

FSP 2

1. Active Directory	2
1.1) Hyperviseur de type 1 Proxmox	2
1.2) Domaine M2L3/DNS/DHCP	4
1.3) Profil itinérant	7
2. Serveurs Web & accessibilités à distance	11
2.1) Installation de GLPI	11
2.2) Installation de GLPI Agent sur les postes utilisateurs	15
2.3) Load balancer via HAProxy	16
2.3.1) Installation du package HAProxy	16
2.3.2) Configuration du fichier etc/haproxy/haproxy.cfg	16
2.3.3) Configuration du HAProxy sur le second serveur répartiteur de charge	17
2.3.4) Ajout d'un certificat	17
2.4) Redondance du load balancer	18
2.5) Routeur, switch et serveurs accessibles en SSH	19
3. Administration du routeur	23
Étape 1: Renommer le Routeur	23
Étape 2:Mettre un nom de domaine	23
Étape 3:Changer l'horodatage	23
Étape 4: Mettre une route par défaut	23
Étape 5 : Sécuriser l'accès à vos matériels	24
a) sécuriser l'accès au port console	24
b) sécuriser l'accès au enable	24
Étape 6: Mise en place du ssh	24
Étape 7:Préparation de l'installation du NAT overload	24
Étape 8: Configuration des interfaces virtuelles	24
Étape 9: Mise en place des ACL	25
4. Administration du switch	25
Étape 1:Renommer le Switch	25
Étape 2:Mettre un nom de domaine	25
Étape 3:Changer l'horodatage	25
Étape 4: Mettre une passerelle par défaut	25
Étape 5 : Sécuriser l'accès à vos matériels	26
Étape 6: Mise en place du ssh	26
Étape 7:Mise en place du VTP	26
Étape 8:Création des Vlans	26
Étape 9:Attribution d'un port à un Vlan	26
a) Access	26
b) Trunk :	27
Étape 10:Mettre une adresse IP(Adresse IP du switch dans le VLAN admin)	27
5. Serveur de téléphonie	27

5.1) Installation de Asterisk	27
5.2) Mise en place du VLAN Téléphonie	28
5.3) Création des utilisateurs	28
5.4) Création des boîtes vocales	30
5.5) Enregistrement DNS du serveur de téléphonie	30
5.6) Mise en place d'un message d'attente Installation des paquets nécessaires	31
5.7) IVR	32
5.8) Test	33
6. Analyse de paquets	34
6.1) Installation de Wireshark	34
6.2) Installation de NpCap afin de réaliser des captures	34
6.3) Sélection de l'interface réseau	35
6.4) Analyse de paquets sur notre infrastructure	35

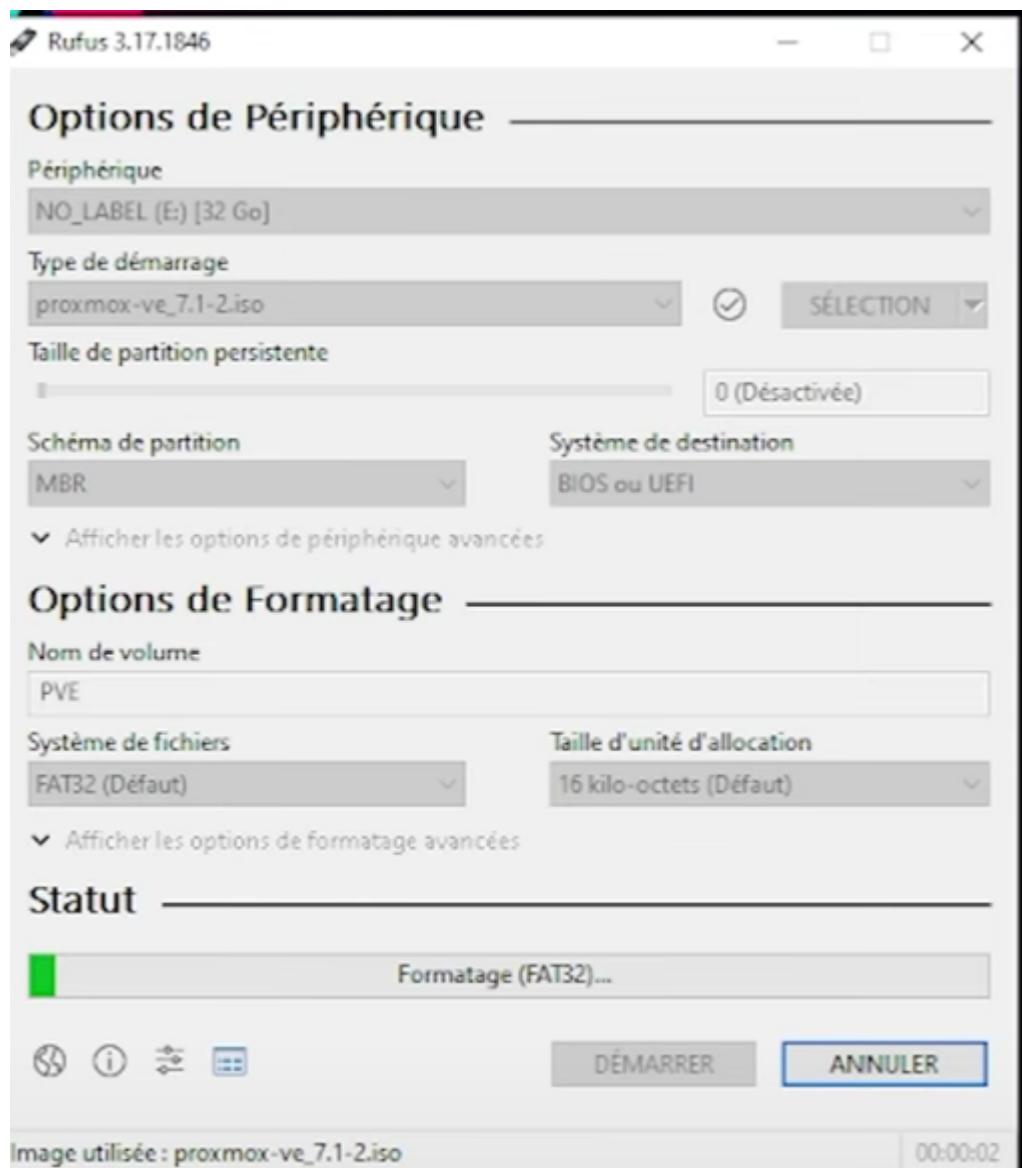
1. Active Directory

1.1) Hyperviseur de type 1 Proxmox

On sélectionne un ISO de Proxmox



On crée une clé bootable contenant Proxmox à l'aide du logiciel Rufus



On insère la clé USB qui contient Proxmox sur notre futur serveur.

Proxmox VE 7.1 (iso release 2) - <https://www.proxmox.com/>



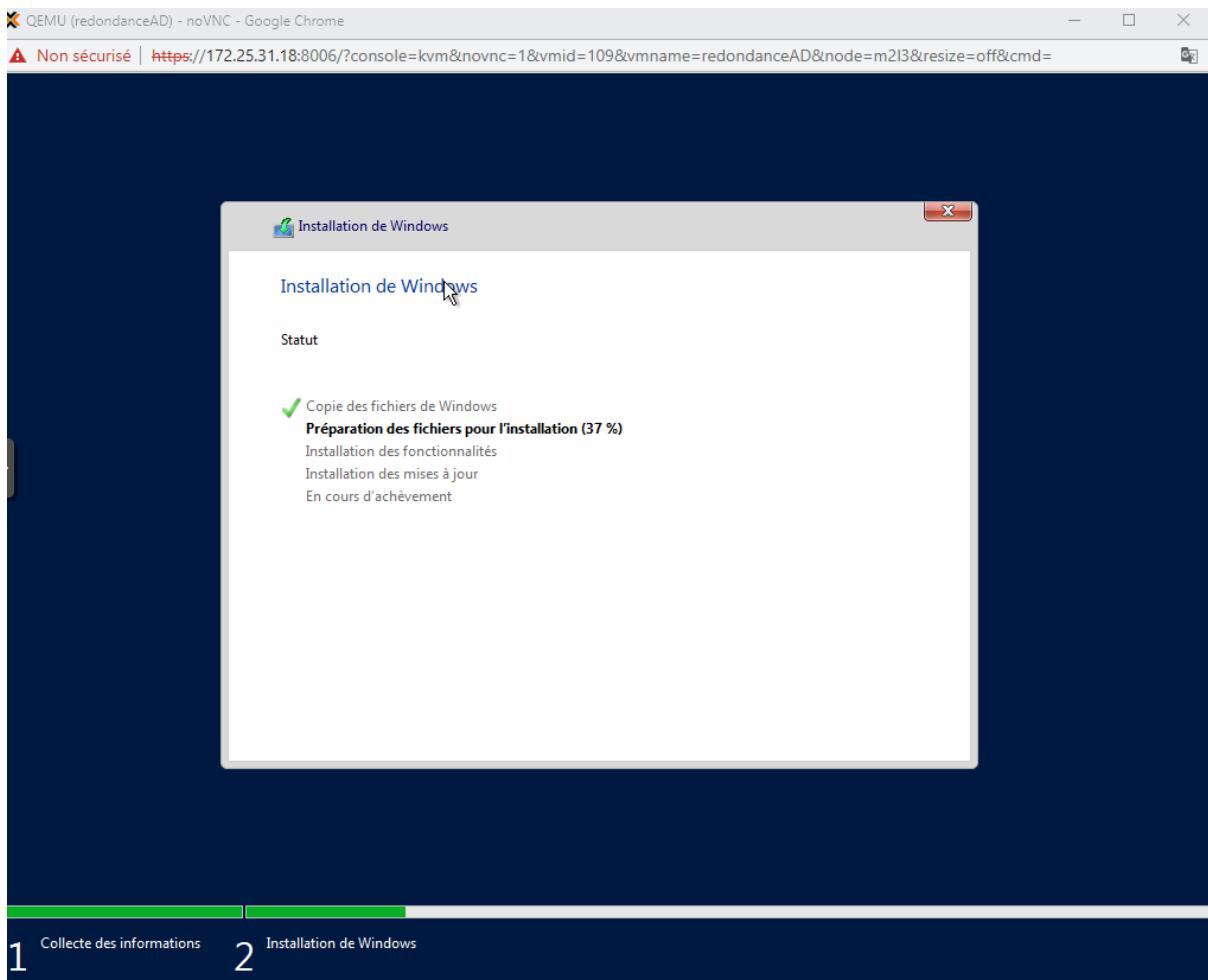
Install Proxmox VE
Install Proxmox VE (Debug mode)
Rescue Boot
Test memory (Legacy BIOS)

On sélectionne une adresse IP et on laisse l'installation se faire.

