

LXD – Configuration de l'hôte et conteneur



Référence: Ubuntu 22.04

Description du projet:

Installation de Ubuntu 22.04 sur une machine physique hôte et installation d'un serveur web dans un conteneur LXD. Plusieurs services sont aussi installés sur l'hôte pour servir de NAS et médiathèque.

Il s'agit vraiment de note complète d'installation afin de servir d'aide mémoire pour recommencer de nouveau si le besoin se fait sentir.

Le Motherboard Supermicro possède un connecteur M.2 mais ne supporte pas le boot à partir de celui-ci

Impossible de faire la mise à jour du bios malgré plusieurs tentatives.

Donc utilisation d'une clef USB rapide et accessible du bios pour configurer le répertoire /boot et grub afin de démarrer le nouveau système sur la carte NVMe M.2

Prérequis:

- carte NVMe 500gb
- clef USB 3.1 16gb (pour grub et /boot)
- clef USB pour support d'installation de Ubuntu 20.04.3

Lors de l'installation de l'OS, simplement configurer la clef USB comme répertoire /boot et sélectionner l'installation du logiciel de démarrage GRUB sur celle-ci

Ajouter une partition unique sur le disque NVMe pour utilisation comme répertoire racine /

Procéder à l'installation normalement en ajoutant `opensshserver` lorsque proposé.

Dans le bios, ajuster les options de boot pour démarrer de la clef usb /boot qui doit alors demeurer en tout temps branchée.

Instructions de configuration:

Désactiver cloud-init:

```
sudo touch /etc/cloud/cloud-init.disabled
```

```
sudo nano /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg
```

```
network: {config: disabled}
```

Sur host1, configurer le réseau avec une adresse IP fixe:

```
ls /etc/netplan
```

```
>50-cloud-init.yaml 50-static-public-ip.yaml
```

```
sudo nano /etc/netplan/50-static-public-ip.yaml
```

```
network:
  version: 2
  renderer: networkd
  ethernets:
    eno1:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.0.2/24]
      nameservers:
        addresses:
          - 192.168.0.5
```

```
routes:
  - to: default
    via: 192.168.0.1
eno2:
  dhcp4: no
  dhcp6: no
  addresses: [192.168.0.11/24]
  nameservers:
    addresses:
      - 192.168.0.5
```

Appliquer les changements:

```
sudo netplan apply
```

Vérifier le résultat des modifications:

```
ip addr show dev eno1
```

```
ip addr show dev eno2
```

Installation des pré-requis:

```
sudo apt install -y git build-essential libssl-dev python3-venv python3-pip python3-dev zfsutils-linux bridge-utils
```

Installation de LXD 4.0 LTS: Probablement déjà installé

```
sudo snap install lxd --channel=4.0/stable
```

Accepter tout les paramètres par défaut:

```
lxd init
```

Pour d'autres instructions de paramétrage de LXD suivre ce lien:

<https://linuxcontainers.org/lxd/getting-started-cli/>

```
mkdir /home/nas/logiciels
```

```
cd /home/nas/logiciels
```

Serveur de temps:

```
sudo apt install ntp ntpdate
```

Vérifier la time zone:

```
timedatectl
```

```
timedatectl list-timezones
```

Ajuster la time zone si nécessaire

```
sudo timedatectl set-timezone America/Montreal
```

```
timedatectl
```

Installer les permissions acl:

```
sudo apt install acl
```

Créer les points de montage pour les disques qui seront en partage NFS et SAMBA

```
cd /media
```

```
sudo mkdir /media/nas1
```

```
sudo mkdir /media/nas2
```

```
sudo chmod 770 /media/nas1
```

```
sudo chmod 770 /media/nas2
```

Création du répertoire de montage du miroir mp3:

```
sudo /media/nas1/Audio/sub_mp3-128
```

Installer serveur NFS et le miroir de fichiers en mp3

```
sudo apt install nfs-kernel-server
```

```
sudo apt install mp3fs
```

```
sudo nano /etc/exports
```

#sous NFSv3, ajouter les lignes suivantes:

```
/media/nas1
```

```
192.168.0.0/24(rw,sync,no_subtree_check,all_squash,anonuid=1000,anongid=150)
```

```
/media/nas2
```

```
192.168.0.0/24(rw,sync,no_subtree_check,all_squash,anonuid=1000,anongid=150)
```

