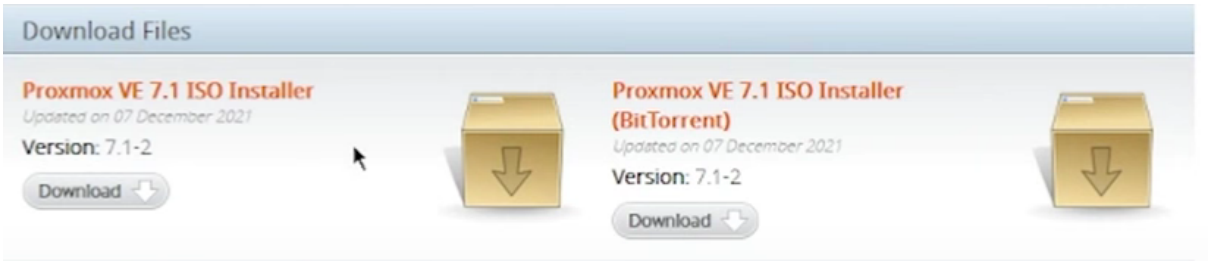
# FSP 1

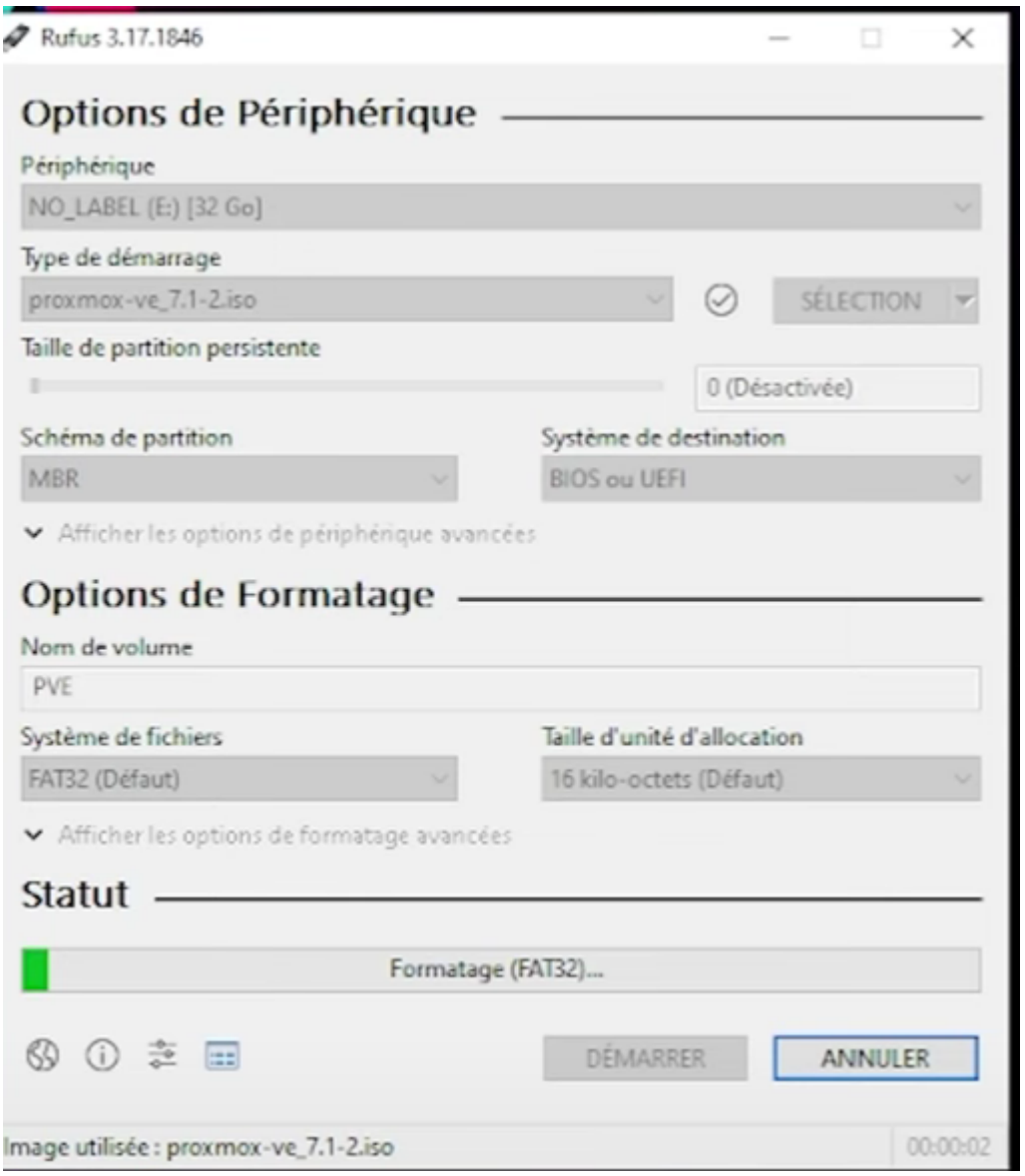
# 1. Active Directory

*1.1) Hyperviseur de type 1 Proxmox*

On sélectionne un ISO de Proxmox

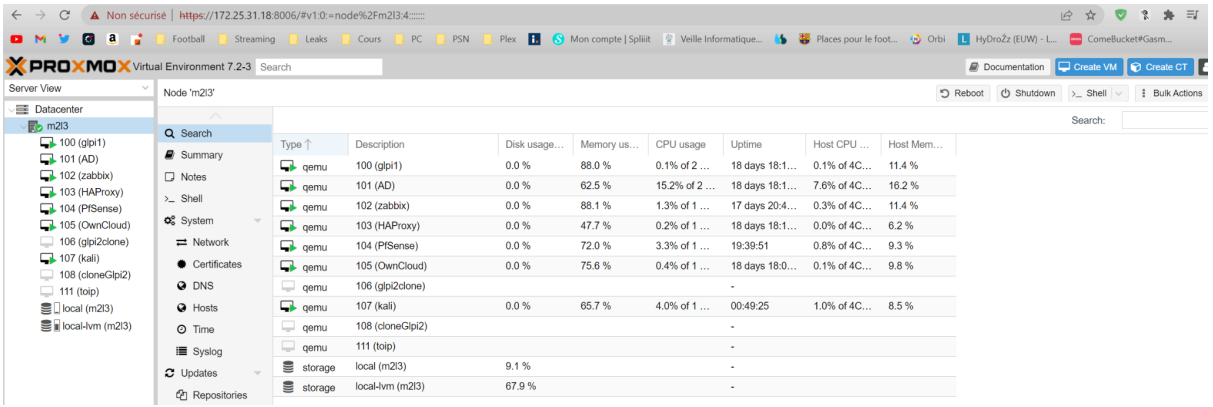



On crée une clé bootable contenant Proxmox à l'aide du logiciel Rufus




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

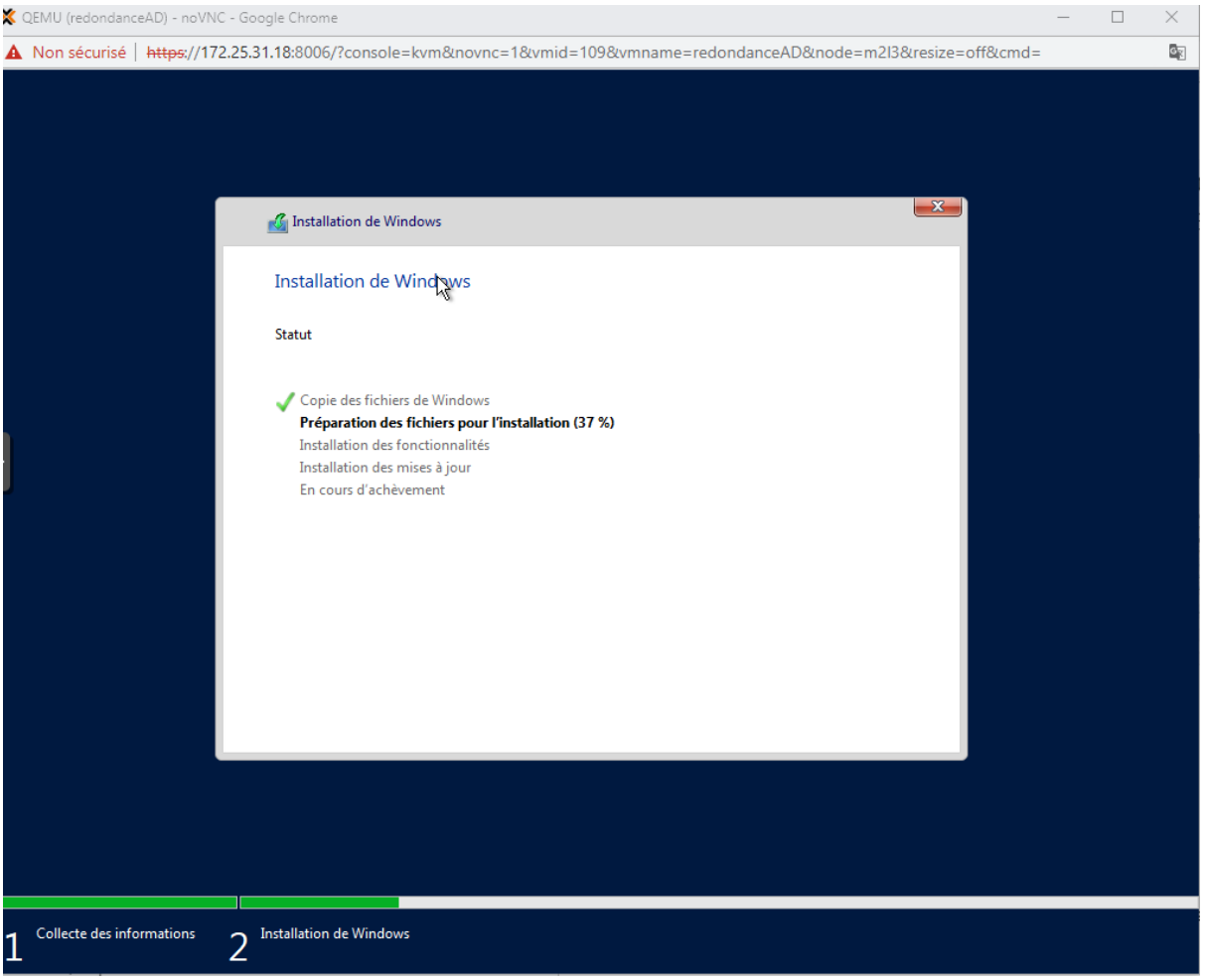
On sélectionne une adresse IP et on laisse l'installation se faire.



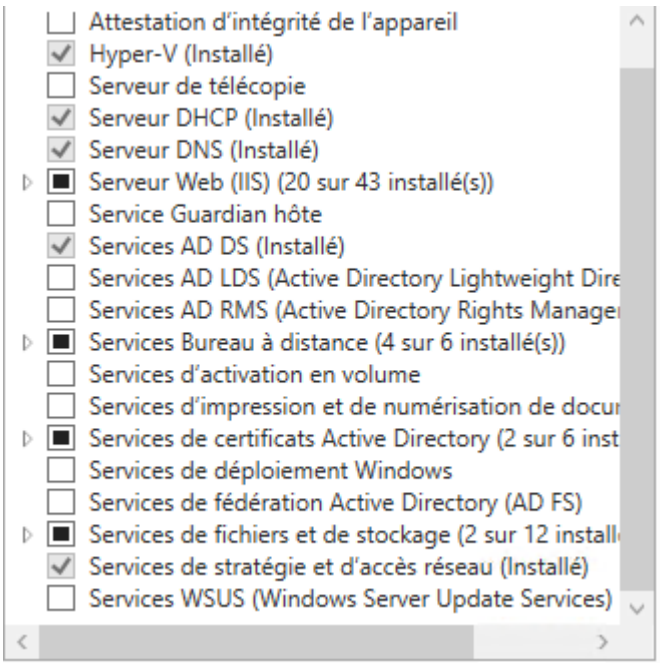

Une fois l'installation terminée,nous sommes prêts à créer des machines virtuelles. Dorénavant, nous allons installer notre contrôleur de domaine.

