

Installation / Configuration

- [Routeurs / VPN](#)
 - [Documentation de la Configuration VPN IPsec Site-to-Site](#)
 - [Création des règles du pare-feu](#)
- [Windows Server Site A](#)
 - [Installation de Windows Server 2022 sur DC1 en mode GUI](#)
 - [Installation de Windows Server 2022 sur DC2 en mode CORE](#)
 - [Configuration - Création du domaine AD, configuration initiale du domaine.](#)
 - [Configuration - Jonction au domaine AD, mise en place des roles DC2](#)
- [Windows Server Site B](#)
 - [Installation de Windows Server 2022 sur DC1 en mode GUI](#)
 - [Installation de Windows Server 2022 sur DC2 en mode CORE](#)
 - [Configuration - Jonction au domaine AD, mise en place des roles DC1](#)
 - [Configuration - Jonction au domaine AD, mise en place des roles DC2](#)
- [DFS](#)
 - [Preparation des disques et partages](#)
 - [Configuration de DFS](#)
 - [Configuration de la replication DFS](#)
- [SAN](#)
 - [Installation de TrueNAS](#)
 - [Configuration de TrueNAS via l'interface Web](#)
- [BACKUP](#)
 - [Configuration de Windows BackUp](#)
 - [Configuration de Shadow Copy](#)
- [GPO et parametres pour clients](#)
 - [Mise en place des disques réseau utilisateurs](#)
 - [Création des GPO de restrictions](#)

- [Personnalisation des postes clients](#)
- [Dépannage](#)
 - [Dépannage](#)

Routeurs / VPN

Documentation de la Configuration VPN IPsec Site-to-Site

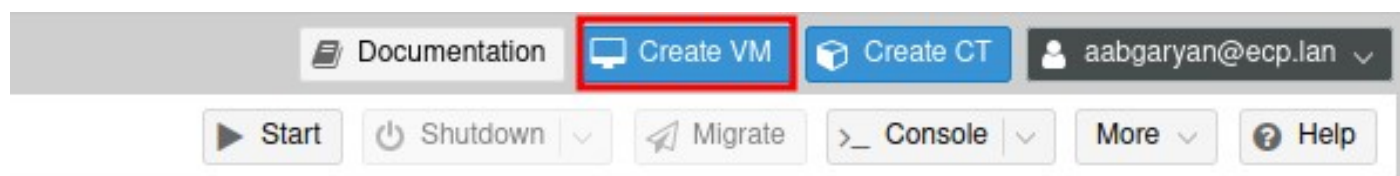
1. Création des Machines Virtuelles et installation

Objectif : Créer le Firewall A (FW-SA), le Firewall B (FW-SB), et les clients Windows correspondants (W11 SA et W11 SB).

A. Création du Firewall SA (FW-SA)

Procédure pour créer la Machine Virtuelle (VM) du FW-SA avec les configurations initiales (les champs encadrés sont ceux qui sont modifiés).

Dans la barre d'outils supérieure de l'interface Proxmox VE, repérez et cliquez sur le bouton "**Create VM**" (Créer une VM).



1. **Nœud (Node) :** Le nœud d'hébergement pour cette VM est sélectionné par défaut ou manuellement (ici, pve01).
2. **ID de la VM (VM ID) :** Un identifiant unique est attribué à la machine virtuelle.
 - **Valeur :** 25005
3. **Nom (Name) :** Un nom descriptif est fourni pour faciliter l'identification de la VM dans l'interface.
 - **Valeur :** GRP1-FW-SA (indiquant qu'il s'agit du Firewall du Site A).
4. **Groupe de Ressources (Resource Pool) :** La VM est associée à un groupe de ressources pour une meilleure organisation au sein de l'environnement Proxmox.
 - **Valeur :** SIO2426

5. **Passage à l'étape suivante** : Une fois les informations générales validées, cliquez sur le bouton **"Next"** (Suivant) pour continuer la configuration dans l'onglet "OS".

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'General' tab selected. The fields are as follows:

- Node: pve01
- VM ID: 25005 (highlighted with a red box and number 1)
- Name: GRP1-FW-SA (highlighted with a red box and number 2)
- Resource Pool: SIO2426 (highlighted with a red box and number 3)

At the bottom right, the 'Next' button is highlighted with a red box and number 4. The 'Advanced' checkbox is unchecked. The 'Back' button is also visible.

1. **Sélection de l'image ISO (CD/DVD disc image file (iso)) :**

- S'assurer que l'option **"Use CD/DVD disc image file (iso)"** est sélectionnée.
- **Storage** : Le stockage contenant l'image ISO (ici, NAS01) est sélectionné.
- **(1) ISO image** : Le fichier ISO de l'OS (qui est probablement pfSense ou un OS basé sur FreeBSD, compte tenu de la nomenclature) est sélectionné.
 - **Valeur** : [Nom du fichier]-RELEASE-amd64.iso

2. **Type d'OS Invité (Guest OS) :**

- **(2) Type** : L'OS invité est spécifié comme Other (Autre), ce qui est courant pour les systèmes d'exploitation moins courants ou les Firewalls spécialisés comme pfSense, car ils ne correspondent pas à une catégorie Linux ou Windows standard.
 - **Valeur** : Other

3. **Passage à l'étape suivante** : Une fois l'image ISO et le type d'OS définis, cliquez sur le bouton **"Next"** (Suivant) pour passer à l'onglet "System" (Système).

- **(3) Action** : Clic sur **"Next"**.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

☒ Use CD/DVD disc image file (iso)

Storage: NAS01

ISO image: -RELEASE-amd64.iso

☐ Use physical CD/DVD Drive

☐ Do not use any media

Guest OS:

Type: Other

Version: -

Advanced ☐

Back Next

1. Type de Machine (Machine) :

- Le type de chipset émulé est sélectionné. Le choix du type q35 permet une meilleure gestion du bus PCIe et est recommandé pour les systèmes d'exploitation modernes.
- **(1) Valeur :** q35

2. Micrologiciel (BIOS) :

- Le type de BIOS est défini. Ici, le BIOS par défaut est conservé pour assurer la compatibilité avec l'installation standard.
- **(2) Valeur :** Default (SeaBIOS)

3. Contrôleur SCSI (SCSI Controller) :

- Sélection du pilote pour la gestion des disques. Le contrôleur VirtIO SCSI est choisi pour ses performances supérieures et sa faible consommation de ressources CPU.
- **(3) Valeur :** VirtIO SCSI

4. Passage à l'étape suivante :

Une fois les paramètres système validés, cliquez sur le bouton **"Next"** (Suivant) pour accéder à l'onglet "Disks" (Disques).

- **(4) Action :** Clic sur **"Next"**.

Create: Virtual Machine

General OS **System** Disks CPU Memory Network Confirm

Graphic card: Default

Machine: **1** q35

Firmware

BIOS: **2** Default (SeaBIOS)

SCSI Controller: **3** VirtIO SCSI

Qemu Agent: ☐

Add TPM: ☐

4

Help Advanced ☐ Back **Next**

1. Bus/Périphérique (Bus/Device) :

- L'interface de connexion du disque est définie sur **SCSI** (scsi0), en cohérence avec le contrôleur VirtIO SCSI sélectionné à l'étape précédente pour des performances optimales.
- **(1) Valeur : SCSI**

2. Stockage (Storage) : Le pool de stockage physique sur lequel le disque virtuel sera créé est sélectionné (ici, Data01).

3. Taille du Disque (Disk size) :

- La capacité du disque dur virtuel est définie. Une taille de 20 GiB est généralement suffisante pour un système d'exploitation de type firewall.
- **(2) Valeur : 20 GiB**

4. Cache :

- La politique de cache pour les opérations d'entrée/sortie (I/O) du disque est définie sur **"Write back"** (Écriture différée). Cette option améliore les performances d'écriture en utilisant la mémoire du host, mais nécessite un agent Qemu ou des mécanismes d'intégrité pour éviter la perte de données en cas de panne de courant du host.
- **(3) Valeur : Write back**

5. Format : Le format de l'image disque (ici, QEMU image format, généralement qcow2) est sélectionné.

6. Passage à l'étape suivante : Une fois la configuration du disque terminée, cliquez sur le bouton **"Next"** (Suivant) pour passer à l'onglet "CPU".

- **(4) Action : Clic sur "Next".**

Create: Virtual Machine

General OS System **Disks** CPU Memory Network Confirm

scsi0

Disk Bandwidth

Bus/Device: **1** SCSI 0 Cache: **3** Write back

SCSI Controller: VirtIO SCSI Discard: ☐

Storage: Data01 IO thread: ☐

Disk size (GiB): **2** 20

Format: QEMU image format

Add

Help Advanced ☐ Back **4**

1. Sockets et Cœurs (Sockets and Cores) :

- **Sockets** : Le nombre de sockets de CPU virtuels est laissé à 1.
- **(1) Cœurs (Cores)** : Le nombre de cœurs alloués au socket est défini sur 2.
- **Total Cores** : La VM aura un total de **2 cœurs virtuels** (1 Socket x 2 Cœurs).
 - **Valeur** : 2

2. Type de CPU (Type) :

- Le type de CPU émulé est défini sur **"host"**. Cette option expose le jeu d'instructions complet du processeur physique du host à la VM. Elle est recommandée pour de meilleures performances, surtout si la VM n'a pas besoin de migrer vers un host avec un processeur différent.
- **(2) Valeur** : host

3. Passage à l'étape suivante : Après avoir configuré l'allocation CPU, cliquez sur le bouton **"Next"** (Suivant) pour passer à l'onglet "Memory" (Mémoire).

- **(3) Action** : Clic sur **"Next"**.

The screenshot shows the 'Create: Virtual Machine' window with the 'CPU' tab selected. The 'Sockets' dropdown is set to '1'. The 'Cores' dropdown is set to '2', highlighted with a red box and a red circle labeled '1'. The 'Type' dropdown is set to 'host', highlighted with a red box and a red circle labeled '2'. The 'Total cores' is displayed as '2'. At the bottom right, the 'Next' button is highlighted with a red box and a red circle labeled '3'. The 'Back' button is also visible. A 'Help' button is on the bottom left, and an 'Advanced' checkbox is next to the 'Back' button.

1. Mémoire (Memory (MiB)) :

- La quantité de mémoire vive dédiée à la VM est spécifiée en MiB (mégaoctets binaires). Une allocation de 1024 MiB est choisie, ce qui équivaut à 1 GiB de RAM. Cette quantité est généralement suffisante pour un système de type firewall ou routeur comme pfSense pour une utilisation standard.
- **(1) Valeur** : 1024 MiB

2. Passage à l'étape suivante : Une fois la mémoire allouée, cliquez sur le bouton **"Next"** (Suivant) pour passer à l'onglet "Network" (Réseau).

- **(2) Action** : Clic sur **"Next"**.

Create: Virtual Machine

General OS System Disks CPU **Memory** Network Confirm

Memory (MiB): 1024

1

2

? Help Advanced ☐ Back Next

1. Pont Réseau (Bridge) :

- L'interface réseau virtuelle est connectée à un pont réseau spécifique de l'hôte Proxmox (le host). Ce pont (vmbr1) permet à la VM de communiquer avec le réseau physique ou d'autres machines virtuelles connectées au même pont.
- **(1) Valeur :** vmbr1

2. Modèle de Carte Réseau (Model) :

- Le modèle de la carte réseau virtuelle est sélectionné. Le modèle "**VirtIO (paravirtualized)**" est choisi car il offre les meilleures performances en réduisant la surcharge de virtualisation.
- **(2) Valeur :** VirtIO (paravirtualized)

3. VLAN Tag et Firewall :

Ces options sont laissées par défaut (pas de VLAN, option Firewall cochée/non cochée en fonction du besoin de gestion par le firewall intégré de Proxmox).

4. Passage à l'étape suivante :

La première interface réseau étant configurée, cliquez sur le bouton "**Next**" (Suivant) pour passer à l'onglet "Confirm" (Confirmer).

- **(3) Action :** Clic sur "**Next**".

Create: Virtual Machine

GeneralOSSystemDisksCPUMemoryNetworkConfirm

☐ No network device

Bridge: 1 vmbr1

Model: 2 VirtIO (paravirtualized)

VLAN Tag: no VLAN

MAC address: auto

Firewall: ☒

3

Help

Advanced ☐

Back

Next

Si la configuration est correcte, cliquez sur le bouton "**Finish**" (Terminer) pour créer la machine virtuelle.

Create: Virtual Machine

General OS System Disks CPU Memory Network **Confirm**

Key ↑	Value
bios	ovmf
cores	2
cpu	host
ide2	NAS01.iso/pfSense-CE-2.7.2-RELEASE-amd64.iso,media=cdrom
machine	q35
memory	1024
name	GRP1-FW-SA
net0	virtio,bridge=vibr1,firewall=1
nodename	pve01
numa	0
ostype	other
pool	SIO2426
scsi0	Data01:20,format=qcow2,cache=writeback
scsihw	virtio-scsi-pci

☐ Start after created

Advanced ☐ **Back** **Finish**

1. **Sélection de la VM** : Dans l'arborescence de gauche, sélectionnez la machine virtuelle nouvellement créée, **25000 (GRP1-FW-SA)**, et naviguez vers l'onglet **"Hardware"** (Matériel).

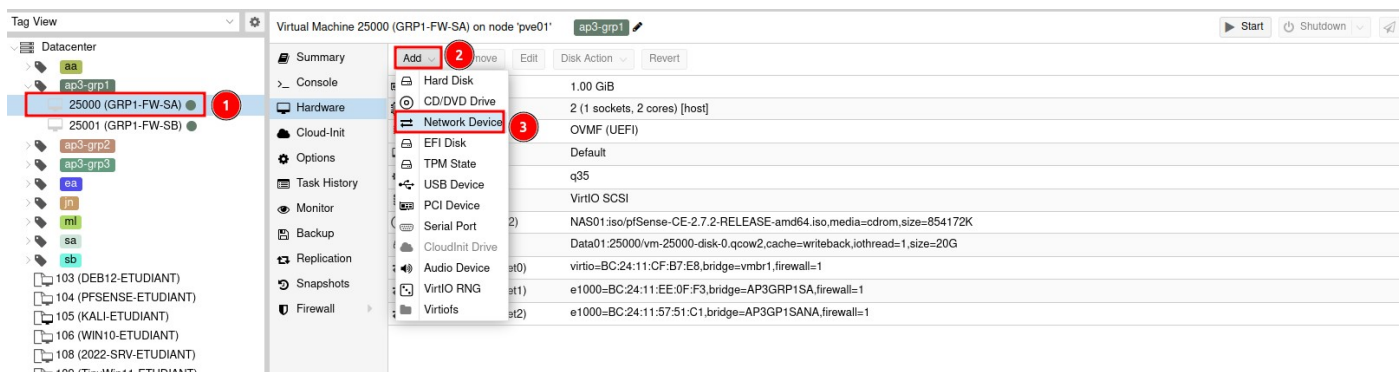
- **(1) Action** : Sélection de 25000 (GRP1-FW-SA) > Onglet Hardware.

2. **Démarrer l'ajout** : Cliquez sur le bouton **"Add"** (Ajouter) dans la barre d'outils au-dessus de la liste des périphériques matériels.

- **(2) Action** : Clic sur **"Add"**.

3. **Choisir le périphérique** : Dans le menu déroulant qui apparaît, sélectionnez **"Network Device"** (Périphérique Réseau).

- **(3) Action** : Sélection de Network Device.



