû exécuter les instructions suivantes :

- Créer une clef publique sur ma machine via la commande « ssh-keygen »

```
administrateur@administrateur-VirtualBox:~$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/administrateur/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/administrateur/.ssh/id_ed25519
Your public key has been saved in /home/administrateur/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:geMojuwaSwaS0e4ZMKPjoiQDkHqkNLHas0jZ+dJ1IU0 administrateur@administrateur-VirtualBox
The key's randomart image is:
+--[ED25519 256]--+
| .                |
| oo   . E         |
|O+o  o +         |
|B&.  o o +       |
|& *  . . S .     |
|B*o+.  . .       |
|*O+o.  . .       |
|O+  ...          |
|= .  ..          |
+----[SHA256]-----+
```

- Exécuter la commande « ssh-copy-id administrateur@192.168.2.2 » (notre serveur SSH) pour copier sa clef publique :

```
administrateur@administrateur-VirtualBox:~$ ssh-copy-id administrateur@192.168.2.2
The authenticity of host '192.168.2.2 (192.168.2.2)' can't be established.
ED25519 key fingerprint is SHA256:pHtcD9lRtrzkXaTAsGCegaPiv0zEj4+Xwgin/qjNKsU.
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: 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
administrateur@192.168.2.2's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'administrateur@192.168.2.2'"
and check to make sure that only the key(s) you wanted were added.

administrateur@administrateur-VirtualBox:~$
```

- J'ai juste à faire la commande « ssh administrateur@192.168.2.2 » pour me connecter

à mon serveur SSH :

```
administrateur@administrateur-VirtualBox:~$ ssh administrateur@192.168.2.2
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-136-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of mer. 30 avril 2025 10:32:11 UTC

System load:  0.0          Processes:            108
Usage of /:   34.3% of 9.75GB   Users logged in:    1
Memory usage: 3%          IPv4 address for enp0s8: 192.168.2.2
Swap usage:  0%

La maintenance de sécurité étendue pour Applications n'est pas activée.

68 mises à jour peuvent être appliquées immédiatement.
14 de ces mises à jour sont des mises à jour de sécurité.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Apr 30 10:27:20 2025 from 192.168.2.1
administrateur@ssh:~$ exit
logout
Connection to 192.168.2.2 closed.
administrateur@administrateur-VirtualBox:~$
```

L'utilisateur admin a sa durée de connexion SSH

Pour afficher la durée de connexion SSH de l'administrateur sur la machine, je suis allé dans le fichier /etc/profile du serveur SSH et ai écrit :

« export LOGIN_TIME=\$(date +%s) » pour récupérer le temps passé entre le moment où je me suis connecté.

Puis je suis allé dans le fichier ~/.bash_logout et ai écrit les lignes suivantes :

```
LOGOUT_TIME=$(date +%s)
DURATION=$((LOGOUT_TIME - LOGIN_TIME))
echo "Session du $(date -d @$LOGIN_TIME) : $DURATION secondes" >> ~/session_log.txt
```

Ensuite, je suis allé sur le poste de travail et ai essayé de me connecter en SSH en ajoutant « time » juste avant. Ce qui me donne l'avantage suivant :

```
System information as of mer. 30 avril 2025 14:46:45 UTC

System load: 0.0          Processes:                107
Usage of /: 34.7% of 9.75GB Users logged in:             1
Memory usage: 2%         IPv4 address for enp0s8: 192.168.2.2
Swap usage: 0%

La maintenance de sécurité étendue pour Applications n'est pas activée.

68 mises à jour peuvent être appliquées immédiatement.
14 de ces mises à jour sont des mises à jour de sécurité.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Apr 30 14:44:26 2025 from 192.168.2.38
administrateur@ssh:~$ exit
logout
-bash: /home/administrateur: Is a directory
Connection to 192.168.2.2 closed.

real    0m6,534s
user    0m0,025s
sys     0m0,094s
administrateur@administrateur-VirtualBox:~$
```

Et en partant j'ai le temps réel de connexion (ligne real).

Invoquer la commande sudo sans mettre le mot de passe :

J'ai tapé la commande « sudo visudo » pour ouvrir & modifier le fichier /etc/sudoers, dans lequel je peux gérer la permission que je cherche à changer.

