

AP 2-1 - SISR

Administration Système & Réseaux

Projet Tamarin

Mission 2

Elaboré par

Yann Duffay & Ousmane Diop

Promotion

1 TSIO

Année scolaire

2023-2024

SOMMAIRE

I. Introduction.....	4
A. Plan d'adressage.....	4
II. Mise en place Windows Serveur 1.....	6
3.1.Active Directory.....	6
3.1. Service DNS.....	9
3.2. Service DHCP.....	23
3.3. Création des utilisateurs et de leurs répertoires de stockage.....	23
3.4. GPO.....	23
3.5 Serveur WSUS.....	23
III. Mise en place Linux Serveur 1.....	24
4.1. Serveur Web.....	24
4.2. Serveur GLPI.....	25
IV. Mise en place Linux Serveur 2.....	25
5.1. Serveur de base de données.....	25
V. Scripts de sauvegardes des pages web.....	26
VI. Sécurité du service web.....	27
7.1. Installation de Wireshark.....	27
7.2. Contrôle des échanges HTTP.....	27
7.3. Solutions de sécurisation.....	27
VII. Conclusion.....	28

I. Introduction

Dans cette deuxième mission de cette AP l'objectif est de mettre en place l'infrastructure avec les différents services.

A. Plan d'adressage

Nom Machine	@IP	@Réseau	Masque	Passerelle	Nom Utilisateur
Linux serveur 1	192.168.66.10	192.168.66.0	/24	192.168.66.254	utl
Linux serveur 2	192.168.66.11				utl
Windows serveur 1	192.168.66.12				Administrateur

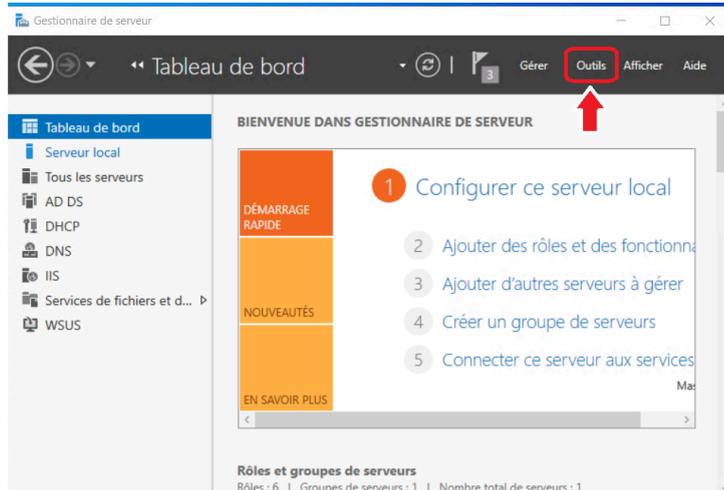
Tache a faire	windows serveur 1	windows serveur 2	Linux serveur 1
annuaire AD (serveur 1)			
DNS (serveur 1)			
DHCP (serveur 1)			
Création des utilisateurs et de leurs répertoires de stockage, connectés automatiquement, gestion des droits (serveur 1)			
GPO (serveur 1)			
serveur web (service web et interpréteur PHP) (serveur 2)			

<p>serveur de base de données, MariaDB, distant du serveur web, sous Debian 12 (serveur 3)</p>			
<p>Mise en place de sauvegardes des pages web automatisées (scripts) vers une machine distante</p>			
<p>Sécurité du service web : o Installer un analyseur de trames et contrôler la sécurisation des échanges web (HTTP) o En fonction des résultats observés proposer des solutions (pourquoi et mode opératoire). Il ne vous est pas demandé de mettre ces solutions en place.</p>			

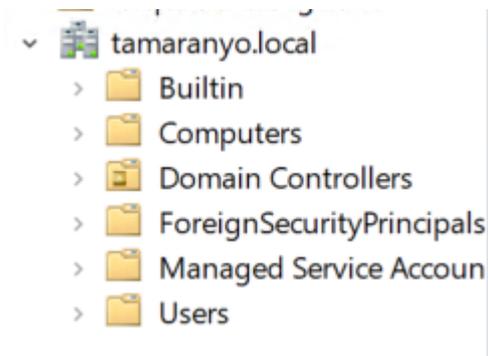
II. Mise en place Windows Serveur 1

3.1.Active Directory

creation users



Utilisateurs et ordinateurs Active Directory



The screenshot shows the Active Directory Users and Computers console. A red circle highlights the 'Users' icon in the toolbar. Below the toolbar is a table listing users and groups.

Nom	Type	Description
Administrat...	Groupe de séc...	Les membres de ce grou...
Administrat...	Groupe de séc...	Administrateurs désigné...
Administrat...	Groupe de séc...	Les membres qui ont un ...
Administrat...	Groupe de séc...	Administrateurs désigné...
Admins du d...	Groupe de séc...	Administrateurs désigné...
Alain Tamaran	Utilisateur	
Baptiste Albert	Utilisateur	



 Créer dans : tamaranyo.local/Users

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :
 @tamaranyo.local

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



 Créer dans : tamaranyo.local/Users

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

Créer dans : tamaranyo.local/Users

Quand vous cliquerez sur Terminer, l'objet suivant sera créé :

Nom complet : Prenom Nom
 Nom de connexion de l'utilisateur : Prenom Nom@tamaranyo.local
 L'utilisateur doit changer de mot de passe à la prochaine ouverture de session.

< Précédent Terminer Annuler

integration groupe

-  Ordinateurs ... Groupe de séc... Toutes les stations de tra...
-  Pole CGPA Groupe de séc...
-  Pole Directeur Groupe de séc...
-  Pole RI Groupe de séc...
-  Pole TEI Groupe de séc...
-  Pole UCI Groupe de séc...
-  Propriétaires ... Groupe de séc... Les membres de ce grou...
-  Protected Us... Groupe de séc... Les membres de ce grou...

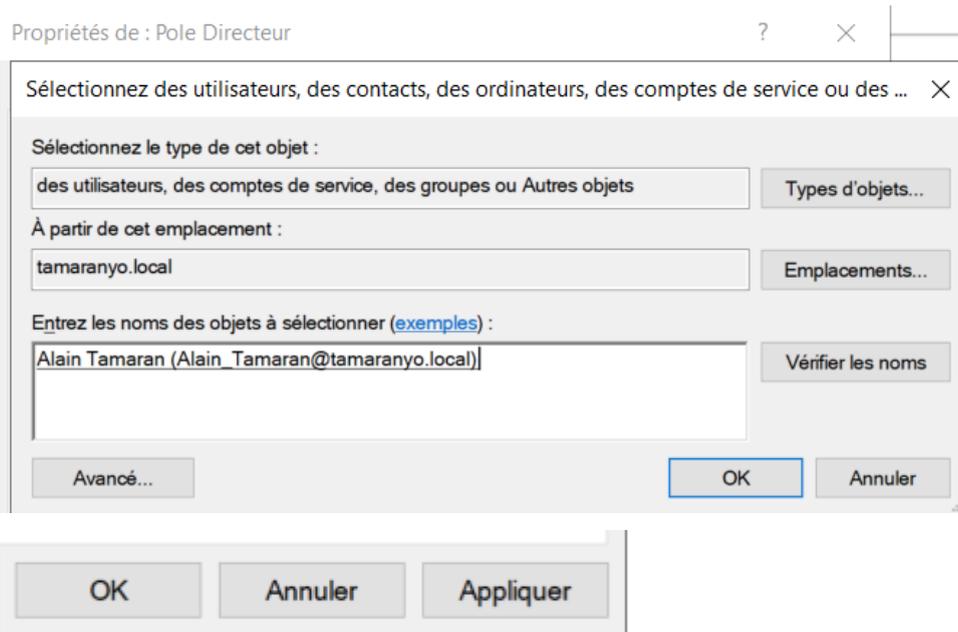
Propriétés de : Pole Directeur ? ×

Général Membres Membre de Géré par

Membres :

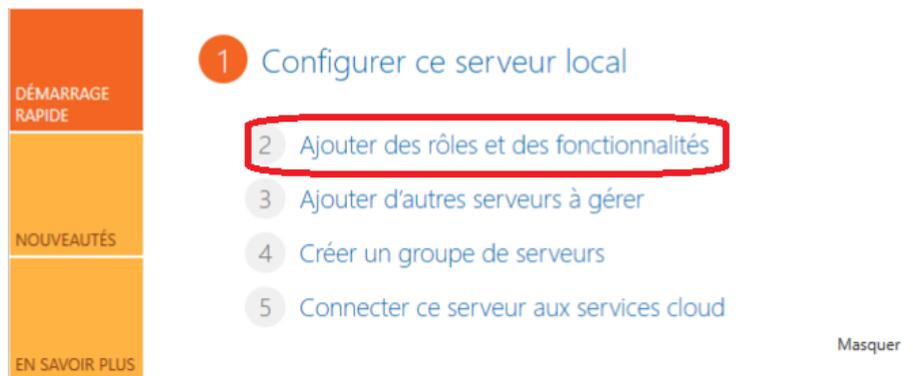
Nom	Dossier Services de domaine Active Directory
 Kevin Rose	tamaranyo.local/Users

Ajouter... Supprimer



3.1. Service DNS

creation dns



Poursuivez à travers les menus jusqu'à la page d'ajout des rôles. Ajoutez le rôle DNS.

