Table des matières

backup-01

Machine

- Partie matérielle
  - Serveur dédié
  - 1 processeur 8 cœursIntel Core i7-7700
  - 2 barrettes pour un total de 32 Go de mémoire RAM DDR4
  - 2 disques SATA Enterprise de 4 To
  - 1 carte réseau 1 Gbit/s Intel I219-LM
- Partie logicielle
  - Système d'exploitation : Debian stable

Configuration

Système d'exploitation

Debian stable (Debian 11 « Bullseye » au moment de la rédaction de cette page)

Adressage IP

```
# cat /etc/network/interfaces
### Hetzner Online GmbH installimage

source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback
iface lo inet6 loopback

auto enp0s31f6
iface enp0s31f6 inet static
  address 95.216.12.179
  netmask 255.255.255.192
  gateway 95.216.12.129
  # route 95.216.12.128/26 via 95.216.12.129
  up route add -net 95.216.12.128 netmask 255.255.255.192 gw 95.216.12.129
dev enp0s31f6

iface enp0s31f6 inet6 static
  address 2a01:4f9:2a:cc8::2
  netmask 64
  gateway fe80::1
```

Paramètres réseau et swap dans sysctl

Depuis fin 2024, nous avons décidé d'activer un bridge réseau afin de pouvoir faire tourner un hyperviseur (comme sur `hypervisor-01`) pour y héberger quelques machines virtuelles visant à soulager `hypervisor-01` (notamment les ressources consommées par Peertube pour le transcodage).

Dans `/etc/sysctl.d/99-liberta.conf` nous avons dû activer les paramètres réseau pour permettre au bridge de router les paquets et passer également la « swappiness » à 0. La mémoire doit être donc complètement saturée avant de commencer à « swapper » sur le disque dur (c'est un SSD) :

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.ip_forward=1
net.ipv6.conf.all.accept_dad=0
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.all.accept_ra_defrtr=0
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.all.accept_source_route=0
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.all.forwarding=1
net.ipv6.conf.default.accept_dad=0
net.ipv6.conf.default.accept_ra=0
net.ipv6.conf.default.accept_ra_defrtr=0
net.ipv6.conf.default.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_redirects=0
net.ipv6.conf.default.accept_source_route=0
net.ipv6.conf.default.autoconf=0
vm.swappiness=0
```

Routages et pare-feu avec iptables

En prévision de la mise en place de machines virtuelles sur cette machine, nous devrons paramétrer un filtrage (cela dit, plus besoin de NAT !)

```
### IPV4 ###

*nat
-A PREROUTING -d 95.216.12.179/128 -p tcp -m tcp --syn -m multiport --dports
80,443,1935 -m comment --comment "Router le trafic Web vers le serveur
web-02" -j DNAT --to-destination 192.168.10.105
-A POSTROUTING -s 192.168.10.0/24 -d 224.0.0.0/24 -m comment --comment "Ne
```

