Mission 10 : FTP et SMB

Pré-requis

Afin de pouvoir réaliser cette mission il faut :

- Un serveur sous Debian 13
- Un routeur sous Debian 13
- La configuration IP des deux machines conforme au cahier des charges,
- La configuration DNS des deux machines conforme au cahier des charges,

Introduction

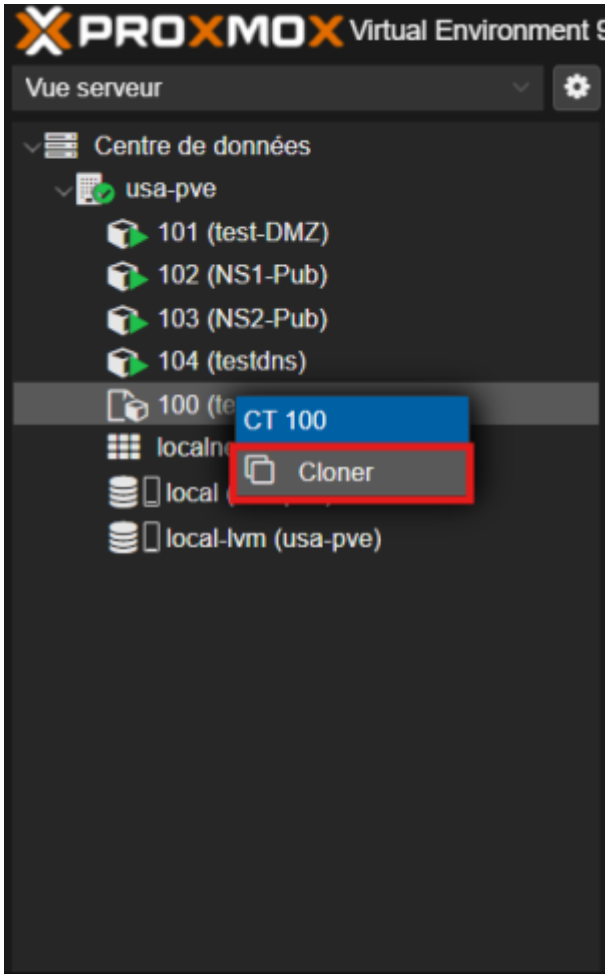
L'objectif est de mettre en place le protocole ftp sur nos machine pour pouvoir l'utilisé pour le transfert de fichiers d'un hôte à un autre sur un réseau TCP, tel qu'Internet. Ainsi que SMB qui permet l'échange de commandes et de données entre un ordinateur ou un logiciel

> **Avantage de FTP et SMB :**
> * Permet de faire des partages.
> * Permet l'échange de commandes et de données entre un ordinateur ou un logiciel.

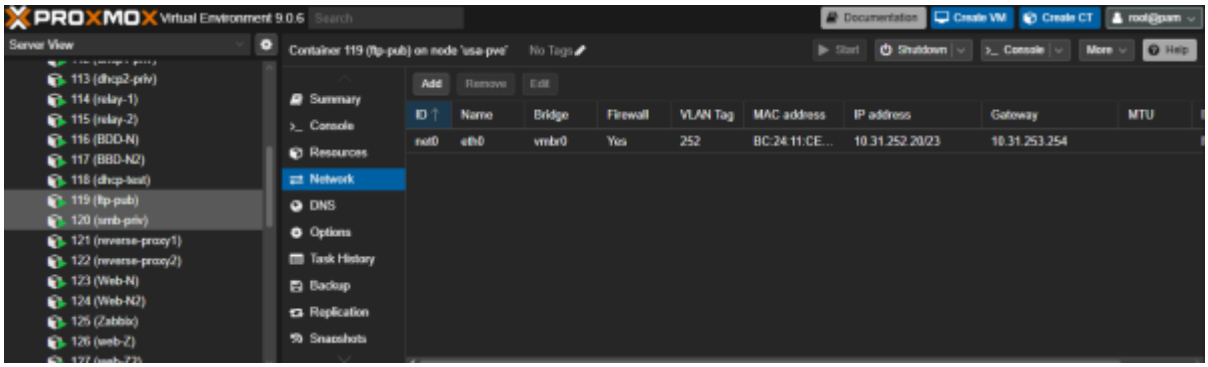
création et paramétrage du conteneur FTP