Sélectionner des rôles de serveurs

SERVERE DE DESTINATION
DNS

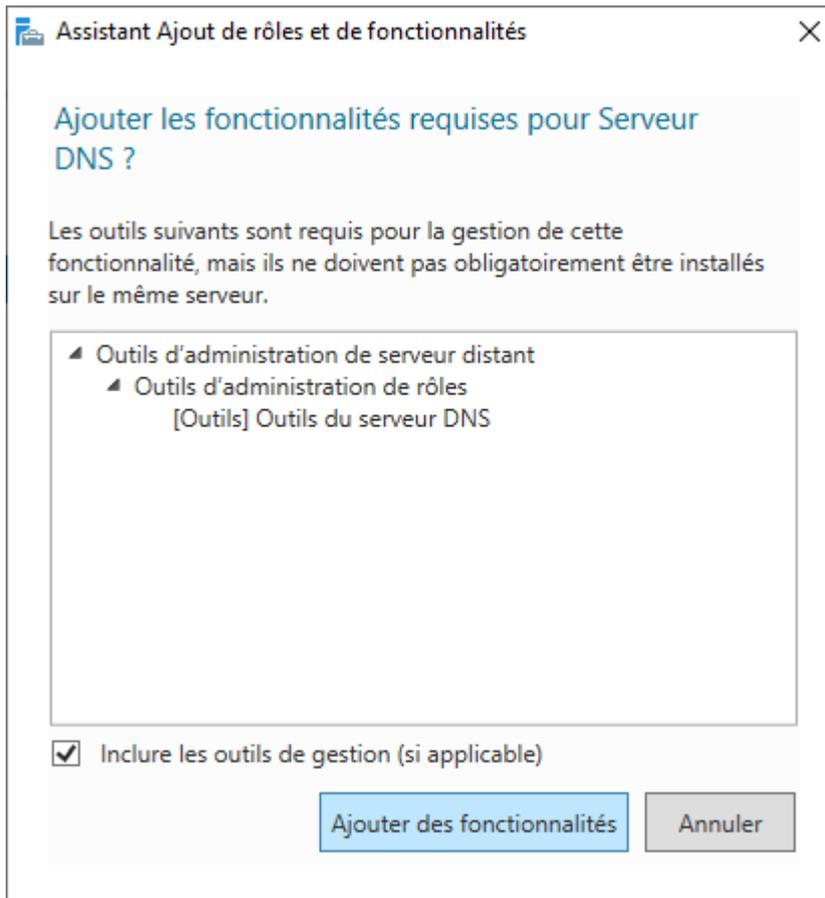
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DNS
Confirmation
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

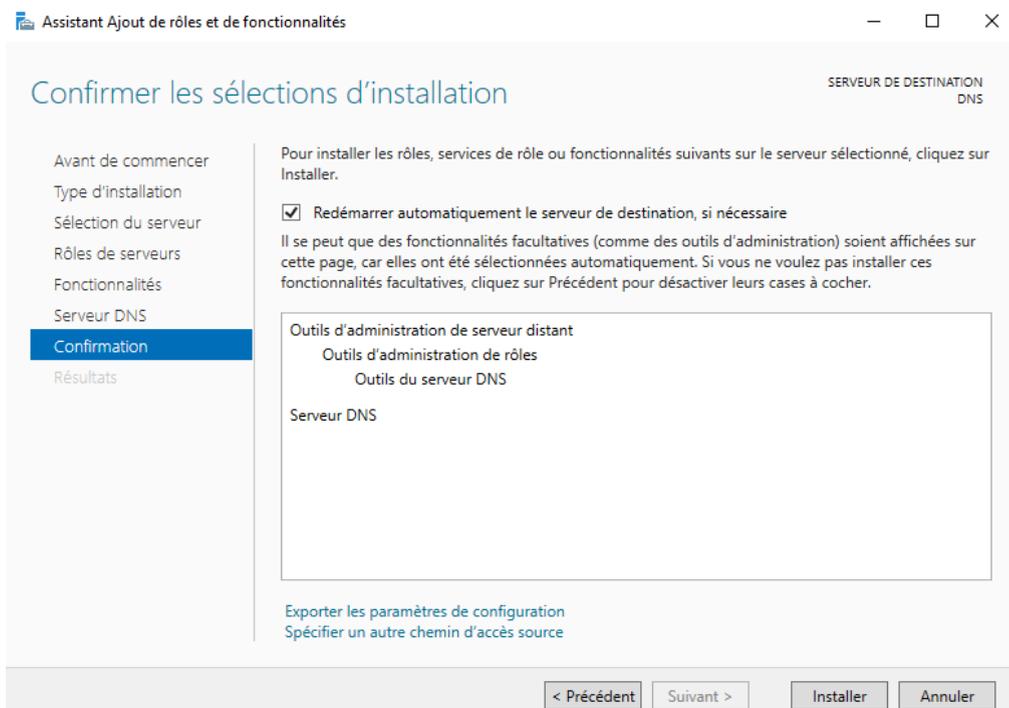
Rôles	Description
<input type="checkbox"/> Accès à distance	Le serveur DNS (Domain Name System) permet la résolution de noms sur les réseaux TCP/IP. Le serveur DNS est plus facile à gérer lorsqu'il est installé sur le même serveur que les services de domaine Active Directory. Si vous sélectionnez le rôle Services de domaine Active Directory, vous pouvez installer et configurer le serveur DNS et les services de domaine Active Directory pour les faire fonctionner conjointement.
<input type="checkbox"/> Attestation d'intégrité de l'appareil	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Serveur de télécopie	
<input type="checkbox"/> Serveur DHCP	
<input checked="" type="checkbox"/> Serveur DNS	
<input type="checkbox"/> Serveur Web (IIS)	
<input type="checkbox"/> Service Guardian hôte	
<input type="checkbox"/> Services AD DS	
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Directory Services)	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Management Services)	
<input type="checkbox"/> Services Bureau à distance	
<input type="checkbox"/> Services d'activation en volume	
<input type="checkbox"/> Services d'impression et de numérisation de documents	
<input type="checkbox"/> Services de certificats Active Directory	
<input type="checkbox"/> Services de déploiement Windows	
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (1 sur 12 installés)	
<input type="checkbox"/> Services de stratégie et d'accès réseau	