```
pas appliquer le masquerading sur le broadcast/multicast" -j RETURN
-A POSTROUTING -s 192.168.10.0/24 -d 255.255.255.255/32 -m comment --comment
"Ne pas appliquer le masquerading sur le broadcast/multicast" -j RETURN
-A POSTROUTING -s 192.168.10.0/24 ! -d 192.168.10.0/24 -p tcp -m comment --
comment "Masquerading sur tous les ports dans le sens sortant (VM ->
Internet)" -j MASQUERADE --to-ports 1024-65535
-A POSTROUTING -s 192.168.10.0/24 ! -d 192.168.10.0/24 -p udp -m comment --
comment "Masquerading sur tous les ports dans le sens sortant (VM ->
Internet)" -j MASQUERADE --to-ports 1024-65535
-A POSTROUTING -s 192.168.10.0/24 ! -d 192.168.10.0/24 -m comment --comment
"" -j MASQUERADE
COMMIT
*filter
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment
"Accepter le trafic des connexions établies, en entrée" -j ACCEPT
-A INPUT -i lo  -m comment --comment "Accepter le trafic basique depuis la
boucle locale, en entrée"-j ACCEPT
-A INPUT -p icmp --icmp-type 8 -m conntrack --ctstate NEW -m comment --
comment "Accepter le trafic basique ICMP, en entrée" -j ACCEPT
-A INPUT -p tcp -m tcp --syn -m conntrack --ctstate NEW --dport 22 -m
comment --comment "Accepter le SSH" -j ACCEPT
-A INPUT -p tcp -m tcp --syn -m conntrack --ctstate NEW --dport 1984 -m
comment --comment "Accepter le SSH" -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 52365 -m comment -
-comment "Accepter le tunnel SSH vers le serveur web-01 sur le port 52365" -
j ACCEPT
-A INPUT -i br2 -p udp -m udp -m multiport --dports 53 -m comment --comment
"Accepter les requêtes DNS (port 53) depuis les VM" -j ACCEPT
-A INPUT -i br2 -p tcp -m tcp -m multiport --dports 53 -m comment --comment
"Accepter les requêtes DNS (port 53) depuis les VM" -j ACCEPT
-A INPUT -i br2 -p tcp -m multiport --dport 2049 -m comment --comment
"Bloquer les requêtes rpcbind/portmap en entrée depuis l'extérieur" -j
ACCEPT
-A INPUT -i br2 -p tcp -m multiport --dport 111 -m comment --comment
"Bloquer les requêtes rpcbind/portmap en entrée depuis l'extérieur" -j
ACCEPT
-A INPUT -p tcp -s 127.0.0.1 --dport 111 -m comment --comment "Bloquer les
requêtes rpcbind/portmap en entrée depuis l'extérieur" -j ACCEPT
-A INPUT -p udp --dport 111 -m comment --comment "Bloquer les requêtes
rpcbind/portmap en entrée depuis l'extérieur" -j DROP
-A INPUT -p tcp --dport 111 -m comment --comment "Bloquer les requêtes
rpcbind/portmap en entrée depuis l'extérieur" -j DROP
-A INPUT -i br2 -p tcp -m tcp -m multiport --dports 10050 -m comment --
comment "Accepter les requêtes Zabbix passives (port 10050) depuis les VM" -
j ACCEPT
-A INPUT -p icmp  --icmp-type 8 -m conntrack --ctstate NEW -m limit --limit
1/s --limit-burst 1 -m comment --comment "On refuse les trop nombreux ping"
-j ACCEPT
-A INPUT -p icmp -m comment --comment "On refuse les trop nombreux ping" -j
DROP
-A INPUT -m conntrack --ctstate INVALID -m comment --comment "On refuse tout
```

```
le reste" -j DROP
-A INPUT -p tcp -m tcp -m comment --comment "On refuse tout le reste" -j
REJECT --reject-with tcp-reset
-A INPUT -m comment --comment "On refuse tout le reste" -j REJECT --reject-
with icmp-port-unreachable
-A FORWARD -d 192.168.10.0/24 -o br2 -m conntrack --ctstate
RELATED,ESTABLISHED -m comment --comment "Accepter les connexions établies
sur le LAN" -j ACCEPT
-A FORWARD -s 192.168.10.0/24 -i br2 -m comment --comment "Accepter le
trafic sortant depuis le LAN" -j ACCEPT
-A FORWARD -i br2 -o br2 -m comment --comment "Accepter le trafic interne
entre les VM" -j ACCEPT
-A FORWARD -d 192.168.10.105/32 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 80,443,1935 -m comment --comment "Accepter
les paquets redirigés vers des ports particuliers pour le Web vers le
serveur web" -j ACCEPT
-A FORWARD -d 192.168.10.250/32 -o br2 -p tcp -m tcp -m conntrack --ctstate
NEW -m multiport --dports 8484 -m comment --comment "Accepter les paquets
redirigés vers des ports particuliers pour le monitoring vers le serveur de
monitoring" -j ACCEPT
-A INPUT -s 102.132.96.0/20 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 103.4.96.0/22 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 129.134.0.0/17 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 129.134.160.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 129.134.25.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 129.134.26.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 129.134.27.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 129.134.28.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 129.134.29.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 129.134.30.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 129.134.31.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 139.223.200.130/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.0.0/17 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.192.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.195.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.196.0/24 -m comment --comment
```

```
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.197.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.198.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.199.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.200.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.201.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.202.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.203.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.204.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.205.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.207.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.208.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.209.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.210.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.211.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.212.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.214.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.215.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.216.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.217.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.218.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.22.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.221.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.222.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.223.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.224.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
```

```
-A INPUT -s 157.240.225.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.226.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.227.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.228.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.229.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.23.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.231.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.232.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.233.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.234.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.235.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.236.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.237.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.238.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.239.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.240.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.24.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.241.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.242.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.243.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.244.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.245.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.247.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.249.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.250.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.25.0/24 -m comment --comment
```

