Table des matières

hypervisor-01

Machine

- Partie matérielle
  - Serveur HP (SB64)
  - 1 processeur 8 cœurs Intel Xeon E3-1275V6
  - 4 barrettes pour un total de 64 Go de mémoire RAM DDR4, ECC
  - 1 disque SSD SATA de 256 Go
  - 2 disques SATA Enterprise de 4 To
  - 1 carte réseau 1 Gbit/s Intel I219-LM
- Partie logicielle
  - Système d'exploitation : Debian stable
  - Technologies de virtualisation : KVM, QEMU, libvirt
  - Stockage des machines virtuelles et des données : ZFS
  - 1 IPv4 : 159.69.59.13/32
  - 1 IPv6 : 2a01:4f8:231:aa6::/64

Topologie

- 1 hyperviseur KVM exposé sur Internet sur 159.69.59.13/32
- plusieurs machines virtuelles KVM/QEMU pour les services, pilotées par libvirt, sur 192.168.10.0/24 :
  - audio-01 : Debian stable, Nginx, application Funkwhale, ffmpeg
  - mail-01 : Debian stable, services mail Postfix, Dovecot, Amavis, Spamassassin, ClamAV, Sieve (déploiement à venir)
  - proxy-01 ~~: Debian stable, proxy frontal Nginx et pare-feu iptables, bannissement par Fail2Ban~~ Ce proxy a été supprimé le 30 janvier 2022.
  - sql-01 : Debian stable, services MySQL et PostgreSQL
  - video-01 : Debian stable, Nginx, application Peertube, ffmpeg
  - visio-01 ~~: Debian stable, Nginx, application Jitsi Meet~~
  - web-01 : Debian stable, Nginx, services web, sites, blogs, sites internes, service Redis

Toutes les requêtes venant d'internet sont pré-routées et redirigées via iptables vers la ou les machines virtuelles concernées. L'infrastructure interne est protégée par plusieurs pare-feu et un système de bannissement.

Configuration

Système d'exploitation

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

Adressage IP

Hetzner offre une IP publique. Nous avons modifié l'adressage pour créer 2 réseaux internes : un pour les machines virtuelles et un pour notre administration, puis on bridgé le réseau des VM sur le réseau adressé avec l'IP publique. L'interface enp0trucmachin est devenue br0. La ligne « pre-up » corrige notamment un problème connu d'instabilité de connexion sur la carte réseau de ce serveur.

L'adressage du réseau d'administration (10.X.X.X) a été masqué pour des raisons de sécurité.

L'adressage en IPv6 est une adaptation du réseau IPv4 vers IPv6. À terme, il sera judicieux qu'on utilise le réseau /64 qu'Hetzner nous offre, ça fait quand même 2^64 adresses IP disponibles, à savoir 18 446 744 073 709 551 616 adresses !

```
root@hypervisor-01 ~ # cat /etc/network/interfaces
### Hetzner Online GmbH installimage

source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback
iface lo inet6 loopback

auto br0
iface br0 inet static
    bridge_ports enp0s31f6
    bridge_hw enp0s31f6
    bridge_fd 0
    bridge_stp off
    bridge_maxwait 0
    address  159.69.59.13
    netmask  255.255.255.192
    gateway  159.69.59.1
    pre-up /usr/sbin/ethtool -K enp0s31f6 tso off gso off

iface br0 inet6 static
    bridge_ports enp0s31f6
    bridge_hz enp0s31f6
    bridge_fd 0
    bridge_stp off
    bridge_maxwait 0
    address 2a01:4f8:231:aa6::13
    netmask 64
    gateway fe80::1

# Management
auto br1
iface br1 inet static
    bridge_ports none
    bridge_fd 0
    bridge_stp off
```

```
    address 10.X.Y.Z
    netmask 255.X.Y.Z

iface br1 inet6 static
    bridge_ports none
    bridge_fd 0
    bridge_stp off
    address ::ffff:a0a:a01
    netmask 120

# VM-LAN
auto br2
iface br2 inet static
    bridge_ports none
    bridge_fd 0
    bridge_stp off
    address 192.168.10.1
    netmask 255.255.255.0

iface br2 inet6 static
    bridge_ports none
    bridge_fd 0
    bridge_stp off
    address ::ffff:c0a8:a01
    netmask 120
```

Routage et filtrage avec iptables

Nous avons dû ensuite router et rediriger tout ça avec iptables afin de communiquer depuis l'extérieur avec le réseau des VM et filtrer les connexions entrantes, c'est le point le plus important.

Le paquet `iptables-persistent` doit avoir été installé pour conserver les modifications du pare-feu entre chaque redémarrage. Le port SSH a été masqué.

Il est bien sûr extrêmement important de sécuriser SSH : interdire le login root avec mot de passe, utiliser de bons algorithmes de chiffrement, changer le port, n'autoriser qu'une IP distante (ou mieux, ne rien autoriser depuis internet et utiliser un VPN) et mettre en place un faux serveur SSH pour que les attaquants perdent leur temps à essayer de se connecter, sans vous faire perdre le vôtre (et ajouter un Fail2Ban évidemment). La recette reste secrète, désolé ! 😉

Les règles concernant le réseau d'administration n'apparaissent pas non plus ici.