< Précédent Suivant > Installer Annuler

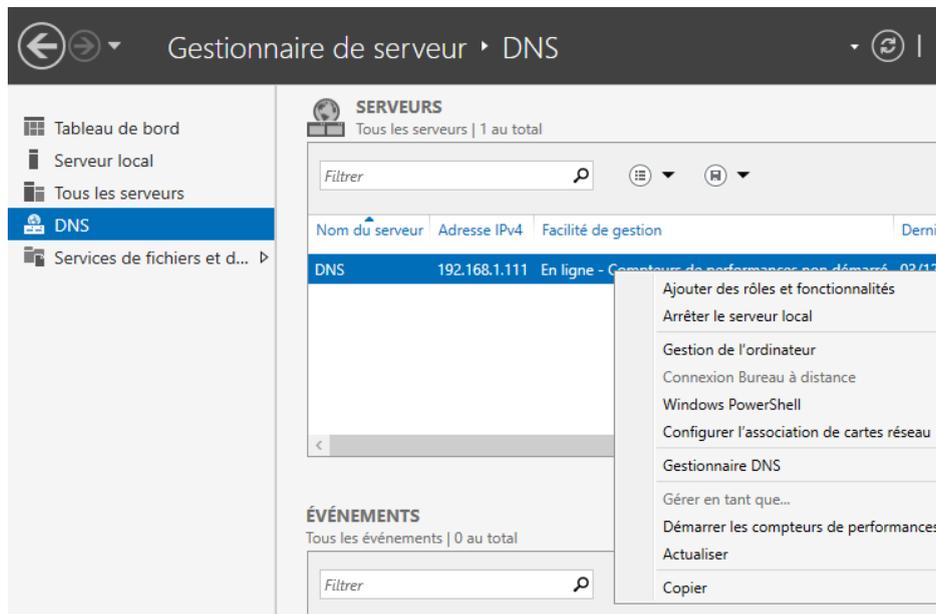
Ajoutez les fonctionnalités recommandées proposées pour l'installation du rôle :



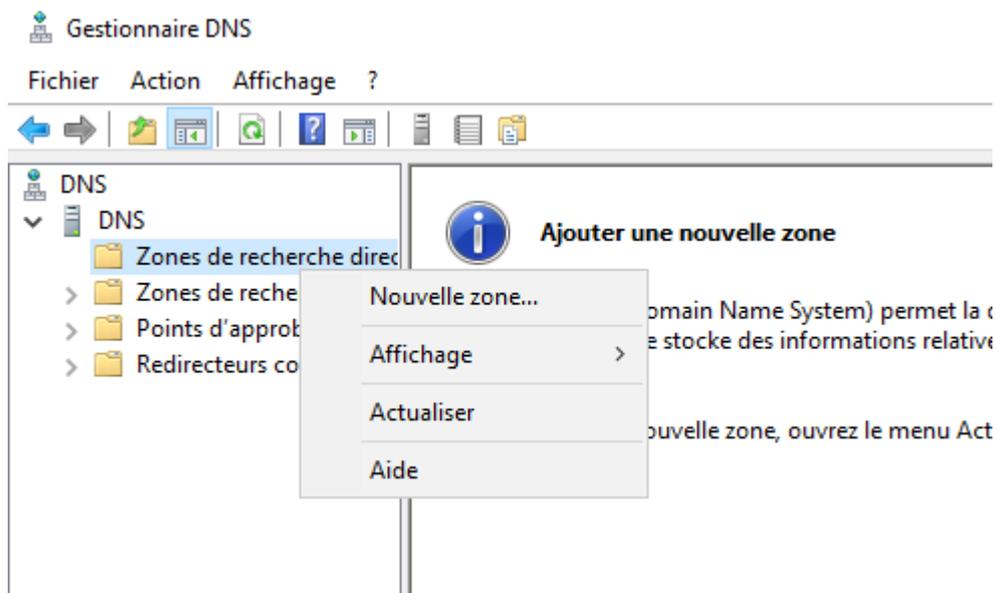
Allez ensuite jusqu'au menu d'installation et cliquez sur installer.



Patiencez jusqu'à la fin de l'installation. Une fois terminé fermez la fenêtre. Ouvrez ensuite le rôle DNS dans le gestionnaire de serveurs. Pour cela cliquez sur DNS, puis cliquez droit sur la ligne contenant l'adresse IP du serveur. Choisissez enfin gestionnaire DNS :



Dans ce gestionnaire, déployez l'icône DNS puis cliquez droit sur zones de recherche directe et cliquez enfin sur nouvelle zone.



Vous arrivez alors dans l'assistant de configuration. Cliquez sur suivant :



Bienvenue !

Cet Assistant vous permet de créer une nouvelle zone pour le serveur DNS.

Une zone traduit les noms DNS en données relatives, telles que des adresses IP ou des services réseau.

Cliquez sur Suivant pour continuer.

< Précédent **Suivant >** Annuler

Comme il s'agit de notre serveur principal, indiquez qu'il s'agit de la zone principale et cliquez sur suivant.

Type de zone

Le serveur DNS prend en charge différents types de zones et de stockages.



Sélectionnez le type de zone que vous voulez créer :

- Zone principale**
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
- Zone secondaire**
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
- Zone de stub**
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.
- Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

< Précédent **Suivant >** Annuler

Indiquez ensuite le nom de domaine de la zone :

Assistant Nouvelle zone

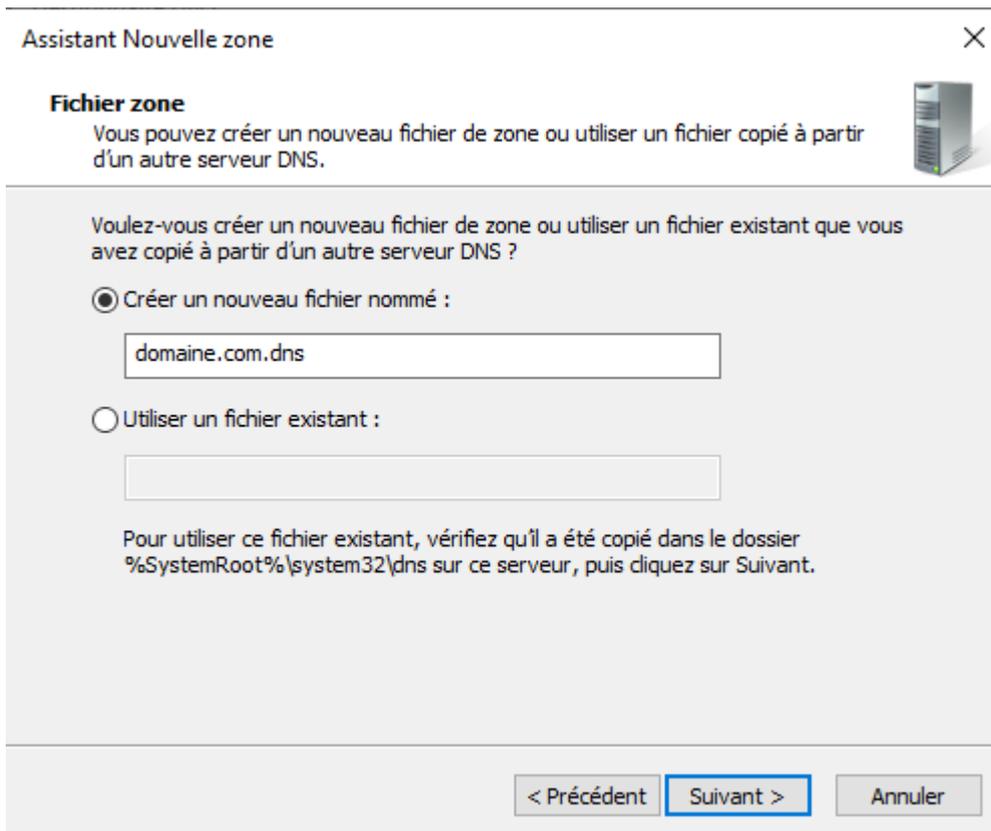
Nom de la zone
Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :

< Précédent Suivant > Annuler

Le serveur va alors générer un fichier contenant les informations de la zone. Cliquez simplement sur suivant :



Autorisez les mises à jour de votre zone afin que les nouveaux hôtes puissent s’y ajouter. Pour des raisons de sécurité, il sera parfois préférable de ne pas autoriser les mises à jour dynamiques et créer les les hôtes à la main.

Assistant Nouvelle zone ✕

Mise à niveau dynamique
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.



Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent Suivant > Annuler

Terminez enfin la configuration.

