Documentation Technique – Projet 2
Optimisation et sécurisation d'une infrastructure multi-services haute disponibilité

Antoine Moreaux
N° candidat : 02543706899
BTS SIO – Option SISR – Session 2026

Période : 01/01/2026 – 15/03/2026
Lieu : Keyce Nîmes

Table des matières

Présentation du projet

Contexte de la mission

Suite à la mise en place de l'infrastructure initiale (Projet 1), l'entreprise **TechSupp** a poursuivi sa croissance. Cette expansion a fait émerger de nouveaux défis critiques : la nécessité d'un accès distant sécurisé pour les techniciens en itinérance, une gestion rigoureuse du parc informatique grandissant, et la garantie d'une continuité d'activité en cas de perte de données.

Le réseau initial, devenu trop simple, devait être amélioré. Le projet visait donc à refondre l'architecture, déployer une solution de VPN SSL, centraliser l'inventaire via GLPI, et sécuriser les ressources par une politique de sauvegarde automatisée avec Veeam. L'objectif final était d'aboutir à une infrastructure mature, résiliente et parfaitement supervisée.

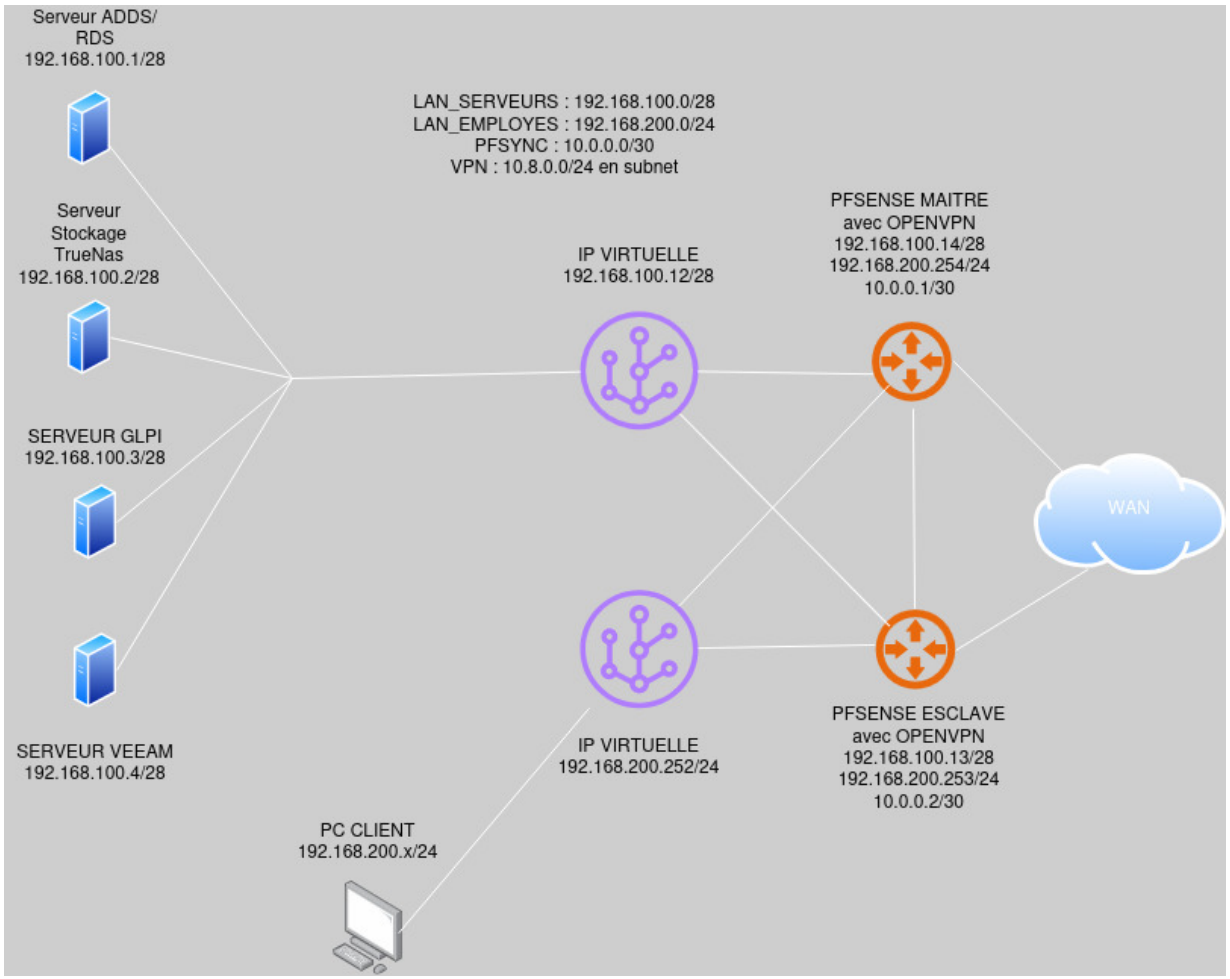
Intitulé de la réalisation professionnelle

1. Mise en place d'un accès distant sécurisé via VPN SSL (OpenVPN)
2. Déploiement d'une solution de gestion d'inventaire (GLPI)
3. Déploiement d'une solution de sauvegarde (Veeam Backup & Replication)
4. Mise en place d'un serveur RDS pour le travail à distance

Ressources fournies

— Contexte et problématique TechSupp
— Schéma réseau
— **Matériel :** Ordinateur sous Ubuntu 25.10
— **Virtualisation :** VM Windows Server 2025 (ADDS/RDS), VM TrueNAS, 2 VM pfSense, VM Debian 13 (GLPI), VM Windows Server 2025 (Veeam), VM Windows 10 (Client), VM Ubuntu 25.10 (Client Linux)
— **Logiciels :** OpenVPN, Veeam Backup & Replication

Schéma réseau



Machine	Adresse IP	Role
Serveur ADDS / RDS	192.168.100.1/28	Annuaire Active Directory + Bureau a distance
Serveur Stockage TrueNAS	192.168.100.2/28	Stockage reseau NAS
Serveur GLPI	192.168.100.3/28	Inventaire + Ticketing
Serveur Veeam	192.168.100.4/28	Sauvegarde
pfSense Maitre	192.168.100.14/28	Routeur principal + OpenVPN
pfSense Esclave	192.168.100.13/28	Routeur secondaire
IP Virtuelle LAN SERVEURS	192.168.100.12/28	VIP CARP
IP Virtuelle LAN EMPLOYES	192.168.200.252/24	VIP CARP
PC Client Windows et Linux	192.168.200.x/24	Poste utilisateur

Première partie

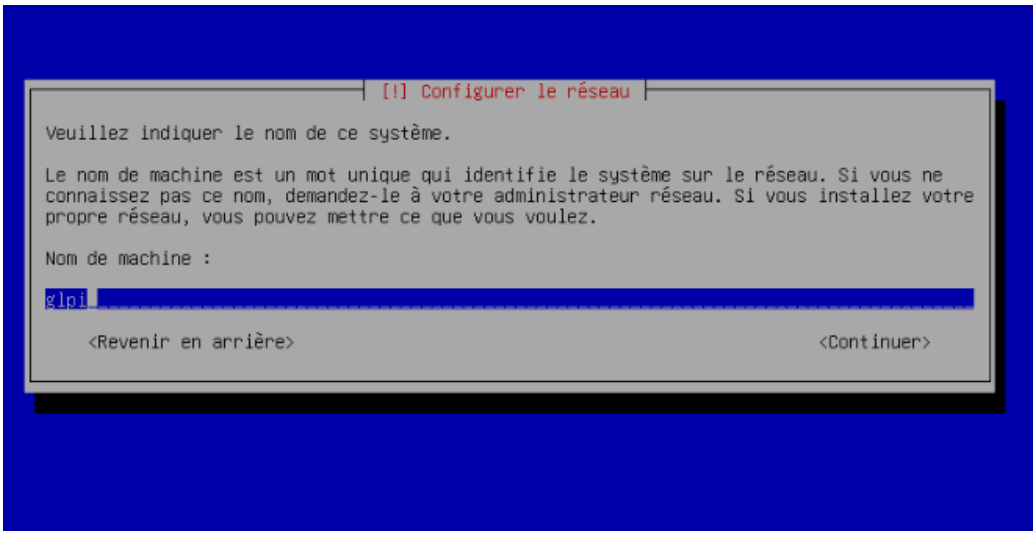
Guide d'Installation et Configuration : GLPI 11

1 Phase 1 : Préparation du Système et du Réseau

La première étape consiste à préparer l'environnement Debian/Ubuntu pour qu'il soit identifiable et joignable sur le réseau local.

1.1 Identification du serveur

Pendant le processus d'installation du système d'exploitation, l'installeur demande de choisir un "nom de machine" (hostname). Ce nom permet de résoudre l'adresse IP du serveur par un nom simple sur le réseau. Nous avons choisi **glpi** pour correspondre à la fonction du serveur.



1.2 Adressage IP Statique

Par défaut, un serveur reçoit une IP dynamique (DHCP), ce qui est risqué car si l'IP change, les agents GLPI ne pourront plus envoyer leurs rapports. Nous utilisons l'éditeur de texte `nano` pour modifier le fichier de configuration des interfaces réseau.

Dans ce fichier, nous passons l'interface `enp0s3` (la carte réseau principale) du mode DHCP au mode **static**. Nous définissons l'adresse **192.168.100.3** avec un masque de sous-réseau en /**28**. La passerelle (`gateway`) est l'adresse du routeur qui permet au serveur de sortir sur Internet.

```
GNU nano 8.4
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.100.3/28
    gateway 192.168.100.12
    nameserver 192.168.100.1
```

1.3 Activation et Validation Réseau

Après avoir enregistré les modifications, il est nécessaire de redémarrer le service réseau pour que le noyau Linux prenne en compte la nouvelle configuration sans avoir à redémarrer toute la machine.

```
root@glpi:~# systemctl restart networking
```

La commande `ip a` (IP Address) permet de lister les interfaces. On observe ici que l'interface `2: enp0s3` affiche bien notre adresse statique et que l'état est "UP", ce qui signifie que le lien physique et logique est actif.

```
root@glpi:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:73:95:5a brd ff:ff:ff:ff:ff:ff
    altname enx08002773955a
    inet 192.168.100.3/28 brd 192.168.100.15 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe73:955a/64 scope link proto kernel_ll
```

1.4 Résolution de noms (DNS)

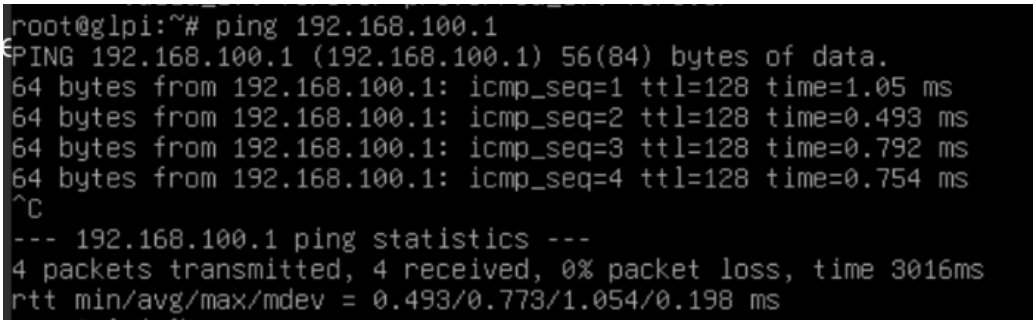
Pour que le serveur puisse télécharger des mises à jour, il doit pouvoir traduire les noms de domaine (comme github.com) en adresses IP. Le fichier `resolv.conf` contient l'adresse du serveur DNS. Ici, le serveur pointe vers **192.168.100.1**.

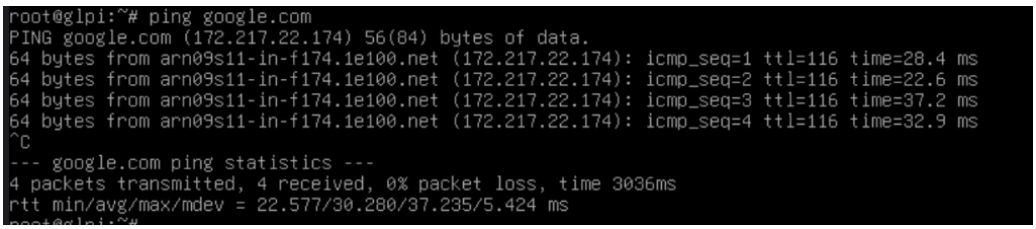
```
root@glpi:~# nano /etc/resolv.conf
```

```
GNU nano 8.4
# Generated by dhcpcd
# /etc/resolv.conf.head can replace this line
# /etc/resolv.conf.tail can replace this line

nameserver 192.168.100.1
```

1.5 Tests de Connectivité par Ping

Le protocole ICMP (Ping) est utilisé pour vérifier la communication. Le premier test vers la passerelle (**192.168.100.1**) confirme que le réseau local fonctionne. Le second test vers **google.com** confirme que le DNS et la sortie Internet sont opérationnels.





2 Phase 2 : Installation de la pile LAMP

GLPI est une application Web. Elle nécessite un serveur HTTP (Apache), une base de données (MariaDB) et un langage de script (PHP).

2.1 Mise à jour des dépôts

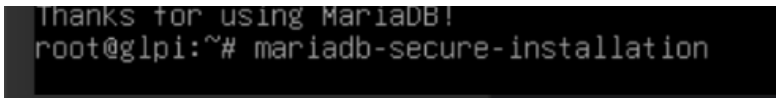
Avant toute installation, on utilise `apt update`. Cette commande télécharge les dernières versions disponibles des logiciels sur les serveurs officiels d'Ubuntu, garantissant ainsi la sécurité du système.

2.2 Installation des services et dépendances PHP

Cette étape installe Apache2 et MariaDB. GLPI a besoin d'extensions PHP spécifiques pour fonctionner : `php-curl` pour les communications distantes, `php-gd` pour les images/graphiques, et `php-intl` pour la gestion des langues.

2.3 Sécurisation du serveur SQL

Par défaut, MariaDB est installé sans mot de passe root. Le script `mariadb-secure-installation` permet de définir un mot de passe robuste, de supprimer les utilisateurs anonymes et de retirer la base de données de test qui pourrait constituer une faille de sécurité.



```
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] n
 ... skipping.

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!
```

2.4 Configuration de la base de données dédiée

Nous créons un environnement SQL propre. La commande `CREATE DATABASE glpi` génère la base de données. L'utilisateur **adminglpi** est créé avec un mot de passe complexe (`Techsupp30`) pour que l'application web puisse se connecter à la base sans utiliser le compte "root" du système.

```
MariaDB [(none)]> CREATE DATABASE glpi;
Query OK, 1 row affected (0,002 sec)
```

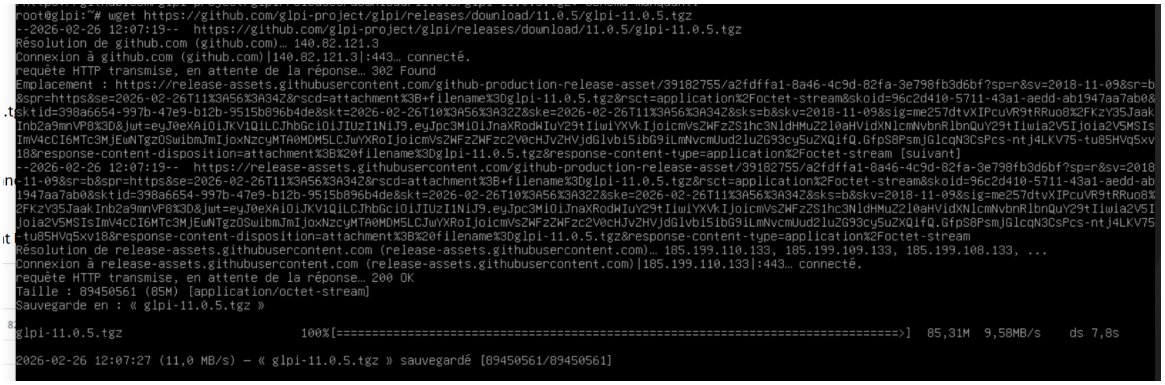
```
MariaDB [(none)]> CREATE USER adminglpi@localhost IDENTIFIED BY 'Techsupp30';
Query OK, 0 rows affected (0,022 sec)
```

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON glpi.* TO adminglpi@localhost;
Query OK, 0 rows affected (0,021 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,001 sec)

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

3 Phase 3 : Déploiement de l'Application GLPI

3.1 Téléchargement de l'archive

Nous utilisons `wget` pour récupérer directement la version **11.0.5** de GLPI depuis le dépôt GitHub officiel. L'archive est au format `.tgz` (compressée).



3.2 Extraction et Permissions de fichiers

L'archive est décompressée dans `/var/www/`, le dossier standard des sites web sous Linux. Ensuite, nous changeons le propriétaire du dossier avec `chown`. L'utilisateur **www-data** (le serveur Apache) devient propriétaire du dossier pour pouvoir écrire les fichiers de logs et uploader des documents.

```
root@glpi:~# tar -xzf glpi-11.0.5.tgz -C /var/www
```

```
root@glpi:~# chown www-data /var/www/glpi/ -R
```

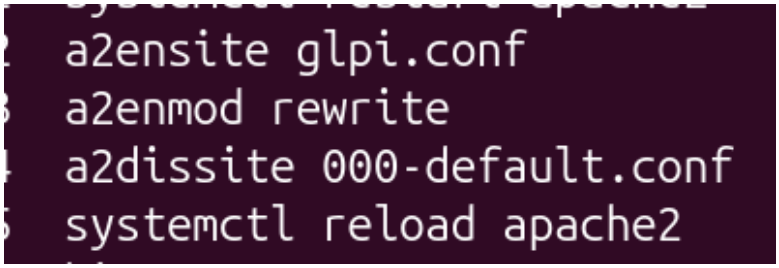
3.3 Configuration du VirtualHost Apache

Pour des raisons de sécurité, nous créons un fichier `glpi.conf`. Au lieu de pointer vers la racine du dossier GLPI, nous pointons vers le sous-dossier /**public**. Cela empêche les utilisateurs d'accéder directement aux fichiers sensibles du moteur de l'application via leur navigateur.

```
root@glpi:~# nano /etc/apache2/sites-available/glpi.conf
```

```
 GNU nano 8.4                    /etc/apache2/sites-available/glpi.conf
<VirtualHost *:80>
    ServerName glpi.localhost
    DocumentRoot /var/www/glpi/public
    <Directory /var/www/glpi/public>
        Require all granted
        RewriteEngine On
# Ensure authorization headers are passed to PHP.
# Some Apache configurations may filter them and break usage of API, CalDAV, ...
        RewriteCond %{HTTP:Authorization} ^(.+)$
        RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
# Redirect all requests to GLPI router, unless file exists.
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>
</VirtualHost>
```

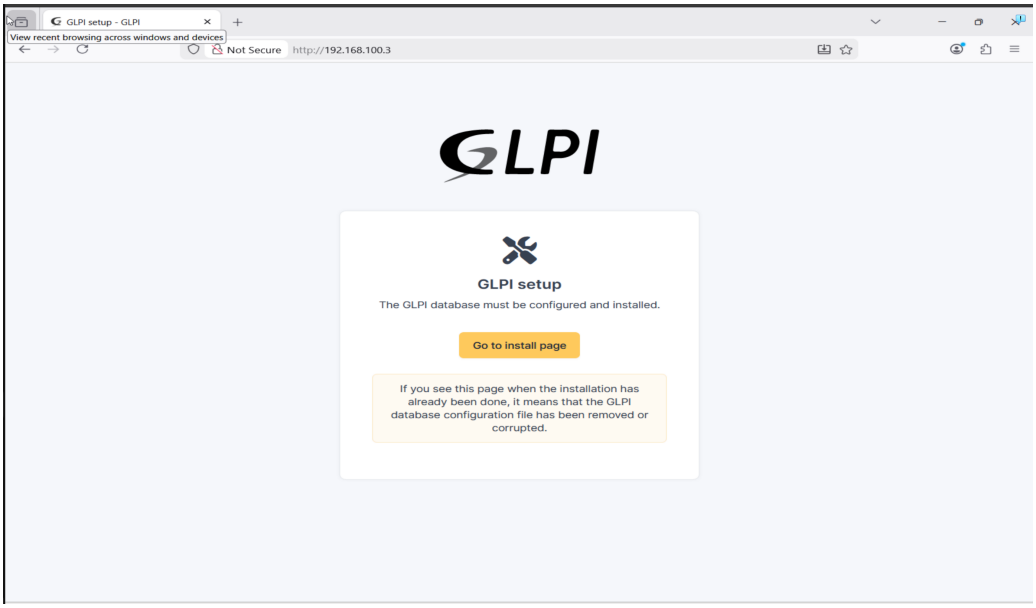
Nous désactivons la configuration par défaut d'Apache (`000-default`) et activons notre nouvelle configuration GLPI. Le module `rewrite` est également activé pour permettre à GLPI de gérer ses URLs proprement.

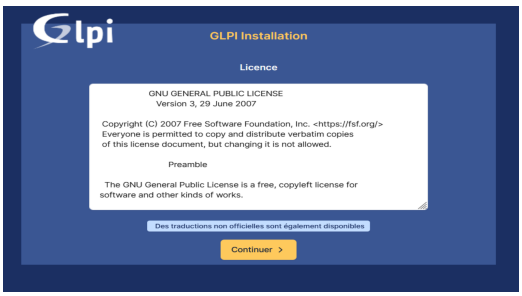


4 Phase 4 : Assistant Web et Finalisation

4.1 Initialisation du Setup

En entrant l'IP du serveur dans un navigateur, l'assistant d'installation démarre. On sélectionne le Français et on accepte la licence GPL qui régit l'utilisation de ce logiciel libre.



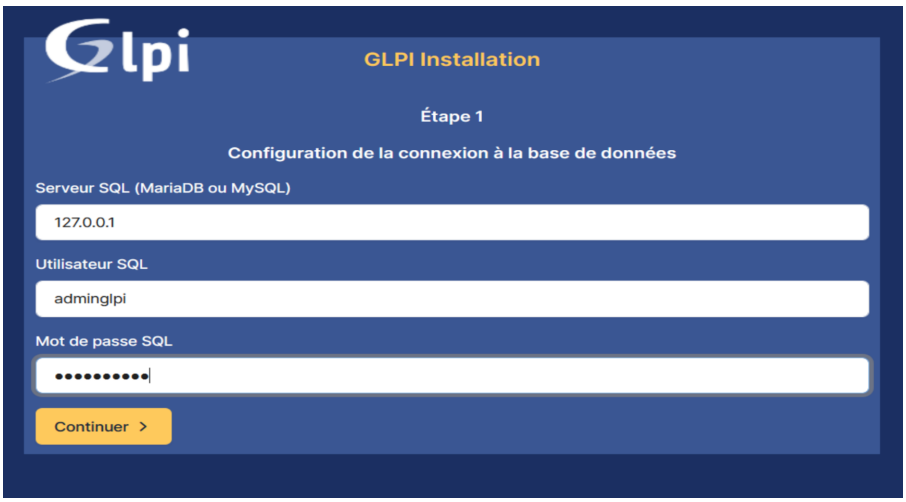


4.2 Contrôle de l'Environnement

GLPI vérifie que toutes les dépendances PHP installées en phase 2 sont présentes. Un voyant vert indique que la mémoire allouée et les bibliothèques (comme `mysqli` pour la base de données) sont prêtes.

4.3 Liaison SQL

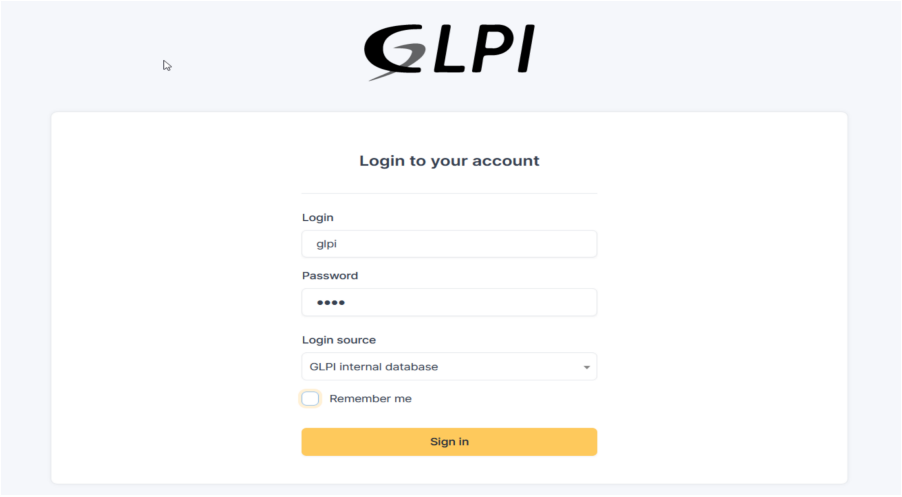
Nous indiquons à GLPI comment joindre sa base de données. L'adresse est `127.0.0.1` (lui-même). Nous utilisons l'utilisateur **adminglpi** créé précédemment. L'assistant détecte alors la base vide nommée `glpi` et l'initialise.



4.4 Accès et Sécurité Finale

Après l'installation, nous nous connectons avec l'identifiant par défaut **glpi/glpi**. Un message d'alerte orange nous rappelle deux actions critiques : changer les mots de passe par défaut et supprimer le fichier `install.php` sur le serveur pour verrouiller l'installation.


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 "Télémétrie", qui envoie anonymement, avec votre permission, des données à notre site de télémétrie.
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 améliorons GLPI et ses plugins !
Voir ce qui serait envoyé...
Référencez 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


Login to your account
Login
glpi
Password
Login source
GLPI internal database
Remember me
Sign in


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

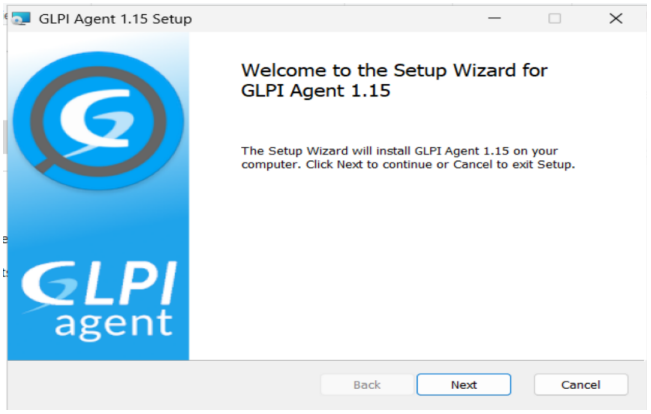

root@glpi:~# rm /var/www/glpi/install/install.php

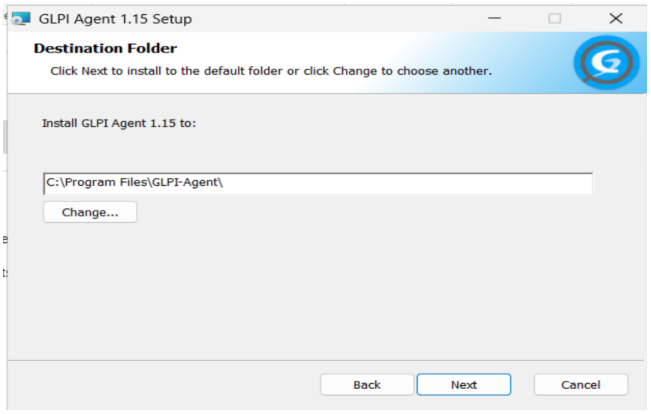
5 Phase 5 : Déploiement de l'Agent et Inventaire

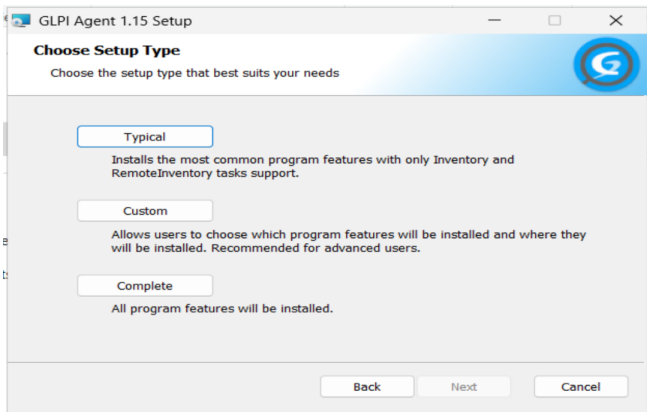
L'agent est un petit logiciel installé sur les ordinateurs du parc qui "scanne" le matériel (CPU, RAM, logiciels installés) et envoie ces données au serveur.

5.1 Installation sur le client

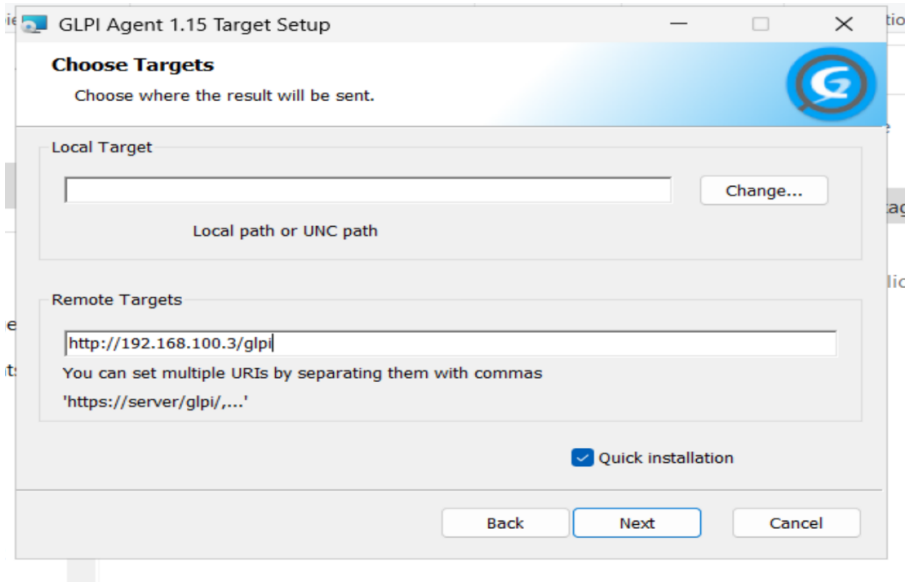
Nous installons l'agent GLPI sur une machine Windows. Pendant l'assistant, nous choisissons le dossier de destination et une installation "Typique".





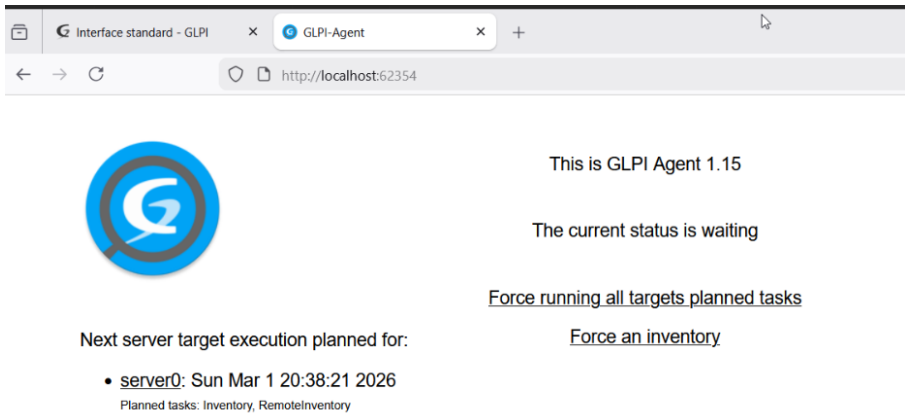


L'étape la plus importante est de renseigner l'URL du serveur. L'agent doit savoir vers quelle adresse envoyer ses données. Nous saisissons l'adresse IP du serveur suivi du nom de l'application.

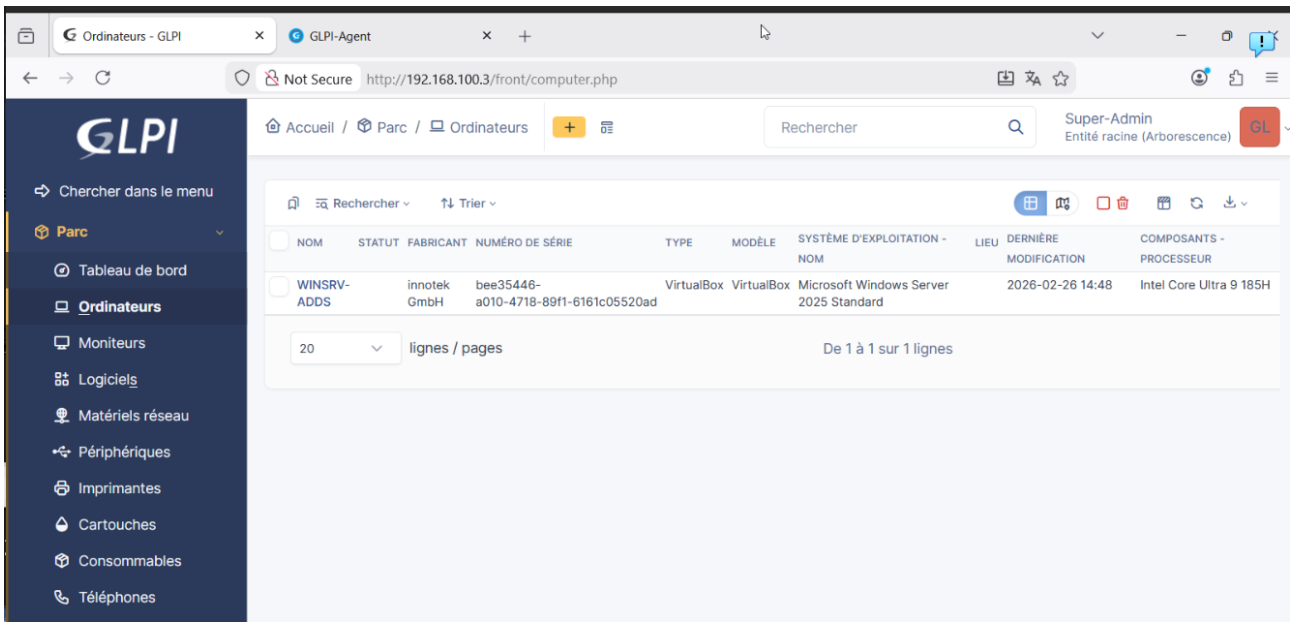


5.2 Remontée de l'Inventaire

L'agent dispose d'une interface web locale sur le port **62354**. En cliquant sur "Force Inventory", l'agent collecte immédiatement les informations du PC et les pousse vers le serveur. Le statut passe de "Waiting" à "Sending".