1. **Pont Réseau (Bridge)** :

- La nouvelle interface réseau est connectée au pont réseau Proxmox qui gère le trafic LAN du Site

A.

- **(1) Valeur** : AP3GRP1SA (Ce pont est spécifiquement nommé pour le groupe/LAN du Site A).

2. **Modèle de Carte Réseau (Model)** :

- Le modèle "**VirtIO (paravirtualized)**" est sélectionné à nouveau pour garantir des performances optimales et une bonne compatibilité avec le système d'exploitation du firewall (pfSense/FreeBSD).

- **(2) Valeur** : VirtIO (paravirtualized)

3. **Autres Paramètres** : VLAN Tag est laissé à "no VLAN" et l'option Firewall est cochée (dans cet environnement, cela peut être utilisé pour les règles Proxmox).

4. **Ajouter la carte réseau** : Cliquez sur le bouton "**Add**" (Ajouter) pour intégrer cette nouvelle carte réseau (qui sera **net1** dans la configuration de la VM) à la machine virtuelle.

- **(3) Action** : Clic sur "**Add**".

The screenshot shows the 'Add: Network Device' dialog box. It has a title bar with a close button. The main area contains four fields: 'Bridge' with a dropdown menu showing 'AP3GRP1SA', 'Model' with a dropdown menu showing 'VirtIO (paravirtualized)', 'VLAN Tag' with a dropdown menu showing 'no VLAN', and 'MAC address' with a text field showing 'auto'. There is a 'Firewall' checkbox which is checked. At the bottom, there is a 'Help' button, an 'Advanced' checkbox, and an 'Add' button. Red circles and boxes are used to highlight the configuration steps: (1) Bridge, (2) Model, and (3) the Add button.

B. Création du Firewall SB (FW-SB)

La configuration de la machine virtuelle pour le **Firewall du Site B (FW-SB)** est **identique** en termes d'étapes de création et d'allocation de ressources (CPU, Mémoire, Disque) à celle du FW-SA.

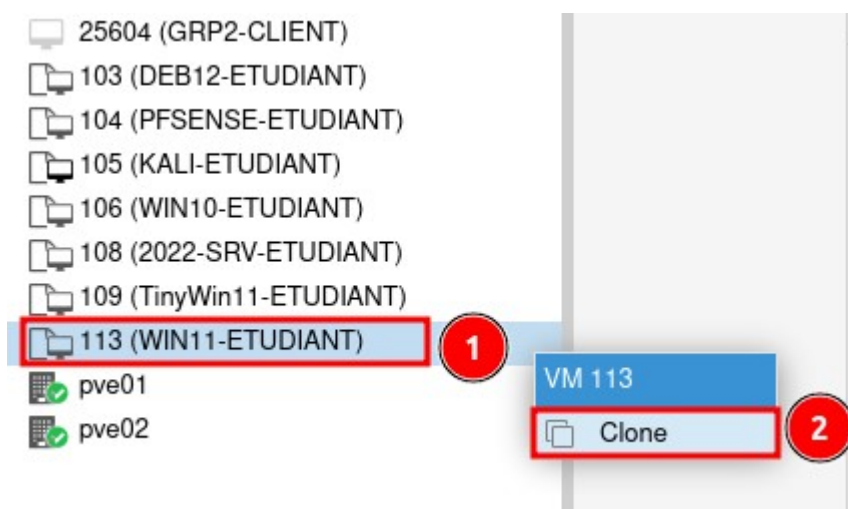
C. Création d'un client W11 sur le site A (W11-C1-SA)

1. **Sélection du Modèle** : Dans l'arborescence de gauche, localisez et effectuez un clic droit sur la machine virtuelle ou le modèle Windows 11 de base.

- **(1) Action** : Clic droit sur 113 (WIN11-ETUDIANT).

2. **Lancer le Clonage** : Dans le menu contextuel qui apparaît, sélectionnez l'option "**Clone**" (Cloner).

- **(2) Action** : Sélection de Clone.



1. ID de la VM (VM ID) et Nom (Name) :

- Un nouvel ID unique est attribué à la VM.
- Un nom clair identifiant le client est donné.
- **(1) VM ID** : 25004
- **(2) Name** : GRP1-W11-C1-SA (Client 1 du Site A).

2. Groupe de Ressources (Resource Pool) :

- Le clone est affecté au même groupe de ressources que le Firewall du Site A.
- **(3) Valeur** : SIO2426

3. Mode de Clonage (Mode) :

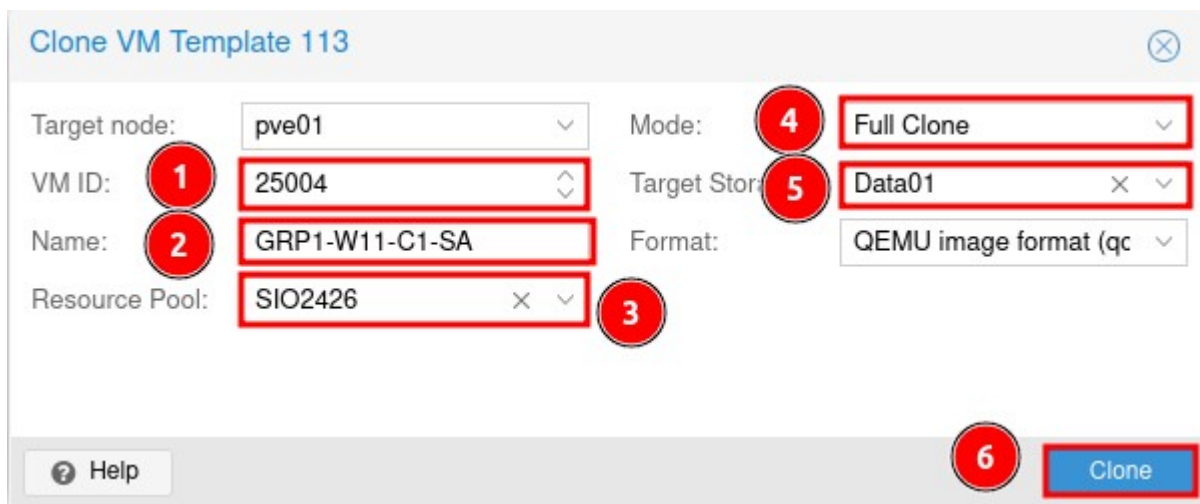
- Le **"Full Clone"** (Clonage Complet) est sélectionné, ce qui crée une copie indépendante du disque de la VM modèle. C'est le mode le plus sûr pour une machine qui sera utilisée de manière permanente.
- **(4) Valeur** : Full Clone

4. Stockage Cible (Target Storage) :

- Le disque dur du clone est placé sur le volume de stockage Data01.
- **(5) Valeur** : Data01

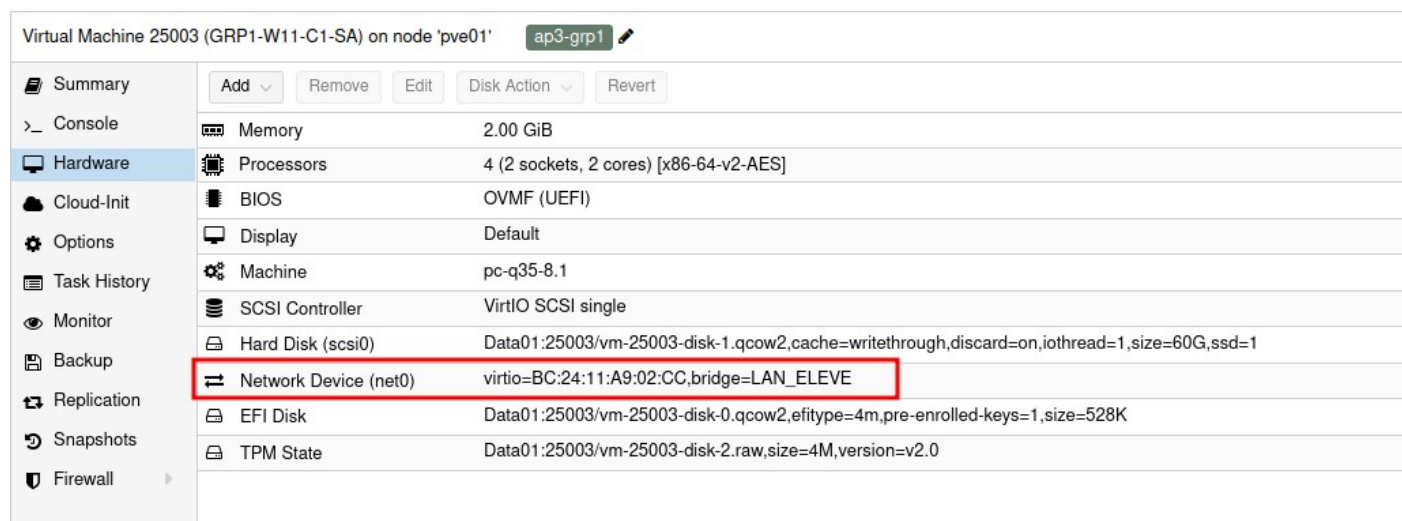
5. Lancer le Clonage : Cliquez sur le bouton **"Clone"** pour démarrer le processus de duplication du modèle.

- **(6) Action** : Clic sur **"Clone"**.



Accès à l'édition : Dans l'onglet **"Hardware"** (Matériel) de la VM GRP1-W11-C1-SA, double-cliquer ou

sélectionner le **Network Device (net0)** pour ouvrir la fenêtre d'édition.

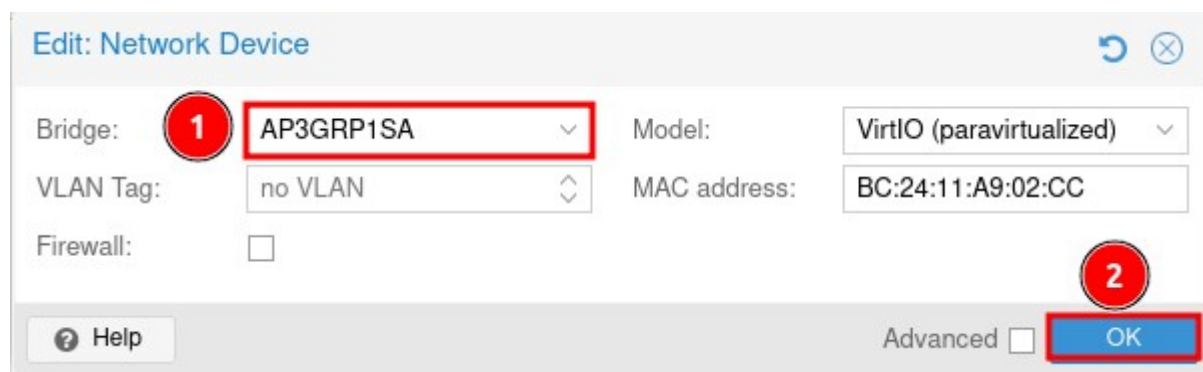


1. Modification du Pont (Bridge) :

- Le pont réseau existant (bridge=LAN_ELEVE dans le matériel original) est remplacé par le pont dédié au LAN du Site A.
- **(1) Valeur :** AP3GRP1SA (Le pont connecté à l'interface LAN du FW-SA).
- Note : Le modèle de la carte réseau reste VirtIO (paravirtualized).

2. **Validation :** Cliquez sur "**OK**" pour enregistrer la modification et connecter le client W11-SA à son réseau local.

- **(2) Action :** Clic sur "**OK**".



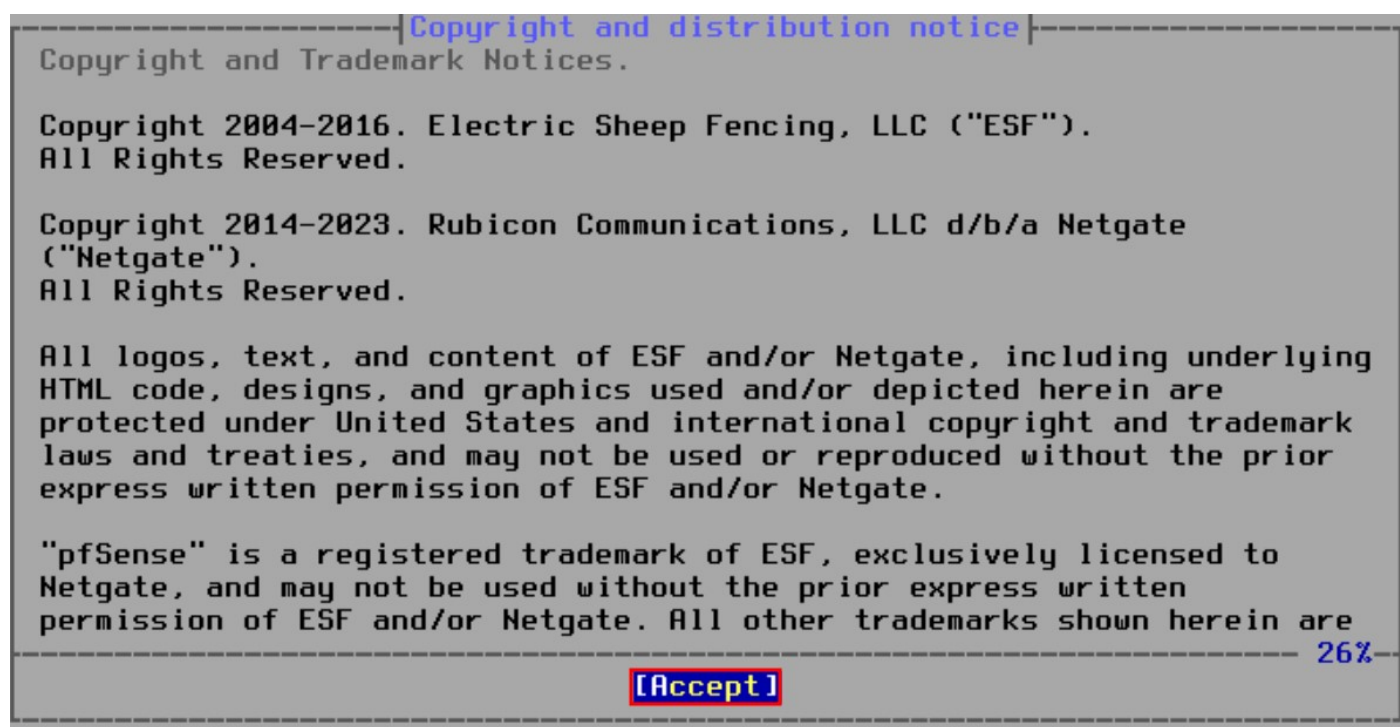
D. Création d'un client W11 sur le site B (W11-C1-SB)

Procédez de manière identique pour la création du client Windows 11 du Site B (W11-SB).

