

# COMPTE RENDU M2L

---

## Table des matières

1	Configuration des interfaces réseaux .....	2
1.1	Interface réseau du Pfsense .....	2
1.2	Interface réseau du Serveur WEB.....	2
1.3	Interface réseau du Serveur GLPI .....	3
2	Configuration des règles de sécurité (Firewall & NAT) .....	3
3	Mise en place du serveur Web Apache (Multi-sites).....	5
4	Installation et configuration du service DNS.....	7
5	Gestion de l'Active Directory et déploiement des utilisateurs .....	10
6	Mise en place de la solution de gestion de parc GLPI.....	15
6.1	Installation : Mise à jour des dépôts, installation des dépendances et sécurisation de la base de données. ....	15
6.2	Configuration de la BDD : .....	17
6.3	Configuration : Déploiement des sources dans /var/www/html/glpi, gestion des droits www-data et activation de l'inventaire dans l'interface.....	18
6.4	Activer l'inventaire GLPI .....	21
6.5	Changer le mot de passe d'un utilisateur .....	22
6.6	Agent : Installation de l'agent GLPI pour remonter les informations du serveur. ....	23
7	Configuration du service DHCP .....	24
7.1	Rôle : Installation du rôle "Serveur DHCP" sur Windows Server.....	24
7.2	Étendue : Création d'une plage d'adresses avec exclusion des IP statiques (routeur et serveurs).....	25
7.3	Options : Renseignement de la passerelle par défaut, du nom de domaine et des serveurs DNS. ....	27

# COMPTE RENDU M2L

---

## 1 Configuration des interfaces réseaux

### 1.1 Interface réseau du PfSense

La première étape consiste à paramétrer les interfaces de la passerelle pfSense:

- Interface WAN (Vtnet2) : 172.16.182.1 / 16                      upstream gateway : 172.16.0.1
- Interface LAN (vtnet0) : 172.17.3.1 /16
- Interface DMZ(Vtnet1) : 10.54.0.1 /24

```
WAN (wan)      -> vtnet2      -> v4: 172.16.182.1/16
LAN (lan)      -> vtnet0      -> v4: 172.17.3.1/16
DMZ (opt1)     -> vtnet1      -> v4: 10.54.0.1/24
```

### 1.2 Interface réseau du Serveur WEB

- Interface réseau du serveur WEB :

```
nano /etc/network/interfaces
```

Puis mettre dans le fichier les paramètres suivants :

```
# The primary network interface
auto ens18
iface ens18 inet static
address 10.54.0.102
netmask 255.255.255.0
gateway 10.54.0.1
dns 172.17.0.100 172.16.0.100 8.8.8.8
```

Enfin, il faut redémarrer les services associés pour valider les paramètres réseaux :

```
systemctl restart networking
```

Résultat de la commande *ip a* afin de voir si les paramètres ont bien été validé :

```
ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:1b:ab:e3 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.54.0.102/24 brd 10.54.0.255 scope global ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe1b:abe3/64 scope link
        valid_lft forever preferred_lft forever
```

# COMPTE RENDU M2L

---

## 1.3 Interface réseau du Serveur GLPI

- Interface réseau du Serveur GLPI

```
nano /etc/network/interfaces
```

Puis mettre dans le fichier les paramètres suivants :

```
# The primary network interface
auto ens18
iface ens18 inet static
Address 10.54.0.100
Netmask 255.255.255.0
Gateway 10.54.0.1
Dns 172.17.0.100 172.16.0.100 8.8.8.8
```

Enfin, il faut redémarrer les services associés pour valider les paramètres réseaux :

```
systemctl restart networking
```

Résultat de la commande *ip a* afin de voir si les paramètres ont bien été validé :

```
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:2b:53:92 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.54.0.100/24 brd 10.54.0.255 scope global ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe2b:5392/64 scope link
        valid_lft forever preferred_lft forever
```

## 2 Configuration des règles de sécurité (Firewall & NAT)

- Attribution d'une adresse IP statique (le serveur DHCP n'étant pas encore fonctionnel) afin de configurer les règles de parefeu /NAT
  - Adresse IP (CIDR) : 172.17.3.10 /16
  - Passerelle par défaut : 172.17.3.1
  - DNS préféré : 172.17.3.100 (futur serveur LDAP)

# COMPTE RENDU M2L

La configuration se fera à partir du PC sur l'interface LAN du pfSense (172.17.3.1).

## Règles interface WAN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/29 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input type="checkbox"/>	0/0 B	IPv4 TCP	WAN subnets	22 (SSH)	10.54.0.102	22 (SSH)	*	none			

La règle dans le WAN permet depuis le réseau SIO (WAN) de pouvoir me connecter au serveur WEB en SSH.

## Règles Interface LAN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2/1.08 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	80 (HTTP)	DMZ subnets	80 (HTTP)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	443 (HTTPS)	DMZ subnets	443 (HTTPS)	*	none			
<input type="checkbox"/>	3/1.28 GiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	DMZ subnets	*	LAN subnets	*	*	none			

Permet au LAN de communiquer avec la DMZ sans restriction mais si par la suite nous décidons de ne plus donner un accès total, la règle 1 permet au serveur de pouvoir accéder en http à internet afin de télécharger des mises à jour et/ou des nouvelles fonctionnalités. Les règles 2 et 3 permettent aux PC du LAN d'accéder au serveur WEB et GLPI en http et https.

## Règles Interface DMZ

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.54.0.100	22 (SSH)	WAN subnets	22 (SSH)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	LAN subnets	*	DMZ subnets	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	DMZ subnets	443 (HTTPS)	LAN subnets	443 (HTTPS)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.54.0.100	80 (HTTP)	LAN subnets	80 (HTTP)	*	none			
<input checked="" type="checkbox"/>	0/3 KiB	IPv4 *	DMZ subnets	*	*	*	*	none		DMZ accès internet	

Elles rejoignent les règles précédentes.

# COMPTE RENDU M2L

## 3 Mise en place du serveur Web Apache (Multi-sites)

Hébergement de deux sites distincts sur un serveur Linux:

- Installation : Services apache2

```
apt-get install apache2 -y
```

- **Arborescence** : Création des répertoires site1 et site2 avec personnalisation des fichiers html

Il faut ensuite aller dans /var/www/html afin de créer les deux pages du site.

Je vais copier la page par défaut et la dupliquer dans des dossiers pour chaque page.