Enfin, sur le serveur GLPI, dans le menu **Parc** > **Ordinateurs**, nous voyons apparaître la machine **WINSRV-ADDS**. On y retrouve le modèle de processeur (Intel Core Ultra 9), la version du système d'exploitation et le numéro de série, prouvant que la chaîne d'inventaire est totalement opérationnelle.


Ordinateurs - GLPI
GLPI-Agent
Not Secure
http://192.168.100.3/front/computer.php
GLPI
Chercher dans le menu
Parc
Tableau de bord
Ordinateurs
Moniteurs
Logiciels
Matériels réseau
Périphériques
Imprimantes
Cartouches
Consommables
Téléphones
Accueil / Parc / Ordinateurs
Rechercher
Super-Admin
Entité racine (Arborescence)
GL
Rechercher
Trier
NOM
STATUT
FABRICANT
NUMÉRO DE SÉRIE
TYPE
MODÈLE
SYSTÈME D'EXPLOITATION - NOM
LIEU
DERNIÈRE MODIFICATION
COMPOSANTS - PROCESSEUR
WINSRV-ADDS
innotek GmbH
bee35446-a010-4718-89f1-6161c05520ad
VirtualBox
VirtualBox
Microsoft Windows Server 2025 Standard
2026-02-26 14:48
Intel Core Ultra 9 185H
20
lignes / pages
De 1 à 1 sur 1 lignes

Deuxième partie

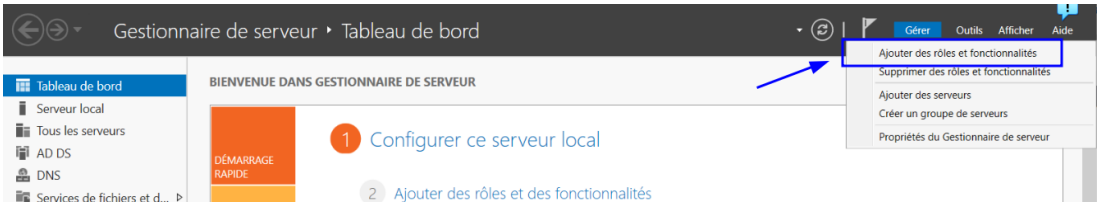
Documentation Technique : Services Bureau à Distance (RDS)

Déploiement et Configuration sur Windows Server 2025

6 Phase 1 : Déploiement des Services de rôle

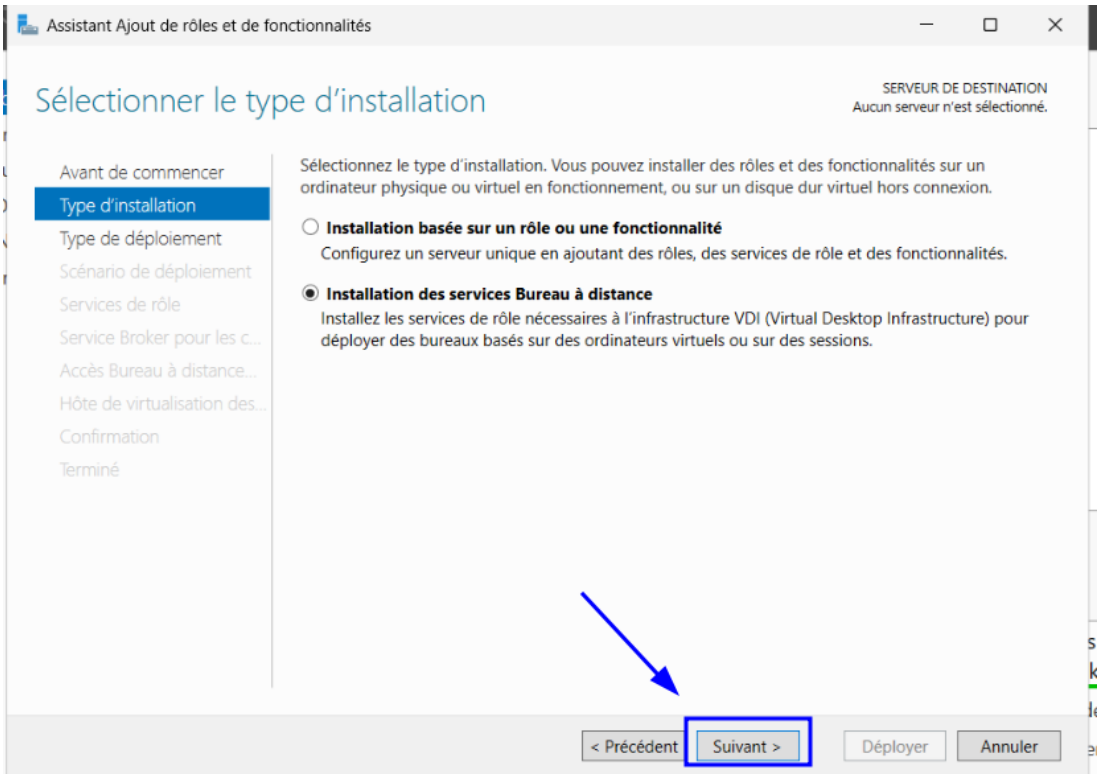
6.1 Lancement de l'assistant d'ajout de rôles

La première étape consiste à préparer le serveur local. Dans le **Gestionnaire de serveur**, nous accédons au menu **Gérer** situé en haut à droite, puis nous cliquons sur **Ajouter des rôles et fonctionnalités**. Cet assistant va permettre d'injecter les composants nécessaires à l'infrastructure RDS.



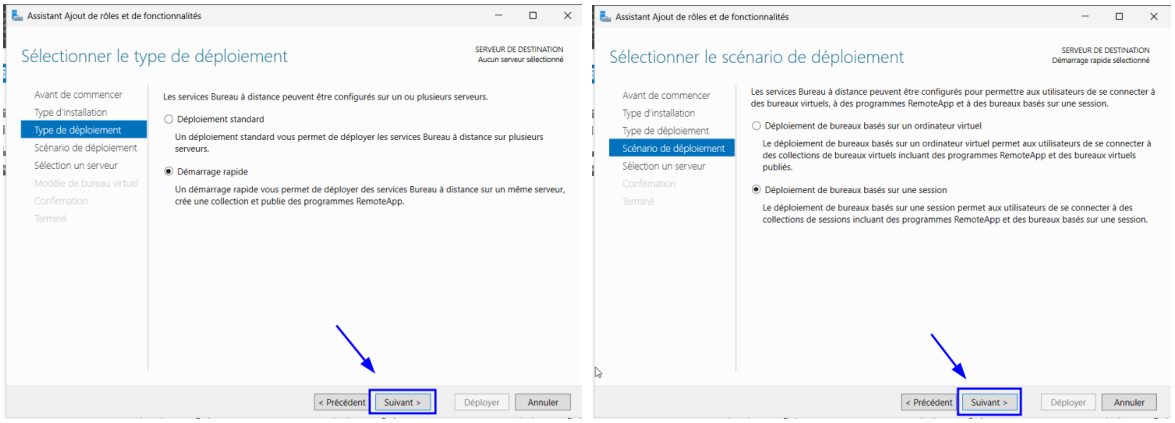
6.2 Sélection du type d'installation

Contrairement à une installation classique de rôle (ADDS, DNS), nous sélectionnons ici l'option **Installation des services Bureau à distance**. Ce mode permet de configurer de manière cohérente les différents composants (Broker, Accès Web, Hôte de session) qui travaillent de concert.



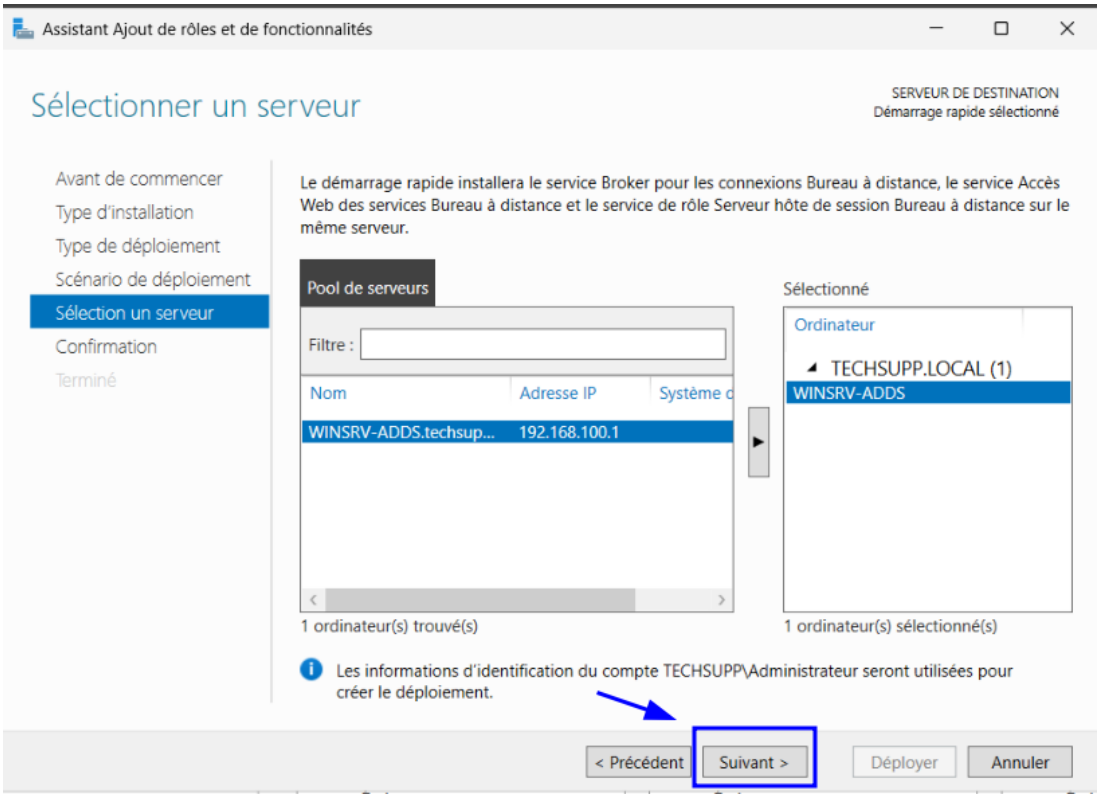
6.3 Choix du type de déploiement et du scénario

Nous optons pour le **Démarrage rapide**. Ce scénario est idéal pour un serveur unique, car il installe et configure automatiquement tous les services de rôle RDS nécessaires sans intervention manuelle complexe. Ensuite, nous sélectionnons **Déploiement de bureaux basés sur une session**, ce qui permettra aux utilisateurs de se connecter via leur session sur le domaine.



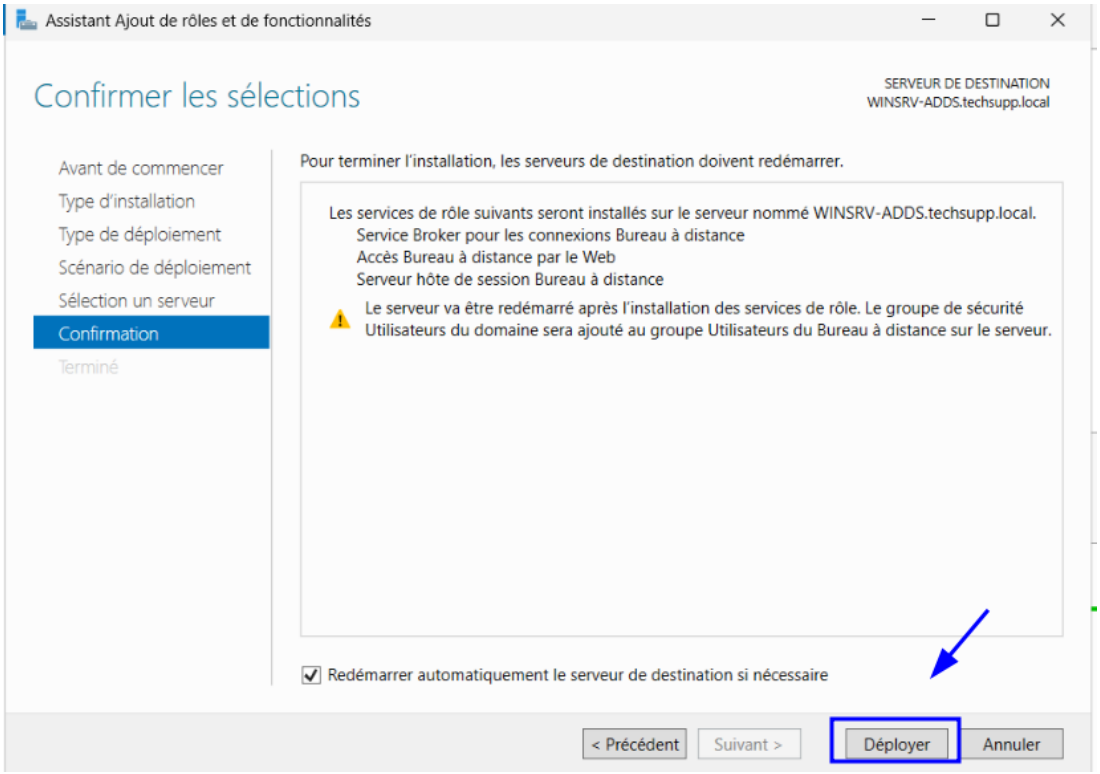
6.4 Sélection du serveur de destination

L'assistant scanne le pool de serveurs. Nous confirmons que le déploiement doit s'effectuer sur **WINSRV-ADDS.techsupp.local** (IP : 192.168.100.1). L'assistant nous informe que le service Broker, l'Accès Web et l'Hôte de session seront installés simultanément.



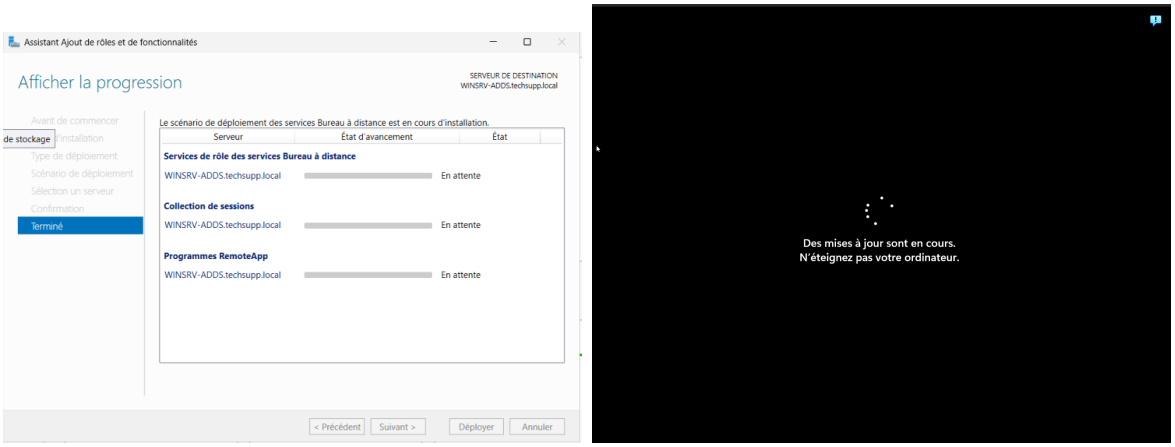
6.5 Confirmation et redémarrage automatique

Avant de lancer le déploiement, il est impératif de cocher la case **Redémarrer automatiquement le serveur de destination si nécessaire**. L'installation des services RDS nécessite en effet une modification profonde du registre et de la pile réseau, imposant un redémarrage pour finaliser la configuration de l'Hôte de session.



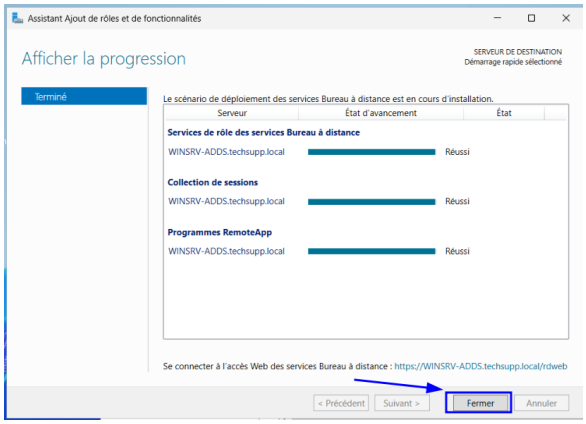
6.6 Suivi de la progression et phase système

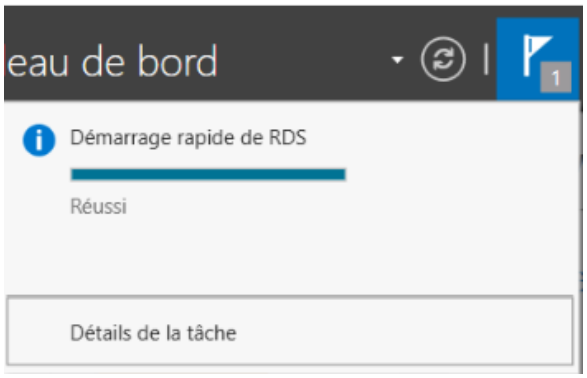
Une fois le déploiement lancé, une barre de progression s'affiche. Le serveur va ensuite basculer sur un écran noir de mise à jour système.



6.7 Validation de la fin d'installation

Après le redémarrage, nous nous reconnectons au serveur. L'assistant reprend automatiquement et confirme que le déploiement, la création de la collection et la publication des programmes RemoteApp ont réussi. Une URL d'accès Web est alors générée par défaut.

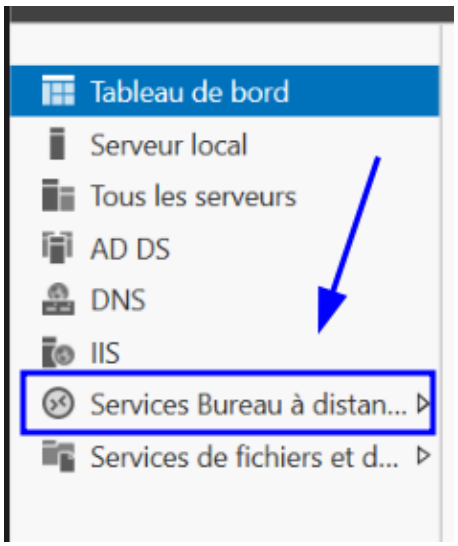

Assistant Ajout de rôles et de fonctionnalités
Afficher la progression
SERVEUR DE DESTINATION
Démarrage rapide sélectionné
Terminé
Le scénario de déploiement des services Bureau à distance est en cours d'installation.
Serveur
État d'avancement
État
Services de rôle des services Bureau à distance
WINSRV-ADDS.techsupp.local
Réussi
Collection de sessions
WINSRV-ADDS.techsupp.local
Réussi
Programmes RemoteApp
WINSRV-ADDS.techsupp.local
Réussi
Se connecter à l'accès Web des services Bureau à distance : https://WINSRV-ADDS.techsupp.local/rdweb
< Précédent
Suivant >
Fermer
Annuler


eau de bord
1
Démarrage rapide de RDS
Réussi
Détails de la tâche

7 Phase 2 : Configuration du Gestionnaire de Licences

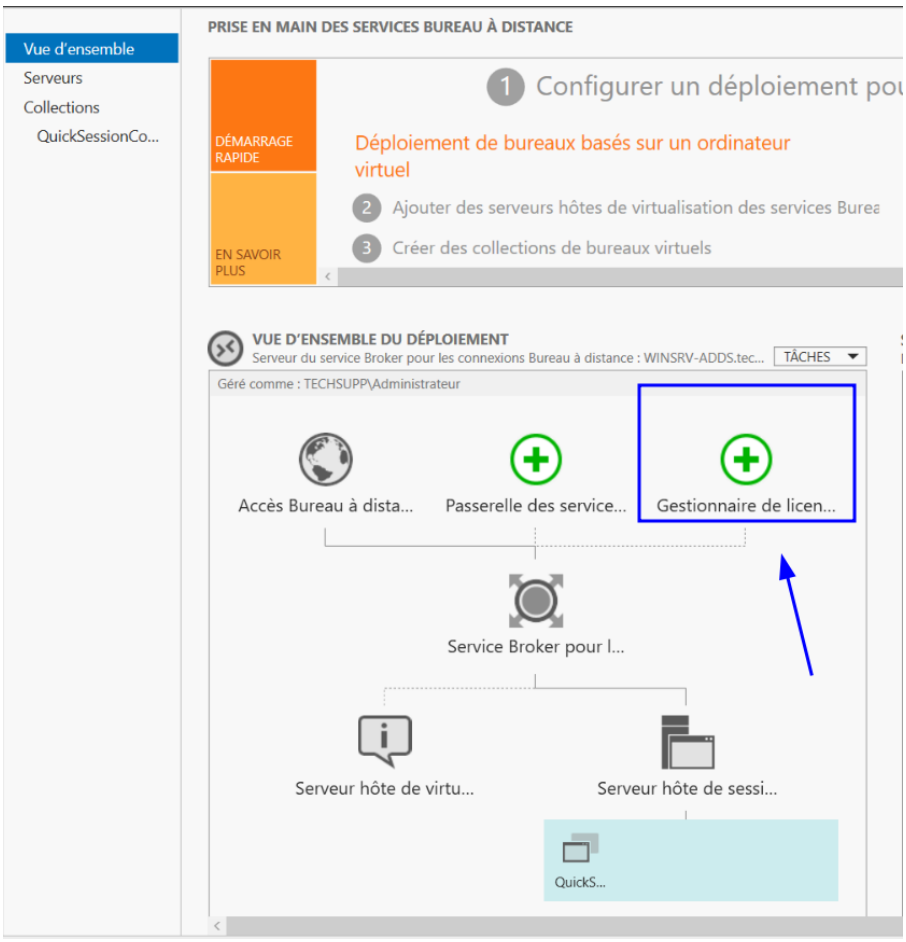
7.1 Accès aux outils de gestion RDS

Dans le volet de navigation du Gestionnaire de serveur, une nouvelle entrée **Services Bureau à distance** est apparue. Elle permet de piloter l'ensemble de l'infrastructure depuis une interface centralisée.



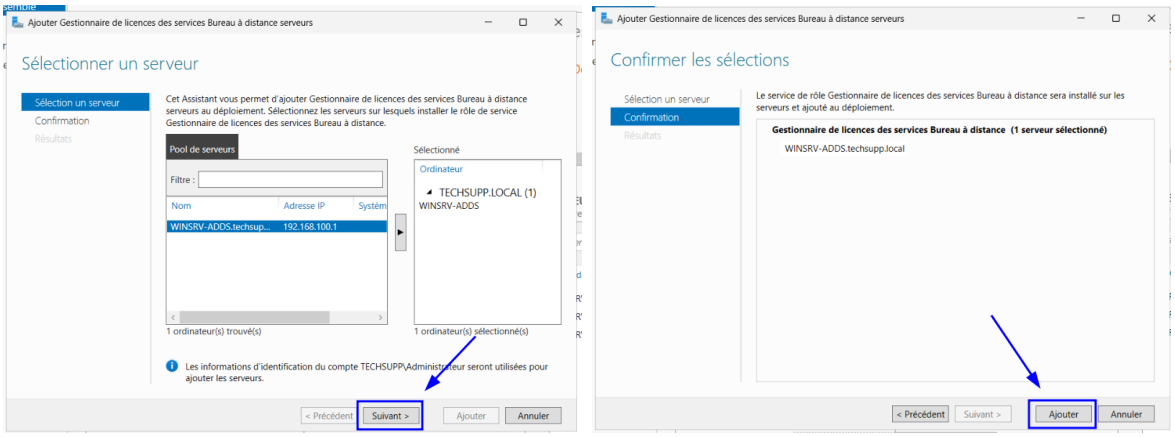
7.2 Installation du rôle Gestionnaire de licences

Le déploiement rapide n'installe pas par défaut le serveur de licences. Dans la "Vue d'ensemble du déploiement", nous cliquons sur l'icône verte avec le symbole + située au-dessus de **Gestionnaire de licences**. Puis nous sélectionnons notre serveur pour y ajouter ce rôle.



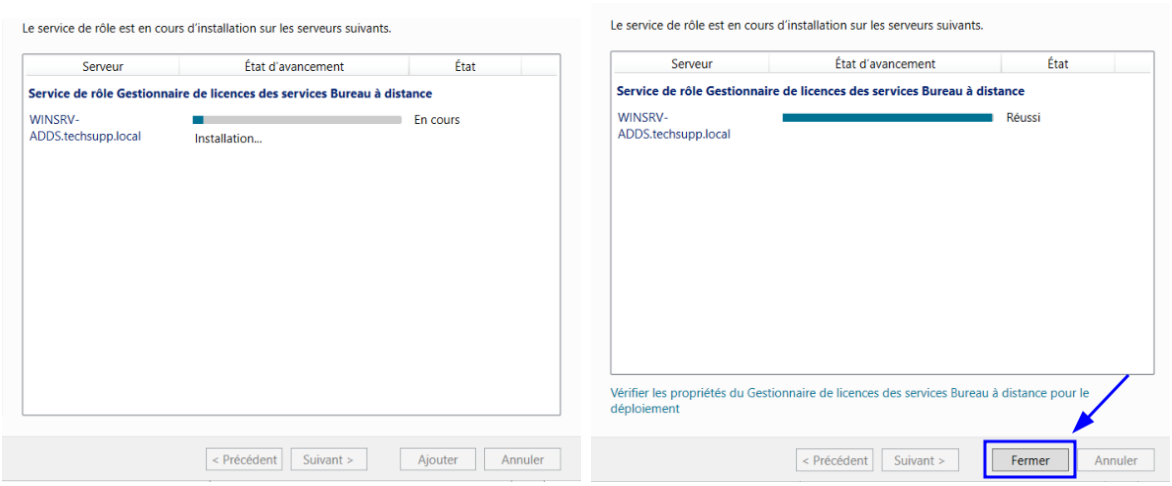
7.3 Confirmation et installation du rôle de licence

Nous validons la sélection du serveur dans le pool. L'assistant installe alors le service de rôle qui permettra de gérer les CAL (Client Access Licenses) pour les utilisateurs ou périphériques.



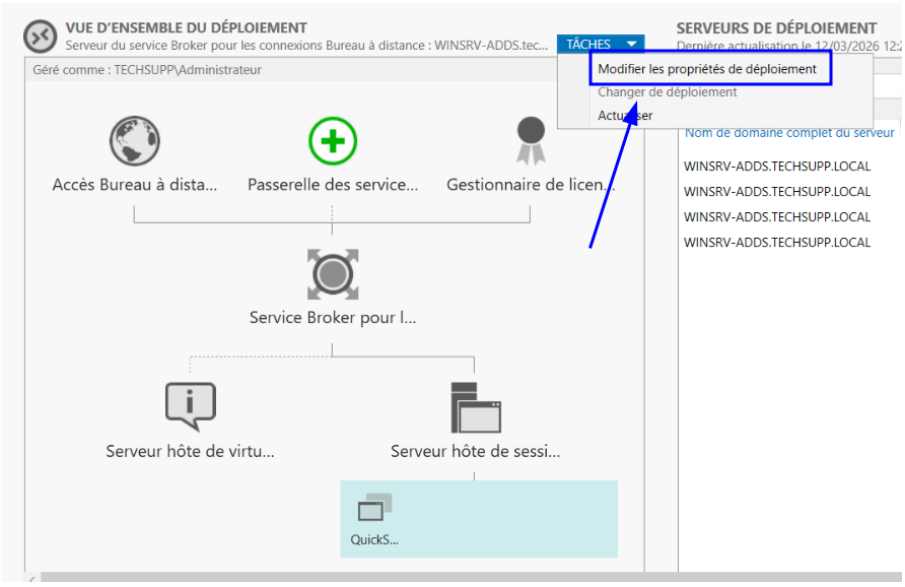
7.4 Statut de l'installation des licences

Une fois la barre de progression terminée, le statut passe à **Réussi**. Le rôle est désormais actif sur le serveur, mais nécessite encore d'être lié au déploiement global.



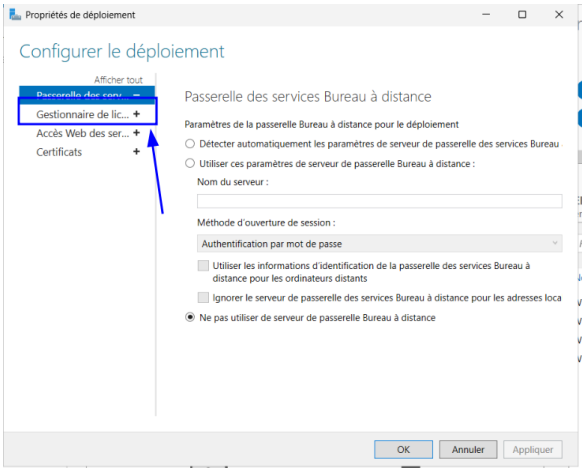
7.5 Liaison du mode de licence au déploiement

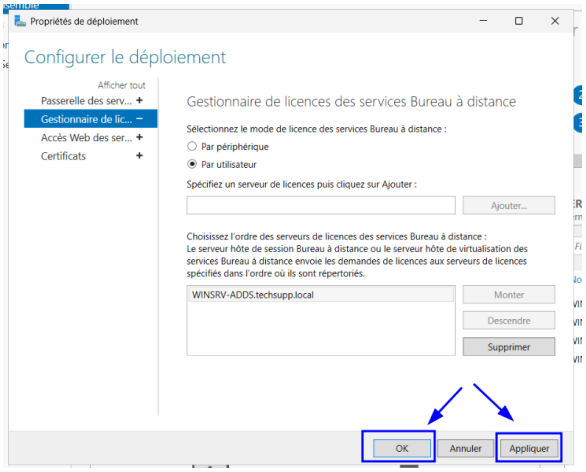
Il est crucial de définir comment le serveur va compter les licences. Nous cliquons alors sur le menu déroulant **TÂCHES** dans la vue d'ensemble, puis sur **Modifier les propriétés de déploiement**.



7.6 Configuration du mode 'Par utilisateur'

Dans la fenêtre des propriétés, nous sélectionnons l'onglet **Gestionnaire de licences**. Puis nous choisissons le mode de licence **Par utilisateur** et nous nous assurons que notre serveur est bien présent dans la liste des serveurs de licences. Enfin nous cliquons sur **Appliquer** pour valider.

