Esteban, Floren, Gauvain

Projet 1

Génèse

1. Préparation du projet

- Floren : l'architecte
- Esteban : le soutien moral
- Gauvain : la petite secrétaire

Notes

Il se peut que les lignes de code affichées dans les captures d'écran ne soient pas 100% conformes avec les blocs de code tapés au-dessus. C'est normal : nous expérimentons au fur et à mesure, et quand la capture d'écran est faite, il se peut que nous ne nous apercevions d'une coquille ou d'un oubli que bien plus tard. Et qu'un paquet installé (genre NMAP) soit désinstallé plus tard, faute d'usage. Règle du **"moins de paquet = moins de surface d'attaque"**.

Le résultat est normalement affiché en capture d'écran, mais en cas de discordance, les blocs de code commentés font foi.

2. Définir l'architecture

A. Les Machines Virtuelles

ROCKY_LINUX - Installation

- Rocky Linux sur Hyperviseur
- Deux connexions réseau : en Accès par Pont ou Réseau NAT
- Pas de GUI

Nous avons décidé d'utiliser :

- 3 VMs Rocky Linux 9.7 (version Boot), les infos sur la version 10 faisant état d'une version peu stabilisée
- sur VirtualBox (par simplicité)

- En réseau NAT (pour avoir une plage réseau vraiment isolée)
- Pas de GUI

```
sudo dnf update -y
sudo dnf install -y firewalld nano curl wget

sudo systemctl enable --now firewalld
```

```
[root@osd1 ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-12-16 16:08:49 CET; 15min ago
       Docs: man:firewalld(1)
    Process: 782 ExecStartPost=/usr/bin/firewall-cmd --state (code=exited, status=0/SUCCESS)
   Main PID: 749 (firewalld)
      Tasks: 2 (limit: 10632)
     Memory: 40.4M (peak: 60.5M)
        CPU: 511ms
     CGroup: /system.slice/firewalld.service
             └─749 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

déc. 16 16:08:48 osd1 systemd[1]: Starting firewalld - dynamic firewall daemon...
déc. 16 16:08:49 osd1 systemd[1]: Started firewalld - dynamic firewall daemon.
[root@osd1 ~]#
```

Synchronisation des serveurs avec `chrony` : *Sur MON/MR*

```
nano /etc/chrony.conf

  allow 10.0.10.0/24
```

Sur OSD1

```
nano /etc/chrony.conf

  server 10.0.10.11 iburst
  peer 10.0.10.13 iburst
```

Sur OSD2

```
nano /etc/chrony.conf

  server 10.0.10.11 iburst
  peer 10.0.10.12 iburst
```

Rocky_MON [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
 GNU nano 5.6.1                                  /etc/chrony.conf
sourcedir /run/chrony-dhcp

# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift

# Allow the system clock to be stepped in the first three updates
# if its offset is larger than 1 second.
makestep 1.0 3

# Enable kernel synchronization of the real-time clock (RTC).
rtcsync

# Enable hardware timestamping on all interfaces that support it.
#hwtimestamp *

# Increase the minimum number of selectable sources required to adjust
# the system clock.
#minsources 2

# Allow NTP client access from local network.
allow 10.0.10.0/24
```

Rocky_OSD1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
 GNU nano 5.6.1                                  /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
server 10.0.10.11 iburst
peer 10.0.10.13 iburst
```

Rocky_OSD2 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
 GNU nano 5.6.1                                  /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
server 10.0.10.11 iburst
peer 10.0.10.12 iburst
```

Et on change les noms des machines :

```
sudo hostnamectl set-hostname ['monmgr', 'osd1', 'osd2']
```

B. Configuration du **bonding**

[REDHAT - Configure Network Bonding]

[Bonding in Rocky Linux]

- Mode *active-backup*
- Bridge dédié au **bond** *active-backup* dans le Ceph

Ajouter le bond :

```
sudo nmcli connection add type bond con-name bond0 ifname bond0 mode active-backup

sudo nmcli connection add type ethernet ifname enp0s3 master bond0
sudo nmcli connection add type ethernet ifname enp0s8 master bond0

sudo nmcli connection modify bond0 \
ipv4.method manual \
ipv4.addresses 10.0.10.[11,12,13]/24 \
ipv4.gateway 10.0.10.1 \
ipv4.dns 1.1.1.1
```

```
sudo nmcli connection up bond0
```

```
[root@osd1 ~]# nmcli connection add type bond con-name bond0 ifname bond0 mode active-backup
Connexion « bond0 » (15222a11-6e5e-48c5-8151-96133fd27397) ajoutée avec succès.
[root@osd1 ~]# 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:a7:92:83 brd ff:ff:ff:ff:ff:ff
    inet 10.0.10.5/24 brd 10.0.10.255 scope global dynamic noprefixroute enp0s3
       valid_lft 347sec preferred_lft 347sec
    inet6 fe80::a00:27ff:fea7:9283/64 scope link noprefixroute
       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 08:00:27:91:bc:45 brd ff:ff:ff:ff:ff:ff
    inet 10.0.10.6/24 brd 10.0.10.255 scope global dynamic noprefixroute enp0s8
       valid_lft 197sec preferred_lft 197sec
    inet6 fe80::a00:27ff:fe91:bc45/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: bond0: <NO-CARRIER,BROADCAST,MULTICAST,MASTER,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether da:2c:0f:e2:59:e9 brd ff:ff:ff:ff:ff:ff
[root@osd1 ~]# nmcli connection add type ethernet ifname enp0s3 master bond0
Connexion « bond-slave-enp0s3 » (330ac5fb-f344-425d-a7f7-4258a8996a31) ajoutée avec succès.
[root@osd1 ~]# nmcli connection add type ethernet ifname enp0s8 master bond0
Connexion « bond-slave-enp0s8 » (82d0a8f1-ceb9-47bd-80f1-a3128ce07f7f) ajoutée avec succès.
[root@osd1 ~]# nmcli connection modify bond0 ipv4.method manual ipv4.addresses 10.0.10.12/24 ipv4.gateway 10.0.10.1 ipv4.dns 1.1.1.1
[root@osd1 ~]# nmcli connection up bond0
Connexion activée (controller waiting for ports) (Chemin D-Bus actif : /org/freedesktop/NetworkManager/ActiveConnection/5)
[root@osd1 ~]#
```

Vérifications :

```
cat /proc/net/bonding/bond0

sudo nmcli device
sudo nmcli connection
```

```
[root@monmgr ~]# cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v5.14.0-611.13.1.el9_7.x86_64

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: enp0s3
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0
Peer Notification Delay (ms): 0

Slave Interface: enp0s3
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 08:00:27:a3:9a:25
Slave queue ID: 0

Slave Interface: enp0s8
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 08:00:27:40:10:7a
Slave queue ID: 0
[root@monmgr ~]# _
```

Rocky_MON [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
Rocky Linux 9.7 (Blue Onyx)
Kernel 5.14.0-611.13.1.el9_7.x86_64 on x86_64

Activate the web console with: systemctl enable --now cockpit.socket

monmgr login: root
Password:
Last login: Tue Dec 16 16:21:45 on tty1
[root@monmgr ~]# 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,SLAVE,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bond0 state UP group default qlen 1000
    link/ether 08:00:27:a3:9a:25 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bond0 state UP group default qlen 1000
    link/ether 08:00:27:a3:9a:25 brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:40:10:7a
4: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:a3:9a:25 brd ff:ff:ff:ff:ff:ff
    inet 10.0.10.11/24 brd 10.0.10.255 scope global noprefixroute bond0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea3:9a25/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@monmgr ~]# nmcli device
DEVICE  TYPE      STATE                   CONNECTION
bond0   bond      connecté                bond0
enp0s3  ethernet  connecté                bond-slave-enp0s3
enp0s8  ethernet  connecté                bond-slave-enp0s8
lo      loopback  connecté (en externe)   lo
[root@monmgr ~]# nmcli connection
NAME             UUID                                  TYPE      DEVICE
bond0            4736a7b6-354a-42a4-aa13-7e4166186a46  bond      bond0
bond-slave-enp0s3  947e250c-fd4d-4f01-a937-40d0395701bf  ethernet  enp0s3
bond-slave-enp0s8  e586aeac-a537-4a18-af27-c72a7f20b946  ethernet  enp0s8
lo               a57355bd-d2bc-4868-ba2e-9eb6daec2ad3  loopback  lo
enp0s3           d08a2421-da05-3c7d-95cf-f866a9509496  ethernet  --
enp0s8           f492c14b-5591-32cb-99b3-3c0b5b22240c  ethernet  --
[root@monmgr ~]#
```

Rocky_OSD1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
Rocky Linux 9.7 (Blue Onyx)
Kernel 5.14.0-611.13.1.el9_7.x86_64 on x86_64

