Table des matières

web-01

Machine virtuelle

- Partie matérielle (virtuelle) KVM/QEMU
  - 8 cœurs virtuels
  - 16 Go de mémoire RAM
  - 1 disque virtuel de 50 Go
  - Accès au 1 Gbit/s
- Partie logicielle
  - Système d'exploitation : Debian stable
  - Technologies de virtualisation : KVM, QEMU, libvirt
  - Stockage des données : ZFS
  - 1 IPv4 : 159.69.59.13/32, via des NAT sur `hypervisor-01` vers les services exposés (web, mail, ports spéciaux, etc.)
  - 1 IPv6 : 2a01:4f8:231:aa6::5/64

Topologie

Cette VM héberge tous les frontaux et applications web de Liberta. Historiquement, des services imposants comme Peertube ou Funkwhale disposaient de leur propre VM dédiée mais à l'usage cela s'est avéré être un gaspillage de ressources.

Ce serveur héberge donc les services :

- Castopod
- CryptPad
- Etherpad-Lite
- Funkwhale
- Nextcloud
- Peertube
- WriteFreely

Configuration

Système d'exploitation

- Debian stable (Debian 12 « Bookworm »)

Adressage IP

La route vers 10.10.10.0/24 via l'hyperviseur permet l'accès (par VPN) au réseau d'administration des VM.

```
# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp1s0
iface enp1s0 inet static
    address 192.168.10.5/24
    gateway 192.168.10.1
    dns-nameservers 213.133.99.99 213.133.100.100 213.133.98.98
    dns-search liberta.vip
    up ip route add 10.10.10.0/24 via 192.168.10.1 dev enp1s0

iface enp1s0 inet6 static
    address 2a01:4f8:231:aa6::5
    netmask 120
    gateway 2a01:4f8:231:aa6::1
```

Paramètres réseau et swap dans sysctl

Dans `/etc/sysctl.d/99-sysctl.conf` nous avons passé la « swappiness » à 0. La mémoire doit être donc complètement saturée avant de commencer à « swapper » sur le disque dur (pratique d'ailleurs sujet à débats dont nous avons conscience). Nous avons également activé le paramètre d'overcommit à 1 pour éviter que Nextcloud ne se prenne les foudres du « Out of Memory Killer » de Linux:

```
# Cloud :
vm.overcommit_memory = 1
# swap à 0% de ram libre :
vm.swappiness=0
```

Routage et filtrage avec iptables

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

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 ! 

Cela dit, pour information une configuration similaire à la suivante est en place :

```
# /etc/ssh/sshd_config.d/liberta.conf

# Common parameters:
Port <un_port>
Port <un_autre_port>
AcceptEnv LANG LC_*
ChallengeResponseAuthentication no
KbdInteractiveAuthentication no
PrintMotd no
PasswordAuthentication no
Subsystem sftp /usr/lib/openssh/sftp-server
UsePAM yes
X11Forwarding no

# Port <un_port> configuration for IPv4/IPv6:
Match
Address="<adresse_ipv4_de_confiance>,127.0.0.0/8,<adresse_ipv6_de_confiance>
,fd00::/8" LocalPort=<un_port>
    AllowUsers root <utilisateurice_de_confiance>

# Port <un_autre_port> configuration for IPv4/IPv6:
Match LocalPort=<un_autre_port>
    AllowUsers <utilisateurice_de_confiance>
```

Pour IPv4, l'hyperviseur s'occupe déjà de tout router et rediriger, nous n'avons besoin d'aucune règle.

En revanche, nous disposons d'une IPv6 routable et exposée sur internet ! Nous devons donc avoir des règles de pare-feu actives. Dans `/etc/iptables-persistent/rules.v6` :

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-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 -d ::1/128 ! -i lo -m comment --comment "Accepter le trafic basique
: ICMP, boucle locale et connexions établies, en entrée" -j REJECT --reject-
with icmp6-port-unreachable
-A INPUT -s 2a01:4f8:231:aa6::/120 -p tcp -m tcp --dport 22 --tcp-flags
FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -m comment --comment
"Accepter le SSH depuis les autres VM" -j ACCEPT
-A INPUT -p tcp -m tcp --dport 1984 --tcp-flags FIN,SYN,RST,ACK SYN -m
conntrack --ctstate NEW -m comment --comment "Accepter le SSH" -j ACCEPT
-A INPUT -s 2a01:4f8:231:aa6::/120 -p udp -m udp -m multiport --dports 53 -m
comment --comment "Accepter les requêtes DNS (port 53) depuis les VM" -j
ACCEPT
```

