Compte-Rendu TP

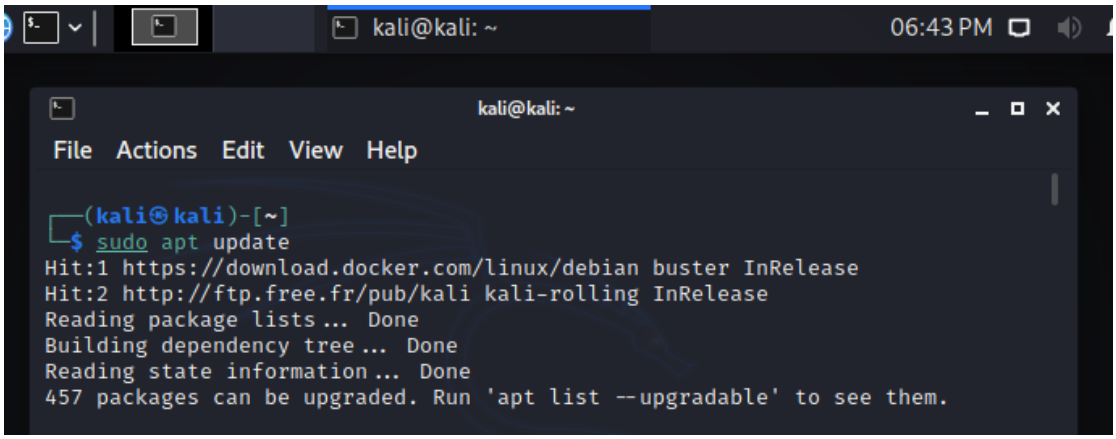
CLOUD, VIRTUALISATION

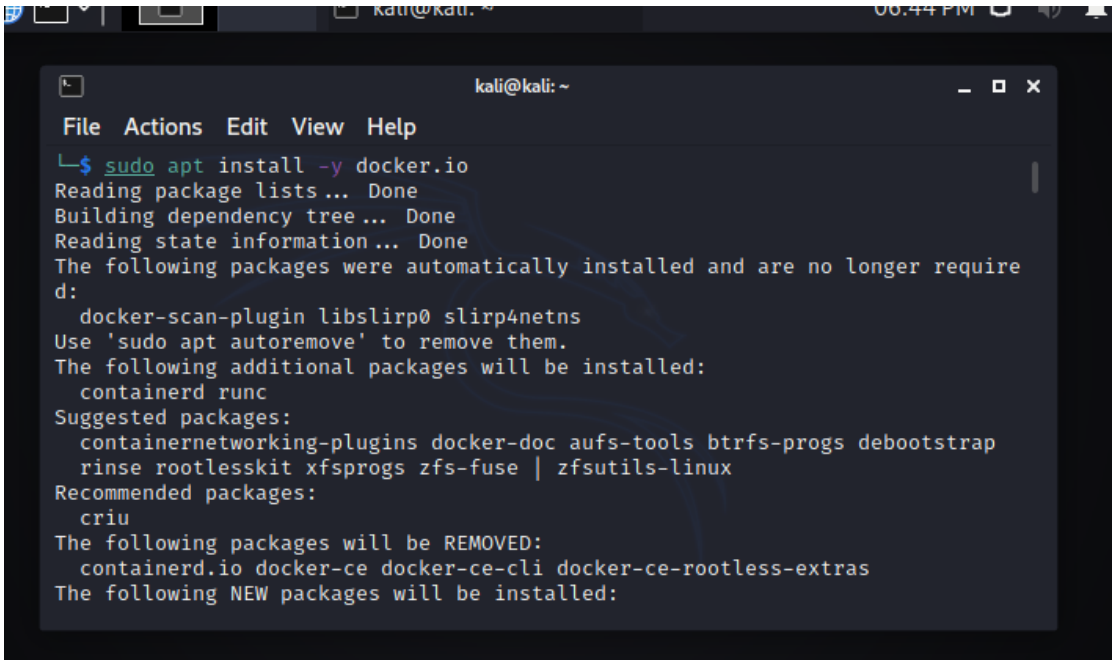
GHAFARI Kevin, PIHATARIOE Raiarii & DE MATTEI Nils | Cloud, Virtualisation | 10/09/2021

Réseaux virtuels (Containers Linux sous Docker)

Exercice 1 : Utilisation de Docker

Exercice 1.1 : Installation de Docker.*





```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable docker --now
Synchronizing state of docker.service with SysV service script with /lib/syst
emd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable docker

┌──(kali㉿kali)-[~]
└─$ docker

Usage:  docker [OPTIONS] COMMAND

A self-sufficient runtime for containers

Options:
      --config string      Location of client config files (default
                           "/home/kali/.docker")
  -c, --context string     Name of the context to use to connect to
                           the daemon (overrides DOCKER_HOST env var
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ docker

Usage:  docker [OPTIONS] COMMAND

A self-sufficient runtime for containers

Options:
      --config string      Location of client config files (default
                           "/home/kali/.docker")
  -c, --context string     Name of the context to use to connect to
                           the daemon (overrides DOCKER_HOST env var
                           and default context set with "docker
                           context use")
  -D, --debug              Enable debug mode
  -H, --host list          Daemon socket(s) to connect to
  -l, --log-level string   Set the logging level
                           ("debug"|"info"|"warn"|"error"|"fatal")
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG docker $(whoami)                                  2 ✗

┌──(kali㉿kali)-[~]
└─$ printf "%s\n" "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-ce-ar
chive-keyring.gpg] https://download.docker.com/linux/debian buster stable" \
  | sudo tee /etc/apt/sources.list.d/docker-ce.list
deb [arch=amd64 signed-by=/usr/share/keyrings/docker-ce-archive-keyring.gpg]
https://download.docker.com/linux/debian buster stable
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ curl -fsSL https://download.docker.com/linux/debian/gpg \
  | gpg --dearmor \
  | sudo tee /usr/share/keyrings/docker-ce-archive-keyring.gpg
X►►*►Z►|►
        ►►►s►@u►V►►►►-►►u►o►a►►2►a►►►►M►►►►►►_T►R`►►►
                                                  ►►►)5►►►►►►X►►►o^►►
•–►►¥►►,P►►An►►L►
                  ~,►%>►►►i►5B►►@►►?"►►]►►/►►►|►►►B►}►►►►H►5X|M
sz►;\►{R►►)►►4►X►►►H►►rK►►
                          ►►),►►4>►►\
rha►xB►►►&8►U►►►►˜►       ["►0[►►►►►►►►►►^►►►m►►u_►►►►V►X►►D►Y►►
                                                        6S►►?^|►►)►►
►\►►►(r►h►►►►►►p►►►►►►\►►D-►►xTV$►^►►►b►►►9!M►►►4►►►T►►:►►An►
P\R►►►►kY]►►►9q►Ht/►►►
                        55►Bp)}]X►►S►►►¿►►<►►►►►►E►e►[►►►7[►|^►►VzhA►►►
j►►s►►►►+Docker Release (CE deldocker@docker.com>com>►►7
!X►►►►
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo apt install -y docker-ce docker-ce-cli containerd.io
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  tini
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  docker-ce-rootless-extras
Suggested packages:
  aufs-tools
The following packages will be REMOVED:
  containerd docker.io runc
The following NEW packages will be installed:
  containerd.io docker-ce docker-ce-cli docker-ce-rootless-extras
0 upgraded, 4 newly installed, 3 to remove and 457 not upgraded.
```

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status docker                                    1 ×
● docker.service - Docker Application Container Engine
     Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor pre>
     Active: active (running) since Sat 2021-10-02 18:40:21 EDT; 11min ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 14653 (dockerd)
      Tasks: 9
     Memory: 40.5M
        CPU: 417ms
     CGroup: /system.slice/docker.service
             └─14653 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/>
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker ps                                                          1 ✗
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES

┌──(root💀 kali)-[/home/kali]
└─#
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker image ls
REPOSITORY   TAG       IMAGE ID   CREATED   SIZE

┌──(root💀 kali)-[/home/kali]
└─# docker images
REPOSITORY   TAG       IMAGE ID   CREATED   SIZE

┌──(root💀 kali)-[/home/kali]
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
2db29710123e: Pull complete
Digest: sha256:9ade9cc2e26189a19c2e8854b9c8f1e14829b51c55a630ee675a5a9540ef6c
cf
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
└─# docker run --name=MonPremierContainer ubuntu echo bonjour
bonjour
```

Exercice 1.1 : Importation d'une image Ubuntu

```
root@kali: /home/kali
File  Actions  Edit  View  Help
┌──(root💀 kali)-[/home/kali]
└─# docker pull ubuntu
Using default tag: latest
latest: Pulling from library/ubuntu
f3ef4ff62e0d: Pull complete
Digest: sha256:44ab2c3b26363823dcb965498ab06abf74a1e6af20a732902250743df0d417
2d
Status: Downloaded newer image for ubuntu:latest
docker.io/library/ubuntu:latest

┌──(root💀 kali)-[/home/kali]
└─# docker images
REPOSITORY    TAG       IMAGE ID       CREATED      SIZE
ubuntu        latest    597ce1600cf4   2 days ago   72.8MB
hello-world   latest    feb5d9fea6a5   9 days ago   13.3kB

┌──(root💀 kali)-[/home/kali]
└─#
```

2 images sont présentes sur la machine

Exercice 1.2 : Lancement d'une commande

```
root@kali: /home/kali
File  Actions  Edit  View  Help
└─# docker run --name=MonPremierContainer ubuntu echo bonjour
bonjour

┌──(root💀 kali)-[/home/kali]
└─# docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES

┌──(root💀 kali)-[/home/kali]
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker ps -a
CONTAINER ID   IMAGE          COMMAND          CREATED          STATUS
               PORTS     NAMES
b8591dfea112   ubuntu         "echo bonjour"   45 seconds ago   Exited (0) 44
seconds ago              MonPremierContainer
24cb4f1c97ae   hello-world    "/hello"         38 minutes ago   Exited (0) 38
minutes ago              blissful_elgamal

┌──(root💀 kali)-[/home/kali]
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker rm $(docker ps -a -q)
b8591dfea112
24cb4f1c97ae

┌──(root💀 kali)-[/home/kali]
└─# docker ps -a
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES

┌──(root💀 kali)-[/home/kali]
```

Exercice 1.3 : Lancement d'une commande en mode interactif.

```
┌──(root💀 kali)-[/home/kali]
└─# docker run -ti --name=MonPremierContainer ubuntu /bin/bash
root@9859a3ceb26f:/#
```

```
root@9859a3ceb26f: /
File  Actions  Edit  View  Help
seconds ago              MonPremierContainer
24cb4f1c97ae   hello-world   "/hello"         38 minutes ago   Exited (0) 38
minutes ago              blissful_elgamal

┌──(root💀 kali)-[/home/kali]
└─# docker rm $(docker ps -a -q)
b8591dfea112
24cb4f1c97ae

┌──(root💀 kali)-[/home/kali]
└─# docker ps -a
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES

┌──(root💀 kali)-[/home/kali]
└─# docker run -ti --name=MonPremierContainer ubuntu /bin/bash
root@9859a3ceb26f:/#
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo docker ps
[sudo] password for kali:
CONTAINER ID   IMAGE     COMMAND       CREATED              STATUS
   PORTS     NAMES
9859a3ceb26f   ubuntu    "/bin/bash"   About a minute ago   Up About a minute
             MonPremierContainer

┌──(kali㉿kali)-[~]
└─$
```

```
root@9859a3ceb26f:/# exit
exit

┌──(root💀 kali)-[/home/kali]
└─#                                                          127 ✗
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo docker ps
[sudo] password for kali:
CONTAINER ID   IMAGE     COMMAND       CREATED              STATUS
   PORTS     NAMES
9859a3ceb26f   ubuntu    "/bin/bash"   About a minute ago   Up About a minute
             MonPremierContainer

┌──(kali㉿kali)-[~]
└─$ sudo docker ps -a
CONTAINER ID   IMAGE     COMMAND       CREATED         STATUS         PORTS
   NAMES
9859a3ceb26f   ubuntu    "/bin/bash"   2 minutes ago   Up 2 minutes
   MonPremierContainer

┌──(kali㉿kali)-[~]
└─$
```

Exercice 1.4 : Lancement d'une commande en mode détaché.

```
┌──(kali㉿kali)-[~]
└─$ sudo docker run -tid --name=BackGroundContainer ubuntu /bin/bash   126 ✗
868862c7dfaf91e24813bbc5c21c737c3489591ccd0d53aabcaa907f8c4898e4
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker attach BackGroundContainer                                127 ✗
root@868862c7dfaf:/#
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker attach BackGroundContainer                                127 ✗
root@868862c7dfaf:/# read escape sequence
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker ps -a                                                       1 ✗
CONTAINER ID   IMAGE     COMMAND       CREATED         STATUS         PORTS
   NAMES
868862c7dfaf   ubuntu    "/bin/bash"   3 minutes ago   Up 3 minutes
   BackGroundContainer
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker stop BackGroundContainer
BackGroundContainer
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker rm $(docker ps -a -q)
868862c7dfaf
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker ps -a
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
```

Exercice 1.5 : Création puis lancement d'un container.

```
┌──(root💀 kali)-[/home/kali]
└─# docker create -ti --name=CreateThenStart ubuntu /bin/bash
f61dd13da5c9539012e0470cfd47049732c1e7b50776945369eba4d306da7b62
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker ps -a
CONTAINER ID   IMAGE     COMMAND       CREATED          STATUS    PORTS     N
AMES
f61dd13da5c9   ubuntu    "/bin/bash"   31 seconds ago   Created           C
reateThenStart
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker start -ai CreateThenStart                                  1 ✗
root@f61dd13da5c9:/#
```

```
root@f61dd13da5c9:/
File  Actions  Edit  View  Help
┌──(root💀 kali)-[/home/kali]
└─# docker create -ti --name=CreateThenStart ubuntu /bin/bash
f61dd13da5c9539012e0470cfd47049732c1e7b50776945369eba4d306da7b62

┌──(root💀 kali)-[/home/kali]
└─# docker ps -a
CONTAINER ID   IMAGE     COMMAND       CREATED          STATUS    PORTS     N
AMES
f61dd13da5c9   ubuntu    "/bin/bash"   31 seconds ago   Created            C
reateThenStart

┌──(root💀 kali)-[/home/kali]
└─# docker start -ai CreateThenStart~
Error: No such container: CreateThenStart~

┌──(root💀 kali)-[/home/kali]
└─# docker start -ai CreateThenStart                                    1 ✗
root@f61dd13da5c9:/#
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀 kali)-[/home/kali]
└─# docker ps
CONTAINER ID   IMAGE     COMMAND       CREATED         STATUS              PO
RTS     NAMES
f61dd13da5c9   ubuntu    "/bin/bash"   2 minutes ago   Up About a minute
        CreateThenStart

┌──(root💀 kali)-[/home/kali]
└─#
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
└─$ sudo su
[sudo] password for kali:
┌──(root💀 kali)-[/home/kali]
└─# docker ps
CONTAINER ID   IMAGE     COMMAND       CREATED         STATUS              PO
RTS     NAMES
f61dd13da5c9   ubuntu    "/bin/bash"   2 minutes ago   Up About a minute
        CreateThenStart

┌──(root💀 kali)-[/home/kali]
└─# docker ps -a
CONTAINER ID   IMAGE     COMMAND       CREATED         STATUS              PO
RTS     NAMES
f61dd13da5c9   ubuntu    "/bin/bash"   3 minutes ago   Up About a minute
        CreateThenStart

┌──(root💀 kali)-[/home/kali]
└─#
```

```
┌──(root💀 kali)-[/home/kali]
└─# docker rm -f CreateThenStart
CreateThenStart
```

Exercice 2 : Docker & Isolation.

Exercice 2.1 :