Activate the web console with: systemctl enable --now cockpit.socket

osd1 login: root
Password:
Last login: Tue Dec 16 16:09:14 on tty1
[root@osd1 ~]# 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,SLAVE,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bond0 state UP group default qlen 1000
    link/ether 08:00:27:a7:92:83 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bond0 state UP group default qlen 1000
    link/ether 08:00:27:a7:92:83 brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:91:bc:45
4: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:a7:92:83 brd ff:ff:ff:ff:ff:ff
    inet 10.0.10.12/24 brd 10.0.10.255 scope global noprefixroute bond0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea7:9283/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@osd1 ~]# nmcli device
DEVICE  TYPE      STATE                   CONNECTION
bond0   bond      connecté                bond0
enp0s3  ethernet  connecté                bond-slave-enp0s3
enp0s8  ethernet  connecté                bond-slave-enp0s8
lo      loopback  connecté (en externe)   lo
[root@osd1 ~]# nmcli connection
NAME             UUID                                  TYPE      DEVICE
bond0            15222a11-6e5e-40c5-8151-96133fd27397  bond      bond0
bond-slave-enp0s3  330ec5fb-f344-425d-a7f7-4258a0996a31  ethernet  enp0s3
bond-slave-enp0s8  8240a0f1-ceb9-47bd-80f1-a3128ce07f7f  ethernet  enp0s8
lo               70ab5ae7-92f5-48bd-b01b-e1967281aa22  loopback  lo
enp0s3           019d3426-174c-3fbe-9804-6237e6a6568fa  ethernet  --
enp0s8           ce80b7fa-dcd9-3644-92b1-8f2c268bfec8  ethernet  --
[root@osd1 ~]#
```

Rocky_OSD2 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
Rocky Linux 9.7 (Blue Onyx)
Kernel 5.14.0-611.13.1.el9_7.x86_64 on x86_64

Activate the web console with: systemctl enable --now cockpit.socket

osd2 login: root
Password:
Last login: Tue Dec 16 16:09:45 on tty1
[root@osd2 ~]# 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,SLAVE,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bond0 state UP group default qlen 1000
    link/ether 08:00:27:26:99:33 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bond0 state UP group default qlen 1000
    link/ether 08:00:27:26:99:33 brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:61:8f:65
4: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:26:99:33 brd ff:ff:ff:ff:ff:ff
    inet 10.0.10.13/24 brd 10.0.10.255 scope global noprefixroute bond0
       valid_lft forever preferred_lft forever
    inet6 fe80::4b95:dc85:e3a9:9b3b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@osd2 ~]# nmcli device
DEVICE  TYPE      STATE                   CONNECTION
bond0   bond      connecté                bond0
enp0s3  ethernet  connecté                bond-slave-enp0s3
enp0s8  ethernet  connecté                bond-slave-enp0s8
lo      loopback  connecté (en externe)   lo
[root@osd2 ~]# nmcli connection
NAME             UUID                                  TYPE      DEVICE
bond0            d411fa31-e471-4ce8-aa54-954de434b5a3  bond      bond0
bond-slave-enp0s3  697de708-bf92-4a5f-a056-3e8e919b9f5d  ethernet  enp0s3
bond-slave-enp0s8  4c2ee25a-4593-4649-96c2-c9214405ccaa  ethernet  enp0s8
lo               67c68fbb-568c-493f-8470-85af5c3742f4  loopback  lo
enp0s3           0f65d4a6-5d31-3ba1-b758-560a714b035c  ethernet  --
enp0s8           9712e4aa-0620-35d1-b1c6-ea0dc8ce77f4  ethernet  --
[root@osd2 ~]# _
```

Vérification de la redondance en débranchant une NIC dans la VM :

MON_MGR (avant tout cassé) [En fonction] - Oracle VirtualBox

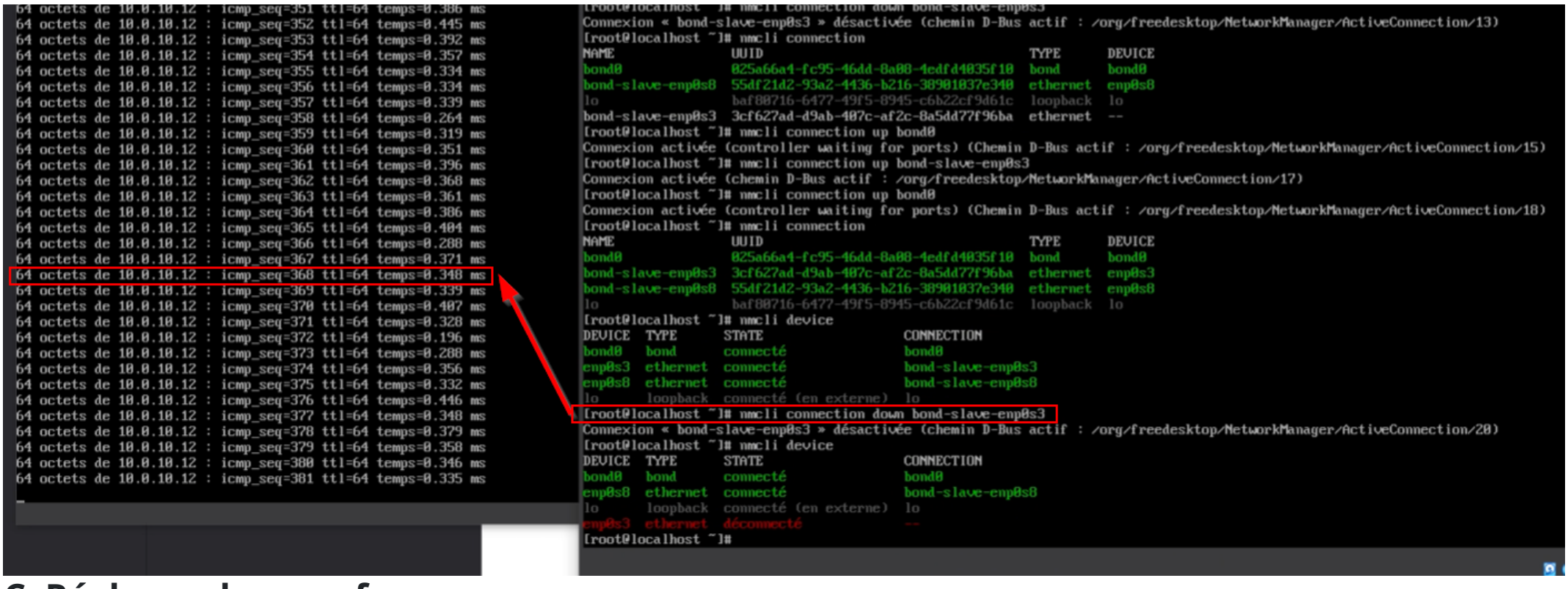
Fichier Machine Écran Entrée Périphériques Aide

```
[root@localhost ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled;
     Active: active (running) since Mon 2025-12-15 15:48:48 CET; 3min 42s
       Docs: man:firewalld(1)
    Process: 824 ExecStartPost=/usr/bin/firewall-cmd --state (code=exited
   Main PID: 749 (firewalld)
      Tasks: 2 (limit: 23100)
     Memory: 44.2M (peak: 64.1M)
        CPU: 788ms
     CGroup: /system.slice/firewalld.service
             └─749 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nop

déc. 15 15:48:46 localhost systemd[1]: Starting firewalld - dynamic firew
déc. 15 15:48:48 localhost systemd[1]: Started firewalld - dynamic firewa
[root@localhost ~]# ping 10.0.10.12
PING 10.0.10.12 (10.0.10.12) 56(84) octets de données.
64 octets de 10.0.10.12 : icmp_seq=1 ttl=64 temps=1.27 ms
64 octets de 10.0.10.12 : icmp_seq=2 ttl=64 temps=0.237 ms
64 octets de 10.0.10.12 : icmp_seq=3 ttl=64 temps=0.527 ms
64 octets de 10.0.10.12 : icmp_seq=4 ttl=64 temps=0.246 ms
64 octets de 10.0.10.12 : icmp_seq=5 ttl=64 temps=0.380 ms
64 octets de 10.0.10.12 : icmp_seq=6 ttl=64 temps=0.215 ms
64 octets de 10.0.10.12 : icmp_seq=7 ttl=64 temps=0.353 ms
64 octets de 10.0.10.12 : icmp_seq=8 ttl=64 temps=0.358 ms
64 octets de 10.0.10.12 : icmp_seq=9 ttl=64 temps=0.280 ms
64 octets de 10.0.10.12 : icmp_seq=10 ttl=64 temps=0.362 ms
64 octets de 10.0.10.12 : icmp_seq=11 ttl=64 temps=0.327 ms
64 octets de 10.0.10.12 : icmp_seq=12 ttl=64 temps=0.361 ms
64 octets de 10.0.10.12 : icmp_seq=13 ttl=64 temps=0.356 ms
64 octets de 10.0.10.12 : icmp_seq=14 ttl=64 temps=0.347 ms
64 octets de 10.0.10.12 : icmp_seq=15 ttl=64 temps=0.393 ms
64 octets de 10.0.10.12 : icmp_seq=16 ttl=64 temps=0.399 ms
64 octets de 10.0.10.12 : icmp_seq=17 ttl=64 temps=0.357 ms
_
```

OSD1 [En fonction] - Oracle VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

```
[root@localhost ~]# 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,SLAVE,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bond0 state UP group default qlen 1000
    link/ether 08:00:27:46:ae:de brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bond0 state UP group default qlen 1000
    link/ether 08:00:27:46:ae:de brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:a7:0c:24
4: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:46:ae:de brd ff:ff:ff:ff:ff:ff
    inet 10.0.10.12/24 brd 10.0.10.255 scope global noprefixroute bond0
       valid_lft forever preferred_lft forever
    inet6 fe80::da7d:71fc:5ad6:e10d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@localhost ~]# nmcli connecti_
```



C. Réglages du pare-feu

[REDHAT - Using and configurind firewalld]

- Zone personnalisée : `ceph-mcs2025`
- Associée à l'interface du **bond0**
- [Autorisation des ports nécessaires à CEPH] et associés

```
sudo firewall-cmd --permanent --new-zone=ceph-mcs2025

# Pour vérifier
sudo firewall-cmd --reload
sudo firewall-cmd --get-zones

sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-interface=bond0
sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-service=ssh

sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=80/tcp
sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=443/tcp
sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=3300-3303/tcp
sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=6789/tcp
sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=6800-7300/tcp
sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=7480/tcp
sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=8443/tcp

sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=123/udp
sudo firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=6800-7300/udp

sudo firewall-cmd --reload
```