E. Installation du pare-feu du site A en CLI

Appuyer sur la touche ENTER pour sélectionner **[Accept]** et passer à l'étape de partitionnement et de

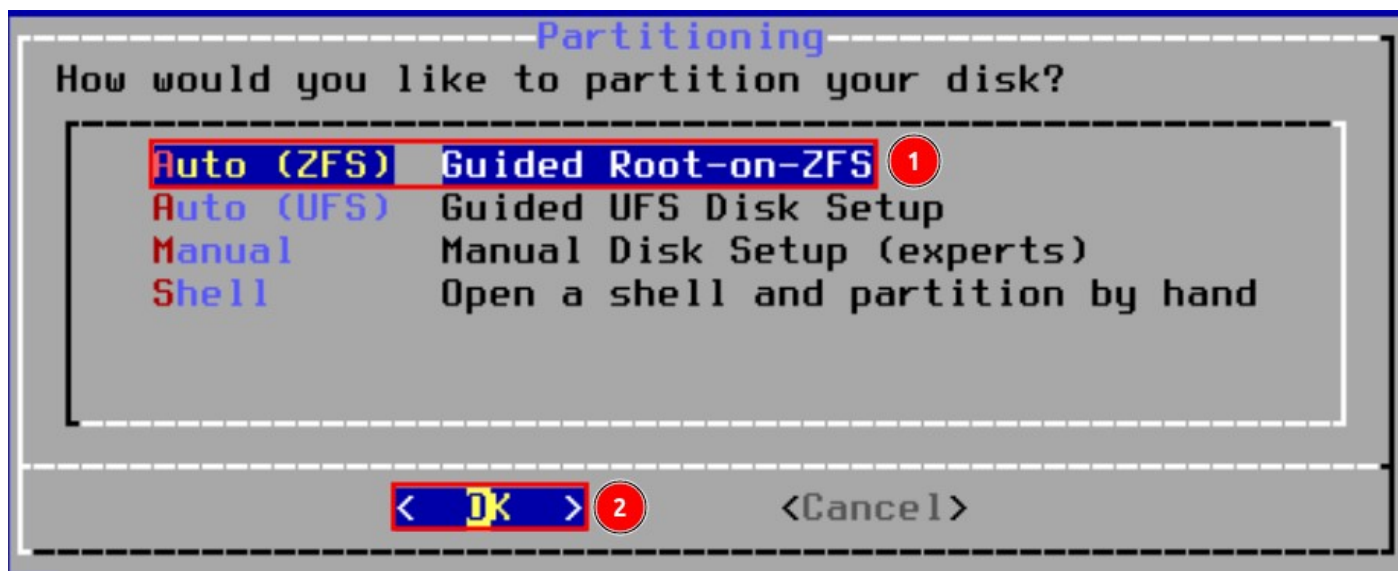
configuration du disque.



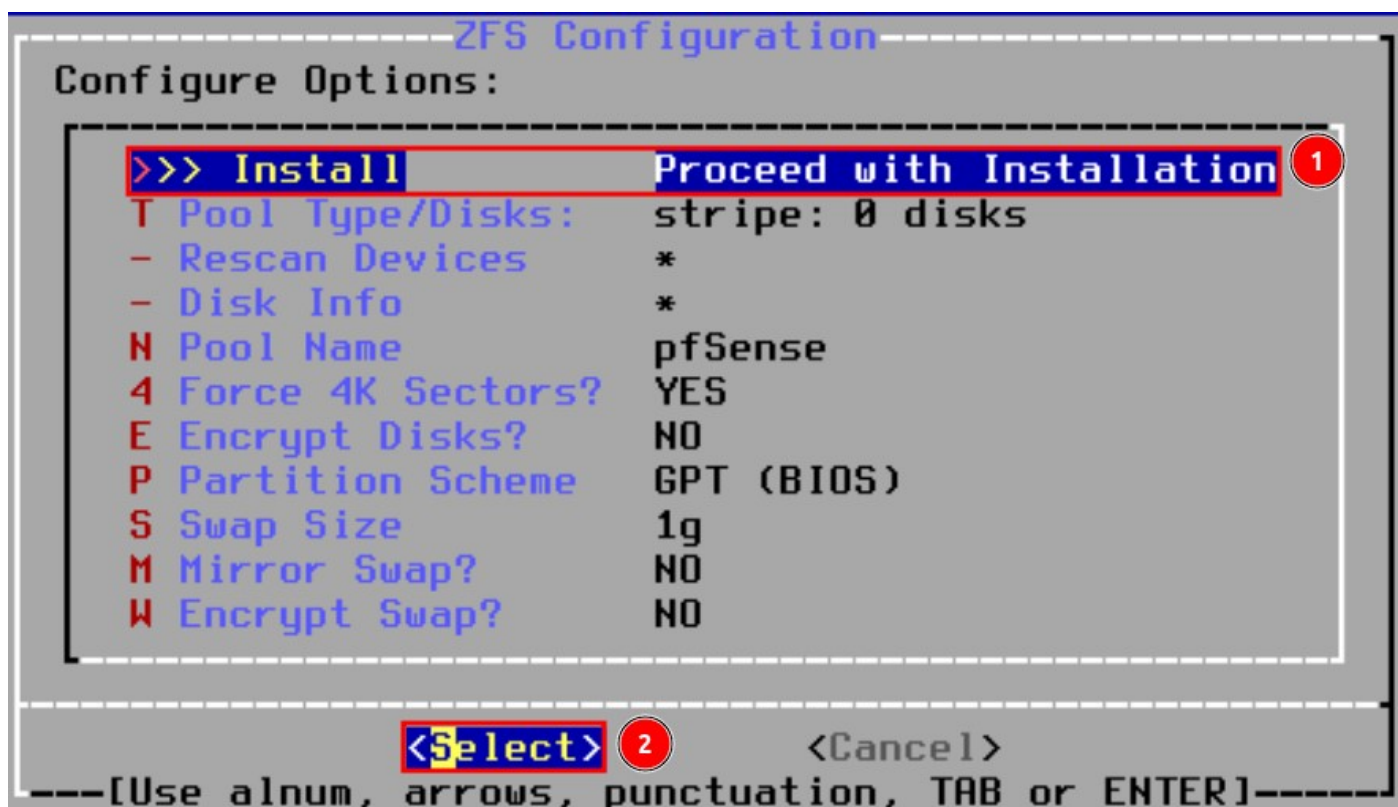
1. **Sélection de l'option** : L'option **Install** (Installer) est présélectionnée.
 - **(1) Action** : S'assurer que l'option Install pfSense est mise en surbrillance.
2. **Validation** : Le bouton **[OK]** est mis en surbrillance.
 - **(2) Action** : Appuyer sur la touche ENTER pour sélectionner **[OK]** et commencer la configuration de l'installation.



1. **Sélection du Mode de Partitionnement** : Le mode **Auto (ZFS) - Guided Root-on-**
ZFS (Partitionnement automatique avec le système de fichiers ZFS) est mis en surbrillance. Ce choix est souvent privilégié pour la résilience et les fonctionnalités avancées de ZFS.
 - **(1) Action** : S'assurer que l'option Auto (ZFS) est sélectionnée.
2. **Validation** : Le bouton **[OK]** est mis en surbrillance.
 - **(2) Action** : Appuyer sur la touche ENTER pour sélectionner **[OK]** et passer à l'écran de sélection du disque.



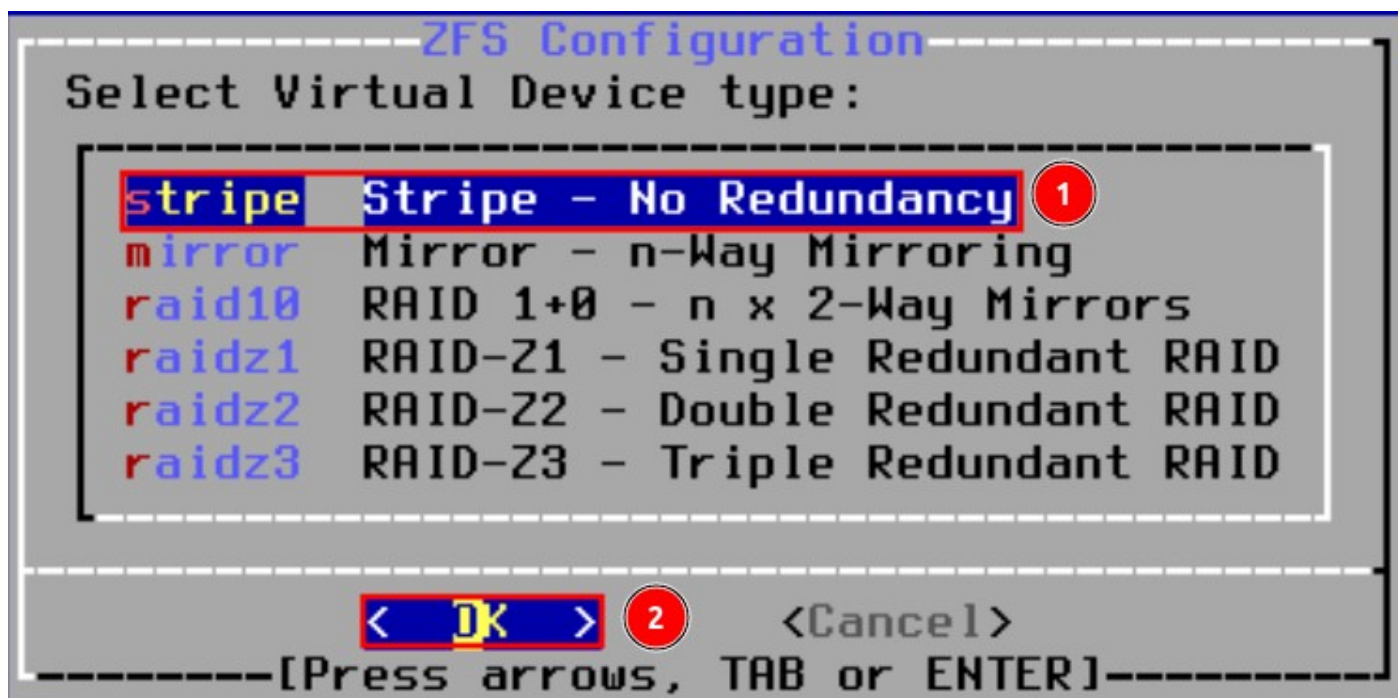
1. **Passage à la Sélection** : Pour l'instant, l'option >>> **Install - Proceed with Installation** est en surbrillance.
 - **(1) Action** : L'installateur suppose que nous allons d'abord sélectionner **T Pool Type/Disks** même si l'option Install est présélectionnée.
2. **Validation** :
 - **(2) Action** : Cliquer sur **[Select]** pour modifier les options (ici, pour sélectionner le disque via l'option Pool Type/Disks).



1. **Sélection du Type de Pool** :
 - L'option **stripe - Stripe - No Redundancy** (Stripe - Aucune Redondance) est sélectionnée. Ce mode est le seul approprié lorsque l'on utilise un seul disque virtuel, car il n'y a pas d'autre disque pour configurer la mise en miroir (mirror) ou les niveaux RAID-Z.
 - **(1) Action** : S'assurer que Stripe - No Redundancy est sélectionné.

2. Validation :

- **(2) Action :** Appuyer sur la touche ENTER pour sélectionner **[OK]** et passer à l'écran de sélection du disque physique.



1. Sélection du Disque :

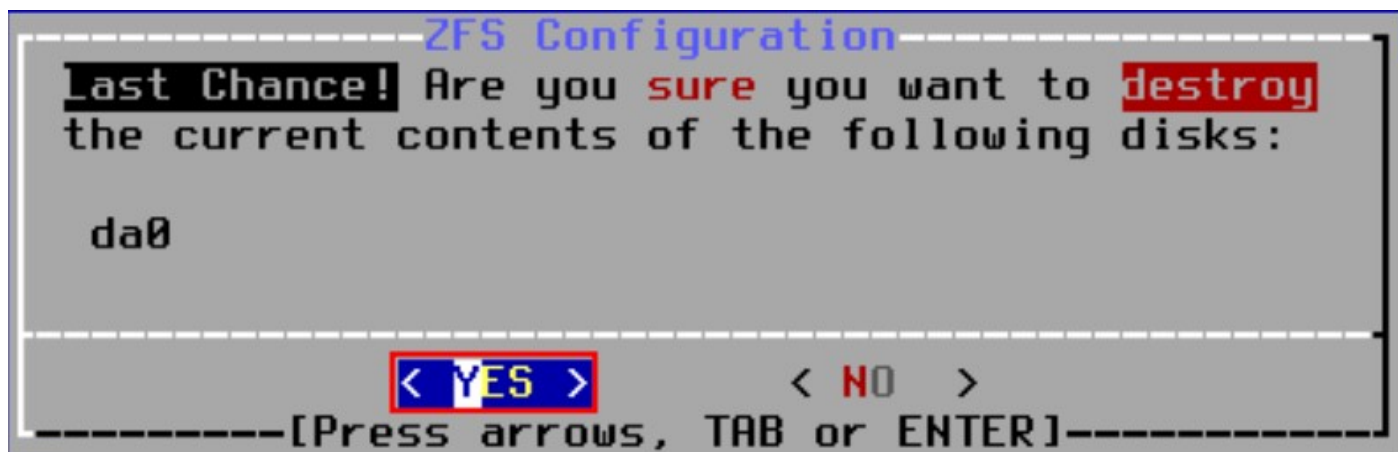
- Le disque disponible (da0 - identifié comme un QEMU QEMU HARDDISK) est mis en surbrillance. Il s'agit du disque virtuel de 20 GiB configuré précédemment dans Proxmox. L'astérisque [*] indique qu'il est sélectionné.
- **(1) Action :** Appuyer sur la barre d'espace pour sélectionner/désélectionner le disque. S'assurer que da0 est sélectionné.

2. Validation :

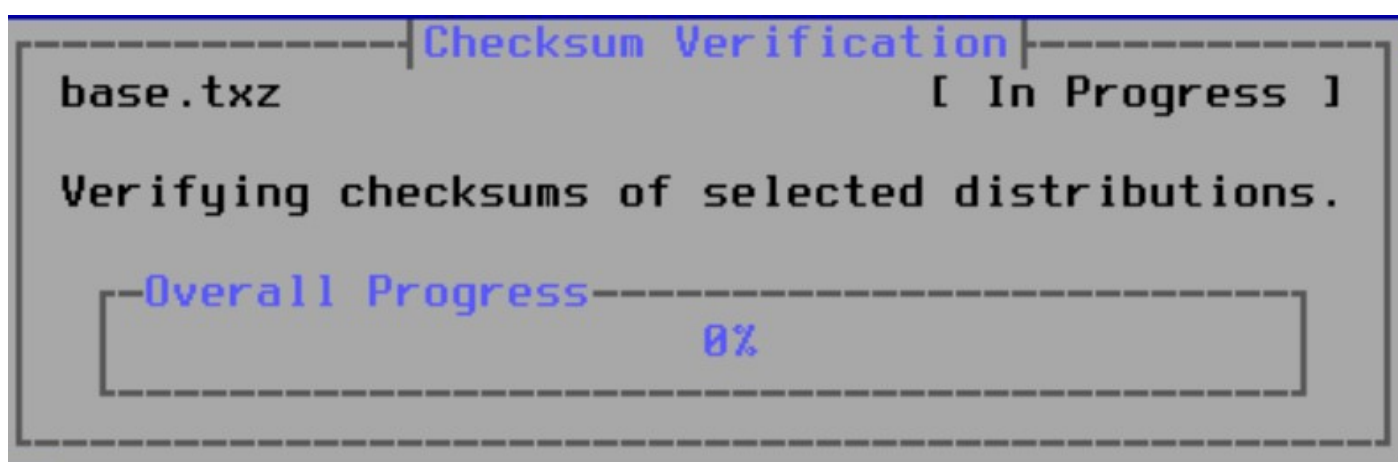
- **(2) Action :** Appuyer sur la touche ENTER pour sélectionner **[OK]** et valider le choix du disque.