Dans le fichier, j'ai ajouté cette ligne :

```
GNU nano 6.2 /etc/sudoers.tmp *
# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d

administrateur ALL=(ALL) NOPASSWD: ALL_

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line   M-E Redo
```

Elle permet à l'utilisateur administrateur (nous) d'exécuter toutes les commandes sans avoir besoin du mot de passe : dont sudo

Après avoir relancé la machine virtuelle, j'ai invoqué la commande sudo et aucun mot de passe ne m'a été demandé.

```
administrateur@ssh:~$ ls
last Test
administrateur@ssh:~$ sudo rm -r Test
administrateur@ssh:~$ ls
last
administrateur@ssh:~$ _
```

L'utilisateur « bastion » du SSH est le seul utilisateur pouvant se connecter aux autres VM.

Pour commencer, cette clause signifie que ni le poste, ni l'hôte ne peuvent se connecter aux serveurs DHCP, FTP et WEB, ni que les serveurs peuvent entre eux, le tout sans passer par le SSH. Ainsi, la solution consiste tout simplement à ouvrir le fichier « /etc/ssh/sshd_config » et d'ajouter cette ligne :

```
AllowUsers bastion@192.168.2.2
```

Avec bastion, notre utilisateur et l'adresse IP du serveur SSH, qui reste la même (voir plus haut). Il ne reste plus qu'à faire ça pour tous les serveurs.

3.4 Serveur Web

Adresse IP dynamique et réservée :

Mettons notre machine en mode de réseau interne.

Ensuite, nous allons dans le fichier /etc/dnsmasq.conf dans le serveur dhcp et ajoutons cette ligne :

```
dhcp-host=08:00:27:e9:62:81, 192.168.2.3
```

Après l'avoir relancé, et après m'être connecté à mon serveur web, celui-ci a bien vu son adresse IP changer :

```
administrateur@web:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e9:62:81 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.3/26 brd 192.168.2.63 scope global dynamic noprefixroute enp0s3
        valid_lft 43190sec preferred_lft 43190sec
    inet6 fe80::a00:27ff:fee9:6281/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Reprise du CDC de R2.05

NB : La plupart des choses ayant déjà été faites, nous allons commencer avec Apache2. En effet, comme montré la VM tourne déjà sans interface graphique, le serveur se nomme web (et non www, mais cela n'a pas grande importance), il existe un compte « administrateur » ayant comme mot de passe « vitrygtr », la machine ne dispose pas d'un accès à internet comme le montre le screen ci-dessous :

```
administrateur@web:~$ sudo apt update
[sudo] password for administrateur:
Ign:1 http://security.debian.org/debian-security bookworm-security InRelease
Ign:2 http://deb.debian.org/debian bookworm InRelease
Ign:3 http://deb.debian.org/debian bookworm-updates InRelease
Ign:1 http://security.debian.org/debian-security bookworm-security InRelease
Ign:2 http://deb.debian.org/debian bookworm InRelease
Ign:3 http://deb.debian.org/debian bookworm-updates InRelease
Ign:1 http://security.debian.org/debian-security bookworm-security InRelease
Ign:2 http://deb.debian.org/debian bookworm InRelease
Ign:3 http://deb.debian.org/debian bookworm-updates InRelease
Err:1 http://security.debian.org/debian-security bookworm-security InRelease
   Temporary failure resolving 'security.debian.org'
Err:2 http://deb.debian.org/debian bookworm InRelease
   Temporary failure resolving 'deb.debian.org'
Err:3 http://deb.debian.org/debian bookworm-updates InRelease
   Temporary failure resolving 'deb.debian.org'
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
W: Failed to fetch http://deb.debian.org/debian/dists/bookworm/InRelease Temporary failure resolving 'deb.debian.org'
W: Failed to fetch http://security.debian.org/debian-security/dists/bookworm-security/InRelease Temporary failure resol
W: Failed to fetch http://deb.debian.org/debian/dists/bookworm-updates/InRelease Temporary failure resolving 'deb.debia
W: Some index files failed to download. They have been ignored, or old ones used instead.
administrateur@web:~$
```

(Incapacité de mettre à jour apt)

La machine est accessible depuis l'hôte et depuis le serveur SSH (qui sert de machine cliente Ubuntu). Ceci nous amène à Apache.

Nous installons le paquet « apache2 » grâce à la commande « sudo apt install apache2 ». Par ailleurs, nous avons ajouté une configuration réseau sur VirtualBox en accès par pont le temps d'installer ce paquet, et de le configurer.