Je vais d'abord créer un dossier Site1 et un dossier site2.

```
mkdir site1 && mkdir site2
```

Il faut maintenant copier le dossier index et le coller dans chaque répertoire avec le nom qui convient.

```
cp index.html /var/www/html/site1/site1 && cp index.html /var/www/html/site2/site2
```

Maintenant, il faut modifier les pages afin de les différencier. Pour cela, il faut modifier les pages html que nous venons de copier. Une simple modification suffit (changer le titre du Site, le contenu, etc)

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Debian Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}
body, html {
padding: 3px 3px 3px 3px;
background-color: #D0DBE2;
font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}
div.main_page {
position: relative;
display: table;
width: 800px;
margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;
border-width: 2px;
border-color: #212738;
border-style: solid;
background-color: #FFFFFF;
text-align: center;
}
div.page_header {
height: 39px;
width: 100%;

```

Nous arrivons ensuite sur cette page. Nous allons juste changer le titre de la page ou apporter une modification afin de différencier cette page de la page index. J'ai change le titre de la page dans <head> <Title> en mettant « Site1 » puis j'ai change le contenu de la page en mettant « Bienvenue sur le site1 de la M2L »

# COMPTE RENDU M2L

---

J'ai apporté les mêmes modifications sur la page du site 2 en adaptants les modifications au site2.  
Afin d'éviter tout problème par la suite, je vais supprimer le fichier index.html

```
rm index.html
```

- **Virtual Hosts** : Création et activation des fichiers de configuration site1.conf et site2.conf dans site available.

Ensuite il faut activer les sites et donner le chemin afin de pouvoir y avoir accès.

Pour se faire il faut aller dans /etc/apache2/sites-available/

Encore une fois, il est possible de copier le fichier 000-default.conf et de l'adapter pour chaque site.

A cette étape, il n'est pas obligatoire de créer un dossier pour chaque site . Il est permis de mettre les fichiers de conf dans le même répertoire. Le premier s'appellera site1.conf et le deuxième site2.conf.

Place maintenant à la modification du fichier site1.conf.

```
nano /etc/apache2/site-available/site1.conf
```

Il faut mettre ces informations :

```
<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
    ServerName site1.182.sio
    DocumentRoot /var/www/html/site1
```

Puis faire les mêmes changements pour le site 2.

Maintenant, il faut activer les sites.

```
a2ensite site1.conf && a2ensite site2.conf
```

Puis ne pas oublier de redémarrer les services apache

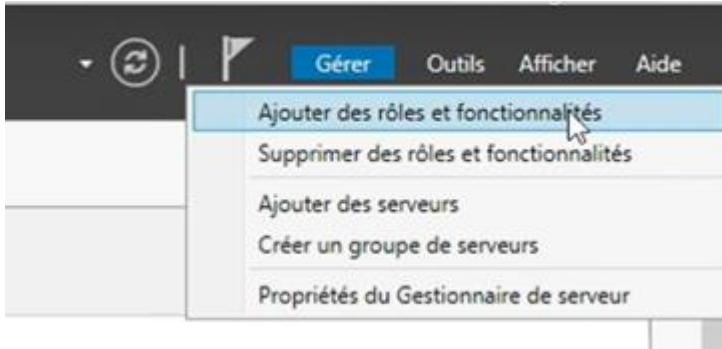
```
systemctl restart apache2
```

# COMPTE RENDU M2L

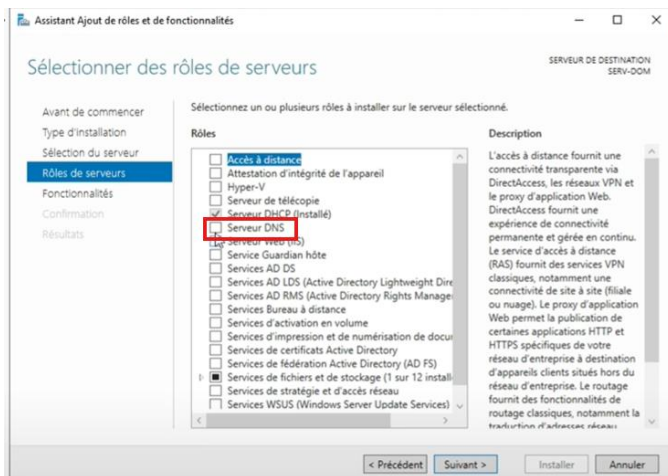
## 4 Installation et configuration du service DNS

Configuration du rôle DNS sur le serveur Windows:

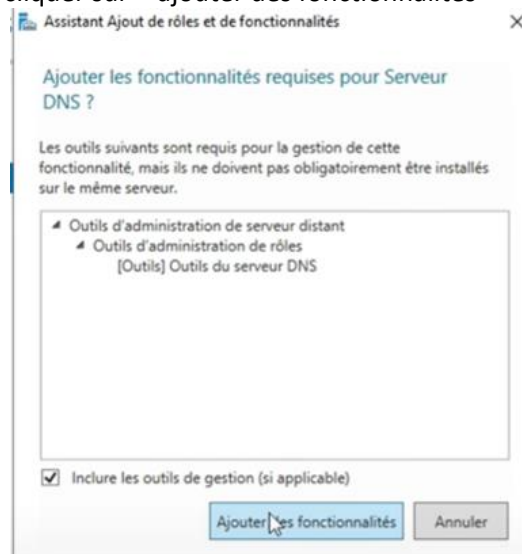
- **Installation du rôle :** Installation du rôle DNS sur le Serveur LDAP (172.17.3.100)  
Pour installer le rôle de serveur DNS sur le serveur, il faut comme pour le rôle LDAP, aller dans le gestionnaire de serveur puis sur Gérer → ajouter des rôles et des fonctionnalités :



Une fenêtre va s'ouvrir, il faut cliquer sur suivant jusqu'à être sur la page « rôle de serveur ». Il faut ensuite sélectionner « Serveur DNS ».



Une fenêtre va s'ouvrir. Il est important de cliquer sur « ajouter des fonctionnalités »



# COMPTE RENDU M2L

---

Ensuite il faut cliquer 3 fois sur Suivant avant d'arriver sur la page « Confirmation » et cliquer sur installer. Il faut maintenant attendre que le rôle s'installe.

- **Zone de recherche directe** : Création d'une nouvelle zone correspondant au domaine.

Après l'installation, il faut configurer le serveur DNS.

Dans la barre de recherche windows, chercher « DNS » puis cliquer sur l'application « DNS ».

Dans le fichier Zone de recherche direct, créer une nouvelle Zone avec le nom de votre domaine de préférence.

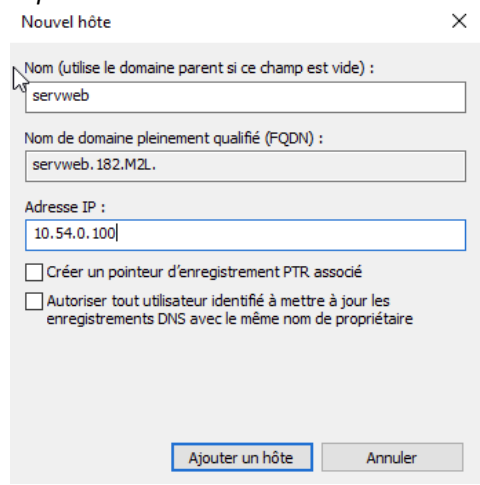
Le DNS est maintenant créé, il faut maintenant ajouter le serveur WEB au DNS.

- **Enregistrements** : Création d'un hôte "servweb" et d'alias (CNAME) pour accéder aux sites via leurs URLs

Il faut créer 1 hôte et 2 Alias.

Pour l'hôte, :

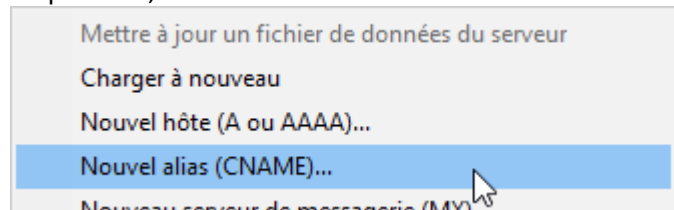
Clique droit → nouvel hôte → mettre l'adresse de son serveur web et l'url qu'on veut lui donner *voir capture d'écran*



Puis Ajouter

Maintenant il faut créer les alias pour les 2 pages.

Clique droit, nouvel alias :



Copier les paramètres de la capture d'écran puis dans le champ « nom de domaine complet », faire parcourir et aller chercher l'hôte « servweb » créé précédemment.

# COMPTE RENDU M2L

Nouvel enregistrement de ressource

Nom canonique (CNAME)

Nom de l'alias (utilisez le domaine parent si ce champ est vide):  
site1

Nom de domaine pleinement qualifié (FQDN):  
site1.182.M2L.

Nom de domaine complet (FQDN) pour l'hôte de destination:  
servweb.182.M2L. Parcourir...

Autoriser tout utilisateur identifié à mettre à jour tous les enregistrements DNS avec le même nom. Ce paramètre s'applique uniquement aux enregistrements DNS pour un nouveau nom.

(Faire la même chose pour le Site 2)

A la fin il faut obtenir ceci

servweb	Hôte (A)	10.54.0.100
site1	Alias (CNAME)	servweb.182.M2L
site2	Alias (CNAME)	servweb.182.M2L

- **Tests :** Tests de la configuration du DNS

Depuis mon PC1, je peux bien accéder à mes deux pages à l'aide de l'url.

pfSense.home.arpa - Firewall: NAT: X | Site2 | Site1

Non sécurisé site1.182.m2l/

Apache2 Debian Default Page

It works!

Bienvenu sur le Site1 de la M2L (/var/www/html1/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
    |-- ports.conf  
|-- mods-enabled  
    |-- *.load  
    |-- *.conf  
|-- conf-enabled  
    |-- *.conf  
|-- sites-enabled  
    |-- *.conf
```