### *1.2) Domaine M2L3/DNS/DHCP*

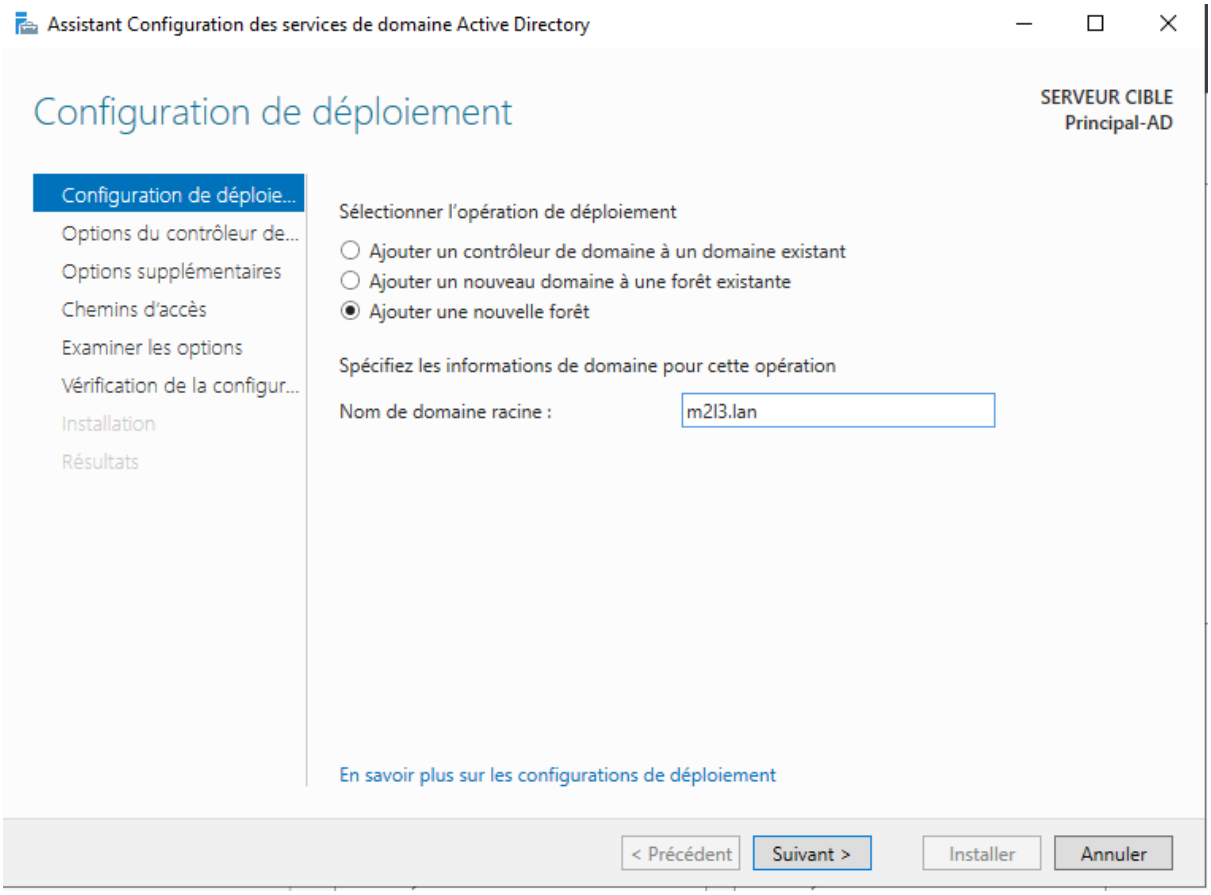
Installation de Windows Serveur 2019

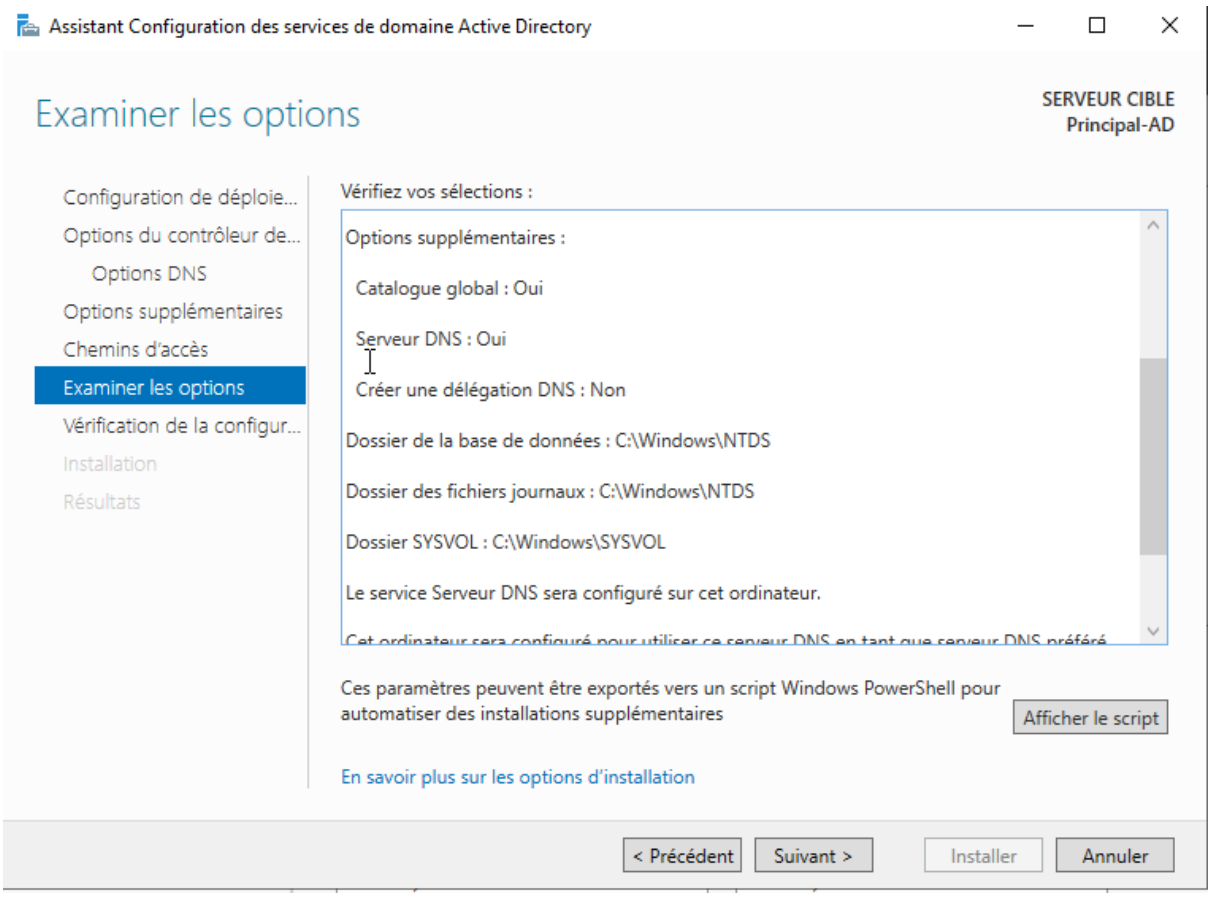



Installation des services AD/DNS/DHCP

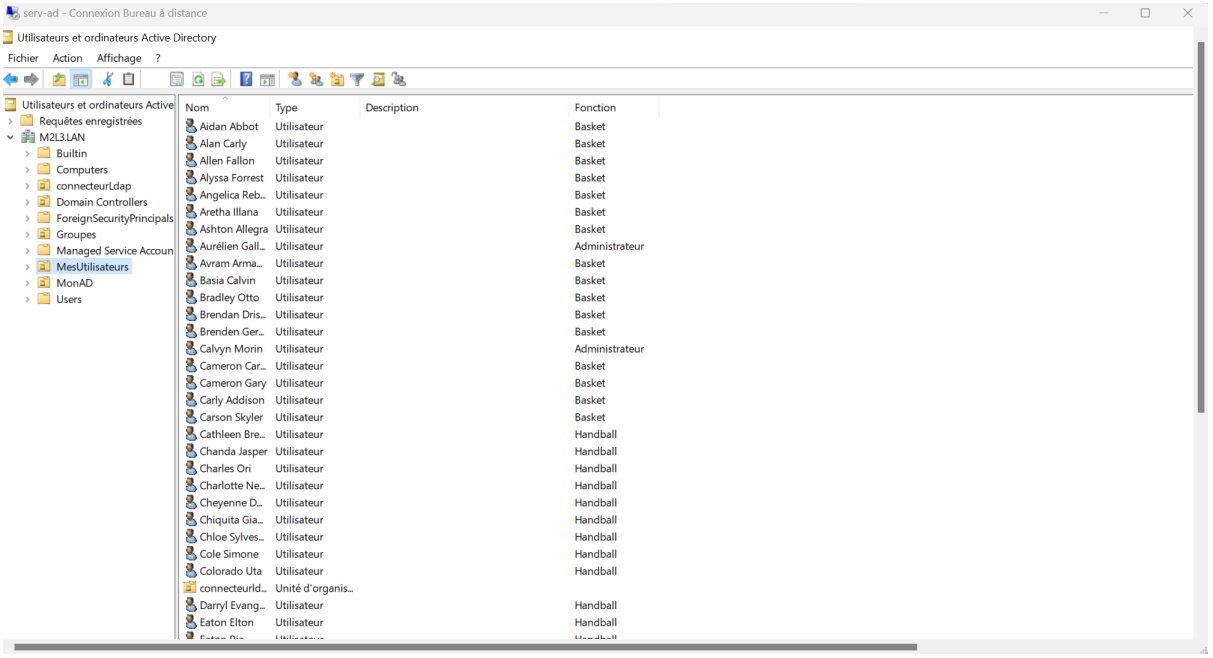



Création du contrôleur de domaine

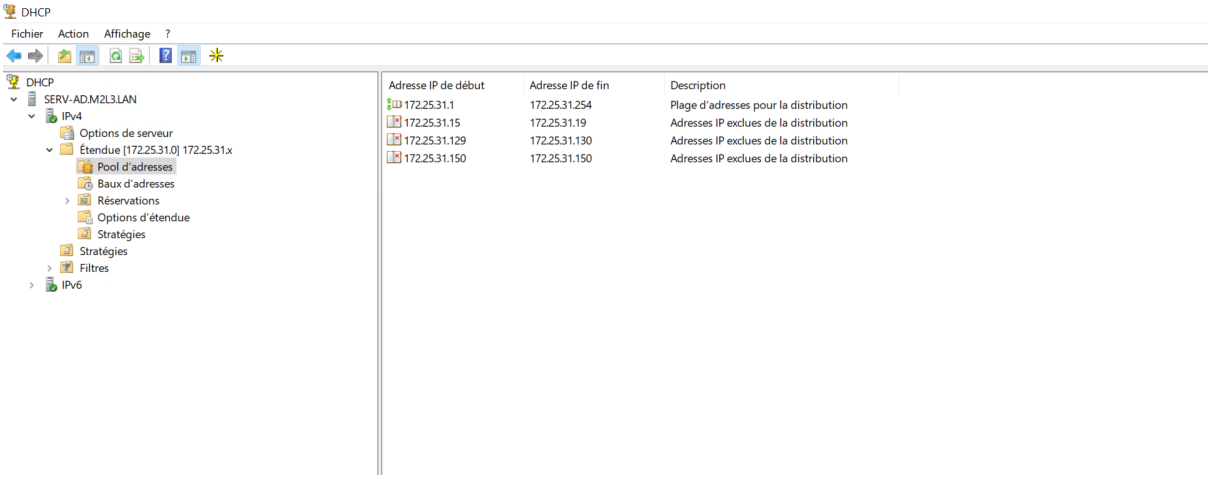




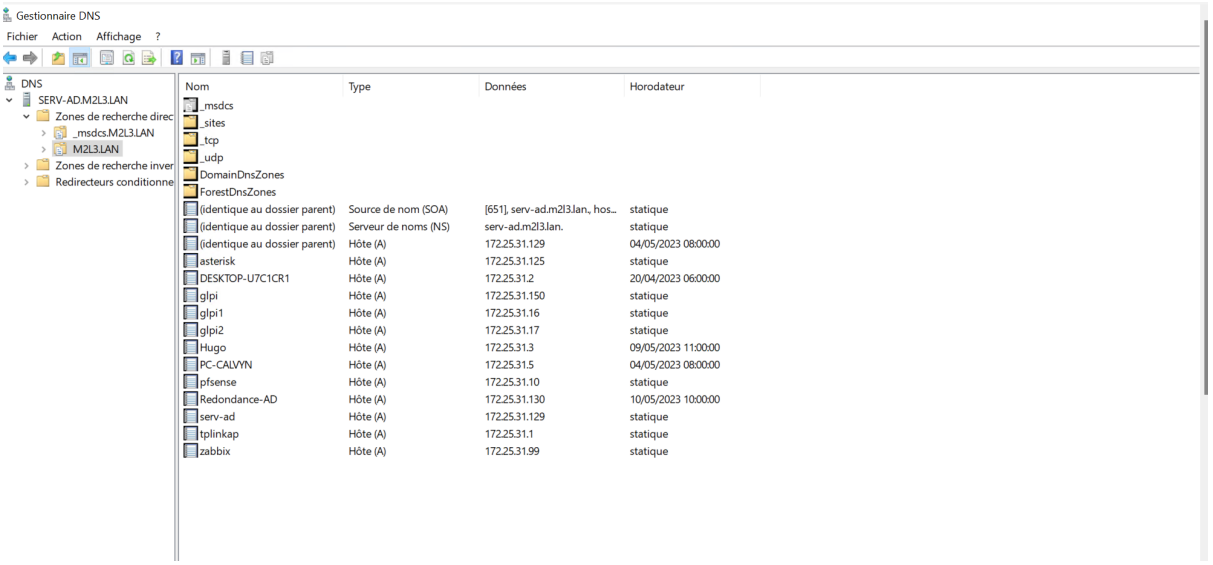

## Création des utilisateurs




## Étendue DHCP




Enregistrement DNS




### *1.3) Script powershell importation des utilisateurs*

On importe les utilisateurs à partir d'un fichier CSV à l'aide du script suivant.

MONSCRIPT.ps1 9+

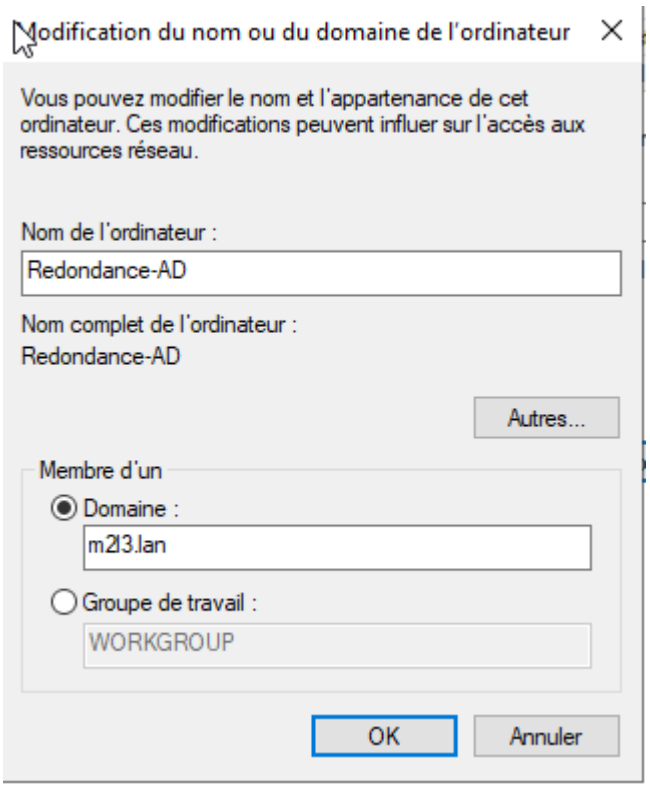
G: > Mon Drive > BTS > AP > 2ème année > MONSCRIPT.ps1 > ...

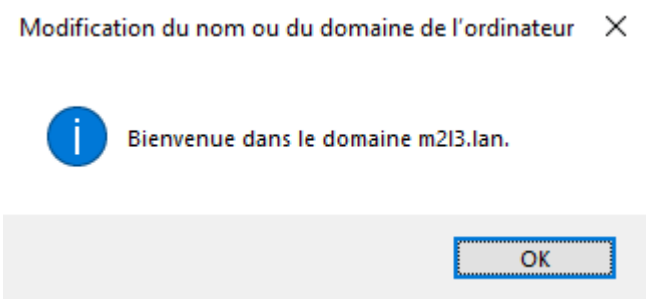
```powershell
Install-Module -Name ImportExcel
$CSVFile="C:\Users\calvyn\Downloads\ListeUserPPE.xlsx"
$CSVData=Import-Excel -Path $CSVFile

foreach($Utilisateur in $CSVData){
    $Domain = "M2L3"
    $EXT = "LAN"
    $Server = "SERV-AD.M2L3.LAN"
    $UserID = $Utilisateur.ID
    $UserIDescription = $Utilisateur.IDescription
    $UserNom= $Utilisateur.Nom
    $UserPrenom=$Utilisateur.Prenom
    $UserLogin = ($UserNom).Substring(0,1).ToLower()+$UserPrenom.ToLower()
    $UserSecteur = $Utilisateur.Secteur
    $UserType=$Utilisateur.Type
    $UserDate_FIn=$Utilisateur.DateFin
    $UserTel = $Utilisateur.Tel
    $UserPays = $Utilisateur.Pays
    $UserVille = $Utilisateur.Ville
    $UserCP = $Utilisateur.CP
    $UserRue = $Utilisateur.Rue
    $UserMDP = "P@ssword3411!"

#Vérifier la présence de l'user dans l'AD
if(Get-AdUser -Filter {SamAccountName -eq $UserLogin})
    {
        Write-Warning "L'identifiant $UserLogin existe déjà dans l'AD"
        }
        else
        {
        New-ADUser -Name "$UserNom $UserPrenom" `
                   -DisplayName "$UserNom $UserPrenom" `
                   -GivenName $UserNom `
                   -Surname $UserPrenom `
                   -SamAccountName $UserLogin `
                   -UserPrincipalName "$UserLogin@m2l3.lan" `
                   -Title $UserSecteur `
                   -Path "OU=MesUtilisateurs, DC=M2L3, DC=LAN" `
                   -AccountPassword(ConvertTo-SecureString $UserMDP -AsPlainText -Force)`
                   -Enabled $true `
                   -ChangePasswordAtLogon $true


    Write-Output "Création de l'user : $UserLogin ($UserPrenom $UserNom) avec l'ID $UserID"
}
```

*1.4) Redondance active directory et serveur à basculement DHCP*

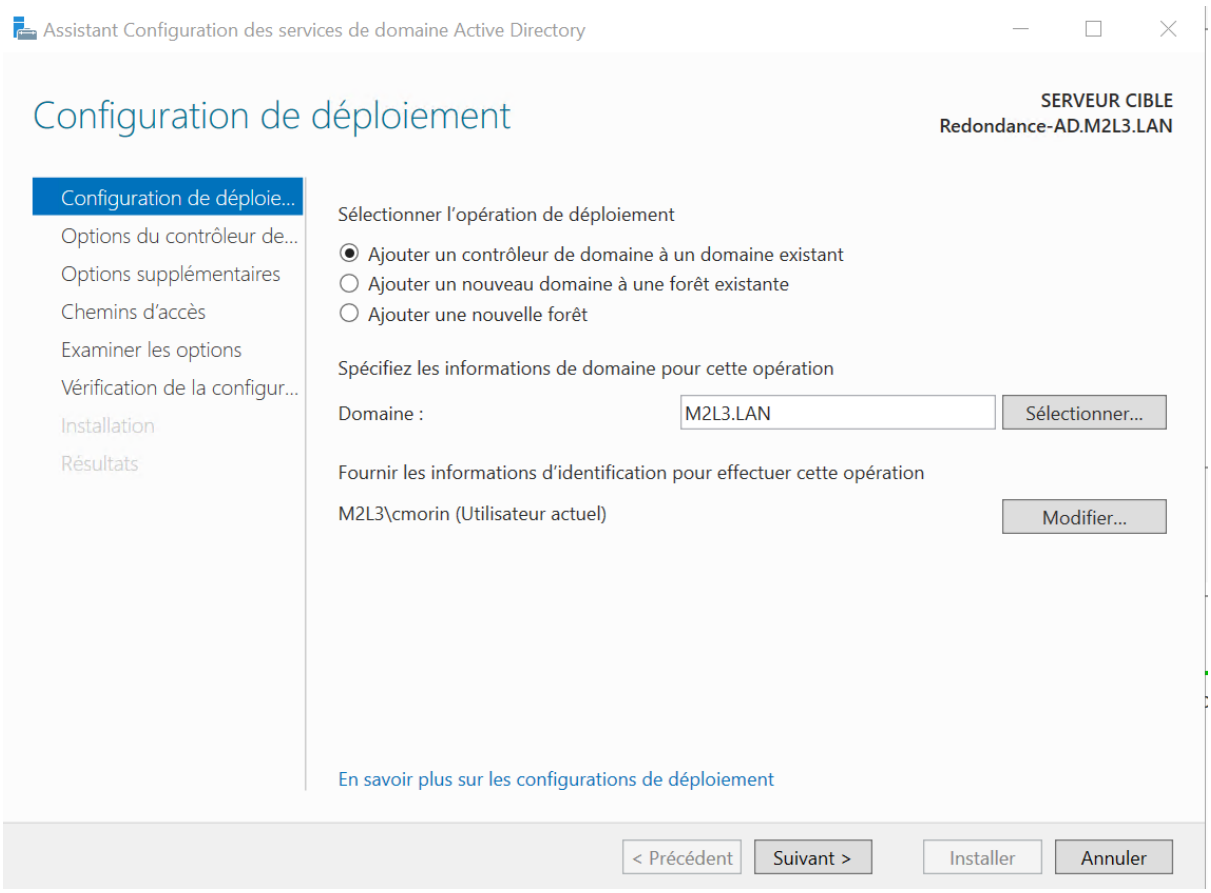
Installation de Windows Serveur 2019

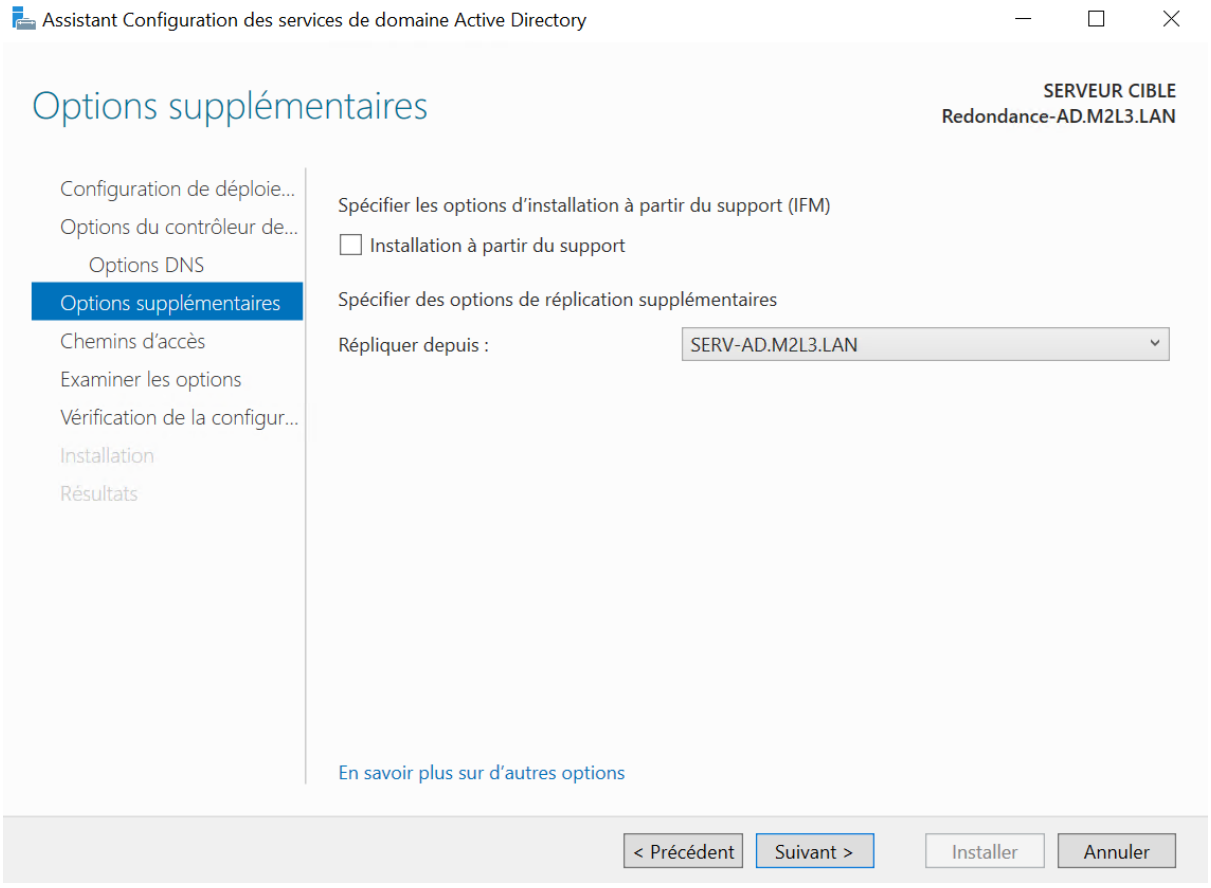
On joint le domaine M2L3 avec le serveur de redondance Redondance-AD



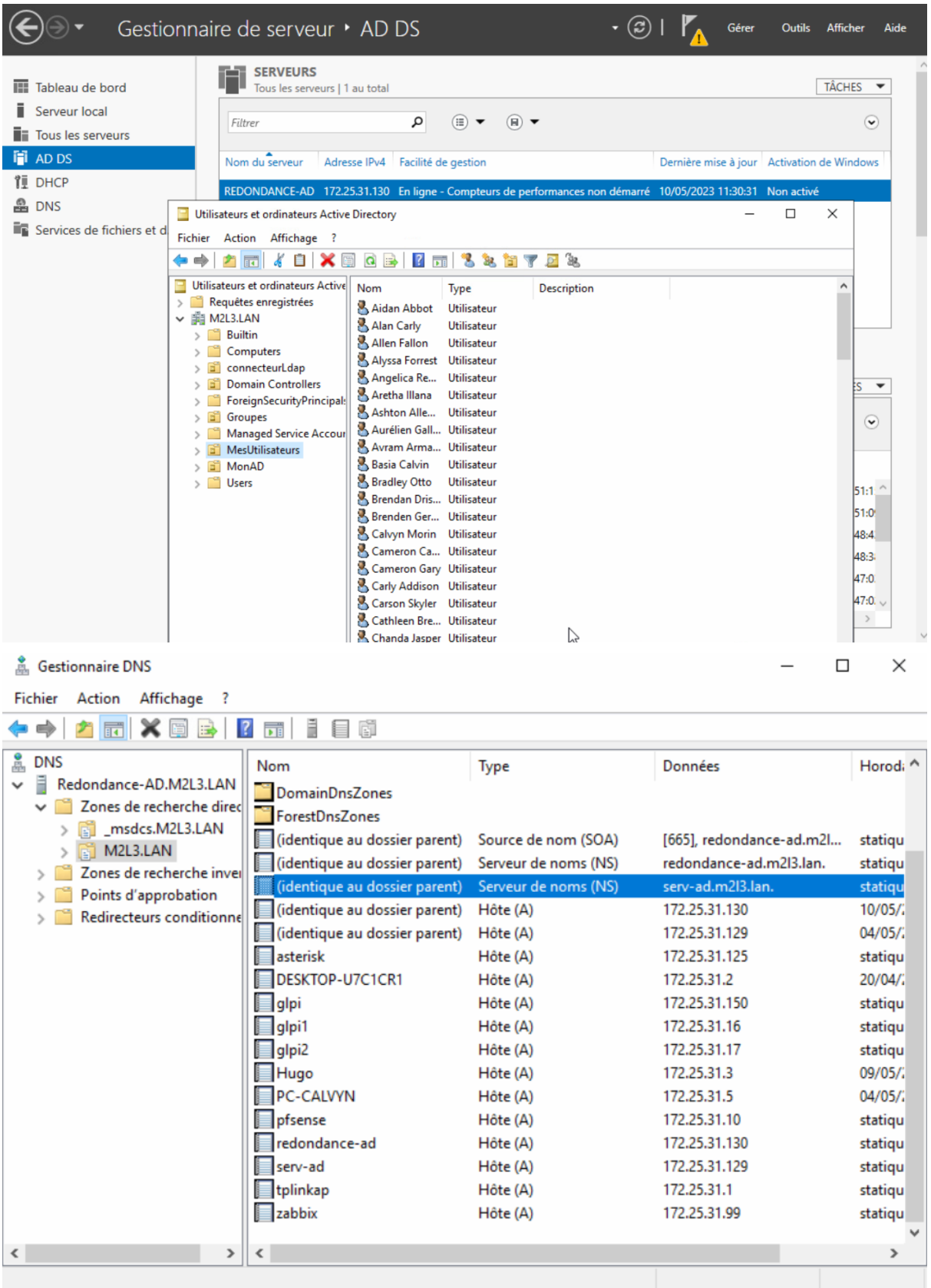




On ajoute un contrôleur de domaine au domaine existant : M2L3.