```
administrateur@web:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-05-12 10:55:17 CEST; 2min 30s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 603 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 649 (apache2)
    Tasks: 55 (limit: 9223)
   Memory: 11.7M
      CPU: 86ms
   CGroup: /system.slice/apache2.service
           └─649 /usr/sbin/apache2 -k start
             └─651 /usr/sbin/apache2 -k start
               └─652 /usr/sbin/apache2 -k start

May 12 10:55:17 web systemd[1]: Starting apache2.service - The Apache HTTP Server...
May 12 10:55:17 web systemd[1]: Started apache2.service - The Apache HTTP Server.
administrateur@web:~$
```

Comme le montre le screen ci-dessus, apache2 a bien été installé et est actif.

Nous allons maintenant créer les 2 pages webs demandées : index.html & perdu.html. Pour index.html, nous allons simplement créer un fichier avec ce nom dans le dossier « /var/www », et dans lequel nous allons mettre du contenu.

Voici nos 2 pages perdu.html & index.html :

```
GNU nano 7.2                                perdu.html
<h1>Lost on the Internet ?</h1>
<h2>Don't worry, we are going to help you.</h2>
<p>* <---- You are here</p>

GNU nano 7.2                                index.html
<h1>Bienvenue sur le site internet de la SAE2.03</h1>
<p>Vous êtes actuellement sur la page internet de <b>VERRIER Joris</b>, <b>KAROU Maya</b> et <b>LEFRANCOIS Pierre</b>.
</br>
<a href="/var/www/perdu.html">Un lien si vous voulez voyager sur internet.</a>
```

Passons désormais au répertoire /private qui est protégé.

Nous allons commencer à créer ce répertoire (pour des soucis de praticité on a déplacé tous nos fichiers dans le dossier /var/www/sae).

```

administrateur@web:/var/www$ sudo mkdir sae
administrateur@web:/var/www$ ls
html index.html perdu.html sae
administrateur@web:/var/www$ ls html
index.html
administrateur@web:/var/www$ mv index.html sae
mv: cannot move 'index.html' to 'sae/index.html': Permission denied
administrateur@web:/var/www$ sudo mv index.html sae
administrateur@web:/var/www$ sudo mv perdu.html sae
administrateur@web:/var/www$ ls
html sae
administrateur@web:/var/www$ ls sae
index.html perdu.html
administrateur@web:/var/www$ cd sae
administrateur@web:/var/www/sae$ mkdir private
mkdir: cannot create directory 'private': Permission denied
administrateur@web:/var/www/sae$ sudo mkdir private
administrateur@web:/var/www/sae$

```

Dans ce dossier /private, nous allons créer le fichier « .htaccess » et y mettre le contenu suivant :

```

GNU nano 7.2 .htaccess *
AuthType Basic
AuthName "Zone privée"
AuthUserFile /etc/apache2/.htpasswd
Require valid-user

```

Par la suite, nous allons exécuter la commande suivante :

```

administrateur@web:/var/www/sae/private$ sudo htpasswd -c /etc/apache2.htpasswd administrateur
New password:
Re-type new password:
Adding password for user administrateur
administrateur@web:/var/www/sae/private$ _

```

Celle-ci va créer un utilisateur et son mot de passe « vitrygtr » qui donneront l'accès au répertoire.

Nous allons ensuite modifier le fichier /etc/apache2/sites-available/000-default.conf qui

ressemblera à ça, la partie entourée ayant été ajoutée :

```
GNU nano 7.2 /etc/apache2/sites-available/000-default.conf *
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

<Directory /var/www/sae>
    AllowOverride All
</Directory>
</VirtualHost>
```

Après avoir relancé apache2 et s'être assurés qu'il fonctionne correctement, nous allons configurer la page d'erreur affichée si la page n'a pas été trouvée.

Pour commencer, nous allons créer la page 404.html comme suit :

```
GNU nano 7.2 404.html
<h1>Dups, on dirait que tu t'es trompé de direction.</h1>
<a href="index.html">Tu devrais essayer celle-ci pour retourner en lieu sûr</a>
```

Ensuite, nous allons retourner dans le fichier /etc/apache2/sites-available/000-default.conf et allons ajouter cette ligne :

```
ErrorDocument 404 /404.html
```

Nous pouvons désormais redémarrer apache, clôturant ainsi cette étape de reproduction du serveur WEB de la R2.05.

Déploiement de la configuration sur une Debian CLI avec accès à internet

La machine Debian aura 2 cartes réseaux : Une en accès par pont pour l'accès internet, et une en réseau internet pour pouvoir communiquer avec notre serveur web.

Sur notre serveur web, on va créer un dossier nommé webDeploy sur lequel on va mettre nos fichiers de configuration, nos fichiers pour le site, et un script Bash qui permet le déploiement et qui ressemble à ça :