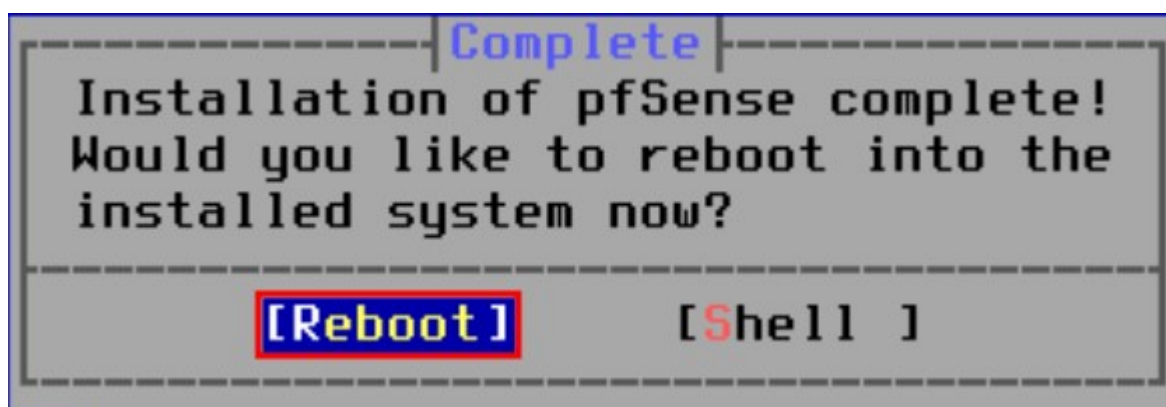
Confirmation : Le bouton **[YES]** (Oui) est présélectionné.



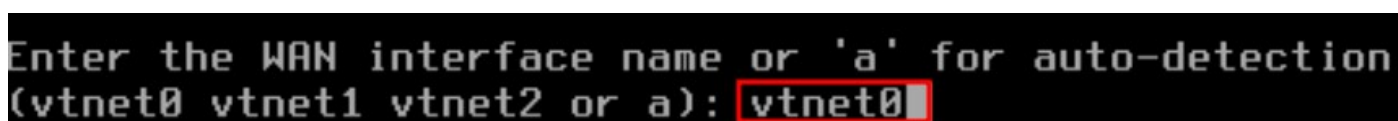
- L'installateur commence par vérifier les sommes de contrôle (checksums) des distributions sélectionnées, y compris le fichier système de base (base.txz), pour garantir l'intégrité des données avant la copie.



L'option **[Reboot]** (Redémarrer) est présélectionnée.



Identifier et assigner la carte réseau dédiée à l'interface WAN (réseau externe/Internet) du Firewall du Site A.



Identifier et assigner la carte réseau dédiée à l'interface LAN (réseau interne) du Firewall du Site A.