```
-A INPUT -s 2a01:4f8:231:aa6::/120 -p udp -m udp -m multiport --dports 53 -m
comment --comment "Accepter les requêtes DNS (port 53) depuis les VM" -j
ACCEPT
-A INPUT -s 2a01:4f8:231:aa6::/120 -p tcp -m tcp -m multiport --dports 53 -m
comment --comment "Accepter les requêtes DNS (port 53) depuis les VM" -j
ACCEPT
-A INPUT -s 2a01:4f8:231:aa6::/120 -p tcp -m multiport --dports 2049 -m
comment --comment "Bloquer les requêtes rpcbind/portmap en entrée depuis
l\'extérieur" -j ACCEPT
-A INPUT -s 2a01:4f8:231:aa6::/120 -p tcp -m multiport --dports 111 -m
comment --comment "Bloquer les requêtes rpcbind/portmap en entrée depuis
l\'extérieur" -j ACCEPT
-A INPUT -s ::1/128 -p tcp -m tcp --dport 111 -m comment --comment "Bloquer
les requêtes rpcbind/portmap en entrée depuis l\'extérieur" -j ACCEPT
-A INPUT -s ::1/128 -p tcp -m tcp --dport 111 -m comment --comment "Bloquer
les requêtes rpcbind/portmap en entrée depuis l\'extérieur" -j DROP
-A INPUT -s 2a01:4f8:231:aa6::/120 -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 ipv6-icmp -m icmp6 --icmpv6-type 4 -m comment --comment "On
accepte l\'ICMPv6 indispensable au fonctionnement d\'IPv6" -j ACCEPT
-A INPUT -p ipv6-icmp -m icmp6 --icmpv6-type 128 -m comment --comment "On
accepte l\'ICMPv6 indispensable au fonctionnement d\'IPv6" -j ACCEPT
-A INPUT -p ipv6-icmp -m icmp6 --icmpv6-type 129 -m comment --comment "On
accepte l\'ICMPv6 indispensable au fonctionnement d\'IPv6" -j ACCEPT
-A INPUT -p ipv6-icmp -m icmp6 --icmpv6-type 134 -m hl --hl-eq 255 -m
comment --comment "On accepte l\'ICMPv6 indispensable au fonctionnement
d\'IPv6" -j ACCEPT
-A INPUT -p ipv6-icmp -m icmp6 --icmpv6-type 133 -m hl --hl-eq 255 -m
comment --comment "On accepte l\'ICMPv6 indispensable au fonctionnement
d\'IPv6" -j ACCEPT
-A INPUT -p ipv6-icmp -m icmp6 --icmpv6-type 136 -m hl --hl-eq 255 -m
comment --comment "On accepte l\'ICMPv6 indispensable au fonctionnement
d\'IPv6" -j ACCEPT
-A INPUT -p ipv6-icmp -m icmp6 --icmpv6-type 135 -m hl --hl-eq 255 -m
comment --comment "On accepte l\'ICMPv6 indispensable au fonctionnement
d\'IPv6" -j ACCEPT
-A INPUT -p ipv6-icmp -m icmp6 --icmpv6-type 128 -m conntrack --ctstate NEW
-m limit --limit 1/sec --limit-burst 1 -m comment --comment "On refuse les
trop nombreux ping" -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --
ctstate NEW -m multiport --dports 80,443 -m comment --comment "Accepter le
Web" -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --
ctstate NEW -m multiport --dports 1935 -m comment --comment "Accepter les
ports pour Peertube" -j ACCEPT
-A INPUT -p ipv6-icmp -m icmp6 --icmpv6-type 128 -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
```

```
--reject-with icmp6-port-unreachable
-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
COMMIT
```

Paquets installés

Nous utilisons certains dépôts tiers : Node.js, Yarn, PHP (afin d'utiliser les plus récentes, actuellement la version 8.4) et les paquets de PostgreSQL :

```
deb [arch=amd64 signed-by=/usr/share/keyrings/nodesource.gpg]
https://deb.nodesource.com/node_22.x nodistro main
```

```
deb http://apt.postgresql.org/pub/repos/apt bookworm-pgdg main
```

```
deb [signed-by=/usr/share/keyrings/yarn-archive-keyring.gpg]
https://dl.yarnpkg.com/debian/ stable main
```

```
deb [signed-by=/usr/share/keyrings/debsuryorg-archive-keyring.gpg]
https://packages.sury.org/php/ bookworm main
```

La liste des paquets :

```
# dpkg -l | grep '^i' |awk '{ print $2 }' | sed '/^$/d'| sort
acl
adduser
alsa-topology-conf
alsa-ucm-conf
apparmor
appstream
apt
apt-listchanges
apt-transport-https
apt-utils
```

```
aspell
aspell-fr
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
build-essential
busybox
bzip2
ca-certificates
certbot
cloud-guest-utils
composer
console-setup
console-setup-linux
coreutils
cpio
cpp
cpp-12
cron
cron-daemon-common
curl
dash
dbus
dbus-bin
dbus-daemon
dbus-session-bus-common
dbus-system-bus-common
dbus-user-session
debconf
debconf-i18n
debian-archive-keyring
debian-faq
debianutils
debsuryorg-archive-keyring
dictionaries-common
diffutils
dirmngr
discover
discover-data
distro-info-data
dmidecode
dmsetup
```