Redémarrer le serveur NFS

```
sudo service nfs-kernel-server restart
```

Configurer le montage des disques durs et ajouter acl à /:

```
sudo nano /etc/fstab
```

```
# /media/nas1
UUID=6edc9052-a976-419c-9741-d60e58b7df62 /media/nas1 ext4 defaults,acl 0 2

# /media/nas2
UUID=612ba999-8696-4c98-8d68-5c593bc595ec /media/nas2 ext4 defaults,acl 0 2

#mp3fs mount
mp3fs#/media/nas1/Audio/Musique/ /media/nas1/Audio/sub_mp3-128/ -ogainmode=1,fuse
allow_other,ro,bitrate=128 0 0
```

```
sudo mount -o remount,acl /
```

```
sudo mount -a
```

Installer Samba

```
sudo apt install samba
```

Cette installation s'inscrit comme un service NAS et donc cette opération doit être effectuée sur toutes les machines linux du réseau afin que le même GID de groupe soit utilisé. Évidemment le no. (150) est à valider, il faut choisir un GID qui est libre sur vos machines.

Vérifier le GID pour sambashare et le modifier pour 150

```
cat /etc/group
```

```
sudo groupmod -g 150 sambashare
```

```
sudo find / -group 118 -exec chgrp -h sambashare {} \;
```

Énumérer les usagers déjà présents sur le système

```
cat /etc/passwd
```

```
nas:x:1000:1000:nas,,,:/home/nas:/bin/bash
```

Ajouter l'utilisateur générique qui sera utilisé sous Windows

```
sudo useradd -s /bin/false -d /dev/null -g sambashare virtuel
```

Énumérer les usagers présents sur le système suite aux ajouts

```
cat /etc/passwd
```

```
virtuel:x:1001:150:./dev/null:/bin/false
nas:x:1000:1000:nas,,,:/home/nas:/bin/bash
```

Dernière chose à faire avant de pouvoir accéder aux répertoires partagés de votre machine sous Samba (Windows), il faut créer des mots de passe pour les comptes qui auront accès à ceux-ci. Samba n'utilise pas les mots de passe du système, mais a son propre fichier pour stocker ceux-ci (/etc/smbpasswd).

Pour créer les mots de passe samba pour chaque utilisateur du partage :

```
sudo smbpasswd -a (remplacer)
```

```
sudo smbpasswd -a nas
```

```
sudo smbpasswd -a virtuel
```

```
New SMB password:
Retype new SMB password:
Added user username.
```

Ensuite, effectuer la configuration de Samba pour la mise en place du partage sous Windows

```
sudo nano /etc/samba/smb.conf
```

```
#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
```

```
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Some options that are often worth tuning have been included as
# commented-out examples in this file.
# - When such options are commented with ";", the proposed setting
#   differs from the default Samba behaviour
# - When commented with "#", the proposed setting is the default
#   behaviour of Samba but the option is considered important
#   enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

#===== Global Settings =====

[global]
#ACL
  vfs objects = acl_xattr
  map acl inherit = yes
  store dos attributes = yes
## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
  workgroup = WORKGROUP

# server string is the equivalent of the NT Description field
  server string = %h server (Samba, Ubuntu)

# Allow old client devices to connect to this machine's samba sever
  server min protocol = NT1
  lm announce = yes
  lanman auth = yes
  ntlm auth = yes

# Allow samba client tools to be able to connect to old servers/nas devices
  client min protocol = NT1
```

```
client ntlmv2 auth = no
client use spnego = no
client lanman auth = yes
```

Networking

```
# The specific set of interfaces / networks to bind to
# This can be either the interface name or an IP address/netmask;
# interface names are normally preferred
; interfaces = 127.0.0.0/8 eth0

# Only bind to the named interfaces and/or networks; you must use the
# 'interfaces' option above to use this.
# It is recommended that you enable this feature if your Samba machine is
# not protected by a firewall or is a firewall itself. However, this
# option cannot handle dynamic or non-broadcast interfaces correctly.
; bind interfaces only = yes
```