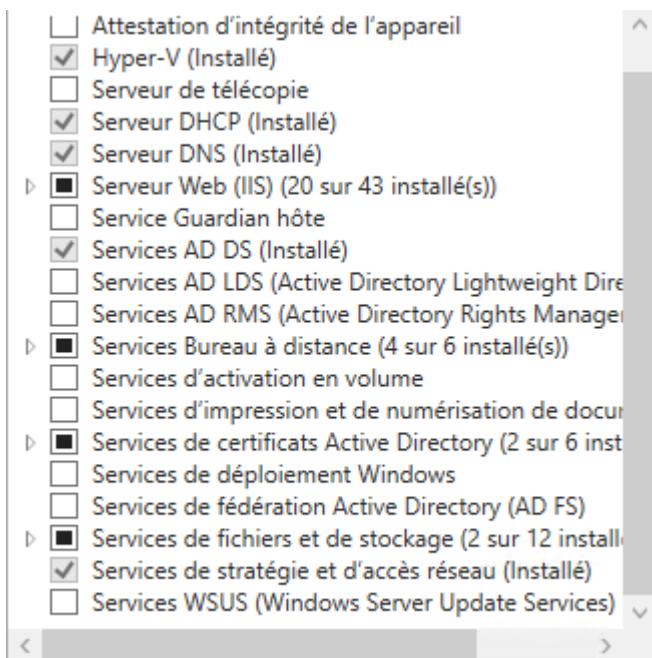
Une fois l'installation terminée, nous sommes prêts à créer des machines virtuelles.
Dorénavant, nous allons installer notre contrôleur de domaine.

1.2) Domaine M2L3/DNS/DHCP

Installation de Windows Server 2019



Installation des services AD/DNS/DHCP



Création du contrôleur de domaine

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
Principal-AD

Configuration de déploiement...

- Options du contrôleur de domaine
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configuration
- Installation
- Résultats

Sélectionner l'opération de déploiement

Ajouter un contrôleur de domaine à un domaine existant

Ajouter un nouveau domaine à une forêt existante

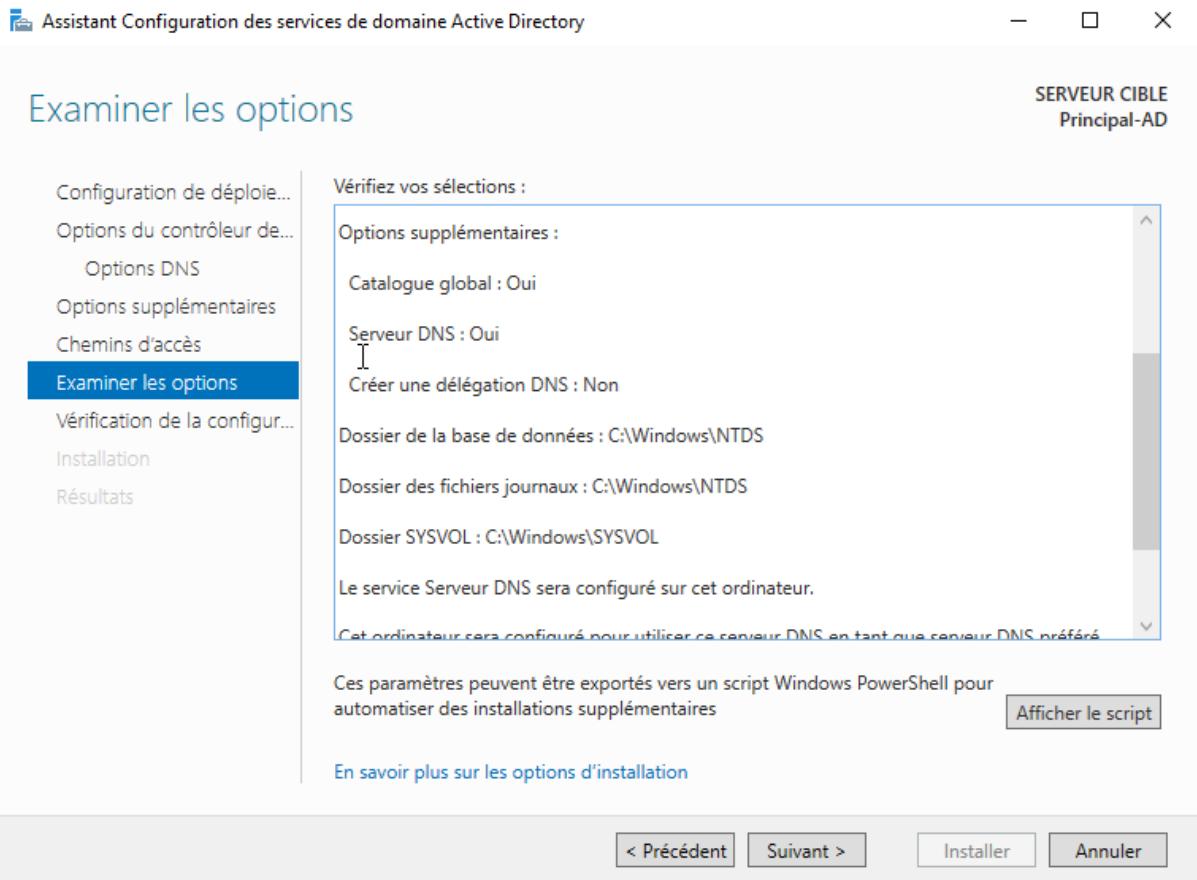
Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine : m2l3.lan

En savoir plus sur les configurations de déploiement

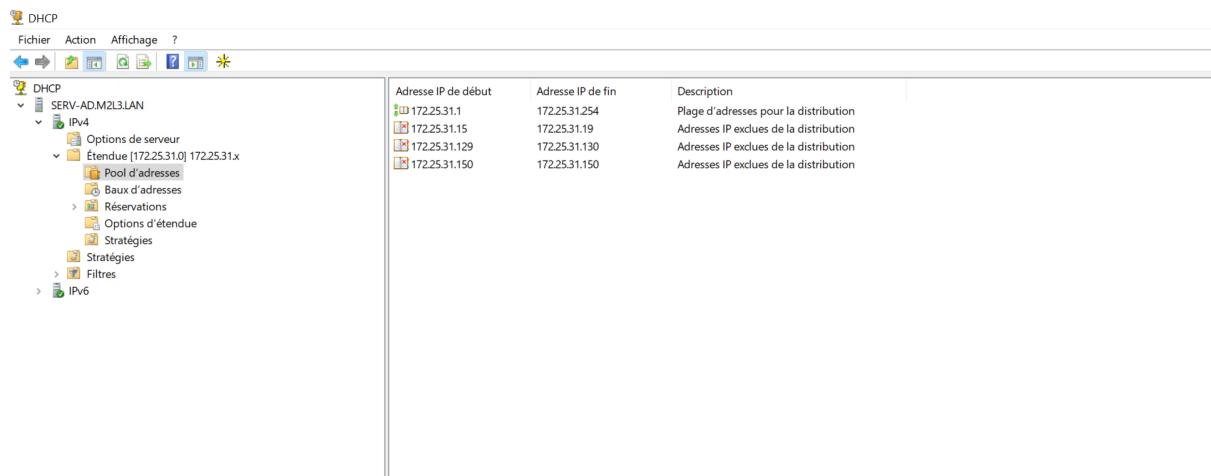
< Précédent Suivant > Installer Annuler



Création des utilisateurs

Nom	Type	Description	Fonction
Aidan Abbot	Utilisateur		Basket
Alan Carly	Utilisateur		Basket
Allen Fallon	Utilisateur		Basket
Alyssa Forrest	Utilisateur		Basket
Angelica Rebe...	Utilisateur		Basket
Aretha Illana	Utilisateur		Basket
Ashton Allegra	Utilisateur		Basket
Aurélien Gall.	Utilisateur		Administrateur
Avram Arma...	Utilisateur		Basket
Basia Calvin	Utilisateur		Basket
Bradley Otto	Utilisateur		Basket
Brendan Dris...	Utilisateur		Basket
Brenden Ger...	Utilisateur		Basket
Calvyn Morin	Utilisateur		Administrateur
Cameron Car...	Utilisateur		Basket
Carly Addison	Utilisateur		Basket
Carson Skyler	Utilisateur		Basket
Cathleen Bre...	Utilisateur		Handball
Chanda Jasper	Utilisateur		Handball
Charles Ori	Utilisateur		Handball
Charlotte Ne...	Utilisateur		Handball
Cheyenne D...	Utilisateur		Handball
Chiquita Gia...	Utilisateur		Handball
Chloe Sylves...	Utilisateur		Handball
Cole Simone	Utilisateur		Handball
Colorado Uta	Utilisateur		Handball
connecteurld...	Unité d'organis...		Handball
Darryl Evang...	Utilisateur		Handball
Eaton Elton	Utilisateur		Handball
Eaton Pi...	Utilisateur		Handball

Étendue DHCP



Enregistrement DNS

The screenshot shows the Windows Server DNS Management console. The left pane shows a tree structure with 'DNS' selected, followed by 'SERV-AD.M2L3.LAN', 'Zones de recherche directe' (selected), 'm2l3.lan' (selected), 'Zones de recherche inversée', and 'Redirecteurs conditionnel'. The right pane displays a table of registered hosts:

Nom	Type	Données	Horodateur
_msdcs	Source de nom (SOA)	[651] serv-ad.m2l3.lan, hos...	statique
_sites	Serveur de noms (NS)	serv-ad.m2l3.lan.	statique
_tcp	Hôte (A)	172.25.31.129	04/05/2023 08:00:00
_udp	Hôte (A)	172.25.31.125	statique
DomainDnsZones	Hôte (A)	172.25.31.12	20/04/2023 06:00:00
ForestDnsZones	Hôte (A)	172.25.31.150	statique
(identique au dossier parent)	Hôte (A)	172.25.31.16	statique
(identique au dossier parent)	Hôte (A)	172.25.31.17	statique
asterisk	Hôte (A)	172.25.31.13	09/05/2023 11:00:00
DESKTOP-U7C1CR1	Hôte (A)	172.25.31.5	04/05/2023 08:00:00
glpi	Hôte (A)	172.25.31.10	statique
glpi1	Hôte (A)	172.25.31.130	10/05/2023 10:00:00
glpi2	Hôte (A)	172.25.31.129	statique
Hugo	Hôte (A)	172.25.31.12	statique
PC-CALVYN	Hôte (A)	172.25.31.1	statique
pfSense	Hôte (A)	172.25.31.99	statique
Redondance-AD	Hôte (A)	172.25.31.12	statique
serv-ad	Hôte (A)	172.25.31.12	statique
tplinkap	Hôte (A)	172.25.31.12	statique
zabbix	Hôte (A)	172.25.31.12	statique

1.3) Profil itinérant

▶ Profils Itinérants - Windows Server 2019

Création d'un dossier Profil itinérant sur le disque C de notre contrôleur de domaine

```
Foreach($User in $Users){
    $ProfilePath = "\CPD01\Profils_itinerants\$"
    $Profilepath = $ProfilePath + $User.samaccountname
    $HomeDirectory = "\CPD01\Utilisateurs\$"
    $Homedirectory = $HomeDirectory + $User.samaccountname
    Set-ADUser $User.samaccountname -ProfilePath $ProfilePath -HomeDirectory
    $HomeDirectory -HomeDrive U}
```