Pour IPv4, dans `/etc/iptables-persistent/rules.v4` :

```
*nat

# Router le trafic Web vers le serveur web :
-A PREROUTING -d 159.69.59.13/32 -p tcp -m tcp --syn -m multiport --dports
80,443 -j DNAT --to-destination 192.168.10.5
```

```
# Router le mail envoi/réception vers le serveur mail :
-A PREROUTING -d 159.69.59.13/32 -p tcp -m tcp --syn -m multiport --dports
587,993,25 -j DNAT --to-destination 192.168.10.7

# Tests
## Router les ports des applications vers le serveur web :
#-A PREROUTING -d 159.69.59.13/32 -p tcp -m tcp --syn -m multiport --dports
1935,1936,3000,3001,9000,9001 -j DNAT --to-destination 192.168.10.5
#
## Router le port 5868 vers le serveur audio pour Funkwhale :
#-A PREROUTING -d 159.69.59.13/32 -p tcp -m tcp --syn -m multiport --dports
5868 -j DNAT --to-destination 192.168.10.9

# Router le 8484 pour Zabbix vers le serveur monitoring :
-A PREROUTING -d 159.69.59.13/32 -p tcp -m tcp --syn -m multiport --dports
8484 -j DNAT --to-destination 192.168.10.250

# Ne pas appliquer le masquerading sur le broadcast/multicast :
-A POSTROUTING -s 192.168.10.0/24 -d 224.0.0.0/24 -j RETURN
-A POSTROUTING -s 192.168.10.0/24 -d 255.255.255.255/32 -j RETURN

# Masquerading sur tous les ports dans le sens sortant (VM -> Internet)
-A POSTROUTING -s 192.168.10.0/24 ! -d 192.168.10.0/24 -p tcp -j MASQUERADE
--to-ports 1024-65535
-A POSTROUTING -s 192.168.10.0/24 ! -d 192.168.10.0/24 -p udp -j MASQUERADE
--to-ports 1024-65535
-A POSTROUTING -s 192.168.10.0/24 ! -d 192.168.10.0/24 -j MASQUERADE

COMMIT

*filter

# Accepter le trafic basique : ICMP, boucle locale et connexions établies,
en entrée :
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp --icmp-type 8 -m conntrack --ctstate NEW -j ACCEPT

# Accepter le SSH :
-A INPUT -p tcp -m tcp --syn -m conntrack --ctstate NEW --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --syn -m conntrack --ctstate NEW --dport 1984 -j
ACCEPT

# Accepter les connexions pour le mail :
-A INPUT -p tcp -m tcp --syn -m conntrack --ctstate NEW -m multiport --
dports 587,993,25 -j ACCEPT

# Accepter le tunnel SSH vers le serveur web-01 sur le port 52365 :
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 52365 -j ACCEPT
```

```
# Accepter les requêtes DNS (port 53) depuis les VM :
-A INPUT -i br2 -p udp -m udp -m multiport --dports 53 -j ACCEPT
-A INPUT -i br2 -p tcp -m tcp -m multiport --dports 53 -j ACCEPT

# Bloquer les requêtes rpcbind/portmap en entrée ***depuis l'extérieur*** :
-A INPUT -i br2 -p tcp -m multiport --dport 2049 -j ACCEPT
-A INPUT -i br2 -p tcp -m multiport --dport 111 -j ACCEPT
-A INPUT -p tcp -s 127.0.0.1 --dport 111 -j ACCEPT
-A INPUT -p udp --dport 111 -j DROP
-A INPUT -p tcp --dport 111 -j DROP

# Accepter les requêtes Zabbix passives (port 10050) depuis les VM :
-A INPUT -i br2 -p tcp -m tcp -m multiport --dports 10050 -j ACCEPT

# On refuse les trop nombreux ping :
-A INPUT -p icmp  --icmp-type 8 -m conntrack --ctstate NEW -m limit --limit
1/s --limit-burst 1 -j ACCEPT
-A INPUT -p icmp -j DROP

# On refuse tout le reste :
-A INPUT -m conntrack --ctstate INVALID -j DROP
-A INPUT -p tcp -m tcp -j REJECT --reject-with tcp-reset
-A INPUT -j REJECT --reject-with icmp-port-unreachable

# Accepter les connexions établies sur le LAN :
-A FORWARD -d 192.168.10.0/24 -o br2 -m conntrack --ctstate
RELATED,ESTABLISHED -j ACCEPT

# Accepter le trafic sortant depuis le LAN :
-A FORWARD -s 192.168.10.0/24 -i br2 -j ACCEPT

# Accepter le trafic interne entre les VM :
-A FORWARD -i br2 -o br2 -j ACCEPT

# Accepter les paquets redirigés vers des ports particuliers pour le Web
vers le serveur web :
-A FORWARD -d 192.168.10.5/32 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 80,443,8484 -j ACCEPT

# Accepter les paquets redirigés vers des ports particuliers pour le mail
vers le serveur mail :
-A FORWARD -d 192.168.10.7/32 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 587,993,25 -j ACCEPT

# Accepter les paquets redirigés vers des ports particuliers pour le
monitoring vers le serveur de monitoring :
-A FORWARD -d 192.168.10.250/32 -o br2 -p tcp -m tcp -m conntrack --ctstate
NEW -m multiport --dports 8484 -j ACCEPT

# Tests
## Accepter les paquets redirigés vers des ports particuliers vers le
```

```
serveur web :
#-A FORWARD -d 192.168.10.5/32 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 1935,1936,3000,3001,9000,9001 -j ACCEPT