```
root@7accf68c4361:/
File  Actions  Edit  View  Help

┌──(root💀 kali)-[/home/kali/Desktop]
└─# docker run -ti --name=MonPremierContainer ubuntu /bin/bash
root@7accf68c4361:/# yes
y
y
y
y
y
y
y
```

```
root@7accf68c4361:/
File  Actions  Edit  View  Help

┌──(root💀 kali)-[/home/kali/Desktop]
└─# docker run -ti --name=MonPremierContainer ubuntu /bin/bash
root@7accf68c4361:/# yes
y
y
y
y
y
y
y
y
y
y
y
y
y
y
y
y
```

```
root@kali: /home/kali/Desktop
File  Actions  Edit  View  Help

┌──(root💀 kali)-[/home/kali/Desktop]
└─# ps -a
    PID TTY          TIME CMD
   6158 pts/1    00:00:00 sudo
   6159 pts/1    00:00:00 su
   6160 pts/1    00:00:00 zsh
   6575 pts/0    00:00:00 sudo
   6576 pts/0    00:00:00 su
   6577 pts/0    00:00:01 zsh
   6637 pts/0    00:00:00 docker
   6752 pts/0    00:00:02 yes
   6755 pts/1    00:00:00 ps

┌──(root💀 kali)-[/home/kali/Desktop]
└─# 
```

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# ps -axfo pid,uname,cmd,pidns 6752
    PID USER     CMD                              PIDNS
      2 root     [kthreadd]                  4026531836
      3 root      \_ [rcu_gp]                4026531836
      4 root      \_ [rcu_par_gp]            4026531836
      6 root      \_ [kworker/0:0H-events_hi 4026531836
      8 root      \_ [mm_percpu_wq]          4026531836
      9 root      \_ [rcu_tasks_rude_]       4026531836
     10 root      \_ [rcu_tasks_trace]       4026531836
```

```
6554 kali      \_ /usr/bin/zsh                4026531836
6575 root          \_ sudo su                4026531836
6576 root              \_ su                 4026531836
6577 root                  \_ zsh            4026531836
6637 root                      \_ docker     4026531836
6665 root      /usr/bin/containerd-shim-ru   4026531836
6686 root      \_ /bin/bash                  4026532642
6752 root          \_ yes                    4026532642

┌──(root💀 kali)-[/home/kali/Desktop]
└─#
```

Exercice 2.2 :

```
root@5d5a9dd7a002:/
File  Actions  Edit  View  Help
y
y
y
y
y
y
y
y
y
y
y
y
y
y
y
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
Fields Management for window 1:Def, whose current sort field is %CPU
   Navigate with Up/Dn, Right selects for move then <Enter> or Left comm
   'd' or <Space> toggles display, 's' sets sort.  Use 'q' or <Esc> to e

* PID     = P   PPID    = P   nTH     = N   SUPGIDS = S   nsPID   = P
* %CPU    = C   UID     = E   P       = L   SUPGRPS = S   nsUSER  = U
* USER    = E   RUID    = R   TIME    = C   TGID    = T   nsUTS   = U
* PR      = P   RUSER   = R   SWAP    = S   OOMa    = O   LXC     = L
* NI      = N   SUID    = S   CODE    = C   OOMs    = O   RSan    = R
* VIRT    = V   SUSER   = S   DATA    = D   ENVIRON = E   RSfd    = R
* RES     = R   GID     = G   nMaj    = M   vMj     = M   RSlk    = R
* SHR     = S   GROUP   = G   nMin    = M   vMn     = M   RSsh    = R
* S       = P   PGRP    = P   nDRT    = D   USED    = R   CGNAME  = C
* %MEM    = M   TTY     = C   WCHAN   = S   nsIPC   = I   NU      = L
* TIME+   = C   TPGID   = T   Flags   = T   nsMNT   = M
* COMMAND = C   SID     = S   CGROUPS = C   nsNET   = N
```

S

```
root@kali: /home/kali
File  Actions  Edit  View  Help
Fields Management for window 1:Def, whose current sort field is PID
   Navigate with Up/Dn, Right selects for move then <Enter> or Left comm
   'd' or <Space> toggles display, 's' sets sort.  Use 'q' or <Esc> to e

* %CPU    = C   UID     = E   P       = L   SUPGRPS = S * PID     = P
* USER    = E   RUID    = R   TIME    = C   TGID    = T   nsUSER  = U
* PR      = P   RUSER   = R   SWAP    = S   OOMa    = O   nsUTS   = U
* NI      = N   SUID    = S   CODE    = C   OOMs    = O   LXC     = L
* VIRT    = V   SUSER   = S   DATA    = D   ENVIRON = E   RSan    = R
* RES     = R   GID     = G   nMaj    = M   vMj     = M   RSfd    = R
* SHR     = S   GROUP   = G   nMin    = M   vMn     = M   RSlk    = R
* S       = P   PGRP    = P   nDRT    = D   USED    = R   RSsh    = R
* %MEM    = M   TTY     = C   WCHAN   = S   nsIPC   = I   CGNAME  = C
* TIME+   = C   TPGID   = T   Flags   = T   nsMNT   = M   NU      = L
* COMMAND = C   SID     = S   CGROUPS = C   nsNET   = N
  PPID    = P   nTH     = N   SUPGIDS = S   nsPID   = P
```

```
root@5d5a9dd7a002:/
File  Actions  Edit  View  Help
y
y
y
y
y
y
y
y
y
y
y
```

```
root@kali: ~
File  Actions  Edit  View  Help
  2020 pts/1    Ss     0:00 /usr/bin/zsh
  2042 pts/1    S      0:00 sudo su
  2043 pts/1    S      0:00 su
  2044 pts/1    S      0:00 zsh
  2051 pts/0    S+     1:00 yes
  2056 pts/1    T      0:00 top
  2066 pts/1    S+     0:00 top
  2077 pts/2    Ss     0:00 /usr/bin/zsh
  2114 pts/2    R+     0:00 ps a

┌──(root💀 kali)-[~]
└─# 
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
┌──(root💀 kali)-[/home/kali]
└─# top                                                    147 × 1 ⚙
top - 13:33:01 up 16 min,  1 user,  load average: 2.56, 2.67, 1.60
Tasks: 211 total,   2 running, 208 sleeping,   1 stopped,   0 zombie
%Cpu(s): 12.0 us, 33.6 sy,  0.0 ni, 51.6 id,  0.0 wa,  0.0 hi,  2.9 si,  0.0 st
MiB Mem :   1975.2 total,     68.9 free,    632.1 used,   1274.2 buff/cache
MiB Swap:    975.0 total,    973.7 free,      1.3 used.   1170.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1418 root      20   0 1273332  72248  55140 R  96.7   3.6  11:22.82 x-terminal-emul
    766 root      20   0 1459476 105444  48856 S  57.1   5.2   6:15.20 dockerd
   2051 root      20   0    2516    580    516 S  10.0   0.0   1:11.17 yes
    665 root      20   0 1209128  99900  44384 S   7.0   4.9   0:49.88 Xorg
    437 root      20   0       0      0      0 I   5.6   0.0   0:23.29 kworker/u64:4-events_unb+
   1184 kali      20   0 1270684  77312  55964 S   3.0   3.8   0:23.36 xfwm4
   1626 root      20   0  712856   8864   5380 S   3.0   0.4   0:52.73 containerd-shim
```

Exercice 2.3 :

```
root@5d5a9dd7a002:/
File  Actions  Edit  View  Help
y
y
y
y
y
y
y
y
y
y
yKilled
root@5d5a9dd7a002:/#
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# sudo kill -9 2349
kill: (2349): No such process

┌──(root💀 kali)-[~]
└─# sudo kill -9 2348                                  1 ✗

┌──(root💀 kali)-[~]
└─# sudo kill -9 2051

┌──(root💀 kali)-[~]
└─#
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
top - 13:38:15 up 21 min,  1 user,  load average: 1.56, 2.42, 1.84
Tasks: 206 total,   1 running, 203 sleeping,   2 stopped,   0 zombie
%Cpu(s):  0.0 us,  1.4 sy,  0.0 ni, 97.9 id,  0.0 wa,  0.0 hi,  0.7 si,  0.0 st
MiB Mem :   1975.2 total,     70.0 free,    638.6 used,   1266.6 buff/cache
MiB Swap:    975.0 total,    973.7 free,      1.3 used.   1161.1 avail Mem
Change delay from 3.0 to
    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    649 root      20   0 1313.4m  35.7m  11.3m S   2.8   1.8   0:03.62 containerd
    665 root      20   0 1180.8m  96.3m  42.1m S   2.8   4.9   1:04.20 Xorg
   2017 kali      20   0 1247.9m  68.5m  54.1m S   2.8   3.5   0:07.57 qterminal
   2066 root      20   0    9.9m   3.7m   3.0m R   2.8   0.2   0:02.31 top
      1 root      20   0  160.2m  10.1m   7.5m S   0.0   0.5   0:05.17 systemd
      2 root      20   0    0.0m   0.0m   0.0m S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20    0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20    0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 rcu_par_gp
      6 root       0 -20    0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 kworker/0:0H-events_high+
```

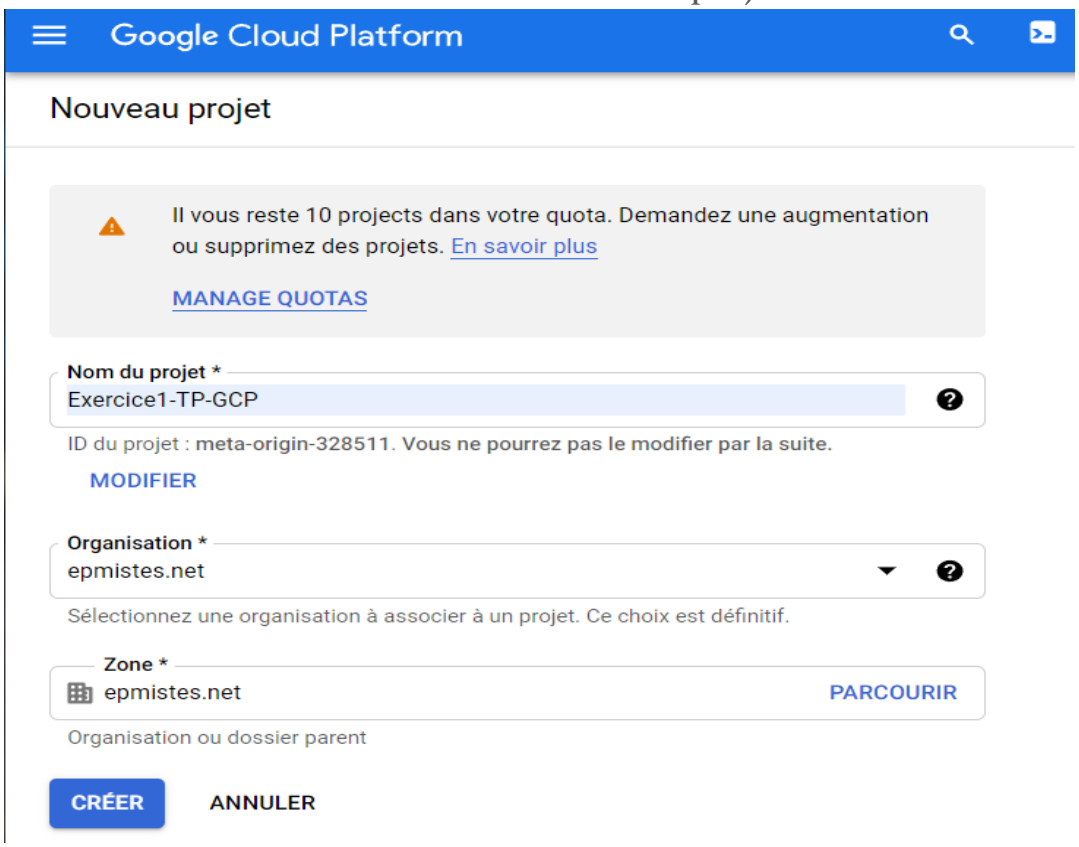
Exercice 2.4 :

```
root@5d5a9dd7a002:/
File  Actions  Edit  View  Help
root@5d5a9dd7a002:/# ps -aef
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 17:19 pts/0    00:00:00 /bin/bash
root          22       0  0 17:47 pts/1    00:00:00 /bin/bash
root          45       1  0 18:28 pts/0    00:00:00 ps -aef
root@5d5a9dd7a002:/#
```

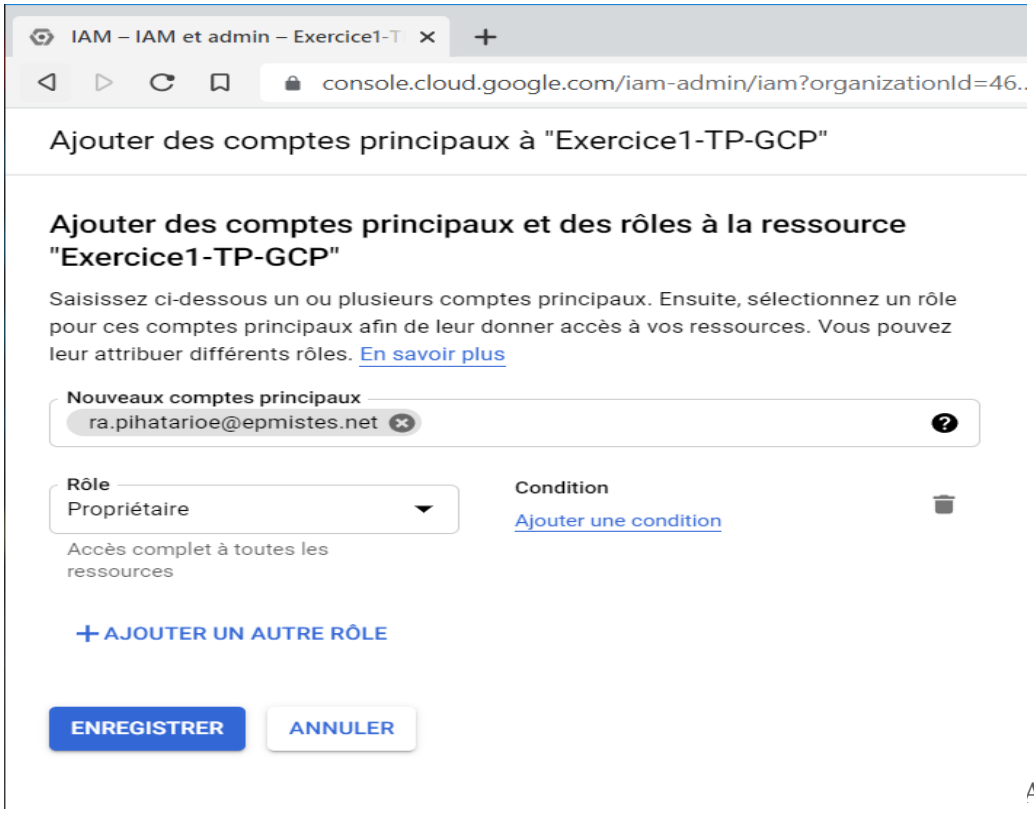
```
┌──(root💀 kali)-[~]
└─# cat /proc/22/status | grep NSpid                    1 ✗
NSpid:  22

┌──(root💀 kali)-[~]
└─#
```

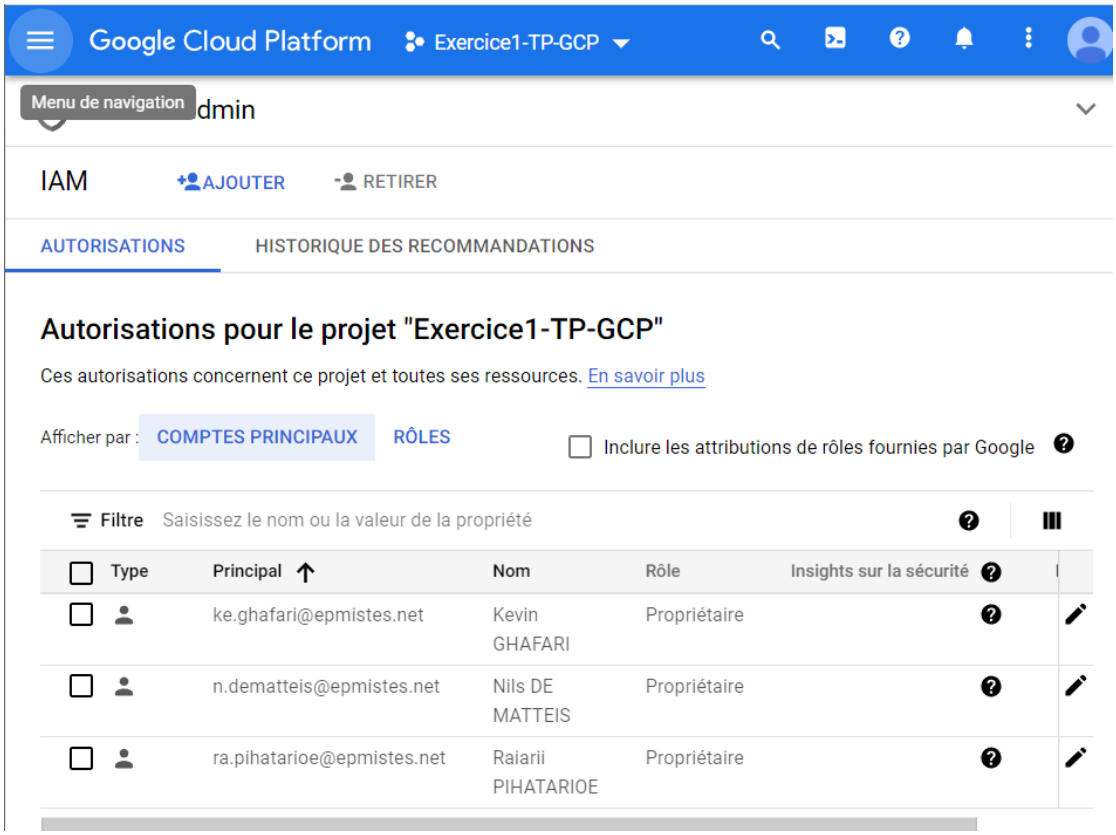
Réseaux virtuels IaaS (Google Cloud Plateform (GCP).