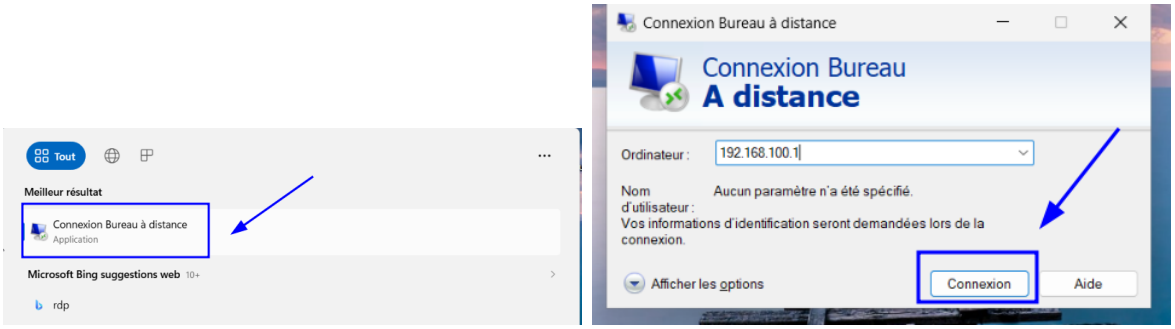

Propriétés de déploiement
Configurer le déploiement
Afficher tout
Gestionnaire de lic...
Accès Web des ser...
Certificats
Passerelle des services Bureau à distance
Paramètres de la passerelle Bureau à distance pour le déploiement
Détecter automatiquement les paramètres de serveur de passerelle des services Bureau
Utiliser ces paramètres de serveur de passerelle Bureau à distance :
Nom du serveur :
Méthode d'ouverture de session :
Authentification par mot de passe
Utiliser les informations d'identification de la passerelle des services Bureau à distance pour les ordinateurs distants
Ignorer le serveur de passerelle des services Bureau à distance pour les adresses loca
Ne pas utiliser de serveur de passerelle Bureau à distance
OK
Annuler
Appliquer


Propriétés de déploiement
Configurer le déploiement
Afficher tout
Passerelle des serv...
Gestionnaire de lic...
Accès Web des ser...
Certificats
Gestionnaire de licences des services Bureau à distance
Sélectionnez le mode de licence des services Bureau à distance :
Par périphérique
Par utilisateur
Spécifiez un serveur de licences puis cliquez sur Ajouter :
Ajouter...
Choisissez l'ordre des serveurs de licences des services Bureau à distance :
Le serveur hôte de session Bureau à distance ou le serveur hôte de virtualisation des services Bureau à distance envoie les demandes de licences aux serveurs de licences spécifiés dans l'ordre où ils sont répertoriés.
WINSRV-ADDS.techsupp.local
Monter
Descendre
Supprimer
OK
Annuler
Appliquer

8 Phase 3 : Validation de la Connexion Cliente

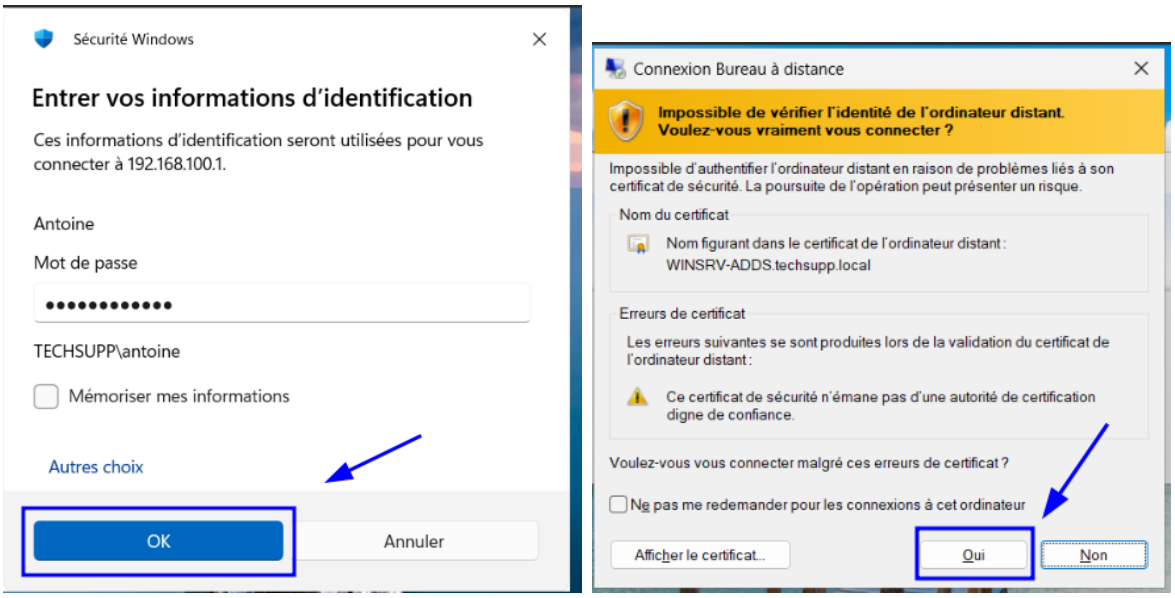
8.1 Préparation du poste client

Depuis une machine Windows cliente, nous ouvrons l'application **Connexion Bureau à distance**. Puis nous saisissons l'adresse IP du serveur cible : **192.168.100.1**.



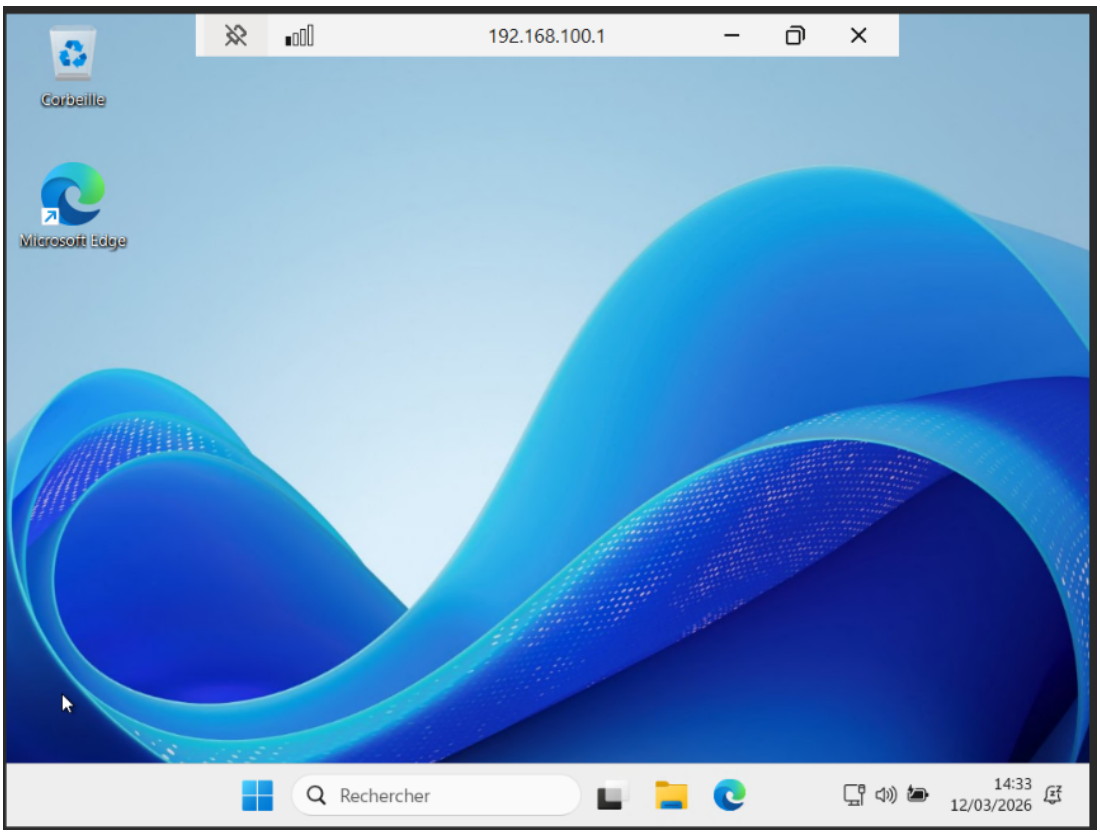
8.2 Authentification et gestion du certificat

Nous saisissons les informations de connexion du domaine (ex : `TECHSUPP\antoine`). Une fenêtre d'avertissement de sécurité apparaît car le certificat du serveur est auto-signé par défaut. Nous cliquons sur **Oui** pour poursuivre.



8.3 Accès final au bureau distant

La session s'ouvre avec succès. L'utilisateur dispose de son propre environnement de bureau hébergé sur Windows Server 2025. Le déploiement est validé et opérationnel.


192.168.100.1
Corbeille
Microsoft Edge
Rechercher
14:33
12/03/2026

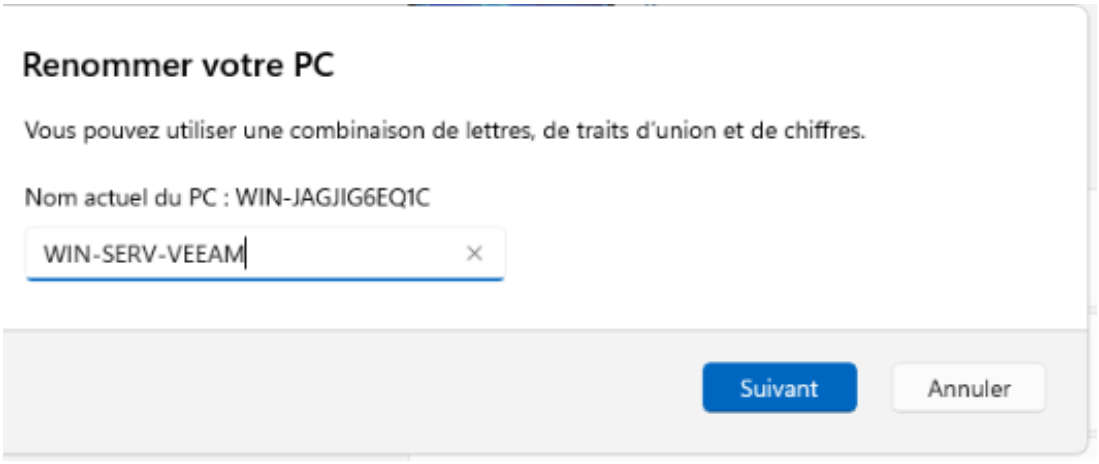
Troisième partie

Manuel d'Installation et Configuration : Veeam Backup & Replication 13

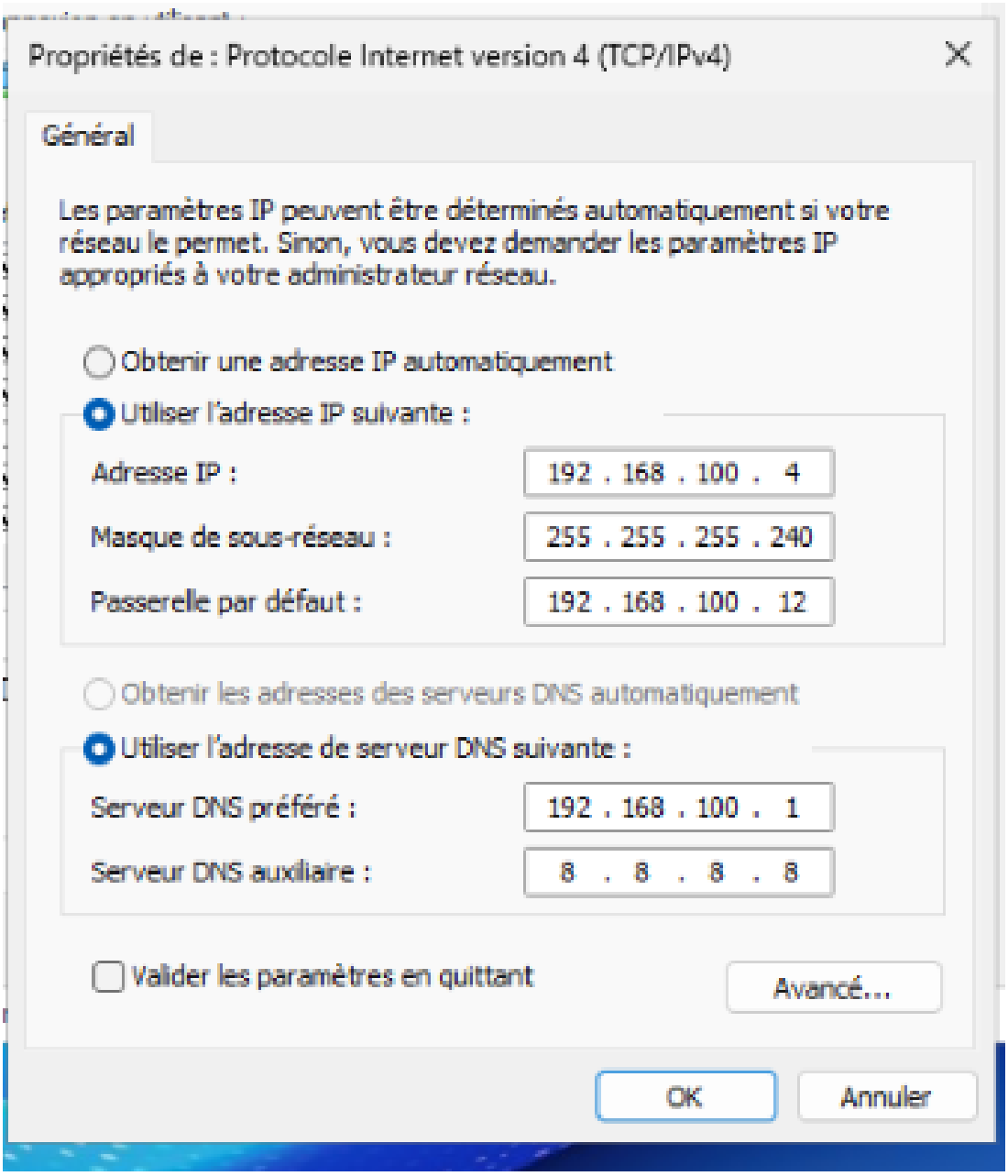
9 Préparation de l'environnement Windows

Avant toute manipulation logicielle, nous devons préparer le socle Windows Server.

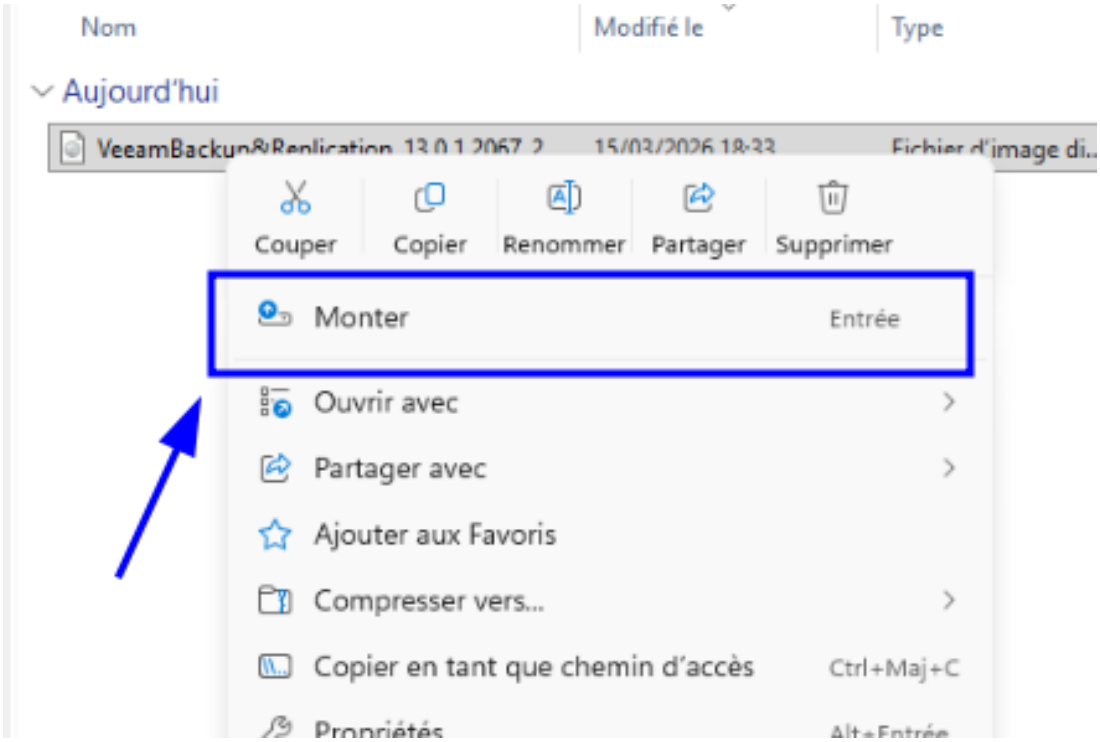
Pour débuter, nous accédons aux propriétés du système afin de renommer l'ordinateur en "WIN-SERV-VEEAM".



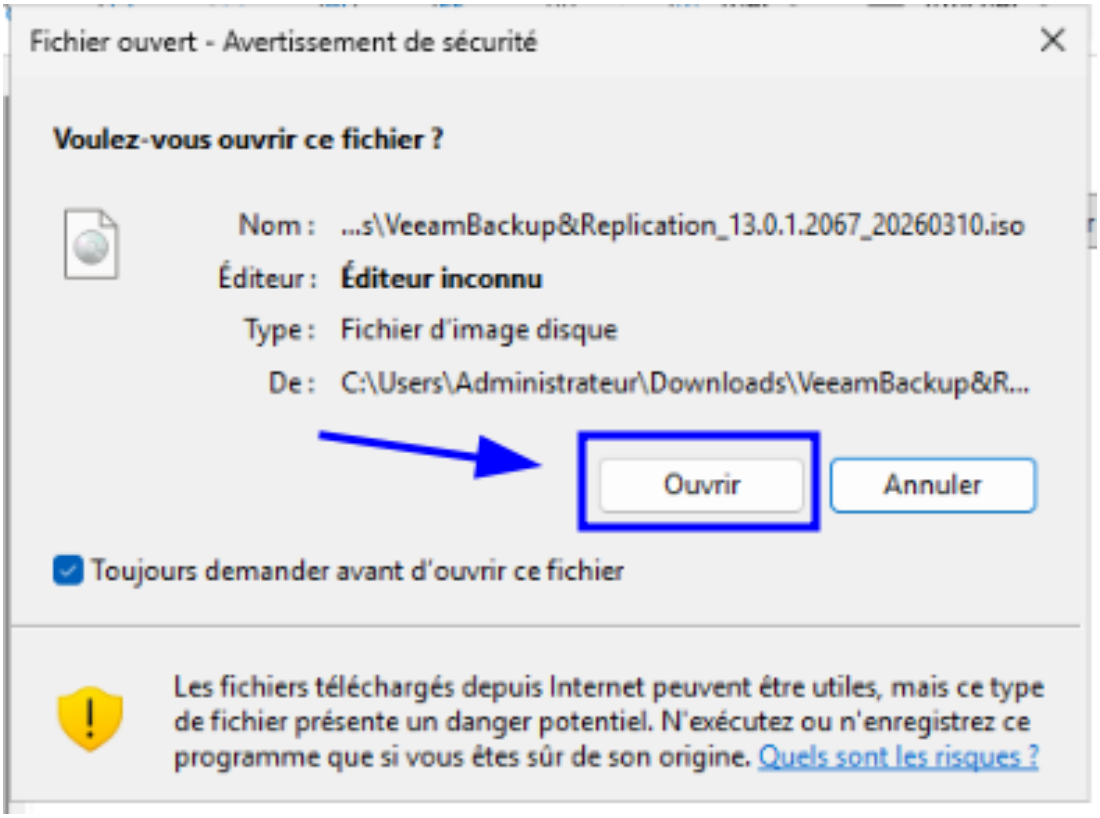
Par la suite, nous configurons les paramètres TCP/IPv4 en fixant l'adresse IP sur 192.168.100.4 avec sa passerelle et ses DNS.



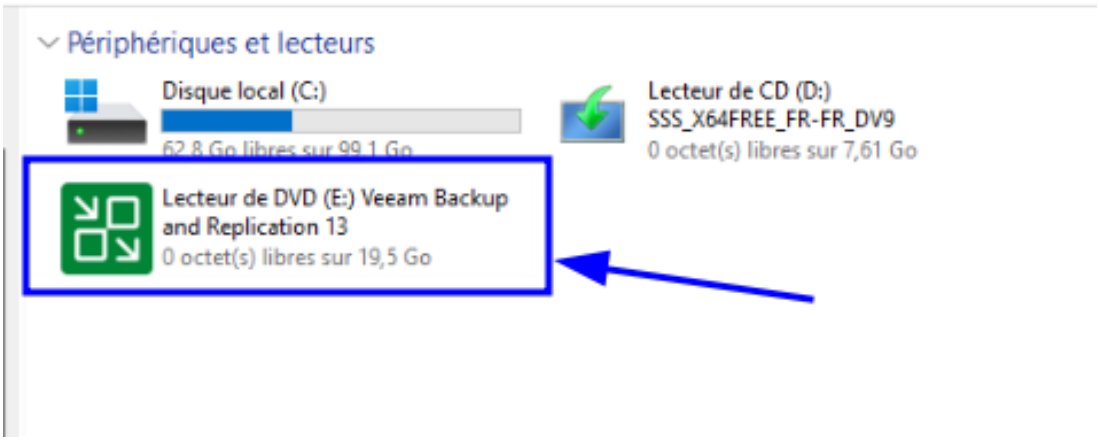
Une fois le réseau stable, nous effectuons un clic droit sur le fichier ISO téléchargé pour sélectionner l'option "Monter".



Aussitôt, nous validons l'avertissement de sécurité Windows en cliquant sur le bouton "Ouvrir" pour accéder au média.

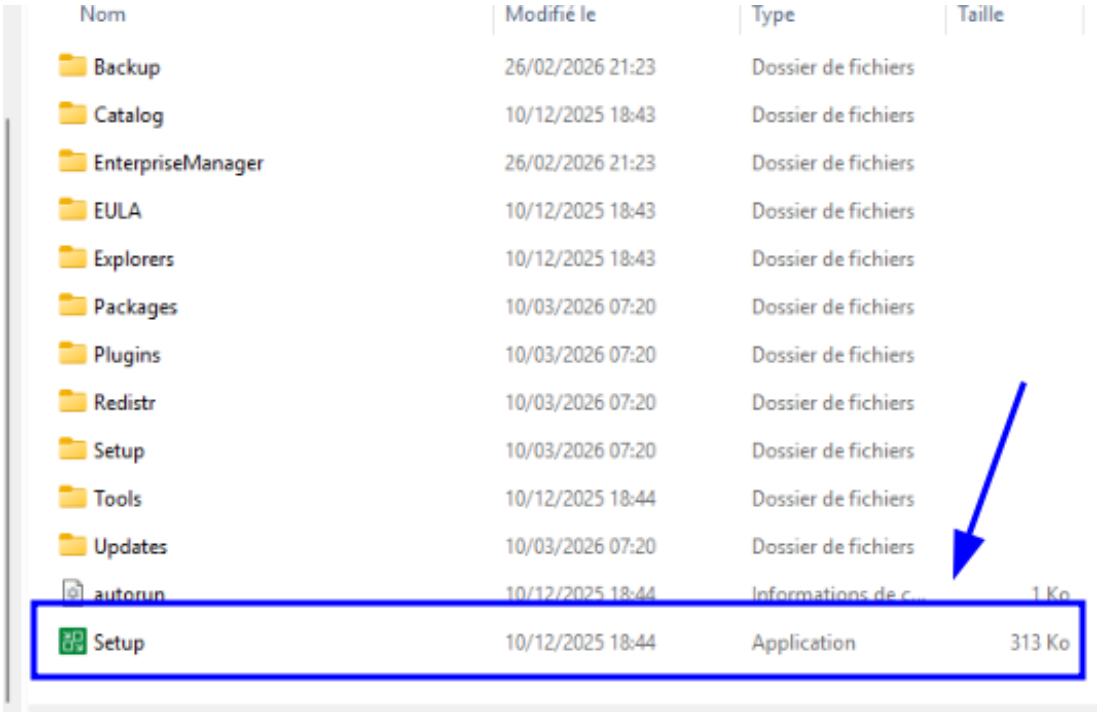


Nous cliquons ensuite sur le lecteur monté afin de rentrer dedans.

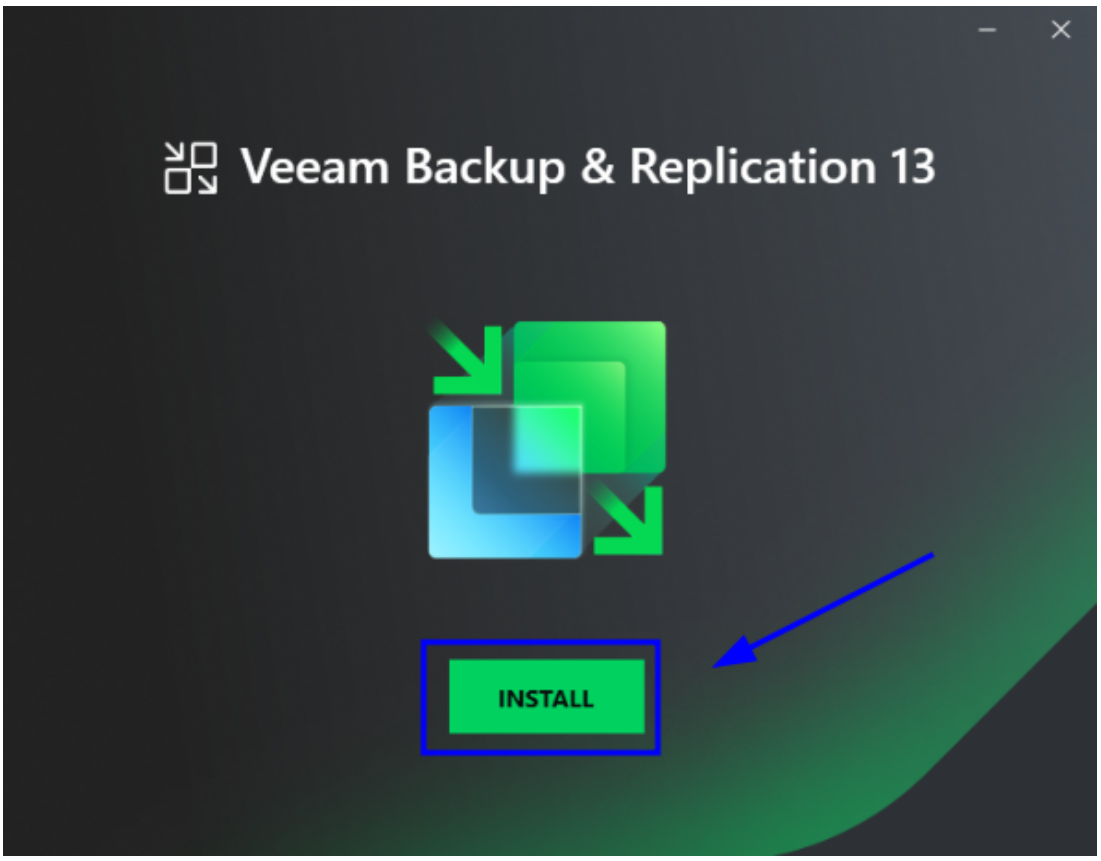


10 Installation de Veeam Backup & Replication

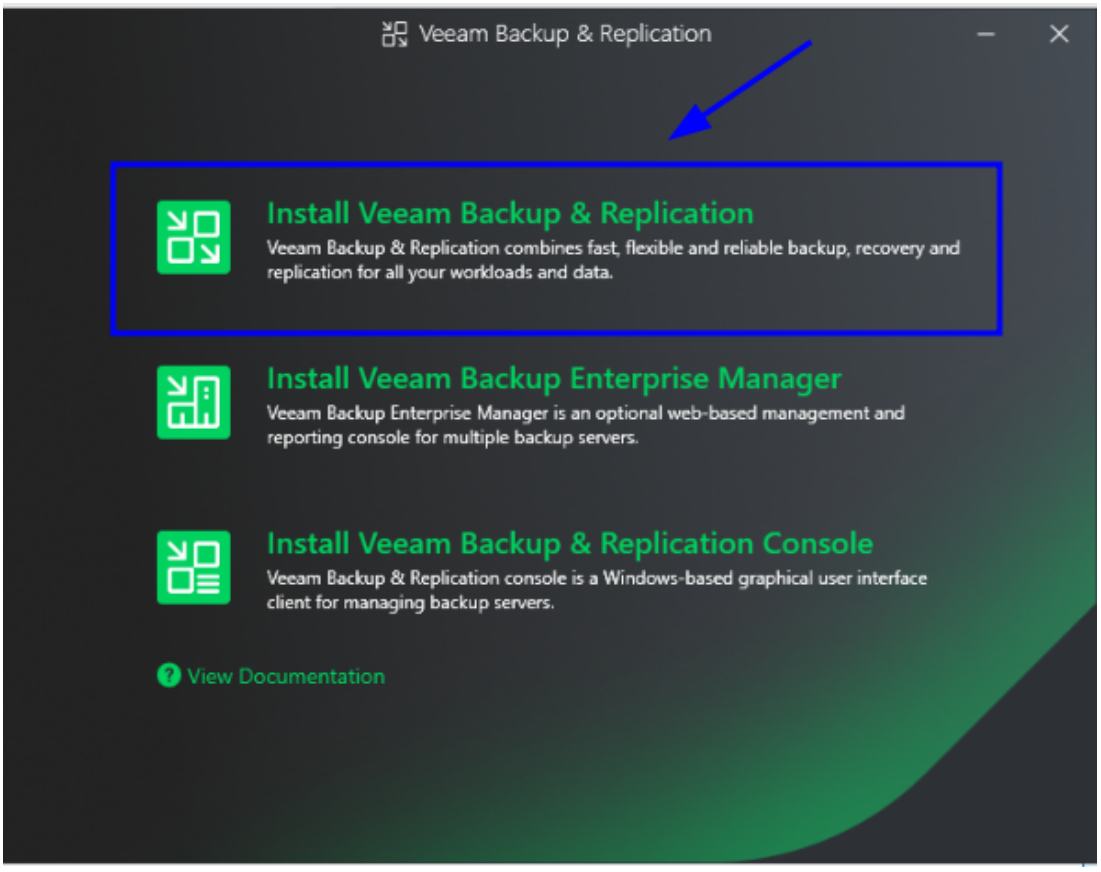
Dès que le contenu du disque virtuel s'affiche, nous localisons et lançons l'application "Setup".



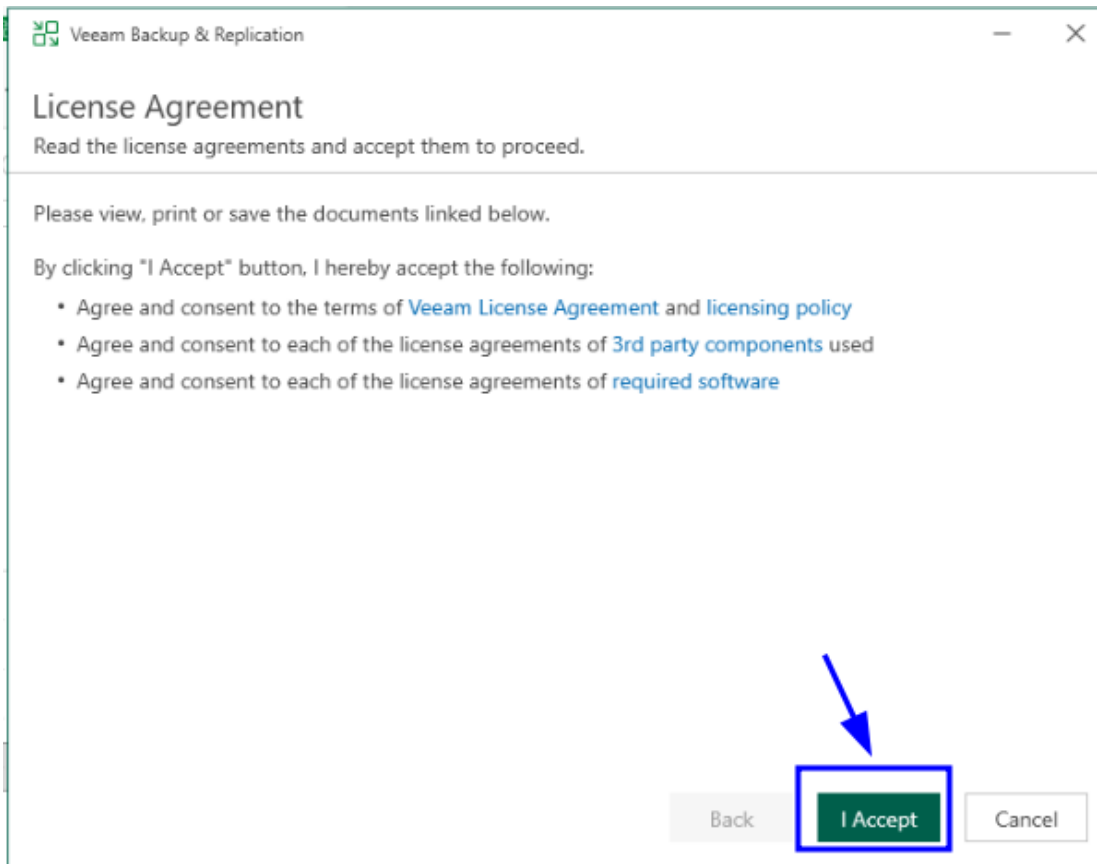
Nous entamons maintenant la phase de déploiement des composants serveurs.
Sur l'écran d'accueil de la version 13, nous cliquons sur le bouton vert "INSTALL".



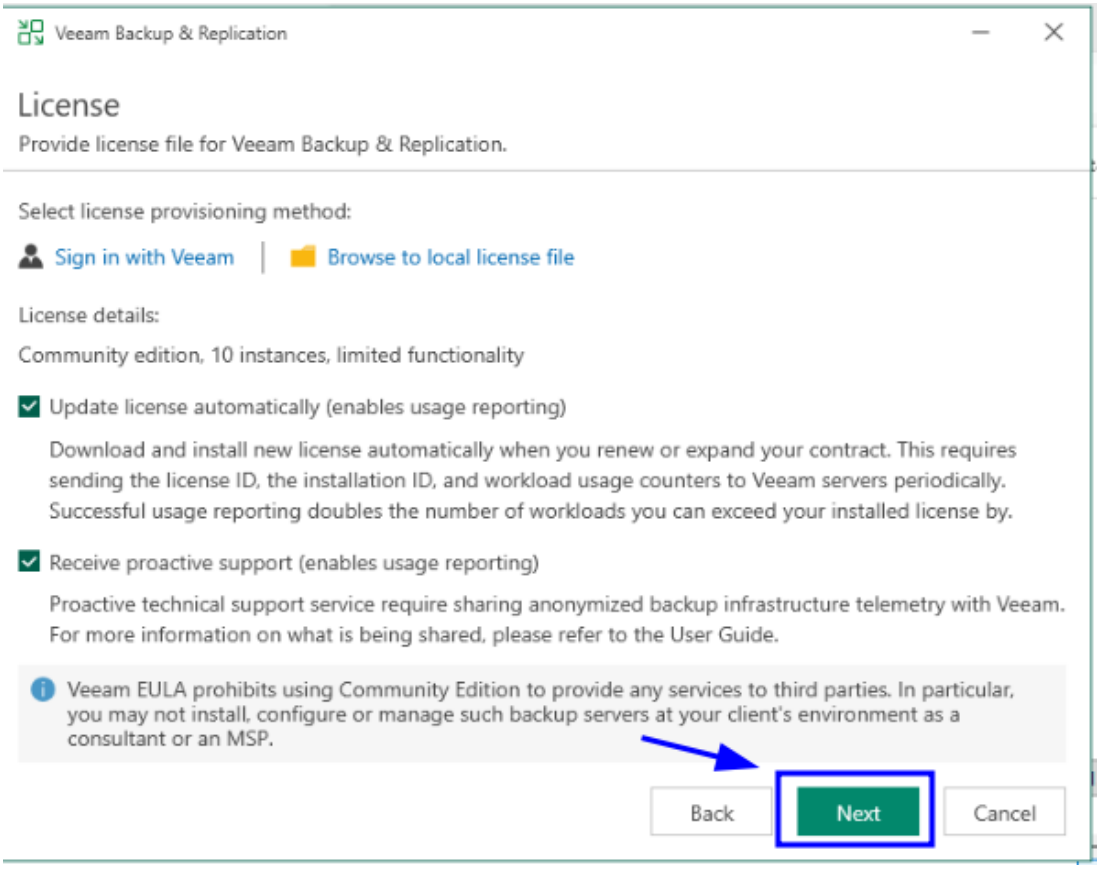
Dans le menu de sélection, nous choisissons d'installer le composant principal "Veeam Backup & Replication".