Environnement	Sessions	Contrôle à distance	Profil des services	Bureau à distance	COM
Général	Adresse	Compte	Profil	Téléphones	Organisation

Profil utilisateur

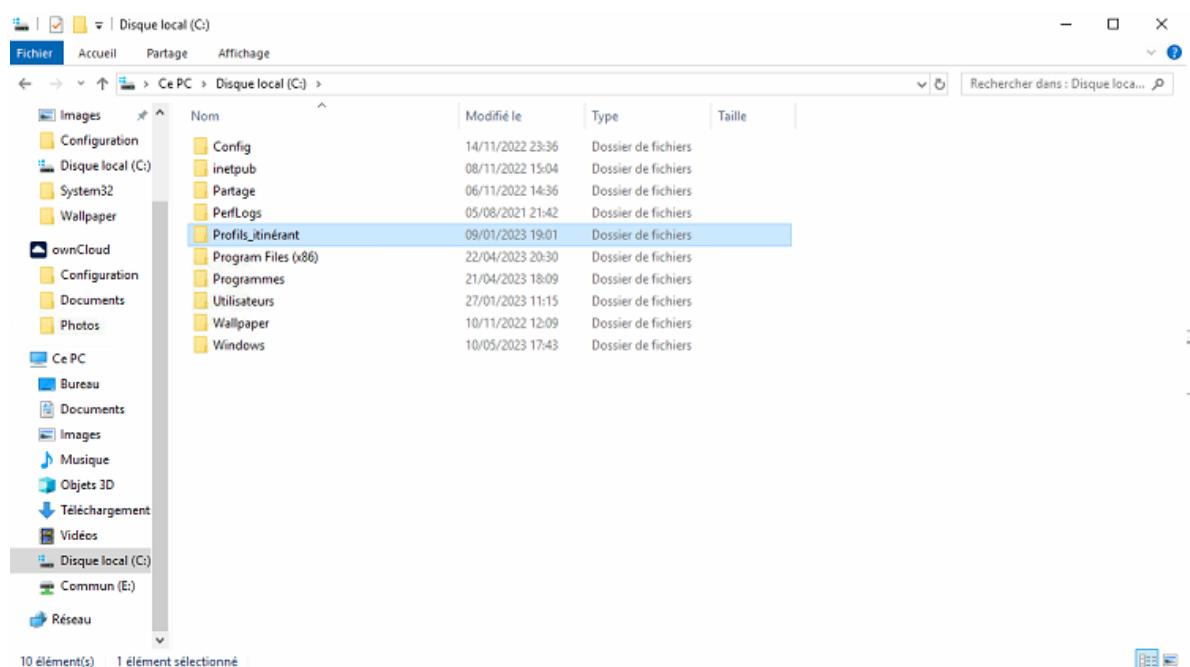
Chemin du profil :

Script d'ouverture de session :

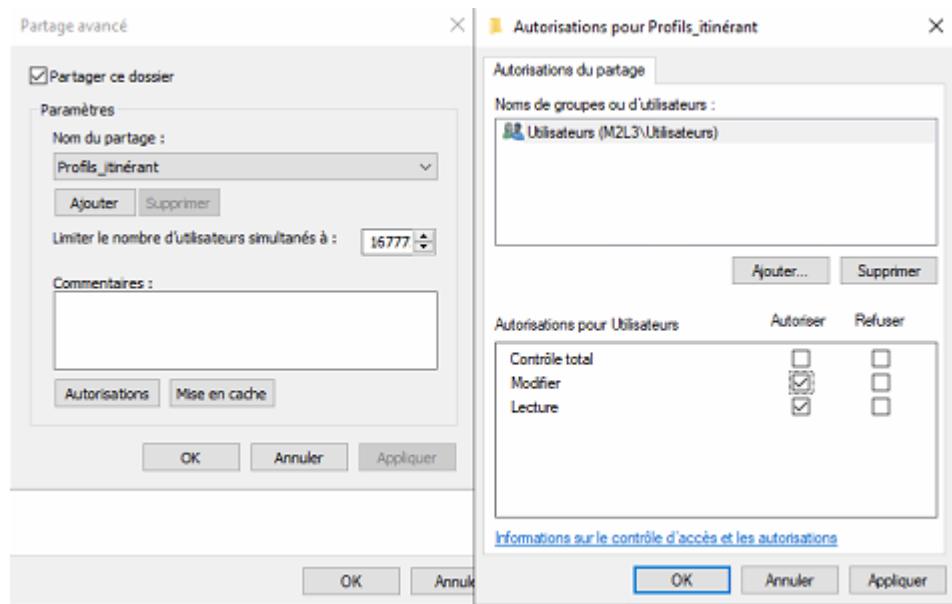
Dossier de base

Chemin d'accès local :

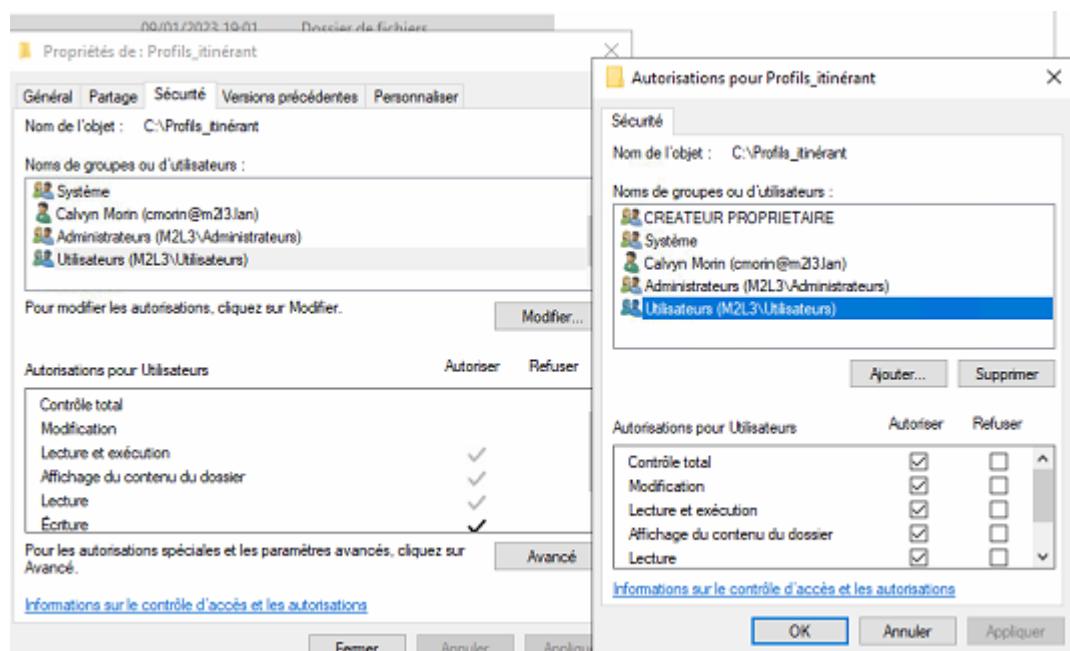
Connecter : U: à :



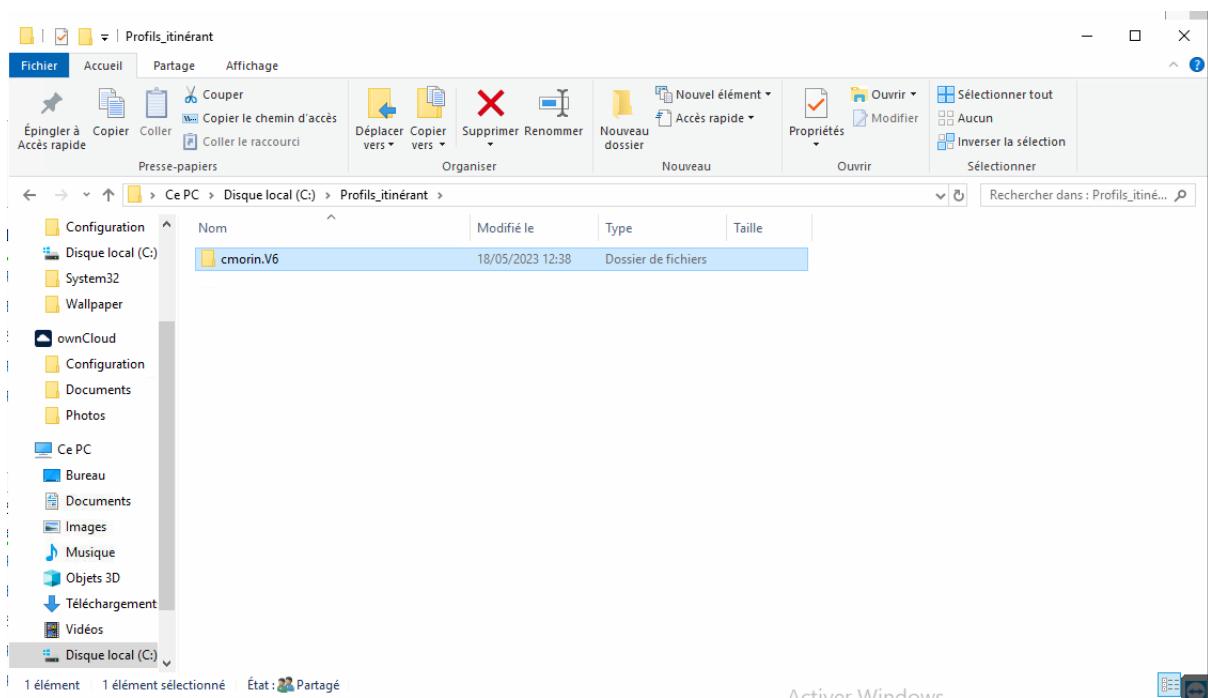
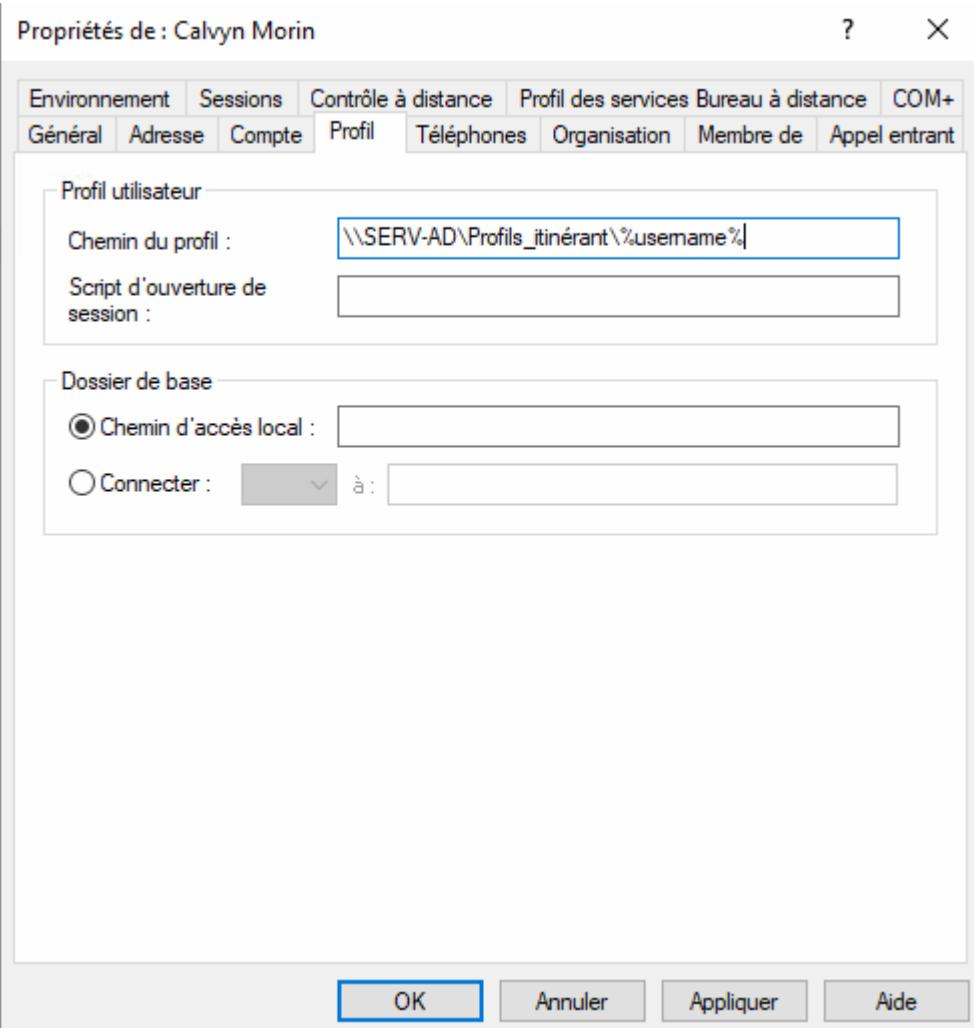
Partage du dossier Profil itinérant aux utilisateurs



