

Table des matières

hypervisor-01	3
Machine	3
Topologie	3
Configuration	3
Système d'exploitation	3
Adressage IP	4
Paquets installés	5
Routage et filtrage avec iptables	23
Stockage ZFS	26
Sauvegardes	27

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
 - [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 une machine virtuelle, [proxy-01](#), protégée par un pare-feu et un système de bannissement. Elle a pour rôle de transférer les requêtes aux machines virtuelles ad-hoc et de protéger l'infrastructure.

Configuration

Système d'exploitation

Debian stable (Debian 10 « Buster » 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.

```
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 enp0s31f6
#iface enp0s31f6 inet static
#  address 159.69.59.13
#  netmask 255.255.255.192
#  gateway 159.69.59.1
#  # route 159.69.59.0/26 via 159.69.59.1
#  up route add -net 159.69.59.0 netmask 255.255.255.192 gw 159.69.59.1 dev
enp0s31f6

auto br0
iface br0 inet static
    bridge_ports enp0s31f6
    bridge_fd 5
    bridge_stp off
    bridge_maxwait 1
    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
    up route add -net 159.69.59.0 netmask 255.255.255.192 gw 159.69.59.1 dev
enp0s31f6

# Management
auto br1
iface br1 inet static
    bridge_ports none
    bridge_fd 5
    bridge_stp off
    address 10.X.X.X
    netmask 255.X.X.X

# VM-LAN
```

```
auto br2
iface br2 inet static
    bridge_ports none
    bridge_fd 5
    bridge_stp off
    address 192.168.10.1
    netmask 255.255.255.0
```

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 :

```
root@hypervisor-01 ~ # dpkg -l | grep '^i' | awk '{ print $2 }' | sed
'/^$/d'| sort
adduser
adwaita-icon-theme
amd64-microcode
apparmor
apt
apt-file
aptitude
aptitude-common
apt-utils
at-spi2-core
attr
augeas-lenses
base-files
base-passwd
bash
bash-completion
bind9-host
binutils
binutils-common:amd64
binutils-x86-64-linux-gnu
bolt
bridge-utils
bsdmainutils
bsdutils
btrfs-progs
build-essential
busybox
bzip2
ca-certificates
ceph-common
ceph-fuse
cifs-utils
console-setup
console-setup-linux
coreutils
```

```
corosync
cpio
cpp
cpp-8
cpufrequtils
cron
cryptsetup-bin
cryptsetup-run
curl
dash
dbus
dbus-user-session
dconf-gsettings-backend:amd64
dconf-service
debconf
debconf-i18n
debian-archive-keyring
debianutils
diffutils
dirmngr
discover
discover-data
distro-info-data
dkms
dmeventd
dmidecode
dmsetup
dnsmasq-base
dns-root-data
dosfstools
dpkg
dpkg-dev
e2fsprogs
ebtables
efibootmgr
eject
ethtool
exim4-base
exim4-config
exim4-daemon-light
exuberant-ctags
fail2ban
fakeroot
fdisk
file
findutils
firmware-bnx2x
firmware-linux-free
firmware-realtek
fontconfig
fontconfig-config
```

fonts-dejavu-core
fuse
fwupd
fwupd-amd64-signed
g++
g++-8
gcc
gcc-8
gcc-8-base:amd64
gdisk
genisoimage
geoip-database
gettext-base
gir1.2-freedesktop:amd64
gir1.2-glib-2.0:amd64
gir1.2-libosinfo-1.0:amd64
glib-networking:amd64
glib-networking-common
glib-networking-services
glusterfs-common
gnupg
gnupg-l10n
gnupg-utils
gpg
gpg-agent
gpgconf
gpgsm
gpgv
gpg-wks-client
gpg-wks-server
grep
groff-base
grub2-common
grub-common
grub-efi-amd64-bin
grub-pc
grub-pc-bin
gsettings-desktop-schemas
gststreamer1.0-libav:amd64
gststreamer1.0-plugins-base:amd64
gststreamer1.0-plugins-good:amd64
gststreamer1.0-plugins-ugly:amd64
gststreamer1.0-x:amd64
gtk-update-icon-cache
guile-2.2-libs:amd64
gzip
haveged
hdparm
hicolor-icon-theme
hostname
htop