Assistant Nouvelle zone ✕



Fin de l'Assistant Nouvelle zone

L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :

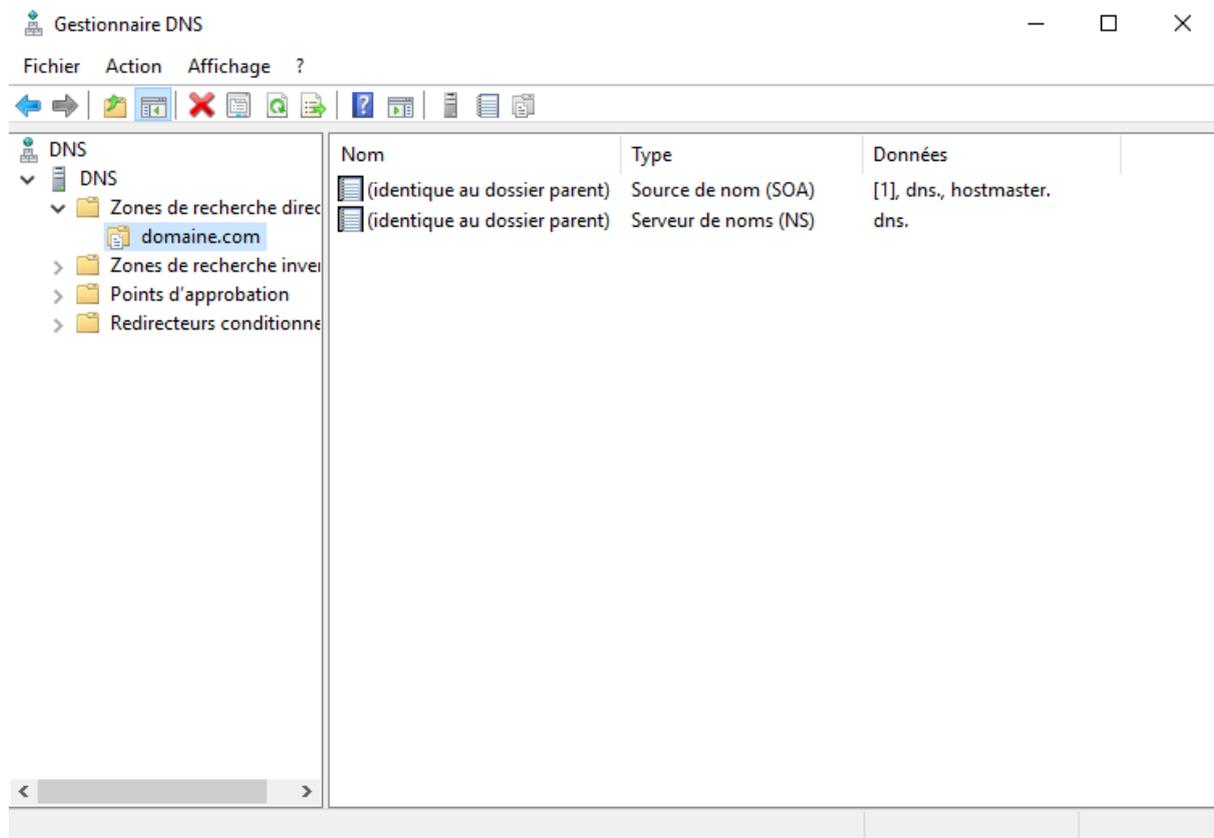
Nom :	domaine.com
Type :	Zone principale standard
Type de recherche :	Directe
Nom de fichier :	domaine.com.dns

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

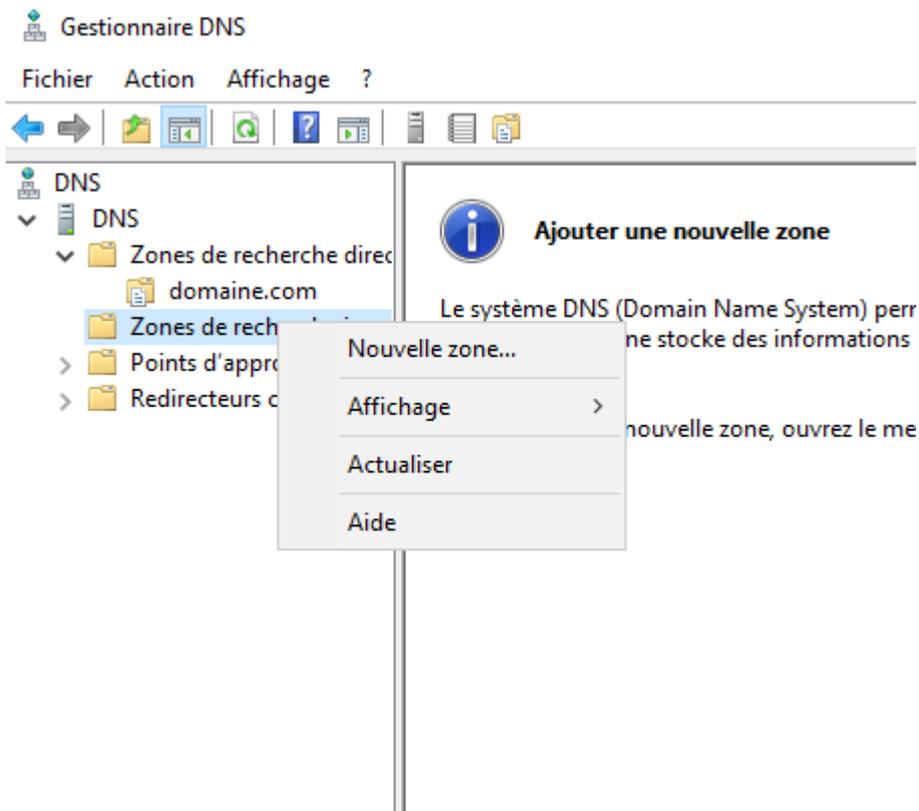
< Précédent Terminer Annuler

Votre zone de recherche directe est maintenant créée. Les nouveaux hôtes devraient apparaître qu'ils sont découverts sur le réseau.

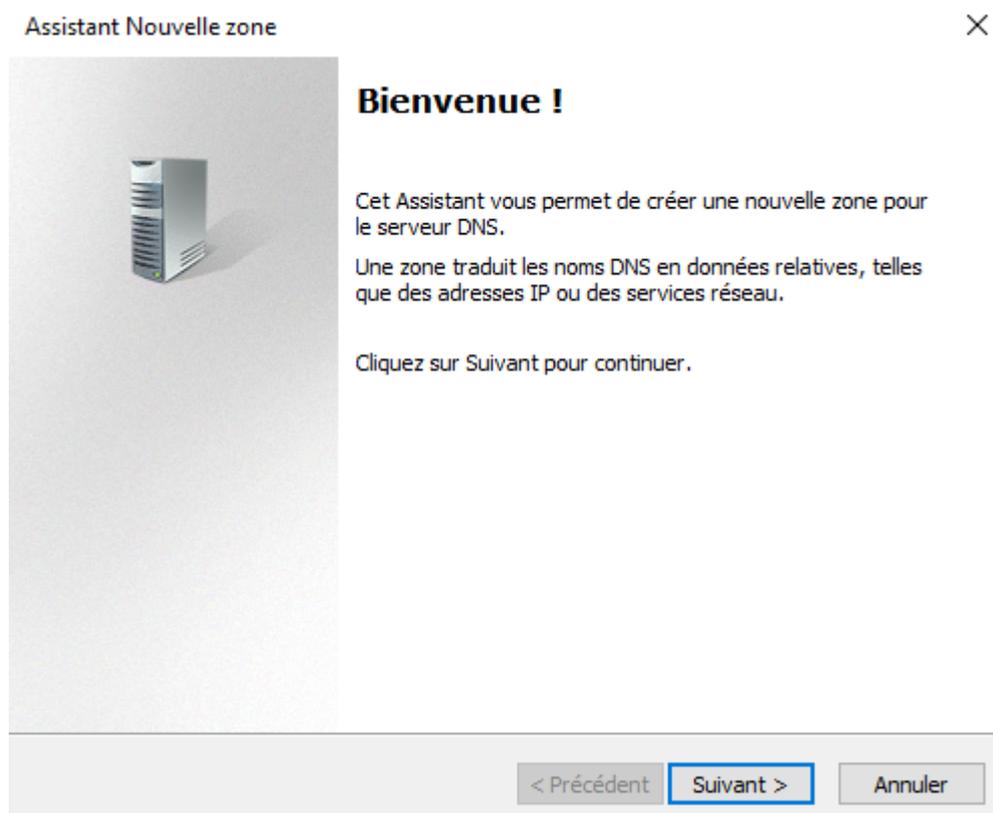


Nous allons mettre en place la recherche inversée sur notre serveur afin d'être également capables de retrouver le nom de domaine à partir de l'IP.