Debugging/Accounting

```
# This tells Samba to use a separate log file for each machine
# that connects
log file = /var/log/samba/log.%m

# Cap the size of the individual log files (in KiB).
max log size = 1000

# We want Samba to only log to /var/log/samba/log.{smbd,nmbd}.
# Append syslog@1 if you want important messages to be sent to syslog too.
logging = file

# Do something sensible when Samba crashes: mail the admin a backtrace
panic action = /usr/share/samba/panic-action %d
```

Authentication

```
# Server role. Defines in which mode Samba will operate. Possible
# values are "standalone server", "member server", "classic primary
# domain controller", "classic backup domain controller", "active
```



```
# directory domain controller".
#
# Most people will want "standalone server" or "member server".
# Running as "active directory domain controller" will require first
# running "samba-tool domain provision" to wipe databases and create a
# new domain.
    server role = standalone server

    obey pam restrictions = yes

# This boolean parameter controls whether Samba attempts to sync the Unix
# password with the SMB password when the encrypted SMB password in the
# passwd is changed.
    unix password sync = yes

# For Unix password sync to work on a Debian GNU/Linux system, the following
# parameters must be set (thanks to Ian Kahan <<kahan@informatik.tu-muenchen.de>
for
# sending the correct chat script for the passwd program in Debian Sarge).
    passwd program = /usr/bin/passwd %u
    passwd chat = *Enter\snew\s*\spassword:* %n\n *Retye\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully* .

# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
    pam password change = yes

# This option controls how unsuccessful authentication attempts are mapped
# to anonymous connections
    map to guest = bad user

##### Domains #####

#
# The following settings only takes effect if 'server role = classic
# primary domain controller', 'server role = classic backup domain controller'
# or 'domain logons' is set
#

# It specifies the location of the user's
# profile directory from the client point of view) The following
```

```
# required a [profiles] share to be setup on the samba server (see
# below)
; logon path = \\%N\profiles\%U
# Another common choice is storing the profile in the user's home directory
# (this is Samba's default)
# logon path = \\%N\%U\profile

# The following setting only takes effect if 'domain logons' is set
# It specifies the location of a user's home directory (from the client
# point of view)
; logon drive = H:
# logon home = \\%N\%U

# The following setting only takes effect if 'domain logons' is set
# It specifies the script to run during logon. The script must be stored
# in the [netlogon] share
# NOTE: Must be store in 'DOS' file format convention
; logon script = logon.cmd

# This allows Unix users to be created on the domain controller via the SAMR
# RPC pipe. The example command creates a user account with a disabled Unix
# password; please adapt to your needs
; add user script = /usr/sbin/adduser --quiet --disabled-password --gecos "" %u

# This allows machine accounts to be created on the domain controller via the
# SAMR RPC pipe.
# The following assumes a "machines" group exists on the system
; add machine script = /usr/sbin/useradd -g machines -c "%u machine account" -d
/var/lib/samba -s /bin/false %u

# This allows Unix groups to be created on the domain controller via the SAMR
# RPC pipe.
; add group script = /usr/sbin/addgroup --force-badname %g

##### Misc #####

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
; include = /home/samba/etc/smb.conf.%m

# Some defaults for winbind (make sure you're not using the ranges
```

```
# for something else.)
; idmap config * : backend = tdb
; idmap config * : range = 3000-7999
; idmap config YOURDOMAINHERE : backend = tdb
; idmap config YOURDOMAINHERE : range = 100000-999999
; template shell = /bin/bash

# Setup usershare options to enable non-root users to share folders
# with the net usershare command.

# Maximum number of usershare. 0 means that usershare is disabled.
# usershare max shares = 100

# Allow users who've been granted usershare privileges to create
# public shares, not just authenticated ones
usershare allow guests = yes

# security = user
#valid users = nas, virtuel, @sambashare
# valid users = @sambashare
# encrypt passwords = true
# password database type you are using.
# passdb backend = tdbsam

##### Share #####

[Serveur - Dossier home]
comment = NAS - Répertoire home de host1
path = /home/nas
read only = no
write list = nas
#read list = utilisateur1, utilisateur2, @groupe12000
create mask = 0775
directory mask = 0770
[Documents des enfants]
comment = Dossier des documents des enfants sur host1
path = /media/nas1/Documents/LesEnfants
read only = yes
write list = @sambashare
```

```
#read list = utilisateur1, utilisateur2, @groupe12000
create mask = 0775
directory mask = 0775
[Documents des parents]
comment = Dossier des documents des parents sur host1
path = /media/nas1/Documents/LesParents
read only = yes
write list = nas, lafontaj, virtuel
#read list = utilisateur1, utilisateur2, @groupe12000
create mask = 0775
directory mask = 0775
[Downloads sur nas1]
comment = Dossier de téléchargements sur host1
path = /media/nas1/Download
read only = yes
write list = @sambashare
#read list = utilisateur1, utilisateur2, @groupe12000
create mask = 0775
directory mask = 0775
[nas1]
comment = Disque en partage sur host1
path = /media/nas1
read only = yes
write list = nas
read list = @sambashare
create mask = 0775
directory mask = 0775
[nas2]
comment = Disque en partage sur host1
path = /media/nas2
read only = Yes
write list = @sambashare
#read list = utilisateur1, utilisateur2, @groupe12000
create mask = 0775
directory mask = 0775
[submp3_128]
comment = Disque en partage sur host1
path = /media/nas1/Audio/sub_mp3-128
read only = yes
write list = nas
read list = @sambashare
create mask = 0775
```

```
directory mask = 0775
[Scan]
comment = Disque en partage sur host1
path = /media/nas1/Documents/LesParents/Projets/Conjoint/Finance/scan/
read only = yes
write list = nas, lafontaj, virtuel
read list = @sambashare
create mask = 0775
directory mask = 0775
```

```
sudo service smb restart
```

```
sudo service nmb restart
```