• apache2.conf is the main configuration file. It puts the pieces together by including all remaining

pfSense.home.arpa - Firewall: NAT: X | Site2 | Site1

Non sécurisé site2.182.m2l/

Apache2 Debian Default Page

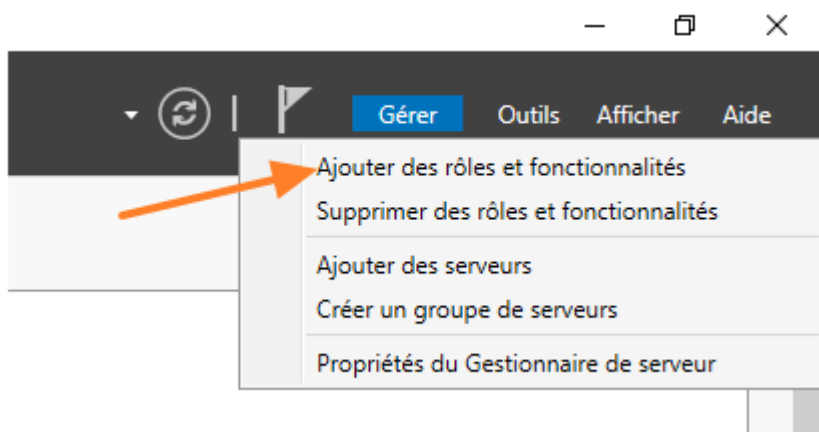
Le Serveur DNS est maintenant configuré.

# COMPTE RENDU M2L

---

## 5 Gestion de l'Active Directory et déploiement des utilisateurs

- **Installation** : Installation du service LDAP Active Directory pour créer un domaine.  
Ouvrir le gestionnaire de serveur, puis cliquer sur « *Gérer* » puis « *Ajouter des rôles et des fonctionnalités* »



Passer l'étape "*Avant de commencer*" et poursuivez ensuite en laissant le type d'installation sur le choix "*Installation basée sur un rôle ou une fonctionnalité*".

Choisir ensuite le serveur sur lequel il faut installer le rôle de serveur LDAP.

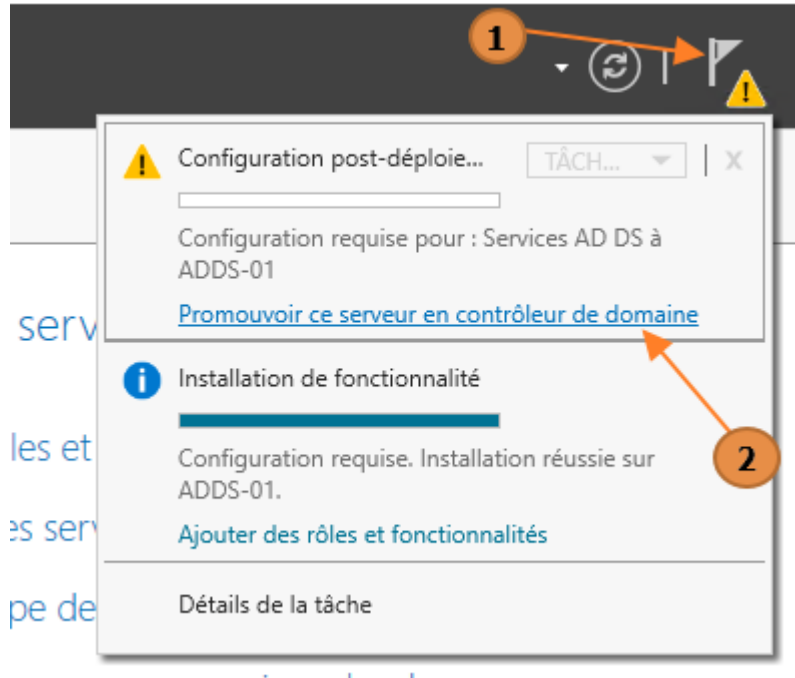
Dans l'onglet « *Rôle du serveur* », sélectionner le Services AD DS puis l'ajouter

Puis faites suivant et installer.