#
## Accepter les paquets redirigés vers des ports particuliers pour funkwhale
service 5868 vers le serveur audio :
#-A FORWARD -d 192.168.10.9/32 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 5868 -j ACCEPT

# On bloque TOUT le trafic en provenance de Meta/Facebook/Instagram/Threads
:
-A INPUT -s 102.132.96.0/20 -j DROP
-A INPUT -s 103.4.96.0/22 -j DROP
-A INPUT -s 129.134.0.0/17 -j DROP
-A INPUT -s 129.134.160.0/24 -j DROP
-A INPUT -s 129.134.25.0/24 -j DROP
-A INPUT -s 129.134.26.0/24 -j DROP
-A INPUT -s 129.134.27.0/24 -j DROP
-A INPUT -s 129.134.28.0/24 -j DROP
-A INPUT -s 129.134.29.0/24 -j DROP
-A INPUT -s 129.134.30.0/24 -j DROP
-A INPUT -s 129.134.31.0/24 -j DROP
-A INPUT -s 139.223.200.130/32 -j DROP
-A INPUT -s 157.240.0.0/17 -j DROP
-A INPUT -s 157.240.192.0/24 -j DROP
-A INPUT -s 157.240.195.0/24 -j DROP
-A INPUT -s 157.240.196.0/24 -j DROP
-A INPUT -s 157.240.197.0/24 -j DROP
-A INPUT -s 157.240.198.0/24 -j DROP
-A INPUT -s 157.240.199.0/24 -j DROP
-A INPUT -s 157.240.200.0/24 -j DROP
-A INPUT -s 157.240.201.0/24 -j DROP
-A INPUT -s 157.240.202.0/24 -j DROP
-A INPUT -s 157.240.203.0/24 -j DROP
-A INPUT -s 157.240.204.0/24 -j DROP
-A INPUT -s 157.240.205.0/24 -j DROP
-A INPUT -s 157.240.207.0/24 -j DROP
-A INPUT -s 157.240.208.0/24 -j DROP
-A INPUT -s 157.240.209.0/24 -j DROP
-A INPUT -s 157.240.210.0/24 -j DROP
-A INPUT -s 157.240.211.0/24 -j DROP
-A INPUT -s 157.240.212.0/24 -j DROP
-A INPUT -s 157.240.214.0/24 -j DROP
-A INPUT -s 157.240.215.0/24 -j DROP
-A INPUT -s 157.240.216.0/24 -j DROP
-A INPUT -s 157.240.217.0/24 -j DROP
-A INPUT -s 157.240.218.0/24 -j DROP
-A INPUT -s 157.240.22.0/24 -j DROP
-A INPUT -s 157.240.221.0/24 -j DROP
-A INPUT -s 157.240.222.0/24 -j DROP
-A INPUT -s 157.240.223.0/24 -j DROP
```

```
-A INPUT -s 157.240.224.0/24 -j DROP
-A INPUT -s 157.240.225.0/24 -j DROP
-A INPUT -s 157.240.226.0/24 -j DROP
-A INPUT -s 157.240.227.0/24 -j DROP
-A INPUT -s 157.240.228.0/24 -j DROP
-A INPUT -s 157.240.229.0/24 -j DROP
-A INPUT -s 157.240.23.0/24 -j DROP
-A INPUT -s 157.240.231.0/24 -j DROP
-A INPUT -s 157.240.232.0/24 -j DROP
-A INPUT -s 157.240.233.0/24 -j DROP
-A INPUT -s 157.240.234.0/24 -j DROP
-A INPUT -s 157.240.235.0/24 -j DROP
-A INPUT -s 157.240.236.0/24 -j DROP
-A INPUT -s 157.240.237.0/24 -j DROP
-A INPUT -s 157.240.238.0/24 -j DROP
-A INPUT -s 157.240.239.0/24 -j DROP
-A INPUT -s 157.240.240.0/24 -j DROP
-A INPUT -s 157.240.24.0/24 -j DROP
-A INPUT -s 157.240.241.0/24 -j DROP
-A INPUT -s 157.240.242.0/24 -j DROP
-A INPUT -s 157.240.243.0/24 -j DROP
-A INPUT -s 157.240.244.0/24 -j DROP
-A INPUT -s 157.240.245.0/24 -j DROP
-A INPUT -s 157.240.247.0/24 -j DROP
-A INPUT -s 157.240.249.0/24 -j DROP
-A INPUT -s 157.240.250.0/24 -j DROP
-A INPUT -s 157.240.25.0/24 -j DROP
-A INPUT -s 157.240.251.0/24 -j DROP
-A INPUT -s 157.240.252.0/24 -j DROP
-A INPUT -s 157.240.253.0/24 -j DROP
-A INPUT -s 157.240.254.0/24 -j DROP
-A INPUT -s 157.240.26.0/24 -j DROP
-A INPUT -s 157.240.27.0/24 -j DROP
-A INPUT -s 157.240.28.0/24 -j DROP
-A INPUT -s 157.240.29.0/24 -j DROP
-A INPUT -s 157.240.30.0/24 -j DROP
-A INPUT -s 157.240.3.0/24 -j DROP
-A INPUT -s 157.240.31.0/24 -j DROP
-A INPUT -s 157.240.5.0/24 -j DROP
-A INPUT -s 157.240.6.0/24 -j DROP
-A INPUT -s 157.240.7.0/24 -j DROP
-A INPUT -s 157.240.8.0/24 -j DROP
-A INPUT -s 157.240.9.0/24 -j DROP
-A INPUT -s 162.254.207.51/32 -j DROP
-A INPUT -s 162.255.119.207/32 -j DROP
-A INPUT -s 172.67.135.213/32 -j DROP
-A INPUT -s 173.252.64.0/18 -j DROP
-A INPUT -s 179.60.192.0/22 -j DROP
-A INPUT -s 185.199.108.153/32 -j DROP
-A INPUT -s 185.199.111.153/32 -j DROP
-A INPUT -s 185.60.216.0/22 -j DROP
```

```
-A INPUT -s 198.54.117.211/32 -j DROP
-A INPUT -s 204.15.20.0/22 -j DROP
-A INPUT -s 27.124.125.189/32 -j DROP
-A INPUT -s 31.13.24.0/21 -j DROP
-A INPUT -s 31.13.64.0/18 -j DROP
-A INPUT -s 34.117.168.233/32 -j DROP
-A INPUT -s 37.9.175.187/32 -j DROP
-A INPUT -s 45.130.41.7/32 -j DROP
-A INPUT -s 45.64.40.0/22 -j DROP
-A INPUT -s 45.91.92.164/32 -j DROP
-A INPUT -s 54.81.116.232/32 -j DROP
-A INPUT -s 61.9.242.43/32 -j DROP
-A INPUT -s 64.225.91.73/32 -j DROP
-A INPUT -s 66.220.144.0/20 -j DROP
-A INPUT -s 69.171.224.0/19 -j DROP
-A INPUT -s 74.119.76.0/22 -j DROP
-A INPUT -s 89.223.68.248/32 -j DROP

# Rejeter tout le reste :
-A FORWARD -i br2 -j REJECT --reject-with icmp-port-unreachable
-A FORWARD -o br2 -j REJECT --reject-with icmp-port-unreachable

COMMIT
```