i965-va-driver:amd64
ibverbs-providers:amd64
ifenslave
iftop
ifupdown
init
initramfs-tools
initramfs-tools-core
init-system-helpers
installation-report
intel-media-va-driver:amd64
intel-microcode
iotop
iperf
iproute2
ipset
iptables
iptables-persistent
iputils-clockdiff
iputils-ping
iputils-tracepath
ipxe-qemu
irqbalance
isc-dhcp-client
isc-dhcp-common
iso-codes
iucode-tool
javascript-common
kbd
keyboard-configuration
keyutils
klibc-utils
kmod
kpartx
krb5-locales
laptop-detect
less
liba52-0.7.4:amd64
libaal:amd64
libaacs0:amd64
libacl1:amd64
libacl1-dev:amd64
libaiol:amd64
libalgorithm-diff-perl
libalgorithm-diff-xs-perl
libalgorithm-merge-perl
libaom0:amd64
libapparmor1:amd64
libapt-inst2.0:amd64
libapt-pkg5.0:amd64
libapt-pkg-perl

libarchive13:amd64
libargon2-1:amd64
libasan5:amd64
libasound2:amd64
libasound2-data
libass9:amd64
libassuan0:amd64
libasyncns0:amd64
libatk1.0-0:amd64
libatk1.0-data
libatk-bridge2.0-0:amd64
libatomic1:amd64
libatspi2.0-0:amd64
libattr1:amd64
libattr1-dev:amd64
libaudit1:amd64
libaudit-common
libaugeas0:amd64
libauthen-sasl-perl
libavahi-client3:amd64
libavahi-common3:amd64
libavahi-common-data:amd64
libavc1394-0:amd64
libavcodec58:amd64
libavfilter7:amd64
libavformat58:amd64
libavutil56:amd64
libbabeltrace1:amd64
libbdplus0:amd64
libbind9-161:amd64
libbinutils:amd64
libblkid1:amd64
libbluetooth3:amd64
libbluray2:amd64
libboost-atomic1.67.0:amd64
libboost-iostreams1.67.0:amd64
libboost-program-options1.67.0:amd64
libboost-regex1.67.0:amd64
libboost-system1.67.0:amd64
libboost-thread1.67.0:amd64
libbrotli1:amd64
libbs2b0:amd64
libbsd0:amd64
libbytes-random-secure-perl
libbz2-1.0:amd64
libc6:amd64
libc6-dev:amd64
libcaca0:amd64
libcacard0:amd64
libcairo2:amd64
libcairo-gobject2:amd64

libcap2:amd64
libcap2-bin
libcap-ng0:amd64
libcapstone3:amd64
libc-bin
libcc1-0:amd64
libc-dev-bin
libcdio18:amd64
libcdparanoia0:amd64
libcephfs2:amd64
libcfg7:amd64
libchromaprint1:amd64
libc-l10n
libcm4:amd64
libcodec2-0.8.1:amd64
libcolord2:amd64
libcom-err2:amd64
libcommon-sense-perl
libconvert-asn1-perl
libcorosync-common4:amd64
libcp4:amd64
libcpufreq0
libcroco3:amd64
libcrypt-random-seed-perl
libcryptsetup12:amd64
libcrypt-ssleay-perl
libcrystalhd3:amd64
libcups2:amd64
libcurl3-gnutls:amd64
libcurl4:amd64
libcwidget3v5:amd64
libdata-dump-perl
libdat1:amd64
libdb5.3:amd64
libdb1:amd64
libdbus-1-3:amd64
libdconf1:amd64
libdebconfclient0:amd64
libdevmapper1.02.1:amd64
libdevmapper-event1.02.1:amd64
libdigest-hmac-perl
libdiscover2
libdns1104:amd64
libdns-export1104
libdpkg-perl
libdrm2:amd64
libdrm-amdgpu1:amd64
libdrm-common
libdrm-intel1:amd64
libdrm-nouveau2:amd64
libdrm-radeon1:amd64