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 vtnet2 a or nothing if finished): vtnet1
```

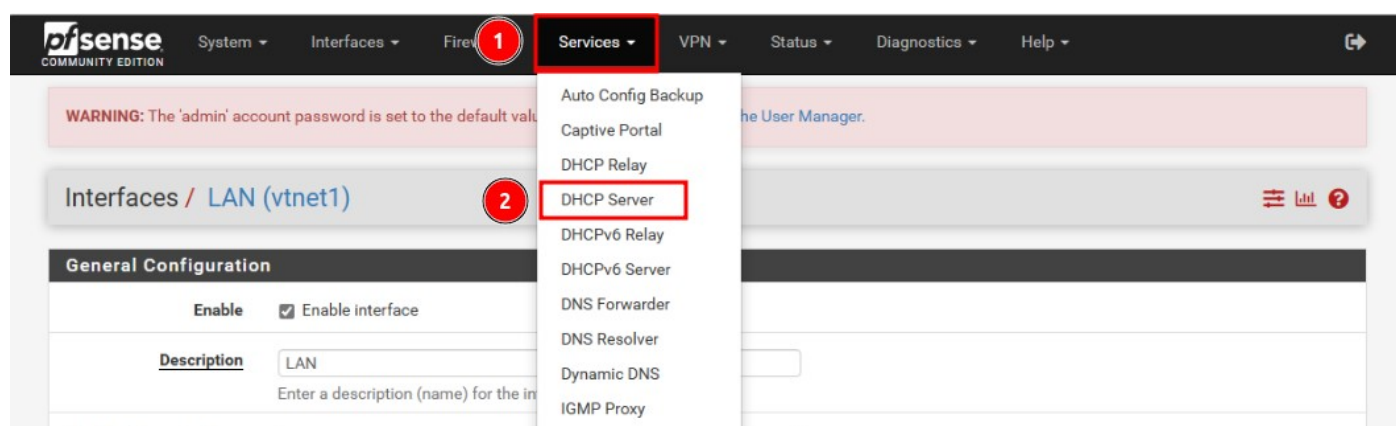
F. Installation du pare-feu du site B en CLI

Répétez l'intégralité de la procédure d'installation pfSense et de la configuration des interfaces CLI (y compris la validation de la licence, le partitionnement ZFS, l'installation des fichiers système et l'assignation des interfaces WAN et LAN) pour le Firewall du Site B (FW-SB).

Assurez-vous que les interfaces WAN et LAN du FW-SB sont correctement assignées aux ponts réseau Proxmox qui leur sont dédiés sur le Site B.

G. Configuration du pare-feu du site A via la GUI

1. **Navigation vers les Services** : Dans la barre de navigation principale de pfSense, cliquez sur le menu **"Services"**.
 - **(1) Action** : Clic sur Services.
2. **Sélection du Serveur DHCP** : Dans le menu déroulant, sélectionnez l'option **"DHCP Server"** (Serveur DHCP).
 - **(2) Action** : Sélection de DHCP Server.



Décochez la case **"Enable DHCP server on LAN interface"**.

General DHCP Options

DHCP Backend ISC DHCP

Enable ☐ Enable DHCP server on LAN interface

BOOTP ☐ Ignore BOOTP queries

Deny Unknown Clients Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

1. **Cliquer sur Interfaces** : Dans la barre de menu, cliquez sur **Interfaces** (1).
2. **Sélectionner LAN** : Dans le menu déroulant, sélectionnez l'interface **LAN** (2).



Attribuer une adresse IP statique (locale) à l'interface LAN du pare-feu.

Static IPv4 Configuration

IPv4 Address 192.168.100.1 / 24

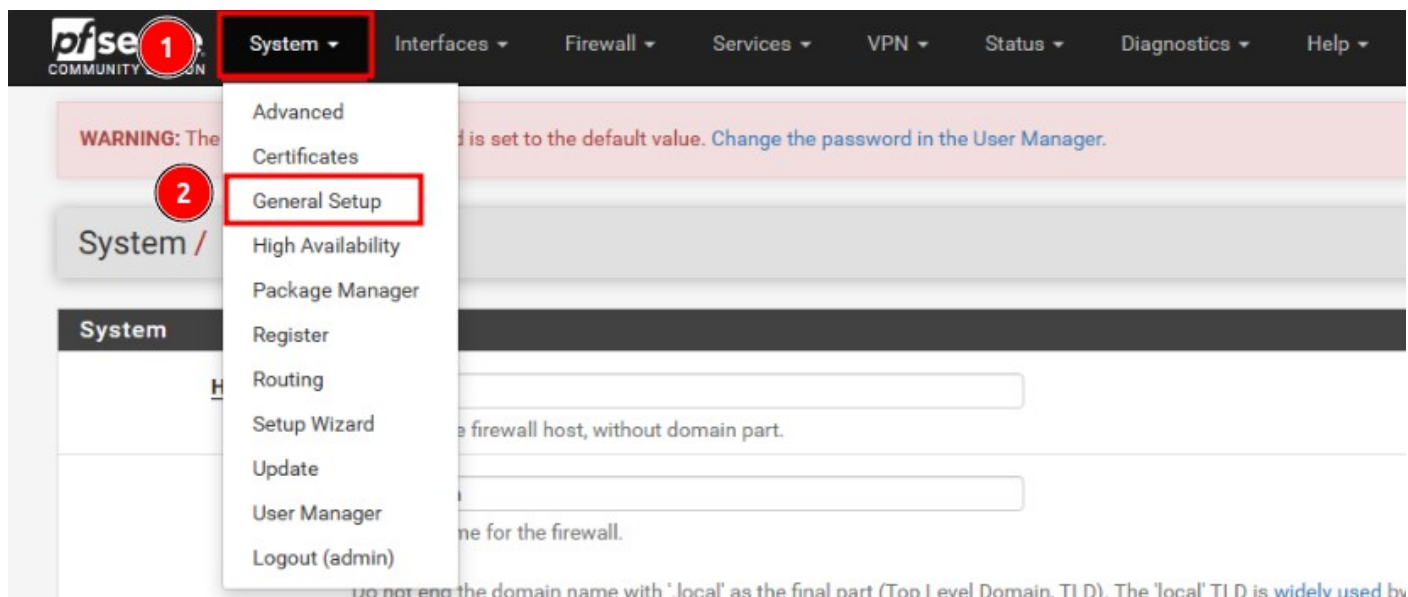
IPv4 Upstream gateway None + Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a **WAN** type interface.
Gateways can be managed by [clicking here](#).

Vérifier que les adresses IP statiques ont été correctement assignées aux interfaces.

Interfaces			
WAN	↑	10Gbase-T <full-duplex>	192.168.42.42
LAN	↑	10Gbase-T <full-duplex>	192.168.100.1
SAN	↑	10Gbase-T <full-duplex>	192.168.50.1

1. **Cliquer sur System** : Dans la barre de menu, cliquez sur **System** (1).
2. **Sélectionner General Setup** : Dans le menu déroulant, sélectionnez **General Setup** (2).



1. **Saisie du Nom d'Hôte (Hostname)** : Entrez un nom d'hôte descriptif pour le firewall.

- (1) **Valeur** : FW-SA (Firewall Site A)

2. **Saisie du Domaine (Domain)** : Entrez le nom de domaine local pour le réseau du Site A.

- (2) **Valeur** : ief.local

A screenshot of the 'System' > 'General Setup' page in pfSense. The 'Hostname' field is filled with 'FW-SA' and is highlighted with a red box and a red circle with the number '1'. The 'Domain' field is filled with 'ief.local' and is highlighted with a red box and a red circle with the number '2'. Below the domain field, there is a warning message: 'Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The '.local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses '.local' as its TLD. Alternatives such as '.home.arpa', '.local.lan', or '.mylocal' are safe.'

Cliquez sur "**Save**" en bas de la page, puis sur "**Apply Changes**" pour appliquer les paramètres.

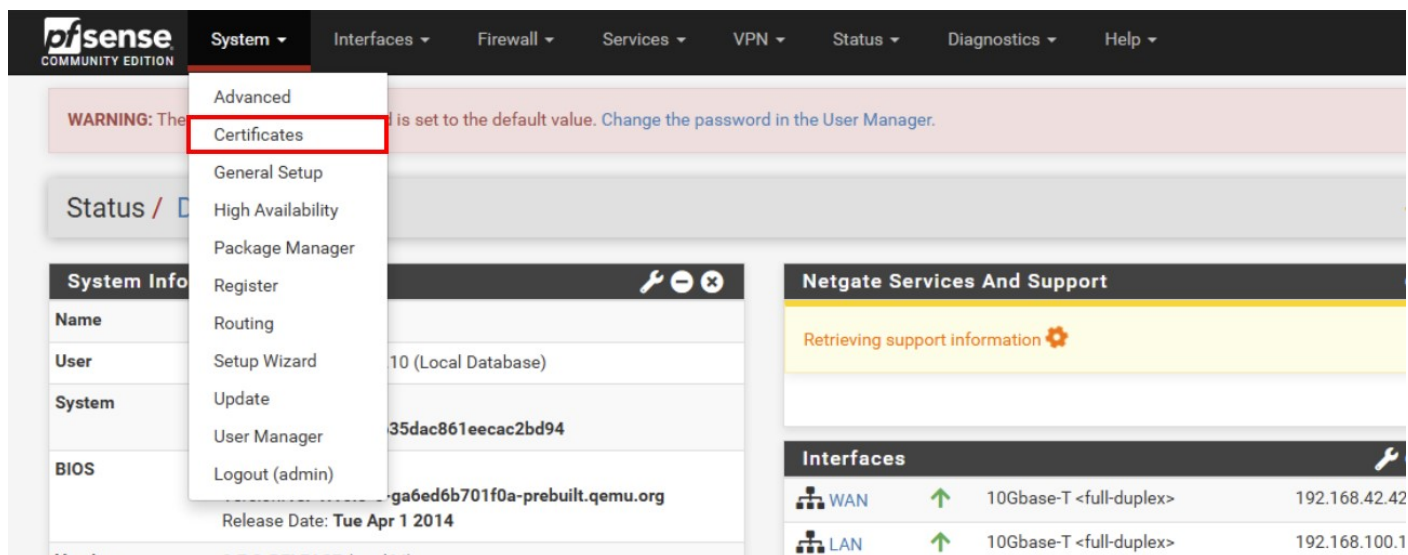
A screenshot of the 'System' > 'General Setup' page in pfSense, showing the bottom section. It includes options for 'Alias Popups', 'Disable dragging', 'Login page color' (set to 'Dark Blue'), and 'Login hostname'. At the bottom, there is a 'Save' button highlighted with a red box.

H. Configuration du pare-feu du site B via la GUI

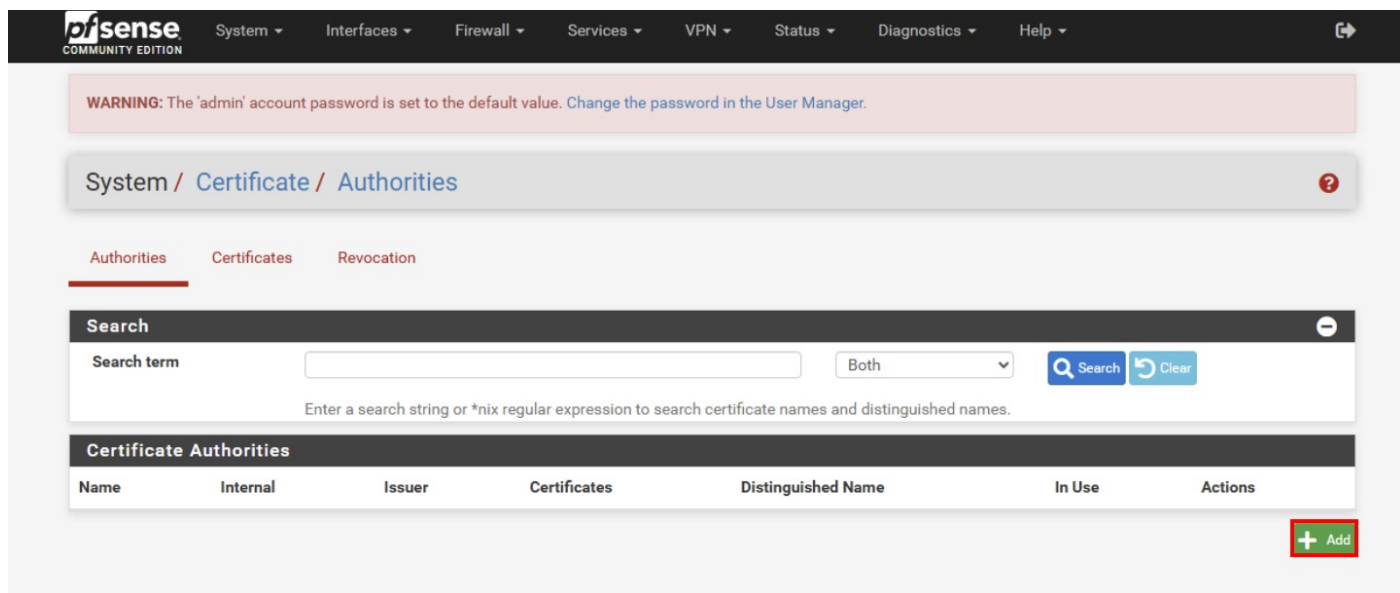
Répétez toutes les étapes de la configuration via la GUI pour le Firewall du Site B (FW-SB), y compris l'activation et la configuration du serveur DHCP sur son interface LAN, et les réglages système généraux.

I. Création d'un certificat d'autorité sur le pare-feu du site A

1. **Cliquer sur System** : Dans la barre de menu de pfSense, cliquez sur le menu **System**.
2. **Sélectionner Certificates** : Dans le menu déroulant, sélectionnez **Certificates**.



Cliquez sur le bouton **+ Add** (Ajouter) situé en bas à droite du tableau des Autorités de Certification.



1. **Nom Descriptif (Descriptive name)** : Entrez un nom clair pour l'Autorité de Certification du Site A.
 - **(1) Valeur** : FW-SA (ou CA-FW-SA pour plus de clarté).
2. **Méthode** : Laissez la méthode sur **Create an internal Certificate Authority** (Créer une Autorité de Certification interne).
3. **Numéros de Série Aléatoires (Randomize Serial)** : Cochez l'option pour utiliser des numéros de série aléatoires lors de la signature des certificats, ce qui est une bonne pratique de sécurité.
 - **(2) Action** : Cochez **Use random serial numbers when signing certificates**.

Authorities Certificates Revocation

Create / Edit CA

Descriptive name FW-SA 1
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 Create an internal Certificate Authority

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 2
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 RSA

1. **Nom Commun (Common Name)** : Entrez le nom qui identifie la CA de manière unique.

- (1) **Valeur** : FW-SA

2. **Sauvegarde** : Cliquez sur le bouton **Save** (Sauvegarder) pour créer la CA.

- (2) **Action** : Clic sur **Save**.

Lifetime (days) 3650

Common Name FW-SA 1

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

Country Code None

State or Province e.g. Texas

City e.g. Austin

Organization e.g. My Company Inc

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

Save 2

La CA **FW-SA** est visible dans la liste. Les détails confirment qu'elle est "Internal" (interne), "self-signed" (auto-signée).






System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both

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

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
FW-SA	✓	self-signed	0	CN=FW-SA Valid From: Wed, 10 Sep 2025 17:29:23 +0000 Valid Until: Sat, 08 Sep 2035 17:29:23 +0000		    

+ Add

Sur l'icone en étoile, cliquez dessus, puis télécharger le certificat.






System / Certificate / Authorities

Authorities Certificates Revocation

Search

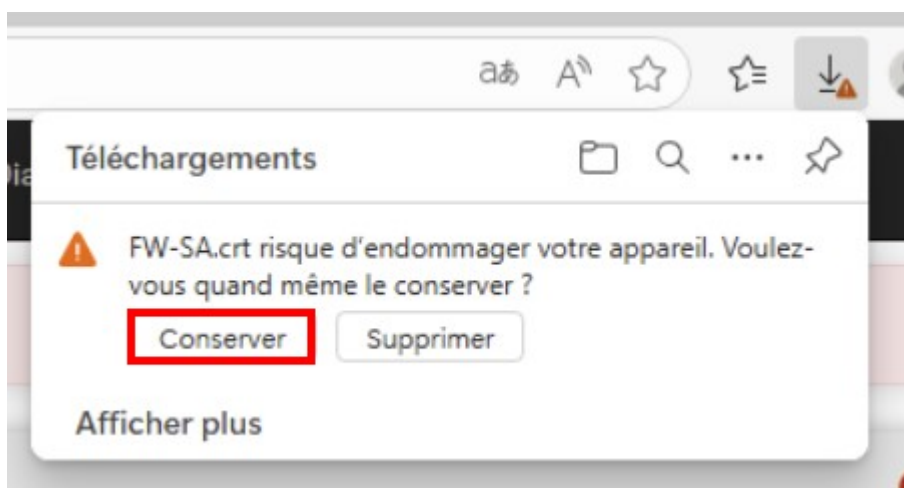
Search term Both

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

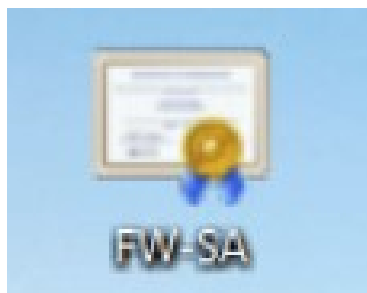
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
FW-SA	✓	self-signed	0	CN=FW-SA Valid From: Wed, 10 Sep 2025 17:29:23 +0000 Valid Until: Sat, 08 Sep 2035 17:29:23 +0000		    

+ Add

1. **Alerte du Navigateur** : Le navigateur affiche un avertissement de sécurité sur le fichier téléchargé (souvent à cause de l'extension .crt).
2. **Confirmation de la Conservation** : Cliquez sur **Conserver** (Keep) pour ignorer l'avertissement et conserver le fichier FW-SA.crt dans les téléchargements.

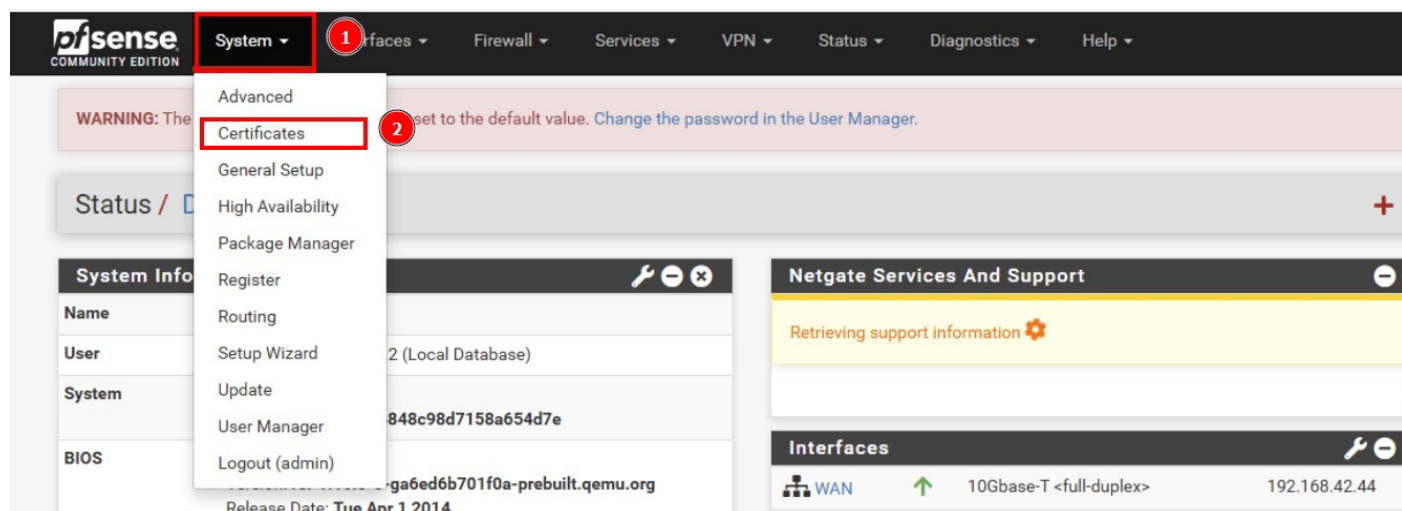


Transfert de Fichier : Transférez le fichier de certificat **FW-SA.crt** (représenté par l'icône de diplôme) du poste de travail utilisé pour la gestion du FW-SA vers une machine accessible du Site B.

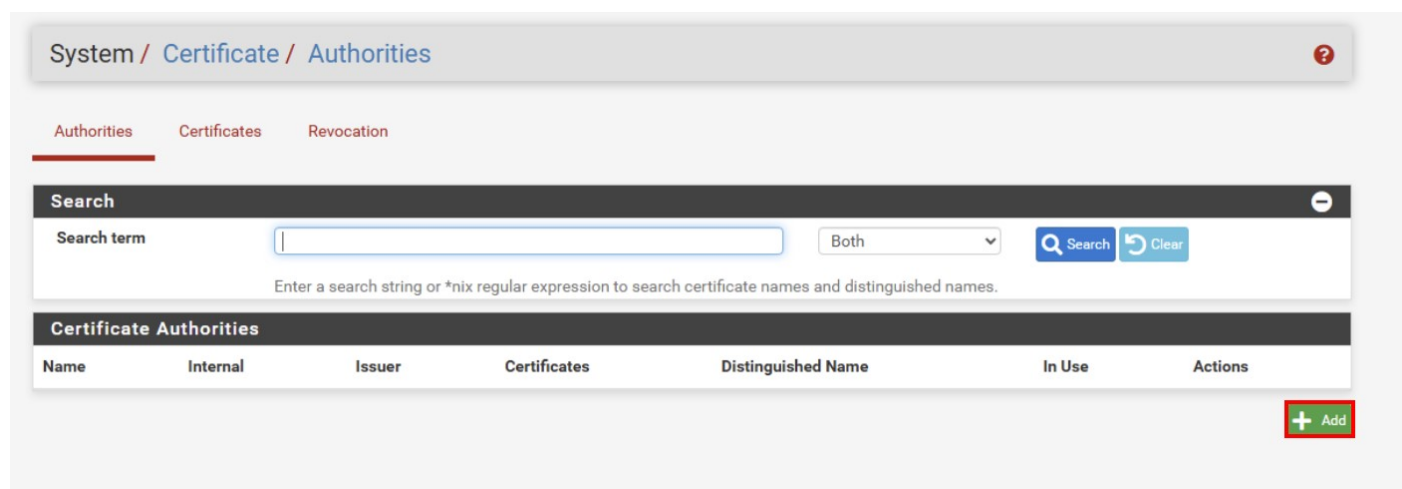


Créer et sauvegarder la CA sur le FW-SB, puis l'exporter comme fait précédemment pour le FW-SA.

1. **Cliquer sur System :** Dans la barre de menu, cliquez sur **System** (1).
2. **Sélectionner Certificates :** Dans le menu déroulant, sélectionnez **Certificates** (2).



Accéder à l'onglet "Authorities" et cliquer sur **+ Add**.



1. **Nom Descriptif (Descriptive name) :** Entrez le nom du certificat que vous êtes sur le point d'importer.

- **(1) Valeur :** FW-SB (Ce nom interne au FW-SA représentera la CA du FW-SB).
2. **Numéros de Série Aléatoires (Randomize Serial) :** Cochez l'option pour utiliser des numéros de série aléatoires lors de la signature des certificats, ce qui est une bonne pratique de sécurité.
- **(2) Action :** Cochez **Use random serial numbers when signing certificates**.

Authorities Certificates Revocation

Create / Edit CA

Descriptive name FW-SB 1
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 Create an internal Certificate Authority

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 2
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 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

Activier Windows

1. **Nom Commun (Common Name) :** Saisissez le Nom Commun de la CA telle qu'elle a été créée sur le FW-SB.
- **(1) Valeur :** FW-SB
 - (2) Clic sur **Save**.

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) 3650

Common Name FW-SB 1
The following certificate authority subject components are optional and may be left blank.

Country Code None

State or Province e.g. Texas

City e.g. Austin

Organization e.g. My Company Inc

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

Save 2

Vérification de la CA Locale (FW-SB) : La CA **FW-SB** est visible, auto-signée et a ses propres dates de validité.