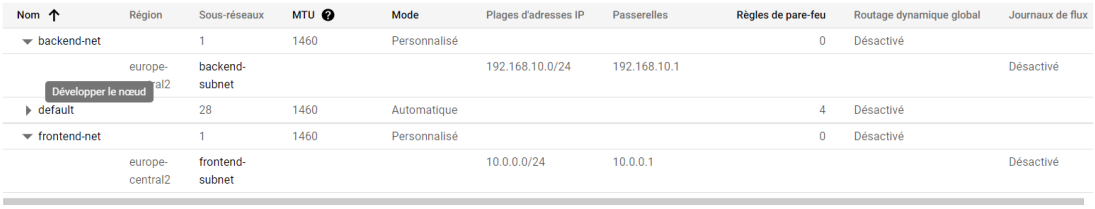
On crée un nouveau projet sur GCP.



On ajoute les différents contributeurs du projet en ajoutant des comptes principaux au projet

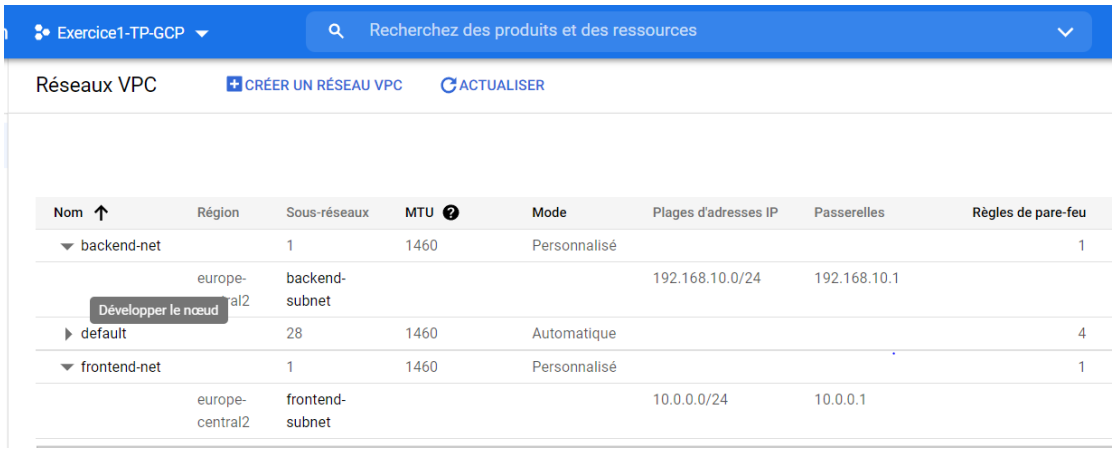






Nom	Région	Sous-réseaux	MTU	Mode	Plages d'adresses IP	Passerelles	Règles de pare-feu	Routage dynamique global	Journaux de flux
backend-net		1	1460	Personnalisé			0	Désactivé	
	europe-central2	backend-subnet			192.168.10.0/24	192.168.10.1			Désactivé
default		28	1460	Automatique			4	Désactivé	
frontend-net		1	1460	Personnalisé			0	Désactivé	
	europe-central2	frontend-subnet			10.0.0.0/24	10.0.0.1			Désactivé

On met en place l'infrastructure réseau de l'énoncé.



Ensuite, on relie les deux réseaux crées.

Exercice1-TP-GCP | Recherchez des produits et des ressources

Appairage de réseaux VPC | CRÉER UNE CONNEXION D'APPAIRAGE | ACTUALISER | SUPPRIMER

Filtre Saisissez le nom ou la valeur de la propriété

Nom	Votre réseau VPC	Réseau VPC appairé	ID du projet appairé	État	Échanger les routes personnalisées	Échanger les routes de sou
interco-be-to-fe	backend-net	frontend-net	exercice1-tp-gcp-328511	Actif	Aucun	Exporter des routes de s
interco-fe-to-be	frontend-net	backend-net	exercice1-tp-gcp-328511	Actif	Aucun	Importer et exporter des IP publique

Il nous reste à mettre en place les règles de firewall pour chaque réseau.

Pare-feu | CRÉER UNE RÈGLE DE PARE-FEU | ACTUALISER | CONFIGURER LES JOURNAUX | SUPPRIMER

- `compute.organizations.setSecurityPolicy`

pour afficher les règles de pare-feu héritées par ce projet.

Les règles de pare-feu contrôlent le trafic entrant ou sortant d'une instance. Par défaut, le trafic entrant en provenance de l'extérieur du réseau est bloqué. En savoir plus

Remarque : Les pare-feu App Engine sont gérés dans la section des règles de pare-feu App Engine.

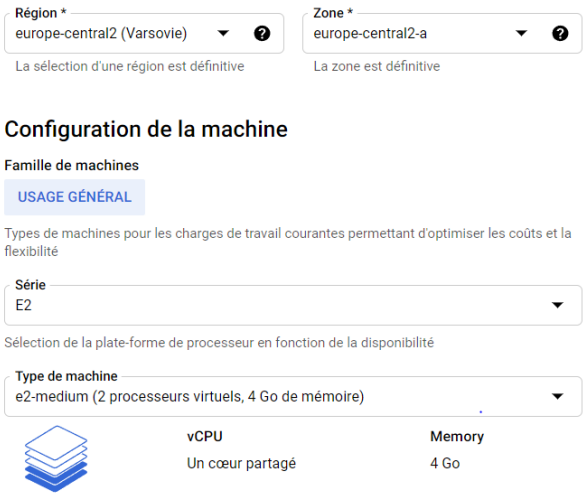
Filtre Saisissez le nom ou la valeur de la propriété

Nom	Type	Cibles	Filtres	Protocoles/Ports	Action	Priorité	Réseau	Journaux	Nombre d'appels	D
allow1	Entrée	Appliquer à	Plages d'adre	all	Autoriser	65000	backend-net	Désactivé	–	–
default-allow-icmp	Entrée	Appliquer à	Plages d'adre	icmp	Autoriser	65534	default	Désactivé	–	–
default-allow-internal	Entrée	Appliquer à	Plages d'adre	tcp:0-65535 udp:0-65535 icmp	Autoriser	65534	default	Désactivé	–	–
default-allow-rdp	Entrée	Appliquer à	Plages d'adre	tcp:3389	Autoriser	65534	default	Désactivé	–	–
default-allow-ssh	Entrée	Appliquer à	Plages d'adre	tcp:22	Autoriser	65534	default	Désactivé	–	–
allow2	Entrée	Appliquer à	Plages d'adre	all	Autoriser	65000	frontend-net	Désactivé	–	–

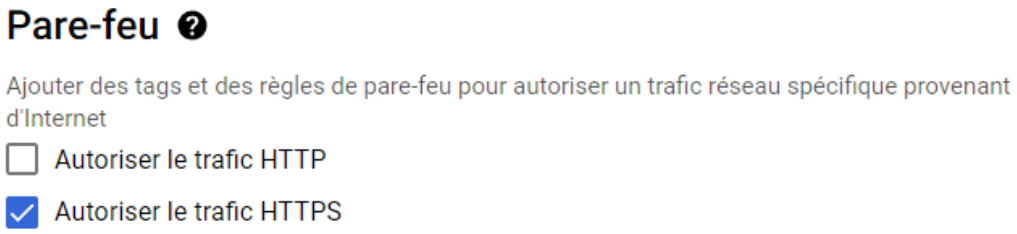
L'infrastructure réseau est crée et configurer, on va maintenant y intégrer les machines virtuelles.

1°) Configuration de la machine virtuelle du réseau privée d'adresse IP publique (VM-FE).

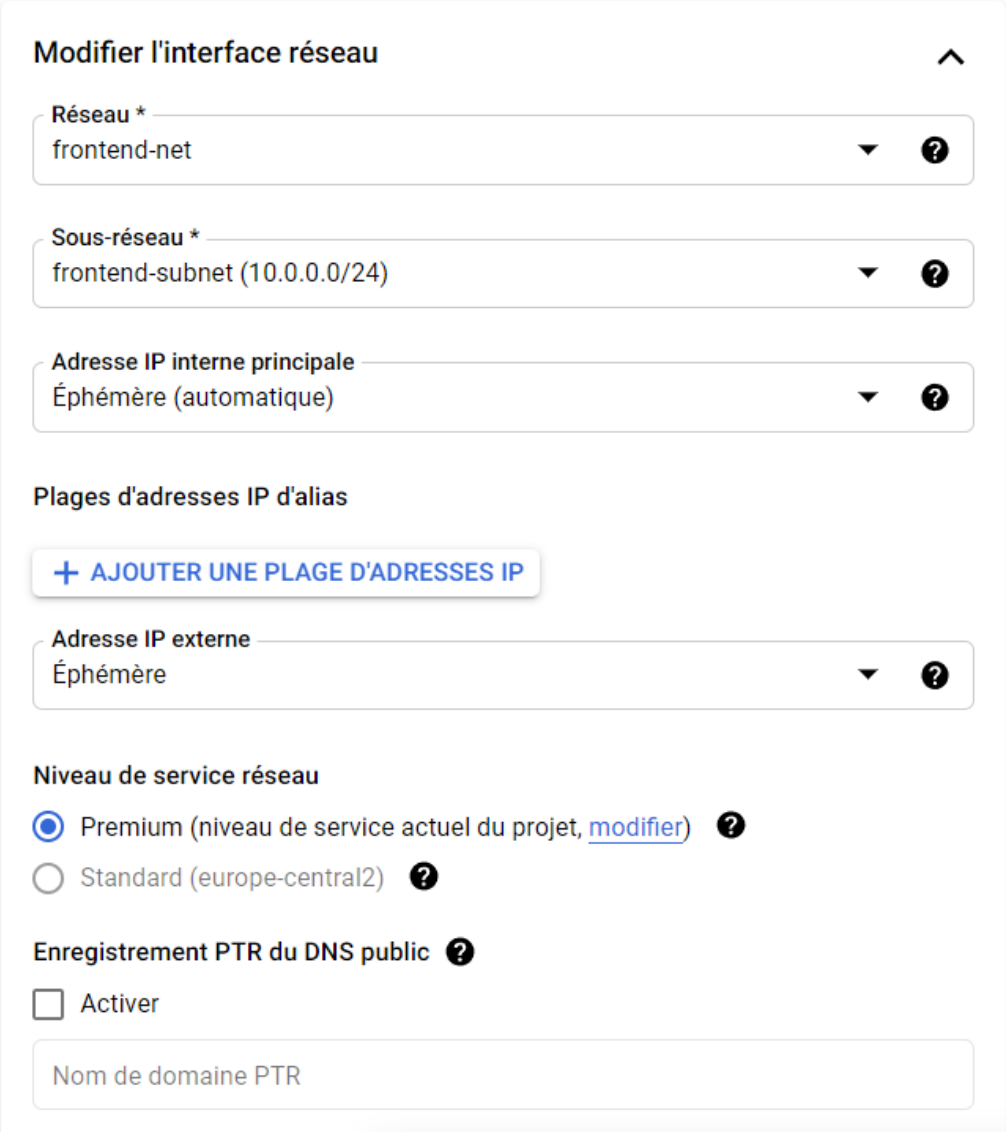
- VM-FE est déployé en Europe.



- Les droits d'accès aux trafics réseaux sont activées uniquement pour des réseaux sécurisés.

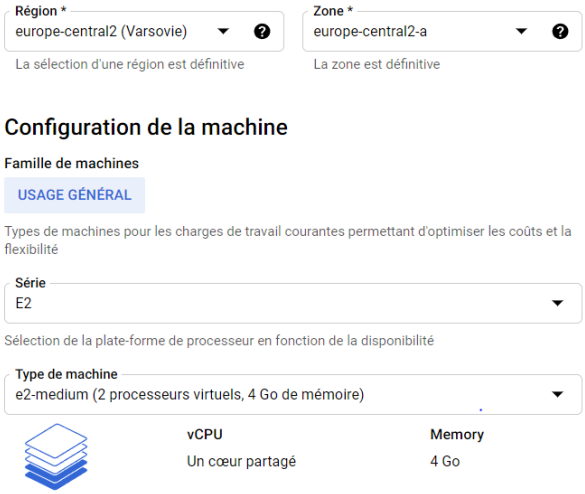


- On associe la machine virtuelle à son interface réseau et on lui attribue une adresse IP publique (IP externe).