```
dnsutils
doc-debian
dpkg
dpkg-dev
e2fsprogs
eject
emacsen-common
ethtool
exiftags
exiftran
exuberant-ctags
fail2ban
fakeroot
fdisk
ffmpeg
file
findutils
firmware-linux-free
fontconfig
fontconfig-config
fonts-dejavu-core
fonts-droid-fallback
fonts-noto-mono
fonts-urw-base35
fuse
g++
g++-12
gcc
gcc-12
gcc-12-base:amd64
gdbm-l10n
gdisk
geoip-database
gettext
gettext-base
ghostscript
gifsicle
gir1.2-glib-2.0:amd64
gir1.2-packagekitglib-1.0
git
git-man
gnupg
gnupg-l10n
gnupg-utils
gnupg2
gpg
gpg-agent
gpg-wks-client
gpg-wks-server
gpgconf
gpgsm
```

```
gpgv
grep
groff-base
grub-common
grub-pc
grub-pc-bin
grub2-common
gsfonts
gzip
hdparm
hicolor-icon-theme
hostname
htop
i965-va-driver:amd64
icu-devtools
ifrench-gut
iftop
ifupdown
imagemagick
imagemagick-6-common
imagemagick-6.q16
inetutils-telnet
init
init-system-helpers
initramfs-tools
initramfs-tools-core
installation-report
intel-media-va-driver:amd64
iotop
iproute2
iptables
iptables-persistent
iputils-ping
isc-dhcp-client
isc-dhcp-common
iso-codes
ispell
javascript-common
jpegoptim
jq
jsonlint
kbd
keyboard-configuration
keyutils
klibc-utils
kmod
krb5-locales
laptop-detect
less
lib32gcc-s1
lib32stdc++6
```

```
libaacs0:amd64
libabsl20220623:amd64
libacl1:amd64
libalgorithm-diff-perl
libalgorithm-diff-xs-perl:amd64
libalgorithm-merge-perl
libaom3:amd64
libapparmor1:amd64
libappstream4:amd64
libapt-inst2.0:amd64
libapt-pkg5.0:amd64
libapt-pkg6.0:amd64
libarchive-zip-perl
libarchive13:amd64
libargon2-1:amd64
libasan8:amd64
libasound2-data
libasound2:amd64
libaspell15:amd64
libass9:amd64
libassuan0:amd64
libasyncns0:amd64
libatomic1:amd64
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libavc1394-0:amd64
libavcodec59:amd64
libavdevice59:amd64
libavfilter8:amd64
libavformat59:amd64
libavif15:amd64
libavutil57:amd64
libbdplus0:amd64
libbinutils:amd64
libblas3:amd64
libblkid1:amd64
libbluray2:amd64
libbpf1:amd64
libbrotli1:amd64
libbs2b0:amd64
libbsd0:amd64
libbz2-1.0:amd64
libc-bin
libc-dev-bin
libc-devtools
libc-l10n
libc6-dev:amd64
```

```
libc6-i386
libc6:amd64
libcaca0:amd64
libcairo-gobject2:amd64
libcairo2:amd64
libcap-ng0:amd64
libcap2-bin
libcap2:amd64
libcbor0.8:amd64
libcc1-0:amd64
libcdio-cdda2:amd64
libcdio-paranoia2:amd64
libcdio19:amd64
libchromaprint1:amd64
libcjson1:amd64
libclang-14-dev
libclang-common-14-dev
libclang-dev
libclang-rt-14-dev:amd64
libclang1-14
libcodec2-1.0:amd64
libcom-err2:amd64
libconfig-inifiles-perl
libcrypt-dev:amd64
libcrypt1:amd64
libcryptsetup12:amd64
libctf-nobfd0:amd64
libctf0:amd64
libcups2:amd64
libcurl3-gnutls:amd64
libcurl4:amd64
libdatrie1:amd64
libdav1d6:amd64
libdb5.3:amd64
libdbd-mariadb-perl
libdbi-perl:amd64
libdbus-1-3:amd64
libdc1394-25:amd64
libde265-0:amd64
libdebconfclient0:amd64
libdecor-0-0:amd64
libdecor-0-plugin-1-cairo:amd64
libdeflate0:amd64
libdevmapper1.02.1:amd64
libdiscover2
libdjvulibre-text
libdjvulibre21:amd64
libdns-export1104
libdpkg-perl
libdrm-amdgpu1:amd64
libdrm-common
```