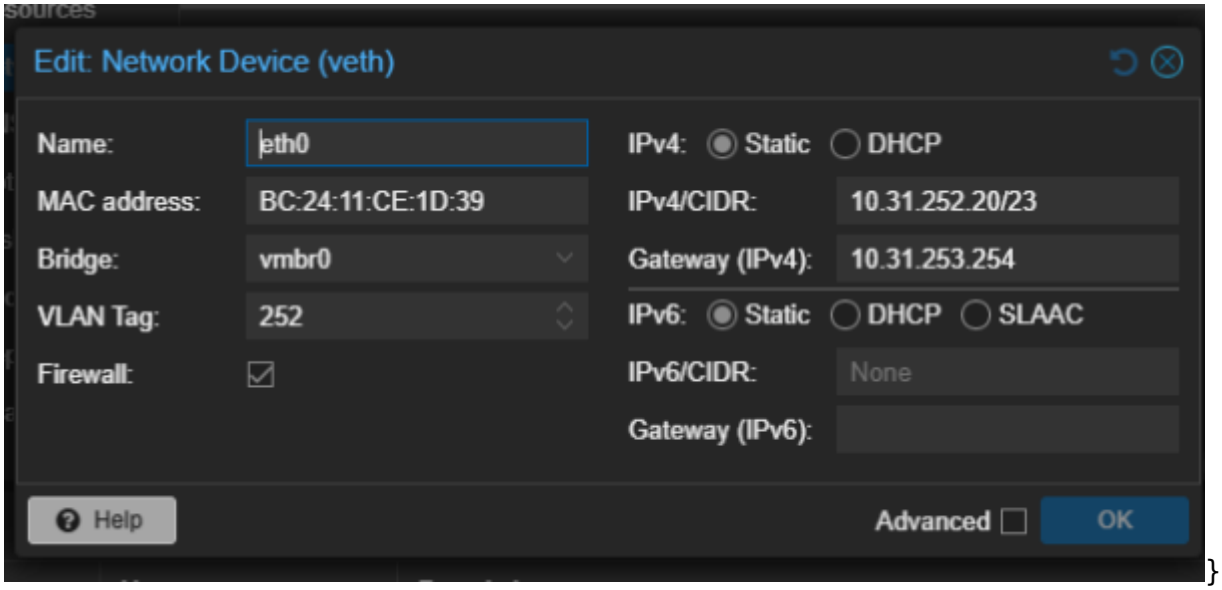
Proxmox

Tout d'abord nous avons réinitialisé la borne wifi pour le reconfigurer sur le logiciel Omada.
Ainsi créer un conteneur pour la borne wifi avec le logiciel Omada.
Pour commencer nous avons cloné le conteneur Template créé au préalable sur Proxmox pour l'appeler NS1-Pub



Après avoir cloné notre Template il fallait modifier les paramètres IP .
Toujours dans proxmox dans l'onglet network modifier les adresses ip que vous voulez.

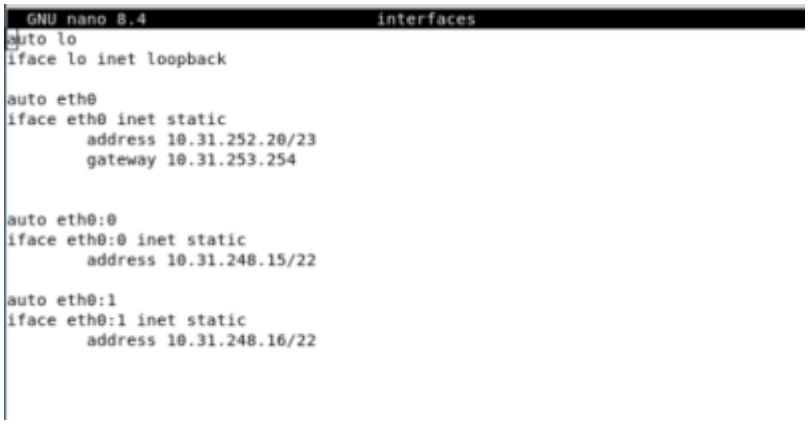




}

Installation et configuration de proftpd

Changé l'interface du conteneur en mettant les adresses suivantes pour les futur utilisateurs comme intranet et extranet :




```
nano /etc/metwork/interfaces
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 10.31.252.20/23
        gateway 10.31.253.254

auto eth0:0
iface eth0:0 inet static
        address 10.31.248.15/22

auto eth0:1
iface eth0:1 inet static
        address 10.31.248.16/22
```

Dans le fichier suivant décommenter les lignes pour le compte anonymous :

```
nano /etc/proftpd/proftpd.conf
```