Pour IPv6, dans `/etc/iptables-persistent/rules.v6` :

```
*nat

# Router le Web vers le serveur web :
-A PREROUTING -d 2a01:4f8:231:aa6::13 -p tcp -m tcp --syn -m multiport --
dports 80,443 -j DNAT --to-destination ::ffff:c0a8:a05

# Router le mail envoi/réception vers le serveur mail :
-A PREROUTING -d 2a01:4f8:231:aa6::13 -p tcp -m tcp --syn -m multiport --
dports 587,993,25 -j DNAT --to-destination ::ffff:c0a8:a07

# Tests
## Router les ports des applications vers le serveur web :
#-A PREROUTING -d 2a01:4f8:231:aa6::13 -p tcp -m tcp --syn -m multiport --
dports 1935,1936,3000,3001,9000,9001 -j DNAT --to-destination
::ffff:c0a8:a05
#
## Router le port 5868 pour Funkwhale vers le serveur audio :
#-A PREROUTING -d 2a01:4f8:231:aa6::13 -p tcp -m tcp --syn -m multiport --
dports 5868 -j DNAT --to-destination ::ffff:c0a8:a09

## Router le 8484 pour Zabbix vers le serveur monitoring (inactif, pas
d'IPv6 pour l'instant sur ce serveur) :
#-A PREROUTING -d 2a01:4f8:231:aa6::13 -p tcp -m tcp --syn -m multiport --
dports 8484 -j DNAT --to-destination ::ffff:c0a8:XYZ
```

```
# Masquerading sur tous les ports dans le sens sortant (VM -> Internet)
-A POSTROUTING -s ::ffff:c0a8:a00/64 ! -d ::ffff:c0a8:0a00/64 -p tcp -j
MASQUERADE --to-ports 1024-65535
-A POSTROUTING -s ::ffff:c0a8:a00/64 ! -d ::ffff:c0a8:0a00/64 -p udp -j
MASQUERADE --to-ports 1024-65535
-A POSTROUTING -s ::ffff:c0a8:a00/64 ! -d ::ffff:c0a8:0a00/64 -j MASQUERADE

COMMIT

*filter

# Accepter le trafic basique : ICMP, boucle locale et connexionx établies,
en entrée :
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT ! -i lo -d ::1/128 -j REJECT

# Accepter le SSH :
-A INPUT -p tcp -m tcp --syn -m conntrack --ctstate NEW --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --syn -m conntrack --ctstate NEW --dport 1984 -j
ACCEPT

# Accepter le tunnel SSH vers le serveur web-01 sur le port 52365 :
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 52365 -j ACCEPT

# Accepter les requêtes DNS (port 53) depuis les VM :
-A INPUT -i br2 -p udp -m udp -m multiport --dports 53 -j ACCEPT
-A INPUT -i br2 -p tcp -m tcp -m multiport --dports 53 -j ACCEPT

# Bloquer les requêtes rpcbind/portmap en entrée ***depuis l'extérieur*** :
-A INPUT -i br2 -p tcp -m multiport --dport 2049 -j ACCEPT
-A INPUT -i br2 -p tcp -m multiport --dport 111 -j ACCEPT
-A INPUT -p tcp -s ::1/128  --dport 111 -j ACCEPT
-A INPUT -p udp --dport 111 -j DROP
-A INPUT -p tcp --dport 111 -j DROP

# Accepter les requêtes Zabbix passives (port 10050) depuis les VM :
-A INPUT -i br2 -p tcp -m tcp -m multiport --dports 10050 -j ACCEPT

# On accepte l'ICMPv6 indispensable au fonctionnement d'IPv6 :
-A INPUT -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type echo-request -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type echo-reply -j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type router-advertisement -m hl --hl-eq 255 -j
ACCEPT
-A INPUT -p icmpv6 --icmpv6-type router-solicitation -m hl --hl-eq 255 -j
ACCEPT
-A INPUT -p icmpv6 --icmpv6-type neighbour-advertisement -m hl --hl-eq 255 -
j ACCEPT
-A INPUT -p icmpv6 --icmpv6-type neighbour-solicitation -m hl --hl-eq 255 -j
ACCEPT
```

```
# On refuse les trop nombreux ping :
-A INPUT  -p icmpv6 --icmpv6-type echo-request -m conntrack --ctstate NEW -m
limit --limit 1/s --limit-burst 1 -j ACCEPT
-A INPUT  -p icmpv6 --icmpv6-type echo-request -j DROP

# On refuse tout le reste en entrée :
-A INPUT -m conntrack --ctstate INVALID -j DROP
-A INPUT -j REJECT

# Accepter les connexions établies sur le LAN :
-A FORWARD -d ::ffff:c0a8:a00/64 -o br2 -m conntrack --ctstate
RELATED,ESTABLISHED -j ACCEPT

# Accepter le trafic sortant depuis le LAN :
-A FORWARD -s ::ffff:c0a8:a00/64 -i br2 -j ACCEPT

# Accepter le trafic interne entre les VM :
-A FORWARD -i br2 -o br2 -j ACCEPT

# Accepter les paquets redirigés vers des ports particuliers pour le Web
vers le serveur web :
-A FORWARD -d ::ffff:c0a8:a05 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 80,443 -j ACCEPT

# Accepter les paquets redirigés vers des ports particuliers pour le mail
vers le serveur mail :
-A FORWARD -d ::ffff:c0a8:a05 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 587,993,25 -j ACCEPT

# Tests
## Accepter les paquets redirigés vers des ports particuliers vers le
serveur web :
#-A FORWARD -d ::ffff:c0a8:a05 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 1935,1936,3000,3001,9000,9001 -j ACCEPT
#
## Accepter les paquets redirigés vers des ports particuliers pour funkwhale
service 5868 vers le serveur audio :
#-A FORWARD -d ::ffff:c0a8:a09 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 5868 -j ACCEPT

# Pas d'IPv6 pour le moment, inactif :
## Accepter les paquets redirigés vers des ports particuliers pour Zabbix
tcp 8484 vers le serveur monitoring :
#-A FORWARD -d ::ffff:c0a8:XYZ -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 8484 -j ACCEPT

# On bloque TOUT le trafic en provenance de Meta/Facebook/Instagram/Threads
:
-A INPUT -s 2620:0:1c00::/40 -j DROP
-A INPUT -s 2620:10d:c090::/44 -j DROP
```

```
-A INPUT -s 2a03:2880::/32 -j DROP
-A INPUT -s 2a03:2887:ff02::/47 -j DROP
-A INPUT -s 2a03:2887:ff19::/48 -j DROP
-A INPUT -s 2a03:2887:ff1b::/48 -j DROP
-A INPUT -s 2a03:2887:ff1c::/46 -j DROP
-A INPUT -s 2a03:2887:ff23::/48 -j DROP
-A INPUT -s 2a03:2887:ff25::/48 -j DROP
-A INPUT -s 2a03:2887:ff27::/48 -j DROP
-A INPUT -s 2a03:2887:ff28::/46 -j DROP
-A INPUT -s 2a03:2887:ff2f::/48 -j DROP
-A INPUT -s 2a03:2887:ff30::/48 -j DROP
-A INPUT -s 2a03:2887:ff35::/48 -j DROP
-A INPUT -s 2a03:2887:ff37::/48 -j DROP
-A INPUT -s 2a03:2887:ff38::/46 -j DROP
-A INPUT -s 2a03:2887:ff3f::/48 -j DROP
-A INPUT -s 2a03:2887:ff40::/48 -j DROP
-A INPUT -s 2a03:2887:ff43::/48 -j DROP
-A INPUT -s 2a03:2887:ff44::/47 -j DROP
-A INPUT -s 2a03:2887:ff48::/46 -j DROP
-A INPUT -s 2a03:2887:ff4d::/48 -j DROP
-A INPUT -s 2a03:2887:ff4e::/47 -j DROP
-A INPUT -s 2a03:2887:ff50::/47 -j DROP
-A INPUT -s 2a03:2887:ff52::/48 -j DROP
-A INPUT -s 2a03:2887:ff58::/47 -j DROP
-A INPUT -s 2c0f:ef78:3::/48 -j DROP
-A INPUT -s 2c0f:ef78:5::/48 -j DROP
-A INPUT -s 2c0f:ef78:6::/48 -j DROP
-A INPUT -s 2c0f:ef78:9::/48 -j DROP
-A INPUT -s 2c0f:ef78:d::/48 -j DROP
-A INPUT -s 2c0f:ef78:e::/47 -j DROP
-A INPUT -s 2c0f:ef78:11::/48 -j DROP
-A INPUT -s 2c0f:ef78:12::/48 -j DROP

# Rejeter tout le reste :
-A FORWARD -i br2 -j REJECT
-A FORWARD -o br2 -j REJECT

COMMIT
```