```
GNU nano 7.2                                deploy.sh
#!/bin/bash

if [ "$EUID" -ne 0 ]; then
    echo "Vous n'avez pas la permission d'exécuter le script."
    exit 1
fi

echo "Etape 1 : Mise à jour du système et installation d'Apache."
apt update
apt install -y apache2 apache2-utils

echo "Etape 2 : Copie des fichiers du site web."
rm -rf /var/www/html/*
mkdir -p /var/www/html/
cp -r sae/* /var/www/html/

echo "Etape 3: Copie du fichier .htpasswd."
cp .htpasswd /etc/apache2/.htpasswd
chown www-data:www-data /etc/apache2/.htpasswd
chown 640 /etc/apache2/.htpasswd

echo "Etape 4: Déploiement de la configuration Apache."
cp apache/000-default.conf /etc/apache2/sites-available/000-default.conf

echo "Etape 5: Déploiement terminé"
```

Ensuite, nous allons compresser ce fichier avec cette commande :

« tar czf webDeploy.tar.gz webDeploy »

Puis le mettre sur la machine Debian grâce à cette commande :

scp webDeploy.tar.gz administrateur@192.168.2.38:/tmp

Nous allons ensuite sur notre serveur Debian chercher notre fichier compressé qui se trouve dans le /tmp.

```
administrateur@debian:~$ cd /tmp
administrateur@debian:/tmp$ ls
systemd-private-11f97e1bf3f84c2d8dc21d2325661516-low-memory-monitor.service-Dnvc1F
systemd-private-11f97e1bf3f84c2d8dc21d2325661516-systemd-logind.service-gHD3xa
systemd-private-11f97e1bf3f84c2d8dc21d2325661516-systemd-timesyncd.service-6zWmNE
webDeploy.tar.gz
administrateur@debian:/tmp$ _
```

Nous allons ensuite le décompresser grâce à « tar xzf webDeploy .tar.gz »

Après exécution, on a bel et bien notre déploiement :

```
administrateur@debian:/tmp/webDeploy$ sudo bash deploy.sh
Etape 1 : Mise à jour du système et installation d'Apache.
Hit:1 http://security.debian.org/debian-security bookworm-security InRelease
Hit:2 http://deb.debian.org/debian bookworm InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.62-1~deb12u2).
apache2-utils is already the newest version (2.4.62-1~deb12u2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Etape 2 : Copie des fichiers du site web.
Etape 3: Copie du fichier .htpasswd.
Etape 4: Déploiement de la configuration Apache.
Etape 5: Déploiement terminé
```

```
administrateur@debian:/tmp/webDeploy$ cd /var/www/
administrateur@debian:/var/www$ ls
html
administrateur@debian:/var/www$ cd html/
administrateur@debian:/var/www/html$ ls
404.html index.html perdu.html private
administrateur@debian:/var/www/html$ _
```

```
administrateur@debian:/var/www/html$ sudo systemctl status apache2
• apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Thu 2025-05-15 15:09:19 CEST; 17min ago
  Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 2005 (apache2)
  Tasks: 55 (limit: 9223)
  Memory: 9.1M
  CPU: 96ms
  CGroup: /system.slice/apache2.service
          └─2005 /usr/sbin/apache2 -k start
            └─2006 /usr/sbin/apache2 -k start
              └─2007 /usr/sbin/apache2 -k start

May 15 15:09:19 debian systemd[1]: Starting apache2.service - The Apache HTTP Server...
May 15 15:09:19 debian systemd[1]: Started apache2.service - The Apache HTTP Server.
administrateur@debian:/var/www/html$
```

3.5 FTP

Adressage IP dynamique et réservé

Cette partie se fait sur le serveur DHCP, au même titre que les autres machines en modifiant le fichier /etc/dnsmasq.conf et en ajoutant l'adresse MAC de la carte réseau, ainsi que sa nouvelle adresse IP.

