

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	4
I Guide d'Installation et Configuration : GLPI 11	6
1 Phase 1 : Préparation du Système et du Réseau	6
1.1 Identification du serveur	6
1.2 Adressage IP Statique	6
1.3 Activation et Validation Réseau	7
1.4 Résolution de noms (DNS)	7
1.5 Tests de Connectivité par Ping	8
2 Phase 2 : Installation de la pile LAMP	9
2.1 Mise à jour des dépôts	9
2.2 Installation des services et dépendances PHP	9
2.3 Sécurisation du serveur SQL	9
2.4 Configuration de la base de données dédiée	10
3 Phase 3 : Déploiement de l'Application GLPI	11
3.1 Téléchargement de l'archive	11
3.2 Extraction et Permissions de fichiers	11
3.3 Configuration du VirtualHost Apache	11
4 Phase 4 : Assistant Web et Finalisation	13
4.1 Initialisation du Setup	13
4.2 Contrôle de l'Environnement	13
4.3 Liaison SQL	14
4.4 Accès et Sécurité Finale	15
5 Phase 5 : Déploiement de l'Agent et Inventaire	17
5.1 Installation sur le client	17
5.2 Remontée de l'Inventaire	18
II Documentation Technique : Services Bureau à Distance (RDS)	20
6 Phase 1 : Déploiement des Services de rôle	21
6.1 Lancement de l'assistant d'ajout de rôles	21
6.2 Sélection du type d'installation	21
6.3 Choix du type de déploiement et du scénario	21
6.4 Sélection du serveur de destination	22
6.5 Confirmation et redémarrage automatique	22
6.6 Suivi de la progression et phase système	23
6.7 Validation de la fin d'installation	23
7 Phase 2 : Configuration du Gestionnaire de Licences	25
7.1 Accès aux outils de gestion RDS	25
7.2 Installation du rôle Gestionnaire de licences	25
7.3 Confirmation et installation du rôle de licence	26

7.4	Statut de l'installation des licences	26
7.5	Liaison du mode de licence au déploiement	27
7.6	Configuration du mode 'Par utilisateur'	27
8	Phase 3 : Validation de la Connexion Client	29
8.1	Préparation du poste client	29
8.2	Authentification et gestion du certificat	29
8.3	Accès final au bureau distant	29
III	Manuel d'Installation et Configuration : Veeam Backup & Re- plication 13	31
9	Préparation de l'environnement Windows	31
10	Installation de Veeam Backup & Replication	34
11	Connexion à la Console de gestion	39
12	Configuration du Backup Repository (Stockage)	43
13	Création d'une tâche de sauvegarde (Job)	50
IV	Documentation Technique de Référence : Déploiement d'une infrastructure OpenVPN sur pfSense	60
14	Introduction et Objectifs	60
15	Installation du package Client Export	60
16	Infrastructure à Clés Publiques (PKI)	64
16.1	L'Autorité de Certification (CA)	64
16.2	Le Certificat Serveur	65
17	Configuration du Service OpenVPN	68
17.1	Paramètres réseau et chiffrement	68
18	Politique de Filtrage (Firewall)	71
19	Provisionnement des Utilisateurs	74
20	Exportation des Profils Clients	76
21	Conclusion	76

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.

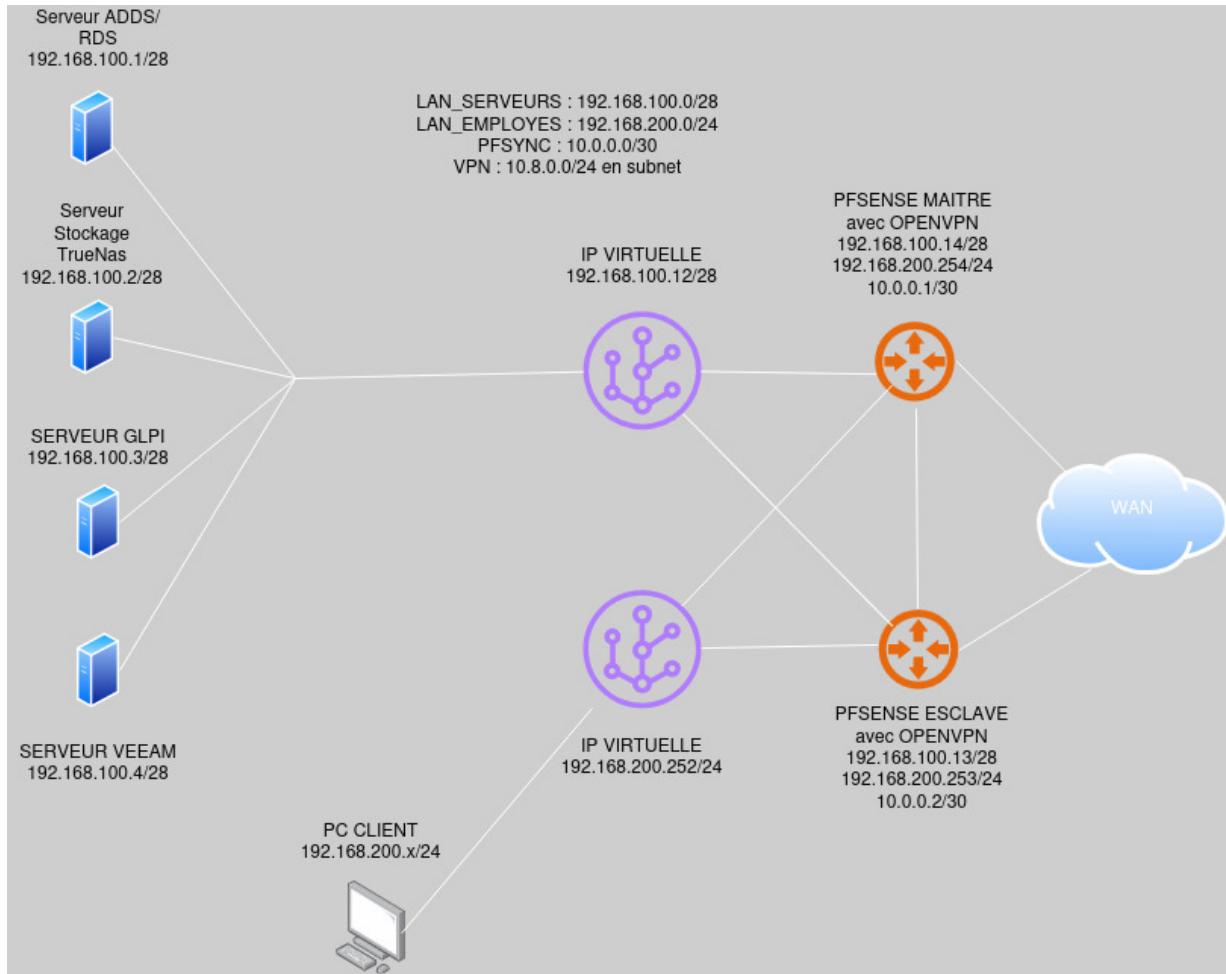
Intitulé de la réalisation professionnelle

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 pf-Sense, 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

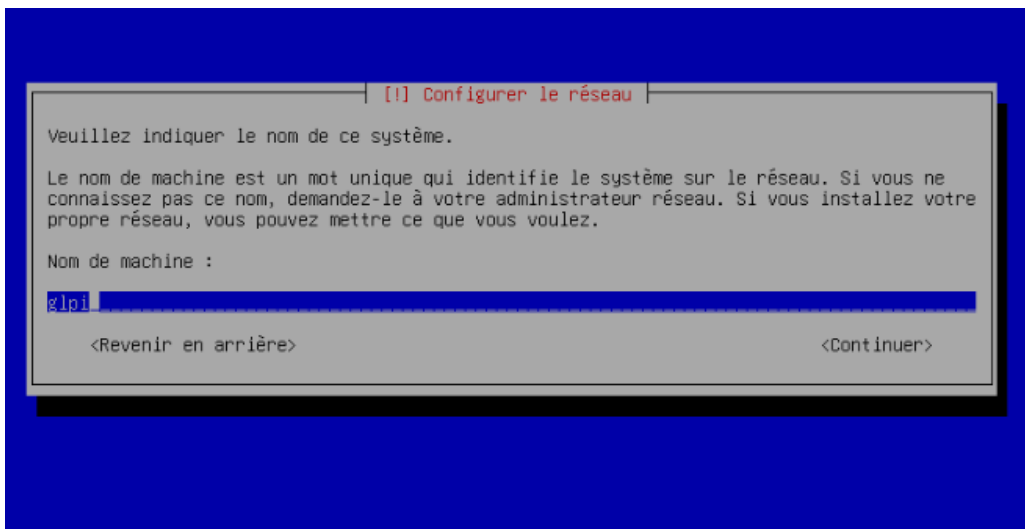
Guide d'Installation et Configuration : GLPI 11

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'installateur 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.

```
root@glpi:~#  
root@glpi:~# nano /etc/network/interfaces
```

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 enx0002773955a
    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**.

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

```
GNU nano 8.4
# Generated by dhcpd
# /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.

```
root@glpi:~# ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=128 time=1.05 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=128 time=0.493 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=128 time=0.792 ms
64 bytes from 192.168.100.1: icmp_seq=4 ttl=128 time=0.754 ms
^C
--- 192.168.100.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3016ms
rtt min/avg/max/mdev = 0.493/0.773/1.054/0.198 ms
```

```
root@glpi:~# ping google.com
PING google.com (172.217.22.174) 56(84) bytes of data.
64 bytes from arn09s11-in-f174.1e100.net (172.217.22.174): icmp_seq=1 ttl=116 time=28.4 ms
64 bytes from arn09s11-in-f174.1e100.net (172.217.22.174): icmp_seq=2 ttl=116 time=22.6 ms
64 bytes from arn09s11-in-f174.1e100.net (172.217.22.174): icmp_seq=3 ttl=116 time=37.2 ms
64 bytes from arn09s11-in-f174.1e100.net (172.217.22.174): icmp_seq=4 ttl=116 time=32.9 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3036ms
rtt min/avg/max/mdev = 22.577/30.280/37.235/5.424 ms
root@glpi:~#
```

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.

```
root@glpi:~# apt update && apt upgrade -y
Atteint : 1 http://security.debian.org/debian-security trixie-security InRelease
Atteint : 2 http://deb.debian.org/debian trixie InRelease
Atteint : 3 http://deb.debian.org/debian trixie-updates InRelease
Tous les paquets sont à jour.
Sommaire :
  Mise à niveau de : 0. Installation de : 0Supprimé : 0. Non mis à jour : 0
```

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.

```
Thanks for using MariaDB!
root@glpi:~# apt install apache2 php php-curl php-gd php-intl php-json php-mbstring php-xml php-zip php-bcmath php-phar php-bz2 php-mariadb-mysql-kbs mariadb-se
rver -y _
```

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.

```
Thanks for using MariaDB!
root@glpi:~# mariadb-secure-installation
```

```

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.

```

```

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)

```

```

Techsupp30 at line 1
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
root@glpi:~#

```

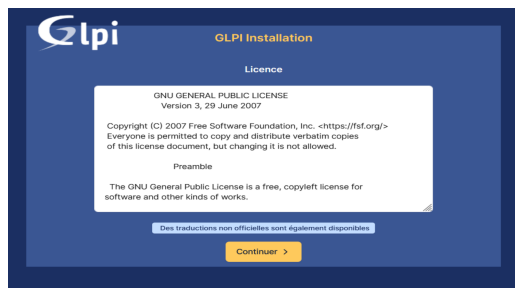
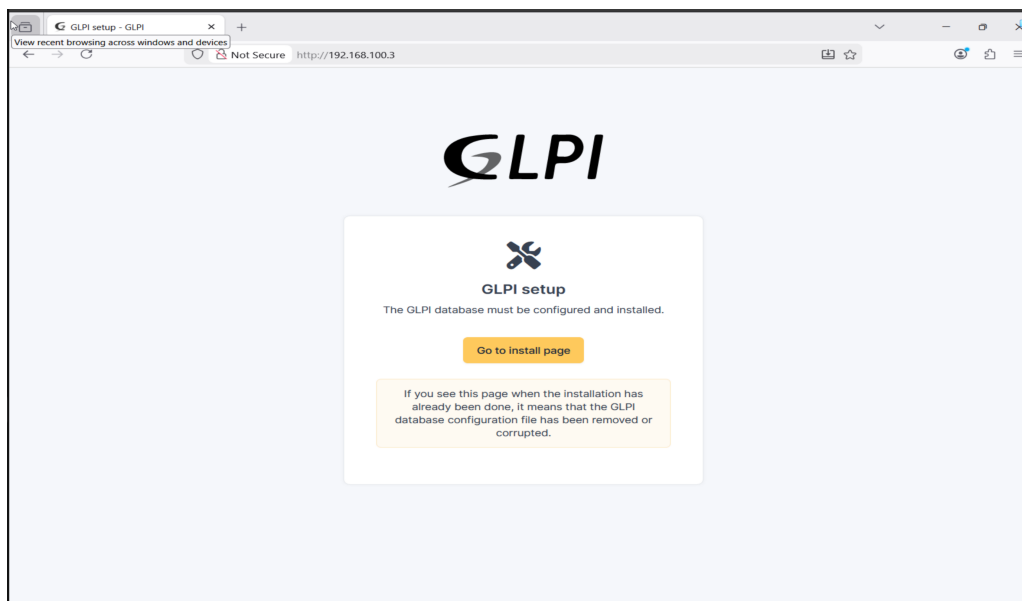

Nous désactivons la configuration par défaut d'Apache (`000-default`) et activons notre nouvelle configuration GLPI. Le module `rewrite` est également activé pour permettre à GLPI de gérer ses URLs proprement.