Paquets installés

Pour virtualiser, il a fallu installer en particulier libvirt-daemon, qemu et zfsutils-linux ainsi que bridge-utils pour créer nos réseaux internes virtuels. La liste des paquets :

```
# dpkg -l | grep '^i' |awk '{ print $2 }' | sed '/^$/d'| sort
acl
acpid
adduser
adwaita-icon-theme
amd64-microcode
```

```
apt
aptitude
aptitude-common
apt-utils
at
at-spi2-common
base-files
base-passwd
bash
bash-completion
bind9-dnsutils
bind9-host
bind9-libs:amd64
binutils
binutils-common:amd64
binutils-x86-64-linux-gnu
bridge-utils
bsdextrautils
bsdutils
btrfs-progs
busybox
bzip2
ca-certificates
console-setup
console-setup-linux
coreutils
cpio
cpp
cpp-10
cpp-12
cron
cron-daemon-common
cryptsetup
cryptsetup-bin
cryptsetup-initramfs
curl
dash
dbus
dbus-bin
dbus-daemon
dbus-session-bus-common
dbus-system-bus-common
dbus-user-session
dconf-gsettings-backend:amd64
dconf-service
debconf
debconf-i18n
debian-archive-keyring
debianutils
diffutils
discover
```

```
discover-data
distro-info-data
dkms
dmeventd
dmidecode
dmsetup
dnsmasq
dnsmasq-base
dnsutils
dosfstools
dpkg
dpkg-dev
e2fsprogs
efibootmgr
ethtool
fail2ban
fdisk
file
findutils
firmware-bnx2x
fontconfig
fontconfig-config
fonts-dejavu-core
gcc
gcc-10
gcc-10-base:amd64
gcc-11-base:amd64
gcc-12
gcc-12-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
gtk-update-icon-cache
gzip
hicolor-icon-theme
hostname
htop
iftop
ifupdown
inetutils-telnet
init
initramfs-tools
initramfs-tools-core
```

```
init-system-helpers
intel-microcode
iotop
ipcalc-ng
iproute2
iptables
iptables-persistent
iputils-ping
ipxe-qemu
isc-dhcp-client
isc-dhcp-common
iso-codes
iucode-tool
kbd
keyboard-configuration
keyutils
klibc-utils
kmod
laptop-detect
less
libacl1:amd64
libaio1:amd64
libapparmor1:amd64
libapt-pkg6.0:amd64
libargon2-1:amd64
libasan6:amd64
libasan8:amd64
libasound2:amd64
libasound2-data
libasyncns0:amd64
libatk1.0-0:amd64
libatk-bridge2.0-0:amd64
libatomic1:amd64
libatspi2.0-0:amd64
libattr1:amd64
libaudit1:amd64
libaudit-common
libavahi-client3:amd64
libavahi-common3:amd64
libavahi-common-data:amd64
libbinutils:amd64
libblkid1:amd64
libboost-iostreams1.74.0:amd64
libbpf0:amd64
libbpf1:amd64
libbrlapi0.8:amd64
libbrotli1:amd64
libbsd0:amd64
libbz2-1.0:amd64
libc6:amd64
libc6-dev:amd64
```

```
libcacard0:amd64
libcairo2:amd64
libcairo-gobject2:amd64
libcap2:amd64
libcap2-bin
libcap-ng0:amd64
libcapstone4:amd64
libc-bin
libcbor0.8:amd64
libcc1-0:amd64
libc-dev-bin
libc-l10n
libcolord2:amd64
libcom-err2:amd64
libcrypt1:amd64
libcrypt-dev:amd64
libcryptsetup12:amd64
libctf0:amd64
libctf-nobfd0:amd64
libcups2:amd64
libcurl3-gnutls:amd64
libcurl4:amd64
libcwidget4:amd64
libdatrie1:amd64
libdaxctl1:amd64
libdb5.3:amd64
libdbus-1-3:amd64
libdconf1:amd64
libdebconfclient0:amd64
libdecor-0-0:amd64
libdeflate0:amd64
libdevmapper1.02.1:amd64
libdevmapper-event1.02.1:amd64
libdiscover2
libdns-export1110
libdpkg-perl
libdrm2:amd64
libdrm-amdgpu1:amd64
libdrm-common
libdrm-intel1:amd64
libdrm-nouveau2:amd64
libdrm-radeon1:amd64
libduktape207:amd64
libdw1:amd64
libedit2:amd64
libefiboot1:amd64
libefivar1:amd64
libelf1:amd64
libepoxy0:amd64
libestr0:amd64
libevent-core-2.1-7:amd64
```

```
libexecs0:amd64
libexpat1:amd64
libext2fs2:amd64
libfastjson4:amd64
libfdisk1:amd64
libfdt1:amd64
libffi7:amd64
libffi8:amd64
libfido2-1:amd64
libfile-find-rule-perl
libflac12:amd64
libfontconfig1:amd64
libfreetype6:amd64
libfribidi0:amd64
libfstrm0:amd64
libfuse2:amd64
libfuse3-3:amd64
libgbm1:amd64
libgcc-10-dev:amd64
libgcc-12-dev:amd64
libgcc-s1:amd64
libgcrypt20:amd64
libgdbm6:amd64
libgdbm-compat4:amd64
libgdk-pixbuf-2.0-0:amd64
libgdk-pixbuf2.0-common
libgl1:amd64
libgl1-mesa-dri:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libglvnd0:amd64
libglx0:amd64
libglx-mesa0:amd64
libgmp10:amd64
libgnutls30:amd64
libgomp1:amd64
libgpg-error0:amd64
libgpm2:amd64
libgprofng0:amd64
libgraphite2-3:amd64
libgssapi-krb5-2:amd64
libgstreamer1.0-0:amd64
libgstreamer-plugins-base1.0-0:amd64
libgtk-3-0:amd64
libgtk-3-common
libharfbuzz0b:amd64
libhogweed6:amd64
libibverbs1:amd64
libicu72:amd64
libidn2-0:amd64
libinih1:amd64
```

```
libip4tc2:amd64
libip6tc2:amd64
libisc-export1105:amd64
libisl23:amd64
libitm1:amd64
libjack-jackd2-0:amd64
libjansson4:amd64
libjbig0:amd64
libjemalloc2:amd64
libjpeg62-turbo:amd64
libjson-c5:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc:amd64
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
liblcms2-2:amd64
libldap-2.5-0:amd64
libldap-common
liblerc4:amd64
libllvm15:amd64
liblmdb0:amd64
liblocale-gettext-perl
liblockfile-bin
liblognorm5:amd64
liblsan0:amd64
liblvm2cmd2.03:amd64
liblz4-1:amd64
liblzma5:amd64
liblzo2-2:amd64
libmagic1:amd64
libmagic-mgc
libmaxminddb0:amd64
libmd0:amd64
libmnl0:amd64
libmount1:amd64
libmp3lame0:amd64
libmpc3:amd64
libmpfr6:amd64
libmpg123-0:amd64
libncurses6:amd64
libncursesw6:amd64
libndctl6:amd64
libnetfilter-conntrack3:amd64
libnettle8:amd64
libnewt0.52:amd64
libnfnetlink0:amd64
libnfsidmap1:amd64
libnftables1:amd64
libnftnl11:amd64
```

```