System / Certificate / Authorities





Authorities Certificates Revocation

Search

Search term Both

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

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
FW-SB	✓	self-signed	0	CN=FW-SB Valid From: Wed, 10 Sep 2025 17:38:44 +0000 Valid Until: Sat, 08 Sep 2035 17:38:44 +0000		   

Cliquez sur l'icône d'exportation pour télécharger le certificat racine de la CA du FW-SB (FW-SB.crt).

System / Certificate / Authorities





Authorities Certificates Revocation

Search


Search term Both


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

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
FW-SB	✓	self-signed	0	CN=FW-SB Valid From: Wed, 10 Sep 2025 17:38:44 +0000 Valid Until: Sat, 08 Sep 2035 17:38:44 +0000		   

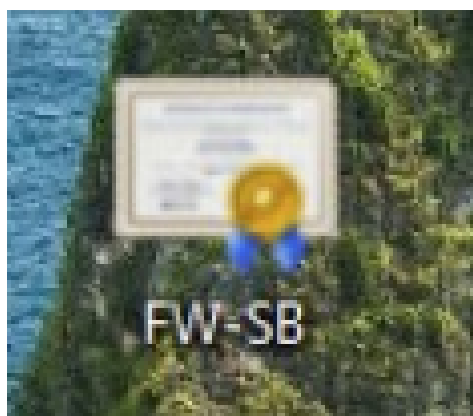
Téléchargements

 FW-SB.crt
[Ouvrir un fichier](#)

 FW-SA.crt
[Ouvrir un fichier](#)

[Afficher plus](#)

Transférez le fichier de certificat **FW-SB.crt** du poste de travail utilisé pour la gestion du FW-SB vers une machine accessible du Site A.



Importer le certificat racine du FW-SB pour que le Firewall du Site A lui fasse confiance.

Clic sur **+ Add** pour accéder à la fenêtre de création/modification de CA, où vous sélectionnerez la méthode d'importation.

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both

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

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
FW-SA	✓	self-signed	0	CN=FW-SA Valid From: Wed, 10 Sep 2025 17:29:23 +0000 Valid Until: Sat, 08 Sep 2035 17:29:23 +0000		

+ Add

1. **Nom Descriptif (Descriptive name)** : Entrez un nom pour identifier la CA externe que vous importez.
 - (1) **Valeur** : FW-SB-CA
2. **Méthode** : Changez la méthode par défaut (Create an internal CA) pour l'importation d'une CA externe.
 - (2) **Valeur** : Import an existing Certificate Authority

Authorities Certificates Revocation

Create / Edit CA

Descriptive name 1

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 2

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.

Copier le contenu textuel du certificat racine (FW-SB.crt) dans le champ de données pour l'importation.

Existing Certificate Authority

Certificate data

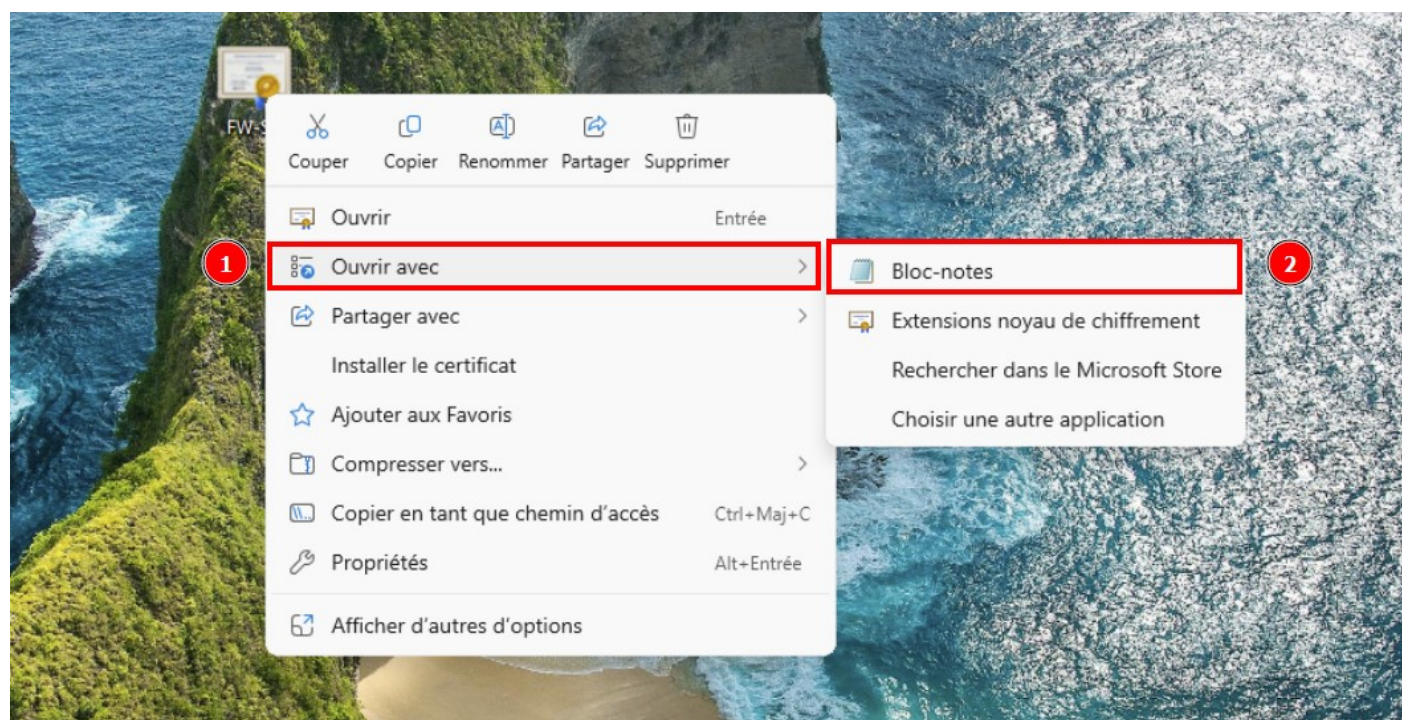
Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional)

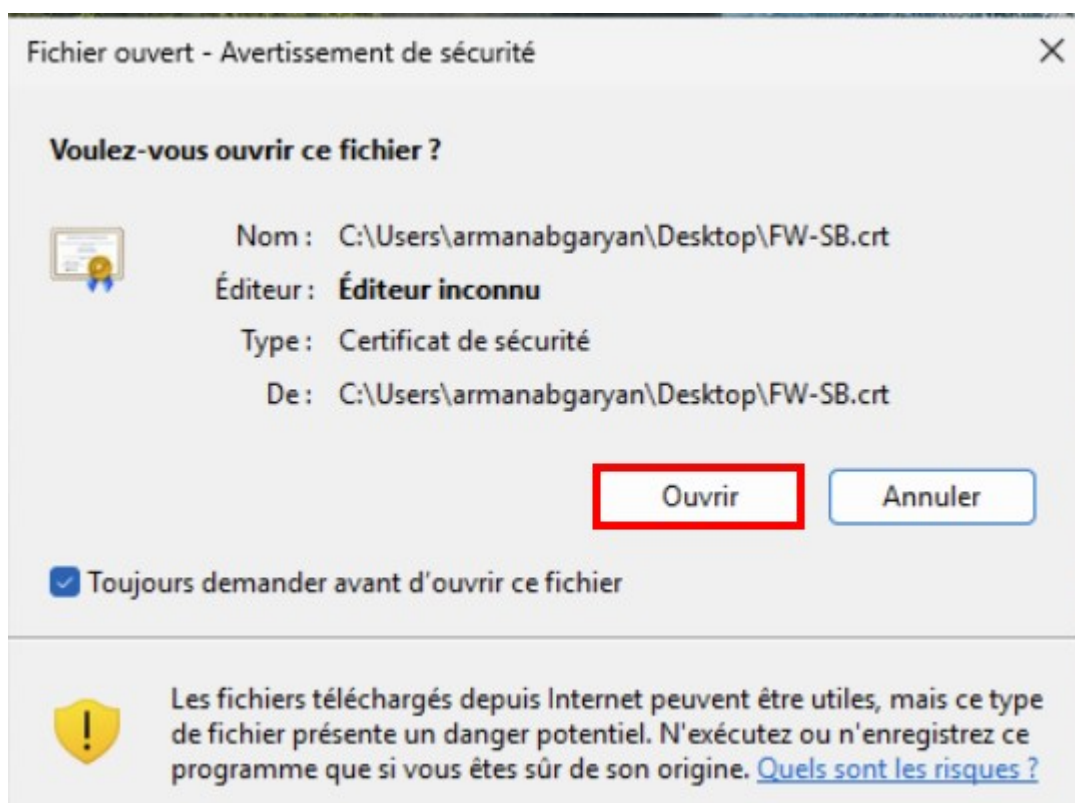
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial

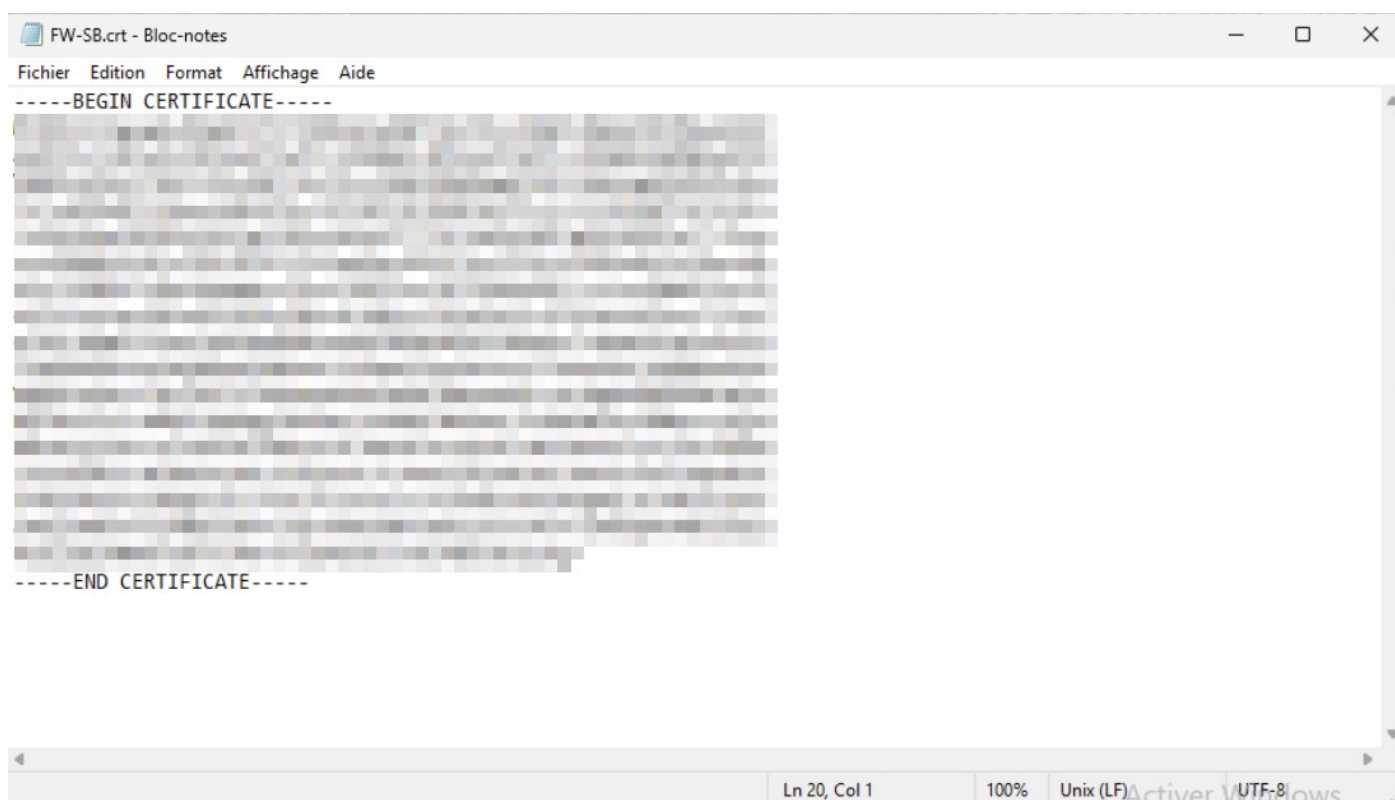
1. **Ouvrir le Fichier** : Effectuez un clic droit sur le fichier FW-SB.crt sur le bureau.
2. **Choix de l'application** : Sélectionnez **Ouvrir avec** (1).
3. **Éditeur de Texte** : Choisissez l'éditeur de texte de base, **Bloc-notes** (2).



Avertissement de Sécurité : Confirmez l'ouverture du fichier en cliquant sur **Ouvrir** dans la fenêtre d'avertissement.



Une fois le fichier ouvert, copiez l'intégralité du texte du certificat dans le Bloc-notes.



Collez le texte copié dans le champ "**Certificate data**" encadré.

Existing Certificate Authority

Certificate data

-----BEGIN CERTIFICATE-----
[Blurred Certificate Data]
-----END CERTIFICATE-----


Paste a certificate in X.509 PEM format here.

Certificate Private Key

Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial

Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is ignored when Randomize Serial is checked.



 Save

L'échange de certificats racines est complet. Le FW-SA fait confiance aux certificats signés par la CA du FW-SB, et inversement. Les firewalls peuvent maintenant créer des certificats d'entité (serveur/client) pour le tunnel IPsec, signés par leurs CAs locales respectives.









System / Certificate / Authorities


Authorities Certificates Revocation

Search

Search term Both  

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

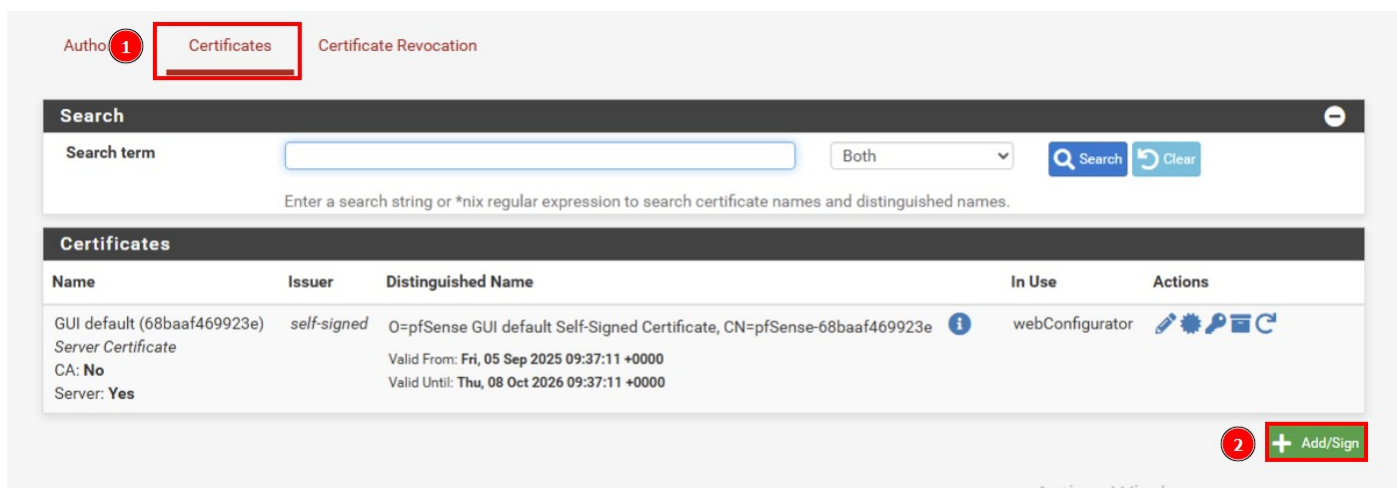
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
FW-SA	✓	self-signed	0	CN=FW-SA Valid From: Wed, 10 Sep 2025 17:29:23 +0000 Valid Until: Sat, 08 Sep 2035 17:29:23 +0000		    
FW-SB-CA	✗	self-signed	0	CN=FW-SB Valid From: Wed, 10 Sep 2025 17:38:44 +0000 Valid Until: Sat, 08 Sep 2035 17:38:44 +0000		  

 Add

Répétez la procédure d'importation de l'Autorité de Certification sur le Firewall du Site B (FW-SB), en utilisant le fichier **FW-SA.crt** précédemment transféré.

J. Création des certificats IPsec sur le pare-feu du site A

1. **Vérification de l'onglet** : Assurez-vous que l'onglet **Certificates** (Certificats) est sélectionné (1).
2. **Lancer l'ajout** : Cliquez sur le bouton + **Add/Sign** (Ajouter/Signer) (2).



Nom Descriptif (Descriptive name) : Entrez un nom pour identifier le certificat d'entité du FW-SA.

- **Valeur** : FW-SA-Certificate

Nom Commun (Common Name) : Saisissez le nom qui sera utilisé comme identifiant principal du certificat pour le FW-SA.

- **Valeur** : FW-SA-Certificate

1. **Nom Alternatif (FQDN/Hostname)** : Ajoutez le FQDN complet du FW-SA comme Nom Alternatif.
 - **Valeur** : FW-SA.ief.local

2. Ajout du SAN pour l'Adresse IP WAN :

- Cliquez sur **+ Add SAN Row** (Ajouter ligne SAN) (2).

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

Alternative Names 1
Type Value

Add SAN Row + Add SAN Row 2

- Sélectionnez le type **IP Address** et entrez l'adresse IP **WAN publique** du FW-SA (c'est l'identifiant que le FW-SB utilisera).

For internal certificates, these attributes are added directly to the certificate as shown.

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

Alternative Names Delete

1 2 Delete
Type Value

Add SAN Row + Add SAN Row

Save 3

Activer Windows
Accédez aux paramètres pour activer Windo

Confirmer que le certificat **FW-SA-Certificate** est correctement listé et signé par la CA locale.

Authorities **Certificates** **Certificate 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 (68baaf469923e) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-68baaf469923e Valid From: Fri, 05 Sep 2025 09:37:11 +0000 Valid Until: Thu, 08 Oct 2026 09:37:11 +0000	webConfigurator	Info Edit Export Import Refresh
FW-SA-Certificate User Certificate CA: No Server: No	FW-SA	CN=FW-SA-Certificate Valid From: Wed, 10 Sep 2025 17:55:26 +0000 Valid Until: Sat, 08 Sep 2035 17:55:26 +0000		Info Edit Export Import Refresh Delete

+ Add/Sign

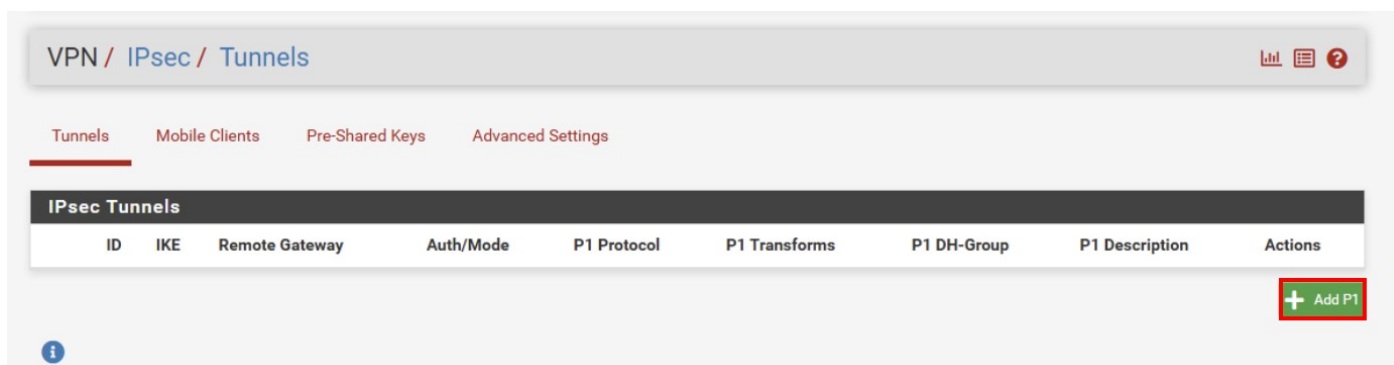
Répéter ce processus sur le FW-SB pour créer le **FW-SB-Certificate**.

K. Création du VPN Site-to-Site IPsec avec la CA sur le pare-feu du site A

1. **Cliquer sur VPN** : Dans la barre de menu, cliquez sur **VPN** (1).
2. **Sélectionner IPsec** : Dans le menu déroulant, sélectionnez l'option **IPsec** (2).

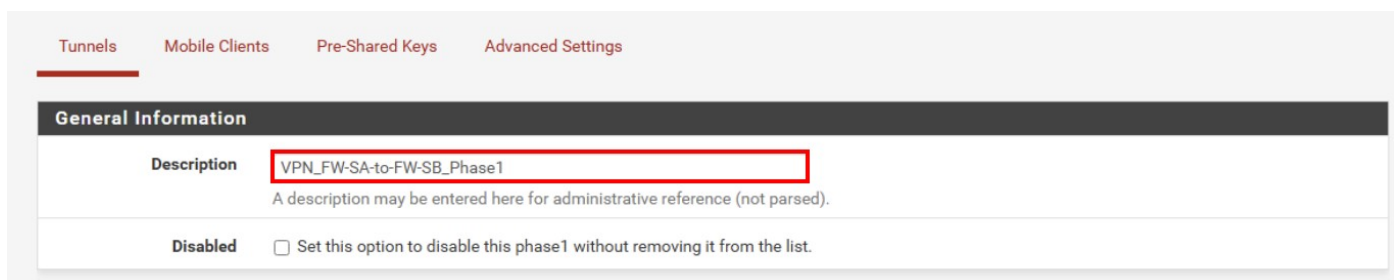


Cliquez sur le bouton vert **+ Add P1** (Ajouter P1) en bas à droite du tableau "IPsec Tunnels".




Description : Saisissez une description pour identifier facilement cette Phase 1.

- **Valeur** : VPN_FW-SA-to-FW-SB_Phase1



Passerelle Distant (Remote Gateway) : Entrez l'adresse IP WAN publique du Firewall du Site B (FW-SB).

- **Valeur** : 192.168.42.44

IKE Endpoint Configuration	
Key Exchange version	<div>IKEv2</div> <div>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</div>
Internet Protocol	<div>IPv4</div> <div>Select the Internet Protocol family.</div>
Interface	<div>WAN</div> <div>Select the interface for the local endpoint of this phase1 entry.</div>
Remote Gateway	<div>192.168.42.44</div> <div>Enter the public IP address or host name of the remote gateway. </div>

- Méthode d'Authentification (Authentication Method)** : Sélectionnez l'authentification mutuelle par certificat.
 - (1) **Valeur** : Mutual Certificate
- Mon Identifiant (My identifier)** : Définissez l'identifiant du FW-SA, qui doit correspondre à un des Noms Communs ou SAN de son certificat. Le FQDN complet est utilisé ici.
 - (2) **Type** : Fully qualified domain name
 - (3) **Valeur** : FW-SA.ief.local
- Identifiant du Pair (Peer identifier)** : Définissez l'identifiant attendu du FW-SB (le firewall distant).
 - (4) **Type** : Fully qualified domain name
 - (5) **Valeur** : FW-SB.ief.local
- Mon Certificat (My Certificate)** : Sélectionnez le certificat local du FW-SA créé précédemment pour l'authentification.
 - (6) **Valeur** : FW-SA-Certificate
- Autorité de Certification du Pair (Peer Certificate Authority)** : Sélectionnez la CA du FW-SB (importée) pour valider le certificat présenté par le FW-SB.
 - (7) **Valeur** : FW-SB-CA

Phase 1 Proposal (Authentication)	
Authentication Method	<div>Mutual Certificate</div> <div>Must match the setting chosen on the remote side.</div>
My identifier	<div>Fully qualified domain name</div> <div>FW-SA.ief.local</div>