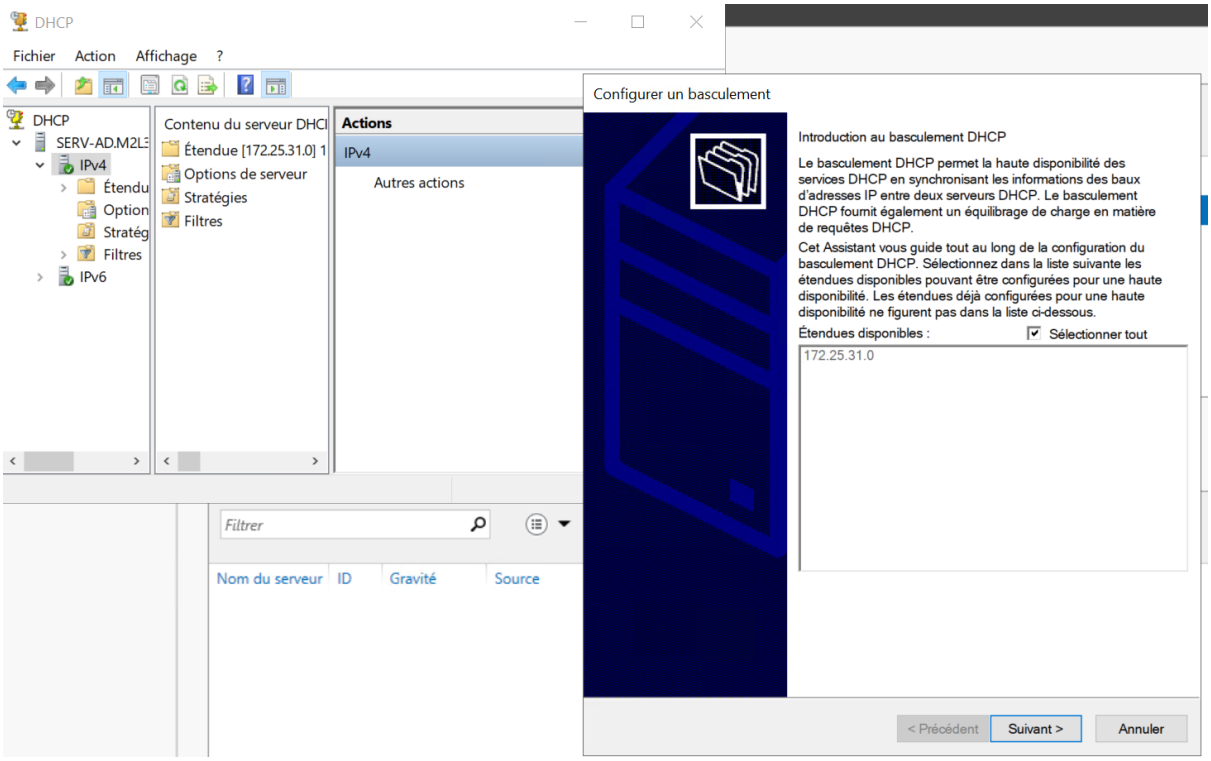

Assistant Configuration des services de domaine Active Directory
Configuration de déploiement
SERVEUR CIBLE
Redondance-AD.M2L3.LAN
Configuration de déploie...
Options du contrôleur de...
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
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
Domaine :
M2L3.LAN
Sélectionner...
Fournir les informations d'identification pour effectuer cette opération
M2L3\cmorin (Utilisateur actuel)
Modifier...
En savoir plus sur les configurations de déploiement
< Précédent
Suivant >
Installer
Annuler


Assistant Configuration des services de domaine Active Directory
Options supplémentaires
SERVEUR CIBLE
Redondance-AD.M2L3.LAN
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Spécifier les options d'installation à partir du support (IFM)
Installation à partir du support
Spécifier des options de réplication supplémentaires
Répliquer depuis :
SERV-AD.M2L3.LAN
En savoir plus sur d'autres options
< Précédent
Suivant >
Installer
Annuler

Le contrôleur de domaine est répliqué.




Serveur de basculement DHCP


DHCP
Fichier Action Affichage ?
DHCP
SERV-AD.M2L3
IPv4
Étendu
Option
Stratég
Filtres
IPv6
Contenu du serveur DHCI
Étendue [172.25.31.0] 1
Options de serveur
Stratégies
Filtres
Actions
IPv4
Autres actions
Filtrer
Nom du serveur
ID
Gravité
Source
Configurer un basculement
Introduction au basculement DHCP
Le basculement DHCP permet la haute disponibilité des services DHCP en synchronisant les informations des baux d'adresses IP entre deux serveurs DHCP. Le basculement DHCP fournit également un équilibrage de charge en matière de requêtes DHCP.
Cet Assistant vous guide tout au long de la configuration du basculement DHCP. Sélectionnez dans la liste suivante les étendues disponibles pouvant être configurées pour une haute disponibilité. Les étendues déjà configurées pour une haute disponibilité ne figurent pas dans la liste ci-dessous.
Étendues disponibles :
Sélectionner tout
172.25.31.0
< Précédent
Suivant >
Annuler

Configurer un basculement

**Créer une relation de basculement**

Créer une relation de basculement avec le partenaire redondance-ad

Nom de la relation : serv-ad.m2l3.lan-redondance-ad

Délai de transition maximal du client (MCLT) : 1 heures 0 minutes

Mode : Équilibrage de charge

Pourcentage d'équilibrage de charge

Serveur local : 50 %

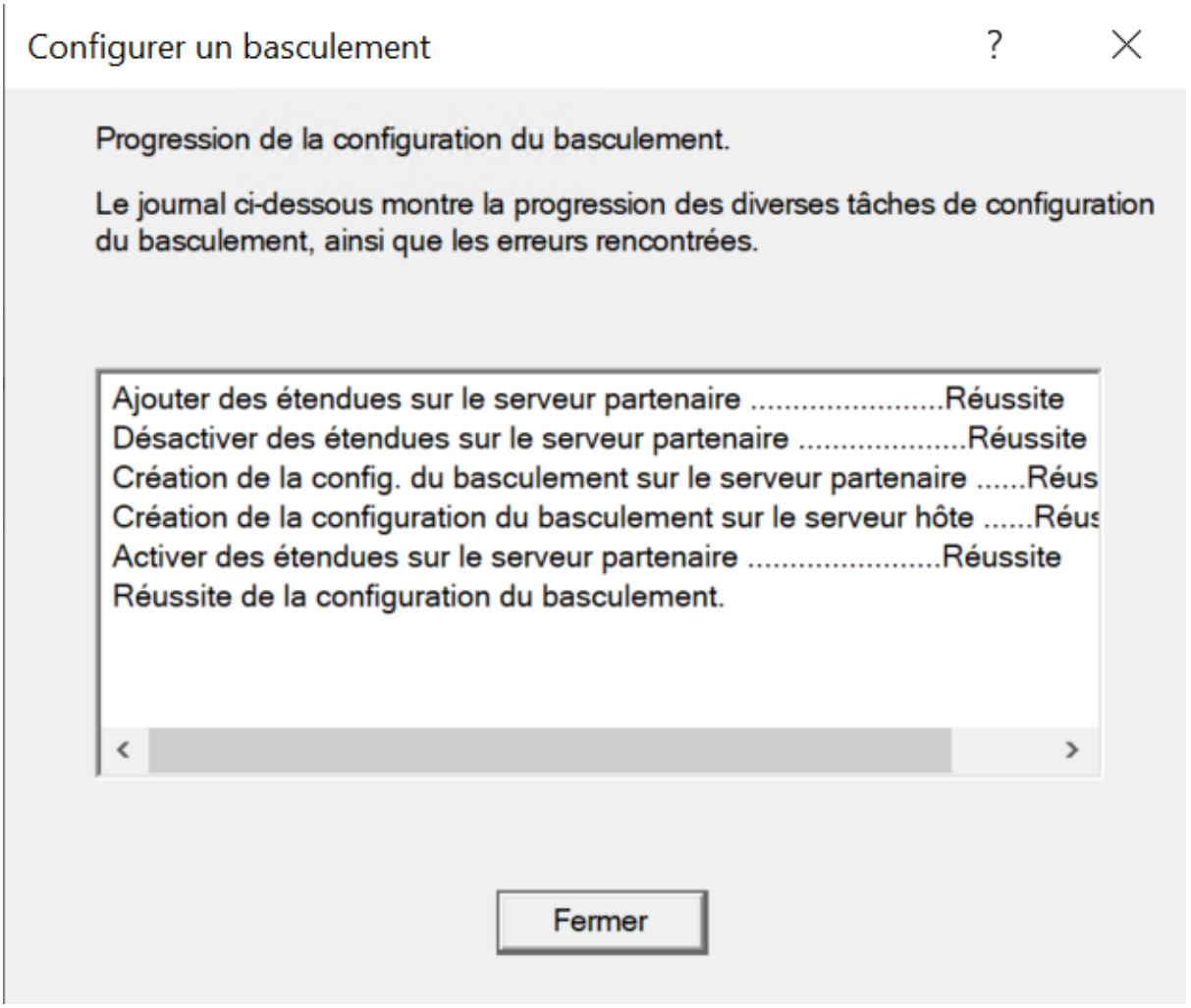
Serveur partenaire : 50 %

☐ Intervalle de basculement d'état : 60 minutes

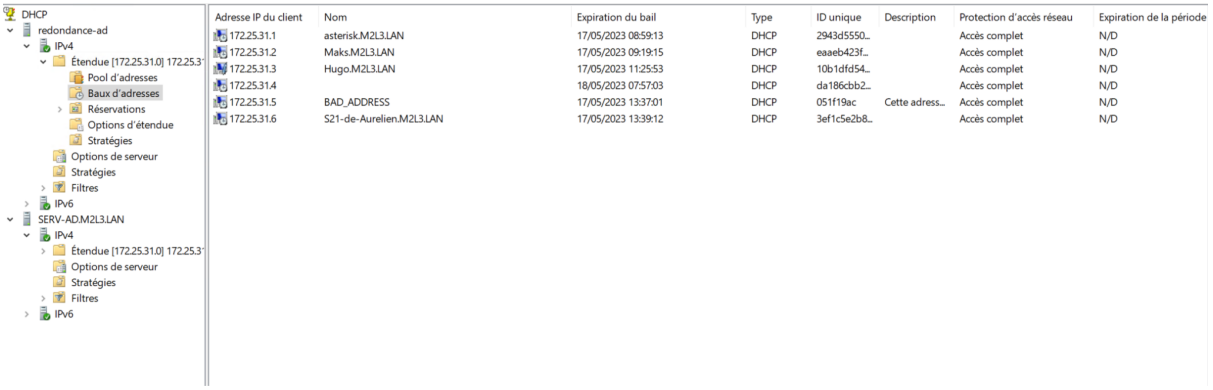
☑ Activer l'authentification du message

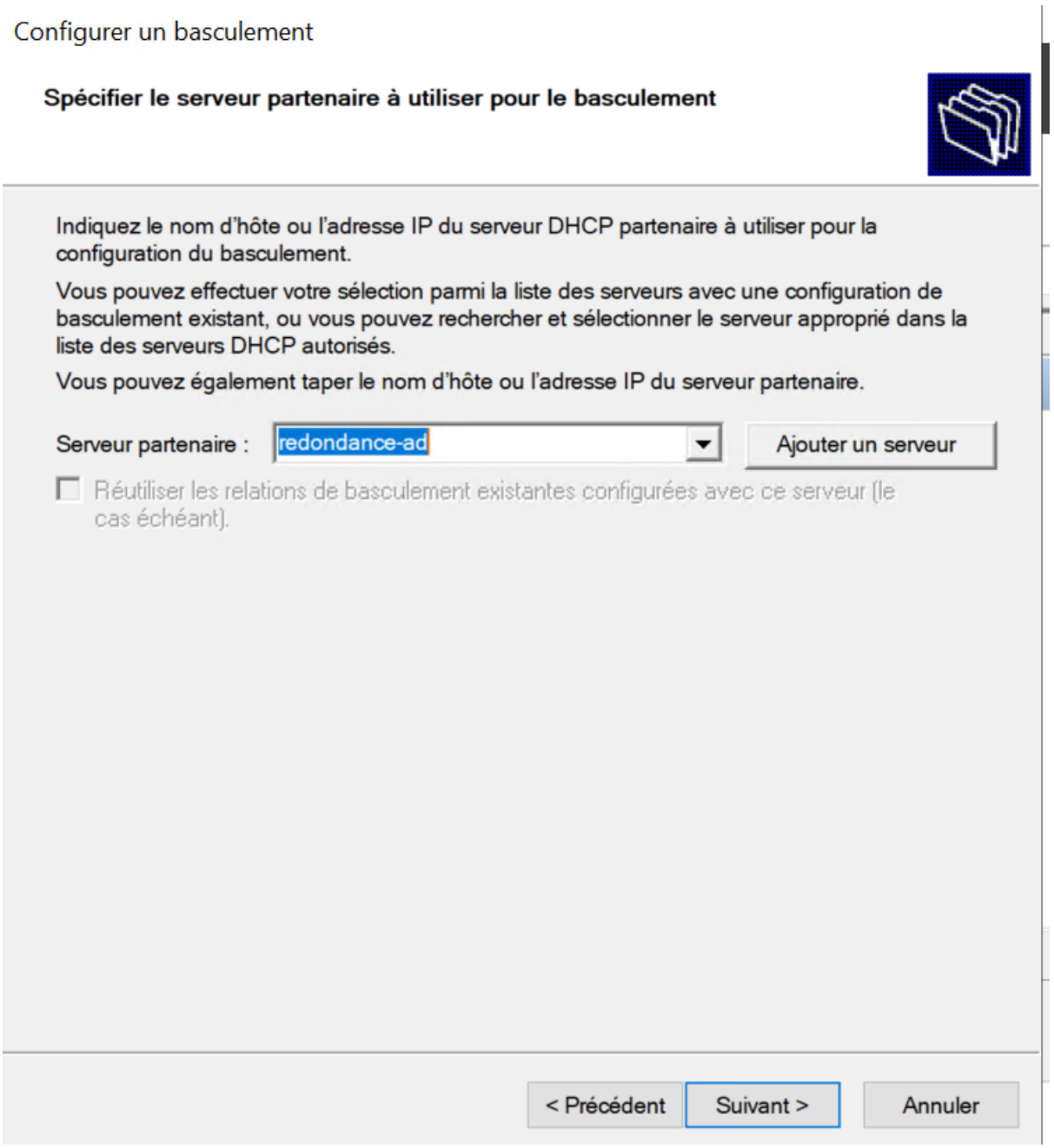
Secret partagé : **********

< Précédent | Suivant > | Annuler

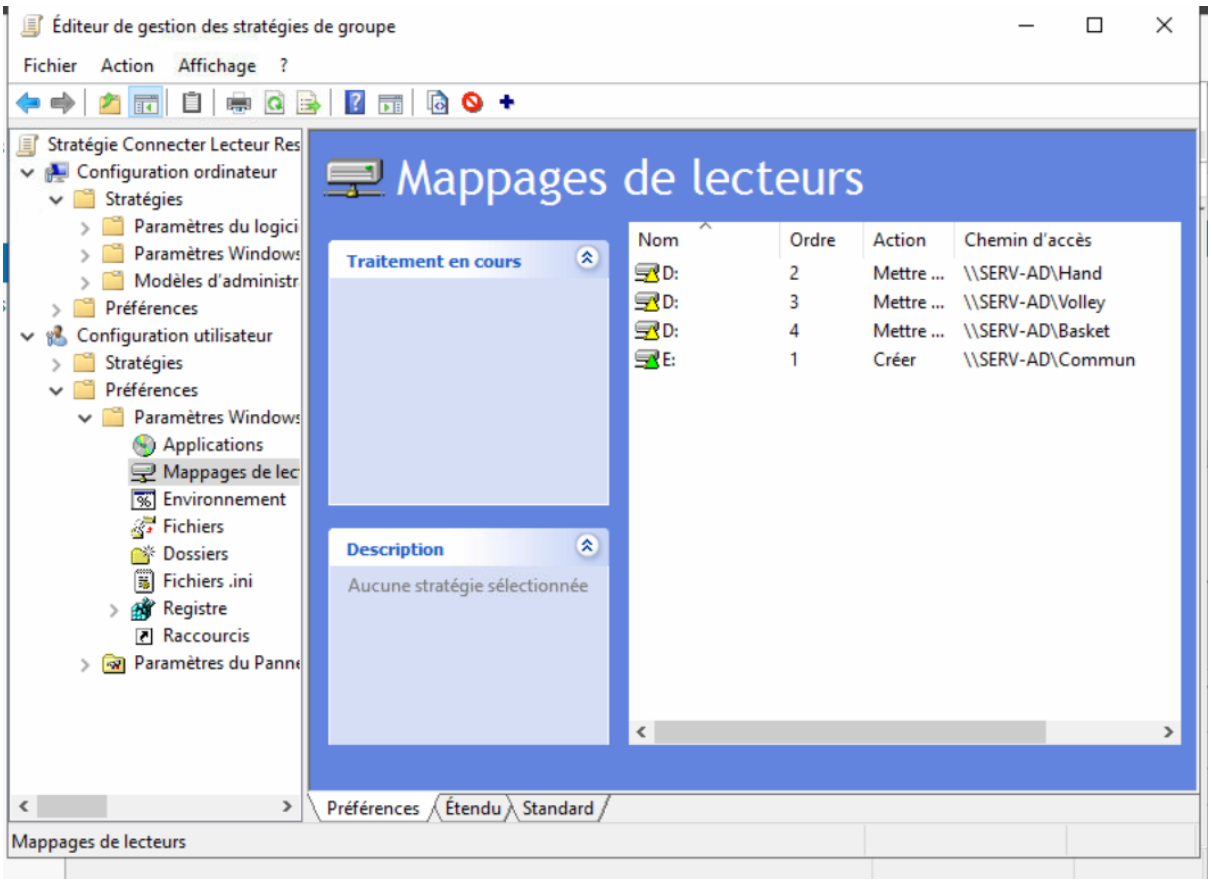



Le cluster DHCP est en place.