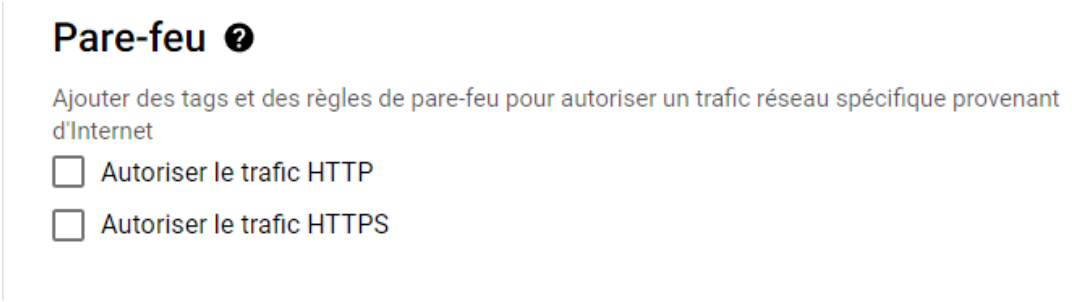


2°) <u>Configuration de la machine virtuelle du réseau privée sans adresse IP publique (VM-BE)</u>

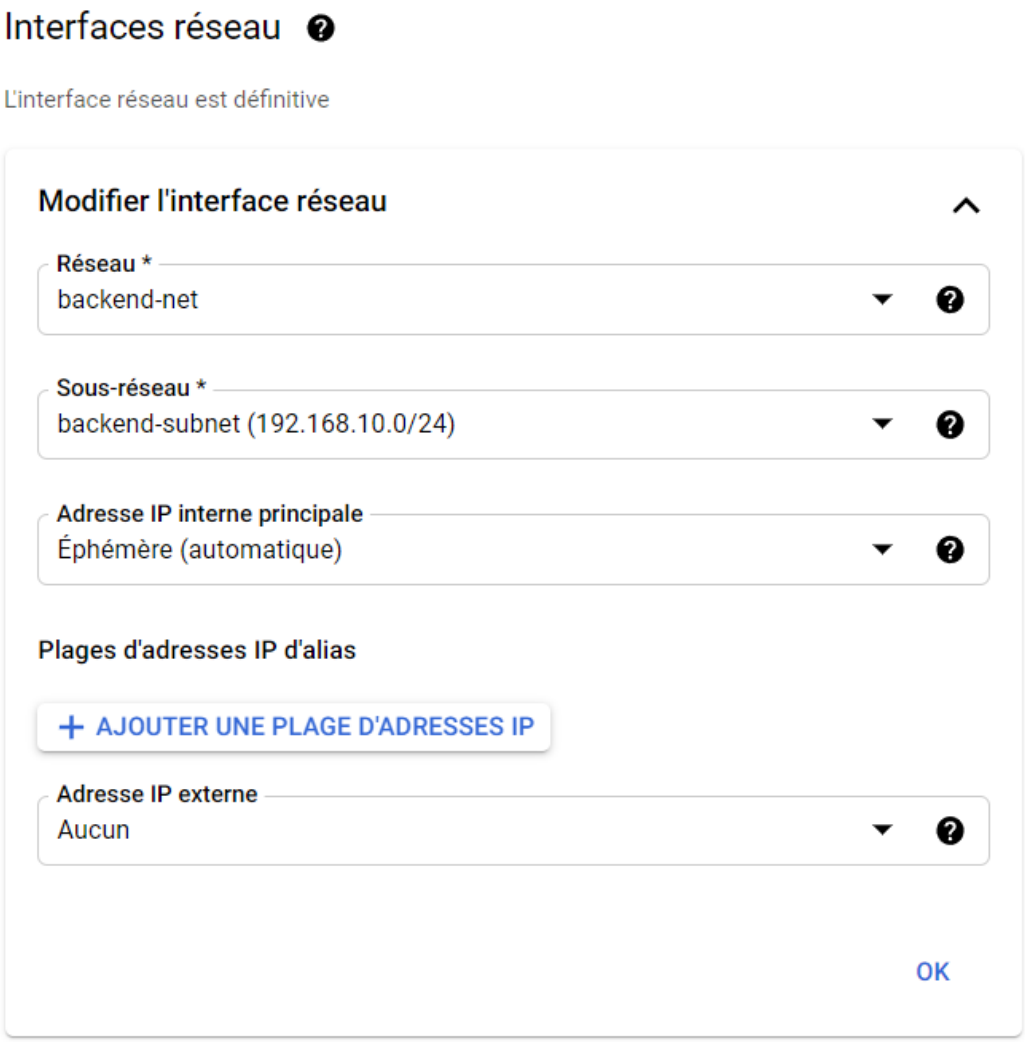
- VM-FE est déployé en Europe.



- Les droits d'accès aux trafics réseaux sont à présent désactivées uniquement pour des réseaux sécurisés.



- On associe la machine virtuelle à son interface réseau sans lui attribuer une adresse IP publique (IP externe).

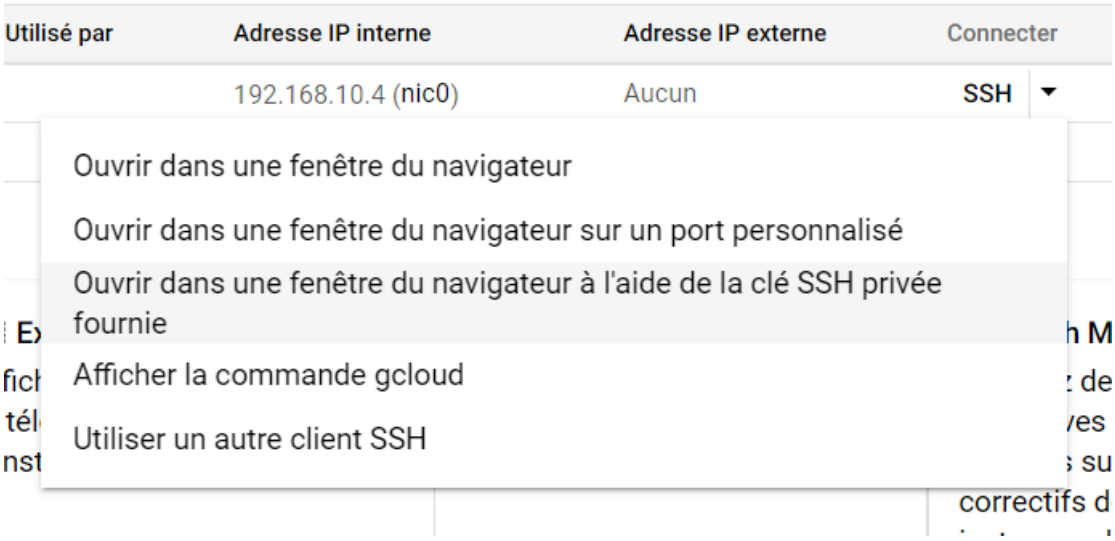


Maintenant que les machines virtuelles sont créées, on démarre chaque instance des machines virtuelles.

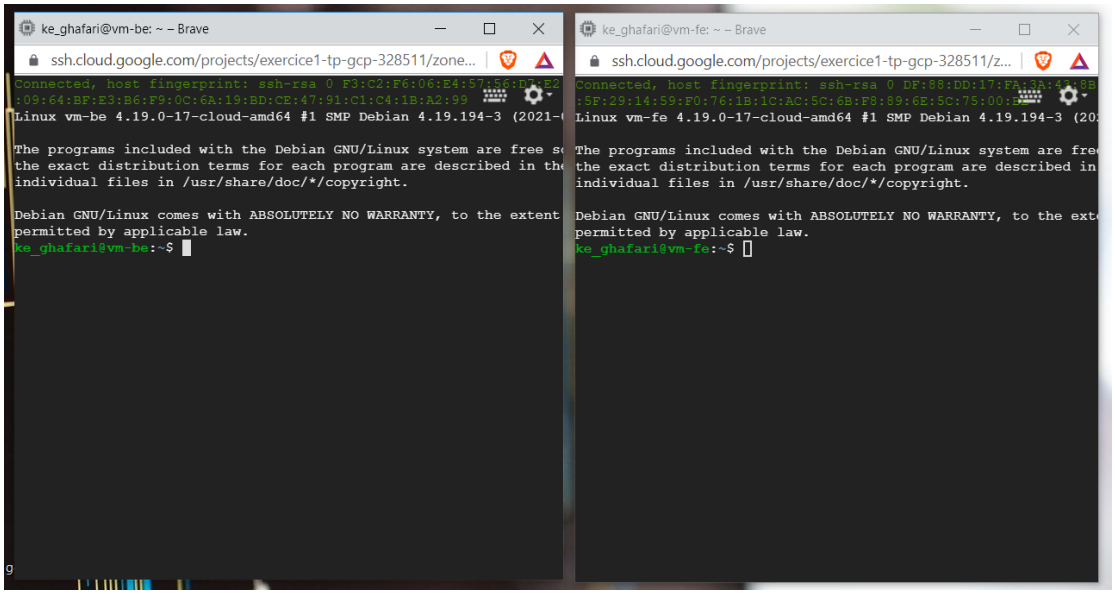
On remarque d'ailleurs la présence d'une adresse IP publique pour la machine virtuelle VM-FE, et la non-présence pour la machine virtuelle VM-BE, ce qui est tout à fait normal.

Maintenant, que les instances sont démarrées, nous allons nous connecter aux deux machines virtuelles instanciées.

Pour se connecter, on ouvre la page instance de VM, où on y trouve les VM que nous avons créés, on démarre les instances (déjà fait) et on se connecte en cliquant sur l'onglet 'Connecter', ensuite on sélectionne 'Ouvrir dans une fenêtre du navigateur'.



Nous nous sommes connectées au VM avec succès.



A présent, essayons de pinger le serveur VMBE depuis le serveur VMFE.

```
ke_ghafari@vm-fe: ~ – Brave
ssh.cloud.google.com/projects/exercice1-tp-gcp-328511/z...
Connected, host fingerprint: ssh-rsa 0 DF:88:DD:17:FA:3A:43:8B
:5F:29:14:59:F0:76:1B:1C:AC:5C:6B:F8:89:6E:5C:75:00:B
Linux vm-fe 4.19.0-17-cloud-amd64 #1 SMP Debian 4.19.194-3 (20

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the ext
permitted by applicable law.
ke_ghafari@vm-fe:~$ ping 192.168.10.4
PING 192.168.10.4 (192.168.10.4) 56(84) bytes of data.
64 bytes from 192.168.10.4: icmp_seq=1 ttl=64 time=1.38 ms
64 bytes from 192.168.10.4: icmp_seq=2 ttl=64 time=0.236 ms
64 bytes from 192.168.10.4: icmp_seq=3 ttl=64 time=0.231 ms
64 bytes from 192.168.10.4: icmp_seq=4 ttl=64 time=0.234 ms
64 bytes from 192.168.10.4: icmp_seq=5 ttl=64 time=0.227 ms
```

La communication est bien possible.

Maintenant, essayons de nous connecter au serveur VMBE depuis le serveur VMFE (à l'aide de la commande SSH).

```
ke_ghafari@vm-fe: ~ – Brave
ssh.cloud.google.com/projects/exercice1-tp-gcp-328511/z...
ke_ghafari@vm-fe:~$ ssh 192.168.10.4
The authenticity of host '192.168.10.4 (192.168.10.4)' can't b
e established.
ECDSA key fingerprint is SHA256:XKq+glDTaa2GDbJSUQaGpypY39HHSE
qtbO+W4mpx8Ac.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.4' (ECDSA) to the list
of known hosts.
ke_ghafari@192.168.10.4: Permission denied (publickey).
ke_ghafari@vm-fe:~$
```

La connexion SSH est refusée ce qui est normal, le serveur VMBE n'a pas d'adresse IP publique.

Exercice 2 : GCP & Automatisation.

Tout d'abord, nous allons installer SDK GCP, sur notre poste de travail. Une fois installer, on peut commencer à utiliser les outils du SDK.

Mais avant tout, il est nécessaire de modifier les politiques d'exécution de script pour pouvoir exécuter le script de l'outil SDK.

```
Sélection Administrateur : Windows PowerShell (x86)
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned

Modification de la stratégie d'exécution
La stratégie d'exécution permet de vous prémunir contre les scripts que vous jugez non fiables. En modifiant la
stratégie d'exécution, vous vous exposez aux risques de sécurité décrits dans la rubrique d'aide
about_Execution_Policies à l'adresse https://go.microsoft.com/fwlink/?LinkID=135170. Voulez-vous modifier la
stratégie d'exécution ?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « N ») : T
```

```
PS C:\Windows\system32> gcloud
ERROR: (gcloud) Command name argument expected.
Command name argument expected.

Available command groups for gcloud:

  AI and Machine Learning
      ai                      Manage entities in Vertex AI.
      ai-platform             Manage AI Platform jobs and models.
      ml                      Use Google Cloud machine learning capabilities.
      ml-engine               Manage AI Platform jobs and models.
      notebooks               Notebooks Command Group.

  API Platform and Ecosystems
      api-gateway             Manage Cloud API Gateway resources.
      apigee                  Manage Apigee resources.
      endpoints               Create, enable and manage API services.
      recommender             Manage Cloud recommendations and recommendation
                              rules.
      services                List, enable and disable APIs and services.

  Anthos CLI
      anthos                  Anthos command Group.

  Billing
      billing                 Manage billing accounts and associate them with
                              projects.
```

Maintenant, on crée un projet intitulé 'exercice2-tp-gcp-328522' sur GCP comme précédemment.

Puis on se connecte à ce projet, depuis le PowerShell :

```
PS C:\Windows\system32> gcloud init
Welcome! This command will take you through the configuration of gcloud.

Settings from your current configuration [default] are:
accessibility:
  screen_reader: 'False'
compute:
  region: europe-west2
  zone: europe-west2-a
core:
  account: ke.ghafari@epmistes.net
  disable_usage_reporting: 'True'
  project: exercice2-tp-gcp-328522

Pick configuration to use:
 [1] Re-initialize this configuration [default] with new settings
 [2] Create a new configuration
Please enter your numeric choice:  1

Your current configuration has been set to: [default]

You can skip diagnostics next time by using the following flag:
  gcloud init --skip-diagnostics

Network diagnostic detects and fixes local network connection issues.
Checking network connection...done.
Reachability Check passed.
Network diagnostic passed (1/1 checks passed).

Choose the account you would like to use to perform operations for
this configuration:
 [1] ke.ghafari@epmistes.net
 [2] kevin.ghafari@gmail.com
 [3] Log in with a new account
Please enter your numeric choice:  1

You are logged in as: [ke.ghafari@epmistes.net].

Pick cloud project to use:
 [1] exercice1-tp-gcp-328511
 [2] exercice2-tp-gcp-328522
 [3] rising-solstice-328511
 [4] Create a new project
Please enter numeric choice or text value (must exactly match list
item):  2

Your current project has been set to: [exercice2-tp-gcp-328522].
```

```
Your current project has been set to: [exercice2-tp-gcp-328522].

Do you want to configure a default Compute Region and Zone? (Y/n)?  n

Your Google Cloud SDK is configured and ready to use!

* Commands that require authentication will use ke.ghafari@epmistes.net by default
* Commands will reference project `exercice2-tp-gcp-328522` by default
Run `gcloud help config` to learn how to change individual settings

This gcloud configuration is called [default]. You can create additional configurations if you work with multip
ounts and/or projects.
Run `gcloud topic configurations` to learn more.
```

2°) Script d'automatisation avec gcloud.

On exécute une par une ces lignes de commande dans le cloud Shell, on a alors déployé une infrastructure en ligne de commande.