```
2 a2ensite glpi.conf  
3 a2enmod rewrite  
4 a2dissite 000-default.conf  
5 systemctl reload apache2
```

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.

The screenshot shows the 'GLPI Installation' interface at 'Etape 0'. The main heading is 'Vérification de la compatibilité de votre environnement avec l'exécution de GLPI'. Below this is a table with two columns: 'TESTS EFFECTUÉS' and 'RÉSULTATS'. The table lists various system requirements and their status, all of which are marked as successful with a checkmark.

TESTS EFFECTUÉS	RÉSULTATS
Requis Parser PHP	✓
Requis Taille d'entier maximal de PHP Le support des entiers est dit sur nécessaire pour les opérations relatives aux adresses IP (inventaire réseau, filtrage des clients API, ...).	✓
Requis Configuration des sessions	✓
Requis Mémoire allouée	✓
Requis Extensions du noyau de PHP	✓
Requis mysql extension Requis pour l'accès à la base de données.	✓
Requis curl extension Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).	✓
Requis gd extension Requis pour le traitement des images.	✓
Requis intl extension Requis pour l'internationalisation.	✓
Requis mbstring extension Requis pour la prise en charge des caractères multioctets et la conversion de jeu de caractères.	✓
Requis zlib extension Requis pour la gestion de la communication compressée avec les agents d'inventaire, l'installation de paquets glpi à partir du Marketplace et la génération de PDF.	✓
Requis bcmath extension Requis pour la prise en charge des QR codes.	✓
Requis Libsodium ChaCha20-Poly1305 constantes de taille Activer l'utilisation du cryptage ChaCha20-Poly1305 requis par GLPI. Il est fourni par libsodium à partir de la version 1.0.32.	✓
Requis openssl extension Requis pour l'envoi d'e-mails via SSL/TLS, la gestion des communications chiffrées avec les agents d'inventaire 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 Une version de PHP maintenue par la communauté PHP devrait être utilisée pour bénéficier des correctifs de sécurité et de bogues de PHP.	✓
Sécurité Configuration de sécurité pour les sessions Permet de s'assurer que la sécurité relative aux cookies de session est renforcée.	✓
Supplés exif extension Renforcer la sécurité de la validation des images.	✓
Supplés ldap extension Active l'utilisation de l'authentification à un serveur LDAP distant.	✓
Supplés Extensions PHP pour le marketplace Permet le support des formats de paquets les plus communs dans le marketplace.	✓
Supplés Zend OPcache extension Améliorer les performances du moteur PHP.	✓
Supplés Extensions émules de PHP Améliorer également les performances.	✓
Supplés Permissions pour le répertoire du marketplace Active l'installation des plugins à partir du Marketplace.	✓

At the bottom of the screen, there is a yellow button labeled 'Continuer >'.

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.



GLPI GLPI Installation

Étape 1

Configuration de la connexion à la base de données

Serveur SQL (MariaDB ou MySQL)

127.0.0.1

Utilisateur SQL

adminglpi

Mot de passe SQL

••••••••

Continuer >



GLPI GLPI Installation

Étape 2

Test de connexion à la base de données

✓ Connexion à la base de données réussie

Veillez sélectionner une base de données :

CRÉER UNE NOUVELLE BASE DE DONNÉES :

OU UTILISER UNE BASE EXISTANTE :

glpi

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...



GLPI GLPI Installation

Étape 3

Initialisation de la base de données.

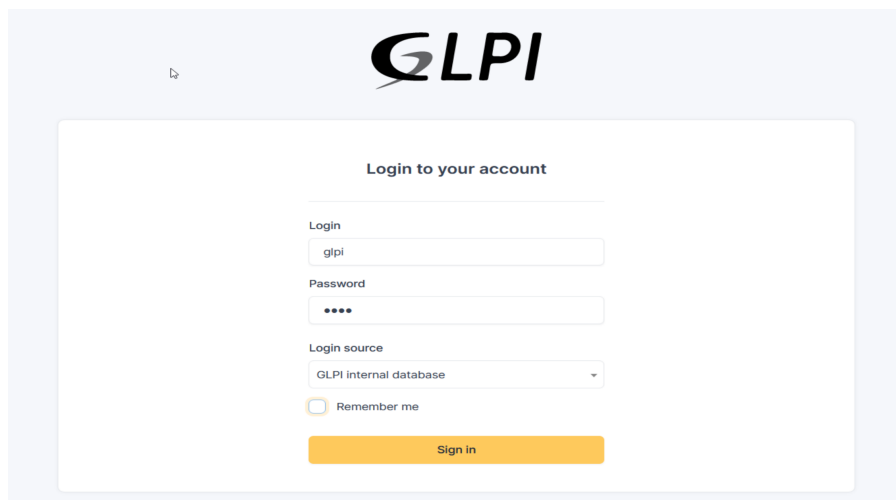
Initialisation des tables de la base de données avec ses données par défaut...

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

Continuer >

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.



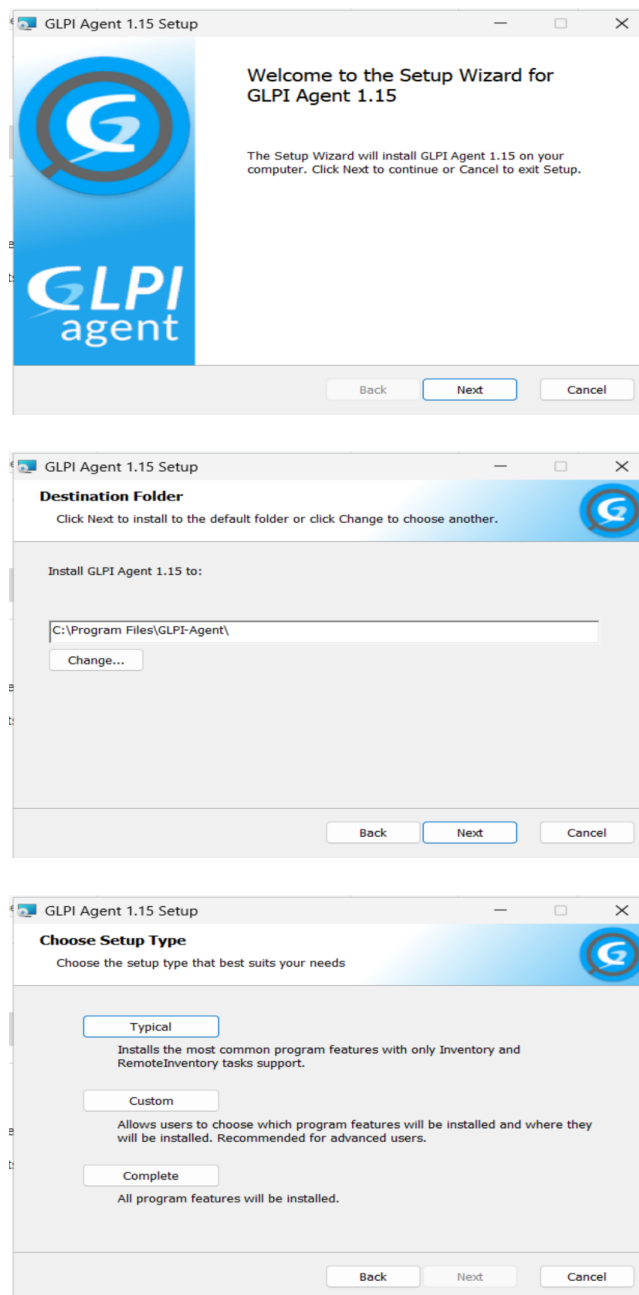
```
root@glpi:~# systemctl restart apache2  
root@glpi:~# rm /var/www/glpi/install/install.php
```

5 Phase 5 : Déploiement de l'Agent et Inventaire

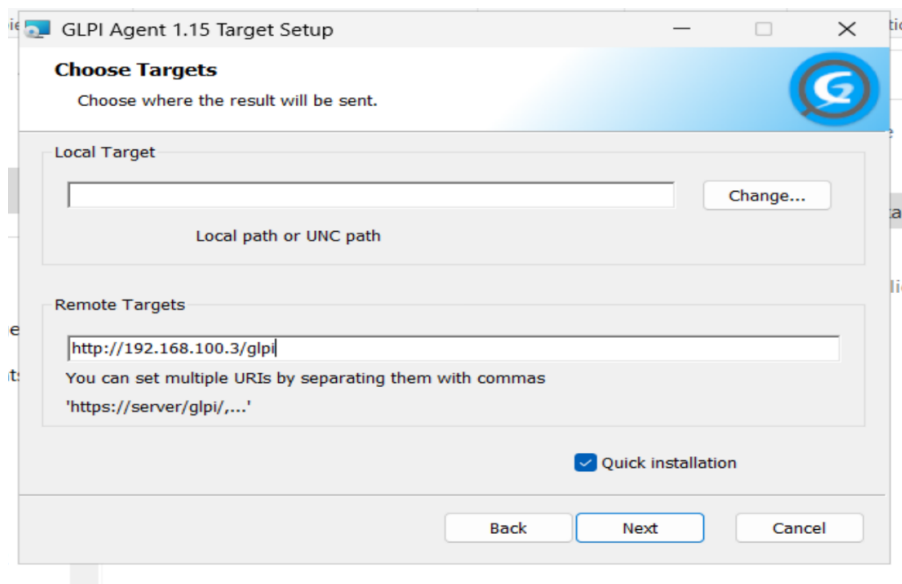