# COMPTE RENDU M2L

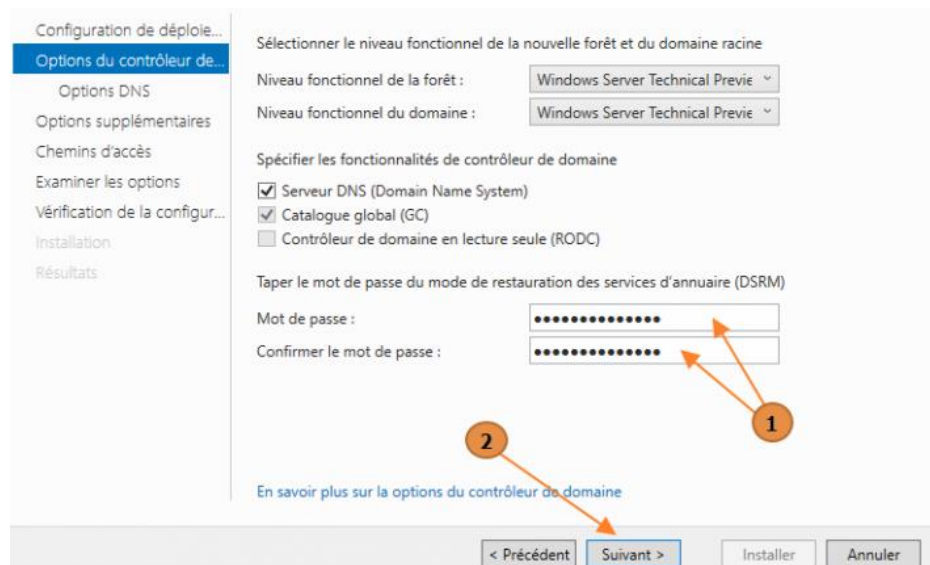
- **Promotion du serveur** : Promotion du serveur en Serveur LDAP.

Une fois installé, il faut promouvoir le serveur. Pour se faire, il faut aller dans le gestionnaire de serveur puis dans les notifications il faut cliquer sur « *promouvoir ce serveur en contrôleur de domaine* »



Une fois sur la page de promotion, il faut choisir « *Ajouter une nouvelle forêt* » puis dans nom de domaine entrer le nom que l'on souhaite attribuer à notre domaine. Faire suivant.

Veiller à bien avoir coché « *Serveur DNS* », d'avoir rentré le mot de passe du mode restauration et faire suivant.



# COMPTE RENDU M2L

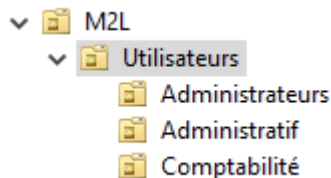
---

Dans le nom de domaine NetBIOS, remettre le même nom que le nom de domaine créé précédemment. (Attention, cette fois ci les chiffres et caractères spéciaux ne sont plus acceptés).

A partir de cette étape, plus besoins de toucher aux paramètres, il est possible de faire suivant jusqu'à la fin et d'installer le rôle.

- **Structure** : Création d'Unités d'Organisation (UO) pour la M2L et ses services (ex: Comptabilité).  
Une fois l'AD créé, il faut maintenant créer des comptes utilisateurs de domaine, en revanche il est préférable de les créer dans des Unité d'Organisation (UO) afin de les ranger.

Je vais maintenant créer des Unité d'organisation afin de ranger mes utilisateurs (par services par exemple)



J'ai créé donc 3 services différents dans une UO Utilisateurs qui est lui-même dans une UO M2L. Maintenant je vais créer un utilisateur « Sandrine » dans la partie comptabilité. Pour se faire il faut se rendre dans l'UO Comptabilité puis faire un clic droit, « nouveau » et « Utilisateur ».

Je créer l'utilisateur Sandrine BOIRAIT. Pour le login je prends la nomenclature des 7 premières lettres du NOM + première lettres du PRÉNOM.

Ça donne :

Nouvel objet - Utilisateur

Créer dans : 182.M2L/M2L/Utilisateurs/Comptabilité

Prénom : Sandrine    Initiales :

Nom : boirait

Nom complet : Sandrine boirait

Nom d'ouverture de session de l'utilisateur : boirais@182.M2L

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : M2L\boirais

< Précédent    Suivant >    Annuler

Je peux ensuite décider de son mot de passe et lui faire changer à la première connexion, le faire expirer ou d'autres fonctionnalités (dans mon cas je laisserai le mot de passe par défaut)

# COMPTE RENDU M2L

Nouvel objet - Utilisateur

Créer dans : 182.M2L/M2L/Utilisateurs/Comptabilité

Mot de passe : .....

Confirmer le mot de passe : .....

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

Le compte est désactivé

< Précédent Suivant > Annuler

Ensuite on fait suivant puis terminer et notre utilisateur Sandrine est créée.

- **Connexion** : Connexion du PC1 au domaine

Paramètres

Accueil

Rechercher un paramètre

Systeme

Stockage

Tablette

Multitâche

Projection sur ce PC

Expériences partagées

Composants système

Presse-papiers

Bureau à distance

Fonctionnalités facultatives

À propos de

À propos de

Votre ordinateur est surveillé et protégé.

Voir les détails dans la sécurité Windows

Mémoire RAM installée: 8,00 Go

Processeur: QEMU Virtual CPU version 2.5+

Carte graphique: Aucune VRAM dédiée

Stockage: 32 GB

BCE0L00501P01

Standard PC (Q35 + ICH9, 2009)

Renommer ce PC

Renommer ce PC (avancé)

Spécifications de l'appareil

Copier

Nom du périphérique: BCE0L00501P01

Processeur: QEMU Virtual CPU version 2.5+ 2.50 GHz

Mémoire RAM installée: 8.00 Go

Stockage: 32 GB Red Hat VirtIO

ID de périphérique: 81758561-04E7-4F40-B2E0-7B6CD473294F

ID de produit: 00378-40000-00001-AA272

Paramètres associés

Mettre à niveau votre édition de Windows ou modifier la clé de produit (Product Key)

Lire les termes du contrat de licence logiciel Microsoft

Paramètres de BitLocker

Gestionnaire de périphériques

Bureau à distance

Protection du système

Paramètres avancés du système

Aide du web

Recherche du nombre de cœurs dont dispose mon processeur

Vérification de la prise en charge de plusieurs langues

Obtenir de l'aide

Donner des commentaires

Ensuite cliquer sur « Modifier » puis cocher « domaine » et y entrer le nom de domaine (182.m2l dans notre cas)

# COMPTE RENDU M2L

Modification du nom ou du domaine de l'ordinateur ✕

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur :  
BCE0L00S01P01

Nom complet de l'ordinateur :  
BCE0L00S01P01

Autres...

Membre d'un


Domaine :  
182.m2l

Groupe de travail :  
WORKGROUP

OK Annuler

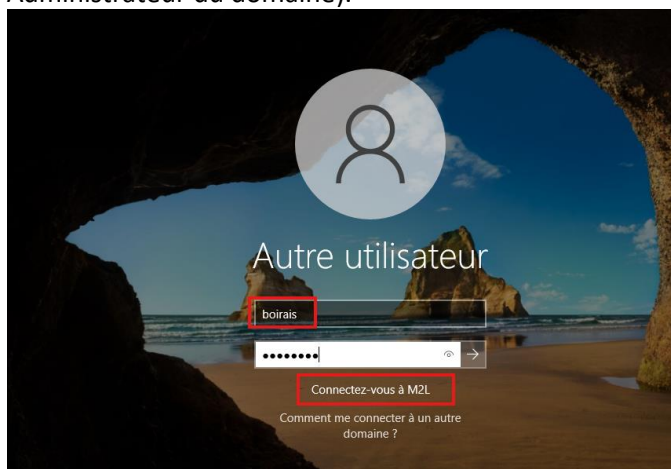
Ensuite faire ok puis une fenetre de login va s'ouvrir. Il faut mettre le login administrateur local. Si tout s'est bien passé, cette fenetre devrait apparaître :

Modification du nom ou du domaine de l'ordinateur ✕

 Bienvenue dans le domaine 182.m2l.