Et on vérifie :

```
sudo firewall-cmd --info-zone=ceph-mcs2025
```

```
[root@osd1 ~]# firewall-cmd --permanent --new-zone=ceph-mcs2025
success
[root@osd1 ~]# firewall-cmd --reload
success
[root@osd1 ~]# firewall-cmd --get-zones
block ceph-mcs2025 dmz drop external home internal nm-shared public trusted work
[root@osd1 ~]# firewall-cmd --permanent --zone=ceph-mcs2025 --add-interface=bond0
The interface is under control of NetworkManager, setting zone to 'ceph-mcs2025'.
success
[root@osd1 ~]# firewall-cmd --permanent --zone=ceph-mcs2025 --add-service=ssh
success
[root@osd1 ~]# firewall-cmd --permanent --zone=ceph-mcs2025 --add-port={80,443,3300,6789,7480}/tcp
success
[root@osd1 ~]# firewall-cmd --permanent --zone=ceph-mcs2025 --add-port=123/udp
success
[root@osd1 ~]# firewall-cmd --reload
success
[root@osd1 ~]# firewall-cmd --permanent --zone=ceph-mcs2025 --list-ports
80/tcp 443/tcp 3300/tcp 6789/tcp 7480/tcp 123/udp
[root@osd1 ~]# firewall-cmd --info-zone=ceph-mcs2025
ceph-mcs2025 (active)
  target: default
  icmp-block-inversion: no
  interfaces: bond0
  sources:
  services: ssh
  ports: 80/tcp 443/tcp 3300/tcp 6789/tcp 7480/tcp 123/udp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@osd1 ~]#
```

3. Installer et configurer Ceph

A. Choix du Ceph

On a décidé d'utiliser RGW pour diverses raisons :

1. c'est celui que nous connaissons le moins (raison éducative)
2. c'est un système basé sur une technologie qui devient un standard nuagique (avec AWS S3 repris même par les concurrents)
3. parce que pourquoi pas

B. Préparation des noeuds

CEPH - cephadm | CEPH - Host Management

- Installer `cephadm` version **`squid`** (*les deux dernières, `Latest` et `tentacles` étant non stabilisées*)
- Déployer le moniteur **MON** et gestionnaire **MGR** sur le premier noeud, ajout des deux autres comme **OSD**

Sur les trois noeuds :

```
sudo dnf install -y centos-release-ceph-squid
sudo dnf install -y cephadm

# Pour les dépendances liées au déploiement de configurations
sudo dnf install -y python3-yaml python3-jinja2
```

Sur les deux noeuds OSD :

```
sudo cephadm add-repo --release squid
sudo cephadm install ceph-common
```

```
[root@osd2 ~]# dnf install -y centos-release-ceph-squid
Dernière vérification de l'expiration des métadonnées effectuée il y a 0:40:55 le mar. 16 déc. 2025 16:17:01.
Dépendances résolues.
================================================================================
 Paquet                          Architecture    Version          Dépôt    Taille
================================================================================
Installation:
 centos-release-ceph-squid       noarch          1.0-1.el9        extras   7.3 k
Installation des dépendances:
 centos-release-storage-common   noarch          2-5.el9          extras   8.4 k

Résumé de la transaction
================================================================================
Installer  2 Paquets

Taille totale des téléchargements : 16 k
Taille des paquets installés : 2.3 k
Téléchargement des paquets :
(1/2): centos-release-storage-common-2-5.el9.noarch.rpm  36 kB/s | 8.4 kB  00:00
(2/2): centos-release-ceph-squid-1.0-1.el9.noarch.rpm    28 kB/s | 7.3 kB  00:00
--------------------------------------------------------------------------------
Total                                                    26 kB/s |  16 kB  00:00
Test de la transaction
La vérification de la transaction a réussi.
Lancement de la transaction de test
Transaction de test réussie.
Exécution de la transaction
  Préparation          :                                                    1/1
  Installation         : centos-release-storage-common-2-5.el9.noarch       1/2
  Installation         : centos-release-ceph-squid-1.0-1.el9.noarch         2/2
  Vérification de      : centos-release-ceph-squid-1.0-1.el9.noarch         1/2
  Vérification de      : centos-release-storage-common-2-5.el9.noarch       2/2

Installé:
  centos-release-ceph-squid-1.0-1.el9.noarch
  centos-release-storage-common-2-5.el9.noarch

Terminé !
[root@osd2 ~]# dnf install -y cephadm
CentOS-9-stream - Ceph Squid                             80 kB/s | 114 kB  00:01
Dépendances résolues.
================================================================================
 Paquet          Architecture    Version                 Dépôt          Taille
================================================================================
Installation:
 cephadm         noarch          2:19.2.3-1.el9s         centos-ceph-squid  346 k

Résumé de la transaction
================================================================================
Installer  1 Paquet

Taille totale des téléchargements : 346 k
Taille des paquets installés : 344 k
Téléchargement des paquets :
cephadm-19.2.3-1.el9s.noarch.rpm                         1.3 MB/s | 346 kB  00:00
--------------------------------------------------------------------------------
Total                                                    296 kB/s | 346 kB  00:01
Test de la transaction
La vérification de la transaction a réussi.
Lancement de la transaction de test
Transaction de test réussie.
Exécution de la transaction
  Préparation          :                                                    1/1
  Exécution du scriptlet: cephadm-2:19.2.3-1.el9s.noarch                    1/1
  Installation         : cephadm-2:19.2.3-1.el9s.noarch                     1/1
  Exécution du scriptlet: cephadm-2:19.2.3-1.el9s.noarch                    1/1
  Vérification de      : cephadm-2:19.2.3-1.el9s.noarch                     1/1

Installé:
  cephadm-2:19.2.3-1.el9s.noarch

Terminé !
```

```
[root@osd2 ~]# dnf install -y python3-yaml python3-jinja2
Dernière vérification de l'expiration des métadonnées effectuée il y a 0:00:46 le mar. 16 déc. 2025 16:58:29.
Le paquet python3-pyyaml-5.4.1-6.el9.x86_64 est déjà installé.
Dépendances résolues.
================================================================================
 Paquet                  Architecture            Version                 Dépôt                    Taille
================================================================================
Installation:
 python3-jinja2          noarch                  2.11.3-8.el9_5          appstream                228 k
Installation des dépendances:
 python3-babel           noarch                  2.9.1-2.el9             appstream                5.8 M
 python3-markupsafe      x86_64                  1.1.1-12.el9            appstream                 32 k
 python3-pytz            noarch                  2021.1-5.el9            appstream                 47 k

Résumé de la transaction
================================================================================
Installer  4 Paquets

Taille totale des téléchargements : 6.1 M
Taille des paquets installés : 28 M
Téléchargement des paquets :
(1/4): python3-markupsafe-1.1.1-12.el9.x86_64.rpm          95 kB/s |  32 kB     00:00
(2/4): python3-jinja2-2.11.3-8.el9_5.noarch.rpm           656 kB/s | 228 kB     00:00
(3/4): python3-pytz-2021.1-5.el9.noarch.rpm               504 kB/s |  47 kB     00:00
(4/4): python3-babel-2.9.1-2.el9.noarch.rpm                11 MB/s | 5.8 MB     00:00
--------------------------------------------------------------------------------
Total                                                     7.5 MB/s | 6.1 MB     00:00
Test de la transaction
La vérification de la transaction a réussi.
Lancement de la transaction de test
Transaction de test réussie.
Exécution de la transaction
  Préparation          :                                                        1/1
  Installation         : python3-pytz-2021.1-5.el9.noarch                       1/4
  Installation         : python3-babel-2.9.1-2.el9.noarch                       2/4
  Installation         : python3-markupsafe-1.1.1-12.el9.x86_64                 3/4
  Installation         : python3-jinja2-2.11.3-8.el9_5.noarch                   4/4
  Exécution du scriptlet: python3-jinja2-2.11.3-8.el9_5.noarch                  4/4
  Vérification de      : python3-babel-2.9.1-2.el9.noarch                       1/4
  Vérification de      : python3-jinja2-2.11.3-8.el9_5.noarch                   2/4
  Vérification de      : python3-markupsafe-1.1.1-12.el9.x86_64                 3/4
  Vérification de      : python3-pytz-2021.1-5.el9.noarch                       4/4

Installé:
  python3-babel-2.9.1-2.el9.noarch     python3-jinja2-2.11.3-8.el9_5.noarch     python3-markupsafe-1.1.1-12.el9.x86_64     python3-pytz-2021.1-5.el9.noarch

Terminé !
```

