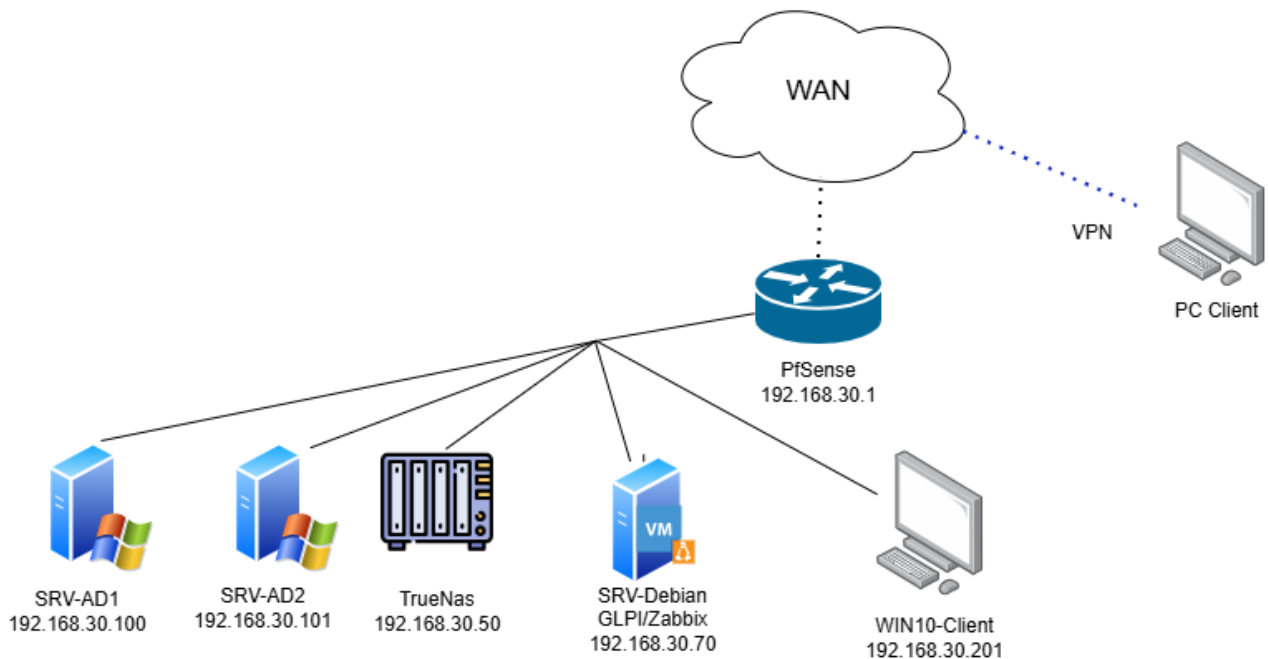


Documentation Technique : Projet 2

L'activité de **Lo-Tech** s'intensifie, l'infrastructure initiale doit évoluer pour garantir une continuité de service optimale. J'ai donc dû l'améliorer pour éviter les pannes, mieux surveiller les équipements et automatiser les tâches répétitives. Le but est de rendre l'informatique de l'entreprise plus fiable et plus sécurisée



Sommaire :

1 – Mise en Place d'une redondance sur l'Active Directory

- **Installation du système d'exploitation** : Déploiement de Windows Server 2022 et configuration initiale.
- **Configuration Post-Installation** : Paramétrage de l'IP fixe (192.168.30.101) et renommage du serveur en SRV-AD-2.
- **Installation du rôle AD/DS et Promotion du serveur** : Ajout des services de domaine et intégration au domaine *projet01.fr*.
- **Tests et diagnostics** : Vérification de la réplication DNS et santé du contrôleur via nslookup et dcdiag.

2– Mise en place d'un logiciel de supervision (Zabbix)

- **Installation de Debian 13** : Configuration de l'environnement hôte pour la solution de supervision.
- **Installation de Zabbix** : Configuration de MariaDB, installation du serveur Zabbix 7.0 et de l'interface Web.
- **Ajout de PfSense dans Zabbix** : Activation du service SNMP et création de l'hôte réseau.
- **Ajout du SRV1 et SRV2 dans Zabbix** : Déploiement des agents Windows sur les contrôleurs de domaine.
- **Ajouts terminaux** : Intégration du poste Windows client et du serveur TrueNAS.
- **État final des supervisions** : Vue récapitulative de la disponibilité des équipements.

3 – Mise en place DHCP

- **Configuration sur PfSense** : Activation du serveur DHCP sur l'interface LAN.
- **Paramétrage du pool** : Définition de la plage d'adresses (192.168.30.202 - .245) et des options DNS.
- **Test client** : Vérification de l'attribution automatique de l'IP sur un poste Windows.

4 – Mise en place d'un script

- **Présentation du script** : Structure PowerShell pour la création d'utilisateurs AD.
- **Mise en pratique** : Test de création d'un utilisateur "Tech test" et vérification dans l'annuaire.

5 – Mise en place de GLPI

- **Installation de l'environnement** : Mise à jour du système et configuration de la pile LAMP.
- **Configuration de l'application** : Installation des extensions PHP, sécurisation SQL et assistant Web.
- **Authentification LDAP** : Liaison avec l'Active Directory et gestion des tickets helpdesk.

6 – Mise en place d'un accès VPN

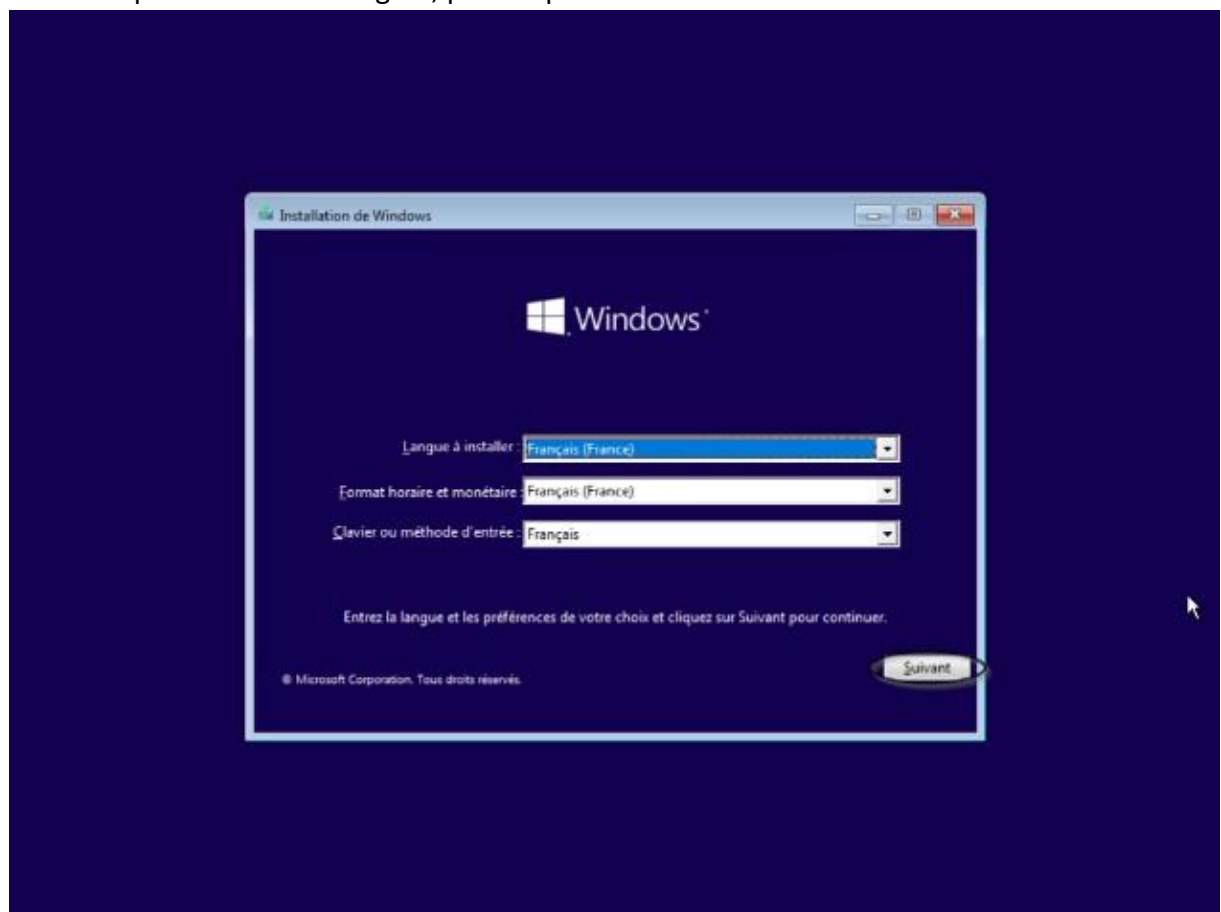
7 – Mise en place de sauvegardes

- **Extension du pool de stockage** : Redimensionnement des disques virtuels sur TrueNAS.
- **Création du Pool de sauvegardes** : Configuration d'un pool RAID 1 (Miroir) et partage SMB.
- **Sauvegarde du SRV-AD1** : Planification de la sauvegarde système Windows.
- **Sauvegarde du PfSense** : Exportation de la configuration au format XML.
- **Sauvegarde du Debian** : Automatisation via script pour les bases Zabbix et dossiers GLPI.

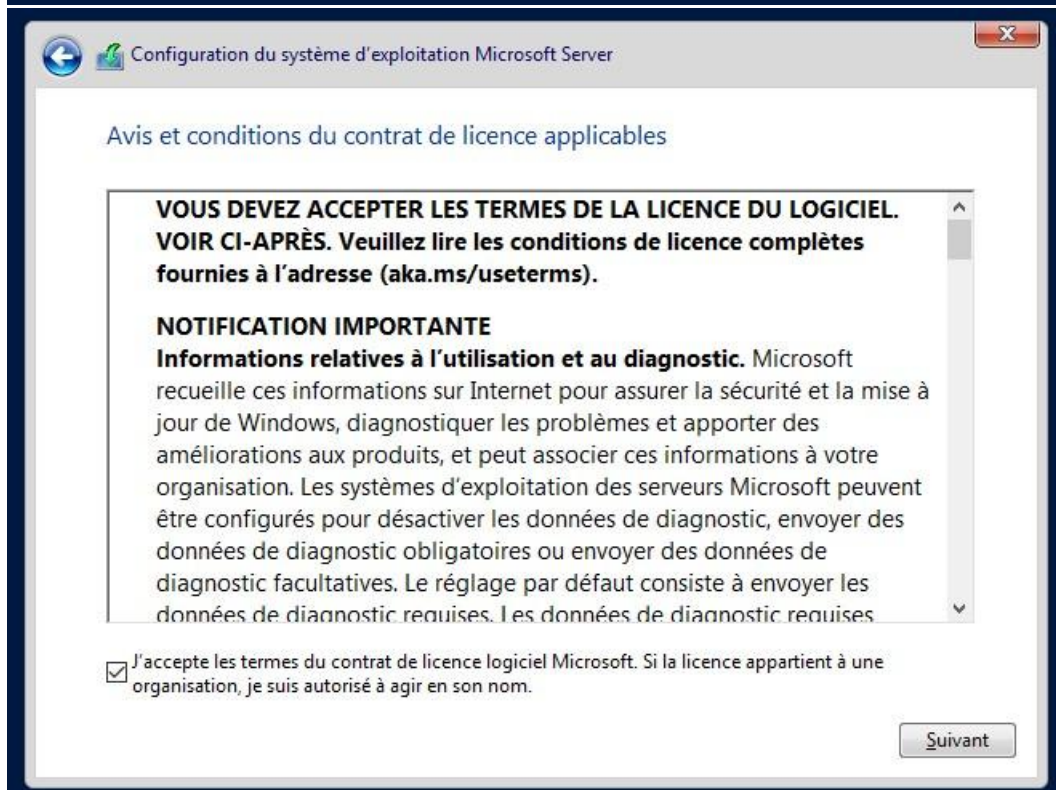
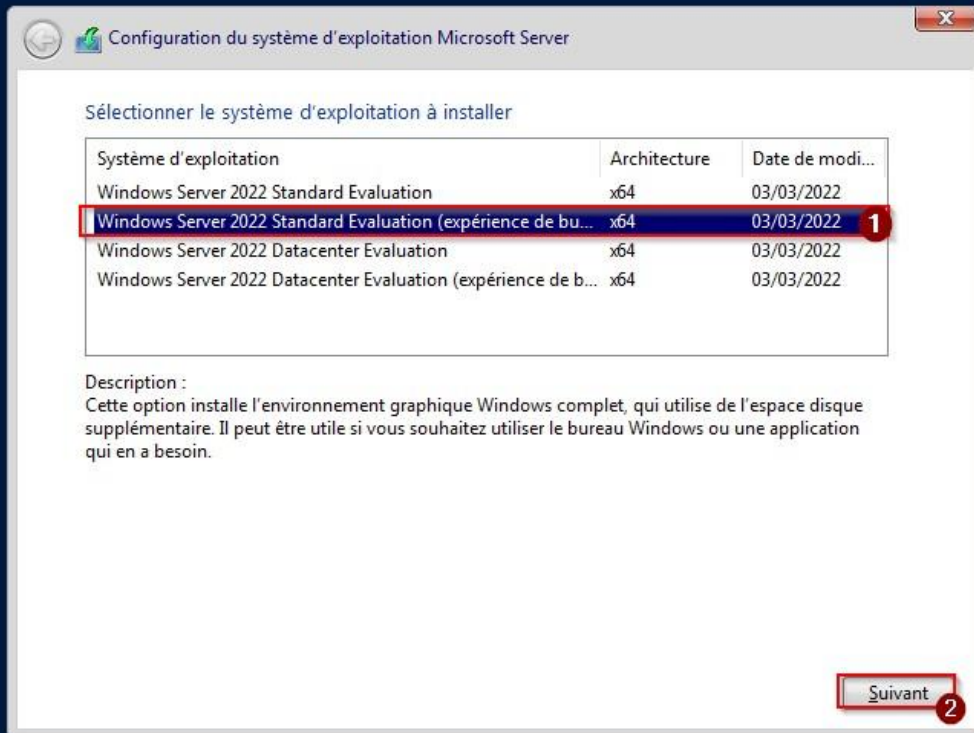
1 – Mise en Place d'une redondance sur l'Active Directory

1- Installation du système d'exploitation

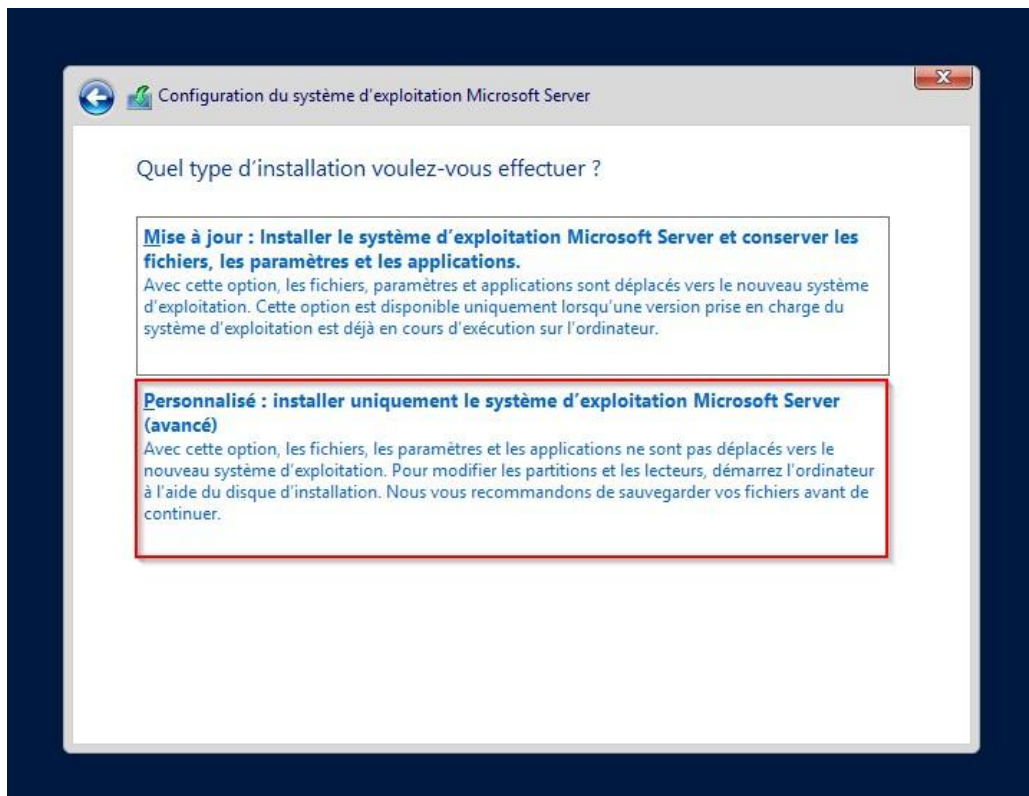
Tout d'abord, je vais installer un serveur Windows Server 2022. Nous avons la configuration initiale de l'assistant d'installation. Sélectionnez la langue "Français", le format horaire et le clavier correspondant à votre région, puis cliquez sur **Suivant**



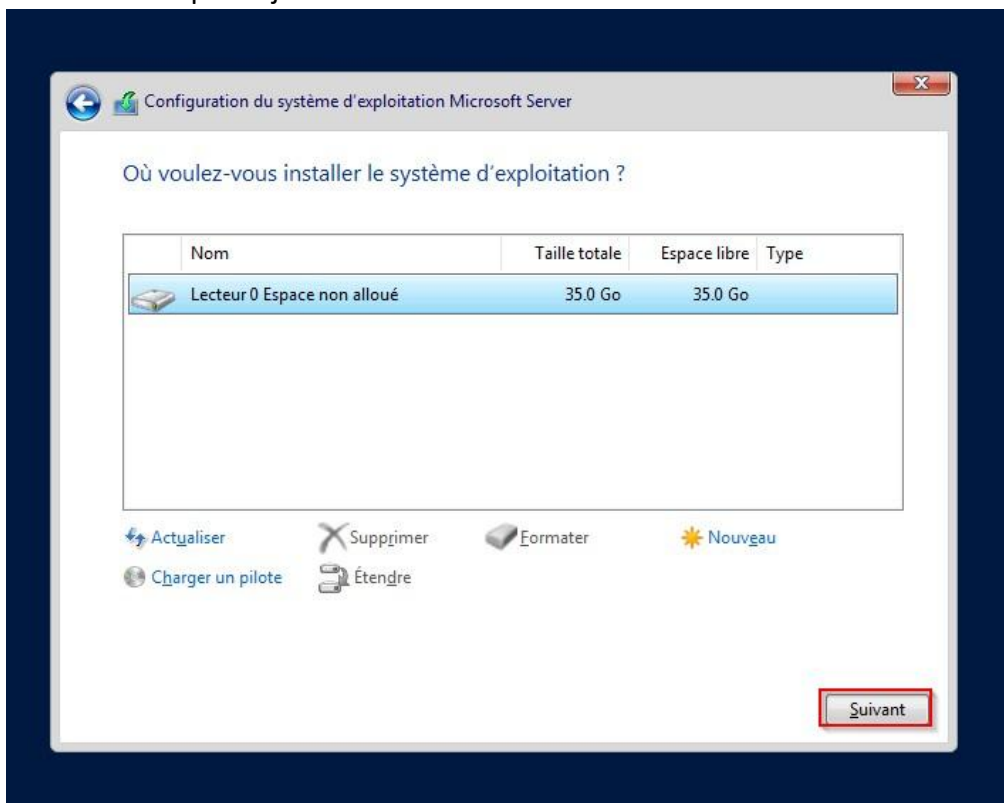
Je clique sur "Installer maintenant", et je choisis la version avec interface graphique et j'accepte les termes du contrat de licence.



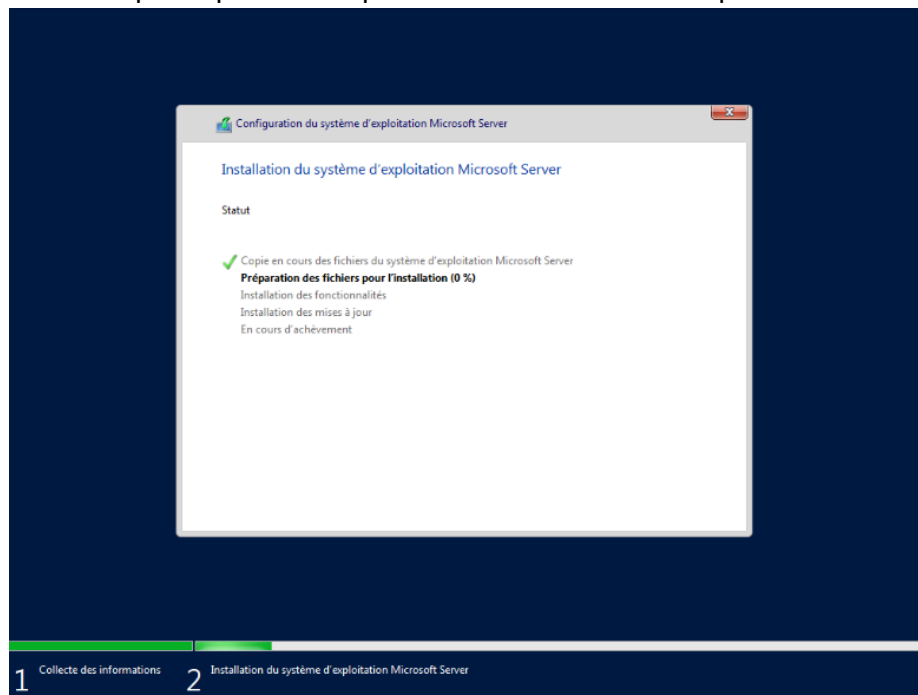
Je suis les étapes de l'assistant pour valider les conditions de licence et choisi le type d'installation "**Personnalisé**".



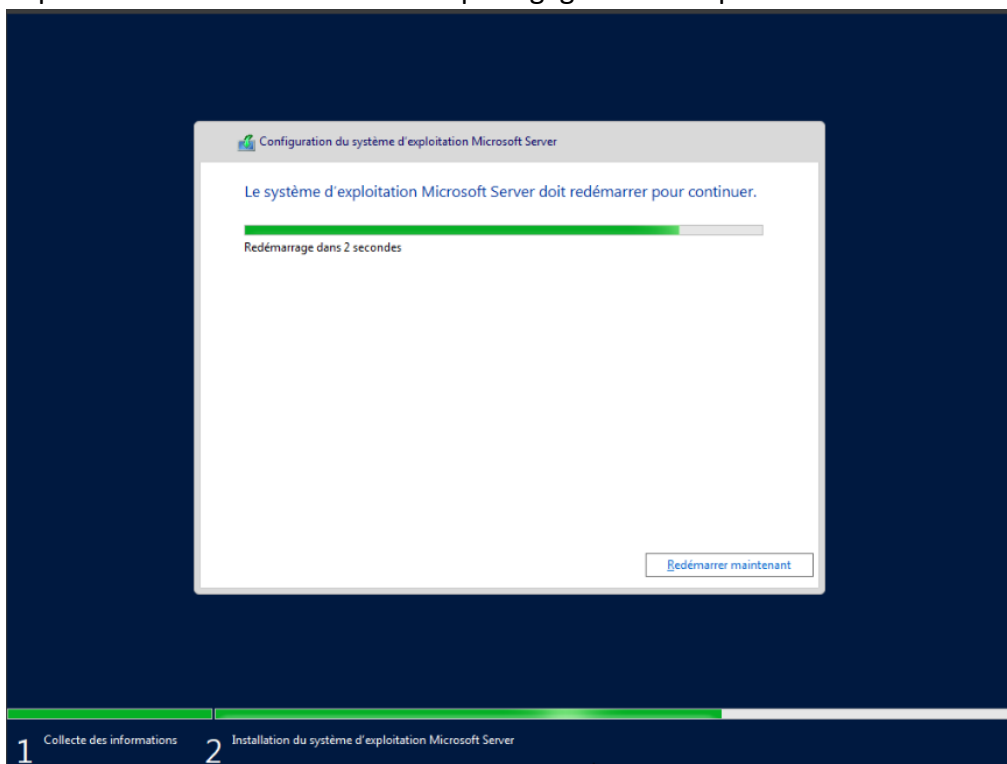
Je choisi le disque et je fais suivant.



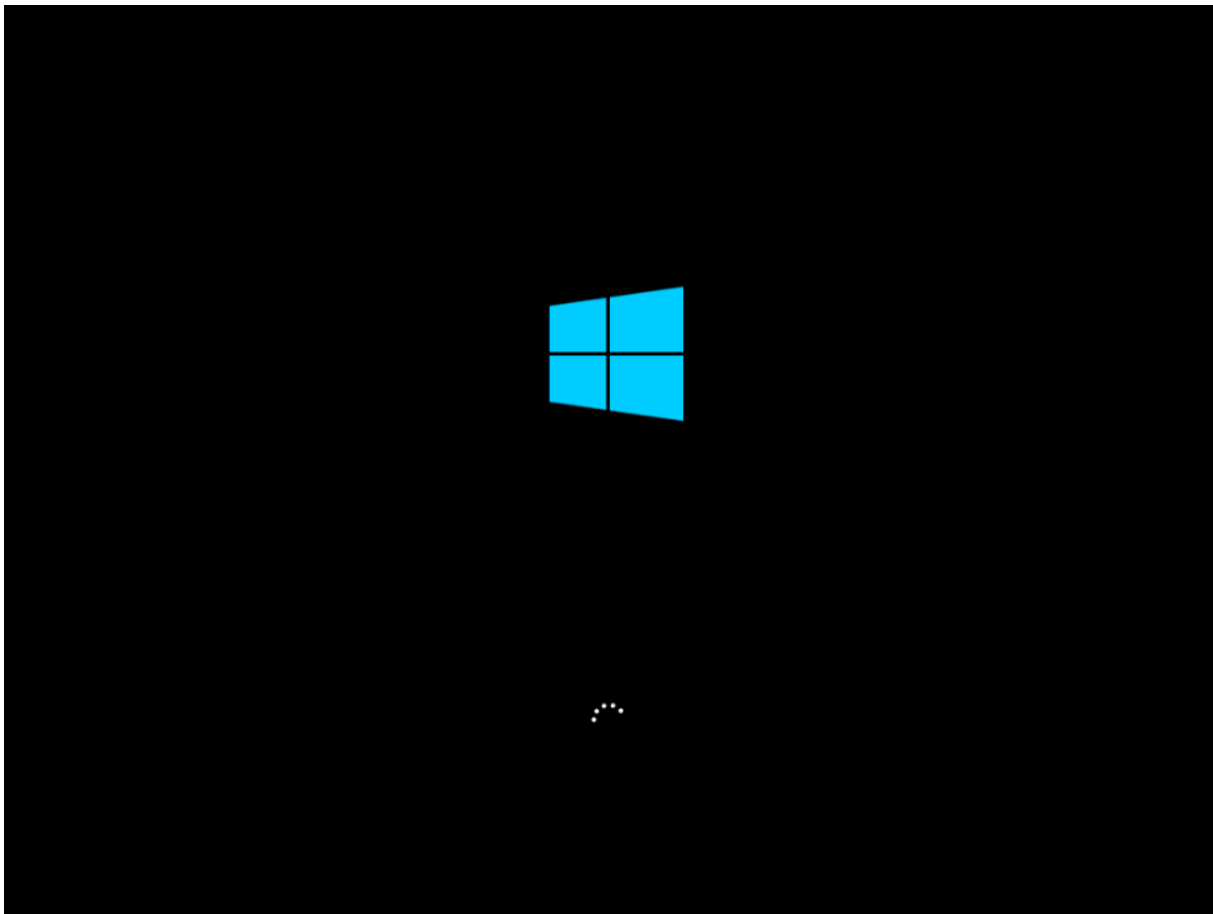
Le processus d'installation copie les fichiers système et prépare les composants. Cette étape est automatique et peut durer plusieurs minutes selon les performances du matériel.



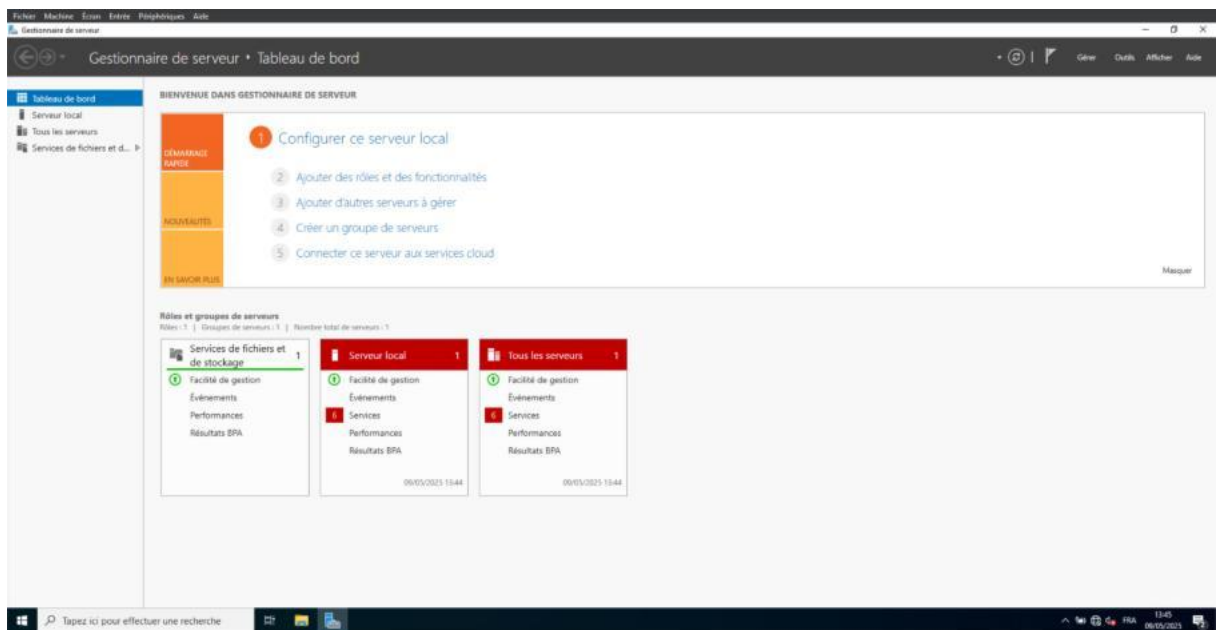
Une fois les fichiers installés, le système doit redémarrer pour finaliser la configuration. Je clique sur **Redémarrer maintenant** pour gagner du temps



Premier démarrage du serveur. Le système prépare les services et charge l'interface de gestion initiale.

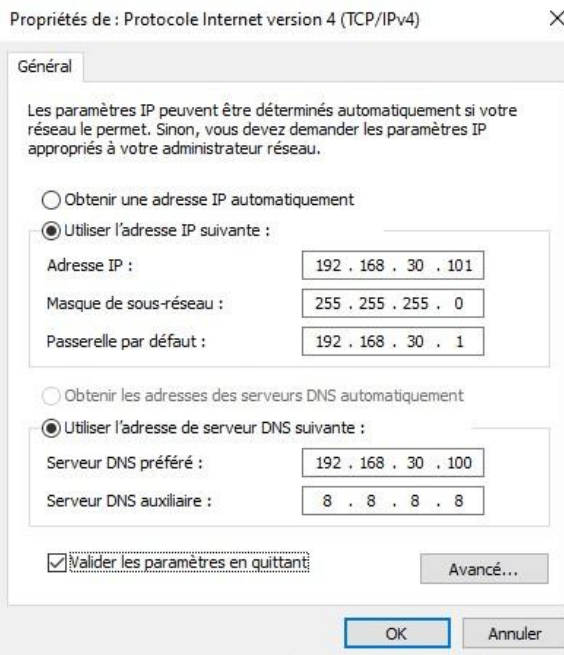
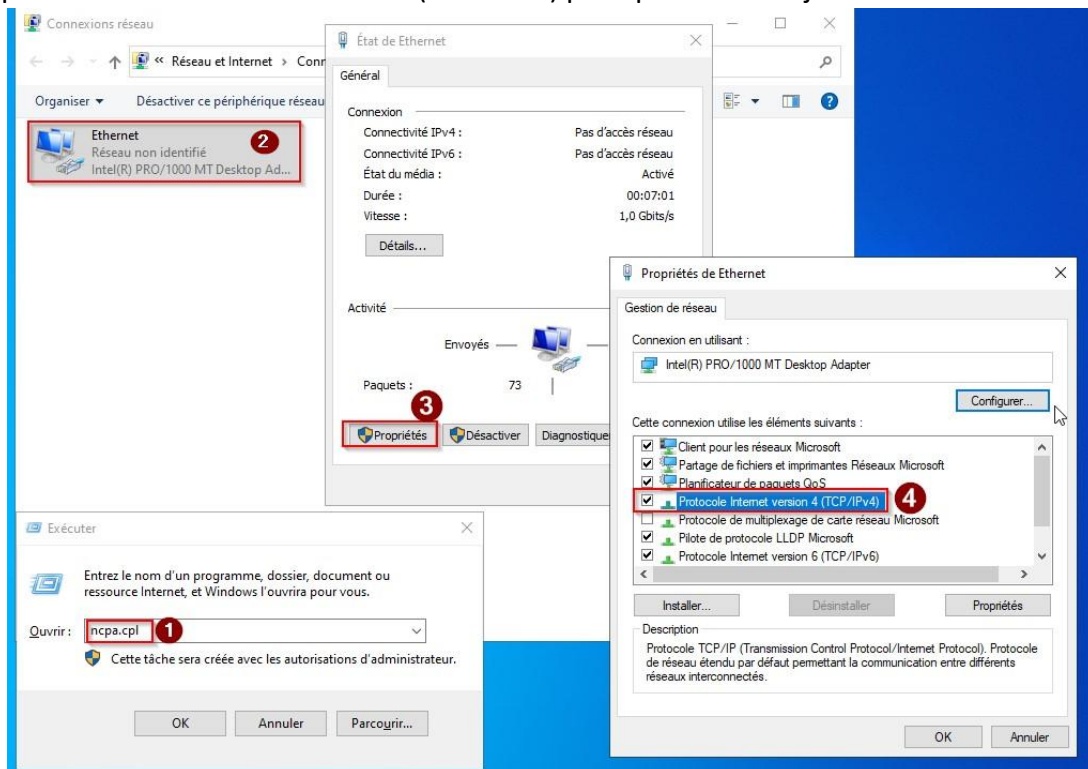


Arrivée sur le Bureau et ouverture automatique du **Gestionnaire de serveur**



2. Configuration Post-Installation

Je configure une adresse IP fixe. Le DNS préféré doit pointer vers l'adresse IP de mon premier contrôleur de domaine (SRV-AD-1) pour permettre la jonction au domaine.



Icône réseau confirmant que le serveur est bien connecté

Sur le SRV-AD-1 :

Serveur DNS auxiliaire : 192.168.30.101

Dans le Gestionnaire de serveur, je modifie le nom de l'ordinateur pour le renommer en SRV-AD-2. Un redémarrage sera nécessaire.

Renommer votre PC

Renommer votre PC

Vous pouvez utiliser une combinaison de lettres, de traits d'union et de chiffres.