OK

Il faudra ensuite redémarrer le PC et se connecter avec un compte de domaine (comme Sandrine ou Administrateur du domaine).



Autre utilisateur

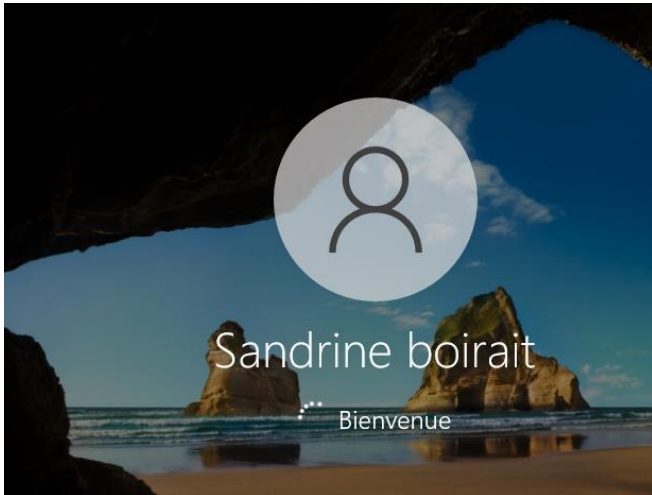
boirais

Connectez-vous à M2L

Comment me connecter à un autre domaine ?

# COMPTE RENDU M2L

---



Notre domaine et nos utilisateurs sont maintenant créés et notre pc est maintenant connecté au domaine.

## 6 Mise en place de la solution de gestion de parc GLPI

### 6.1 Installation : Mise à jour des dépôts, installation des dépendances et sécurisation de la base de données.

Tout d'abord, il ne faut pas oublier d'installer les dernières mise à jour GLPI.

```
apt-get update && apt-get upgrade -y
```

Ensuite, il faut installer les applications

```
apt install apache2 php libapache2-mod-php mariadb-server -y
```

Maintenant, il faut installer les dépendances :

```
apt install php-mysql php-mbstring php-curl php-gd php-simplexml php-intl php-ldap  
php-apcu php-xmlrpc php-cas php-zip php-bz2 php-imap -y
```

Après avoir installé toutes les applications et les dépendances, il faut sécuriser la base de données :

```
mysql_secure_installation
```

# COMPTE RENDU M2L

---

Copier ces paramètres pour la sécurisation de la BDD.

```
Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] y
Enabled successfully!
Reloading privilege tables..
... Success!

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

# COMPTE RENDU M2L

---

Une fois la sécurisation de la BDD faites, il faut s'y connecter :

```
mysql -u root -p
```

## 6.2 Configuration de la BDD :

```
MariaDB [(none)]> create database bdd_glpi;
Query OK, 1 row affected (0,002 sec)

MariaDB [(none)]> grant all privileges on bdd_glpi.* to
->
-> adminbdd_glpi@localhost identified by 'Azerty31';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds
to your MariaDB server version for the right syntax to use near 'Azerty31' at line 3
MariaDB [(none)]> create database bdd_glpi;
ERROR 1007 (HY000): Can't create database 'bdd_glpi'; database exists
MariaDB [(none)]> grant all privileges on bdd_glpi.* to
-> adminbdd_glpi@localhost identified by "Azerty31";
Query OK, 0 rows affected (0,017 sec)

MariaDB [(none)]> exit
Bye
root@debian12:/home/neo#
```

Une fois la BDD configurée, il faut télécharger et installer GLPI :

Dans le répertoire /tmp

```
wget https://github.com/glpi-project/glpi/releases/download/10.0.20/glpi-10.0.20.tgz
```

Après avoir téléchargé le fichier .tgz, il faut le décompresser :

```
tar -xvzf glpi-10.0.20.tgz
```

# COMPTE RENDU M2L

---

## 6.3 Configuration : Déploiement des sources dans /var/www/html/glpi, gestion des droits www-data et activation de l'inventaire dans l'interface.

Copier le contenu du dossier décompressé nommé « /var/www/html (Il est aussi possible de le déplacer. Il faut aussi supprimer au passage le fichier index.html qui n'est autre qu'une sorte de page d'accueil d'apache :

```
rm /var/www/html/index.html
```

```
cp -r glpi/* /var/www/html/
```

Rendre l'utilisateur des services web propriétaire des nouveaux fichiers :

```
Chown -R www-data /etc/glpi
```

Créer un dossier nommé « glpi » dans /etc et rendez www-data propriétaire de ce dossier :

```
mkdir /etc/glpi  
chown -R www-data /etc/glpi
```

Déplacer le dossier config :

```
mv /var/www/html/files /var/lib/glpi
```

Créer un dossier dans var/www/html/inc nommé downstream.php :

```
Nano /var/www/html/inc/downstream.php
```

Puis y mettre cette config :

```
< ?php  
  
define ('GLPI_CONFIG_DIR', '/etc/glpi/');  
if  
    (file_exists (GLPI_CONFIG_DIR . '/local_define.php'))  
    {  
        require_once  
            GLPI_CONFIG_DIR . '/local_define.php';
```

# COMPTE RENDU M2L

```
}
```

Créer un fichier local\_define dans etc/glipi :

```
Nano /etc/glipi/local_define.php
```

```
< ?php  
define('GLPI_VAR_DIR', '/var/lib/glipi');
```

Modifier le fichier php.ini :

```
Nano /etc/php/8.2/apache2/php.ini
```

Et rajouter le « On » après le session.cookie\_httponly

```
 ; Initialize session on request startup.  
 ; https://php.net/session.auto-start  
session.auto_start = 0  
  
 ; Lifetime in seconds of cookie or, if 0, until browser is restarted.  
 ; https://php.net/session.cookie-lifetime  
session.cookie_lifetime = 0  
  
 ; The path for which the cookie is valid.  
 ; https://php.net/session.cookie-path  
session.cookie_path = /  
  
 ; The domain for which the cookie is valid.  
 ; https://php.net/session.cookie-domain  
session.cookie_domain =  
  
 ; Whether or not to set the httponly flag on the cookie, which makes it  
 ; inaccessible to browser scripting languages such as JavaScript.  
 ; https://php.net/session.cookie-httponly  
session.cookie_httponly = on  
  
 ; Add SameSite attribute to cookie to help mitigate Cross-Site Request Forgery (CSRF)  
 ; Current valid values are "Strict", "Lax" or "None". When using "None",  
 ; make sure to include the quote, as "None" is interpreted like "false" in old files.  
 ; https://tools.ietf.org/html/rfc6265#section-6.3.3.2  
session.cookie_samesite =  
  
 ; Handler used to serialize data. php is the standard serializer of PHP.  
 ; https://php.net/session.serialize-handler  
session.serialize_handler = php  
  