```
libdrm-intel1:amd64
libdrm-nouveau2:amd64
libdrm-radeon1:amd64
libdrm2:amd64
libduktape207:amd64
libdw1:amd64
libedit2:amd64
libefiboot1:amd64
libefivar1:amd64
libelf1:amd64
libepoxy0:amd64
liberror-perl
libestr0:amd64
libevent-core-2.1-7:amd64
libexif12:amd64
libexpat1-dev:amd64
libexpat1:amd64
libext2fs2:amd64
libfakeroot:amd64
libfastjson4:amd64
libfdisk1:amd64
libffi-dev:amd64
libffi6:amd64
libffi7:amd64
libffi8:amd64
libfftw3-double3:amd64
libfido2-1:amd64
libfile-fcntllock-perl
libfile-find-rule-perl
libflac12:amd64
libflite1:amd64
libfontconfig1:amd64
libfontenc1:amd64
libfreetype6:amd64
libfribidi0:amd64
libfstrm0:amd64
libfuse2:amd64
libgav1-1:amd64
libgbm1:amd64
libgc1:amd64
libgcc-12-dev:amd64
libgcc-s1:amd64
libgcrypt20:amd64
libgd3:amd64
libgdbm-compat4:amd64
libgdbm6:amd64
libgdk-pixbuf-2.0-0:amd64
libgdk-pixbuf2.0-bin
libgdk-pixbuf2.0-common
libgeoip1:amd64
libgfortran5:amd64
```

```
libgirepository-1.0-1:amd64
libgl1-mesa-dri:amd64
libgl1:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libglib2.0-bin
libglib2.0-data
libglvnd0:amd64
libglx-mesa0:amd64
libglx0:amd64
libgme0:amd64
libgmp10:amd64
libgnutls30:amd64
libgomp1:amd64
libgpg-error0:amd64
libgpgme11:amd64
libgpm2:amd64
libgprofng0:amd64
libgraphite2-3:amd64
libgs-common
libgs10-common
libgs10:amd64
libgsm1:amd64
libgssapi-krb5-2:amd64
libgstreamer1.0-0:amd64
libharfbuzz0b:amd64
libheif1:amd64
libhogweed4:amd64
libhogweed6:amd64
libhwy1:amd64
libice6:amd64
libicu-dev:amd64
libicu72:amd64
libidn11:amd64
libidn12:amd64
libidn2-0:amd64
libiec61883-0:amd64
libigdgmm12:amd64
libijs-0.35:amd64
libimage-exiftool-perl
libimagequant0:amd64
libimath-3-1-29:amd64
libip4tc0:amd64
libip4tc2:amd64
libip6tc0:amd64
libip6tc2:amd64
libiptc0:amd64
libisc-export1100:amd64
libisl23:amd64
libitm1:amd64
libjack-jackd2-0:amd64
```

```
libjansson4:amd64
libjbig0:amd64
libjbig2dec0:amd64
libjemalloc2:amd64
libjpeg-dev:amd64
libjpeg62-turbo-dev:amd64
libjpeg62-turbo:amd64
libjq1:amd64
libjs-jquery
libjs-sphinxdoc
libjs-underscore
libjson-c3:amd64
libjson-c5:amd64
libjxl0.7:amd64
libjxr-tools
libjxr0:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc:amd64
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
libksba8:amd64
liblapack3:amd64
liblcms2-2:amd64
libldap-2.5-0:amd64
libldap-common
libldap-dev:amd64
libldap2-dev
libldb2:amd64
liblerc4:amd64
liblilv-0-0:amd64
liblinear4:amd64
libllvm14:amd64
libllvm15:amd64
liblmdb0:amd64
liblocale-gettext-perl
liblockfile-bin
liblognorm5:amd64
liblqr-1-0:amd64
liblsan0:amd64
libltdl7:amd64
liblua5.3-0:amd64
liblz4-1:amd64
liblzma5:amd64
libmagic-dev:amd64
libmagic-mgc
libmagic1:amd64
libmagickcore-6.q16-6-extra:amd64
libmagickcore-6.q16-6:amd64
libmagickwand-6.q16-6:amd64
```

```
libmariadb3:amd64
libmaxminddb0:amd64
libmbedcrypto7:amd64
libmd0:amd64
libmfx1:amd64
libmime-charset-perl
libmnl0:amd64
libmount1:amd64
libmp3lame0:amd64
libmpc3:amd64
libmpfr6:amd64
libmpg123-0:amd64
libmysofa1:amd64
libncurses5:amd64
libncurses6:amd64
libncursesw6:amd64
libnetfilter-conntrack3:amd64
libnetpbm11:amd64
libnettle6:amd64
libnettle8:amd64
libnewt0.52:amd64
libnfnetlink0:amd64
libnfsidmap1:amd64
libnftnl11:amd64
libnghttp2-14:amd64
libnginx-mod-http-auth-pam
libnginx-mod-http-dav-ext
libnginx-mod-http-echo
libnginx-mod-http-geoip
libnginx-mod-http-image-filter
libnginx-mod-http-subs-filter
libnginx-mod-http-upstream-fair
libnginx-mod-http-xslt-filter
libnginx-mod-stream
libnginx-mod-stream-geoip
libnl-3-200:amd64
libnl-genl-3-200:amd64
libnorm1:amd64
libnpth0:amd64
libnsl-dev:amd64
libnsl2:amd64
libnss-nis:amd64
libnss-nisplus:amd64
libnss-systemd:amd64
libnuma1:amd64
libnumber-compare-perl
libobjc-12-dev:amd64
libobjc4:amd64
libogg0:amd64
libonig5:amd64
libopenal-data
```