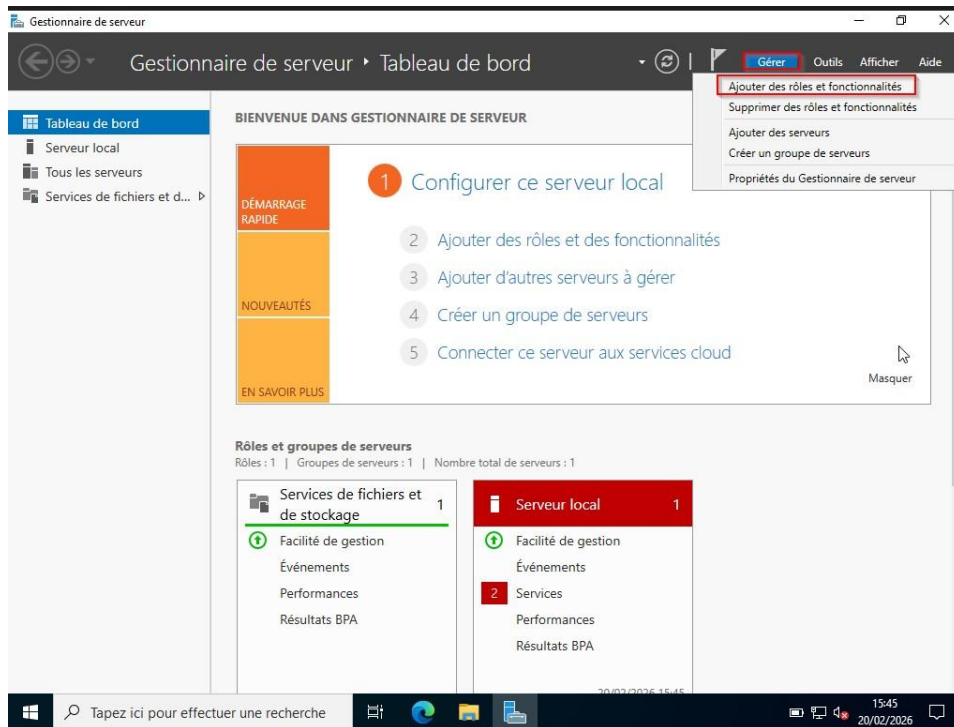
Nom actuel du PC : WIN-NGNLV3V2RAP

Suivant

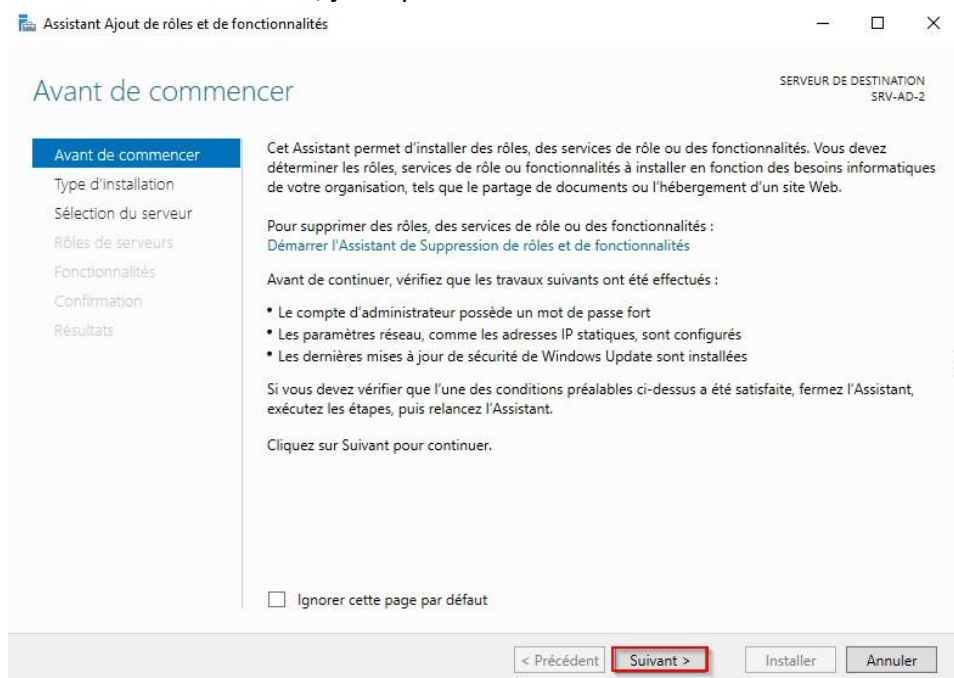
Annuler

3. Installation du rôle AD/DS et Promotion du serveur

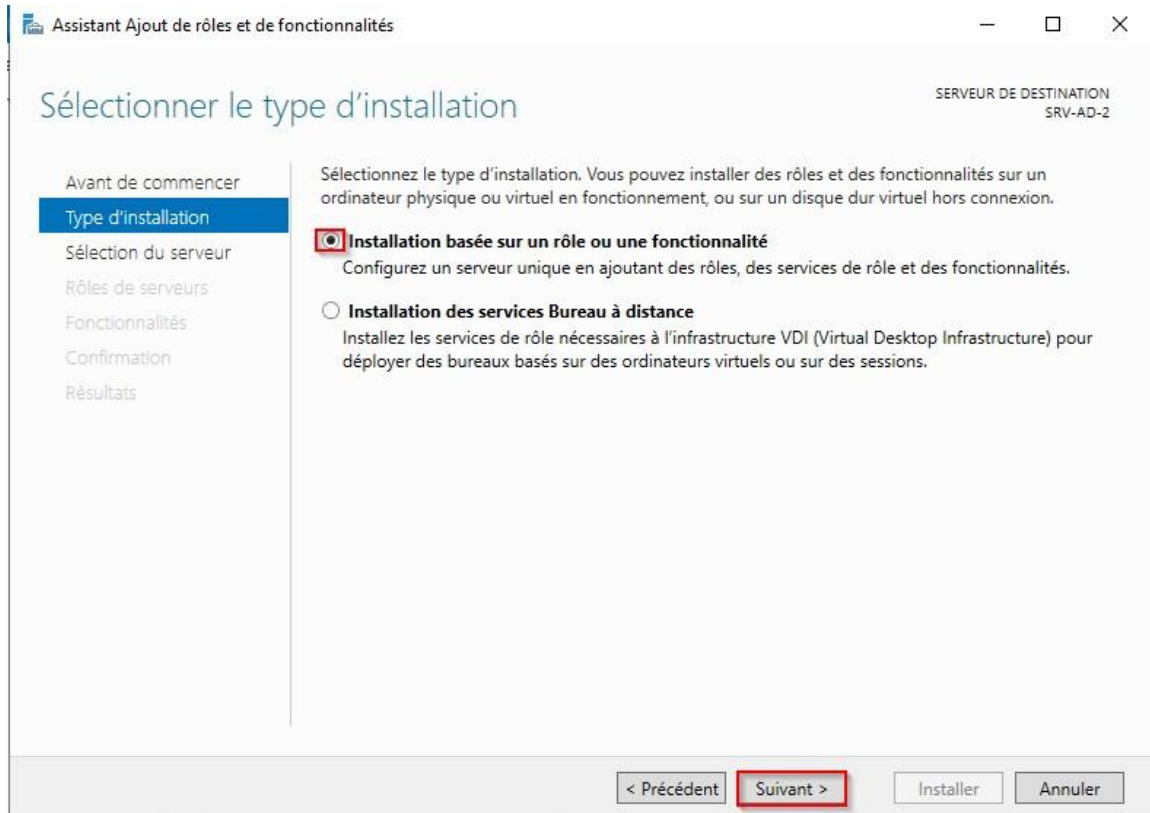
Sur **SRV-AD-2**, j'ajoute le rôle "Services AD DS" via l'assistant d'ajout de rôles et fonctionnalités.



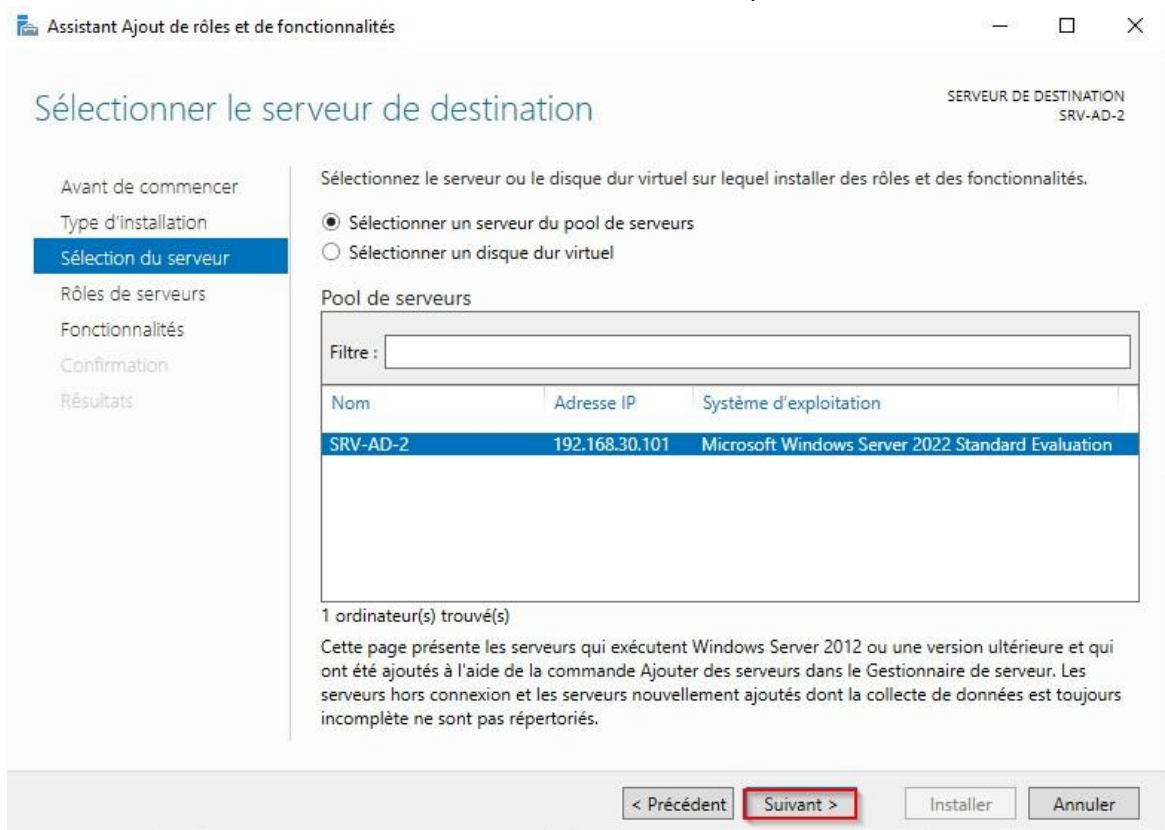
Écran d'accueil de l'assistant, je clique sur **Suivant**.



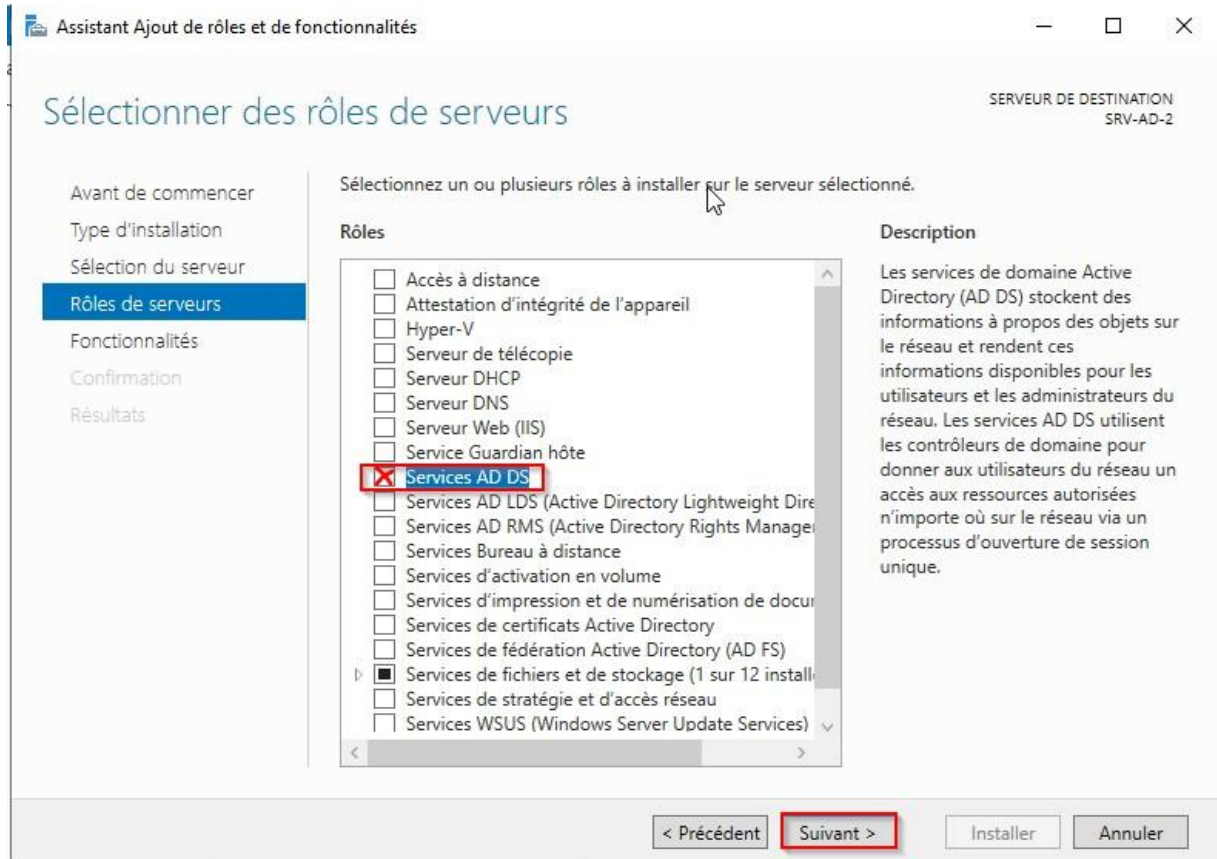
Je sélectionne le type d'installation : **Installation basée sur un rôle ou une fonctionnalité.**



Confirmation de la sélection du serveur **SRV-AD-2** dans le pool.



Je coche la case **Services AD DS** (Active Directory Domain Services).



Une fenêtre s'ouvre pour valider l'ajout des outils d'administration requis ; je clique sur **Ajouter des fonctionnalités**.



Écran des fonctionnalités supplémentaires, je passe par **Suivant**.

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES FONCTIONNALITÉS

SERVEUR DE DESTINATION
SRV-AD-2

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

Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités	Description
<input checked="" type="checkbox"/> .NET Framework 4.8 Features (2 sur 7 installé(s))	.NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.
<input checked="" type="checkbox"/> Antivirus Microsoft Defender (Installé)	
<input type="checkbox"/> Assistance à distance	
<input type="checkbox"/> Base de données interne Windows	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Chiffrement de lecteur BitLocker	
<input type="checkbox"/> Client d'impression Internet	
<input type="checkbox"/> Client pour NFS	
<input type="checkbox"/> Client Telnet	
<input type="checkbox"/> Client TFTP	
<input type="checkbox"/> Clustering de basculement	
<input type="checkbox"/> Collection des événements de configuration et de	
<input type="checkbox"/> Compression différentielle à distance	
<input type="checkbox"/> Conteneurs	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Déverrouillage réseau BitLocker	
<input type="checkbox"/> DirectPlay	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Équilibrage de la charge réseau	

< Précédent **Suivant >** Installer Annuler

Résumé informatif sur le rôle AD DS, je clique sur **Suivant**.

Assistant Ajout de rôles et de fonctionnalités

SERVICES DE DOMAINE ACTIVE DIRECTORY


SERVEUR DE DESTINATION
SRV-AD-2

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

Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations de façon sécurisée et facilitent le partage des ressources et la collaboration entre les utilisateurs.

À noter :

- Pour veiller à ce que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine par domaine.
- Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installé, vous serez invité à installer le rôle de serveur DNS sur cet ordinateur.

 Azure Active Directory, un service en ligne distinct, peut fournir une gestion simplifiée des identités et des accès, des rapports de sécurité et une authentification unique aux applications web dans le cloud et sur site.
[En savoir plus sur Azure Active Directory](#)
[Configurer Office 365 avec Azure Active Directory Connect](#)

< Précédent **Suivant >** Installer Annuler

Confirmation de l'installation, je clique sur **Installer**.

Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION
SRV-AD-2

Confirmer les sélections d'installation

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

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

- 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
 - Centre d'administration Active Directory
 - Composants logiciels enfichables et outils en ligne de commande AD DS
- Services AD DS

[Exporter les paramètres de configuration](#)
[Spécifier un autre chemin d'accès source](#)

< Précédent Suivant > **Installer** Annuler

Une fois l'installation finie, je clique sur le lien bleu **Promouvoir ce serveur en contrôleur de domaine**.

Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION
SRV-AD-2

Progression de l'installation

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

Afficher la progression de l'installation

i Installation de fonctionnalité

Configuration requise. Installation réussie sur SRV-AD-2.

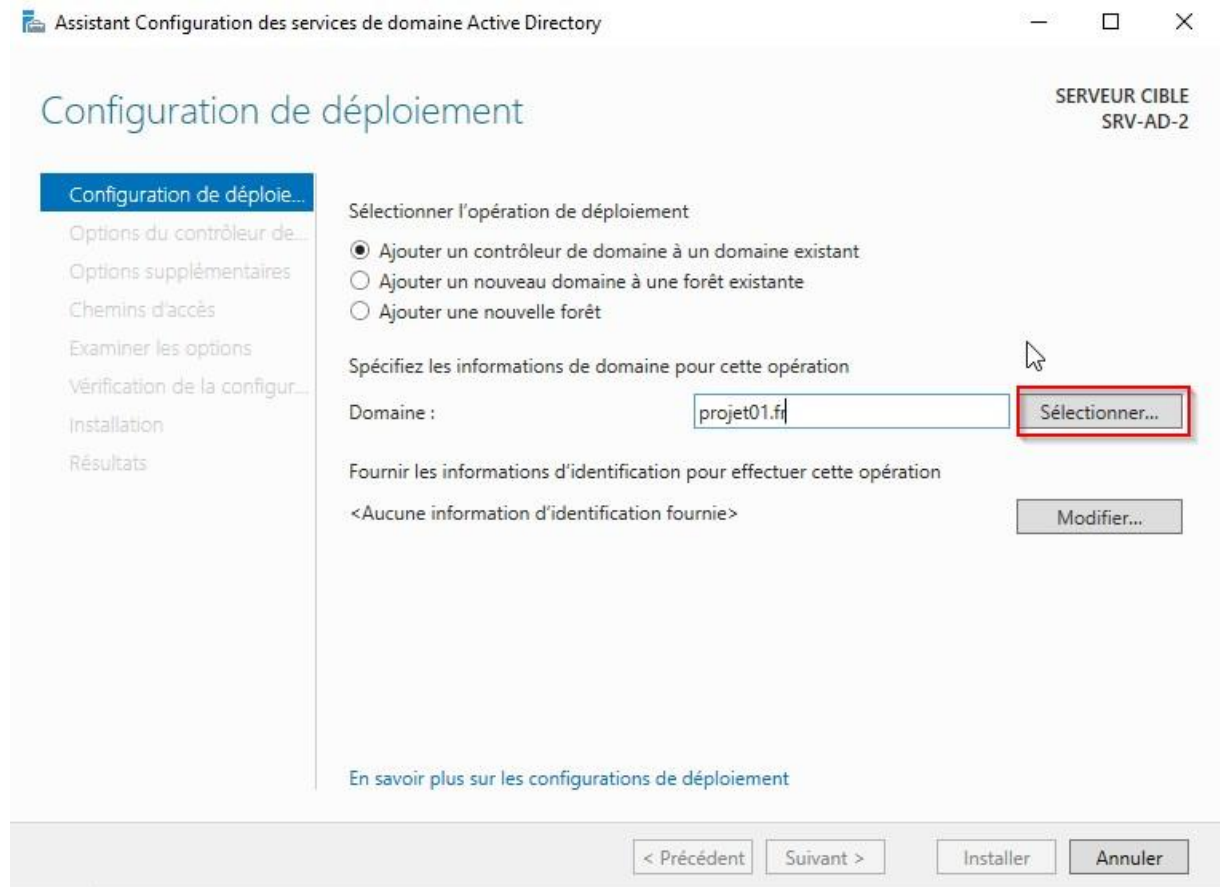
- Services AD DS**
Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.
Promouvoir ce serveur en contrôleur de domaine
- Gestion de stratégie de groupe
- Outils d'administration de serveur distant
 - Outils d'administration de rôles
 - Outils AD DS et AD LDS
 - Module Active Directory pour Windows PowerShell
 - Outils AD DS

1 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.

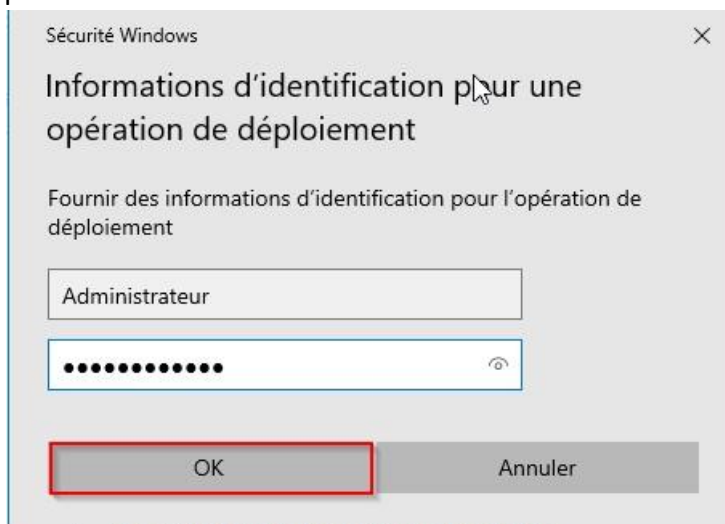
[Exporter les paramètres de configuration](#)

< Précédent Suivant > Fermer Annuler

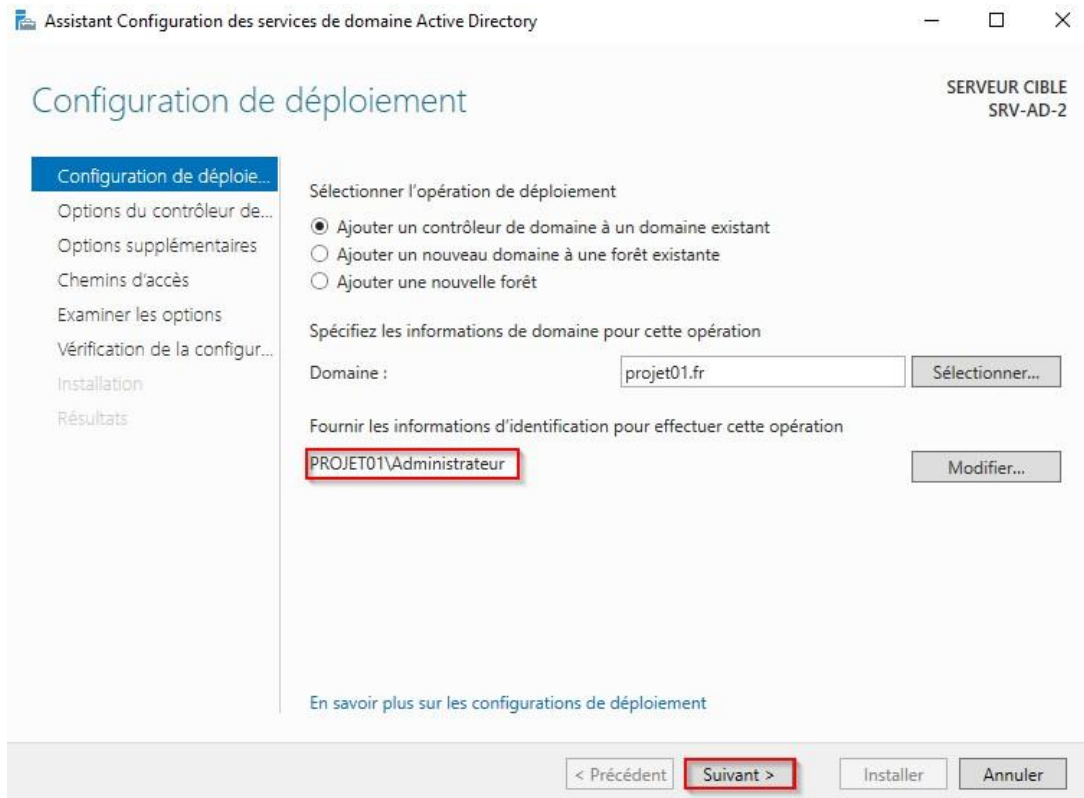
Configuration de déploiement. Je choisis **Ajouter un contrôleur de domaine à un domaine existant** et on indique le domaine **projet01.fr**.



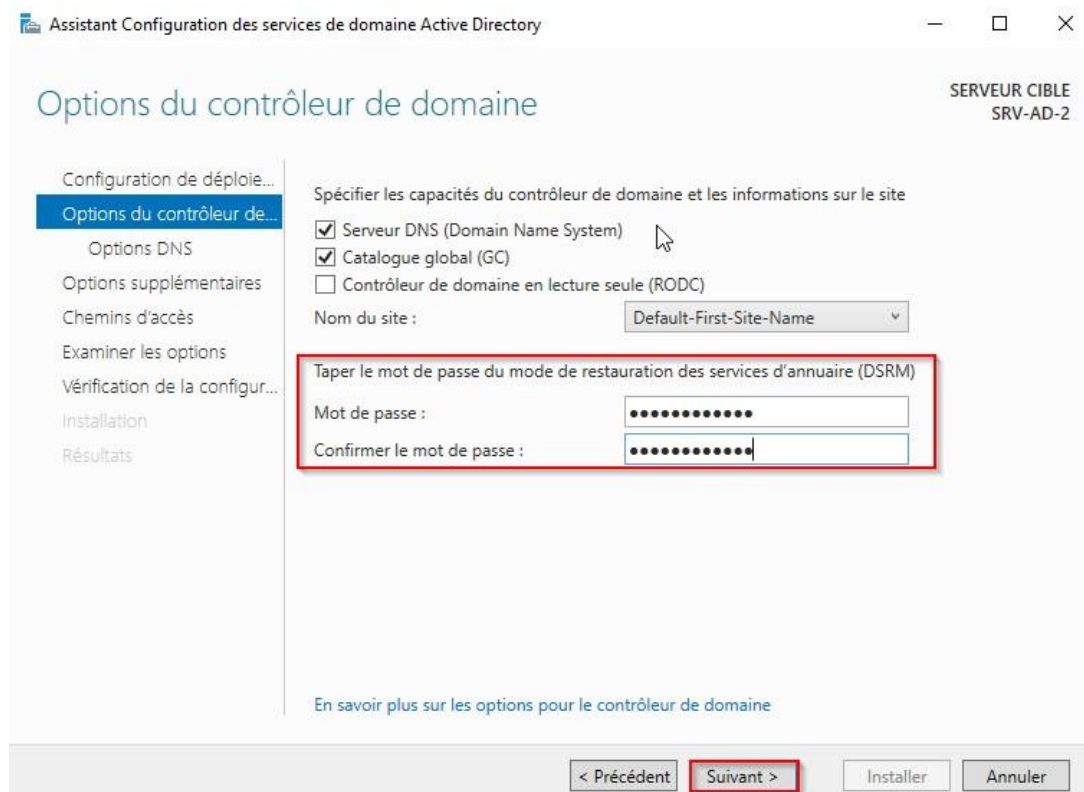
Authentification. Je saisi le mot de passe de l'administrateur du domaine pour autoriser la promotion.



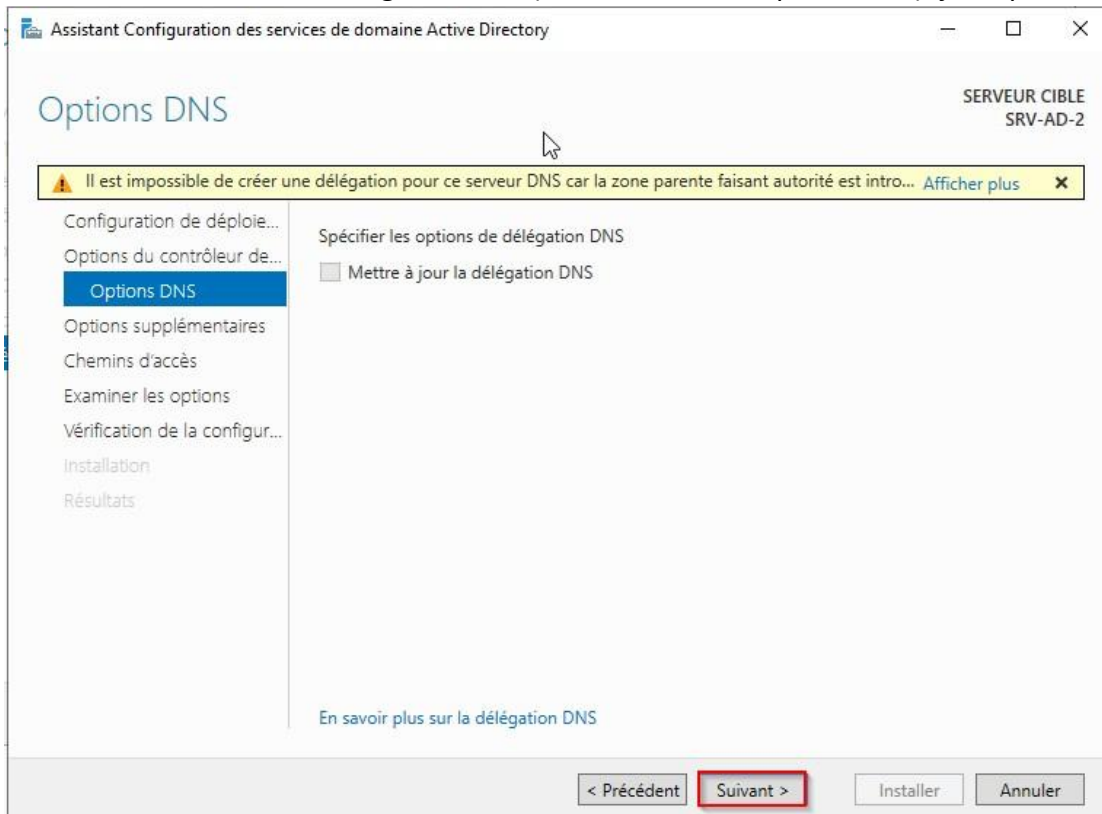
Je valide les informations d'identification pour le domaine **PROJET01\Administrateur**.



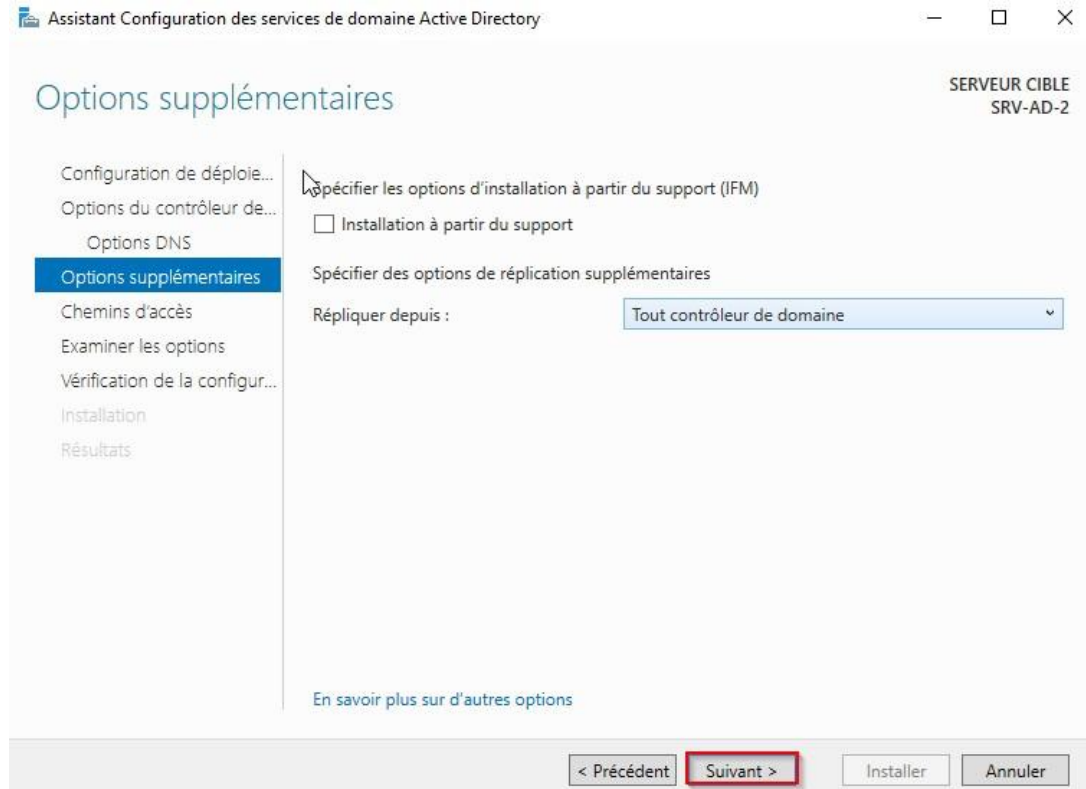
Options du contrôleur. Je laisse DNS et Catalogue Global cochés, puis je définit le mot de passe de restauration (**DSRM**)



Avertissement sur la délégation DNS (normal lors d'une promotion), je clique sur **Suivant**.



Options de répliquon. Je choisit de répliquer les données depuis **Tout contrôleur de domaine** (ou spécifiquement SRV-AD-1).



Confirmation des chemins d'accès pour les bases de données (NTDS) et SYSVOL.

Assistant Configuration des services de domaine Active Directory — □ ×

SERVEUR CIBLE
SRV-AD-2

Chemins d'accès

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

Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

Dossier de la base de données : ...

Dossier des fichiers journaux : ...

Dossier SYSVOL : ...

[En savoir plus sur les chemins d'accès Active Directory](#)

< Précédent **Suivant >** Installer Annuler

Examen des options. Un récapitulatif de la configuration s'affiche avant de cliquer sur **Suivant**.

Assistant Configuration des services de domaine Active Directory — □ ×

SERVEUR CIBLE
SRV-AD-2

Examiner les options

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 contrôleur de domaine Active Directory supplémentaire pour le domaine « projet01.fr ».

Nom du site : Default-First-Site-Name

Options supplémentaires :

Contrôleur de domaine en lecture seule : Non

Catalogue global : Oui

Serveur DNS : Oui

Mettre à jour la délégation DNS : Non

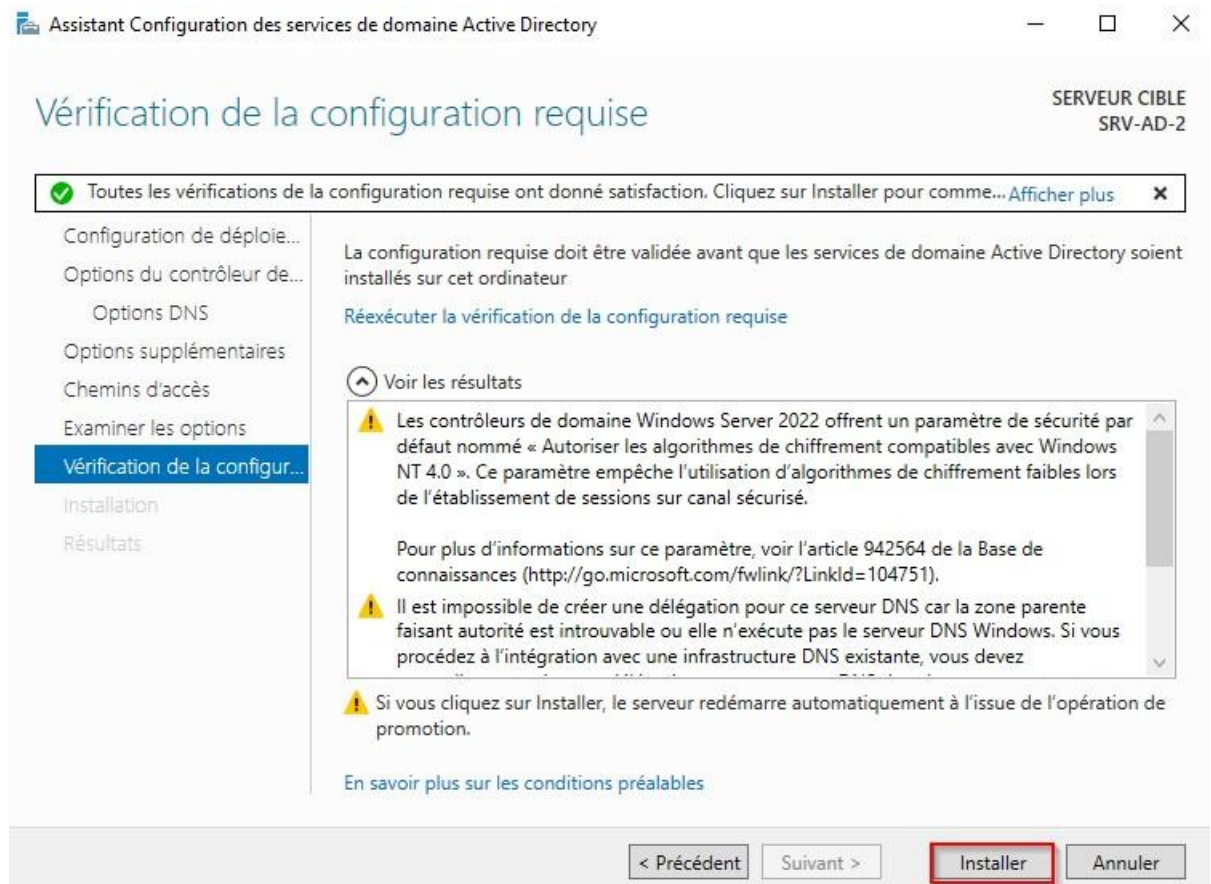
Contrôleur de domaine source : n'importe quel contrôleur de domaine accessible en écriture

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

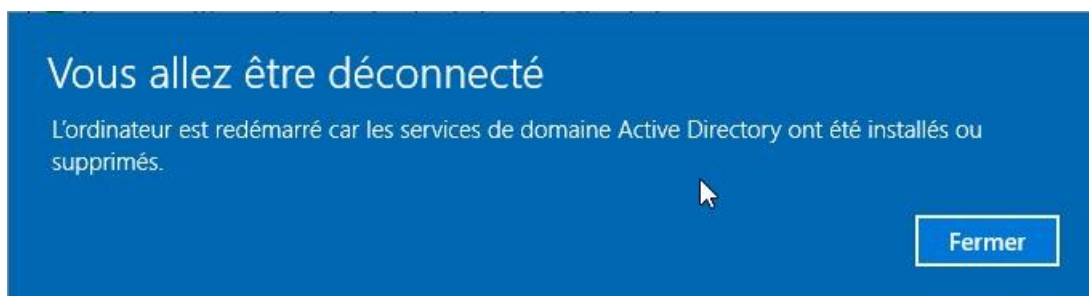
[En savoir plus sur les options d'installation](#)

< Précédent **Suivant >** Installer Annuler

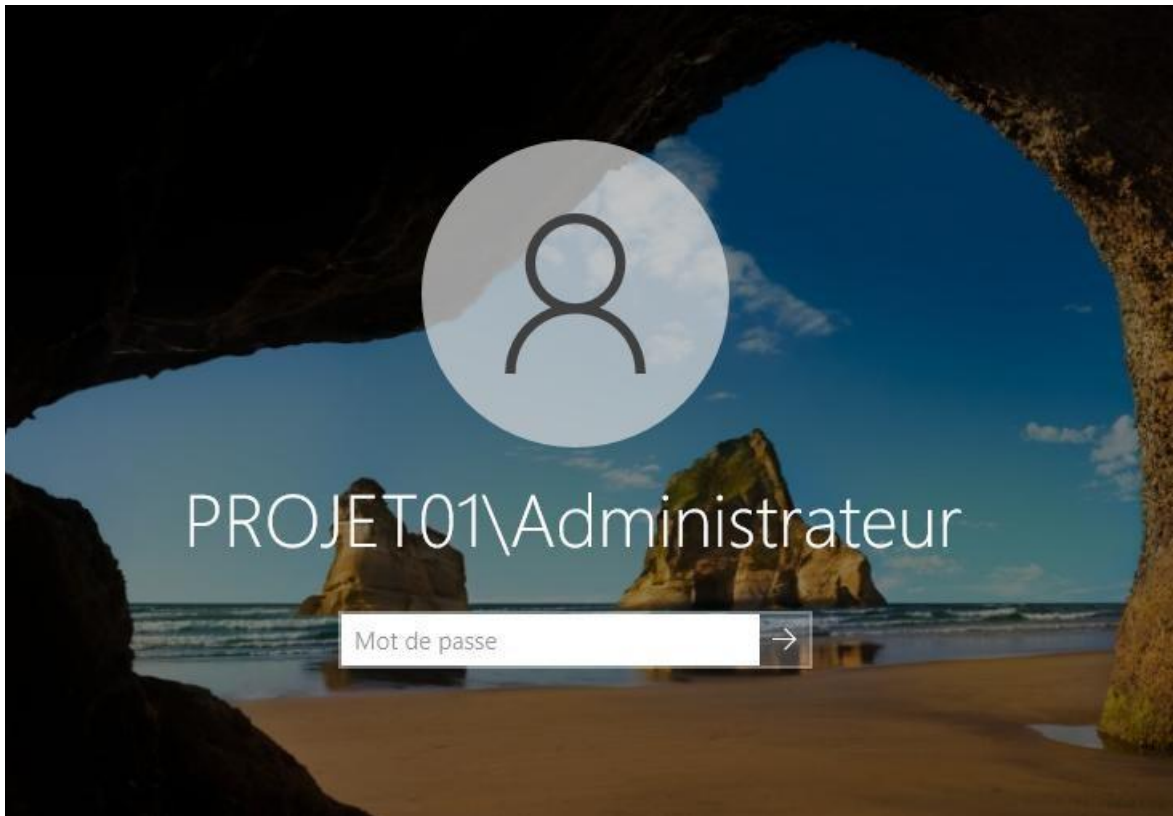
Vérification des prérequis. Une fois le voyant vert allumé, je clique sur **Installer**.