Ajout des permissions avec ACL

```
sudo setfacl -Rm g:sambashare:rwX /media/nas1
```

```
sudo setfacl -Rm g:sambashare:rwX /media/nas2
```

```
sudo setfacl -Rm d:g:sambashare:rwX /media/nas1
```

```
sudo setfacl -Rm d:g:sambashare:rwX /media/nas2
```

```
sudo setfacl -Rm d:o:rx /media/nas1
```

```
sudo setfacl -Rm d:o:rx /media/nas2
```

```
sudo getfacl /media/nas1
```

```
sudo getfacl /media/nas2
```

Redémarrer le serveur

```
sudo reboot
```

Installer MusicIP selon le WIKI: <https://blog.infolaf.ca/wiki/musicip/>

Installer Logitech Media Server selon le WIKI:

<https://blog.infolaf.ca/wiki/howto-logitech-media-server-lms/>

Installer BlissHQ selon le WIKI: <https://blog.infolaf.ca/wiki/blisshq/>

Installation de Gerbera selon le WIKI: <https://blog.infolaf.ca/wiki/gerbera/>

Installation de Deluge selon le WIKI: <https://blog.infolaf.ca/wiki/deluge/>

Installation de Veracryp selon le WIKI: <https://blog.infolaf.ca/wiki/veracrypt/>

Installation de logiciel de gestion du UPS Cyberpower:

<https://blog.infolaf.ca/wiki/ups-cyberpower/>

Installation de vlc

```
sudo apt install vlc
```

Donner accès à VLC aux périphériques audio lorsque lancer sous l'utilisateur nas.

```
sudo adduser nas audio
```

Afin de mettre en place le contrôle d'accès aux fichiers, il faut ajouter chacun des utilisateurs au groupe sambashare incluant les services démarrés sous un autre nom d'utilisateur tel que LMS, Mediatomb, Deluge car on veut que ces services puissent lire ou écrire des listes de lectures, fichiers en téléchargement etc:

```
sudo usermod -a -G sambashare nas
```

```
sudo usermod -a -G sambashare squeezeboxserver
```

```
sudo usermod -a -G sambashare gerbera
```

```
sudo usermod -a -G sambashare deluge
```

```
sudo usermod -a -G sambashare virtuel
```

Pour vérifier les associations via la console:

```
cat /etc/group
```

```
sambashare:x:150:nas,virtuel,squeezeboxserver,gerbera,deluge
```

Installation de rsync sur HOST1

```
sudo apt install rsync
```

Sauvegarder et quitter

```
sudo nano /etc/rsyncd.conf
```

```
sudo systemctl enable rsync
```