libdv4:amd64
libdvdnv4:amd64
libdvread4:amd64
libdw1:amd64
libedit2:amd64
libefiboot1:amd64
libefivar1:amd64
libelf1:amd64
libelf-dev:amd64
libencode-locale-perl
libepoxy0:amd64
libestr0:amd64
libevent-2.1-6:amd64
libexpat1:amd64
libexporter-tiny-perl
libext2fs2:amd64
libfakeroot:amd64
libfastjson4:amd64
libfdisk1:amd64
libfdt1:amd64
libffi6:amd64
libfftw3-double3:amd64
libfile-fcntllock-perl
libfile-listing-perl
libflac8:amd64
libflite1:amd64
libfont-afm-perl
libfontconfig1:amd64
libfreetype6:amd64
libfribidi0:amd64
libfstrm0:amd64
libfuse2:amd64
libfwupd2:amd64
libgbm1:amd64
libgcl2:amd64
libgcab-1.0-0:amd64
libgcc1:amd64
libgcc-8-dev:amd64
libgcrypt20:amd64
libgdbm6:amd64
libgdbm-compat4:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-bin
libgdk-pixbuf2.0-common
libgeoip1:amd64
libgfapi0:amd64
libgfchangelog0:amd64
libgfdb0:amd64
libgfrpc0:amd64
libgfxdr0:amd64
libgirepository-1.0-1:amd64

```
libgl1:amd64
libgl1-mesa-dri:amd64
libglapi-mesa:amd64
libgl2.0-0:amd64
libglusterfs0:amd64
libglusterfs-dev
libglvnd0:amd64
libglx0:amd64
libglx-mesa0:amd64
libgme0:amd64
libgmp10:amd64
libgnutls30:amd64
libgnutls-dane0:amd64
libgomp1:amd64
libgoogle-perftools4:amd64
libgovirt2:amd64
libgovirt-common
libgpg-error0:amd64
libgpgme11:amd64
libgpm2:amd64
libgraphite2-3:amd64
libgsasl7
libgsm1:amd64
libgssapi-krb5-2:amd64
libgssapi-perl
libgstreamer1.0-0:amd64
libgstreamer-plugins-base1.0-0:amd64
libgtk-3-0:amd64
libgtk-3-bin
libgtk-3-common
libgtk-vnc-2.0-0:amd64
libgudev-1.0-0:amd64
libgusb2:amd64
libgvnc-1.0-0:amd64
libharfbuzz0b:amd64
libhavege1:amd64
libhogweed4:amd64
libhtml-format-perl
libhtml-form-perl
libhtml-parser-perl
libhtml-tagset-perl
libhtml-tree-perl
libhttp-cookies-perl
libhttp-daemon-perl
libhttp-date-perl
libhttp-message-perl
libhttp-negotiate-perl
libibverbs1:amd64
libice6:amd64
libicu63:amd64
libidn11:amd64
```

libidn2-0:amd64
libiec61883-0:amd64
libigdgmm5:amd64
libio-html-perl
libio-socket-ssl-perl
libip4tc0:amd64
libip6tc0:amd64
libipset11:amd64
libiptc0:amd64
libisc1100:amd64
libisccc161:amd64
libisccfg163:amd64
libisc-export1100:amd64
libisl19:amd64
libisns0:amd64
libitm1:amd64
libjack-jackd2-0:amd64
libjansson4:amd64
libjbig0:amd64
libjpeg62-turbo:amd64
libjson-c3:amd64
libjson-glib-1.0-0:amd64
libjson-glib-1.0-common
libjson-perl
libjson-xs-perl
libk5crypto3:amd64
libkeyutils1:amd64
libklibc:amd64
libkmod2:amd64
libknet1:amd64
libkrb5-3:amd64
libkrb5support0:amd64
libksba8:amd64
libkyotocabinet16v5:amd64
liblcms2-2:amd64
libldap-2.4-2:amd64
libldap-common
libldb1:amd64
liblilv-0-0:amd64
liblist-moreutils-perl
libllvm7:amd64
liblmb0:amd64
liblocale-gettext-perl
liblognorm5:amd64
liblsan0:amd64
libltdl7:amd64
liblvm2cmd2.03:amd64
liblwp-mediatypes-perl
liblwp-protocol-https-perl
liblwres161:amd64
liblz4-1:amd64