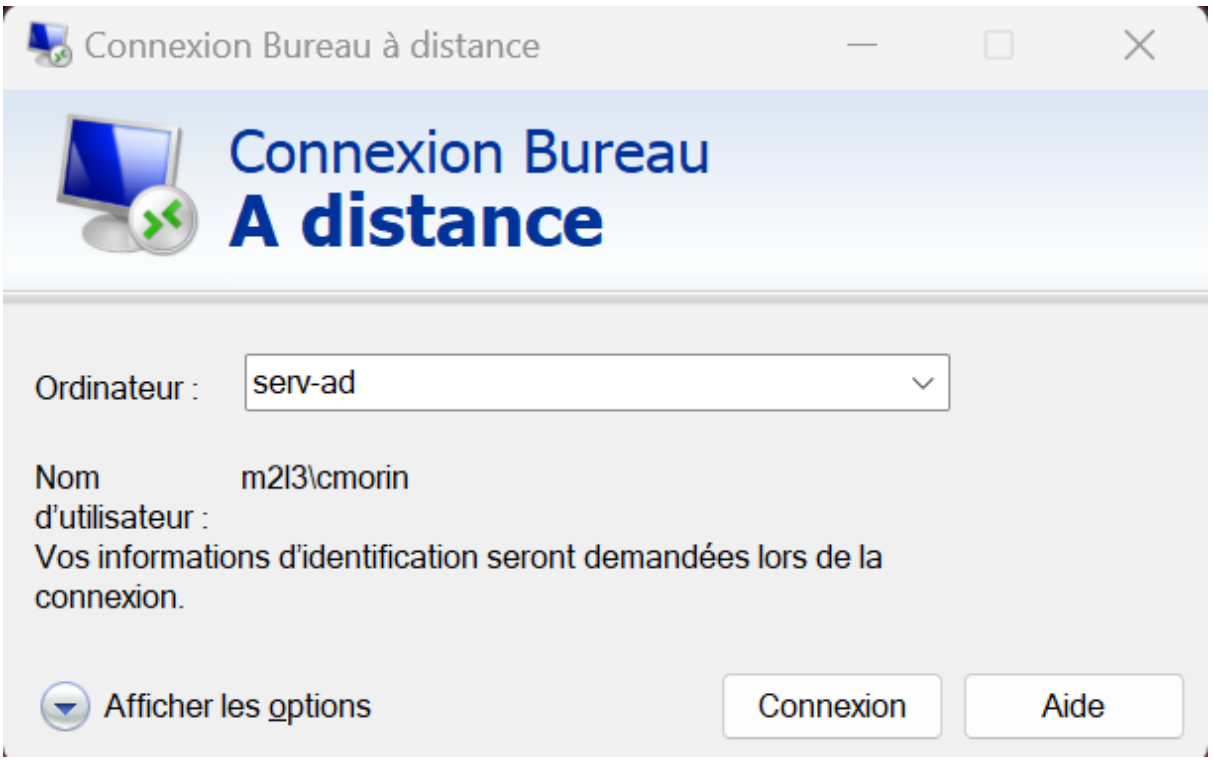


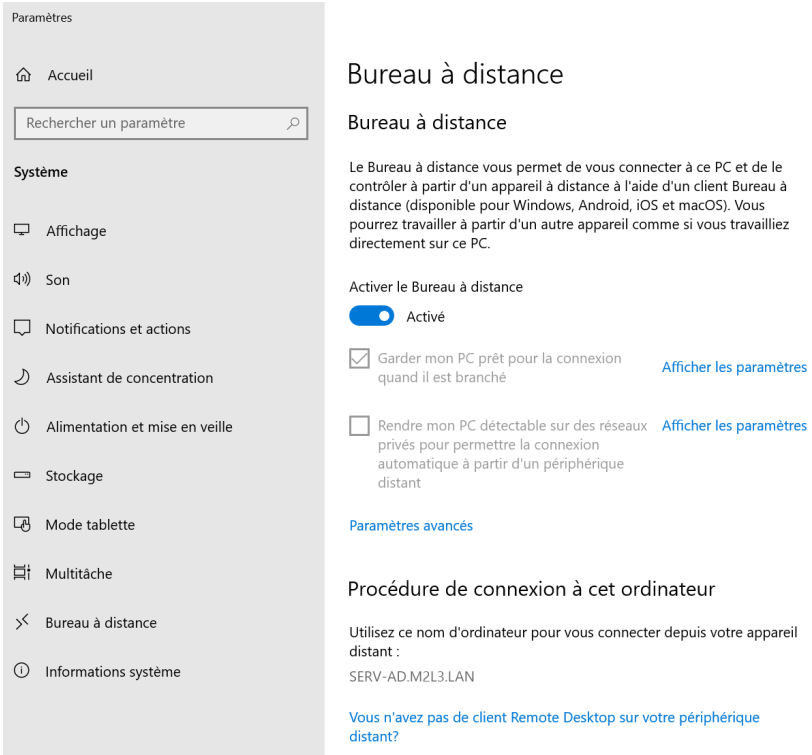

*1.5) Partages réseaux*




# 2. Serveurs accessibles à distance

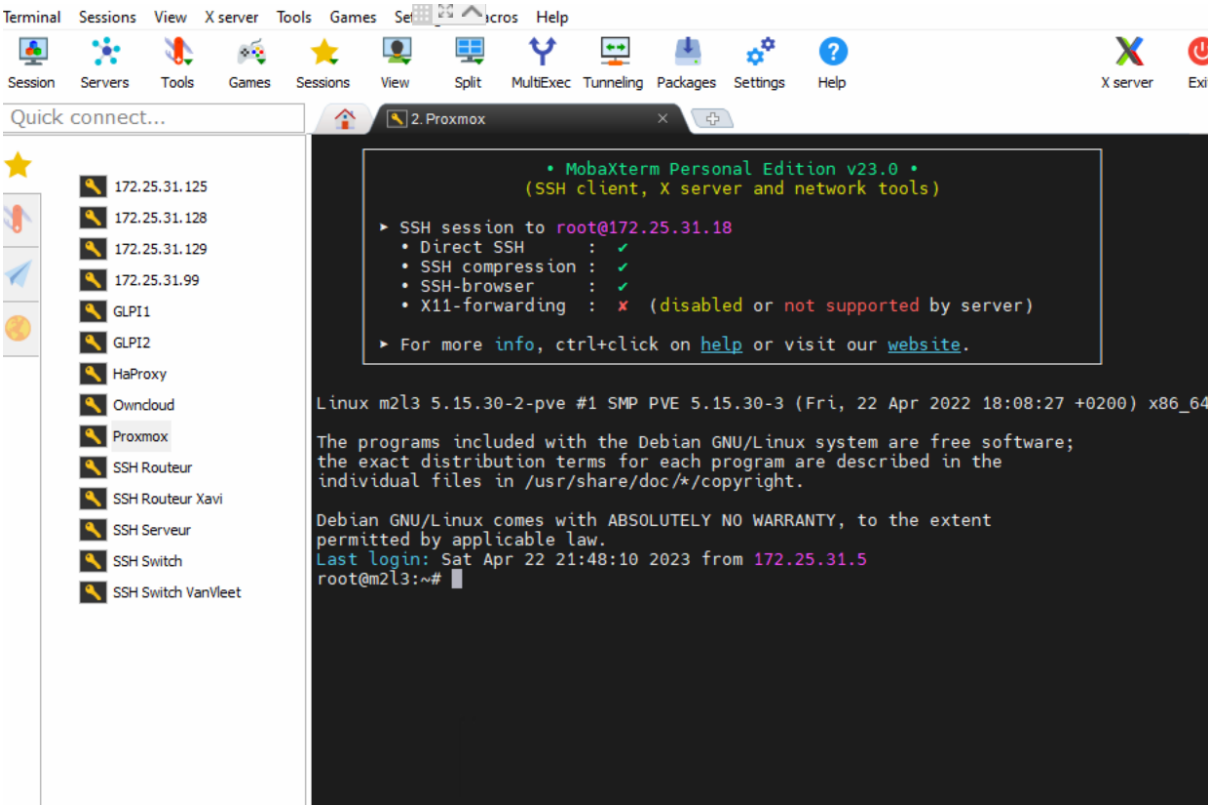
*2.1) WS2019 accessibles via RDP*




*2.2) GLPI, Zabbix, Proxmox,HaProxy accessibles via SSH*

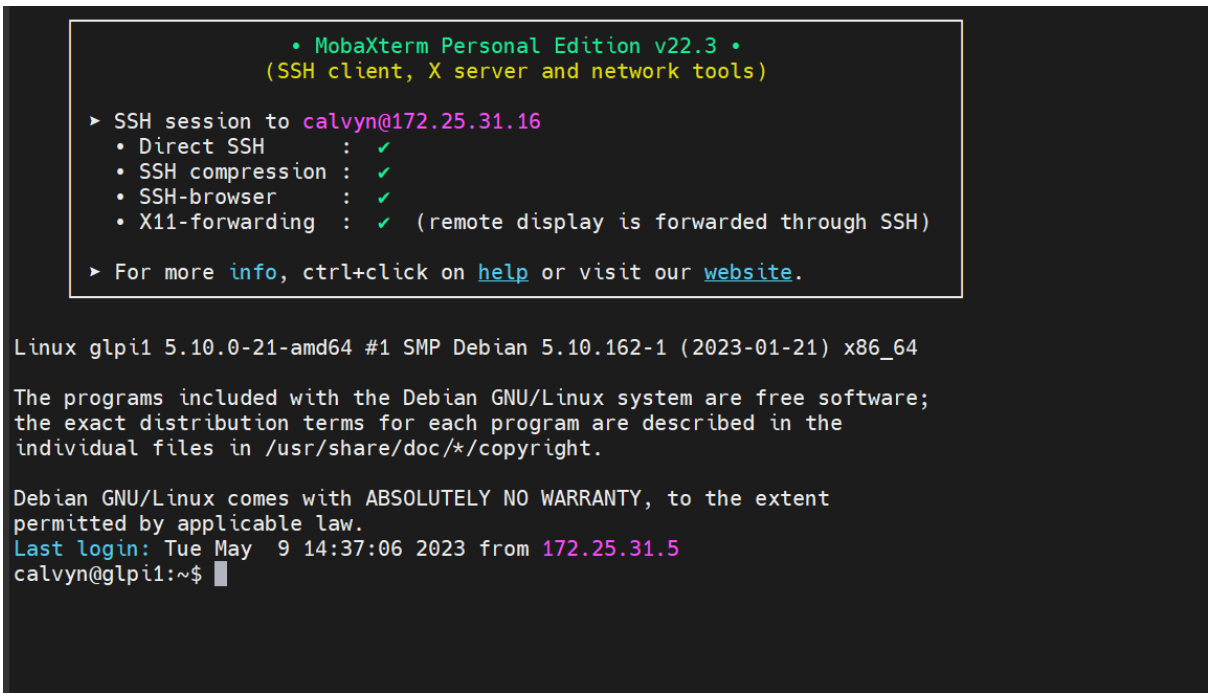
Proxmox :



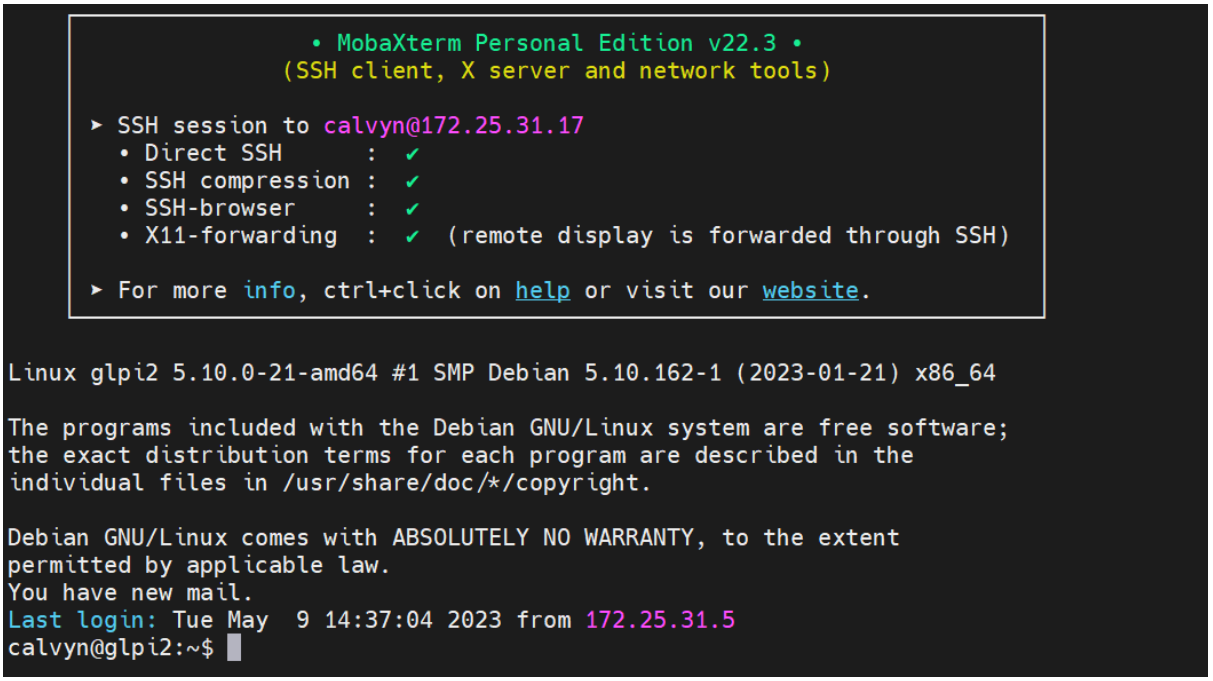

HaProxy :

```
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 :




GLPI2:

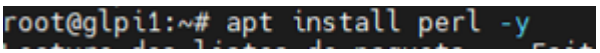



# 3. GLPI

*3.1) Installation de GLPI*

Fiche AP GLPI, **INSTALLATION GLPI (DEBIAN 11 & GLPI 10.0.2)**

**Installation de Perl**



**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/gl
pi-10.0.7.tgz
```

**On les décompresse**

```
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**

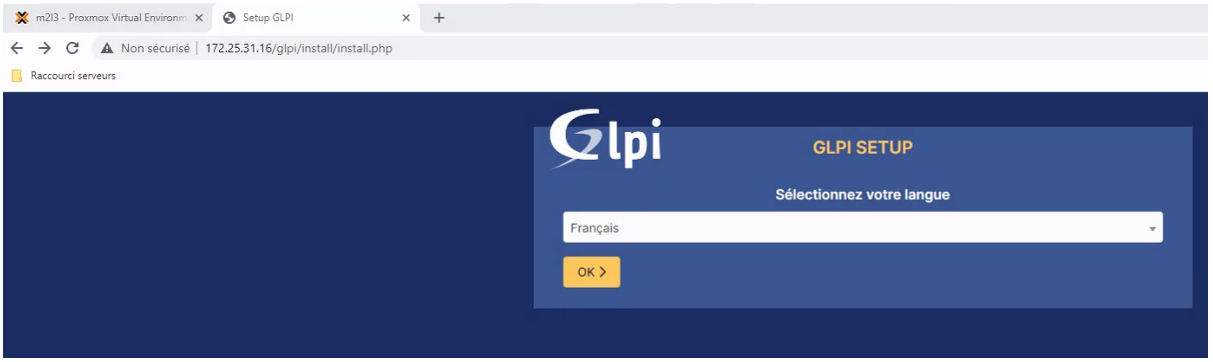
```
MariaDB [(none)]> create user glpiuser@localhost identified by '1234';
Query OK, 0 rows affected (0,004 sec)
```

**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)
```

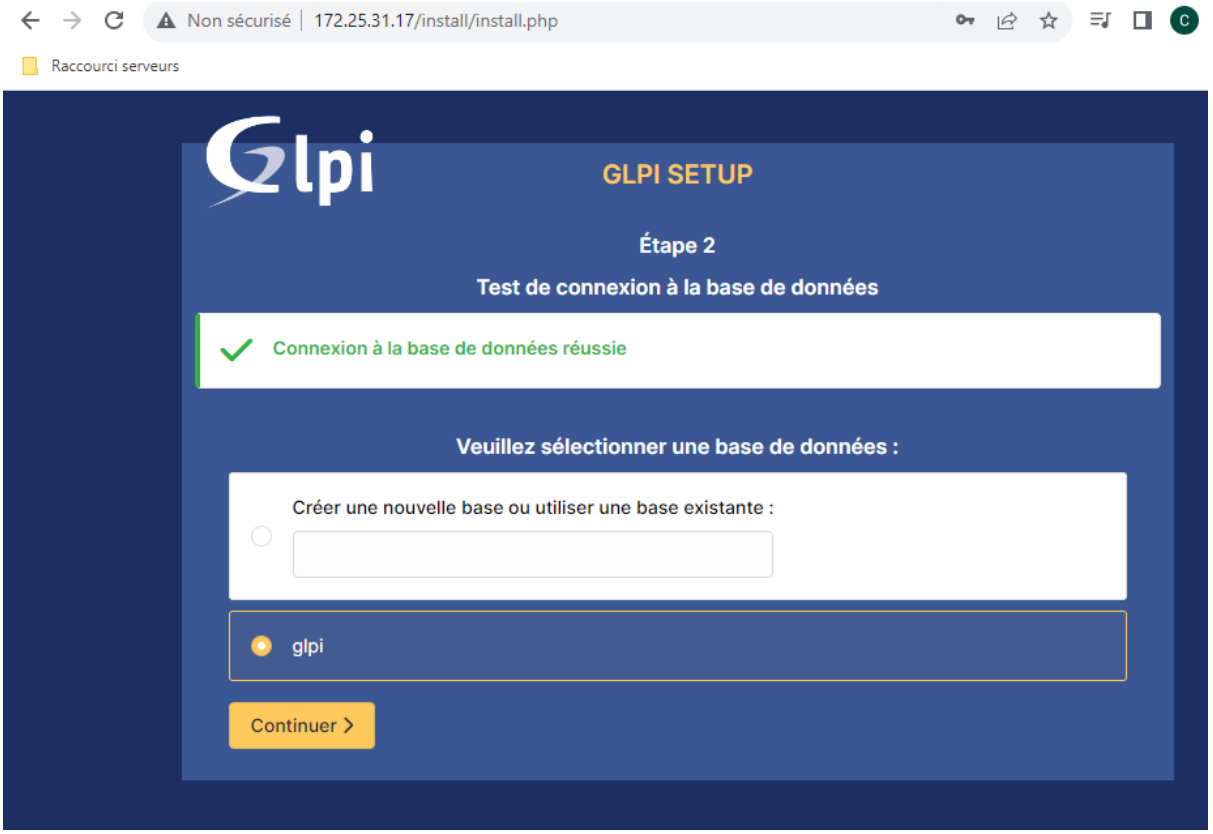
**Installation de GLPI**

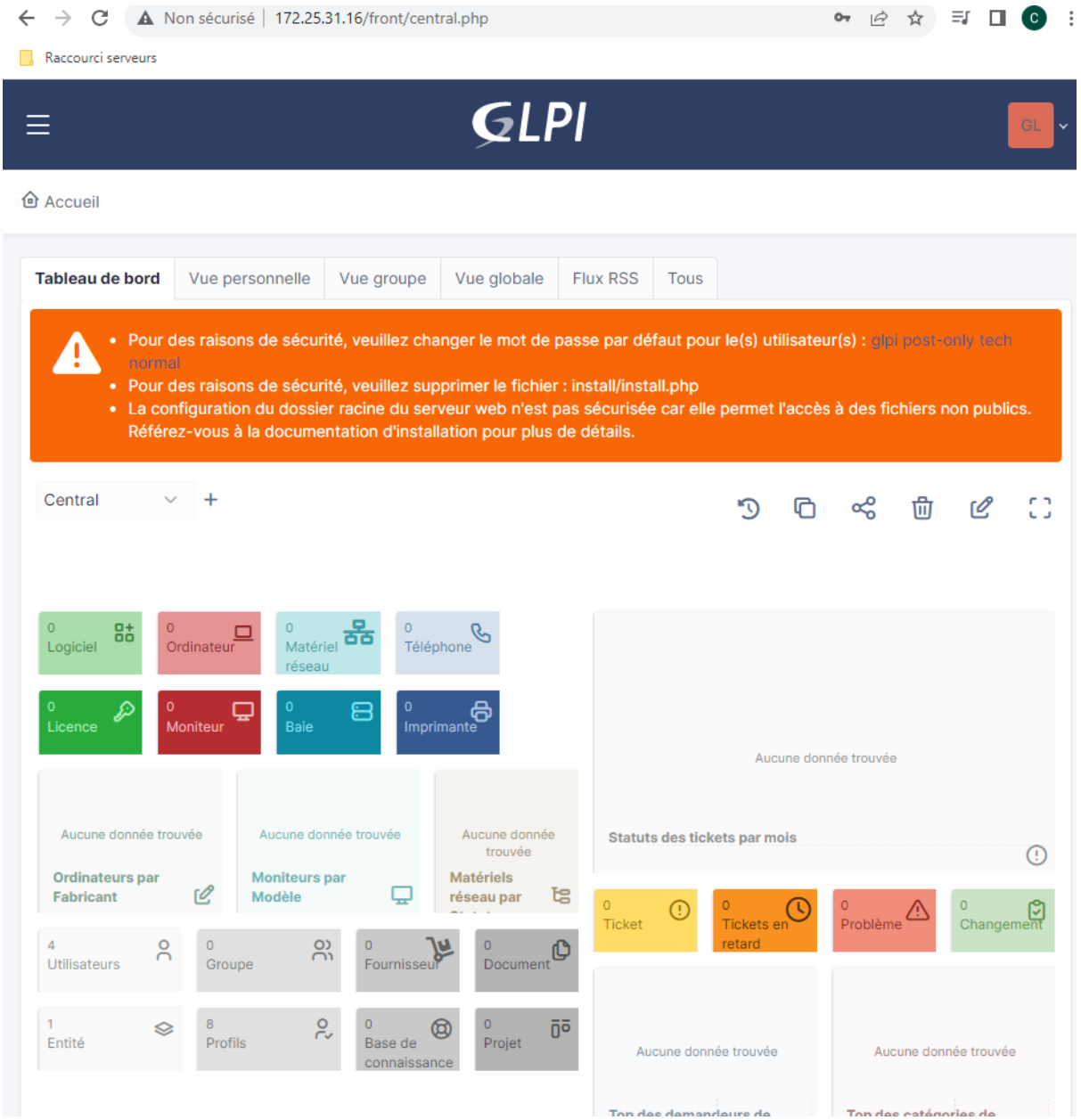

m2l3 - Proxmox Virtual Environm
Setup GLPI
Non sécurisé | 172.25.31.16/glpi/install/install.php
Raccourci serveurs
GLPI SETUP
Sélectionnez votre langue
Français
OK

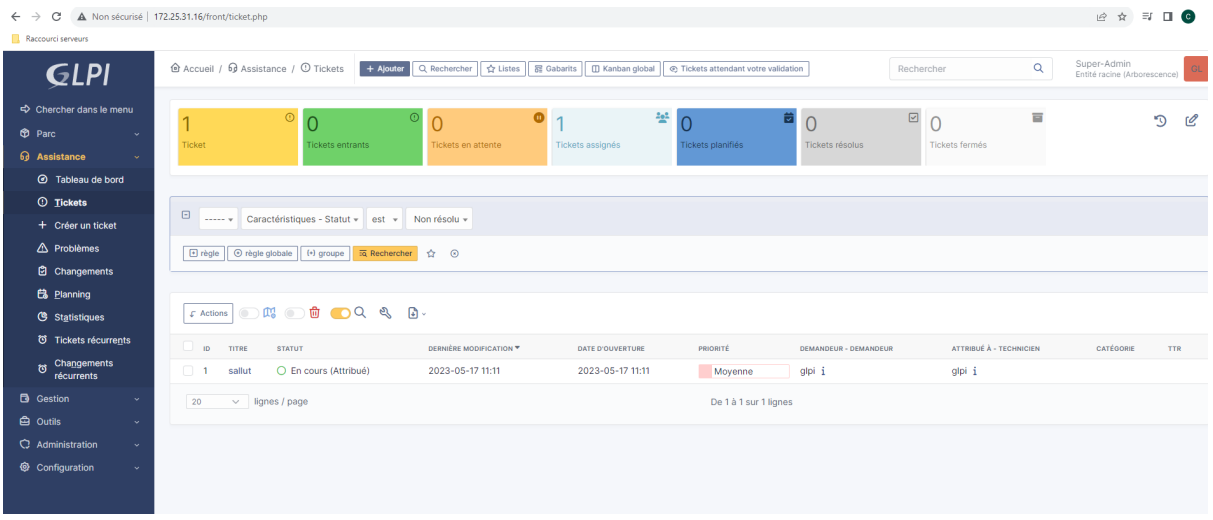

GLPI SETUP
Début de l'installation
Installation ou mise à jour de GLPI
Choisissez 'Installation' pour une nouvelle installation de GLPI.
Choisissez 'Mise à jour' pour lancer la mise à jour de votre version de GLPI à partir d'une version antérieure.
Installer
Mettre à jour

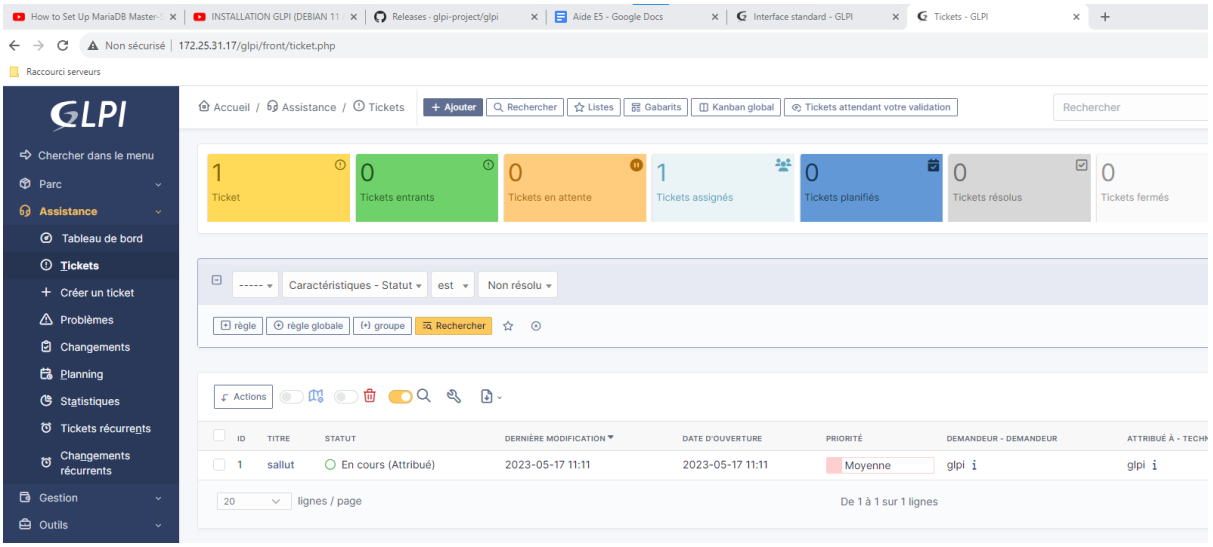

GLPI SETUP
Étape 1
Configuration de la connexion à la base de données
Serveur SQL (MariaDB ou MySQL)
localhost
Utilisateur SQL
glpiuser
Mot de passe SQL
••••
Continuer