Décommenter les lignes suivantes pour le comte anonymous :
Fichier proftpd.conf complet :

```
LoadModule mod_tls.c
#
# /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes, reload proftpd after modifications, if
# it runs in daemon mode. It is not required in inetd/xinetd mode.
#

# Includes DSO modules
Include /etc/proftpd/modules.conf

# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 on
# If set on you can experience a longer connection delay in many cases.
<IfModule mod_ident.c>
  IdentLookups off
</IfModule>

ServerName "Debian"
# Set to inetd only if you would run proftpd by inetd/xinetd/socket.
# Read README.Debian for more information on proper configuration.
ServerType standalone
DeferWelcome off

# Disable MultilineRFC2228 per
https://github.com/proftpd/proftpd/issues/1085
# MultilineRFC2228on
DefaultServer on
ShowSymlinks on

TimeoutNoTransfer 600
TimeoutStalled 600
TimeoutIdle 1200

DisplayLogin welcome.msg
DisplayChdir .message true
ListOptions "-l"

DenyFilter \*.*/

# Use this to jail all users in their homes
# DefaultRoot ~

# Users require a valid shell listed in /etc/shells to login.
# Use this directive to release that constrain.
# RequireValidShell off
```

```
# Port 21 is the standard FTP port.
Port 21

# In some cases you have to specify passive ports range to by-pass
# firewall limitations. Ephemeral ports can be used for that, but
# feel free to use a more narrow range.
 PassivePorts 40000 41000

# If your host was NATted, this option is useful in order to
# allow passive tranfers to work. You have to use your public
# address and opening the passive ports used on your firewall as well.
# MasqueradeAddress 1.2.3.4

# This is useful for masquerading address with dynamic IPs:
# refresh any configured MasqueradeAddress directives every 8 hours
<IfModule mod_dynmasq.c>
# DynMasqRefresh 28800
</IfModule>

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances 30

# Set the user and group that the server normally runs at.
User proftpd
Group nogroup

# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask 022 022
# Normally, we want files to be overwriteable.
AllowOverwrite on

# Uncomment this if you are using NIS or LDAP via NSS to retrieve passwords:
# PersistentPasswd off

# This is required to use both PAM-based authentication and local passwords
# AuthOrder mod_auth_pam.c* mod_auth_unix.c

# Be warned: use of this directive impacts CPU average load!
# Uncomment this if you like to see progress and transfer rate with ftpwho
# in downloads. That is not needed for uploads rates.
#
# UseSendFile off

TransferLog /var/log/proftpd/xferlog
SystemLog /var/log/proftpd/proftpd.log
```

```
# Logging onto /var/log/lastlog is enabled but set to off by default
#UseLastlog on

# In order to keep log file dates consistent after chroot, use timezone info
# from /etc/localtime.  If this is not set, and proftpd is configured to
# chroot (e.g. DefaultRoot or <Anonymous>), it will use the non-daylight
# savings timezone regardless of whether DST is in effect.
#SetEnv TZ :/etc/localtime

<IfModule mod_quotatab.c>
QuotaEngine off
</IfModule>

<IfModule mod_ratio.c>
Ratios off
</IfModule>


# Delay engine reduces impact of the so-called Timing Attack described in
# http://www.securityfocus.com/bid/11430/discuss
# It is on by default.
<IfModule mod_delay.c>
DelayEngine on
</IfModule>

<IfModule mod_ctrls.c>
ControlsEngine off
ControlsMaxClients 2
ControlsLog /var/log/proftpd/controls.log
ControlsInterval 5
ControlsSocket /var/run/proftpd/proftpd.sock
</IfModule>

<IfModule mod_ctrls_admin.c>
AdminControlsEngine off
</IfModule>

#
# Alternative authentication frameworks
#
#Include /etc/proftpd/ldap.conf
#Include /etc/proftpd/sql.conf

#
# This is used for FTPS connections
#
Include /etc/proftpd/tls.conf

#
# This is used for SFTP connections
#
```

```
#Include /etc/proftpd/sftp.conf

#
# This is used for other add-on modules
#
#Include /etc/proftpd/dnsbl.conf
#Include /etc/proftpd/geoip.conf
#Include /etc/proftpd/snmp.conf

#
# Useful to keep VirtualHost/VirtualRoot directives separated
#
Include /etc/proftpd/virtuals.conf

# A basic anonymous configuration, no upload directories.

 <Anonymous /home/ftpdocs>
   User ftp
   Group nogroup
   # We want clients to be able to login with "anonymous" as well as "ftp"
   UserAlias anonymous ftp
   # Cosmetic changes, all files belongs to ftp user
   DirFakeUser on ftp
   DirFakeGroup on ftp

   RequireValidShell off

   # Limit the maximum number of anonymous logins
   MaxClients 10

   # We want 'welcome.msg' displayed at login, and '.message' displayed
   # in each newly chdired directory.
   DisplayLogin welcome.msg
   DisplayChdir .message

   # Limit WRITE everywhere in the anonymous chroot
   <Directory *>
     <Limit WRITE>
       DenyAll
     </Limit>
   </Directory>

   # Uncomment this if you're brave.
   # <Directory incoming>
   #   # Umask 022 is a good standard umask to prevent new files and dirs
   #   # (second parm) from being group and world writable.
   #   Umask 022  022
   #   <Limit READ WRITE>
   #     DenyAll
   #     </Limit>
   #       <Limit STOR>
```

```
   #         AllowAll
   #     </Limit>
   # </Directory>

 </Anonymous>

# Include other custom configuration files
# !! Please note, that this statement will read /all/ file from this subdir,
# i.e. backup files created by your editor, too !!!
# Eventually create file patterns like this: /etc/proftpd/conf.d/*.conf
#
Include /etc/proftpd/conf.d/
```