Ensuite, nous acceptons les termes du contrat de licence en cliquant sur "I Accept".

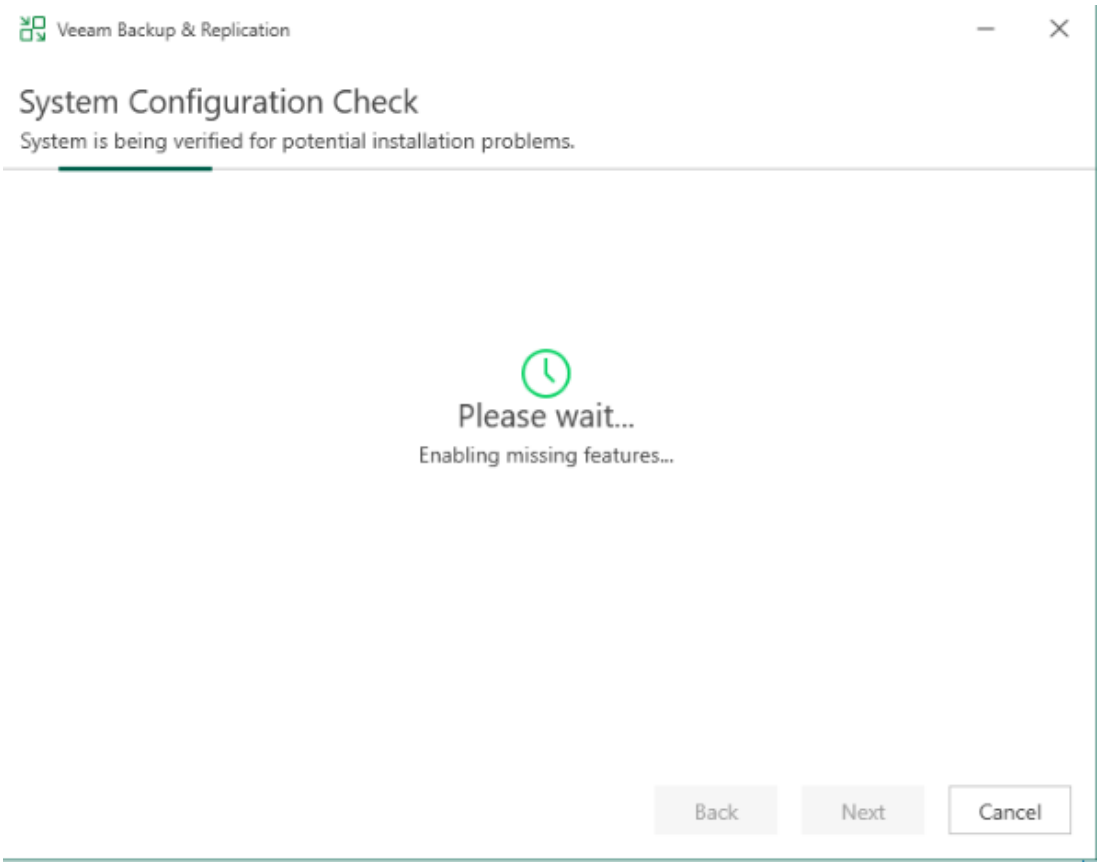


Concernant la licence, nous poursuivons sans fichier externe afin d'utiliser la "Community Edition".

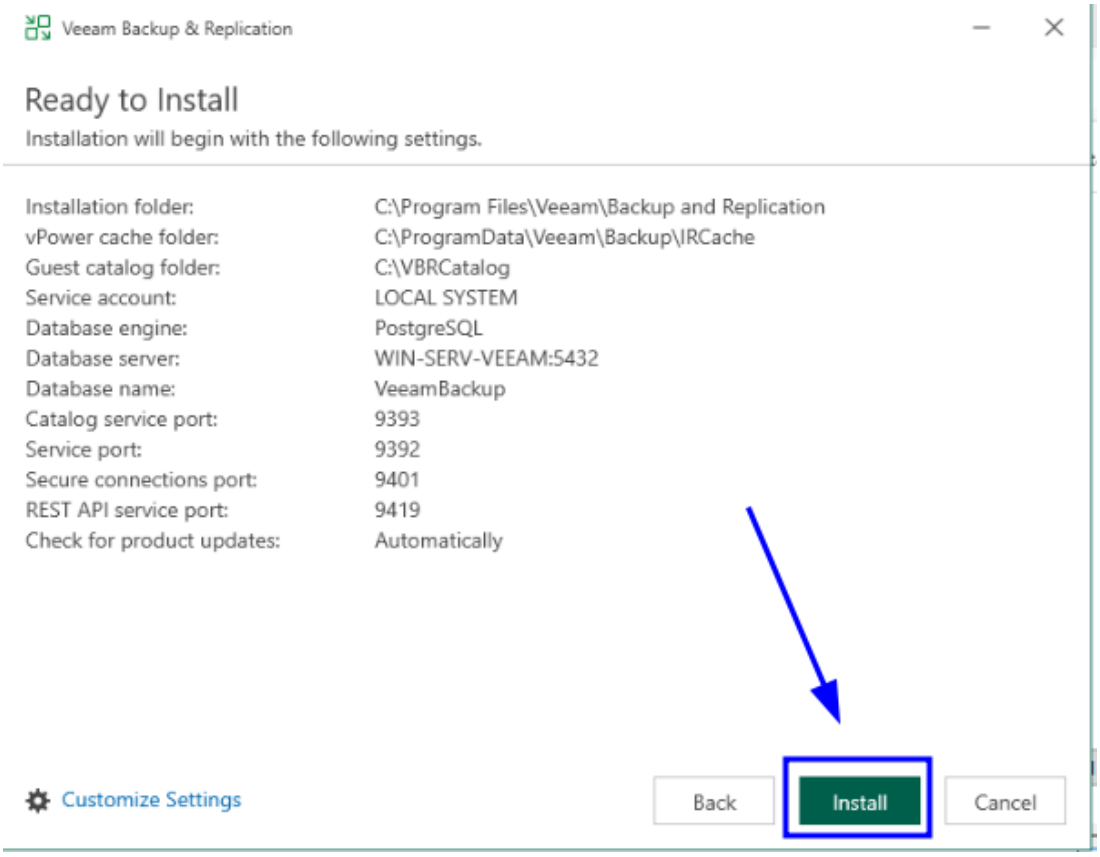


À ce stade, nous laissons l'assistant vérifier la configuration et activer les fonctionnalités

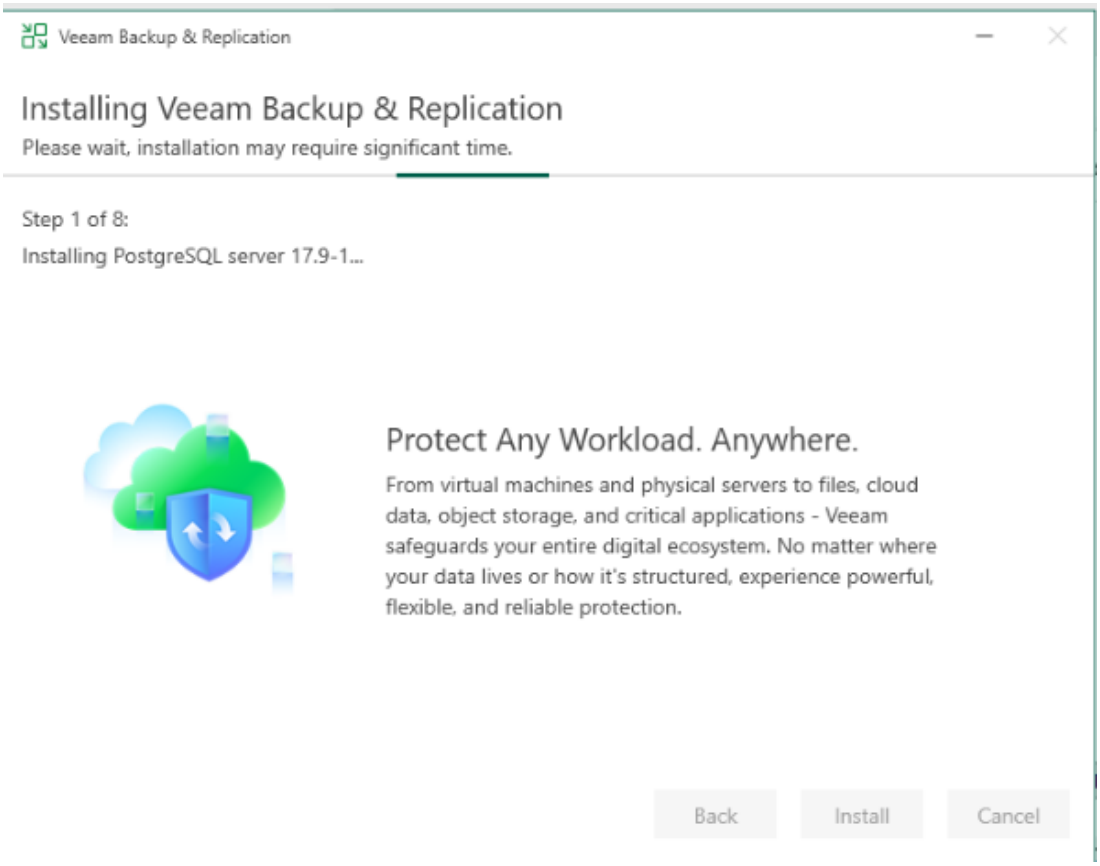
système requises.



Avant de lancer la copie, nous vérifions le résumé des ports et de l'instance PostgreSQL puis cliquons sur "Install".

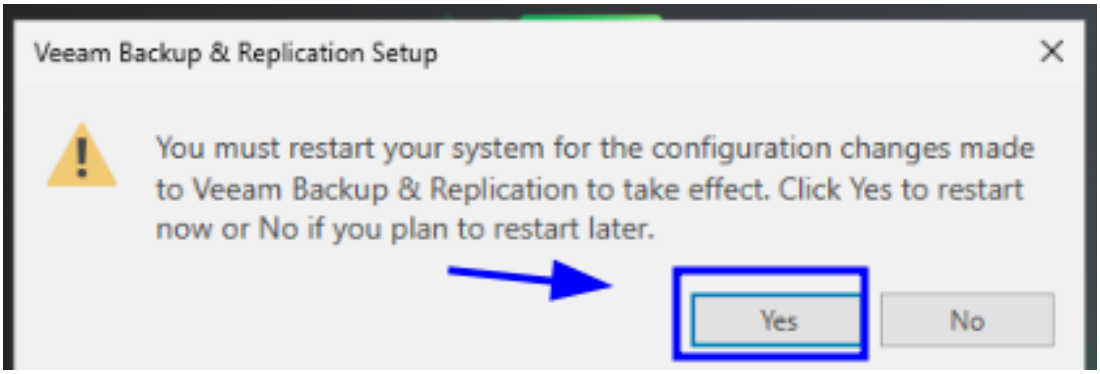


Progressivement, nous suivons la barre d'avancement de l'installation des différents packages.



Une fois l'opération terminée avec succès, nous fermons l'installeur en cliquant sur "Finish"

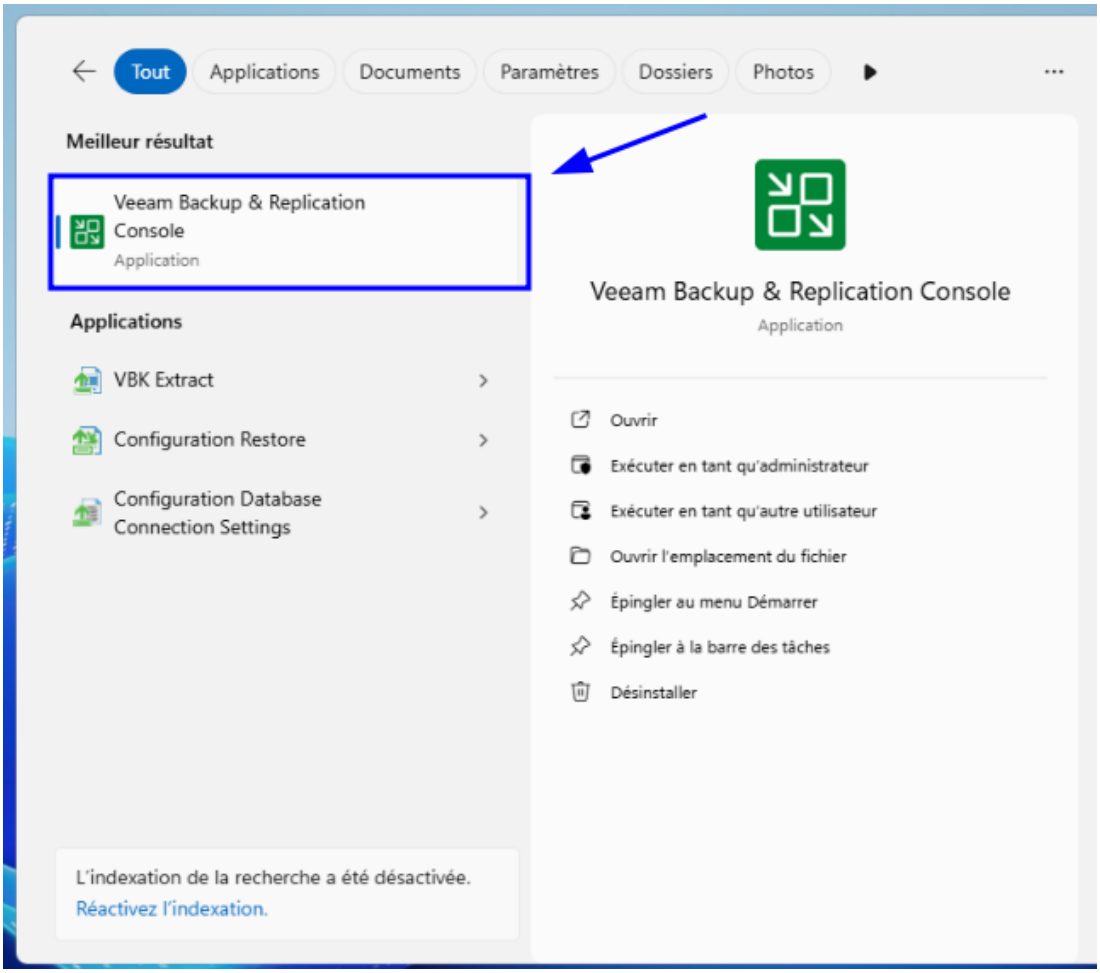
Enfin, nous acceptons le redémarrage immédiat du serveur pour appliquer les modifications finales.



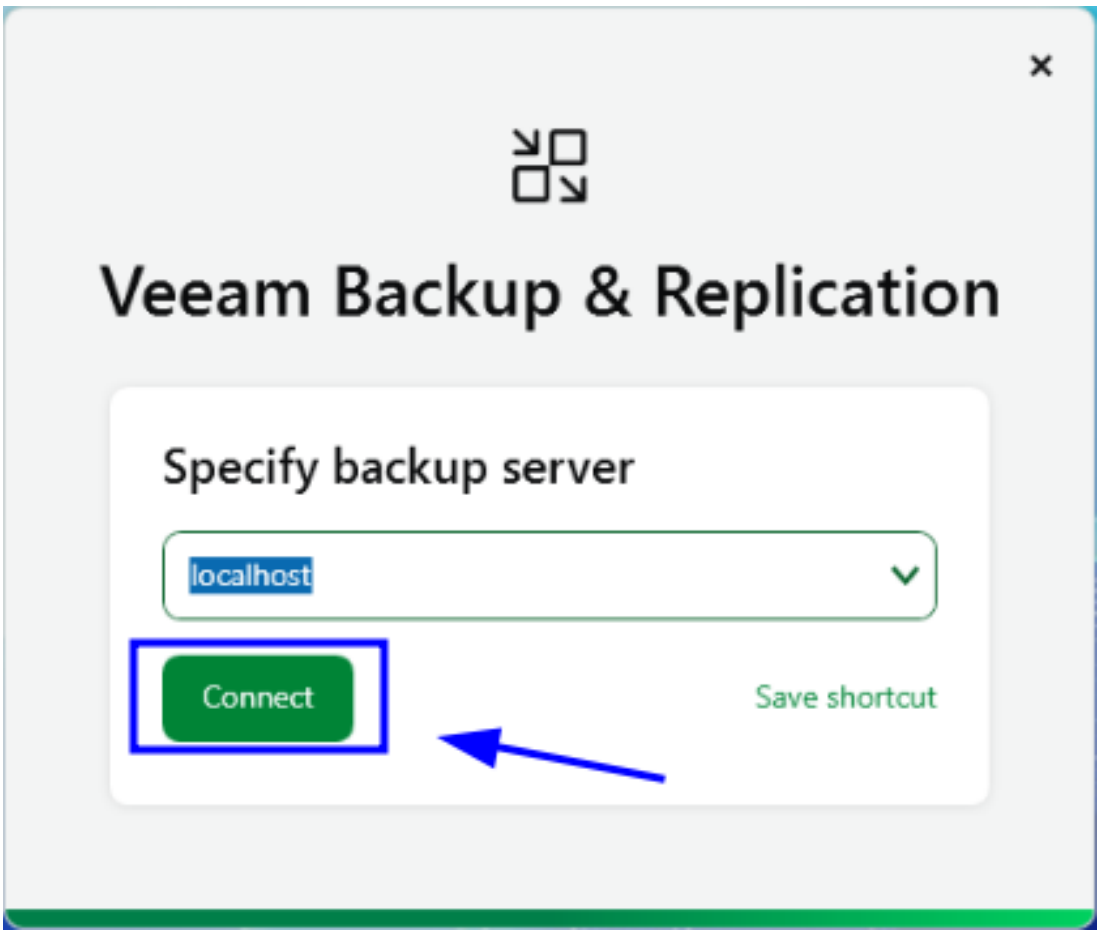
11 Connexion à la Console de gestion

Le serveur étant opérationnel, nous allons maintenant initialiser l'interface de pilotage.

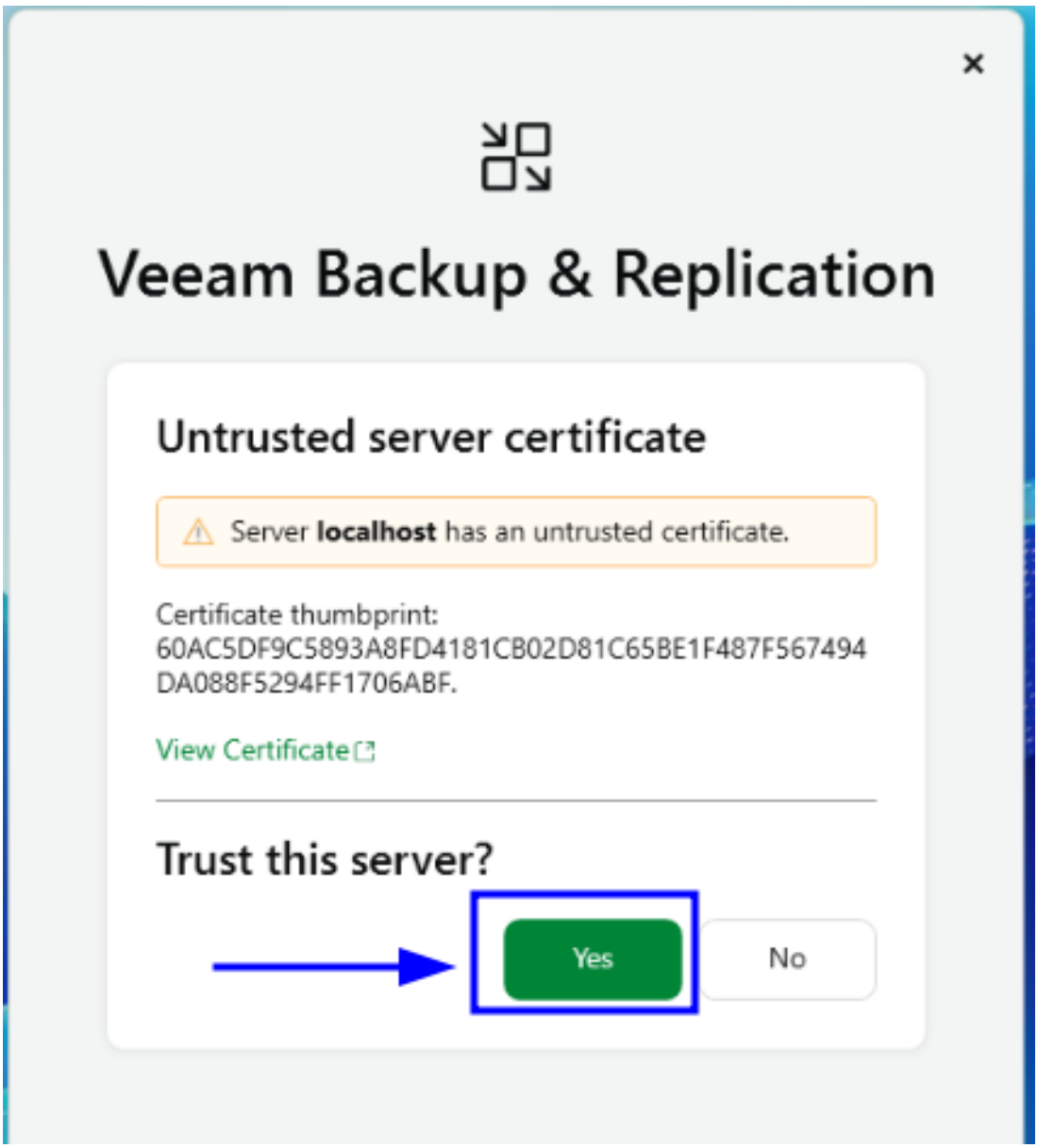
Dans le menu de recherche Windows, nous lançons l'application "Veeam Backup & Replication Console".



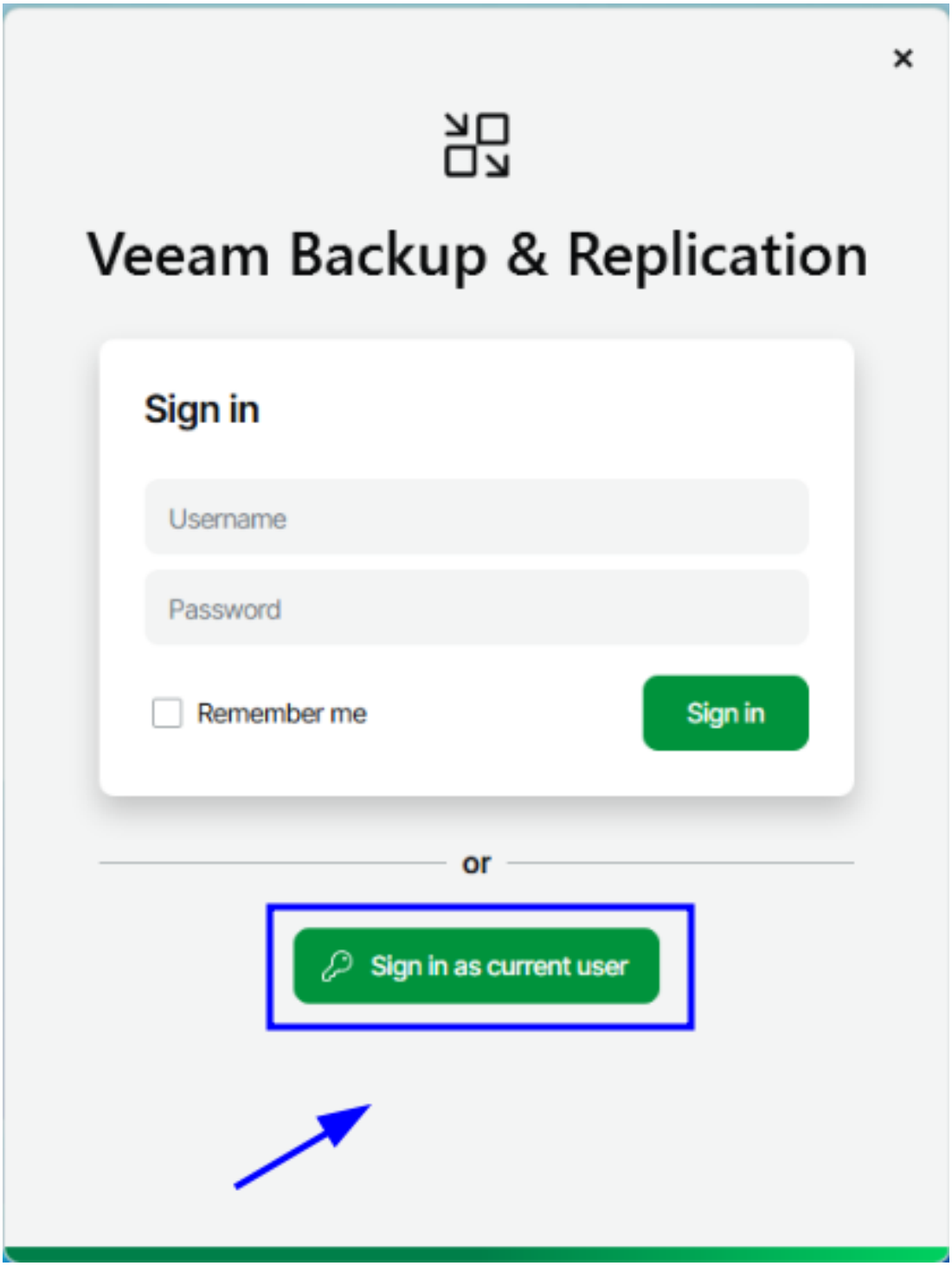
Dans la fenêtre de connexion, nous spécifions le serveur "localhost" et cliquons sur "Connect".



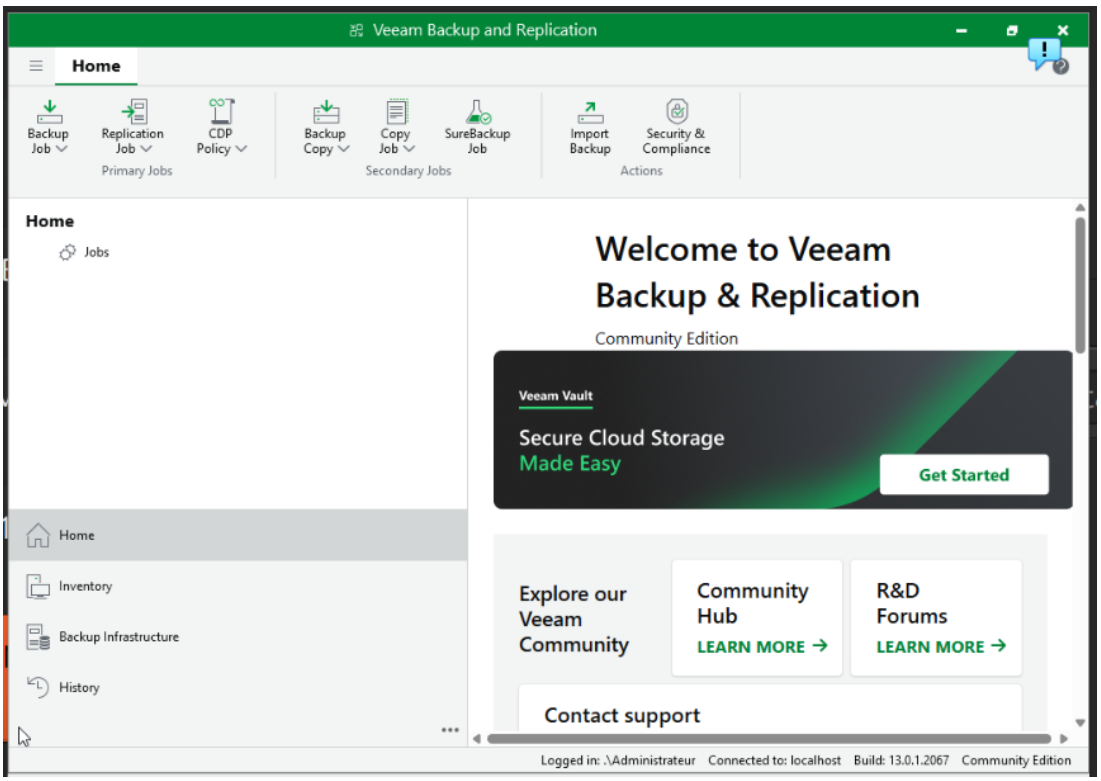
Face au message sur le certificat non approuvé, nous cliquons sur "Yes" pour confirmer la confiance. À ce moment-là, nous pouvons visualiser l'empreinte numérique du certificat SSL du serveur.



Pour accéder à l'interface, nous optons pour la connexion simplifiée "Sign in as current user".



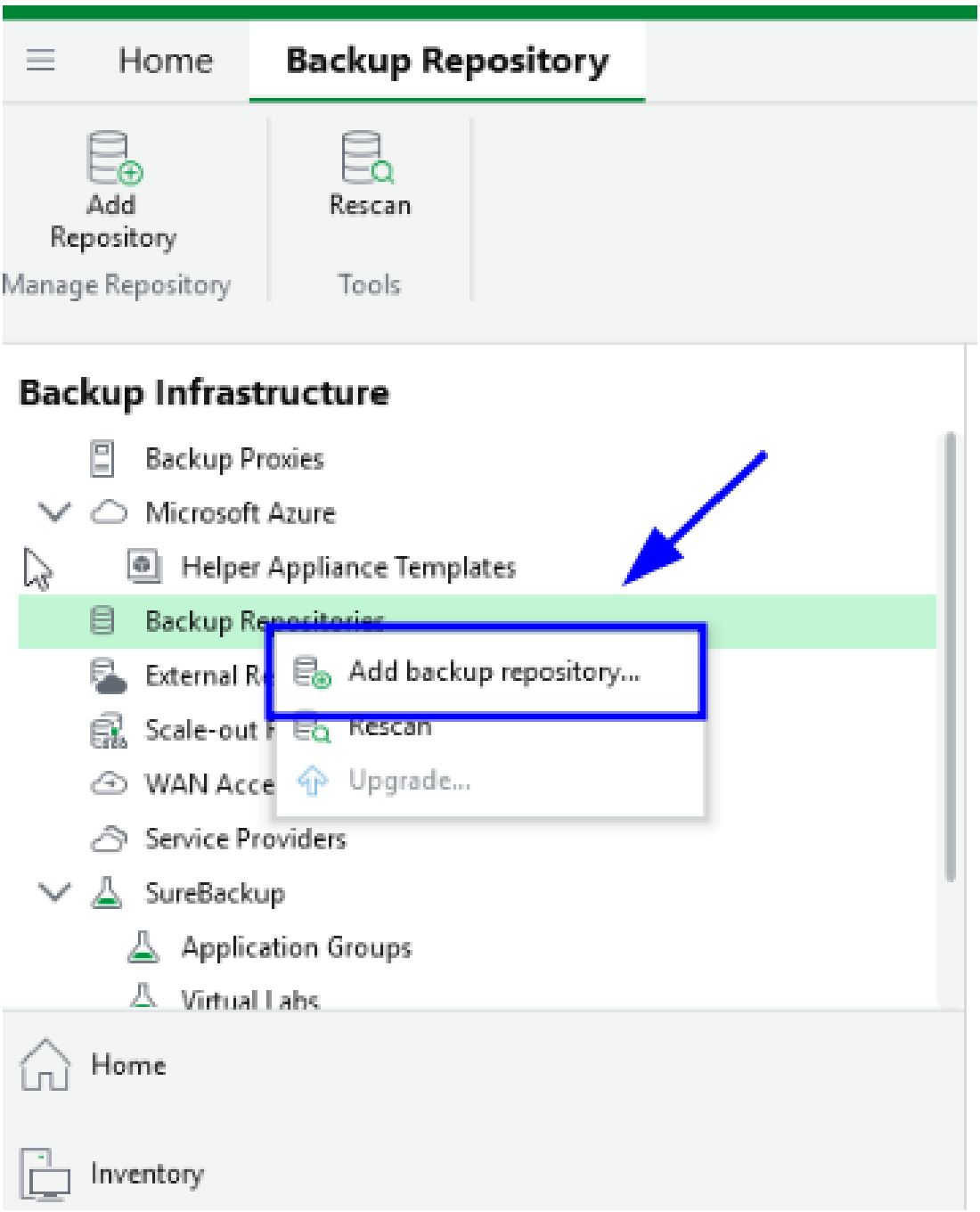
Finalement, nous arrivons sur le tableau de bord principal nous souhaitant la bienvenue.