Message d'information indiquant que le serveur va redémarrer automatiquement à la fin du processus.



Page de connexion affichant **PROJET01\Administrateur**, prouvant que le serveur est bien intégré au domaine



Test final avec la commande nslookup projet01.fr. On voit bien les deux adresses IP (**192.168.30.100** et **192.168.30.101**) répondre pour le domaine.

```
C:\Users\Administrateur.PROJET01>nslookup projet01.fr
Serveur : UnKnown
Address: ::1

Nom : projet01.fr
Addresses: 192.168.30.101
           192.168.30.100
```

J'aurais aussi pu faire un dcdiag pour vérifier la santé globale et la réplication du contrôleur de domaine.

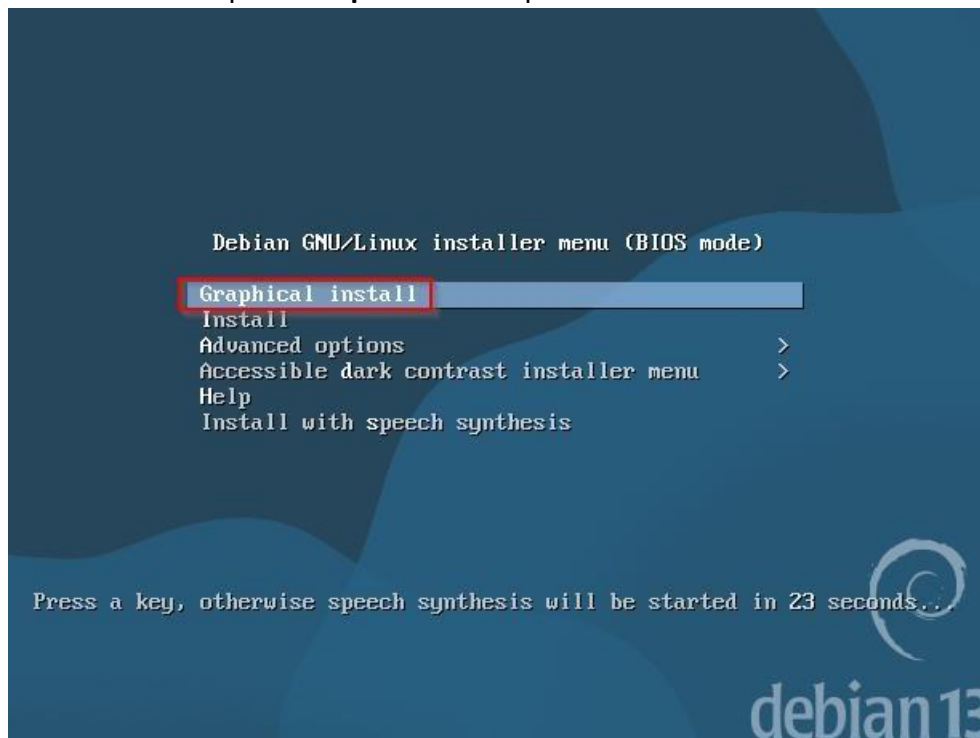
2 – Mise en place d'un logiciel de supervision (Zabbix)

Zabbix est une solution de supervision, conçue pour surveiller en temps réel l'état de vos serveurs, équipements réseau et services informatiques. Il permet de collecter des données précises sur les performances de votre infrastructure et d'alerter les administrateurs en cas d'anomalie.

Les étapes suivantes détaillent le déploiement de la version 7.0 sur un environnement Debian 13.

1 – Installation de Debian 13

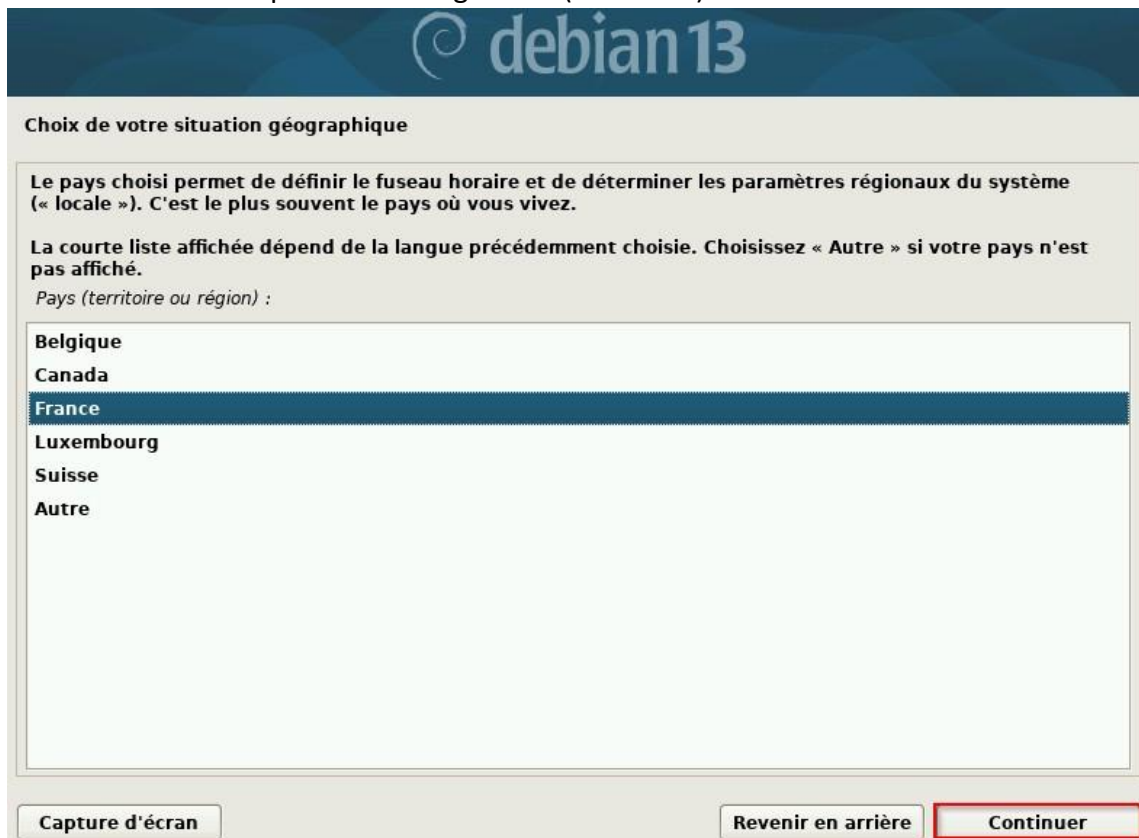
Je sélectionne l'option **Graphical install** pour lancer l'assistant d'installation visuel.



Je choisi **French - Français** pour définir la langue de l'installateur et du système final.



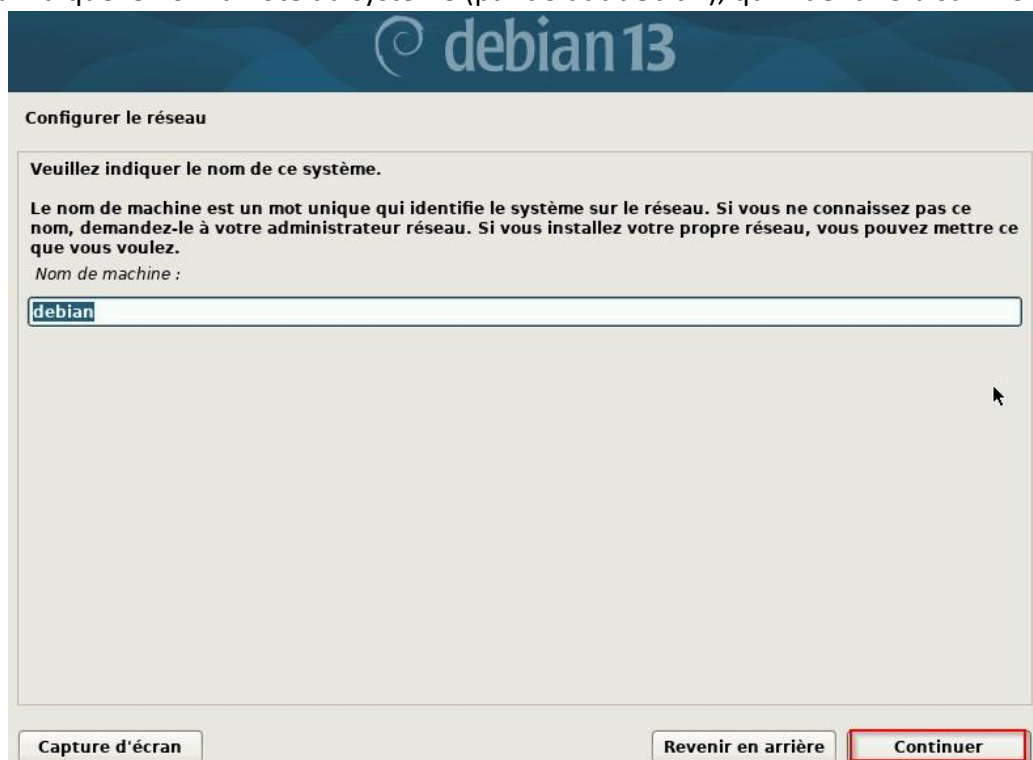
Je sélectionne **France** (ou votre pays de résidence) pour configurer automatiquement le fuseau horaire et les paramètres régionaux (« locale »).



Je choisis la disposition **Français** pour correspondre à mon matériel.



J'indique le nom d'hôte du système (par défaut **debian**), qui l'identifiera sur mon réseau.



Je saisi le **nom complet** du nouvel utilisateur (ex: user).

debian 13

Créer les utilisateurs et choisir les mots de passe

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

Veuillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse d'origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

Nom complet du nouvel utilisateur :

Je choisi un **identifiant de connexion** (login).

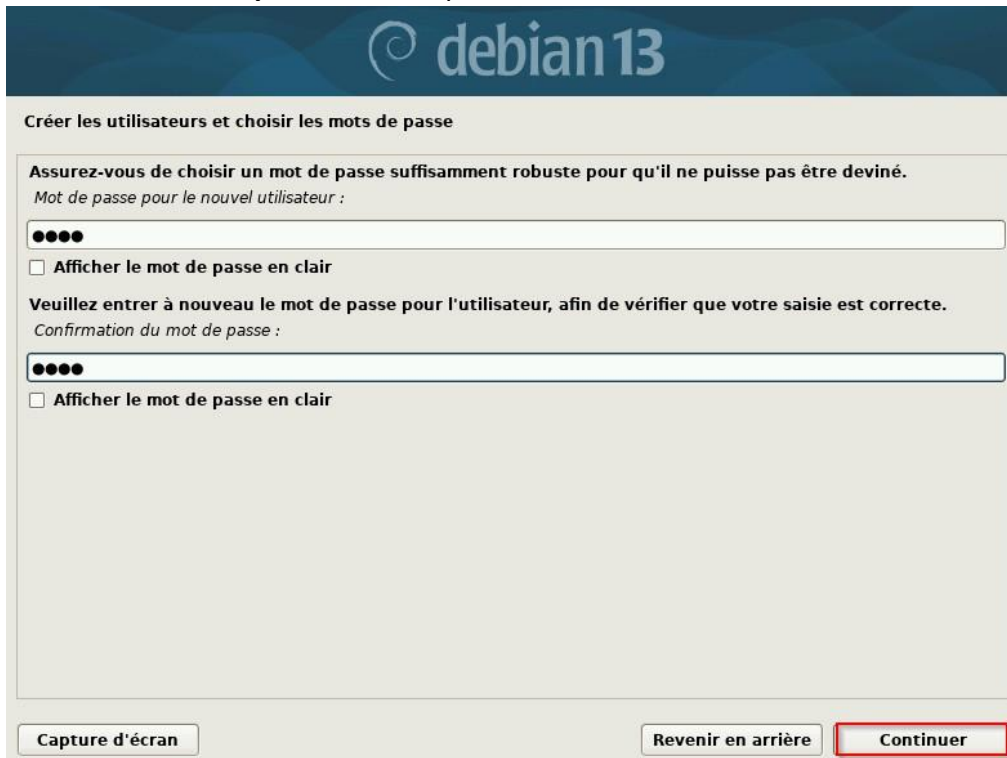
debian 13

Créer les utilisateurs et choisir les mots de passe

Veuillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.

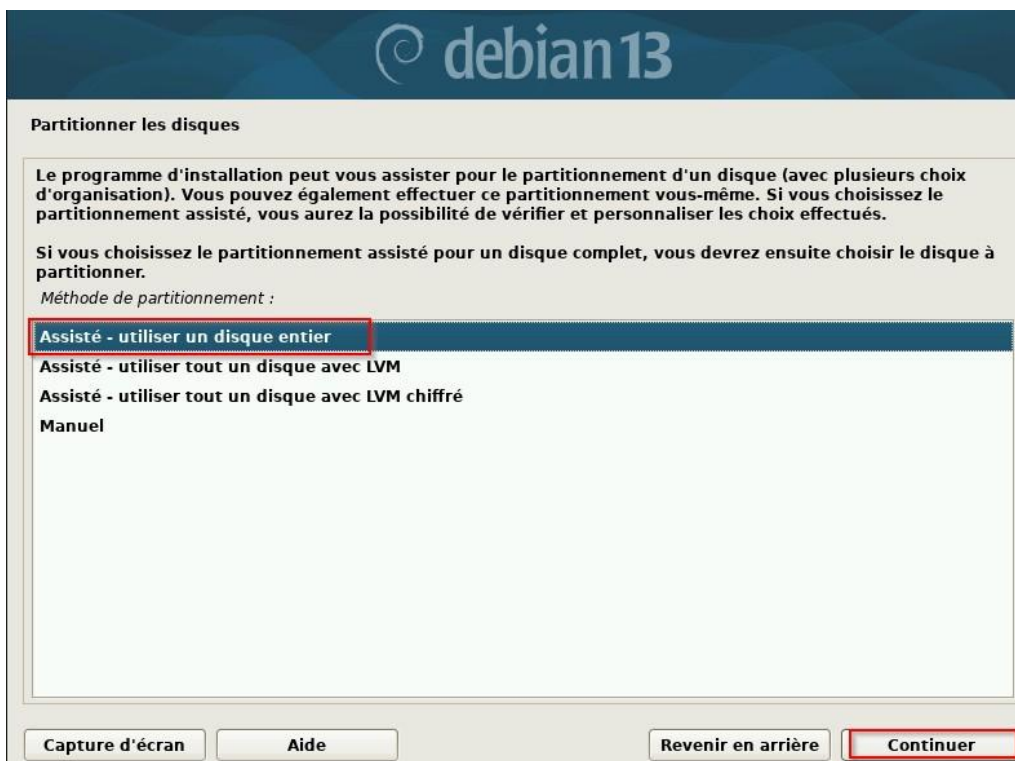
Identifiant pour le compte utilisateur :

Je défini un **mot de passe robuste** pour cet utilisateur courant.



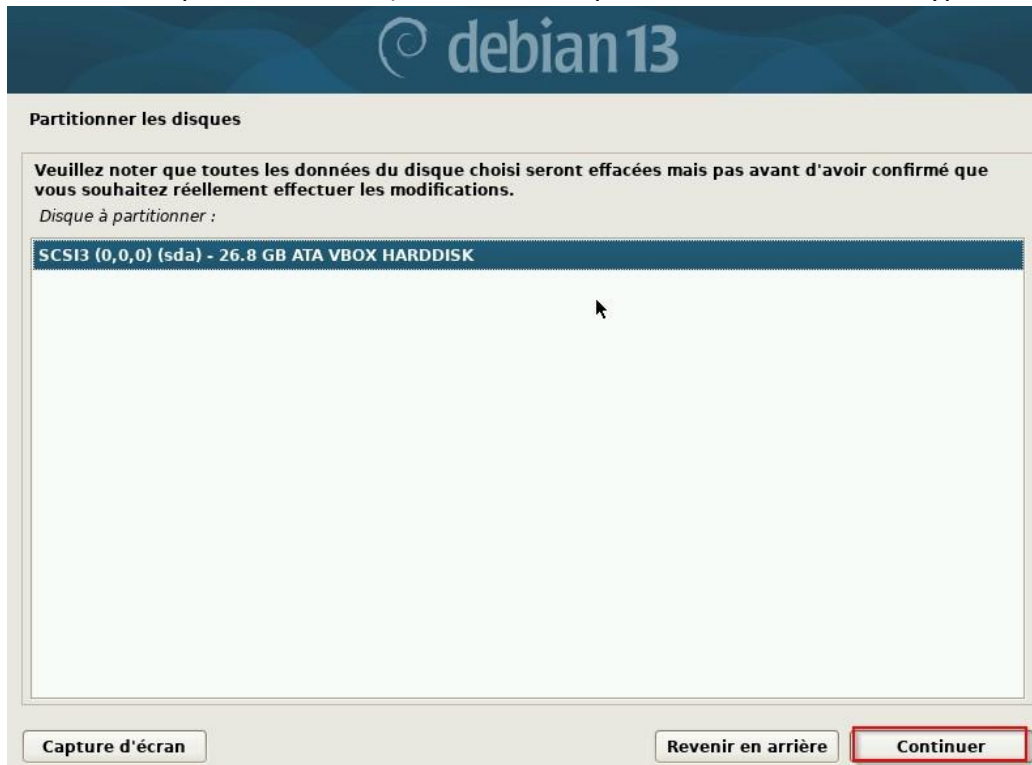
The screenshot shows the 'Créer les utilisateurs et choisir les mots de passe' (Create users and choose passwords) screen in the Debian 13 installer. The header features the Debian 13 logo. The main content area contains two password input sections. The first section is titled 'Assurez-vous de choisir un mot de passe suffisamment robuste pour qu'il ne puisse pas être deviné.' (Make sure you choose a sufficiently robust password so it cannot be guessed.) and includes a text input field with four black dots, a checkbox for 'Afficher le mot de passe en clair' (Show password in plain text), and a confirmation instruction: 'Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.' (Please enter the password again for the user to verify that your entry is correct.) The second section is titled 'Confirmation du mot de passe :'. It also has a text input field with four black dots and a checkbox for 'Afficher le mot de passe en clair'. At the bottom, there are three buttons: 'Capture d'écran', 'Revenir en arrière', and 'Continuer' (highlighted with a red border).

Je sélectionne **Assisté - utiliser un disque entier**. C'est l'option recommandée pour une installation standard.

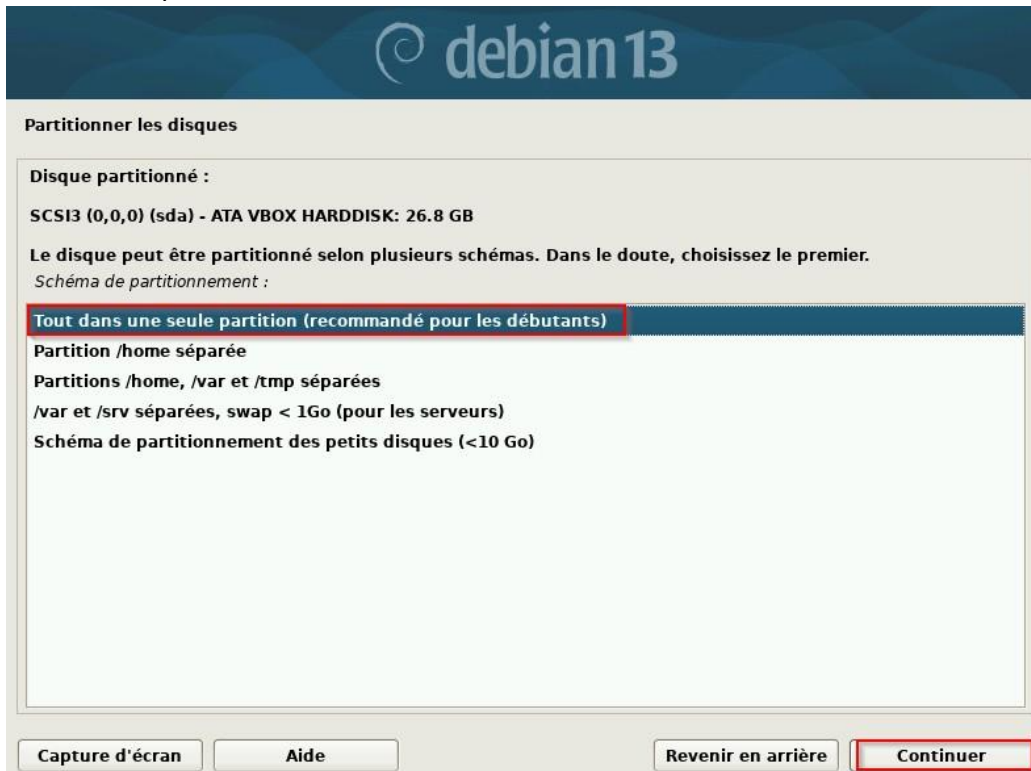


The screenshot shows the 'Partitionner les disques' (Partition disks) screen in the Debian 13 installer. The header features the Debian 13 logo. The main content area contains a list of partitioning methods. The first option, 'Assisté - utiliser un disque entier' (Assisted - use the whole disk), is highlighted with a blue background and a red border. The other options are 'Assisté - utiliser tout un disque avec LVM', 'Assisté - utiliser tout un disque avec LVM chiffré', and 'Manuel'. At the bottom, there are four buttons: 'Capture d'écran', 'Aide', 'Revenir en arrière', and 'Continuer' (highlighted with a red border).

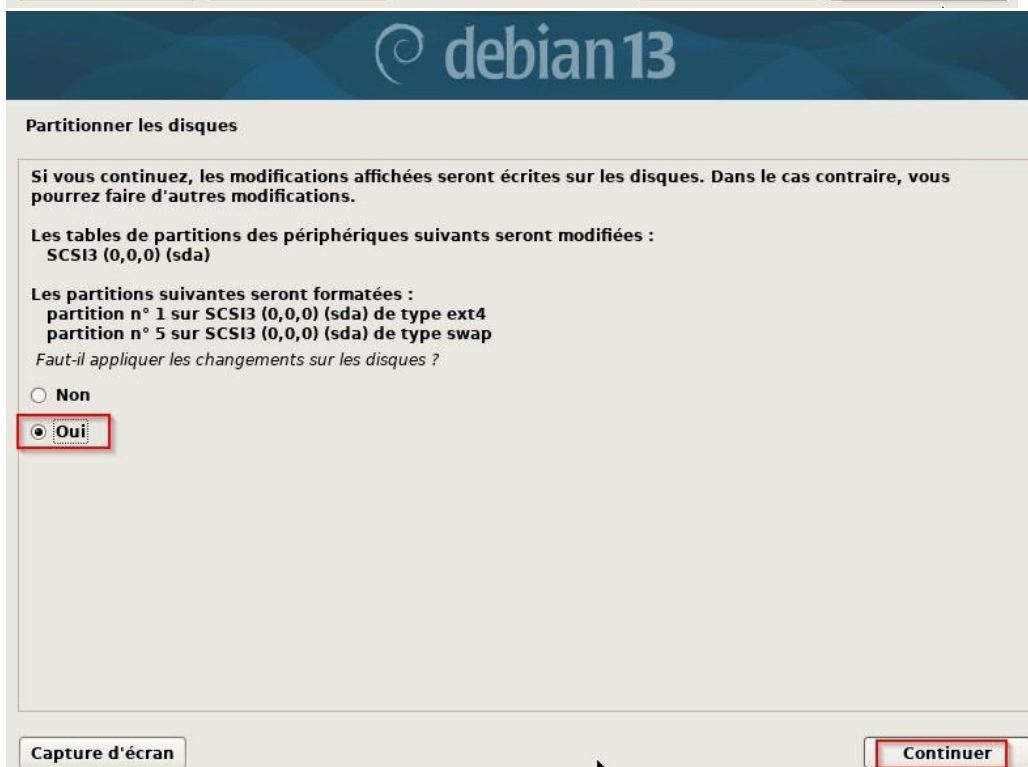
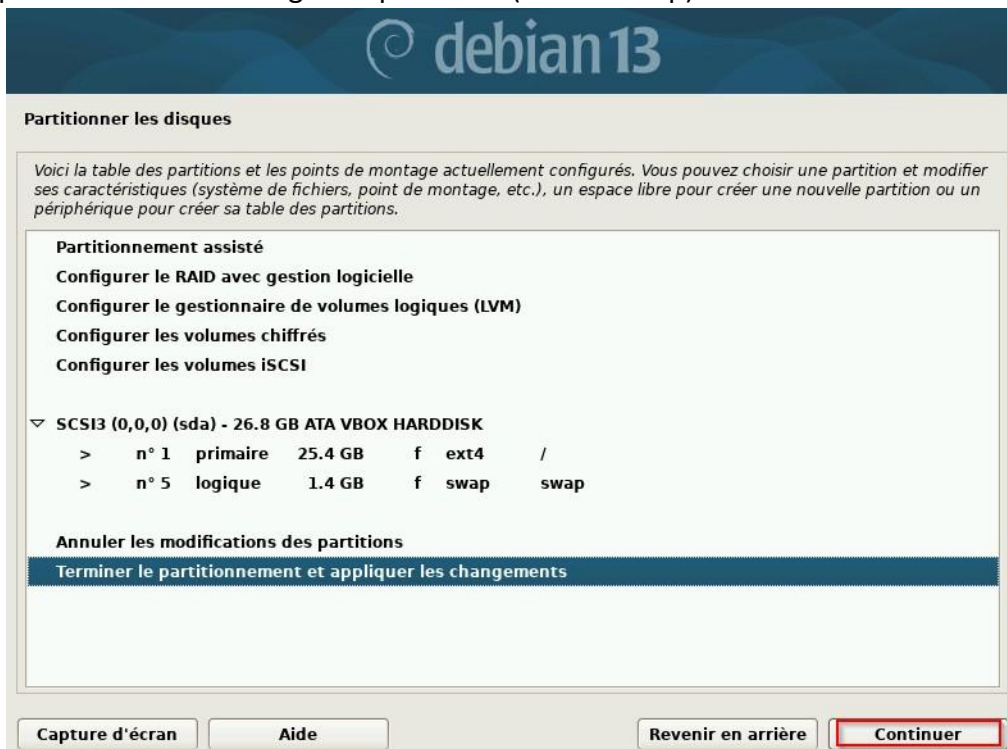
Je choisi le disque dur détecté (souvent un disque virtuel sda ou vda de type VBOX HARDDISK).



Je sélectionne pour **Tout dans une seule partition**, ce qui est idéal pour les débutants et les serveurs simples.



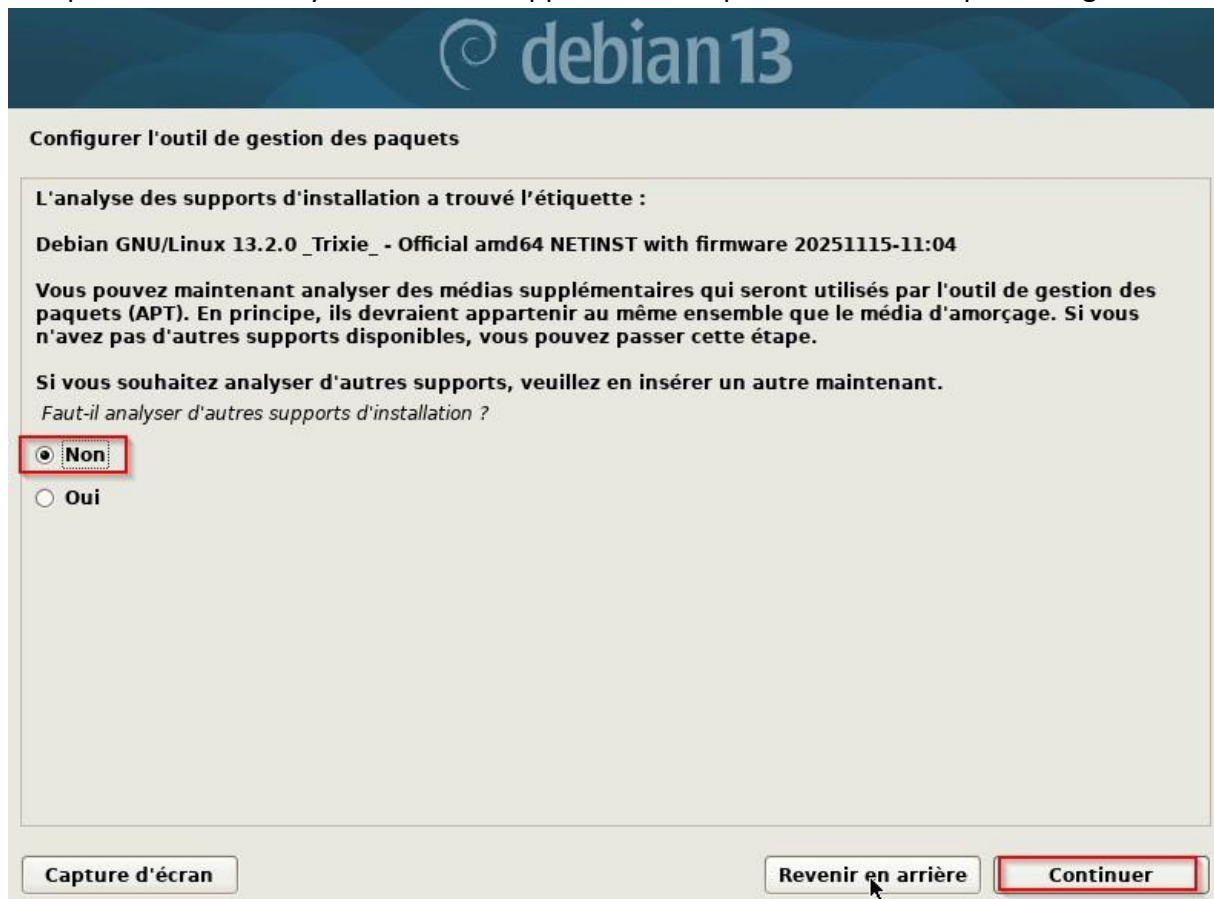
Je sélectionne **Terminer le partitionnement et appliquer les changements**, puis valide par **Oui** pour lancer le formatage des partitions (ext4 et swap).



L'installateur extrait et configure les paquets fondamentaux de Debian.



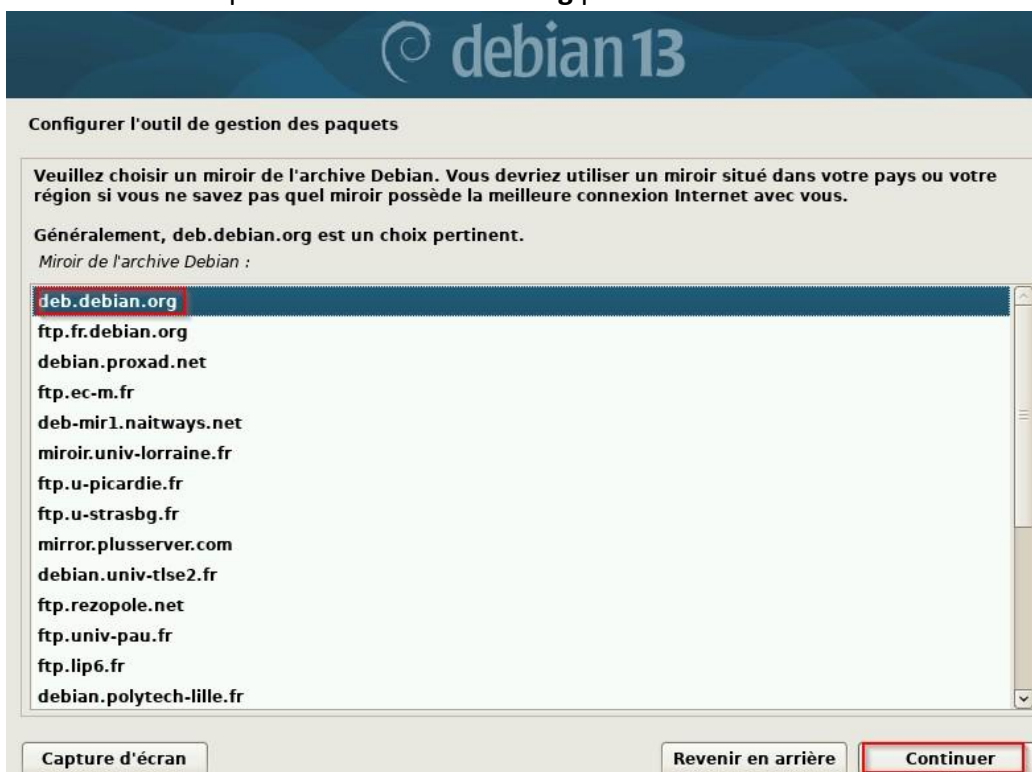
Je réponds **Non** à l'analyse de médias supplémentaires pour utiliser les dépôts en ligne.



Je sélectionne **France** comme pays du miroir.



Je choisis le miroir par défaut **deb.debian.org** pour une meilleure fiabilité.



Je laisse vide.



debian 13

Configurer l'outil de gestion des paquets

Si vous avez besoin d'utiliser un mandataire HTTP (souvent appelé « proxy ») pour accéder au monde extérieur, indiquez ses paramètres ici. Sinon, laissez ce champ vide.

Les paramètres du mandataire doivent être indiqués avec la forme normalisée « http://[[utilisateur]:mot-de-passe]@hôte[:port]/ ».

Mandataire HTTP (laisser vide si aucun) :

Capture d'écran Revenir en arrière Continuer

Installation des logiciels en cours



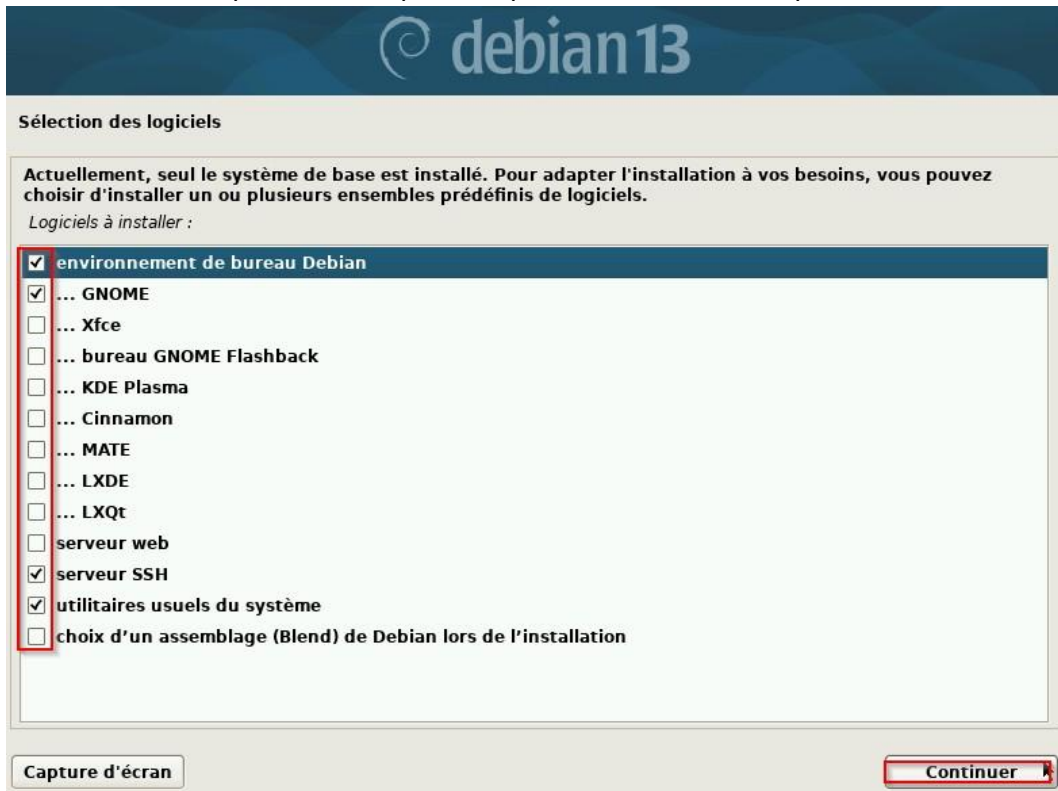
debian 13

Choisir et installer des logiciels

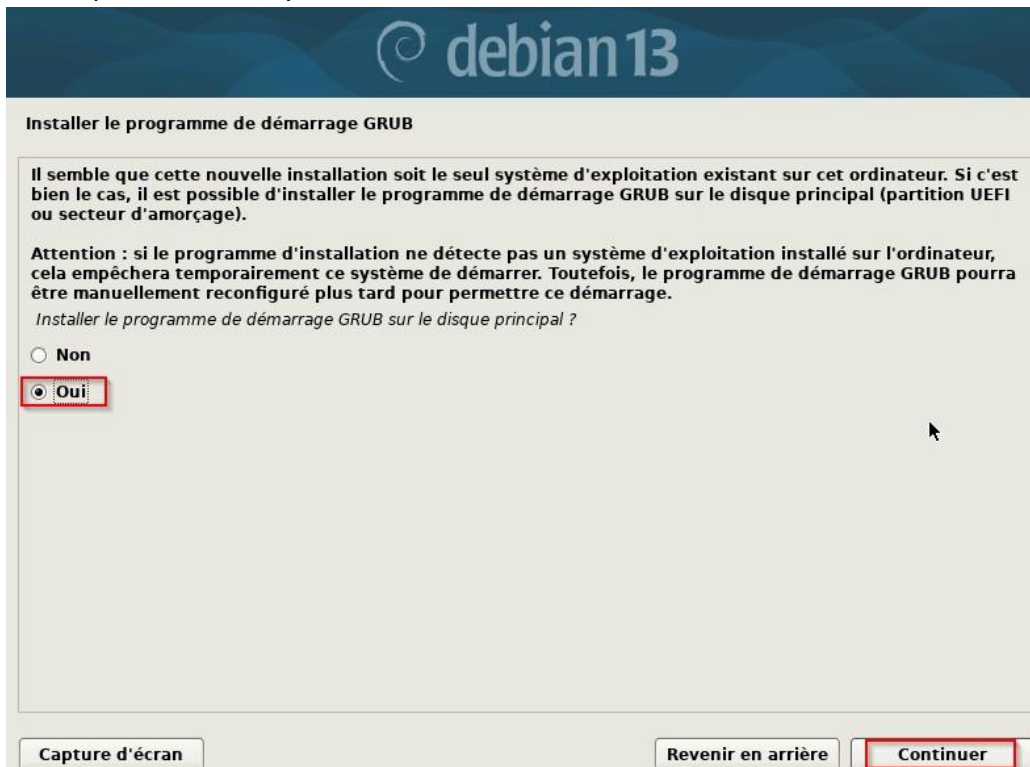
Choisir et installer des logiciels

Veuillez patienter...