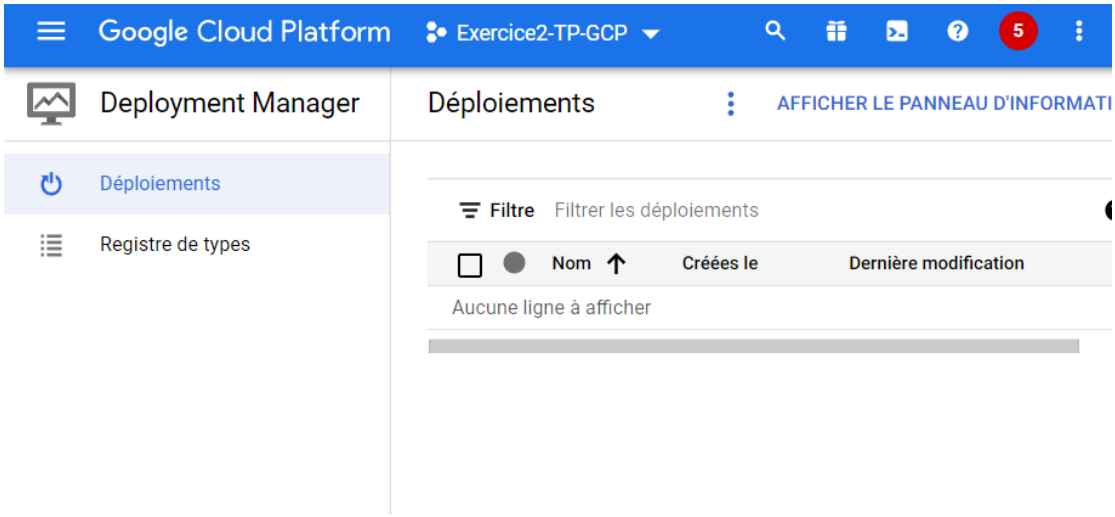
```
#!/bin/bash
Write-Host "Create VPC and Subnet"echo "
1- Create front-end network"
gcloud compute networks create frontend-net
Write-Host "1.1- Create front-end sub-networks
gcloud compute networks subnets create frontend-subnet --range='10.0.0.0/24' --network='frontend-net' --region='europe-central2'
Write-Host  "2- Create back-end network"
gcloud compute networks create backend-net
Write-Host  "2.1- Create back-end sub-networks
gcloud compute networks subnets create backend-subnet --range='10.0.0.0/24' --network='backend-net' --region='europe-central2'
Write-Host  "Creating Kali instance for front-end"
gcloud compute instances create kali-1 --tags=vmfe\
  --metadata startup-script='
  #!/bin/bash
  sudo su -
  apt-get update
  # TO DO: Install KALI Tools
  EOF'
Write-Host "Creating second Kali instance for back-end"
gcloud compute instances create kali-1 --tags=vmbe\
  --metadata startup-script='
  #!/bin/bash
  sudo su -
  apt-get update
  # TO DO: Install KALI Tools
  EOF'
Write-Host  "Adding firewall rules"
gcloud compute firewall-rules create allow-ingress-admin-backend-net --direction=INGRESS --priority=1000
--network=lab-net --action=ALLOW --rules=tcp:22,tcp:3389,tcp:443,icmp --source-ranges=0.0.0.0/0 --target-tags=vmbe
gcloud compute firewall-rules create allow-ingress-admin-frontend-net --direction=INGRESS --priority=1000
--network=lab-net --action=ALLOW --rules=all --source-ranges=0.0.0.0/0 --target-tags=vmfe
Write-Host "Done"
```

On peut aussi supprimer ces instances, par le script de suppression suivant :

```
#!/bin/bash

echo "Deleting instances..."
gcloud compute instances delete vm-fe -q
gcloud compute instances delete vm-be -q

echo "Removing firewall rules..."
gcloud compute firewall-rules delete allow-ingress-admin-backend-net -q
gcloud compute firewall-rules delete allow-ingress-insecure-frontend-net -q

echo "Removing subnets and network..."
gcloud compute networks subnets delete backend-subnet -q
gcloud compute networks subnets delete frontend-subnet -q
gcloud compute networks delete frontend-net -q
gcloud compute networks delete backend-net -q

echo "Done"
```

Exercice 3/6 : Google Deployment.

On active l'API Google Deployment Manager, on suit les étapes de configuration de l'API. Il faut au préalable créer un compte de service via l'onglet IAM et Services, pour pouvoir utiliser cet API.



A présent, nous allons utiliser cet API, afin de déployer automatiquement l'infrastructure semblable à l'exercice 1.

Tout d'abord, il est nécessaire de créer un fichier de configuration de l'infrastructure voulue, nous allons l'éditer sous Visual Studio Code, il sera au format YALM.

Ce fichier de configuration (vm-gcd.yml) est présent dans notre GitHub :

https://github.com/ghafari-web/gcp_automation/blob/main/vm-gcd.yml

Voici un extrait :

```yaml
resources:
- type: compute.v1.instance
  name: vm-fe
  properties:
    zone: europe-central2-a
    machineType: https://www.googleapis.com/compute/v1/projects/exercice2-tp-gcp-328522/zones/europe-central2-a/machineTypes/f1-micro
    disks:
    - deviceName: boot
      type: PERSISTENT
      boot: true
      autoDelete: true
      initializeParams:
        sourceImage: https://www.googleapis.com/compute/v1/projects/debian-cloud/global/images/family/debian-9
    networkInterfaces:
    - network: $(ref.frontend-net.selfLink)
      subnetwork: $(ref.frontend-sub.selfLink)
      accessConfigs:
      - name: External NAT
        type: ONE_TO_ONE_NAT
- type: compute.v1.network
  name: frontend-net
  properties:
    autoCreateSubnetworks: false
- name: frontend-sub
  type: compute.v1.subnetwork
  properties:
```

Ensuite, depuis le cloud Shell de GCP, on se connecte à notre GitHub, afin d'accéder au fichier de configuration de notre infrastructure.

```
ke_ghafari@cloudshell:~ (exercice2-tp-gcp-328522)$ git clone https://github.com/ghafari-web/gcp_automation
Cloning into 'gcp_automation'...
remote: Enumerating objects: 36, done.
remote: Counting objects: 100% (36/36), done.
remote: Compressing objects: 100% (34/34), done.
remote: Total 36 (delta 8), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (36/36), done.
ke_ghafari@cloudshell:~ (exercice2-tp-gcp-328522)$ ls
cloudshell_open  gcp_automation
ke_ghafari@cloudshell:~ (exercice2-tp-gcp-328522)$ cd ./gcp_automation
ke_ghafari@cloudshell:~/gcp_automation (exercice2-tp-gcp-328522)$ ls
vm-gcd.yml  vm-sdk.sh
ke_ghafari@cloudshell:~/gcp_automation (exercice2-tp-gcp-328522)$
```

Le fichier vm-gcd.yml est maintenant accessible.

Maintenant, on déploie l'infrastructure avec la commande suivante :

```
tomation (exercice2-tp-gcp-328522)$ gcloud deployment-manager deployments create deployment-00 --config vm-gcd.yml
ent is b'BzIjqqSJHVYUiwx6BHtH0Q=='
1634480887229-5ce8d3cacee2a-3f667592-ee05b734]...working...
```

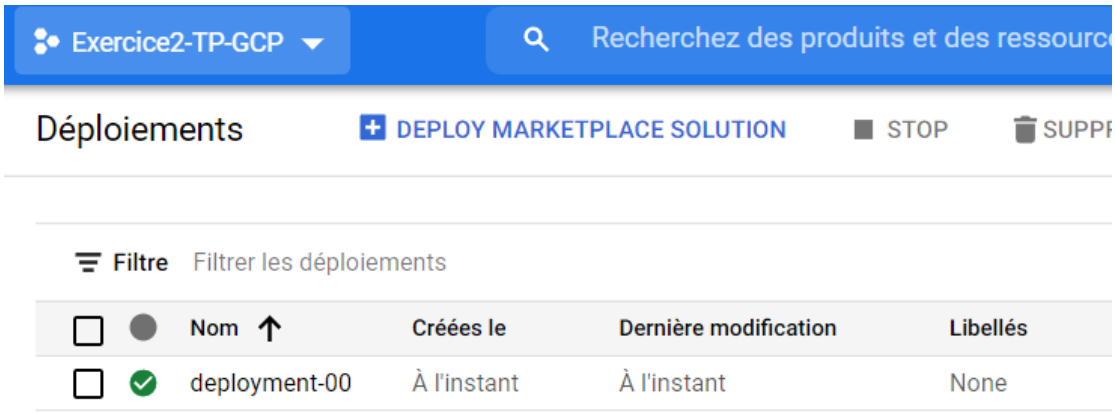
L’infrastructure à été déployé dans notre cloud GCP.

```
NAME: backend-net
TYPE: compute.v1.network
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: backend-sub
TYPE: compute.v1.subnetwork
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: backtofront
TYPE: gcp-types/compute-v1:compute.networks.addPeering
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: frontend-net
TYPE: compute.v1.network
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: frontend-sub
TYPE: compute.v1.subnetwork
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: fronttoback
TYPE: gcp-types/compute-v1:compute.networks.addPeering
STATE: COMPLETED
ERRORS: []
INTENT:
```

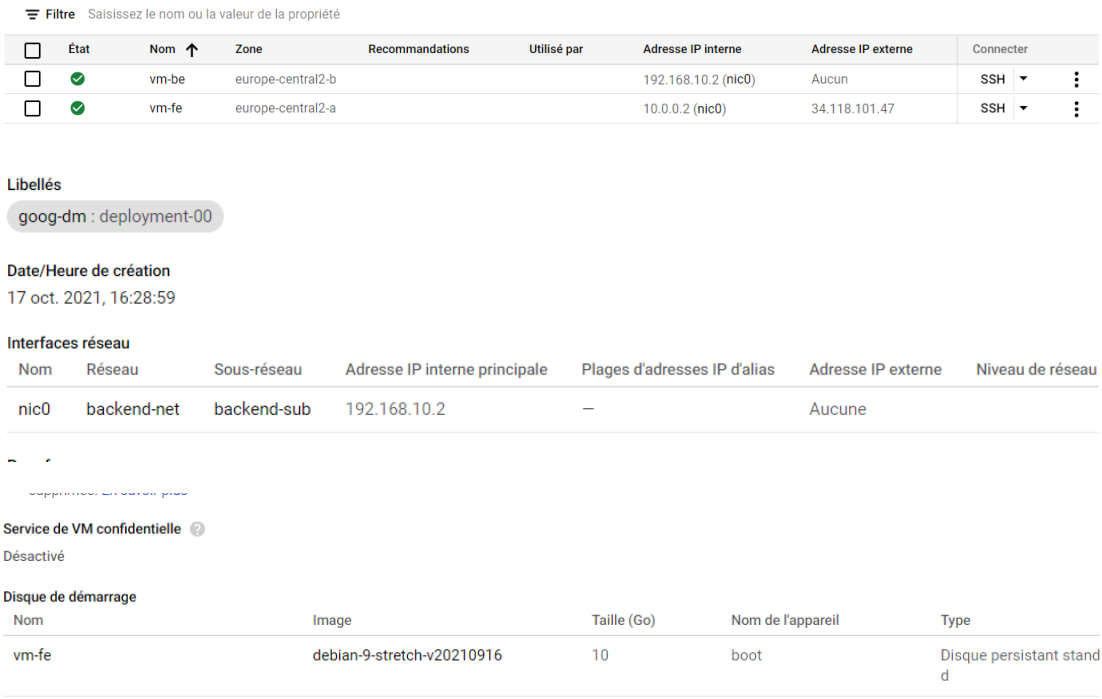
```
NAME: icmp-backend-net
TYPE: compute.v1.firewall
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: icmp-frontend-net
TYPE: compute.v1.firewall
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: ssh-backend-net
TYPE: compute.v1.firewall
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: ssh-frontend-net
TYPE: compute.v1.firewall
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: vm-be
TYPE: compute.v1.instance
STATE: COMPLETED
ERRORS: []
INTENT:

NAME: vm-fe
TYPE: compute.v1.instance
STATE: COMPLETED
ERRORS: []
INTENT:
```

Résultat sur le cloud GCP :

Le déploiement à bien eu lieu.



Les machines virtuelles ont bien été créés et configurer comme voulu.



L'interface réseau a bien été configuré et les règles de firewall bien prise en compte :

Nom	Réduire le nœud	égion	Sous-réseaux	MTU	Mode	Plages d'adresses IP	Passerelles	Règles de pare-feu	Routage dynamique glo
backend-net			1	1460	Personnalisé			2	Désactivé
		europe-central2	backend-sub			192.168.10.0/24	192.168.10.1		
default			28	1460	Automatique			3	Désactivé
frontend-net			1	1460	Personnalisé			2	Désactivé
		europe-central2	frontend-sub			10.0.0.0/24	10.0.0.1		

L'appairage des réseaux a bien eu lieue :

Nom	Votre réseau VPC	Réseau VPC appairé	ID du projet appairé	État	Échanger les routes personnalisées	Échanger les routes de sous-rése
vpc-1-2	backend-net	frontend-net	exercice2-tp-gcp-328522	Actif	Aucun	Exporter des routes de sous-ré
vpc-2-1	frontend-net	backend-net	exercice2-tp-gcp-328522	Actif	Aucun	Exporter des routes de sous-ré

On peut supprimer automatiquement le déploiement créer avec la commande suivante, il faut au préalable arréter les VM :

```
ke_ghafari@cloudshell:~ (exercice2-tp-gcp-328522)$ gcloud deployment-manager deployments delete deployment-00
The following deployments will be deleted:
- deployment-00

Do you want to continue (y/N)?  y

Waiting for delete [operation-1634482895106-5ce8db45ab1a7-87f5d33d-5e509f73]...
```

```
ke_ghafari@cloudshell:~/gcp_automation (exercice2-tp-gcp-328522)$ gcloud deployment-manager deployments delete deployment-00
The following deployments will be deleted:
- deployment-00

Do you want to continue (y/N)?  y

Waiting for delete [operation-1634483399785-5ce8dd26f7d5f-8d691a34-d3002466]...done.
Delete operation operation-1634483399785-5ce8dd26f7d5f-8d691a34-d3002466 completed successfully.
```

Exercice 4 : Ansible

Tout d'abord, on installe Ansible sur GCP

```
ke_ghafari@cloudshell:~ (exercice2-tp-gcp-328522)$ sudo apt install python-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-pip is already the newest version (18.1-5).
0 upgraded, 0 newly installed, 0 to remove and 7 not upgraded.
ke_ghafari@cloudshell:~ (exercice2-tp-gcp-328522)$ pip install -U pip
********************************************************************************
Python 2 is deprecated. Upgrade to pip3 as soon as possible.
See https://cloud.google.com/python/docs/python2-sunset

To suppress this warning, create an empty ~/.cloudshell/no-pip-warning file.
The command will automatically proceed in 5 seconds or on any key.
********************************************************************************
Collecting pip
  Downloading https://files.pythonhosted.org/packages/27/79/8a850fe3496446ff0d584327ae44e750
    100% |[redacted]| 1.5MB 671kB/s
Installing collected packages: pip
Successfully installed pip-20.3.4
ke_ghafari@cloudshell:~ (exercice2-tp-gcp-328522)$ pip install -U ansible
********************************************************************************
Python 2 is deprecated. Upgrade to pip3 as soon as possible.
See https://cloud.google.com/python/docs/python2-sunset

To suppress this warning, create an empty ~/.cloudshell/no-pip-warning file.
The command will automatically proceed in 5 seconds or on any key.
********************************************************************************
```

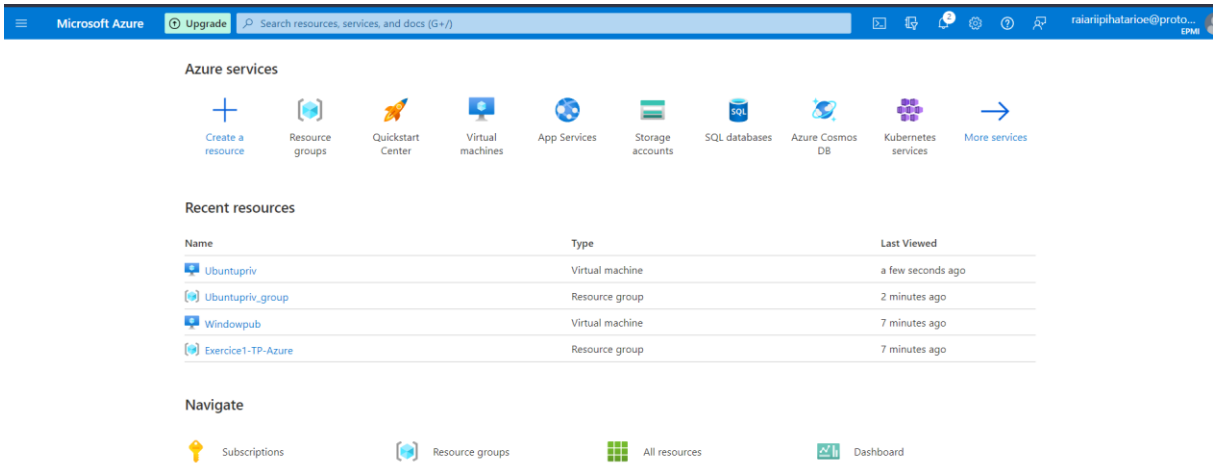
On installe les modules Python « requests », « Google-Auth » et « libcloud »

```
ke_ghafari@cloudshell:~ (exercice2-tp-gcp-328522)$ pip install requests google-auth apache-libcloud
********************************************************************************
Python 2 is deprecated. Upgrade to pip3 as soon as possible.
See https://cloud.google.com/python/docs/python2-sunset

To suppress this warning, create an empty ~/.cloudshell/no-pip-warning file.
The command will automatically proceed in 5 seconds or on any key.
********************************************************************************
WARNING: pip is being invoked by an old script wrapper. This will fail in a future version of pip.
Please see https://github.com/pypa/pip/issues/5599 for advice on fixing the underlying issue.
To avoid this problem you can invoke Python with '-m pip' instead of running pip directly.
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no
2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-proce
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: requests in /usr/local/lib/python2.7/dist-packages (2.26.0)
Requirement already satisfied: google-auth in /usr/local/lib/python2.7/dist-packages (1.35.0)
Collecting apache-libcloud
  Downloading apache_libcloud-2.8.3-py2.py3-none-any.whl (3.4 MB)
     |[redacted]| 3.4 MB 11.9 MB/s
```