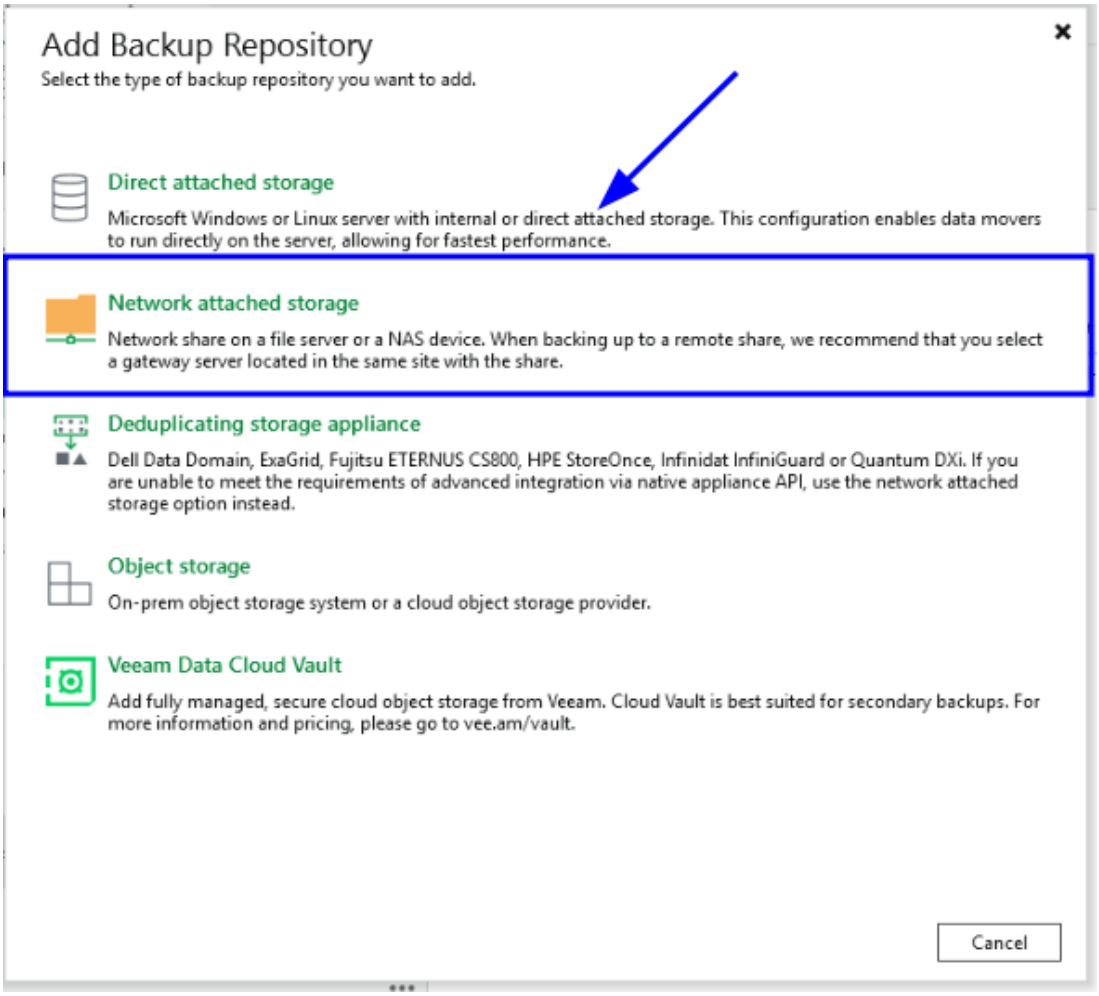
12 Configuration du Backup Repository (Stockage)

Nous devons maintenant déclarer l'espace où seront stockées nos données de sauvegarde.

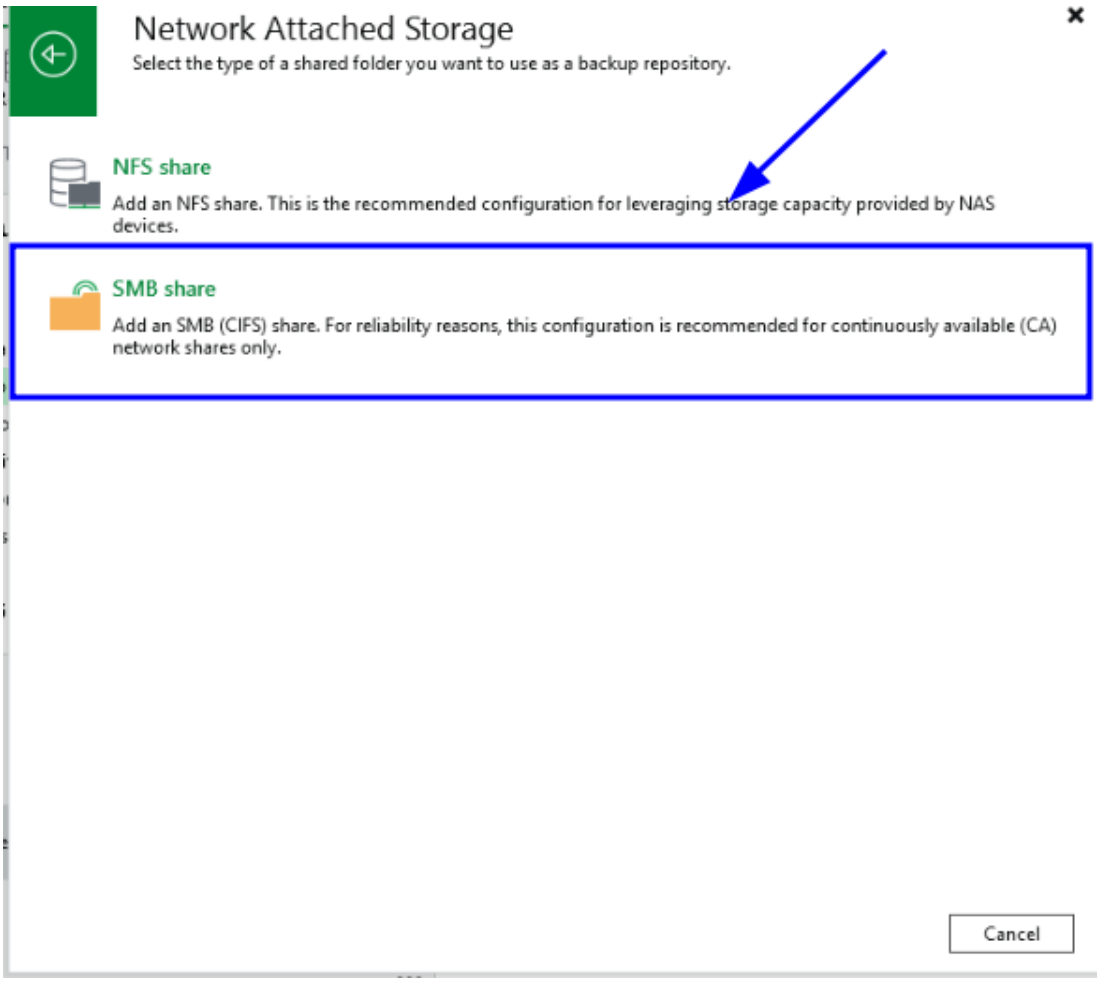
Aussitôt, nous effectuons un clic droit sur "Backup Repositories" pour choisir "Add backup repository".



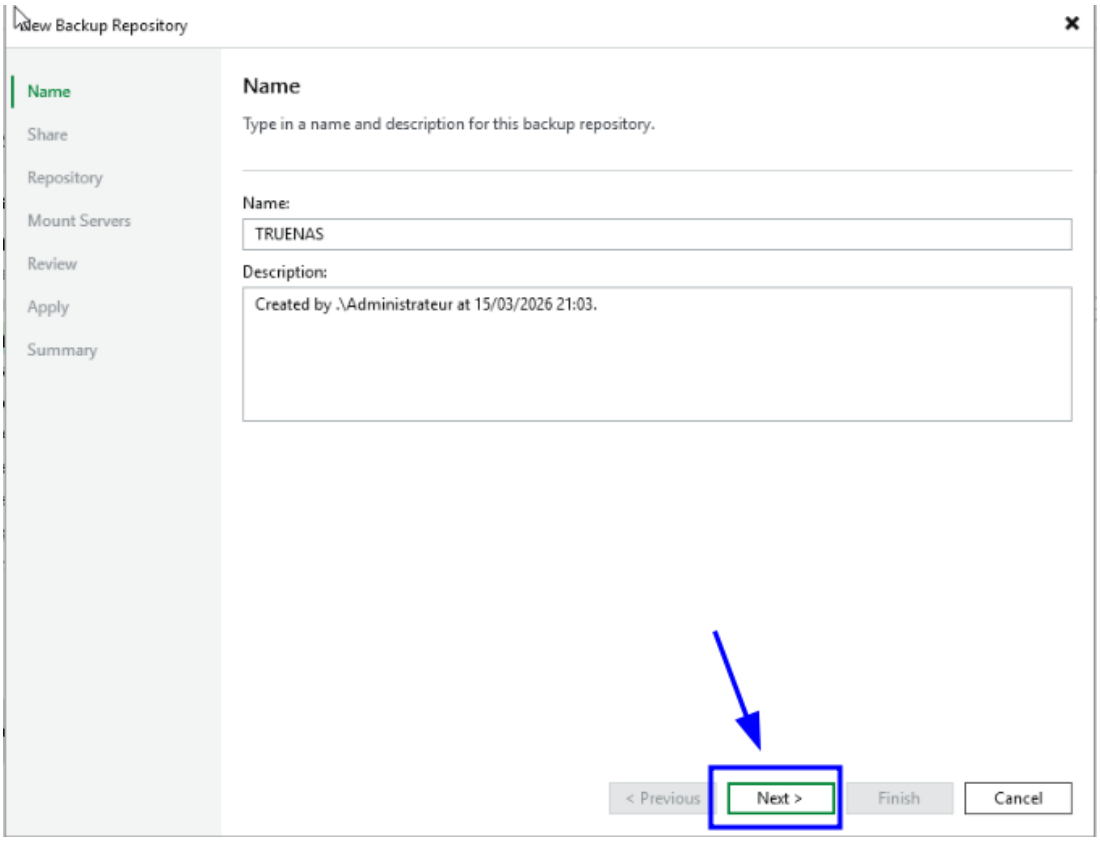
Dans le menu des types de stockage, nous sélectionnons l'option "Network attached storage".



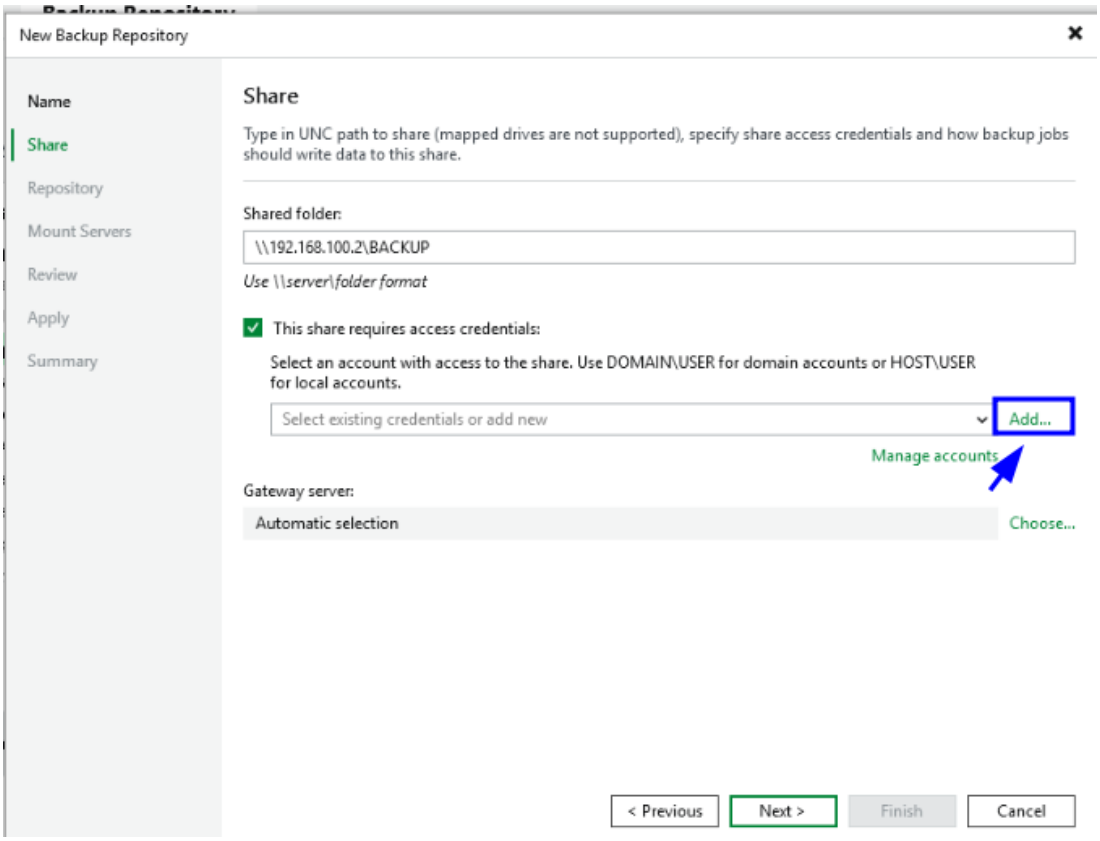
Puis, nous choisissons le protocole "SMB share" pour notre partage réseau.



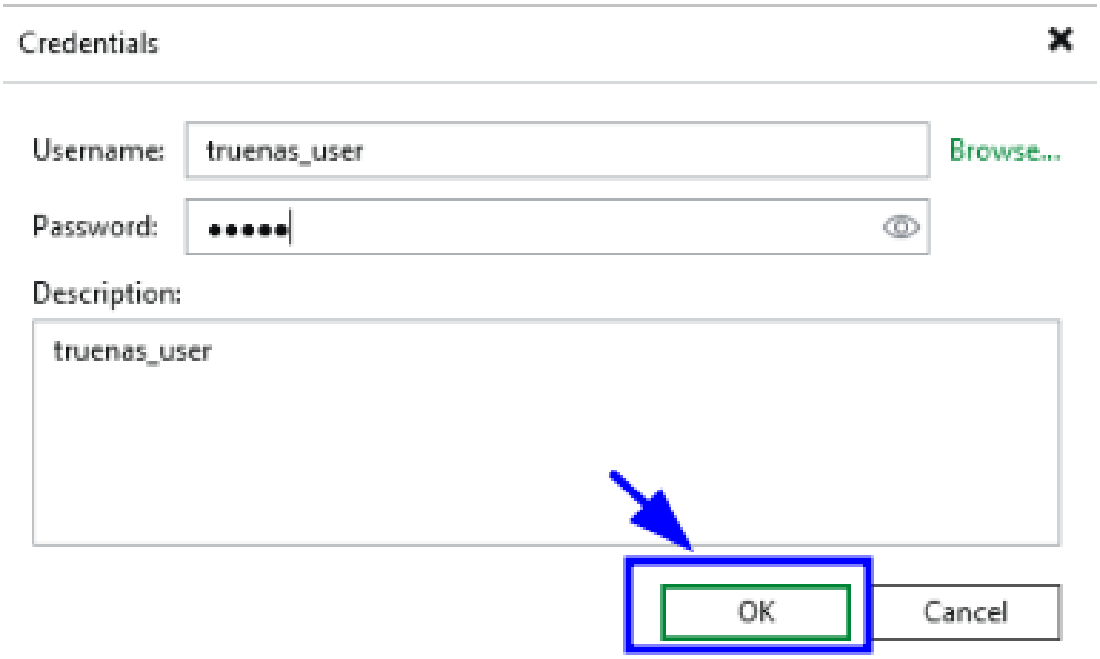
Pour identifier le dépôt, nous saisissons le nom "TRUENAS" dans l'assistant.



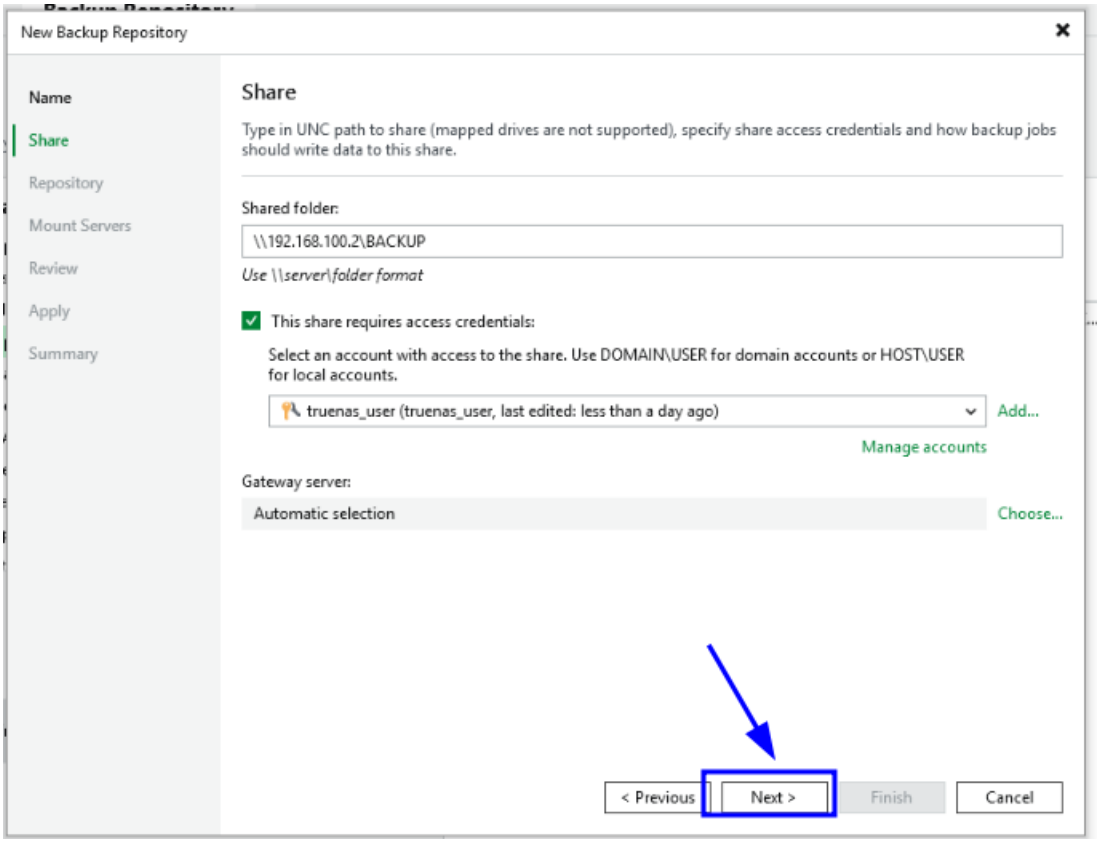
Il nous faut alors renseigner le chemin UNC du partage : \\192.168.100.2\BACKUP. Simultanément, nous cliquons sur "Add" afin d'ajouter les credentials de la machine.



Nous renseignons le compte "truenas_user" et son mot de passe.

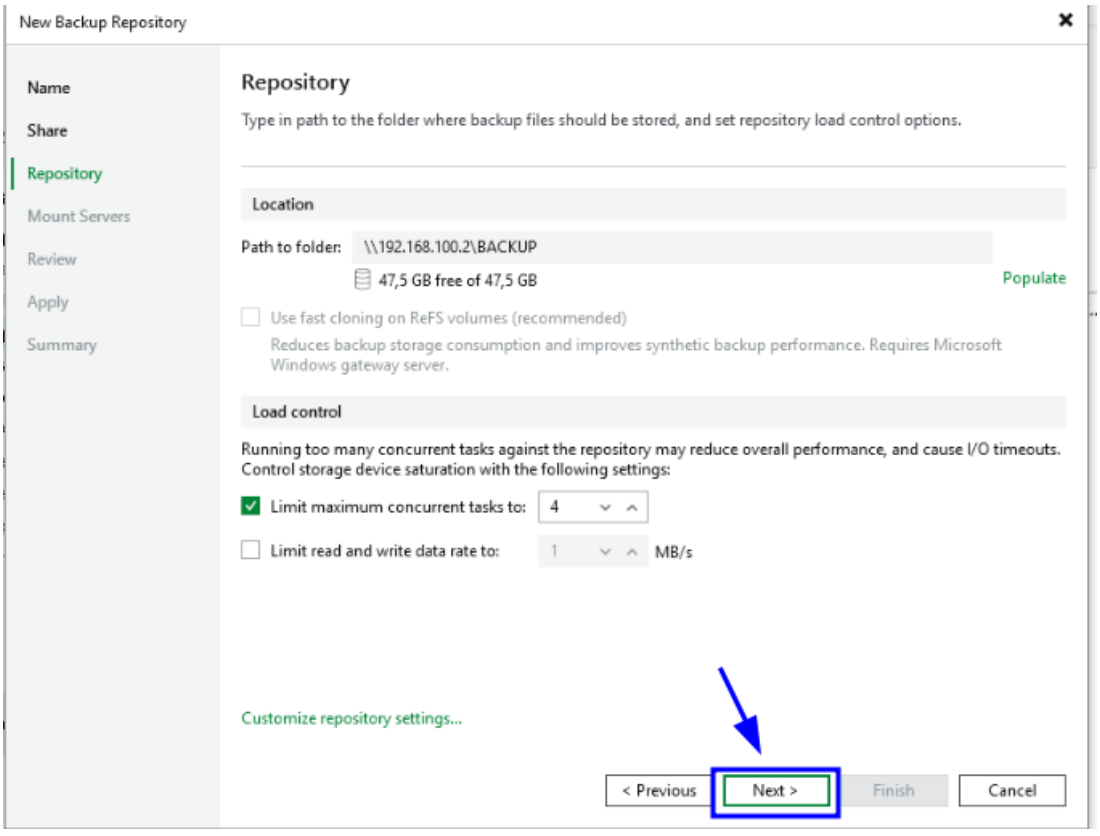


Nous passons après cela à la suite.

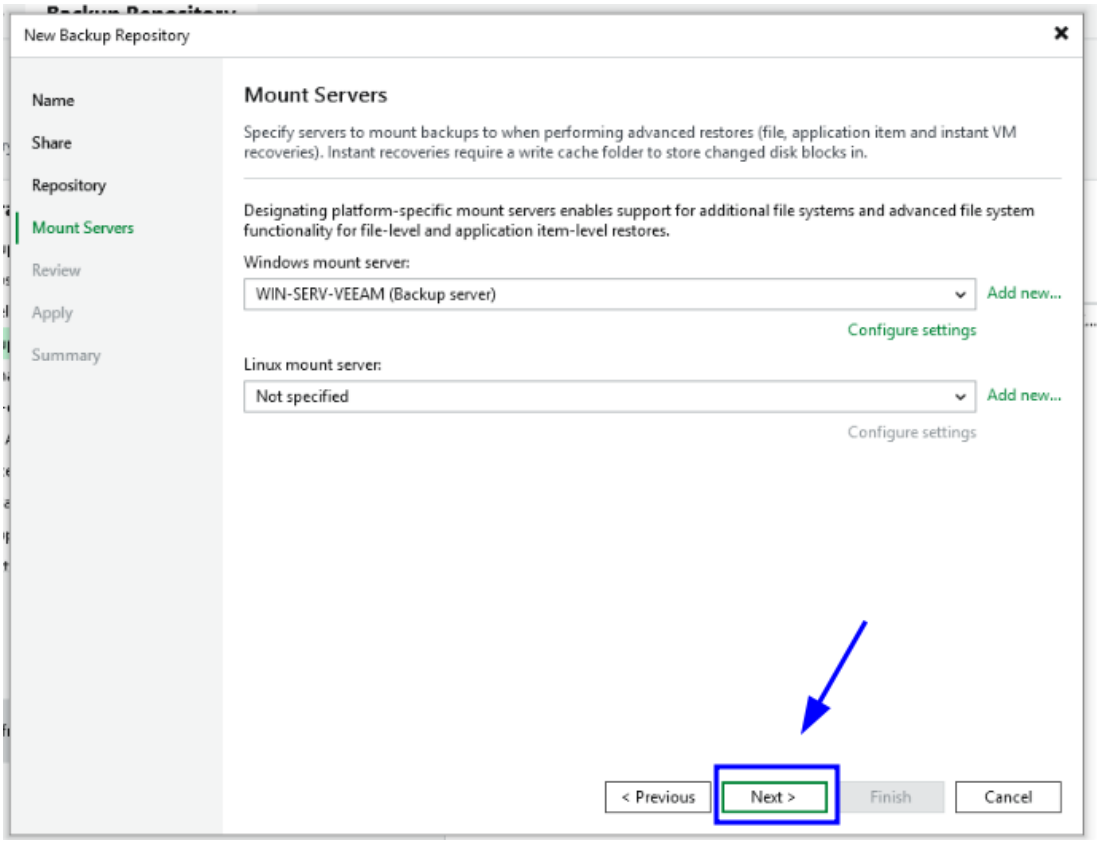


Après avoir validé les accès, nous cliquons sur "Populate" pour scanner l'espace disque disponible. Puis nous passons à la suite.

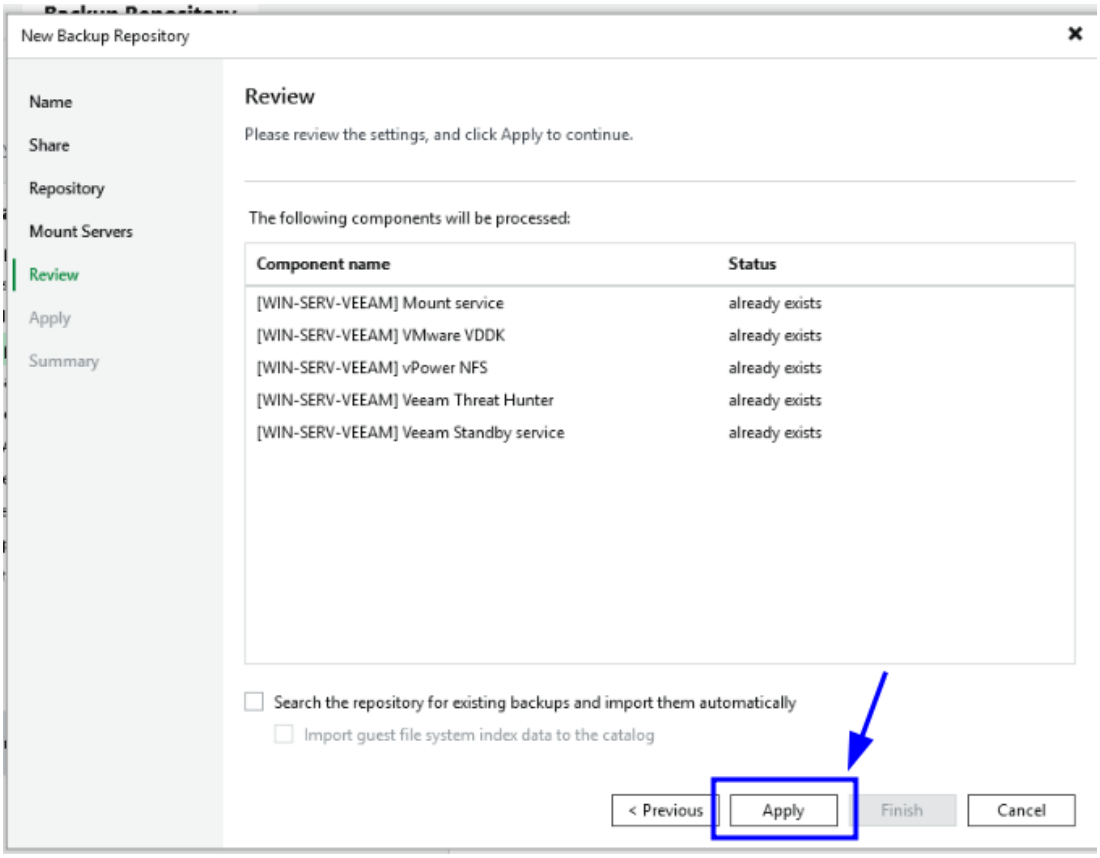
Par mesure de performance, nous limitons ici le nombre de tâches simultanées à 4.



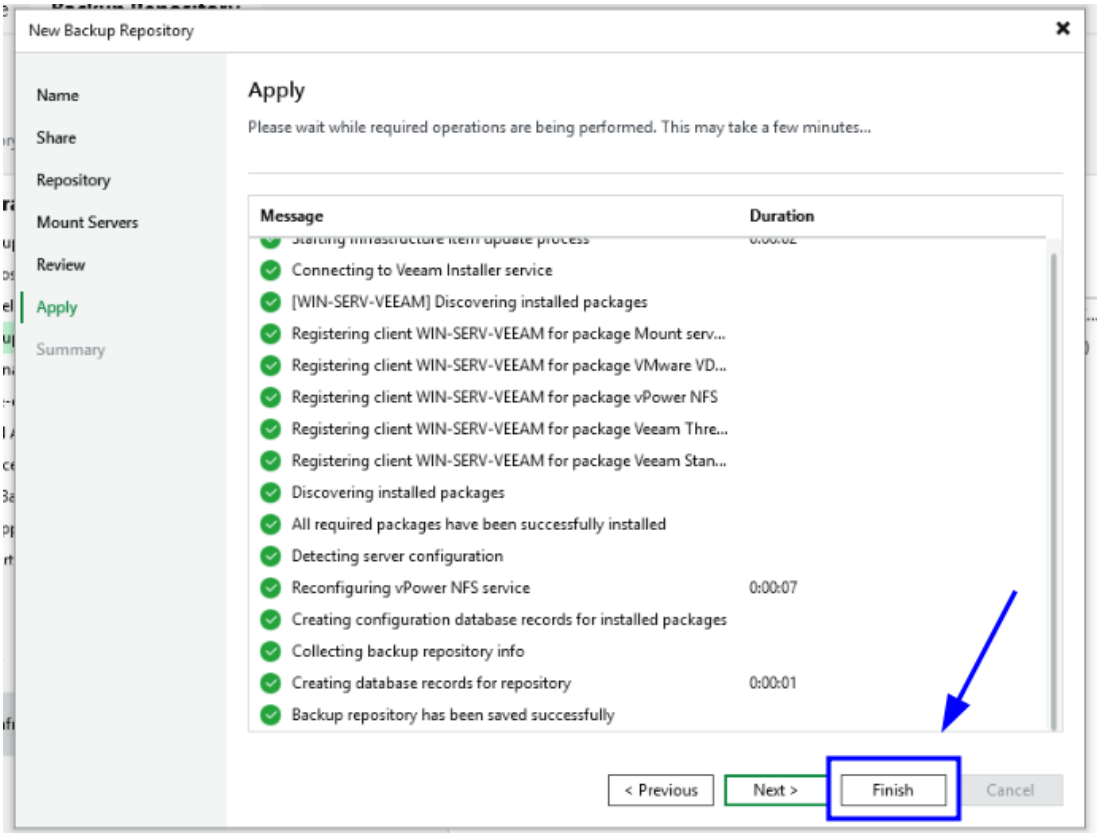
Nous confirmons ensuite que le serveur local sera utilisé comme point de montage (Mount Server).



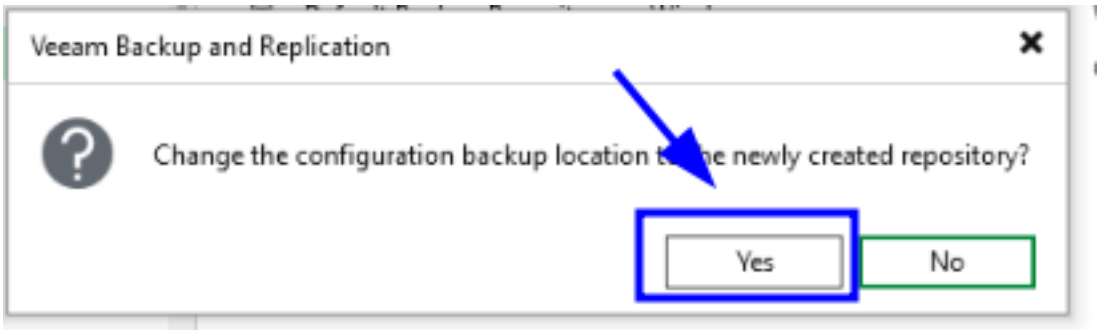
À ce stade, nous passons en revue la liste des composants logiciels qui vont être déployés ou qui sont déjà installé.



Pendant l'application des paramètres, nous suivons l'avancement de l'installation des agents. Puis une fois celle-ci terminer on appuie sur "Finish".



