



Implémentation d'un Contrôleur de Domaine avec Windows Server 2019/2022 et Déploiement PXE d'Images Personnalisées

**LECCE Baptiste
Projet déploiement PXE – Epreuve E5**

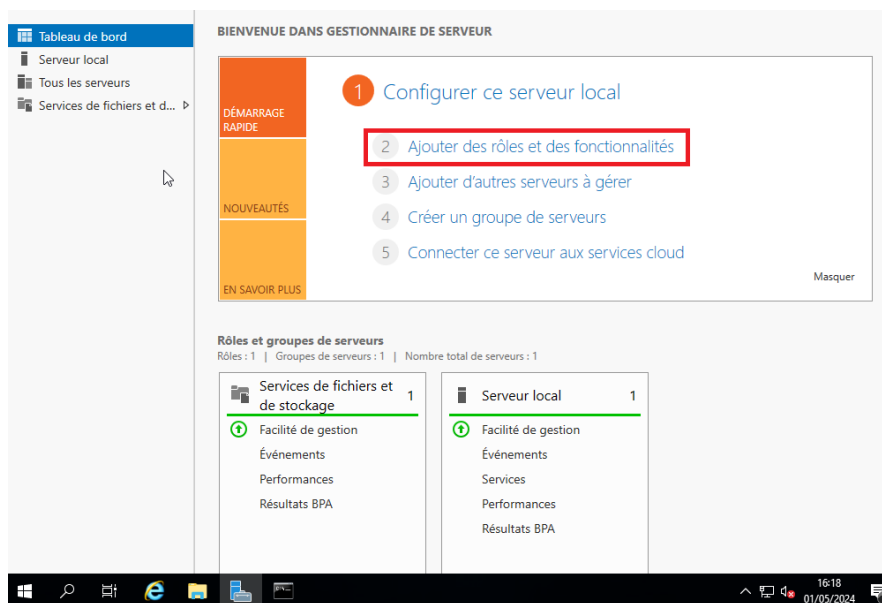
Session 2024

Installation de l'Active Directory.

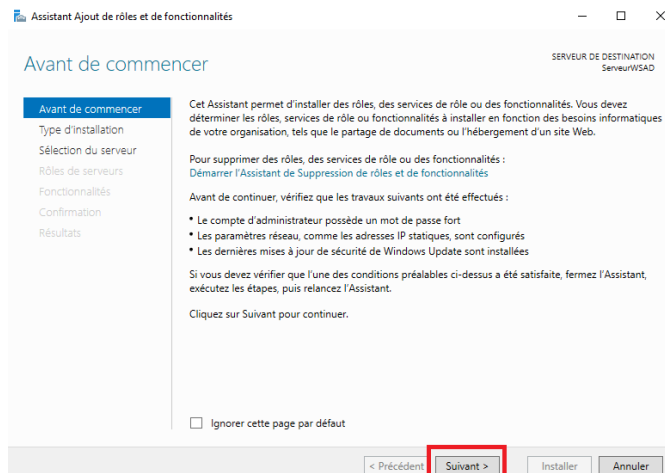


- Renommez votre serveur pour plus de clarté (facultatif mais recommandé).
- Configurez une IP statique.

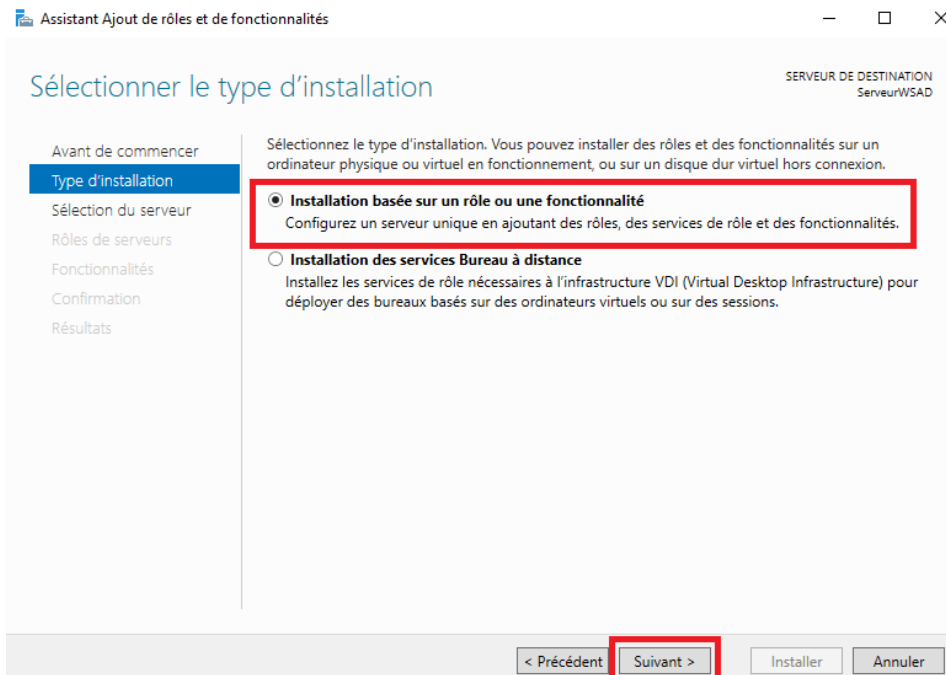
1) Accédez au gestionnaire de serveur et sélectionnez "Ajouter des rôles et des fonctionnalités".



2) Cliquez sur « suivant ».



3) Optez pour l'installation basée sur un rôle ou une fonctionnalité pour configurer un serveur unique avec des rôles, des services de rôle et des fonctionnalités personnalisés.



4) Choisissez votre serveur, qu'un seul disponible pour le moment, puis suivant.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
ServeurWSAD

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

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
ServeurWSAD	192.168.174.138	Microsoft Windows Server 2019 Standard

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Installer Annuler

5) Cocher « Serveur DNS » et « Services AD DS »

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
ServeurWSAD

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Serveur DNS

AD DS

Confirmation

Résultats

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

Rôles

- ☐ Accès à distance
- ☐ Attestation d'intégrité de l'appareil
- ☐ Hyper-V
- ☐ Serveur de télécopie
- ☐ Serveur DHCP
- ☒ Serveur DNS
- ☐ Serveur web (IIS)
- ☐ Service Guard du hôte
- ☒ Services AD DS
- ☐ Services AD LDS (Active Directory Lightweight Directory Services)
- ☐ Services AD RMS (Active Directory Rights Management Services)
- ☐ Services Bureau à distance
- ☐ Services d'activation en volume
- ☐ Services d'impression et de numérisation de documents
- ☐ Services de certificats Active Directory
- ☐ Services de déploiement Windows
- ☐ Services de fédération Active Directory (AD FS)
- ☒ Services de fichiers et de stockage (1 sur 12 installés)
- ☐ Services de stratégie et d'accès réseau

Description

Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.