**Installation du GLPI sur le second serveur Web, avec la mise en place de la redondance de BDD**

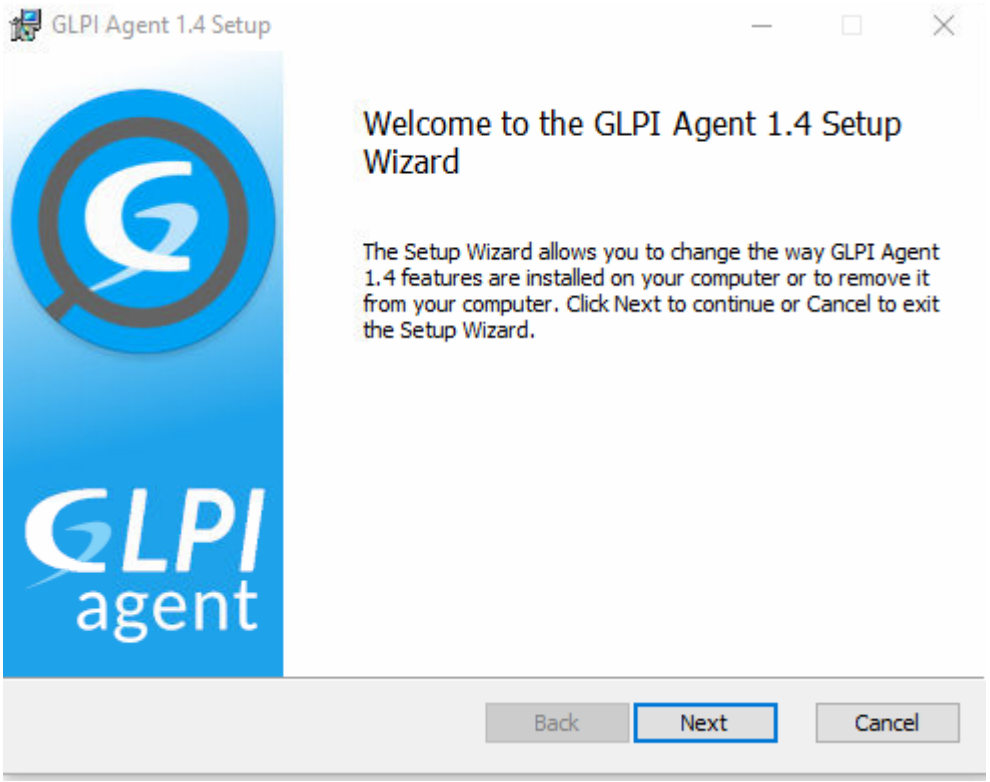


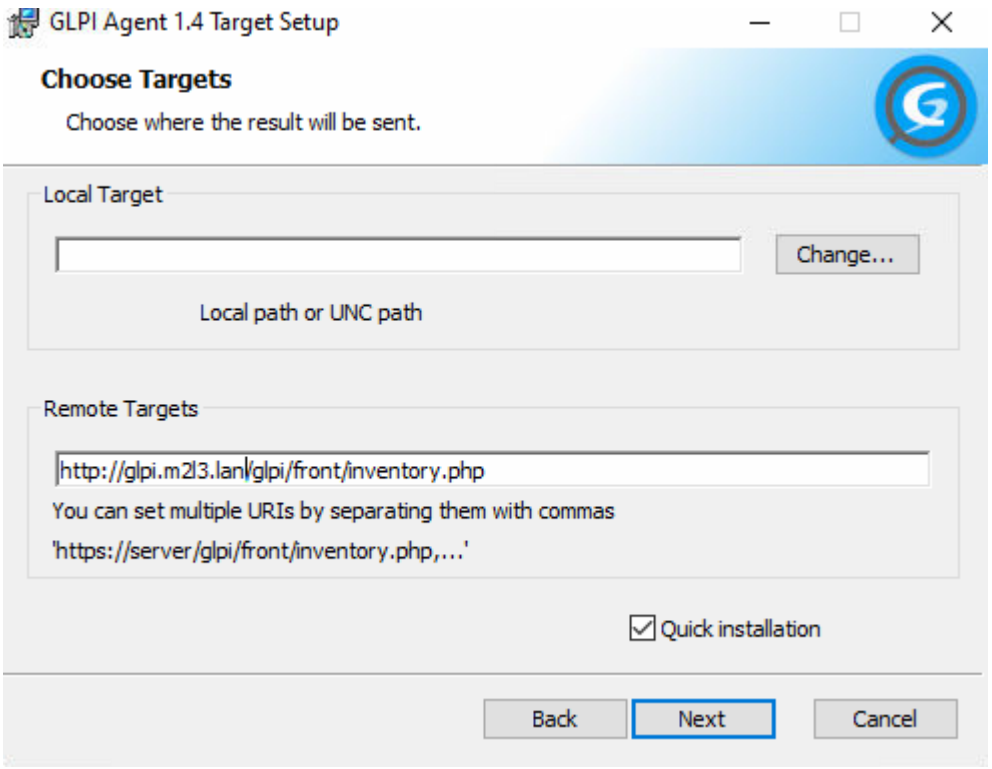

Non sécurisé | 172.25.31.16/front/central.php
Raccourci serveurs
GLPI
GL
Accueil
Tableau de bord
Vue personnelle
Vue groupe
Vue globale
Flux RSS
Tous
Pour des raisons de sécurité, veuillez changer le mot de passe par défaut pour le(s) utilisateur(s) : glpi post-only tech normal
Pour des raisons de sécurité, 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
0 Logiciel
0 Ordinateur
0 Matériel réseau
0 Téléphone
0 Licence
0 Moniteur
0 Baie
0 Imprimante
Aucune donnée trouvée
Ordinateurs par Fabricant
Aucune donnée trouvée
Moniteurs par Modèle
Aucune donnée trouvée
Matériels réseau par
Aucune donnée trouvée
Statuts des tickets par mois
4 Utilisateurs
0 Groupe
0 Fournisseur
0 Document
1 Entité
8 Profils
0 Base de connaissance
0 Projet
0 Ticket
0 Tickets en retard
0 Problème
0 Changement
Aucune donnée trouvée
Aucune donnée trouvée

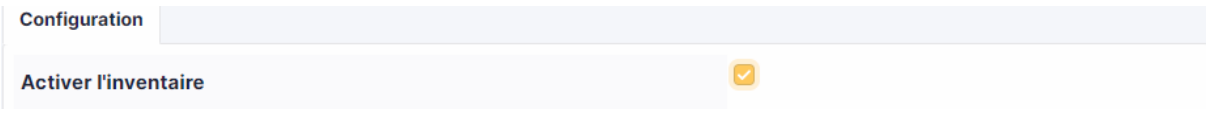

Non sécurisé | 172.25.31.16/front/ticket.php
Raccourci serveurs
GLPI
Accueil / Assistance / Tickets
Ajouter
Rechercher
Listes
Gabarits
Kanban global
Tickets attendant votre validation
Super-Admin
Chercher dans le menu
Parc
Assistance
Tableau de bord
Tickets
Créer un ticket
Problèmes
Changements
Planning
Statistiques
Tickets récurrents
Changements récurrents
Gestion
Outils
Administration
Configuration
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
règle
règle globale
groupe
Rechercher
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
glpi
lignes / page
De 1 à 1 sur 1 lignes




*3.2) Installation de GLPI Agent sur les postes utilisateurs*

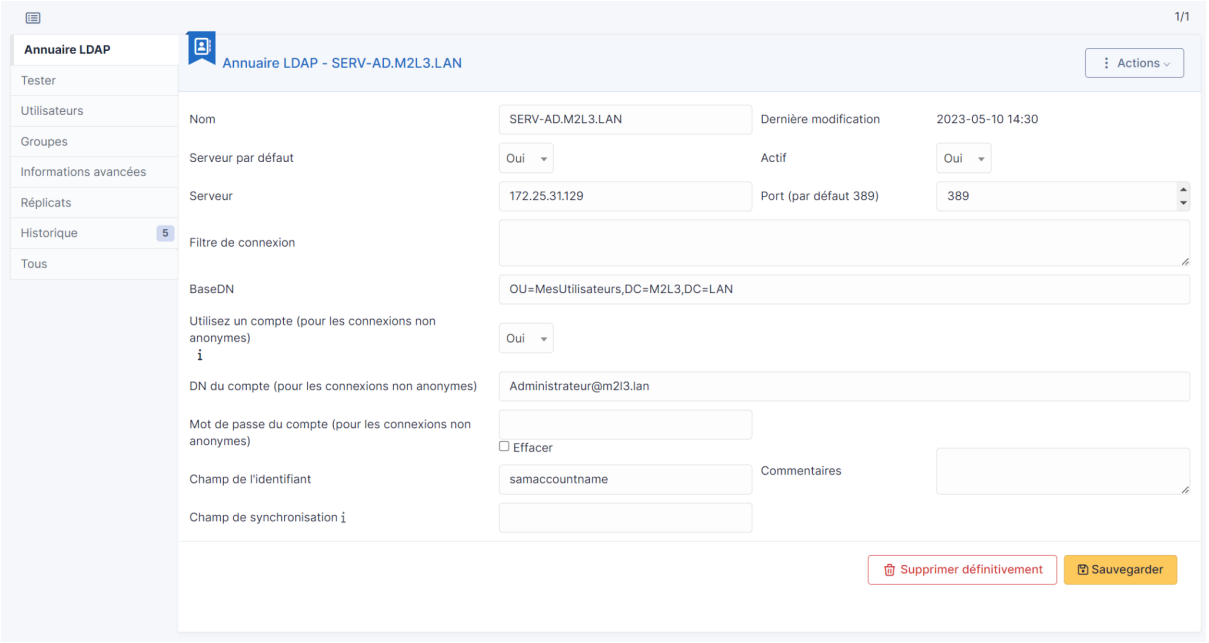





*3.3) Intégration LDAP*

On entre l'adresse IP du serveur Active Directory ou son nom DNS(SERV-AD.M2L3.LAN).Le port utilisé est le port par défaut du LDAP, le port 389.La baseDN correspond à l'arborescence de l'annuaire LDAP de l'Active Directory.On utilise un compte administrateur pour se connecter à l'annuaire LDAP.

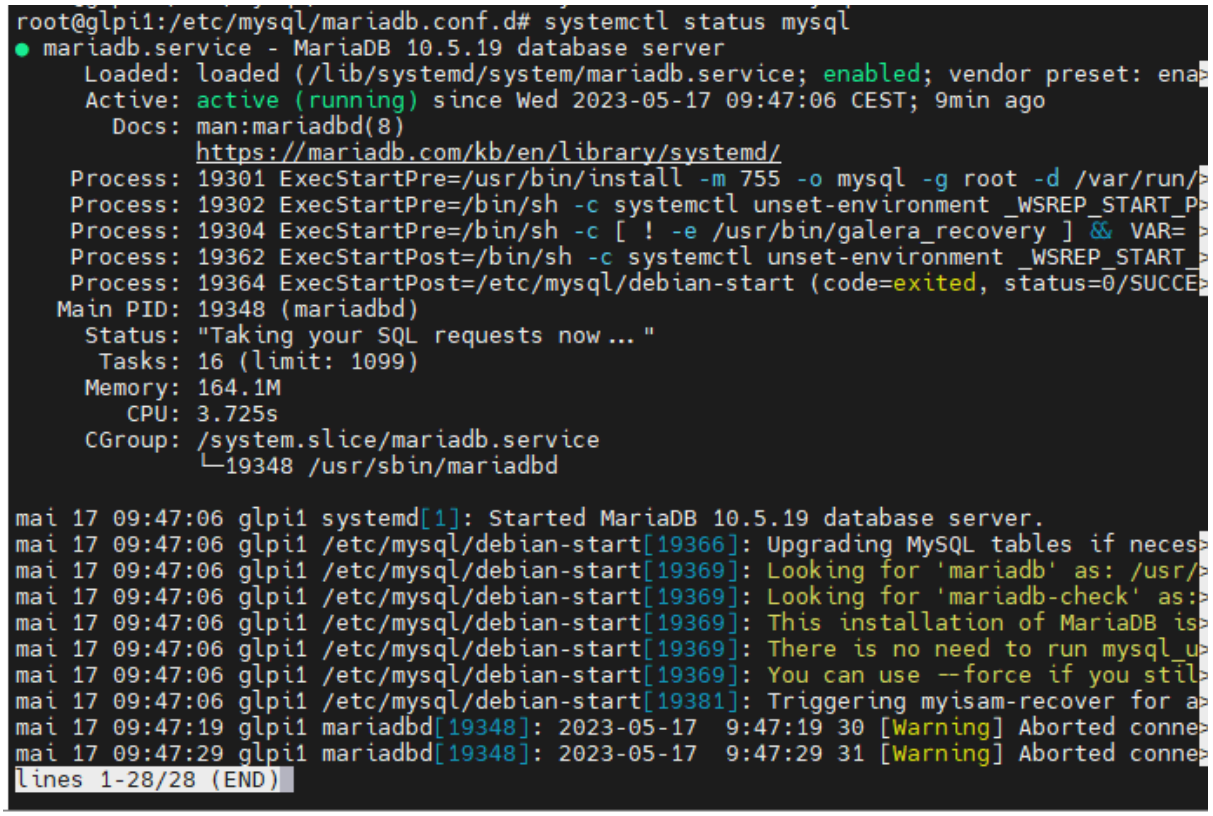


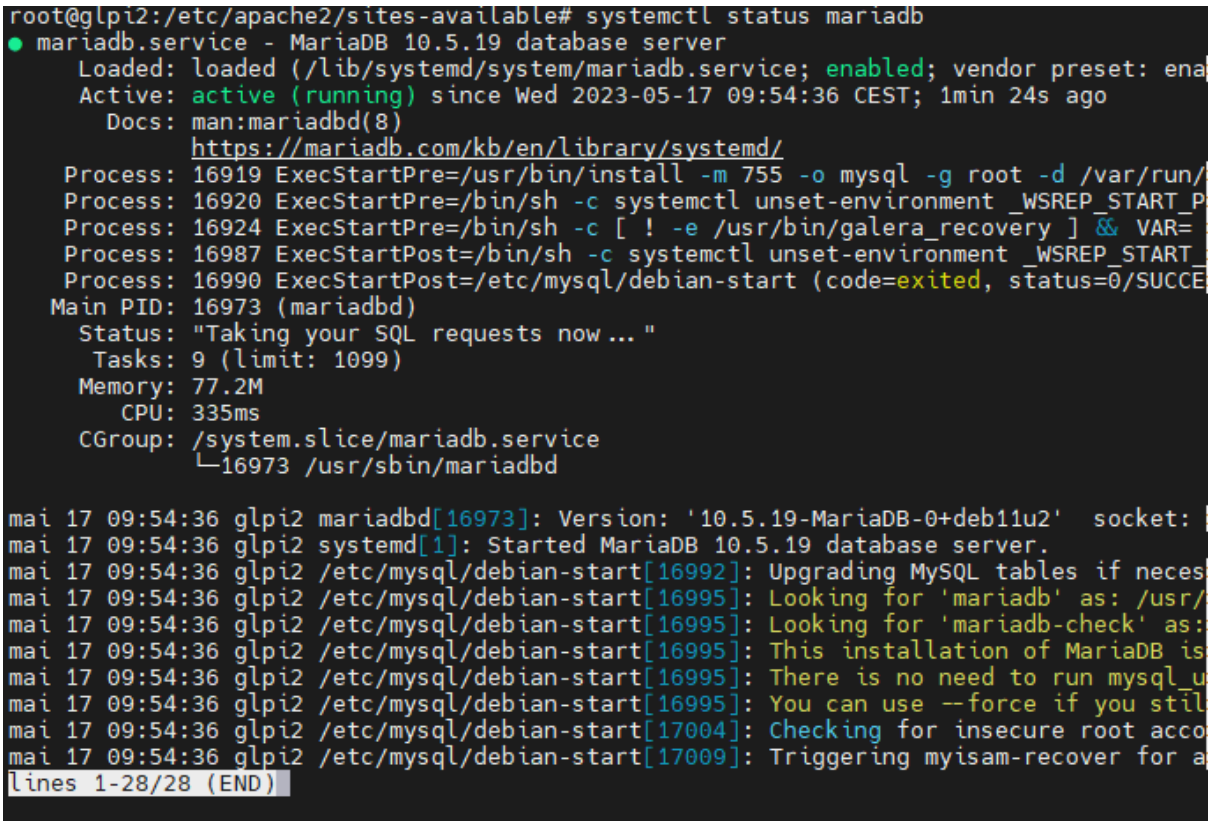
*3.4) Redondance Master-Master de la base de données*

Fiche AP GLPI, How to Configure MySQL Master-Slave Replication on Ubuntu | Debinan
Commande GitHub

Ne pas oublier de créer les fichiers log !

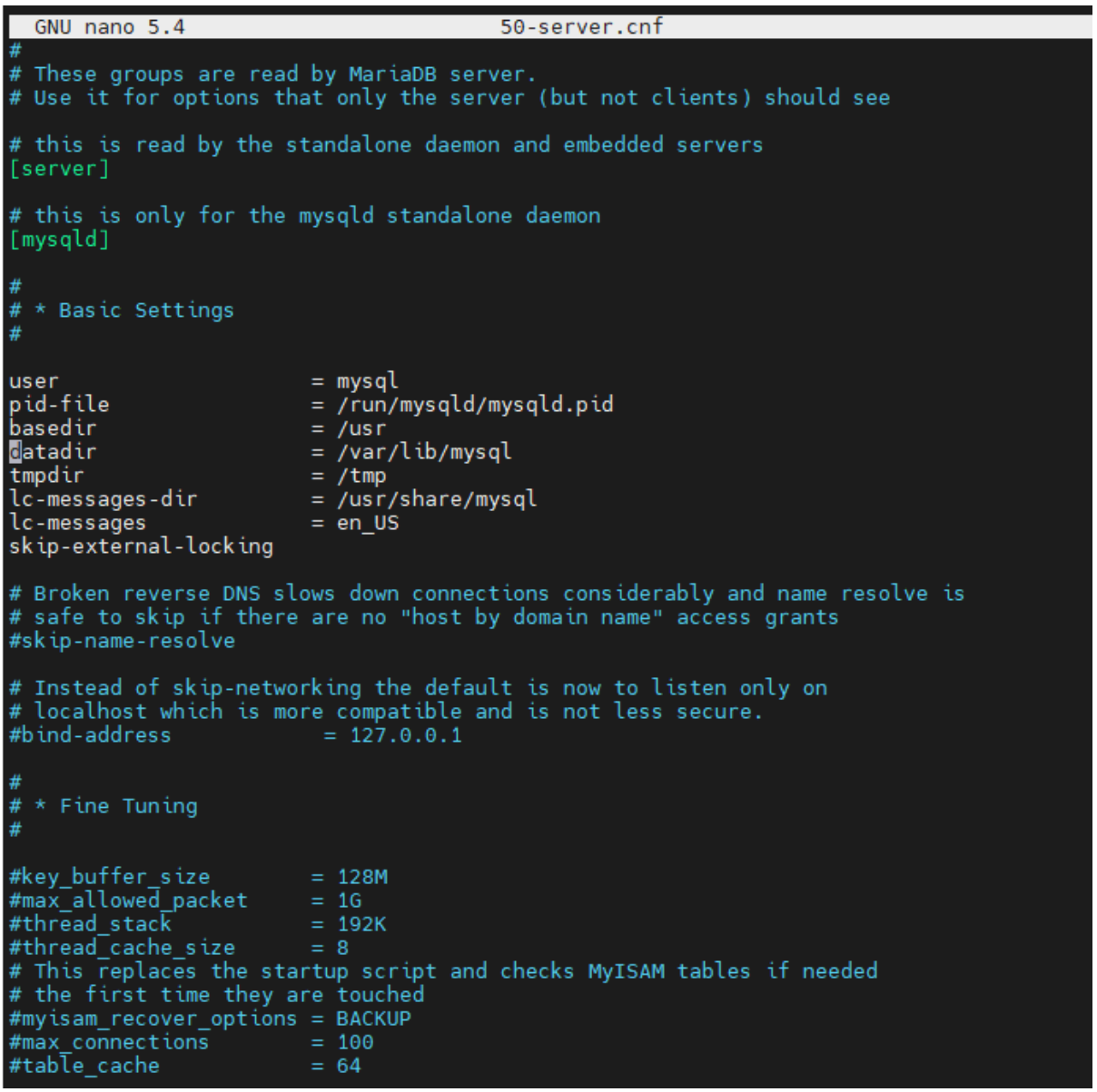
Chaque serveur doit posséder sa propre base de données.