Bootstrap du cluster sur le noeud principal :

```
sudo cephadm bootstrap \
--mon-ip 10.0.10.11 \
--allow-fqdn-hostname \
--initial-dashboard-user admin \
--initial-dashboard-password 'Dashboard123!'

  # Copie de la clef publique du MON/MGR sur les OSD
ssh-copy-id -f -i /etc/ceph/ceph.pub root@10.0.10.12
ssh-copy-id -f -i /etc/ceph/ceph.pub root@10.0.10.13

  # Vérification
sudo ceph orch host ls
```

```
Deploying mon service with default placement...
Deploying mgr service with default placement...
Deploying crash service with default placement...
Deploying ceph-exporter service with default placement...
Deploying prometheus service with default placement...
Deploying grafana service with default placement...
Deploying node-exporter service with default placement...
Deploying alertmanager service with default placement...
Enabling the dashboard module...
Waiting for the mgr to restart...
Waiting for mgr epoch 9...
mgr epoch 9 is available
Generating a dashboard self-signed certificate...
Creating initial admin user...
Fetching dashboard port number...
firewalld ready
Ceph Dashboard is now available at:

             URL: https://monmgr:8443/
            User: admin
        Password: Dashboard123!

Enabling client.admin keyring and conf on hosts with "admin" label
Saving cluster configuration to /var/lib/ceph/f3c55ff8-da99-11f0-94de-080027a39a25/config directory
You can access the Ceph CLI as following in case of multi-cluster or non-default config:

        sudo /usr/sbin/cephadm shell --fsid f3c55ff8-da99-11f0-94de-080027a39a25 -c /etc/ceph/ceph.conf -k /etc/ceph/ceph.client.admin.keyring

Or, if you are only running a single cluster on this host:

        sudo /usr/sbin/cephadm shell

Please consider enabling telemetry to help improve Ceph:

        ceph telemetry on

For more information see:

        https://docs.ceph.com/en/latest/mgr/telemetry/

Bootstrap complete.
[root@monmgr ~]# curl https://monmgr:8443 -k | tail -n 15
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  6490  100  6490    0     0   316k      0 --:--:-- --:--:-- --:--:--  316k
  <noscript>
    <div class="noscript container"
         ng-if="false">
      <div class="jumbotron alert alert-danger">
        <h2 i18n>JavaScript required!</h2>
        <p i18n>A browser with JavaScript enabled is required in order to use this service.</p>
        <p i18n>When using Internet Explorer, please check your security settings and add this address to your trusted sites.</p>
      </div>
    </div>
  </noscript>

  <cd-root></cd-root>
<script src="runtime.c5db0882e177464e.js" type="module"></script><script src="polyfills.374f1f989f34e1be.js" type="module"></script><script src="main.f2f8367e2c
a3522b.js" type="module"></script>

</body></html>[root@monmgr ~]#
```

Copie de la configuration du MON/MGR sur les OSD :

```
scp /etc/ceph/ceph.conf root@10.0.10.12:/etc/ceph/
scp /etc/ceph/ceph.conf root@10.0.10.13:/etc/ceph/
scp /etc/ceph/ceph.client.admin.keyring root@10.0.10.12:/etc/ceph/
scp /etc/ceph/ceph.client.admin.keyring root@10.0.10.13:/etc/ceph/
ssh root@10.0.10.12 "chmod 600 /etc/ceph/*.keyring && chmod 644 /etc/ceph/ceph.conf"
ssh root@10.0.10.13 "chmod 600 /etc/ceph/*.keyring && chmod 644 /etc/ceph/ceph.conf"
```

```
[root@monmgr ~]# ls -l /etc/ceph/
total 16
-rw-------. 1 root root 151 16 déc.  17:14 ceph.client.admin.keyring
-rw-r--r--. 1 root root 171 16 déc.  17:14 ceph.conf
-rw-r--r--. 1 root root 595 16 déc.  17:12 ceph.pub
-rw-r--r--. 1 root root  92 30 juil. 01:11 rbdmap
[root@monmgr ~]# scp /etc/ceph/ceph.conf root@10.0.10.13:/etc/ceph/
The authenticity of host '10.0.10.13 (10.0.10.13)' can't be established.
ED25519 key fingerprint is SHA256:9OXFbs6Wl/jV3D2G9i3pU5qkLP8sct4OHNUMPFDILJk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.10.13' (ED25519) to the list of known hosts.
root@10.0.10.13's password:
ceph.conf                                                                                     100%  171   253.4KB/s   00:00
[root@monmgr ~]# scp /etc/ceph/ceph.conf root@10.0.10.12:/etc/ceph/
The authenticity of host '10.0.10.12 (10.0.10.12)' can't be established.
ED25519 key fingerprint is SHA256:0TP68eccaJQQ9bgYFTeyNC6bpkTZ0MsSLpmGSFpFoHs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.10.12' (ED25519) to the list of known hosts.
root@10.0.10.12's password:
ceph.conf                                                                                     100%  171   333.2KB/s   00:00
[root@monmgr ~]# scp /etc/ceph/ceph.client.admin.keyring root@10.0.10.12:/etc/ceph/
root@10.0.10.12's password:
ceph.client.admin.keyring                                                                     100%  151   145.7KB/s   00:00
[root@monmgr ~]# scp /etc/ceph/ceph.client.admin.keyring root@10.0.10.13:/etc/ceph/
root@10.0.10.13's password:
ceph.client.admin.keyring                                                                     100%  151   351.5KB/s   00:00
[root@monmgr ~]# ssh root@10.0.10.12 "chmod 600 /etc/ceph/*.keyring && chmod 644 /etc/ceph/ceph.conf"
root@10.0.10.12's password:
[root@monmgr ~]# ssh root@10.0.10.13 "chmod 600 /etc/ceph/*.keyring && chmod 644 /etc/ceph/ceph.conf"
root@10.0.10.13's password:
[root@monmgr ~]#
```

Ajout des hôtes dans le cluster **Ceph** :

```
sudo ceph orch host add osd1 10.0.10.12
sudo ceph orch host add osd2 10.0.10.13
```

```
[root@monmgr ~]# ceph orch daemon add osd monmgr:/dev/sdb
Created osd(s) 0 on host 'monmgr'
[root@monmgr ~]# ceph orch daemon add osd osd1:/dev/sdb
Invalid 'host:device' spec: host not found in cluster. Please check 'ceph orch host ls' for available hosts
[root@monmgr ~]# ceph orch host ls
HOST    ADDR        LABELS  STATUS
monmgr  10.0.10.11  _admin
1 hosts in cluster
[root@monmgr ~]# ceph orch host add osd1 10.0.10.12
Added host 'osd1' with addr '10.0.10.12'
[root@monmgr ~]# ceph orch host add osd2 10.0.10.13
Added host 'osd2' with addr '10.0.10.13'
[root@monmgr ~]# ceph orch host ls
HOST    ADDR        LABELS  STATUS
monmgr  10.0.10.11  _admin
osd1    10.0.10.12
osd2    10.0.10.13
3 hosts in cluster
[root@monmgr ~]# _
```

Ajout des **OSD** dans le cluster :

```
sudo ceph orch device ls

# Si on veut tout asservir sans distinction
sudo ceph orch apply osd --all-available-devices

# Si on veut asservir un panel précis de volumes
sudo ceph orch daemon add osd monmgr:/dev/sdb
sudo ceph orch daemon add osd osd1:/dev/sdb
sudo ceph orch daemon add osd osd2:/dev/sdb
```

```
[root@monmgr ~]# ceph -s
  cluster:
    id:     f3c55ff8-da99-11f0-94de-080027a39a25
    health: HEALTH_WARN
            clock skew detected on mon.osd1, mon.osd2

  services:
    mon: 3 daemons, quorum monmgr,osd1,osd2 (age 47s)
    mgr: monmgr.zzxafd(active, since 41s), standbys: osd1.pujncj
    osd: 3 osds: 3 up (since 41s), 3 in (since 12m)
    rgw: 3 daemons active (2 hosts, 1 zones)

  data:
    pools:   5 pools, 129 pgs
    objects: 194 objects, 582 KiB
    usage:   167 MiB used, 60 GiB / 60 GiB avail
    pgs:     127 active+clean
             2   active+clean+scrubbing

[root@monmgr ~]# ceph osd tree
ID  CLASS  WEIGHT   TYPE NAME        STATUS  REWEIGHT  PRI-AFF
-1         0.05846  root default
-3         0.01949      host monmgr
 0    hdd  0.01949          osd.0        up   1.00000  1.00000
-5         0.01949      host osd1
 1    hdd  0.01949          osd.1        up   1.00000  1.00000
-7         0.01949      host osd2
 2    hdd  0.01949          osd.2        up   1.00000  1.00000
[root@monmgr ~]#
```

C. Déployer le service RGW

https://docs.ceph.com/en/squid/radosgw/ https://docs.ceph.com/en/squid/radosgw/s3/

- Créer un *daemon* RGW avec `ceph orch apply rgw`
- Configurer le domaine S3, clefs d'accès et politiques des seaux

Déploiement du service RGW :

```
sudo ceph orch apply rgw rgw-mcs \
--realm=realm-mcs \
--zone=zone-mcs \
--placement="2 osd1 osd2"

# Ou en version "triviale"
sudo ceph orch apply rgw rgw-mcs
```

Vérifier l'intégrité du cluster RGW :

```
sudo ceph orch ps --daemon_type rgw
```

```
[root@monmgr ~]# ceph orch ps --daemon_type rgw
NAME                     HOST  PORTS  STATUS         REFRESHED  AGE  MEM USE  MEM LIM  VERSION  IMAGE ID      CONTAINER ID
rgw.rgw-mcs.osd1.zwdzqa  osd1  *:80   running (3m)     3m ago   3m    18.5M        -  19.2.3   aade1b12b8e6  4b69eada461c
rgw.rgw-mcs.osd2.toumux  osd2  *:80   running (3m)     3m ago   3m    19.2M        -  19.2.3   aade1b12b8e6  777a2b921c9f
```

Créer un admin S3 :

```
sudo dnf install -y epel-release
sudo dnf install -y ceph-radosgw

sudo radosgw-admin user create --uid=egf2025 --display-name="EstGauFlo 2025"
```

```
[root@monmgr ceph]# radosgw-admin user create --uid="bonjour" --display-name="Bonjour"
{
    "user_id": "bonjour",
    "display_name": "Bonjour",
    "email": "",
    "suspended": 0,
    "max_buckets": 1000,
    "subusers": [],
    "keys": [
        {
            "user": "bonjour",
            "access_key": "I9QJMFGPP61HIGTD38G4",
            "secret_key": "TrGC3cTFBhtnhhJHZ2LqSnBuAyD9elPsLLCaDxx3"
        }
    ],
    "swift_keys": [],
    "caps": [],
    "op_mask": "read, write, delete",
    "default_placement": "",
    "default_storage_class": "",
    "placement_tags": [],
    "bucket_quota": {
        "enabled": false,
        "check_on_raw": false,
        "max_size": -1,
        "max_size_kb": 0,
        "max_objects": -1
    },
    "user_quota": {
        "enabled": false,
        "check_on_raw": false,
        "max_size": -1,
        "max_size_kb": 0,
        "max_objects": -1
    },
    "temp_url_keys": [],
    "type": "rgw",
    "mfa_ids": []
}
```