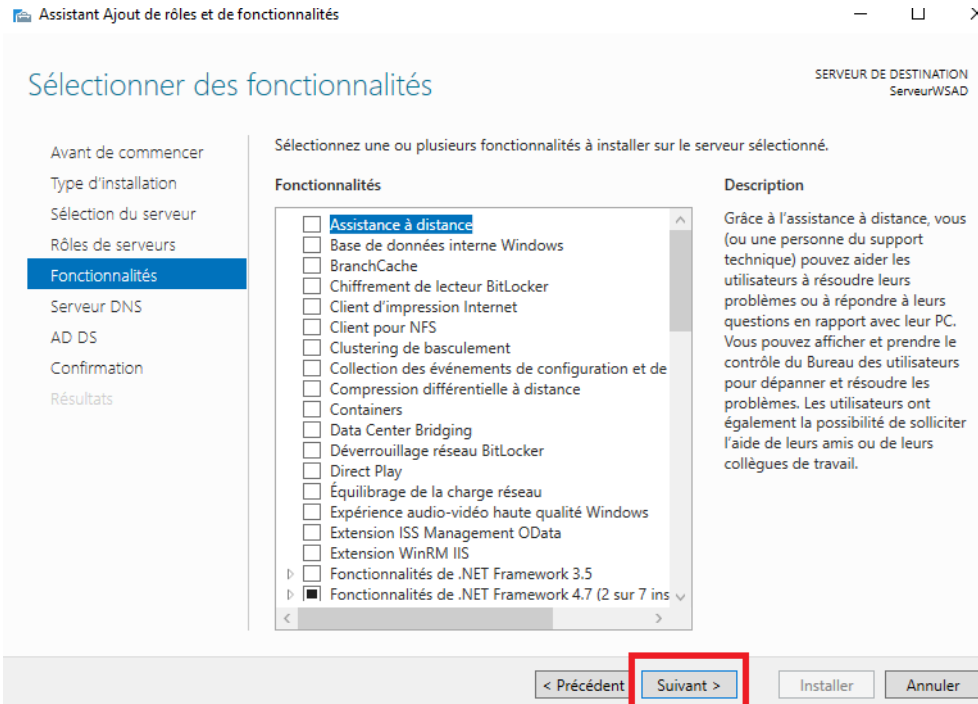
< Précédent

Suivant >

Installer

Annuler

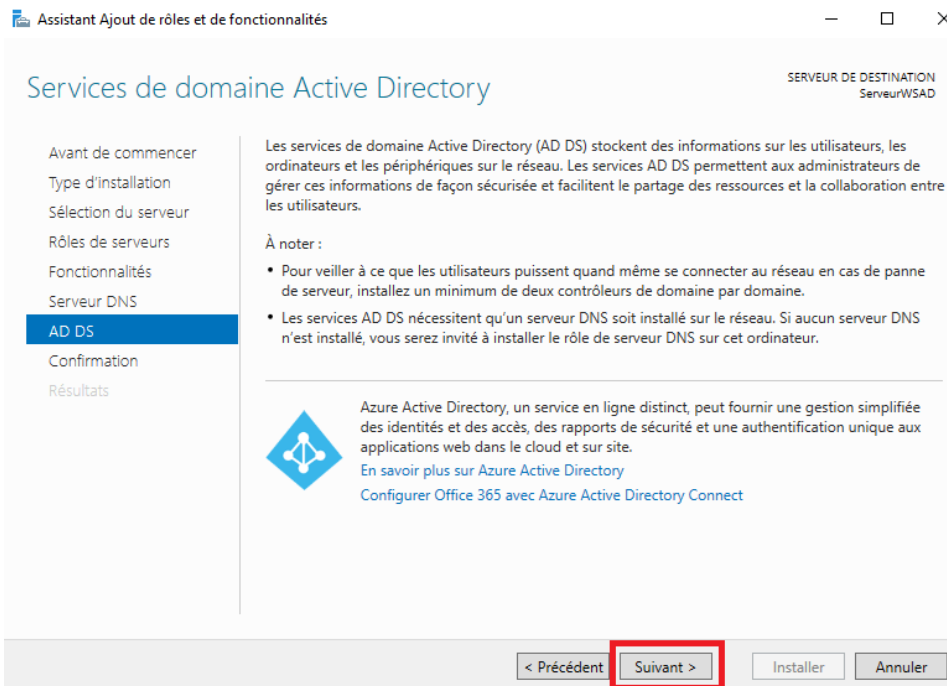
6) Aucune fonctionnalité nécessaire pour le moment, cliquez sur suivant.



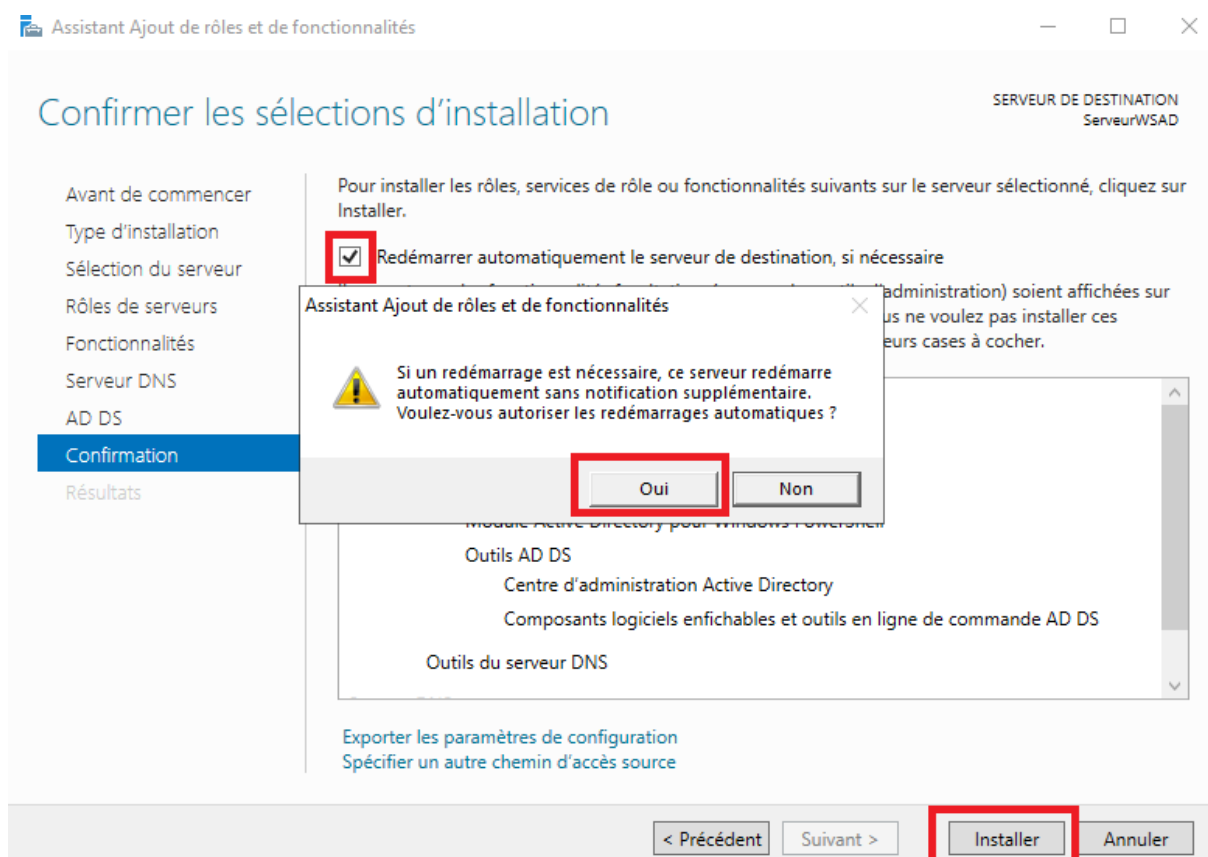
7) Cliquez sur « Suivant ».



8) Cliquez sur « Suivant »



- 9) Dans l'ordre suivant cliqué sur « Redémarrer automatiquement le serveur.. », cliqué sur 'oui' dans la fenêtre « Assistant Ajout de rôles et de fonctionnalités » puis « Installer » en bas à droite.



10) *Après l'installation des rôles et le redémarrage du serveur, dès que ce processus sera terminé, une fenêtre s'ouvrira. À ce moment-là, procédez à la promotion de ce serveur en tant que contrôleur de domaine, comme ci-dessous.*



Progression de l'installation

SERVEUR DE DESTINATION
ServeurWSAD

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Serveur DNS

AD DS

Confirmation

Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité

Configuration requise. Installation réussie sur ServeurWSAD.

Services AD DS

Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.

Promouvoir ce serveur en contrôleur de domaine**Gestion de stratégie de groupe****Outils d'administration de serveur distant****Outils d'administration de rôles****Outils AD DS et AD LDS****Module Active Directory pour Windows PowerShell****Outils AD DS**

Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

[Exporter les paramètres de configuration](#)

< Précédent

Suivant >

Fermer

Annuler

- 11) Si vous souhaitez créer un domaine, sélectionnez l'option "Nouvelle forêt" (notre cas). Toutefois, si vous disposez déjà d'un domaine existant, optez pour la première option. Ensuite, veuillez renseigner un nom de domaine.

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
ServeurWSAD

- 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

Nom de domaine racine :

[En savoir plus sur les configurations de déploiement](#)

< Précédent Suivant > Installer Annuler

- 12)** Choisissez soigneusement un mot de passe pour la restauration des services d'AD et prenez soin de le noter, car cela pourrait s'avérer nécessaire à l'avenir, puis cliquez sur « Suivant ».

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SERVEUR CIBLE
ServeurWSAD

Configuration de déploiement...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configuration...
Installation
Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

☒ Serveur DNS (Domain Name System)
☒ Catalogue global (GC)
☐ Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent **Suivant >** Installer Annuler

- 13)** Cliquez sur « Suivant ».

Assistant Configuration des services de domaine Active Directory

Options DNS

SERVEUR CIBLE
ServeurWSAD

Configuration de déploiement...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configuration...
Installation
Résultats

Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est intro... [Afficher plus](#)