```
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.251.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.252.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.253.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.254.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.26.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.27.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.28.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.29.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.30.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.3.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.31.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.5.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.6.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.7.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.8.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 157.240.9.0/24 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 162.254.207.51/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 162.255.119.207/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 172.67.135.213/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 173.252.64.0/18 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 179.60.192.0/22 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 185.199.108.153/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 185.199.111.153/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 185.60.216.0/22 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 198.54.117.211/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
```

```
-A INPUT -s 204.15.20.0/22 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 27.124.125.189/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 31.13.24.0/21 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 31.13.64.0/18 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 34.117.168.233/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 37.9.175.187/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 45.130.41.7/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 45.64.40.0/22 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 45.91.92.164/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 54.81.116.232/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 61.9.242.43/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 64.225.91.73/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 66.220.144.0/20 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 69.171.224.0/19 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 74.119.76.0/22 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 89.223.68.248/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A FORWARD -i br2 -m comment --comment "Rejeter tout le reste" -j REJECT --
reject-with icmp-port-unreachable
-A FORWARD -o br2 -m comment --comment "Rejeter tout le reste" -j REJECT --
reject-with icmp-port-unreachable
COMMIT

### IPV6 ###

*filter
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED  -m comment --comment
"Accepter le trafic basique : ICMP, boucle locale et connexions établies, en
entrée" -j ACCEPT
-A INPUT -i lo  -m comment --comment "Accepter le trafic basique : ICMP,
boucle locale et connexions établies, en entrée" -j ACCEPT
-A INPUT ! -i lo -d ::1/128  -m comment --comment "Accepter le trafic
basique : ICMP, boucle locale et connexions établies, en entrée" -j REJECT
-A INPUT -p tcp -m tcp --syn -m conntrack --ctstate NEW --dport 22 -m
comment --comment "Accepter le SSH" -j ACCEPT
-A INPUT -p tcp -m tcp --syn -m conntrack --ctstate NEW --dport 1984 -m
```

```
comment --comment "Accepter le SSH" -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 52365 -m comment --comment "Accepter le tunnel SSH vers le serveur web-01 sur le port 52365" -j ACCEPT
-A INPUT -i br2 -p udp -m udp -m multiport --dports 53 -m comment --comment "Accepter les requêtes DNS (port 53) depuis les VM" -j ACCEPT
-A INPUT -i br2 -p tcp -m tcp -m multiport --dports 53 -m comment --comment "Accepter les requêtes DNS (port 53) depuis les VM" -j ACCEPT
-A INPUT -i br2 -p tcp -m multiport --dport 2049 -m comment --comment "Bloquer les requêtes rpcbind/portmap en entrée depuis l'extérieur" -j ACCEPT
-A INPUT -i br2 -p tcp -m multiport --dport 111 -m comment --comment "Bloquer les requêtes rpcbind/portmap en entrée depuis l'extérieur" -j ACCEPT
-A INPUT -p tcp -s ::1/128  --dport 111  -m comment --comment "Bloquer les requêtes rpcbind/portmap en entrée depuis l'extérieur" -j ACCEPT
-A INPUT -p udp --dport 111 -m comment --comment "Bloquer les requêtes rpcbind/portmap en entrée depuis l'extérieur" -j DROP
-A INPUT -p tcp --dport 111 -m comment --comment "Bloquer les requêtes rpcbind/portmap en entrée depuis l'extérieur" -j DROP
-A INPUT -i br2 -p tcp -m tcp -m multiport --dports 10050 -m comment --comment "Accepter les requêtes Zabbix passives (port 10050) depuis les VM" -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type parameter-problem -m comment --comment "On accepte l'ICMPv6 indispensable au fonctionnement d'IPv6" -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type echo-request -m comment --comment "On accepte l'ICMPv6 indispensable au fonctionnement d'IPv6" -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type echo-reply -m comment --comment "On accepte l'ICMPv6 indispensable au fonctionnement d'IPv6" -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type router-advertisement -m hl --hl-eq 255 -m comment --comment "On accepte l'ICMPv6 indispensable au fonctionnement d'IPv6" -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type router-solicitation -m hl --hl-eq 255 -m comment --comment "On accepte l'ICMPv6 indispensable au fonctionnement d'IPv6" -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type neighbour-advertisement -m hl --hl-eq 255 -m comment --comment "On accepte l'ICMPv6 indispensable au fonctionnement d'IPv6" -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type neighbour-solicitation -m hl --hl-eq 255 -m comment --comment "On accepte l'ICMPv6 indispensable au fonctionnement d'IPv6" -j ACCEPT
-A INPUT  -p icmpv6 --icmpv6-type echo-request -m conntrack --ctstate NEW -m limit --limit 1/s --limit-burst 1 -m comment --comment "On refuse les trop nombreux ping" -j ACCEPT
-A INPUT  -p icmpv6 --icmpv6-type echo-request -m comment --comment "On refuse les trop nombreux ping" -j DROP
-A INPUT -m conntrack --ctstate INVALID -m comment --comment "On refuse tout le reste en entrée" -j DROP
-A INPUT -m comment --comment "On refuse tout le reste en entrée" -j REJECT
-A FORWARD -d 2a01:4f9:2a:cc8::/64 -o br2 -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "Accepter les connexions établies
```