Modifier le ceph.conf :

```
sudo nano /etc/ceph/ceph.conf
  [client.radosgw.gateway]
    host = [monmgr, osd1, osd2]
    keyring = /etc/ceph/ceph.client.radosgw.gateway.keyring
    rgw_frontends = "beast port=7480"
```

```
sudo systemctl start ceph-radosgw@rgw.gateway

sudo nano /etc/ceph/ceph.client.radosgw.keyring
  [client.admin]
    key = *******
    caps mds = "allow *"
    caps mgr = "allow *"
    caps mon = "allow *"
    caps osd = "allow *"
```

Vérifier la santé du cluster Ceph :

```
sudo ceph -s
sudo ceph health detail
```

```
[root@monmgr ~]# ceph -s
  cluster:
    id:     f3c55ff8-da99-11f0-94de-080027a39a25
    health: HEALTH_OK

  services:
    mon: 3 daemons, quorum monmgr,osd1,osd2 (age 11m)
    mgr: monmgr.zzxafd(active, since 11m), standbys: osd1.pujncj
    osd: 3 osds: 3 up (since 11m), 3 in (since 102m)
    rgw: 2 daemons active (2 hosts, 1 zones)

  data:
    pools:   6 pools, 161 pgs
    objects: 228 objects, 584 KiB
    usage:   144 MiB used, 60 GiB / 60 GiB avail
    pgs:     161 active+clean

[root@monmgr ~]# ceph health detail
HEALTH_OK
```

Configurer l'accès S3 :

```
sudo dnf install -y awscli

aws configure set aws_access_key_id XXOKHTFX8OUAW4YEFBVT
aws configure set aws_secret_access_key b3Cn2vYARkbnGWlPVdCg16ZYUZ3IczXC4SvtBBMy
aws s3 ls --endpoint-url http://10.0.10.11:7480
```

Notes sur le précédent bloc

Ca ne sert à rien de copier le couple ID-Clef, ce sont des utilisateurs locaux, mais ce sont bien des vraies. On sait ce qu'on fait présentement, mais il est évident qu'on ne fait jamais ça en production.

La solution de niveau 1 c'est d'utiliser une variable d'environnement temporaire (`AWS_ID="XXOKHTFX8OUAW4YEFBVT"` et ensuite appeler avec un `$AWS_ID` dans le shell pour une expiration à déconnexion), et la solution de niveau 2 serait de déployer un serveur Consul/Vault sur le réseau pour gérer des secrets.

Vérifications :

```
[root@monmgr ~]# dnf install -y awscli
Dernière vérification de l'expiration des métadonnées effectuée il y a 1:09:25 le mer. 17 déc. 2025 09:21:38.
Dépendances résolues.
================================================================================
 Paquet                  Architecture      Version                 Dépôt     Taille
================================================================================
Installation:
 awscli2                 noarch            2.15.31-3.el9           appstream  11 M
Installation des dépendances:
 python3-awscrt          x86_64            0.27.2-1.el9            appstream 979 k
 python3-cffi            x86_64            1.14.5-5.el9            baseos    241 k
 python3-colorama        noarch            0.4.6-3.el9             appstream  52 k
 python3-cryptography    x86_64            36.0.1-5.el9_6          baseos    1.2 M
 python3-docutils        noarch            0.16-6.el9.0.1          appstream 1.5 M
 python3-jmespath        noarch            0.9.4-11.el9            appstream  45 k
 python3-ply             noarch            3.11-14.el9.0.1         baseos    103 k
 python3-prompt-toolkit  noarch            3.0.38-4.el9            appstream 616 k
 python3-pycparser       noarch            2.20-6.el9              baseos    124 k
 python3-ruamel-yaml     x86_64            0.16.6-7.el9.1.0.1      appstream 190 k
 python3-ruamel-yaml-clib x86_64           0.2.7-3.el9             appstream 143 k
 python3-wcwidth         noarch            0.2.5-8.el9             appstream  41 k
Installation des dépendances faibles:
 groff                   x86_64            1.22.4-10.el9.0.1       appstream 1.2 M

Résumé de la transaction
================================================================================
Installer  14 Paquets

Taille totale des téléchargements : 17 M
Taille des paquets installés : 129 M
Téléchargement des paquets :
(1/14): python3-ply-3.11-14.el9.0.1.noarch.rpm                  14 kB/s | 103 kB     00:07
(2/14): python3-cffi-1.14.5-5.el9.x86_64.rpm                    33 kB/s | 241 kB     00:07
(3/14): python3-cryptography-36.0.1-5.el9_6.x86_64.rpm         160 kB/s | 1.2 MB     00:07
(4/14): python3-pycparser-2.20-6.el9.noarch.rpm                 1.8 MB/s | 124 kB     00:00
(5/14): groff-1.22.4-10.el9.0.1.x86_64.rpm                      654 kB/s | 1.2 MB     00:01
(6/14): python3-colorama-0.4.6-3.el9.noarch.rpm                 188 kB/s |  52 kB     00:00
(7/14): python3-awscrt-0.27.2-1.el9.x86_64.rpm                  255 kB/s | 979 kB     00:03
(8/14): python3-jmespath-0.9.4-11.el9.noarch.rpm                205 kB/s |  45 kB     00:00
(9/14): python3-prompt-toolkit-3.0.38-4.el9.noarch.rpm          248 kB/s | 616 kB     00:02
(10/14): python3-ruamel-yaml-0.16.6-7.el9.1.0.1.x86_64.rpm      171 kB/s | 190 kB     00:01
(11/14): python3-ruamel-yaml-clib-0.2.7-3.el9.x86_64.rpm        177 kB/s | 143 kB     00:00
(12/14): python3-wcwidth-0.2.5-8.el9.noarch.rpm                  82 kB/s |  41 kB     00:00
(13/14): python3-docutils-0.16-6.el9.0.1.noarch.rpm             214 kB/s | 1.5 MB     00:07
(14/14): awscli2-2.15.31-3.el9.noarch.rpm          54% [=============================-  ] 941 kB/s | 9.4 MB     00:08 ETA
```

```
[root@monmgr .aws]# aws s3 ls --endpoint-url http://10.0.10.11:7480

An error occurred (SignatureDoesNotMatch) when calling the ListBuckets operation: Unknown
[root@monmgr .aws]# aws s3 ls

An error occurred (InvalidAccessKeyId) when calling the ListBuckets operation: The AWS Access Key Id you provided does not exist in our records.
[root@monmgr .aws]# aws s3 ls --endpoint-url http://10.0.10.11

Could not connect to the endpoint URL: "http://10.0.10.11/"
[root@monmgr .aws]# aws s3 ls --endpoint-url http://10.0.10.11:7480

An error occurred (SignatureDoesNotMatch) when calling the ListBuckets operation: Unknown
[root@monmgr .aws]# vi credentials
[root@monmgr .aws]# aws s3 ls --endpoint-url http://10.0.10.11:7480
2025-12-17 10:21:19 test-compartiment
[root@monmgr .aws]# aws s3 ls --endpoint-url http://10.0.10.12:7480
2025-12-17 10:21:19 test-compartiment
[root@monmgr .aws]#
```

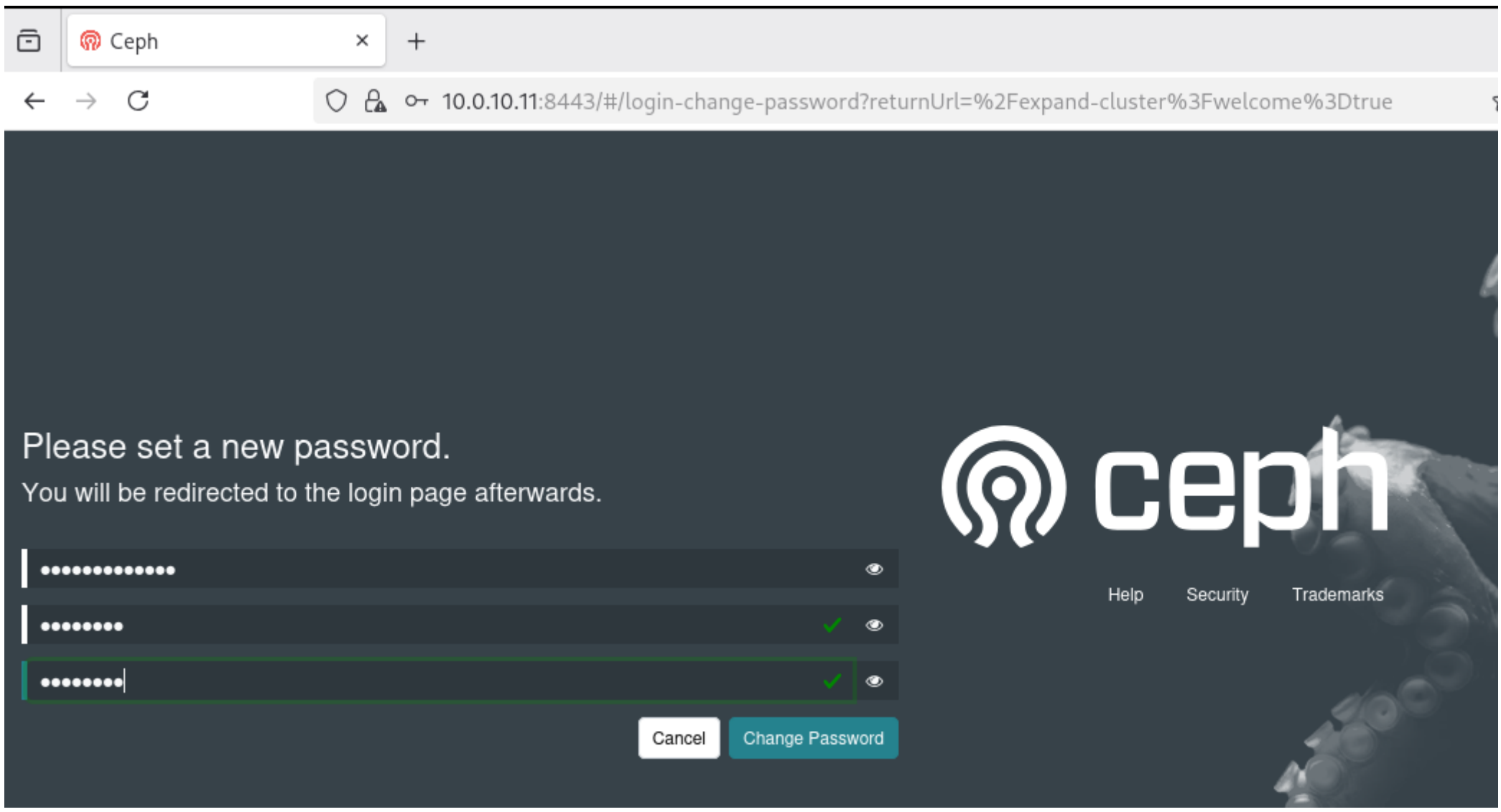
Et ensuite faire un test de téléversement dans un seau S3 avec la documentation officielle