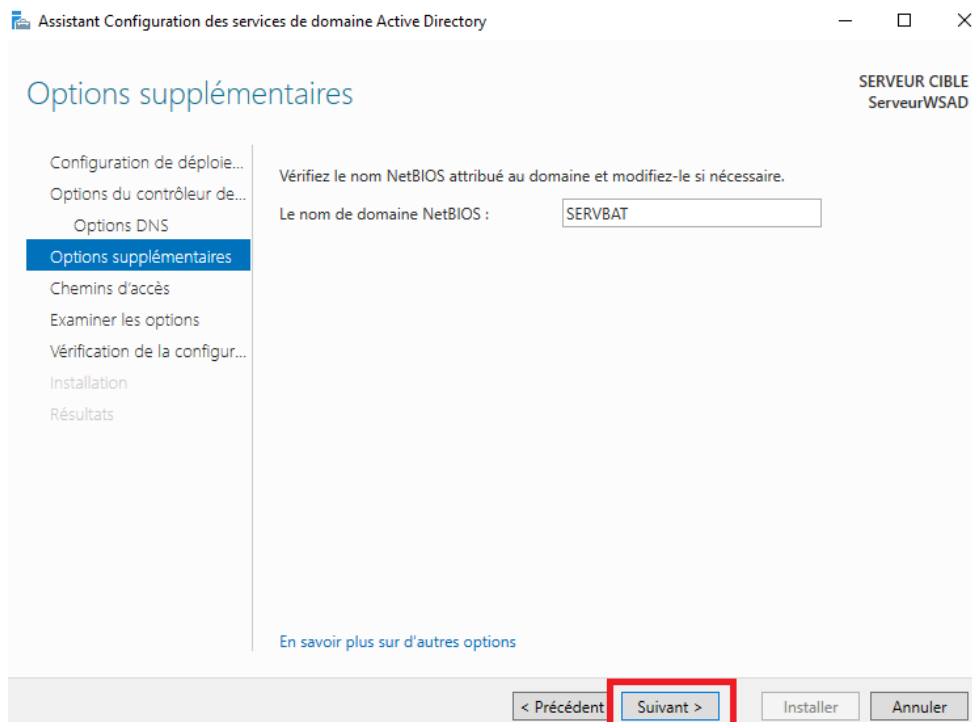
Spécifier les options de délégation DNS

☐ Créer une délégation DNS

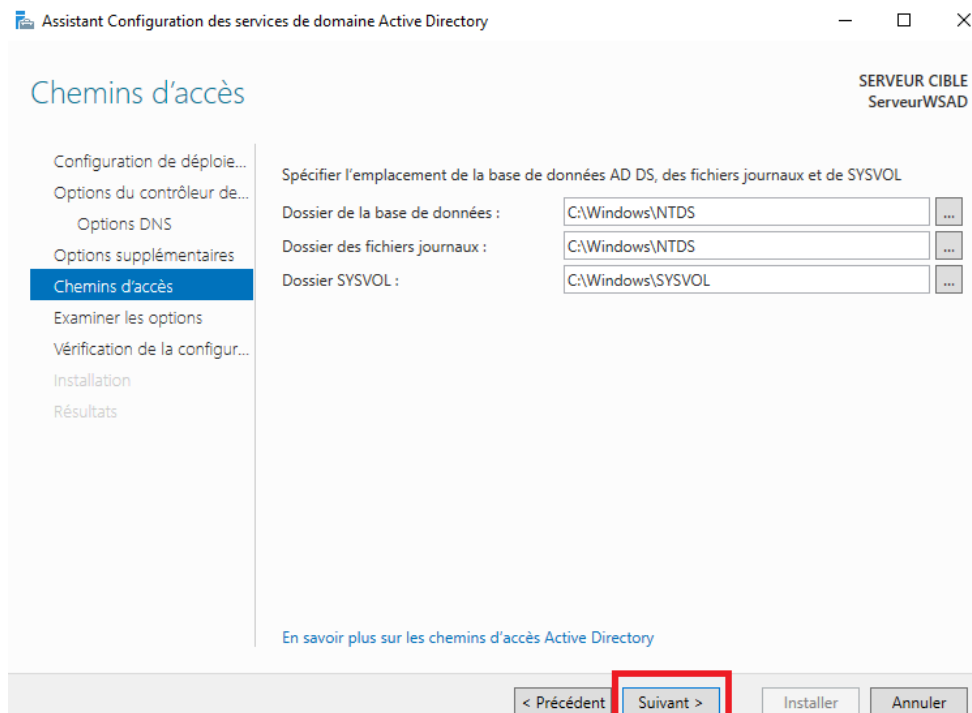
[En savoir plus sur la délégation DNS](#)

< Précédent **Suivant >** Installer Annuler

- 14)** Cliquez sur « Suivant »



15) Cliquez sur « Suivant ».



16) Après vérification que toutes les informations sont correctes, cliquez « Suivant ».

Examiner les options

SERVEUR CIBLE
ServeurWSAD

- Configuration de déploie...
- Options du contrôleur de...
- Options DNS
- Options supplémentaires
- Chemins d'accès
- Examiner les options**
- Vérification de la configur...
- Installation
- Résultats

Vérifiez vos sélections :

Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.

Le nouveau nom de domaine est « servbat.local ». C'est aussi le nom de la nouvelle forêt.

Nom NetBIOS du domaine : SERVBAT

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Options supplémentaires :

Catalogue global : Oui

Serveur DNS : Oui

Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires

Afficher le script

[En savoir plus sur les options d'installation](#)

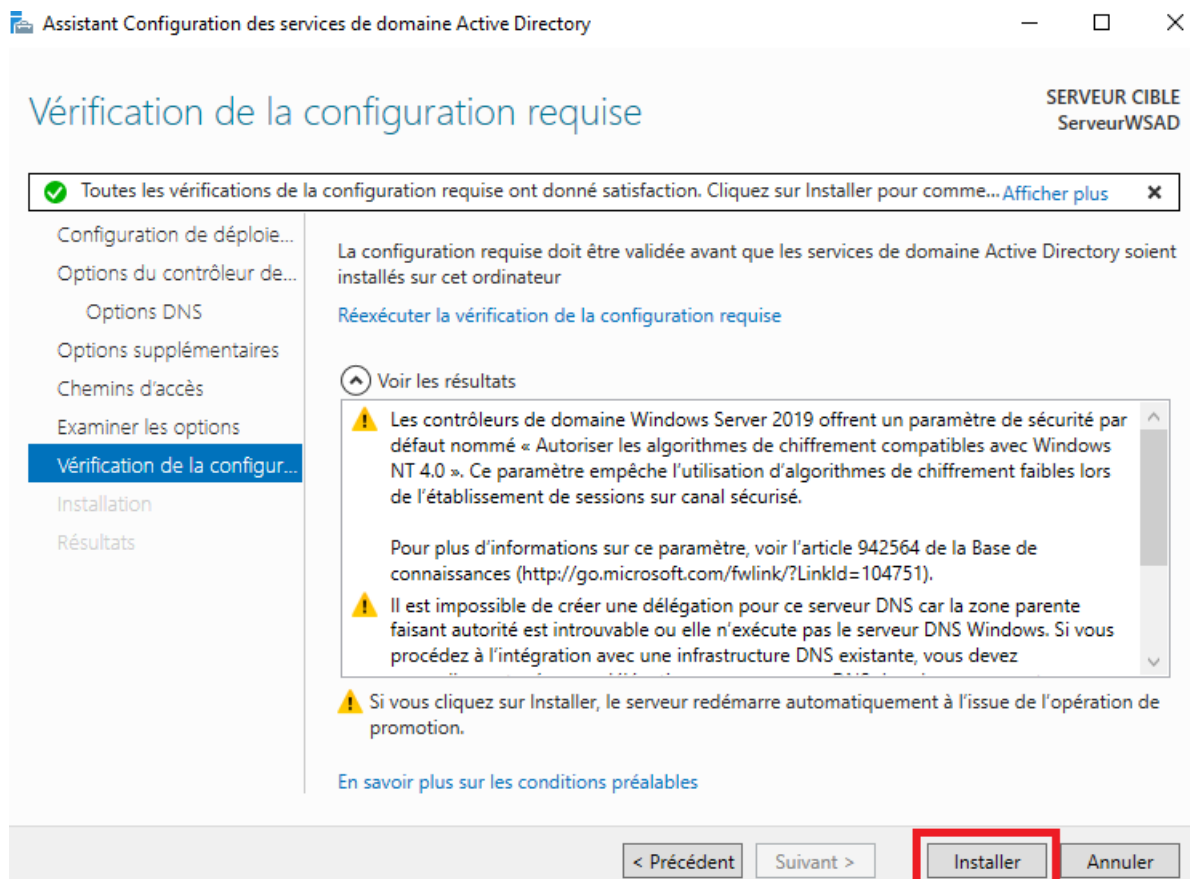
< Précédent

Suivant >

Installer

Annuler

17) Attendre quelques secondes la vérification, puis cliqué sur « Installer ».



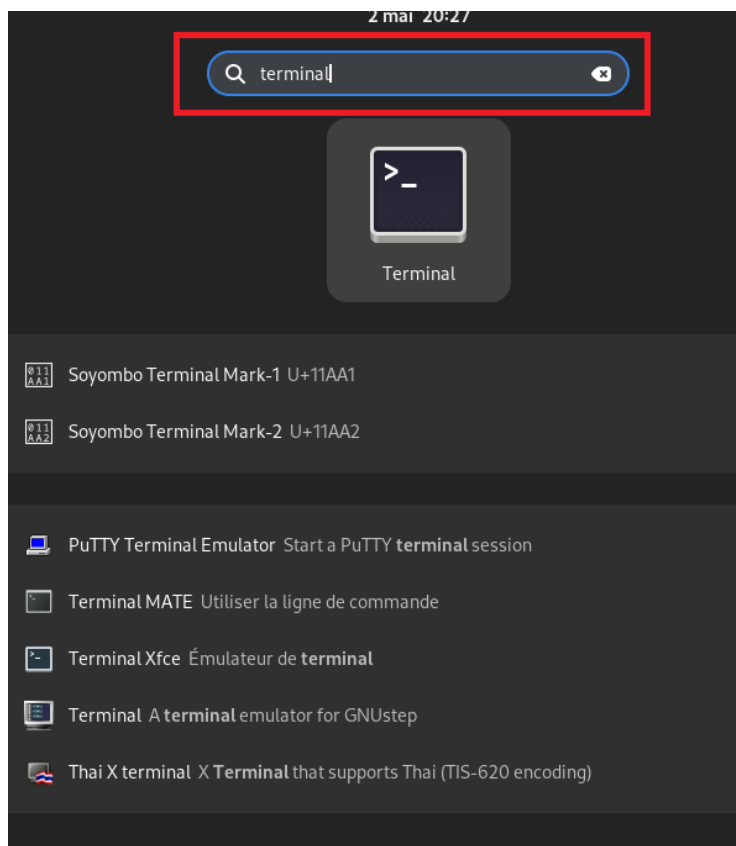
Désormais, vous pouvez intégrer vos postes de travail ou d'autres serveurs dans le domaine. Une fois cela fait, vous pourrez vous connecter en utilisant le format domaine\utilisateur.