liblzma5:amd64
liblzo2-2:amd64
libmagic1:amd64
libmagic-mgc
libmailtools-perl
libmailutils5:amd64
libmariadb3:amd64
libmath-random-isaac-perl
libmath-random-isaac-xs-perl
libmnl0:amd64
libmount1:amd64
libmp3lame0:amd64
libmpc3:amd64
libmpdec2:amd64
libmpeg2-4:amd64
libmpfr6:amd64
libmpg123-0:amd64
libmpx2:amd64
libmysofa0:amd64
libncurses6:amd64
libncursesw6:amd64
libnetcf1
libnetfilter-conntrack3:amd64
libnet-http-perl
libnet-ldap-perl
libnet-libidn-perl
libnet-smtp-ssl-perl
libnet-ssleay-perl
libnettle6:amd64
libnewt0.52:amd64
libnfnetworklink0:amd64
libnfsidmap2:amd64
libnftnl11:amd64
libnghttp2-14:amd64
libnl-3-200:amd64
libnl-route-3-200:amd64
libnorm1:amd64
libnpth0:amd64
libnspr4:amd64
libnss3:amd64
libntlm0:amd64
libnuma1:amd64
libnvpair1linux
libogg0:amd64
libopencore-amrnb0:amd64
libopencore-amrwb0:amd64
libopenjp2-7:amd64
libopenmpt0:amd64
libopus0:amd64
liborc-0.4-0:amd64
libosinfo-1.0-0: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
libperl5.28:amd64
libpgm-5.2-0:amd64
libphodav-2.0-0:amd64
libphodav-2.0-common
libpipeline1:amd64
libpixman-1-0:amd64
libpng16-16:amd64
libpolkit-agent-1-0:amd64
libpolkit-backend-1-0:amd64
libpolkit-gobject-1-0:amd64
libpopt0:amd64
libpostproc55:amd64
libprocps7:amd64
libprotobuf-c1:amd64
libproxy1v5:amd64
libpsl5:amd64
libpulse0:amd64
libpulse-mainloop-glib0:amd64
libpython2.7:amd64
libpython2.7-minimal:amd64
libpython2.7-stdlib:amd64
libpython2-stdlib:amd64
libpython3.7:amd64
libpython3.7-minimal:amd64
libpython3.7-stdlib:amd64
libpython3-stdlib:amd64
libpython-stdlib:amd64
libqb0:amd64
libquadmath0:amd64
libquorum5:amd64
librados2:amd64
libradosstriper1:amd64
libraw1394-11:amd64
librbd1:amd64
librdmacm1:amd64

libreadline5:amd64
libreadline7:amd64
libregex-assemble-perl
librest-0.7-0:amd64
librrd8:amd64
librsvg2-2:amd64
librsvg2-common:amd64
librtmp1:amd64
librubberband2:amd64
libsamplerate0:amd64
libsasl2-2:amd64
libsasl2-modules-db:amd64
libseccomp2:amd64
libselinux1:amd64
libsemanage1:amd64
libsemanage-common
libsensors5:amd64
libsensors-config
libsepol1:amd64
libserd-0-0:amd64
libshine3:amd64
libshout3:amd64
libsidplaylv5:amd64
libsigc++-2.0-0v5:amd64
libslang2:amd64
libsm6:amd64
libsmartcols1:amd64
libsmbios-c2
libsnappy1v5:amd64
libsndfile1:amd64
libsodium23:amd64
libsord-0-0:amd64
libsoup2.4-1:amd64
libsoup-gnome2.4-1:amd64
libsoxr0:amd64
libspeex1:amd64
libspice-client-glib-2.0-8:amd64
libspice-client-gtk-3.0-5:amd64
libspice-server1:amd64
libsqlite3-0:amd64
libsratom-0-0:amd64
libss2:amd64
libssh2-1:amd64
libssh-gcrypt-4:amd64
libssl1.1:amd64
libstatgrab10
libstdc++6:amd64
libstdc++-8-dev:amd64
libswresample3:amd64
libswscale5:amd64
libsystemd0:amd64