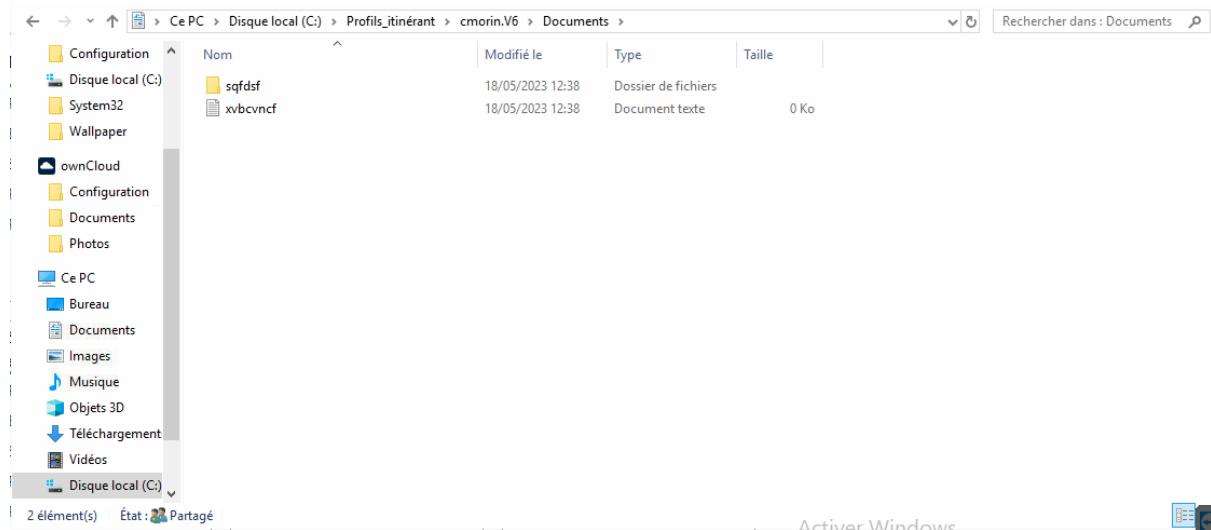
Permissions NTFS



Ensuite, on doit lier le dossier que l'on vient de créer à nos utilisateurs.



Les documents créés sur la session de l'utilisateur sont disponibles sur le profil itinérant.



2. Serveurs Web & accessibilités à distance

2.1) Installation de GLPI

Installation de Perl

```
root@glpi1:~# apt install perl -y
```

Installation des dépendances PHP

```
root@glpi1:~# apt install php-ldap php-imap php-apcu php-xmlrpc php-cas php-mysqli php-mbstring php-curl php-gd php-simplexml php-xml php-intl php-zip php-bz2 -y
```

Installation d'Apache

```
root@glpi1:~# apt install apache2
```

On redémarre le service Apache

```
root@glpi1:~# systemctl reload apache2
```

On télécharge les paquets de GLPI

```
root@glpi1:/tmp# wget https://github.com/glpi-project/glpi/releases/download/10.0.7/glpi-10.0.7.tgz
```

On les décomprime

```
root@glpi1:/tmp# tar xzf glpi-10.0.7.tgz -C /var/www/html
```

On accorde les droits aux fichiers de GLPI

```
root@glpi1:/tmp# chown -R www-data:www-data /var/www/html/glpi
root@glpi1:/tmp# chmod -R 775 /var/www/html/glpi
```

On installe MariaDB

```
root@glpi1:/tmp# apt install mariadb-server
```

Création de la BDD glpidb

```
root@glpi1:/tmp# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.5.19-MariaDB-0+deb11u2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database glpidb;
```

Création de l'utilisateur glpiuser

```
MariaDB [(none)]> create user glpiuser@localhost identified by '1234';
Query OK, 0 rows affected (0,004 sec)
```

On accorde tous les privilèges à l'utilisateur glpiuser sur la BDD glpidb

```
MariaDB [(none)]> grant all privileges on glpidb.* to glpiuser@localhost;
```

```
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0,000 sec)
```

Installation de GLPI



glpi

GLPI SETUP

Étape 1

Configuration de la connexion à la base de données

Serveur SQL (MariaDB ou MySQL)

localhost

Utilisateur SQL

glpiuser

Mot de passe SQL

••••

Continuer >

This screenshot shows the first step of the GLPI setup process. The title 'GLPI SETUP' is at the top right. Below it, 'Étape 1' and 'Configuration de la connexion à la base de données' are displayed. There are three input fields: 'Serveur SQL (MariaDB ou MySQL)' containing 'localhost', 'Utilisateur SQL' containing 'glpiuser', and 'Mot de passe SQL' containing four redacted dots. A yellow 'Continuer >' button is at the bottom.

← → C ⚠ Non sécurisé | 172.25.31.17/install/install.php

Raccourci serveurs

glpi

GLPI SETUP

Étape 2

Test de connexion à la base de données

Connexion à la base de données réussie

Veuillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

glpi

Continuer >

This screenshot shows the second step of the GLPI setup process. The title 'GLPI SETUP' is at the top right. Below it, 'Étape 2' and 'Test de connexion à la base de données' are displayed. A green box indicates 'Connexion à la base de données réussie'. Below this, there's a section for selecting a database: 'Veuillez sélectionner une base de données :' with 'Créer une nouvelle base ou utiliser une base existante :'. Two options are shown: one with an empty input field and one with 'glpi' selected. A yellow 'Continuer >' button is at the bottom.

Non sécurisé | 172.25.31.16/front/central.php

Raccourci serveurs

GLPI

Accueil

Tableau de bord

- Pour des raisons de sécurité, veuillez changer le mot de passe par défaut pour le(s) utilisateur(s) : glpi post-only tech normal
- Pour des raisons de sécurité, veuillez supprimer le fichier : install/install.php
- La configuration du dossier racine du serveur web n'est pas sécurisée car elle permet l'accès à des fichiers non publics. Référez-vous à la documentation d'installation pour plus de détails.

Central

Logiciel (0), Ordinateur (0), Matériel réseau (0), Téléphone (0), Licence (0), Moniteur (0), Balle (0), Imprimante (0)

Aucune donnée trouvée

Ordinateurs par Fabricant, Moniteurs par Modèle, Matériels réseau par Type

Utilisateurs (4), Groupe (0), Fournisseur (0), Document (0), Entité (1), Profils (8), Base de connaissance (0), Projet (0)

Statuts des tickets par mois

Ticket (0), Tickets en retard (0), Problème (0), Changement (0)

Aucune donnée trouvée

Aucune donnée trouvée

Aucune donnée trouvée

Aucune donnée trouvée

Non sécurisé | 172.25.31.16/front/ticket.php

Raccourci serveurs

GLPI

Accueil / Assistance / Tickets / + Ajouter / Rechercher / Listes / Gabarits / Kanban global / Tickets attendant votre validation

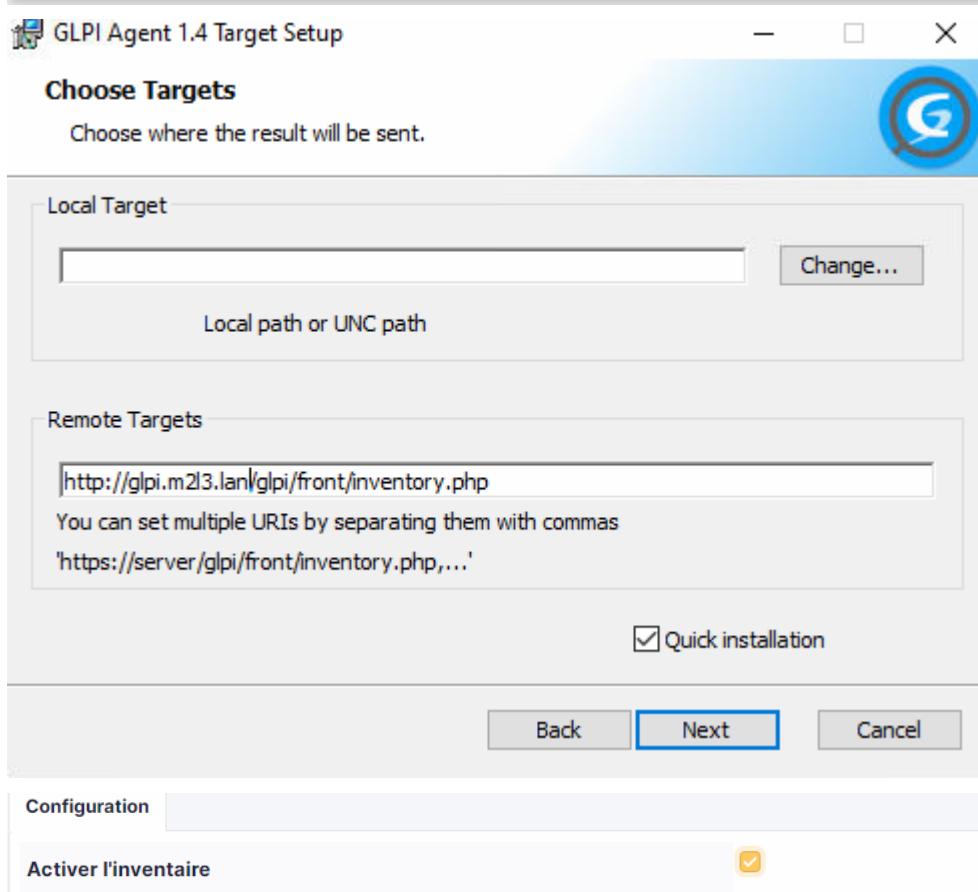
Rechercher / Super-Admin, Utilité racine (Arborescence) [0]