Je coche les cases précédentes pour un poste de travail classique :



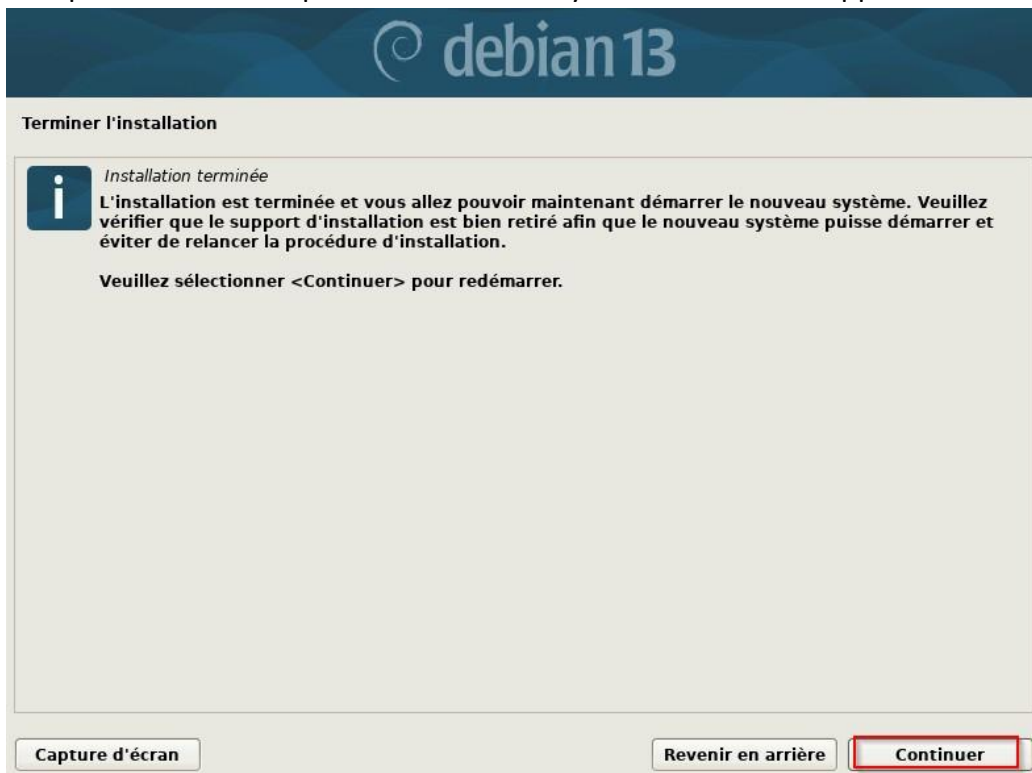
Je sélectionne **Oui** pour installer le programme de démarrage GRUB sur le disque principal afin de permettre au système de démarrer.

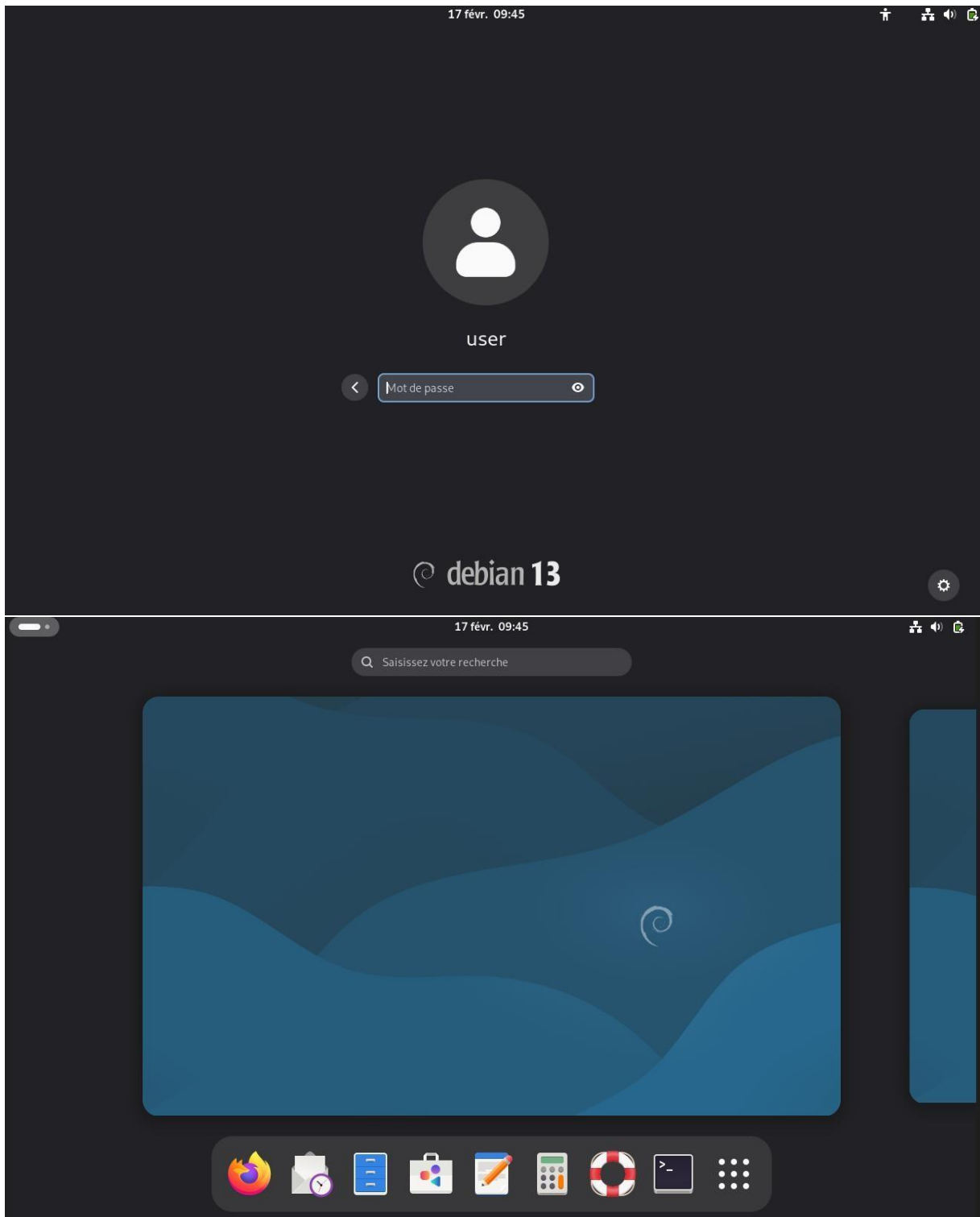


Je choisis manuellement mon disque (ex: /dev/sda) pour y inscrire le GRUB.



Je clique sur **Continuer** pour redémarrer le système une fois le support d'installation retiré.





J'attribue comme IP fixe 192.168.30.70 à mon debian 13

2 – Installation de Zabbix

Veillez noter que les commandes à exécuter dans le terminal sont indiquées ci-dessous en bleu.

Mise à jour de la liste des paquets et des logiciels installés

```
apt update && apt upgrade
```

Installation du serveur de base de données MariaDB `sudo`

```
apt install mariadb-server
```

Téléchargement du dépôt officiel Zabbix 7.0 pour Debian 13

```
wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbixrelease_latest_7.0+debian13_all.deb
```

Ajout des répertoires systèmes au PATH pour garantir l'accès aux commandes d'administration

```
export PATH=$PATH:/usr/local/sbin:/usr/sbin:/sbin
```

Installation du paquet de configuration du dépôt Zabbix `dpkg`

```
-i zabbix-release_latest_7.0+debian13_all.deb
```

Mise à jour des dépôts et installation du serveur Zabbix, de l'interface web et de l'agent `apt update`

```
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

Connexion à MariaDB en tant que root

```
mysql -uroot -p
```

Création de la base de données 'zabbix' avec support de l'UTF-8 complet `create database zabbix character set utf8mb4 collate utf8mb4_bin;`

Création de l'utilisateur dédié 'zabbix' avec son mot de passe `create user zabbix@localhost identified by 'password';`

Attribution de tous les privilèges sur la base 'zabbix' à l'utilisateur créé `grant all privileges on zabbix.* to zabbix@localhost;`

Autorisation temporaire de la création de fonctions pour l'importation du schéma

```
set global log_bin_trust_function_creators = 1; quit;
```

Importation des données initiales dans la base de données Zabbix

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

On désactive l'option de création de fonctions par sécurité: `mysql`

```
-uroot -p
```

```
set global log_bin_trust_function_creators = 0; quit;
```

Redémarrage des services pour appliquer les changements `systemctl`

```
restart zabbix-server zabbix-agent apache2
```

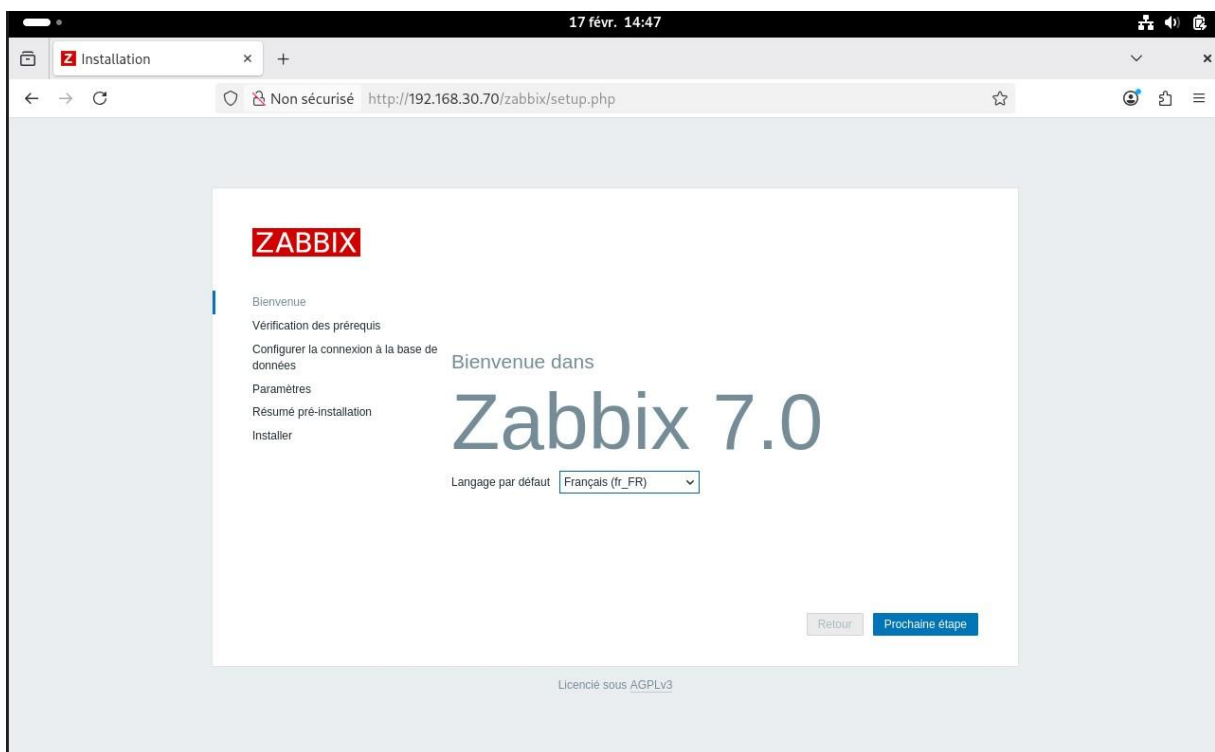
Activation du lancement automatique des services au démarrage du serveur `systemctl`