L'agent est un petit logiciel installé sur les ordinateurs du parc qui "scanne" le matériel (CPU, RAM, logiciels installés) et envoie ces données au serveur.

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".

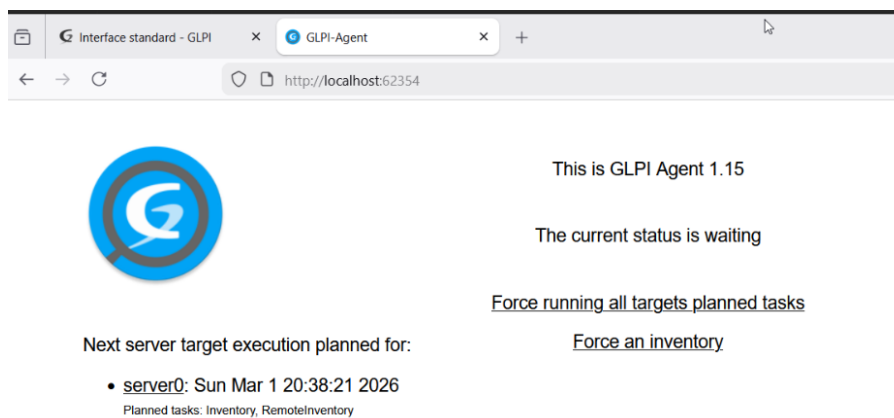


L'étape la plus importante est de renseigner l'URL du serveur. L'agent doit savoir vers quelle adresse envoyer ses données. Nous saisissons l'adresse IP du serveur suivi du nom de l'application.

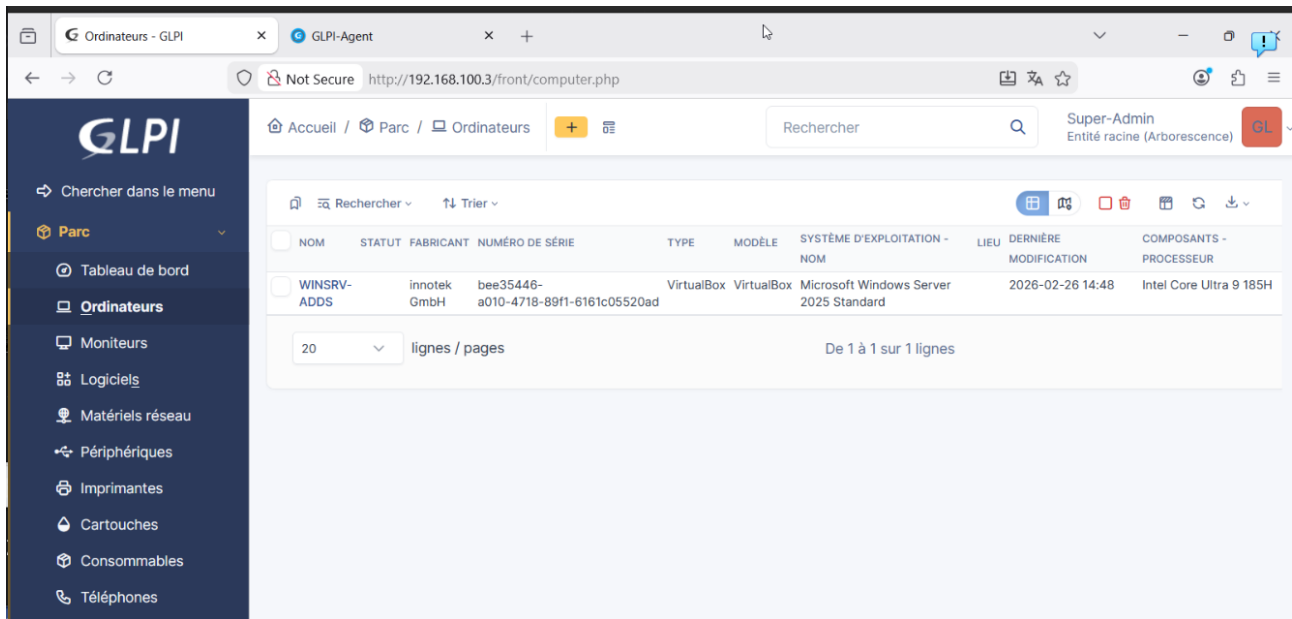


5.2 Remontée de l'Inventaire

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.



Deuxième partie

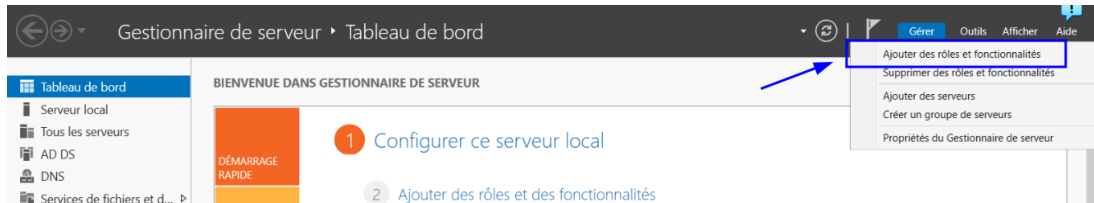
Documentation Technique : Services Bureau à Distance (RDS)

Déploiement et Configuration sur Windows Server 2025

6 Phase 1 : Déploiement des Services de rôle

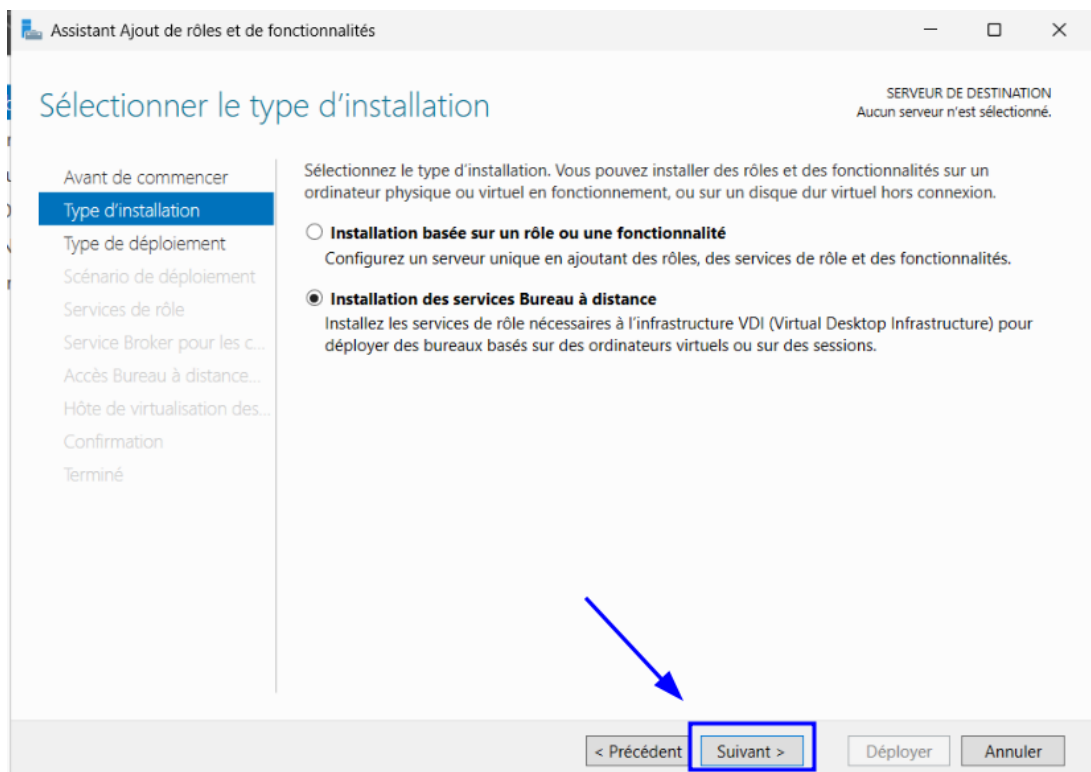
6.1 Lancement de l'assistant d'ajout de rôles

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.



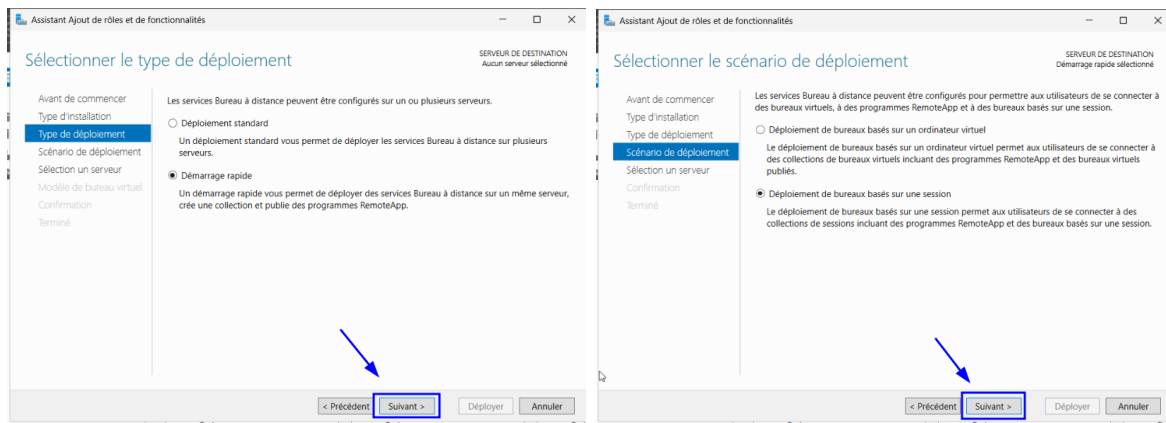
6.2 Sélection du type d'installation

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.



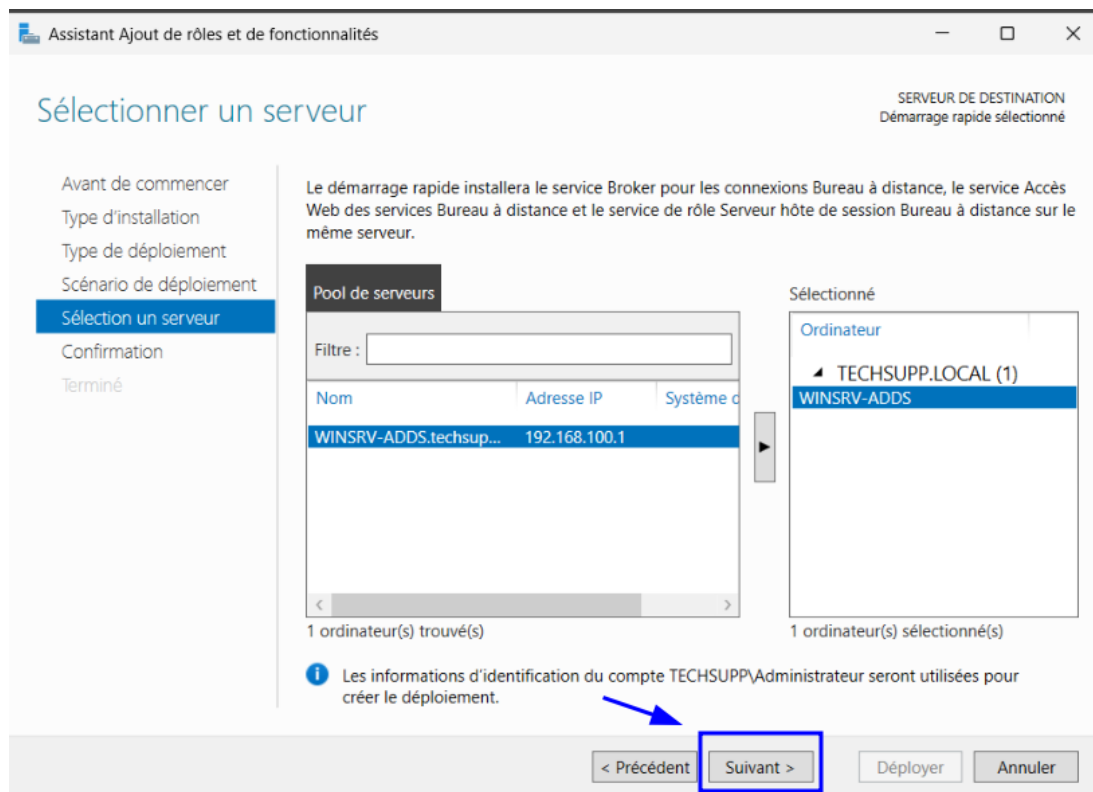
6.3 Choix du type de déploiement et du scénario

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.



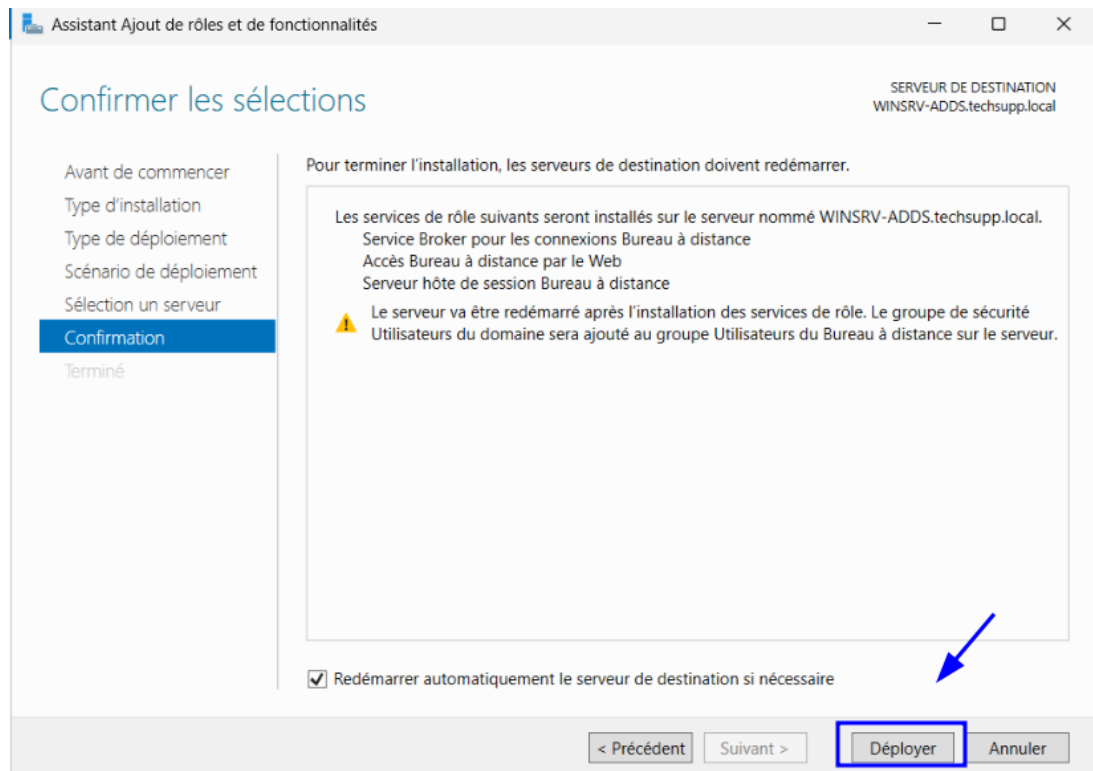
6.4 Sélection du serveur de destination

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.



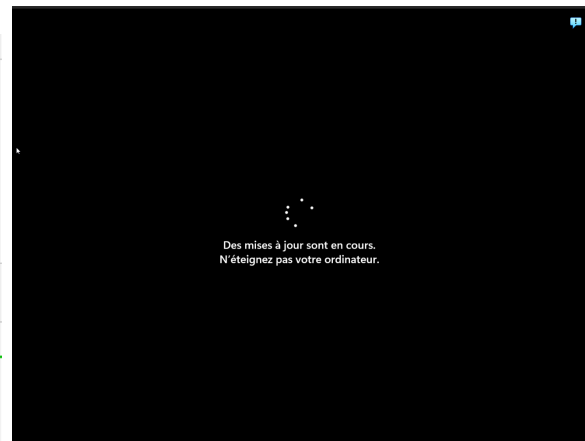
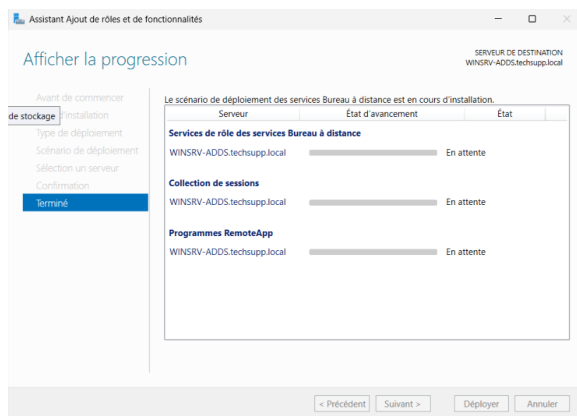
6.5 Confirmation et redémarrage automatique

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.



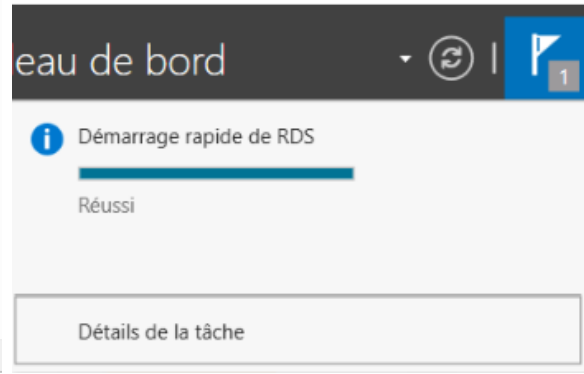
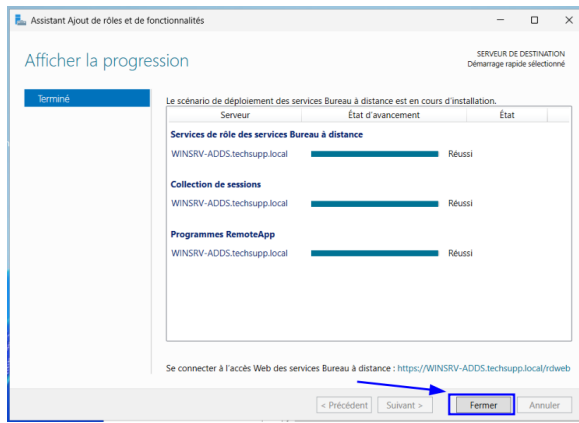
6.6 Suivi de la progression et phase système

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

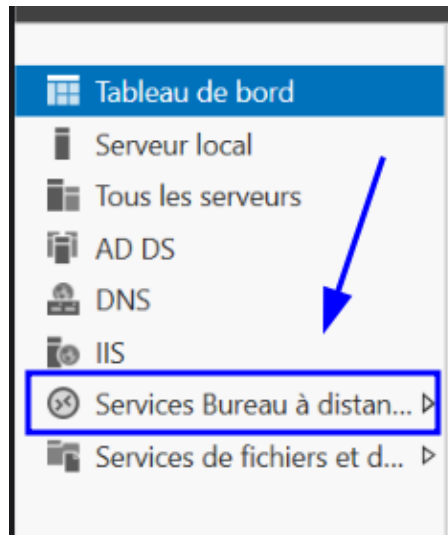
Après le redémarrage, nous nous reconnectons au serveur. L'assistant reprend automatiquement et confirme que le déploiement, la création de la collection et la publication des programmes RemoteApp ont réussi. Une URL d'accès Web est alors générée par défaut.



7 Phase 2 : Configuration du Gestionnaire de Licences

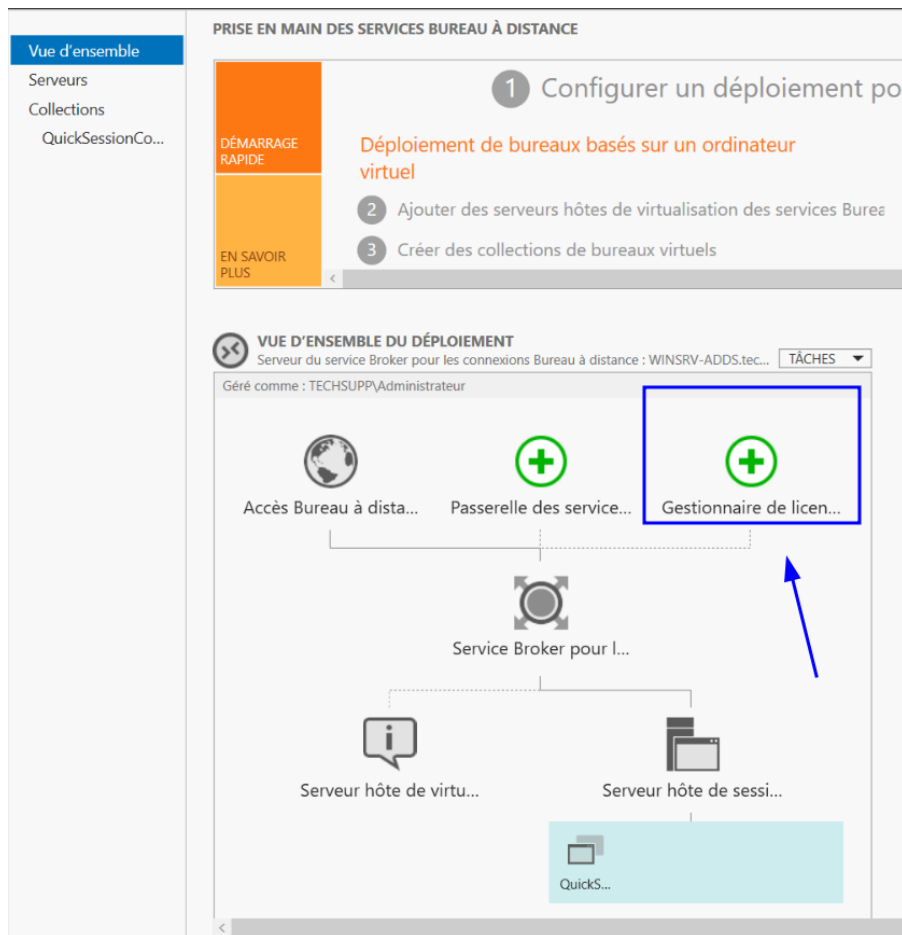
7.1 Accès aux outils de gestion RDS

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.



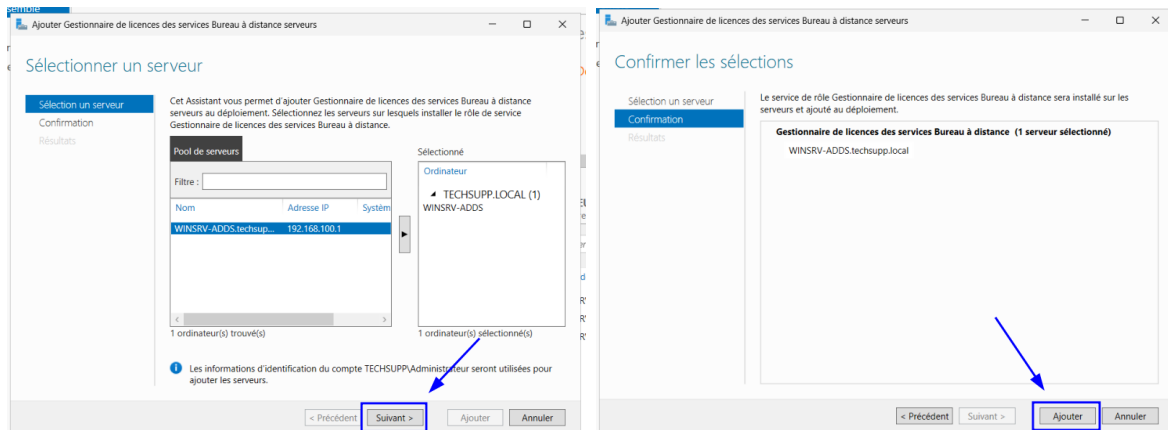
7.2 Installation du rôle Gestionnaire de licences

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.



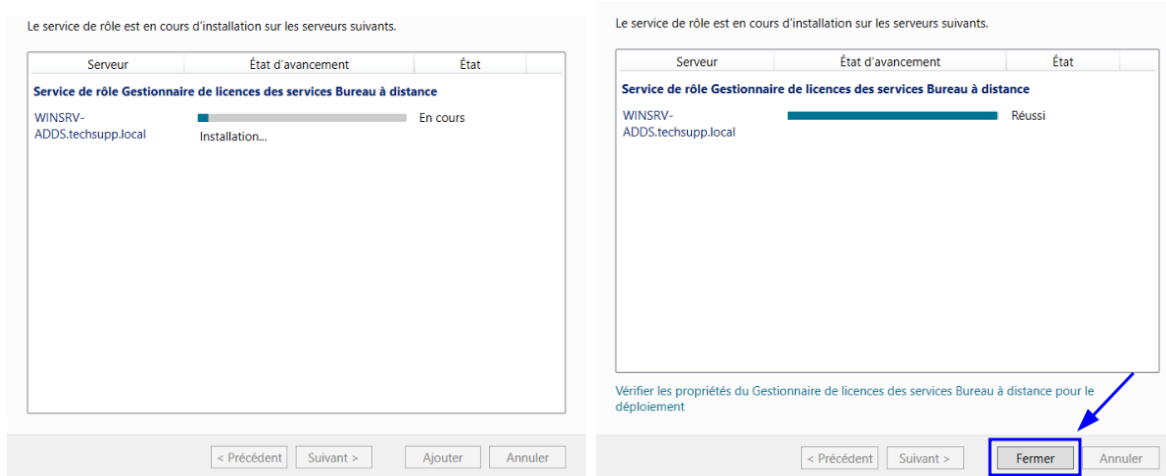
7.3 Confirmation et installation du rôle de licence

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.



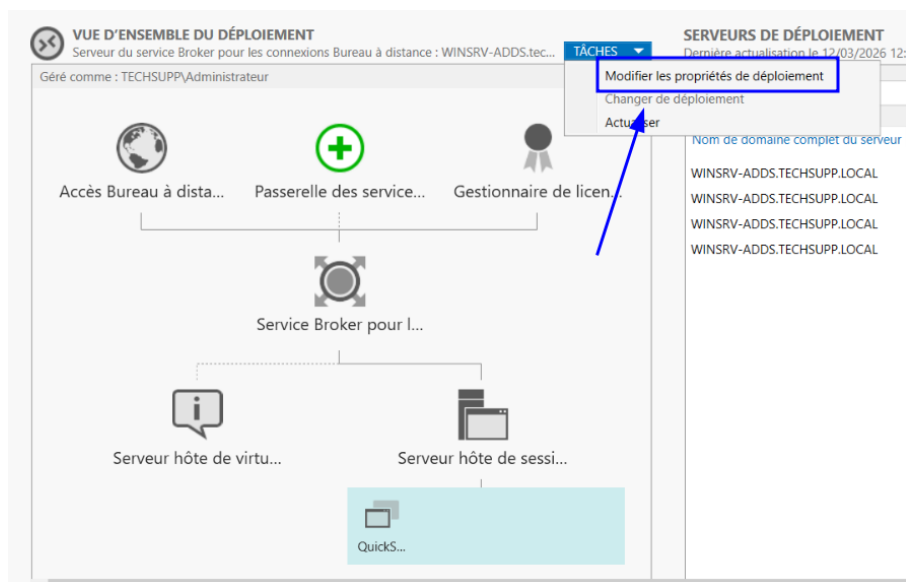
7.4 Statut de l'installation des licences

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.



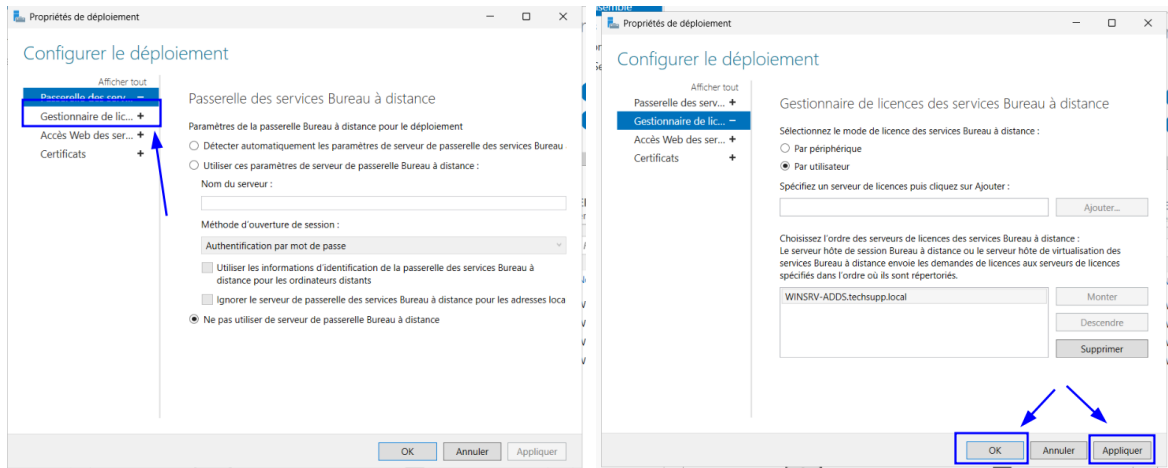
7.5 Liaison du mode de licence au déploiement

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'

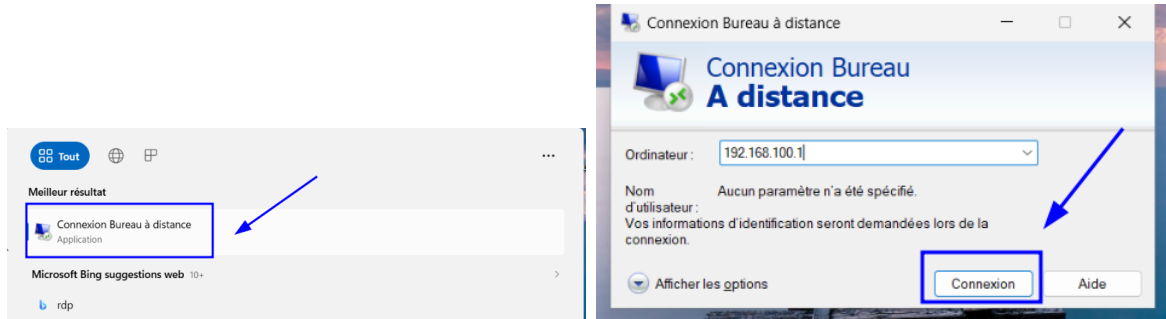
Dans la fenêtre des propriétés, nous sélectionnons l'onglet **Gestionnaire de licences**. Puis nous choisissons le mode de licence **Par utilisateur** et nous nous assurons que notre serveur est bien présent dans la liste des serveurs de licences. Enfin nous cliquons sur **Appliquer** pour valider.



8 Phase 3 : Validation de la Connexion Cliente

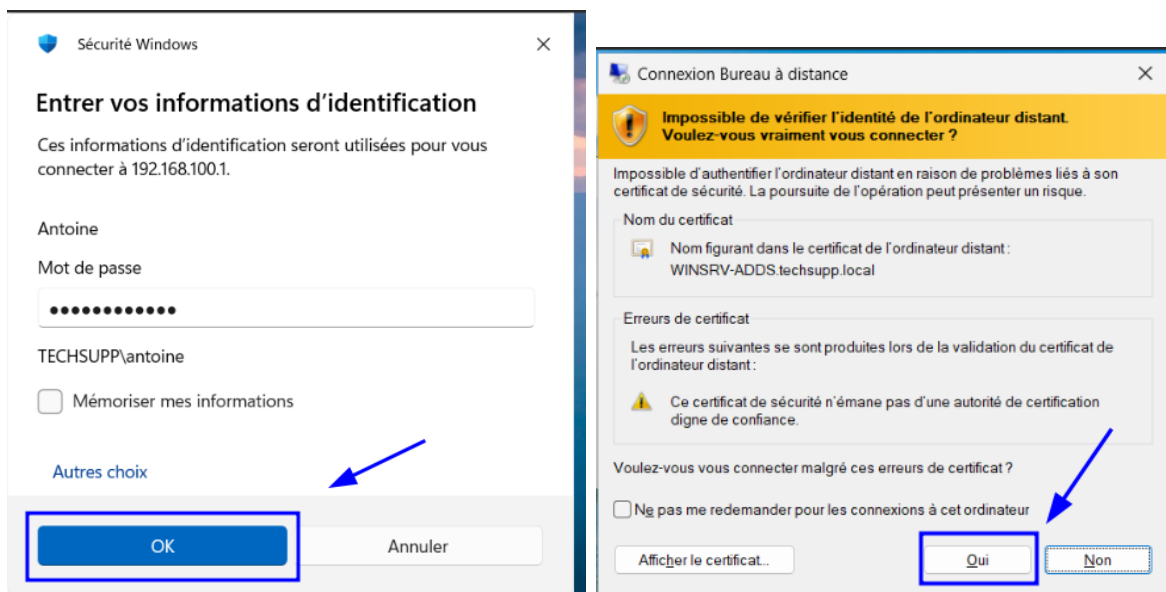
8.1 Préparation du poste client

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**.



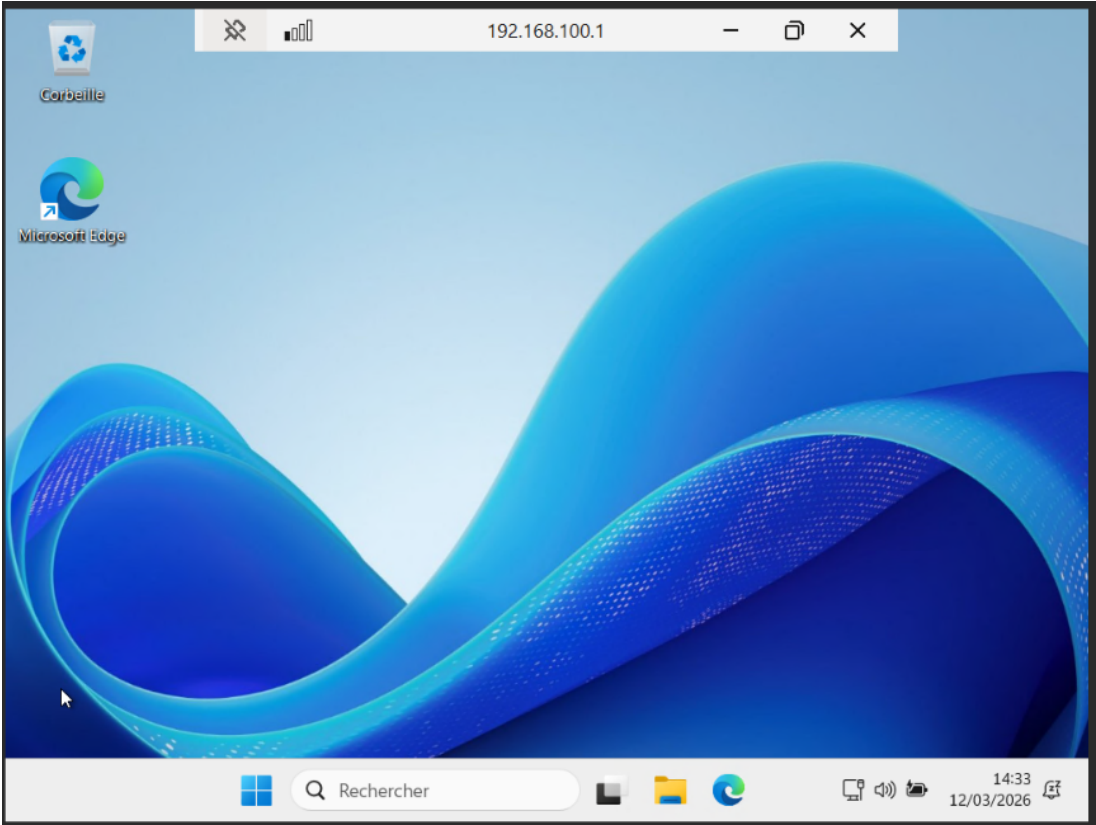
8.2 Authentification et gestion du certificat

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.



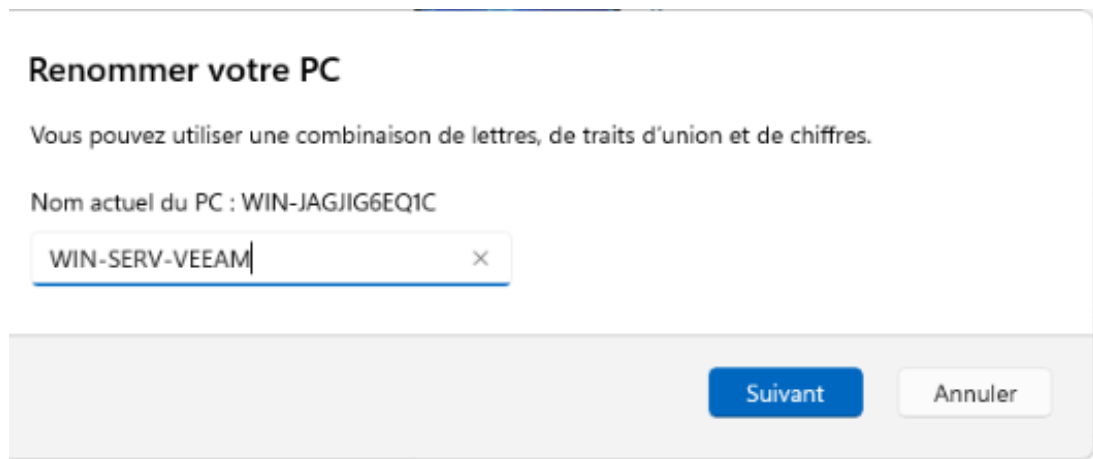
Troisième partie

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

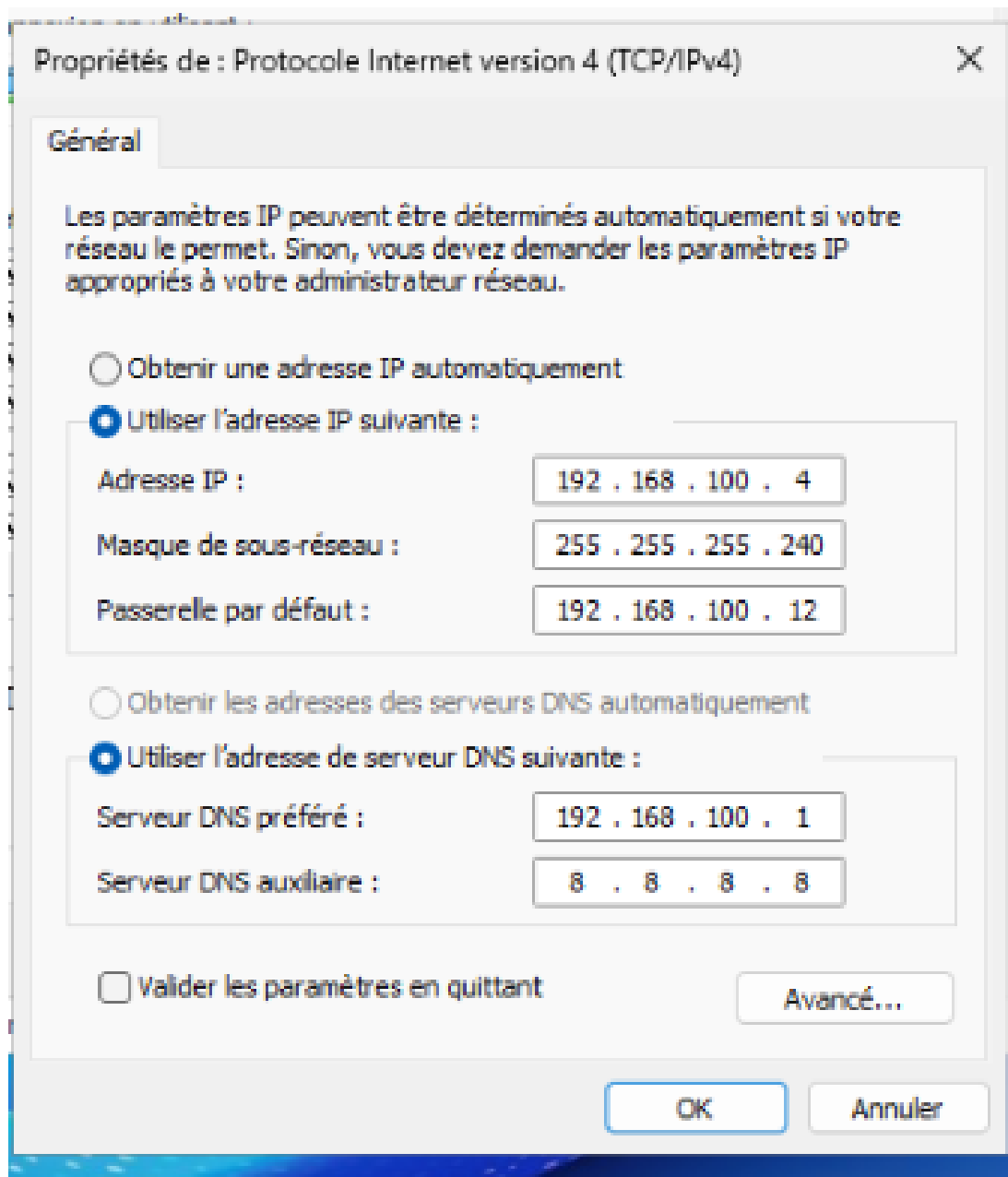
9 Préparation de l'environnement Windows

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

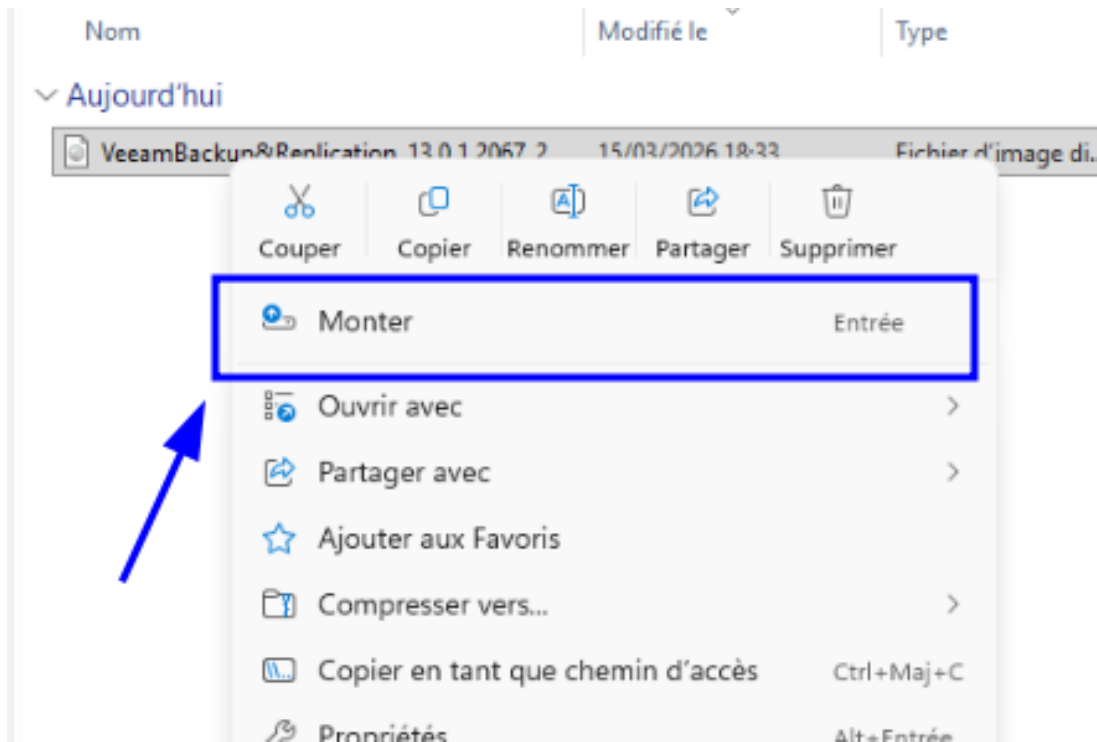
Pour débuter, nous accédons aux propriétés du système afin de renommer l'ordinateur en "WIN-SERV-VEEAM".