1 Ticket	0 Tickets entrants	0 Tickets en attente	1 Tickets assignés	0 Tickets planifiés	0 Tickets résolus	0 Tickets fermés			
Caractéristiques - Statut est Non résolu									
Actions									
ID	TITRE	STATUT	DERNIÈRE MODIFICATION	DATE D'OUVERTURE	PRIORITÉ	DEMANDEUR - DEMANDEUR	ATTRIBUÉ À - TECHNICIEN	CATÉGORIE	TTR
1	sallut	En cours (Attribué)	2023-05-17 11:11	2023-05-17 11:11	Moyenne	glpi i	glpi i		

20 lignes / page

De 1 à 1 sur 1 lignes

2.2) Installation de GLPI Agent sur les postes utilisateurs



2.3) Load balancer via HAProxy

2.3.1) Installation du package HAProxy

```
calvyn@HaProxy:~$ apt install haproxy
```

2.3.2) Configuration du fichier etc/haproxy/haproxy.cfg

On utilise l'algorithme round robin pour équilibrer la charge sur les serveurs Web. Le serveur va acheminer les requêtes sur les serveurs à tour de rôle, un à un.

Dans la partie back_end, on entre l'adresse IP de nos serveurs Web.

```
GNU nano 5.4                               /etc/haproxy/haproxy.cfg

global
  log  /dev/log  local0 notice
  log  /dev/log  local1 notice
  chroot /var/lib/haproxy
  stats socket /run/haproxy/admin.sock mode 660 level admin expose-fd listeners
  stats timeout 30s
  user haproxy
  group haproxy
  daemon

# Default SSL material locations
ca-base /etc/ssl/certs
crt-base /etc/ssl/private

# See: https://ssl-config.mozilla.org/#server=haproxy&version=2.0_36config-intermediate
ssl-default-bind-ciphersuites TLS_AES_128_GCM_SHA256:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256:TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384:TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_ECDHE_RSA_CHACHA20_POLY1305
ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets

defaults
  log     global
  mode    http
  option  httplog
  option  dontlognull
  timeout connect 5000
  timeout client  50000
  timeout server  50000
  errorfile 400 /etc/haproxy/errors/400.http
  errorfile 401 /etc/haproxy/errors/401.http
  errorfile 403 /etc/haproxy/errors/403.http
  errorfile 408 /etc/haproxy/errors/408.http
  errorfile 500 /etc/haproxy/errors/500.http
  errorfile 502 /etc/haproxy/errors/502.http
  errorfile 503 /etc/haproxy/errors/503.http
  errorfile 504 /etc/haproxy/errors/504.http

frontend http_haproxy
  bind *:80
  mode http
  default_backend http_roundrobin

backend http_roundrobin
  balance roundrobin
  server gpli2 172.25.31.17
  server gpli1 172.25.31.16
```

2.3.3) Configuration du HAProxy sur le second serveur répartiteur de charge

```

Global
    log /dev/log local0
    log /dev/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin expose-fd list
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

    # Default SSL material locations
    ca-base /etc/ssl/certs
    crt-base /etc/ssl/private

    # See: https://ssl-config.mozilla.org/#server=haproxy&server-version=2.0
    ssl-default-bind-ciphers ECDHE-ECDSA-AES128-GCM-SHA256;ECDHE-RSA-AES128-
    ssl-default-bind-ciphersuites TLS_AES_128_GCM_SHA256;TLS_AES_256_GCM_SHA384
    ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
    timeout server 50000
    errorfile 400 /etc/haproxy/errors/400.http
    errorfile 403 /etc/haproxy/errors/403.http
    errorfile 408 /etc/haproxy/errors/408.http
    errorfile 500 /etc/haproxy/errors/500.http
    errorfile 502 /etc/haproxy/errors/502.http
    errorfile 503 /etc/haproxy/errors/503.http
    errorfile 504 /etc/haproxy/errors/504.http

frontend http_haproxy
    bind *:80
    mode http
    default_backend http_roundrobin

backend http_roundrobin
    balance roundrobin
    server glpi2 172.25.31.16
    server glpi1 172.25.31.17

calvyn@RedondanceHAProxy: ~
GNU nano 5.4          /etc/haproxy/haproxy.cfg *
timeout connect 5000
timeout client 50000
timeout server 50000
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
errorfile 502 /etc/haproxy/errors/502.http
errorfile 503 /etc/haproxy/errors/503.http
errorfile 504 /etc/haproxy/errors/504.http

frontend http_haproxy
    bind *:80
    mode http
    default_backend http_roundrobin

backend http_roundrobin
    balande roundrobin
    server glpi1 172.25.31.16
    server glpi2 172.25.31.17

```

2.3.4) Ajout d'un certificat

```

root@HaProxy:/etc/ssl/m2l3.lan# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/m2l3.lan.key -out /etc/ssl/m2l3.lan.crt
Generating a RSA private key
.....+++++
writing new private key to '/etc/ssl/m2l3.lan.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields, there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:HR
Locality Name (eg, city) []:MTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:m2l3.lan
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:glpi.m2l3.lan
Email Address []:calvyn.morin@gmail.com
root@HaProxy:/etc/ssl/m2l3.lan#

```

```

root@HaProxy:/etc/ssl/m2l3.lan# cat m2l3.lan.crt m2l3.lan.key > m2l3.lan.pem
root@HaProxy:/etc/ssl/m2l3.lan# ls -l
total 16
-rw-r--r-- 1 root root 1415 18 mai 15:28 '^cl3.lan.crt'
-rw-r--r-- 1 root root 1415 18 mai 15:29 m2l3.lan.crt
-rw----- 1 root root 1704 18 mai 15:29 m2l3.lan.key
-rw-r--r-- 1 root root 3119 18 mai 15:30 m2l3.lan.pem
root@HaProxy:/etc/ssl/m2l3.lan#

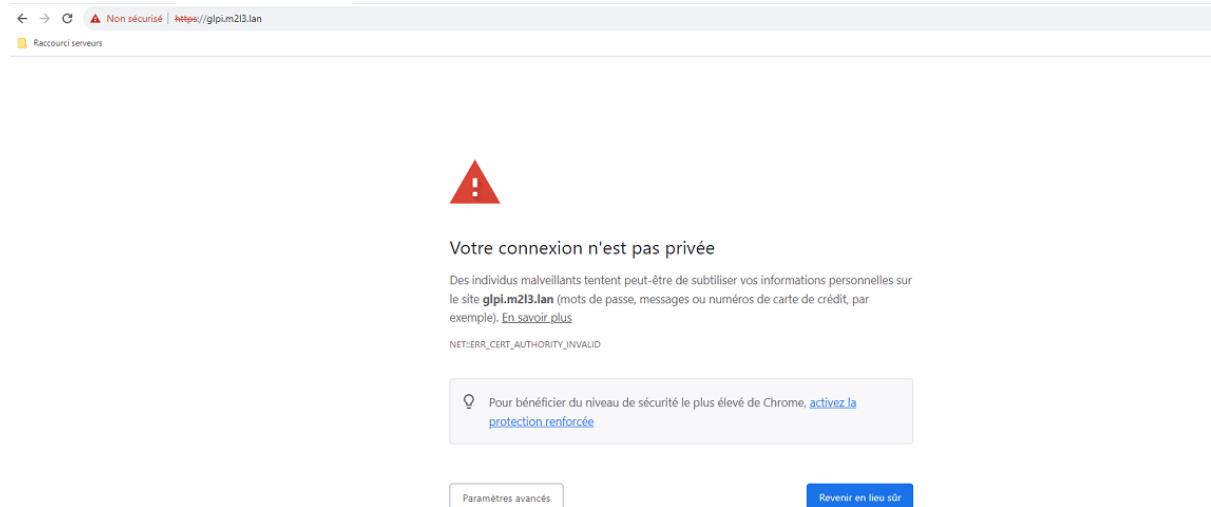
```

On modifie le fichier /etc/haproxy/haproxy.cfg

```

frontend http_haproxy
    bind *:80
    bind *:443 ssl crt /etc/ssl/m2l3.lan/m2l3.lan.pem
    redirect scheme https if !{ ssl_fc }
    mode http
    acl http ssl_fc,not
    acl https ssl_fc
    http-request set-header X-Forwarded-Protocol http if http
    http-request set-header X-Forwarded-Protocol https if https
    default_backend http_roundrobin

```



2.4) Redondance du load balancer

- Setup Active-Passive Cluster with Keepalived & HAProxy (Two raspberry pis)
On installe le service KeepAlive.

calvyn@RedondanceHAProxy:~\$ sudo apt install keepalived

On initie une instance VRRP

```
calvyn@RedondanceHAProxy:~$ nano /etc/keepalived/keepalived.conf
GNU nano 5.4                               /etc/keepalived/keepalived.conf
vrrp_instance pi1 {
    state BACKUP
    interface ens18
    virtual_router_id 101
    priority 200
    virtual_ipaddress{
        172.25.31.152
    }
}
```

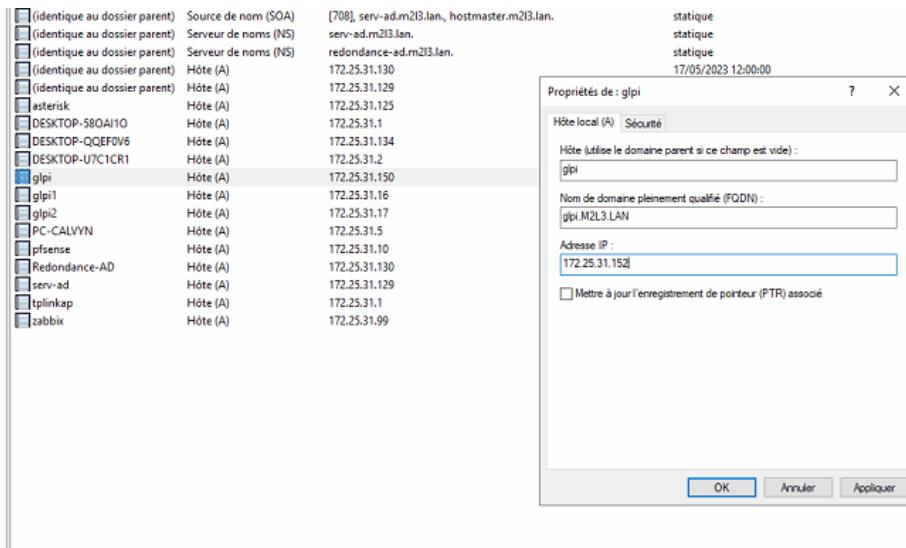
The terminal shows the configuration of a VRRP instance named "pi1" in the file "/etc/keepalived/keepalived.conf". The configuration includes setting the interface to "ens18", the virtual router ID to 101, a priority of 200, and a virtual IP address of 172.25.31.152. The terminal window has a status bar at the bottom with French keyboard shortcuts for various functions like Help, Write, Find, Cut, Paste, and Justify.

root@RedondanceHAProxy:/home/calvyn# systemctl restart keepalived

On fait la même chose sur le serveur HAProxy principal.