```
enable zabbix-server zabbix-agent apache2
```

L'assistant d'installation Web de Zabbix 7.0 s'affiche après avoir accédé à l'adresse IP du serveur. Je sélectionne la langue "Français" pour la suite de la configuration.

J'accède à l'interface via l'adresse <http://192.168.30.70/zabbix> (ip du debian).

L'assistant de configuration Zabbix 7.0 s'affiche. Je sélectionne la langue "Français" et clique sur **Prochaine étape**



Zabbix vérifie la configuration de PHP (version, limites de mémoire, extensions comme bcmath ou mbstring). Tous les voyants doivent être sur **OK** ;

ZABBIX

Vérification des prérequis

	Valeur actuelle	Requis	
Version de PHP	8.4.16	8.0.0	OK
Option PHP "memory_limit"	128M	128M	OK
Option PHP "post_max_size"	16M	16M	OK
Option PHP "upload_max_filesize"	2M	2M	OK
Option PHP "max_execution_time"	300	300	OK
Option PHP "max_input_time"	300	300	OK
support de bases de données par PHP	MySQL		OK
bcmath pour PHP	actif		OK
mbstring pour PHP	actif		OK
Option PHP "mbstring.func_overload"	inatif	inatif	OK

[Retour](#) [Prochaine étape](#)

Je renseigne les informations de la base de données créée précédemment (Hôte : localhost, Nom : zabbix, Utilisateur : zabbix et mon mot de passe).

ZABBIX

Configurer la connexion à la base de données

Veillez créer la base de données manuellement et configurer les paramètres de connexion. Appuyez sur le bouton "Prochaine étape" quand c'est fait.

Type de base de données

Hôte base de données

Port de la base de données 0 - utiliser le port par défaut

Nom de la base de données

Stocker les informations d'identification dans Texte brut Coffre HashiCorp Coffre CyberArk

Utilisateur

Mot de passe

Chiffrement TLS de la base de données La connexion ne sera pas chiffrée car elle utilise un fichier socket (sous Unix) ou de la mémoire partagée (Windows).

[Retour](#) [Prochaine étape](#)

Je donne un nom à mon serveur (ici : projet) et confirmez le fuseau horaire.

ZABBIX

Paramètres

Nom du serveur Zabbix

Fuseau horaire par défaut

Thème par défaut

[Retour](#) [Prochaine étape](#)

Un récapitulatif de mes choix s'affiche avant l'installation finale du fichier de configuration.

ZABBIX

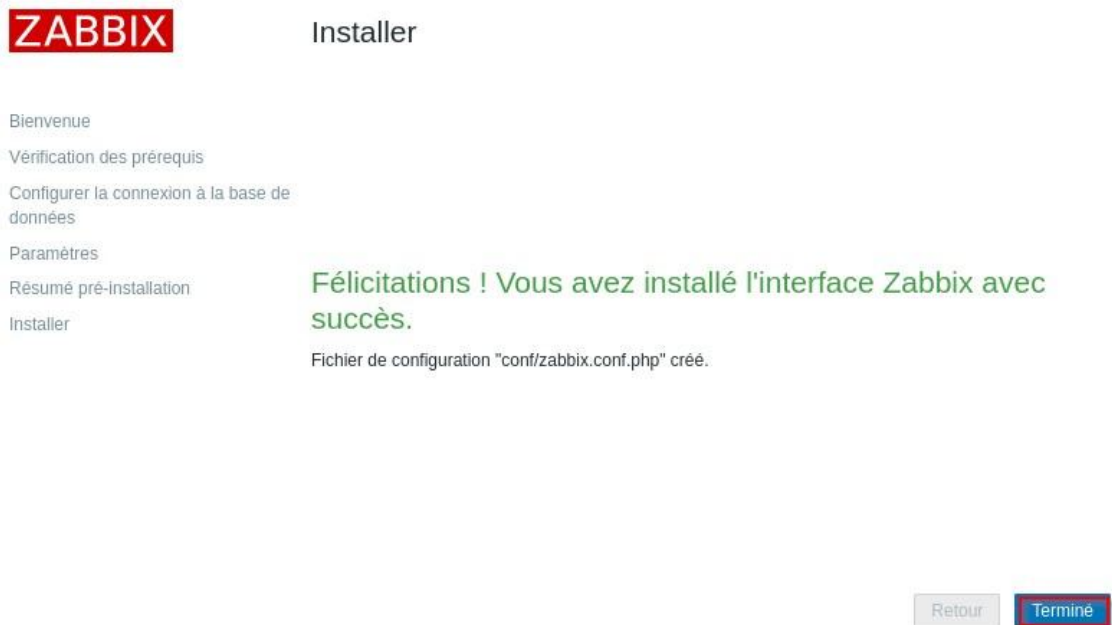
Résumé pré-installation

Veuillez vérifier les paramètres de configuration. Si tout est correct, appuyez sur le bouton "Prochaine étape" ; sinon, le bouton "Retour" pour changer les paramètres.

Type de base de données	MySQL
Serveur base de données	localhost
Port de la base de données	défaut
Nom de la base de données	zabbix
Utilisateur base de données	zabbix
Mot de passe utilisateur de la base de données	*****
Chiffrement TLS de la base de données	false
Nom du serveur Zabbix	projet

[Retour](#) [Prochaine étape](#)

Le message de succès confirme la création du fichier conf/zabbix.conf.php. Je clique sur **Terminé**.



The screenshot shows the Zabbix installation interface. At the top left is the ZABBIX logo. To its right is the word "Installer". Below the logo is a vertical list of navigation links: "Bienvenue", "Vérification des prérequis", "Configurer la connexion à la base de données", "Paramètres", "Résumé pré-installation", and "Installer". The "Installer" link is highlighted. To the right of this list, a green message reads: "Félicitations ! Vous avez installé l'interface Zabbix avec succès." Below this message, it says "Fichier de configuration 'conf/zabbix.conf.php' créé." At the bottom right, there are two buttons: "Retour" and "Terminé", with "Terminé" being highlighted.

Je me connecte avec les identifiants par défaut :
Utilisateur : Admin / Mot de passe : zabbix.



The screenshot shows the Zabbix login form. At the top is the ZABBIX logo. Below it is the label "Nom d'utilisateur" followed by a text input field containing "Admin". Below the input field is a red error message: "Nom d'utilisateur ou mot de passe incorrect ou le compte est temporairement bloqué." Below this is the label "Mot de passe" followed by a password input field with six dots. Below the password field is a checkbox labeled "Me rappeler toutes les 30 jours" which is checked. At the bottom is a blue button labeled "S'enregistrer".

Je tape dans l'invite de commande : `systemctl restart zabbix-server`

J'arrive sur la "Global view". Ce tableau de bord centralise l'état du système, les alertes en cours et la carte géographique des hôtes surveillés. Je vais maintenant ajouter mes appareils à surveiller.

The screenshot displays the Zabbix Global view dashboard. The left sidebar contains navigation options: Tableaux de bord, Surveillance, Services, Inventaire, Rapports, Collecte de données, Alertes, Utilisateurs, Administration, Support, Intégrations, Aide, Paramètres utilisateur, and Déconnexion. The main content area is titled "Global view" and includes several widgets:

- Top hosts by CPU utilization:** A table with columns for Host name, Utilization, 1m avg, 5m avg, 15m avg, and Processes. The only entry is "Zabbix_server".
- Information système:** A table with columns for Paramètre, Valeur, and Détails. It lists system parameters such as "Le serveur Zabbix est en cours d'exécution" (Non), "Version du serveur Zabbix", "Version du frontend Zabbix" (7.0.23), "Nombre d'hôtes (activé/désactivé)", "Nombre de modèles", "Nombre d'éléments (activés/désactivés/non supportés)", and "Nombre de déclencheurs (activés/désactivés [problème/])".
- Disponibilité de l'hôte:** A bar chart showing host availability status: 0 Disponi..., 0 Non dis..., 0 Mixte, 1 Inconnu, and 1 Tot.
- Problèmes par sévérité:** A bar chart showing the number of problems by severity: 0 Désastre, 0 Haut, 0 Moyen, 0 Avertisse..., 0 Information, and 0 Non classé.
- Carte géographique:** A map showing the location of monitored hosts, with "Riga" labeled.

A large number "1" is overlaid on the right side of the dashboard.

3– Ajout de PfSense dans Zabbix

Configuration du service SNMP sur le pare-feu pfSense. J'active le "SNMP Daemon", je définit la communauté sur "public" et j'enregistre les modifications. **Sur pfSense** : je me rend dans Services > SNMP. Je coche "Enable", choisi SNMPv2c et défini une **Communauté** (public) puis fais **Save**

SNMP Daemon

Enable Enable the SNMP Daemon and its controls

SNMP Daemon Settings

Polling Port
Enter the port to accept polling events on (default 161).

System Location

System Contact

Read Community String
The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.

SNMP Traps Enable

Enable Enable the SNMP Trap and its controls

SNMP Modules

SNMP modules

- MibII
- Netgraph
- PF
- Host Resources
- UCD
- Regex

Interface Binding

Internet Protocol

Bind Interfaces
WAN
LAN
Localhost

Ensuite coté zabbix, il faut faire la création d'un nouvel hôte dans Zabbix avec son nom et son adresse IP.

Navigation dans l'interface Zabbix vers "Collecte de données" > "Hôtes" pour initier l'ajout d'un nouvel appareil via le bouton "Créer un hôte"

The screenshot shows the Zabbix web interface. On the left, a dark blue sidebar contains a menu with 'Collecte de données' (1) and 'Hôtes' (2) highlighted with red boxes. In the top right corner, a button labeled 'Créer un hôte' (3) is also highlighted with a red box. The main content area shows the 'Hosts' configuration page with various search and filter fields, and a table of hosts. A warning message at the bottom states: 'Le serveur Zabbix ne fonctionne pas : les informations affichées peuvent ne pas être actuelles.'

Paramétrage de l'hôte dans Zabbix avec son nom, l'application du modèle "PfSense by SNMP", et l'ajout de l'interface SNMP sur l'IP 192.168.30.1.

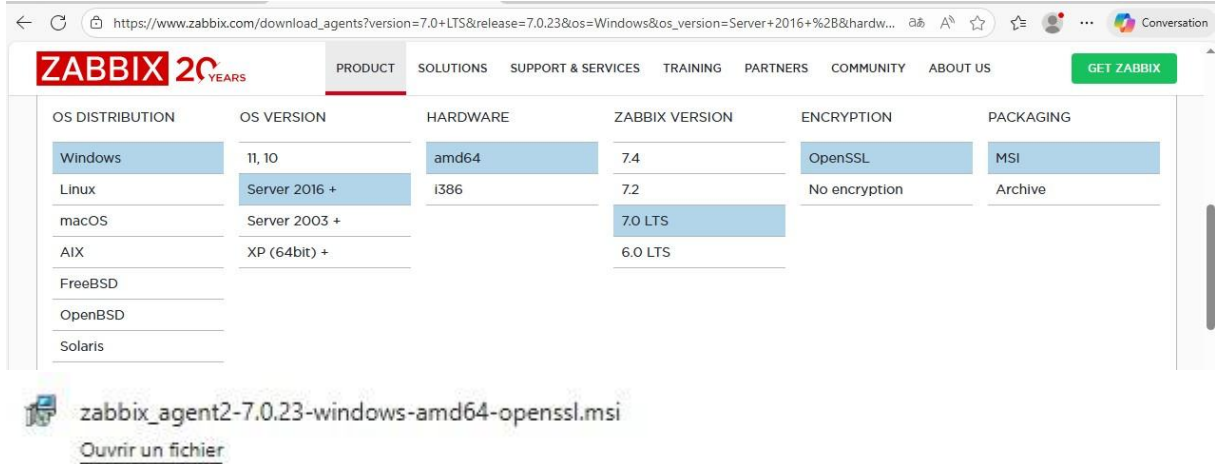
The screenshot shows the 'Nouvel hôte' (New host) configuration form in Zabbix. The form is titled 'Nouvel hôte' and has several tabs: 'Hôte', 'IPMI', 'Tags', 'Macros', 'Inventaire', 'Chiffrement', and 'Table de correspondance'. The 'Hôte' tab is active. The form contains the following fields and options:

- Nom de l'hôte:** PfSense
- Nom visible:** PfSense
- Modèles:** PfSense by SNMP (selected)
- Groupes d'hôtes:** Virtual machines (selected)
- Interfaces:** A table with columns: Type, adresse IP, Nom DNS, Connexion à, Port, and Défaut. One interface is defined: Type: SNMP, adresse IP: 192.168.30.1, Connexion à: IP, DNS, Port: 161, Défaut: Supprimer.
- Version SNMP:** SNMPv2 (selected)
- Communauté SNMP:** public
- Nombre maximal de répétitions:** 10
- Utiliser des requêtes combinées:**
- Description:** routeur PfSense
- Surveillé par:** Serveur (selected)
- Activé:**

At the bottom right, there are two buttons: 'Ajouter' and 'Annuler'.

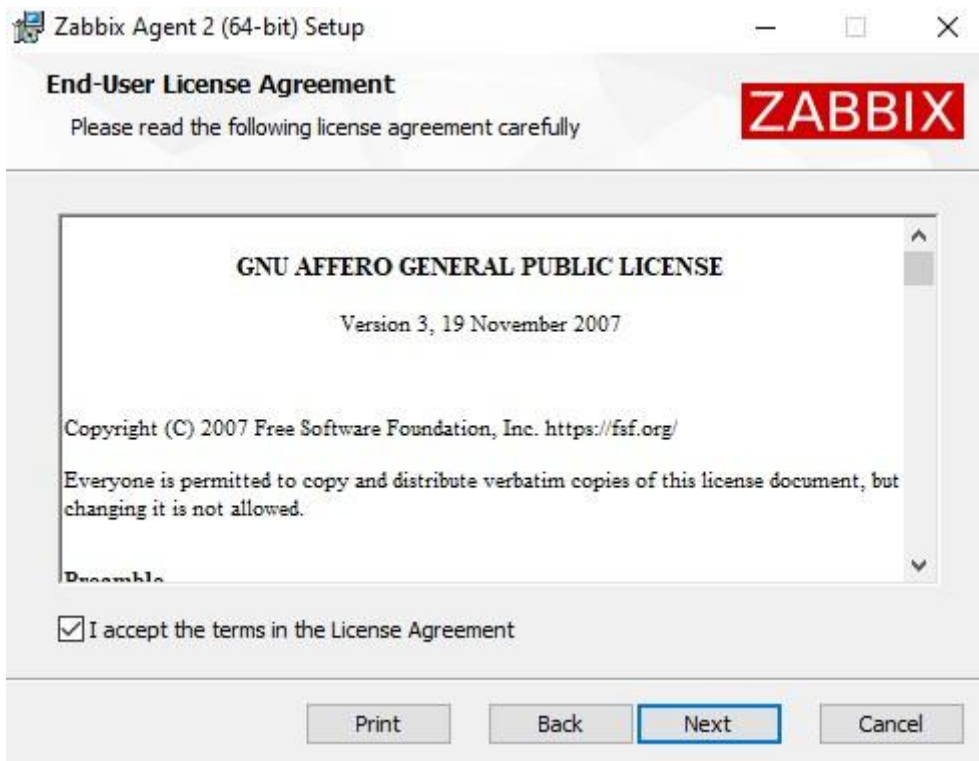
4 – Ajout du SRV1 dans Zabbix

Sur le serveur Windows, téléchargement de l'installateur MSI de l'agent Zabbix 7.0 depuis le site officiel.

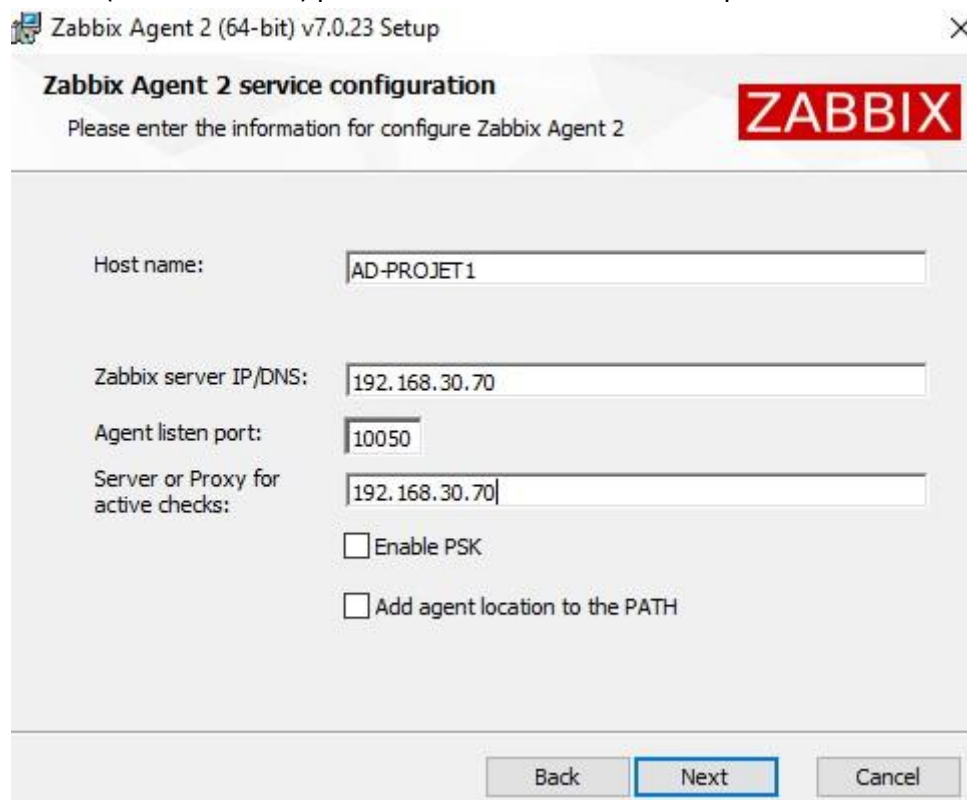


Lancement de l'assistant de configuration de l'agent Windows et acceptation des termes de la licence.

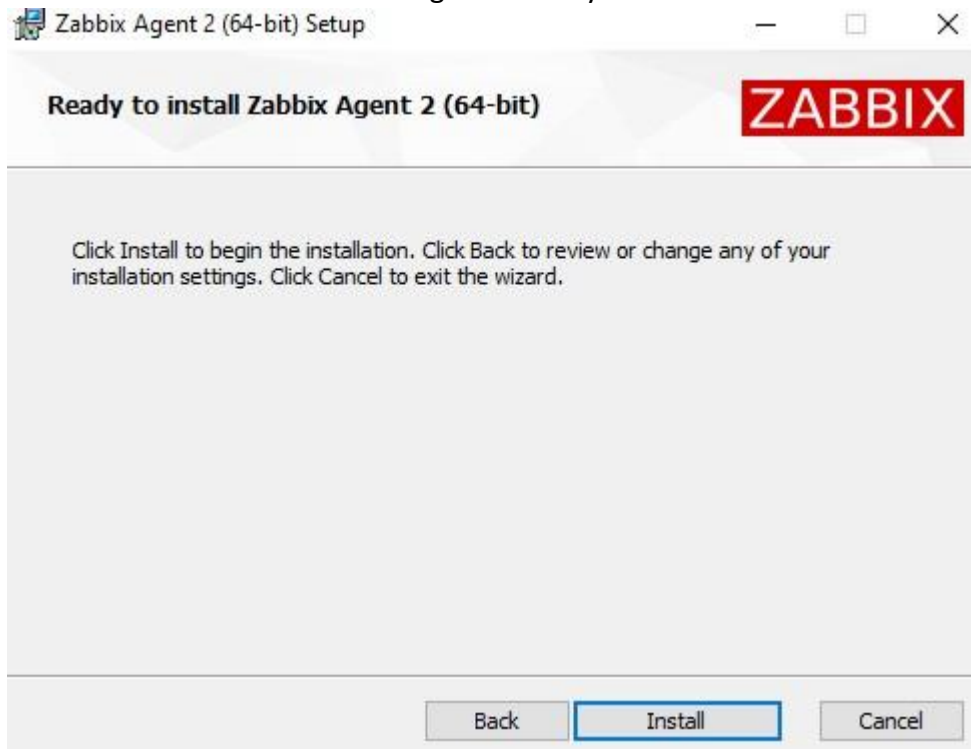




Étape cruciale où je renseigne le nom de l'hôte (ex: AD-PROJET1) et l'adresse IP du serveur Zabbix (192.168.30.70) pour les vérifications actives et passives.



Finalisation de l'installation de l'agent sur le système Windows.



Maintenant coté zabbix

Déclaration du serveur dans l'interface Zabbix avec l'IP 192.168.30.100 et le modèle "Windows by Zabbix agent".

Nouvel hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte

Nom visible

Modèles Sélectionner
taper ici pour rechercher

* Groupes d'hôtes Sélectionner
taper ici pour rechercher

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
	Agent	<input type="text" value="192.168.30.100"/>	<input type="text"/>	<input type="text" value="IP"/> <input type="text" value="DNS"/>	<input type="text" value="10050"/>	<input checked="" type="radio"/> Supprimer

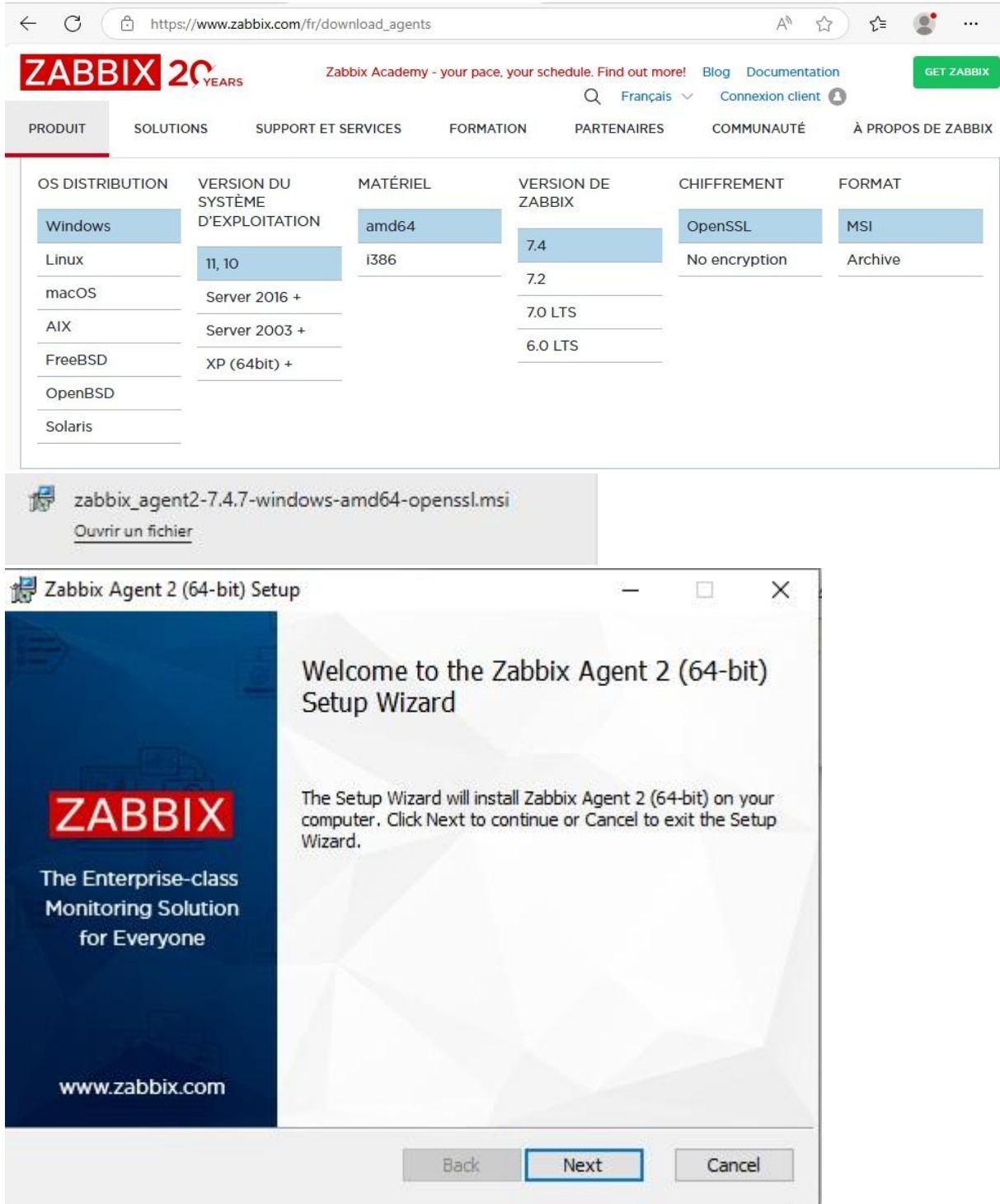
[Ajouter](#)

Description

Surveillé par

5 – Ajout du Windows client dans zabbix

Procédure identique à celle des serveurs pour le déploiement de l'agent sur le poste client Windows 10. Le nom d'hôte configuré ici est WIN10-CLIENT



The screenshot shows the Zabbix website's download agents page. The browser address bar displays https://www.zabbix.com/fr/download_agents. The page features a navigation menu with categories: PRODUIT, SOLUTIONS, SUPPORT ET SERVICES, FORMATION, PARTENAIRES, COMMUNAUTÉ, and À PROPOS DE ZABBIX. A search bar is set to 'Français' and a 'Connexion client' button is visible. A 'GET ZABBIX' button is in the top right corner.

OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	MATÉRIEL	VERSION DE ZABBIX	CHIFFREMENT	FORMAT
Windows		amd64	7.4	OpenSSL	MSI
Linux	11, 10	i386	7.2	No encryption	Archive
macOS	Server 2016 +		7.0 LTS		
AIX	Server 2003 +		6.0 LTS		
FreeBSD	XP (64bit) +				
OpenBSD					
Solaris					

Below the table, a file download link is shown: `zabbix_agent2-7.4.7-windows-amd64-openssl.msi` with the text 'Ouvrir un fichier'.

The second part of the screenshot shows the 'Zabbix Agent 2 (64-bit) Setup' window. The title bar reads 'Zabbix Agent 2 (64-bit) Setup'. The main content area displays the Zabbix logo and the text: 'The Enterprise-class Monitoring Solution for Everyone' and 'www.zabbix.com'. The main text says: 'Welcome to the Zabbix Agent 2 (64-bit) Setup Wizard. The Setup Wizard will install Zabbix Agent 2 (64-bit) on your computer. Click Next to continue or Cancel to exit the Setup Wizard.' At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

End-User License Agreement

Please read the following license agreement carefully



GNU AFFERO GENERAL PUBLIC LICENSE
Version 3, 19 November 2007

Copyright (C) 2007 Free Software Foundation, Inc. <https://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

I accept the terms in the License Agreement

Print Back Next Cancel

Zabbix Agent 2 service configuration

Please enter the information for configure Zabbix Agent 2



Host name: WIN10-CLIENT

Zabbix server IP/DNS: 192.168.30.70

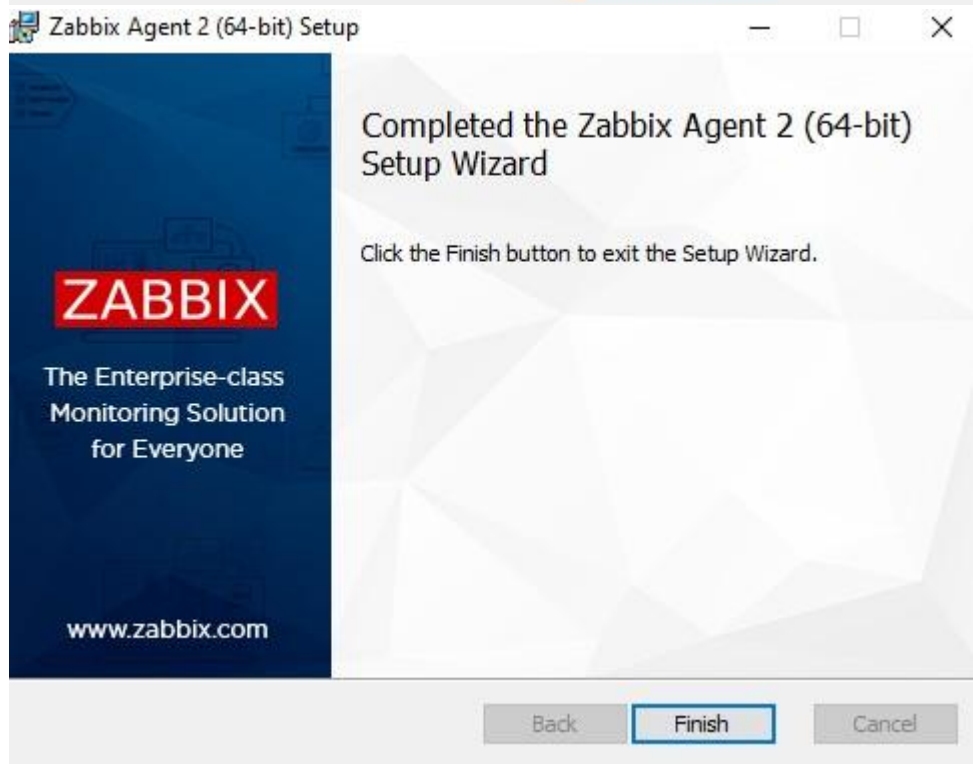
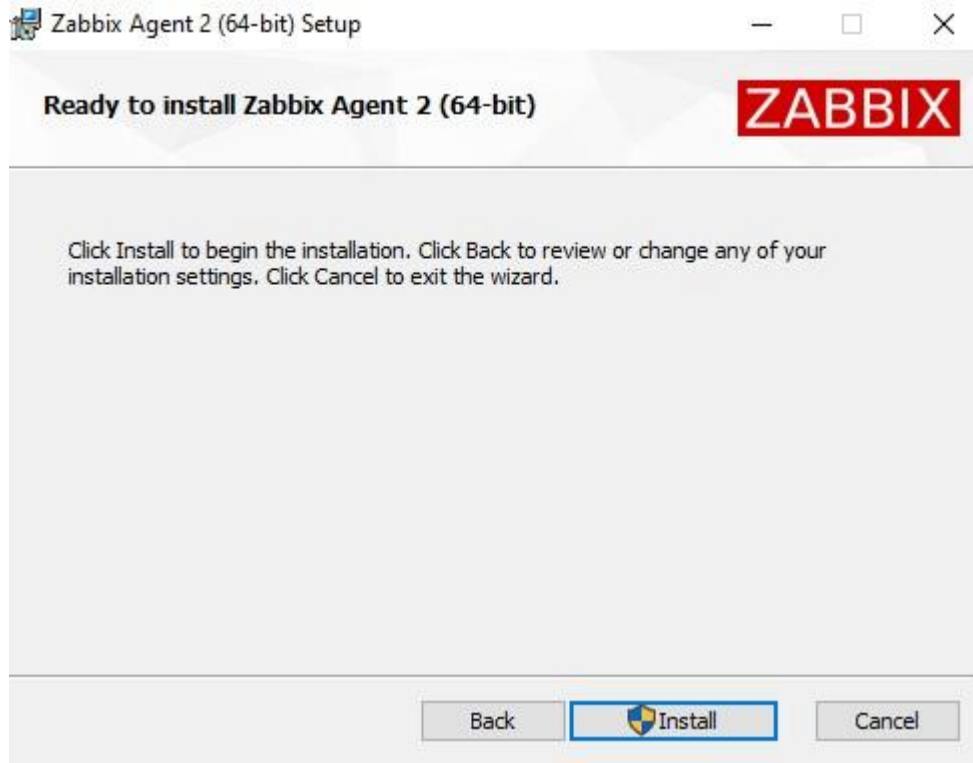
Agent listen port: 10050

Server or Proxy for active checks: 192.168.30.70

Enable PSK

Add agent location to the PATH

Back Next Cancel



Coté zabbix :

Ajout final du poste de travail avec l'adresse IP 192.168.30.201.

Nouvel hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte Win10-client

Nom visible Win10-client

Modèles Windows by Zabbix agent x Sélectionner
taper ici pour rechercher

* Groupes d'hôtes Virtual machines x Sélectionner
taper ici pour rechercher

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent		192.168.30.201		IP DNS	10050	<input checked="" type="radio"/> Supprimer

Ajouter

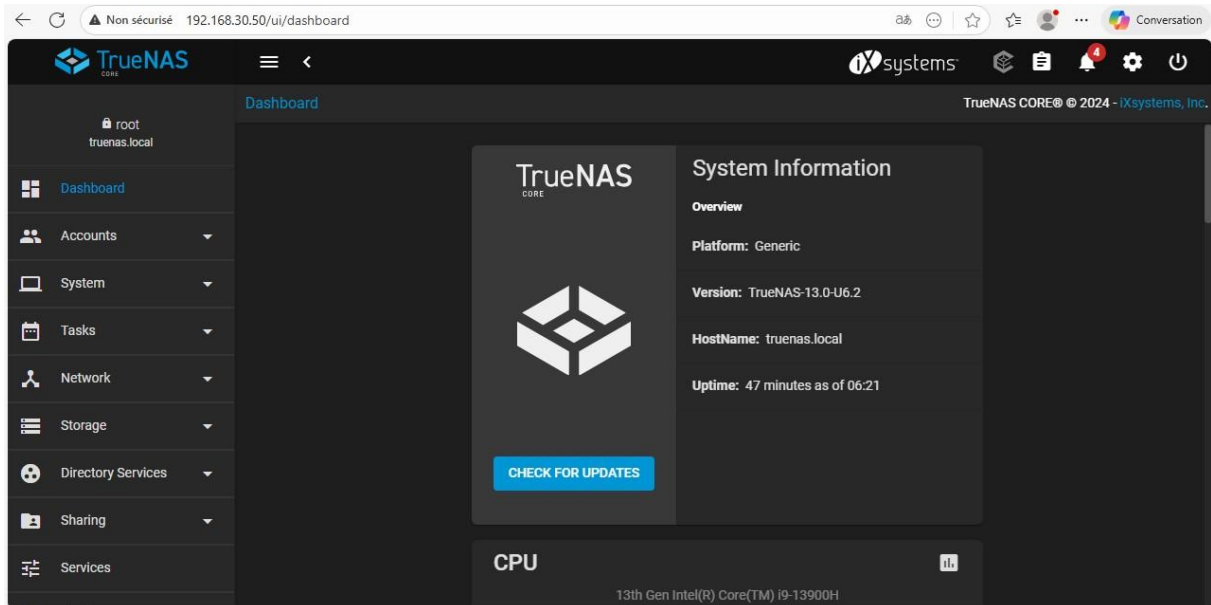
Description windows client

Surveillé par Serveur Proxy Groupe de proxy

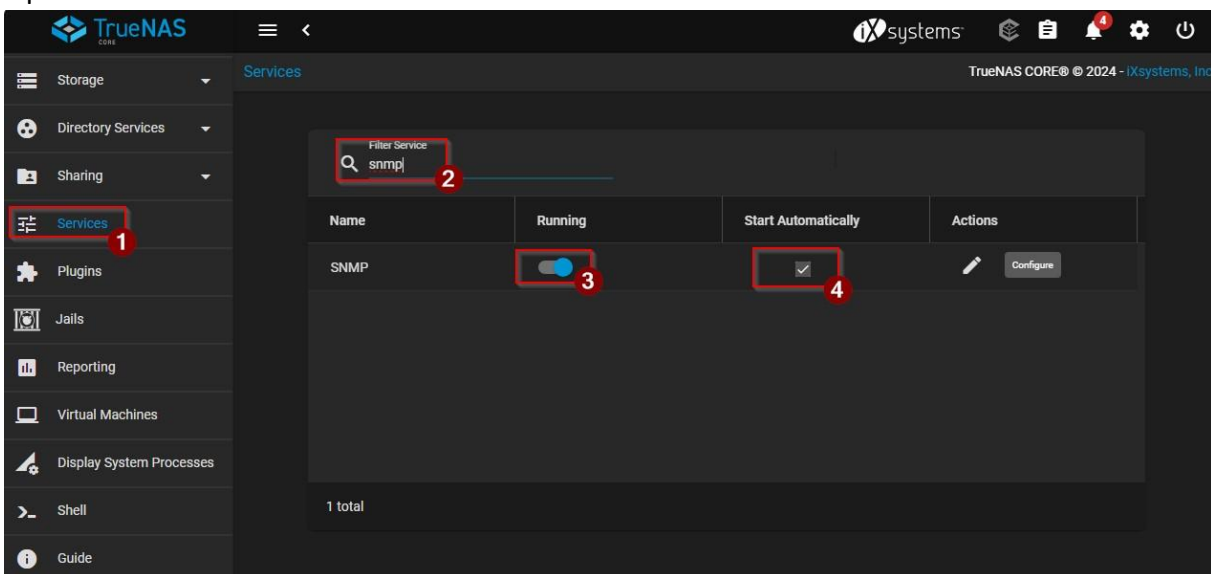
Ajouter Annuler

6 – Ajout de TrueNas dans zabbix

Vue du tableau de bord système de TrueNAS Core (version 13.0).



Activation et configuration du service SNMP dans l'onglet "Services" pour permettre la supervision distante.



Configuration de l'hôte dans Zabbix utilisant le modèle "TrueNAS CORE by SNMP" et l'adresse IP 192.168.30.50.

Nouvel hôte ? x

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte

Nom visible

Modèles Sélectionner
taper ici pour rechercher

* Groupes d'hôtes Sélectionner
taper ici pour rechercher

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
^ SNMP		<input type="text" value="192.168.30.50"/>	<input type="text"/>	<input checked="" type="radio" value="IP"/> IP <input type="radio" value="DNS"/> DNS	<input type="text" value="161"/>	<input checked="" type="radio" value="Supprimer"/> Supprimer

* Version SNMP

* Communauté SNMP

Nombre maximal de répétitions

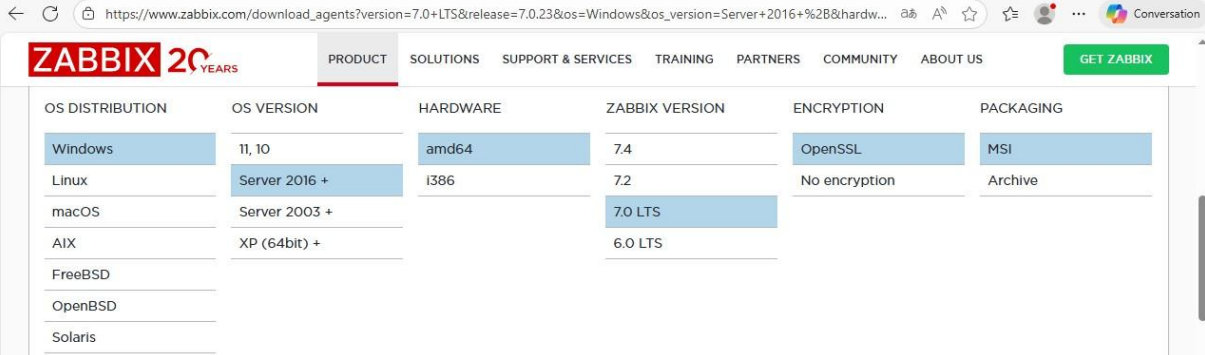
Utiliser des requêtes combinées

[Ajouter](#)


Description

7 – Ajout du SRV2 dans zabbix

Répétition du processus d'installation de l'agent sur le deuxième serveur Windows nommé SRV-AD-2



OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	11, 10	amd64	7.4	OpenSSL	MSI
Linux	Server 2016 +	I386	7.2	No encryption	Archive
macOS	Server 2003 +		7.0 LTS		
AIX	XP (64bit) +		6.0 LTS		
FreeBSD					
OpenBSD					
Solaris					

 zabbix_agent2-7.0.23-windows-amd64-openssl.msi
[Ouvrir un fichier](#)



ZABBIX
The Enterprise-class
Monitoring Solution
for Everyone
www.zabbix.com

Welcome to the Zabbix Agent 2 (64-bit)
Setup Wizard

The Setup Wizard will install Zabbix Agent 2 (64-bit) on your
computer. Click Next to continue or Cancel to exit the Setup
Wizard.

Back Next Cancel

End-User License Agreement

Please read the following license agreement carefully



GNU AFFERO GENERAL PUBLIC LICENSE
Version 3, 19 November 2007

Copyright (C) 2007 Free Software Foundation, Inc. <https://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

I accept the terms in the License Agreement

Print Back **Next** Cancel

Zabbix Agent 2 service configuration

Please enter the information for configure Zabbix Agent 2



Host name:

Zabbix server IP/DNS:

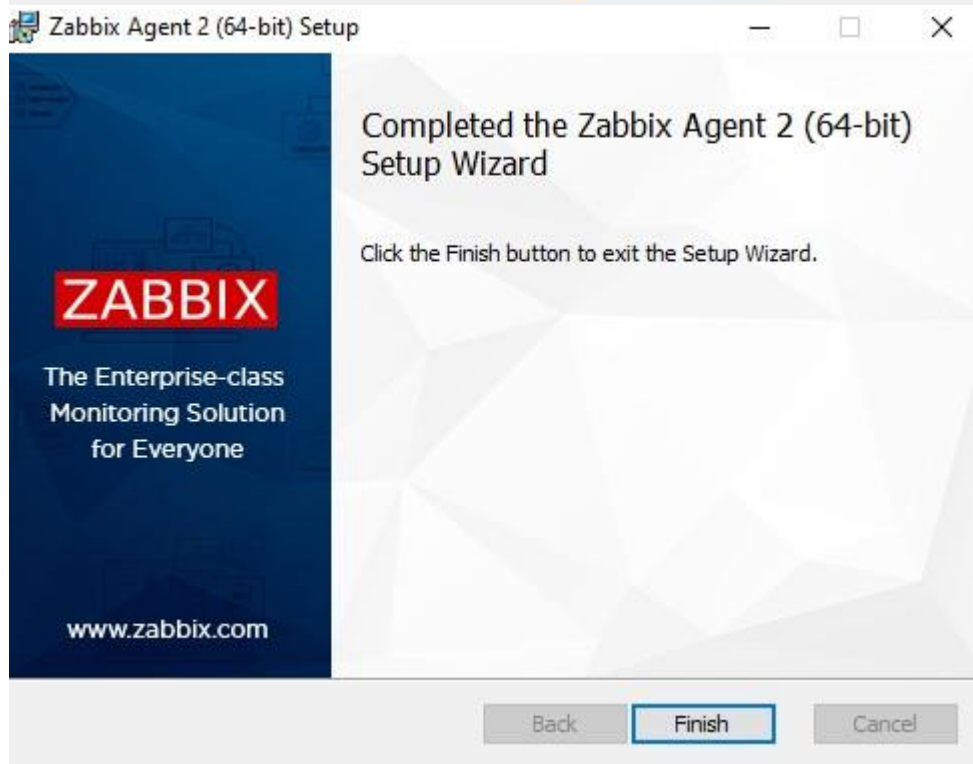
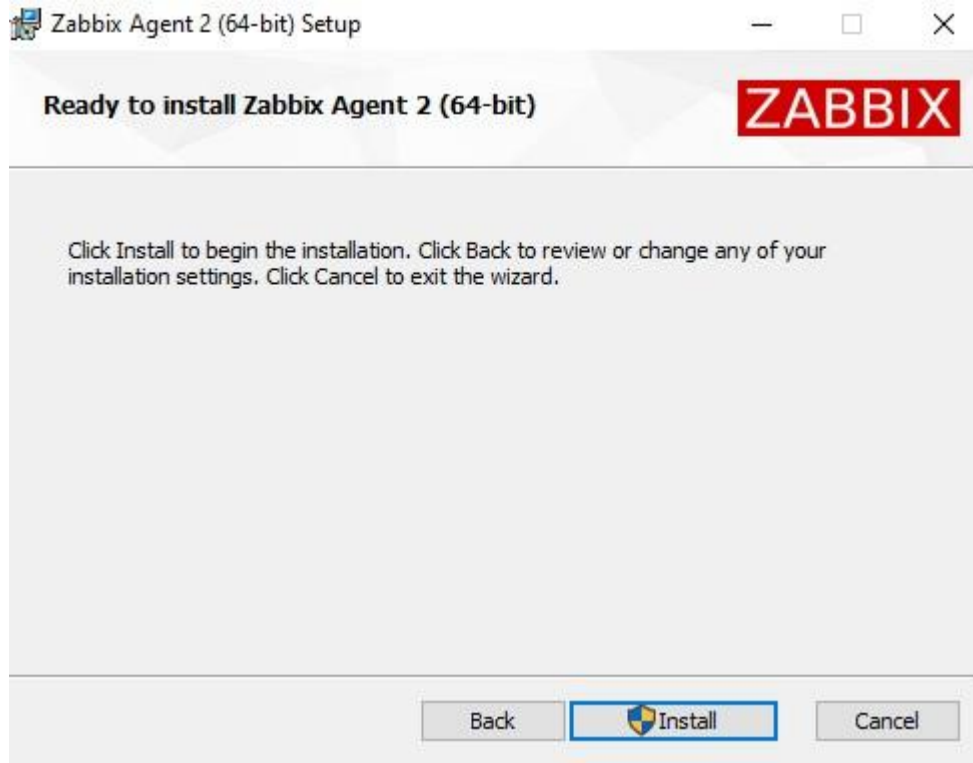
Agent listen port:

Server or Proxy for active checks:

Enable PSK

Add agent location to the PATH

Back **Next** Cancel



Déclaration finale de SRV-AD2 dans la console Zabbix avec l'IP 192.168.30.101

Nouvel hôte ? ✕

[Hôte](#) [IPMI](#) [Tags](#) [Macros](#) [Inventaire](#) [Chiffrement](#) [Table de correspondance](#)

* Nom de l'hôte

Nom visible

Modèles Sélectionner
taper ici pour rechercher

* Groupes d'hôtes Sélectionner
taper ici pour rechercher

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent		<input type="text" value="192.168.30.101"/>	<input type="text"/>	<input checked="" type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio"/> Supprimer

[Ajouter](#)

Description

Surveillé par

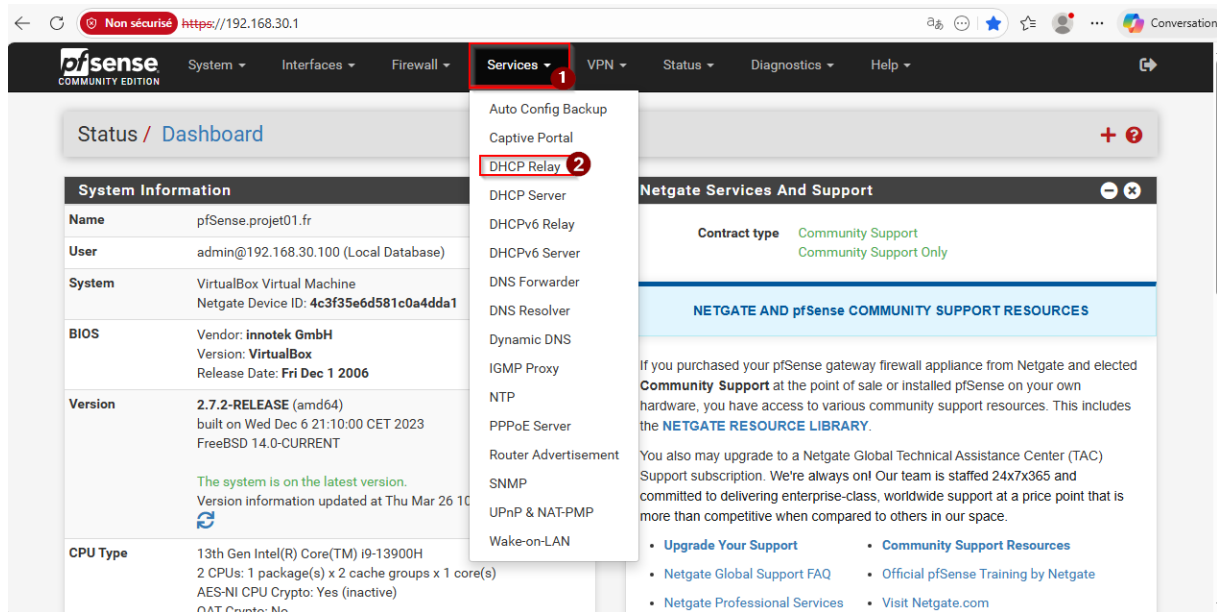
8 – État final des supervisions

Vue récapitulative de tous les équipements supervisés. On constate que tous les hôtes (Debian, PfSense, TrueNas, serveurs et clients Windows) sont "Activés" et que leurs indicateurs de disponibilité (ZBX pour l'agent, SNMP pour le réseau) sont passés au vert.

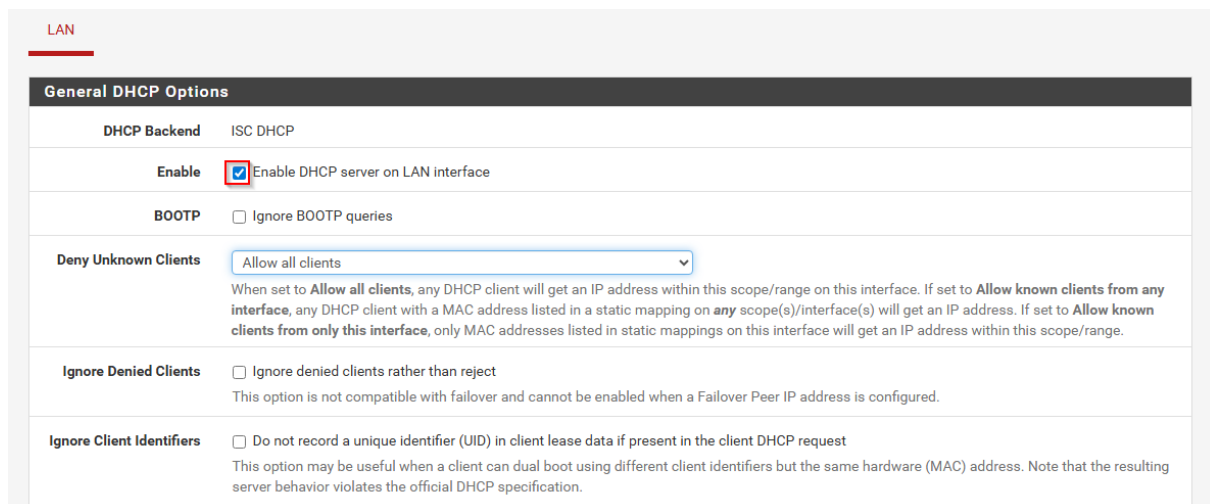
Nom ▲	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques
AD-PROJET1	192.168.30.100:10050	ZBX	class: os target: windows	Activé	Dernières données 116	1	Graphiques 9
Debian	127.0.0.1:10050	ZBX	class: os class: software target: linux ***	Activé	Dernières données 146	Problèmes	Graphiques 14
PfSense	192.168.30.1:161	SNMP	class: software target: pfsense	Activé	Dernières données 74	1	Graphiques 7
SRV-AD2	192.168.30.101:10050	ZBX	class: os target: windows	Activé	Dernières données 103	Problèmes	Graphiques 8
TrueNas	192.168.30.50:161	SNMP	class: hardware target: truenas-core	Activé	Dernières données 101	Problèmes	Graphiques 17
Win10-client	192.168.30.201:10050	ZBX	class: os target: windows	Activé	Dernières données 48	Problèmes	Graphiques 8

3 – Mise en place DHCP

Navigation dans l'interface d'administration de pfSense. Je me rend dans le menu **Services** (1), puis je sélectionne **DHCP Server** (2) pour accéder aux options de configuration de l'adressage automatique.



Dans l'onglet correspondant à l'interface **LAN**, le serveur est activé en cochant la case "**Enable DHCP server on LAN interface**".



Configuration de la **Primary Address Pool**. Le sous-réseau est défini sur 192.168.30.0/24. La plage d'adresses distribuées aux clients est fixée ici de 192.168.30.202 à 192.168.30.245

Primary Address Pool	
Subnet	192.168.30.0/24
Subnet Range	192.168.30.1 - 192.168.30.254
Address Pool Range	<input type="text" value="192.168.30.202"/> <input type="text" value="192.168.30.245"/>
	From To
	The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	<input type="button" value="+ Add Address Pool"/>
	If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Définition des serveurs de noms dans **Server Options**. Le premier serveur DNS renseigné est l'adresse locale de pfSense (192.168.30.1), complété par un DNS externe (Google, 8.8.8.8) pour assurer la résolution de noms.

Server Options	
WINS Servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.30.1"/>
	<input type="text" value="8.8.8.8"/>
	<input type="text" value="DNS Server 3"/>
	<input type="text" value="DNS Server 4"/>

Ces réglages sont pour le contrôle à distance du serveur DHCP, ici je **laisse vide** car pas nécessaire.

OMAPI	
OMAPI Port	<input type="text" value="OMAPI Port"/> Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.
OMAPI Key	<input type="text" value="OMAPI Key"/> <input type="checkbox"/> Generate New Key Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint. Generate a new key based on the selected algorithm.
Key Algorithm	<input type="text" value="HMAC-SHA256 (current bind9 default)"/> Set the algorithm that OMAPI key will use.

Configuration des **Other DHCP Options**. Je confirme la passerelle par défaut (192.168.30.1) et le nom de domaine du réseau (projet01.fr). Le temps de bail par défaut (Default lease time) est réglé sur 7200 secondes.

Other DHCP Options	
Gateway	<input type="text" value="192.168.30.1"/> <small>The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.</small>
Domain Name	<input type="text" value="projet01.fr"/> <small>The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.</small>
Domain Search List	<input type="text" value="example.com;sub.example.com"/> <small>The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.</small>
Default Lease Time	<input type="text" value="7200"/> <small>This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.</small>
Maximum Lease Time	<input type="text" value="86400"/> <small>This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.</small>
Failover peer IP	<input type="text"/> <small>Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primary or Secondary. Ensure the advertising skew for the VIP on one firewall is < 20 and the other is > 20.</small>
Static ARP	<input type="checkbox"/> Enable Static ARP entries <small>Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will be able to communicate with the firewall on this interface. This behavior is enforced even when DHCP server is disabled.</small>

Fin de la page de configuration, je clique sur le bouton **Save** pour enregistrer les paramètres.

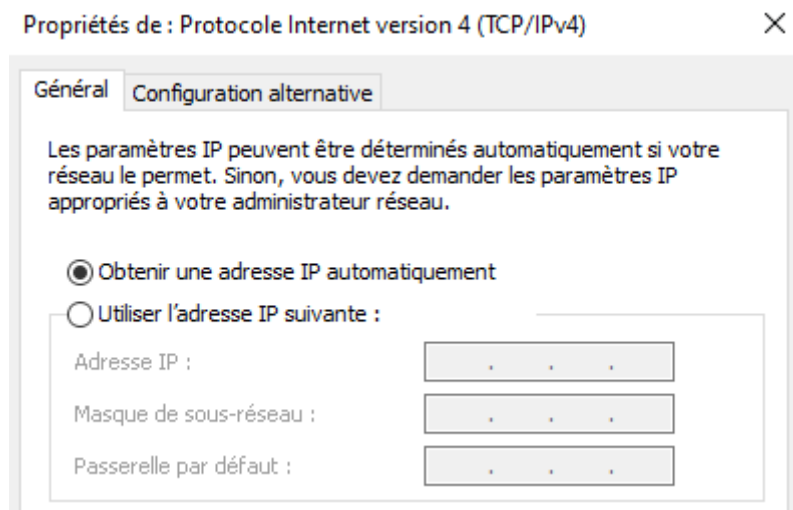
Statistics graphs	<input type="checkbox"/> Enable monitoring graphs for DHCP lease statistics <small>Enable this to add DHCP leases statistics to the Monitoring graphs. Disabled by default.</small>
Ping check	<input type="checkbox"/> Disable ping check <small>When enabled dhcpd sends a ping to the address being assigned, and if no response has been heard, it assigns the address. Enabled by default.</small>
Dynamic DNS	<input type="button" value="Display Advanced"/>
MAC Address Control	<input type="button" value="Display Advanced"/>
NTP	<input type="button" value="Display Advanced"/>
TFTP	<input type="button" value="Display Advanced"/>
LDAP	<input type="button" value="Display Advanced"/>
Network Booting	<input type="button" value="Display Advanced"/>
Custom DHCP Options	<input type="button" value="Display Advanced"/>

Une bannière de confirmation apparaît en haut de l'écran. Il est impératif de cliquer sur **Apply Changes** pour que le serveur DHCP démarre avec la nouvelle configuration.

The DHCP Server configuration has changed.
The changes must be applied for them to take effect.

Test :

Côté client (Windows), dans les propriétés du protocole **TCP/IPv4**, l'option "**Obtenir une adresse IP automatiquement**" doit être sélectionnée pour solliciter le serveur pfSense.



Vérification via l'invite de commande avec ipconfig. Le résultat confirme que le client a bien reçu l'adresse 192.168.30.202 (la première de la plage définie), le masque de sous-réseau est correct, ainsi que le DNS projet01.fr.

```
C:\Windows\system32>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : projet01.fr
    Adresse IPv6 de liaison locale. . . . : fe80::773d:43d5:81:a4dc%6
    Adresse IPv4. . . . . : 192.168.30.202
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.30.1
```

4 – Mise en place d'un script

Présentation du script.ps1. La première section permet la **configuration des variables** (nom, prénom, identifiant, Unité d'Organisation (OU) cible et mot de passe sécurisé).

La seconde partie utilise un bloc try { ... } catch { ... } pour tenter la création de l'utilisateur avec la commande New-ADUser et retourner une erreur explicite en cas d'échec.

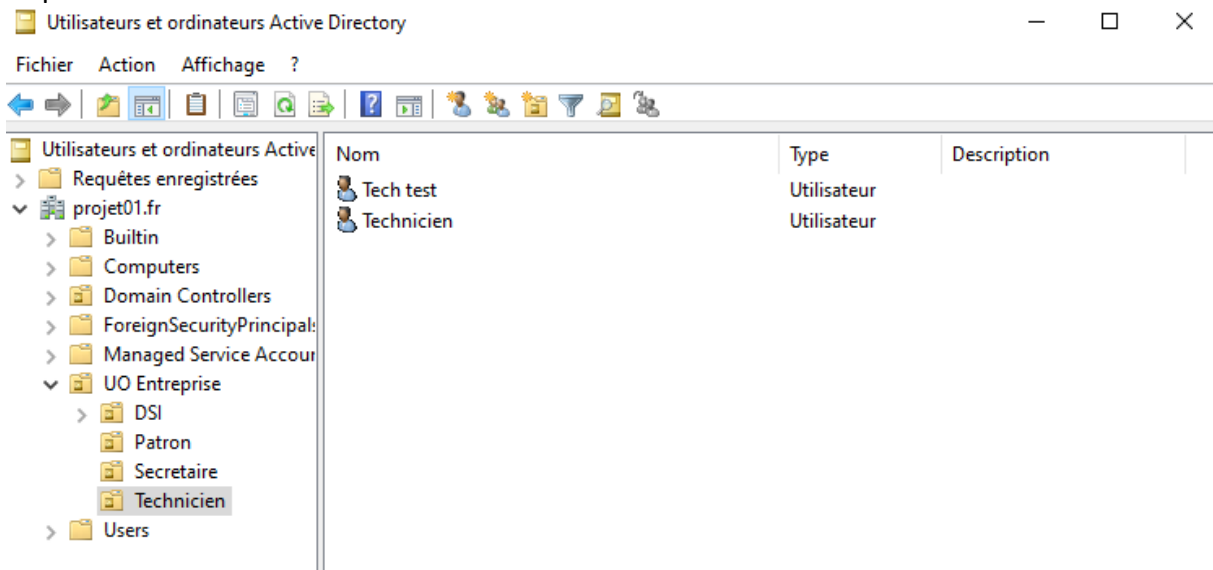
```
script.ps1* X
1 # --- Configuration des variables ---
2 $FirstName = ""
3 $LastName = ""
4 $UserName = ""
5 $OU = "OU=,DC=,DC="
6 $Password = ConvertTo-SecureString "" -AsPlainText -Force
7
8 # --- Création de l'utilisateur ---
9 try {
10 # J'ai retiré le paramètre -UserPrincipalName ici
11 New-ADUser -Name "$FirstName $LastName" `
12           -GivenName $FirstName `
13           -Surname $LastName `
14           -SamAccountName $UserName `
15           -Path $OU `
16           -AccountPassword $Password `
17           -ChangePasswordAtLogon $true `
18           -Enabled $true
19
20 Write-Host "L'utilisateur $UserName a été créé avec succès dans l'OU : $OU" -ForegroundColor Green
21 }
22 catch {
23 Write-Error "Erreur lors de la création de l'utilisateur : $($_.Exception.Message)"
24 }
```

Mise en pratique du script pour un cas concret. Je vais maintenant créer un nouveau technicien pour tester. Le terminal en bas de l'image confirme l'exécution réussie par un message en vert

```
script.ps1 X
1 # --- Configuration des variables ---
2 $FirstName = "Tech"
3 $LastName = "test"
4 $UserName = "techtest"
5 $OU = "OU=Technicien,OU=UO Entreprise,DC=projet01,DC=fr"
6 $Password = ConvertTo-SecureString "MDPtemp*" -AsPlainText -Force
7
8 # --- Création de l'utilisateur ---
9 try {
10 # J'ai retiré le paramètre -UserPrincipalName ici
11 New-ADUser -Name "$FirstName $LastName" `
12           -GivenName $FirstName `
13           -Surname $LastName `
14           -SamAccountName $UserName `
15           -Path $OU `
16           -AccountPassword $Password `
17           -ChangePasswordAtLogon $true `
18           -Enabled $true
19
20 Write-Host "L'utilisateur $UserName a été créé avec succès dans l'OU : $OU" -ForegroundColor Green
21 }
22 catch {
23 Write-Error "Erreur lors de la création de l'utilisateur : $($_.Exception.Message)"
24 }
```

```
PS C:\Users\Administrateur\Desktop> C:\Users\Administrateur\Desktop\script.ps1
L'utilisateur techtest a été créé avec succès dans l'OU : OU=Technicien,OU=UO Entreprise,DC=projet01,DC=fr
```

L'utilisateur "**Tech test**" apparaît bien dans la liste, confirmant que le script a correctement créé et positionné le nouvel utilisateur.



5 - Mise en place de GLPI

GLPI est une solution complète de gestion de parc informatique et d'helpdesk (gestion des tickets). Elle permet de centraliser l'inventaire du matériel, des logiciels et de gérer les interventions techniques au sein d'une infrastructure.

Avant d'installer GLPI, il est nécessaire de configurer un environnement web complet (pile LAMP).

Mise à jour du système :

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

Installation de MariaDB et Apache2 :

```
root@debian:/home/user# sudo apt-get install apache2 php mariadb-server
```

Installation des extensions :

```
root@debian:/home/user# 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-apcu
```

Installation de l'extension ldap pour AD :

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

Sécurisation de la BDD :

```
root@debian:/home/user# sudo mariadb-secure-installation
```

```
NOTE: MariaDB is secure by default in Debian. Running this script is
useless at best, and misleading at worst. This script will be
removed in a future MariaDB release in Debian. Please read
mariadb-server.README.Debian for details.
```

```
Enter root user password or leave blank:
```

```
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] 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
SQL executed without errors!
The operation might have been successful, or it might have not done anything.
```

```
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
SQL executed without errors!
The operation might have been successful, or it might have not done anything.
```

```
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...
SQL executed without errors!
The operation might have been successful, or it might have not done anything.
- Removing privileges on test database...
SQL executed without errors!
The operation might have been successful, or it might have not done anything.
```

```
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!
root@debian:/home/user# |
```

Connexion sur la BDD et création de la base et ajout de l'utilisateur :

```
root@debian:/home/user# sudo mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 73
Server version: 11.8.3-MariaDB-0+deb13u1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

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 db_glpi;
Query OK, 1 row affected (0,002 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON db_glpi.* TO glpi_admin@localhost IDENTIFIED BY "root";
Query OK, 0 rows affected (0,127 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> EXIT
Bye
```

Téléchargement de GLPI :

```
root@debian:/home/user# cd /tmp
root@debian:/tmp# wget https://github.com/glpi-project/glpi/releases/download/11.0.5/glpi-11.0.5.tgz
root@debian:/tmp# sudo tar -xzvf glpi-11.0.5.tgz -C /var/www/|
```

Ajouts des droits et créations des répertoires

```
root@debian:/tmp# sudo chown www-data /var/www/glpi/ -R
root@debian:/tmp# sudo mkdir /etc/glpi
root@debian:/tmp# sudo chown www-data /etc/glpi/
```

Déplacement du répertoire :

```
root@debian:/tmp# sudo mv /var/www/glpi/config /etc/glpi
root@debian:/tmp# sudo mkdir /var/lib/glpi
root@debian:/tmp# sudo mv /var/www/glpi/files /var/lib/glpi
```

Stockage des journaux :

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

Configurer GLPI pour qu'il sache où aller chercher les données :

```
root@debian:/tmp# sudo nano /var/www/glpi/inc/downstream.php
GNU nano 8.4 /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';
}
```

Création d'un second fichier :

```
root@debian:/tmp# sudo nano /etc/glpi/local_define.php
GNU nano 8.4 /etc/glpi/local_define.php *
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi/files');
define('GLPI_LOG_DIR', '/var/log/glpi');
```

Configuration de apache2 :

```
root@debian:/tmp# sudo nano /etc/apache2/sites-available/loris-glpi.local.conf
GNU nano 8.4 /etc/apache2/sites-available/loris-glpi.local.conf *
<VirtualHost *:80>
    ServerName loris-glpi.local

    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 its
    # 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>
```

Activation du site :

```
root@debian:/tmp# sudo a2ensite loris-glpi.local.conf
Enabling site loris-glpi.local.
To activate the new configuration, you need to run:
systemctl reload apache2
```

Désactivation des sites par défaut :

```
root@debian:/tmp# sudo a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Activation du module :

```
root@debian:/tmp# sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

Redémarrage du service apache2 :

```
root@debian:/tmp# sudo systemctl restart apache2
```

Installation de PHP :

```
root@debian:/tmp# apt install php-fpm
Installation de :
  php-fpm

Installation de dépendances :
  php8.4-fpm

Paquets suggérés :
  php-pear

Sommaire :
  Mise à niveau de : 0. Installation de : 2Supprimé : 0. Non mis à jour : 1
  Taille du téléchargement : 1 866 kB
  Espace nécessaire : 6 161 kB / 11,9 GB disponible

Continuer ? [O/n] o
Réception de : 1 http://security.debian.org/debian-security trixie-security/main amd64 php8.4-fpm amd64 8.4.16-1-deb13u1
[1 862 kB]
Réception de : 2 http://deb.debian.org/debian trixie/main amd64 php-fpm all 2:8.4+96 [4 024 B]
16% [1 php8.4-fpm 132 kB/1 862 kB 7%]
```

Activation des deux modules :

```
root@debian:/tmp# sudo a2enmod proxy_fcgi setenvif
Considering dependency proxy for proxy_fcgi:
Enabling module proxy.
Enabling module proxy_fcgi.
Module setenvif already enabled
To activate the new configuration, you need to run:
  systemctl restart apache2
```

```
root@debian:/tmp# sudo apt-get install php-fpm
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
php-fpm est déjà la version la plus récente (2:8.4+96).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
```

Relancer APACHE02 :

```
root@debian:/tmp# sudo systemctl reload apache2
```

Activer `session.cookie_httponly` qui sert à empêcher les scripts malveillants de voler tes sessions.