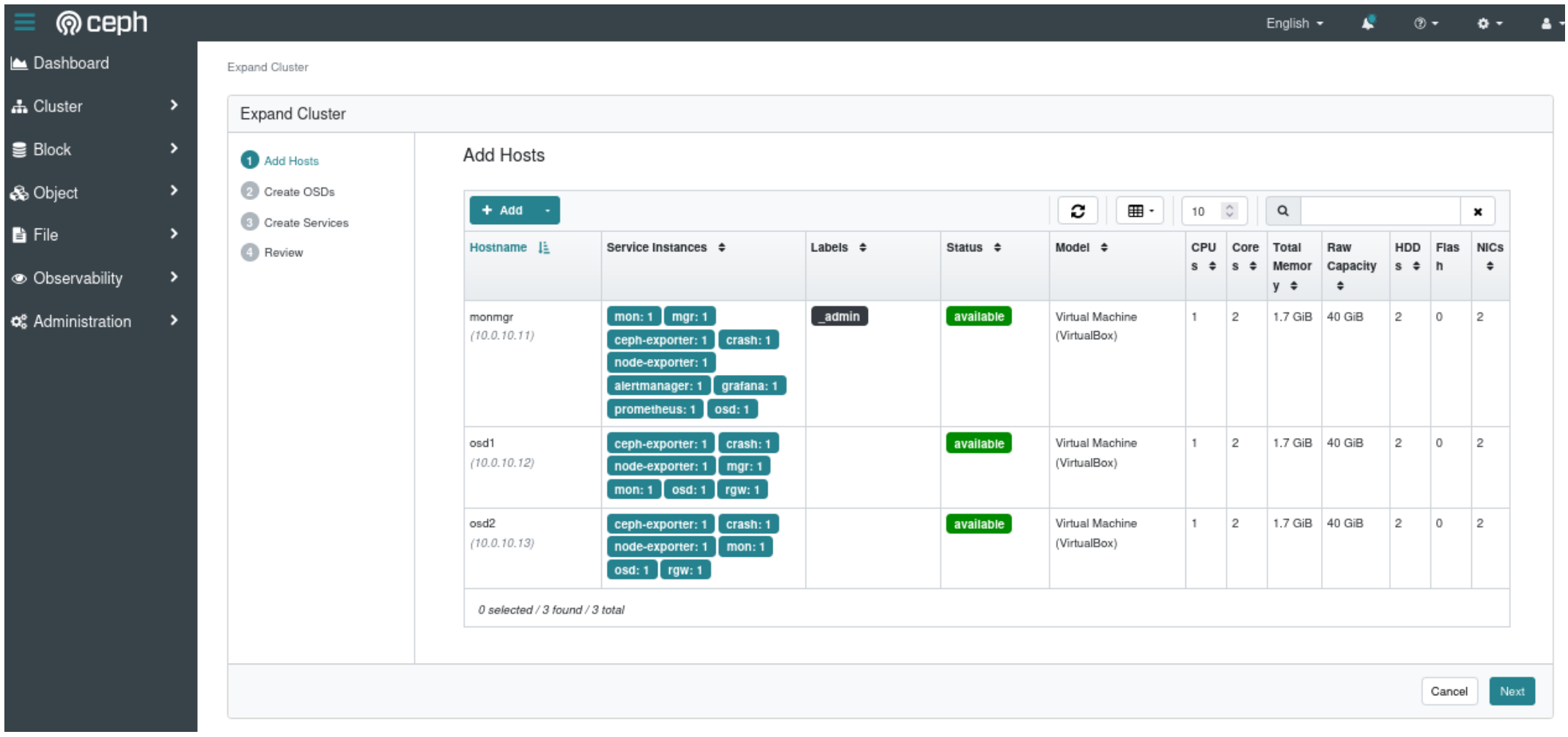
```
aws s3 cp ./fichier s3://bucket/ --endpoint-url http://10.0.10.11:7480
```

```
[root@monmgr rocky]# touch bonjour.txt
[root@monmgr rocky]# aws s3 cp ./bonjour.txt s3://test-compartiment/ --endpoint-url http://10.0.10.11:7480
upload: ./bonjour.txt to s3://test-compartiment/bonjour.txt
[root@monmgr rocky]# aws s3 help
[root@monmgr rocky]# aws s3 ls s3://test-compartiment/

An error occurred (InvalidAccessKeyId) when calling the ListObjectsV2 operation: The AWS Access Key Id you provided does not exist in our records.
[root@monmgr rocky]# aws s3 ls s3://test-compartiment/ --endpoint-url http://10.0.10.11:7480
2025-12-17 11:21:25          0 bonjour.txt
```

D. (Bonus) Vérifier sur le Dashboard

Nous avons rajouté dans le réseau NAT (mais pas le Ceph) une machine tierce avec interface graphique, Rocky Linux ou Debian pour se connecter sur le dashboard :