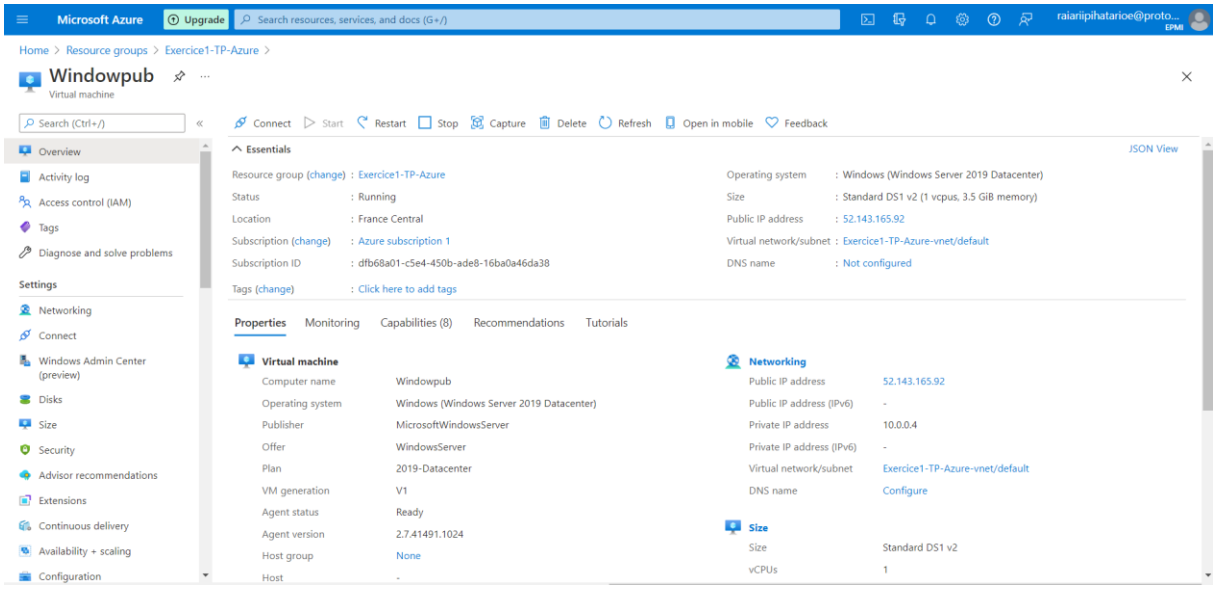
Réseaux virtuels IaaS (Microsoft Azure)

Exercice 1 : premiers pas sur Azure.

Sous Azure nous avons créé un groupe de ressource nommé « Exercice1-TP-Azure » qui contient 2 serveurs (linux et window):



Le serveur Window possède une IP publique 52.143.165.92 et un port ouvert pour pouvoir se connecter. (Ici le port 3389 en utilisant le contrôle à distance « RDP »)



Attach network interface Detach network interface Feedback

windowpub468

IP configuration

ipconfig1 (Primary)

Network Interface: windowpub468 Effective security rules Troubleshoot VM connection issues Topology

Virtual network/subnet: Exercice1-TP-Azure-vnet/default NIC Public IP: **52.143.165.92** NIC Private IP: **10.0.0.4** Accelerated networking: **Enabled**

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group Windowpub-nsg (attached to network interface: windowpub468)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Le serveur Linux possède aucune IP publique et seulement une IP privée qui est 192.168.10.4.

Donc ce serveur est « privé » et la seule manière de se connecter est via le 1er serveur en utilisant l'adresse IP privée.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) raiariipihatarioe@proto...

Home >

ubuntuprivate
Virtual machine

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Extensions
Continuous delivery
Availability + scaling
Configuration
Identity

Connect Start Restart Stop Capture Delete Refresh Open in mobile Feedback

Resource group (change) : Exercice1-TP-Azure
Status : Running
Location : France Central
Subscription (change) : Azure subscription 1
Subscription ID : dfb68a01-c5e4-450b-ade8-16ba0a46da38
Tags (change) : Click here to add tags

Operating system : Linux (ubuntu 20.04)
Size : Standard DS1 v2 (1 vcpus, 3.5 GiB memory)
Public IP address : -
Virtual network/subnet : Exercice1-TP-Azure-vnet/Routeur
DNS name : -

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine

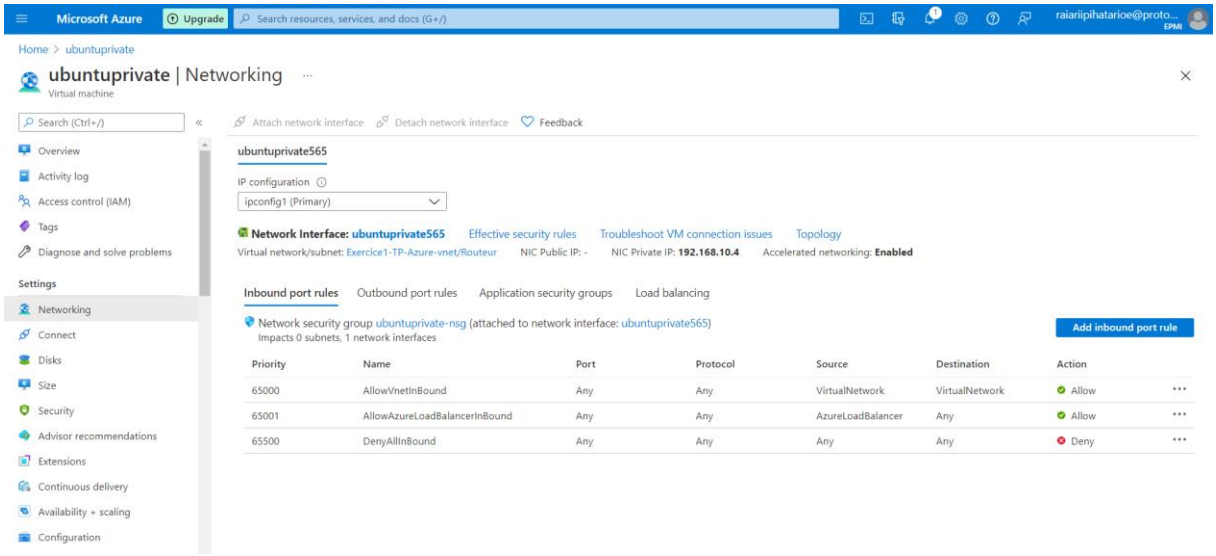
Computer name	ubuntuprivate
Operating system	Linux (ubuntu 20.04)
Publisher	canonical
Offer	0001-com-ubuntu-server-focal
Plan	20_04-lts
VM generation	V1
Agent status	Ready
Agent version	2.4.0.2
Host group	None
Host	-

Networking

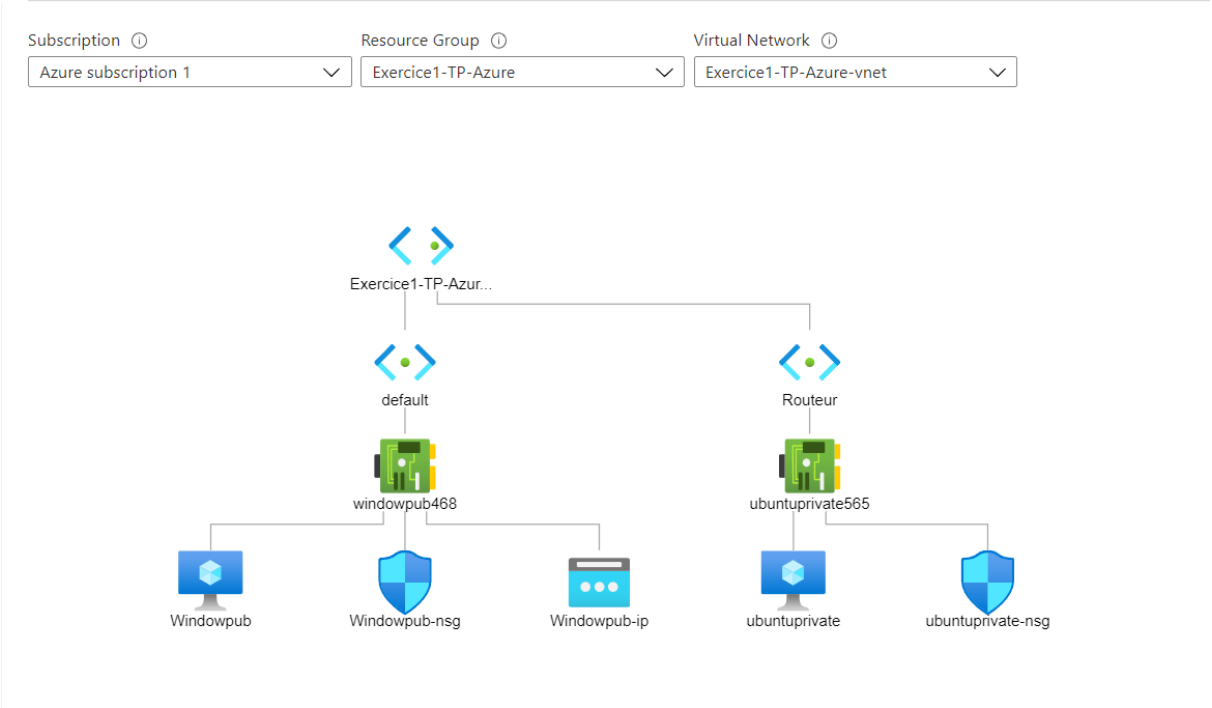
Public IP address	-
Public IP address (IPv6)	-
Private IP address	192.168.10.4
Private IP address (IPv6)	-
Virtual network/subnet	Exercice1-TP-Azure-vnet/Routeur
DNS name	-

Size

Size	Standard DS1 v2
vCPUs	1



Voici le diagramme du réseau obtenu avec les 2 serveurs :

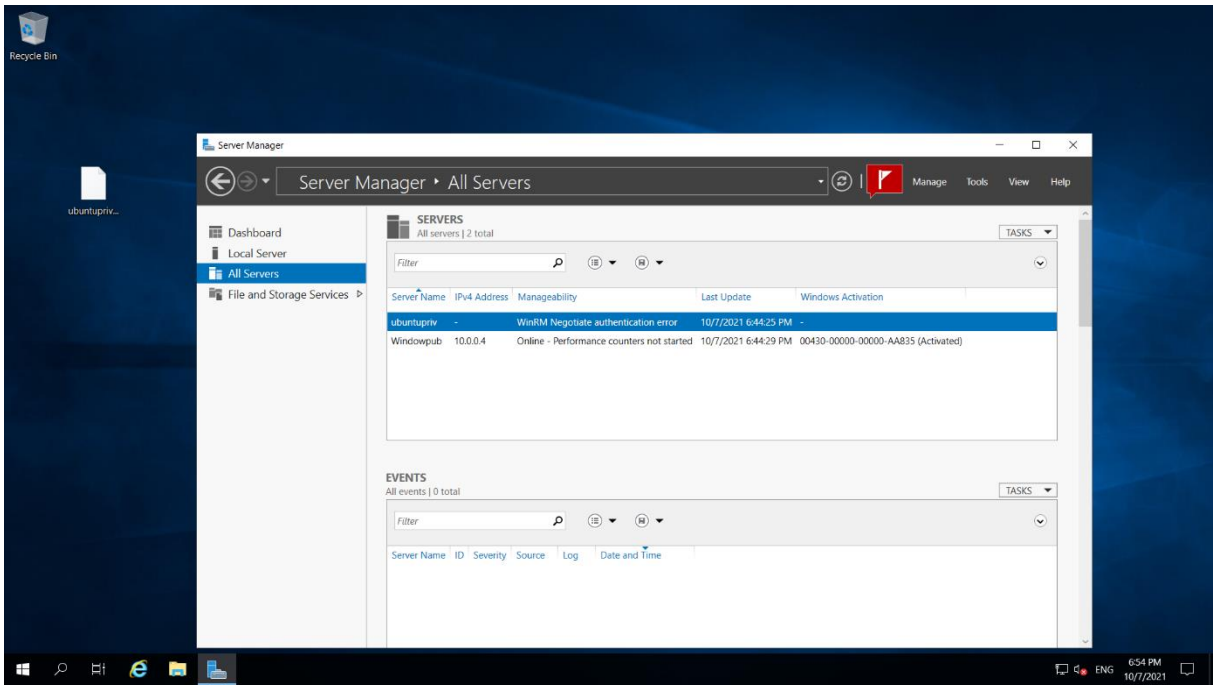


Vérifications :

- Essayer de vous connecter sur le serveur ayant une adresse IP publique. Attention les règles de sécurité (NSG) doivent être modifiée pour autoriser RDP (TCP/3389) ou SSH (TCP/22).

En utilisant le logiciel RDP fournie par Microsoft on arrive à se connecter sur notre serveur public.

Nous voilà sur notre serveur public.



1°) Essayer de pinger le serveur VMBE depuis le serveur VMFE :

Une fois arriver sur le serveur public on essaye de lancer une commande ping vers le serveur privé pour voir si la connexion est bien présente.

L'adresse IP de nôtre serveur privé est 192.168.10.4, on lance la commande « PING » et voici ce qu'on obtient.

```
lolo@ubuntuprivate: ~
Microsoft Windows [Version 10.0.17763.2183]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Lolo>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:
Reply from 192.168.10.4: bytes=32 time=2ms TTL=64
Reply from 192.168.10.4: bytes=32 time=1ms TTL=64
Reply from 192.168.10.4: bytes=32 time=1ms TTL=64
Reply from 192.168.10.4: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\Lolo>ssh
```

Le serveur nous répond donc la connexion entre les 2 serveurs est fonctionnel.

2°) Lancement de la commande SSH pour se connecter avec la clé privée.

```
lolo@ubuntuprivate: ~
C:\Users\Lolo>ssh -i C:\Users\Lolo\Desktop\ubuntupriv_key.pem lolo@192.168.10.4
The authenticity of host '192.168.10.4 (192.168.10.4)' can't be established.
ECDSA key fingerprint is SHA256:GdjqFLLnh1I/YIcuZRa2edZu3E+vkDceTbqsq82fbrI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.4' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.8.0-1042-azure x86_64)

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

  System information as of Sat Oct  9 17:57:41 UTC 2021

  System load:  0.08              Processes:             118
  Usage of /:   4.5% of 28.90GB   Users logged in:       0
  Memory usage: 7%                IPv4 address for eth0: 192.168.10.4
  Swap usage:   0%

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

lolo@ubuntuprivate:~$
```

La connexion à réussi.

Exercice 2 : Création d'un service Web sous Azure.