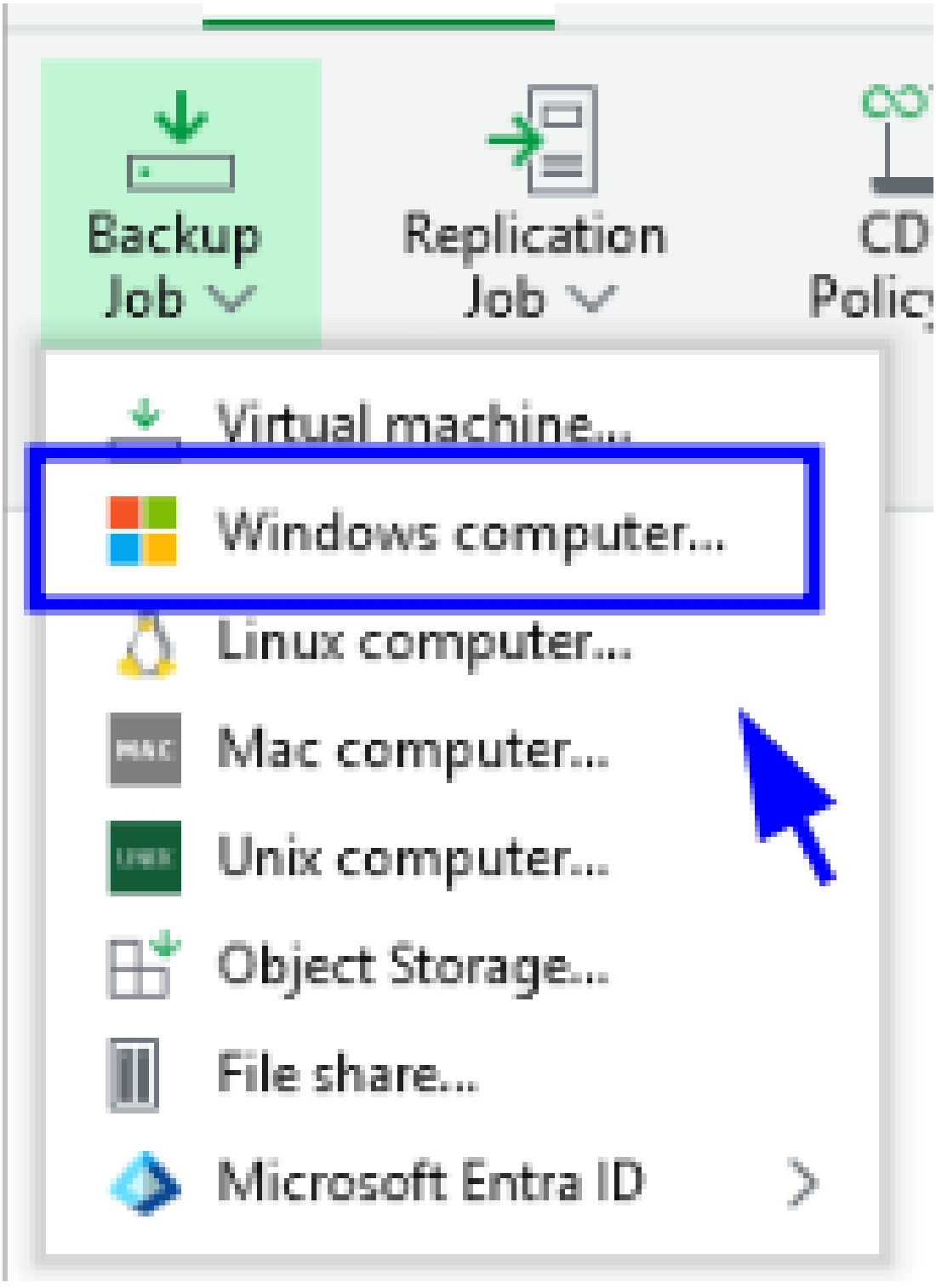
Une fenêtre nous demande alors de confirmer l'utilisation de ce dépôt pour les sauvegardes de configuration.



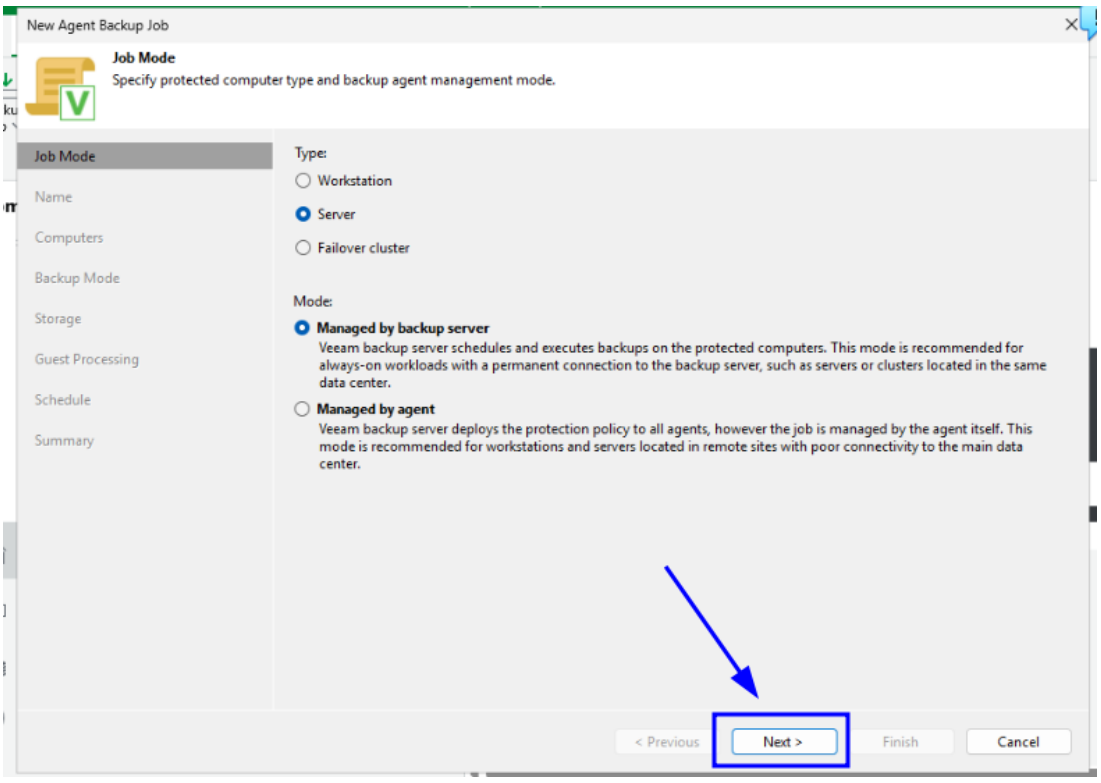
13 Création d'une tâche de sauvegarde (Job)

La mise en place se termine par la configuration d'un Job pour protéger un ordinateur Windows.

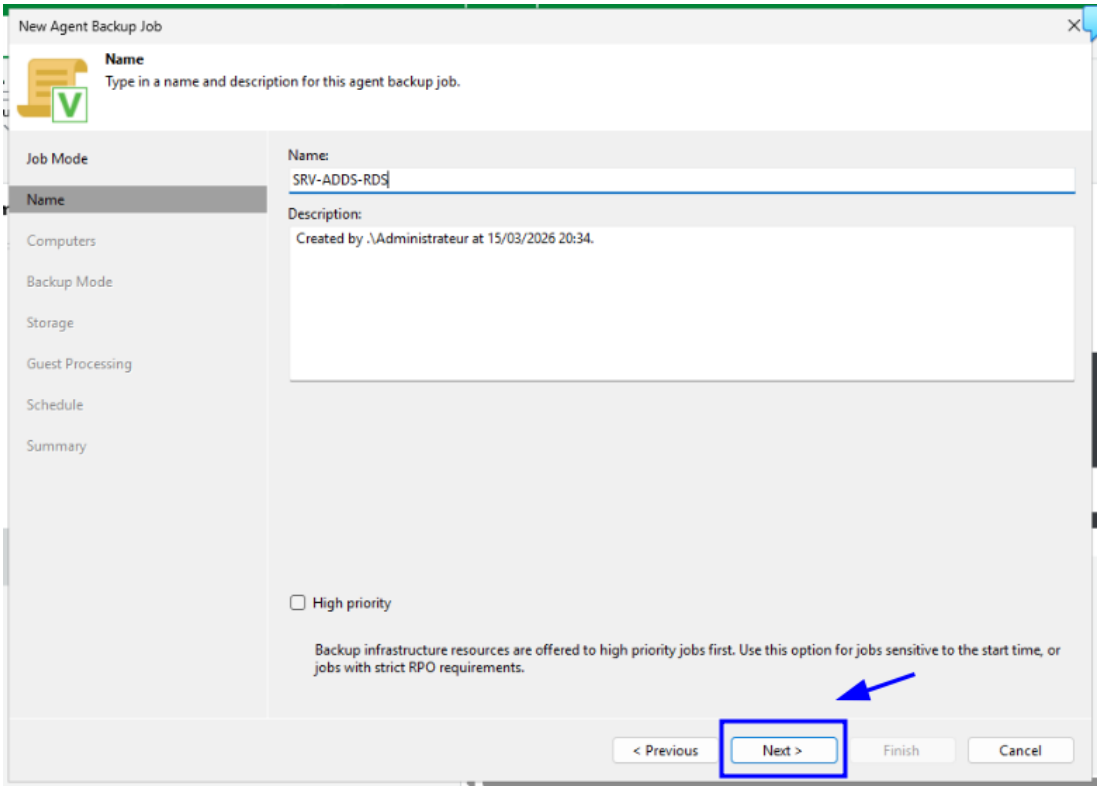
D'abord, nous ouvrons le menu "Backup Job" et sélectionnons "Windows computer".



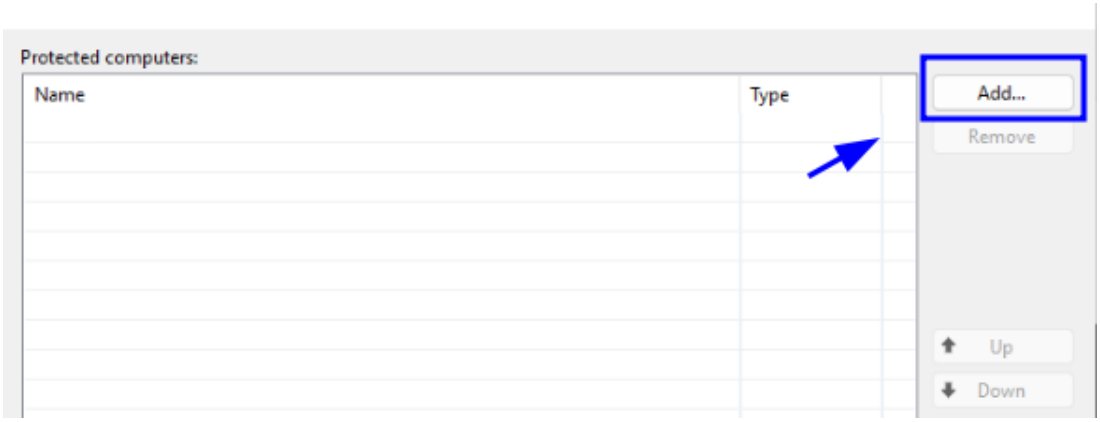
Nous définissons le type de job sur "Server" et le mode sur "Managed by backup server".



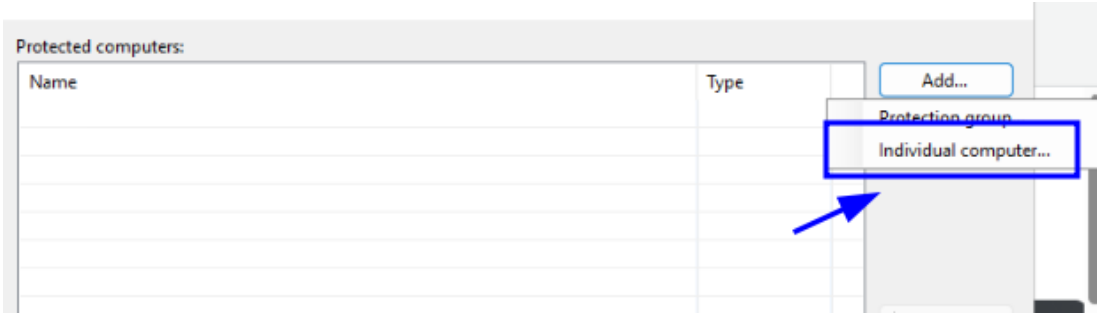
Ensuite, nous nommons cette nouvelle tâche "SRV-ADDS-RDS" afin de pouvoir la retrouver facilement.



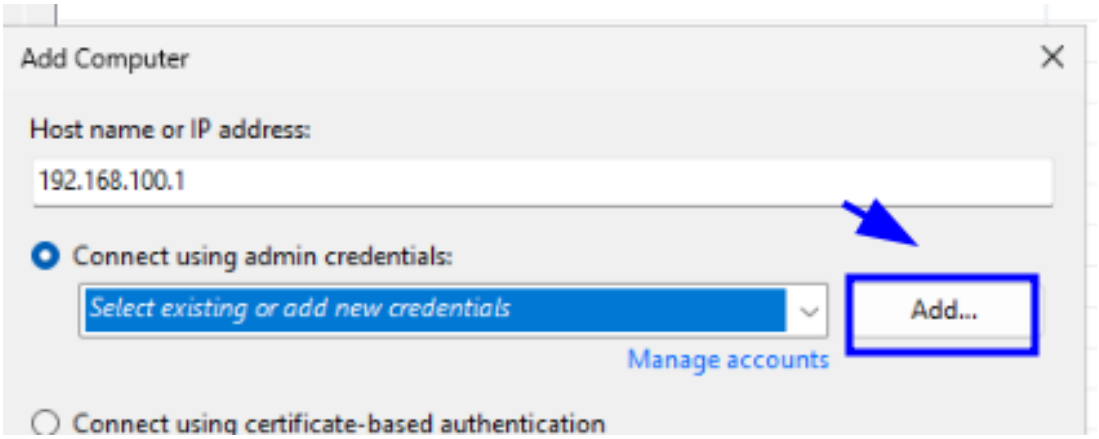
Nous allons ensuite ajouter le serveur que l'on souhaite sauvegarder, pour cela on commence en appuyant sur "Add".



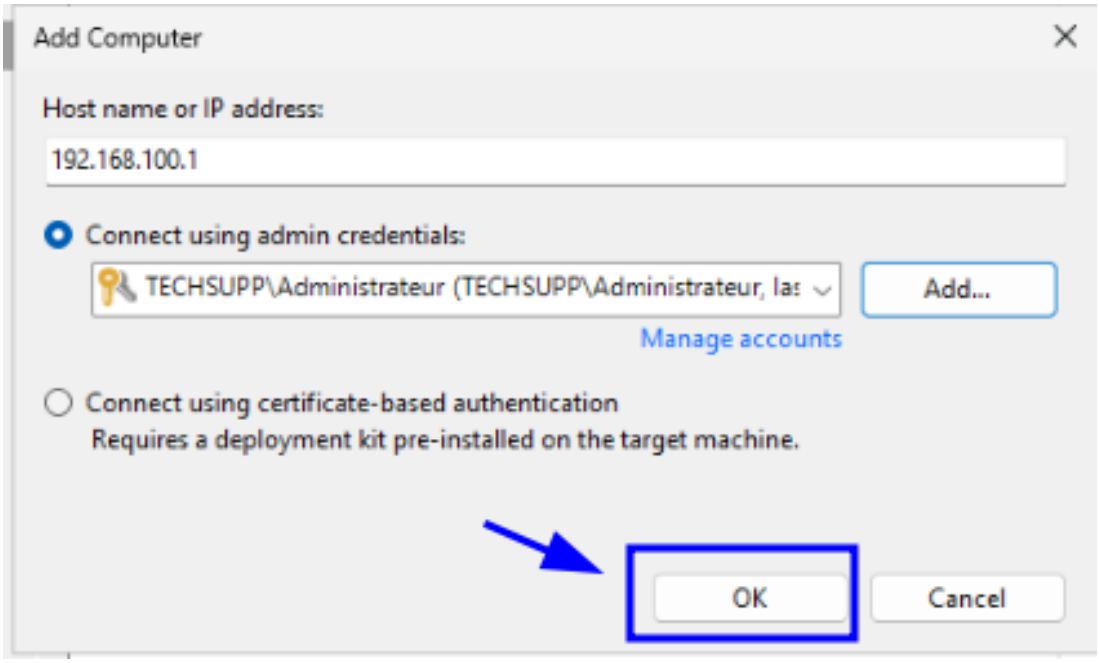
Puis nous allons spécifier que c'est un ordinateur seul que nous souhaitons sauvegarder.

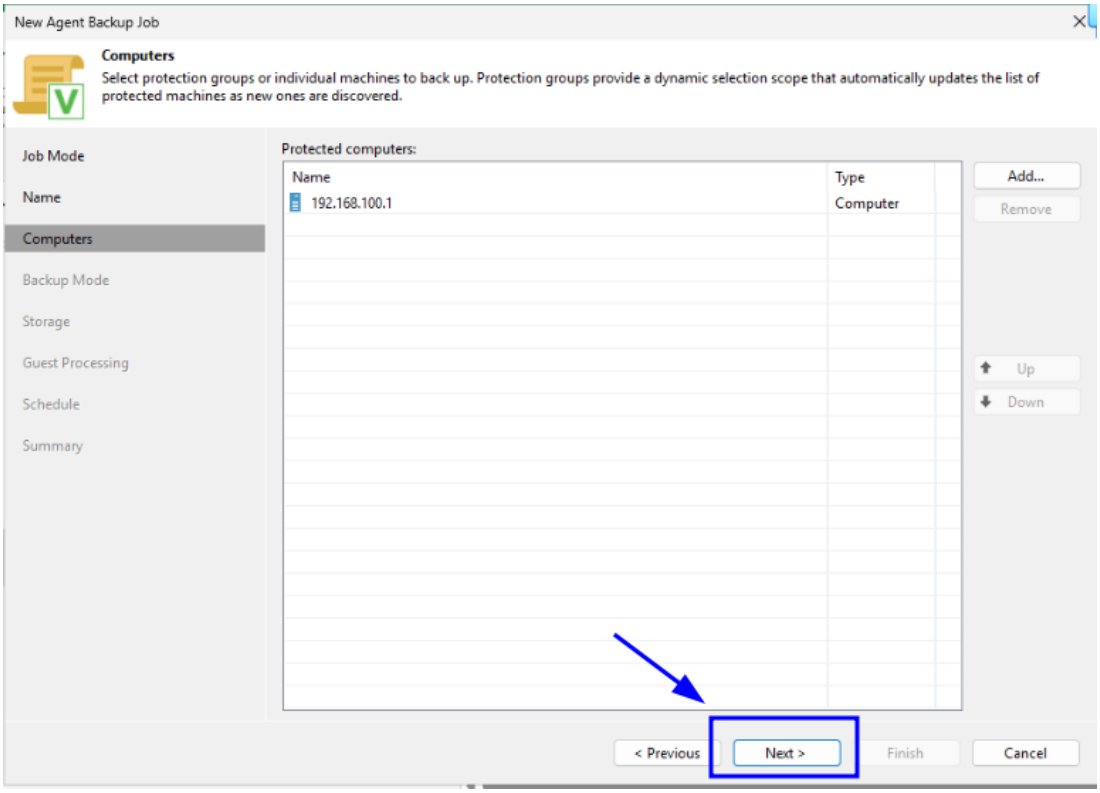


Il nous faut maintenant ajouter l'ordinateur cible en saisissant son adresse IP : 192.168.100.1, puis nous ajoutons les credentials de la machine à sauvegarder.

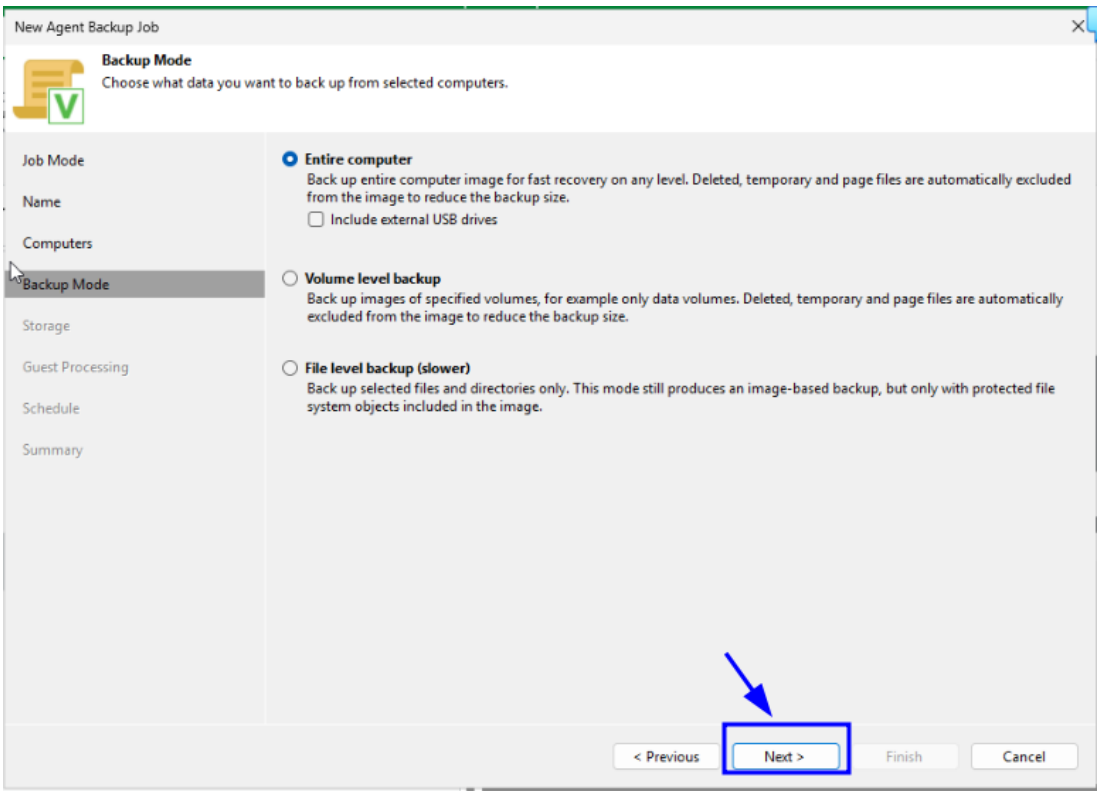


Après ceci effectué, nous passons à la suite.

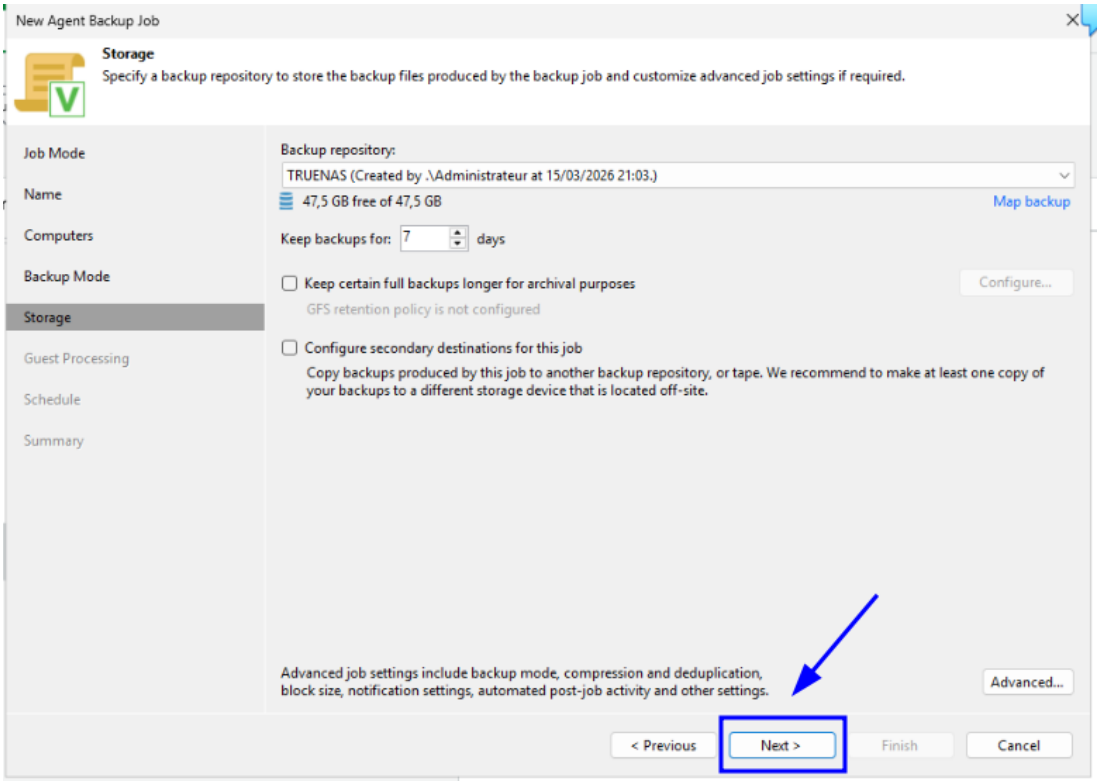




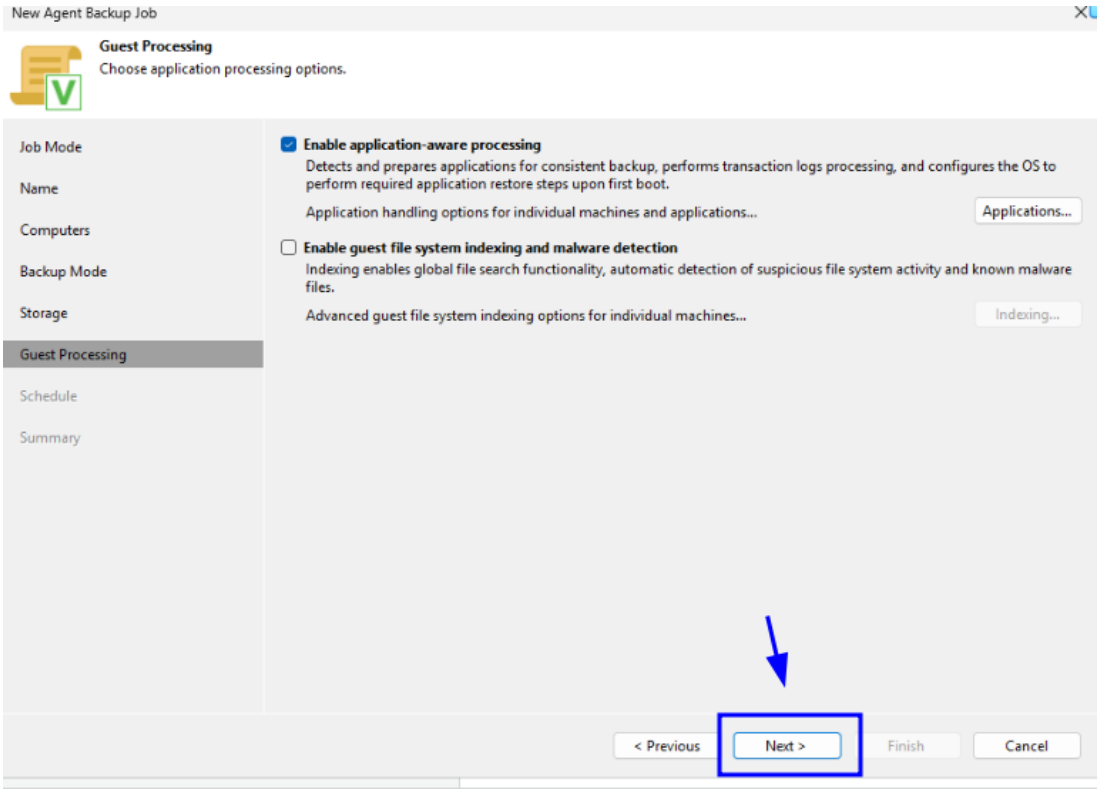
Nous optons alors pour le mode de sauvegarde "Entire computer" (image complète du système).



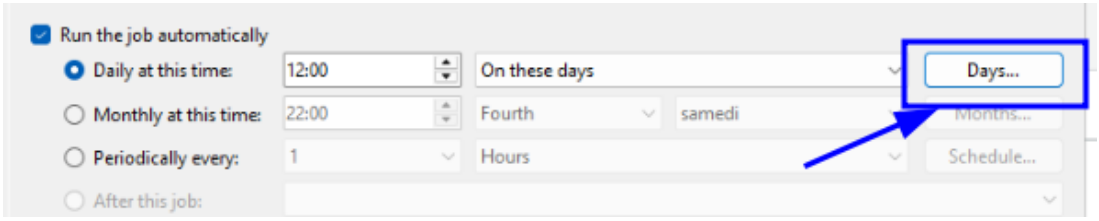
À cette étape, nous sélectionnons notre dépôt "TRUENAS" comme destination des fichiers.



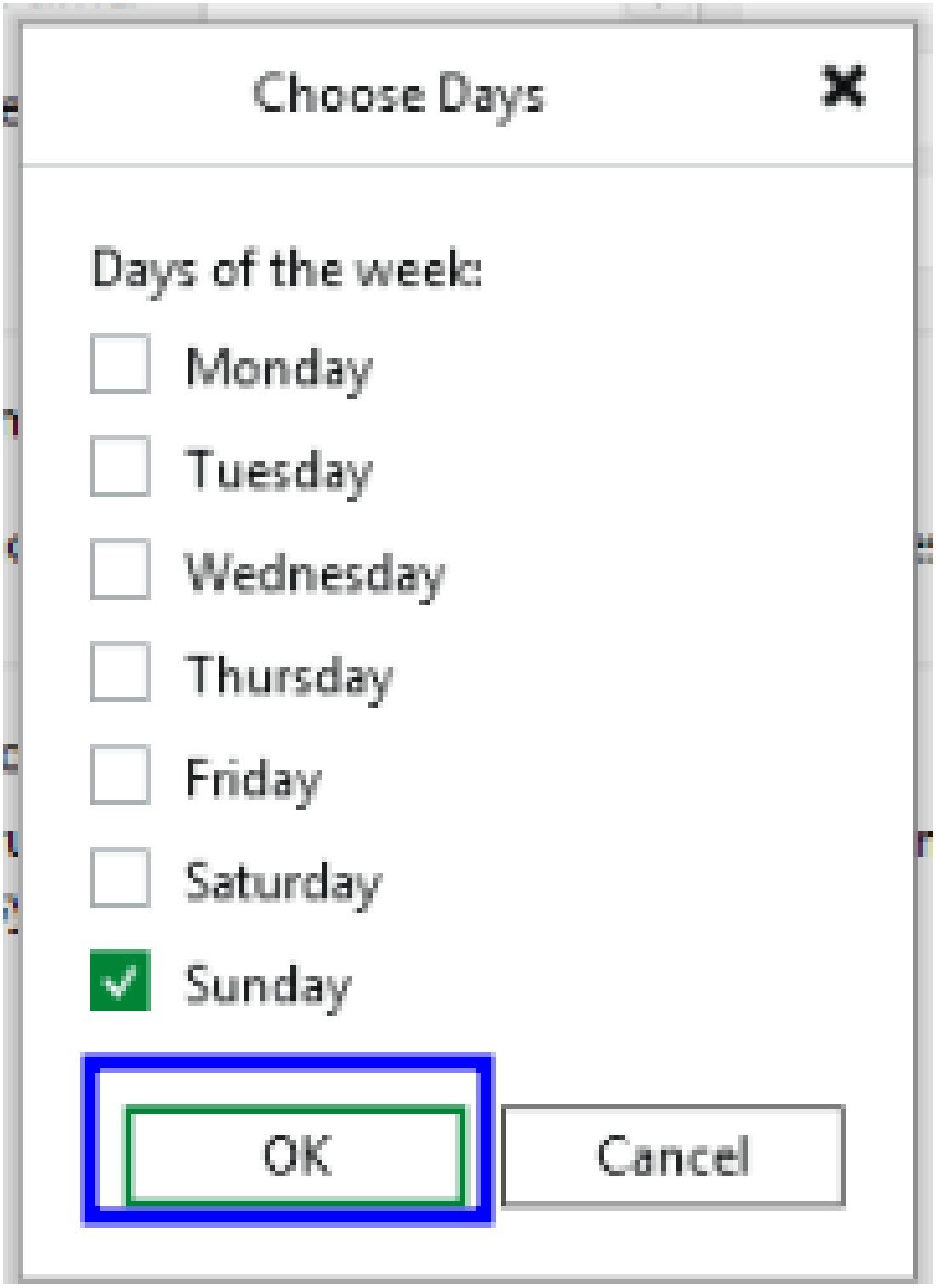
Nous activons l'application-aware processing afin que VEEAM puisse envoyer un signal avant les backup pour mettre en pause toutes les applications qui sont en cours et ne pas sauvegarder de données corrompues.



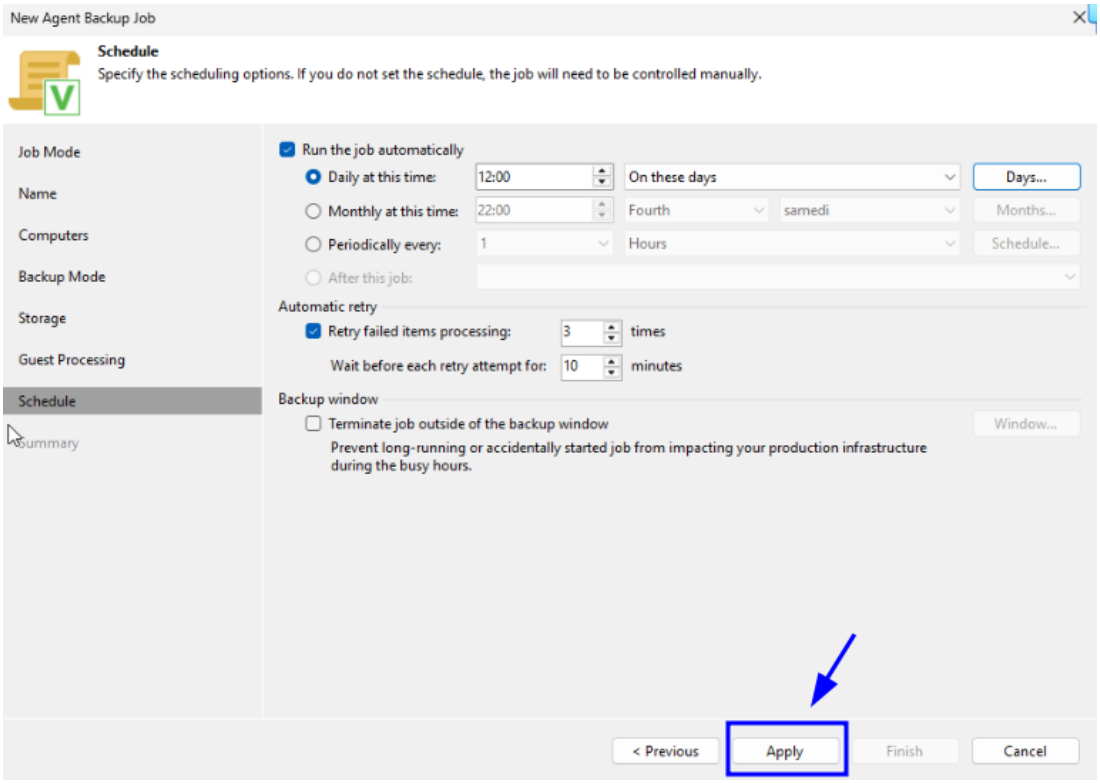
Nous allons définir une politique de sauvegarde basée sur certains jours dans la semaine pour cela nous allons sélectionner les jours sur lesquels les sauvegardes s'effectueront en appuyant sur le bouton "Days".