Dans le fichier de conf virtuals.conf mettez les virtual host suivant :

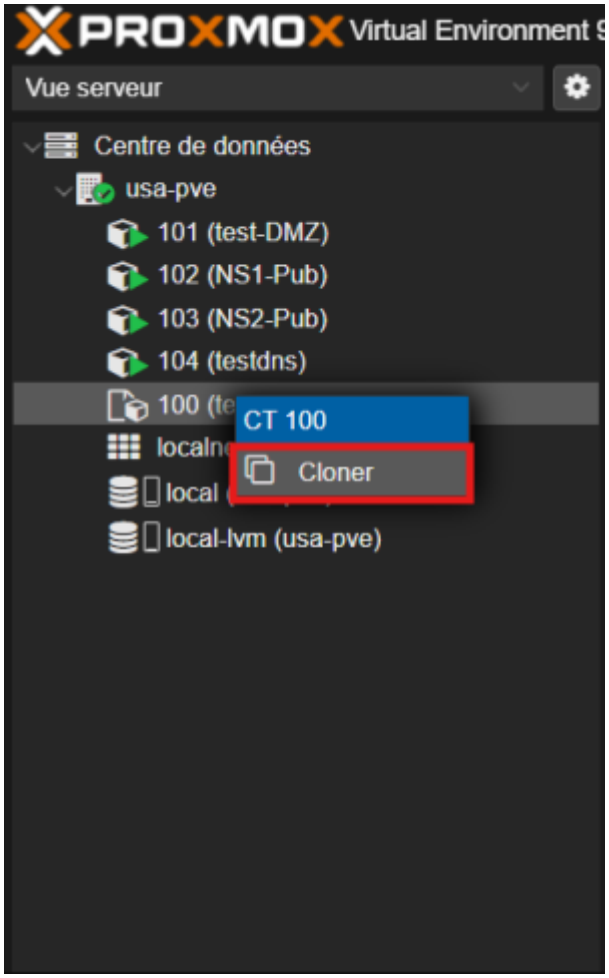
```
#
Proftpd sample configuration for Virtual Hosts and Virtual Roots.
#
Note that FTP protocol requires IP based virtual host, not name based.
#

#
A generic sample virtual host.
<VirtualHost 10.31.248.15>
        ServerAdmin     admin@gsb.org
        ServerName      "FTP INTRANET"
        User            intra
        Group           intra
        Port            2100

        <Limit LOGIN>
                Order Allow,Deny
                Allowgroup intra
                Deny from all
        </Limit>


        Umask                   022
        TransferLog             /var/log/proftpd/xfer/ftpin.usa.gsb.org
        MaxLoginAttempts        10
        DefaultRoot             /srv/ftp/intranet
        AllowOverwrite          yes

    Include /etc/proftpd/tls.conf
</VirtualHost>

<VirtualHost 10.31.248.16>
        ServerAdmin     admin@gsb.org
        ServerName      "FTP EXTRANET"
        User            extra
        Group           extra
```

```
        Port            2200

        <Limit LOGIN>
                Order Allow,Deny
                Allowgroup extra
                Deny from all
        </Limit>


        Umask                   022
        TransferLog             /var/log/proftpd/xfer/ftpex.zone.gsb.org
        MaxLoginAttempts        10
        DefaultRoot             /srv/ftp/extranet
        AllowOverwrite          yes

        Include /etc/proftpd/tls.conf
</VirtualHost>
#
The vroot module is not required, but can be useful for shared
directories.
<IfModule mod_vroot.c>
#VRootEngine on

#DefaultRoot ~
#VRootAlias upload /var/ftp/upload
#
#<VirtualHost a.b.c.d>
#VRootEngine on
#VRootServerRoot /etc/ftpd/a.b.c.d/
#VRootOptions allowSymlinks
#DefaultRoot ~
#</VirtualHost>
</IfModule>
```