Peer identifier	<div>Fully qualified domain name</div> <div>FW-SB.ief.local</div>
My Certificate	<div>FW-SA-Certificate</div> <div>Select a certificate which identifies this firewall. The certificate must have at least one non-wildcard SAN.</div>
Peer Certificate Authority	<div>FW-SB-CA</div> <div>Select a certificate authority to validate the peer certificate.</div>

Algorithme de Chiffrement (Encryption Algorithm) : Sélectionnez un algorithme moderne et fort.

- Valeur : AES256-GCM

Phase 1 Proposal (Encryption Algorithm)				
Encryption Algorithm	<div>AES256-GCM</div>	<div>128 bits</div>	<div>SHA256</div>	<div>14 (2048 bit)</div>
Algorithm		Key length	Hash	DH Group
Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.				
Add Algorithm	<div>+ Add Algorithm</div>			

Action de Fermeture Child SA (Child SA Close Action) : Cette option contrôle le comportement du FW-SA lorsque le pair distant ferme inopinément l'association de sécurité (P2).

- **Valeur :** Restart/Reconnect (Redémarrer/Reconnecter) est sélectionné pour assurer une tentative de reconnexion automatique en cas de rupture de P2.

Advanced Options	
Child SA Start Action	<div>Default</div>
Set this option to force specific initiation/responder behavior for child SA (P2) entries	
Child SA Close Action	<div>Restart/Reconnect</div>
Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)	
NAT Traversal	<div>Auto</div>
Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.	
MOBIKE	<div>Disable</div>
Set this option to control the use of MOBIKE	
Gateway duplicates	<input type="checkbox"/> Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pfSense does not manage routing to the remote gateway and traffic will follow the default route without regard for the chosen interface. Static routes can override this behavior.
Split connections	<input type="checkbox"/> Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.

Clic sur **Save**.

Delay	<div>10</div>
Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.	
Max failures	<div>5</div>
Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the retransmission timeout is used instead.	
<div><div>Save</div></div>	

La Phase 1 (VPN_FW-SA-to-FW-SB_Phase1) est listée avec l'ID 1, IKEv2, Remote Gateway 192.168.42.44 et l'authentification Mutual Certificate.

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 192.168.42.44	Mutual Certificate -	AES256-GCM (128 bits)	SHA256	14 (2048 bit)	VPN_FW-SA-to-FW-SB_Phase1	

Show Phase 2 Entries (0)

+ Add P1 Delete P1s

Une fois les changements appliqués, cliquez sur **+ Show Phase 2 Entries (0)**

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 192.168.42.44	Mutual Certificate -	AES256-GCM (128 bits)	SHA256	14 (2048 bit)	VPN_FW-SA-to-FW-SB_Phase1	

Show Phase 2 Entries (0)

+ Add P1 Delete P1s

Sur le bouton **+ Add P2** (Ajouter P2) pour créer la Phase 2.

	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 192.168.42.44	Mutual Certificate -	AES256-GCM (128 bits)	SHA256	14 (2048 bit)	VPN_FW-SA-to-FW-SB_Phase1	

	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<div>+ Add P2</div>									

Description : Saisissez une description pour identifier cette Phase 2.

- **Valeur :** VPN_FW-SA-to-FW-SB_Phase2

General Information

Description
A description may be entered here for administrative reference (not parsed).

Disabled ☐ Disable this phase 2 entry without removing it from the list.

Mode

Phase 1 VPN_FW-SA-to-FW-SB_Phase1 (IKE ID 1)

1. Réseau Local (Local Network) :

- Sélectionnez **LAN subnet** pour indiquer que tout le trafic provenant du réseau local du FW-SA (192.168.100.0/24) doit être chiffré et envoyé dans le tunnel.
- **(1) Valeur** : LAN subnet

2. Réseau Distant (Remote Network) :

- Sélectionnez **Network** comme type pour définir manuellement le réseau du Site B.
- **(2) Type** : Network
- **(3) Adresse** : Entrez l'adresse du sous-réseau LAN du FW-SB.
- **Valeur** : 192.168.200.0 / 24

Networks

Local Network LAN subnet 1 / 0

Type Address

Local network component of this IPsec security association.

NAT/BINAT translation None / 0

Type Address

2 If NAT/BINAT is required on this network specify the address to be translated 3

Remote Network Network 192.168.200.0 / 24

Type Address

Remote network component of this IPsec security association.

Algorithme de Chiffrement (Encryption Algorithms) : Cochez l'algorithme de chiffrement souhaité, de préférence un algorithme GCM pour l'efficacité et la sécurité.

- **Action** : Cochez **AES256-GCM**.

Phase 2 Proposal (SA/Key Exchange)

Protocol ESP

Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

Encryption Algorithms

☐ AES 128 bits

☐ AES128-GCM 128 bits

☐ AES192-GCM Auto

☒ AES256-GCM Auto

☐ CHACHA20-POLY1305

Hash Algorithms

☐ SHA1 ☒ SHA256 ☐ SHA384 ☐ SHA512 ☐ AES-XCBC

Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

PFS key group 14 (2048 bit)

Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Hôte à Pinger Automatiquement (Automatically ping host) : Entrez l'adresse IP d'un hôte du réseau distant (Site B). Ce ping ICMP sera envoyé à travers le tunnel pour vérifier la connectivité et maintenir l'association de sécurité (P2) établie. L'adresse IP de l'interface LAN du FW-SB est utilisée ici.

- **(1) Valeur** : 192.168.200.1 (IP LAN du FW-SB)

Keep Alive

Automatically ping host 192.168.200.1 1
Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a tunnel mode P2, but does not trigger initiation of a VTI mode P2.

Keep Alive ☐ Enable periodic keep alive check
Periodically check this P2 and initiate it if disconnected; does not send traffic inside the tunnel. This check ignores the P1 option "Child SA Start Action" and works for both VTI and tunnel mode P2s. For IKEv2 without split connections, this only needs to be enabled on one P2.

Save 2

Vérifiez que l'entrée de la Phase 1 et la nouvelle entrée de la Phase 2 sont correctement listées.

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect. ✓ Apply Changes

IPsec Tunnels

	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> Disable	1	V2	WAN 192.168.42.44	Mutual Certificate -	AES256-GCM (128 bits)	SHA256	14 (2048 bit)	VPN_FW-SA-to-FW-SB_Phase1	
			Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/> Disable	1	tunnel	LAN	192.168.200.0/24	ESP	AES256-GCM (auto)		VPN_FW-SA-to-FW-SB_Phase2	
+ Add P2									

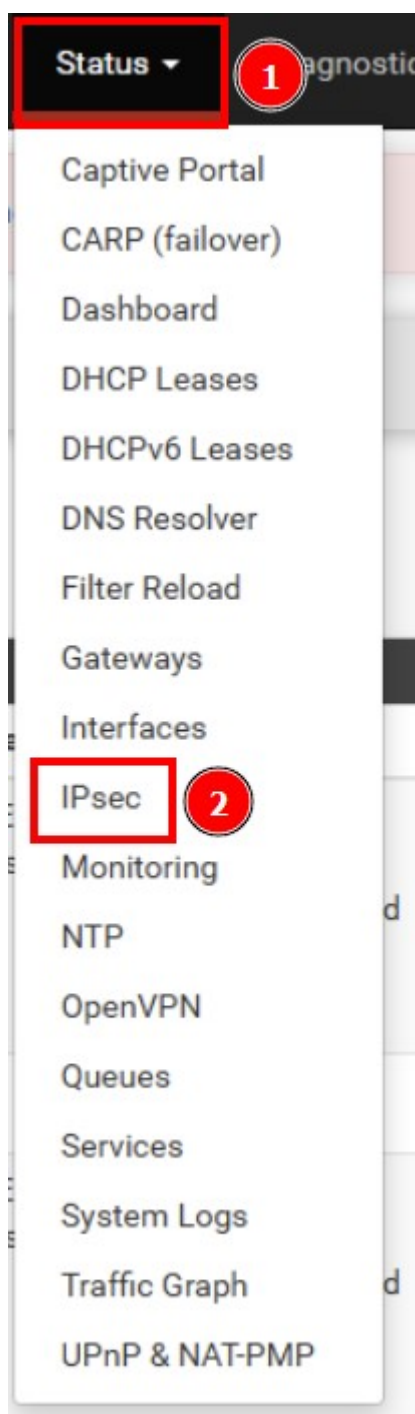
+ Add P1 Delete P1s

Activier Windows
Accédez aux paramètres pour activer Windows

Répétez la procédure complète de création de tunnel IPsec sur le Firewall du Site B (FW-SB), en vous assurant que les configurations de Phase 1 (IKE) et de Phase 2 (ESP) sont en miroir de celles du FW-SA.

L. Vérification et test du tunnel IPsec entre les deux sites

1. **Cliquer sur Status** : Dans la barre de menu, cliquez sur **Status** (1).
2. **Sélectionner IPsec** : Dans le menu déroulant, sélectionnez l'option **IPsec** (2).



Confirmer que la Phase 1 (IKE) de l'association de sécurité est établie et active.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / IPsec / Overview

Overview Leases SADs SPDs

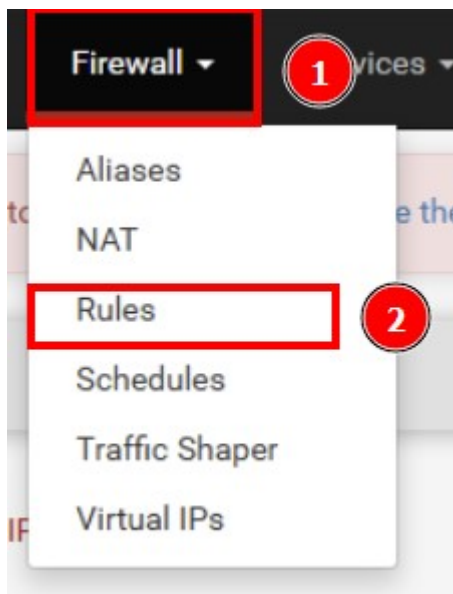
IPsec Status

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #18	VPN_FW-SB-to-FW- SA_Phase1	ID: FW-SB.ief.local Host: 192.168.42.44:500 SPI: ab8156e7b5d2a64d	ID: FW-SA.ief.local Host: 192.168.42.42:500 SPI: c986f5c36df78948	IKEv2 Responder	Rekey: 23208s (06:26:48) Reauth: Disabled	AES_GCM_16 (256) PRF_HMAC_SHA2_256 MODP_2048	Established 14 seconds (00:00:14) ago Disconnect P1

[+ Show child SA entries \(1 Connected\)](#)

M. Autorisation des flux sur l'interface IPsec

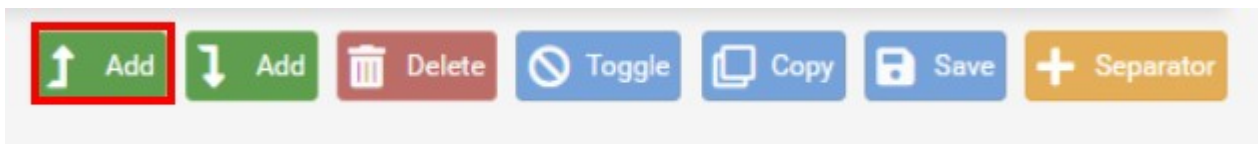
1. **Cliquer sur Firewall** : Dans la barre de menu de pfSense, cliquez sur **Firewall** (1).
2. **Sélectionner Rules** : Dans le menu déroulant, sélectionnez **Rules** (Règles) (2).



Allez dans l'onglet IPsec.



Ajoutez en haut une nouvelle règle.



Choisissez comme Protocol "Any".

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

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

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

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

N'oubliez pas d'enregistrer.

Extra Options

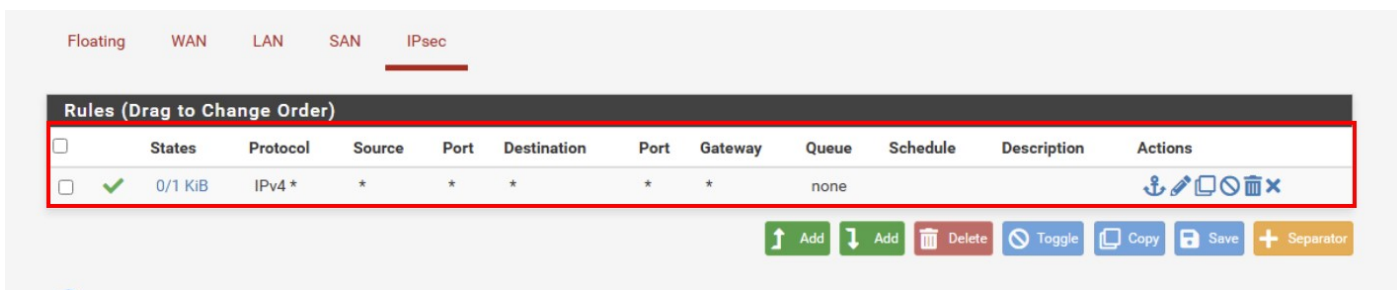
Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

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

Advanced Options Display Advanced

Save

Vous pouvez constater dans les règles IPsec la présence de celui-ci. Cela nous permettra d'autoriser tous les flux entre les deux sites (qui seront d'ailleurs modifié plus tard).



N. Test de la liaison sur les deux sites à l'aide des clients W11

Sur un client du site A, nous essayons de ping le client du site B. Nous pouvons constater que cela fonctionne et que le tunnel est opérationnel.