Attention, lors de l'ajout d'un poste ou d'un serveur au domaine, assurez-vous d'ajouter l'adresse IP de votre serveur AD en tant que serveur DNS sur les machines cibles. Sans cela, la machine que vous souhaitez ajouter risque de ne pas trouver le domaine.

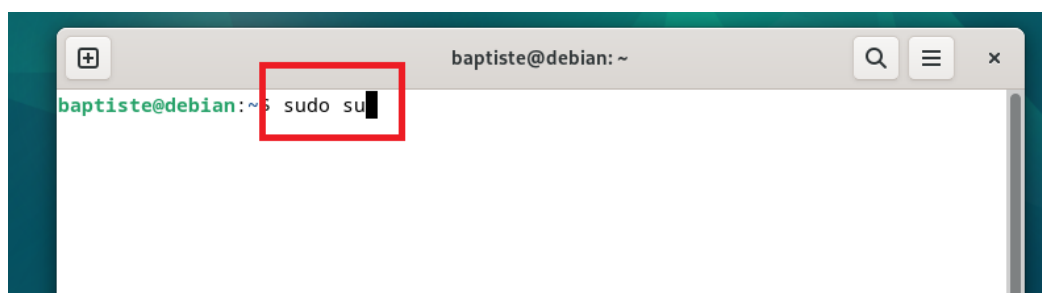
Procédure d'installation GLPI



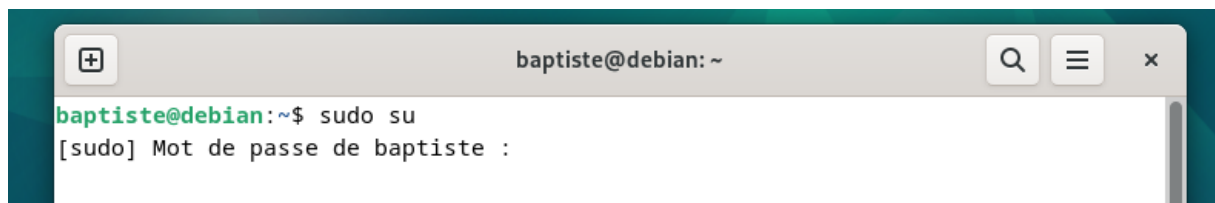
- 1) Accédez au « Terminal » de votre Debian.



- 2) Insérez dans un premier temps « sudo su » afin de vous connectez en tant qu'administrateur et éviter de taper le mot de passe pour toutes commandes suivantes.

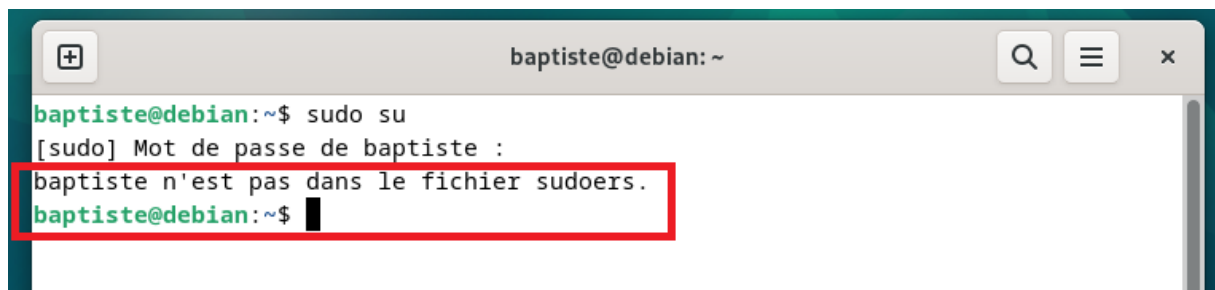


- 3) Insérez votre mot de passe de connexion



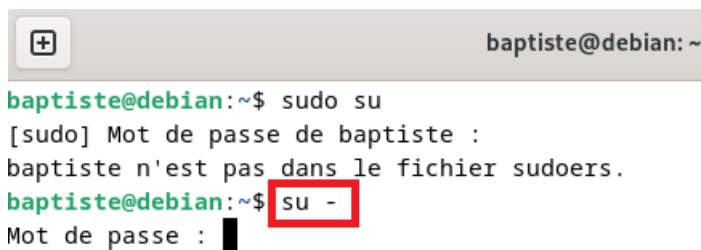
```
baptiste@debian: ~  
baptiste@debian:~$ sudo su  
[sudo] Mot de passe de baptiste :
```

- 4) **ATTENTION**, si cette erreur apparaît il vous suffit de rajouter votre utilisateur dans le fichier sudoers. (capture en dessous).



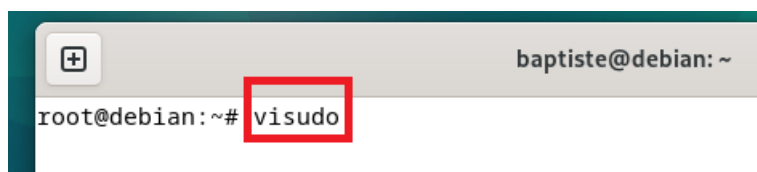
```
baptiste@debian:~$ sudo su  
[sudo] Mot de passe de baptiste :  
baptiste n'est pas dans le fichier sudoers.  
baptiste@debian:~$
```

- 5) Insérez **su -** puis entrez votre mot de passe, puis press ENTER.



```
baptiste@debian:~$ sudo su  
[sudo] Mot de passe de baptiste :  
baptiste n'est pas dans le fichier sudoers.  
baptiste@debian:~$ su -  
Mot de passe :
```

- 6) Insérez « visudo » puis press ENTER.



```
root@debian:~# visudo
```

- 7) Descendre tout en bas jusqu'à trouver « root ALL=(ALL : ALL) ALL » puis insérez comme-ci-dessous votre utilisateur.


```
baptiste@debian: ~
GNU nano 7.2 /etc/sudoers.tmp *

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
baptiste ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
```

POUR ENREGISTRER FAITE **CTRL+X** puis **MAJ+O** puis **ENTER**.

- 8) Insérez **exit**, press ENTER, insérez **sudo su**, press ENTER, puis entrez votre mot de passe, press ENTER.

```
baptiste@debian: ~
root@debian:~# visudo
root@debian:~# exit
déconnexion
baptiste@debian:~$ sudo su
[sudo] Mot de passe de baptiste : 
root@debian:/home/baptiste#
```

- 9) Démarrez par la mise à jour des paquets sur Debian 12, attribuez une adresse IP et configurez le système, à l'aide de cette commande, press ENTER.

```
root@debian:/home/baptiste# sudo apt-get update && sudo apt-get upgrade
```

- 10)** La première étape clé est d'installer le socle LAMP (Linux, Apache2, MariaDB, PHP) sur Debian 12, où PHP 8.2 est inclus par défaut dans les dépôts officiels, à l'aide de cette commande, press ENTER.

```
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.  
root@debian:/home/baptiste# sudo apt-get install apache2 php mariadb-server
```

Souhaitez-vous continuer ? [0/n] INSERER « o » pour continuer, press ENTER.

- 11)** Ensuite, installez les extensions nécessaires pour le fonctionnement optimal de GLPI, à l'aide de cette commande, puis press ENTER.

```
root@debian:/home/baptiste# sudo apt-get install php-xml php-common php-json php-  
-mysql php-mbstring php-curl php-gd php-intl  
php-zip php-bz2 php-imap php-apcu
```

Souhaitez-vous continuer ? [0/n] INSERER « o » pour continuer, press ENTER.

- 12)** Ces commandes récupèrent les versions adaptées à PHP 8.2 des extensions nécessaires. Si vous prévoyez d'intégrer GLPI avec un annuaire LDAP tel qu'Active Directory, installez l'extension LDAP de PHP ; sinon, cela peut être ajouté ultérieurement si nécessaire.

```
root@debian:/home/baptiste# sudo apt-get install php-ldap
```

Souhaitez-vous continuer ? [0/n] INSERER « o » pour continuer, press ENTER.