Dans le gestionnaire DNS, cliquez droit sur zone de recherche inversée puis nouvelle zone.



Passez la page de Bienvenue en cliquant sur suivant.



Comme précédemment définissez la zone en zone principale.

Assistant Nouvelle zone ×

Type de zone
Le serveur DNS prend en charge différents types de zones et de stockages. 

Sélectionnez le type de zone que vous voulez créer :

- Zone principale
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
- Zone secondaire
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
- Zone de stub
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

Choisissez la version d'IP qui correspond à votre infrastructure.

Assistant Nouvelle zone



Nom de la zone de recherche inversée

Une zone de recherche inversée traduit les adresses IP en noms DNS.



Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

- Zone de recherche inversée IPv4
- Zone de recherche inversée IPv6

< Précédent

Suivant >

Annuler

Indiquez l'ID de votre réseau sur lequel vous voulez faire fonctionner cette recherche inversée :

Assistant Nouvelle zone



Nom de la zone de recherche inversée

Une zone de recherche inversée traduit les adresses IP en noms DNS.



Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

- ID réseau :

192 .168 .1 | .

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

- Nom de la zone de recherche inversée :

1.168.192.in-addr.arpa

< Précédent

Suivant >

Annuler

Le serveur va également créer un fichier pour cette zone donnée. Cliquez simplement sur suivant.

Assistant Nouvelle zone



Fichier zone

Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS.



Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?

Créer un nouveau fichier nommé :

1.168.192.in-addr.arpa.dns

Utiliser un fichier existant :

Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.

< Précédent

Suivant >

Annuler

Vous pouvez autoriser les mises à jour automatiques pour l'ajout de nouveaux serveurs. Pour des raisons de sécurité il est préférable de renseigner les nouveaux hôtes à la main.

Assistant Nouvelle zone ✕

Mise à niveau dynamique 

Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent Suivant > Annuler

Terminez maintenant la configuration de la recherche inversée.

Assistant Nouvelle zone ✕

Fin de l'Assistant Nouvelle zone

L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :

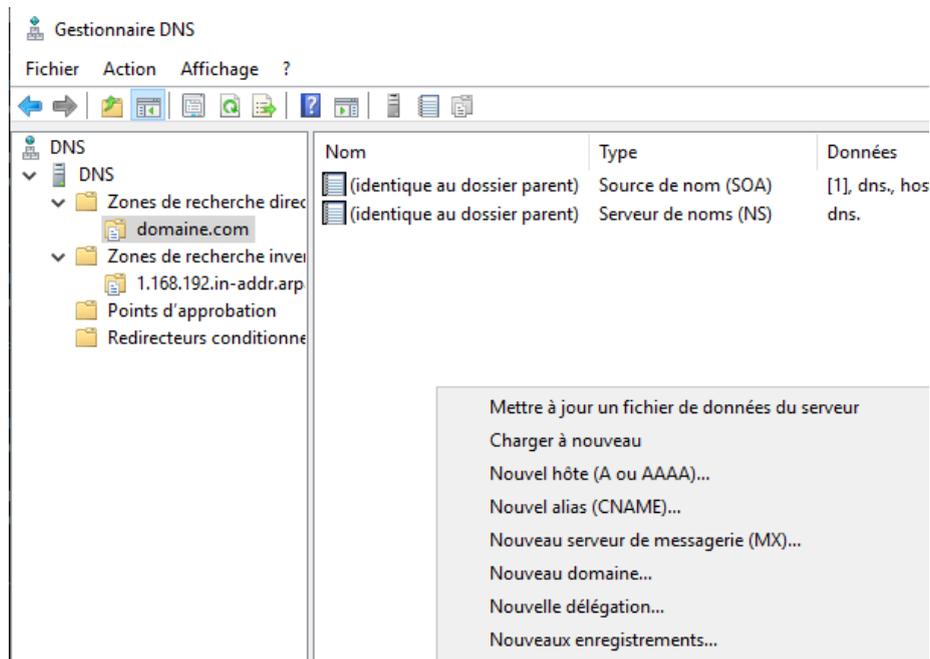
Nom :	1.168.192.in-addr.arpa
Type :	Zone principale standard
Type de recherche :	Inversée
Nom de fichier :	1.168.192.in-addr.arpa.dns

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

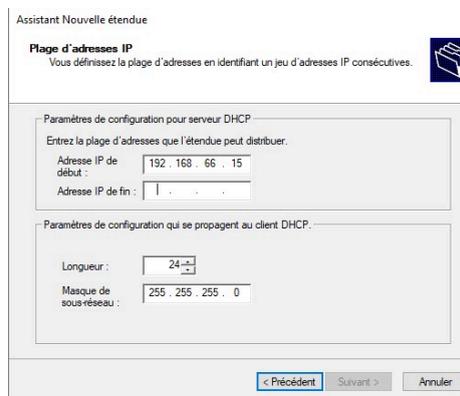
Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

< Précédent Terminer Annuler

Pour tester cette configuration, nous allons créer un hôte réseau dans le gestionnaire DNS. Pour cela cliquez droit dans la liste des enregistrement DNS et cliquez sur nouvel hôte.



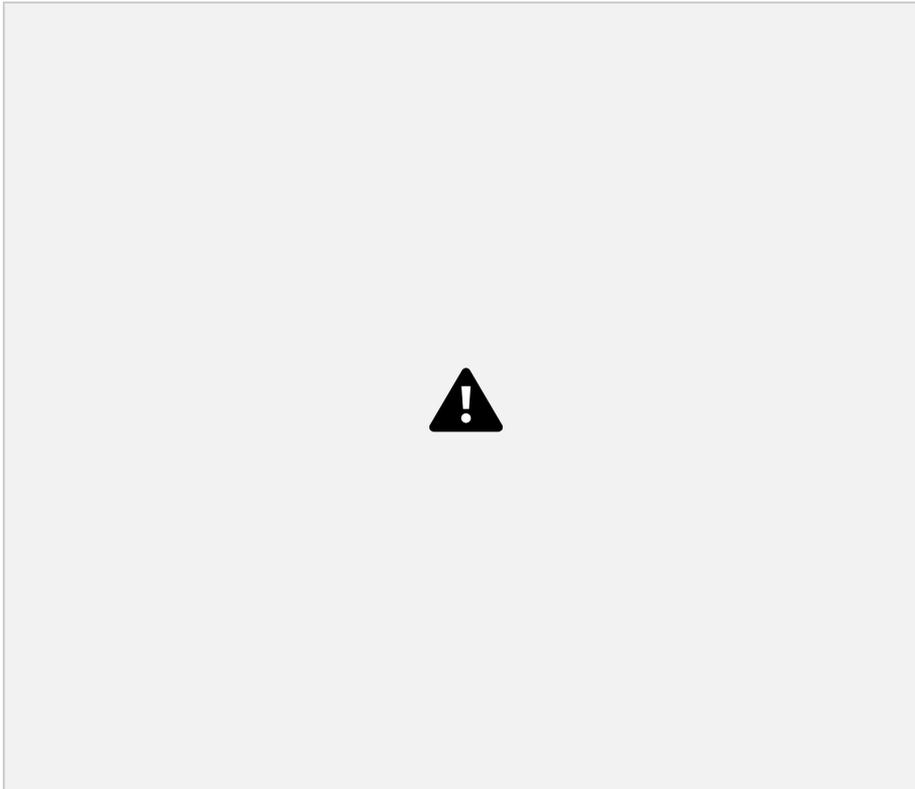
3.2. Service DHCP



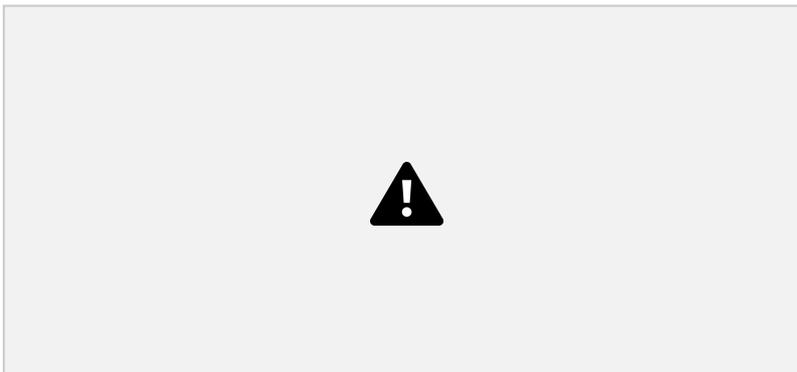
3.3. Création des utilisateurs et de leurs répertoires de stockage

3.4. GPO

Créez une stratégie de groupe.