```
libopenal1:amd64
libopenexr-3-1-30:amd64
libopenjp2-7:amd64
libopenmpt0:amd64
libopus0:amd64
libp11-kit0:amd64
libpackagekit-glib2-18:amd64
libpam-modules-bin
libpam-modules:amd64
libpam-runtime
libpam-systemd:amd64
libpam0g:amd64
libpango-1.0-0:amd64
libpangocairo-1.0-0:amd64
libpangoft2-1.0-0:amd64
libpaper-utils
libpaper1:amd64
libpcap0.8:amd64
libpci3:amd64
libpciaccess0:amd64
libpcre2-8-0:amd64
libpcre3:amd64
libperl5.36:amd64
libpgm-5.3-0:amd64
libpipeline1:amd64
libpixman-1-0:amd64
libpkgconf3:amd64
libplacebo208:amd64
libpng16-16:amd64
libpocketsphinx3:amd64
libpolkit-agent-1-0:amd64
libpolkit-gobject-1-0:amd64
libpopt0:amd64
libposix-strptime-perl
libpostproc56:amd64
libpq-dev
libpq5:amd64
libproc2-0:amd64
libprocps7:amd64
libprotobuf-c1:amd64
libpsl5:amd64
libpulse0:amd64
libpython2.7-minimal:amd64
libpython2.7-stdlib:amd64
libpython3-dev:amd64
libpython3-stdlib:amd64
libpython3.11-dev:amd64
libpython3.11-minimal:amd64
libpython3.11-stdlib:amd64
libpython3.11:amd64
libquadmath0:amd64
```

```
librabbitmq4:amd64
librav1e0:amd64
libraw1394-11:amd64
libreadline8:amd64
librist4:amd64
librsvg2-2:amd64
librsvg2-common:amd64
librtmp1:amd64
librubberband2:amd64
libsamplerate0:amd64
libsasl2-2:amd64
libsasl2-dev
libsasl2-modules-db:amd64
libsasl2-modules:amd64
libsdl2-2.0-0:amd64
libseccomp2:amd64
libselinux1:amd64
libsemanage-common
libsemanage2:amd64
libsensors-config
libsensors5:amd64
libsepol1:amd64
libsepol2:amd64
libserd-0-0:amd64
libshine3:amd64
libslang2:amd64
libsm6:amd64
libsmartcols1:amd64
libsmbclient:amd64
libsnappy1v5:amd64
libsndfile1:amd64
libsndio7.0:amd64
libsodium23:amd64
libsombok3:amd64
libsord-0-0:amd64
libsoxr0:amd64
libspeex1:amd64
libsphinxbase3:amd64
libsqlite3-0:amd64
libsratom-0-0:amd64
libsrt1.5-gnutls:amd64
libss2:amd64
libssh-gcrypt-4:amd64
libssh2-1:amd64
libssl-dev:amd64
libssl1.1:amd64
libssl3:amd64
libstdc++-12-dev:amd64
libstdc++6:amd64
libstemmer0d:amd64
libsvtav1enc1:amd64
```

```
libswresample4:amd64
libswscale6:amd64
libsystemd-shared:amd64
libsystemd0:amd64
libtalloc2:amd64
libtasn1-6:amd64
libtdb1:amd64
libterm-readkey-perl
libtevent0:amd64
libtext-charwidth-perl:amd64
libtext-glob-perl
libtext-iconv-perl:amd64
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtheora0:amd64
libtiff6:amd64
libtinfo5:amd64
libtinfo6:amd64
libtirpc-common
libtirpc-dev:amd64
libtirpc3:amd64
libtsan2:amd64
libtwolame0:amd64
libubsan1:amd64
libuchardet0:amd64
libudev1:amd64
libudfread0:amd64
libunicode-linebreak-perl
libunistring2:amd64
libunwind8:amd64
liburing2:amd64
libusb-1.0-0:amd64
libutempter0:amd64
libuuid1:amd64
libuv1:amd64
libva-drm2:amd64
libva-x11-2:amd64
libva2:amd64
libvdpau-va-gl1:amd64
libvdpau1:amd64
libvidstab1.1:amd64
libvorbis0a:amd64
libvorbisenc2:amd64
libvorbisfile3:amd64
libvpx7:amd64
libvulkan1:amd64
libwayland-client0:amd64
libwayland-cursor0:amd64
libwayland-egl1:amd64
libwayland-server0:amd64
```