On configure la base de données du serveur maître

On commente la ligne bind-address



```
  GNU nano 5.4                          50-server.cnf
#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
[mysqld]

#
# * Basic Settings
#

user                    = mysql
pid-file                = /run/mysqld/mysqld.pid
basedir                 = /usr
datadir                 = /var/lib/mysql
tmpdir                  = /tmp
lc-messages-dir         = /usr/share/mysql
lc-messages             = en_US
skip-external-locking

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address            = 127.0.0.1

#
# * Fine Tuning
#

#key_buffer_size        = 128M
#max_allowed_packet     = 1G
#thread_stack           = 192K
#thread_cache_size      = 8
# This replaces the startup script and checks MyISAM tables if needed
# the first time they are touched
#myisam_recover_options = BACKUP
#max_connections        = 100
#table_cache            = 64
```

On ajoute ces lignes sur le serveur maître 1

```
[mysqld]

#
# * Basic Settings
#
bind-address = 172.25.31.16
server-id=1
report_host=glpi1
#
log_bin=/var/log/mysql/mariadb-bin
log_bin_index=/var/log/mysql/mariadb-bin.index
#
relay_log=/var/log/mysql/relay-bin
relay_log_index=/var/log/mysql/relay-bin.index
user                    = mysql
pid-file                = /run/mysqld/mysqld.pid
basedir                 = /usr
datadir                 = /var/lib/mysql
tmpdir                  = /tmp
lc-messages-dir         = /usr/share/mysql
lc-messages             = en_US
skip-external-locking
```

Même chose sur le serveur maître 2

```
#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
[mysqld]

#
# * Basic Settings
#

bind-address    = 172.25.31.17
server-id       = 2
report_host     = glpi2
log_bin         = /var/log/mysql/mariadb-bin
log_bin_index   = /var/log/mysql/mariadb-bin.index
relay_log       = /var/log/mysql/relay-bin
relay_log_index = /var/log/mysql/relay-bin.index

user                    = mysql
pid-file                = /run/mysqld/mysqld.pid
basedir                 = /usr
datadir                 = /var/lib/mysql
tmpdir                  = /tmp
lc-messages-dir         = /usr/share/mysql
lc-messages             = en_US
skip-external-locking

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address            = 127.0.0.1

#
# * Fine Tuning
#

#key_buffer_size        = 128M
```

On crée un utilisateur dédié à la synchronisation des bases de données. On effectue les mêmes commandes sur les 2 serveurs maîtres.

```
MariaDB [(none)]> CREATE USER 'rep_user'@'%' IDENTIFIED BY '1234';
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> GRANT REPLICATION SLAVE ON *.* TO 'rep_user'@'%';
Query OK, 0 rows affected (0,004 sec)
```

On vérifie le statut du serveur maître 1

```
MariaDB [(none)]> show master status;
+--------------------+----------+--------------+------------------+
| File               | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+--------------------+----------+--------------+------------------+
| mariadb-bin.000001 |      772 |              |                  |
+--------------------+----------+--------------+------------------+
1 row in set (0,000 sec)
```

On vérifie le statut du serveur maître 2

```
MariaDB [(none)]> show master status;
+--------------------+----------+--------------+------------------+
| File               | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+--------------------+----------+--------------+------------------+
| mariadb-bin.000001 |      772 |              |                  |
+--------------------+----------+--------------+------------------+
1 row in set (0,000 sec)
```

Les positions sont similaires.

On arrête le service slave sur le serveur maître 1.

```
MariaDB [(none)]> stop slave;
Query OK, 0 rows affected, 1 warning (0,000 sec)
```

Sur le premier serveur maître, on implémente la réplication de base de données

```
MariaDB [(none)]> CHANGE MASTER TO
    -> MASTER_HOST='172.25.31.16',
    -> MASTER_USER='rep_user',
    -> MASTER_PASSWORD='1234',
    -> MASTER_LOG_FILE='mariadb-bin.000001',
    -> MASTER_LOG_POS=772;
Query OK, 0 rows affected (0,037 sec)
```

On relance le service slave

```
MariaDB [(none)]> start slave;
Query OK, 0 rows affected (0,001 sec)
```

La réplication est donc active sur le premier serveur maître.

```
MariaDB [(none)]> start slave;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> show slave status\G;
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: 172.25.31.17
                  Master_User: rep_user
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mariadb-bin.000001
          Read_Master_Log_Pos: 772
               Relay_Log_File: relay-bin.000002
                Relay_Log_Pos: 557
        Relay_Master_Log_File: mariadb-bin.000001
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
```

On fait la même chose sur le serveur maître 2.

```
MariaDB [(none)]> show slave status\G;
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: 172.25.31.16
                  Master_User: rep_user
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mariadb-bin.000001
          Read_Master_Log_Pos: 772
               Relay_Log_File: relay-bin.000002
                Relay_Log_Pos: 557
        Relay_Master_Log_File: mariadb-bin.000001
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
              Replicate_Do_DB:
```

On ouvre les ports 3306, 4567,4568 et 4444 pour permettre la communication entre les deux serveurs.

```
To                         Action      From
--                         ------      ----
3306                       ALLOW       Anywhere
22                         ALLOW       Anywhere
80                         ALLOW       Anywhere
443                        ALLOW       Anywhere
4564                       ALLOW       Anywhere
4568                       ALLOW       Anywhere
4444                       ALLOW       Anywhere
3306 (v6)                  ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
4564 (v6)                  ALLOW       Anywhere (v6)
4568 (v6)                  ALLOW       Anywhere (v6)
4444 (v6)                  ALLOW       Anywhere (v6)
```

*3.5) Test de la réplication*

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| glpi               |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0,000 sec)
```

```
MariaDB [(none)]> show slave status\G
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: 172.25.31.16
                  Master_User: rep_user
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mariadb-bin.000002
          Read_Master_Log_Pos: 475
               Relay_Log_File: mysqld-relay-bin.000002
                Relay_Log_Pos: 557
        Relay_Master_Log_File: mariadb-bin.000002
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
                   Last_Errno: 0
                   Last_Error:
                 Skip_Counter: 0
          Exec_Master_Log_Pos: 475
              Relay_Log_Space: 867
              Until_Condition: None
               Until_Log_File:
                Until_Log_Pos: 0
           Master_SSL_Allowed: No
           Master_SSL_CA_File:
           Master_SSL_CA_Path:
              Master_SSL_Cert:
            Master_SSL_Cipher:
               Master_SSL_Key:
        Seconds_Behind_Master: 0
Master_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 0
                Last_IO_Error:
               Last_SQL_Errno: 0
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Master_Server_Id: 1
               Master_SSL_Crl:
           Master_SSL_Crlpath:
                   Using_Gtid: No
                  Gtid_IO_Pos:
      Replicate_Do_Domain_Ids:
  Replicate_Ignore_Domain_Ids:
                Parallel_Mode: optimistic
                    SQL_Delay: 0
          SQL_Remaining_Delay: NULL
      Slave_SQL_Running_State: Slave has read all relay log; waiting for more updates
             Slave_DDL_Groups: 5
Slave_Non_Transactional_Groups: 1
    Slave_Transactional_Groups: 0
1 row in set (0,000 sec)

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| glpi               |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0,000 sec)
```

*3.6) Modification du fichier 000-default.conf*

```
  GNU nano 5.4                          000-default.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/glpi

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

```
root@glpi1:/etc/apache2/sites-available# sudo a2ensite 000-default.conf
Site 000-default already enabled
```

En tapant le nom de domaine du site, on atterrit directement sur le GLPI.

# 4. Sécurité du système

COMMENT SURVEILLER SON RESEAU INFORMATIQUE ? ZABBIX !

*4.1) Supervision via Zabbix*

Installation des paquets nécessaires au fonctionnement de Zabbix :

```
root@zabbix:/home/calvyn# apt install apache2 php php-{mysql,mysqlnd,ldap,bcmath,mbstring,gd,pdo,xml} libapache2
-mod-php mariadb-server mariadb-client
```

Installation du paquet Zabbix :

```
root@zabbix:/# wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+
bian11_all.deb
--2023-04-22 16:09:51--  https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6
-1+debian11_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)… 178.128.6.101, 2604:a880:2:d0::2062:d001
Connexion à repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 3740 (3,7K) [application/octet-stream]
Sauvegarde en : « zabbix-release_6.4-1+debian11_all.deb »

bbix-release_6.4-1+debian 100%[=========================================>]   3,65K  --.-KB/s    ds 0s

023-04-22 16:09:52 (164 MB/s) – « zabbix-release_6.4-1+debian11_all.deb » sauvegardé [3740/3740]
```

On décompresse l’archive :

```
oot@zabbix:/# sudo dpkg -i zabbix-release_6.4-1+debian11_all.deb
Sélection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 146255 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_6.4-1+debian11_all.deb ...
Dépaquetage de zabbix-release (1:6.4-1+debian11) ...
Paramétrage de zabbix-release (1:6.4-1+debian11) ...
```

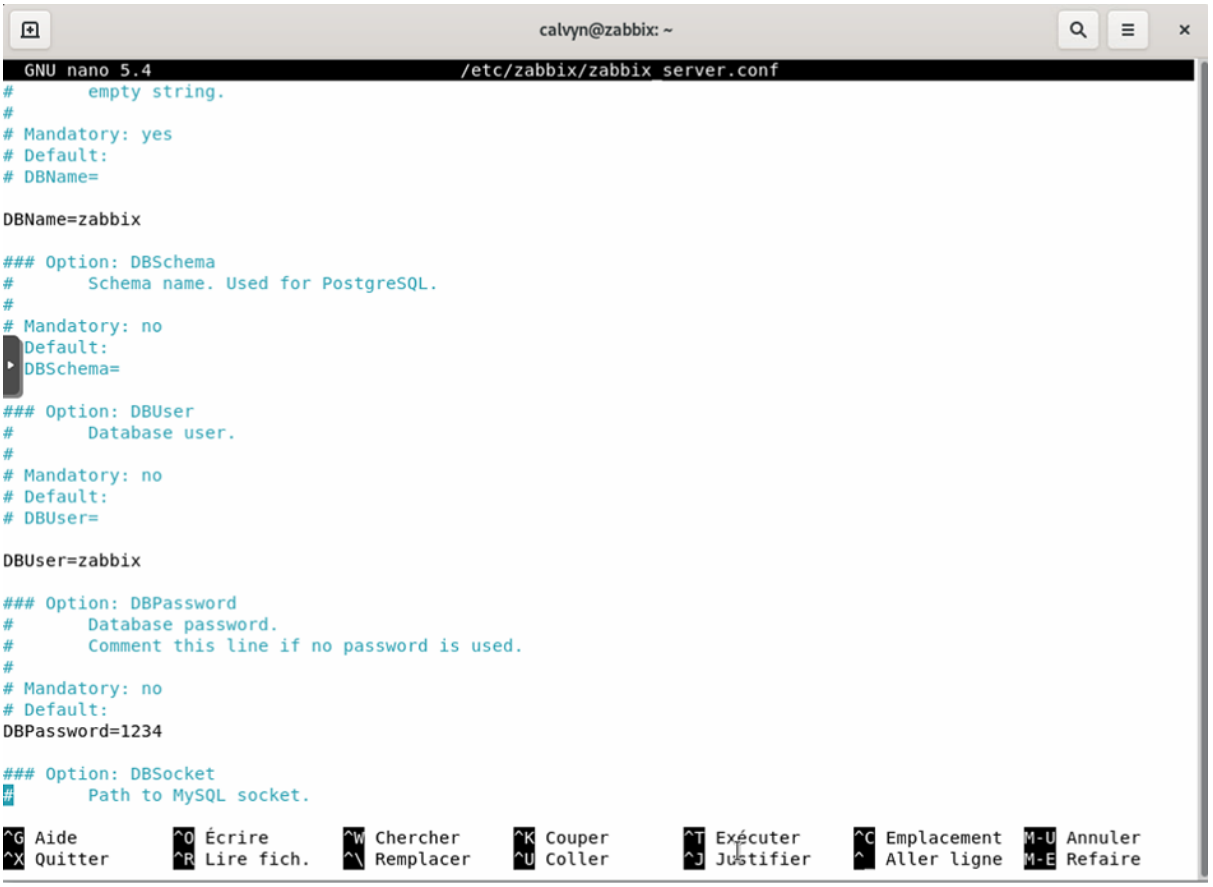
Installation de Zabbix Server, Frontend,Agent

```
root@zabbix:/# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent
```

**On crée la base de données initiale**

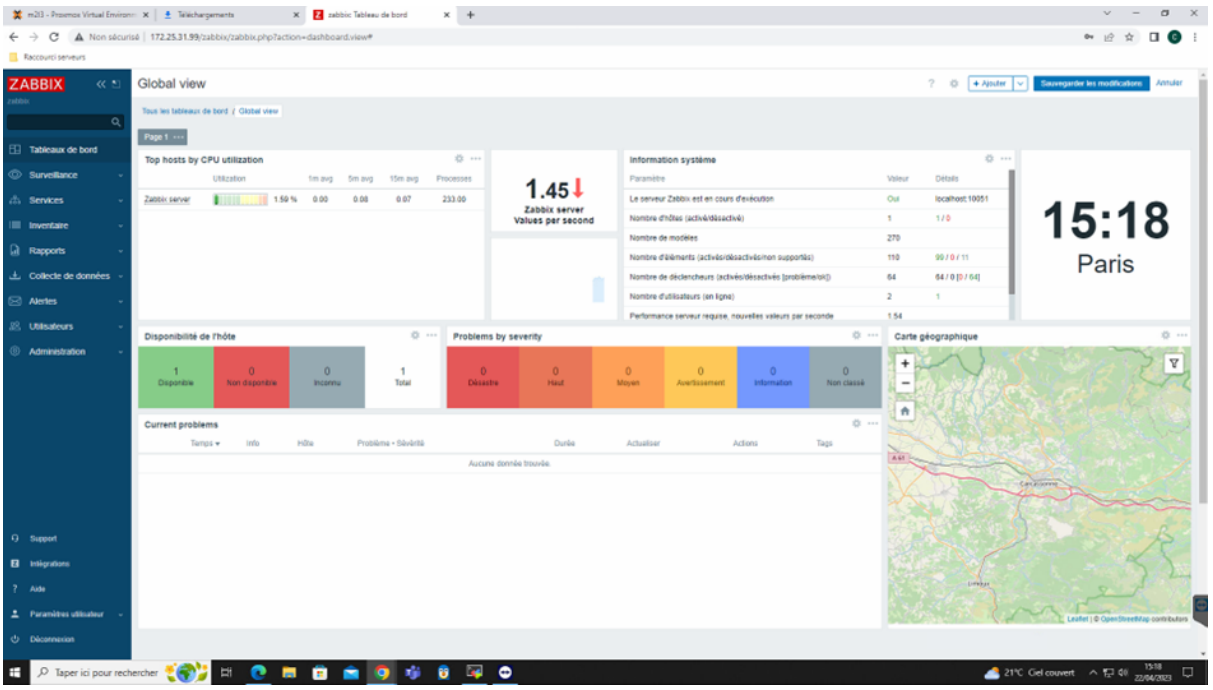
```
MariaDB [(none)]> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected (0,021 sec)

MariaDB [(none)]> create user zabbix@localhost identified by '1234';
Query OK, 0 rows affected (0,017 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,003 sec)

MariaDB [(none)]> quit;
Bye
root@zabbix:/#
```

## 4.1.1) Modification du fichier zabbix_server.conf



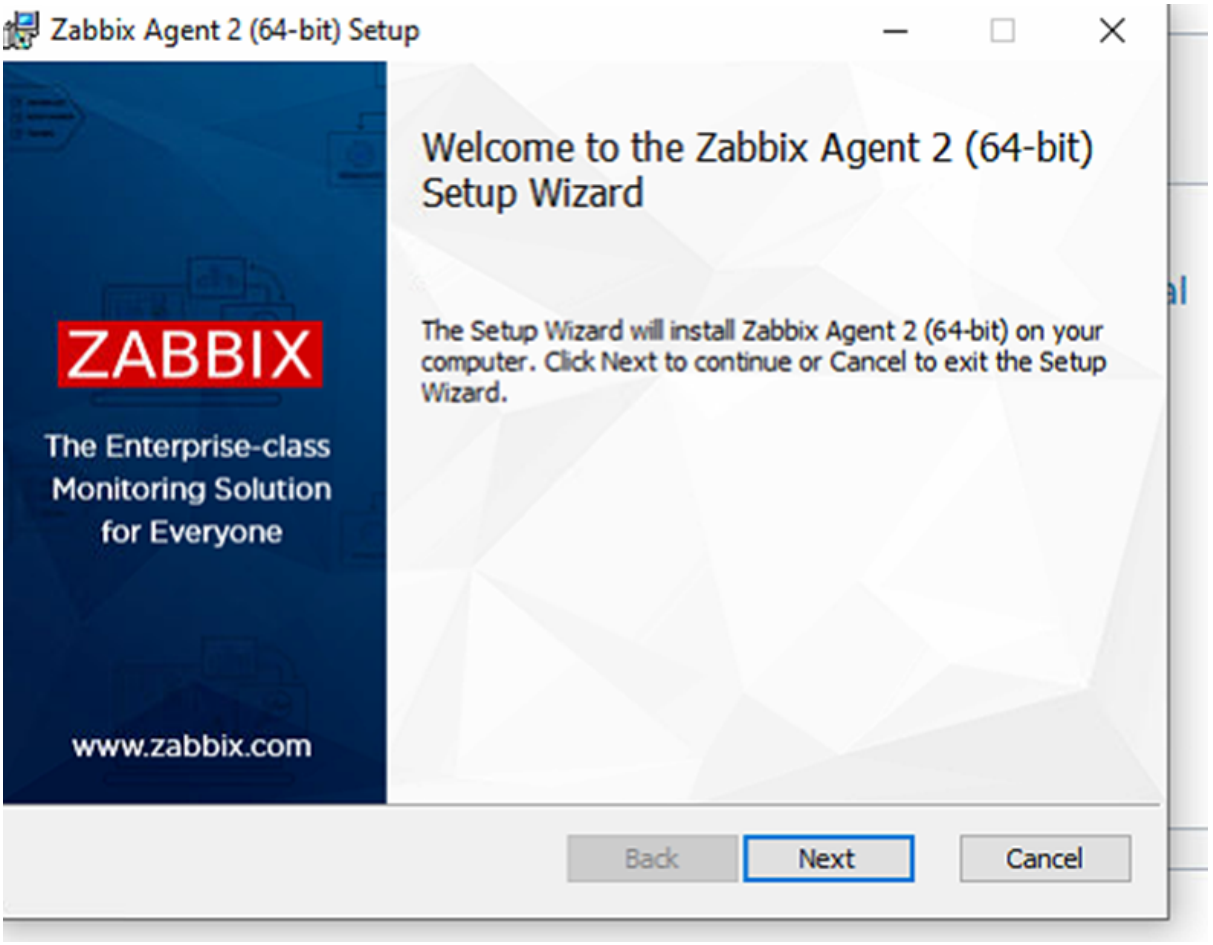
## 4.1.2) On redémarre les services zabbix-server, zabbix-agent et apache2