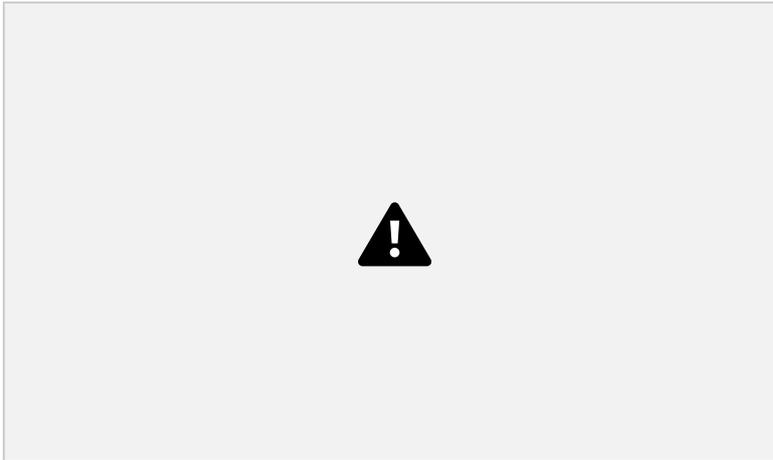
Entrez un nom pour la nouvelle stratégie de groupe.



Dans notre exemple, le nouveau GPO a été nommé : MY-GPO.

Dans l'écran Gestion des stratégies de groupe, développez le dossier nommé Objets de stratégie de groupe.

Cliquez avec le bouton droit sur votre nouvel objet stratégie de groupe et sélectionnez l'option Modifier.

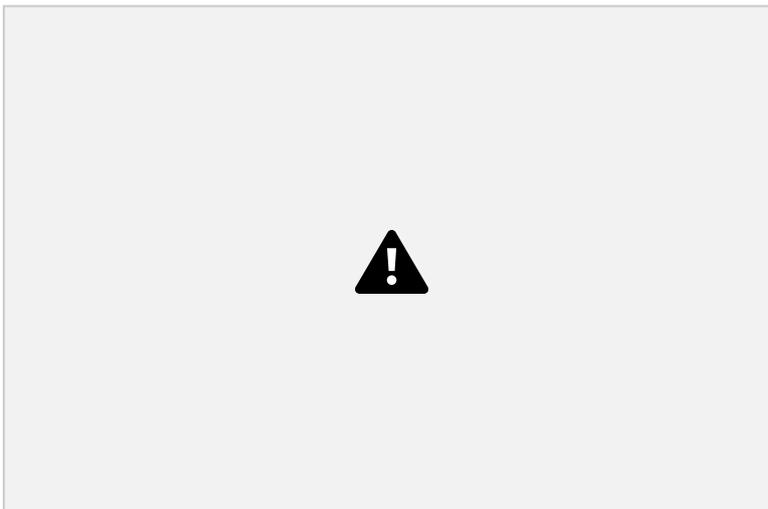


Dans l'écran de l'éditeur de stratégie de groupe, développez le dossier configuration utilisateur et recherchez l'élément suivant.

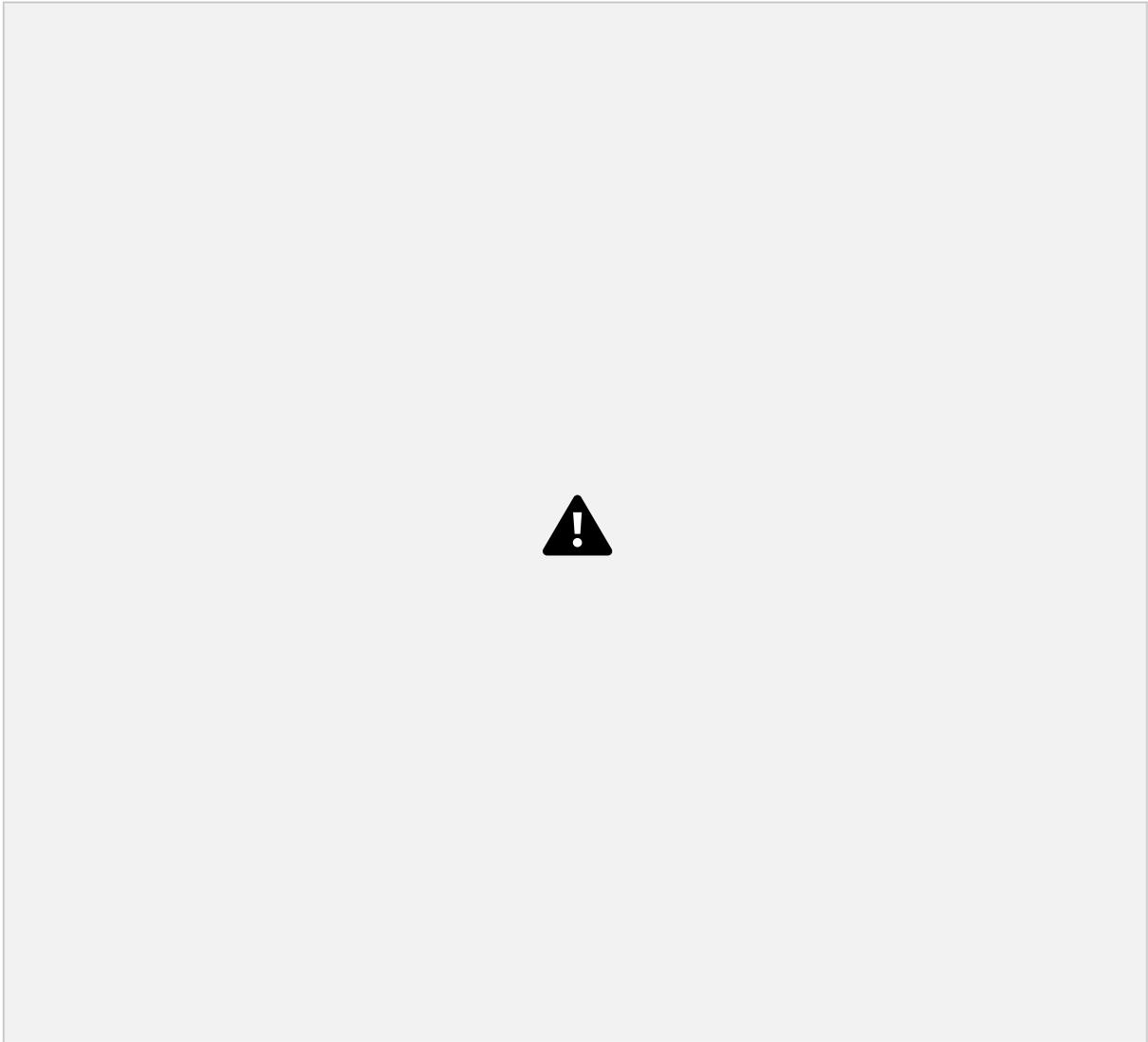
Syntax Highlighter

User Configuration > Politiques > Administrative Templates > Control Panel

Accédez au dossier nommé Panneau de configuration.



Activez l'élément nommé Interdire l'accès aux paramètres du Panneau de configuration et du PC.

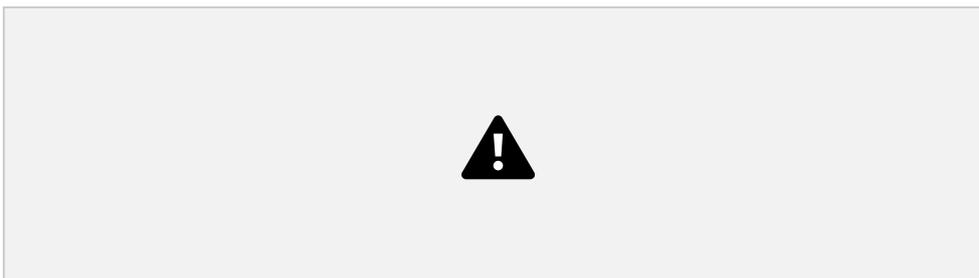


Pour enregistrer la configuration de stratégie de groupe, vous devez fermer l'éditeur de stratégie de groupe.