```
libwbclient0:amd64
libwebp7:amd64
libwebpdemux2:amd64
libwebpmux3:amd64
libwmflite-0.2-7:amd64
libwrap0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx264-164:amd64
libx265-199:amd64
libxau6:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-xfixes0:amd64
libxcb1:amd64
libxcursor1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxi6:amd64
libxkbcommon0:amd64
libxml2-dev:amd64
libxml2:amd64
libxmlb2:amd64
libxmlrpc-epi0:amd64
libxmuu1:amd64
libxpm4:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxslt1-dev:amd64
libxslt1.1:amd64
libxss1:amd64
libxt6:amd64
libxtables12:amd64
libxv1:amd64
libxvidcore4:amd64
libxxf86vm1:amd64
libxxhash0:amd64
libyaml-0-2:amd64
libyuv0:amd64
libz3-4:amd64
libzimg2:amd64
```

```
libzip4:amd64
libzmq5:amd64
libzstd1:amd64
libzvbi-common
libzvbi0:amd64
linux-base
linux-image-6.1.0-37-amd64
linux-image-6.1.0-39-amd64
linux-image-amd64
linux-libc-dev:amd64
locales
locate
login
logrotate
logsave
lsb-base
lsb-release
lsof
lua-lpeg:amd64
mailcap
make
man-db
manpages
manpages-dev
manpages-fr
mariadb-client
mariadb-client-core
mariadb-common
mawk
media-types
mesa-va-drivers:amd64
mesa-vdpau-drivers:amd64
mesa-vulkan-drivers:amd64
mime-support
mount
mysql-common
nano
ncal
ncdu
ncurses-base
ncurses-bin
ncurses-term
net-tools
netbase
netcat-traditional
netfilter-persistent
netpbm
nfs-common
nfs-kernel-server
nginx
nginx-common
```

```
nmap
nmap-common
nodejs
ocl-icd-libopencl1:amd64
openssh-client
openssh-server
openssh-sftp-server
openssl
optipng
os-prober
packagekit
packagekit-tools
passwd
patch
pci.ids
pciutils
perl
perl-base
perl-modules-5.28
perl-modules-5.36
php-common
php-composer-ca-bundle
php-composer-class-map-generator
php-composer-metadata-minifier
php-composer-pcre
php-composer-semver
php-composer-spdx-licenses
php-composer-xdebug-handler
php-json-schema
php-psr-container
php-psr-log
php-react-promise
php-seld-signal-handler
php-symfony-console
php-symfony-deprecation-contracts
php-symfony-filesystem
php-symfony-finder
php-symfony-process
php-symfony-service-contracts
php-symfony-string
php8.4-apcu
php8.4-apcu-dbgsym
php8.4-bcmath
php8.4-bz2
php8.4-cli
php8.4-common
php8.4-curl
php8.4-fpm
php8.4-gd
php8.4-gmp
php8.4-igbinary
```

```
php8.4-imagick
php8.4-intl
php8.4-mbstring
php8.4-mysql
php8.4-opcache
php8.4-pgsql
php8.4-phpdbg
php8.4-readline
php8.4-redis
php8.4-xml
php8.4-xmlrpc
php8.4-zip
pinentry-curses
pkexec
pkg-config:amd64
pkgconf-bin
pkgconf:amd64
pngquant
pocketsphinx-en-us
policykit-1
polkitd
polkitd-pkla
poppler-data
powermgmt-base
procps
psmisc
publicsuffix
python-apt-common
python-certbot-nginx
python-is-python3
python2.7
python2.7-minimal
python3
python3-acme
python3-apt
python3-blinker
python3-brotli
python3-certbot
python3-certbot-dns-gandi
python3-certbot-nginx
python3-certifi
python3-cffi-backend:amd64
python3-chardet
python3-charset-normalizer
python3-click
python3-colorama
python3-configargparse
python3-configobj
python3-cryptography
python3-dbus
python3-debconf
```

```
python3-debian
python3-debianbts
python3-dev
python3-distro
python3-distutils
python3-gi
python3-gpg
python3-httplib2
python3-icu
python3-idna
python3-josepy
python3-jwt
python3-lazr.restfulclient
python3-lazr.uri
python3-ldb
python3-lib2to3
python3-minimal
python3-mutagen
python3-oauthlib
python3-openssl
python3-parsedatetime
python3-pip
python3-pip-whl
python3-pkg-resources
python3-pycryptodome
python3-pycurl
python3-pyinotify
python3-pyparsing
python3-pysimplesoap
python3-pyxattr:amd64
python3-reportbug
python3-requests
python3-rfc3339
python3-samba
python3-setuptools
python3-setuptools-whl
python3-six
python3-software-properties
python3-systemd
python3-talloc:amd64
python3-tdb
python3-tz
python3-urllib3
python3-venv
python3-wadllib
python3-websockets
python3-wheel
python3-yaml
python3.11
python3.11-dev
python3.11-minimal
```