 ; Defines the probability that the 'garbage collection' process is started on every  
 ; session initialization. The probability is calculated by using gc_probability/gc_divisor,  
 ; e.g. 1/100 means about 1% chance that the GC process starts on each request.  
 ; Default Value: 1  
 ; Recommended Value: 1  
 ; Production Value: 1  
 ; https://php.net/session.gc-probability  
session.gc_probability = 0  
  
-- INSERTION --
```

Puis redémarrer les services apaches :

# COMPTE RENDU M2L

```
systemctl restart apache2
```

Depuis l'interface web, Entrer dans le barre de recherche du navigateur l'adresse IP du serveur GLPI afin de rentrer sur l'interface web de l'installation de l'outil GLPI :



Faites OK puis continuer.

Arriver sur la page « Début de l'installation, cliquer sur Installer :



# COMPTE RENDU M2L

---

Pour la première étape, il faut rentrer toutes les informations utilisées précédemment :

[Configuration de la BDD :](#)

Et les rentrer comme demandé :



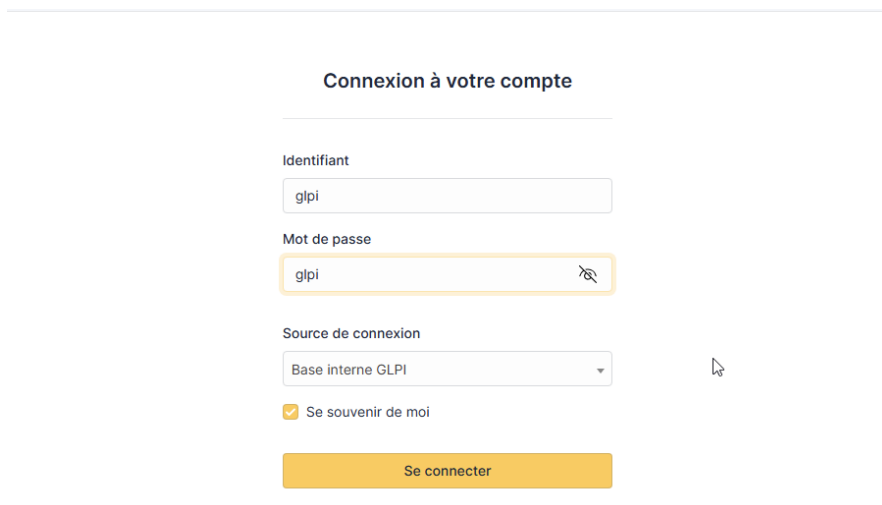
The screenshot shows the GLPI Setup interface. At the top left is the GLPI logo. To the right, it says 'GLPI SETUP'. Below that, 'Étape 1' and 'Configuration de la connexion à la base de données'. The form includes three input fields: 'Serveur SQL (MariaDB ou MySQL)' with 'localhost', 'Utilisateur SQL' with 'adminbdd\_glpi', and 'Mot de passe SQL' with 'Azerty31'. A 'Continuer >' button is at the bottom.

Puis pour l'étape 2, il faut sélectionner la base de données déjà existante.

A partir d'ici, il est possible de faire continuer jusqu'à arriver à l'étape 6.

Après avoir cliqué sur « Utiliser GLPI », nous sommes redirigé sur une page de login.

Les identifiants par défauts sont : glpi glpi

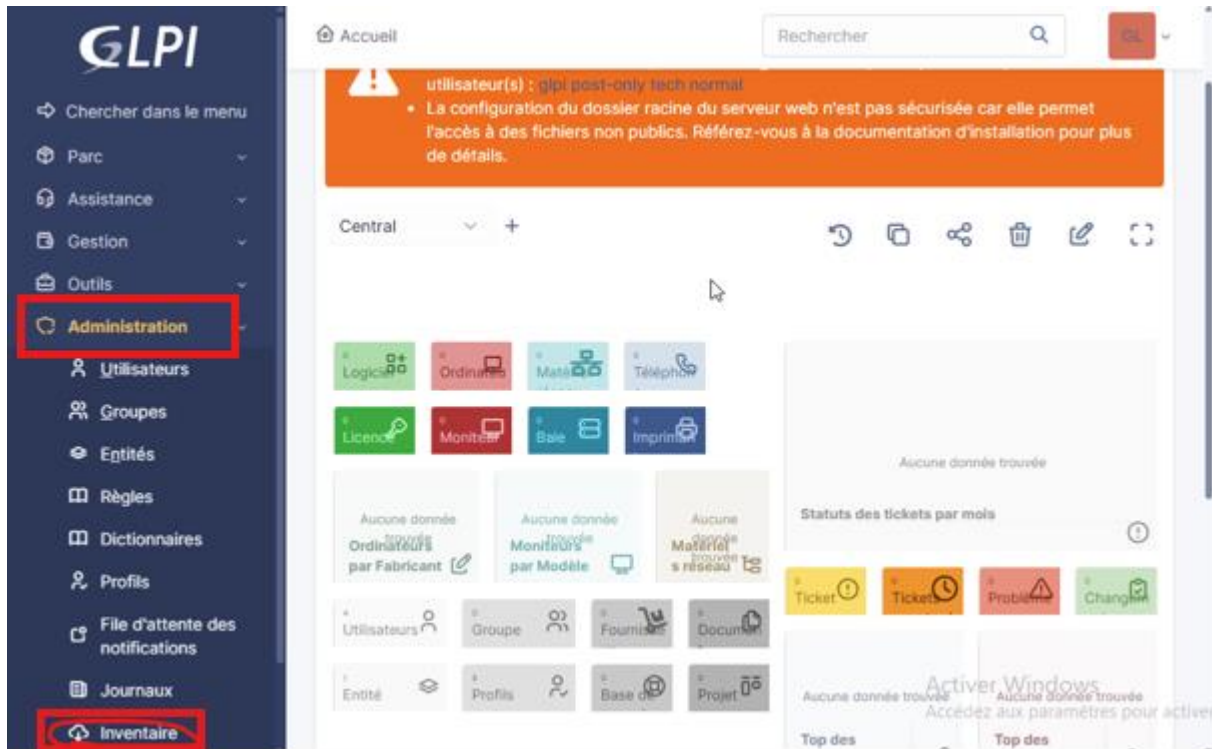


The screenshot shows the login page titled 'Connexion à votre compte'. It has three input fields: 'Identifiant' with 'glpi', 'Mot de passe' with 'glpi', and 'Source de connexion' with a dropdown menu set to 'Base interne GLPI'. There is a checked checkbox for 'Se souvenir de moi' and a 'Se connecter' button at the bottom.

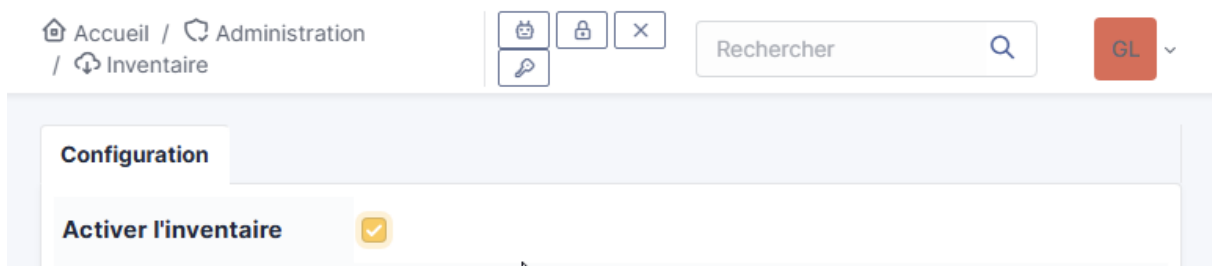
# COMPTE RENDU M2L

## 6.4 Activer l'inventaire GLPI

Une fois loggé comme administrateur (compte par défaut), il faut se rendre dans Administration puis Inventaire :



Et cocher la case « Activer l'inventaire » puis « Sauvegarder tout en bas ».

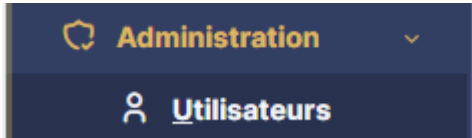


# COMPTE RENDU M2L

---

## 6.5 Changer le mot de passe d'un utilisateur

Aller dans Administration puis Utilisateurs :



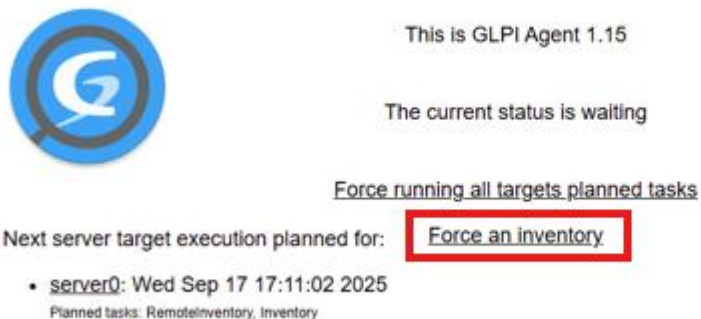
Cliquer sur un utilisateur et changer le mot de passe dans le champ mot de passe puis sauvegarder

## 6.6 Agent : Installation de l'agent GLPI pour remonter les informations du serveur.

Se connecter à l'agent avec l'adresse :