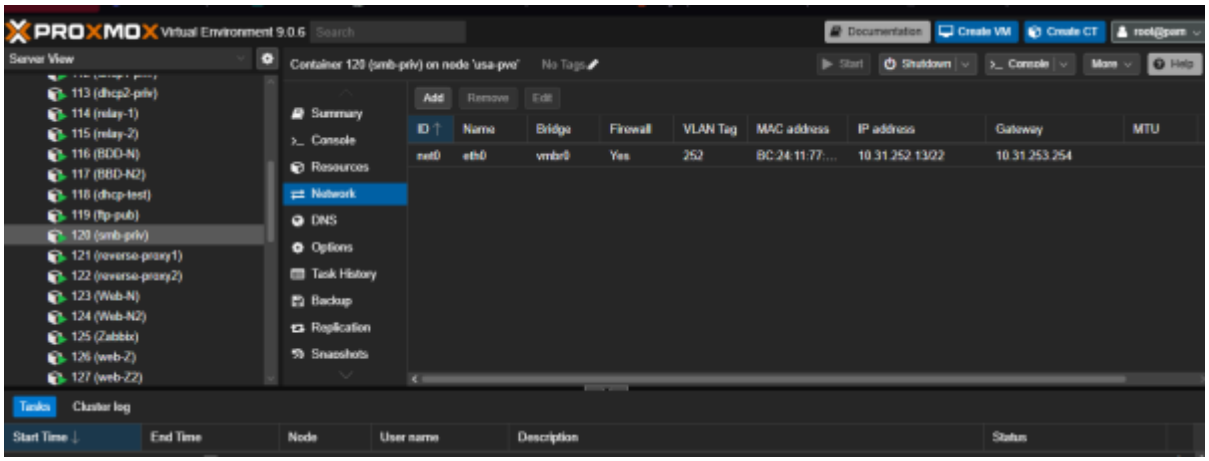
création et paramétrage du conteneur SMB