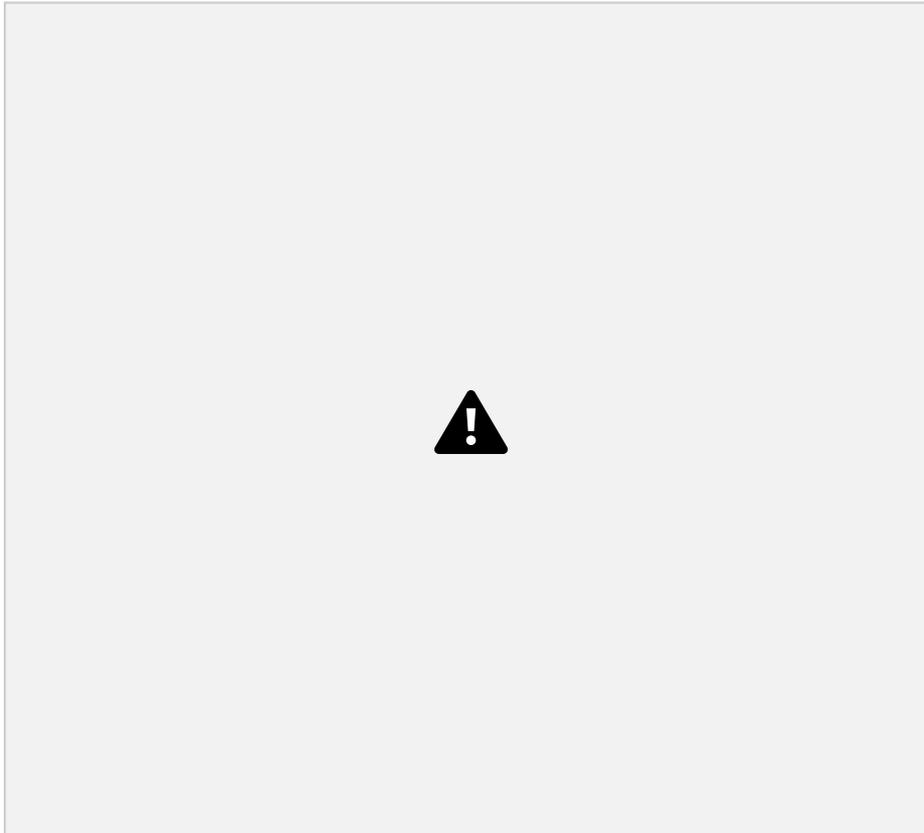
félicitations! Vous avez terminé la création de GPO.

Didacticiel GPO - Désactiver l'accès au Panneau de configuration

Dans l'écran Gestion des stratégies de groupe, vous devez cliquer avec le bouton droit sur l'unité organisationnelle souhaitée et sélectionner l'option pour lier un objet de stratégie de stratégie existant.



Dans notre exemple, nous allons lier la stratégie de groupe nommée MY-GPO à la racine du domaine.



Après l'application de l'objet, vous devez attendre 10 ou 20 minutes. Pendant ce temps, le GPO sera répliqué à d'autres contrôleurs de domaine. Sur un ordinateur distant, essayez d'accéder au panneau De configuration.



Dans notre exemple, nous avons utilisé un GPO pour empêcher l'accès au Panneau de configuration.

3.5 Serveur WSUS

III. Mise en place Linux Serveur 1

Avant toute opération, il nous est important de mettre à jour et à niveau nos paquets.

Pour cela on utilise la commande suivant:

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

Rappel configuration :

@IP	User	Password
192.168.66.10	ut1	P@ssw0rd24

r4.1. Serveur Web

Dans un premier il nous faut installer **Apache** qui est un logiciel de serveur web gratuit et open-source.

`apt install apache2` va nous permettre de l'installer.

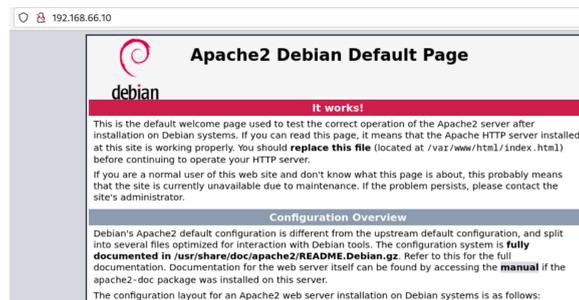
`systemctl status apache2` si l'on souhaite vérifier le statut de notre serveur. Dans notre cas, on voit bien qu'il est actif.

```
ut1@debian:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/ap
   Active: active (running) since Tue 202
```

🔍 192.168.66.10

On devrait pouvoir à présent avoir accès à la page, pour cela il nous suffit d'entrer dans l'url d'un navigateur l'@IP de notre serveur.

Nous arrivons sur cette page si l'installation à bien fonctionner.



Maintenant il nous faut installer PHP afin qu'Apache puisse interpréter des scripts PHP.

`apt install php libapache2-mod-php`



 192.168.66.10/index.php

L'interpréteur fonctionne.

4.2. Serveur GLPI

Dans un premier temps il nous faut télécharger une archive disponible sur github ou sur le site officiel ou contient les pages web qui composent l'application GLPI.



Version GLPI : 10.0.14

3.

Une fois le fichier télécharger il faut veiller à ce que le fichier soit dans le répertoire de publication d'apache.

```
tar -xvzf glpi-10.0.14.taz va nous permettre d'extraire le fichier.
```

Maintenant il est nécessaire de créer un **virtualhost** qui va permette de faire cohabiter plusieurs serveurs web sur une même machine, dans notre cas cela nous sert à accéder à notre GLPI.

Étape 1 : Création d'un fichier **glpi.conf**

```
nano /etc/apache2/sites-available/glpi.conf
```

0

Étape 2 : Configuration du fichier

```
<VirtualHost *:80>

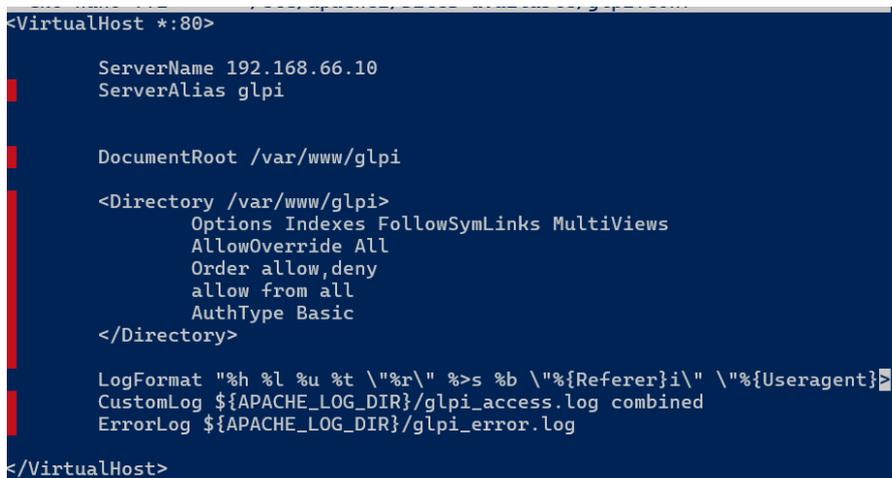
    ServerName 192.168.66.10
    ServerAlias glpi

    DocumentRoot /var/www/glpi

    <Directory /var/www/glpi>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
        Order allow,deny
        allow from all
        AuthType Basic
    </Directory>

    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{Useragent}i\"" combined
    CustomLog ${APACHE_LOG_DIR}/glpi_access.log combined
    ErrorLog ${APACHE_LOG_DIR}/glpi_error.log

</VirtualHost>
```



```
<VirtualHost *:80>

    ServerName 192.168.66.10
    ServerAlias glpi

    DocumentRoot /var/www/glpi

    <Directory /var/www/glpi>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
        Order allow,deny
        allow from all
        AuthType Basic
    </Directory>

    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{Useragent}i\"" combined
    CustomLog ${APACHE_LOG_DIR}/glpi_access.log combined
    ErrorLog ${APACHE_LOG_DIR}/glpi_error.log

</VirtualHost>
```