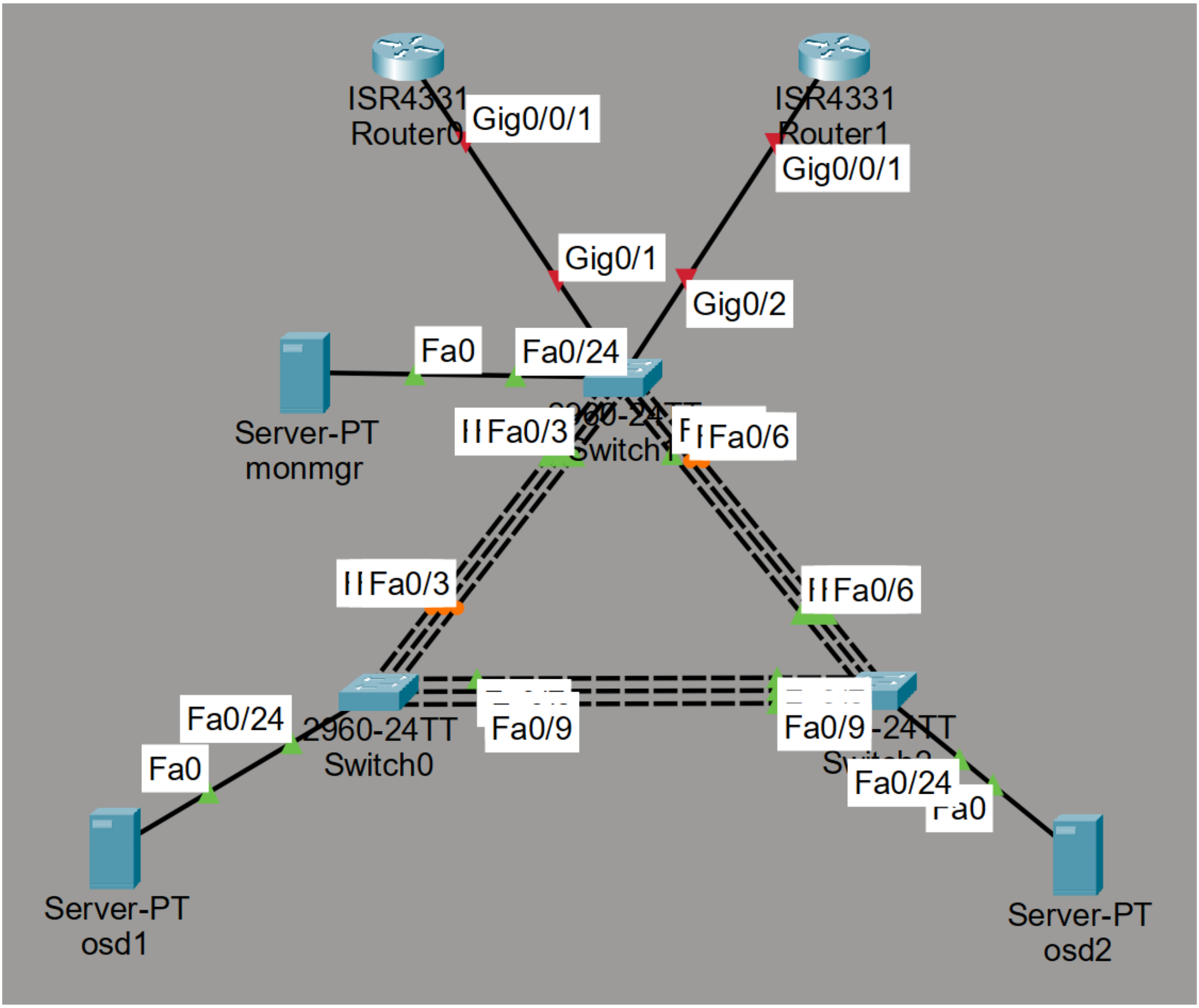

ceph
English
Dashboard
Cluster
Block
Object
File
Observability
Administration
Expand Cluster
Expand Cluster
1 Add Hosts
2 Create OSDs
3 Create Services
4 Review
Add Hosts
+ Add
10
Hostname
Service Instances
Labels
Status
Model
CPUs
Cores
Total Memory
Raw Capacity
HDDs
Flash
NICs
monmgr
(10.0.10.11)
mon: 1
mgr: 1
ceph-exporter: 1
crash: 1
node-exporter: 1
alertmanager: 1
grafana: 1
prometheus: 1
osd: 1
_admin
available
Virtual Machine (VirtualBox)
1
2
1.7 GiB
40 GiB
2
0
2
osd1
(10.0.10.12)
ceph-exporter: 1
crash: 1
node-exporter: 1
mgr: 1
mon: 1
osd: 1
rgw: 1
available
Virtual Machine (VirtualBox)
1
2
1.7 GiB
40 GiB
2
0
2
osd2
(10.0.10.13)
ceph-exporter: 1
crash: 1
node-exporter: 1
mon: 1
osd: 1
rgw: 1
available
Virtual Machine (VirtualBox)
1
2
1.7 GiB
40 GiB
2
0
2
0 selected / 3 found / 3 total
Cancel
Next

Selected Object Gateway: rgw-mcs.osd1.nijhjq (default)
Object » Users
Users
Roles
+ Create
10
Username
Tenant
Full name
Email address
Suspended
Max. buckets
Capacity Limit %
Object Limit %
dashboard
Ceph Dashboard
1000
No Limit
No Limit
egf2025
EstGauFlo 2025
1000
No Limit
No Limit
user-test
Testing User
Unlimited
No Limit
No Limit
0 selected / 3 total
Selected Object Gateway: rgw-mcs.osd1.nijhjq (default)
Object » Buckets
+ Create
10
Name
Owner
Used Capacity
Capacity Limit %
Objects
Object Limit %
estgauflo-s3-mac-2025
egf2025
0 B
No Limit
0
No Limit
Details
Policies
Bucket policy
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Principal": {
"AWS": "egf2025"
},
"Action": "s3:*",
"Resource": "arn:aws:s3:::estgauflo-*"
},
{
"Sid": "Statement2",
"Effect": "Allow",
"Principal": {
"AWS": "egf2025"
},
"Action": [
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:GetObjectTagging",
"s3:GetObjectVersion",
test-bucket
user-test
0 B
No Limit
0
No Limit

4. Cisco Packet Tracer

A. Créer la topologie en GUI

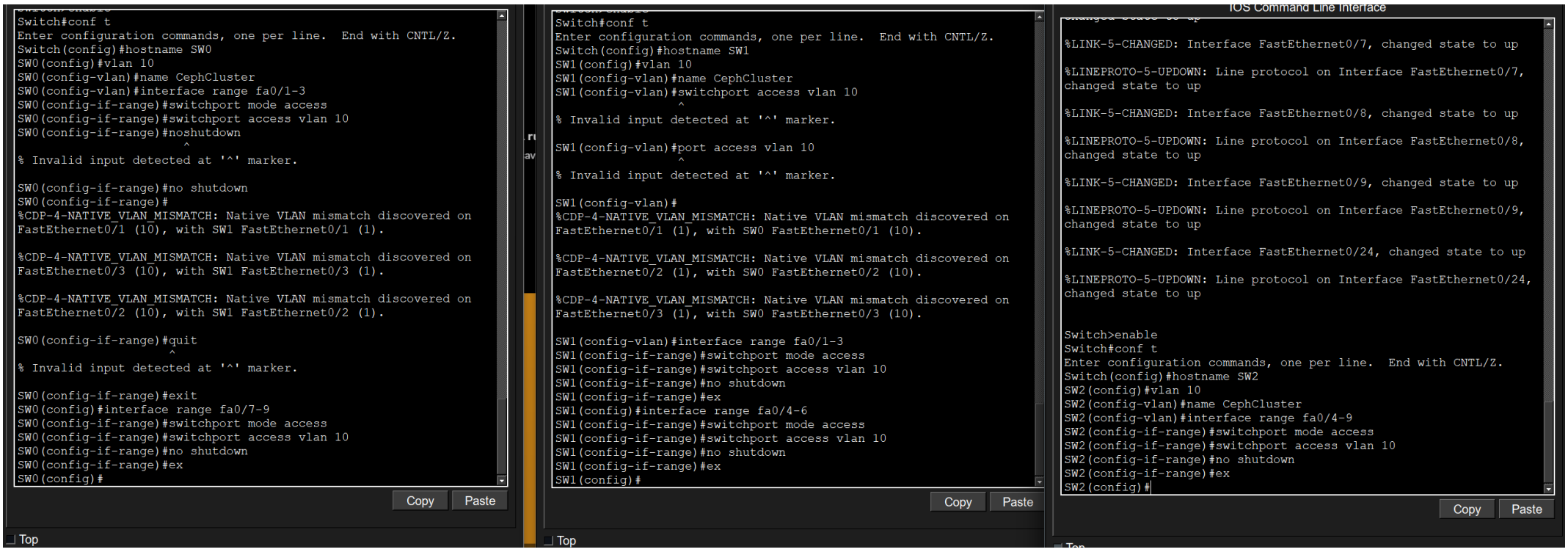
- VLAN unique pour les 3
- Switchs Layer 2 (un ou plusieurs)



B. Créer la topologie en CLI

Création des LAGs :

```
enable
  conf t
    interface range fa0/[1-7]-[3-9]
      channel-group [1,2,3] mode active
      no shutdown
      end
write memory
```



Créer les VLAN :

```
enable
  conf t
    vlan 10
      name CephCluster
      exit
    interface fa0/24
      switchport mode access
      switchport access vlan 10
      no shutdown
      exit
    interface port-channel [1,2,3]
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10
      no shutdown
      end
write memory
```

```
SW2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8,
changed state to up

%LINK-3-UPDOWN: Interface Port-channel3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9,
changed state to up

%LINK-5-CHANGED: Interface Port-channel3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3,
changed state to up
switchport trunk native vlan 1
SW2(config-if)#switchport trunk allowed vlan 1,10
SW2(config-if)#no shutdown
SW2(config-if)#exit
SW2(config)#
```

[Créer la passerelle HSRP sur les routeurs :]

```
enable
  conf t
    ip routing
    interface Gig0/0/1.10
      encapsulation dot1q 10
      ip address 10.0.10.[2,3] 255.255.255.0
      standby 1 ip 10.0.10.1
      standby 1 priority [100, 150]
      standby 1 preempt
      no shutdown
      end
show standby
write memory
```

```
Router0(config)#interface GigabitEthernet0/0/0
Router0(config-if)#
Router0(config-if)#exit
Router0(config)#interface GigabitEthernet0/0/1
Router0(config-if)#ip address 10.0.10.2 255.0.0.0
Router0(config-if)#ip address 10.0.10.2 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1, changed state to up
```

Copy Paste

```
Router1(config)#interface GigabitEthernet0/0/0
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface GigabitEthernet0/0/1
Router1(config-if)#ip address 10.0.10.3 255.0.0.0
Router1(config-if)#ip address 10.0.10.3 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1, changed state to up
```

Copy Paste

Router0

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
%SYS-5-CONFIG_I: Configured from console by console
show standby
GigabitEthernet0/0/1 - Group 1
  State is Active
    5 state changes, last state change 00:22:17
  Virtual IP address is 10.0.10.1
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.794 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  Group name is hsrp-Gig0/0/1-1 (default)
Router0#
%HSRP-6-STATECHANGE: GigabitEthernet0/0/1 Grp 1 state Speak ->
Standby
show standby
GigabitEthernet0/0/1 - Group 1
  State is Standby
    9 state changes, last state change 00:24:59
  Virtual IP address is 10.0.10.1
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.86 secs
  Preemption enabled
  Active router is 10.0.10.3, priority 150 (expires in 6 sec)
    MAC address is 0000.0C07.AC01
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig0/0/1-1 (default)
Router0#
```

Copy | Paste

Router1

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1, changed state to up

Router1(config-if)#
Router1(config-if)#
Router1(config-if)#
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface Gig0/0/1
Router1(config-if)#standby 1 ip 10.0.10.1
Router1(config-if)#standby 1 priority 150
Router1(config-if)#standby 1 preempt
Router1(config-if)#exit
 %HSRP-6-STATECHANGE: GigabitEthernet0/0/1 Grp 1 state Standby ->
Active

Router1(config)#exit
Router1#
%SYS-5-CONFIG_I: Configured from console by console
show standby
GigabitEthernet0/0/1 - Group 1
  State is Active
    3 state changes, last state change 00:24:38
  Virtual IP address is 10.0.10.1
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.244 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 100 (expires in 1 sec)
  Priority 150 (configured 150)
  Group name is hsrp-Gig0/0/1-1 (default)
Router1#
```