```
root@debian:/home/user# nano /etc/php/8.4/fpm/php.ini
GNU nano 8.4 /etc/php/8.4/fpm/php.ini *
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 add the httpOnly flag to 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/XSRF)
; Current valid values are "Strict", "Lax" or "None". When using "None",
; make sure to include the quotes, as 'none' is interpreted like 'false' in ini files.
; https://tools.ietf.org/html/draft-west-first-party-cookies-07
session.cookie_samesite =
```

Appliquer les modifications :

```
root@debian:/home/user# sudo systemctl restart php8.4-fpm.service
```

Ajout de PHP-FPM dans le fichier conf

```
root@debian:/home/user# sudo nano /etc/apache2/sites-available/loris-glpi.local.conf
GNU nano 8.4 /etc/apache2/sites-available/loris-glpi.local.conf
<VirtualHost *:80>
    ServerName loris-glpi.local

    DocumentRoot /var/www/glpi/public

    # If you want to place GLPI in a subfolder of your site (e.g. your virtual host is serving m
    # you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT target
    # Alias "/glpi" "/var/www/glpi/public"

    <Directory /var/www/glpi/public>
        Require all granted

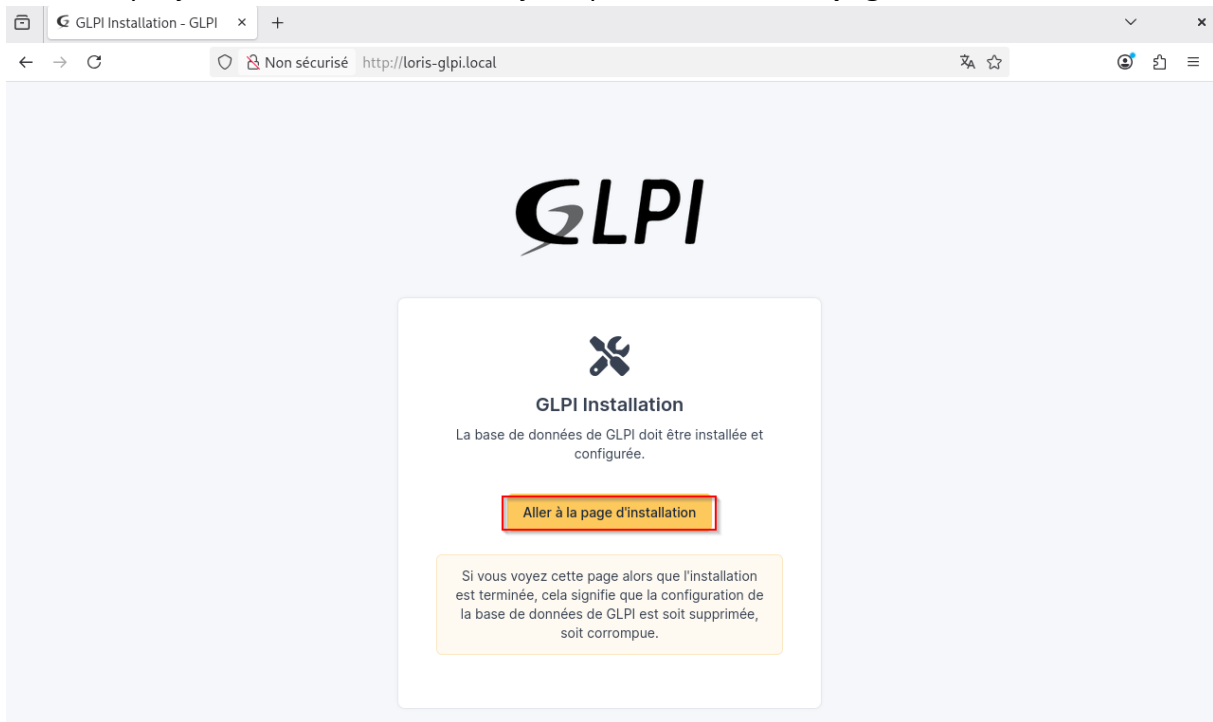
        RewriteEngine On

        # 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/php8.4-fpm.sock|fcgi://localhost/"
    </FilesMatch>
</VirtualHost>
```

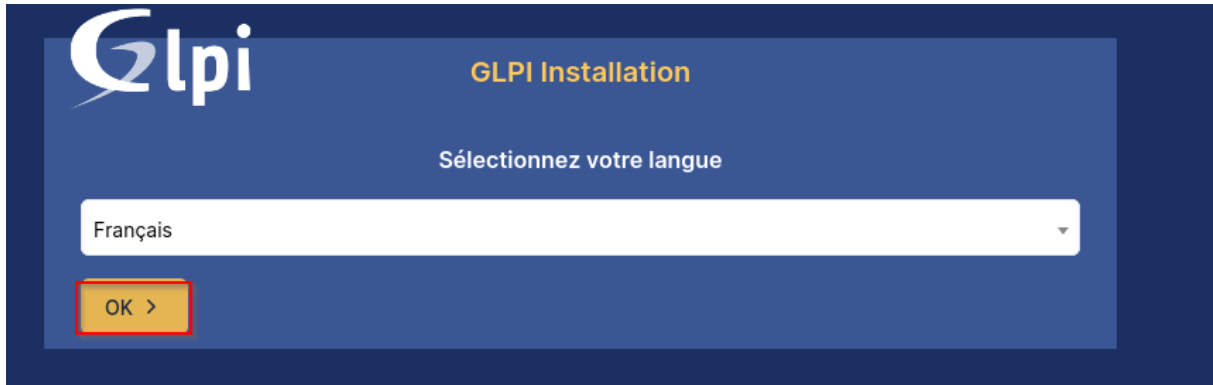
Relancer APACHE02 :

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

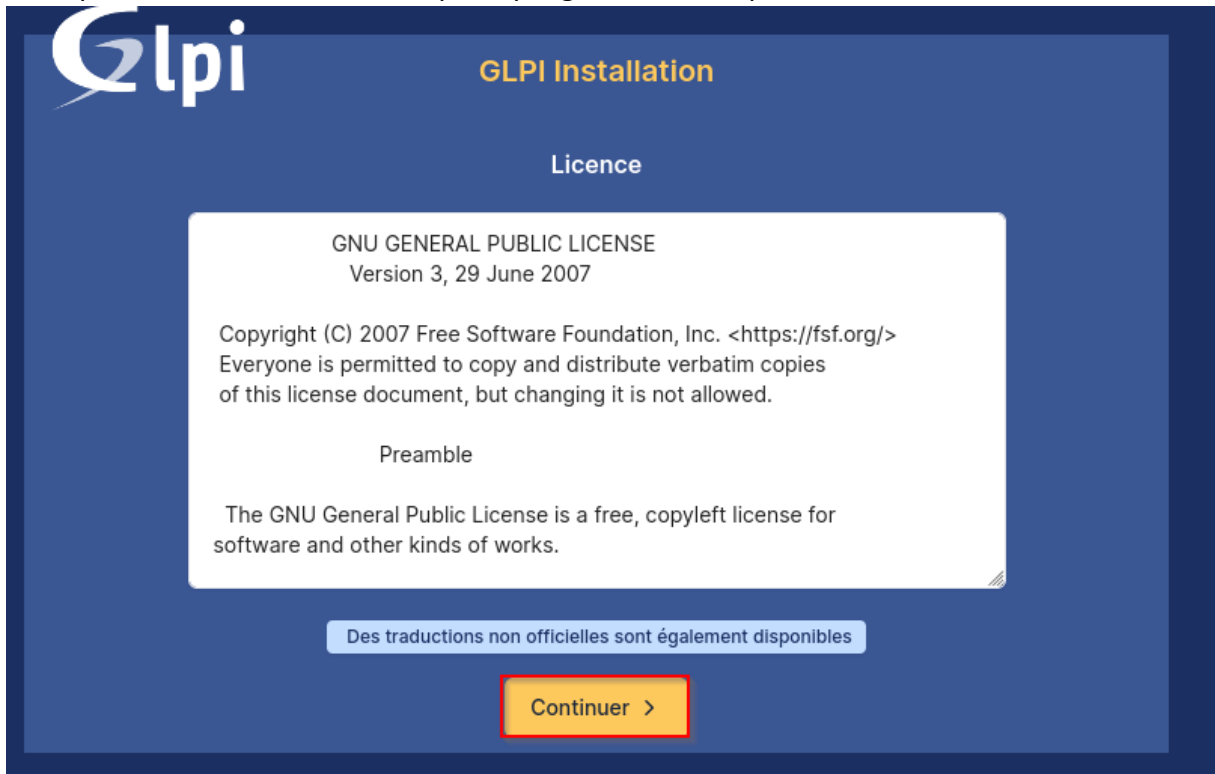
Une fois que je suis sur l'interface web, je clique sur « **Aller à la page d'installation** »



Je sélectionne **Français (France)** pour l'interface d'installation et clique sur "OK".




J'accepte les termes de la licence publique générale GNU pour continuer.



Je clique sur **Installer** pour lancer une création de base de données complète.



L'assistant vérifie la compatibilité de mon serveur (extensions PHP et droits d'écriture). Si tout est "OK", je clique sur **Continuer**.



GLPI Installation

Étape 0

Vérification de la compatibilité de votre environnement avec l'exécution de GLPI

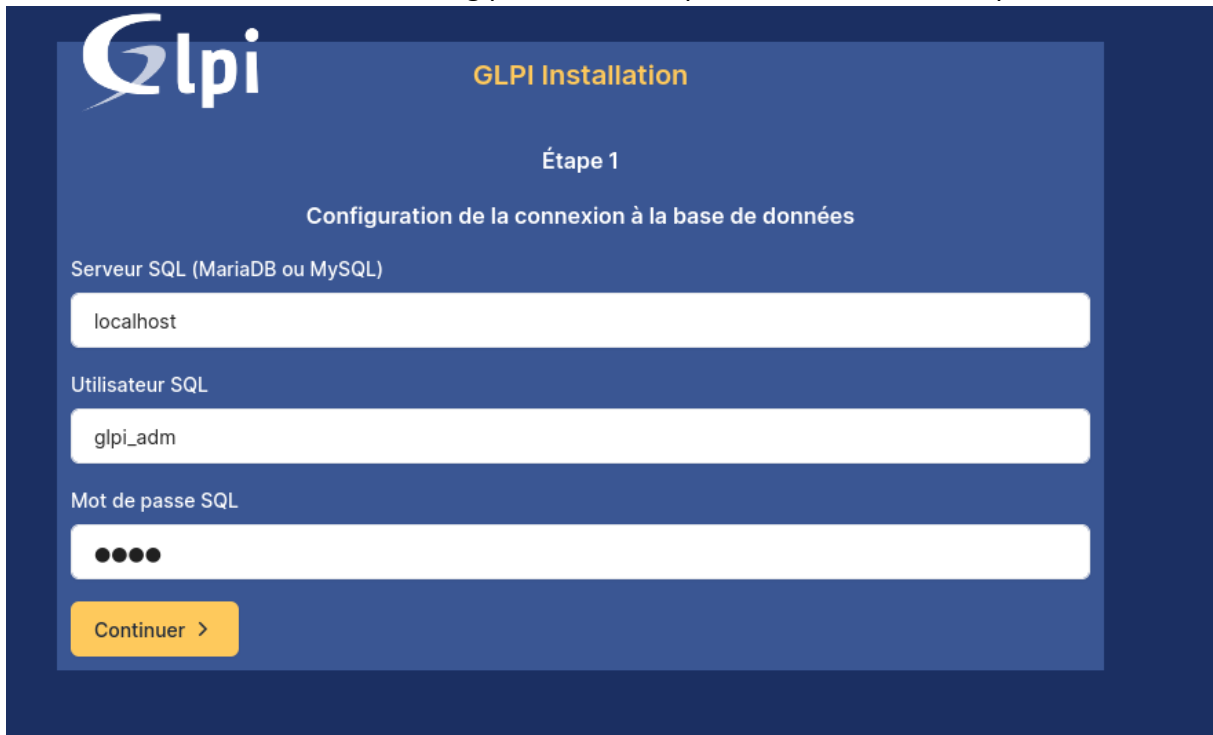
TESTS EFFECTUÉS	RÉSULTATS
Requis Parser PHP	✓
Requis Taille d'entier maximal de PHP <i>Le support des entiers 64 bits est nécessaire pour les opérations relatives aux adresses IP (inventaire réseau, filtrage des clients API, ...).</i>	✓
Requis Configuration des sessions	✓
Requis Mémoire allouée	✓
Requis Extensions du noyau de PHP	✓
Requis mysql extension <i>Requis pour l'accès à la base de données.</i>	✓
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	✓

et l'authentification OAuth 2.0.

Requis Permissions pour les fichiers de log	✓
Requis Permissions pour les dossiers de données	✓
Sécurité Version de PHP maintenue <i>Une version de PHP maintenue par la communauté PHP devrait être utilisée pour bénéficier des correctifs de sécurité et de bogues de PHP.</i>	✓
Sécurité Configuration de sécurité pour les sessions <i>Permet de s'assurer que la sécurité relative aux cookies de session est renforcée.</i>	✓
Suggéré exif extension <i>Renforcer la sécurité de la validation des images.</i>	✓
Suggéré ldap extension <i>Active l'utilisation de l'authentification à un serveur LDAP distant.</i>	✓
Suggéré Extensions PHP pour le marketplace <i>Permet le support des formats de paquets les plus communs dans le marketplace.</i>	✓
Suggéré Zend OPcache extension <i>Améliorer les performances du moteur PHP.</i>	✓
Suggéré Extensions émulées de PHP <i>Améliorer légèrement les performances.</i>	✓
Suggéré Permissions pour le répertoire du marketplace <i>Active l'installation des plugins à partir du Marketplace.</i>	✓

[Continuer >](#)

J'entre l'hôte localhost, l'utilisateur glpi et le mot de passe défini lors de l'étape SQL.



The screenshot shows the 'GLPI Installation' interface at '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 four dots. A yellow 'Continuer >' button is at the bottom.

Je sélectionne la base de données existante nommée glpi que j'ai créé précédemment.



The screenshot shows the 'GLPI Installation' interface at 'Étape 2'. The title is 'Test de connexion à la base de données'. A grey bar with a checkmark and the text 'Connexion à la base de données réussie' is displayed. Below, the text 'Veuillez sélectionner une base de données :' is followed by two options: 'CRÉER UNE NOUVELLE BASE DE DONNÉES :' with an empty input field, and 'OU UTILISER UNE BASE EXISTANTE :'. Under the second option, a radio button is selected next to 'db_glpi', which is highlighted with a red box. A yellow 'Continuer >' button is at the bottom.

Le système prépare les tables. Une fois l'étape terminée, je clique sur **Continuer**.



Glpi **GLPI Installation**

Étape 3

Initialisation de la base de données.

Initialisation des tables de la base de données avec ses données par défaut...

Création de la structure de la base de données...

Initialisation des tables de la base de données avec ses données par défaut...

100 %

- ✓ Structure de la base de données créée.
- ✓ Données par défaut importées.
- ✓ Formulaires par défaut créés.
- ✓ Règles par défaut initialisées.
- ✓ Clefs de sécurités générées.
- ✓ Paramètres par défaut définis.
- ✓ Installation terminée.

Continuer >

Je choisis que je souhaite partager des statistiques d'usage anonymes pour aider le projet GLPI.



GLPI Installation

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 "Télémetrie", qui envoie anonymement, avec votre permission, des données à notre site de télémetrie. 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 Installation

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 Installation

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](#)

L'installation est terminée. L'assistant rappelle les identifiants par défaut : **glpi / glpi**
Je saisi mes identifiants sur la page de login pour accéder à l'application.

Connexion à votre compte

Identifiant
glpi

Mot de passe
●●●●

Source de connexion
Base interne GLPI

Se souvenir de moi

Se connecter

J'accède à l'interface de gestion de parc. Le système est prêt pour la gestion des tickets de support.

Accueil

Rechercher

Super-Admin
Entité racine (Arborescence)

Tableau de bord

Vue personnelle

Vue groupe

Vue globale

Flux RSS

Tous

⚠ Pour des raisons de sécurité, veuillez changer le mot de passe par défaut pour le(s) utilisateur(s) : glpi post-only tech normal

Central

Vous visionnez actuellement des données de démonstration.
Désactiver les données de démonstration

114.7K Logiciels

5.4K Ordinateurs

1.2K Matériels réseau

1.5K Téléphones

130 Licences

3.8K Moniteurs

12 Baies

1.4K Imprimantes

5.4K Ordinateurs par Fabricant

3.5K Moniteurs par Modèle

1.1K Matériels réseau par Statut

Nouveau

Validation

En cours (Attribué)

En cours (Planifié)

En attente

Résolu

Clos

Statuts des tickets par mois

1.5K Tickets

2 Tickets en retard

1.5K Problèmes

1.5K Changements

Navigation dans le menu "Configuration" > "Authentification" pour paramétrer les sources externes.

The screenshot shows the GLPI web interface. The left sidebar menu has "Configuration" highlighted with a red box and a red circle containing the number "1". Below it, "Authentification" is also highlighted with a red box and a red circle containing the number "2". The main content area is titled "Authentifications externes" and contains a list of configuration items: "Configuration", "Annuaire LDAP" (highlighted with a red box and a red circle containing the number "3"), "Serveur mails", and "Autres méthodes d'authentification". The browser address bar shows "http://loris-glpi.local/front/setup.auth.php".

Accès à la gestion des annuaires LDAP pour lier GLPI à un domaine Windows.

The screenshot shows the GLPI web interface for LDAP management. The left sidebar menu has "Configuration" expanded, and "Annuaire LDAP" is highlighted with a red box. The main content area is titled "Annuaire LDAP" and shows a search bar with a red box around the "+" icon. Below the search bar, there is a message "Aucun résultat trouvé" (No results found). The browser address bar shows "http://loris-glpi.local/front/authldap.php".

Configuration des paramètres du serveur AD (nom, IP, filtre de connexion).

Nom

Serveur par défaut Activé

Serveur Port (par défaut 389)

Commentaires

Filtre de connexion

Saisie du DN de base, des identifiants du compte de liaison et des champs de synchronisation.

BaseDN

Utiliser bind ?

DN du compte (pour les connexions non anonymes)

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

Champ de l'identifiant Champ de synchronisation ?

[+ Ajouter](#)

Notification confirmant l'ajout réussi du serveur LDAP SRV-AD1.

Information ✕

Élément ajouté : SRV-AD1
Test réussi

Résultat du test de connexion LDAP montrant que toutes les étapes (flux TCP, Base DN, Bind) sont réussies.

Annuaire LDAP - AD-SRV1 - ID 2

Annuaire LDAP

Tester

Utilisateurs

Groupes

Informations avancées

Réplicats

Historique 2

Tous

Test LDAP Serveur : AD-SRV1

- 1 Flux TCP
Connexion à 192.168.30.100 sur le port 389 réussie
- 2 Base DN
Base DN "DC=projet01,DC=fr" configurée
- 3 LDAP URI
Vérification de l'URI LDAP réussie
- 4 Connexion Bind
Authentification réussie
- 5 Chercher (50 premiers résultats)
Recherche réussie (5 entrées trouvées)

Page de connexion personnalisée utilisant la source LDAP pour un compte technicien.

Authentification - GLPI

Non sécurisé 192.168.30.70

GLPI

Connexion à votre compte

Identifiant

Technicien

Mot de passe

Source de connexion

AD-SRV1

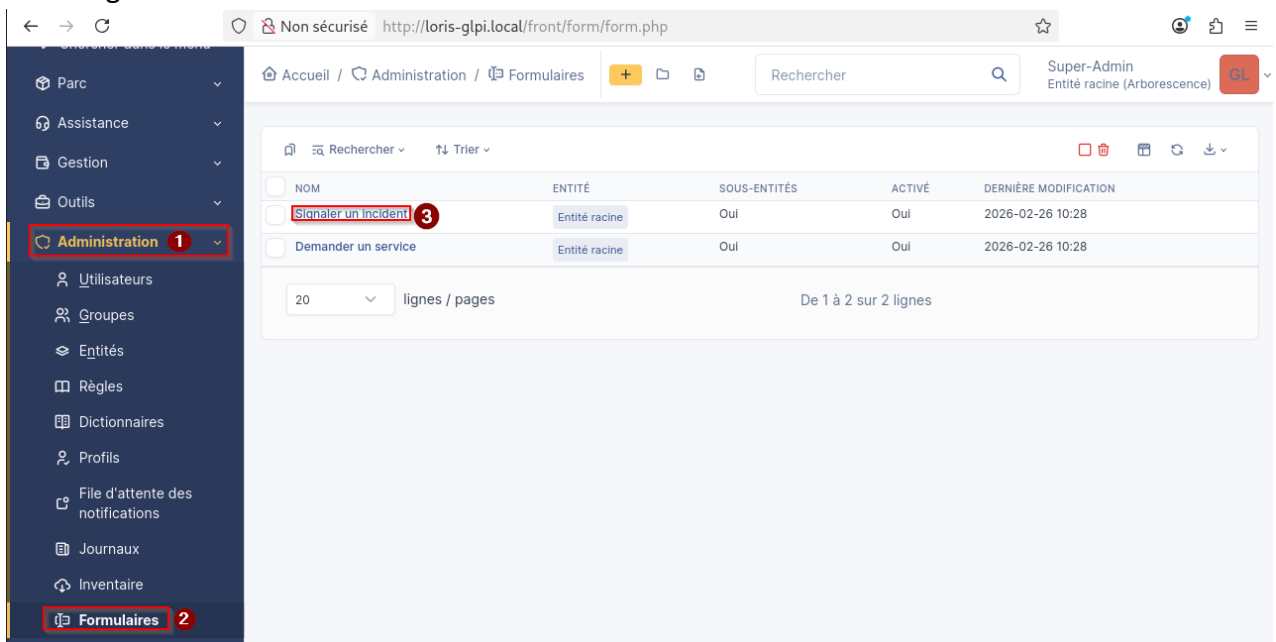
Se souvenir de moi

Se connecter

Interface simplifiée du portail Helpdesk pour les utilisateurs finaux.



Je vais maintenant créer les catégories, et formulaire de création de ticket permettant de définir les catégories d'incidents.



C'est ici que je vais créer mes catégories, matériels de l'utilisateur, lieu ect pour la description du ticket

Formulaire - Signaler un incident - ID 1

Formulaire

Catalogue de services

Contrôles d'accès 1

Destinations 1

Traductions 67

Documents

Historique 14

Signaler un incident Activé

Ajouter une description à votre formulaire...

Urgence

Catégorie

Matériels de l'utilisateur

Propriétés du formulaire

Mise en page

Section par section

Conditions d'affichage du bouton d'envoi

Toujours visible

Prévisualisation

Mettre à la corbeille

Enregistrer

Catégorie

Problème réseau

Problème réseau

Problème matériel

Problème système

Problème logiciel

Test de signalement d'un incident depuis l'interface Helpdesk utilisateur.

Non sécurisé 192.168.30.70/Helpdesk

Conversation

GLPI

Besoin d'aide ? Une question ?

Rechercher des articles de la base de connaissances ou des formulaires

FORMULAIRES 2

Demander un service
Demander un service réalisé par notre équipe.

Signaler un incident
Demander du support auprès de notre équipe helpdesk.



Signaler un incident

Urgence

Basse

Catégorie

Problème réseau

Matériels de l'utilisateur

Ordinateur Fixe

Observateurs

x Technicien

Lieu

Sur site

Titre

Problème réseau (test)



Formulaire envoyé

Votre formulaire a été envoyé avec succès.

[Retour à l'accueil](#)

[Voir mes tickets](#)

Information

Item créé avec succès : Problème réseau (test)

Le ticket remonte bien :

ID	TITRE	STATUT	DERNIÈRE MODIFICATION	DATE D'OUVERTURE	PRIORITÉ	DEMANDEUR - DEMANDEUR	ATTRIBUÉ À - TECHNICIEN	CATÉGORIE	TTR
2	Problème réseau (test)	● Nouveau	2026-04-03 11:59	2026-04-03 11:59	● Basse	Technicien			

Réponse :

Problème réseau (test) (2) 1/2 > >>

Ticket 1

- Statistiques
- Validations
- Base de connaissances
- Éléments
- Coûts
- Projets
- Tâches de projet
- Problèmes
- Changements
- Contrats
- Historique 9
- Tous

T Créé : il y a 5 minutes par Technicien Dernière mise à jour : À l'instant par glpi

Problème réseau (test)

Ceci est un test depuis le poste client

GL Créé : À l'instant par glpi

Bonjour,
Je viens de redémarrer les équipements
Problème résolu ?

Helpdesk

Répondre

Acteurs 2

Demandeur

Technicien 1

Observateur

Technicien 1

Attribué à

Éléments 1

Sauvegarder

La réponse est bien visible coté client

GL Créé : il y a 1 minutes par glpi

Bonjour,
Je viens de redémarrer les équipements
Problème résolu ?

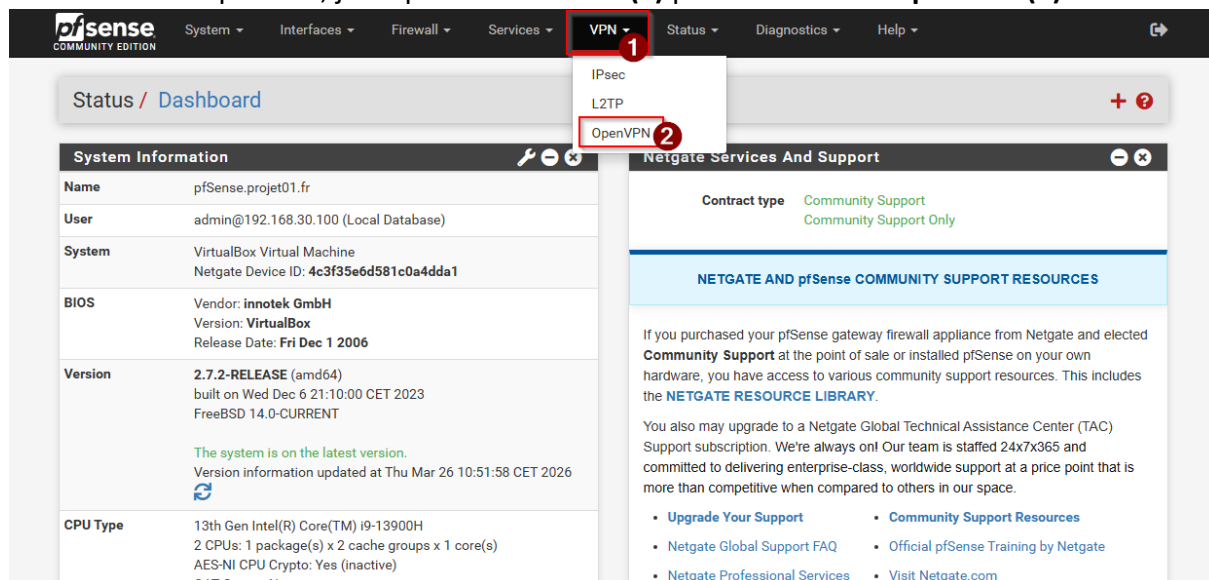
Helpdesk

T Créé : À l'instant par Technicien

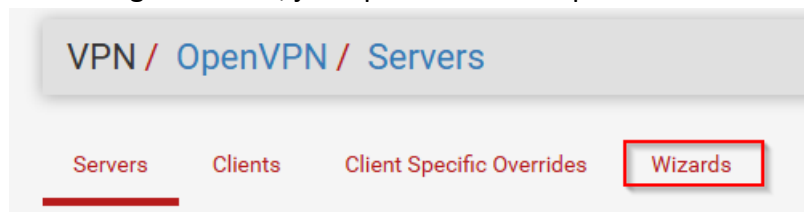
oui merci
bonne journée

6 - Mise en Place d'un accès VPN

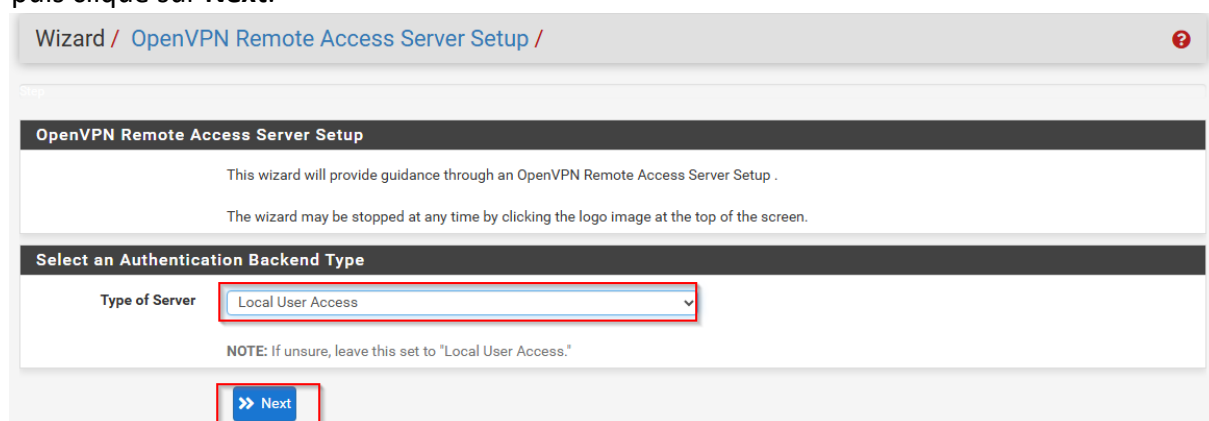
Dans l'interface pfSense, je clique le menu **VPN (1)** puis sélectionne **OpenVPN (2)**



Dans l'onglet **Servers**, je clique sur **Wizards** pour démarrer la configuration guidée.



Pour le mode d'accès distant, je sélectionne **Local User Access** comme moteur d'authentification, puis clique sur **Next**.



Création de l'Autorité de Certification (CA) : * Dans **Descriptive name** je saisis VPN_LO-TECH

Create a New Certificate Authority (CA) Certificate	
Descriptive name	<input type="text" value="VPN_LO-TECH"/> <small>A name for administrative reference, to identify this certificate.</small>
Randomize Serial	<input checked="" type="checkbox"/> Use random serial numbers when signing certificates. <small>When enabled, serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using sequential values.</small>
Key length	<input type="text" value="2048 bit"/> <small>Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com</small>
Lifetime	<input type="text" value="3650"/> <small>Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)</small>
Common Name	<input type="text" value="VPN_LO-TECH"/> <small>The internal name of the CA, used as a part of the CA subject. If left blank, the descriptive name will be used instead.</small>
Country Code	<input type="text" value="FR"/> <small>Two-letter ISO country code (e.g. US, AU, CA)</small>

Sur la sélection du certificat, je clique sur le bouton **Add new Certificate**.

Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection ?

Step 7 of 11

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate

Je ne remplis rien, et je clique directement sur **Create new Certificate**.

Lifetime in days. Server certificates should not have a lifetime over 390 days or some platforms may consider the certificate invalid.

Common Name	<input type="text"/> <small>The internal name of the server certificate, used as a part of the certificate subject. Typically set to the hostname of this system. This value is also used as a Subject Alternative Name (SAN). If left blank, the Descriptive Name value will be used for the Common Name and SAN instead.</small>
Country Code	<input type="text" value="FR"/> <small>Two-letter ISO country code (e.g. US, AU, CA)</small>
State or Province	<input type="text"/> <small>Full State of Province name, not abbreviated (e.g. Texas, Indiana, Ontario).</small>
City	<input type="text"/> <small>City or other Locality name (e.g. Austin, Indianapolis, Toronto).</small>
Organization	<input type="text"/> <small>Organization name, often the company or group name.</small>
Organizational Unit	<input type="text"/> <small>Organizational Unit name, often a department or team name.</small>

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Description

A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Endpoint Configuration

Protocol

Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

Interface

The interface where OpenVPN will listen for incoming connections (typically WAN.)

Local Port

Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

Je ne modifie rien, les options **TLS Authentication** et **Generate TLS Key** sont cochées pour sécuriser les paquets.

Cryptographic Settings

TLS Authentication

 Enable authentication of TLS packets.

Generate TLS Key

 Automatically generate a shared TLS authentication key.

TLS Shared Key

Paste in a shared TLS key if one has already been generated.

DH Parameters Length

Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.

Data Encryption Algorithms

List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.

Fallback Data Encryption Algorithm

Je saisis comme réseau virtuel du VPN :10.0.8.0/24 et je coche Redirect IPv4 Gateway pour forcer tout le trafic du client à travers le tunnel.

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.0.8.0/24"/> <small>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</small>
Redirect IPv4 Gateway	<input checked="" type="checkbox"/> Force all client generated traffic through the tunnel.
IPv4 Local Network	<input type="text" value="192.168.30.0/24"/> <small>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent Connections	<input type="text" value="5"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
Allow Compression	<input type="text" value="Refuse any non-stub compression (Most secure)"/> <small>Allow compression to be used with this VPN instance, which is potentially insecure.</small>
Compression	<input type="text" value="Disable Compression [Omit Preference]"/> <small>Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.</small>
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.

Je configure les adresses DNS fournies aux clients : 192.168.30.1 et 8.8.8.8

Client Settings	
Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Topology	<input type="text" value="Subnet -- One IP address per client in a common subnet"/> <small>Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".</small>

Advanced Client Settings	
DNS Default Domain	<input type="text"/> <small>Provide a default domain name to clients.</small>
DNS Server 1	<input type="text" value="192.168.30.1"/> <small>DNS server IP to provide to connecting clients.</small>
DNS Server 2	<input type="text" value="8.8.8.8"/> <small>DNS server IP to provide to connecting clients.</small>
DNS Server 3	<input type="text"/> <small>DNS server IP to provide to connecting clients.</small>
DNS Server 4	<input type="text"/> <small>DNS server IP to provide to connecting clients.</small>

L'assistant présente les options pour créer les règles de filtrage, cliquer sur « next »

NTP Server	<input type="text"/>
	Network Time Protocol server to provide to connecting clients.
NTP Server 2	<input type="text"/>
	Network Time Protocol server to provide to connecting clients.
NetBIOS Options	<input type="checkbox"/> Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type	<input type="text" value="none"/>
	Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
NetBIOS Scope ID	<input type="text"/>
	A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.
WINS Server 1	<input type="text"/>
	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2	<input type="text"/>
	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
	<input type="button" value="» Next"/>

Je clique sur « next »

Wizard / [OpenVPN Remote Access Server Setup](#) / [Firewall Rule Configuration](#) ?

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Firewall Rules

Rules control passing or blocking network traffic as it flows through the firewall.

Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

Je coche les deux cases **Firewall Rule** (pour autoriser le trafic vers le serveur) et **OpenVPN rule** (pour autoriser le trafic à travers le tunnel), puis clique sur **Next**.

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Firewall Rules

Rules control passing or blocking network traffic as it flows through the firewall.

Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[Next](#)

Je clique sur **Finish** pour valider la configuration complète.

Wizard / OpenVPN Remote Access Server Setup / Finished!

Step 11 of 11

Finished!

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

The configuration is now complete.

Adding users for the VPN depends on the chosen authentication method. For example, add local users with certificates under [System > User Manager](#). For remote authentication servers, add certificates directly in [System > Certificate Manager](#).

To easily export client configurations, browse to [System > Packages](#) and install the OpenVPN Client Export package.

[Finish](#)

Le serveur apparaît désormais dans la liste **VPN > OpenVPN > Servers** avec l'interface WAN et le protocole UDP.

VPN / OpenVPN / Servers

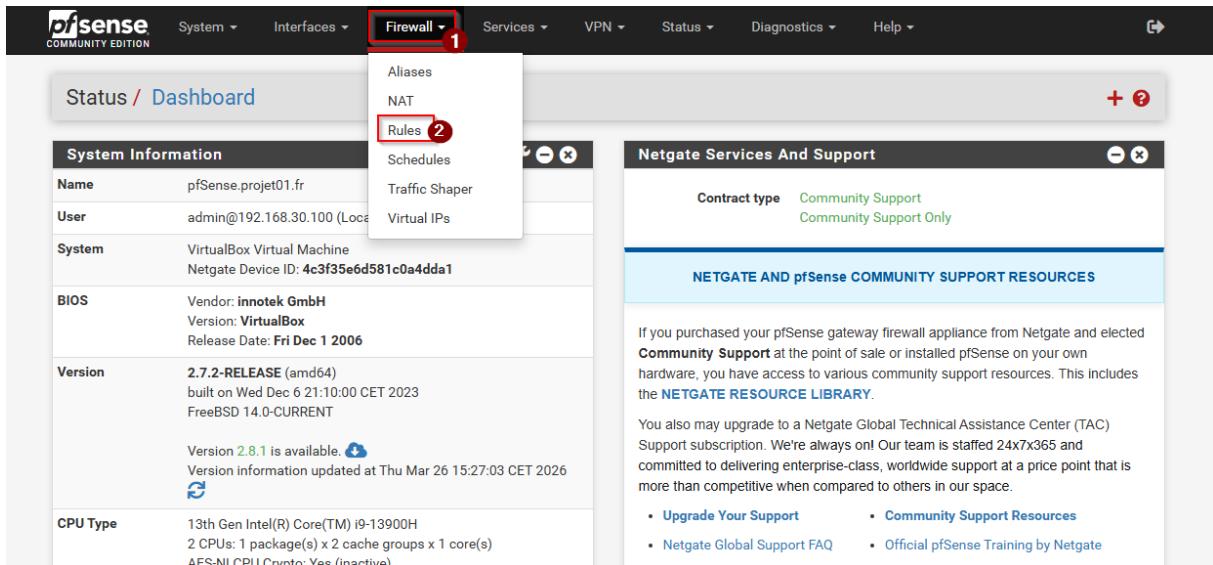
Servers Clients Client Specific Overrides Wizards

OpenVPN Servers

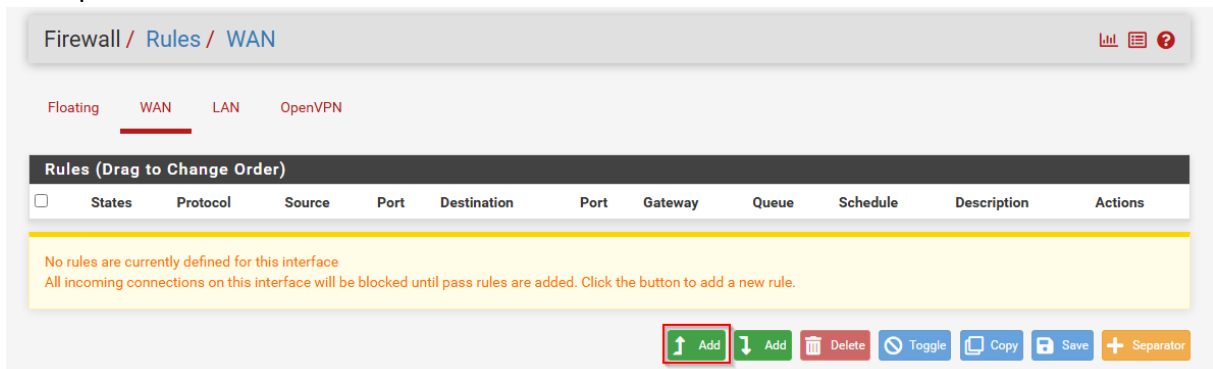
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.8.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	OpenVPN_Remote_Access	Edit Copy Delete

[+ Add](#)

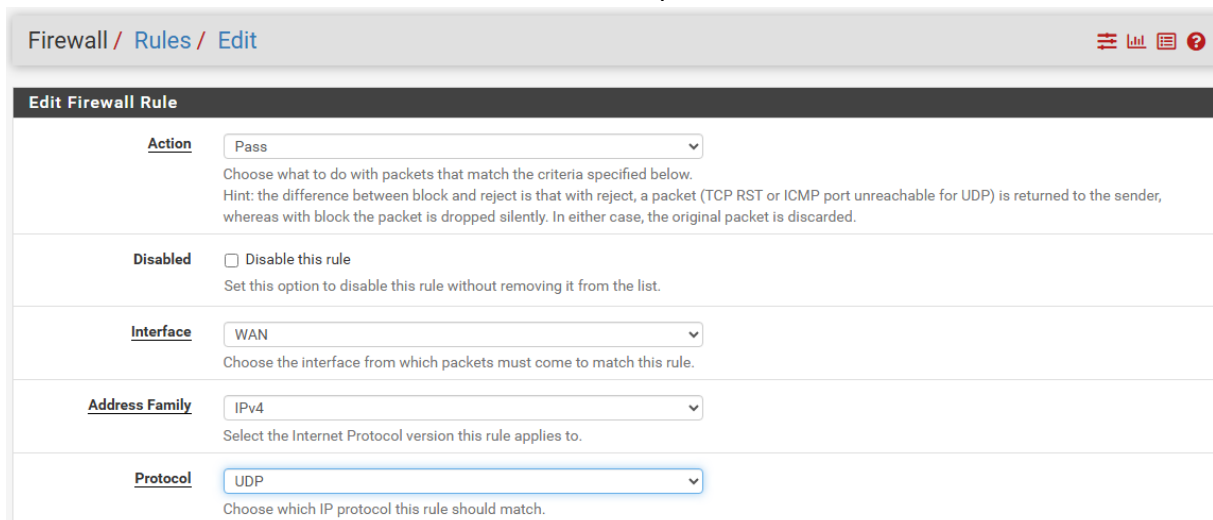
Je me rend à Firewall > Rules.



Je clique sur le bouton Add.



Je sélection en Action "Pass" sur l'interface WAN, protocole UDP.



Port réglé sur OpenVPN (1194).

Source

Invert match Any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Invert match Any Destination Address /

Destination Port Range OpenVPN (1194) OpenVPN (1194)

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description VPN_LO-TECH

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Je clique sur le bouton **Add**.

Firewall / Rules / OpenVPN

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.										

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

Je sélectionne en Action "**Pass**" pour autoriser tout le trafic via le VPN vers le LAN.

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface OpenVPN

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol Any

Choose which IP protocol this rule should match.

Règle nommée "Allow VPN clients to access LAN".

Source

Source Invert match Any Source Address /

Destination

Destination Invert match Any Destination Address /

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Je me rend à System > User Manager.

System 1 Interfaces Firewall Services VPN Status Diagnostics Help

VPN / OpenVPN Servers

Advanced
Certificates
General Setup
High Availability
Package Manager
OpenVPN Servers
Register
Routing
Setup Wizard
Update
User Manager 2
Logout (admin)

Interface	Priority	Network	Mode / Crypto	Description	Actions
WAN	100	192.168.1.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	OpenVPN_Remote_Access	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Je clique sur le bouton Add.

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	<input type="button" value="Edit"/>

Je créer l'utilisateur Technicien et je coche "Click to create a user certificate".

Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="Technicien"/>
Password	<input type="password" value="*****"/> <input type="password" value="*****"/>
Full name	<input type="text" value="Technicien"/> User's full name, for administrative information only
Expiration date	<input type="text"/> Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	<input type="text" value="admins"/> <input type="text"/> Not member of Member of
	<input type="button" value="» Move to 'Member of' list"/> <input type="button" value="« Move to 'Not member of' list"/>
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate

Je nomme vpn-tech.

Create Certificate for User	
Descriptive name	<input type="text" value="vpn-tech"/>
Certificate authority	<input type="text" value="VPN_LO-TECH"/>
Key type	<input type="text" value="RSA"/>
	<input type="text" value="2048"/> The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	<input type="text" value="sha256"/> The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime	<input type="text" value="3650"/>

Je clique sur « Save » pour la validation de la création du compte

Keys	
Authorized SSH Keys	<input type="text"/> Enter authorized SSH keys for this user
IPsec Pre-Shared Key	<input type="text"/>
Shell Behavior	
Keep Command History	<input type="checkbox"/> Keep shell command history between login sessions If this user has shell access, this option preserves the last 1000 unique commands entered at a shell prompt between login sessions. The user can access history using the up and down arrows at an SSH or console shell prompt and search the history by typing a partial command and then using the up or down arrows.
<input type="button" value="Save"/>	

Vue de la liste des utilisateurs (DSI, Patron, Secrétaire, Technicien).

System / User Manager / Users ?

Users Groups Settings Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	DSI	DSI	✓		
<input type="checkbox"/>	Patron	Patron	✓		
<input type="checkbox"/>	Secrétaire	Secrétaire	✓		
<input type="checkbox"/>	Technicien	Technicien	✓		
<input type="checkbox"/>	admin	System Administrator	✓	admins	

+ Add Delete

Je clique sur **Add** pour créer un groupe.

System / User Manager / Groups ?

Users Groups Settings Authentication Servers

Groups

Group name	Description	Member Count	Actions
all	All Users	5	
admins	System Administrators	1	

+ Add

J'ajoute les utilisateurs au nouveau groupe "Lo-Tech".

System / User Manager / Groups / Edit ?

Users Groups Settings Authentication Servers

Group Properties

Group name

Scope
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description
Group description, for administrative information only

Group membership

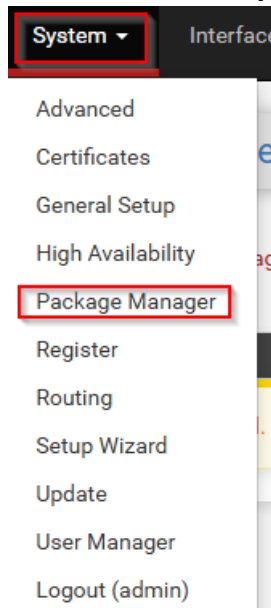
<input type="text" value="admin"/>	<input type="text" value="Technicien"/> DSI Secrétaire Patron
<small>Not members</small>	<small>Members</small>

Move to "Members" Move to "Not members"

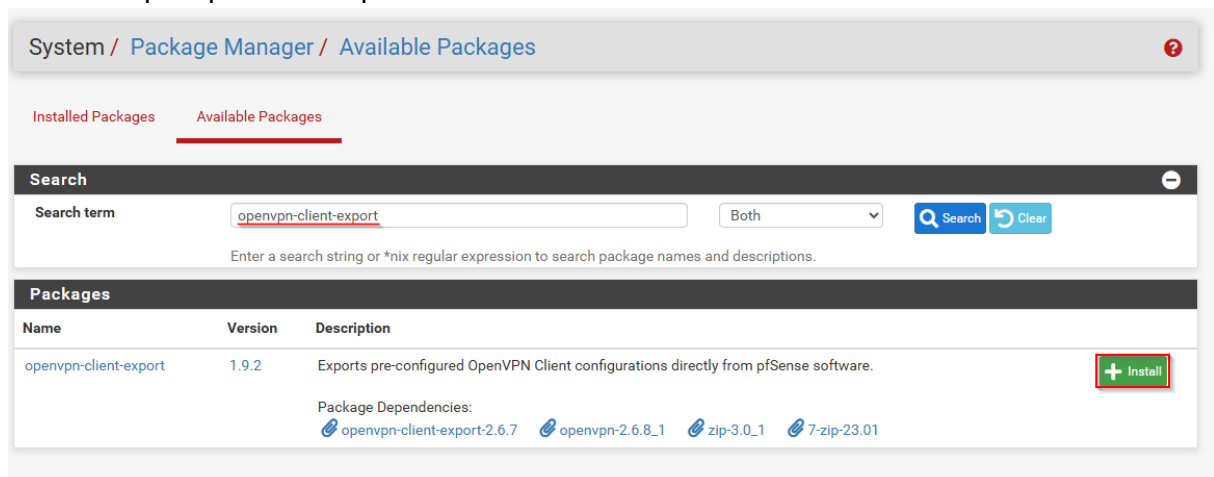
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Save

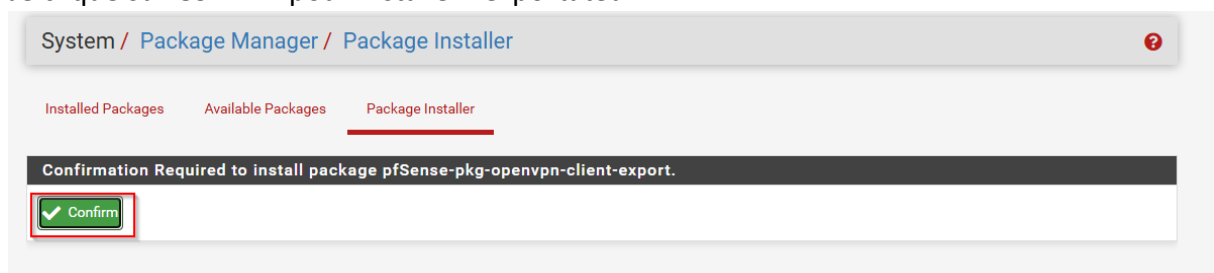
Je me rends dans **System > Package Manager**.



J'installe **openvpn-client-export**.



Je clique sur **Confirm** pour installer l'exportateur.



L'installation est terminée

System / Package Manager / Package Installer

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages **Package Installer**

Package Installation