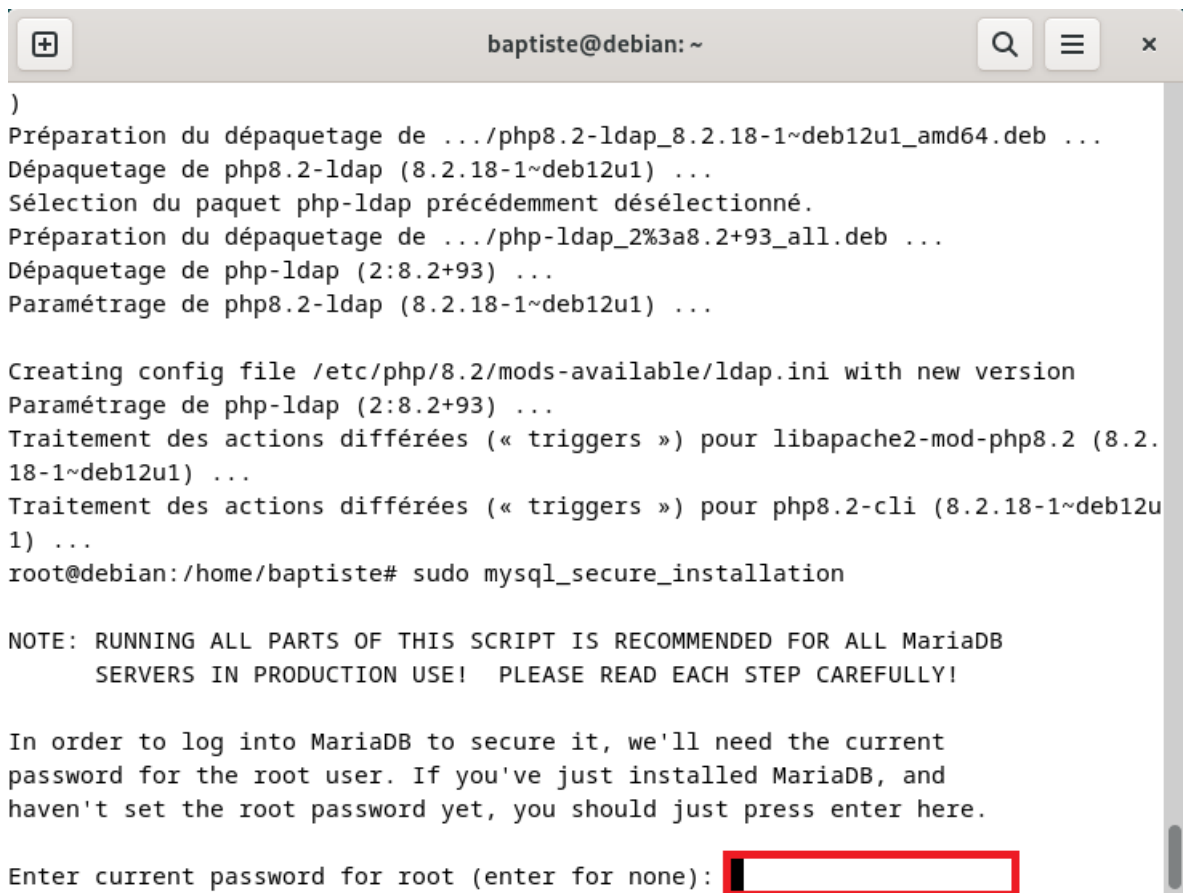
Nous venons d'installer Apache2, MariaDB, PHP et un ensemble d'extensions.

Préparer une base de données pour GLPI

Préparez MariaDB à héberger la base de données GLPI. Commencez par exécuter la commande suivante pour sécuriser au minimum MariaDB, à l'aide de cette commande, press ENTER. root@debian:/home/baptiste# `sudo mysql_secure_installation`

Vous serez invité à changer le mot de passe root, supprimer les utilisateurs anonymes, désactiver l'accès root à distance, et plus. Chaque étape est clairement expliquée. Voici un exemple pour vous guider :

13) Définir un mot de passe pour l'administrateur de la base de donnée, press ENTER.



```
baptiste@debian: ~  
)  
Préparation du dépaquetage de .../php8.2-ldap_8.2.18-1~deb12u1_amd64.deb ...  
Dépaquetage de php8.2-ldap (8.2.18-1~deb12u1) ...  
Sélection du paquet php-ldap précédemment désélectionné.  
Préparation du dépaquetage de .../php-ldap_2%3a8.2+93_all.deb ...  
Dépaquetage de php-ldap (2:8.2+93) ...  
Paramétrage de php8.2-ldap (8.2.18-1~deb12u1) ...  
  
Creating config file /etc/php/8.2/mods-available/ldap.ini with new version  
Paramétrage de php-ldap (2:8.2+93) ...  
Traitement des actions différées (« triggers ») pour libapache2-mod-php8.2 (8.2.18-1~deb12u1) ...  
Traitement des actions différées (« triggers ») pour php8.2-cli (8.2.18-1~deb12u1) ...  
root@debian:/home/baptiste# sudo mysql_secure_installation  
  
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB  
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!  
  
In order to log into MariaDB to secure it, we'll need the current  
password for the root user. If you've just installed MariaDB, and  
haven't set the root password yet, you should just press enter here.  
  
Enter current password for root (enter for none): 
```

14) Une liste de questions vous sera demandez, ci-dessous, la liste des réponses à insérez.

```

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] n
... skipping.

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!

```

Ensuite, créez une base de données dédiée pour GLPI, accessible via un utilisateur spécifique. Il est essentiel de ne pas utiliser le compte root de MariaDB : une base de données correspond à un utilisateur distinct.

Connectez-vous à votre instance MariaDB, à l'aide de cette commande :

root@debian:/home/baptiste# **sudo mysql -u root -p** , press ENTER.

Saisissez le mot de passe défini à l'étape précédente.

Ensuite, exécutez les requêtes SQL suivantes pour créer la base de données "db23_glpi" et l'utilisateur "glpi_adm" avec un mot de passe provisoire. Assurez-vous de changer ce mot de passe. Cet utilisateur disposera de tous les droits sur cette base de données uniquement.

COMMANDE à insérer :

CREATE DATABASE db23_glpi;

GRANT ALL PRIVILEGES ON db23_glpi.* TO glpi_adm@localhost IDENTIFIED BY "MotDePasse";

FLUSH PRIVILEGES;

SANS OUBLIER LE « EXIT » PRESS ENTER DE FIN.



```
baptiste@debian: ~  
Thanks for using MariaDB!  
root@debian:/home/baptiste# sudo mysql -u root -p  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 39  
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12  
  
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 db23_glpi;  
Query OK, 1 row affected (0,000 sec)  
  
MariaDB [(none)]> GRANT ALL PRIVILEGES ON db23_glpi.* TO glpi_adm@localhost IDENTIFIED BY "MotDePasse";  
Query OK, 0 rows affected (0,001 sec)  
  
MariaDB [(none)]> FLUSH PRIVILEGES;  
Query OK, 0 rows affected (0,001 sec)  
  
MariaDB [(none)]> EXIT  
Bye  
root@debian:/home/baptiste#
```

La base de données prête.

Télécharger GLPI et préparer son installation

La prochaine étape est de télécharger l'archive ".tgz" contenant les sources d'installation de GLPI. Récupérez le lien vers la dernière version depuis le GitHub de GLPI. Actuellement, c'est la version GLPI 10.0.10 qui est installée.

- 15) L'archive sera téléchargée dans le répertoire "/tmp" en insérant « cd /tmp », press ENTER.

```
root@debian:/home/baptiste# cd /tmp
```

16) Insérez la commande ci-dessous, press ENTER.

```
root@debian:/tmp# wget https://github.com/glpi-project/glpi/releases/download/10.0.10/glpi-10.0.10.tgz
```

17) Ensuite, exécutez la commande ci-dessous pour décompresser l'archive .tgz dans le répertoire "/var/www/", créant ainsi le chemin d'accès "/var/www/glpi" pour GLPI, à l'aide de la commande ci-dessous. `sudo tar -xzf glpi-10.0.10.tgz -C /var/www/`

```
root@debian:/tmp# sudo tar -xzf glpi-10.0.10.tgz -C /var/www/
```

18) Définissez l'utilisateur "www-data", qui correspond à Apache2, comme propriétaire des fichiers GLPI.

REVENIR AU TERMINAL INITIAL, à l'aide de la commande ci-dessous, press ENTER.

```
root@debian:/tmp# cd /home/baptiste
root@debian:/home/baptiste#
```

Insérez ensuite cette commande, press ENTER.

```
root@debian:/home/baptiste# sudo chown www-data /var/www/glpi/ -R
```

19) Ensuite, créez plusieurs dossiers pour déplacer certaines données hors de la racine Web (/var/www/glpi). Cette organisation contribue à une installation sécurisée de GLPI, conforme aux recommandations de l'éditeur.

Le répertoire /etc/glpi*

Commencez par créer le répertoire "/etc/glpi" pour y stocker les fichiers de configuration de GLPI. Attribuez les autorisations nécessaires à l'utilisateur "www-data" pour qu'il puisse y accéder, à l'aide des commandes ci-dessous.

```
root@debian:/home/baptiste# sudo mkdir /etc/glpi , press ENTER.
```

```
root@debian:/home/baptiste# sudo chown www-data /etc/glpi/ , press ENTER.
```

Ensuite, déplacez le répertoire "config" de GLPI vers le nouveau dossier "/etc/glpi", à l'aide de cette commande.

```
root@debian:/home/baptiste# sudo mv /var/www/glpi/config /etc/glpi , press ENTER.
```

Le répertoire /var/lib/glpi

Répétez cette opération en créant le répertoire "/var/lib/glpi", à l'aide des commandes ci-dessous, press ENTER.

```
root@debian:/home/baptiste# sudo mkdir /var/lib/glpi
root@debian:/home/baptiste# sudo chown www-data /var/lib/glpi/
```

Dans ce nouveau répertoire "/var/lib/glpi", déplacez également le dossier "files", qui contient la majorité des fichiers de GLPI, tels que les CSS, plugins, etc, à l'aide de la commande ci-dessous.

```
root@debian:/home/baptiste# sudo mv /var/www/glpi/files /var/lib/glpi
```

Le répertoire /var/log/glpi

Terminez en créant le répertoire "/var/log/glpi", destiné à stocker les journaux de GLPI, en suivant le même principe, à l'aide des commandes ci-dessous, press ENTER.

```
root@debian:/home/baptiste# sudo mkdir /var/log/glpi
root@debian:/home/baptiste# sudo chown www-data /var/log/glpi
```

Rien à déplacer dans ce répertoire.