libtaglv5:amd64
libtaglv5-vanilla:amd64
libtalloc2:amd64
libtasn1-6:amd64
libtcmalloc-minimal4:amd64
libtdb1:amd64
libterm-readline-gnu-perl
libtevent0:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapil8n-perl
libthai0:amd64
libthai-data
libtheora0:amd64
libtiff5:amd64
libtimedate-perl
libtinfo6:amd64
libtirpc3:amd64
libtirpc-common
libtry-tiny-perl
libtsan0:amd64
libtss2-esys0
libtss2-udev
libtwolame0:amd64
libtypes-serialiser-perl
libubsan1:amd64
libuchardet0:amd64
libudev1:amd64
libunbound8:amd64
libunistring2:amd64
libunwind8:amd64
liburcu6:amd64
liburi-perl
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libusbredirhost1:amd64
libusbredirparser1:amd64
libutempter0:amd64
libuuid1:amd64
libuutil1linux
libv4l-0:amd64
libv4lconvert0:amd64
libva2:amd64
libva-drm2:amd64
libva-x11-2:amd64
libvdeplug2
libvdpau1:amd64
libvdpau-va-gll:amd64
libvidstab1.1:amd64
libvirglrenderer0:amd64
libvirt0:amd64

```
libvirt-clients
libvirt-daemon
libvirt-daemon-system
libvirt-glib-1.0-0:amd64
libvisual-0.4-0:amd64
libvorbis0a:amd64
libvorbisenc2:amd64
libvorbisfile3:amd64
libvotequorum8:amd64
libvpx5:amd64
libvte-2.91-0:amd64
libvte-2.91-common
libwavpack1:amd64
libwayland-client0:amd64
libwayland-cursor0:amd64
libwayland-egl1:amd64
libwayland-server0:amd64
libwbclient0:amd64
libwebp6:amd64
libwebpmux3:amd64
libwrap0:amd64
libwww-perl
libwww-robotrules-perl
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx264-155:amd64
libx265-165:amd64
libxapian30:amd64
libxau6:amd64
libxcb1:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-present0:amd64
libxcb-render0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-xfixes0:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxencall1:amd64
libxendevicemodel1:amd64
libxenevtchn1:amd64
libxenforeignmemory1:amd64
libxengnttab1:amd64
libxenmisc4.11:amd64
libxenstore3.0:amd64
libxentoolcore1:amd64
```

```
libxentoollog1:amd64
libxext6:amd64
libxfixes3:amd64
libxi6:amd64
libxinerama1:amd64
libxkbcommon0:amd64
libxml2:amd64
libxml2-utils
libxmlb1:amd64
libxml-namespacesupport-perl
libxml-parser-perl
libxml-sax-base-perl
libxml-sax-expat-perl
libxml-sax-perl
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxslt1.1:amd64
libxtables12:amd64
libxtst6:amd64
libxv1:amd64
libxvidcore4:amd64
libxxf86vm1:amd64
libyajl2:amd64
libzfs2linux
libzmq5:amd64
libzpool2linux
libzstd1:amd64
libzvbi0:amd64
libzvbi-common
linux-base
linux-compiler-gcc-8-x86
linux-headers-4.19.0-13-amd64
linux-headers-4.19.0-13-common