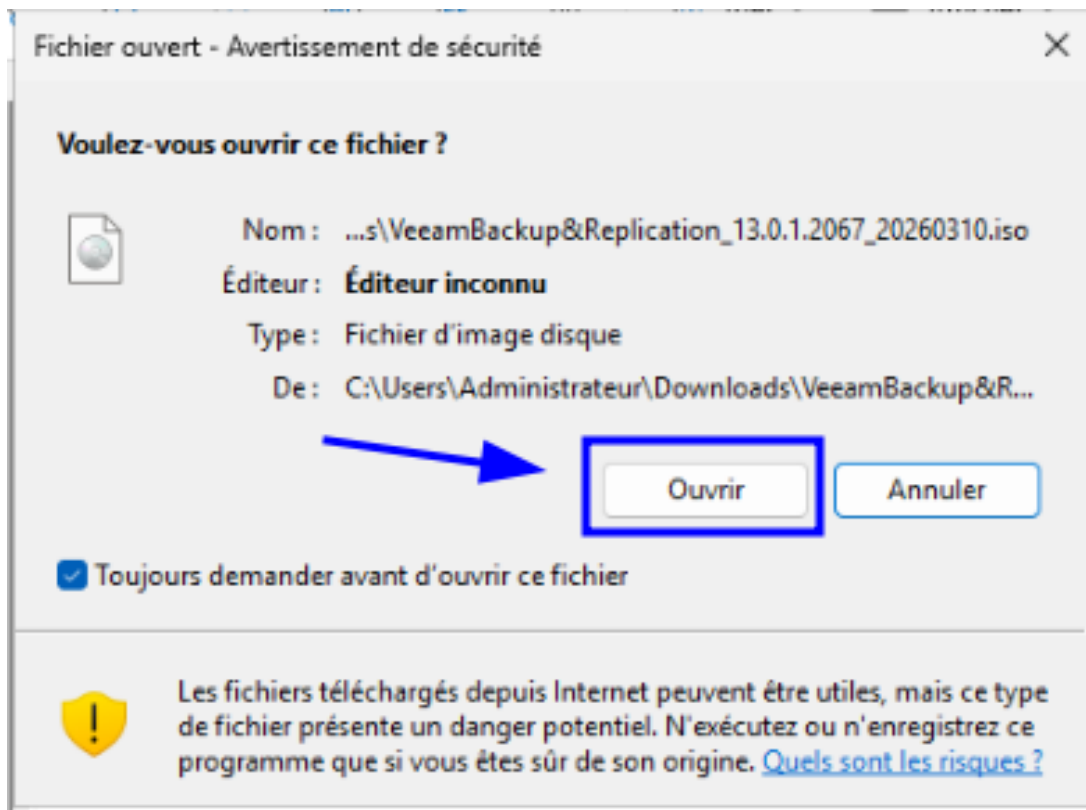
Par la suite, nous configurons les paramètres TCP/IPv4 en fixant l'adresse IP sur 192.168.100.4 avec sa passerelle et ses DNS.



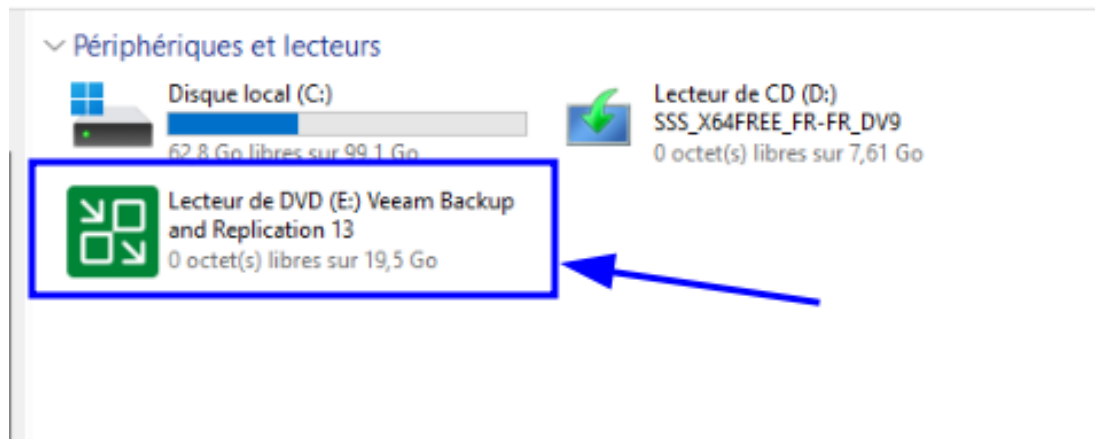
Une fois le réseau stable, nous effectuons un clic droit sur le fichier ISO téléchargé pour sélectionner l'option "Monter".



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.



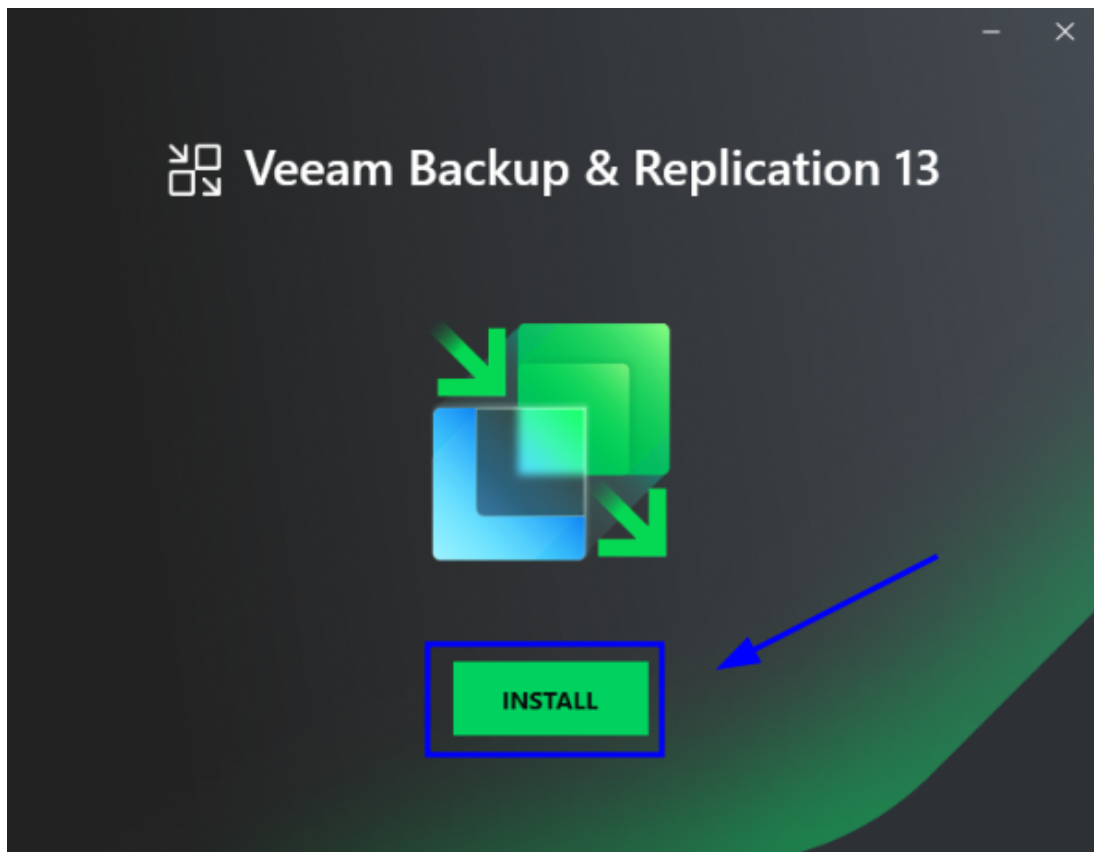
10 Installation de Veeam Backup & Replication

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

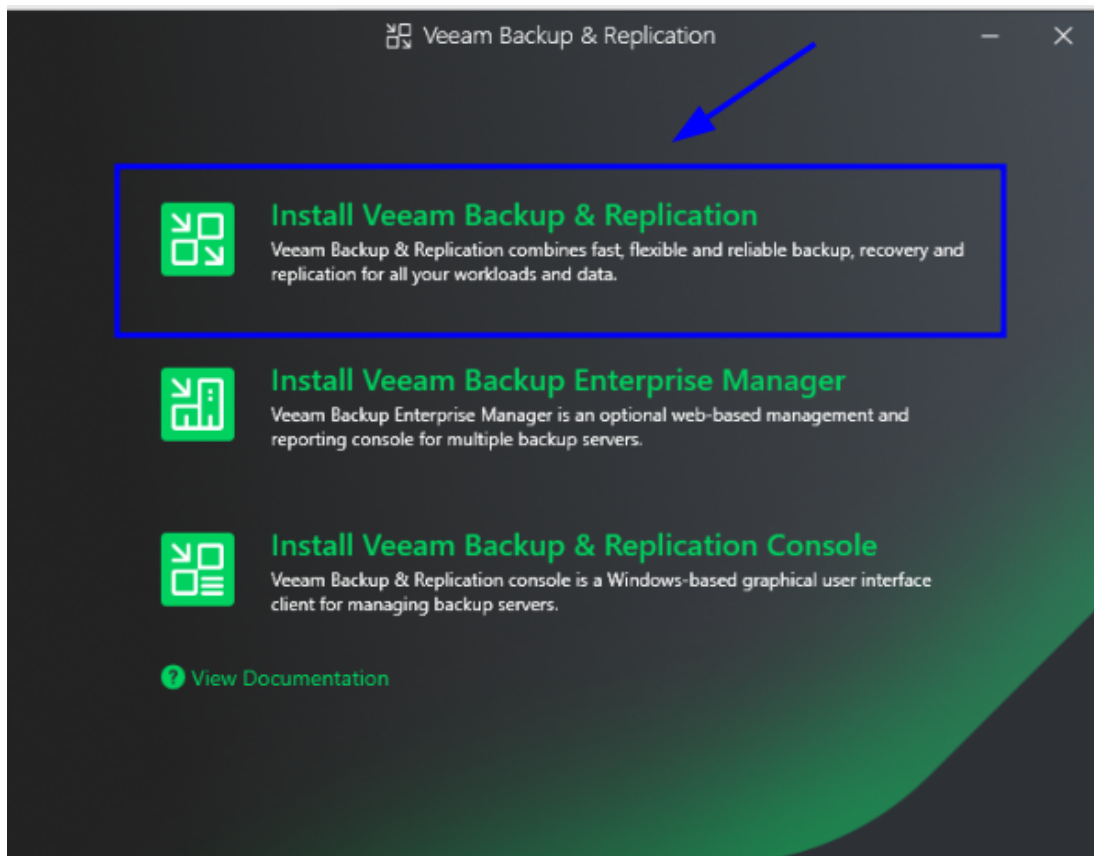
The screenshot shows a file explorer window displaying a directory listing. The columns are 'Nom', 'Modifié le', 'Type', and 'Taille'. The 'Setup' file is highlighted with a blue box and a blue arrow points to it.

Nom	Modifié le	Type	Taille
Backup	26/02/2026 21:23	Dossier de fichiers	
Catalog	10/12/2025 18:43	Dossier de fichiers	
EnterpriseManager	26/02/2026 21:23	Dossier de fichiers	
EULA	10/12/2025 18:43	Dossier de fichiers	
Explorers	10/12/2025 18:43	Dossier de fichiers	
Packages	10/03/2026 07:20	Dossier de fichiers	
Plugins	10/03/2026 07:20	Dossier de fichiers	
Redistr	10/03/2026 07:20	Dossier de fichiers	
Setup	10/03/2026 07:20	Dossier de fichiers	
Tools	10/12/2025 18:44	Dossier de fichiers	
Updates	10/03/2026 07:20	Dossier de fichiers	
autorun	10/12/2025 18:44	Informations de c...	1 Ko
Setup	10/12/2025 18:44	Application	313 Ko

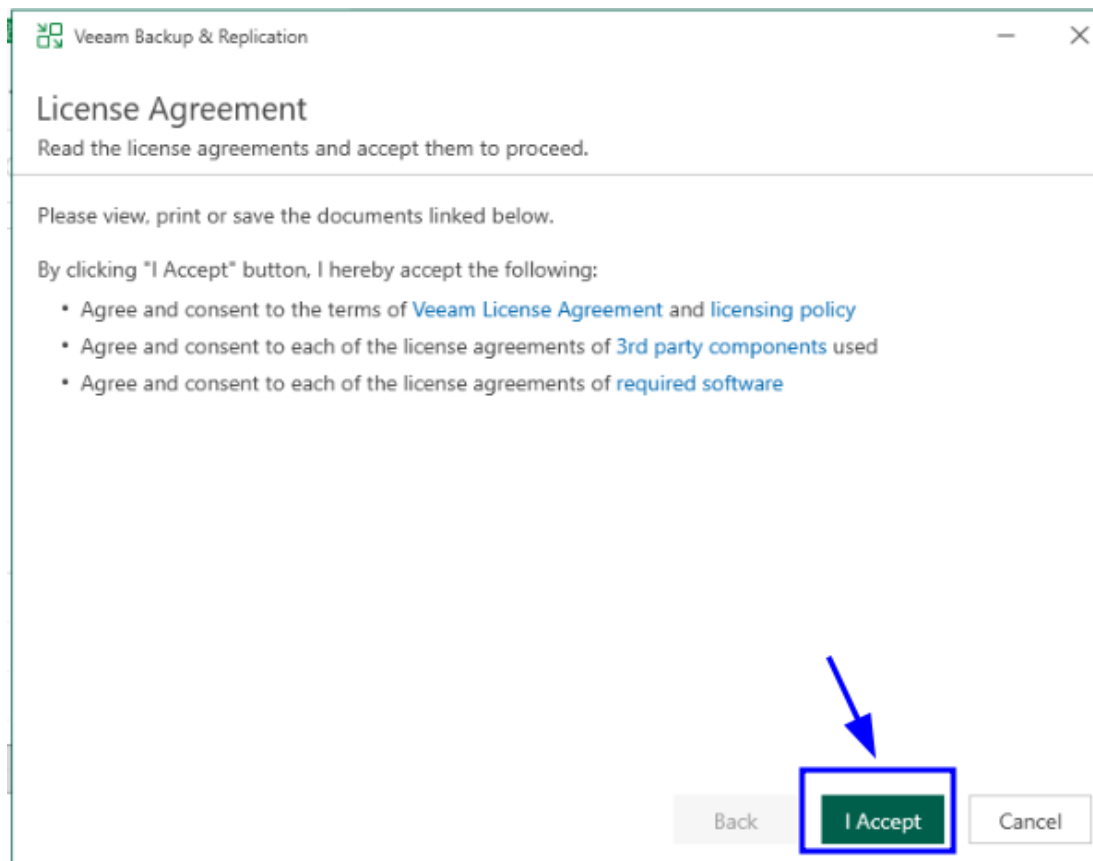
Nous entamons maintenant la phase de déploiement des composants serveurs. Sur l'écran d'accueil de la version 13, nous cliquons sur le bouton vert "INSTALL".



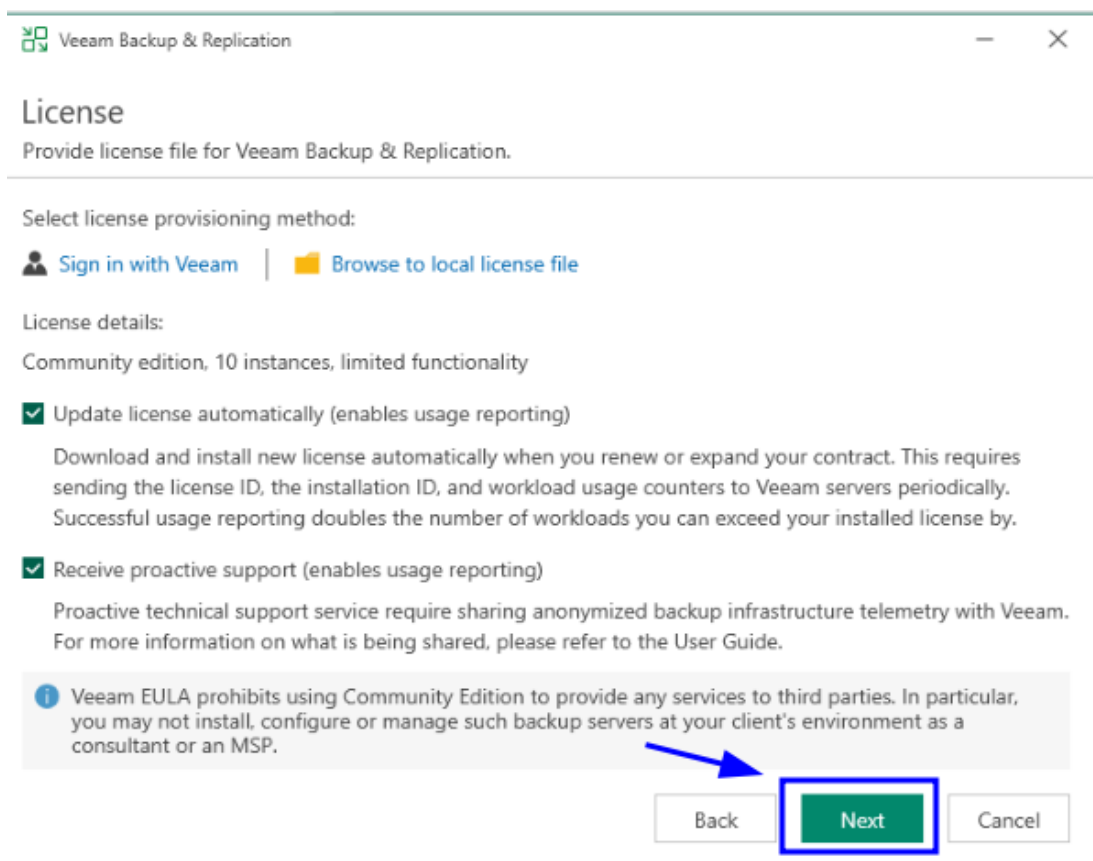
Dans le menu de sélection, nous choisissons d'installer le composant principal "Veeam Backup & Replication".



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

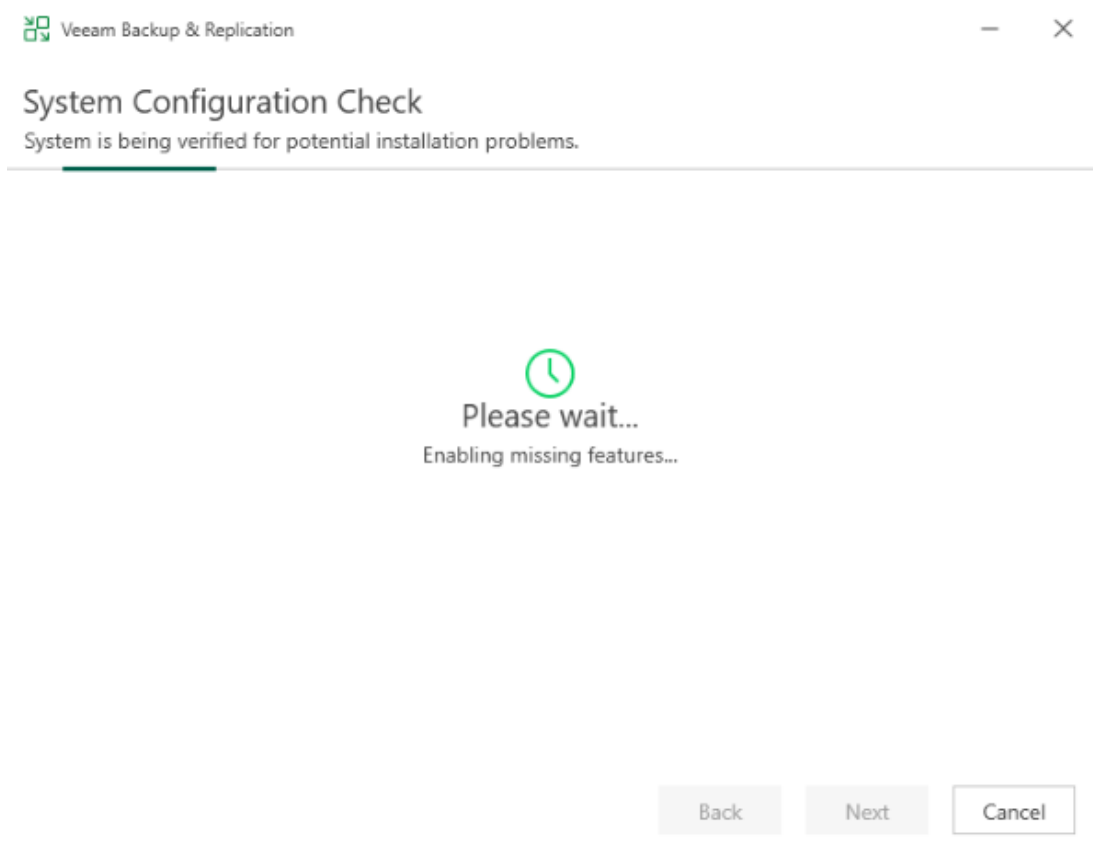


Concernant la licence, nous poursuivons sans fichier externe afin d'utiliser la "Community Edition".

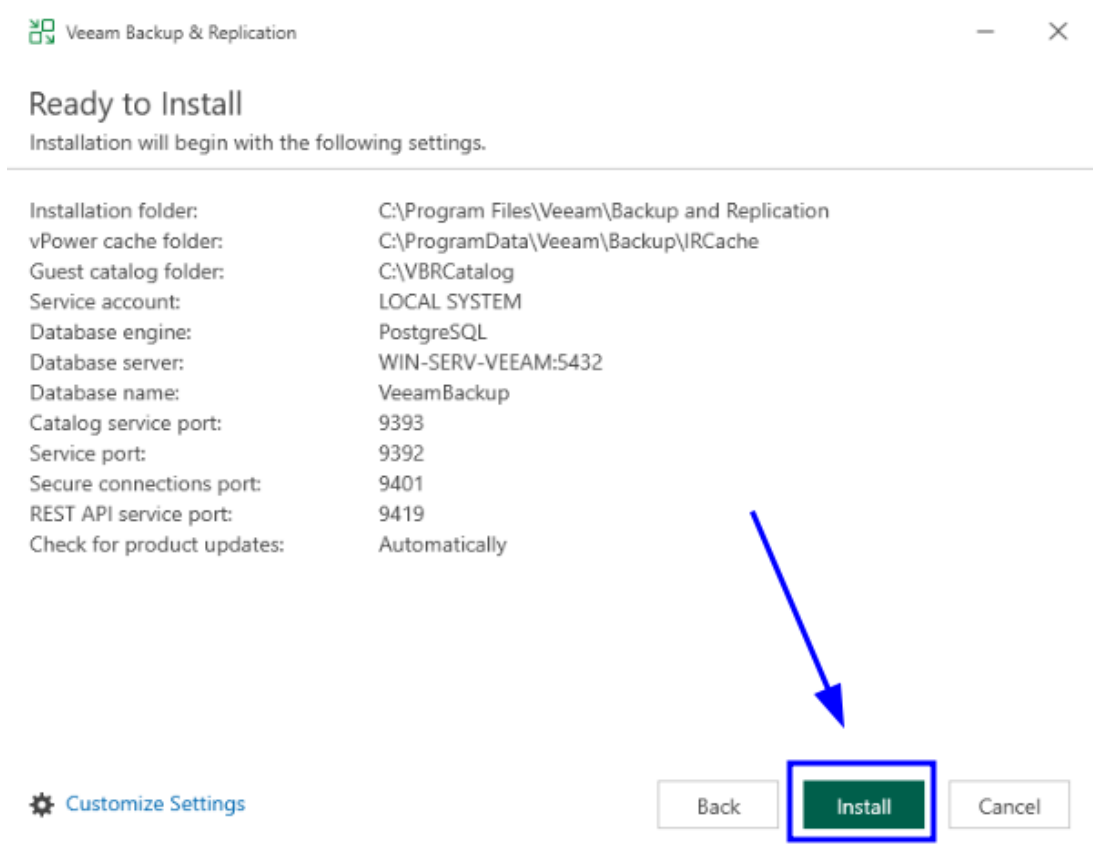


À ce stade, nous laissons l'assistant vérifier la configuration et activer les fonctionnalités

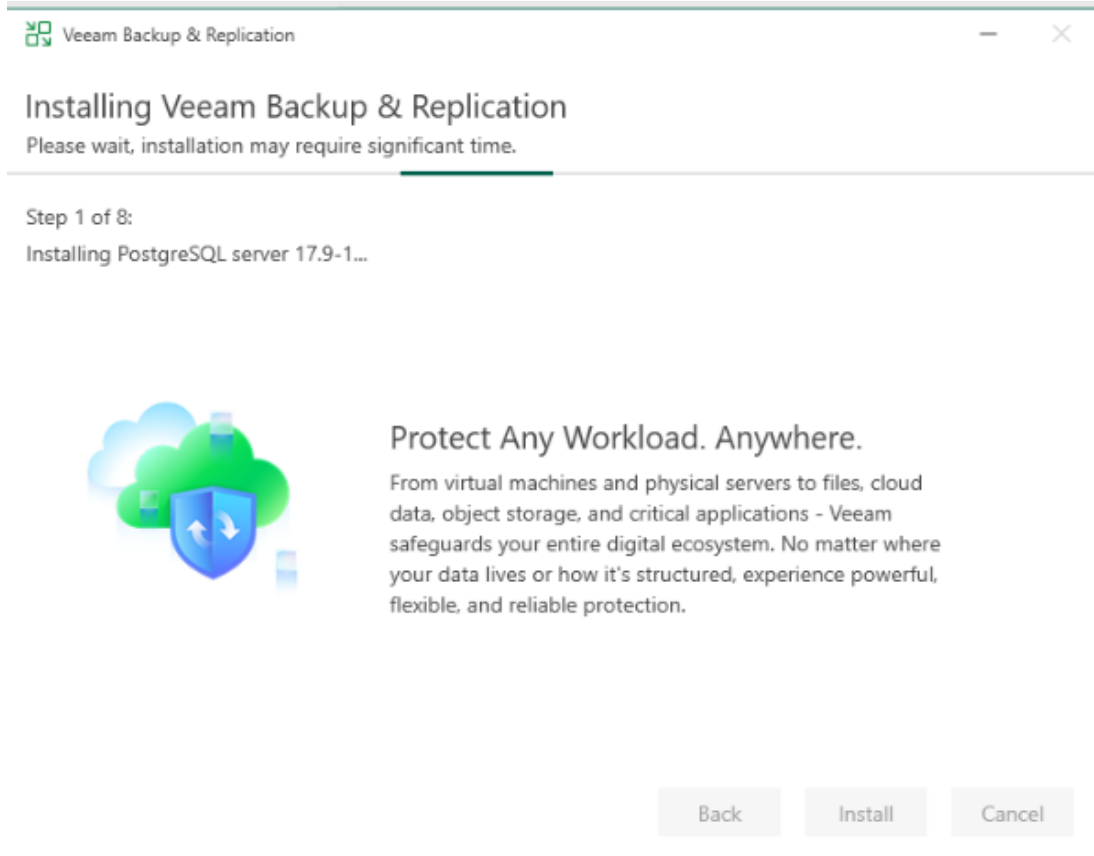
système requises.



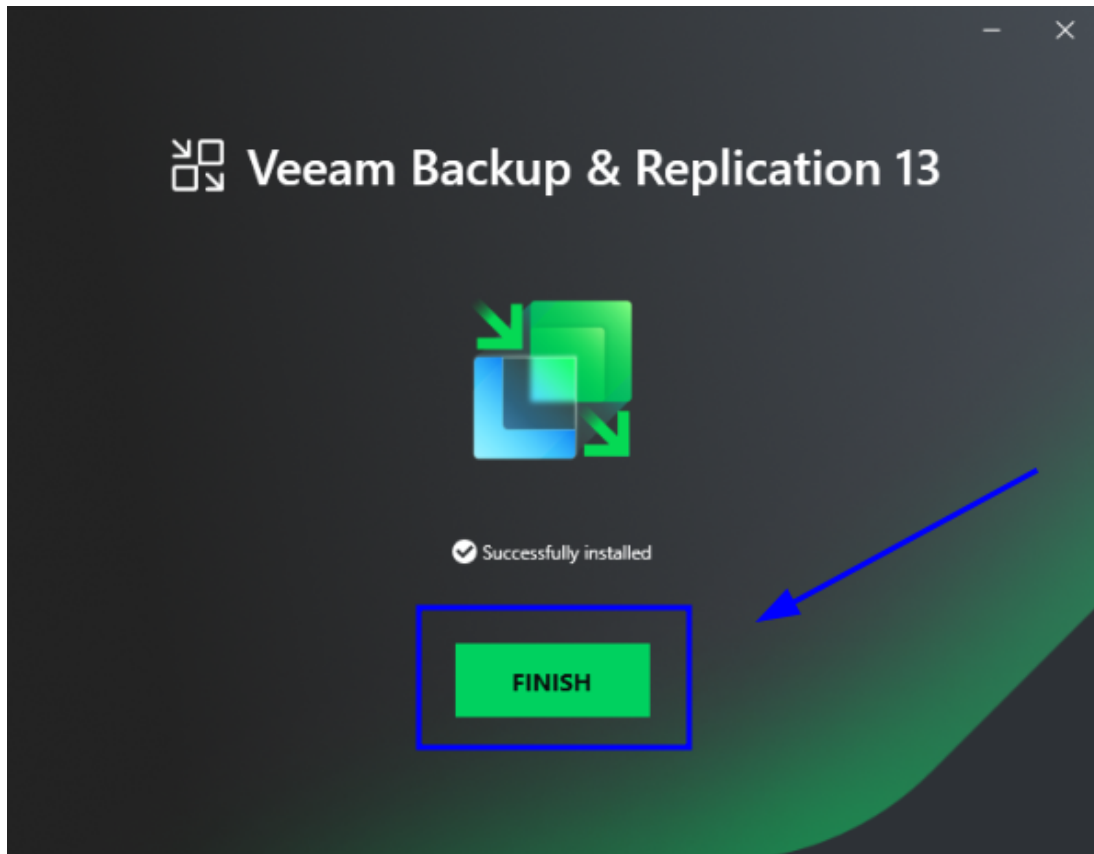
Avant de lancer la copie, nous vérifions le résumé des ports et de l'instance PostgreSQL puis cliquons sur "Install".



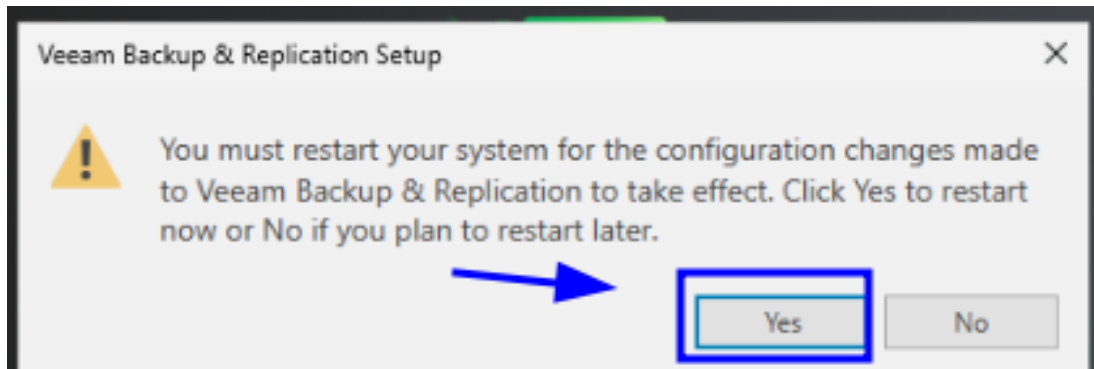
Progressivement, nous suivons la barre d'avancement de l'installation des différents packages.



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



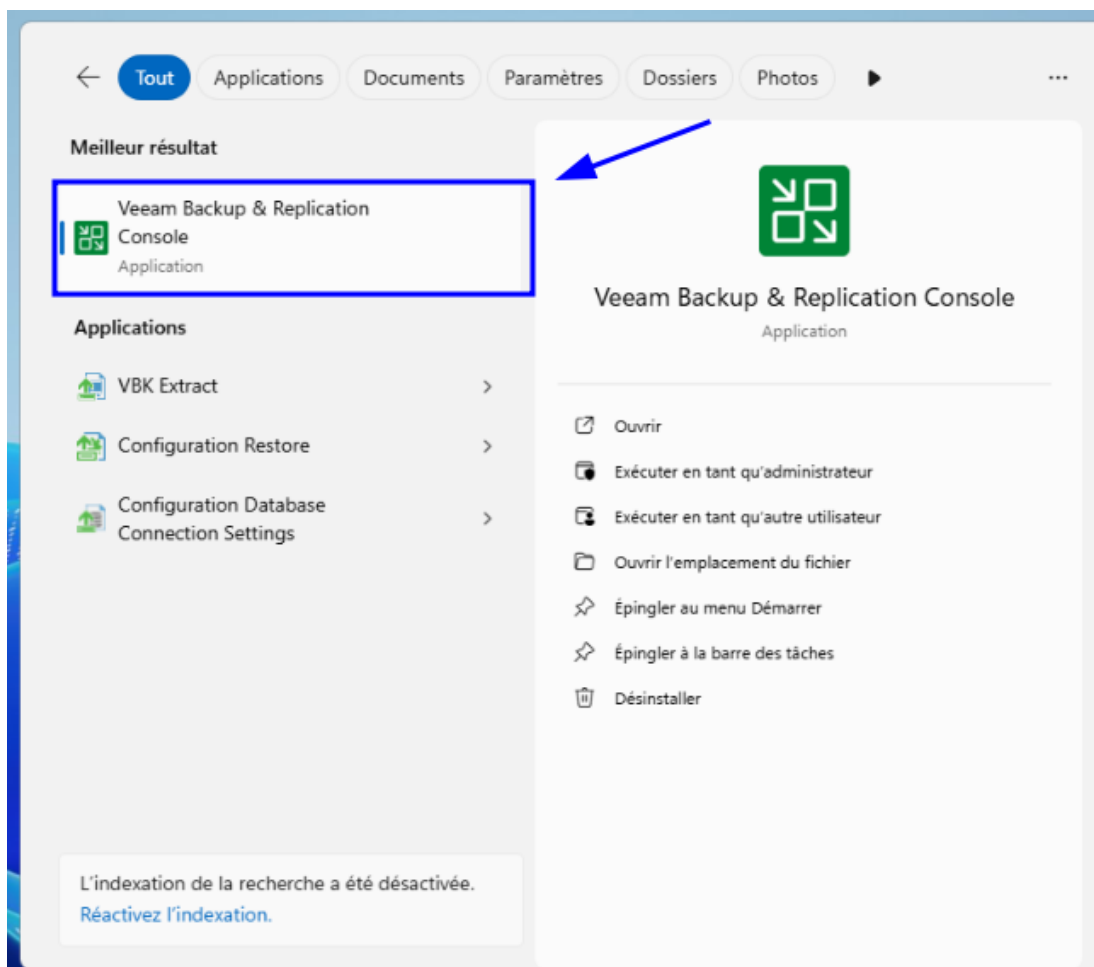
Enfin, nous acceptons le redémarrage immédiat du serveur pour appliquer les modifications finales.



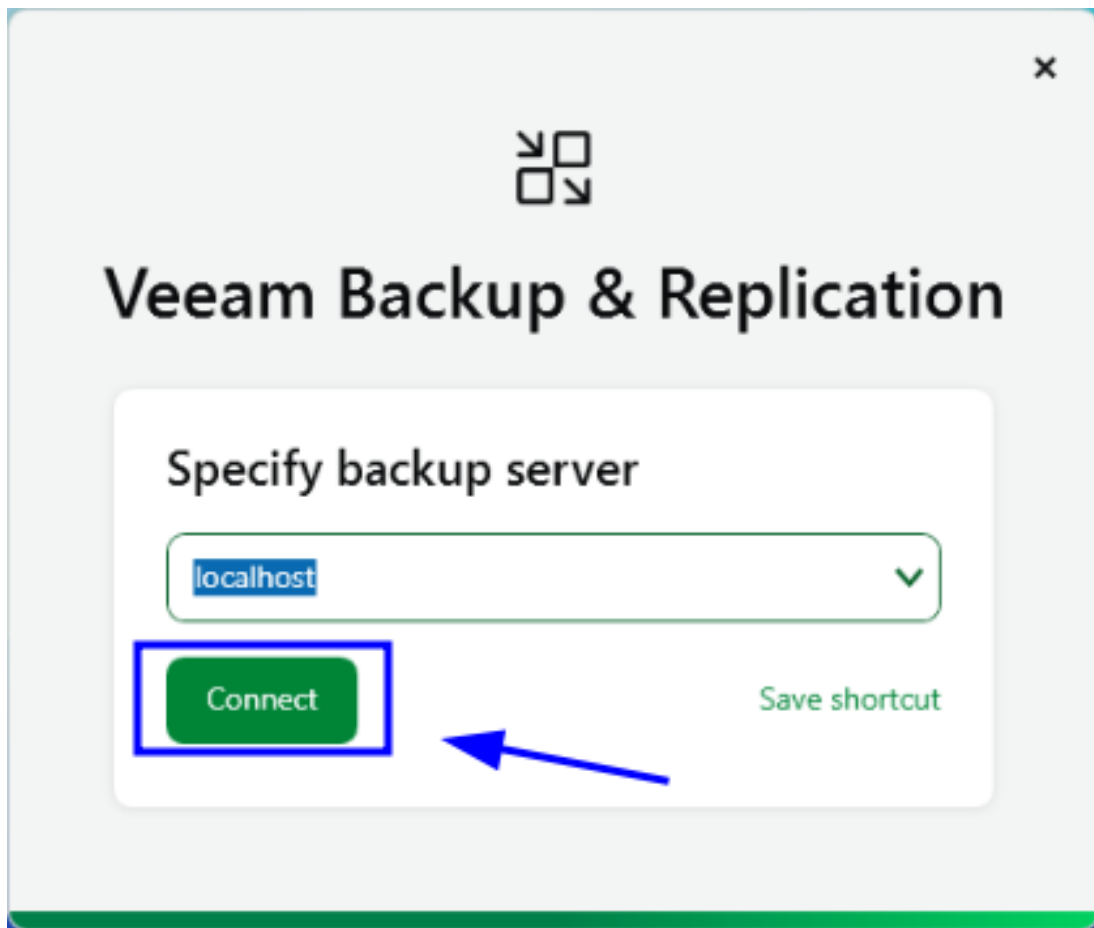
11 Connexion à la Console de gestion

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

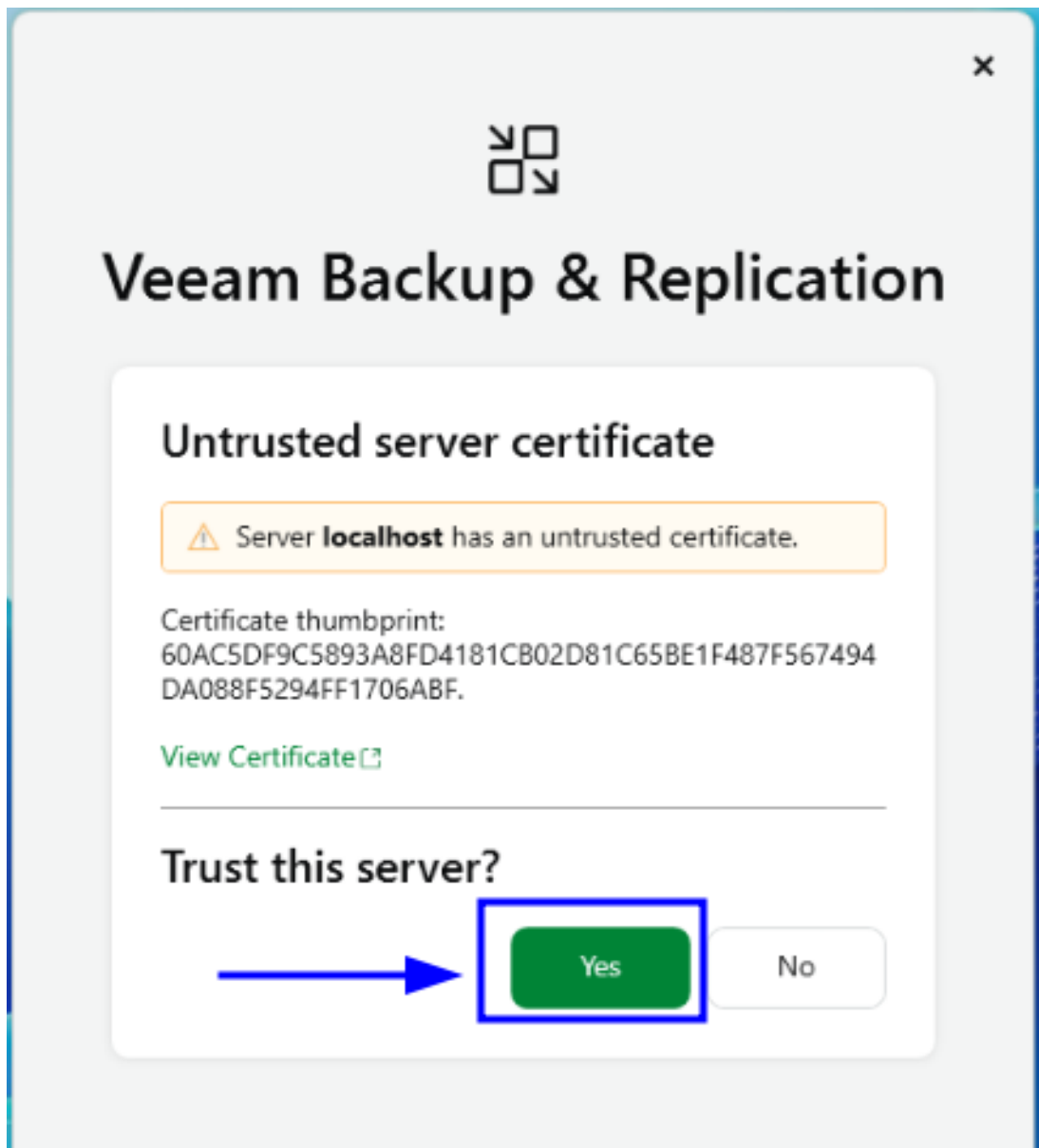
Dans le menu de recherche Windows, nous lançons l'application "Veeam Backup & Replication Console".



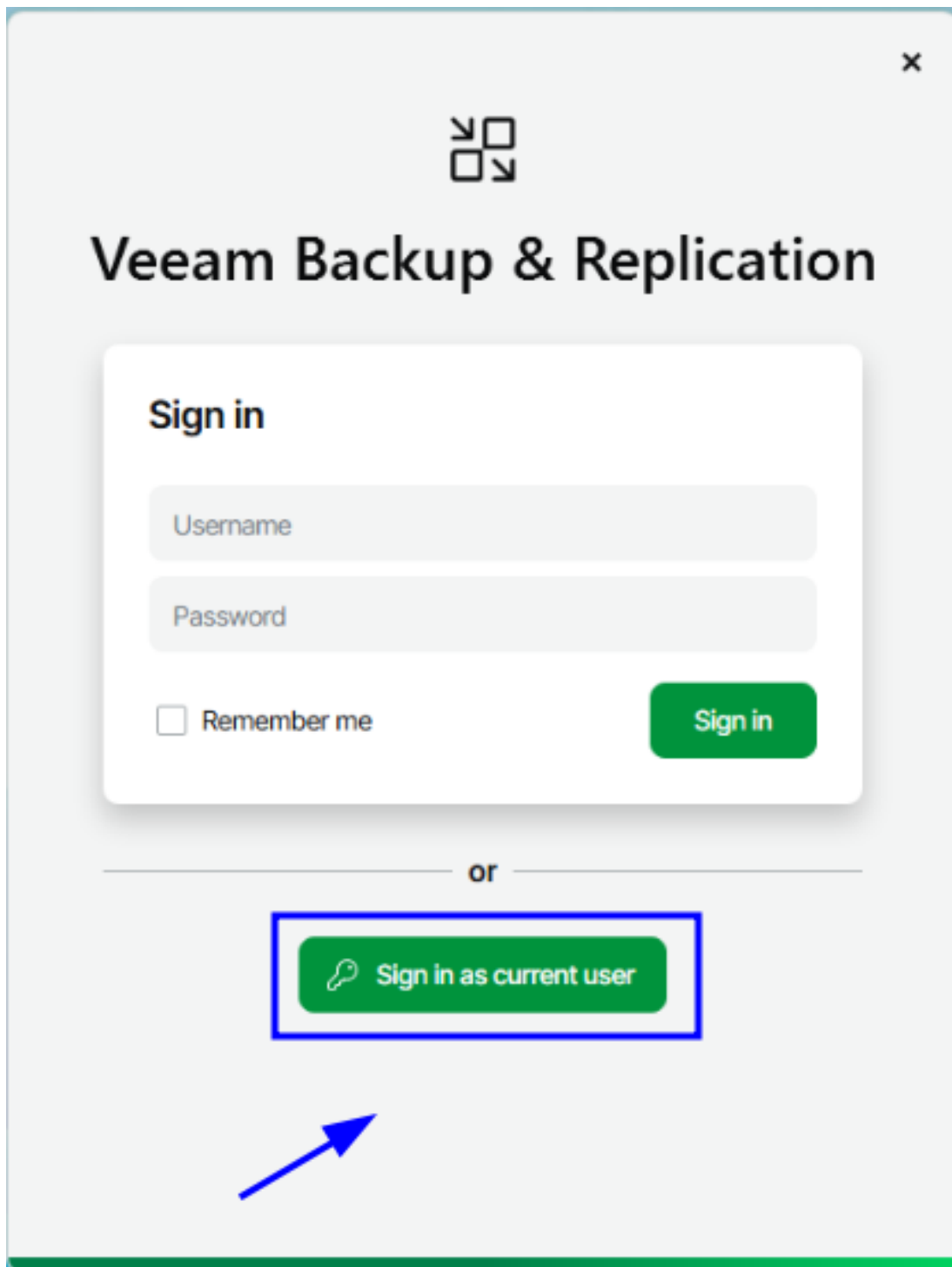
Dans la fenêtre de connexion, nous spécifions le serveur "localhost" et cliquons sur "Connect".



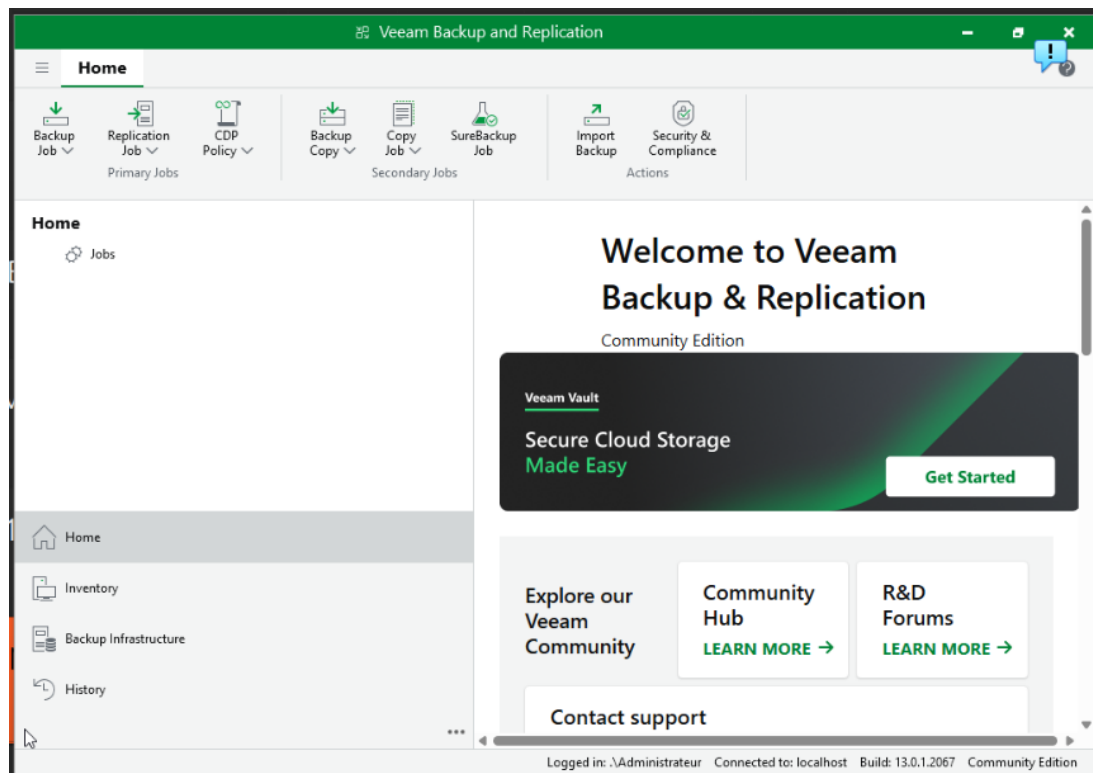
Face au message sur le certificat non approuvé, nous cliquons sur "Yes" pour confirmer la confiance. À ce moment-là, nous pouvons visualiser l’empreinte numérique du certificat SSL du serveur.



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



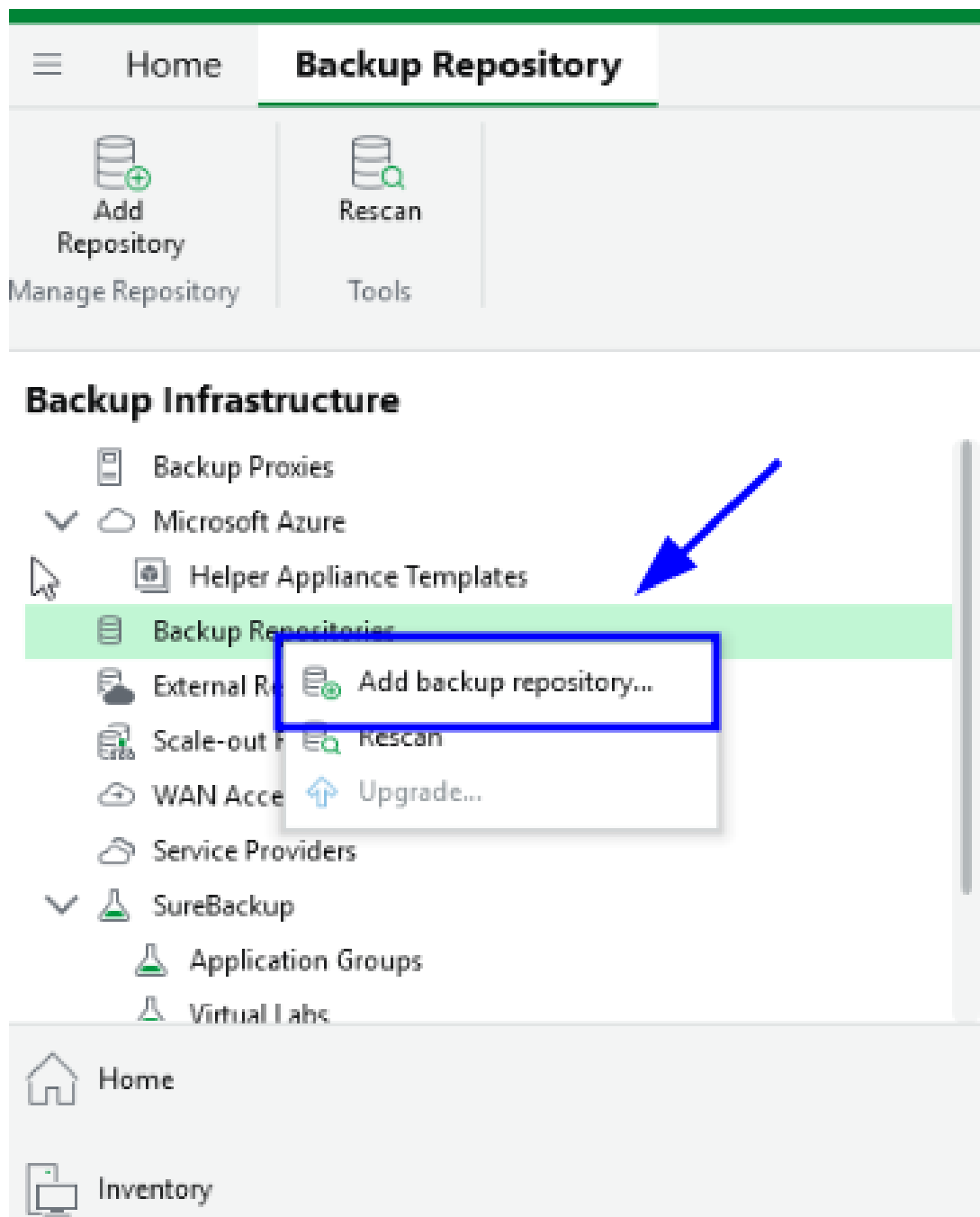
Finalement, nous arrivons sur le tableau de bord principal nous souhaitant la bienvenue.



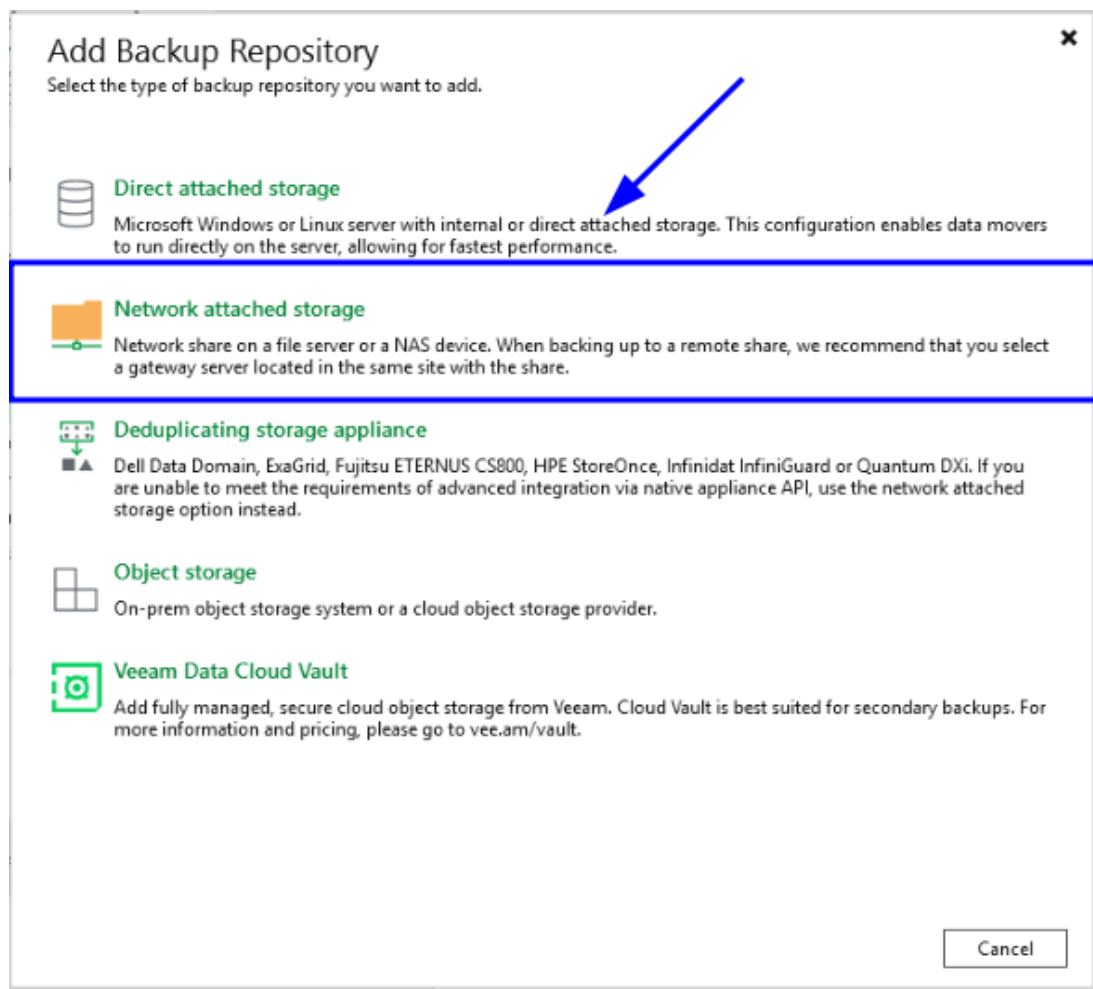
12 Configuration du Backup Repository (Stockage)

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

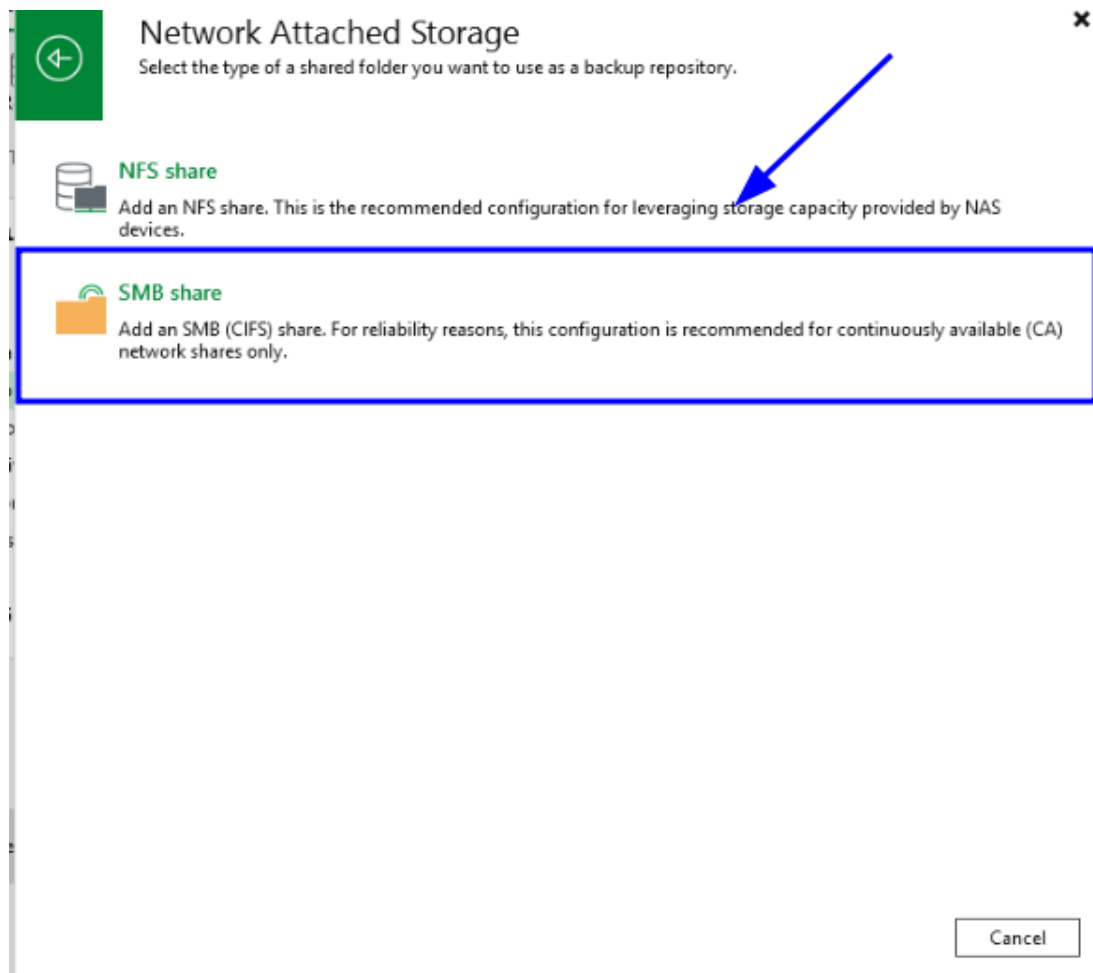
Aussitôt, nous effectuons un clic droit sur "Backup Repositories" pour choisir "Add backup repository".



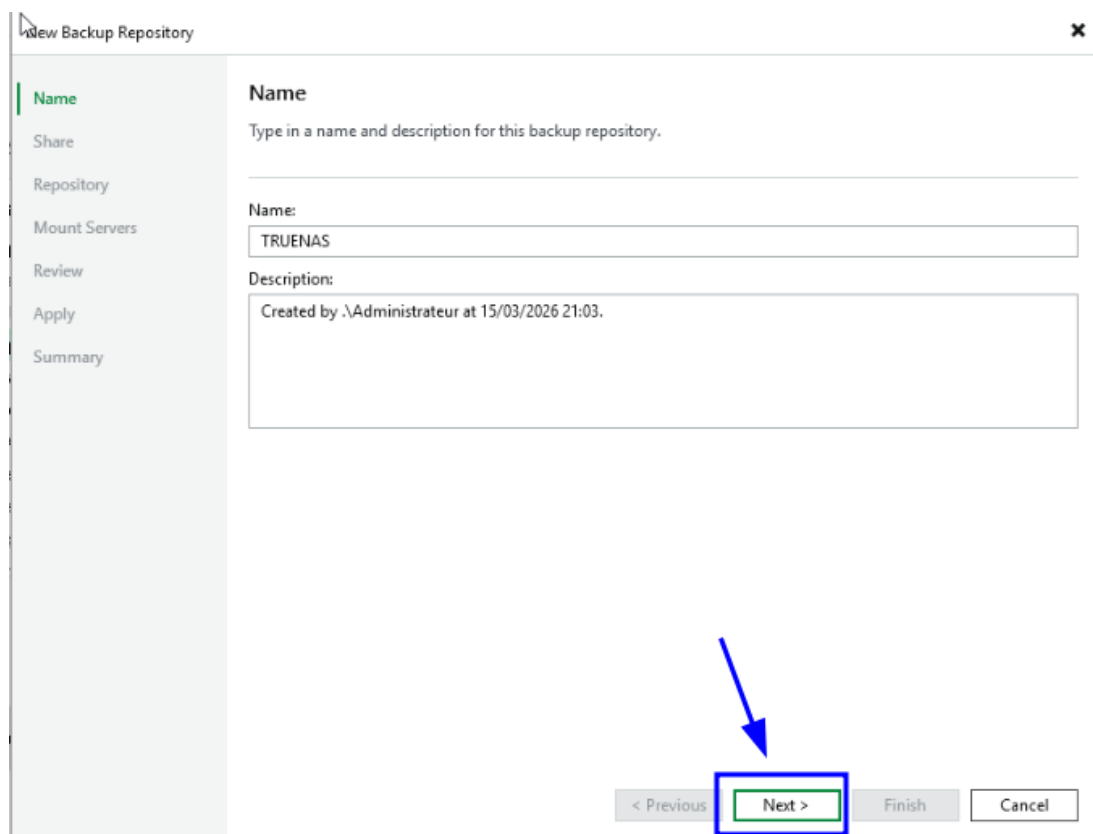
Dans le menu des types de stockage, nous sélectionnons l'option "Network attached storage".