20) Créez les fichiers de configuration nécessaires.

Configurez GLPI pour qu'il reconnaisse les nouveaux répertoires créés comme emplacements de stockage des données.

Créez ce premier fichier de configuration, à l'aide de la commande ci-dessous.

```
|root@debian:/home/baptiste# sudo nano /var/www/glpi/inc/downstream.php
```

Ajoutez le contenu suivant qui spécifie le chemin vers le répertoire de configuration, à l'aide des commandes suivantes :

```
<?php
```

```
define('GLPI_CONFIG_DIR', '/etc/glpi/');
```

```
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {
```

```
require_once GLPI_CONFIG_DIR . '/local_define.php';
```

```
}
```



```
baptiste@debian: ~  
GNU nano 7.2 /var/www/glpi/inc/downstream.php *  
<?php  
define('GLPI_CONFIG_DIR', '/etc/glpi/');  
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {  
require_once GLPI_CONFIG_DIR . '/local_define.php';  
}
```

Une fois cela insérez, faite **CTRL+X MAJ O ENTER**

Créez ensuite ce second fichier de configuration, à l'aide de la commande ci-dessous :

root@debian:/home/baptiste# **sudo nano /etc/glpi/local_define.php** , press ENTER.

Ajoutez le contenu ci-dessous pour déclarer deux variables spécifiant les chemins vers les répertoires "files" et "log" préparés précédemment, à l'aide de la commande ci-dessous.

```
<?php
```

```
define('GLPI_VAR_DIR', '/var/lib/glpi/files');
```

```
define('GLPI_LOG_DIR', '/var/log/glpi'); CTRL+X MAJ O ENTER
```

Cette étape est terminée.

21) Préparer la configuration Apache2

Procédons à la configuration du serveur web Apache2. Créez un nouveau fichier de configuration pour établir le VirtualHost dédié à GLPI. Dans ce cas, nommez le fichier "configuration.glpi.conf", à l'aide de la commande suivante.

root@debian:/home/baptiste# **sudo nano /etc/apache2/sites-available/configuration.glpi.conf** , press ENTER.

Voici la configuration selon le modèle officiel de la documentation :

```
<VirtualHost *:80>
```

```
ServerName localhost
```

```
DocumentRoot /var/www/glpi/public
```



```
# If you want to place GLPI in a subfolder of your site (e.g. your virtual host is serving multiple
applications),

# you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT target the
GLPI directory itself.

# Alias "/glpi" "/var/www/glpi/public"

<Directory /var/www/glpi/public>

Require all granted

RewriteEngine On

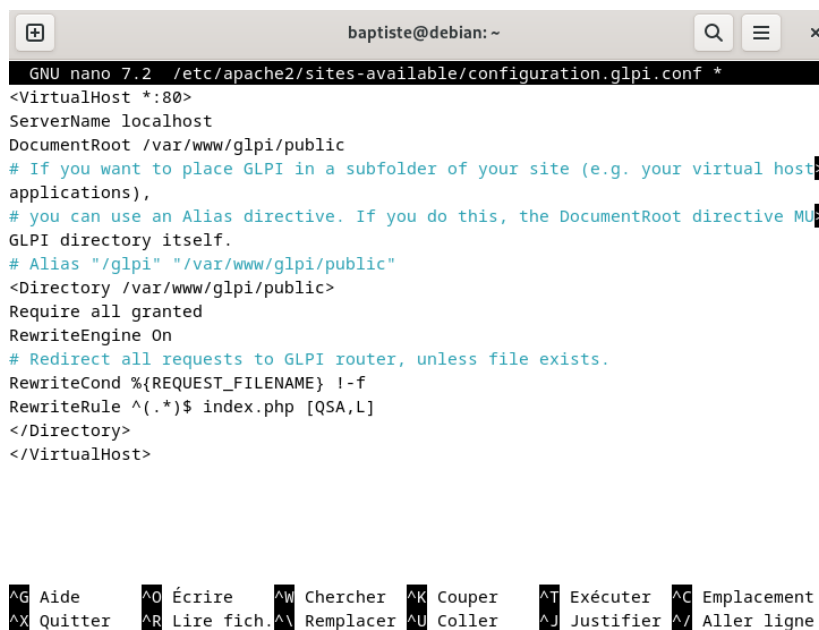
# Redirect all requests to GLPI router, unless file exists.

RewriteCond %{REQUEST_FILENAME} !-f

RewriteRule ^(.*)$ index.php [QSA,L]

</Directory>

</VirtualHost>
```



```
GNU nano 7.2 /etc/apache2/sites-available/configuration.glpi.conf *
<VirtualHost *:80>
ServerName localhost
DocumentRoot /var/www/glpi/public
# If you want to place GLPI in a subfolder of your site (e.g. your virtual host
applications),
# you can use an Alias directive. If you do this, the DocumentRoot directive MU
GLPI directory itself.
# Alias "/glpi" "/var/www/glpi/public"
<Directory /var/www/glpi/public>
Require all granted
RewriteEngine On
# Redirect all requests to GLPI router, unless file exists.
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(.*)$ index.php [QSA,L]
</Directory>
</VirtualHost>
```

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

Une fois cela insérez, **CTRL+X MAJ O ENTER**.

Activez ce nouveau site dans Apache2, à l'aide de la commande ci-dessous.

```
root@debian:/home/baptiste# sudo a2ensite configuration.glpi.conf, press ENTER.
```

Désactivez également le site par défaut d'Apache2, car il n'est pas nécessaire, à l'aide de la commande ci-dessous.

```
root@debian:/home/baptiste# sudo a2dissite 000-default.conf
```

Activez également le module "rewrite" d'Apache2, utilisé pour les règles de réécriture (RewriteCond / RewriteRule) dans le fichier de configuration du VirtualHost, à l'aide de la commande suivante.

```
root@debian:/home/baptiste# sudo a2enmod rewrite
```

Il ne reste plus qu'à redémarrer le service Apache2 pour appliquer les modifications, à l'aide de la commande ci-dessous.

```
root@debian:/home/baptiste# sudo systemctl restart apache2
```

22) Utilisation de PHP8.2-FPM avec Apache2

Pour utiliser PHP avec Apache2, optez pour PHP-FPM pour plus de performances, car il fonctionne comme un service indépendant, contrairement à libapache2-mod-php8.2 où chaque processus Apache exécute son propre moteur PHP. Si vous choisissez PHP-FPM, suivez les instructions ci-dessous ; sinon, passez à la suite en configurant "session.cookie_httponly". Commencez par installer PHP8.2-FPM avec la commande suivante :

```
root@debian:/home/baptiste# sudo apt-get install php8.2-fpm
```

Activez deux modules dans Apache et configurez PHP-FPM, puis rechargez Apache2, à l'aide de ces différentes commandes ci-dessous.

```
root@debian:/home/baptiste# sudo a2enmod proxy_fcgi setenvif
```

, press ENTER.

```
root@debian:/home/baptiste# sudo a2enconf php8.2-fpm
```

, press ENTER.

```
root@debian:/home/baptiste# >sudo systemctl reload apache2
```

, press ENTER.

Pour configurer PHP-FPM pour Apache2, modifiez non pas le fichier "/etc/php/8.2/apache2/php.ini", mais plutôt ce fichier spécifique :

```
root@debian:/home/baptiste# sudo nano /etc/php/8.2/fpm/php.ini
```

, press ENTER.

La page ci-dessous s'ouvrira, faite CTRL+W afin de faire une recherche, Dans ce fichier, chercher l'option "session.cookie_httponly" en définissant la valeur "on" pour activer cette fonctionnalité et ainsi renforcer la protection des cookies de GLPI.

```
baptiste@debian: ~
GNU nano 7.2 /etc/php/8.2/fpm/php.ini *
7[[PHP]

;;;;;;;;;;;;;;;;
; About php.ini  ;
;;;;;;;;;;;;;;;;
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.

; PHP attempts to find and load this configuration from a number of locations.
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable.
; 3. A number of predefined registry keys on Windows
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path compile time option, or the
; Windows directory (usually C:\windows)
; See the PHP docs for more specific information.
; https://php.net/configuration.file

[ Lecture de 1974 lignes ]
^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^J Coller    ^_ Justifier ^_ Aller ligne
```

Rechercher : session.cookie_httponly, press ENTER.

Rajouter « on » à droit du = de session.cookie_httponly

```
|session.cookie_httponly = on|
```

CTRL+X MAJ O ENTER.

Enregistrez le fichier une fois la modification effectuée. À l'avenir, vous devrez peut-être apporter d'autres ajustements, comme augmenter la limite de taille des fichiers téléchargeables sur GLPI.