libnghttp2-14:amd64
libnl-3-200:amd64
libnl-genl-3-200:amd64
libnl-route-3-200:amd64
libnsl2:amd64
libnsl-dev:amd64
libnspr4:amd64
libnss3:amd64
libnss-systemd:amd64
libnuma1:amd64
libnumber-compare-perl
libnvpair3linux
libogg0:amd64
libopus0:amd64
liborc-0.4-0:amd64
libp11-kit0:amd64
libpam0g:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam-systemd:amd64
libpango-1.0-0:amd64
libpangocairo-1.0-0:amd64
libpangoft2-1.0-0:amd64
libparted2:amd64
libpcap0.8:amd64
libpci3:amd64
libpciaccess0:amd64
libpcre2-8-0:amd64
libpcre3:amd64
libpcsclite1:amd64
libperl5.36:amd64
libpipeline1:amd64
libpixman-1-0:amd64
libpmem1:amd64
libpng16-16:amd64
libpolkit-agent-1-0:amd64
libpolkit-gobject-1-0:amd64
libpopt0:amd64
libproc2-0:amd64
libprocps8:amd64
libprotobuf-c1:amd64
libpsl5:amd64
libpulse0:amd64
libpython3.11-minimal:amd64
libpython3.11-stdlib:amd64
libpython3-stdlib:amd64
libquadmath0:amd64
librdmacm1:amd64
libreadline8:amd64
librtmp1:amd64
```

```
libsamplerate0:amd64
libsasl2-2:amd64
libsasl2-modules:amd64
libsasl2-modules-db:amd64
libsdl2-2.0-0:amd64
libseccomp2:amd64
libselinux1:amd64
libsemanage2:amd64
libsemanage-common
libsensors5:amd64
libsensors-config
libsepol1:amd64
libsepol2:amd64
libsigc++-2.0-0v5:amd64
libslang2:amd64
libslirp0:amd64
libsmartcols1:amd64
libsndfile1:amd64
libsndio7.0:amd64
libsodium23:amd64
libspice-server1:amd64
libsqlite3-0:amd64
libss2:amd64
libssh2-1:amd64
libssh-4:amd64
libssl1.1:amd64
libssl3:amd64
libstdc++6:amd64
libsystemd0:amd64
libsystemd-shared:amd64
libtasn1-6:amd64
libtext-charwidth-perl:amd64
libtext-glob-perl
libtext-iconv-perl:amd64
libtext-wrapi18n-perl
libthai0:amd64
libthai-data
libtiff6:amd64
libtinfo6:amd64
libtirpc3:amd64
libtirpc-common
libtirpc-dev:amd64
libtsan0:amd64
libtsan2:amd64
libubsan1:amd64
libuchardet0:amd64
libudev1:amd64
libunistring2:amd64
libunwind8:amd64
liburcu8:amd64
liburing2:amd64
```

```
libusb-1.0-0:amd64
libusbredirparser1:amd64
libuuid1:amd64
libuutil3linux
libuv1:amd64
libva2:amd64
libva-drm2:amd64
libvdeplug2:amd64
libvirglrenderer1:amd64
libvirt0:amd64
libvirt-clients
libvirt-daemon
libvirt-daemon-config-network
libvirt-daemon-config-nwfilter
libvirt-daemon-driver-qemu
libvirt-daemon-system
libvirt-daemon-system-systemd
libvorbis0a:amd64
libvorbisenc2:amd64
libvte-2.91-0:amd64
libvte-2.91-common
libvulkan1:amd64
libwayland-client0:amd64
libwayland-cursor0:amd64
libwayland-egl1:amd64
libwayland-server0:amd64
libwebp7:amd64
libwrap0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libxapian30:amd64
libxau6:amd64
libxcb1:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-xfixes0:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxi6:amd64
libxinerama1:amd64
```

```
libxkbcommon0:amd64
libxml2:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxss1:amd64
libxtables12:amd64
libxxf86vm1:amd64
libxxhash0:amd64
libyajl2:amd64
libz3-4:amd64
libzfs4linux
libzpool5linux
libzstd1:amd64
linux-base
linux-compiler-gcc-10-x86
linux-compiler-gcc-12-x86
linux-headers-5.10.0-15-amd64
linux-headers-5.10.0-15-common
linux-headers-5.10.0-16-amd64
linux-headers-5.10.0-16-common
linux-headers-5.10.0-17-amd64
linux-headers-5.10.0-17-common
linux-headers-5.10.0-18-amd64
linux-headers-5.10.0-18-common
linux-headers-5.10.0-19-amd64
linux-headers-5.10.0-19-common
linux-headers-5.10.0-25-amd64
linux-headers-5.10.0-25-common
linux-headers-6.1.0-12-amd64
linux-headers-6.1.0-12-common
linux-headers-amd64
linux-image-5.10.0-25-amd64
linux-image-6.1.0-12-amd64
linux-image-amd64
linux-kbuild-5.10
linux-kbuild-6.1
linux-libc-dev:amd64
lm-sensors
locales
login
logrotate
logsave
lsb-base
lsb-release
lsof
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
netfilter-persistent
net-tools
nfs-common
nfs-kernel-server
nftables
openssh-client
openssh-server
openssh-sftp-server
openssl
passwd
patch
pci.ids
pciutils
perl
perl-base
perl-modules-5.36
pkexec
policykit-1
polkitd
procps
publicsuffix
python3
python3.11
python3.11-minimal
python3-apt
python3-certifi
python3-chardet
python3-charset-normalizer
python3-debian
python3-debianbts
python3-distutils
python3-httplib2
python3-idna
python3-lib2to3
python3-minimal
python3-pkg-resources
python3-pycurl
```

```
python3-pyparsing
python3-pysimplesoap
python3-reportbug
python3-requests
python3-six
python3-urllib3
python-apt-common
python-is-python3
qemu-system-common
qemu-system-data
qemu-system-gui
qemu-system-x86
qemu-utils
readline-common
reportbug
rpcbind
rpcsvc-proto
rsync
rsyslog
runit-helper
seabios
sed
sensible-utils
sgml-base
shared-mime-info
shim-helpers-amd64-signed
shim-signed:amd64
shim-signed-common
shim-unsigned
smartmontools
spl-dkms
sudo
sysstat
systemd
systemd-container
systemd-sysv
systemd-timesyncd
sysvinit-utils
tar
task-english
tasksel
tasksel-data
task-ssh-server
tcpdump
traceroute
tree
tzdata
ucf
udev
usrmerge
util-linux
```

```
util-linux-extra
util-linux-locales
vim
vim-common
vim-runtime
vim-tiny
wget
whiptail
x11-common
xfsprogs
xkb-data
xml-core
xxd
xz-utils
zabbix-agent2
zfs-dkms
zfsutils-linux
zlib1g:amd64
znapzend
zstd
```