linux-headers-4.19.0-14-amd64
linux-headers-4.19.0-14-common
linux-headers-amd64
linux-image-4.19.0-13-amd64
linux-image-4.19.0-14-amd64
linux-image-amd64
linux-kbuild-4.19
linux-libc-dev:amd64
locales
login
logrotate
lsb-base
lsb-release
lsof
lvm2
lxcfs
mailutils
```

```
mailutils-common
make
man-db
manpages
manpages-dev
mariadb-common
mawk
mdadm
mesa-va-drivers:amd64
mesa-va-drivers:amd64
mime-support
mount
mysql-common
nano
ncurses-base
ncurses-bin
ncurses-term
netbase
netcat-openbsd
netfilter-persistent
net-tools
nfs-common
nfs-kernel-server
ntpdate
open-iscsi
openssh-client
openssh-server
openssh-sftp-server
openssl
osinfo-db
ovmf
parted
passwd
patch
pciutils
perl
perl-base
perl-modules-5.28
perl-openssl-defaults:amd64
pinentry-curses
policykit-1
powermgmt-base
procps
psmisc
python
python2
python2.7
python2.7-minimal
python2-minimal
python3
python3.7
```

```
python3.7-minimal
python3-asn1crypto
python3-certifi
python3-cffi-backend
python3-chardet
python3-cryptography
python3-distutils
python3-gi
python3-idna
python3-jwt
python3-lib2to3
python3-libvirt
python3-libxml2:amd64
python3-minimal
python3-pkg-resources
python3-prettytable
python3-pyinotify
python3-requests
python3-six
python3-systemd
python3-urllib3
python-asn1crypto
python-cephfs
python-certifi
python-cffi-backend
python-chardet
python-crypto
python-cryptography
python-enum34
python-gpg
python-idna
python-ipaddress
python-ldb
python-minimal
python-openssl
python-pkg-resources
python-prettytable
python-rados
python-rbd
python-requests
python-samba
python-six
python-talloc:amd64
python-tdb
python-urllib3
qemu-kvm
qemu-system-common
qemu-system-data
qemu-system-gui
qemu-system-x86
qemu-utils
```

```
readline-common
rename
rpcbind
rrdcached
rsync
rsyslog
runit-helper
samba-common
samba-common-bin
samba-dsdb-modules:amd64
samba-libs:amd64
screen
seabios
sed
sensible-utils
sgml-base
shared-mime-info
smartmontools
spice-client-glib-usb-acl-helper
spl-dkms
sqlite3
ssl-cert
strace
sysstat
systemd
systemd-sysv
sysvinit-utils
tar
task-english
tasksel
tasksel-data
task-ssh-server
tcpdump
telnet
thin-provisioning-tools
tpm2-abrmd
tpm2-tools
tree
tzdata
ucf
udev
ufw
usb.ids
usbutils
util-linux
util-linux-locales
va-driver-all:amd64
vdpau-driver-all:amd64
vim
vim-common
vim-runtime
```

```
vim-tiny
virtinst
virt-viewer
wget
whiptail
whois
x11-common
xdg-user-dirs
xfsprogs
xkb-data
xml-core
xsltproc
xxd
xz-utils
zfs-dkms
zfsutils-linux
zfs-zed
zlib1g:amd64
zlib1g-dev:amd64
```