Pour appliquer les modifications, redémarrez le service PHP-FPM, à l'aide de cette commande.

```
root@debian:/home/baptiste# sudo systemctl restart php8.2-fpm.service
```

Pour terminer, modifiez votre VirtualHost pour indiquer à Apache2 d'utiliser PHP-FPM pour le traitement des fichiers PHP, à l'aide de cette commande.

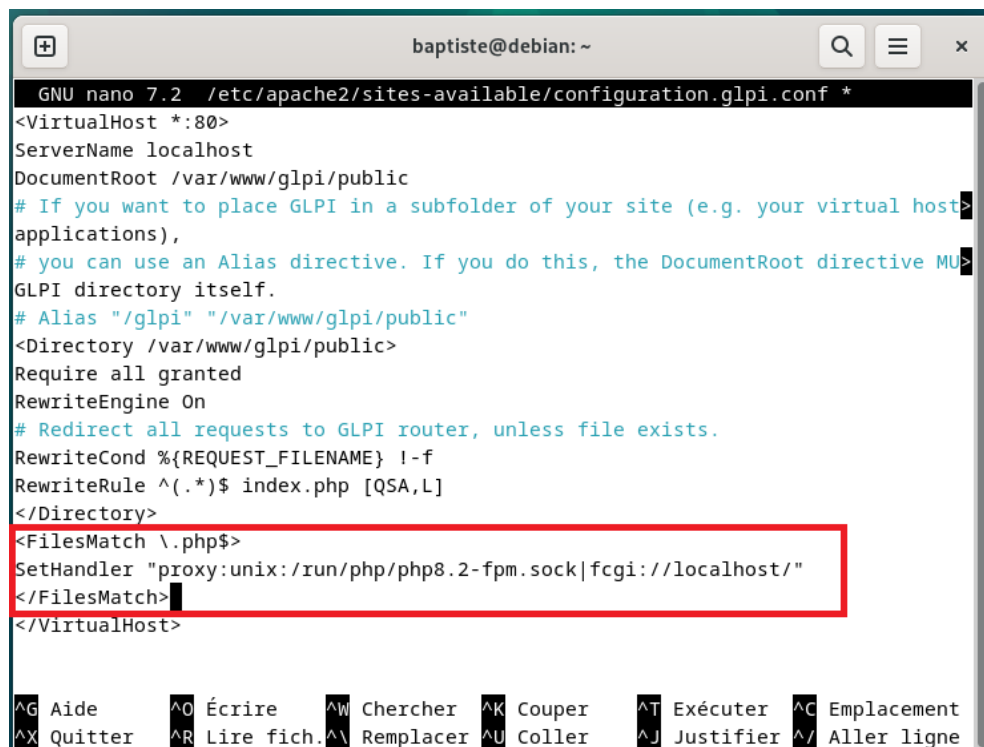
```
root@debian:/home/baptiste# sudo nano /etc/apache2/sites-available/configuration  
glpi.conf  
press ENTER.
```

Finalisez en modifiant votre VirtualHost pour spécifier à Apache2 d'utiliser PHP-FPM pour les fichiers PHP, en insérant la commande ci-dessous au bon endroit comme sur la capture.

```
<FilesMatch \.php$>
```

```
SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"
```

```
</FilesMatch>
```



```
GNU nano 7.2 /etc/apache2/sites-available/configuration.glpi.conf *
<VirtualHost *:80>
ServerName localhost
DocumentRoot /var/www/glpi/public
# If you want to place GLPI in a subfolder of your site (e.g. your virtual host
applications),
# you can use an Alias directive. If you do this, the DocumentRoot directive MU
GLPI directory itself.
# Alias "/glpi" "/var/www/glpi/public"
<Directory /var/www/glpi/public>
Require all granted
RewriteEngine On
# Redirect all requests to GLPI router, unless file exists.
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(.*)$ index.php [QSA,L]
</Directory>
<FilesMatch \.php$>
SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"
</FilesMatch>
</VirtualHost>
```

CTRL+X MAJ O ENTER, toujours pour sauvegarder.

Une fois cette modification effectuée, relancez le service Apache2, à l'aide de cette commande.

```
root@debian:/home/baptiste# sudo systemctl restart apache2
```

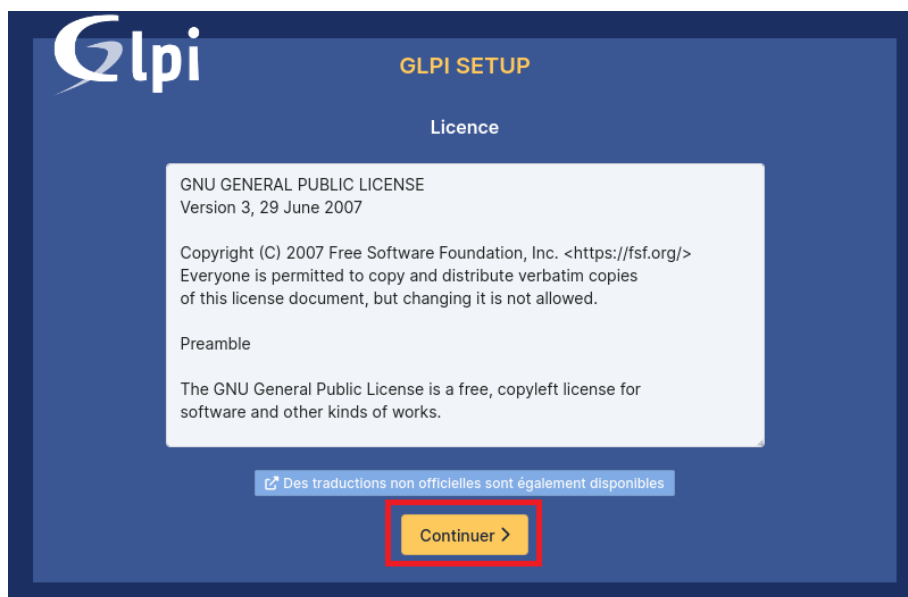
Création GLPI

Pour accéder à l'application hébergée localement, ouvrez votre navigateur et entrez localhost dans la barre d'adresse. Si cela ne fonctionne pas, ouvrez un terminal et exécutez la commande suivante pour activer les modules nécessaires : `sudo a2enmod proxy_fcgi setenvif`. Ensuite, redémarrez Apache pour appliquer les changements.

Si vous avez correctement suivi toutes les étapes, vous devriez voir apparaître une page vous invitant à choisir la langue. Sélectionnez la langue souhaitée pour continuer.



Puisque c'est une nouvelle installation, cliquez sur "Continuer" pour démarrer le processus.



Cliquez sur « Installer »



Étape importante : GLPI vérifie la configuration du serveur pour s'assurer que tous les prérequis sont respectés. Si tout est conforme, vous pouvez continuer, comme ci-dessous.



À l'étape suivante, saisissez les informations nécessaires pour vous connecter à la base de données. Utilisez "localhost" pour le serveur SQL, car MariaDB est installé localement sur le

même serveur que GLPI. Ensuite, entrez le nom d'utilisateur "glpi_adm" et le mot de passe associé.



The screenshot shows the 'GLPI SETUP' interface for 'Étape 1'. The title is 'Configuration de la connexion à la base de données'. It contains three input fields: 'Serveur SQL (MariaDB ou MySQL)' with the value 'localhost', 'Utilisateur SQL' with the value 'glpi_adm', and 'Mot de passe SQL' which is masked with dots. A red rectangle highlights the 'Continuer >' button at the bottom left.

Après avoir cliqué sur "Continuer", sélectionnez la base de données "db23_glpi" que vous avez créée précédemment.

Poursuivez.... En cochant db23_glpi puis « Continuer »



The screenshot shows the 'GLPI SETUP' interface for 'Étape 2'. The title is 'Test de connexion à la base de données'. A green checkmark and the text 'Connexion à la base de données réussie' are displayed. Below, under the heading 'Veuillez sélectionner une base de données :', there is a section 'Créer une nouvelle base ou utiliser une base existante :'. This section contains a radio button (selected), an empty text input field, and a list item 'db23_glpi' which is marked with a red 'X' and is selected. A 'Continuer >' button is at the bottom.



Décochez la case, puis « Continuer »



Cliquez sur « Continuer »





Félicitations, vous avez réussi à installer GLPI ! Comme indiqué à la dernière étape, le compte administrateur par défaut est "glpi" pour l'utilisateur et "glpi" pour le mot de passe.

Connectez-vous en utilisant le compte "glpi" avec le mot de passe "glpi".