Redémarrer le service

```
sudo systemctl restart rsync
```

```
nano /etc/rsyncd.conf
```

```
log file = /var/log/rsync.log

[scripts_HOST1]
uid = nas
gid = nas
path = /home/nas/scripts
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup scripts_HOST1
read only = true
auth users = test
secrets file = /etc/rsyncd.scr

[musicip_HOST1]
uid = nas
gid = nas
path = /home/nas/logiciels/MusicIP
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup musicip_HOST1
read only = true
auth users = test
secrets file = /etc/rsyncd.scr

[MusicMagic_HOST1]
uid = nas
gid = nas
path = /home/nas
```

```
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup .MusicMagic_HOST1
read only = true
auth users = test
secrets file = /etc/rsyncd.scr
```

```
[rsync_HOST1]
uid = root
gid = root
path = /etc/
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup rsync_HOST1
read only = true
auth users = test
secrets file = /etc/rsyncd.scr
```

```
[bind_HOST1]
uid = root
gid = root
path = /etc/bind
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup bind_HOST1
read only = true
auth users = test
secrets file = /etc/rsyncd.scr
```

```
[samba_HOST1]
uid = root
gid = root
path = /etc/samba/
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup samba_HOST1
read only = true
auth users = test
secrets file = /etc/rsyncd.scr
```

```
[nfs_HOST1]
uid = root
gid = root
path = /etc/
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup nfs_HOST1
```



```
read only = true
auth users = test
secrets file = /etc/rsyncd.scrpt

[gerbera_HOST1]
uid = root
gid = root
path = /etc/gerbera
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup gerbera_HOST1
read only = true
auth users = test
secrets file = /etc/rsyncd.scrpt

[crontab_HOST1]
uid = root
gid = root
path = /var/spool/cron/crontabs/
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup crontab_HOST1
read only = true
auth users = test
secrets file = /etc/rsyncd.scrpt
```

```
sudo nano /etc/rsyncd.scrpt
```

```
test:votremotdepasse
```

```
sudo chmod 640 /etc/rsyncd.scrpt
```