## 4.1.3) Interface de Zabbix

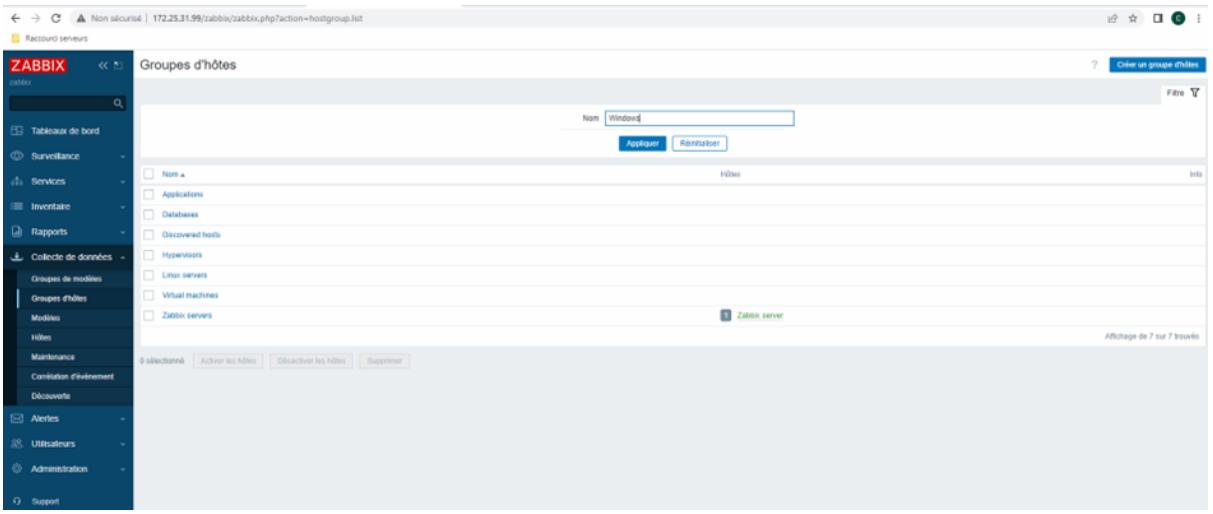




## 4.1.4) Ajout d'un client Windows 10

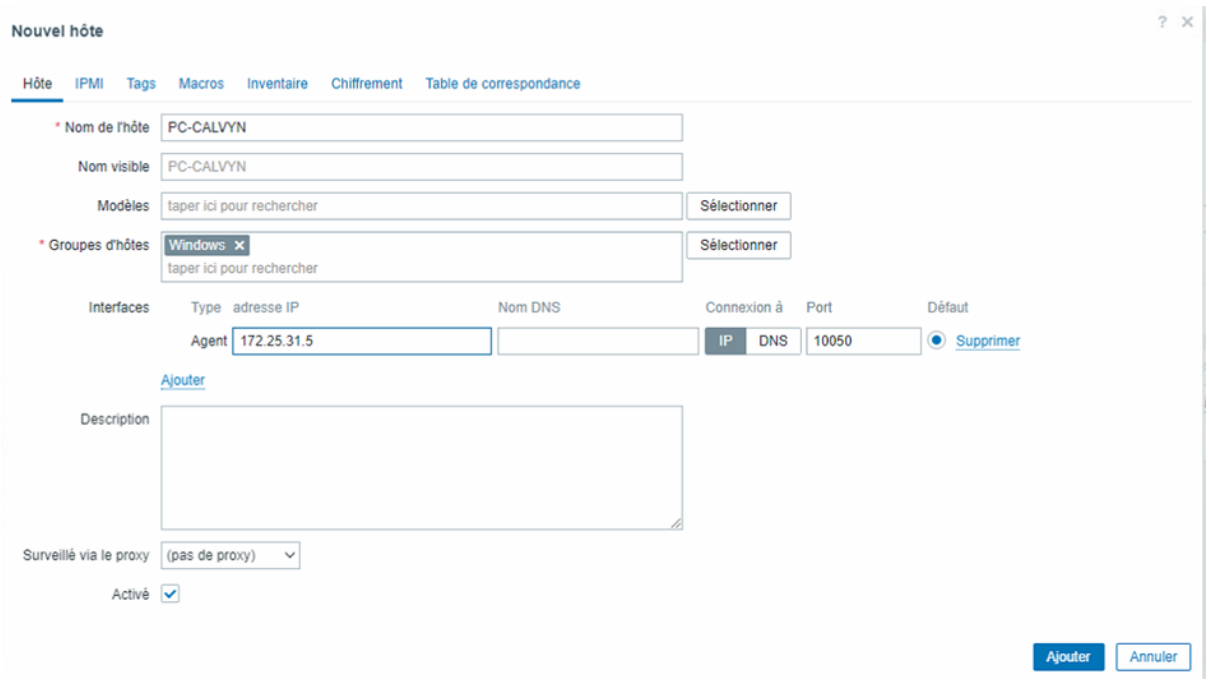
***Installation de l'agent Zabbix***



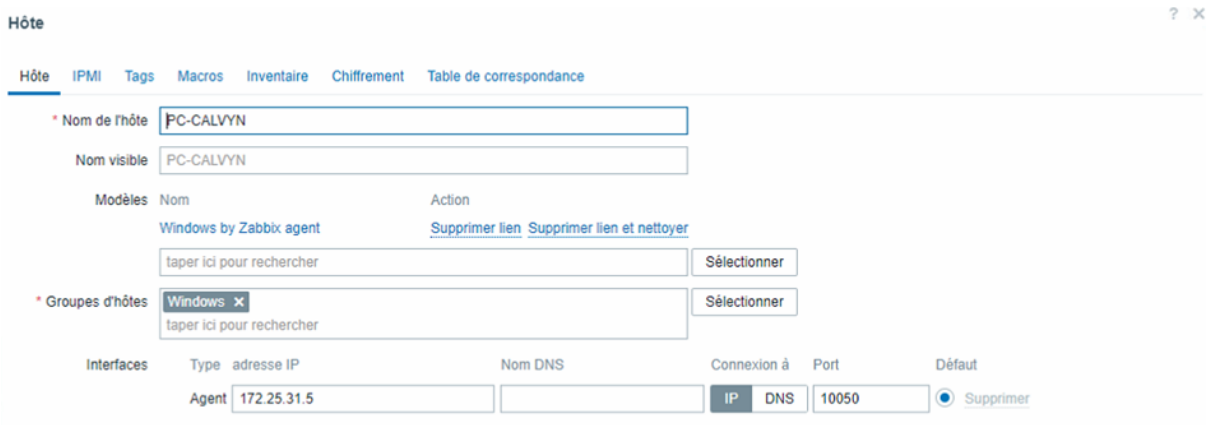

***Création d'un groupe d'hôtes sur le superviseur***




***Création d'un hôte***



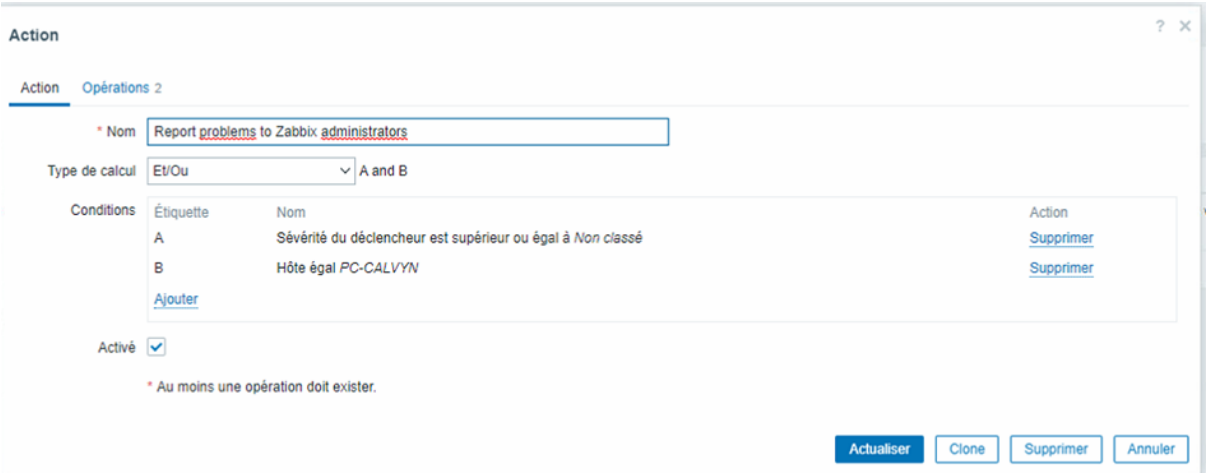

***Ajout d'un modèle à l'hôte***



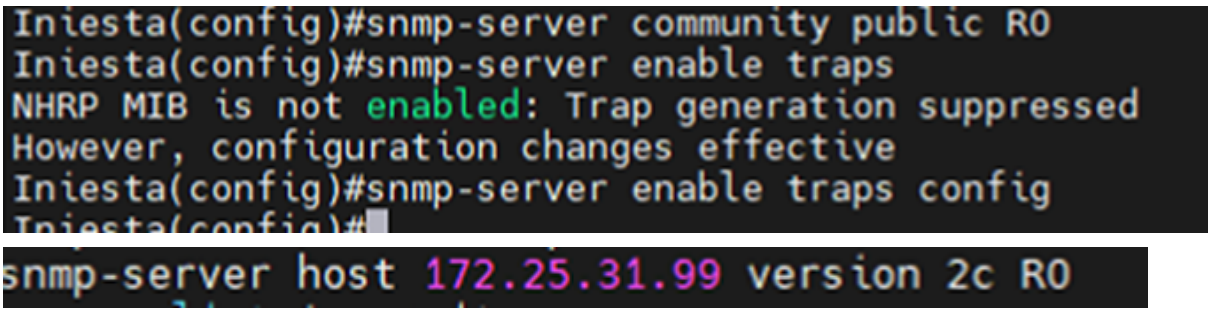

## 4.1.5) Superviser notre infrastructure

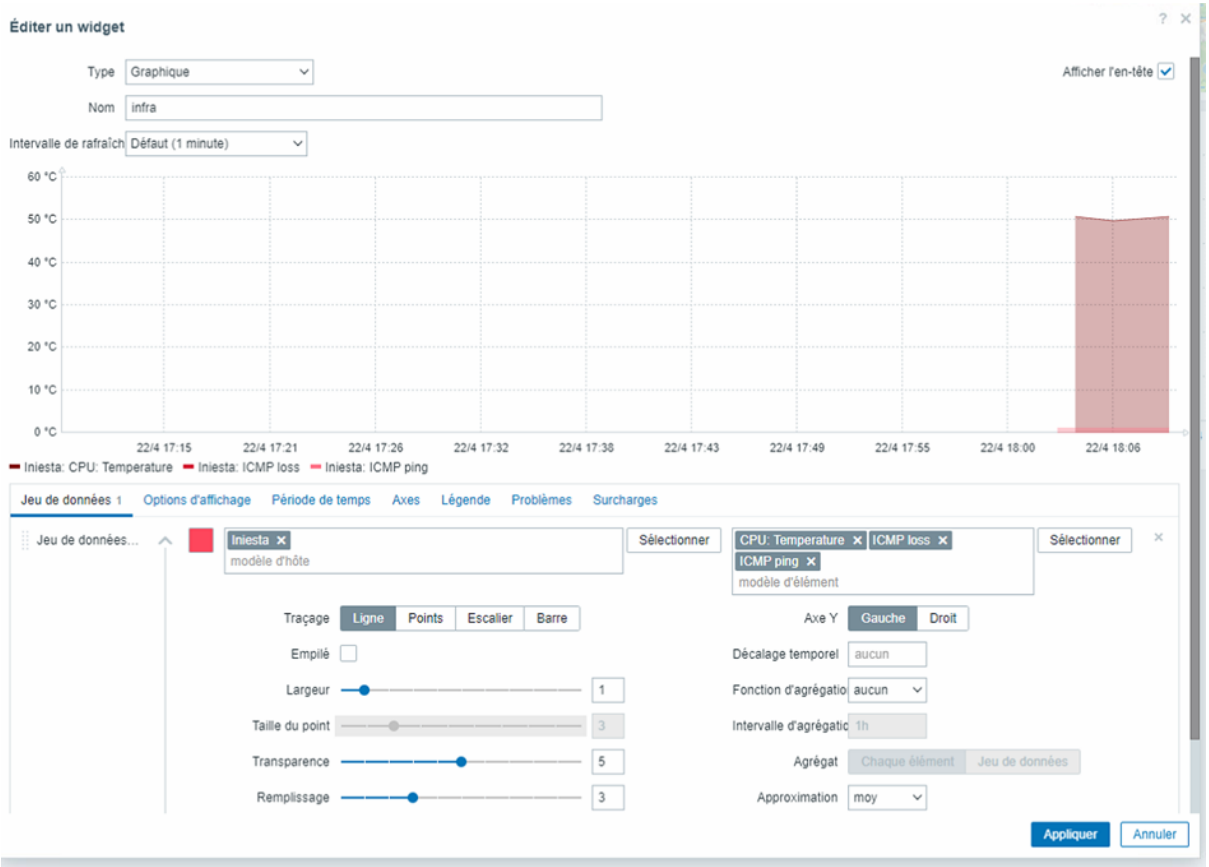
***Création d'un graphique***


***Envoi de mail***

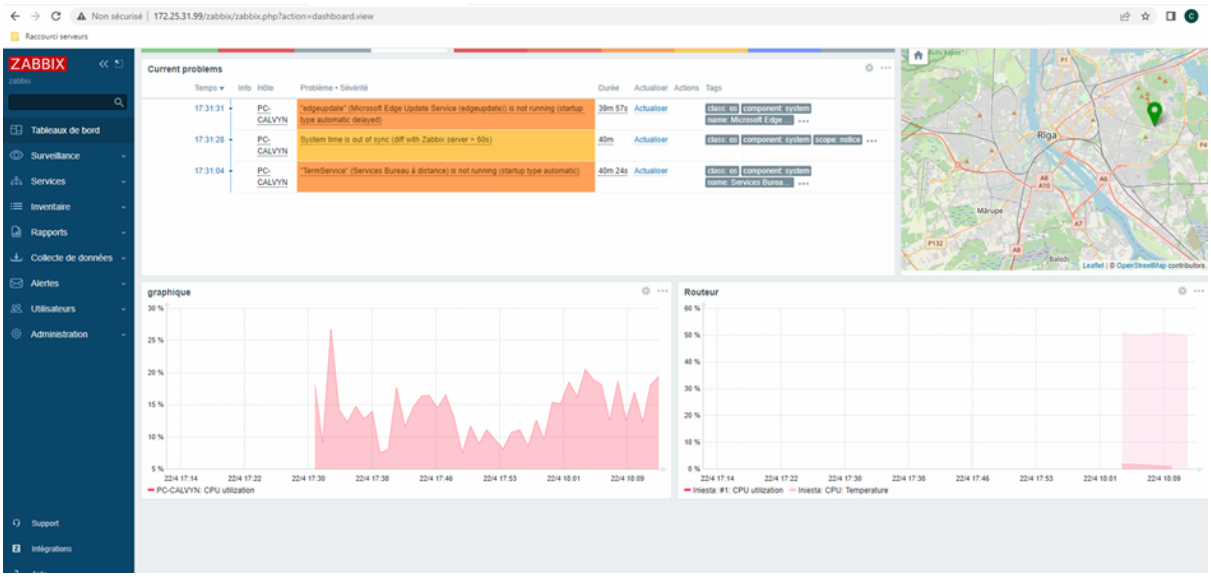

## 4.1.6) Supervision du routeur





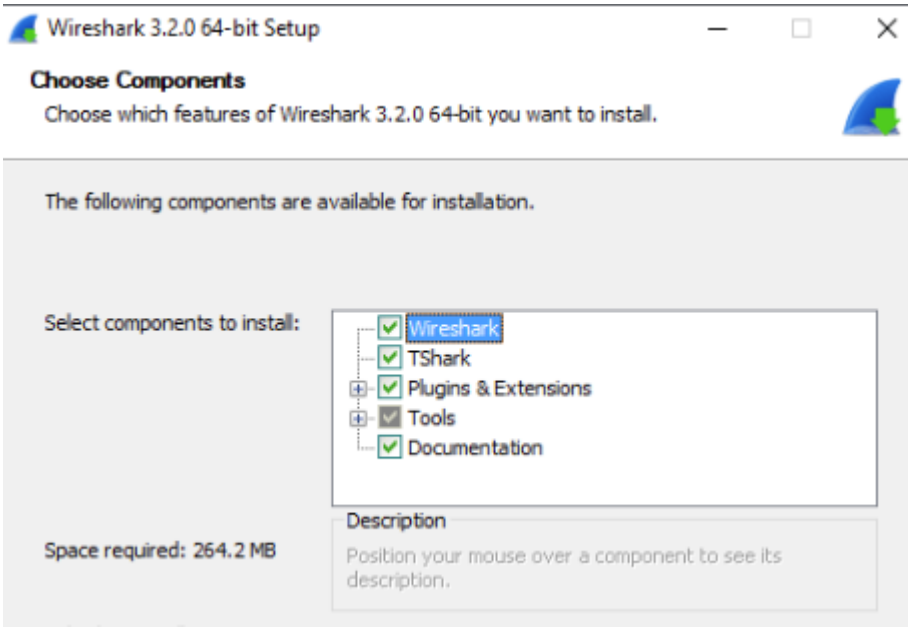

## 4.1.7) Réalisations des tests

Notre PC ainsi que notre routeur sont bien remontés sur notre serveur de supervision Zabbix.