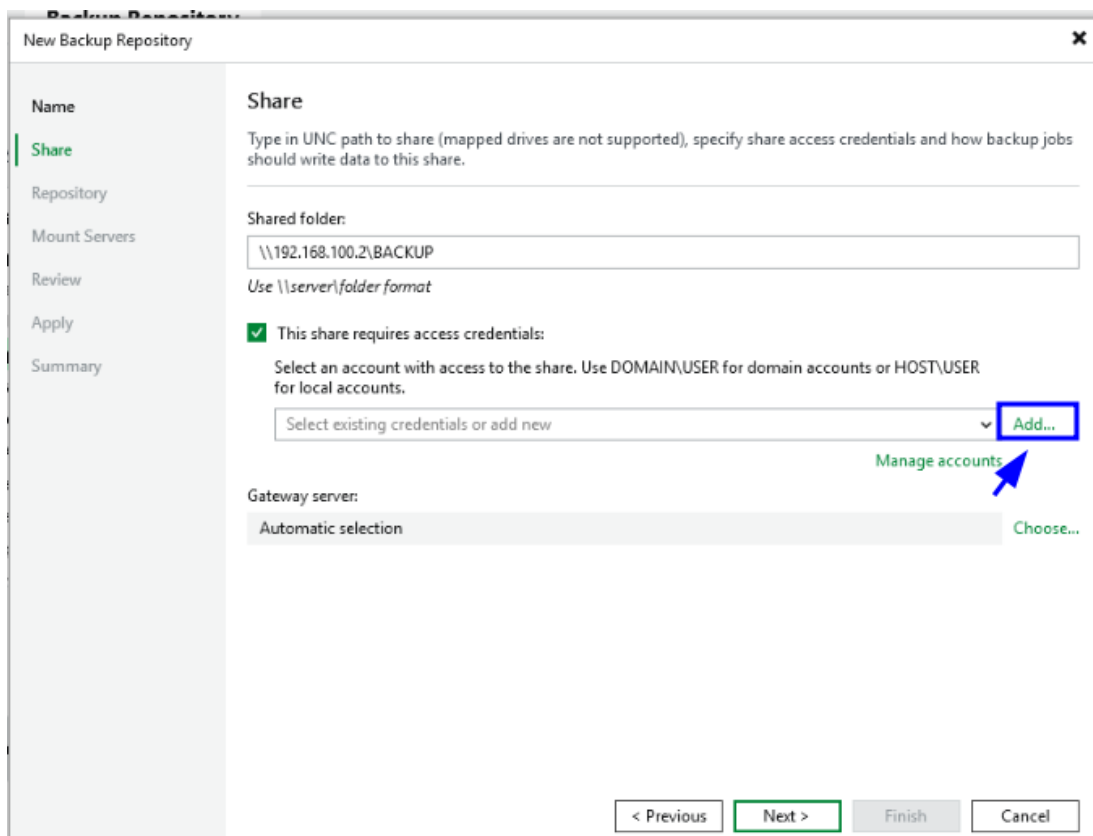
Puis, nous choisissons le protocole "SMB share" pour notre partage réseau.



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

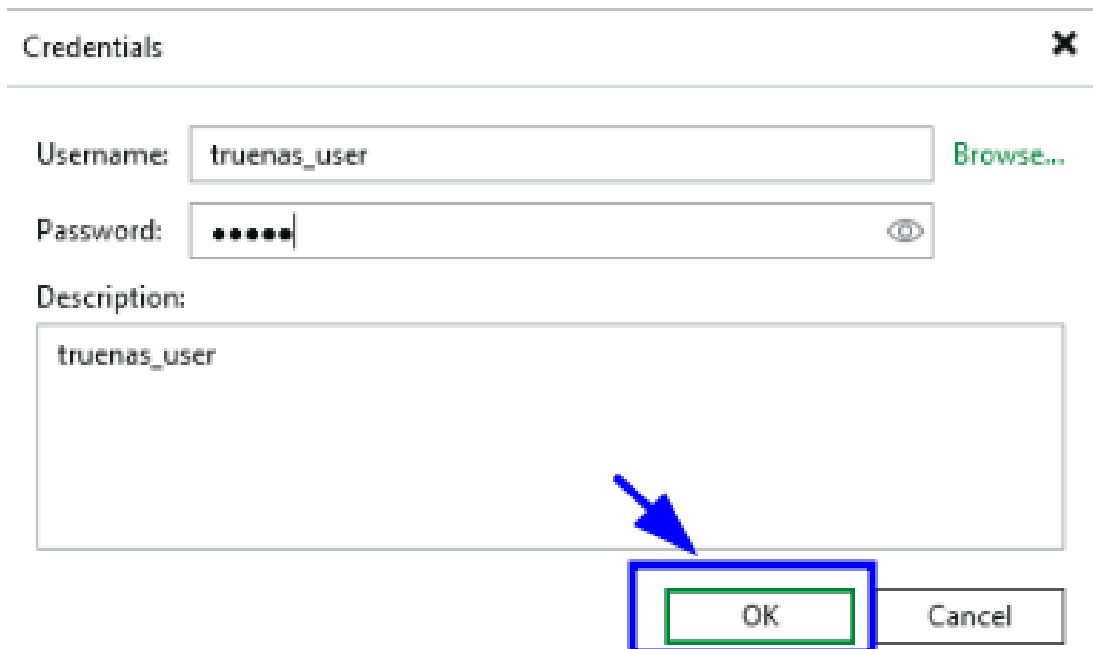


Il nous faut alors renseigner le chemin UNC du partage : `\\192.168.100.2\BACKUP`. Simultanément, nous cliquons sur "Add" afin d'ajouter les credentials de la machine.



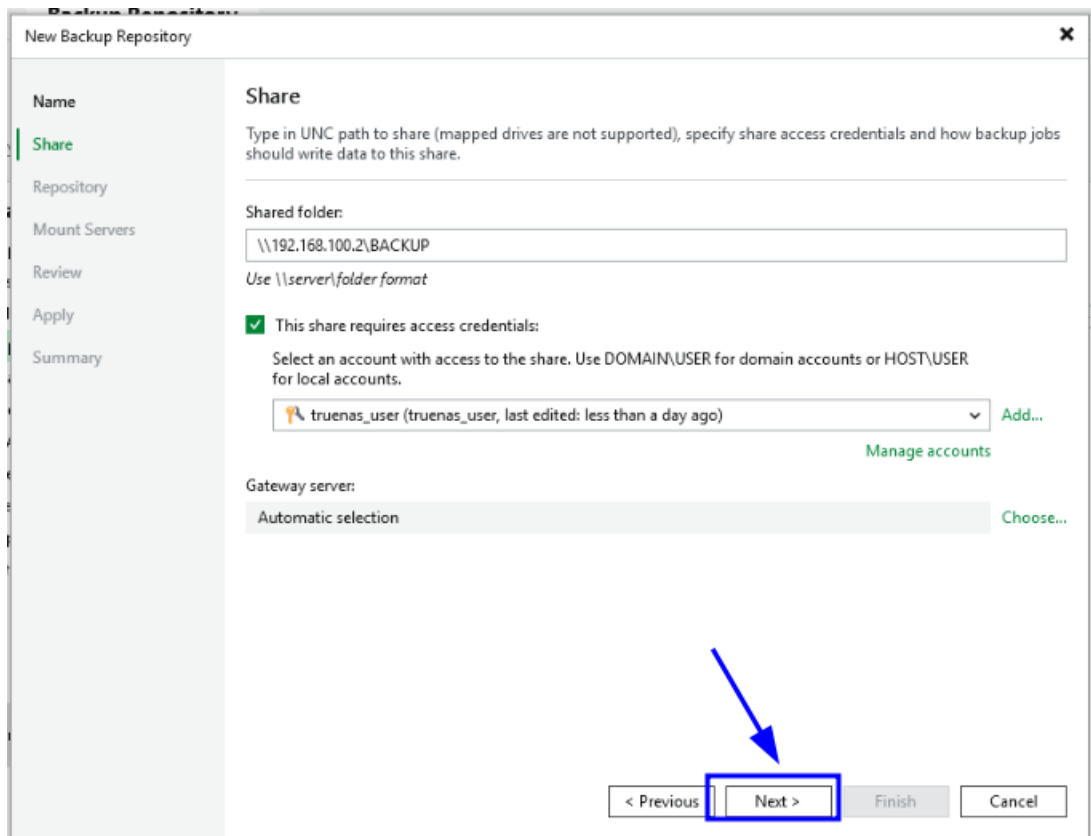
The screenshot shows the 'New Backup Repository' dialog box with the 'Share' tab selected. The 'Shared folder' field is filled with the UNC path `\\192.168.100.2\BACKUP`. Below this, the checkbox 'This share requires access credentials' is checked. A dropdown menu for selecting credentials is open, and the 'Add...' button is highlighted with a blue box. A blue arrow points to the 'Add...' button. The 'Next >' button at the bottom is highlighted with a green box.

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



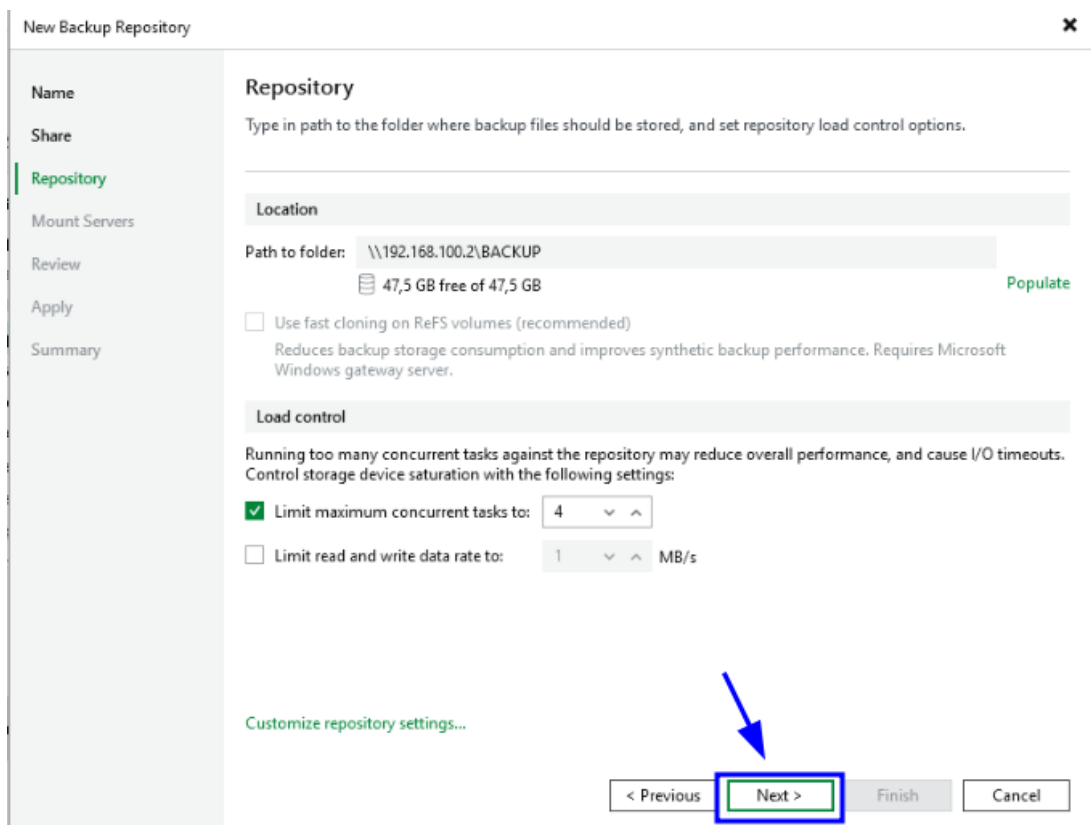
The screenshot shows the 'Credentials' dialog box. The 'Username' field contains the text 'truenas_user'. The 'Password' field contains masked characters (dots). The 'Description' field contains the text 'truenas_user'. The 'OK' button is highlighted with a blue box, and a blue arrow points to it.

Nous passons après cela à la suite.

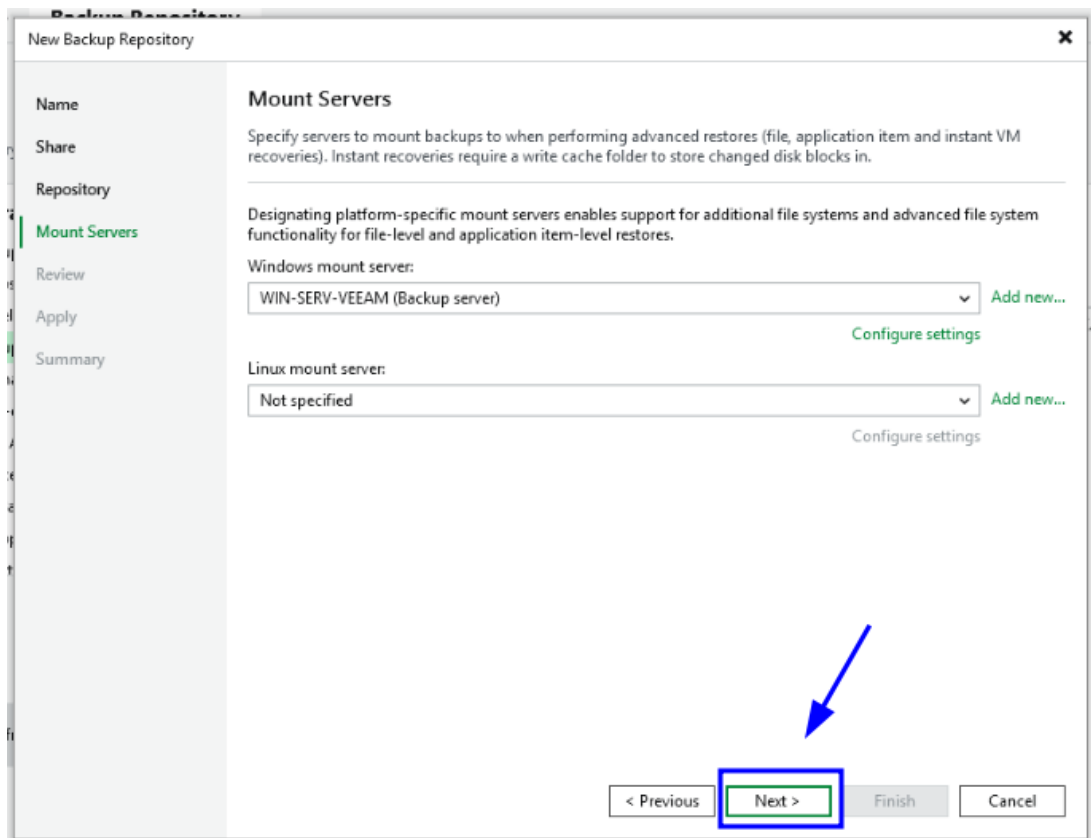


Après avoir validé les accès, nous cliquons sur "Populate" pour scanner l'espace disque disponible. Puis nous passons à la suite.

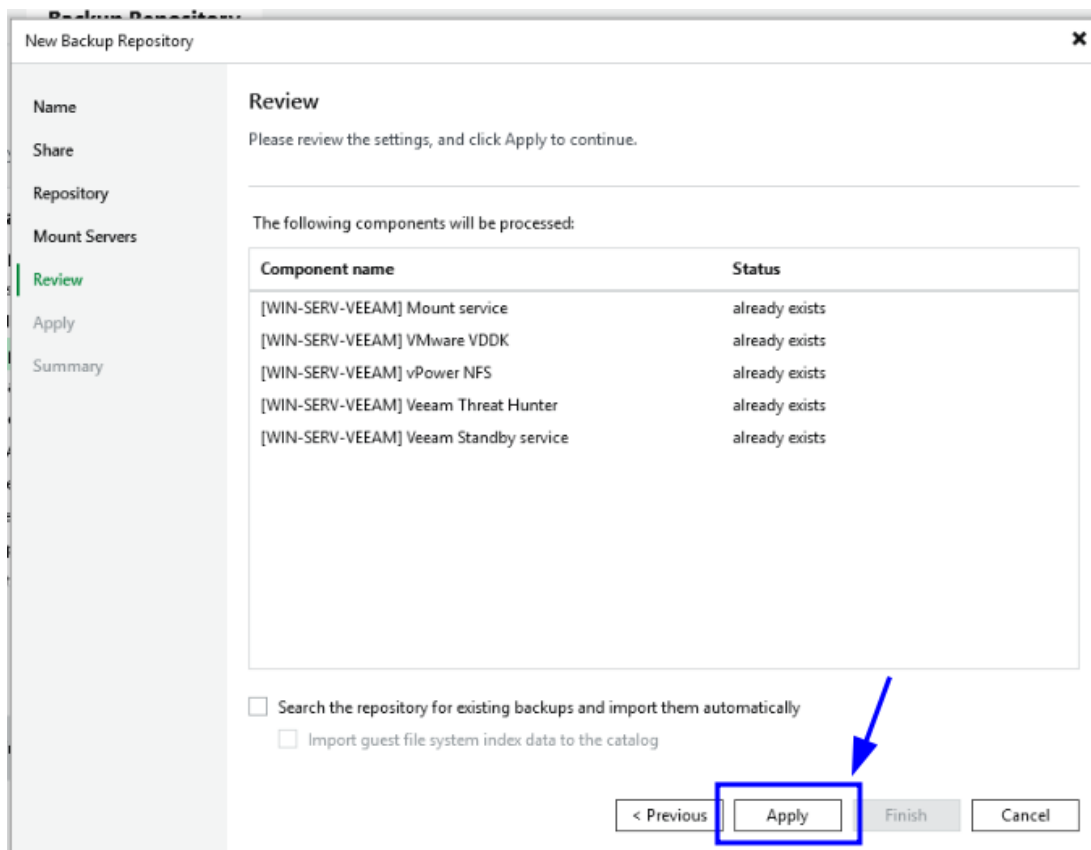
Par mesure de performance, nous limitons ici le nombre de tâches simultanées à 4.



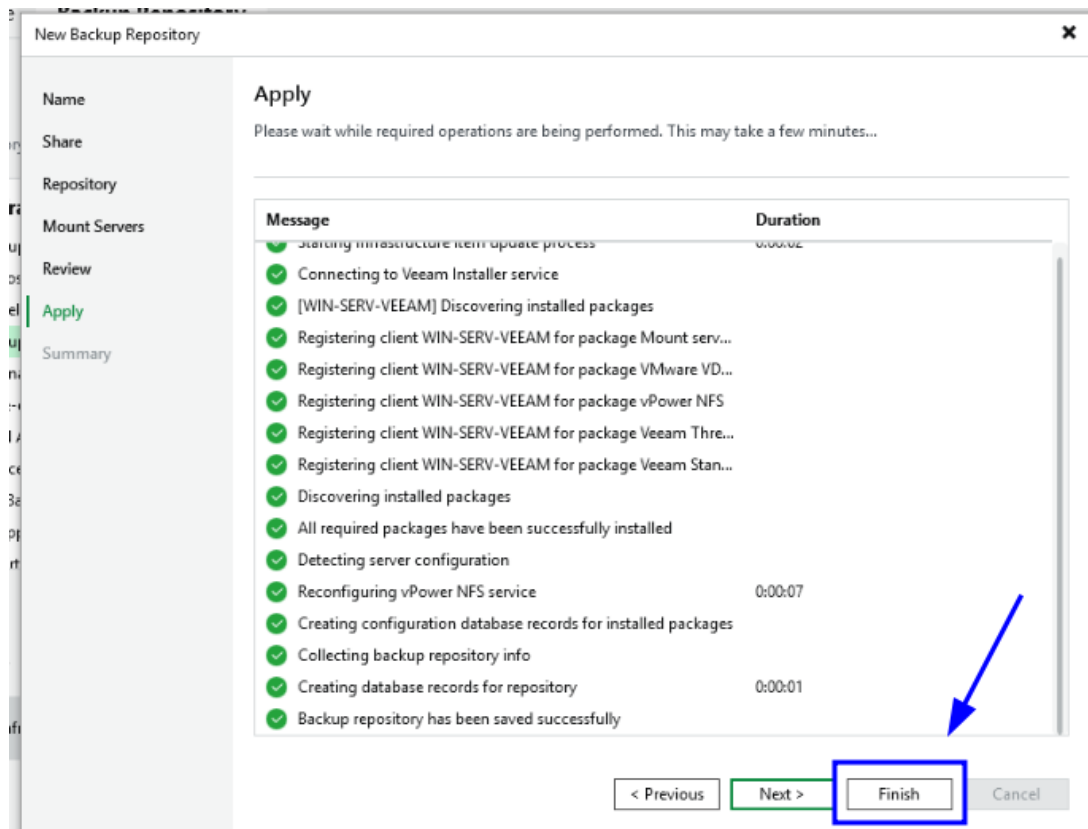
Nous confirmons ensuite que le serveur local sera utilisé comme point de montage (Mount Server).



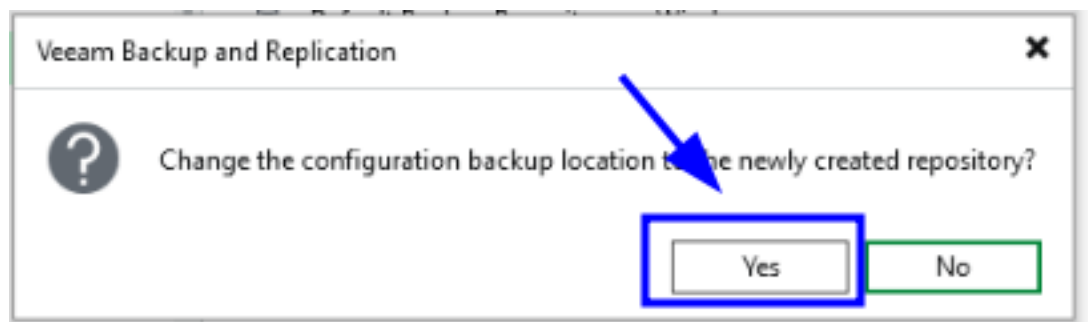
À ce stade, nous passons en revue la liste des composants logiciels qui vont être déployés ou qui sont déjà installé.



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



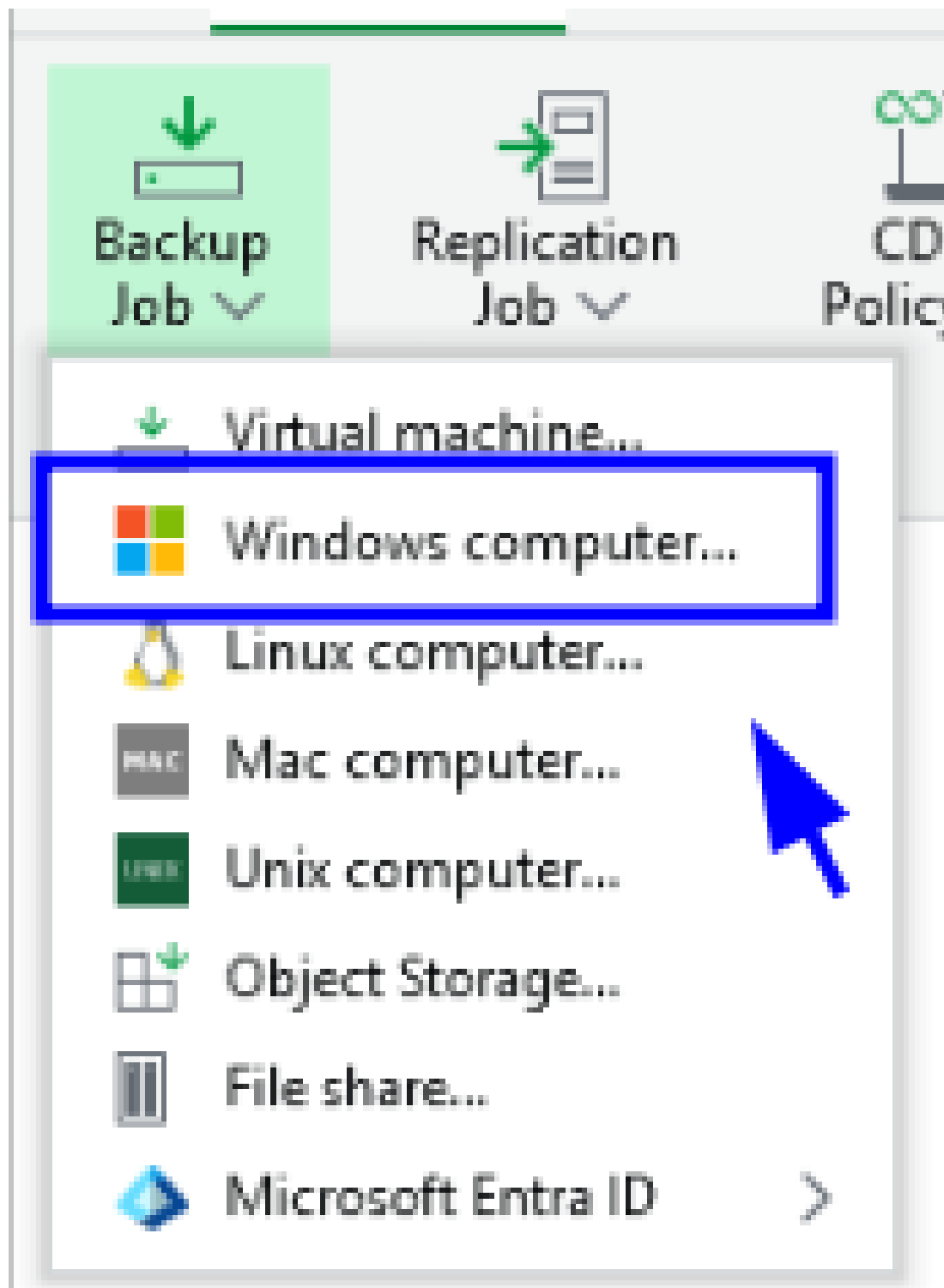
Une fenêtre nous demande alors de confirmer l'utilisation de ce dépôt pour les sauvegardes de configuration.



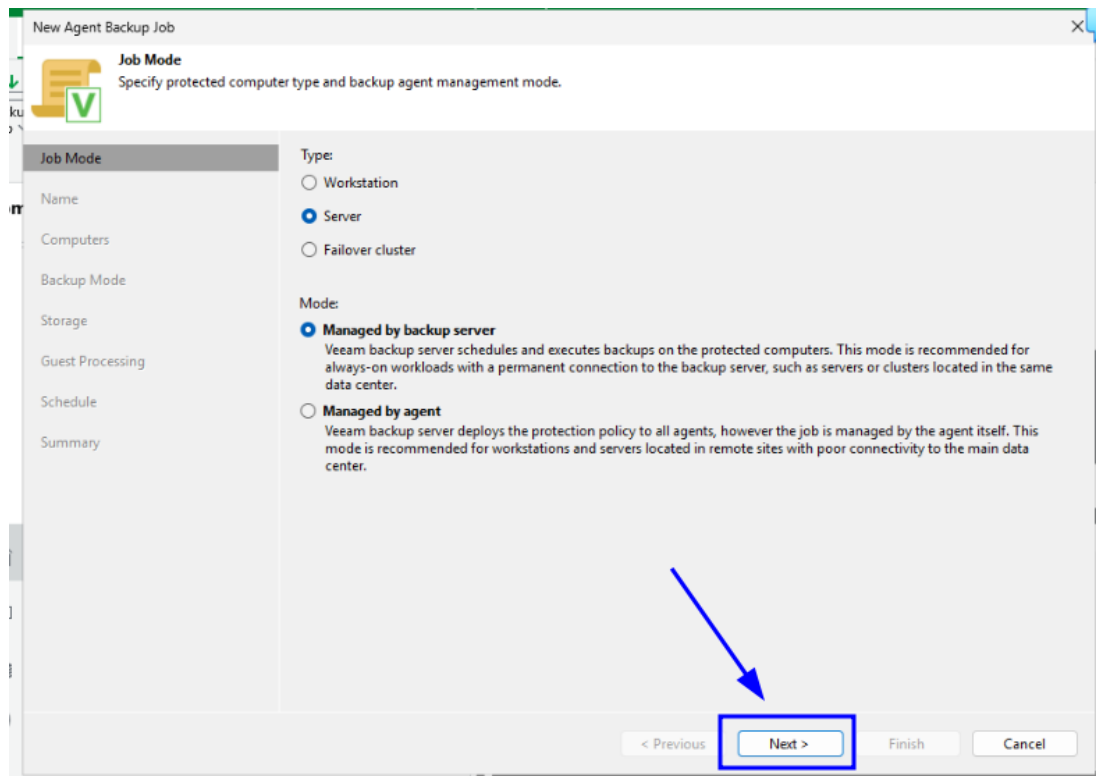
13 Création d'une tâche de sauvegarde (Job)

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

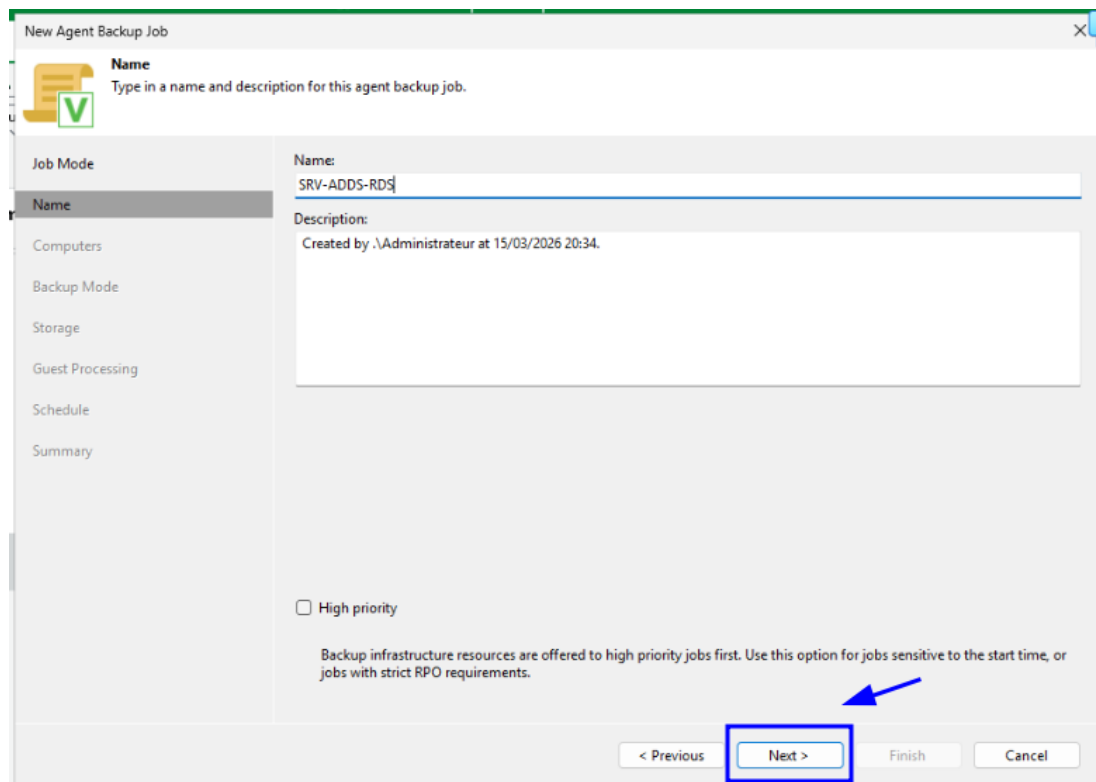
D'abord, nous ouvrons le menu "Backup Job" et sélectionnons "Windows computer".



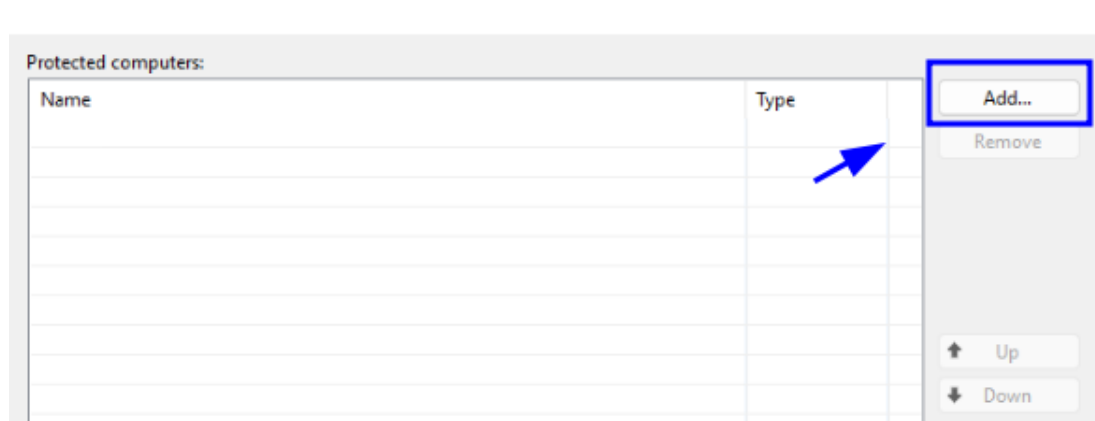
Nous définissons le type de job sur "Server" et le mode sur "Managed by backup server".



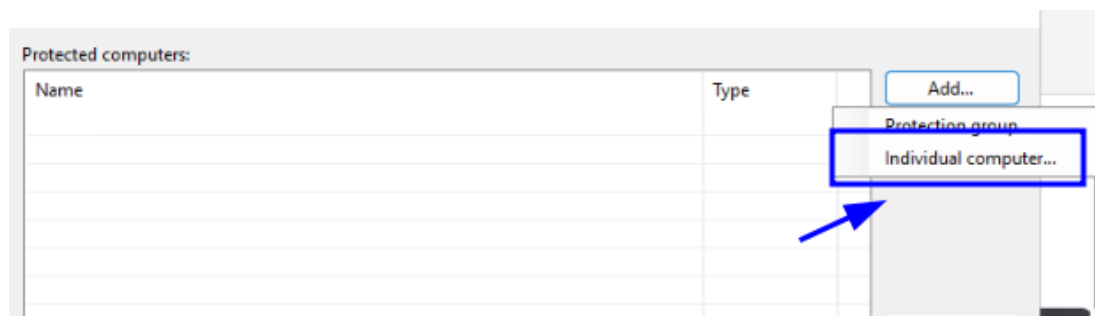
Ensuite, nous nommons cette nouvelle tâche "SRV-ADDS-RDS" afin de pouvoir la retrouver facilement.



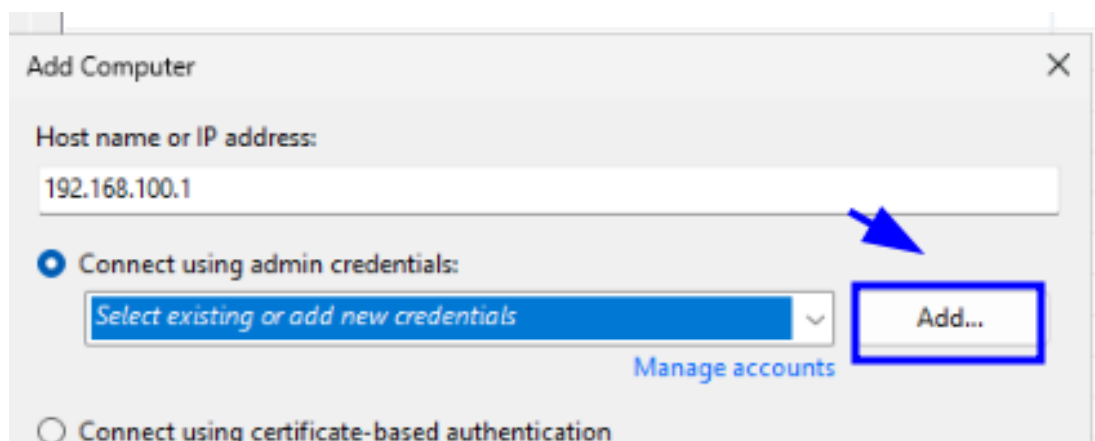
Nous allons ensuite ajouter le serveur que l'on souhaite sauvegarder, pour cela on commence en appuyant sur "Add".



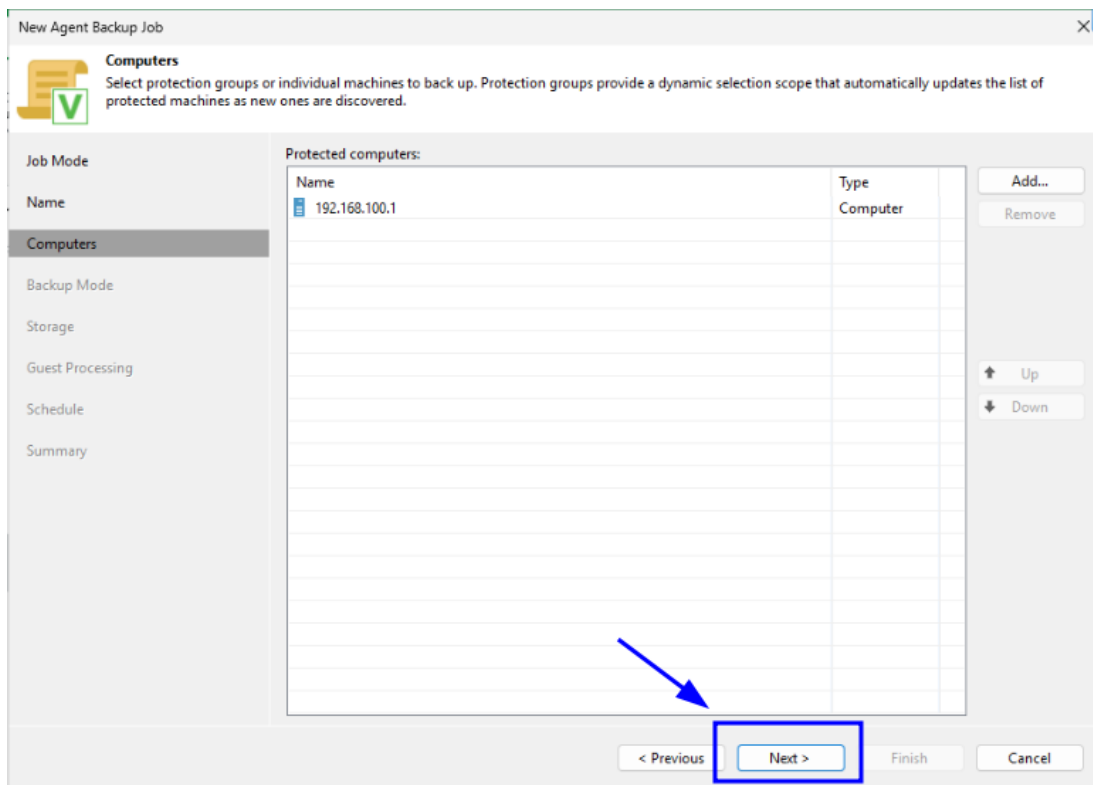
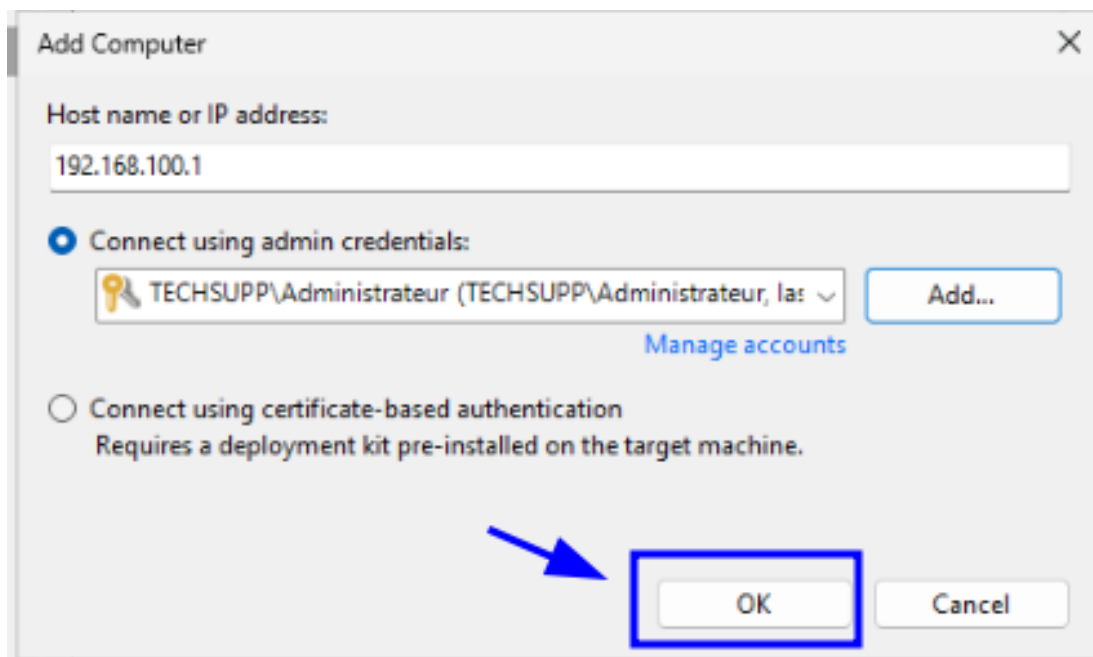
Puis nous allons spécifier que c'est un ordinateur seul que nous souhaitons sauvegarder.



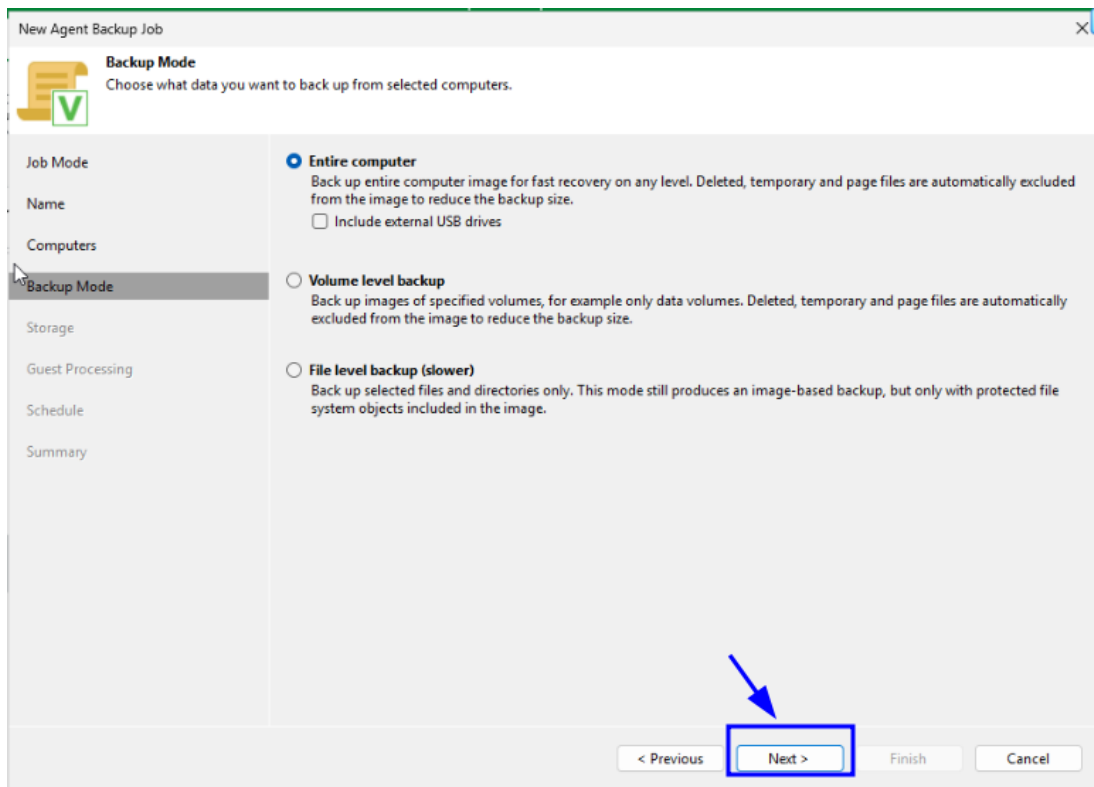
Il nous faut maintenant ajouter l'ordinateur cible en saisissant son adresse IP : 192.168.100.1, puis nous ajoutons les credentials de la machine à sauvegarder.



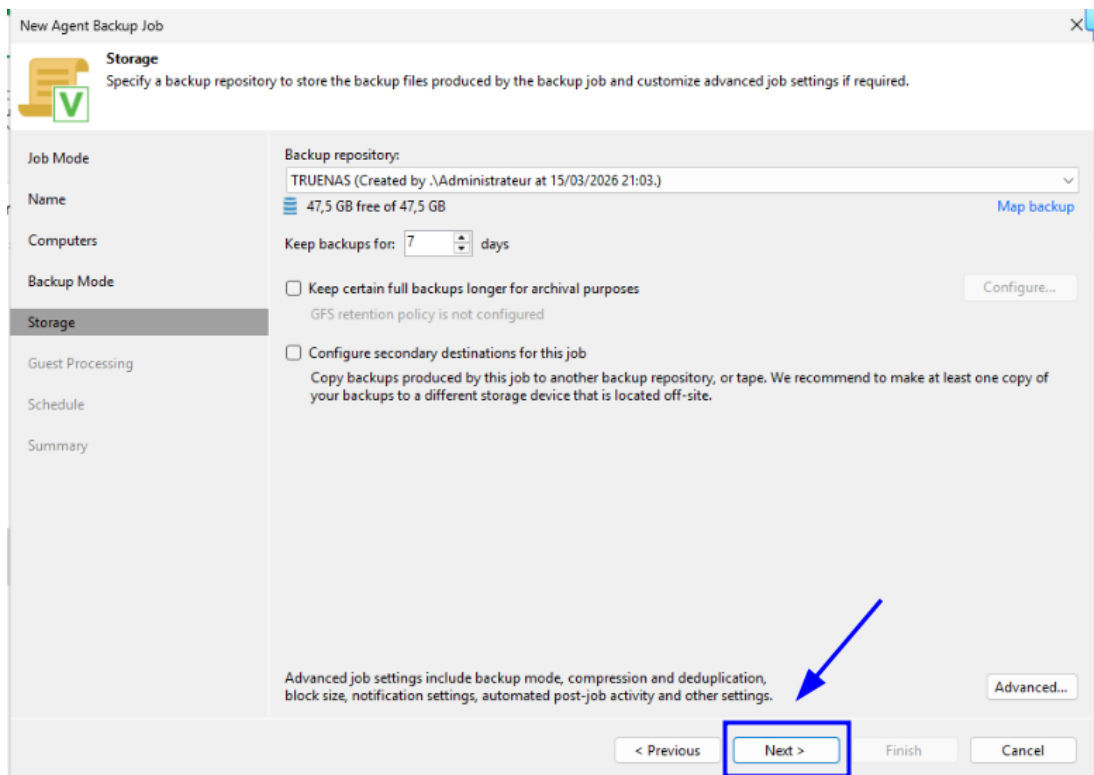
Après ceci effectué, nous passons à la suite.



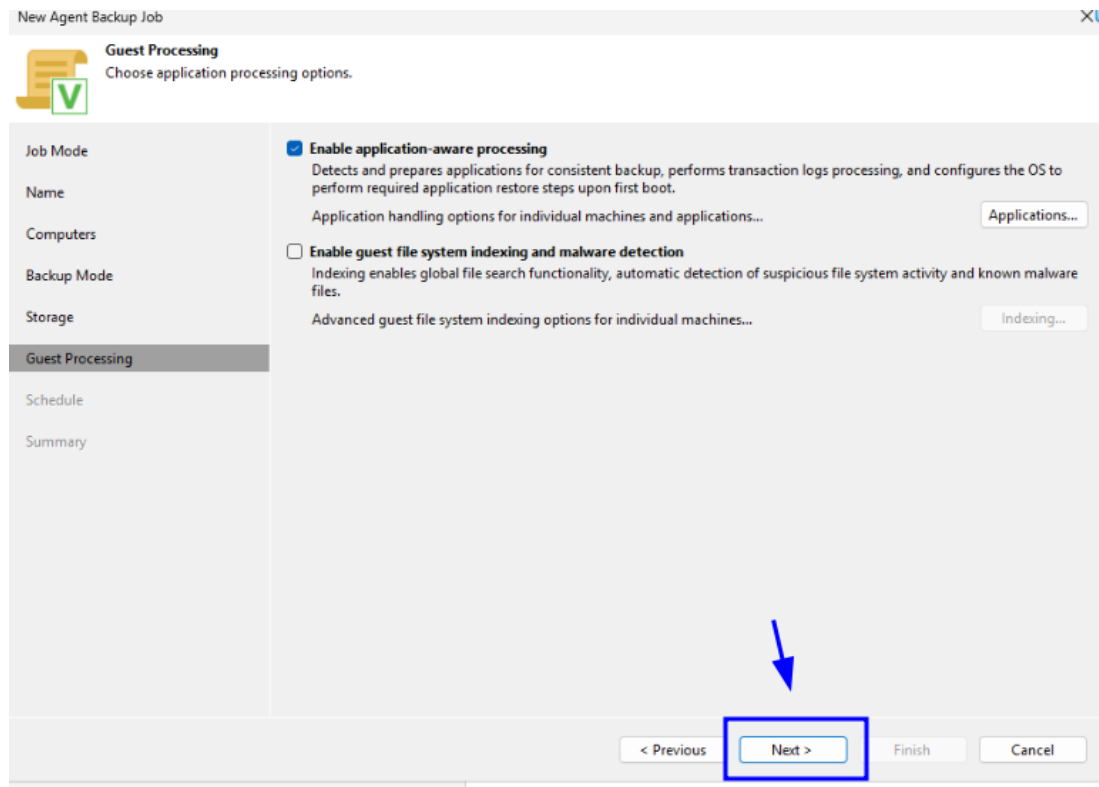
Nous optons alors pour le mode de sauvegarde "Entire computer" (image complète du système).



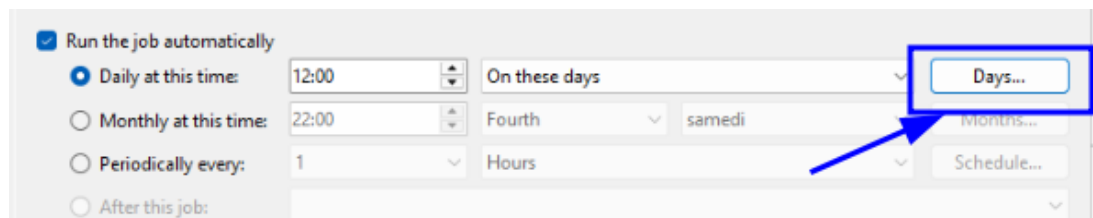
À cette étape, nous sélectionnons notre dépôt "TRUENAS" comme destination des fichiers.



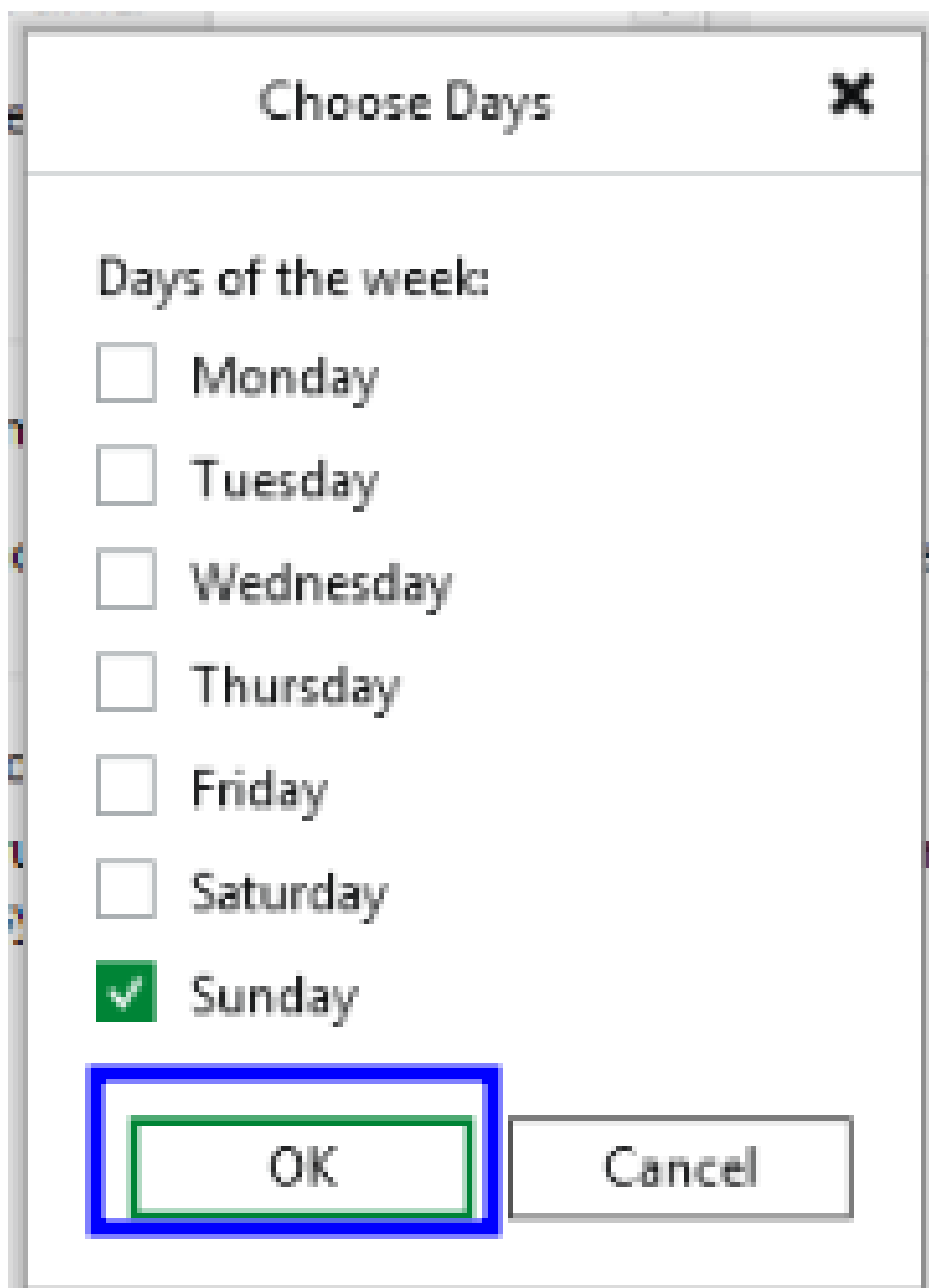
Nous activons l'application-aware processing afin que VEEAM puisse envoyer un signal avant les backup pour mettre en pause toutes les applications qui sont en cours et ne pas sauvegarder de données corrompues.



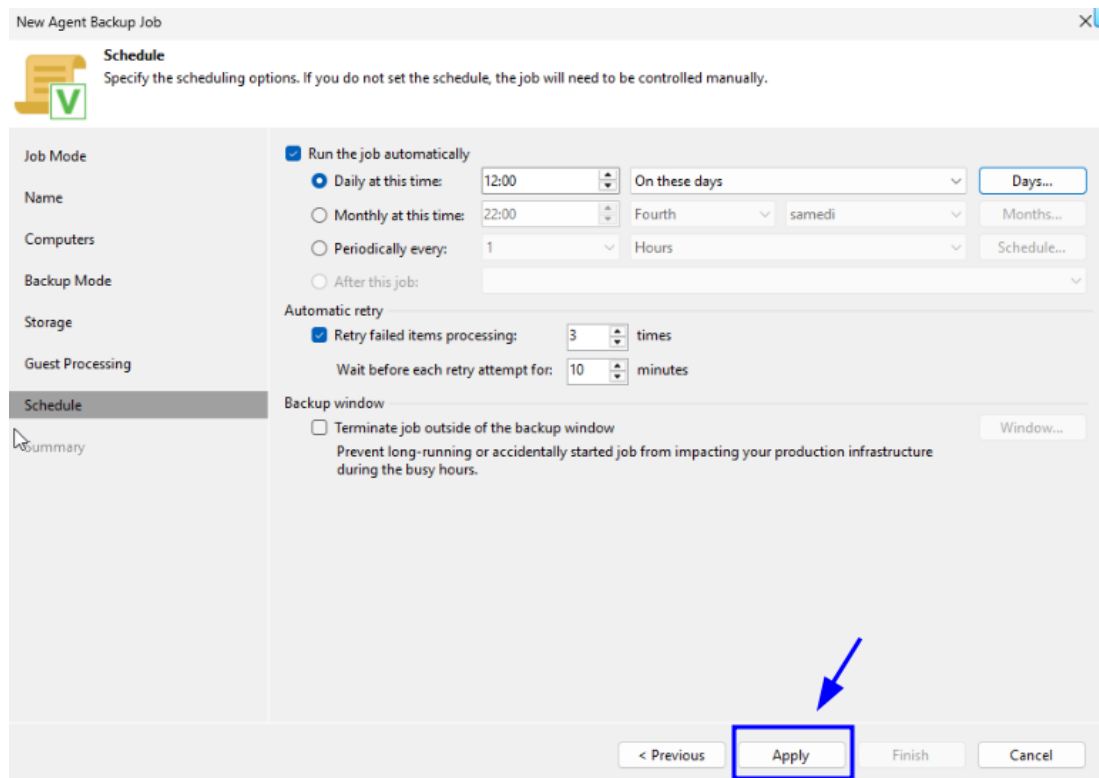