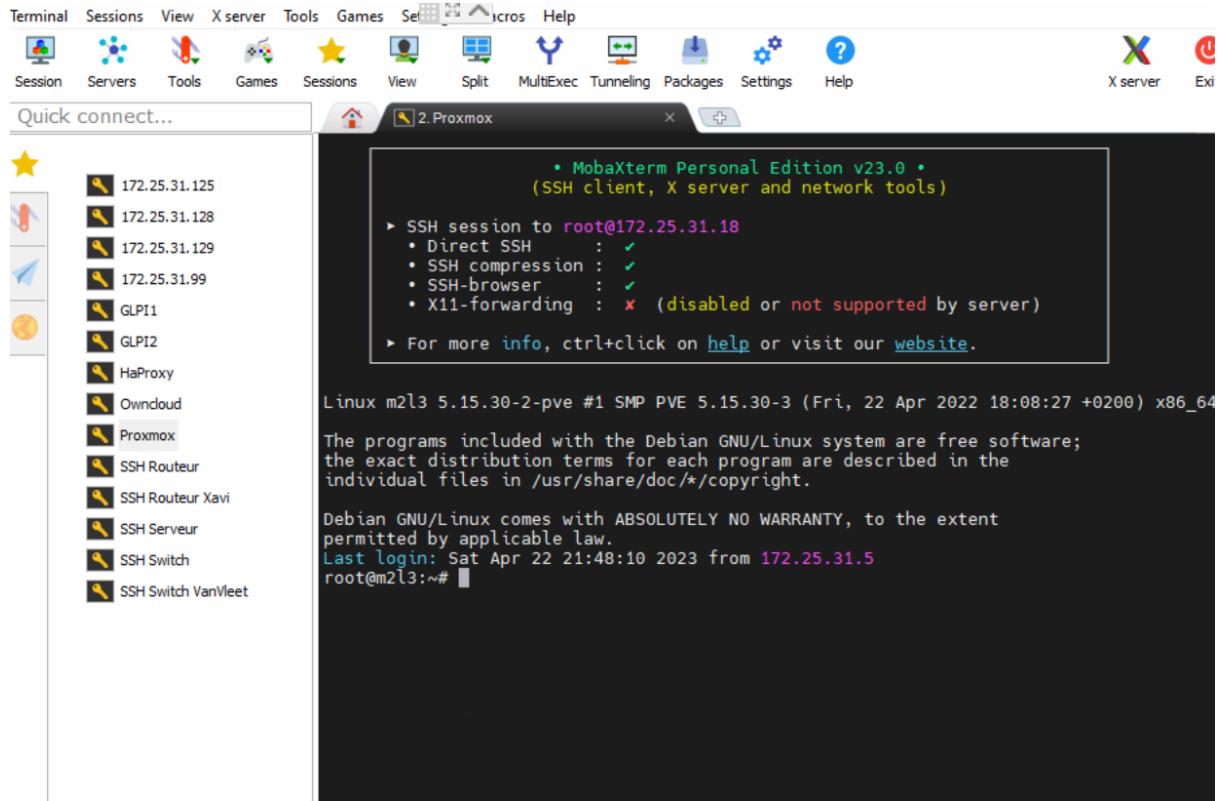
```
GNU nano 5.4
vrrp_instance haproxy {
    state MASTER
    interface ens18
    virtual_router_id 101
    priority 220
    virtual_ipaddress{
        172.25.31.152
    }
}
```

L'adresse VIP est 172.25.31.152. Cette adresse doit être renseignée dans notre DNS.



2.5) Routeur, switch et serveurs accessibles en SSH

Proxmox :



HaProxy :

```
C:\Users\calvy>ssh calvyn@172.25.31.150
calvyn@172.25.31.150's password:
Linux HaProxy 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May  9 14:36:31 2023 from 172.25.31.5
calvyn@HaProxy:~$
```

GLPI1 :

```
• MobaXterm Personal Edition v22.3 •
(SSH client, X server and network tools)

► SSH session to calvyn@172.25.31.16
• Direct SSH      : ✓
• SSH compression : ✓
• SSH-browser    : ✓
• X11-forwarding : ✓ (remote display is forwarded through SSH)

► For more info, ctrl+click on help or visit our website.
```

Linux glpi1 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Tue May 9 14:37:06 2023 from 172.25.31.5
calvyn@glpi1:~\$ █

GLPI2:

```
• MobaXterm Personal Edition v22.3 •
(SSH client, X server and network tools)

► SSH session to calvyn@172.25.31.17
• Direct SSH      : ✓
• SSH compression : ✓
• SSH-browser    : ✓
• X11-forwarding : ✓ (remote display is forwarded through SSH)

► For more info, ctrl+click on help or visit our website.
```

Linux glpi2 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

You have new mail.

Last login: Tue May 9 14:37:04 2023 from 172.25.31.5
calvyn@glpi2:~\$ █

Asterisk :

calvyn@asterisk: /etc/ssh

```
GNU nano 5.4          sshd_config *
```

```
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^_ Aller ligne

```
root@asterisk:/etc/ssh# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-05-18 15:07:57 CEST; 4s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
     Process: 2696 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 2697 (sshd)
      Tasks: 1 (limit: 4617)
     Memory: 1.0M
        CPU: 23ms
       CGroup: /system.slice/ssh.service
               └─2697 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

mai 18 15:07:57 asterisk systemd[1]: Starting OpenBSD Secure Shell server...
mai 18 15:07:57 asterisk sshd[2697]: Server listening on 0.0.0.0 port 22.
mai 18 15:07:57 asterisk sshd[2697]: Server listening on :: port 22.
mai 18 15:07:57 asterisk systemd[1]: Started OpenBSD Secure Shell server.
```

lines 1-17/17 (END)

```
• MobaXterm Personal Edition v23.0 •
(SSH client, X server and network tools)

▶ SSH session to calvyn@172.25.31.125
  • Direct SSH      : ✓
  • SSH compression : ✓
  • SSH-browser     : ✓
  • X11-forwarding  : ✓ (remote display is forwarded through SSH)

▶ For more info, ctrl+click on help or visit our website.
```

Linux asterisk 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Apr 16 11:57:56 2023 from 172.25.31.1
calvyn@asterisk:~\$ █

3. Administration du routeur

Étape 1: Renommer le Routeur

```
Routeur>enable
Routeur#configure terminale
Routeur(config):hostname Giroud (dans mon cas j'utiliserais le nom Giroud)
```

Étape 2:Mettre un nom de domaine

```
Giroud(config):ip domain-name m2l3.lan
```

Étape 3:Changer l'horodatage

```
Giroud(config):clock set hh:mn:sc month day year
Giroud#Show clock (permet de voir l'horodatage)
```

Étape 4: Mettre une route par défaut

```
Giroud(config): ip route 0.0.0.0 0.0.0.0 (votre passerelle)
La route 0.0.0.0 0.0.0.0 correspond à la route par défaut.
```

Étape 5 : Sécuriser l'accès à vos matériels

a) sécuriser l'accès au port console

```
Giroud(config):username (nom du matériel) secret (MotdePasse Choisit)
line console 0
login local
```

b) sécuriser l'accès au enable

```
Giroud(config):enable secret (MotdePasse Choisit)
```

La commande secret permet de rendre illisible vos mots de passes si on voit votre configuration

Étape 6: Mise en place du ssh

```
Giroud(config):crypto key generate rsa general-keys modulus 1024
ip ssh version 2
line vty 0 4
login local
transport input ssh
```

Étape 7:Préparation de l'installation du NAT overload

```
Giroud(config):access-list 2 permit 172.25.0.0 0.0.0.255.255
ip nat inside source list 2 int gig0/0 overload
```

Étape 8: Configuration des interfaces virtuelles

On commence par l'interface relié à la prise RJ45

```
Giroud(config):Int gi 0/0
ip address dhcp OU ip address static
ip nat outside
no shutdown
```

Le switch que j'utiliserais sera connecté sur le port Gi0/2

```
Giroud(config):Int Gi 0/2.100    <- le .100 de l'interface représente le vlan ou l'on
                                attribuera l'interface
Encapsulation dot1Q 100
ip address (l'adresse choisie) (masque choisi)
ip nat inside
```

no shutdown

Étape 9: Mise en place des ACL

```
Router(config)#access-list 2 deny 10.1.2.0 0.0.0.255
```

```
Router(config)#access-list 2 permit 10.1.3.0 0.0.0.255
```

```
Router(config)#interface gigabitEthernet 0/2
```

```
Router(config-if)# ip access-group 2 out
```

Le "2" étant le numéro de l'ACL créée à la première étape, et "out" signifie que la règle s'applique sur les paquets sortants de l'interface.

4. Administration du switch

Étape 1:Renommer le Switch

```
Switch>enable
```

```
Switch#configure terminale
```

```
Switch(config):hostname Zizou
```

Étape 2:Mettre un nom de domaine

```
Zizou(config):ip domain-name m2l3.lan
```

Étape 3:Changer l'horodatage

```
Zizou(config):clock set hh:mn:sc month day year
```

Étape 4: Mettre une passerelle par défaut

```
ip default-gateway 172.25.31.23
```

```
Zizou(config): ip default-gateway (l'adresse ip de votre routeur)
```

Étape 5 : Sécuriser l'accès à vos matériels

a)sécuriser l'accès au port console

```
Zizou(config):username (nom du matériel) secret (MotdePasse Choisit)
line console 0
login local
```

b)sécuriser l'accès au enable

```
Zizou(config):enable secret (MotdePasse Choisit)
```

Étape 6: Mise en place du ssh

```
Zizou(config):crypto key generate rsa general-keys modulus 1024
ip ssh version 2
line vty 0 4
login local
transport input ssh
```

Étape 7:Mise en place du VTP

Switch coeur de réseau:

```
Zizou(config):VTP domain m2l3.lan
Zizou(config):VTP mode server
Zizou(config):VTP version 2
```

Autres switch:

```
Switch(config)#: VTP domain m2l3.lan
Switch(config)#: VTP mode client
Switch(config)#: VTP version 2
```

Étape 8:Création des Vlans

```
Zizou(config):vlan (numéro du vlan choisi)
Zizou(config):name (nom du vlan choisis)
```

Étape 9:Attribution d'un port à un Vlan

a) Access