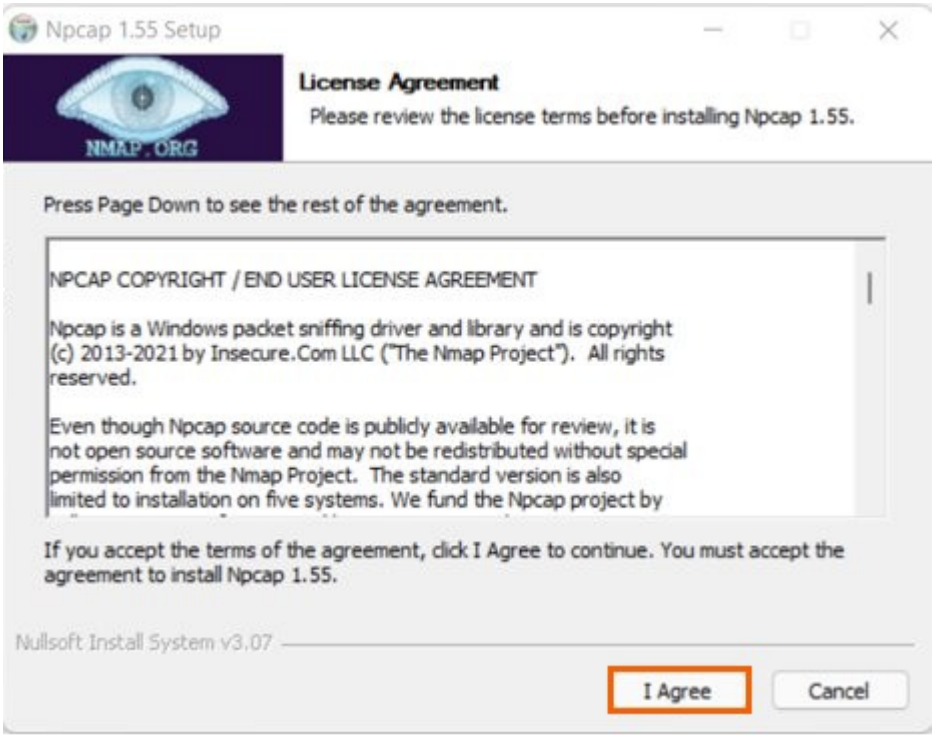


*4.2) Solution d'analyse de paquets*

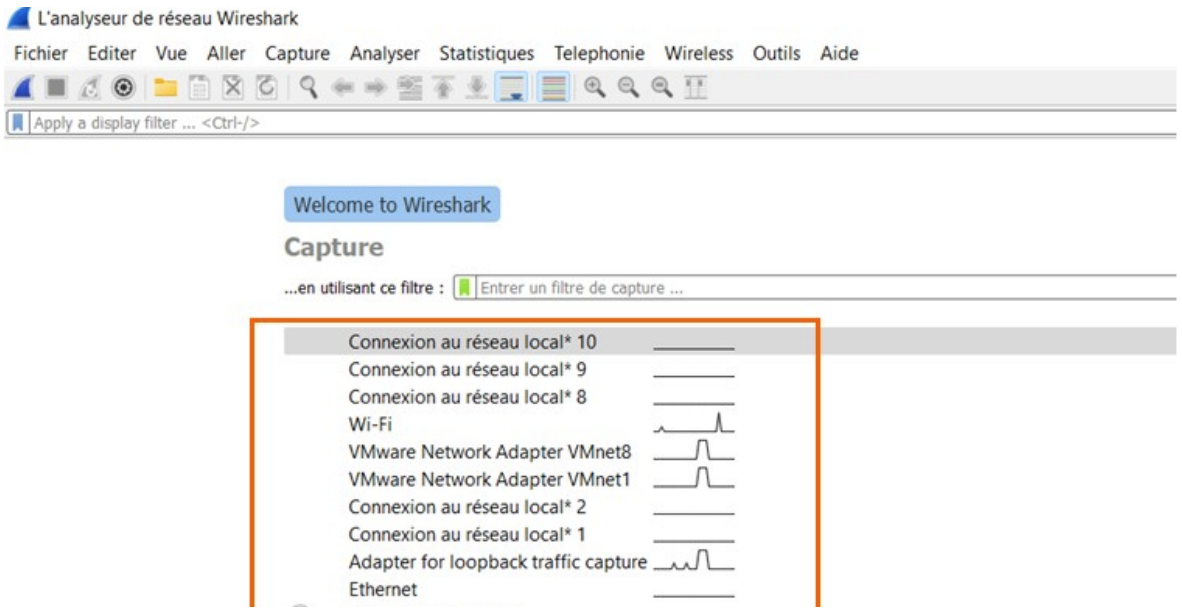
## 4.2.1) Installation de Wireshark



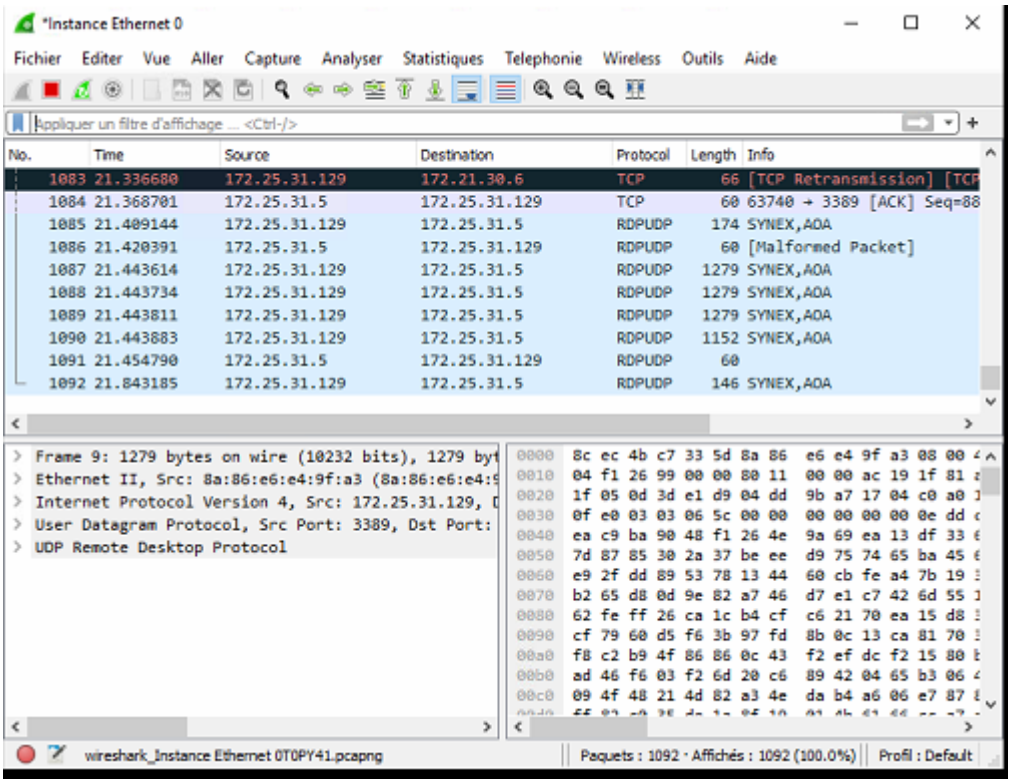

## 4.2.2) Installation de NpCap afin de réaliser des captures



## 4.2.3) Sélection de l’interface réseau

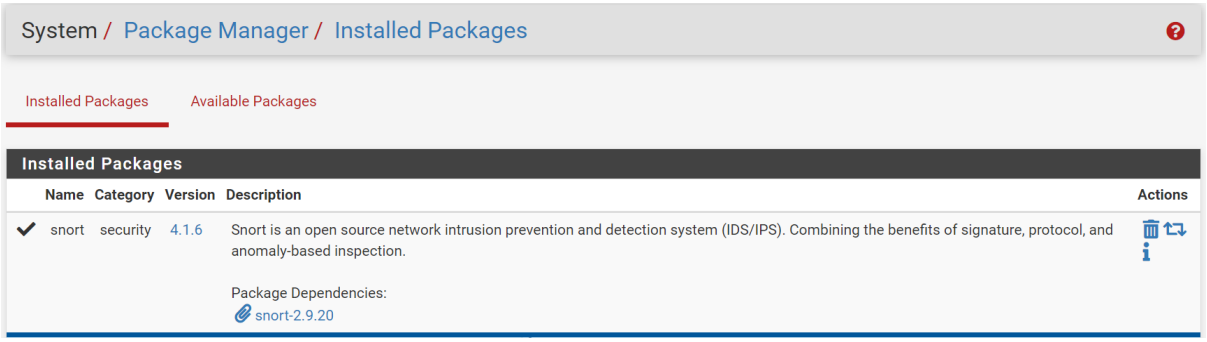



## 4.2.4) Analyse de paquets sur notre infrastructure

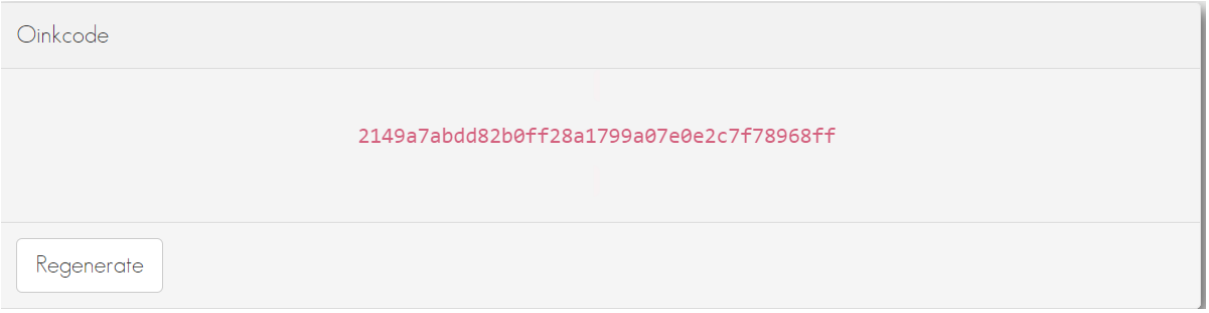



*4.3) Mise en place d’un IDS*

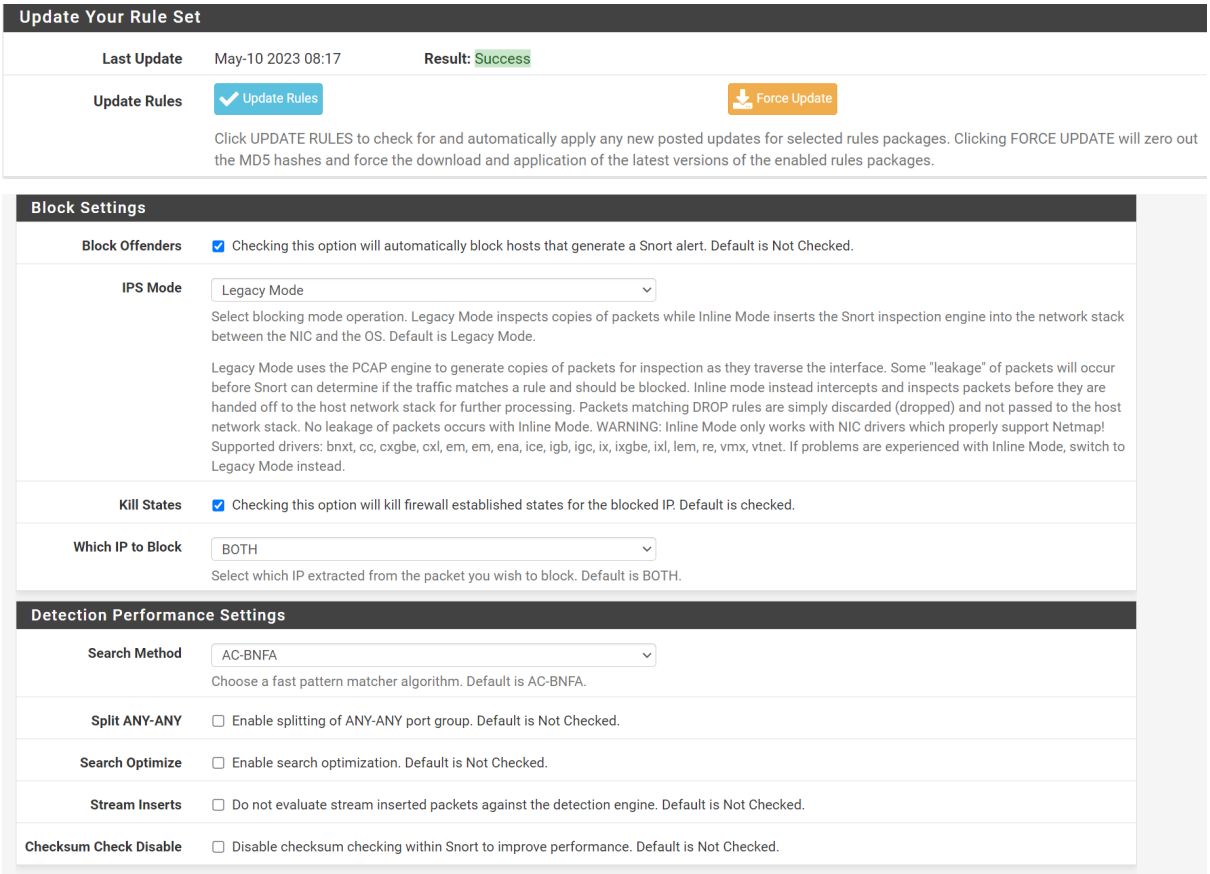
## 4.3.1) Installation du package Snort




## 4.3.2) Récupération d'un token sur le site officiel de Snort




## 4.3.3) Mise en place des règles



## Block Settings

**Block Offenders** — Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

**IPS Mode** — Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

**Kill States** — Checking this option will kill firewall established states for the blocked IP. Default is checked.

**Which IP to Block** — BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

## Detection Performance Settings

**Search Method** — AC-BNFA

Choose a fast pattern matcher algorithm. Default is AC-BNFA.

**Split ANY-ANY** — Enable splitting of ANY-ANY port group. Default is Not Checked.

**Search Optimize** — Enable search optimization. Default is Not Checked.

**Stream Inserts** — Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.

**Checksum Check Disable** — Disable checksum checking within Snort to improve performance. Default is Not Checked.

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

WAN Settings | WAN Categories | WAN Rules | WAN Variables | WAN Preprocs | WAN IP Rep | WAN Logs

## Automatic Flowbit Resolution

**Resolve Flowbits** — If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.

Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

**Auto-Flowbit Rules** — View

Disabling auto-flowbit rules is strongly discouraged for security reasons. Auto-enabled flowbit rules that generate unwanted alerts should have their GID:SID added to the Suppression List for the interface instead of being disabled.

## Snort Subscriber IPS Policy Selection

**Use IPS Policy** — If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.

Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

**IPS Policy Selection** — Balanced

Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.
Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

## Select the rulesets (Categories) Snort will load at startup

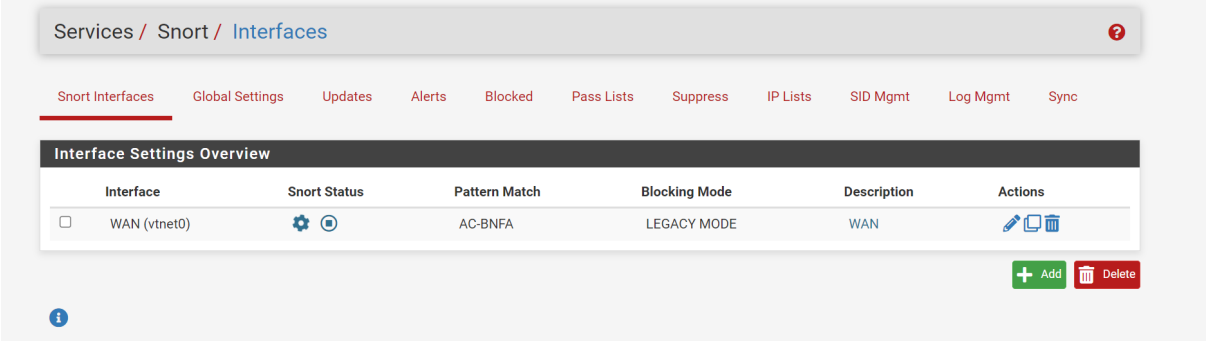
- Category is auto-enabled by SID Mgmt conf files
- Category is auto-disabled by SID Mgmt conf files

Select All | Unselect All | Save

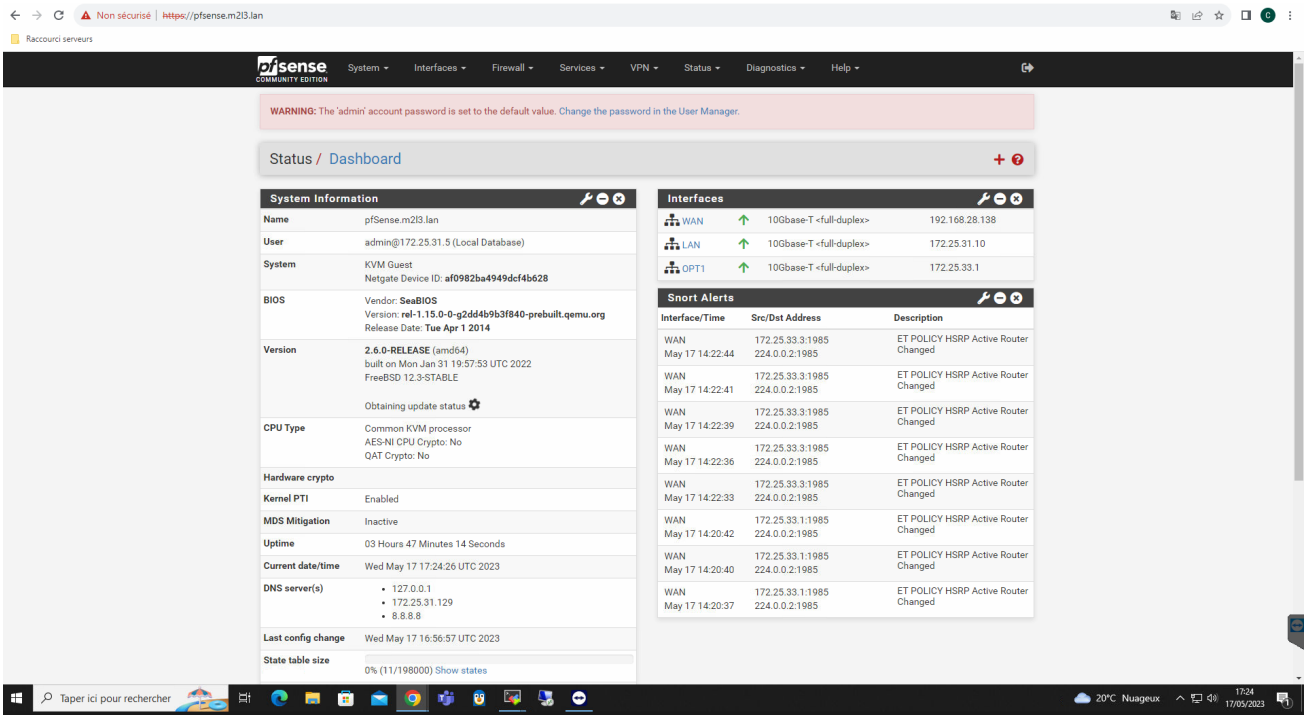
| Enable | Ruleset: Snort GPLv2 Community Rules |
|---|---|
| ☑ | Snort GPLv2 Community Rules (Talos certified) |

| Enable | Ruleset: ET Open Rules | Enable | Ruleset: Snort Text Rules | Enable | Ruleset: Snort SO Rules | Snort OPENAPPID rules are not enabled. |
|---|---|---|---|---|---|---|
| ☑ | emerging-activex.rules | ☐ | snort_app-detect.rules | ☐ | snort_browser-chrome.so.rules | |
| ☑ | emerging-attack_response.rules | ☐ | snort_blacklist.rules | ☐ | snort_browser-ie.so.rules | |

## 4.3.4) Activation de l'interface WAN

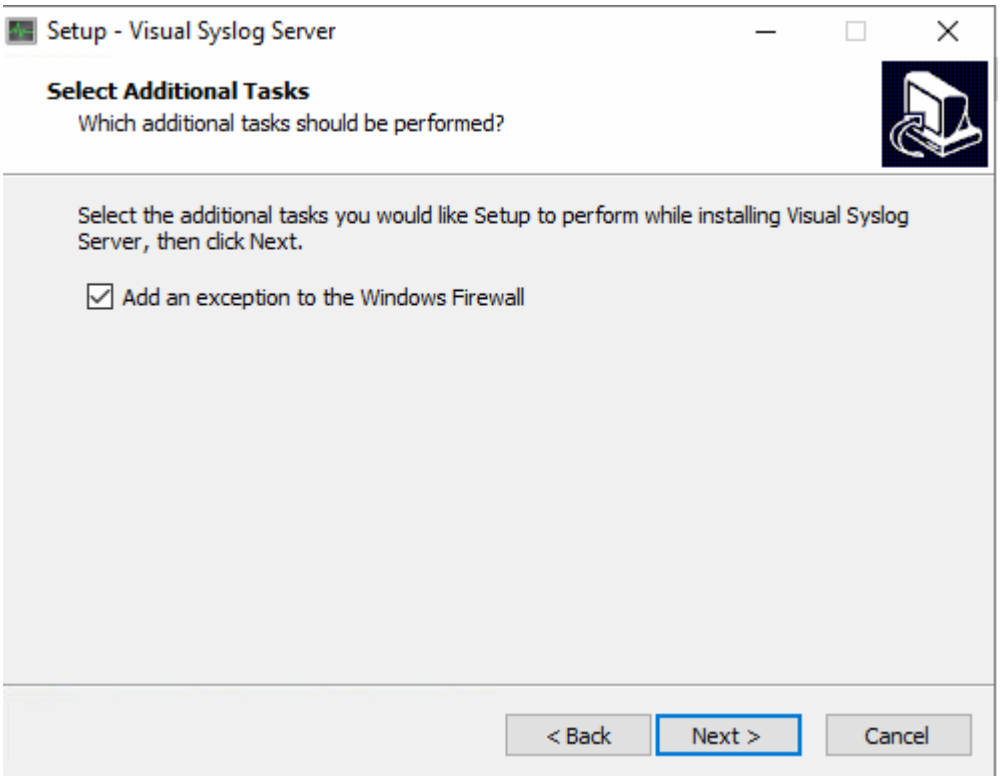


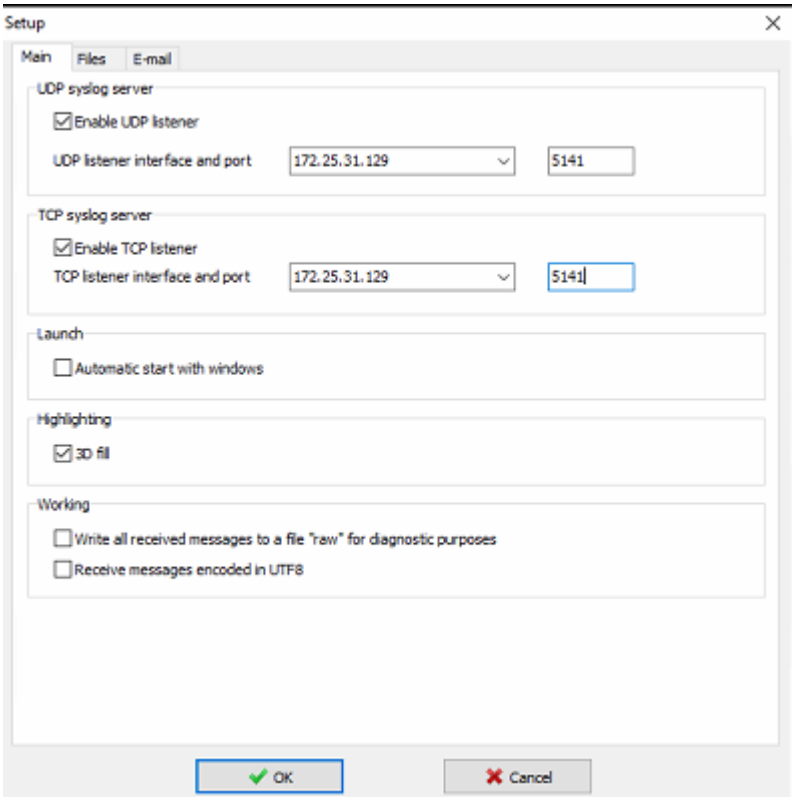

## 4.3.4) Détection des intrusions




*4.4) Système de logs du SI*

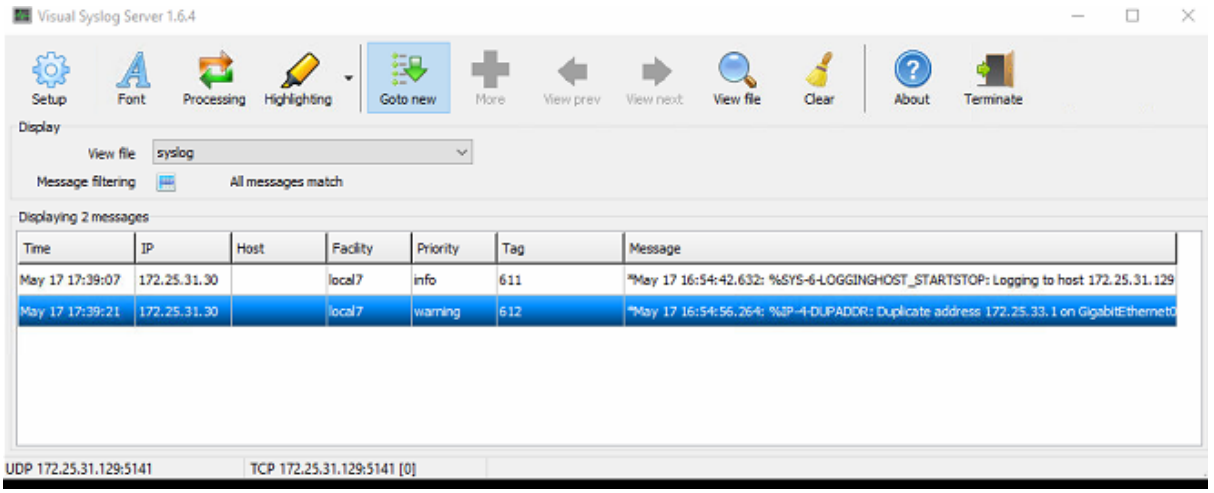
## 4.4.1) Installation de Visual Syslog Server




On envoie le trafic vers notre serveur centralisant les logs.

```
Iniesta(config)#logg
Iniesta(config)#logging on
Iniesta(config)#logging 172.25.31.129
Iniesta(config)#logging trap 6
```




## 4.4.2) Récupération des logs sous Linux

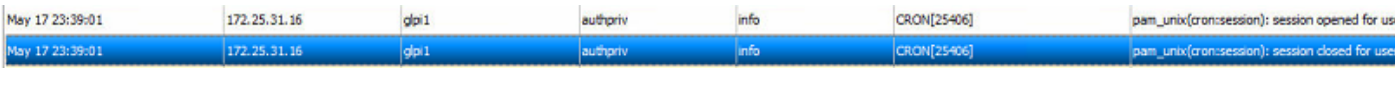
On modifie le fichier rsyslog.conf

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
```

Enfin, on modifie le fichier /etc/rsyslog.d/50-default.conf

```
 GNU nano 5.4                          50-default.conf
auth,authpriv.* @172.25.31.129:514
```

On envoie les informations de connexion vers notre serveur de centralisation de log.




**Solution de Supervision(Zabbix):**

**COMMENT SURVEILLER SON RESEAU INFORMATIQUE ? ZABBIX !**