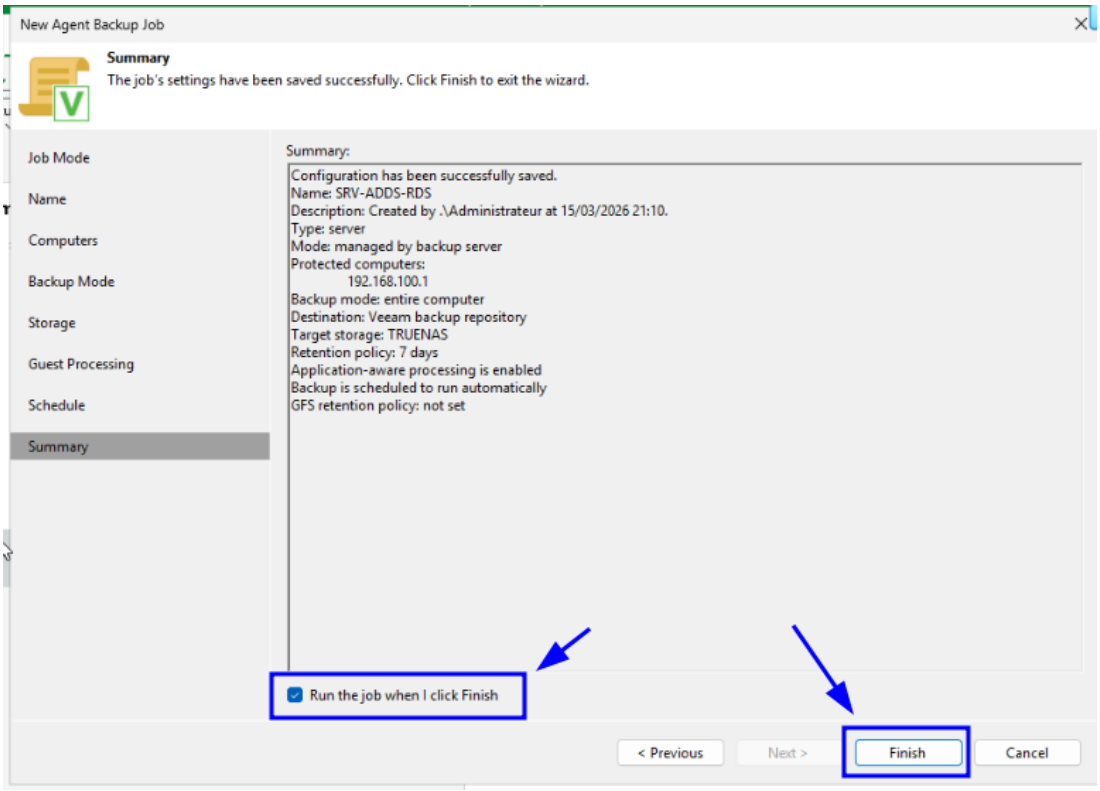
Nous cochons alors les jours de la semaine souhaités, dans notre cas ce sera le dimanche uniquement.



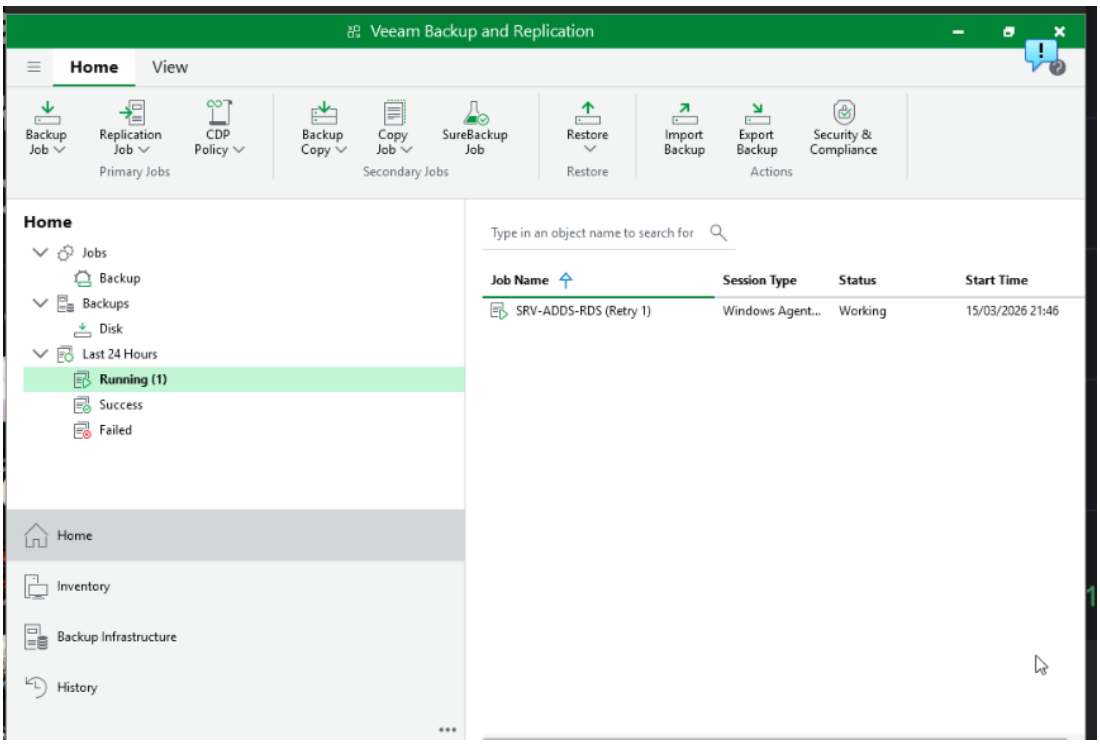
La sauvegarde s'effectuera donc tout les dimanche, à 12h. Après cela nous appliquons ces conditions.



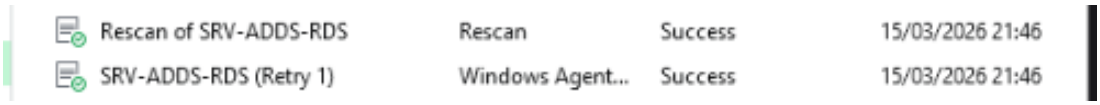
Avant de confirmer, nous passons en revue le résumé global de tous les paramètres du Job. Puis nous sélectionnons le fait que la tâche s'effectue une fois la configuration terminé, puis nous validons.



Nous validons la création et observons que notre tâche apparaît bien dans la console.



Finalement, nous observons que la tâche s'est bien effectué, puisqu'elle est en success.



Quatrième partie

Documentation Technique de Référence : Déploiement d'une infrastructure OpenVPN sur pfSense

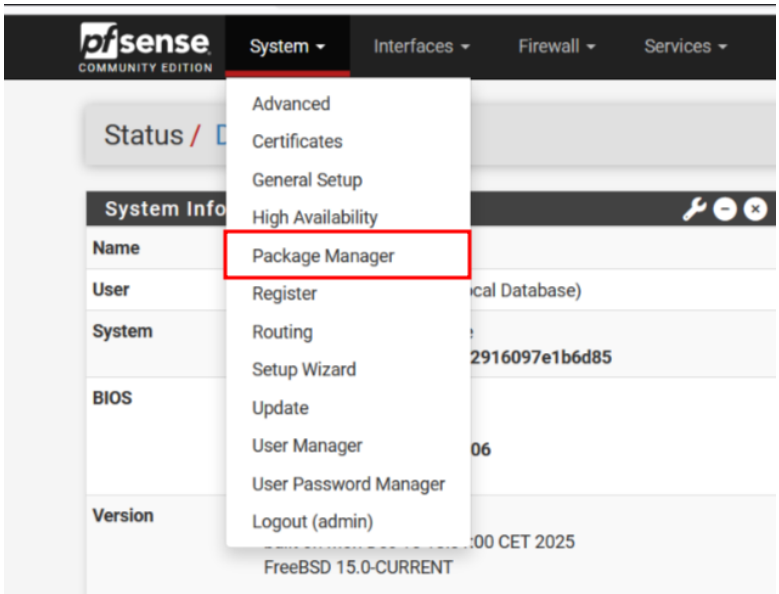
14 Introduction et Objectifs

L'objectif de cette procédure est de mettre en place un accès distant sécurisé de type "Road Warrior". Nous utilisons le protocole OpenVPN pour sa robustesse et sa flexibilité. Cette documentation détaille l'implémentation d'une architecture à double facteur (Certificat + Authentification locale).

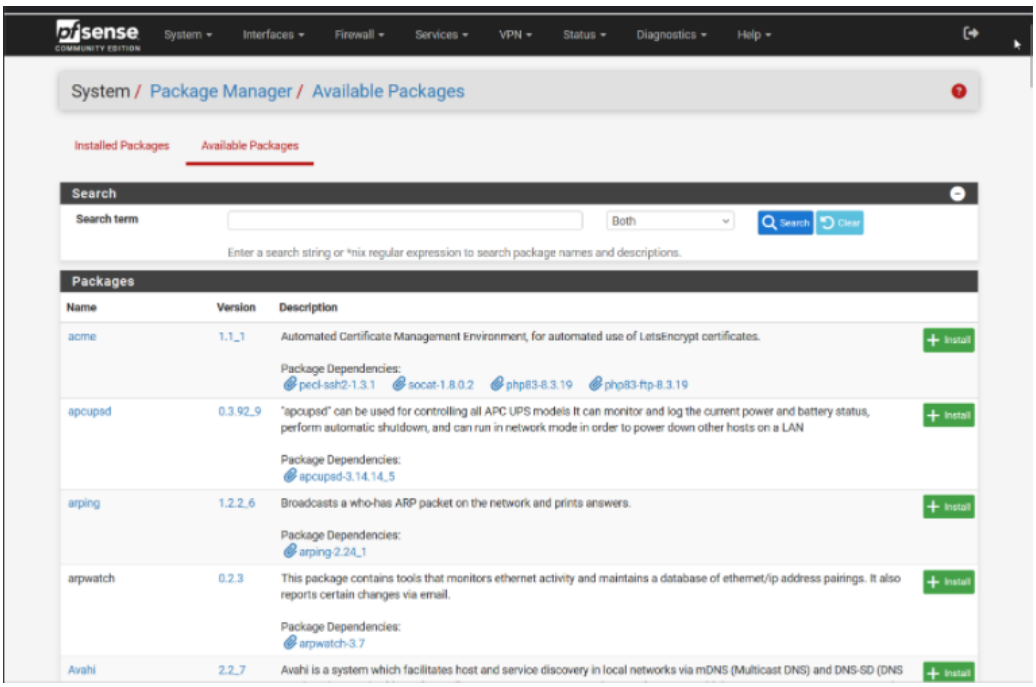
15 Installation du package Client Export

pfSense ne dispose pas nativement d'un outil de packaging pour les clients. Nous installons donc le paquet `openvpn-client-export`. Ce module technique sert de "moulinette" pour compiler la clé TLS, les certificats et les directives de connexion dans un fichier `.ovpn` unique.

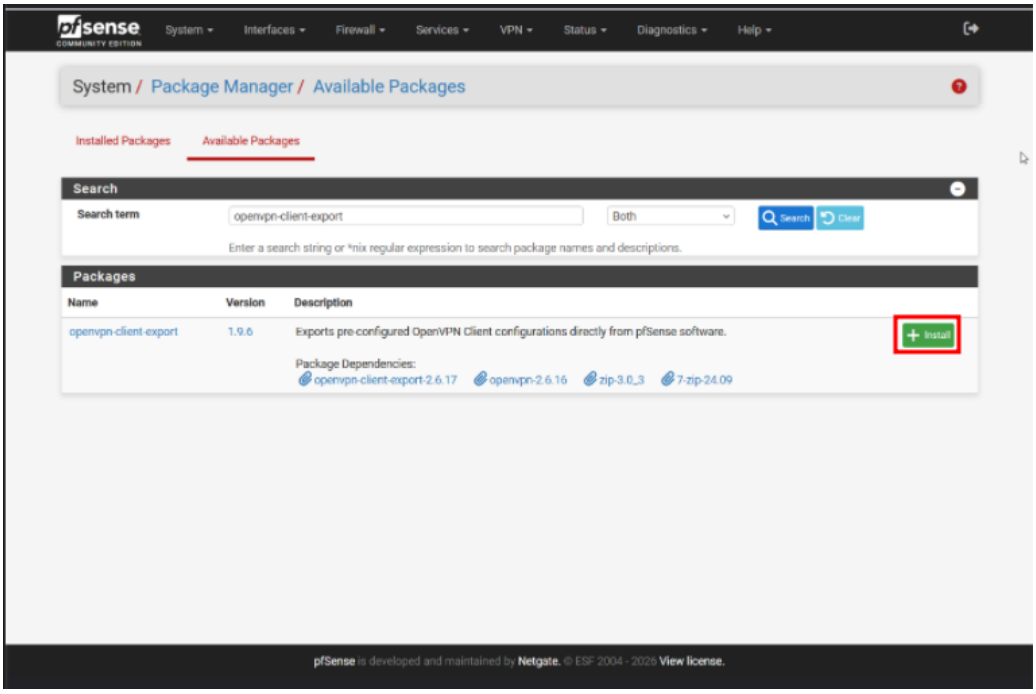
Nous accédons au menu System pour sélectionner le Package Manager, point d'entrée pour étendre les fonctionnalités du pare-feu.



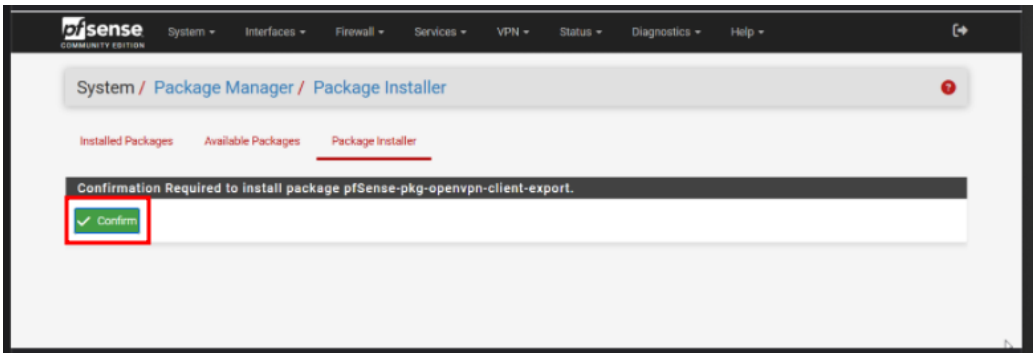
Nous visualisons ici le catalogue des dépôts officiels pfSense classés par ordre alphabétique.



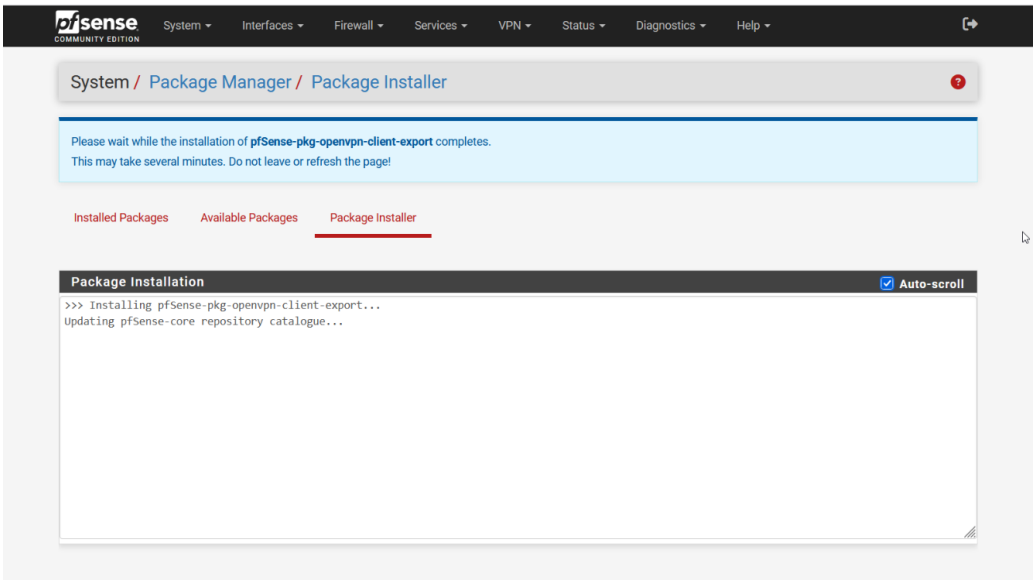
Nous isolons le paquet openvpn-client-export. Ce dernier est indispensable pour générer des profils compatibles avec les différents systèmes d'exploitation existant.



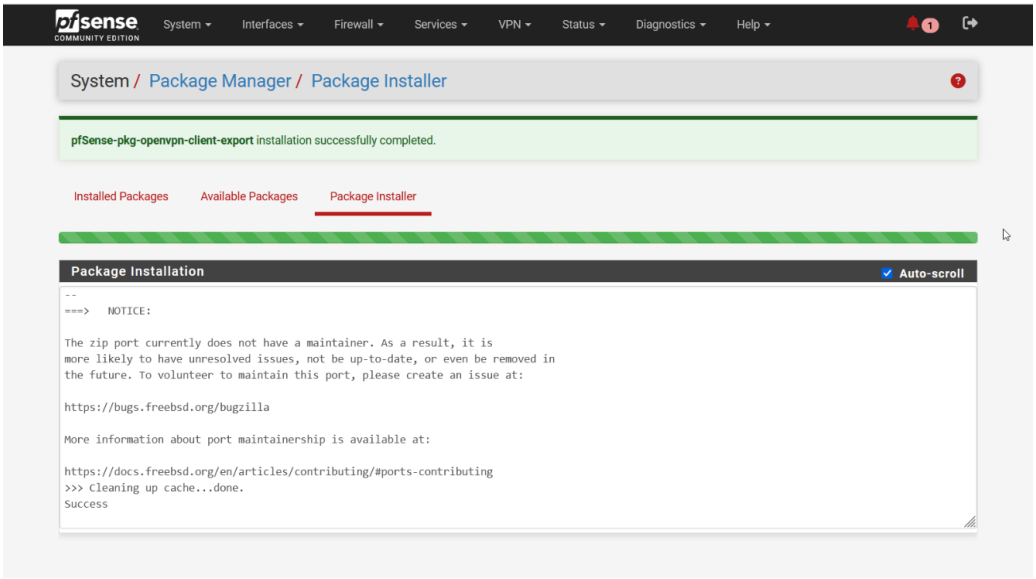
Nous confirmons l'installation. pfSense va alors récupérer les dépendances nécessaires sur les serveurs de Netgate.



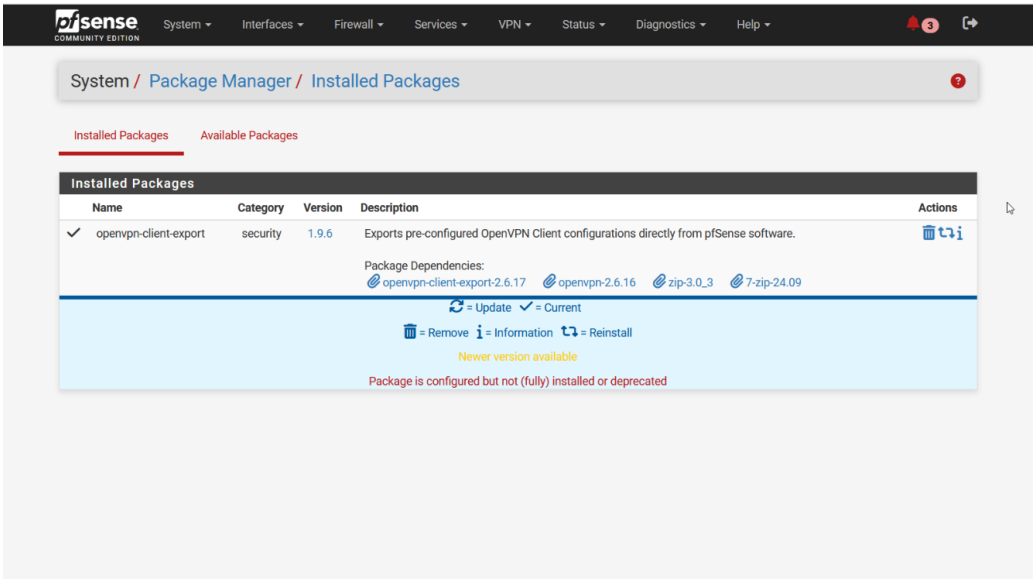
Le système procède à la mise à jour des catalogues et au téléchargement des binaires en temps réel.



Nous vérifions le message de succès de l'installation, confirmant que les scripts PHP d'exportation sont prêts.



Nous consultons l'onglet "Installed Packages" pour valider la version et la disponibilité du module d'exportation.


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
System / Package Manager / Installed Packages
Installed Packages
Available Packages
Installed Packages
Name
Category
Version
Description
Actions
openvpn-client-export
security
1.9.6
Exports pre-configured OpenVPN Client configurations directly from pfSense software.
Package Dependencies:
openvpn-client-export-2.6.17
openvpn-2.6.16
zip-3.0_3
7-zip-24.09
= Update
= Current
= Remove
= Information
= Reinstall
Newer version available
Package is configured but not (fully) installed or deprecated

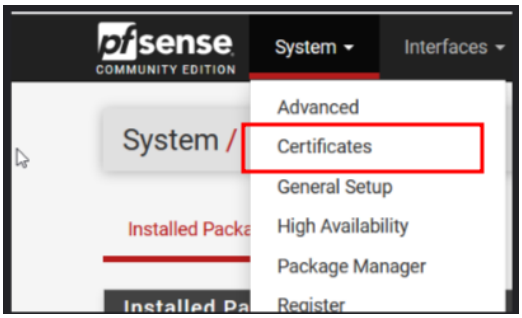
16 Infrastructure à Clés Publiques (PKI)

Le chiffrement asymétrique est le cœur de la sécurité VPN. Nous devons établir une chaîne de confiance locale.

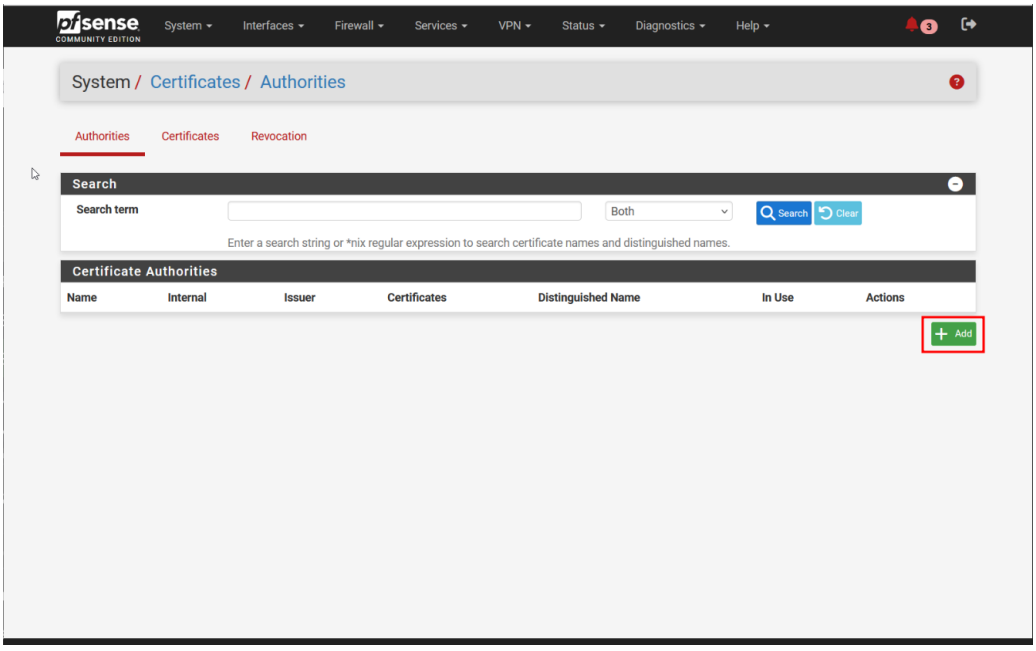
16.1 L'Autorité de Certification (CA)

Nous créons notre propre autorité racine. Techniquement, cela nous permet de signer nos propres certificats sans dépendre d'une entité tierce, garantissant que seuls les porteurs de certificats signés par **cette** CA pourront solliciter le serveur.

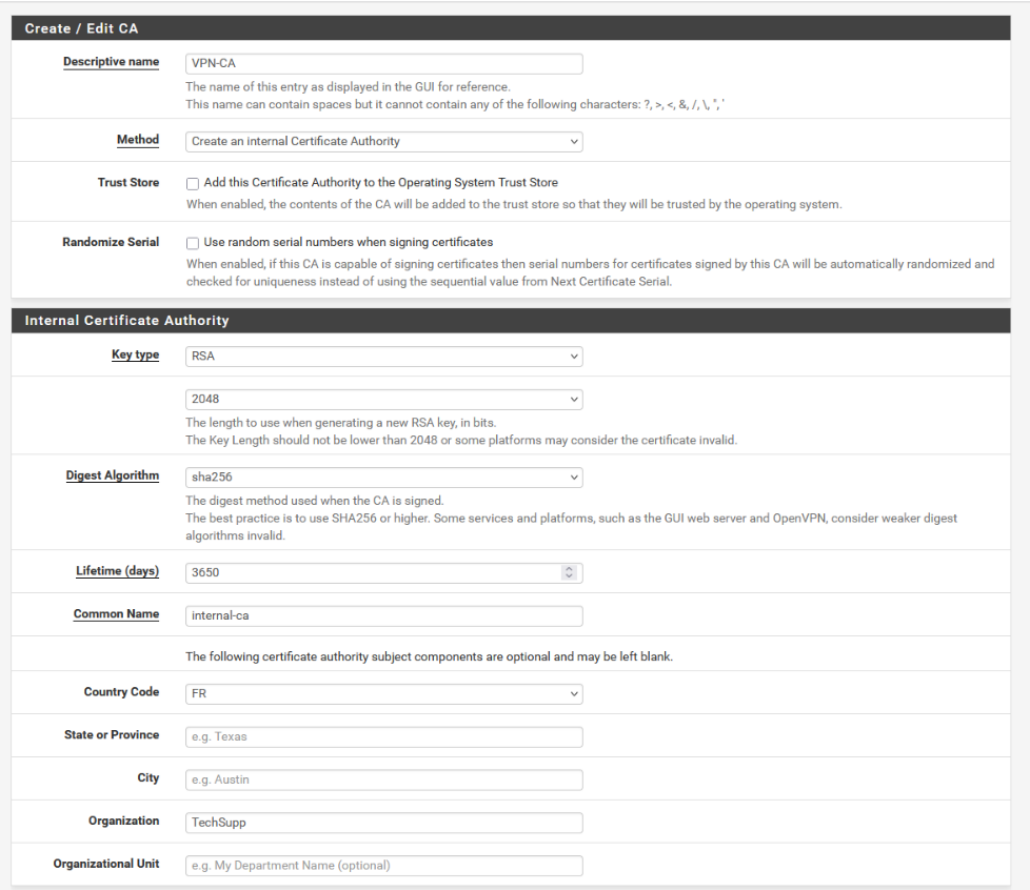
Nous retournons dans le menu System pour accéder au gestionnaire de certificats (Certificates).



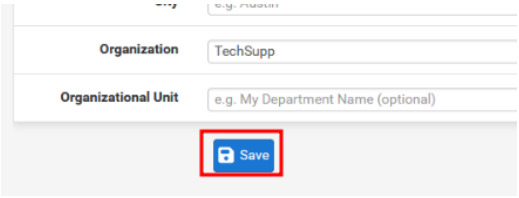
Dans l'onglet Authorities, nous ajoutons une nouvelle entité qui servira de racine de confiance pour notre VPN.



Nous configurons la CA : nous choisissons l'algorithme RSA 2048 bits et SHA256 pour assurer un niveau de sécurité optimal.



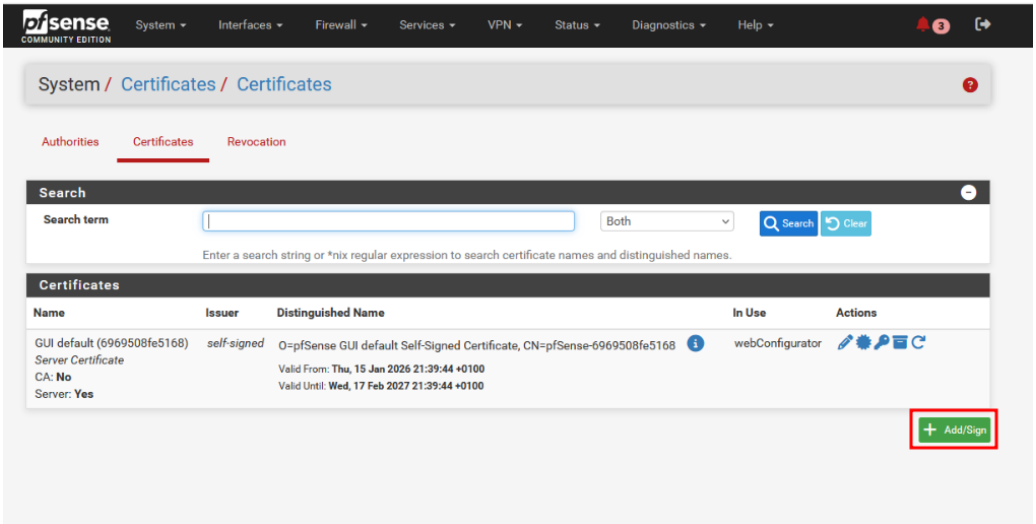
Nous validons l'enregistrement de la "VPN-CA" dans la base de données interne de pfSense.



16.2 Le Certificat Serveur

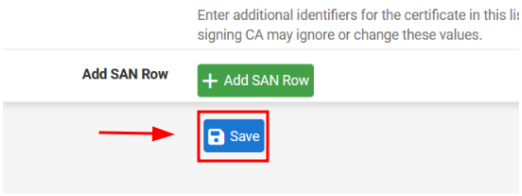
Ce certificat permet au client d'authentifier le pare-feu lors de la phase de "Handshake" SSL/TLS. Nous définissons ici l'identité cryptographique du service VPN.

Nous basculons sur l'onglet Certificates pour générer le certificat propre au service OpenVPN.

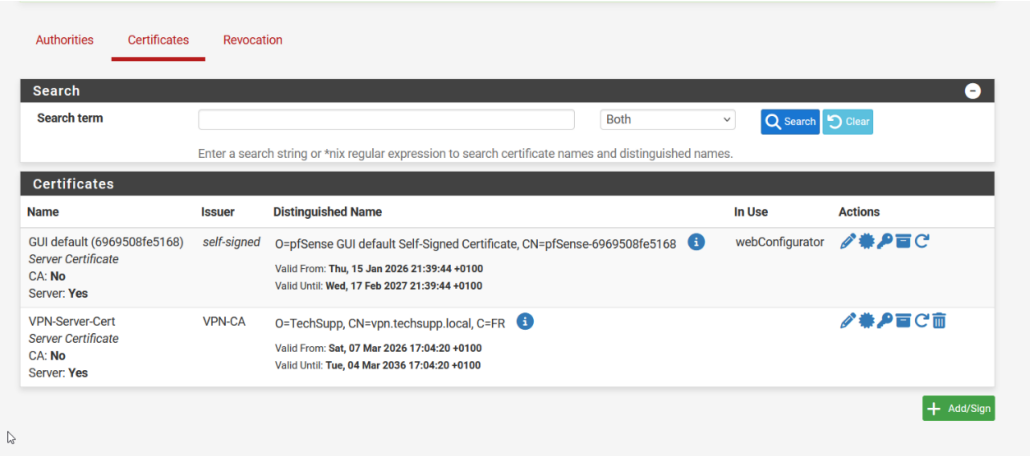


Nous définissons le type de certificat sur "Server Certificate" et renseignons le Common Name associé au domaine interne de l'entreprise.

Nous finalisons la création du certificat serveur en l'enregistrant.

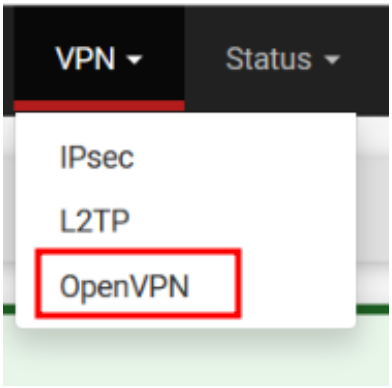


Nous vérifions ici la liste des certificats : le certificat serveur est correctement signé par notre autorité VPN-CA.