Vous pouvez maintenant lancer rsync:

```
sudo service rsync start
```

```
mkdir -p /home/nas/scripts/rsync/auto/
```

```
nano /home/nas/scripts/rsync/auto/backup_web-ns1.sh
```

```
echo "Bonjour,"
```

```
echo ""
echo "Ce message vous confirme que les sites web sont bien sauvegardee localement
dans /media/nas1/Backups/"
echo ""
echo ""
echo ""
echo "Message produit par le script de sauvegarde execute par CRON sur
nas@host1.reseau.maison"
echo ""
rsync -avz --stats --delete --exclude='quota.*' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.4::cumulus/
/media/nas1/Backups/lxdvm-ns1_20.04_www/cumulus
rsync -avz --stats --delete --exclude='quota.*' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.4::matomo/
/media/nas1/Backups/lxdvm-ns1_20.04_www/matomo
rsync -avz --stats --delete --exclude='quota.*' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.4::photos/
/media/nas1/Backups/lxdvm-ns1_20.04_www/photos
#rsync -avz --stats --delete --exclude='quota.*' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.4::blog/
/media/nas1/Backups/lxdvm-ns1_20.04_www/blog
#rsync -avz --stats --delete --exclude='quota.*' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.4::webmail/
/media/nas1/Backups/lxdvm-ns1_20.04_www/webmail
rsync -avz --stats --delete --exclude='quota.*' --exclude='lost+found/' --
password-file /home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.4::www-full/
/media/nas2/Backups/lxdvm-ns1_20.04_www-full_path
```

```
chmod 777 /home/nas/scripts/rsync/auto/backup_web-ns1.sh
```

```
nano /home/nas/scripts/rsync/auto/backup_mysql-ns1.sh
```

```
echo "Bonjour,"
echo ""
echo "Ce message vous confirme que les bases de donnees MYSQL sont bien
sauvegardee dans /media/nas1/Backups/lxdvm-ns1_20.04_MySQL_db/"
echo ""
echo ""
echo ""
echo "Message produit par le script de sauvegarde execute par CRON sur
```

```
nas@host1.reseau.maison"
echo ""
rsync -avz --stats --delete --exclude='lost+found/' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.4::mysql/
/media/nas1/Backups/lxdvm-ns1_20.04_MySQL_db
```

```
chmod 777 /home/nas/scripts/rsync/auto/backup_mysql-ns1.sh
```

```
nano /home/nas/scripts/rsync/auto/backup_scripts.sh
```

```
echo "Bonjour,"
echo ""
echo "Ce message vous confirme que les scripts de lxdvm-ns1 sont bien sauvegarde
dans /media/nas1/Backups/Scripts/lxdvm-ns1"
echo "Ce message vous confirme que les scripts de HOST1 sont bien sauvegarde dans
/media/nas1/Backups/Scripts/HOST1"
echo ""
echo ""
echo ""
echo "Message produit par le script de sauvegarde execute par CRON sur
nas@host1.reseau.maison"
echo ""
echo "scripts_NS1"
rsync -avz --stats --delete --exclude='lost+found/' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.4::scripts_NS1/
/media/nas1/Backups/Scripts/lxdvm-ns1_20.04
echo ""
echo "scripts_HOST1"
rsync -avz --stats --delete --exclude='lost+found/' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.11::scripts_HOST1/
/media/nas1/Backups/Scripts/HOST1_20.04
```

```
chmod 777 /home/nas/scripts/rsync/auto/backup_scripts.sh
```

```
nano /home/nas/scripts/rsync/auto/backup_config.sh
```

```
echo "Bonjour,"
echo ""
echo "Ce message vous confirme que les fichiers de configuration de lxdvm-ns1
```

```
sont bien sauvegardes dans /media/nas1/Backups/Config/lxdvm-ns1"
echo "Ce message vous confirme que les fichiers de configuration de host1 sont
bien sauvegardes dans /media/nas1/Backups/Config/host1"
echo ""
echo ""
echo "Message produit par le script de sauvegarde execute par CRON sur
nas@host1.reseau.maison"
echo ""
#rsync -avz --stats --delete --exclude='lost+found/' --include='/bind/**' --
exclude='**'
echo ""
echo "Crontab_NS1"
rsync -avz --stats --delete --exclude='lost+found/' --include='infolaf' --
exclude='**' --password-file /home/nas/scripts/rsync/auto/rsync_pass
test@192.168.0.4::crontab_NS1/ /media/nas1/Backups/Config/lxdvm-ns1_20.04/crontab
echo ""
echo "Crontab_HOST1"
rsync -avz --stats --delete --exclude='lost+found/' --include='nas' --
exclude='**' --password-file /home/nas/scripts/rsync/auto/rsync_pass
test@192.168.0.11::crontab_HOST1/ /media/nas1/Backups/Config/HOST1_20.04/crontab
echo ""
echo "rsync_NS1"
rsync -avz --stats --delete --exclude='lost+found/' --include='rsyncd.conf' --
exclude='**' --password-file /home/nas/scripts/rsync/auto/rsync_pass
test@192.168.0.4::rsync_NS1/ /media/nas1/Backups/Config/lxdvm-ns1_20.04/rsync
echo ""
echo "rsync_HOST1"
rsync -avz --stats --delete --exclude='lost+found/' --include='rsyncd.conf' --
exclude='**' --password-file /home/nas/scripts/rsync/auto/rsync_pass
test@192.168.0.11::rsync_HOST1/ /media/nas1/Backups/Config/HOST1_20.04/rsync
echo ""
echo "bind_NS1"
rsync -avz --stats --delete --exclude='lost+found/' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.4::bind_NS1/
/media/nas1/Backups/Config/lxdvm-ns1_20.04/bind
echo ""
echo "bind_HOST1"
rsync -avz --stats --delete --exclude='lost+found/' --password-file
/home/nas/scripts/rsync/auto/rsync_pass test@192.168.0.11::bind_HOST1/
/media/nas1/Backups/Config/HOST1_20.04/bind
echo ""
echo "samba_HOST1"
```

```
rsync -avz --stats --delete --exclude='lost+found/' --include='smb.conf' --  
exclude='**' --password-file /home/nas/scripts/rsync/auto/rsync_pass  
test@192.168.0.11::samba_HOST1/ /media/nas1/Backups/Config/HOST1_20.04/  
echo ""  
echo "nfs_HOST1"  
rsync -avz --stats --delete --exclude='lost+found/' --include='exports' --  
exclude='**' --password-file /home/nas/scripts/rsync/auto/rsync_pass  
test@192.168.0.11::nfs_HOST1/ /media/nas1/Backups/Config/HOST1_20.04/  
echo ""  
echo "gerbera_HOST1"  
rsync -avz --stats --delete --exclude='lost+found/' --include='config.xml' --  
exclude='**' --password-file /home/nas/scripts/rsync/auto/rsync_pass  
test@192.168.0.11::gerbera_HOST1/ /media/nas1/Backups/Config/HOST1_20.04/
```

```
chmod 777 /home/nas/scripts/rsync/backup_config.sh
```

```
nano /home/nas/scripts/rsync/auto/backup_logiciels.sh
```

```
echo "Bonjour,"  
echo ""  
echo "Ce message vous confirme que les logiciels de HOST1 sont bien sauvegarde  
dans /media/nas1/Backups/"  
echo ""  
echo ""  
echo ""  
echo "Message produit par le script de sauvegarde execute par CRON sur  
nas@HOST1.reseau.maison"  
echo ""  
echo "musicip_HOST1"  
rsync -avz --stats --delete --exclude='lost+found/' --include='MusicIP/**' --  
exclude='**' --password-file /home/nas/scripts/rsync/auto/rsync_pass  
test@192.168.0.11::musicip_HOST1/ /media/nas1/Backups/musicip_20.04  
echo "MusicMagic_HOST1"  
rsync -avz --stats --delete --exclude='lost+found/' --include='.MusicMagic/**' -  
-exclude='**' --password-file /home/nas/scripts/rsync/auto/rsync_pass  
test@192.168.0.11::MusicMagic_HOST1/ /media/nas1/Backups/musicip_20.04
```

```
chmod 777 /home/nas/scripts/rsync/backup_logiciels.sh
```