```
sur le LAN" -j ACCEPT
-A FORWARD -s 2a01:4f9:2a:cc8::/64 -i br2 -m comment --comment "Accepter le
trafic sortant depuis le LAN" -j ACCEPT
-A FORWARD -i br2 -o br2 -m comment --comment "Accepter le trafic interne
entre les VM" -j ACCEPT
-A FORWARD -d 2a01:4f9:2a:cc8::105/128 -o br2 -p tcp -m tcp --syn -m
conntrack --ctstate NEW -m multiport --dports 80,443,1935  -m comment --
comment "Accepter les paquets redirigés vers des ports particuliers pour le
Web vers le serveur web (inutile, mais au cas où)" -j ACCEPT
-A INPUT -s 2620:0:1c00::/40 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2620:10d:c090::/44 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2880::/32 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff02::/47 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff19::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff1b::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff1c::/46 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff23::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff25::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff27::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff28::/46 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff2f::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff30::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff35::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff37::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff38::/46 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff3f::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff40::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff43::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff44::/47 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff48::/46 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
```

```
-A INPUT -s 2a03:2887:ff4d::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff4e::/47 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff50::/47 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff52::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2a03:2887:ff58::/47 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2c0f:ef78:3::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2c0f:ef78:5::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2c0f:ef78:6::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2c0f:ef78:9::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2c0f:ef78:d::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2c0f:ef78:e::/47 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2c0f:ef78:11::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A INPUT -s 2c0f:ef78:12::/48 -m comment --comment
"Meta/Facebook/Instagram/Threads Adios!" -j DROP
-A FORWARD -i br2 -m comment --comment "Rejeter tout le reste" -j REJECT
-A FORWARD -o br2 -m comment --comment "Rejeter tout le reste" -j REJECT
COMMIT
```

Paquets installés

La liste des paquets :

```
# dpkg -l | grep '^i' |awk '{ print $2 }' | sed '/^$/d'| sort
acl
acpid
adduser
amd64-microcode
apt
aptitude
aptitude-common
apt-utils
at
base-files
base-passwd
bash
bash-completion
bind9-dnsutils
bind9-host
```

```
bind9-libs:amd64
binutils
binutils-common:amd64
binutils-x86-64-linux-gnu
bsdextrautils
bsdutils
btrfs-progs
busybox
bzip2
ca-certificates
console-setup
console-setup-linux
coreutils
cpio
cpp
cpp-10
cron
cryptsetup
cryptsetup-bin
cryptsetup-initramfs
curl
dash
dbus
dctrl-tools
debconf
debconf-i18n
debian-archive-keyring
debianutils
diffutils
discover
discover-data
distro-info-data
dkms
dmeventd
dmidecode
dmsetup
dnsutils
dosfstools
dpkg
dpkg-dev
e2fsprogs
efibootmgr
ethtool
fail2ban
fdisk
file
findutils
firmware-bnx2x
gcc
gcc-10
gcc-10-base:amd64
```

```
gcc-9-base:amd64
gdisk
gettext-base
gpgv
grep
groff-base
grub2-common
grub-common
grub-efi-amd64
grub-efi-amd64-bin
grub-pc-bin
gzip
hostname
htop
iftop
ifupdown
init
initramfs-tools
initramfs-tools-core
init-system-helpers
intel-microcode
iotop
iproute2
iptables
iputils-ping
isc-dhcp-client
isc-dhcp-common
iucode-tool
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
less
libacl1:amd64
libaio1:amd64
libapparmor1:amd64
libapt-pkg6.0:amd64
libargon2-1:amd64
libasan6:amd64
libatomic1:amd64
libattr1:amd64
libaudit1:amd64
libaudit-common
libbinutils:amd64
libblas3:amd64
libblkid1:amd64
libboost-iostreams1.74.0:amd64
libbpf0:amd64
libbrotli1:amd64
libbsd0:amd64
```