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 en 192.168.10.0/24 et filtrer les connexions entrantes, c'est le point le plus important.

L'idée est de rediriger les requêtes d'Internet vers les bonnes VM et de pouvoir administrer à distance de façon graphique avec virt-manager l'ensemble des VM. 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.

```
root@hypervisor-01 ~ # cat /etc/iptables/rules.v4
# Router le Web vers le proxy Nginx :
-A PREROUTING -d 159.69.59.13/32 -p tcp -m tcp --syn -m multiport --dports
80,443 -j DNAT --to-destination 192.168.10.2
# 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
# Router le 9000 vers le serveur peertube :
-A PREROUTING -d 159.69.59.13/32 -p tcp -m tcp --syn -m multiport --dports
9000 -j DNAT --to-destination 192.168.10.8
```

```
# Router le 4443 et les 10000-20000 tcp/udp vers le serveur jitsi :
-A PREROUTING -d 159.69.59.13/32 -p tcp -m tcp --syn -m multiport --dports
10000:20000 -j DNAT --to-destination 192.168.10.10
-A PREROUTING -d 159.69.59.13/32 -p udp -m udp -m multiport --dports
10000:20000 -j DNAT --to-destination 192.168.10.10
-A PREROUTING -d 159.69.59.13/32 -p tcp -m tcp --syn -m multiport --dports
4443 -j DNAT --to-destination 192.168.10.10
# 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

# 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 XXXX -j
ACCEPT
# Accepter Spice et VNC (console virtuelle de virt-manager) :
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5900 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5900 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5901 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5901 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5902 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5902 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5903 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5903 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5904 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5904 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5905 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5905 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5906 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5906 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5907 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5907 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5908 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5908 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5909 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5909 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5910 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5910 -j ACCEPT
-A INPUT -p tcp -m tcp -m conntrack --ctstate NEW --dport 5911 -j ACCEPT
-A INPUT -p udp -m udp -m conntrack --ctstate NEW --dport 5911 -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

# 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 proxy :
-A FORWARD -d 192.168.10.2/32 -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 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 peertube
service 9000 vers le serveur video :
-A FORWARD -d 192.168.10.8/32 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 9000 -j ACCEPT
# Accepter les paquets redirigés vers des ports particuliers pour funkwhale
service 5000 vers le serveur video :
-A FORWARD -d 192.168.10.9/32 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 5000 -j ACCEPT
# Accepter les paquets redirigés vers des ports particuliers pour jitsi meet
service tcp 10000-20000 vers le serveur visio :
-A FORWARD -d 192.168.10.10/32 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 10000:20000 -j ACCEPT
# Accepter les paquets redirigés vers des ports particuliers pour jitsi meet
service udp 10000-20000 vers le serveur visio :
-A FORWARD -d 192.168.10.10/32 -o br2 -p udp -m udp -m conntrack --
ctstate NEW -m multiport --dports 10000:20000 -j ACCEPT
# Accepter les paquets redirigés vers des ports particuliers pour jitsi meet
service tcp 4443 vers le serveur visio :
-A FORWARD -d 192.168.10.10/32 -o br2 -p tcp -m tcp --syn -m conntrack --
ctstate NEW -m multiport --dports 4443 -j ACCEPT

# 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
```

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 :

```
root@hypervisor-01 ~ # zpool status
pool: zdata
state: ONLINE
scan: scrub repaired 0B in 3h4m with 0 errors on Sun Feb 14 03:28:19 2021
config:
```

NAME	STATE	READ	WRITE	CKSUM
zdata	ONLINE	0	0	0
mirror-0	ONLINE	0	0	0
ata-ST4000NM0245-1Z2107_XXXXX	ONLINE	0	0	0
ata-ST4000NM0245-1Z2107_XXXXX	ONLINE	0	0	0

```
errors: No known data errors
```

```
root@hypervisor-01 ~ # zfs list
NAME                                USED  AVAIL  REFER  MOUNTPOINT
zdata                              895G  2.64T   112K   /zdata
zdata/audio_data                   21.8G  2.64T   19.6G   /zdata/audio_data
zdata/cloud_data                   72.4G  2.64T   71.3G   /zdata/cloud_data
zdata/iso                          3.65G  2.64T   3.65G   /zdata/iso
zdata/mail_data                    288K  2.64T    224K   /zdata/mail_data
zdata/prod-01                      144G  2.64T   76.3G   /zdata/prod-01
zdata/video_data                   653G  2.64T   651G   /zdata/video_data
```

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

```
root@hypervisor-01 ~ # cat /etc/exports
```

```
/zdata/cloud_data
192.168.10.X/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
/zdata/mail_data
192.168.10.X/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
/zdata/video_data
192.168.10.X/255.255.255.0(rw,async,no_subtree_check,no_root_squash)
/zdata/audio_data
192.168.10.X/255.255.255.0(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 ! Nous avons mis en place des snapshots ZFS que nous répliquons en France via SSH sur un autre pool ZFS en miroir. Les données sont donc techniquement répliquées 3 fois (4 disque sur deux sites géographiques différents). En utilisant les snapshots différentiels et incrémentiels, cela devient très rapide à faire.

Nous aimerions pouvoir chiffrer les données nativement, une fois que ZFS 2.0 aura atterri dans Debian stable. Pour le moment, seul Nextcloud permet de chiffrer le stockage nativement.

From:

<https://doc.liberta.vip/> - **Documentation Liberta**

Permanent link:

<https://doc.liberta.vip/tech/hypervisor-01?rev=1614860774>

Last update: **04/03/2021 13:26**