Créer le fichier de mot de passe d'exécution automatique. Le mot de passe est celui indiqué dans le fichier /etc/rsyncd.scrpt

```
nano /home/nas/scripts/rsync/auto/rsync_pass
```

```
votremotdepasse
```

on change les permissions du fichier.

```
chmod 640 /home/nas/scripts/rsync/rsync_pass
```

et on ajoute les commandes suivantes dans crontab :

```
crontab -e
```

```
# m h dom mon dow command
MAILTO=postmaster@reseau.maison
15 00 * * 0-7 sh /home/nas/scripts/rsync/auto/backup_mysql-ns1.sh
20 00 * * 0-7 sh /home/nas/scripts/rsync/auto/backup_web-ns1.sh
45 00 * * 0-7 sh /home/nas/scripts/rsync/auto/backup_scripts.sh
50 00 * * 0-7 sh /home/nas/scripts/rsync/auto/backup_config.sh
55 00 * * 0-7 sh /home/nas/scripts/rsync/auto/backup_scripts_n73.sh
00 01 * * 0-7 sh /home/nas/scripts/rsync/auto/backup_logiciels.sh
00 05 1 * * sh /home/nas/scripts/lxdbbackup.sh lxdvm-ns1 >
/home/nas/scripts/lxdbbackup_lxdvm-ns1.log
```

Pour faire une sauvegarde du crontab:

```
crontab -u nas -l > /media/nas1/Backups/Config/HOST1_20.04/crontab.txt
```

Configuration LXD

Lors de la première utilisation de LXD seulement ajouter le profile macvlan:

```
lxc profile create macvlan
```

```
Profile macvlan created
```

```
lxc profile list
```

```
+-----+-----+
| NAME   | USED BY |
+-----+-----+
| default | 1      |
+-----+-----+
| macvlan | 0      |
+-----+-----+
```

```
lxc profile show macvlan
```

```
config: {}
description: ""
devices: {}
name: macvlan
used_by: []
```

```
ip route show default 0.0.0.0/0
```

```
default via 192.168.0.1 dev eno2 proto static
default via 192.168.0.1 dev eno1 proto static
```

```
lxc profile device add macvlan eth0 nic nictype=macvlan parent=enol
```

```
Device eth0 added to macvlan
```

```
lxc profile show macvlan ou lxc config show lxdvm-ns1 -e
```

```
config: {}
description: ""
devices:
eth0:
nictype: macvlan
parent: eno1
```

```
type: nic
name: macvlan
used_by: []
```