```
[4/5] Installing 7-zip-23.01...
[4/5] Extracting 7-zip-23.01: ..... done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9.2...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9.2: ..... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```

Accès via le menu VPN.

VPN ▾ Status ▾

- IPsec
- L2TP
- OpenVPN**

Je clique sur l'onglet "Client Export".

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards **Client Export**

Je configure l'IP de l'interface pour l'hôte.

OpenVPN Server

Remote Access Server OpenVPN_Remote_Access UDP4:1194 ▾

Client Connection Behavior

Host Name Resolution Interface IP Address ▾

Verify Server CN Automatic - Use verify-x509-name where possible ▾
Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Legacy Client Do not include OpenVPN 2.5 and later settings in the client configuration.
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer Create Windows installer for unattended deploy.
Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.


Bind Mode Do not bind to the local port ▾
If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

Je clique sur "**Config File Only**" pour télécharger le fichier conf de l'utilisateur Technicien.

Technicien vpn-tech

- Inline Configurations:
 - Most Clients
 - Android
 - OpenVPN Connect (iOS/Android)
- Bundled Configurations:
 - Archive
 - Config File Only**
- Current Windows Installers (2.6.7-ix001):
 - 64-bit
 - 32-bit
- Previous Windows Installers (2.5.9-ix601):
 - 64-bit
 - 32-bit
- Legacy Windows Installers (2.4.12-ix601):
 - 10/2016/2019
 - 7/8/8.1/2012r2
- Viscosity (Mac OS X and Windows):
 - Viscosity Bundle
 - Viscosity Inline Config

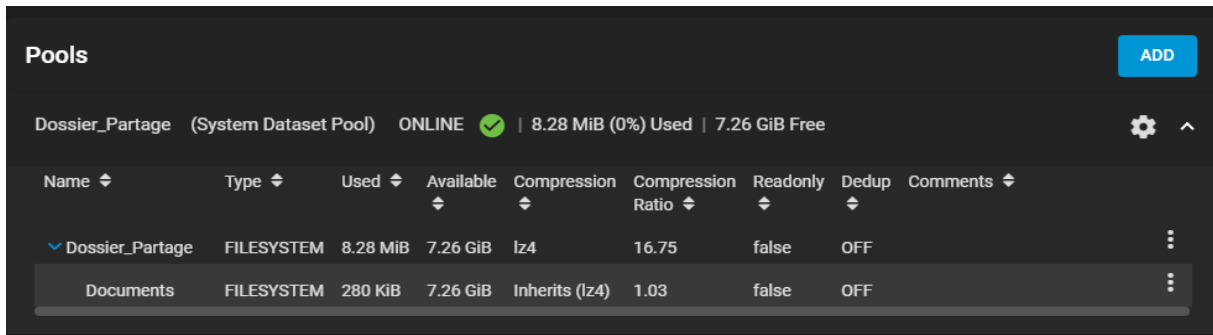
Téléchargement du fichier .ovpn terminé.

 pfSense-UDP4-1194-Technicien-config.ovpn
[Ouvrir un fichier](#)

7 – Mise en place de sauvegardes

1 – Extension du pool de stockage

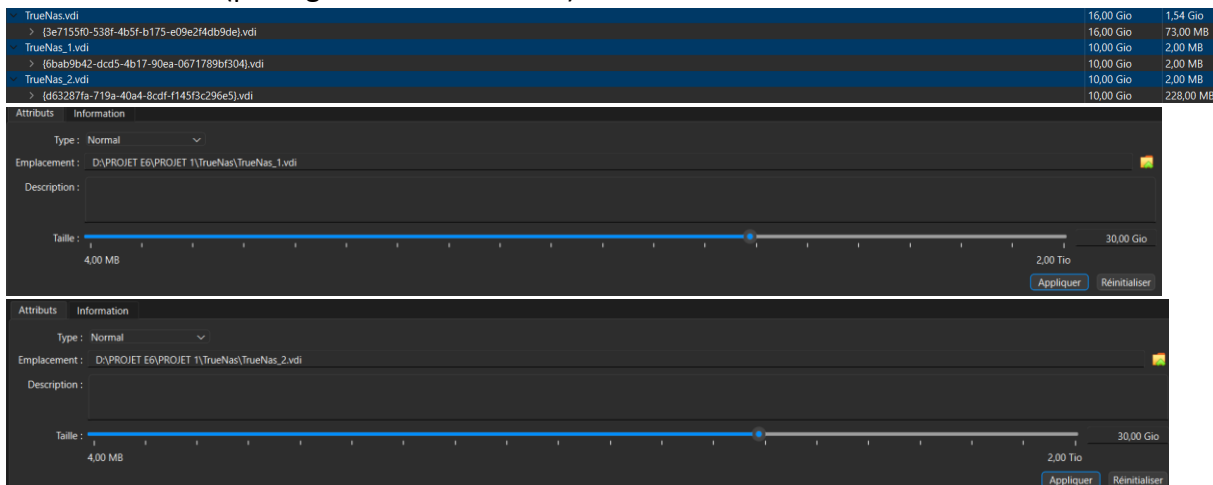
J'observe le menu **Storage > Pools** de TrueNAS. Le pool Dossier_Partage est "ONLINE" avec **7.26 GiB** d'espace libre.



The screenshot shows the TrueNAS Pools management interface. At the top, the 'Dossier_Partage' pool is shown as 'ONLINE' with a green checkmark. It has 8.28 MiB (0%) used and 7.26 GiB free. Below this is a table of datasets:

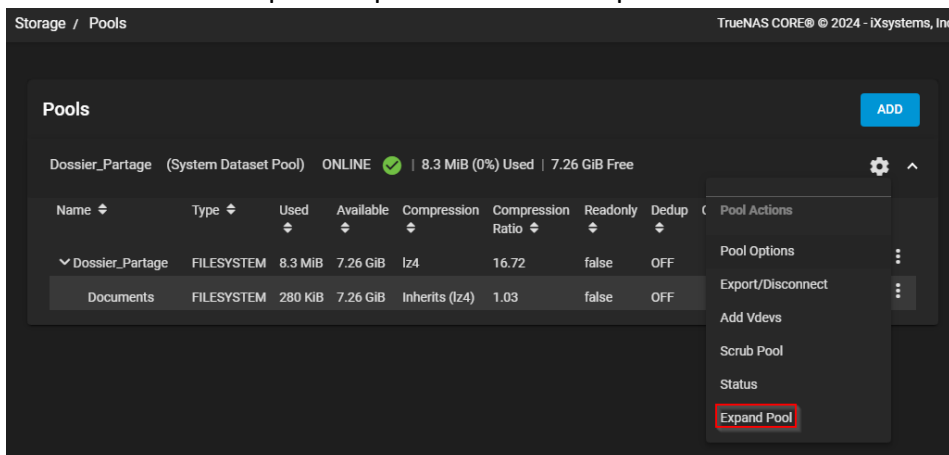
Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
▼ Dossier_Partage	FILESYSTEM	8.28 MiB	7.26 GiB	lz4	16.75	false	OFF	
Documents	FILESYSTEM	280 KiB	7.26 GiB	Inherits (lz4)	1.03	false	OFF	

Les disques virtuels (.vdi) liés à la VM TrueNAS et plus précisément au pool Dossier_Partage sont redimensionnés (passage de 10 Go à 30 Go).



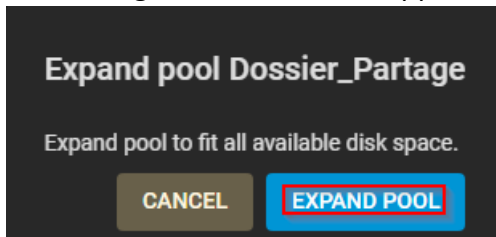
The screenshot shows the configuration for two virtual disks (VDI) in a VM. The top disk is 'TrueNas_1.vdi' and the bottom is 'TrueNas_2.vdi'. Both are currently set to 10.00 GiB. The interface shows a slider for 'Taille' (Size) that has been moved to 30.00 GiB. The 'Appliquer' (Apply) button is visible at the bottom of each configuration panel.

Retour sur l'interface TrueNAS. En cliquant sur la roue crantée (Pool Actions) du pool Dossier_Partage, l'option **Expand Pool** est sélectionnée pour que le système de fichiers ZFS détecte le nouvel espace disponible sur les disques VDI.



The screenshot shows the TrueNAS Pools interface with the 'Dossier_Partage' pool selected. The 'Pool Actions' menu is open, and the 'Expand Pool' option is highlighted with a red box. The pool status is now 'ONLINE' with 8.3 MiB (0%) used and 7.26 GiB free.

Un message de confirmation apparaît pour valider l'extension sur tout l'espace disque disponible.



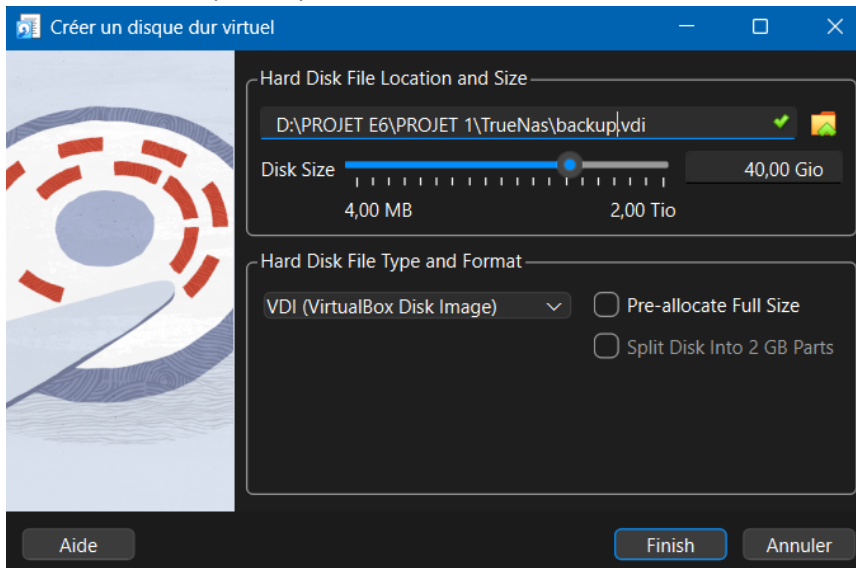
Le pool Dossier_Partage dispose désormais de **26.63 GiB** d'espace libre.

The screenshot shows a "Pools" management interface. At the top right is an "ADD" button. Below it, the "Dossier_Partage" pool is shown as "ONLINE" with a green checkmark. It has "8.59 MiB (0%) Used" and "26.63 GiB Free". A table below lists the datasets within the pool.

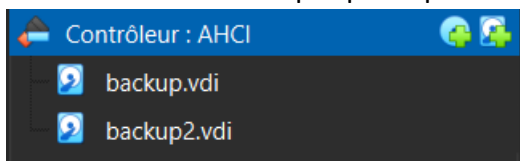
Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
▼ Dossier_Partage	FILESYSTEM	8.59 MiB	26.63 GiB	lz4	17.05	false	OFF	⋮
Documents	FILESYSTEM	280 KiB	26.63 GiB	Inherits (lz4)	1.03	false	OFF	⋮

2 – Création du Pool de sauvegardes

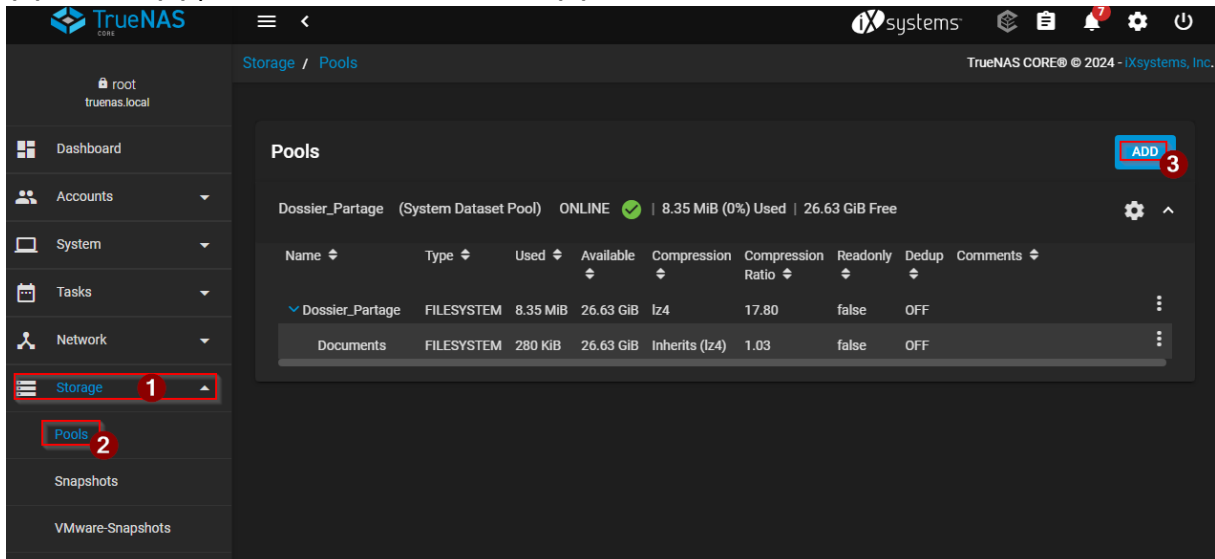
Création de deux nouveaux disques virtuels de **40 Go** (fichiers backup.vdi et backup2.vdi) afin de faire un RAID 1 (miroir)



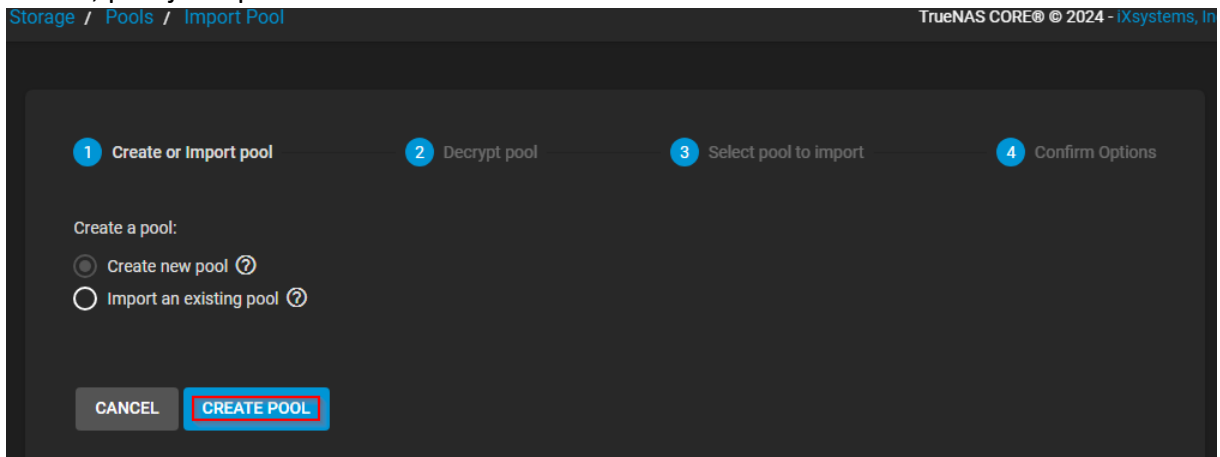
Ajout d'un contrôleur **AHCI (SATA)** dans VirtualBox pour gérer ces nouveaux disques, car l'IDE est limitée en nombre de périphériques.



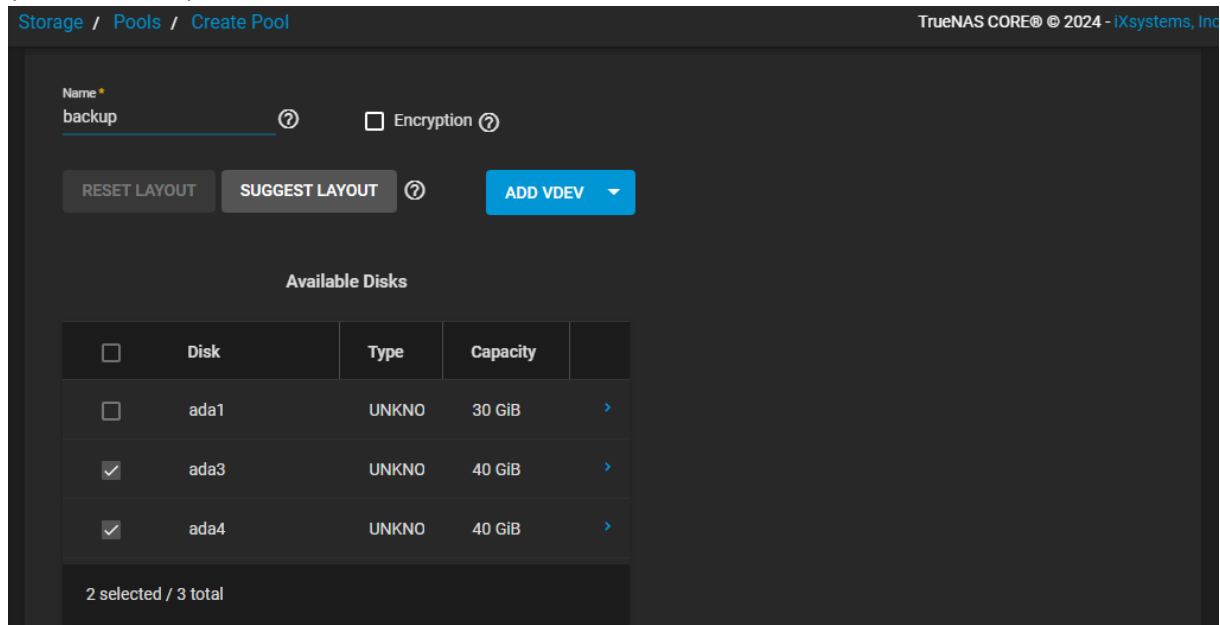
Une fois les disques créés, je vais créer un nouveau pool, dans TrueNAS, navigation vers **Storage (1) > Pools (2)** puis clic sur le bouton **ADD (3)** en haut à droite.



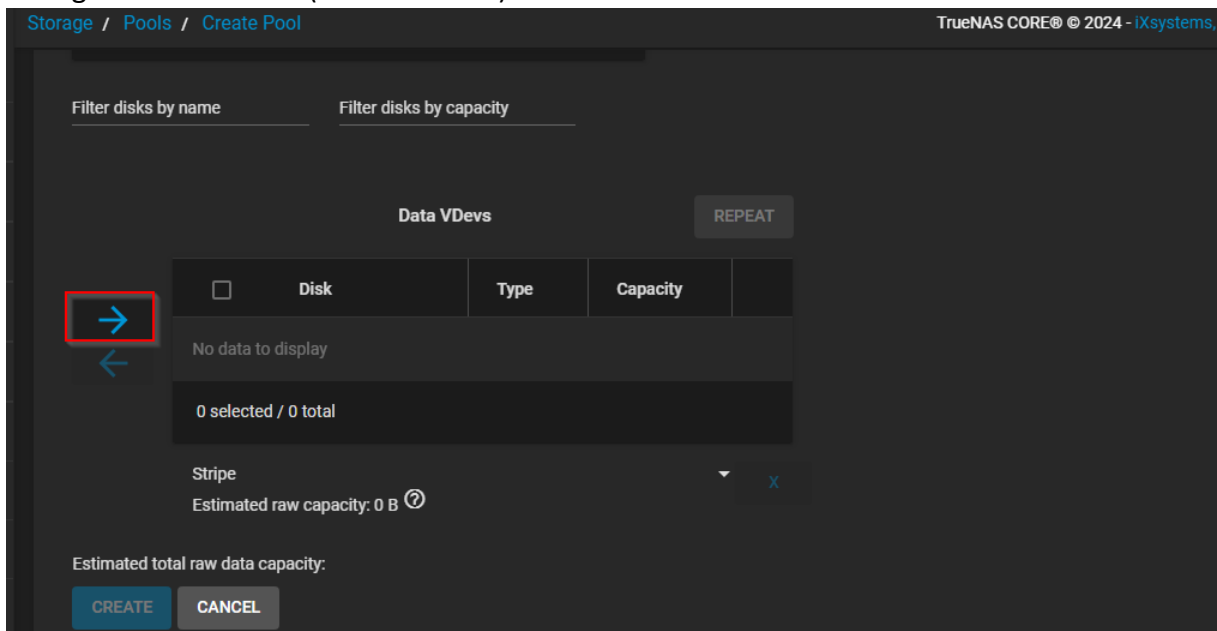
L'assistant propose de créer ou d'importer un pool. L'option **Create new pool** est cochée par défaut, puis je clique sur **CREATE POOL**.



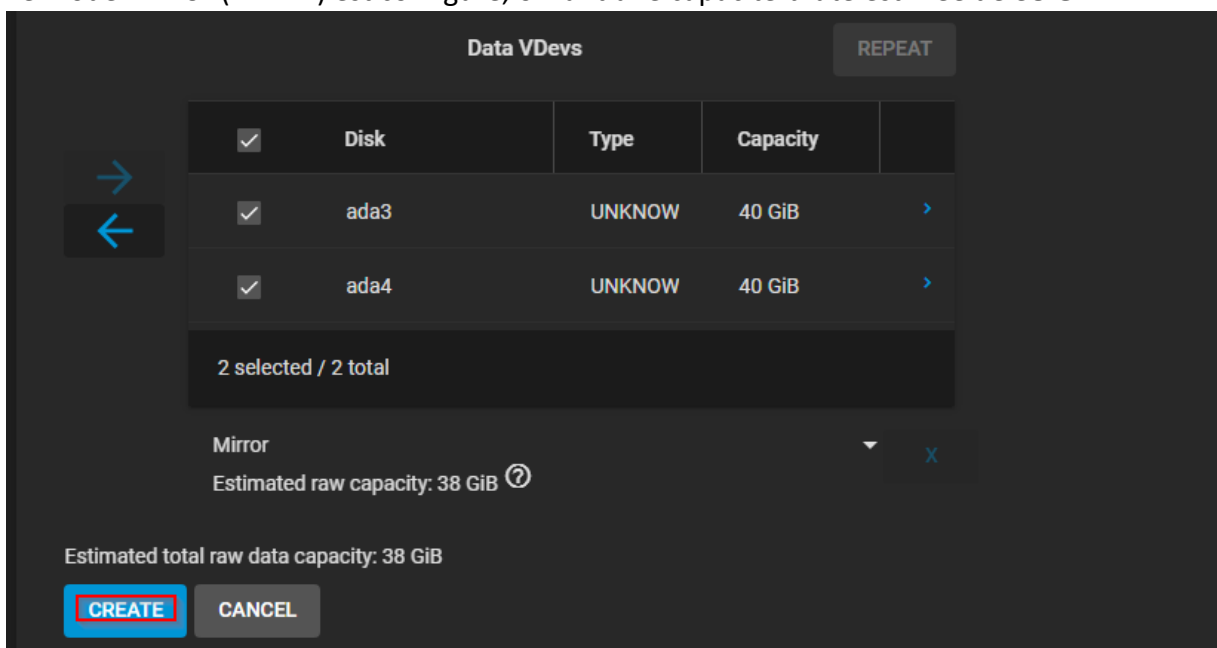
Le pool est nommé backup. Dans la liste des disques disponibles, les deux disques de 40 GiB (ada3 et ada4) sont sélectionnés.



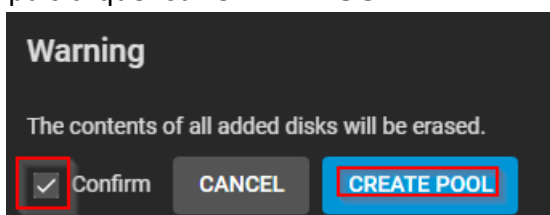
Je clique sur la flèche vers la droite pour déplacer les disques sélectionnés vers la section de configuration du VDEV (Virtual Device).



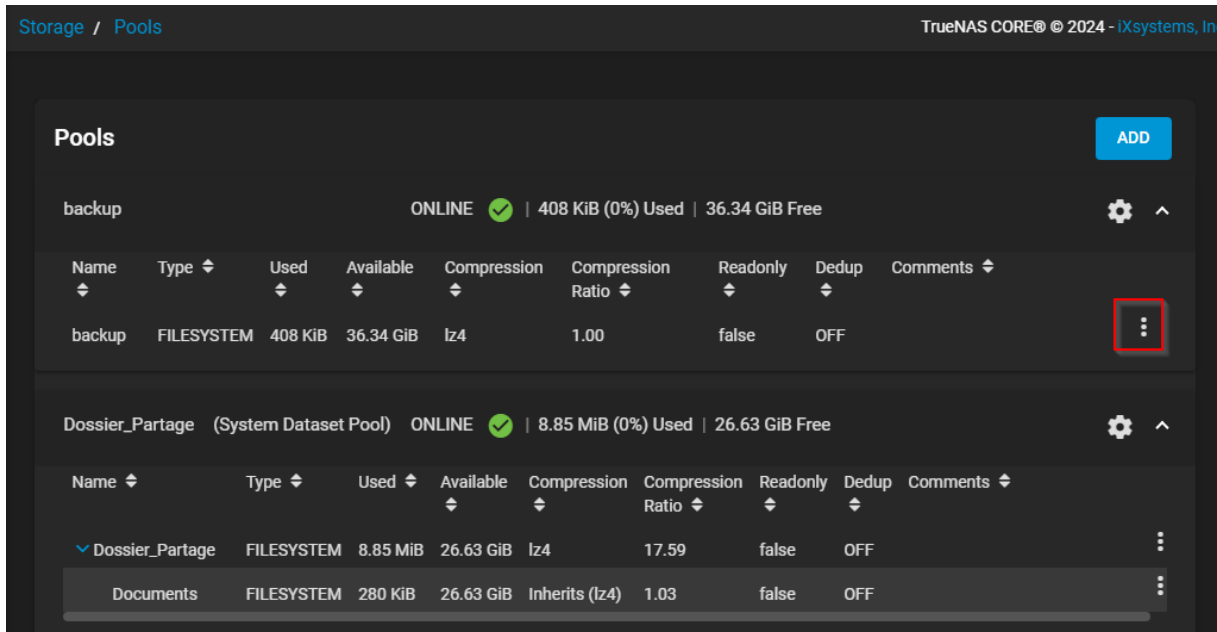
Le mode **Mirror** (RAID 1) est configuré, offrant une capacité brute estimée de **38 GiB**



Une fenêtre "Warning" prévient que le contenu des disques sera effacé. Il faut cocher **Confirm** puis cliquer sur **CREATE POOL**.



Le pool backup apparaît désormais dans la liste, "ONLINE", avec **36.34 GiB** libres. je clique sur les trois points verticaux à droite du pool pour gérer les datasets.



Storage / Pools TrueNAS CORE® © 2024 - iXsystems, Inc.

Pools ADD

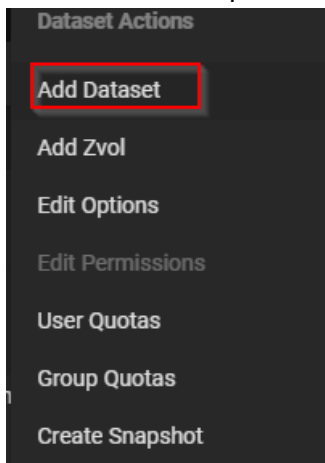
backup ONLINE ✓ | 408 KiB (0%) Used | 36.34 GiB Free ⚙️ ^

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments	
backup	FILESYSTEM	408 KiB	36.34 GiB	lz4	1.00	false	OFF		⋮

Dossier_Partage (System Dataset Pool) ONLINE ✓ | 8.85 MiB (0%) Used | 26.63 GiB Free ⚙️ ^

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments	
▼ Dossier_Partage	FILESYSTEM	8.85 MiB	26.63 GiB	lz4	17.59	false	OFF		⋮
Documents	FILESYSTEM	280 KiB	26.63 GiB	Inherits (lz4)	1.03	false	OFF		⋮

Je sélectionne l'option **Add Dataset** dans la liste des actions.



Dataset Actions

- Add Dataset**
- Add Zvol
- Edit Options
- Edit Permissions
- User Quotas
- Group Quotas
- Create Snapshot

Le nom "Sauvegarde" est saisi. Les autres options (compression, chiffrement) sont laissées en héritage par défaut. On valide par **SUBMIT**.