Nous allons définir une politique de sauvegarde basée sur certains jours dans la semaine pour cela nous allons sélectionner les jours sur lesquels les sauvegardes s'effectueront en appuyant sur le bouton "Days".



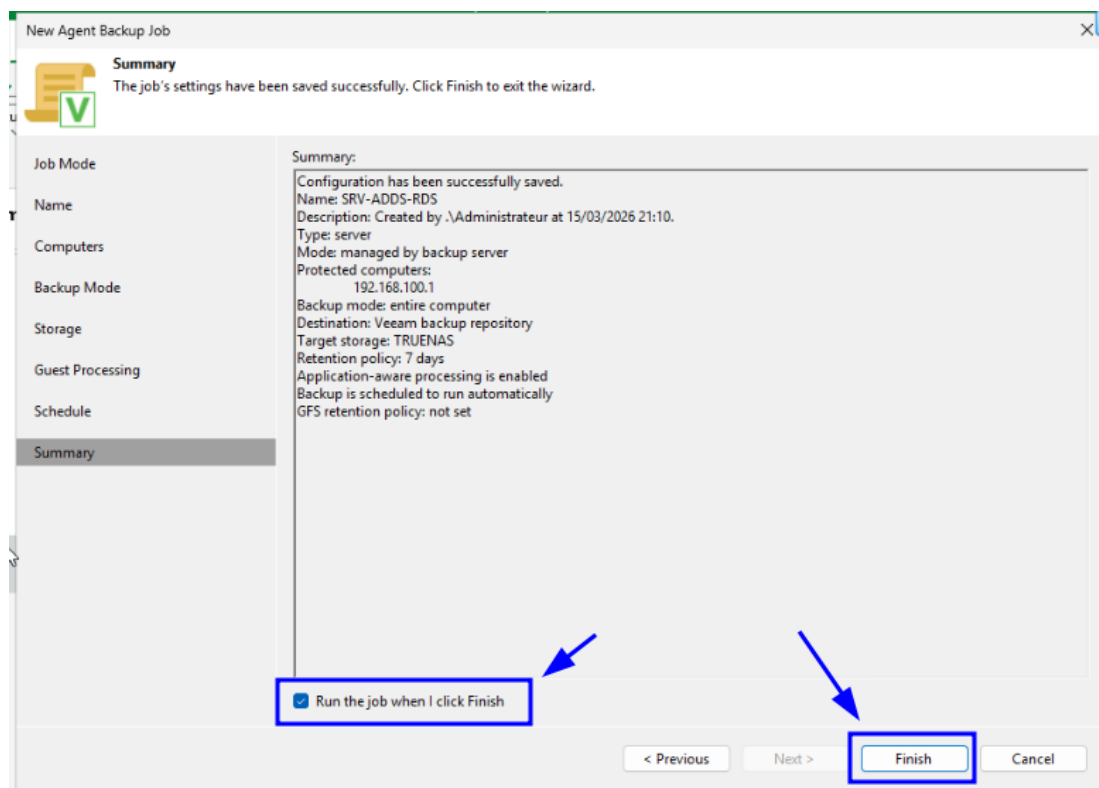
Nous cochons alors les jours de la semaine souhaités, dans notre cas ce sera le dimanche uniquement.



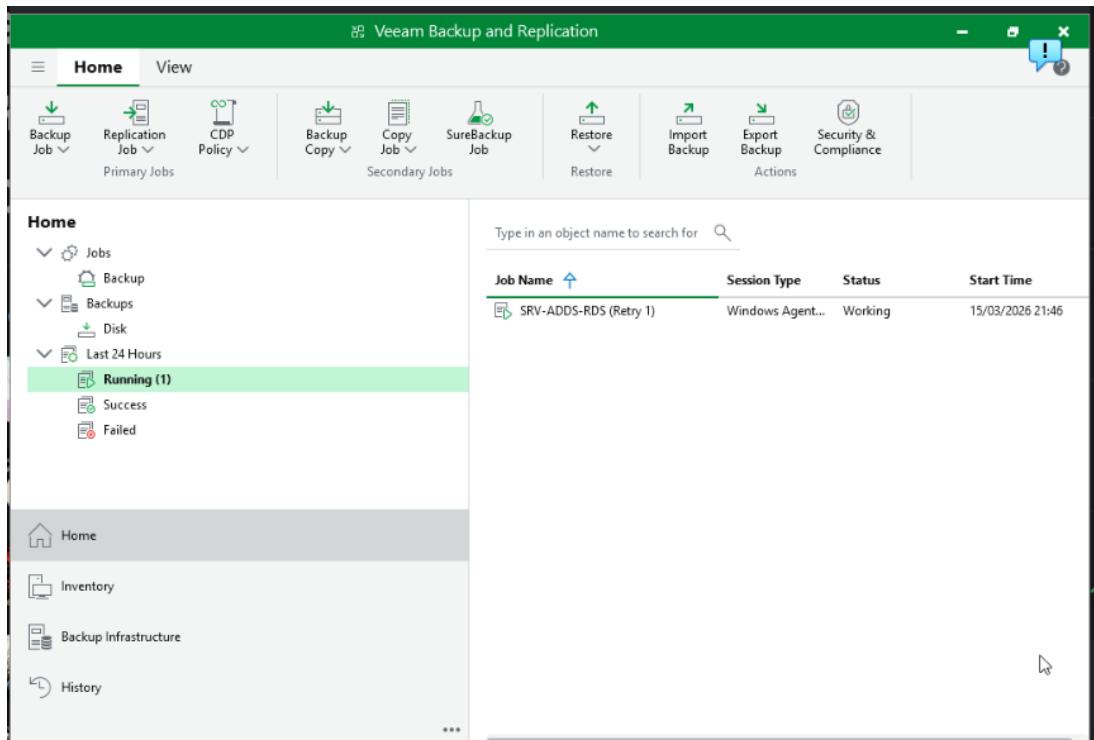
La sauvegarde s'effectuera donc tout les dimanche, à 12h. Après cela nous appliquons ces conditions.



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 terminée, 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.

Rescan of SRV-ADDS-RDS	Rescan	Success	15/03/2026 21:46
SRV-ADDS-RDS (Retry 1)	Windows Agent...	Success	15/03/2026 21:46

Quatrième partie

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

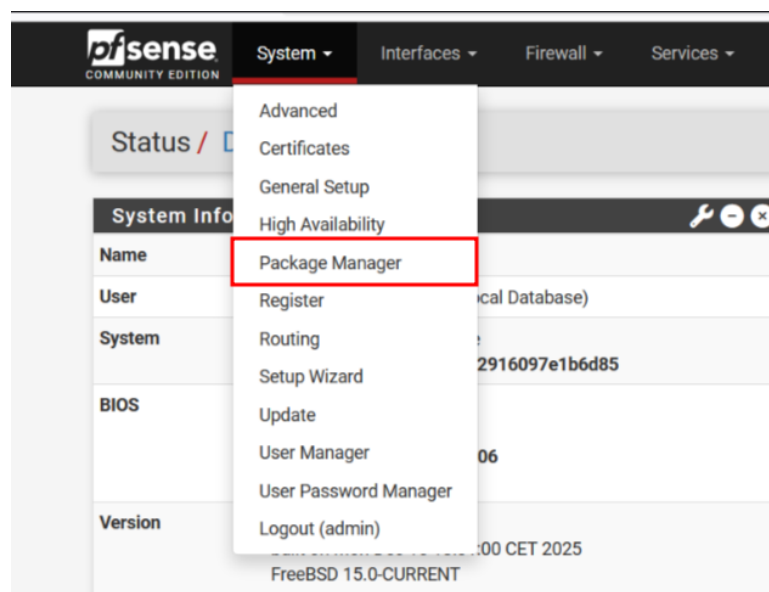
14 Introduction et Objectifs

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).

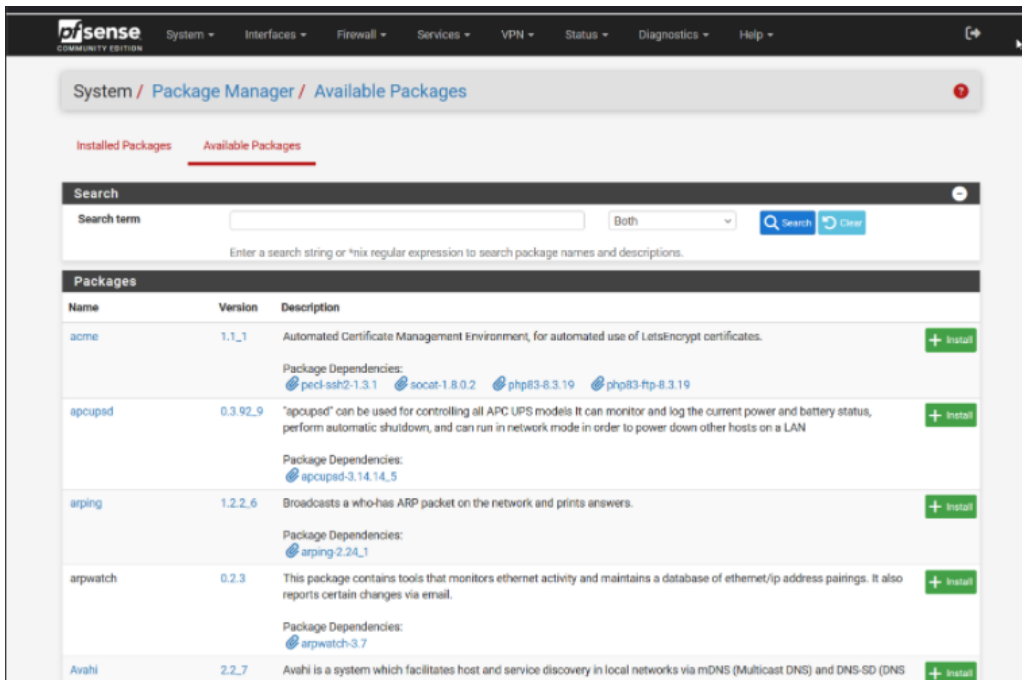
15 Installation du package Client Export

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.

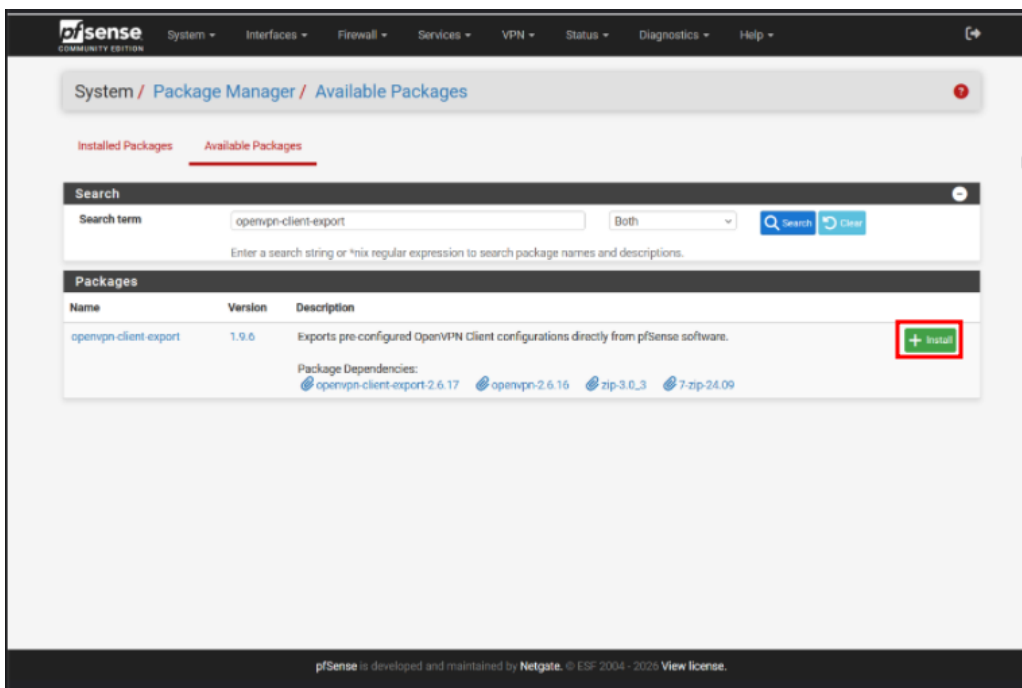
Nous accédons au menu System pour sélectionner le Package Manager, point d'entrée pour étendre les fonctionnalités du pare-feu.



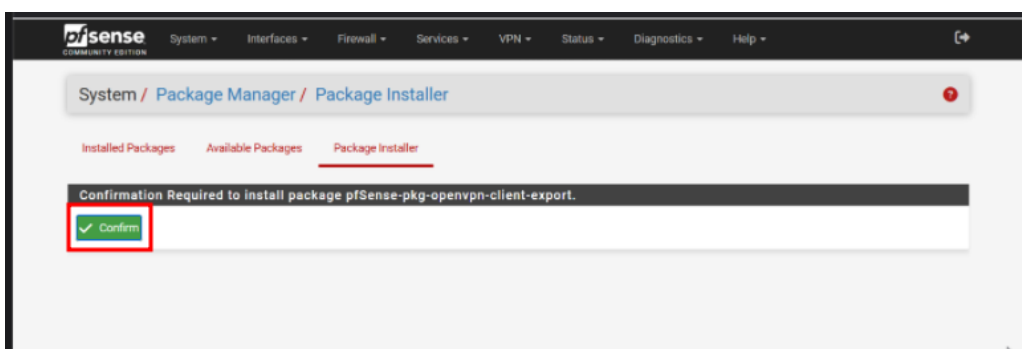
Nous visualisons ici le catalogue des dépôts officiels pfSense classés par ordre alphabétique.



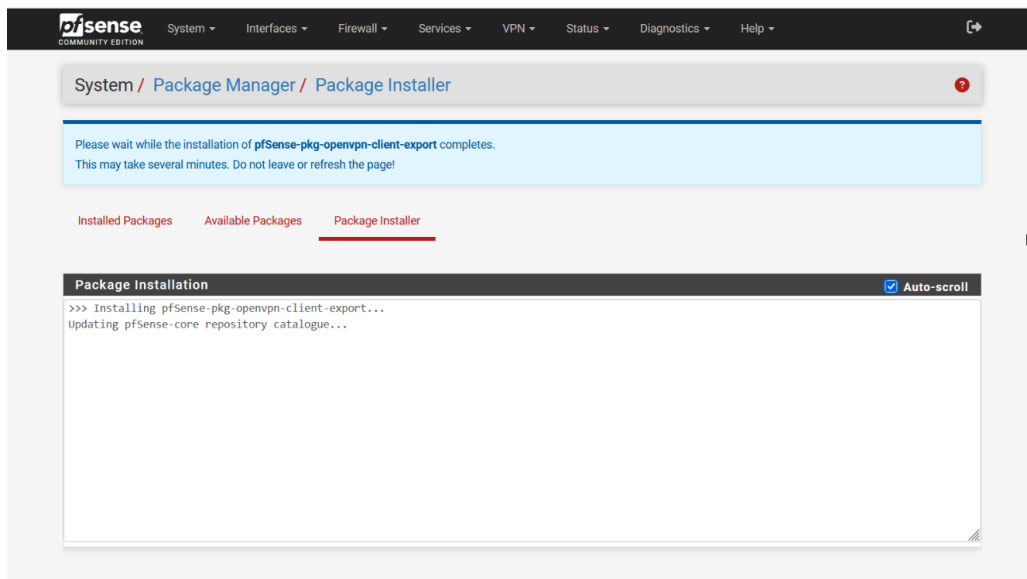
Nous isolons le paquet openvpn-client-export. Ce dernier est indispensable pour générer des profils compatibles avec les différents systèmes d'exploitation existant.



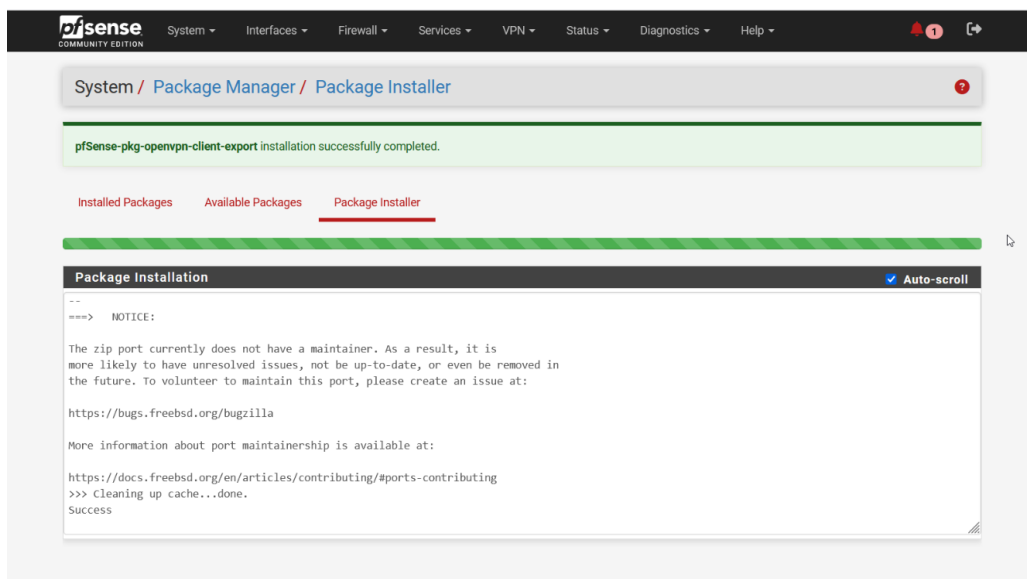
Nous confirmons l'installation. pfSense va alors récupérer les dépendances nécessaires sur les serveurs de Netgate.



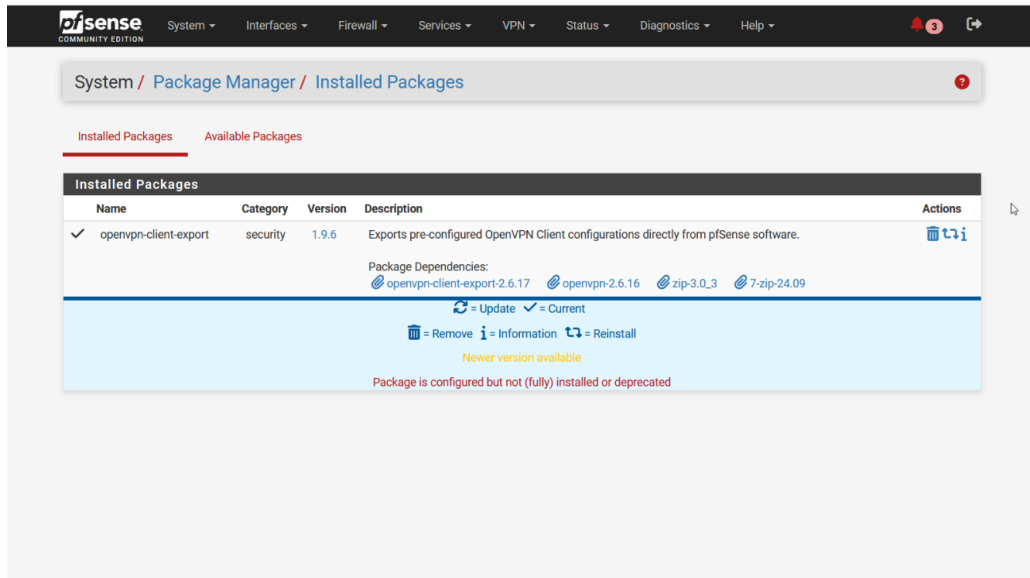
Le système procède à la mise à jour des catalogues et au téléchargement des binaires en temps réel.



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.



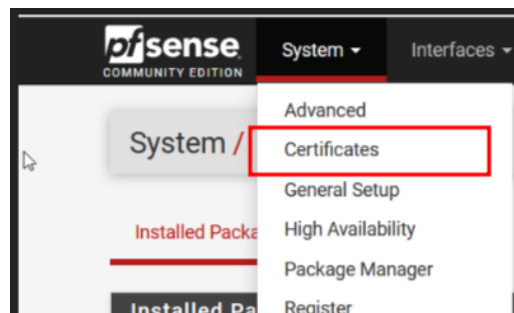
16 Infrastructure à Clés Publiques (PKI)

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

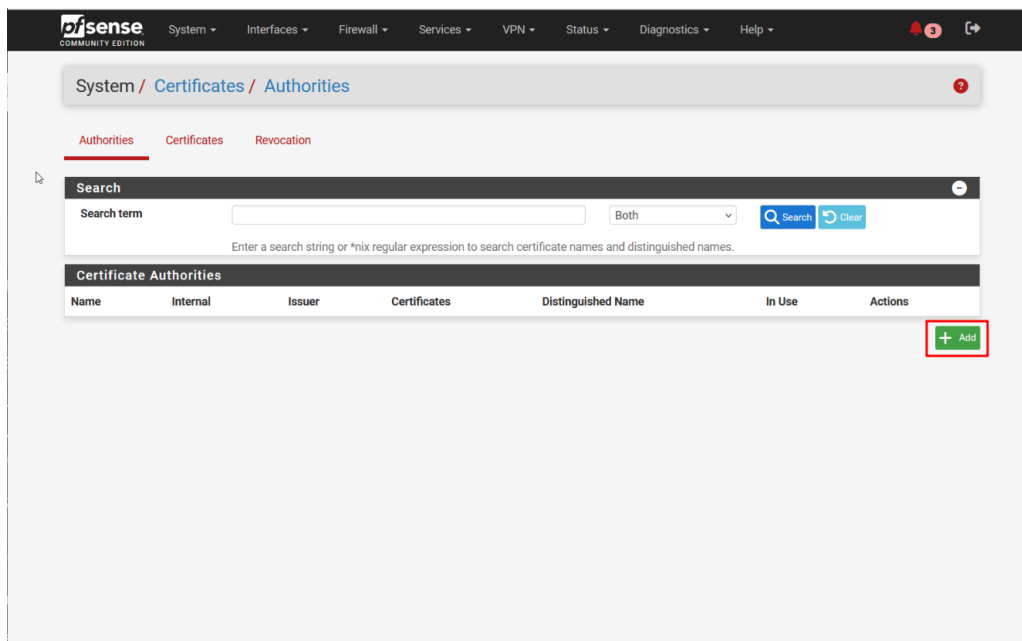
16.1 L'Autorité de Certification (CA)

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.

Create / Edit CA

Descriptive name
The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ' , "

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type
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
The digest method used when the CA is signed.
 The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days)

Common Name
The following certificate authority subject components are optional and may be left blank.

Country Code

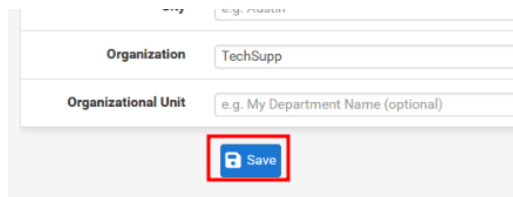
State or Province

City

Organization

Organizational Unit

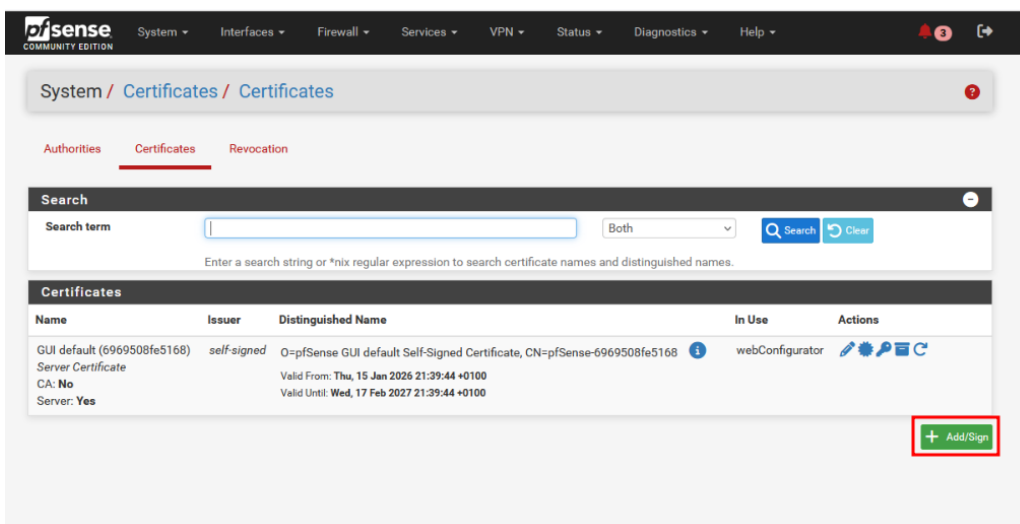
Nous validons l'enregistrement de la "VPN-CA" dans la base de données interne de pfSense.



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.

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name VPN-Server-Cert
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, '.

Internal Certificate

Certificate authority VPN-CA

Key type RSA
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 sha256
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) 3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name vpn.techsupp.local
The following certificate subject components are optional and may be left blank.

Country Code FR

State or Province e.g. Texas

City e.g. Austin

Organization TechSupp

Organizational Unit e.g. My Department Name (optional)

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

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

Enter additional identifiers for the certificate in this list: signing CA may ignore or change these values.

Add SAN Row + Add SAN Row

→ Save

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