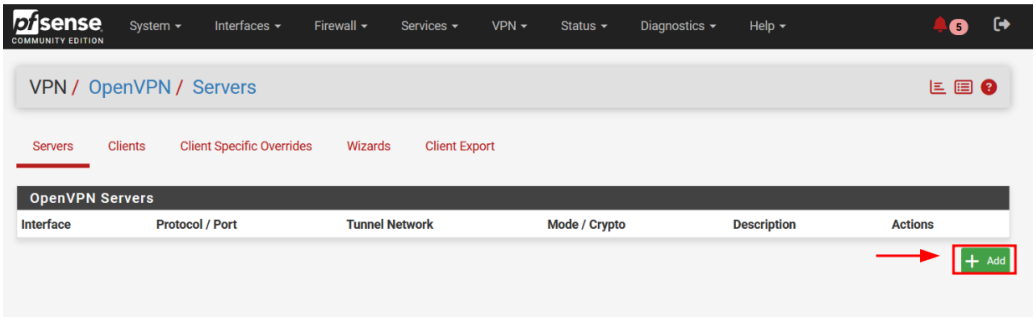

Authorities
Certificates
Revocation
Search
Search term
Both
Search
Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.
Certificates
Name
Issuer
Distinguished Name
In Use
Actions
GUI default (6969508fe5168)
Server Certificate
CA: No
Server: Yes
self-signed
O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6969508fe5168
Valid From: Thu, 15 Jan 2026 21:39:44 +0100
Valid Until: Wed, 17 Feb 2027 21:39:44 +0100
webConfigurator
VPN-Server-Cert
Server Certificate
CA: No
Server: Yes
VPN-CA
O=TechSupp, CN=vpn.techsupp.local, C=FR
Valid From: Sat, 07 Mar 2026 17:04:20 +0100
Valid Until: Tue, 04 Mar 2036 17:04:20 +0100
Add/Sign

17 Configuration du Service OpenVPN

Nous accédons au menu VPN pour configurer les paramètres de l'instance serveur.



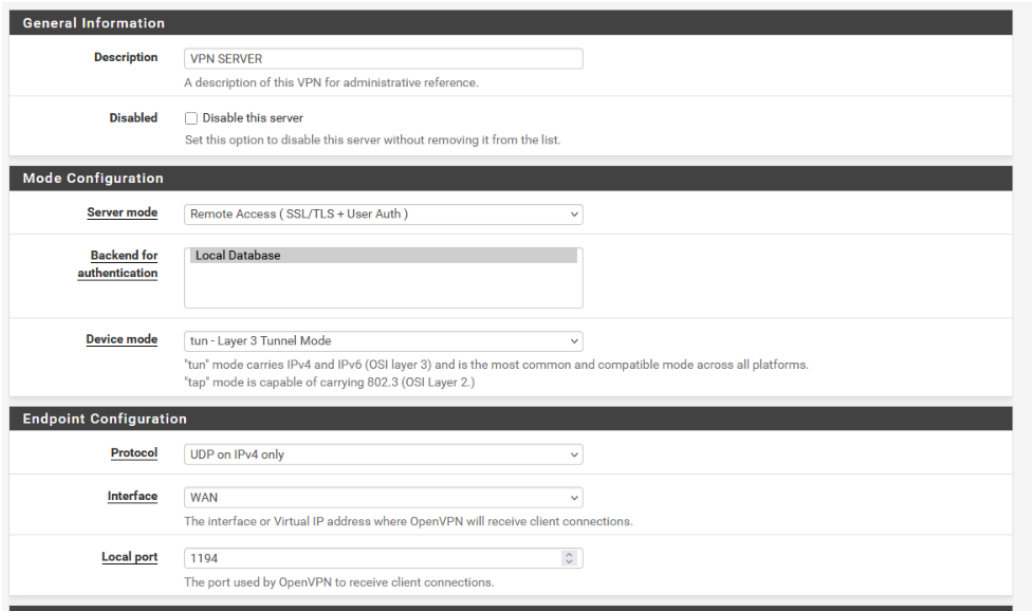
Nous créons une nouvelle instance de serveur VPN en cliquant sur le bouton d'ajout.



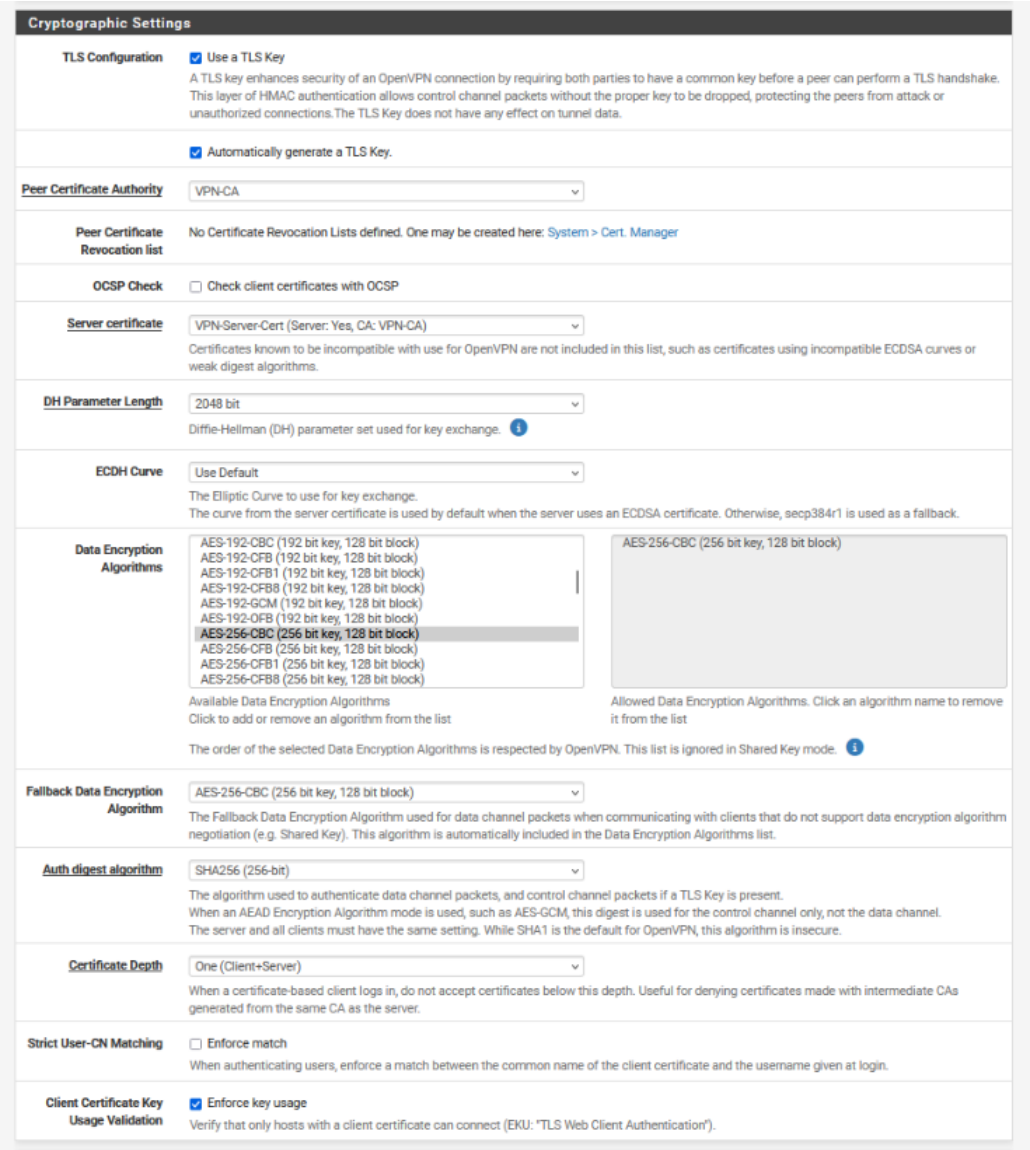
17.1 Paramètres réseau et chiffrement

Nous utilisons le protocole **UDP** sur le port **1194**. L'UDP est privilégié car il évite l'empilement des mécanismes de contrôle de flux, ce qui améliorerait considérablement la latence.

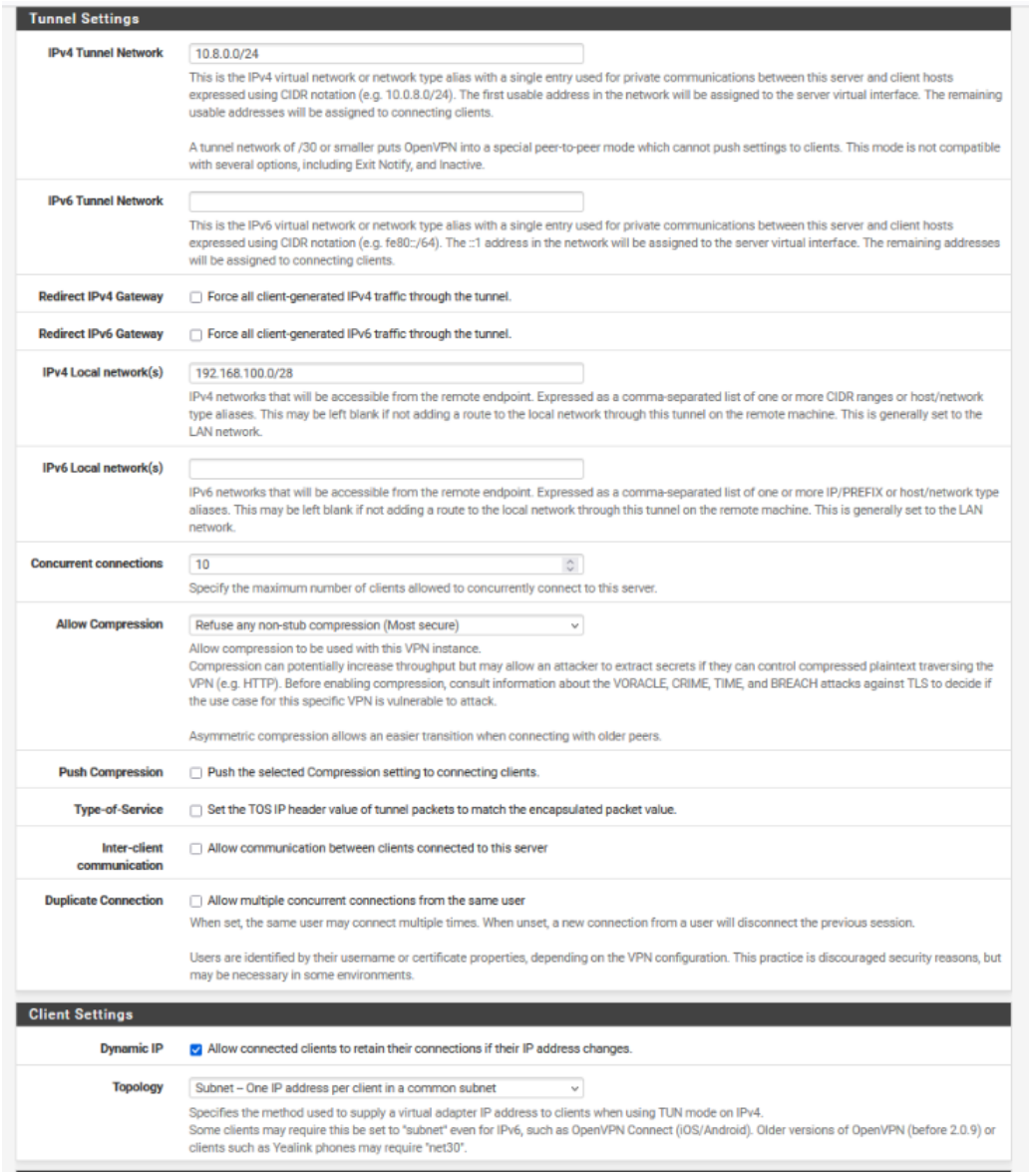
Nous configurons le mode d'accès distant et l'interface WAN sur laquelle le serveur écoutera les requêtes entrantes.



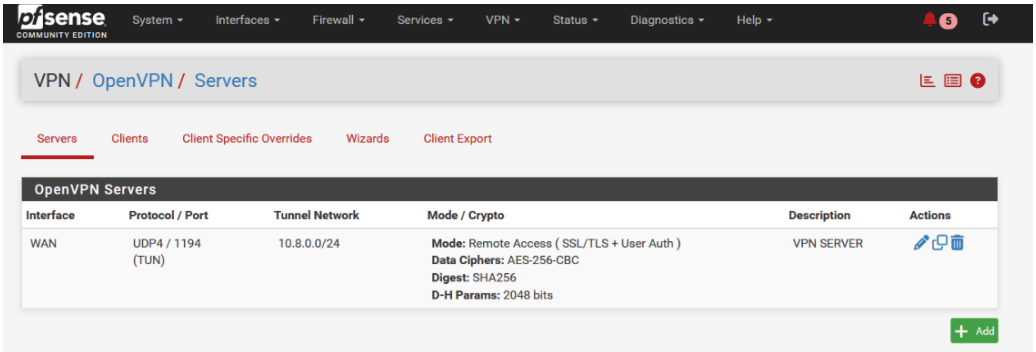
Nous paramétrons le chiffrement AES-256-CBC. Nous activons également le TLS Key pour renforcer l'authentification mutuelle.



Nous spécifions le réseau du tunnel (IP attribuées aux clients) et les réseaux locaux que les clients ont l'autorisation de contacter.

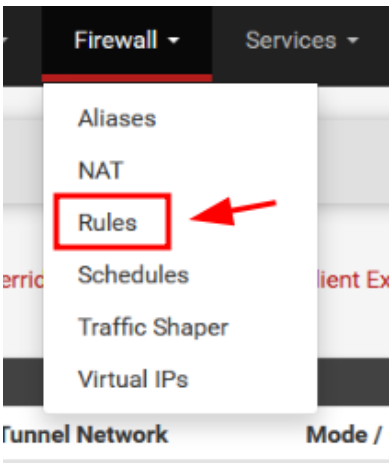


Nous validons le résumé de configuration du serveur qui récapitule les protocoles et algorithmes actifs.



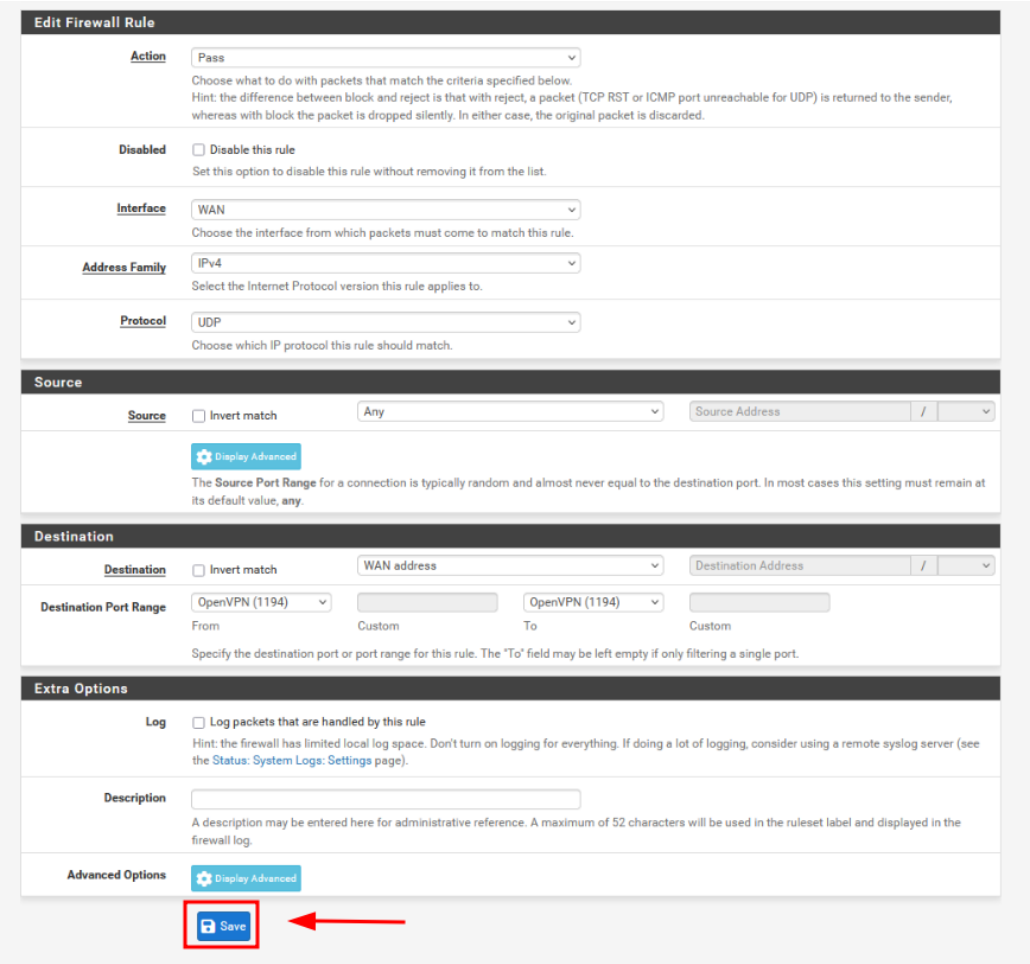
18 Politique de Filtrage (Firewall)

Nous nous rendons dans les règles du Firewall pour modifier la politique de sécurité du WAN.

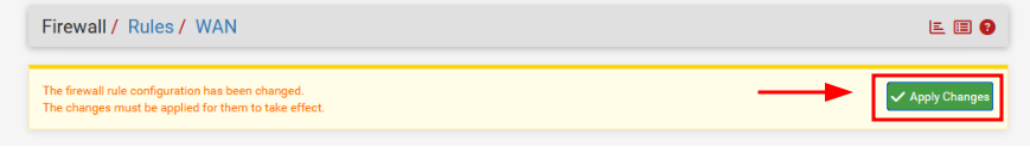


Nous cliquons sur "Add" pour insérer une nouvelle règle de passage.

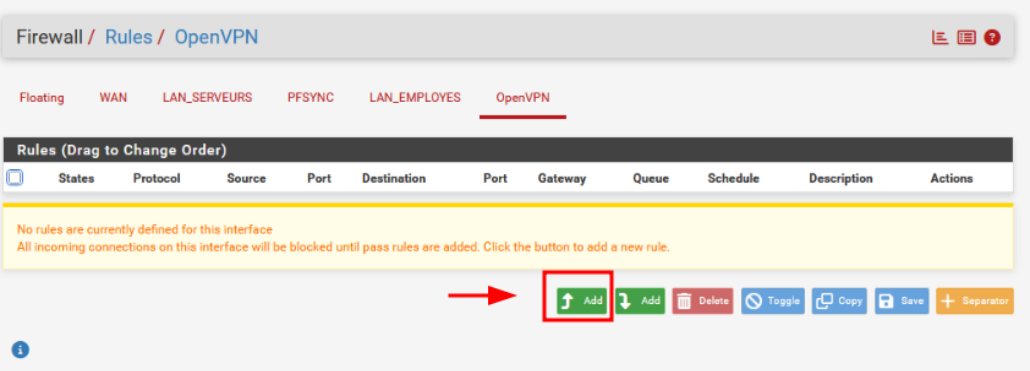
Nous autorisons le flux UDP vers le port 1194. Cette règle permet au pare-feu d'accepter les connexions VPN initiales.



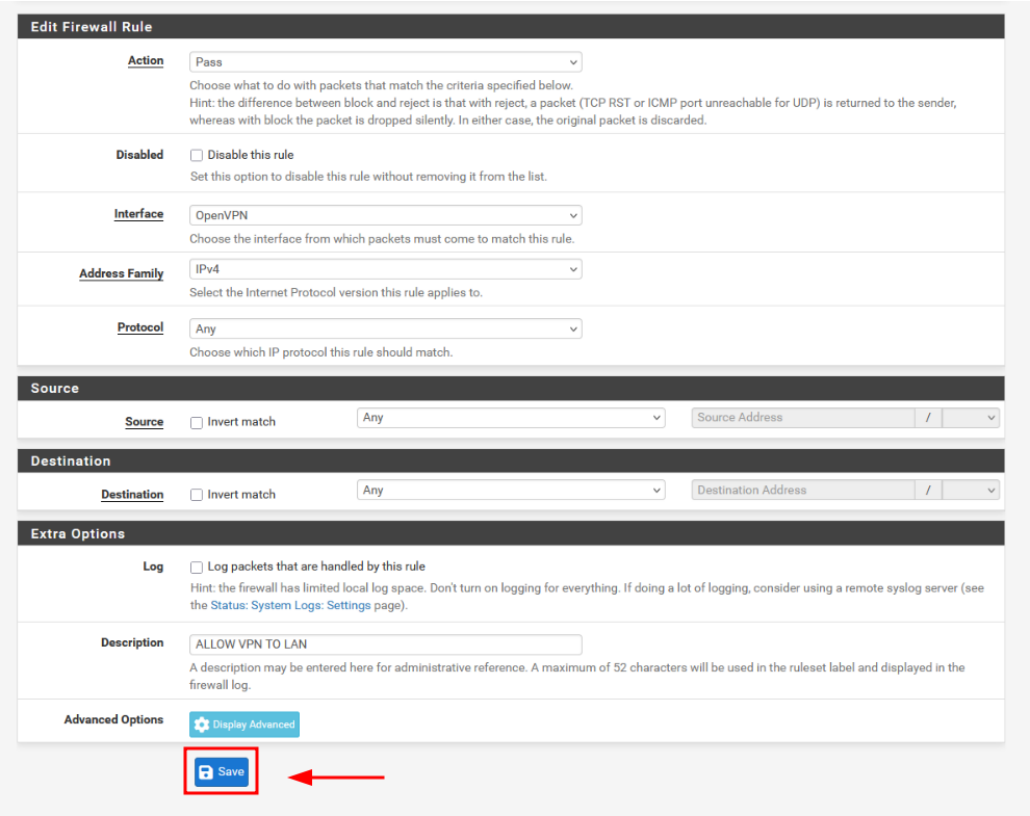
Nous appliquons la configuration pour que le moteur de filtrage prenne en compte l'ouverture du port.



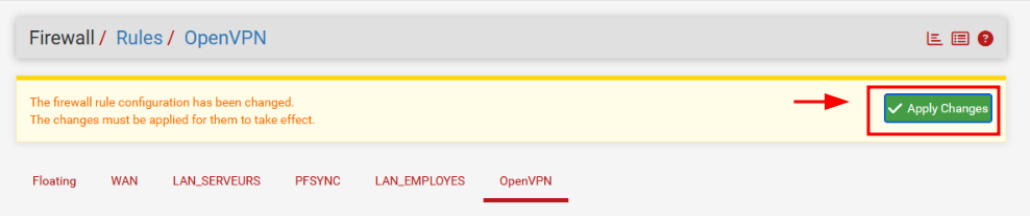
Nous passons sur l'onglet spécifique OpenVPN pour gérer le trafic à l'intérieur du tunnel.



Nous créons une règle "Pass" autorisant tout trafic provenant du tunnel à destination du réseau LAN.

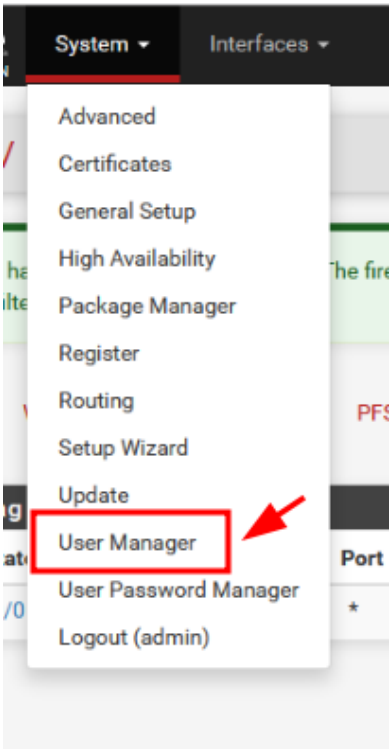


Nous appliquons les changements. Sans cette règle, les utilisateurs seraient connectés mais bloqués à l'entrée du réseau local.

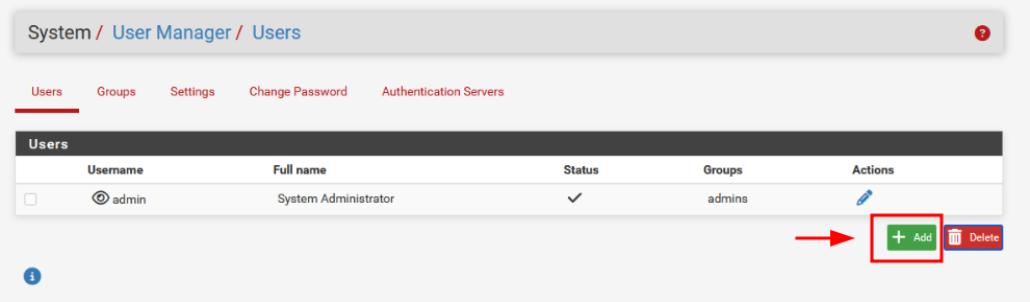


19 Provisionnement des Utilisateurs

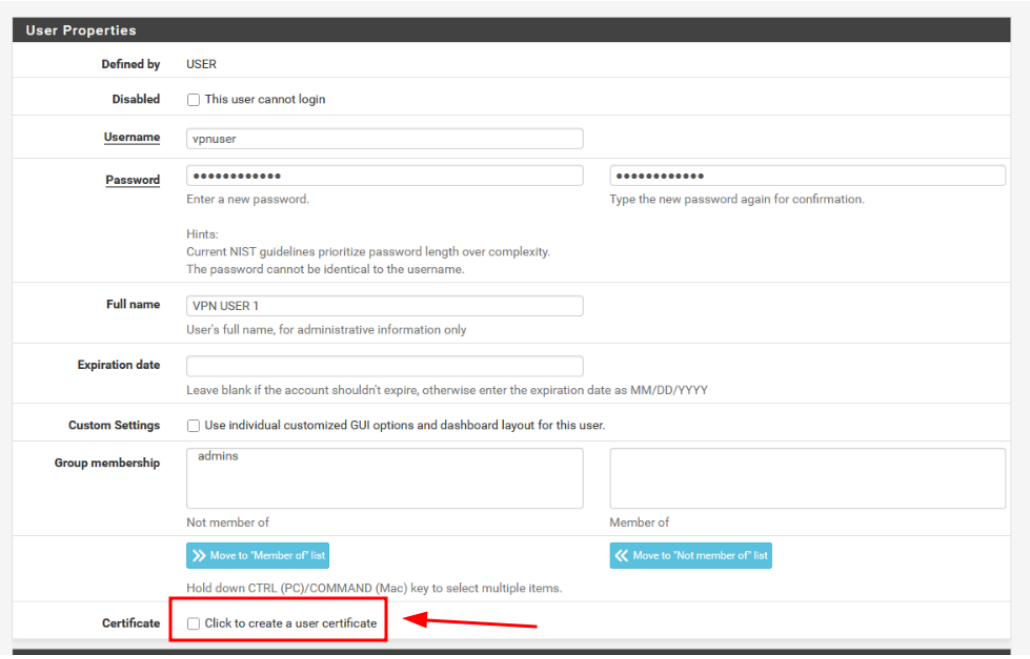
Nous accédons au User Manager pour créer les comptes de nos collaborateurs.



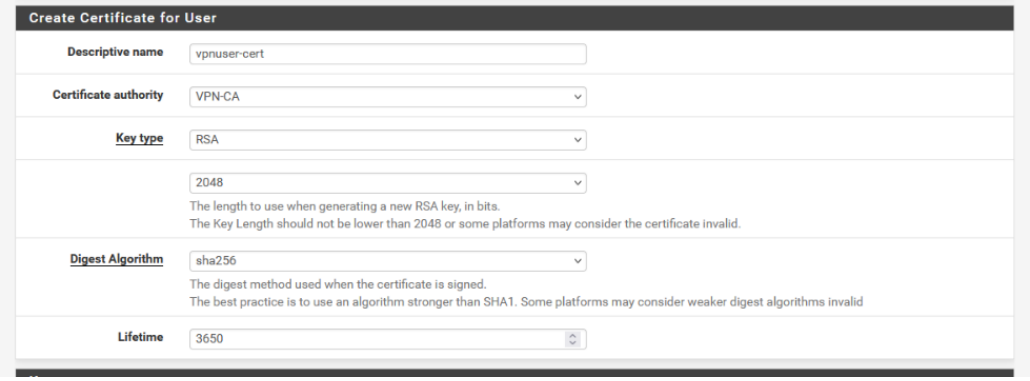
Nous cliquons sur "Add" pour enregistrer un nouvel utilisateur dans la base locale.



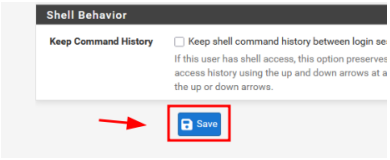
Nous renseignons le nom d'utilisateur et le mot de passe, puis nous cochons la case de création de certificat individuel.



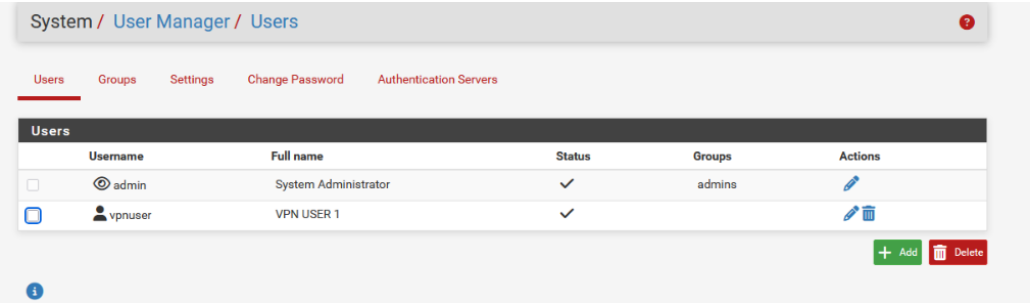
Nous configurons le certificat de l'utilisateur, signé par notre autorité racine VPN-CA.



Nous enregistrons la fiche utilisateur complète.

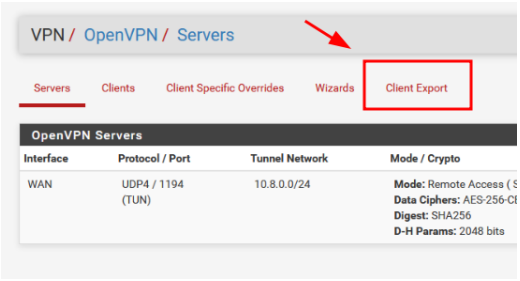


Nous constatons que l'utilisateur vpnuser est désormais présent et actif dans le système.

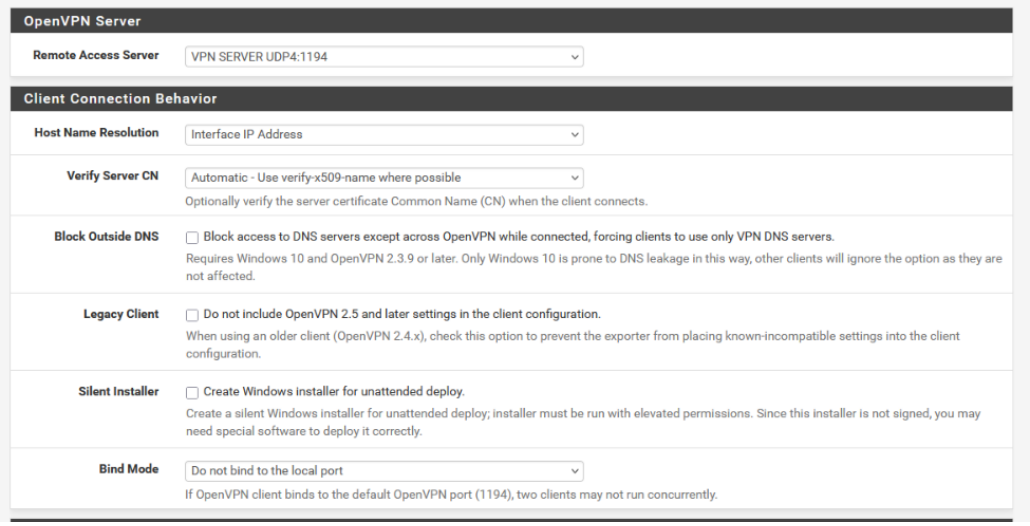


20 Exportation des Profils Clients

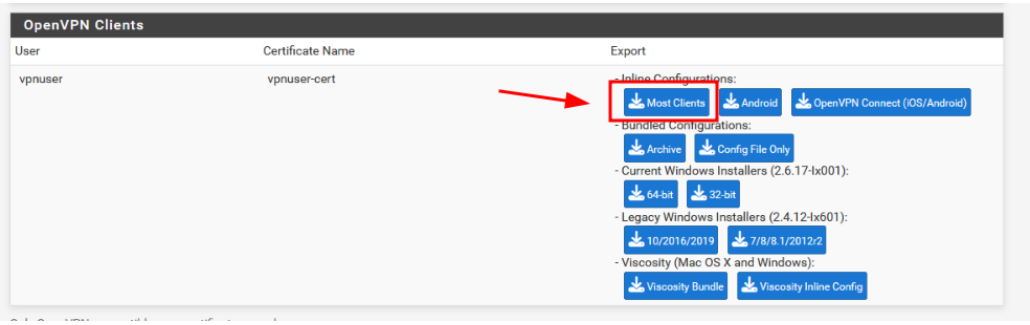
Nous retournons dans l'onglet Client Export pour finaliser la procédure.



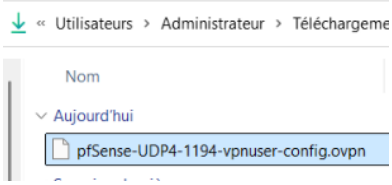
Nous configurons la résolution du nom d'hôte pour que le client sache à quelle adresse IP publique se connecter.



Nous localisons l'utilisateur dans la liste et téléchargeons son profil de connexion standard.



Nous vérifions la réception du fichier .ovpn, prêt à être importé dans le logiciel client.



21 Conclusion

Nous avons achevé la configuration. Notre serveur est prêt à recevoir des connexions sécurisées et nous avons vérifié que chaque étape de la PKI à l'exportation a été respectée.