The screenshot shows the 'Add Dataset' configuration page in TrueNAS. The 'Name and Options' section has 'Name' set to 'Sauvegarde'. The 'Encryption Options' section has 'Inherit (non-encrypted)' checked. The 'Other Options' section has 'ZFS Deduplication' set to 'Inherit (off)', 'Data Sensitivity' set to 'Sensitive', and 'Share Type' set to 'Generic'. At the bottom, there are 'SUBMIT', 'CANCEL', and 'ADVANCED OPTIONS' buttons.

Sharing > Windows Shares (SMB) > Add, pour ajouter un partage smb

The screenshot shows the 'Add' page for Windows Shares (SMB) in TrueNAS. The left sidebar has 'Sharing' (1) and 'Windows Shares (SMB)' (2) highlighted. The main area shows a table with one entry: 'Documents' at path '/mnt/Dossier_Partage/Documents' with 'Enabled' set to 'yes'. An 'ADD' button (3) is in the top right.

Je sélectionne le chemin /mnt/backup/Sauvegarde via l'explorateur de fichiers intégré. Je valide par **SUBMIT**.

The screenshot shows the 'Basic' configuration page for an SMB share. The 'Path' field is set to '/mnt/backup/Sauvegarde'. The 'Name' field is set to 'Sauvegarde'. The 'Purpose' dropdown is set to 'Default share parameters'. The 'Enabled' checkbox is checked. At the bottom, there are 'SUBMIT', 'CANCEL', and 'ADVANCED OPTIONS' buttons.

L'utilisateur **patron** est défini comme propriétaire avec un accès de type **Allow**.

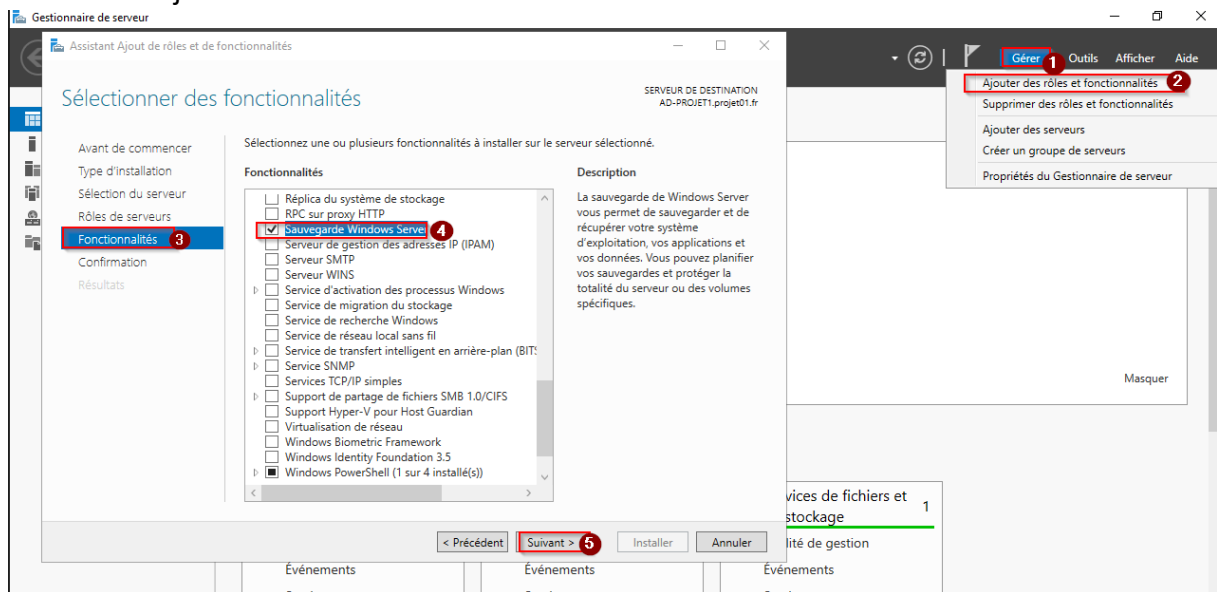
The screenshot shows two panels. The left panel, titled "File Information", displays the path "/mnt/backup/Sauvegarde", the user "root", and the group "wheel". There are checkboxes for "Apply User" and "Apply Group", both currently unchecked. The right panel, titled "Access Control List", shows a list of entries. The first entry is "User" with a dropdown arrow and a help icon. The second entry is "User" with the value "patron" selected in the dropdown. The third entry is "ACL Type" with the value "Allow" selected. The fourth entry is "Permissions Type" with the value "Advanced" selected. The fifth entry is "Permissions" with the value "Read Data, Write Data, Append Data, Read Named Attributes,..." selected.

Les permissions sont appliquées de manière **récursive** pour inclure tous les sous-dossiers futurs.

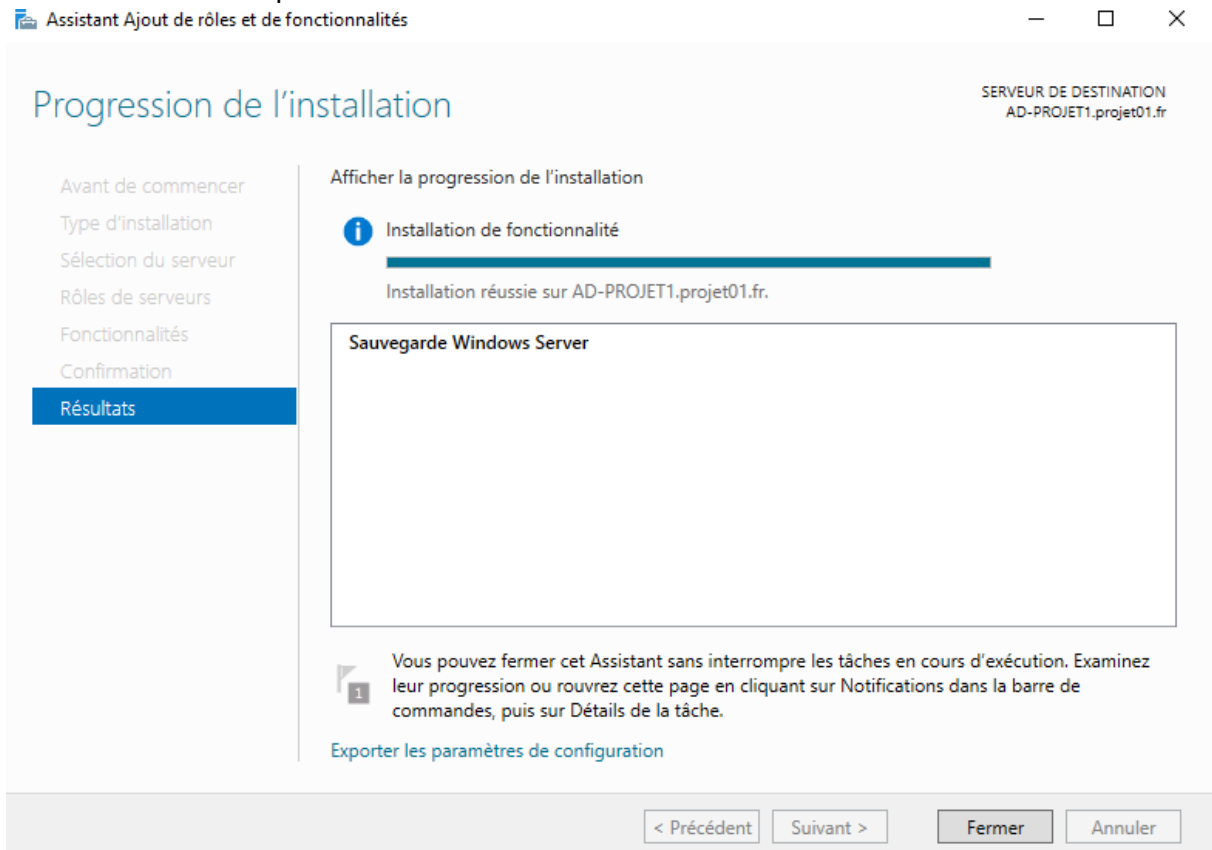
The screenshot shows a dialog box titled "Advanced". It contains two checkboxes: "Apply permissions recursively" which is checked and highlighted with a red box, and "Apply permissions to child datasets" which is unchecked. At the bottom of the dialog, there are three buttons: "SAVE" (highlighted with a red box), "CANCEL", and "USE PERMISSIONS EDITOR".

3 – Sauvegarde du SRV-AD1

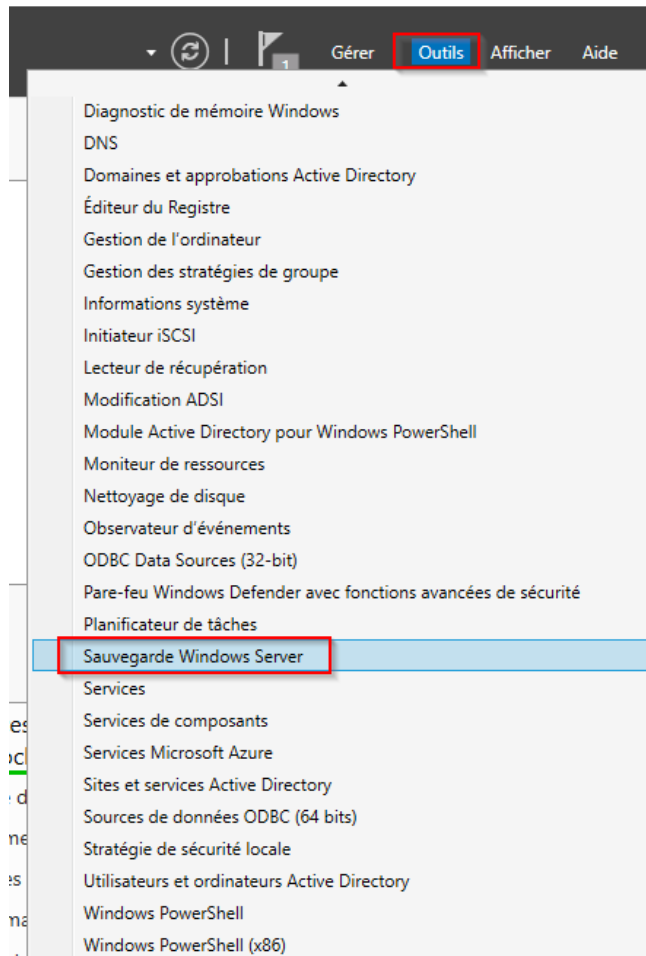
Dans le Gestionnaire de serveur, j'ajoute la fonctionnalité **Sauvegarde Windows Server** via l'assistant "Ajouter des rôles et fonctionnalités".



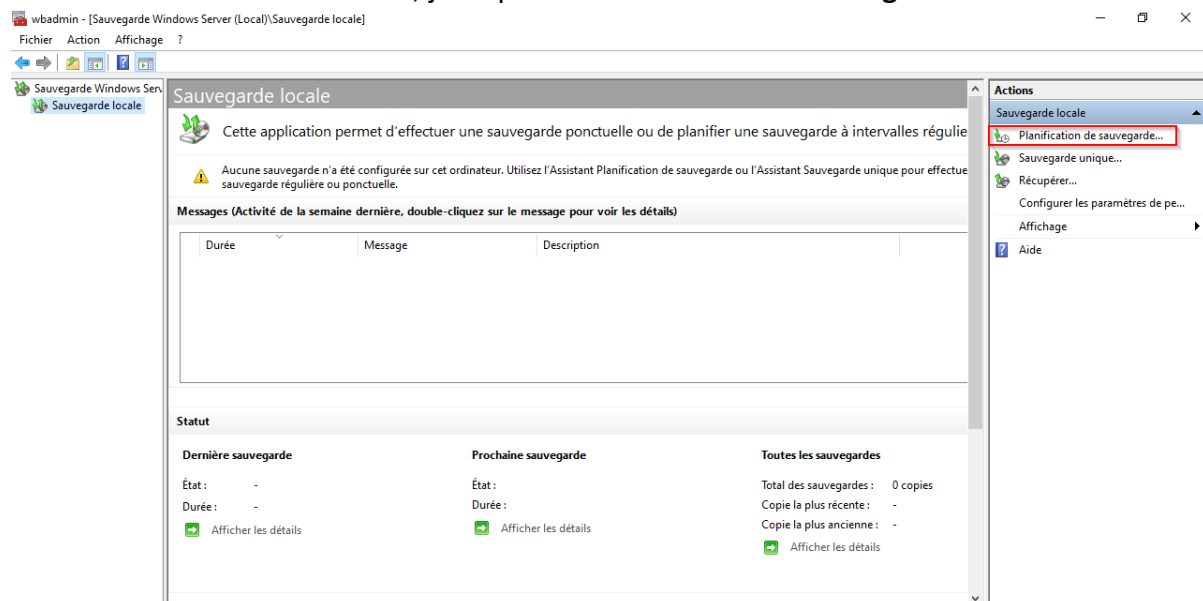
Fenêtre confirmant que l'installation du rôle a réussi sur le serveur de destination.



Navigation dans le menu **Outils** du Gestionnaire de serveur pour lancer **Sauvegarde Windows Server**.



Dans le volet "Actions" à droite, je clique sur **Planification de sauvegarde...**



Je sélectionne l'option **Serveur complet (recommandé)** qui englobe toutes les données, applications et l'état du système (taille estimée : 15,65 Go).

Assistant Planification de sauvegarde



Sélectionner la configuration de la sauvegarde

Mise en route

Sélectionner la configurat...

Spécifier l'heure de la sau...

Spécifier le type de destin...

Confirmation

Résumé

Quel type de configuration voulez-vous planifier ?

Serveur complet (recommandé)
Je veux sauvegarder toutes les données et les applications présentes sur le serveur, ainsi que l'état du système.
Taille de la sauvegarde : 15,65 Go

Personnalisé
Je veux choisir des volumes et des fichiers personnalisés pour la sauvegarde.

< Précédent

Suivant >

Terminer

Annuler

Je fais le choix de faire une sauvegarde **Tous les jours** à une heure fixe : **23:30**.

Assistant Planification de sauvegarde



Spécifier l'heure de la sauvegarde

Mise en route

Sélectionner la configurat...

Spécifier l'heure de la sau...

Spécifier le type de destin...

Confirmation

Résumé

À quelle fréquence et à quel moment voulez-vous exécuter les sauvegardes ?

Tous les jours
Sélectionnez une heure : 23:30

Plusieurs fois par jour
Cliquez sur une heure disponible, puis sur Ajouter pour l'ajouter à la planification de sauvegarde.

Temps disponible :

00:00
00:30
01:00
01:30
02:00
02:30
03:00
03:30
04:00
04:30

Ajouter >

< Supprimer

Heure planifiée :

21:00

< Précédent

Suivant >

Terminer

Annuler

Je sélectionne l'option **Sauvegarder sur un dossier réseau partagé**.

Assistant Planification de sauvegarde

Spécifier le type de destination

Mise en route
Sélectionner la configurat...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Spécifier le dossier partag...
Confirmation
Résumé

Où voulez-vous stocker les sauvegardes ?

- Sauvegarder vers un disque dur dédié aux sauvegardes (recommandé)
Sélectionnez cette option pour stocker de la manière la plus sûre les sauvegardes. Le disque dur utilisé sera formaté, puis utilisé uniquement pour stocker les sauvegardes.
- Sauvegarder vers un volume
Sélectionnez cette option si vous ne pouvez pas dédier tout un disque à la sauvegarde. Notez que cette option peut réduire les performances du volume de 200 pour cent durant le stockage des sauvegardes. Il est recommandé de ne pas stocker d'autres données de serveur sur le même volume.
- Sauvegarder sur un dossier réseau partagé**
Sélectionnez cette option uniquement si vous ne voulez pas stocker les sauvegardes sur le serveur lui-même. Notez que vous ne disposerez que d'une sauvegarde à la fois lorsque vous créez une nouvelle sauvegarde, car celle-ci remplace la précédente.

< Précédent **Suivant >** Terminer Annuler

Je saisi l'adresse du NAS : \\192.168.30.50\Sauvegarde. L'option **Hériter** est cochée pour le contrôle d'accès.

Assistant Planification de sauvegarde

Spécifier le dossier partagé distant

Mise en route
Sélectionner la configurat...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Spécifier le dossier partag...
Confirmation
Résumé

Emplacement :

Exemple : \\Mon_serveur_fichiers\Nom_dossier_partagé
Cet Assistant crée un dossier d'après le nom du serveur sauvegardé, comme par exemple Mon_serveur-Fichiers_de_sauvegarde.

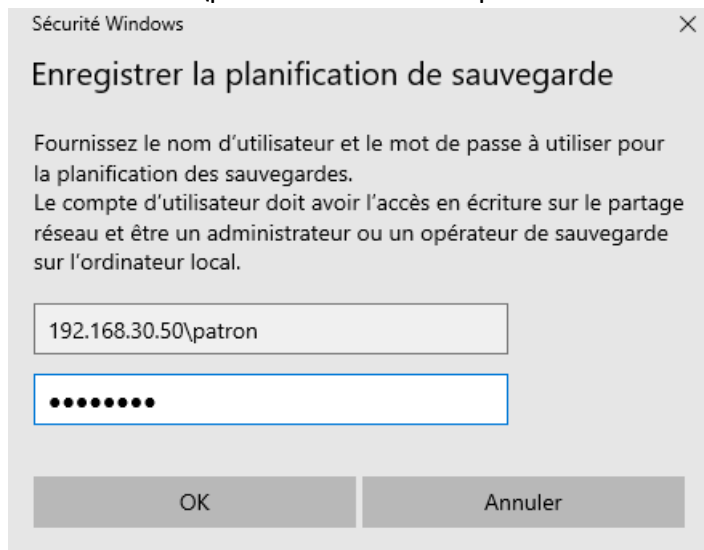
Contrôle d'accès

- Ne pas hériter
Cette option donne accès à la sauvegarde uniquement à l'utilisateur dont les informations d'identification sont fournies à l'étape suivante.
- Hériter**
Cette option permet à tous les utilisateurs ayant accès au dossier partagé distant spécifié d'accéder à la sauvegarde.

i Les données sauvegardées ne peuvent pas être protégées de manière sécurisée pour cette destination.
[Informations](#)

< Précédent **Suivant >** Terminer Annuler

Fenêtre de sécurité Windows demandant les identifiants pour accéder au partage. Je saisi 192.168.30.50\patron et du mot de passe associé.



Sécurité Windows

Enregistrer la planification de sauvegarde

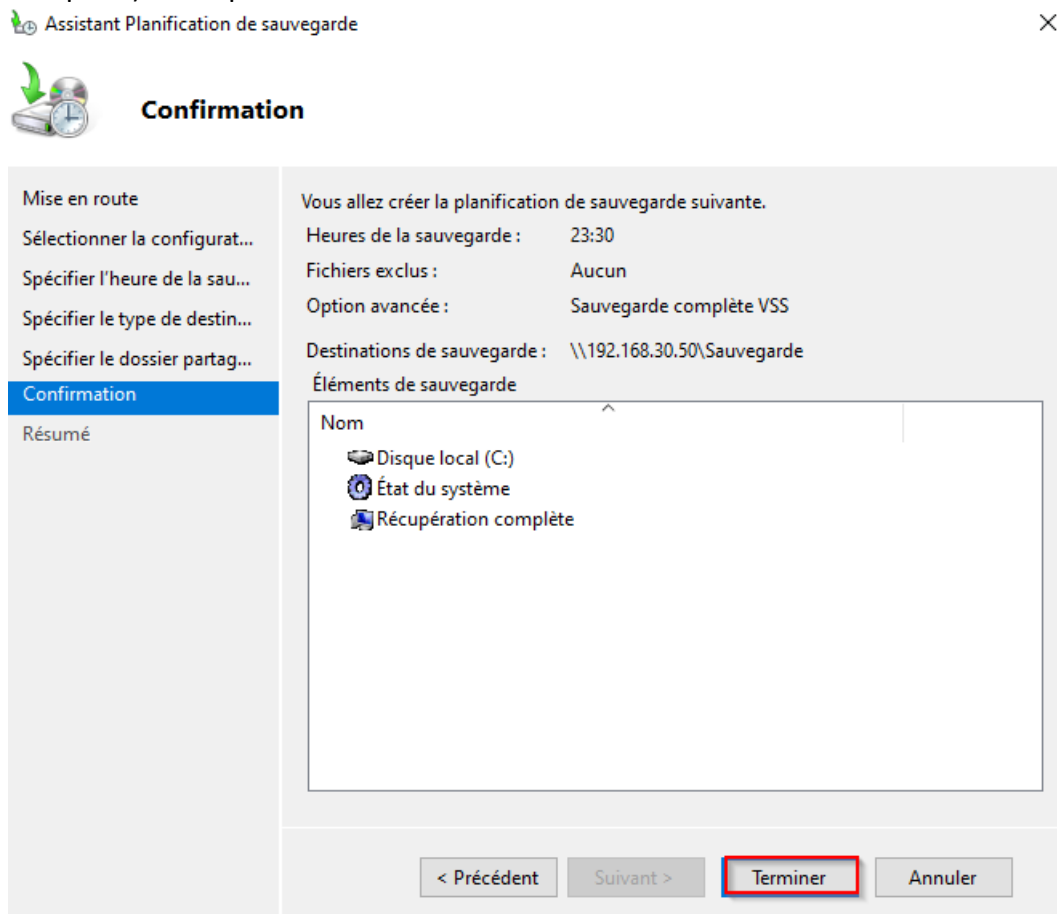
Fournissez le nom d'utilisateur et le mot de passe à utiliser pour la planification des sauvegardes.
Le compte d'utilisateur doit avoir l'accès en écriture sur le partage réseau et être un administrateur ou un opérateur de sauvegarde sur l'ordinateur local.

192.168.30.50\patron

••••••••

OK Annuler

Récapitulatif montrant les éléments à sauvegarder (Disque C:, État du système, Récupération complète). Je clique sur **Terminer**.



Assistant Planification de sauvegarde

Confirmation

Mise en route
Sélectionner la configurat...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Spécifier le dossier partag...
Confirmation
Résumé

Vous allez créer la planification de sauvegarde suivante.

Heures de la sauvegarde : 23:30
Fichiers exclus : Aucun
Option avancée : Sauvegarde complète VSS
Destinations de sauvegarde : \\192.168.30.50\Sauvegarde

Éléments de sauvegarde

Nom

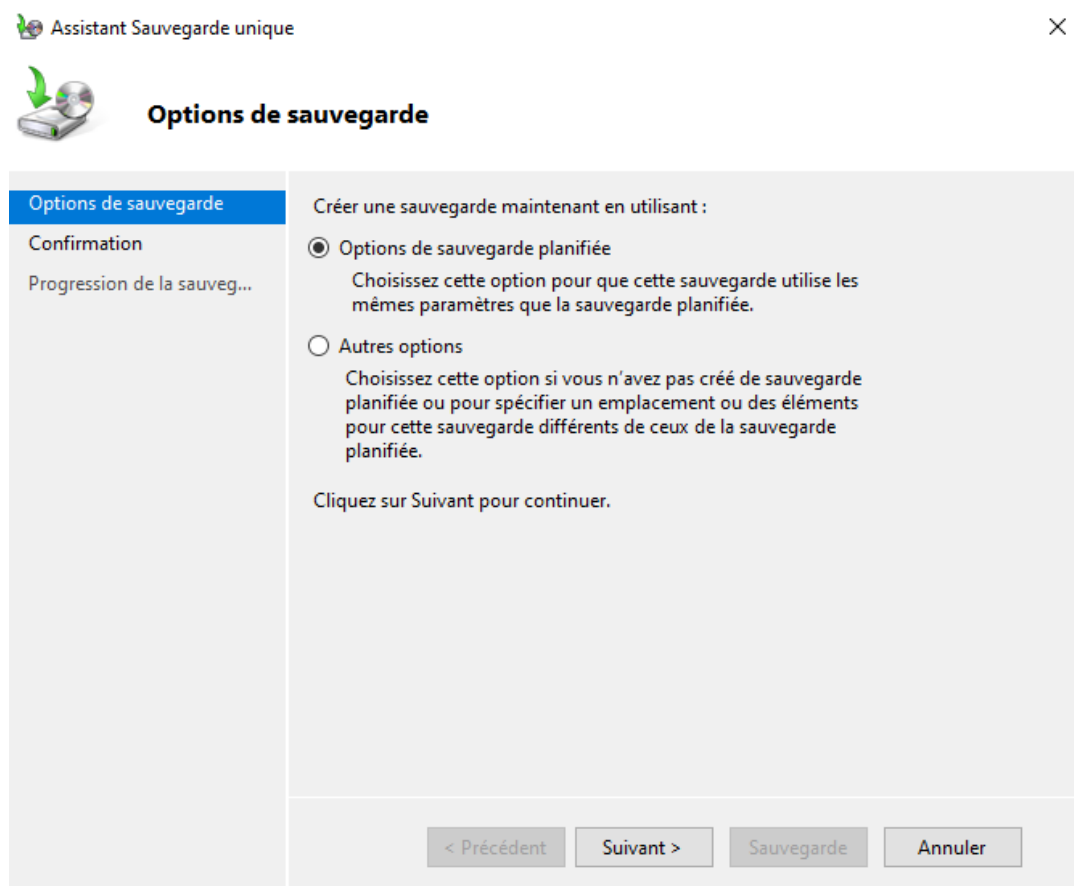
- Disque local (C:)
- État du système
- Récupération complète

< Précédent Suivant > **Terminer** Annuler

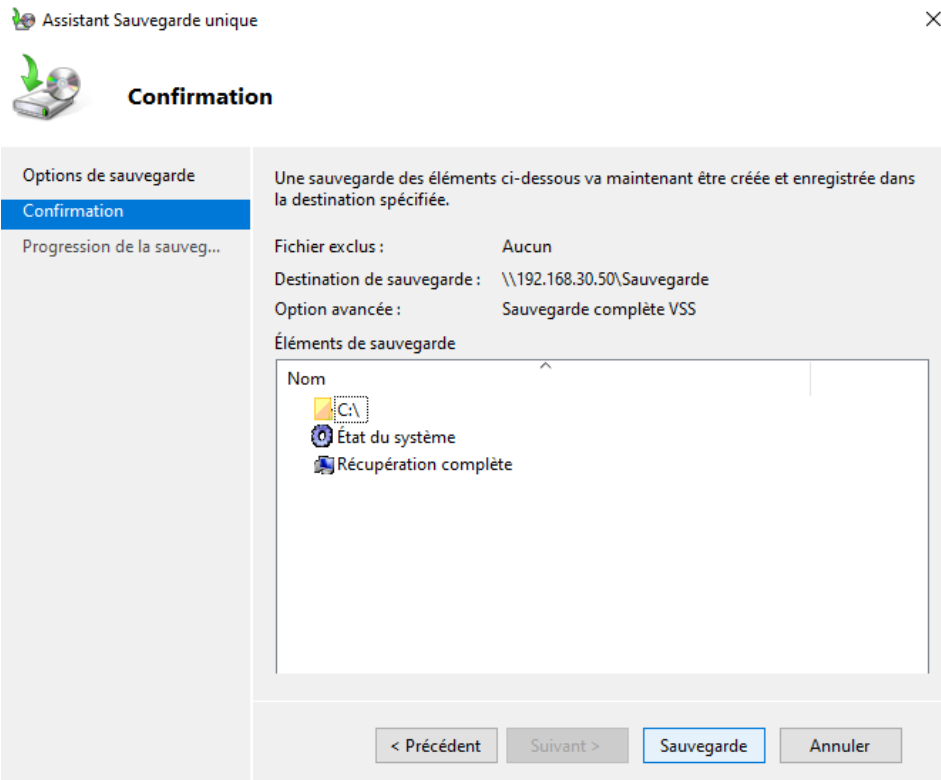
Message confirmant que la planification a bien été créée. La première occurrence est prévue pour le 31/03/2026 à 23:30.

Statut : La planification de sauvegarde a bien été créée.
Votre première sauvegarde planifiée aura lieu à 31/03/2026 23:30.

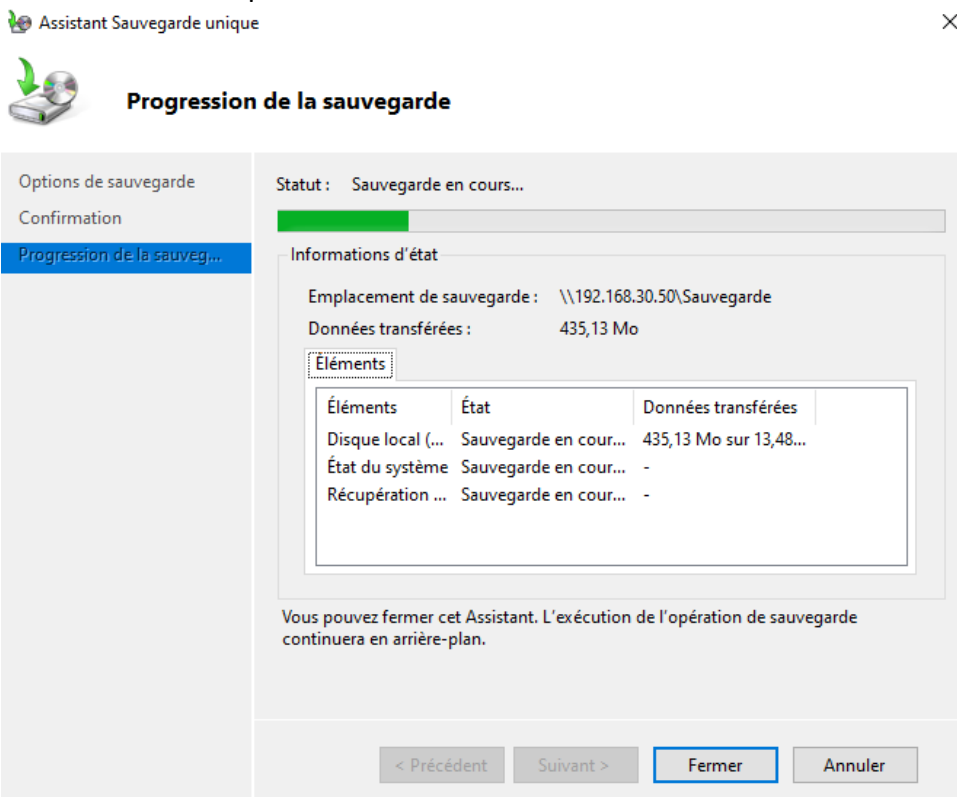
Pour ne pas attendre 23:30, lancement d'une "Sauvegarde unique" via l'assistant. Je choisis **Options de sauvegarde planifiée** pour tester les réglages précédents.



Confirmation finale avant le déclenchement du transfert.

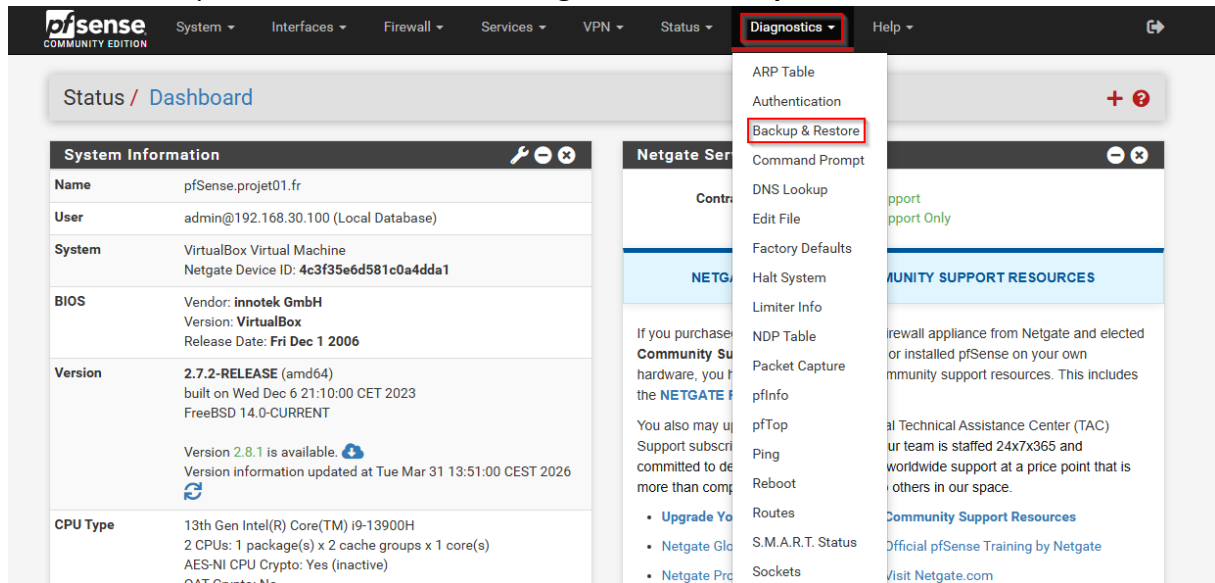


Barre de progression affichant le statut "Sauvegarde en cours..." avec le volume de données transférées en temps réel.

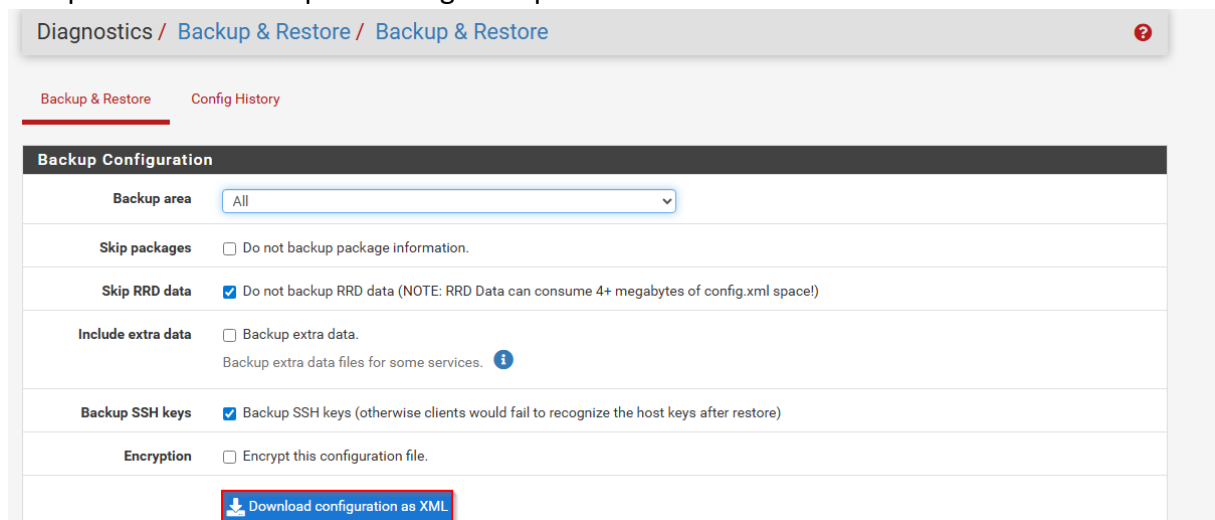


4 – Sauvegarde du PfSense

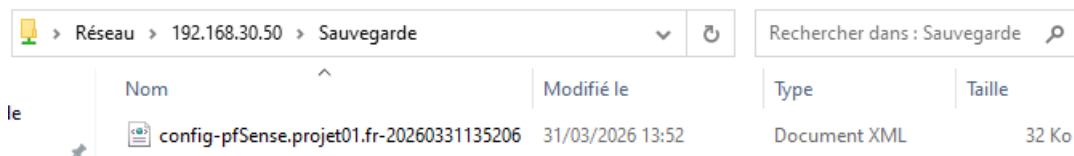
Sur l'interface pfSense, accès au menu **Diagnostics > Backup & Restore**.



Dans l'onglet Backup, je clique sur le bouton bleu **Download configuration as XML** pour récupérer le fichier de paramétrage complet.



Le fichier .xml de pfSense a été déposé dans le dossier réseau \\192.168.30.50\Sauvegarde.



5 – Sauvegarde du Debian (zabbix et glpi)

Création et édition du script backup_debian.sh. Le script monte le partage via mount -t cifs, effectue un mysqldump des bases de données et un tar des dossiers GLPI avant de copier les archives sur le NAS.

```
GNU nano 8.4 /home/user/backup_debian.sh *
#!/bin/bash

NAS_IP="192.168.30.50"
USER="Patron"
PASS=""
DATE=$(date +%Y-%m-%d)
DEST="/mnt/nas_backup"

sudo mount -t cifs //$NAS_IP/Sauvegarde $DEST -o username=$USER,password=$PASS

mysqldump --all-databases | gzip > /tmp/db_backup_$DATE.sql.gz

tar -czf /tmp/glpi_files_complet_$DATE.tar.gz /var/www/glpi /etc/glpi /var/lib/glpi

cp /tmp/*.gz $DEST/
rm /tmp/*.gz

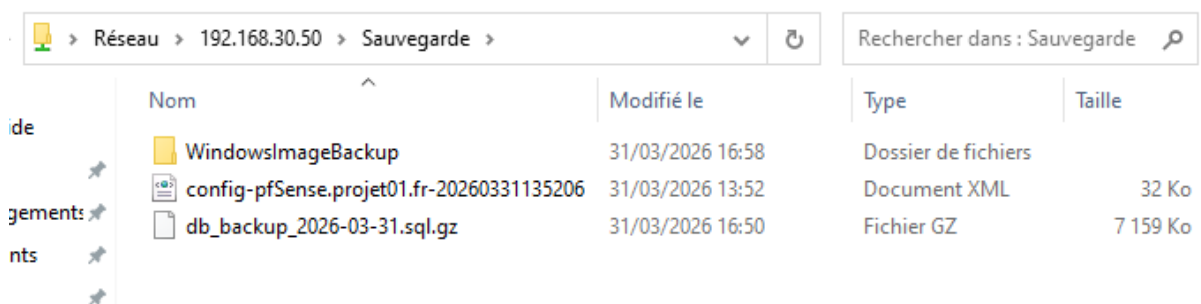
sudo umount $DEST

echo "Sauvegarde Debian terminée avec succès le $DATE !"
```

Lancement du script en mode root. Le terminal affiche les logs de compression et le message final "Sauvegarde Debian terminée avec succès".

```
root@debian:/home/user# /home/user/backup_debian.sh
tar: Suppression de « / » au début des noms des membres
tar: Suppression de « / » au début des liens physiques
Sauvegarde Debian terminée avec succès le 2026-03-31 !
```

Vue finale du dossier réseau contenant désormais : le dossier WindowsImageBackup, le fichier de configuration pfSense, et l'archive SQL de la base de données Debian.



id	Nom	Modifié le	Type	Taille
	WindowsImageBackup	31/03/2026 16:58	Dossier de fichiers	
gements:	config-pfSense.projet01.fr-20260331135206	31/03/2026 13:52	Document XML	32 Ko
nts	db_backup_2026-03-31.sql.gz	31/03/2026 16:50	Fichier GZ	7 159 Ko