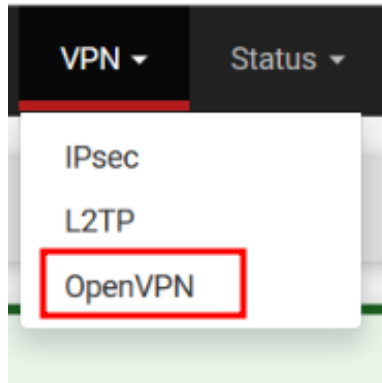
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

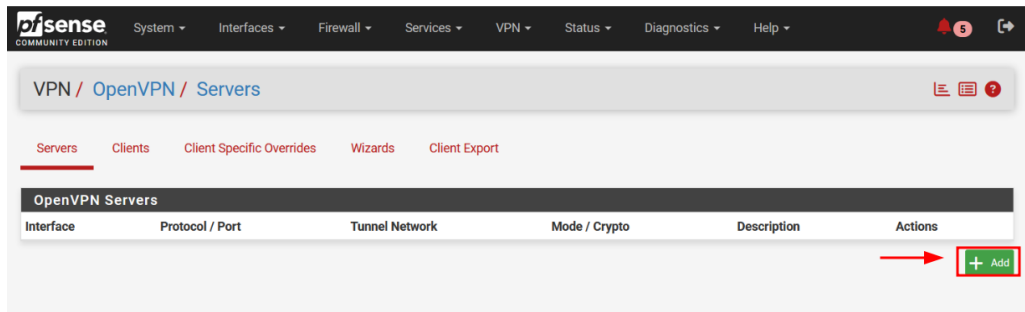
Name	Issuer	Distinguished Name	In Use	Actions
GUI default (6969508fe5168) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6969508fe5168 Valid From: Thu, 15 Jan 2026 21:39:44 +0100 Valid Until: Wed, 17 Feb 2027 21:39:44 +0100	webConfigurator	   
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		   

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.

General Information	
Description	VPN SERVER A description of this VPN for administrative reference.
Disabled	<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.

Mode Configuration	
Server mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	Local Database
Device mode	tun - Layer 3 Tunnel Mode "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2).

Endpoint Configuration	
Protocol	UDP on IPv4 only
Interface	WAN The interface or Virtual IP address where OpenVPN will receive client connections.
Local port	1194 The port used by OpenVPN to receive client connections.

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

Cryptographic Settings

TLS Configuration Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

Peer Certificate Authority VPN-CA

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check Check client certificates with OCSP

Server certificate VPN-Server-Cert (Server: Yes, CA: VPN-CA)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length 2048 bit
Diffie-Hellman (DH) parameter set used for key exchange. ⓘ

ECDH Curve Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Algorithms

AES-192-CBC (192 bit key, 128 bit block)	AES-256-CBC (256 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)	
AES-192-CFB1 (192 bit key, 128 bit block)	
AES-192-CFB8 (192 bit key, 128 bit block)	
AES-192-GCM (192 bit key, 128 bit block)	
AES-192-OFB (192 bit key, 128 bit block)	
AES-256-CBC (256 bit key, 128 bit block)	
AES-256-CFB (256 bit key, 128 bit block)	
AES-256-CFB1 (256 bit key, 128 bit block)	
AES-256-CFB8 (256 bit key, 128 bit block)	

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. ⓘ

Fallback Data Encryption Algorithm AES-256-CBC (256 bit key, 128 bit block)
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm SHA256 (256-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Certificate Depth One (Client+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Strict User-CN Matching Enforce match
When authenticating users, enforce a match between the common name of the client certificate and the username given at login.

Client Certificate Key Usage Validation Enforce key usage
Verify that only hosts with a client certificate can connect (EKU: 'TLS Web Client Authentication').

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

Tunnel Settings

IPv4 Tunnel Network

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. 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.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. 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.

Concurrent connections

Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression

Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Asymmetric compression allows an easier transition when connecting with older peers.

Push Compression Push the selected Compression setting to connecting clients.

Type-of-Service Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication Allow communication between clients connected to this server

Duplicate Connection Allow multiple concurrent connections from the same user

When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Client Settings

Dynamic IP Allow connected clients to retain their connections if their IP address changes.

Topology

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".

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

pfsense COMMUNITY EDITION