Stockage ZFS

Un « pool » sur les 2 gros disques mécaniques a été créé en miroir (RAID1). Si vous vous demandez pourquoi nous n'avons pas créé de RAIDZ*, RAID5, RAID10, etc., vous pouvez jeter un coup d'oeil à ce très bon article.

Nous avons décidé d'offrir un maximum de 4 Go à l'ARC, le cache adaptatif de ZFS :

```
echo 4294967296 >> /sys/module/zfs/parameters/zfs_arc_max
```

```
root@hypervisor-01 ~ # cat /etc/modprobe.d/zfs.conf
options zfs zfs_arc_max=4294967296
```

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: zdata
 state: ONLINE
  scan: scrub repaired 0B in 05:42:22 with 0 errors on Sun Aug 14 06:06:23
2022
config:

    NAME                                    STATE     READ WRITE CKSUM
    zdata                                   ONLINE       0     0     0
      mirror-0                              ONLINE       0     0     0
        ata-ST4000NM0245-1Z2107_ZC17DQEF    ONLINE       0     0     0
```

```
        ata-ST4000NM0245-1Z2107_ZC17EN25  ONLINE       0     0     0

errors: No known data errors
```

```
# zfs list
NAME                    USED  AVAIL     REFER  MOUNTPOINT
zdata                  2.11T  1.40T      120K  /zdata
zdata/audio_data       57.9G  1.40T     45.4G  /zdata/audio_data
zdata/cloud_data        587G  1.40T      489G  /zdata/cloud_data
zdata/cryptpad_data     812M  1.40T      793M  /zdata/cryptpad_data
zdata/iso                96K  1.40T       96K  /zdata/iso
zdata/mail_data         736K  1.40T      480K  /zdata/mail_data
zdata/mobilizon_data    473M  1.40T      471M  /zdata/mobilizon_data
zdata/mysql_data        100M  1.40T      100M  /zdata/mysql_data
zdata/pleroma_data      127M  1.40T     80.2M  /zdata/pleroma_data
zdata/postgresql_data   465M  1.40T      465M  /zdata/postgresql_data
zdata/prod-01           562G  1.40T      333G  /zdata/prod-01
zdata/video_data        951G  1.40T      907G  /zdata/video_data
```

Nous n'avions plus qu'à ajouter ces partages dans les exports NFS pour que nos VM puissent y accéder :