Configuration virtualHost :

```
sudo chown -R www-data:www-data /var/www/ glpi
```

droit

On peut maintenant taper l'adresse ip dans la barre :



```
root@debian:/# sudo a2ensite glpi.conf
Site glpi already enabled
root@debian:/# sudo service apache2 reload
```



on installe

<p>Requis Extensions du noyau de PHP</p> <p><i>Les extensions suivantes sont installées : fileinfo, filter, libxml, json.</i></p> <p><i>Les extensions suivantes sont manquantes : dom, simplexml, xmlreader, xmlwriter.</i></p>	×
<p>Requis curl extension</p> <p><i>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</i></p> <p><i>l'extension curl est absente.</i></p>	×
<p>Requis gd extension</p> <p><i>Requis pour le traitement des images.</i></p> <p><i>l'extension gd est absente.</i></p>	×
<p>Requis intl extension</p> <p><i>Requis pour l'internationalisation.</i></p> <p><i>l'extension intl est absente.</i></p>	×

On peut voir qu'il nous manque des extensions c'est pourquoi nous allons les installer sur le serveur web.

```
apt install php-curl php-gd php-intl php-xml php-xmlreader php-xmlwriter
```

sans oublier de redémarrer apache.

```
systemctl restart apache2
```

TESTS EFFECTUÉS	RÉSULTATS
Requis Parser PHP	✓
Requis Configuration des sessions	✓
Requis Mémoire allouée	✓
Requis mysqli extension	✓
Requis Extensions du noyau de PHP	✓
Requis curl extension <i>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</i>	✓
Requis gd extension <i>Requis pour le traitement des images.</i>	✓
Requis intl extension <i>Requis pour l'internationalisation.</i>	✓
Requis zlib extension <i>Requis pour la gestion de la communication compressée avec les agents d'inventaire, l'installation de paquets gzip à partir du Marketplace et la génération de PDF.</i>	✓

Maintenant on remarque que tout tes passer en vert après cliquer sur



GLPI **GLPI SETUP**

Étape 1
Configuration de la connexion à la base de données

Serveur SQL (MariaDB ou MySQL)
192.168.66.11

Utilisateur SQL
glpi

Mot de passe SQL
P@ssw0rd24

Continuer >

Maintenant on configure la bdd, en entrant l'adresse ip du serveur sql, ainsi que l'utilisateur et mot de passe que nous avons créer ayant les droits à la base tamaran_glpi

Mais avant de procéder à ça sur notre serveur sql il faut vérifier que dans

```
nano /etc/mysql/mariadb.conf.d/50-server.cnf
```

Il est `bind-address = 0.0.0.0`

Sans oublier de redémarrer notre système sql

```
systemctl restart mysql
```

C'est bon la connexion à réussie, on sélectionne la base que nous avons créé précédemment sur notre server bdd

GLPI **GLPI SETUP**

Étape 2
Test de connexion à la base de données

✓ Connexion à la base de données réussie

Veillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

tamaran_glpi

Continuer >



GLPI SETUP

Étape 3

Initialisation de la base de données.

OK - La base a bien été initialisée

[Continuer >](#)



GLPI SETUP

Étape 4

Récolter des données

Envoyer "statistiques d'usage"

Nous avons besoin de vous pour améliorer GLPI et son écosystème de plugins !

Depuis GLPI 9.2, nous avons introduit une nouvelle fonctionnalité de statistiques appelée "Téléométrie", qui envoie anonymement, avec votre permission, des données à notre site de téléométrie. Une fois envoyées, les statistiques d'usage sont agrégées et rendues disponibles à une large audience de développeurs GLPI.

Dites-nous comment vous utilisez GLPI pour que nous améliorions GLPI et ses plugins !

[Voir ce qui serait envoyé...](#)

Référez votre GLPI

Par ailleurs, si vous appréciez GLPI et sa communauté, prenez une minute pour référencer votre organisation en remplissant le formulaire suivant [Le formulaire d'inscription](#)

[Continuer >](#)



Glpi **GLPI SETUP**

Étape 5

Une dernière chose avant de démarrer

Vous souhaitez obtenir de l'aide pour intégrer GLPI dans votre SI, faire corriger un bug ou bénéficier de règles ou dictionnaires pré-configurés ?

Nous mettons à votre disposition l'espace <https://services.glpi-network.com>.
GLPI-Network est un service commercial qui comprend une souscription au support niveau 3, garantissant la correction des bugs rencontrés avec un engagement de délai.

Sur ce même espace, vous pourrez contacter un partenaire officiel pour vous aider dans votre intégration de GLPI.

Continuer >



Glpi **GLPI SETUP**

Étape 6

L'installation est terminée

Les identifiants et mots de passe par défaut sont :

- glpi/glpi pour le compte administrateur
- tech/tech pour le compte technicien
- normal/normal pour le compte normal
- post-only/postonly pour le compte postonly

Vous pouvez supprimer ou modifier ces comptes ainsi que les données initiales.

Utiliser GLPI

Connexion à votre compte

Identifiant

glpi

Mot de passe

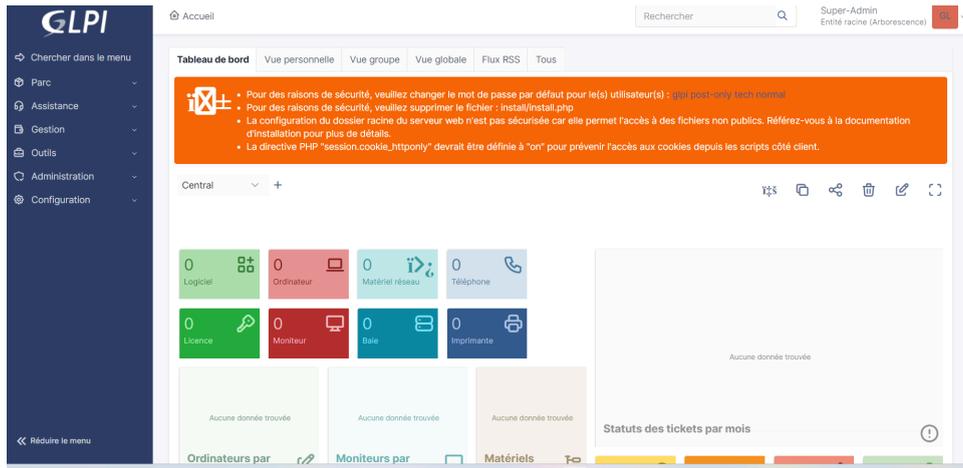
glpi

Source de connexion

Base interne GLPI

Se souvenir de moi

Se connecter



IV. Mise en place Linux Serveur 2

Avant toute opération, il nous est important de mettre à jour et à niveau nos paquets.

Pour cela on utilise la commande suivant:

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

Rappel configuration :

@IP	User	Password
192.168.66.11	ut1	P@ssw0rd24

5.1. Serveur de base de données

Il nous faut installer mariadb

```
apt install mariadb-server
```

Affecte un mot de passe au root pour la connexion à la bdd.

```
mysql_secure_installation
```

Ensuite on se connecte pour créer notre base de donnée

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

```
CREATE DATABASE tamaran_glpi;
```

Création de la bdd

Création d'un
utilisateur glpi

```
CREATE USER 'glpi'@'192.168.66.10' IDENTIFIED BY 'P@ssw0rd24';
```

pour accès à la bdd. L'adresse est celle du serveur web.

```
GRANT ALL PRIVILEGES ON tamaran_glpi.* TO 'glpi'@'192.168.66.10';
```

On affecte nos privilèges à l'utilisateur à notre base de données tamaran_glpi

On active ensuite

```
FLUSH PRIVILEGES;
```


V. Scripts de sauvegardes des pages web

```
# Sauvegarder BDD MySQL
mysqldump -u admin-p Tamarin > /home/user1/DossierSauvegarde/sauvegarde -$(date
+%y%m%d).sql

# Transférer sauvegarde vers un hôte
scp /home/ut1/DossierSauvegarde/sauvegarde- $(date +%y%m%d).sql
ut1@192.168.66.15:/home/ut1/SauvegardeWeb
```

VI. Sécurité du service web

7.1. Installation de Wireshark

7.2. Contrôle des échanges HTTP

7.3. Solutions de sécurisation

VII. Conclusion