Installation de LXD Dashboard dans un conteneur LXD, C'est un logiciel de gestion de conteneur LXD qui est lui-même installé dans un conteneur (lui associer macvlan)

<https://lxdware.com/installing-the-lxd-dashboard-on-ubuntu-22-04/>

Lors de l'installation de LXD Dashboard, associer macvlan pour l'accès au réseau

```
lxc profile add lxd-dashboard macvlan
```

```
lxc launch ubuntu:22.04 lxdvm-ns1
```

Ensuite ajouter macvlan au container nouvellement créer:

```
lxc profile add lxdvm-ns1 macvlan
```

J'ai effacé la carte réseau par défaut en mode bridge pour qu'enfin le profile macvlan se connecte au réseau domestique directement sans network

Avec **lxd-dashboard** (logiciel de gestion de conteneur LXD à installer) configurer pour lxdvm-ns1 les paramètres avancés suivants:

- limits.cpu.allowance 40%
- limits.memory 6000MB
- limits.memory.inforce soft
- security.privileged true

```
lxc config set lxdvm-ns1 boot.autostart true
```

Pour avoir les mêmes uid et gid que le host

```
lxc config set lxdvm-ns1 security.privileged true
```

Avant de configurer les disques vmail et WWW dans le conteneur, tous les

fichiers d'une installation précédente doivent être effacés. Certains fichiers ont un attribut qui empêche l'effacement.

Pour effacer les fichiers dans php, il faut retirer l'attribut avec la commande:

```
sudo chattr -i /var/www/php-fcgi-scripts/ispconfig/.php-fcgi-starter
```

```
sudo chattr -i /var/www/php-fcgi-scripts/apps/.php-fcgi-starter
```

Si requis seulement, il est possible de formater les partitions de nouveau

```
sudo mkfs -t ext4 /dev/sdf1
```

```
sudo mkfs -t ext4 /dev/sdf2
```

```
ls -l /dev/disk/by-id/
```

```
lrwxrwxrwx 1 root root 10 Nov 18 16:14 scsi-1ATA_ST2000NM0033-9ZM175_Z1Y0SDX7-  
part1 -> ../../sdf1  
lrwxrwxrwx 1 root root 10 Nov 18 16:14 scsi-1ATA_ST2000NM0033-9ZM175_Z1Y0SDX7-  
part2 -> ../../sdf2
```

```
lxc config device add lxdvm-ns1 courriel disk source=/dev/disk/by-id/scsi-  
SATA_ST2000NM0033-9ZM_Z1Y0SDX7-part1 path=/var/vmail
```

```
lxc config device add lxdvm-ns1 web disk source=/dev/disk/by-  
id/scsi-1ATA_ST2000NM0033-9ZM175_Z1Y0SDX7-part2 path=/var/www
```

Si nécessaire, pour retirer un device:

```
lxc config device remove lxdvm-ns1 courriel
```

Configuration de base ds le conteneur avant de pouvoir s'y connecter en SSH

Ouvrir un terminal dans le conteneur:

```
lxc exec lxdvm-ns1 /bin/bash
```

Permettre de se connecter en SSH avec le mot de passe

```
sudo nano /etc/ssh/sshd_config
```

```
PasswordAuthentication yes
```

```
sudo systemctl restart sshd
```

```
sudo adduser infolaf
```

```
Adding user `infolaf' ...  
Adding new group `infolaf' (1001) ...  
Adding new user `infolaf' (1001) with group `infolaf' ...  
Creating home directory `/home/infolaf' ...  
Copying files from `/etc/skel' ...
```

```
New password:  
Retype new password:
```

```
passwd: password updated successfully  
Changing the user information for infolaf  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] y
```

Ajouter l'utilisateur au groupe des sudoer:

```
usermod -aG sudo infolaf
```

```
sudo dpkg-reconfigure locales
```

```
Generating locales (this might take a while)...  
en_US.UTF-8... done  
fr_CA.UTF-8... done  
Generation complete.
```

Authentifiez-vous avec ssh pour poursuivre la configuration du conteneur

```
ssh infolaf@ip-address
```

Pour la suite: <https://blog.infolaf.ca/wiki/lxd-apache-multi-php-ispconfig/>