```
python3.11-venv
qemu-guest-agent
readline-common
reportbug
rpcbind
rpcsvc-proto
rsync
rsyslog
rtmpdump
runit-helper
samba-common
samba-common-bin
samba-dsdb-modules:amd64
samba-libs:amd64
screen
sed
sensible-utils
sgml-base
shared-mime-info
smbclient
socat
software-properties-common
ssl-cert
sudo
sysstat
systemd
systemd-sysv
systemd-timesyncd
sysvinit-utils
tar
task-french
task-ssh-server
tasksel
tasksel-data
tcpdump
traceroute
tree
tzdata
ucf
udev
unzip
usbutils
usrmerge
util-linux
util-linux-extra
util-linux-locales
va-driver-all:amd64
vdpau-driver-all:amd64
vim
vim-common
vim-runtime
```

```
vim-tiny
wamerican
wfrench
wget
whiptail
whois
wkhtmltox
x11-common
xauth
xdg-user-dirs
xfonts-75dpi
xfonts-base
xfonts-encodings
xfonts-utils
xkb-data
xml-core
xxd
xz-utils
yarn
yt-dlp
zabbix-agent2
zip
zlib1g-dev:amd64
zlib1g:amd64
zstd
```

Stockage

Nous montons les partages ZFS de notre hyperviseur en NFS pour chaque application :

Dans `/etc/fstab` :

```
# cloud_data ZFS NFS share:
192.168.10.1:/zdata/cloud_data      /cloud_data                    nfs  auto
0 0
# cryptpad_data ZFS NFS share:
192.168.10.1:/zdata/cryptpad_data   /home/cryptpad/cryptpad_data   nfs  auto
0 0
# castpod_data ZFS NFS share:
192.168.10.1:/zdata/castopod_data   /var/www/castopod/public/media nfs  auto
0 0
# video_data ZFS NFS share:
192.168.10.1:/zdata/video_data      /var/www/peertube/storage      nfs  auto
0 0
# audio_data ZFS NFS share:
192.168.10.1:/zdata/audio_data      /var/www/funkwhale/data        nfs  auto
0 0
```

Partie logicielle

Toutes les applications web des services sont servies par le serveur / reverse-proxy Nginx dont voici les configurations pour chaque application ainsi que les configurations communes.

Nous avons décidé de bannir dans la configuration générale un certain nombre de pays nous noyant de spam et d'attaques en tout genre :

```
# cat /etc/nginx/nginx.conf
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
    worker_connections 1024;
    multi_accept on;
    use epoll;
}

http {
    server_names_hash_bucket_size 64;

    # Liberta : no more reverse proxy:
    #set_real_ip_from 127.0.0.1;
    #set_real_ip_from 192.168.10.0/24;
    #real_ip_header X-Forwarded-For;
    #real_ip_recursive on;

    include /etc/nginx/mime.types;
    default_type application/octet-stream;
    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log warn;
    sendfile on;
    send_timeout 3600;
    tcp_nopush on;
    tcp_nodelay on;
    open_file_cache max=500 inactive=10m;
    open_file_cache_errors on;
    keepalive_timeout 65;
    reset_timedout_connection on;
    server_tokens off;
    resolver_timeout 5s;
    proxy_buffers 16 16k;
    proxy_buffer_size 16k;
    fastcgi_buffers 64 4K;
    client_max_body_size 8G;

    ##
    # Logging Settings
```

```
    ##

    rewrite_log on;
    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log notice;

    # Liberta : ban all countries except those:
    geoip_country /usr/share/GeoIP/GeoIP.dat;
    map $geoip_country_code $allowed_country {
            default no;
            AL yes;
            AD yes;
            AM yes;
            AT yes;
            BA yes;
            BE yes;
            BG yes;
            BY yes;
            CH yes;
            CY yes;
            CZ yes;
            DK yes;
            EE yes;
            FI yes;
            FR yes;
            FO yes;
            DE yes;
            GB yes;
            GE yes;
            GI yes;
            GR yes;
            HR yes;
            HU yes;
            IE yes;
            IM yes;
            IS yes;
            IT yes;
            LI yes;
            LV yes;
            LT yes;
            LU yes;
            MC yes;
            MD yes;
            ME yes;
            MK yes;
            MT yes;
            NL yes;
            NO yes;
            PL yes;
            PT yes;
            RO yes;
```

```
            SK yes;
            SI yes;
            ES yes;
            RS yes;
            RU yes;
            SE yes;
            SM yes;
            TR yes;
            UA yes;
            VA yes;
            XK yes;
        # Allowed countries list:
        #
AL,AD,AM,AT,BA,BE,BG,BY,CH,CY,CZ,DK,EE,FI,FR,FO,DE,GB,GE,GI,GR,HR,HU,IE,IM,I
S,IT,LI,LV,LT,LU,MC,MD,ME,MK,MT,NL,NO,PL,PT,RO,SK,SI,ES,RS,RU,SE,SM,TR,UA,VA
,XK
    }