```
localhost:62354
```

Puis cliquer sur « Force an inventory »



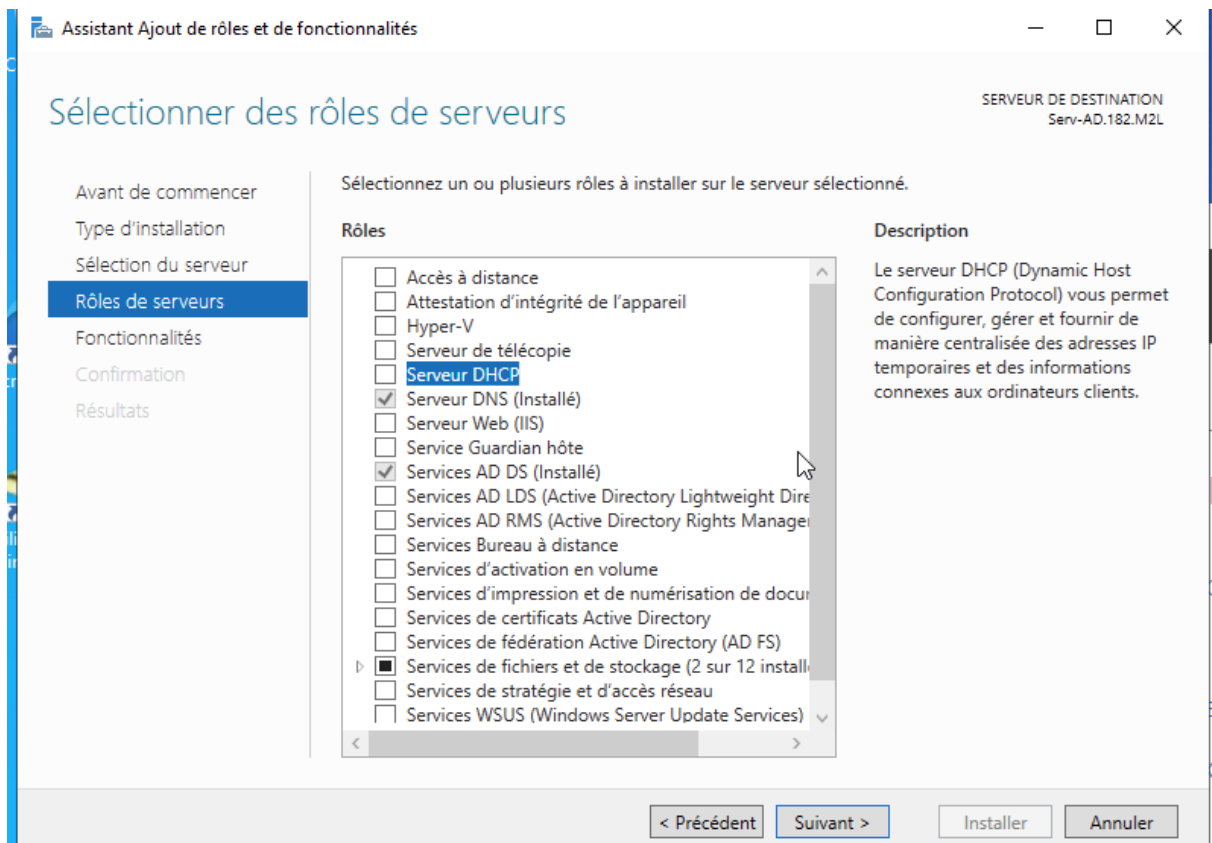
Puis faire back et server0 .

# COMPTE RENDU M2L

## 7 Configuration du service DHCP

### 7.1 Rôle : Installation du rôle "Serveur DHCP" sur Windows Server.

Comme pour l'AD et pour le serveur DNS, pour installer le serveur DHCP il faut aller dans « ajouter des rôles et des fonctionnalités » puis dans la partie « rôle de serveurs », il faut cocher le « Serveur DHCP » puis « ajouter le rôle » et installer.

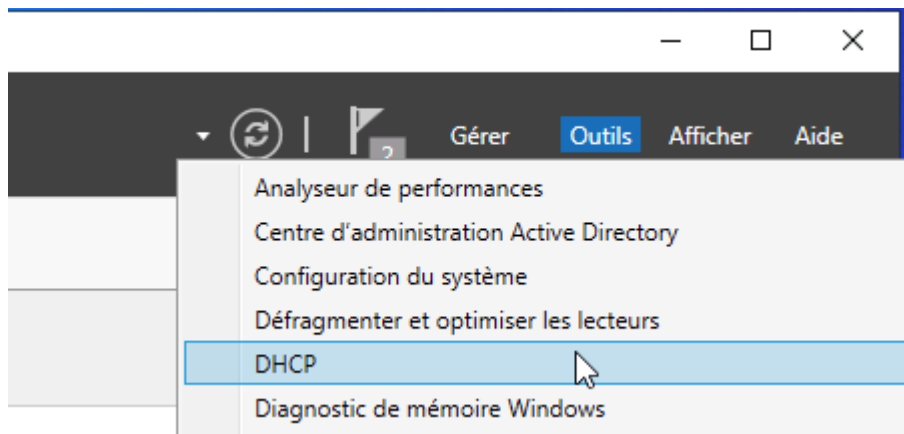


Puis faire suivant et l'installer

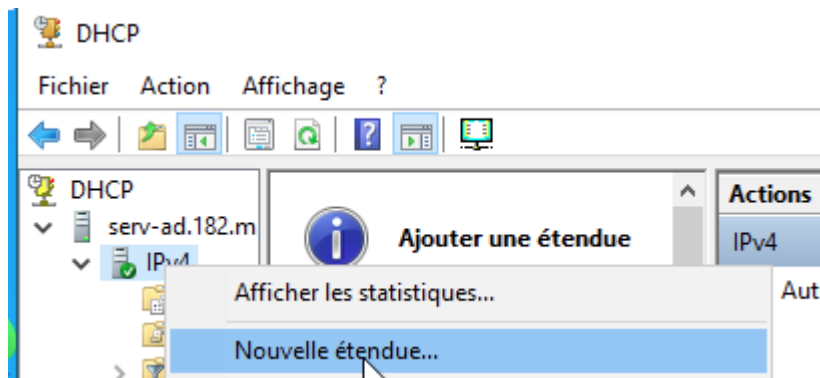
# COMPTE RENDU M2L

## 7.2 Étendue : Création d'une plage d'adresses avec exclusion des IP statiques (routeur et serveurs).

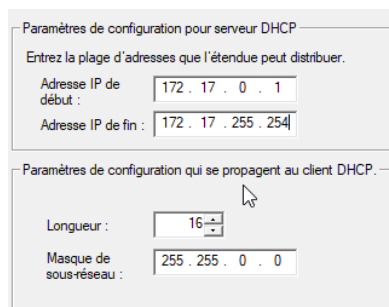
Pour configurer le DHCP, il faut aller dans « outil » → « DHCP »



Il faut dérouler le menu puis faire clique droit sur IPv4 et « nouvelle étendue »



Puis configurer l'étendue :

A screenshot of the 'Paramètres de configuration pour serveur DHCP' dialog box. The 'Entrez la plage d'adresses que l'étendue peut distribuer.' section has 'Adresse IP de début' set to '172 . 17 . 0 . 1' and 'Adresse IP de fin' set to '172 . 17 . 255 . 254'. The 'Paramètres de configuration qui se propagent au client DHCP.' section has 'Longueur' set to '16' and 'Masque de sous-réseau' set to '255 . 255 . 0 . 0'. A mouse cursor is pointing at the 'Longueur' field.

# COMPTE RENDU M2L

---

Il faut exclure les adresses de notre routeur et de notre serveur DHCP afin d'éviter les conflits d'adresses :

Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début :    Adresse IP de fin :  
           

Plage d'adresses exclue :

Adresse 172.17.3.1	<input type="button" value="Supprimer"/>
Adresse 172.17.3.100	

Retard du sous-réseau en millisecondes :

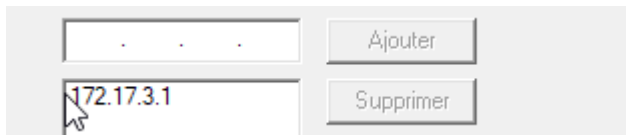
Il faut laisser le bail de 8 jours par défaut (peut être modifié selon les utilisations. Dans notre cas c'est inutile.).

# COMPTE RENDU M2L

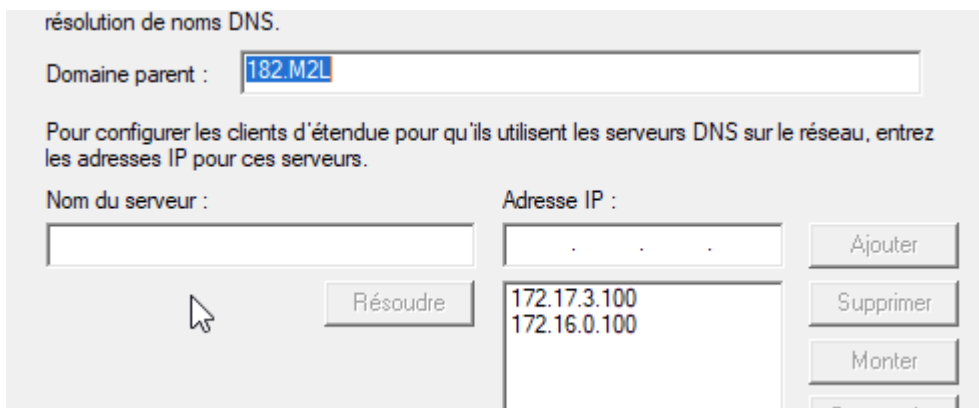
## 7.3 Options : Renseignement de la passerelle par défaut, du nom de domaine et des serveurs DNS.

Dans la configuration de l'étendue (la même que précédemment, il faut cocher la case « Oui, je veux configurer ces options maintenant » :

La première étape demandé est d'ajouter l'adresse IP de la passerelle par défaut (routeur) :



L'étape suivante est pour la résolution DNS. Dans notre cas, nous avons un domaine qui par défaut s'occupe de la résolution DNS. Il faut donc mettre le nom et l'adresse du serveur LDAP :



Dans ce cas-là, j'ai mis un DNS auxiliaire au cas où, mais c'est facultatif.

Il faut ensuite faire suivant jusqu'à la page « activer l'étendue » et cocher « oui ».

Le serveur DHCP est maintenant configuré.

Si je me mets en DHCP sur le pc1, je devrais normalement avoir une adresse IP qui m'est attribué.