```
libbz2-1.0:amd64
libc6:amd64
libc6-dev:amd64
libcap2:amd64
libcap2-bin
libcap-ng0:amd64
libc-bin
libcbor0:amd64
libcc1-0:amd64
libc-dev-bin
libc-l10n
libcom-err2:amd64
libcrypt1:amd64
libcrypt-dev:amd64
libcryptsetup12:amd64
libctf0:amd64
libctf-nobfd0:amd64
libcurl3-gnutls:amd64
libcurl4:amd64
libcwidget4:amd64
libdb5.3:amd64
libdbus-1-3:amd64
libdebconfclient0:amd64
libdevmapper1.02.1:amd64
libdevmapper-event1.02.1:amd64
libdiscover2
libdns-export1110
libdpkg-perl
libedit2:amd64
libefiboot1:amd64
libefivar1:amd64
libelf1:amd64
libestr0:amd64
libexpat1:amd64
libext2fs2:amd64
libfastjson4:amd64
libfdisk1:amd64
libffi7:amd64
libfido2-1:amd64
libfl2:amd64
libfreetype6:amd64
libfstrm0:amd64
libfuse2:amd64
libgcc-10-dev:amd64
libgcc-s1:amd64
libgcrypt20:amd64
libgdbm6:amd64
libgdbm-compat4:amd64
libgmp10:amd64
libgnutls30:amd64
libgomp1:amd64
```

```
libgpg-error0:amd64
libgssapi-krb5-2:amd64
libhogweed6:amd64
libicu67:amd64
libidn2-0:amd64
libinih1:amd64
libip4tc2:amd64
libip6tc2:amd64
libisc-export1105:amd64
libisl23:amd64
libitm1:amd64
libjansson4:amd64
libjson-c5:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc:amd64
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
libldap-2.4-2:amd64
libldap-common
liblinear4:amd64
liblmdb0:amd64
liblocale-gettext-perl
liblockfile-bin
liblognorm5:amd64
liblsan0:amd64
liblua5.3-0:amd64
liblvm2cmd2.03:amd64
liblz4-1:amd64
liblzma5:amd64
liblzo2-2:amd64
libmagic1:amd64
libmagic-mgc
libmaxminddb0:amd64
libmd0:amd64
libmnl0:amd64
libmount1:amd64
libmpc3:amd64
libmpdec3:amd64
libmpfr6:amd64
libncurses6:amd64
libncursesw6:amd64
libnetfilter-conntrack3:amd64
libnettle8:amd64
libnewt0.52:amd64
libnfnetlink0:amd64
libnftables1:amd64
libnftnl11:amd64
libnghttp2-14:amd64
libnl-3-200:amd64
```

```
libnl-genl-3-200:amd64
libnsl2:amd64
libnsl-dev:amd64
libnss-systemd:amd64
libnvpair3linux
libp11-kit0:amd64
libpam0g:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam-systemd:amd64
libpcap0.8:amd64
libpci3:amd64
libpcre2-8-0:amd64
libpcre3:amd64
libperl5.32:amd64
libpipeline1:amd64
libpng16-16:amd64
libpopt0:amd64
libprocps8:amd64
libprotobuf-c1:amd64
libpsl5:amd64
libpython3.9-minimal:amd64
libpython3.9-stdlib:amd64
libpython3-stdlib:amd64
libquadmath0:amd64
libreadline8:amd64
librtmp1:amd64
libsasl2-2:amd64
libsasl2-modules:amd64
libsasl2-modules-db:amd64
libseccomp2:amd64
libselinux1:amd64
libsemanage1:amd64
libsemanage-common
libsepol1:amd64
libsigc++-2.0-0v5:amd64
libslang2:amd64
libsmartcols1:amd64
libsqlite3-0:amd64
libss2:amd64
libssh2-1:amd64
libssl1.1:amd64
libstdc++6:amd64
libsystemd0:amd64
libtasn1-6:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libtinfo6:amd64
libtirpc3:amd64
```