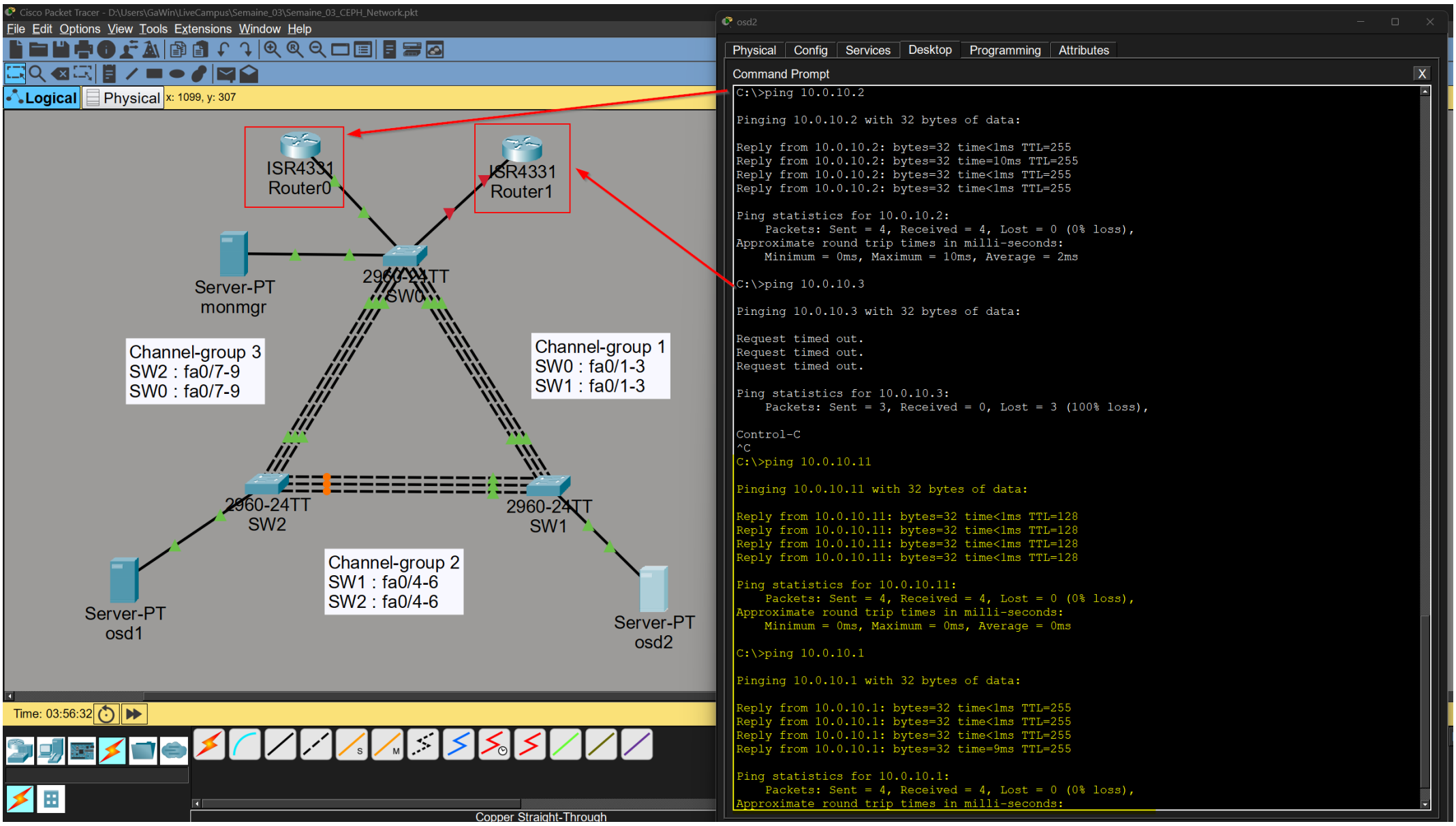
Copy | Paste

Et on vérifie par un PING d'un OSD à un autre :

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:97FF:FE8A:BA5E
   IPv6 Address.....: ::
   IPv4 Address.....: 10.0.10.12
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                         10.0.10.1

C:\>ping 10.0.10.13

Pinging 10.0.10.13 with 32 bytes of data:

Reply from 10.0.10.13: bytes=32 time<1ms TTL=128
Reply from 10.0.10.13: bytes=32 time<1ms TTL=128
Reply from 10.0.10.13: bytes=32 time<1ms TTL=128
Reply from 10.0.10.13: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.10.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>tracert 10.0.10.13
```

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:C9FF:FEDC:3D99
   IPv6 Address.....: ::
   IPv4 Address.....: 10.0.10.13
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                         10.0.10.1

C:\>ping 10.0.10.12

Pinging 10.0.10.12 with 32 bytes of data:

Reply from 10.0.10.12: bytes=32 time<1ms TTL=128
Reply from 10.0.10.12: bytes=32 time<1ms TTL=128
Reply from 10.0.10.12: bytes=32 time<1ms TTL=128
Reply from 10.0.10.12: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\> 10.0.10.12
```

Et on teste avec un routeur éteint :



C. Sécurisation

https://www.cisco.com/c/deleteme/sec/b_1710_sec_9300_cg/port_security.html

- Limiter le *MAC-address learning*
- Activer *port-security* en mettant 1 dresse MAC maximum
- Configurer les ports d'administration (console/VTY) avec authentification locale
- Activer le SSH sur les switchs avec restriction aux adresses du VLAN
- Autoriser le trafic Ceph, IMCP et SNMP uniquement depuis les adresses de gestion

Sécurité des ports :

```
enable
  conf t
    interface range fa0/#-#       // ports non utilisés
      shutdown
      exit
    interface range fa0/#-#       // ports en usage
      switchport port-security
      switchport port-security maximum 1
      switchport port-security violation restrict
      switchport port-security mac-address sticky
```

```
SW0>enable
SW0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW0(config)#int range fa0/1-3
SW0(config-if-range)#switchport port-security
SW0(config-if-range)#switchport port-security maximum 1
SW0(config-if-range)#switchport port-security violation restrict
SW0(config-if-range)#switchport port-security mac-address sticky
SW0(config-if-range)#end
SW0#
%SYS-5-CONFIG_I: Configured from console by console
conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW0(config)#int range fa0/7-9
SW0(config-if-range)#switchport port-security
SW0(config-if-range)#switchport port-security maximum 1
SW0(config-if-range)#switchport port-security violation restrict
SW0(config-if-range)#switchport port-security mac-address sticky
SW0(config-if-range)#end
SW0#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
SW0#
```

Activer le SSH :

```
ip domain-name mcs2025.local
username admin secret mcs2025
crypto key generate rsa general-keys modulus 2048
ip ssh version 2
```

```
SW0(config)#ip domain-name mcs2025.local
SW0(config)#username admin secret mcs2025
SW0(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: SW0.mcs2025.local

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:47:50.899: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW0(config)#ip ssh version 2
SW0(config)#
```

Protection par mot de passe :

```
enable
  conf t
    enable password encryption
    line console 0
      password CisCanne
      login local
    line vty 0 4
      login local
      transport input ssh
    enable secret Conf-Iture
    end
write memory
```

```
SW0(config)#enable password encryption
SW0(config)#line console 0
SW0(config-line)#password CisCanne
SW0(config-line)#login local
SW0(config-line)#exit
SW0(config)#line vty 0 4
SW0(config-line)#login local
SW0(config-line)#transport input ssh
SW0(config-line)#exit
SW0(config)#enable secret Conf-Iture
SW0(config)#end
SW0#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
SW0#exit
```

```
User Access Verification

Username:
Username: admin
Password:        mcs2025

SW0>enable
Password:        Conf-Iture
SW0#
```

ACL pour le trafic Ceph :

```
ip access-list extended CEPH-ALLOW
  permit tcp any any eq 80
  permit tcp any any eq 443
  permit tcp any any eq 6789
  permit tcp any any eq 7480
  permit tcp any any eq 8443
  permit tcp any any range 3300 3303
  permit tcp any any range 6800 7300
  permit udp any any range 6800 7300
  permit icmp any any
  permit udp any any eq 161
  deny ip any any
```

```
SW0(config)#ip access-list extended CEPH-ALLOW
SW0(config-ext-nacl)#permit tcp any any eq 80
SW0(config-ext-nacl)#permit tcp any any eq 443
SW0(config-ext-nacl)#permit tcp any any eq 6789
SW0(config-ext-nacl)#permit tcp any any eq 7480
SW0(config-ext-nacl)#permit tcp any any eq 8443
SW0(config-ext-nacl)#permit tcp any any range 3300 3303
SW0(config-ext-nacl)#permit tcp any any range 6800 7300
SW0(config-ext-nacl)#permit udp any any range 6800 7300
SW0(config-ext-nacl)#permit icmp any any
SW0(config-ext-nacl)#permit udp any any eq 161
SW0(config-ext-nacl)#deny ip any any
SW0(config-ext-nacl)#exit
SW0(config)#exit
SW0#
%SYS-5-CONFIG_I: Configured from console by console
show access-list
Extended IP access list CEPH-ALLOW
    10 permit tcp any any eq www
    20 permit tcp any any eq 443
    30 permit tcp any any eq 6789
    40 permit tcp any any eq 7480
    50 permit tcp any any eq 8443
    60 permit tcp any any range 3300 3303
    70 permit tcp any any range 6800 7300
    80 permit udp any any range 6800 7300
    90 permit icmp any any
    100 permit udp any any eq snmp
    110 deny ip any any

SW0#
```

Liens utiles

Bibliographie

Ceph

Tutoriel Scaleway d'un cluster Ceph

Tutoriel d'installer Ceph sur Rocky Linux

Configuration RGW sur RedHat

Cephadm pour RGW

Déployer Ceph sur Rocky Linux 9

Pare-feu Rocky

Mettre en place FirewallD

Ports pour cluster Ceph

FirewallD par Stéphane Robert

Détails sur la configuration

"Beast" pour RadosGW

Ressources

Rocky Linux