 System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

VPN / OpenVPN / Servers

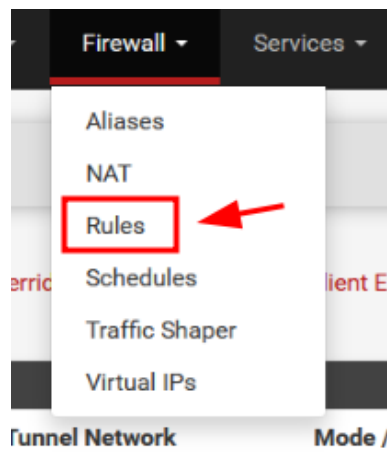
Servers
Clients
Client Specific Overrides
Wizards
Client Export

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.8.0.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN SERVER	✎ 📄 🗑️

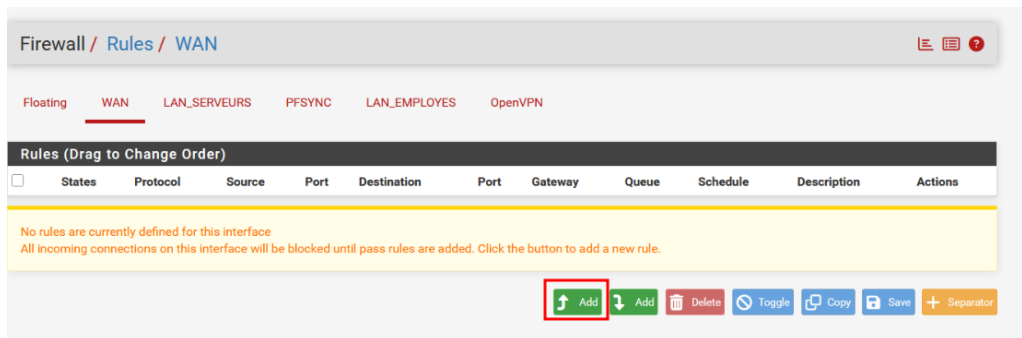
+ Add

18 Politique de Filtrage (Firewall)

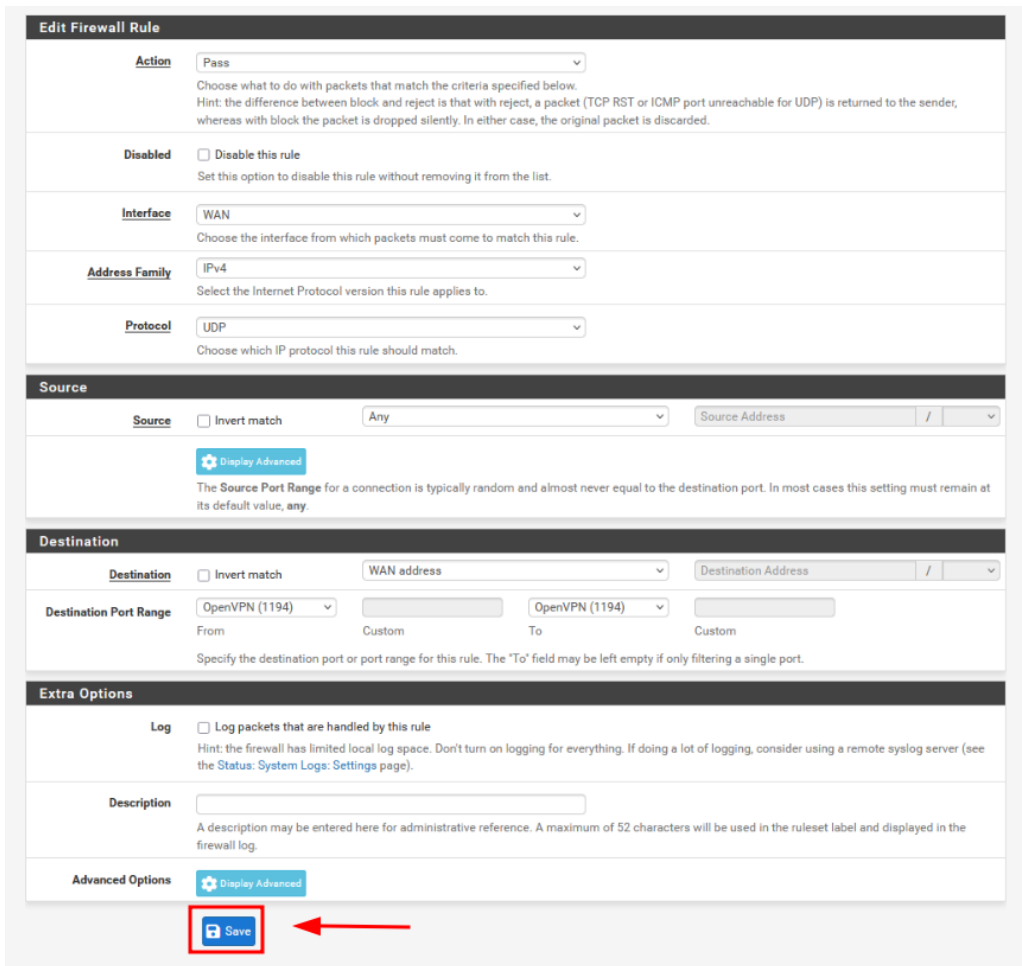
Nous nous rendons dans les règles du Firewall pour modifier la politique de sécurité du WAN.



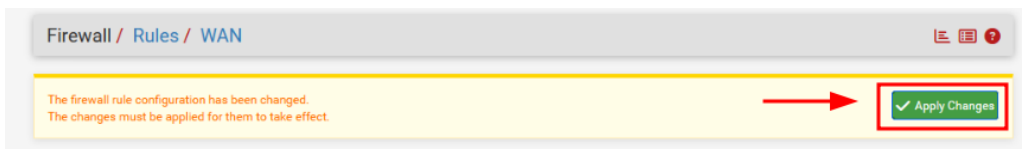
Nous cliquons sur "Add" pour insérer une nouvelle règle de passage.



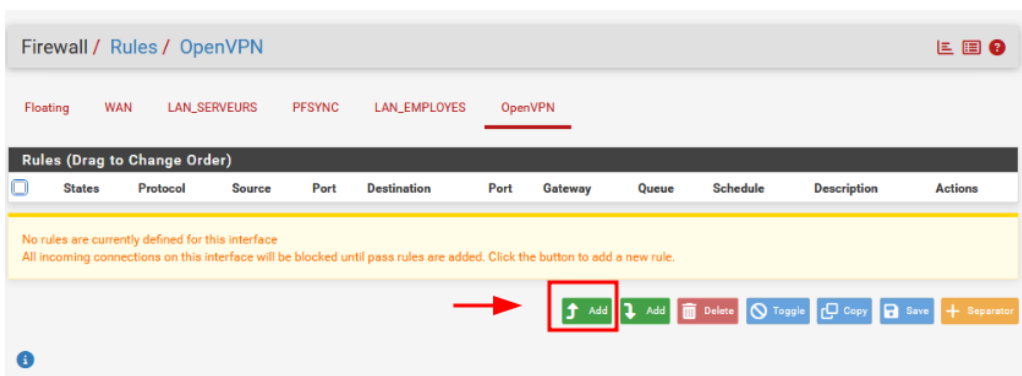
Nous autorisons le flux UDP vers le port 1194. Cette règle permet au pare-feu d'accepter les connexions VPN initiales.



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.

Edit Firewall Rule

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

Address Family
 Select the Internet Protocol version this rule applies to.

Protocol
 Choose which IP protocol this rule should match.

Source

Source Invert match /

Destination

Destination Invert match /

Extra Options

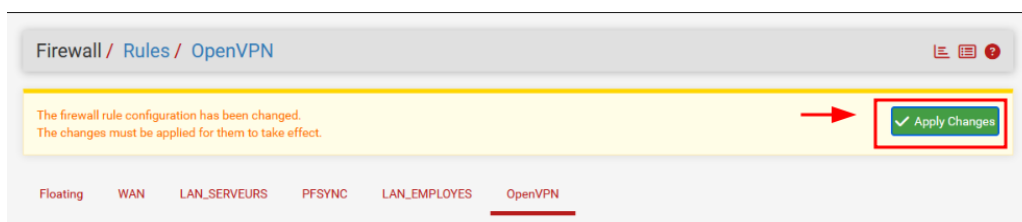
Log Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

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

Advanced Options

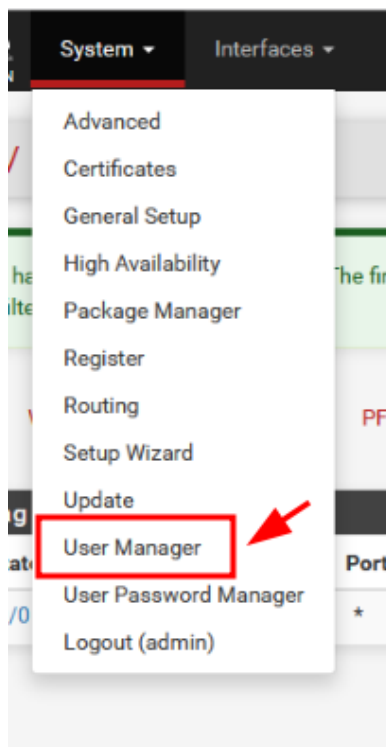
←

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

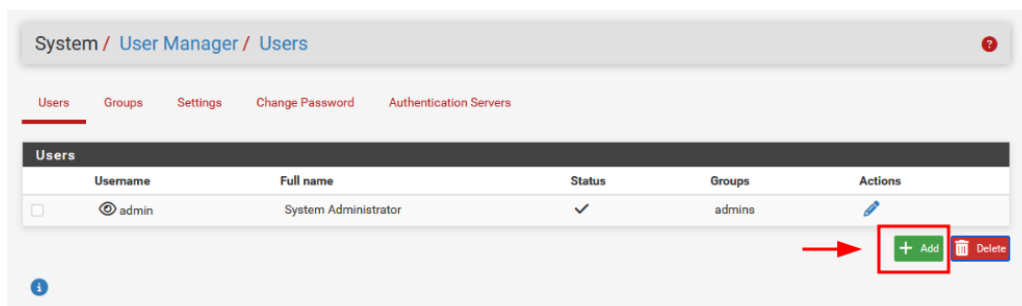


19 Provisionnement des Utilisateurs

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.

User Properties

Defined by: USER

Disabled: This user cannot login

Username: vpnuser

Password: [masked] [masked]
Enter a new password. Type the new password again for confirmation.

Hints:
Current NIST guidelines prioritize password length over complexity.
The password cannot be identical to the username.

Full name: VPN USER 1
User's full name, for administrative information only

Expiration date: [empty]
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings: Use individual customized GUI options and dashboard layout for this user.

Group membership: admins [empty]
Not member of: [empty] Member of: [empty]
[>> Move to "Member of" list] [<< Move to "Not member of" list]

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

Certificate: Click to create a user certificate

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

Create Certificate for User

Descriptive name: vpnuser-cert

Certificate authority: VPN-CA

Key type: RSA

Key length: 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: 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: 3650

Nous enregistrons la fiche utilisateur complète.

Shell Behavior

Keep Command History Keep shell command history between login sessions. If this user has shell access, this option preserves access history using the up and down arrows at the top or bottom arrows.

[Save]

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

System / User Manager / Users

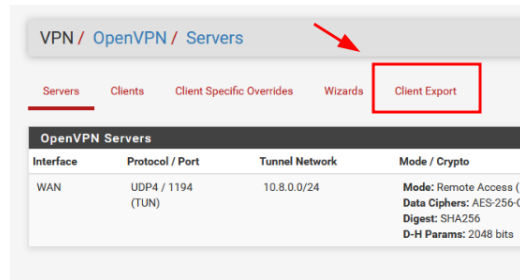
Users Groups Settings Change Password Authentication Servers

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	[edit]
<input checked="" type="checkbox"/>	vpnuser	VPN USER 1	✓		[edit] [delete]

[+ Add] [Delete]

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.

OpenVPN Server

Remote Access Server: VPN SERVER UDP4:1194

Client Connection Behavior

Host Name Resolution: Interface IP Address

Verify Server CN: Automatic - Use verify-x509-name where possible

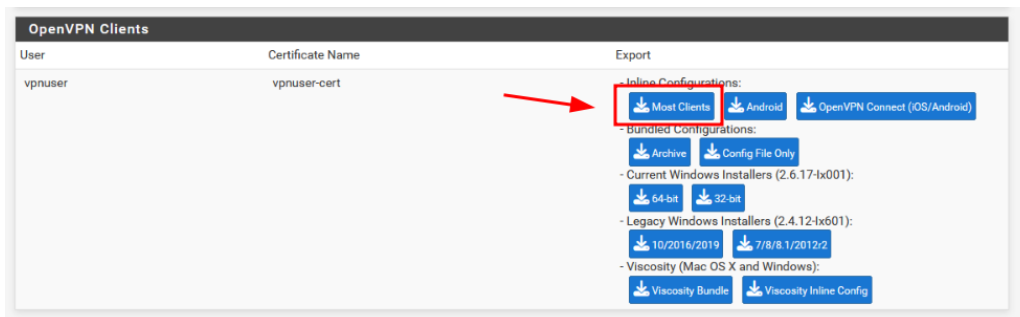
Block Outside DNS: Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.

Legacy Client: Do not include OpenVPN 2.5 and later settings in the client configuration.

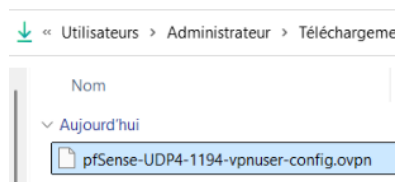
Silent Installer: Create Windows installer for unattended deploy.

Bind Mode: Do not bind to the local port

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.