```
Zizou(config):Interface (Numéro de l'interface(n°port) que l'on veut utiliser pour le vlan)
Zizou(config-if):switchport mode access
Zizou(config-if):switchport access vlan (N° du vlan)
```

Zizou(config):no shutdown

b) Trunk :

Zizou(config):Interface GigabitEthernet0/1(n° de l'interface)

Zizou(config):switchport mode trunk

Étape 10:Mettre une adresse IP(Adresse IP du switch dans le VLAN admin)

```
interface Vlan400
| ip address 172.25.31.29 255.255.255.128
```

Zizou(config):interface(n° du Vlan administrateur)

Zizou(config-if):ip address (votre adresse ip) (votre masque)

5. Serveur de téléphonie

5.1) Installation de Asterisk

```
root@asterisk:/usr/share/asterisk/agi-bin# apt install asterisk
```

Téléchargement d'une voix de synthèse

```
root@asterisk:/usr/share/asterisk/agi-bin# wget https://github.com/zaf/asterisk-goolletts/tarball/master
--2023-04-16 11:48:03--  https://github.com/zaf/asterisk-goolletts/tarball/master
Résolution de github.com (github.com)... 140.82.121.3
Connexion à github.com (github.com)|140.82.121.3|:443... connecté.
requête HTTP transmise, en attente de la réponse... 302 Found
Emplacement : https://codeload.github.com/zaf/asterisk-goolletts/legacy.tar.gz/refs/heads/master [suivant]
--2023-04-16 11:48:03--  https://codeload.github.com/zaf/asterisk-goolletts/legacy.tar.gz/refs/heads/master
Résolution de codeload.github.com (codeload.github.com)... 140.82.121.9
Connexion à codeload.github.com (codeload.github.com)|140.82.121.9|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : non indiqué [application/x-gzip]
Sauvegarde en : « master »

master                                [ =>                                         ] 17,06K  ---KB/s   ds 0,02s
2023-04-16 11:48:04 (787 KB/s) - « master » sauvegardé [17467]
root@asterisk:/usr/share/asterisk/agi-bin#
```

Téléchargement des éléments audios supplémentaires

```
root@asterisk:~# apt install perl libwww-perl sox mpg123
```

5.2) Mise en place du VLAN Téléphonie

5.3) Création des utilisateurs

```
[general]
hasvoicemail = yes
hassip = yes
hasiax = yes
callwaiting = yes
threeewaycalling = yes
callwaitingcallerid = yes
transfer = yes
canpark = yes
cancallforward = yes
callreturn = yes
callgroup = 1
pickupgroup = 1
nat = yes
```

```
[3001]
type=friend
host=dynamic
dtmfmode=rfc2833
disallow=all
allow=ulaw
fullname=John DOE
username=jdoe
secret=jdoe
context=m2l3
```

```
[3002]
type=friend
host=dynamic
dtmfmode=rfc2833
disallow=all
allow=ulaw
fullname=Calvyn MORIN
username=cmorin
secret=cmorin
context=m2l3
```

```
[3003]
type=friend
host=dynamic
dtmfmode=rfc2833
disallow=all
allow=ulaw
fullname=Aurelien GALLEZ
username=agallez
secret=agallez
context=m2l3
```

```
[3004]
type=friend
host=dynamic
dtmfmode=rfc2833
disallow=all
allow=ulaw
fullname=Sami BOURGOIN
```

5.4) Création des boîtes vocales

```
[m2l3]
exten => _3XXX,1,Dial(SIP/${EXTEN},20)
exten => _3XXX,2,VoiceMail(${EXTEN}@m2l3)

exten => 3999,1,VoiceMailMain(${CALLERID(num)}@m2l3,s)
```

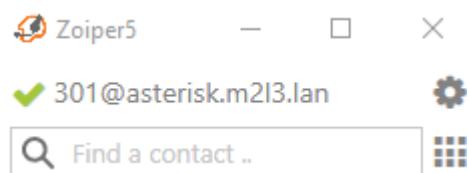
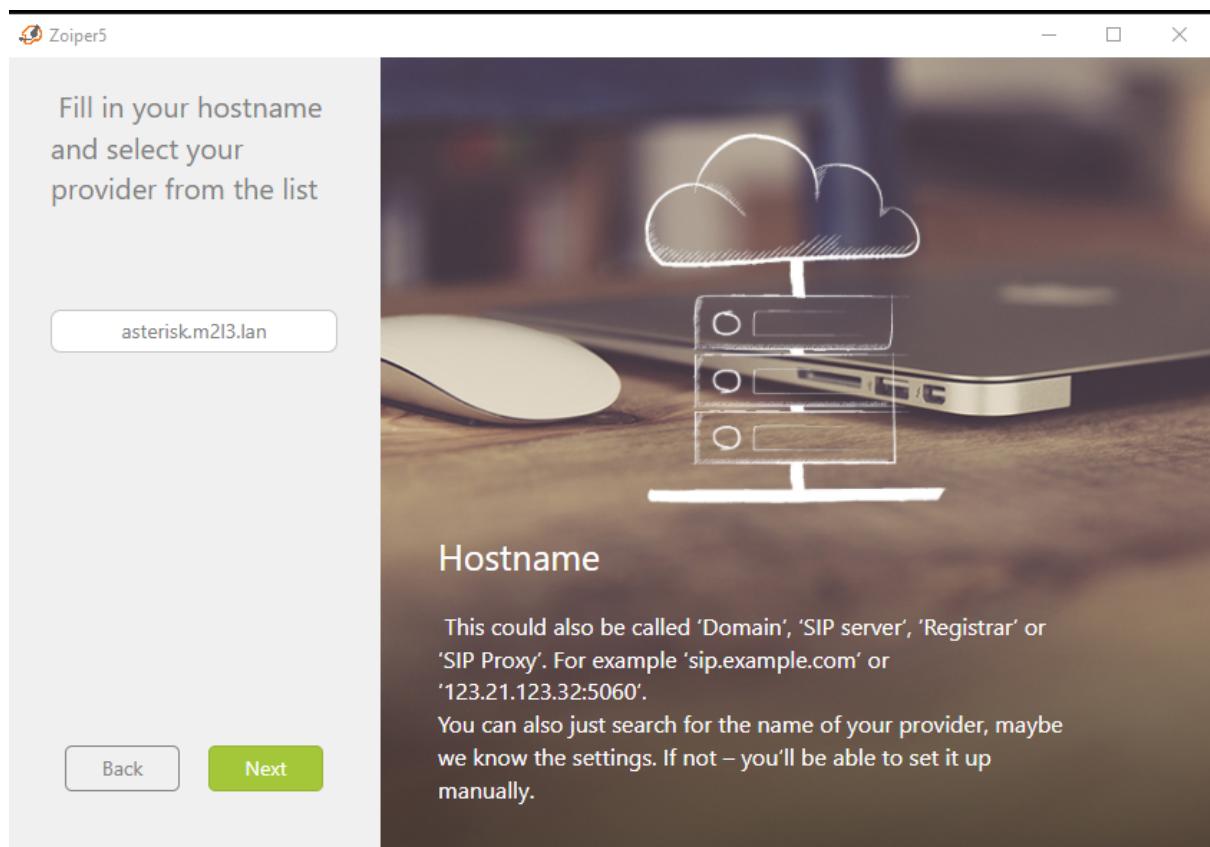
Pour écouter les messages vocaux, l'utilisateur doit composer le numéro 3999.

```
[general]
format=wav49|gsm|wav
maxmsg=100
maxsecs=0
minsec=s2
maxlogins=3
review=no
saycid=no

[m2l3]
3001 => , John DOE
3002 => , Calvyn MORIN
3003 => , Aurelien GALLEZ
3004 => , Sami BOURGOIN
3005 => , Hugo DUPATY
3006 => , Elouan CHURLET
3007 => , Maxence TRACHEZ
3008 => , Anthony LEHMANN
```

5.5) Enregistrement DNS du serveur de téléphonie

Enregistrement DNS du serveur de téléphonie



5.6) Mise en place d'un message d'attente

Installation des paquets nécessaires

```

root@asterisk:/usr/share/asterisk/agi-bin# wget https://github.com/zaf/asterisk-googlelets/tarball/master
--2023-05-22 16:09:28-- https://github.com/zaf/asterisk-googlelets/tarball/master
Résolution de github.com (github.com)... 140.82.121.4
Connexion à github.com (github.com)|140.82.121.4|:443... connecté.
requête HTTP transmise, en attente de la réponse... 302 Found
Emplacement : https://codeload.github.com/zaf/asterisk-googlelets/legacy.tar.gz/refs/heads/master [suivant]
--2023-05-22 16:09:29-- https://codeload.github.com/zaf/asterisk-googlelets/legacy.tar.gz/refs/heads/master
Résolution de codeload.github.com (codeload.github.com)... 140.82.121.10
Connexion à codeload.github.com (codeload.github.com)|140.82.121.10|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : non indiqué [application/x-gzip]
Sauvegarde en : « master.1 »

master.1                                [ <=>
2023-05-22 16:09:29 (543 KB/s) - « master.1 » sauvegardé [17467]

root@asterisk:/usr/share/asterisk/agi-bin# tar -xvf master
zaf-asterisk-googlelets-5566ddc/
zaf-asterisk-googlelets-5566ddc/COPYING
zaf-asterisk-googlelets-5566ddc/ChangeLog
zaf-asterisk-googlelets-5566ddc/README
zaf-asterisk-googlelets-5566ddc/authors
zaf-asterisk-googlelets-5566ddc/cli/
zaf-asterisk-googlelets-5566ddc/cli/goolelets-cli-tiny.pl
zaf-asterisk-googlelets-5566ddc/cli/goolelets-cli.pl
zaf-asterisk-googlelets-5566ddc/goolelets-tiny.agi
zaf-asterisk-googlelets-5566ddc/goolelets.agi
root@asterisk:/usr/share/asterisk/agi-bin# ls
goolelets.agi  master  master.1  zaf-asterisk-googlelets-5566ddc
root@asterisk:/usr/share/asterisk/agi-bin# mv ./zaf-asterisk-googlelets-5566ddc/goolelets ./goolelets.agi
root@asterisk:/usr/share/asterisk/agi-bin# nano goolelets.agi
root@asterisk:/usr/share/asterisk/agi-bin# chmod +x ./goolelets.agi
root@asterisk:/usr/share/asterisk/agi-bin# apt install perl libwww-perl sox mpg123

```