```
Carte Ethernet Ethernet :
  Suffixe DNS propre à la connexion. . . : 182.M2L
  Description. . . . . : Red Hat VirtIO Ethernet Adapter
  Adresse physique . . . . . : BC-24-11-C3-BF-37
  DHCP activé. . . . . : Oui
  Configuration automatique activée. . . : OUI
  Adresse IPv6 de liaison locale. . . . . : fe80::586c:92cc:7b1e:e89b%4(préféré)
  Adresse IPv4. . . . . : 172.17.0.1(préféré)
  Masque de sous-reseau. . . . . : 255.255.0.0
  Bail obtenu. . . . . : jeudi 22 janvier 2026 08:36:29
  Bail expirant. . . . . : vendredi 30 janvier 2026 08:36:29
  Passerelle par défaut. . . . . : 172.17.3.1
  Serveur DHCP . . . . . : 172.17.3.100
  IAID DHCPv6 . . . . . : 112993297
  DUID de client DHCPv6. . . . . : 00-01-00-01-30-FA-3E-DB-BC-24-11-C3-BF-37
  Serveurs DNS. . . . . : 172.17.3.100
                          172.16.0.100
  NetBIOS sur Tcpip. . . . . : Activé
```

Notre DHCP est maintenant configuré et fonctionnel.