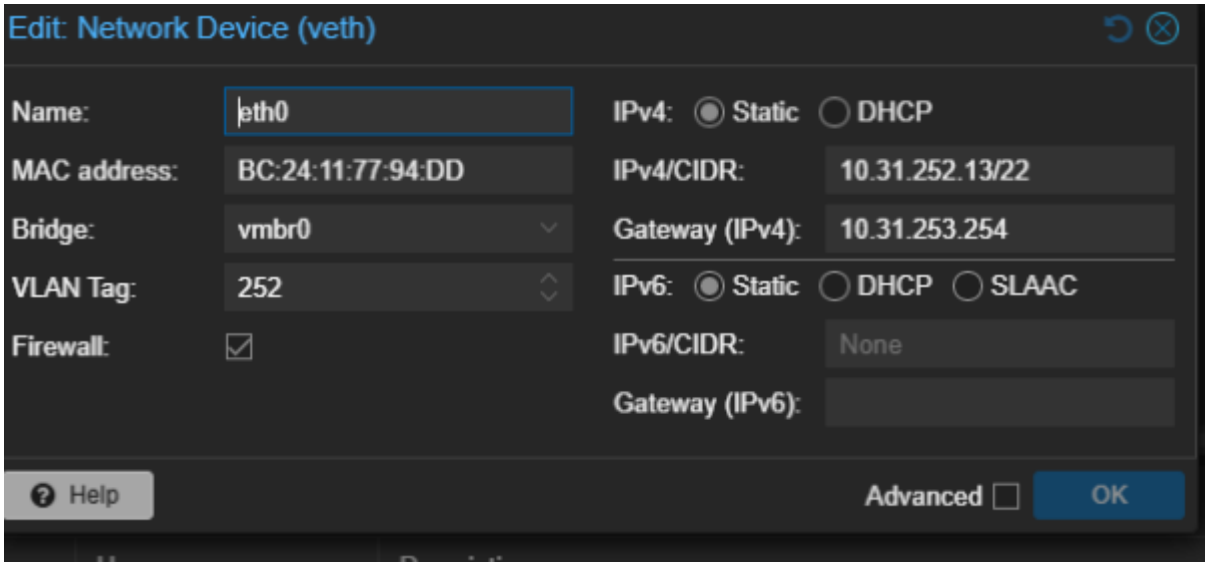
Proxmox

Tout d'abord nous avons réinitialisé la borne wifi pour le reconfigurer sur le logiciel Omada.
Ainsi créer un conteneur pour la borne wifi avec le logiciel Omada.
Pour commencer nous avons cloné le conteneur Template créé au préalable sur Proxmox pour l'appeler NS1-Pub



Après avoir cloné notre Template il fallait modifier les paramètres IP .
Toujours dans proxmox dans l'onglet network modifier les adresses ip que vous voulez.





Installation et configuration de Samba

Tout d'abord installer Samba :

```
apt install samba
```

Dans le fichier suivant rajouté les lignes manquante (fichier complet):

```
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]
```

```
## Browsing/Identification ###

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

#### 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
# passdb 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 *Retype\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/useradd --create-home %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

#======================= Share Definitions =======================

[homes]
   comment = Home Directories
   browseable = no
   read only = yes
```

```
   create mask = 0700
   directory mask = 0700
   valid users = %S


[admin]
 comment = Share directory
 browseable = yes
 path = /srv/admin
 writable = yes
 create mask = 0660
 directory mask = 0770
 valid users = @admins


[user]
 comment = Share directory
 browseable = yes
 path = /srv/users
 writable = yes
 create mask = 0660
 directory mask = 0770
 valid users = @users @admins




;[netlogon]
;   comment = Network Logon Service
;   path = /home/samba/netlogon
;   guest ok = yes
;   read only = yes
;[profiles]
;   comment = Users profiles
;   path = /home/samba/profiles
;   guest ok = no
;   browseable = no
;   create mask = 0600
;   directory mask = 0700

;[printers]
 ;  comment = All Printers
;   browseable = no
;   path = /var/tmp
;   printable = yes
;   guest ok = no
;   read only = yes
;   create mask = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
```

```
#[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
;   write list = root, @lpadmin
```

Quelques commandes clés :

● Créer un groupe système : $ groupadd groupname
● Créer un utilisateur système appartenant à ce groupe : $ useradd -m -g groupname username
-m pour créer le home directory et -g pour ajouter le groupe.
● Créer un compte SAMBA : $ smbpasswd -a username
➔ changer le propriétaire / groupe d'un répertoire : chown -R user:group directory
➔ changer les droits d'accès à un répertoire : chmod -R xxx directory (ex: xxx = 755

Dans le chemin suivant : /home
Vous allez retrouver les utilisateurs que vous avez crée :

```
adduser user1
adduser admin1
```

Dans le chemin suivant : /srv
Vous allez retrouver les groupes que vous avez crée :

```
groupadd admins
groupadd users
```

Ainsi mettre les comptes dans les bons groupe en écrivant les commandes suivantes :

```
sudo chown -R root:admin /srv/admins
sudo chown -R root:users /srv/users
```

Il faut aussi mettre les bons droits

```
chmod 760 /srv/admins
chmod 760 /srv/users
```

Voici comment doit être les droits des utilisateurs et des groupes :

```
drwxr-xr-x  5 root   root   4096 Nov  7 08:18 .
drwxr-xr-x 18 root   root   4096 Feb 23 12:43 ..
drwx------  2   1000 admin  4096 Nov  7 08:18 admin1
drwx------  2 admin1 admin1 4096 Nov  7 07:54 user1
drwx------  2 admin1 users  4096 Nov  7 08:18 users1
root@smb-priv:/home#
total 16
drwxr-xr-x  4 root root  4096 Nov  7 10:03 .
drwxr-xr-x 18 root root  4096 Feb 23 12:43 ..
drwxrw----  2 root admin 4096 Nov  7 10:02 admins
drwxrw----  2 root users 4096 Nov  7 10:03 users
root@smb-priv:/srv#
```

Ainsi dans le gestionnaire de fichier essayé de vous connectez au partage :

```
\\10.31.252.13\
```