```

;exten => _3XXX,1,Answer() ; message attente avec la voix de synthèse
;exten => _3XXX,n.agi(goolelets.agi,"Bonjour le dieu de l'informatique Julien DUBOIS du lycée Paul Sabatier va vous répondre veuillez patienter",fr)
;exten => _3XXX,n,Dial(SIP/${EXTEN},10) ;appel en cours
;exten => _3XXX,2,VoiceMail(${EXTEN}@m2l3);messagerie si pas de réponse
;exten => 3999,1,VoiceMailMain(${CALLERID(num)}@m2l3)

```

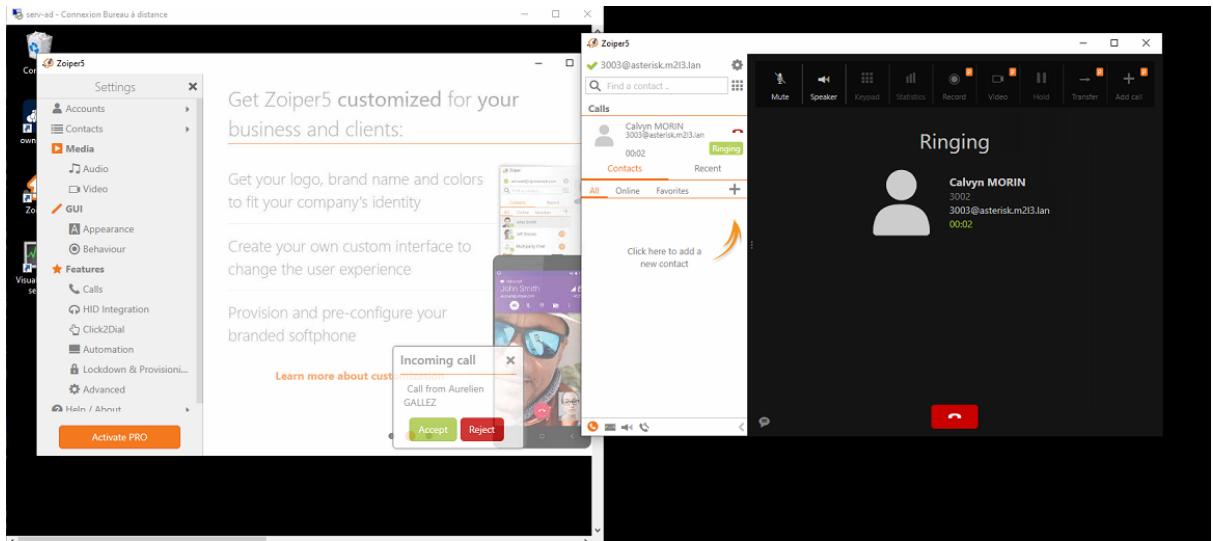
5.7) IVR

```

;exten => _3XXX,1,Answer()
;exten => _3XXX,2,Set(TIMEOUT(response)=5) ;Temps max pour faire un choix
;exten => _3XXX,3,agi(goolelets.agi,"Bonjour merci de laisser un message après le bip",fr)
;exten => _3XXX,4,agi(goolelets.agi,"Taper 1 pour appeler le 3001",fr)
;exten => _3XXX,5,agi(goolelets.agi,"Taper 2 pour appeler le 3002",fr)
;exten => _3XXX,6,agi(goolelets.agi,"Taper 3 pour appeler le 3003",fr)
;exten => _3XXX,7,WaitExten()
;exten => 1,1,Dial(SIP/3001)
;exten => 2,1,Dial(SIP/3002)
;exten => 3,1,Dial(SIP/3003)
;exten => _[04-9*#],1,agi(goolelets.agi,"Entrée invalide",fr)
;exten => _[04-9*#],2,Goto(m2l3,_3XXX,1)
;exten => _3XXX,1,Goto(m2l3,_3XXX,3)

```

5.8) Test

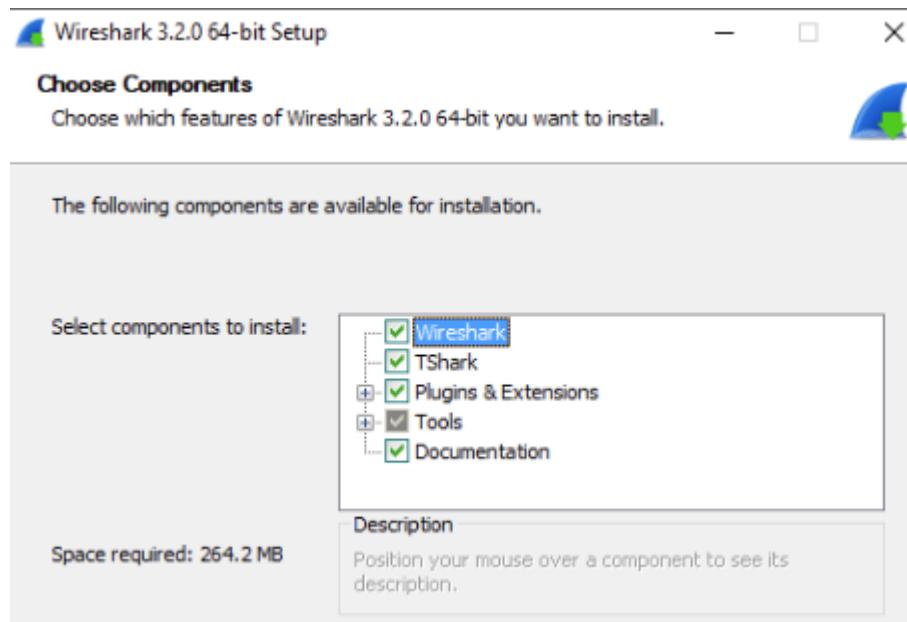


```
Connected to Asterisk 16.28.0~dfsg-0+deb11u2 currently running on asterisk (pid = 666)
== Using SIP RTP CoS mark 5
-- Executing [3002@m2l3:1] Dial("SIP/3001-00000007", "SIP/3002,20") in new task
== Using SIP RTP CoS mark 5
-- Called SIP/3002
-- SIP/3002-00000008 is ringing
-- SIP/3002-00000008 answered SIP/3001-00000007
-- Channel SIP/3002-00000008 joined 'simple_bridge' basic-bridge <3d852c50-750-40d2-84a0-73526c515f2f>
-- Channel SIP/3001-00000007 joined 'simple_bridge' basic-bridge <3d852c50-750-40d2-84a0-73526c515f2f>
asterisk*CLI>
```

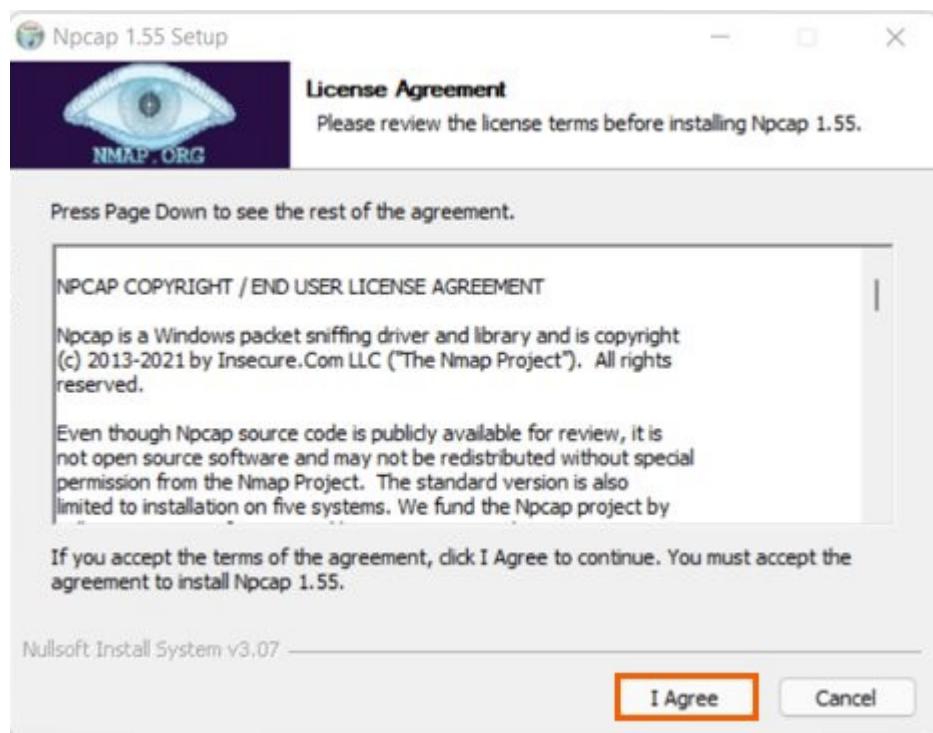
```
Connected to Asterisk 16.28.0~dfsg-0+deb11u2 currently running on asterisk (pid = 2359)
[Apr 20 18:59:26] NOTICE[2469][C-00000005]: Ext. 3099:1 @ m213: Dialing out from "Calvyn MORIN" <3099> to VoiceMail(3099)
[Apr 20 19:00:56] NOTICE[2469][C-00000005]: app_voicemail.c:9144 close_mailbox: 1 messages received after mailbox opened.
asterisk*CLI>
```

6. Analyse de paquets

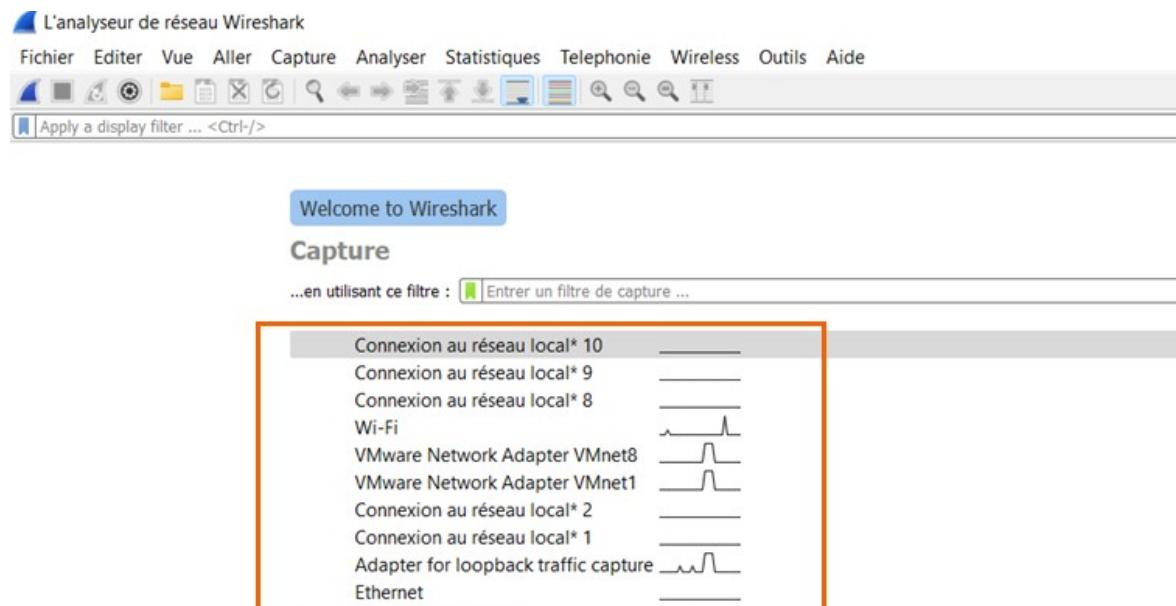
6.1) Installation de Wireshark



6.2) Installation de NpCap afin de réaliser des captures



6.3) Sélection de l'interface réseau



6.4) Analyse de paquets sur notre infrastructure