```
#SSH
dhcp-host=08:00:27:dd:e1:b2, 192.168.2.2

#WEB
dhcp-host=08:00:27:e9:62:81, 192.168.2.3

#FTP
dhcp-host=08:00:27:31:6e:1d, 192.168.2.4
```

```
administrateur@ftp:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:31:6e:1d brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.4/26 brd 192.168.2.63 scope global dynamic noprefixroute enp0s3
        valid_lft 43194sec preferred_lft 43194sec
    inet6 fe80::a00:27ff:fe31:6e1d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
administrateur@ftp:~$ _
```

Les utilisateurs peuvent se connecter avec leur identifiant

Pour répondre à cette consigne, il a juste fallu que j'aie dans le fichier /etc/vsftpd.conf, disponible grâce au téléchargement du package vsftpd, et que je mette YES à cette ligne :

```
# Uncomment this to allow local users to log in.
local_enable=YES
```

L'accès est en lecture/écriture sauf pour le compte « anonymous » qui est en lecture seule

Pour cette étape, nous allons installer VSFTPD avec apt install. Cela va nous donner accès au fichier /etc/vsftpd.conf dans lequel nous pourrions modifier cette ligne :

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
```

En la faisant passer de NO à YES. Ce changement nous permet de se connecter en FTP à la machine en ayant un « compte invité ».

Nous allons ensuite créer un dossier pour cet utilisateur avec la commande « sudo mkdir -p /home/ftp/anonymous », duquel nous allons modifier les permissions avec la commande « sudo chmod u=rwx, g=rx, o=rx /home/ftp/anonymous »

```
administrateur@ftp:~$ ls -ld /home/ftp/anonymous
drwxr-xr-x 2 root root 4096 May 19 09:57 /home/ftp/anonymous
administrateur@ftp:~$
```

Nous voyons bien que le fichier est en lecture seule pour les utilisateurs et groupes qui

ne sont pas le root. Nous aurons juste à modifier les permissions de chacun des utilisateurs de telle sorte à ce qu'ils aient le droit de le modifier.

Les utilisateurs peuvent déposer et télécharger leurs fichiers en SFTP sans taper leur mot de passe (authentification par clé publique)

Pour faire ça, je dois copier la clef publique qui a été générée, sur le serveur ftp. Pour ça, nous utilisons la commande « ssh-copy-id administrateur@192.168.2.4 » sur le poste client (on utilisera cette machine pour montrer le bon fonctionnement).

Par la suite, je dois modifier le fichier « /etc/ss/sshd_config » et le faire ressembler à ça :

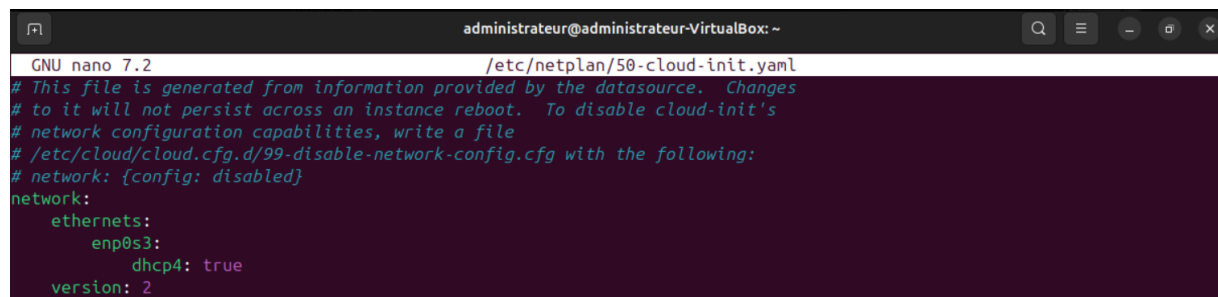
```
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
PasswordAuthentication no
ChallengeResponseAuthentication no
Subsystem sftp /usr/lib/openssh/sftp-server
```

Finalement, et très facilement, je peux me connecter en SFTP à mon serveur sans avoir à taper le mot de passe comme le montre la photo ci-dessous :

```
administrateur@administrateur-VirtualBox:~$ sftp administrateur@192.168.2.4
Connected to 192.168.2.4.
sftp> |
```

3.6 Poste de travail

Toutes les demandes fait concernant le poste de travail ont été rempli comme le montre le screen ci-dessous :



```
administrateur@administrateur-VirtualBox: ~
GNU nano 7.2 /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      dhcp4: true
  version: 2
```

L'adressage IP est dynamique comme le montre le screen ci-dessous :

```
administrateur@administrateur-VirtualBox:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:70:63:76 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.20/26 brd 192.168.2.63 scope global dynamic noprefixroute enp0s3
        valid_lft 43169sec preferred_lft 43169sec
    inet6 fe80::a00:27ff:fe70:6376/64 scope link
        valid_lft forever preferred_lft forever
```