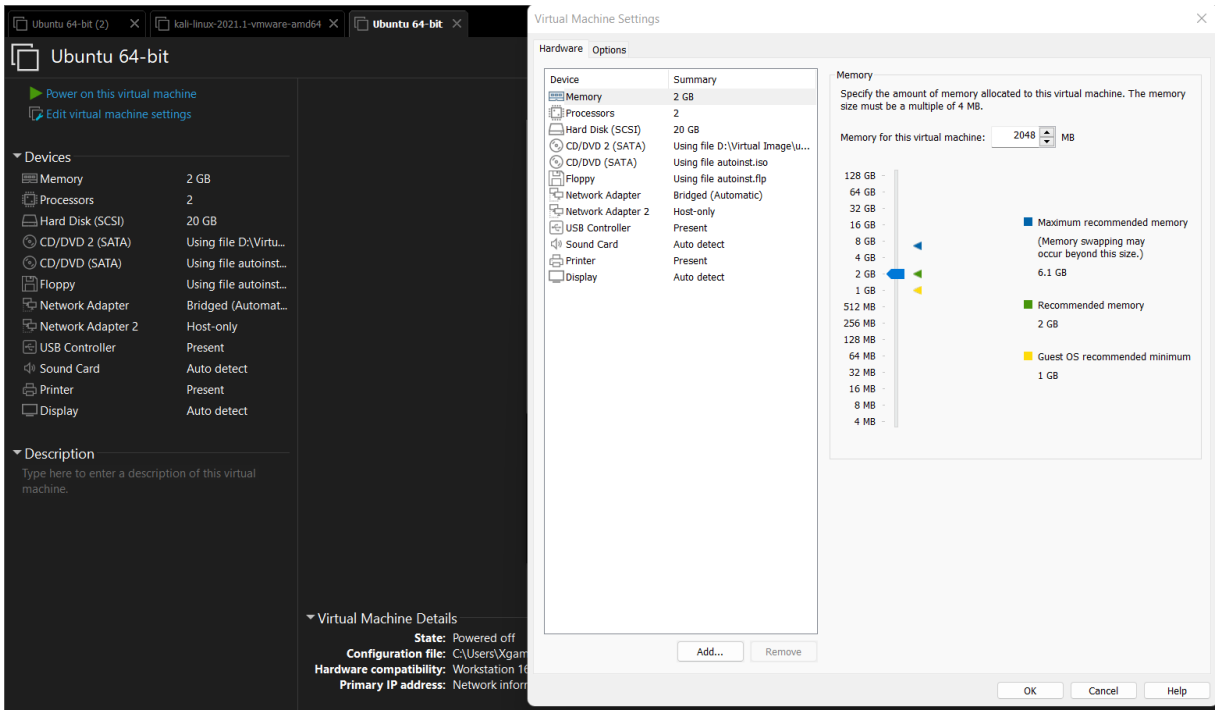
Réseaux virtuels (Virtualisation avec VMware Workstation)

Pour ce TP nous utiliserons VMware Workstation, nous avons créé 3 machines sous une distribution Linux :

Machine 1 :

- 2 interfaces réseaux :
    1. Interface 1 en mode NAT (accès Internet)
    2. Interface 2 en mode « réseau privé d'hôte » 192.168.24.0/24

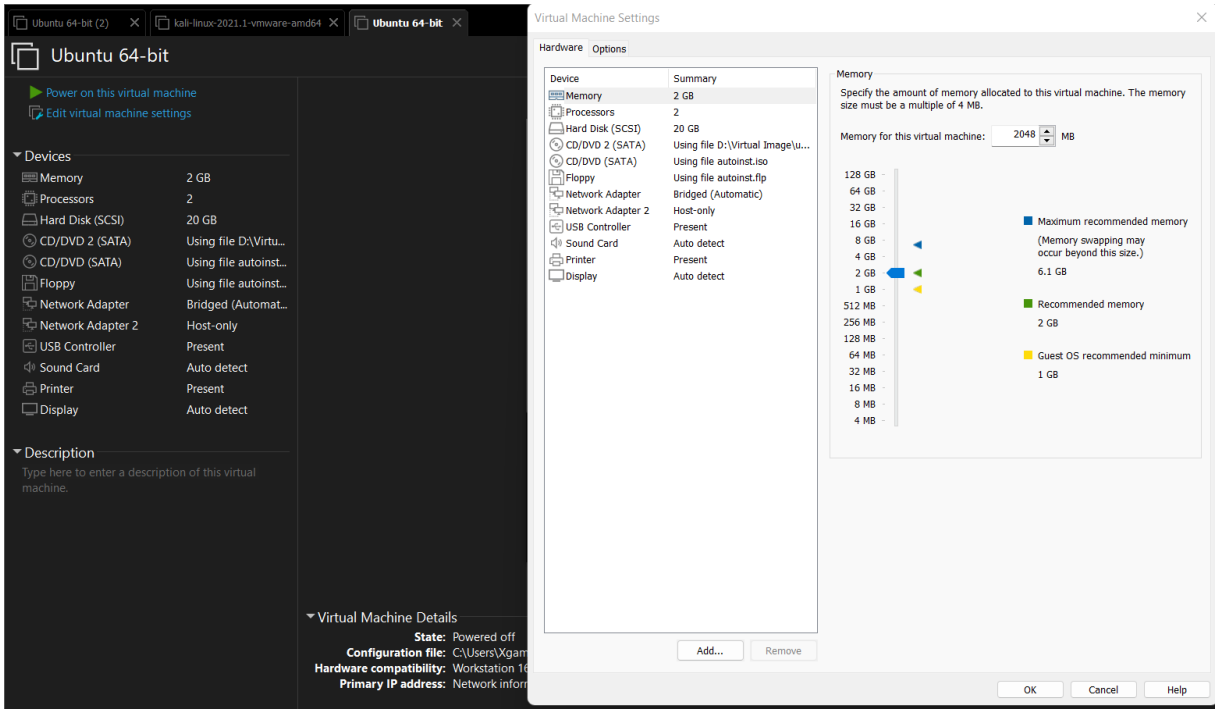
Adresse IP (private-host) : 194.168.24.2



Machine 2 :

- 2 interfaces réseaux :
    1. Interface 1 en accès par Pont (accès Internet)
    2. Interface 2 en mode « réseau privé d'hôte » 192.168.24.0/24

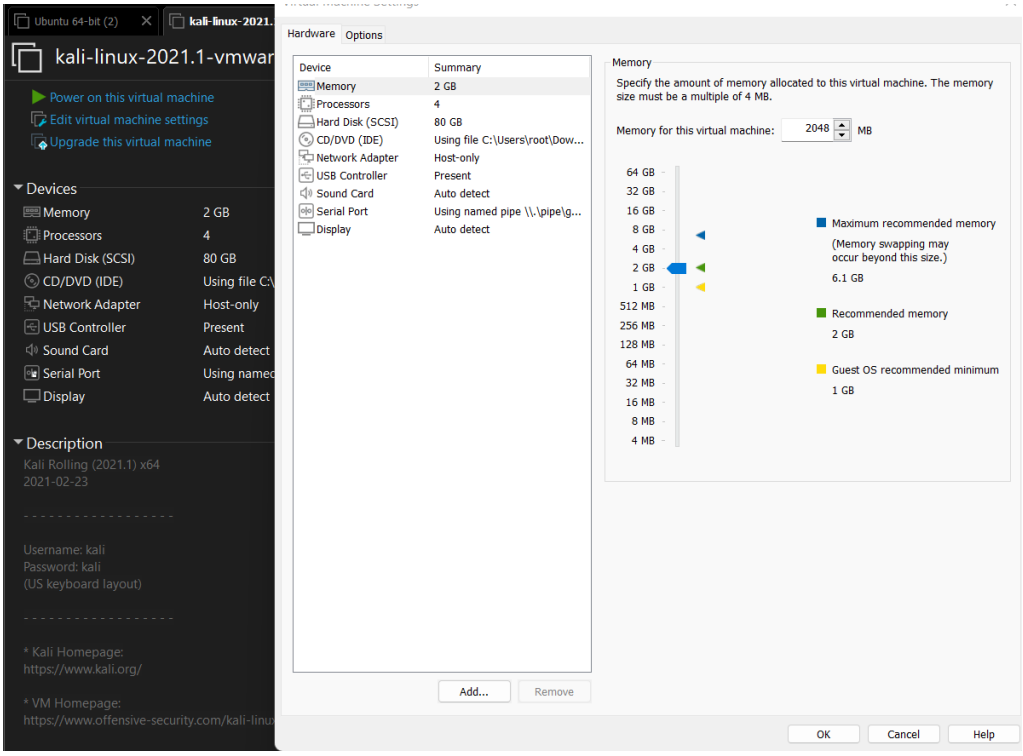
Adresse IP (private-host) : 192.168.24.1



Machine 3 :

- Interface réseau :
  1. Interface 1 en mode « réseau privé d'hôte » 192.168.24.0/24

Adresse IP (private-host) : 194.168.24.3



1°) Vérifier que les machines 1, 2 et 3 peuvent communiquer via le réseau privé d'hôtes.

On utilise la commande ping avec les adresses IP (private-host) pour vérifier qu'elles communiquent ensemble. On utilise la machine 1 qui a pour IP 192.168.24.2

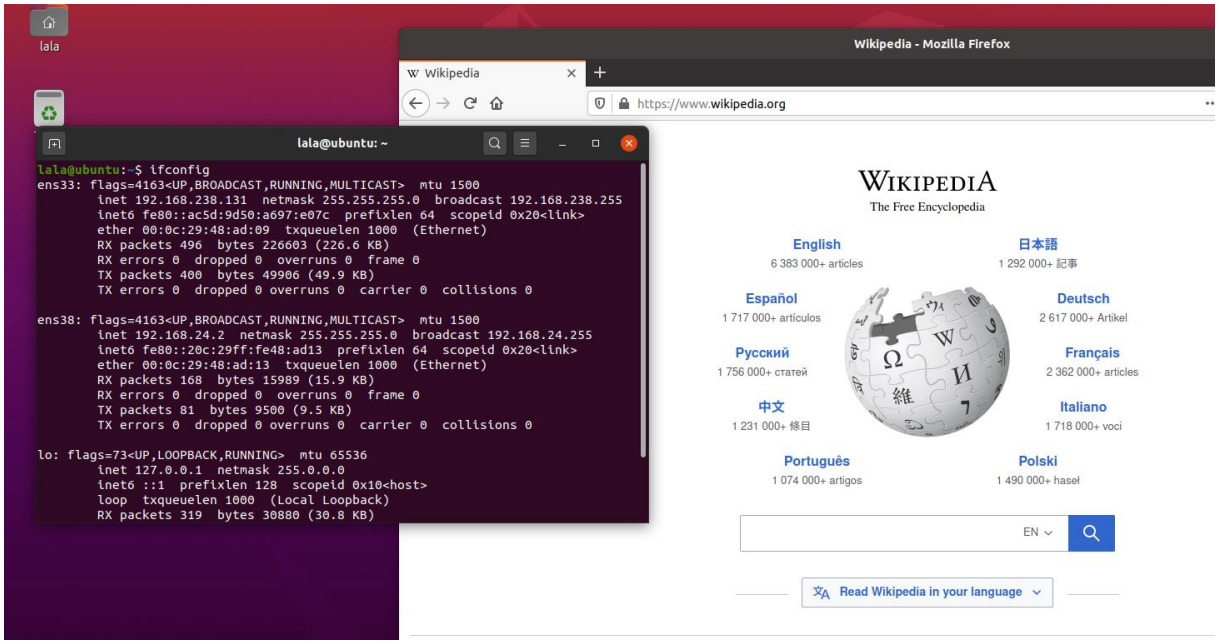
```
lala@ubuntu: ~
lala@ubuntu: ~        lala@ubuntu: ~
lala@ubuntu:~$ ping 192.168.24.1
PING 192.168.24.1 (192.168.24.1) 56(84) bytes of data.
64 bytes from 192.168.24.1: icmp_seq=1 ttl=128 time=0.525 ms
64 bytes from 192.168.24.1: icmp_seq=2 ttl=128 time=0.588 ms
64 bytes from 192.168.24.1: icmp_seq=3 ttl=128 time=1.10 ms
64 bytes from 192.168.24.1: icmp_seq=4 ttl=128 time=1.04 ms
64 bytes from 192.168.24.1: icmp_seq=5 ttl=128 time=0.806 ms
```

```
lala@ubuntu: ~
lala@ubuntu:~$ ping 192.168.24.3
PING 192.168.24.3 (192.168.24.3) 56(84) bytes of data.
64 bytes from 192.168.24.3: icmp_seq=1 ttl=128 time=0.953 ms
64 bytes from 192.168.24.3: icmp_seq=2 ttl=128 time=0.989 ms
64 bytes from 192.168.24.3: icmp_seq=3 ttl=128 time=1.45 ms
64 bytes from 192.168.24.3: icmp_seq=4 ttl=128 time=0.844 ms
64 bytes from 192.168.24.3: icmp_seq=5 ttl=128 time=1.92 ms
64 bytes from 192.168.24.3: icmp_seq=6 ttl=128 time=1.48 ms
64 bytes from 192.168.24.3: icmp_seq=7 ttl=128 time=0.816 ms
64 bytes from 192.168.24.3: icmp_seq=8 ttl=128 time=1.43 ms
64 bytes from 192.168.24.3: icmp_seq=9 ttl=128 time=1.84 ms
64 bytes from 192.168.24.3: icmp_seq=10 ttl=128 time=0.690 ms
64 bytes from 192.168.24.3: icmp_seq=11 ttl=128 time=0.621 ms
64 bytes from 192.168.24.3: icmp_seq=12 ttl=128 time=1.52 ms
64 bytes from 192.168.24.3: icmp_seq=13 ttl=128 time=1.51 ms
64 bytes from 192.168.24.3: icmp_seq=14 ttl=128 time=0.762 ms
64 bytes from 192.168.24.3: icmp_seq=15 ttl=128 time=0.713 ms
64 bytes from 192.168.24.3: icmp_seq=16 ttl=128 time=0.657 ms
64 bytes from 192.168.24.3: icmp_seq=17 ttl=128 time=1.56 ms
```

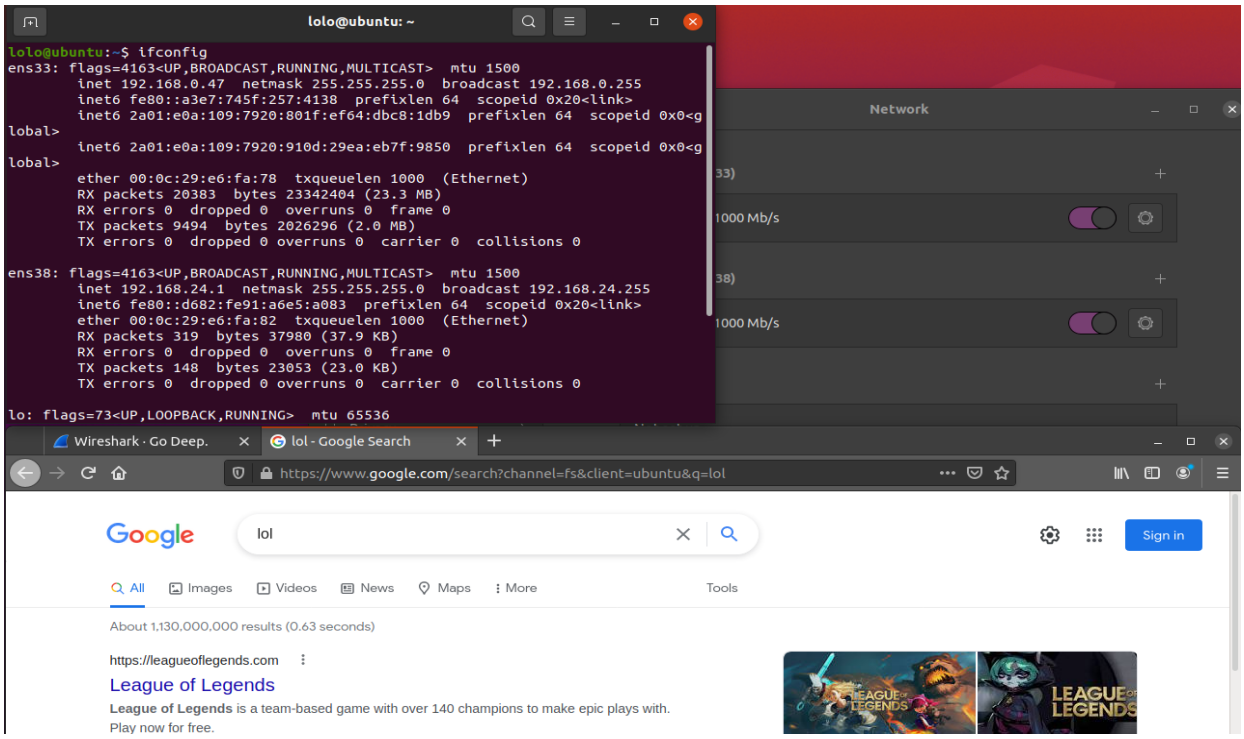
Les machines communiquent entre elles donc le réseau Host est fonctionnel.