    ##
    # Virtual Host Configs
    ##

    include /etc/nginx/conf.d/*.conf;
    include /etc/nginx/sites-enabled/*;
}
```

Nous avons créé le fichier commun `/etc/nginx/letsencrypt_security.conf` afin de pouvoir générer et renouveler facilement des certificats TLS Let's Encrypt pour chacune de nos applications web.

Le fichier est agrémenté de directives de sécurité recommandées pour la plupart des applications (certaines modifient ces directives via leur propre configuration évidemment) :

```
# cat /etc/nginx/letsencrypt_security.conf
# Security headers
add_header X-XSS-Protection          "1; mode=block" always;
add_header X-Content-Type-Options    "nosniff" always;
add_header Referrer-Policy           "no-referrer-when-downgrade" always;
add_header Content-Security-Policy   "default-src 'self' http: https: ws:
wss: data: blob: 'unsafe-inline'; frame-ancestors 'self';" always;
add_header Permissions-Policy        "interest-cohort=()" always;
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains"
always;

# Dotfiles
location ~ /\.(?!well-known) {
    deny all;
}

# ACME-challenge
location ^~ /.well-known/acme-challenge/ {
```

```
    root /var/www/_letsencrypt;
}
```

Liberta (Site principal)

Le site de Liberta est en pur HTML et CSS.

Ce fichier contient la gestion globale du HTTP, lequel redirige tous les domaines vers HTTPS, notamment le site de Liberta qui est sur le sous-domaine `www.`.

Nous listons volontairement notre répertoire `img/` pour exposer nos images et pouvoir les utiliser facilement pour les includre sur nos pages ; c'est notamment utile pour insérer des images sur notre blog (WriteFreely ne le permet pas dans sa version communautaire malheureusement) :

```
# Configuration globale :
# HTTP + redirect
server {
    server_name _;
    listen      80;
    listen      [::]:80;

    include letsencrypt_security.conf;

    location / {
        return 301 https://$host$request_uri;
    }
}

# Domaine liberta.vip sans sous-domaine :
# HTTP + redirect
server {
    server_name liberta.vip;
    listen      80;
    listen      [::]:80;

    include letsencrypt_security.conf;

    location / {
        return 301 https://www.$host$request_uri;
    }
}
server {
        server_name liberta.vip;
        listen 443 ssl http2;
        listen [::]:443 ssl http2;
        ssl_certificate
/etc/letsencrypt/live/liberta.vip-0001/fullchain.pem;
        ssl_certificate_key
/etc/letsencrypt/live/liberta.vip-0001/privkey.pem;
        return 301 https://www.liberta.vip;
```

```
}
# Liberta (Pur HTML / CSS)
# HTTP + redirect
server {
        server_name www.liberta.vip;
        listen      80;
        listen      [::]:80;

    include letsencrypt_security.conf;

        location / {
                return 301 https://$host$request_uri;
        }
}
server {
        server_name www.liberta.vip;
        listen 443 ssl http2;
        listen [::]:443 ssl http2;
        ssl_certificate
/etc/letsencrypt/live/liberta.vip-0001/fullchain.pem;
        ssl_certificate_key
/etc/letsencrypt/live/liberta.vip-0001/privkey.pem;

        # Secure headers
        add_header X-Frame-Options "SAMEORIGIN" always;
        add_header Strict-Transport-Security "max-age=31536000;
includeSubDomains";
        add_header X-Xss-Protection "1; mode=block" always;
        add_header Content-Security-Policy "default-src 'self' 'unsafe-
inline'; script-src www.liberta.vip; img-src *;";
        add_header X-Content-Type-Options "nosniff" always;


        root /var/www/www.liberta.vip;
        access_log /var/log/nginx/www.liberta.vip_access.log;
        error_log /var/log/nginx/www.liberta.vip_error.log warn;
        index index.html;

        location = /favicon.ico {
                log_not_found off;
                access_log off;
        }

        location = /robots.txt {
                allow all;
                log_not_found off;
                access_log off;
        }

    location = /img/ {
                allow all;
```

```
                log_not_found off;
                access_log off;
        autoindex on;
        }

        location ~* \.(js|css|png|jpg|jpeg|gif|ico)$ {
                expires max;
                log_not_found off;
        }
}
```

Nous ne fournirons pas tous les détails des configurations pour chaque application, lesquelles sont souvent appelées à changer lors des mises à jour et rendraient la maintenance de cette documentation fort fastidieuse.

À terme, nous prévoyons de publier notre configuration complète sur notre dépôt git, d'autant plus que nous désirons l'industrialiser / l'automatiser via `ansible`.

CryptPad (Liberta Docs)

Etherpad-Lite (Liberta Pad)

Funkwhale (Liberta Audio)

Nextcloud (Liberta Cloud)

Peertube (Liberta Vidéo)

WriteFreely (Liberta Blogs)