```
libtirpc-common
libtirpc-dev:amd64
libtsan0:amd64
libubsan1:amd64
libuchardet0:amd64
libudev1:amd64
libunistring2:amd64
libusb-0.1-4:amd64
libuuid1:amd64
libuutil3linux
libuv1:amd64
libwrap0:amd64
libxapian30:amd64
libxml2:amd64
libxtables12:amd64
libxxhash0:amd64
libzfs4linux
libzpool4linux
libzstd1:amd64
linux-base
linux-compiler-gcc-10-x86
linux-headers-5.10.0-16-amd64
linux-headers-5.10.0-16-common
linux-headers-amd64
linux-image-5.10.0-16-amd64
linux-image-5.10.0-9-amd64
linux-image-amd64
linux-kbuild-5.10
linux-libc-dev:amd64
locales
login
logrotate
logsave
lsb-base
lsb-release
lsof
lua-lpeg:amd64
lvm2
mailcap
make
man-db
manpages
mawk
mbuffer
mdadm
media-types
mime-support
mokutil
mount
mtr-tiny
nano
```

```
ncurses-base
ncurses-bin
ncurses-term
netbase
netcat-traditional
net-tools
nftables
nmap
nmap-common
openssh-client
openssh-server
openssh-sftp-server
openssl
passwd
patch
pci.ids
pciutils
perl
perl-base
perl-modules-5.32
procps
publicsuffix
python3
python3.9
python3.9-minimal
python3-apt
python3-certifi
python3-chardet
python3-debian
python3-debianbts
python3-distutils
python3-httplib2
python3-idna
python3-lib2to3
python3-minimal
python3-pkg-resources
python3-pycurl
python3-pysimplesoap
python3-reportbug
python3-requests
python3-six
python3-urllib3
python-apt-common
readline-common
reportbug
rsync
rsyslog
runit-helper
sed
sensible-utils
shim-helpers-amd64-signed
```

```
shim-signed:amd64
shim-signed-common
shim-unsigned
sudo
systemd
systemd-sysv
systemd-timesyncd
sysvinit-utils
tar
task-english
tasksel
tasksel-data
task-ssh-server
tcpdump
traceroute
tzdata
ucf
udev
util-linux
util-linux-locales
vim-common
vim-tiny
wget
whiptail
xfsprogs
xkb-data
xxd
xz-utils
zfs-dkms
zfsutils-linux
zlib1g:amd64
```

Stockage ZFS

Un « pool » de sauvegarde sur les 2 gros disques mécaniques a été créé en miroir (RAID1).

Nous avons ensuite créé un « pool » avec les numéros de série des disques (qu'on trouve dans `/dev/disk/by-id`), avons activé la compression LZ4 et avons créé un ensemble de partages ZFS pour stocker les disques durs virtuels des VM (le partage `prod-01`), et sur d'autres partages les données de hébergé·e·s, etc. qu'on montera plus tard dans chaque VM en NFS :

```
# zpool status -v
  pool: zdatabackup
 state: ONLINE
config:

    NAME                                        STATE     READ WRITE CKSUM
    zdatabackup                                 ONLINE       0     0     0
      mirror-0                                  ONLINE       0     0     0
        ata-ST4000NM0245-1Z2107_ZC137LB6-part5  ONLINE       0     0     0
```

```
        ata-ST4000NM0245-1Z2107_ZC139JEZ-part5  ONLINE       0     0     0

errors: No known data errors
```

```
# zfs list
NAME                          USED  AVAIL     REFER  MOUNTPOINT
zdatabackup                  1.66M  3.47T      144K  /zdatabackup
zdatabackup/audio_data         96K  3.47T       96K  /zdatabackup/audio_data
zdatabackup/cloud_data         96K  3.47T       96K  /zdatabackup/cloud_data
zdatabackup/cryptpad_data      96K  3.47T       96K
/zdatabackup/cryptpad_data
zdatabackup/mail_data          96K  3.47T       96K  /zdatabackup/mail_data
zdatabackup/mobilizon_data     96K  3.47T       96K
/zdatabackup/mobilizon_data
zdatabackup/mysql_data         96K  3.47T       96K  /zdatabackup/mysql_data
zdatabackup/pleroma_data       96K  3.47T       96K
/zdatabackup/pleroma_data
zdatabackup/postgresql_data    96K  3.47T       96K
/zdatabackup/postgresql_data
zdatabackup/prod-01            96K  3.47T       96K  /zdatabackup/prod-01
zdatabackup/video_data         96K  3.47T       96K  /zdatabackup/video_data
```

Ce serveur reçoit la réplication des snapshots ZFS du serveur `hypervisor-01`, cf. la page dédiée.