2°) <u>Vérifier que les machines 1 et 2 accèdent à Internet. Noter les adresses IP de leur interface « Internet ». Que notez-vous ?</u>

<u>Machine 1 NAT :</u>



Machine 2 Bridge :



Les 2 machines sont connectées à interface via leur 1eres interfaces on note leurs IP.

IP Machine1(NAT): 192.168.238.131

IP Machine 2(BRIDGE): 192.168.0.47

On remarque que l'adresse IP de la machine 2(Bridge) est sur le même réseau que l'adresse IP de l'hyperviseur et celle de la machine 1 est sur le même réseau que l'adaptateur Vmnet8 (Adaptateur NAT de VMware)

```
C:\Users\Xgame456>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6. . . . . . . . . . . . . .: 2a01:e0a:109:7920:5802:9da8:d825:d9e6
   Adresse IPv6 temporaire . . . . . . . .: 2a01:e0a:109:7920:2c92:a16b:50c9:451c
   Adresse IPv6 temporaire . . . . . . . .: 2a01:e0a:109:7920:6c1a:f153:a4cc:6e57
   Adresse IPv6 temporaire . . . . . . . .: 2a01:e0a:109:7920:9dd9:381c:5586:d30d
   Adresse IPv6 temporaire . . . . . . . .: 2a01:e0a:109:7920:d49b:c1c0:824b:b6e8
   Adresse IPv6 de liaison locale. . . . .: fe80::5802:9da8:d825:d9e6%28
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.0.42
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : fe80::e69e:12ff:fe8c:33f6%28
                                            192.168.0.254

Carte Ethernet VirtualBox Host-Only Network :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::dd83:612:8330:1f54%30
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.24.0
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte inconnue Connexion au réseau local :
```

```
Carte Ethernet VMware Network Adapter VMnet1 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::6d25:6c23:8192:45c5%20
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.24.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet VMware Network Adapter VMnet8 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::f964:ce36:b088:8be0%17
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.238.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet VMware Network Adapter VMnet2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::973:a793:9b0e:e66b%29
   Adresse d'autoconfiguration IPv4 . . . : 169.254.230.107
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet VMware Network Adapter VMnet3 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::6ce2:a46c:90d0:3973%31
   Adresse d'autoconfiguration IPv4 . . . : 169.254.57.115
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . :
```

3°) Permettre à la machine 3 d'accéder à Internet via la machine 1.

Pour répondre à cette question nous avons besoin de configuré notre machine 1 afin qu'elle fonctionne comme un routeur. Voici les commandes utilisées sous le terminal de la machine 1.

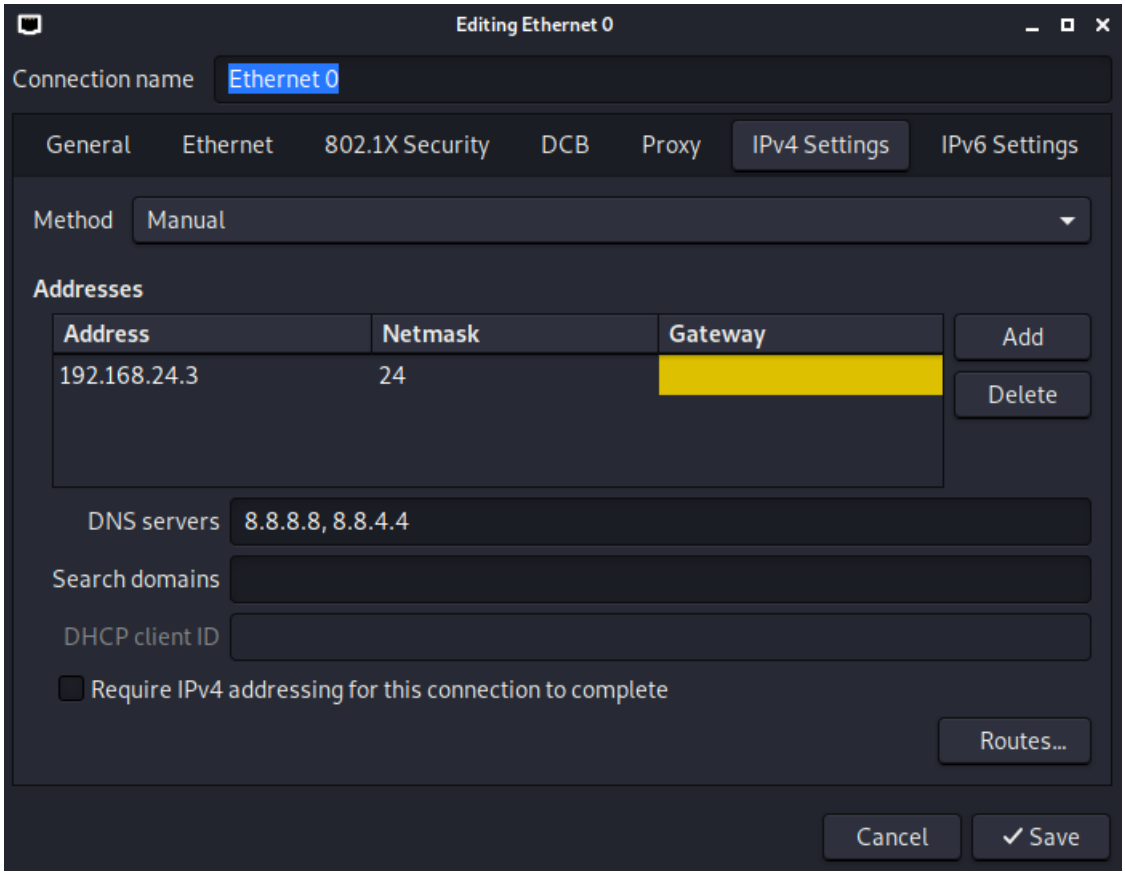
Premièrement on active le mode FORWARD qui permet à la machine 1 de laisser passez les packets extérieur « à travers » elle.

```
lala@ubuntu: ~
lala@ubuntu:~$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for lala:
Sorry, try again.
[sudo] password for lala:
net.ipv4.ip_forward = 1
lala@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.238.131  netmask 255.255.255.0  broadcast 192.168.238.255
        inet6 fe80::ac5d:9d50:a697:e07c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:48:ad:09  txqueuelen 1000  (Ethernet)
        RX packets 7407  bytes 10704200 (10.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3954  bytes 259272 (259.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.24.2  netmask 255.255.255.0  broadcast 192.168.24.255
        inet6 fe80::20c:29ff:fe48:ad13  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:48:ad:13  txqueuelen 1000  (Ethernet)
        RX packets 600  bytes 65616 (65.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 188  bytes 20467 (20.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ensuite nous allons créer une route vers l'interface réseau « ens33 » qui est l'interface réseau NAT et nous allons dire à notre machine 1 d'accepter les paquets venant du sous réseau 192.168.0.0/16. Donc les paquets qui passe par l'interface « ens38) qui est l'interface réseau Private-Host.

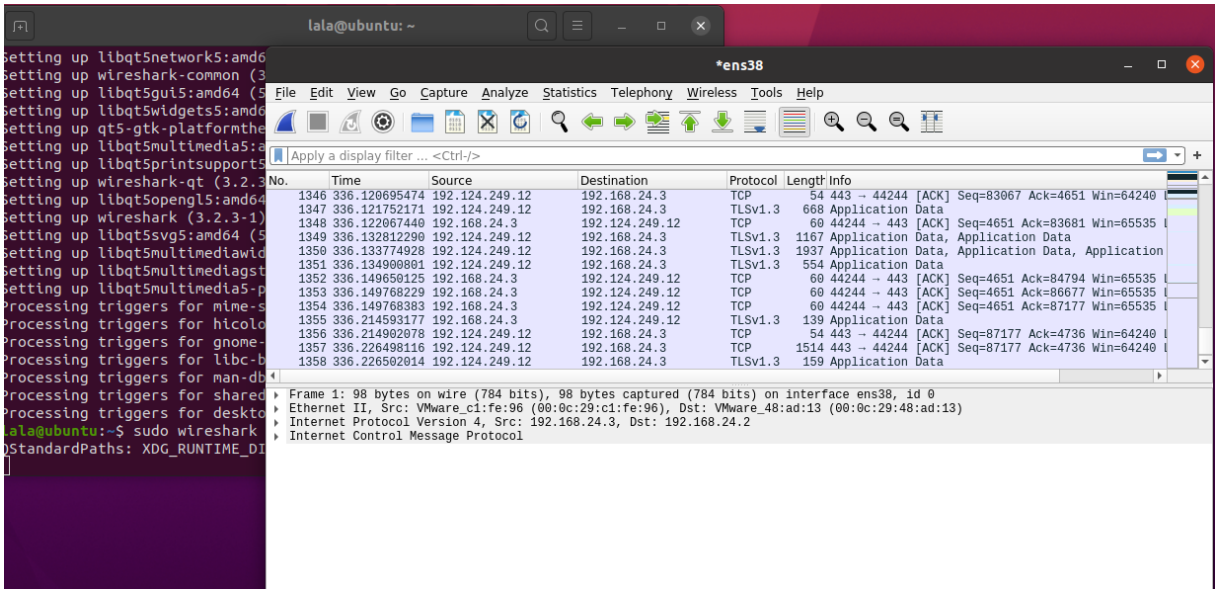
```
lala@ubuntu: ~
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 275  bytes 25217 (25.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 275  bytes 25217 (25.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lala@ubuntu:~$ sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE
lala@ubuntu:~$ sudo iptables -I FORWARD -o ens33 -s 192.168.0.0/16 -j ACCEPT
lala@ubuntu:~$ sudo iptables -I INPUT -s 192.168.0.0/16 -j ACCEPT
lala@ubuntu:~$ sudo wireshark
sudo: wireshark: command not found
lala@ubuntu:~$ wireshark

Command 'wireshark' not found, but can be installed with:

sudo apt install wireshark-qt

lala@ubuntu:~$ sudo apt install wireshark-qt
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

On configure aussi notre machine 3 :



Pour la configuration de notre machine 3, il faut rajouter comme DNS celui de Google (8.8.8.8).

Nous lançons wireshark sur la machine 1 pour voir en détails les informations qui transite lorsque que la machine 3 va faire une recherche internet.

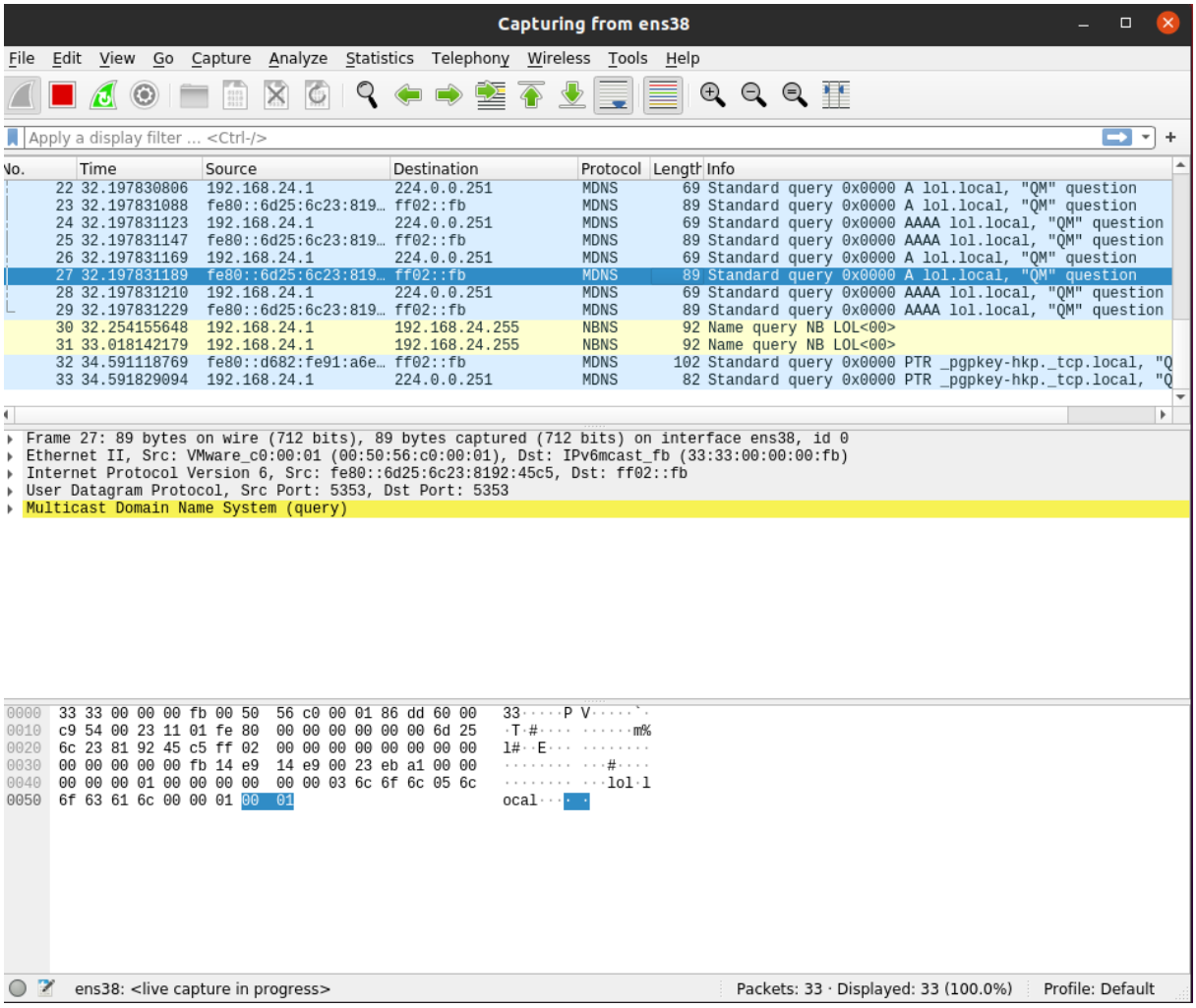


On remarque grâce à Wireshark que des informations transite bien de l'ip source 192.168.24.3 (Machine 3) vers un IP extérieur.

4°) <u>Tenter d'autoriser l'accès à Internet de la machine 3 via la machine 2. Que se passe-t-il ? Expliquer.</u>

Pour cette question on refait la méthode citée précédemment mais sur la machine 2.

Or après avoir fait les mêmes manipulations nous obtenons la fenêtre ci-dessous avec Wireshark.



On remarque à droite de la fenêtre Wireshark dans la colonne info des mots tel que « lol.local »ou bien « tcp.local » cela signifie que les paquets qui transit via la machine 2 n'est pas ceux de la machine 3 mais de l'hyperviseur (recherche « lol » sur google).

Donc avec une connexion bridge il n'est pas possible de faire transiter des paquets via une machine car elle utilise le réseau physique de l'hyperviseur, il faudra aussi configurer l'hyperviseur pour qu'il laisse aussi passez les paquets.