```
# cat /etc/exports
/zdata/cloud_data
192.168.10.0/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
10.10.10.0/255.255.255.252(rw,async,no_subtree_check,no_root_squash)
/zdata/mail_data
192.168.10.0/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
10.10.10.0/255.255.255.252(rw,async,no_subtree_check,no_root_squash)
/zdata/video_data
192.168.10.0/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
10.10.10.0/255.255.255.252(rw,async,no_subtree_check,no_root_squash)
/zdata/audio_data
192.168.10.0/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
10.10.10.0/255.255.255.252(rw,async,no_subtree_check,no_root_squash)
/zdata/pleroma_data
192.168.10.0/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
10.10.10.0/255.255.255.252(rw,async,no_subtree_check,no_root_squash)
/zdata/cryptpad_data
192.168.10.0/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
10.10.10.0/255.255.255.252(rw,async,no_subtree_check,no_root_squash)
/zdata/mobilizon_data
192.168.10.0/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
10.10.10.0/255.255.255.252(rw,async,no_subtree_check,no_root_squash)
/zdata/mysql_data
192.168.10.0/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
10.10.10.0/255.255.255.252(rw,async,no_subtree_check,no_root_squash)
/zdata/postgresql_data
192.168.10.0/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
10.10.10.0/255.255.255.252(rw,async,no_subtree_check,no_root_squash)
```

Il ne restait plus qu'à créer nos VM tranquillement avec `virt-manager` sur notre réseau `br2` et sur le stockage `prod-01` pour héberger les disques durs de chaque système d'exploitation, en les démarrant depuis le stockage `iso` contenant nos images ISO pour installer Debian.

Sauvegardes

Toujours sauvegarder !

Concernant les bases de données MySQL et PostgreSQL, nous utilisons les outils natifs `mysqldump` et `pg_dump`, dont nous stockons les résultats sous forme compressée dans les partages ZFS respectifs (`zdata/mysql_data` et `zdata/postgresql_data`)

Nous utilisons ZFS pour snapshoter et répliquer toutes les données stockées sur 3 sites géographiques différents, dans des pays différents.

Nous utilisons ZnapZend pour les snapshots ZFS et leur réplication via SSH vers un deuxième serveur sous Debian chez Hetzner, dans leur datacenter de Helsinki en Finalande.

Sur la machine de production hypervisor-01 à Falkenstein en Allemagne, nous avons une rétention glissante de snapshots ZFS :

- horaire de 24 heures
- journalière d'une semaine

Sur le serveur de backup backup-01 à Helsinki, nous avons une réplication avec une rétention glissante de snapshots ZFS :

- horaire de 24 heures
- journalière d'une semaine
- hebdomadaire sur deux mois

Nous avons en sus mis en place une réplication des snapshots ZFS en France, dans le Tarn au domicile de l'administrateur, via SSH sur un autre pool ZFS en miroir.

Les donnés sont donc techniquement répliquées 5 fois (6 disques sur 3 sites géographiques différents).

Voici les commandes invoquées pour la mise en place des snapshots et de la réplication dans le sens production ⇒ backup avec ZnapZend :

```
wget https://github.com/Gregy/znapzend-debian/releases/download/0.21.1/znapzend_0.21.1-1_amd64.deb
mv znapzend_0.21.1-1_amd64.deb /tmp/
apt install /tmp/znapzend_0.21.1-1_amd64.deb
apt install mbuffer
```

```
for f in audio_data cloud_data cryptpad_data mail_data mobilizon_data mysql_data pleroma_data postgresql_data prod-01 video_data; do \
    znapzendzetup create --recursive --mbuffer=/usr/bin/mbuffer --mbuffersize=1G \
    --tsformat='%Y%m%d-%H%M%S' --send-delay=28800 \
```

```
    SRC '1d=>1h,7d=>1d' zdata/${f} \
    DST:a '1d=>1h,7d=>1d,2month=>1w' \
    root@backup-01:zdatabackup/${f}; done;

*** backup plan: zdata/audio_data ***
           dst_a = root@backup-01:zdatabackup/audio_data
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
    mbuffer_size = 1G
   post_znap_cmd = off
    pre_znap_cmd = off
       recursive = on
             src = zdata/audio_data
        src_plan = 1day=>1hour,7days=>1day
        tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800

Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
*** backup plan: zdata/cloud_data ***
           dst_a = root@backup-01:zdatabackup/cloud_data
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
    mbuffer_size = 1G
   post_znap_cmd = off
    pre_znap_cmd = off
       recursive = on
             src = zdata/cloud_data
        src_plan = 1day=>1hour,7days=>1day
        tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800

Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
*** backup plan: zdata/cryptpad_data ***
           dst_a = root@backup-01:zdatabackup/cryptpad_data
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
    mbuffer_size = 1G
   post_znap_cmd = off
    pre_znap_cmd = off
       recursive = on
             src = zdata/cryptpad_data
        src_plan = 1day=>1hour,7days=>1day
        tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800
```

```
Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
*** backup plan: zdata/mail_data ***
           dst_a = root@backup-01:zdatabackup/mail_data
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
     mbuffer_size = 1G
    post_znap_cmd = off
     pre_znap_cmd = off
        recursive = on
              src = zdata/mail_data
         src_plan = 1day=>1hour,7days=>1day
         tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800

Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
*** backup plan: zdata/mobilizon_data ***
           dst_a = root@backup-01:zdatabackup/mobilizon_data
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
     mbuffer_size = 1G
    post_znap_cmd = off
     pre_znap_cmd = off
        recursive = on
              src = zdata/mobilizon_data
         src_plan = 1day=>1hour,7days=>1day
         tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800

Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
*** backup plan: zdata/mysql_data ***
           dst_a = root@backup-01:zdatabackup/mysql_data
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
     mbuffer_size = 1G
    post_znap_cmd = off
     pre_znap_cmd = off
        recursive = on
              src = zdata/mysql_data
         src_plan = 1day=>1hour,7days=>1day
         tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800
```

```
Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
*** backup plan: zdata/pleroma_data ***
           dst_a = root@backup-01:zdatabackup/pleroma_data
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
     mbuffer_size = 1G
    post_znap_cmd = off
     pre_znap_cmd = off
        recursive = on
              src = zdata/pleroma_data
        src_plan = 1day=>1hour,7days=>1day
        tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800

Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
*** backup plan: zdata/postgresql_data ***
           dst_a = root@backup-01:zdatabackup/postgresql_data
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
     mbuffer_size = 1G
    post_znap_cmd = off
     pre_znap_cmd = off
        recursive = on
              src = zdata/postgresql_data
        src_plan = 1day=>1hour,7days=>1day
        tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800

Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
*** backup plan: zdata/prod-01 ***
           dst_a = root@backup-01:zdatabackup/prod-01
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
     mbuffer_size = 1G
    post_znap_cmd = off
     pre_znap_cmd = off
        recursive = on
              src = zdata/prod-01
        src_plan = 1day=>1hour,7days=>1day
        tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800
```

```
Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
*** backup plan: zdata/video_data ***
           dst_a = root@backup-01:zdatabackup/video_data
      dst_a_plan = 1day=>1hour,7days=>1day,2months=>1week
         enabled = on
         mbuffer = /usr/bin/mbuffer
     mbuffer_size = 1G
    post_znap_cmd = off
     pre_znap_cmd = off
        recursive = on
              src = zdata/video_data
        src_plan = 1day=>1hour,7days=>1day
        tsformat = %Y%m%d-%H%M%S
      zend_delay = 28800

Do you want to save this backup set [y/N]? y
NOTE: if you have modified your configuration, send a HUP signal
(pkill -HUP znapzend) to your znapzend daemon for it to notice the change.
```