Connexion à votre compte

Identifiant

Mot de passe

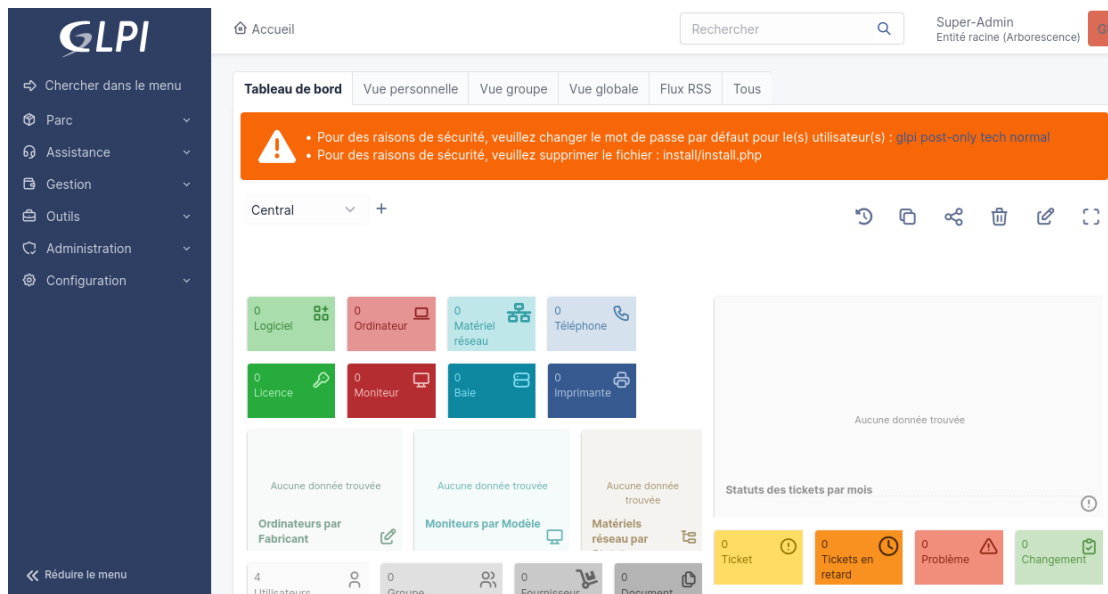
Source de connexion

Base interne GLPI ▼

☒ Se souvenir de moi

Se connecter

Bienvenue sur votre nouveau serveur GLPI !



Bienvenue sur votre nouveau serveur GLPI ! Voici quelques étapes finales pour sécuriser votre installation :

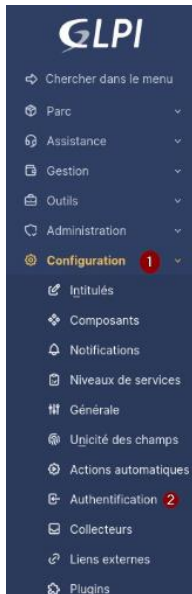
- Changez les mots de passe des comptes par défaut.
- Supprimez le fichier "install.php" avec la commande :
- `sudo rm /var/www/glpi/install/install.php`.

Votre GLPI est maintenant prêt à être utilisé et personnalisé.

Procédure Liaison AD + GLPI

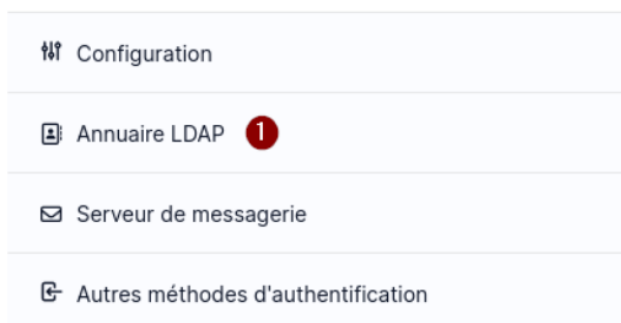
Configuration de l'annuaire Active Directory dans GLPI

Depuis le menu de navigation aller sur Configuration (1) > Authentifications (2).



Dans la liste des authentifications externes, cliquez sur "Annuaire LDAP (1)".

Authentifications externes



Cliquer sur le « + » pour ajouter un annuaire.



Cliquez sur "Active Directory" pour pré-remplir automatiquement les champs nécessaires.

The screenshot shows the 'Nouvel élément - Annuaire LDAP' form. The 'Active Directory' tab is selected and highlighted with a red box. The form contains the following fields:

- Nom:
- Serveur par défaut: Actif:
- Serveur: Port (par défaut 389):
- Filtre de connexion:
- BaseDN:
- Utiliser bind:
- DN du compte (pour les connexions non anonymes):
- Mot de passe du compte (pour les connexions non anonymes):
- Champ de l'identifiant: Commentaires:
- Champ de synchronisation:

A yellow button labeled '+ Ajouter' is located at the bottom right.

Configurer l'Active Directory :

- 1 Entrer un nom
- 2 Mettre cet annuaire par défaut
- 3 Rendre le serveur Actif
- 4 Entrer l'IP de votre contrôleur de domaine
- 5 Saisir la BaseDN de votre domaine
- 6 Identifiant et mot de passe d'un compte autorisé à se connecter
- 7 Cliquer sur Ajouter.

The screenshot shows the 'Nouvel élément - Annuaire LDAP' form with the 'Active Directory' tab selected. The form is pre-filled with the following values:

- Nom:
- Serveur par défaut: Actif:
- Serveur: Port (par défaut 389):
- Filtre de connexion:
- BaseDN:
- Utiliser bind:
- DN du compte (pour les connexions non anonymes):
- Mot de passe du compte (pour les connexions non anonymes):
- Champ de l'identifiant: Commentaires:
- Champ de synchronisation:

A yellow button labeled '+ Ajouter' is located at the bottom right, highlighted with a red box.

Cliquer sur le serveur qui vient d'être ajouté.

<input type="checkbox"/>	NOM ^	SERVEUR	DERNIÈRE MODIFICATION	ACTIF
<input type="checkbox"/>	servbaptiste.local	192.168.174.138	2024-05-03 14:12	Oui

20

lignes / page

De 1 à 1 sur 1 lignes

L'onglet "Annuaire LDAP", vous retrouverez la configuration de l'annuaire que vous avez saisie précédemment.

Annuaire LDAP

Tester

Utilisateurs

Groupes

Informations avancées

Réplicats

Historique 1

Tous

Nom

servbaptiste.local

Dernière modification

2024-05-03 14:12

Serveur par défaut

Oui

Actif

Oui

Serveur

192.168.174.138

Port (par défaut 389)

389

Filtre de connexion

(&(objectClass=user)(objectCategory=person)!(userAccountControl:1.2.840.113556.1.4.803:=2)))

BaseDN

DC=servbaptiste,DC=local

Utiliser bind i

Oui

DN du compte (pour les connexions non anonymes)

Administrateur@servbaptiste.local

Mot de passe du compte (pour les connexions non anonymes)

••••••••••••••••

☐ Effacer

Champ de l'identifiant

userprincipalname

Commentaires

Champ de synchronisation i

objectguid

Supprimer définitivement

Sauvegarder

Allez à l'onglet "Tester (1)" et cliquez sur le bouton "Tester (2)". Si la configuration est correcte, vous devriez voir apparaître un message de confirmation (3).

Annuaire LDAP

Tester la connexion à l'annuaire LDAP

Tester 1

Utilisateurs

Groupes

Informations avancées

Réplicats

Historique 17

Tous

Test réussi : Serveur principal servesteban.local 3

Tester 2

Import des utilisateurs

Depuis le menu de navigation, allez sur "Administration (1)" puis cliquez sur "Utilisateurs (2)".



Pour le moment, seuls les utilisateurs par défaut sont présents. Cliquez sur le bouton "Liaison annuaire LDAP" pour procéder.



Depuis cette page, vous pouvez également synchroniser les utilisateurs déjà importés en cas de modification dans l'Active Directory. Cliquez sur "Importation de nouveaux utilisateurs (1)".

Import en masse d'utilisateurs depuis un annuaire LDAP

 Synchronisation des utilisateurs déjà importés

 Importation de nouveaux utilisateurs

1

Depuis ce formulaire, vous pouvez appliquer des filtres de recherche. Si vous souhaitez importer tous les utilisateurs, cliquez sur "Rechercher (1)".

Activer le filtrage par date

Critère de recherche pour les utilisateurs

Identifiant

Champ de synchronisation (objectguid)

Courriel

Nom de famille

Prénom

Téléphone

Rechercher1

Sous le formulaire s'affiche le résultat de recherche

Affichage (nombre d'éléments)	20	De 1 à 1 sur 1
Actions		
<input type="checkbox"/>	CHAMP DE SYNCHRONISATION	UTILISATEURS
<input type="checkbox"/>	655d0b23-c8c7-4ea7-b491-0abf0e1cf105	tetest1@servbat.local
<input type="checkbox"/>	Champ de synchronisation	Utilisateurs
Dernière mise à jour dans l'annuaire LDAP		
2024-05-03 14:24		
Dernière mise à jour dans l'annuaire LDAP		
Actions		
Affichage (nombre d'éléments)	20	De 1 à 1 sur 1

Cocher les utilisateurs(1) que vous souhaitez importer, puis cliquez sur le bouton "Actions(2)".

Actions		
<input type="checkbox"/> CHAMP DE SYNCHRONISATION	UTILISATEURS	DERNIÈRE MISE À JOUR DANS L'ANNUAIRE LDAP
<input checked="" type="checkbox"/> 655d0b23-c8c7-4ea7-b491-0abf0e1cf105	tetest1@servbat.local	2024-05-03 14:24
<input type="checkbox"/> Champ de synchronisation	Utilisateurs	Dernière mise à jour dans l'annuaire LDAP

Au niveau de l'action sélectionner « Importer » et cliquer sur « Envoyer ».

Actions

Action

Importer

Envoyer

**A présent votre utilisateur AD est importé dans votre système GLPI.
FIN.**