```
C:\Users\armanabgaryan>ping 192.168.200.2

Envoi d'une requête 'Ping' 192.168.200.2 avec 32 octets de données :
Réponse de 192.168.200.2 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.200.2 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.200.2 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.200.2 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 192.168.200.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Faite le même test sur l'autre site afin d'obtenir la même conclusion.

```
C:\Users\user>ping 192.168.100.1

Envoi d'une requête 'Ping' 192.168.100.1 avec 32 octets de données :
Réponse de 192.168.100.1 : octets=32 temps=2 ms TTL=63
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=63
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=63
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=63

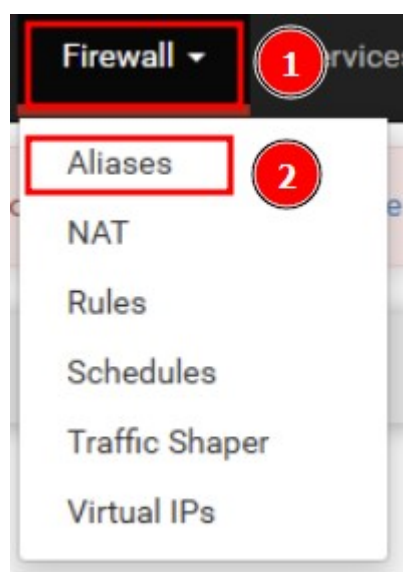
Statistiques Ping pour 192.168.100.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 2ms, Moyenne = 0ms
```

Routeurs / VPN

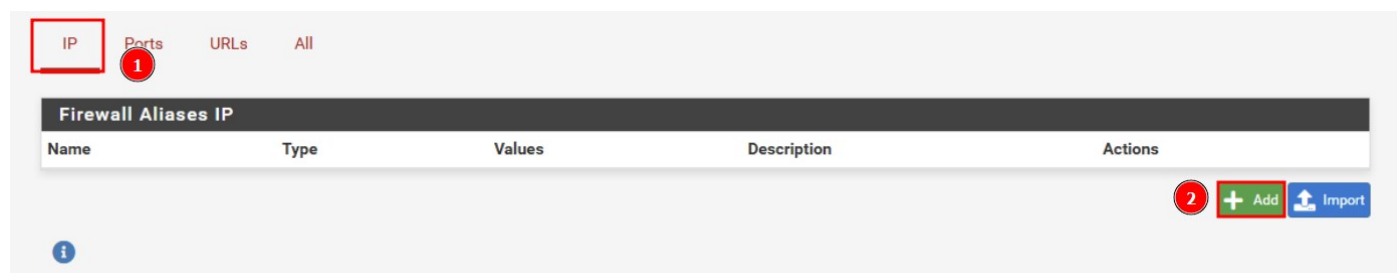
Création des règles du pare-feu

1. Gestion des Alias (Adresses IP et Réseaux)

On accède d'abord au menu **Firewall** > **Aliases**.



On clique sur le bouton "+" (Ajouter) pour créer un nouvel alias.



Alias DC_SITE_A : On définit un nom et on liste les adresses IP spécifiques des machines du site A.

Properties

Name 1

DC_SITE_A

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN 2

192.168.100.200

DC_PRIMAIRE

Delete

3

192.168.100.201

DC_SECONDAIRE

Delete

4

Save

+ Add Host

Alias SAN_SITE_A : Création d'un alias pour le réseau de stockage (SAN) avec ses IP.

Properties

Name 1

SAN_SA

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

192.168.50.2

SAN_PRIMAIRE_SA

2

3

Save

+ Add Host

Alias DC_ALL : Création d'un alias regroupant tous les contrôleurs de domaine (DC) des deux sites.

Properties

Name

DC_ALL

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN			
192.168.100.200	DC_PRIMAIRE_SA	Delete	
192.168.100.201	DC_SECONDAIRE_SA	Delete	
192.168.200.200	DC_PRIMAIRE_SB	Delete	
192.168.200.201	DC_SECONDAIRE_SB	Delete	

Save

Add Host

Alias LAN_SITE_B : Création d'un alias de type réseau pour englober tout le sous-réseau du site B.

Properties

Name

LAN_SITE_B

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

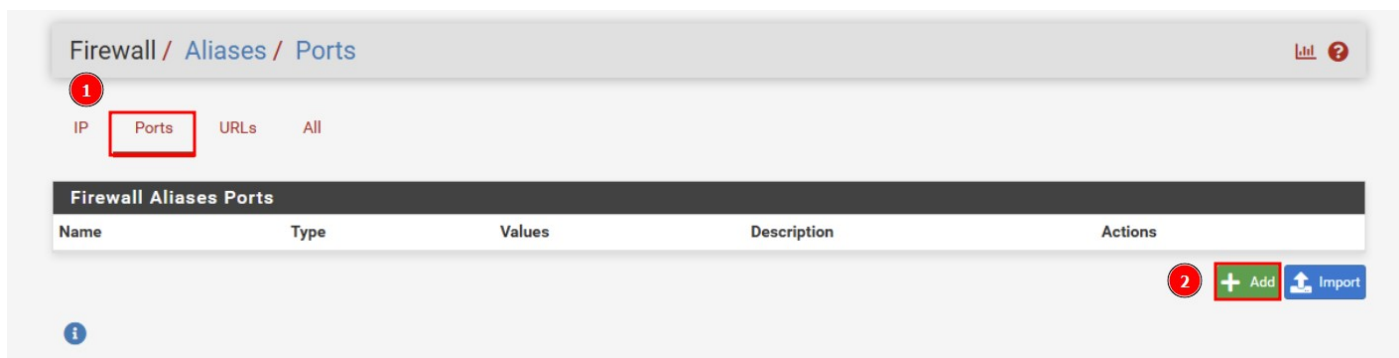
IP or FQDN	Description
192.168.200.0/24	

Save

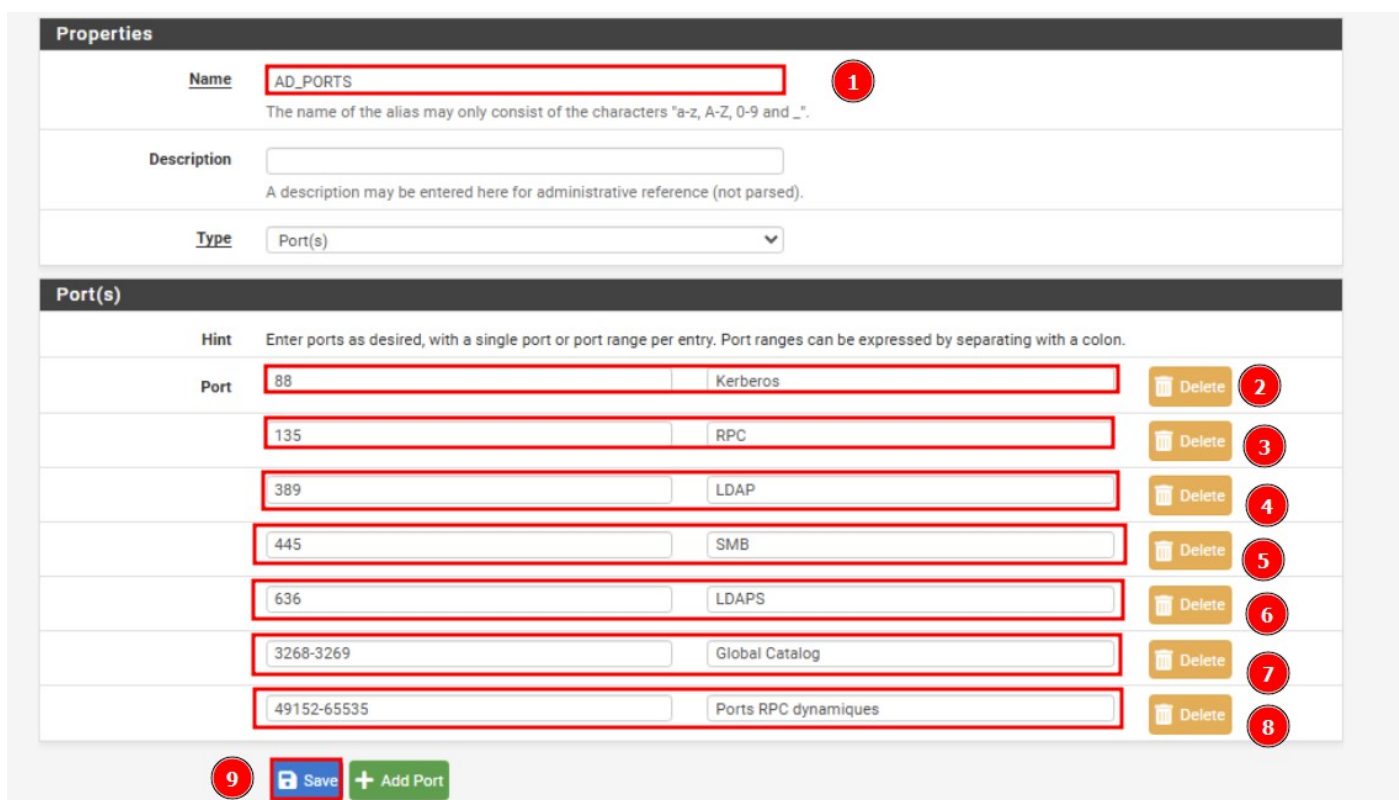
Add Host

2. Gestion des Alias de Ports

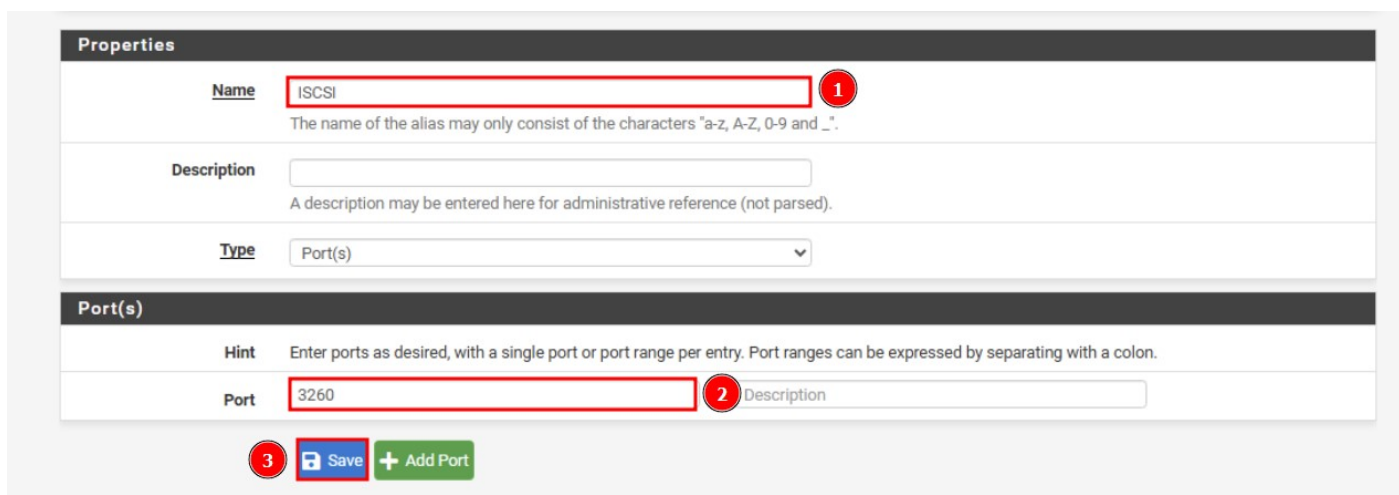
On bascule sur l'onglet **"Ports"** dans la section Aliases.



Alias PORTS_AD : On crée un groupe de ports nécessaires à l'Active Directory. L'encadré montre la liste des ports saisis : **53** (DNS), **88** (Kerberos), **135** (RPC), **389** (LDAP), **445** (SMB), **3268** (Global Catalog) et la plage RPC dynamique (**49152-65535**).

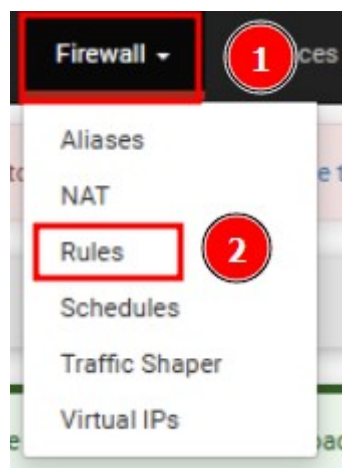


On crée également un alias pour le port ISCSI.

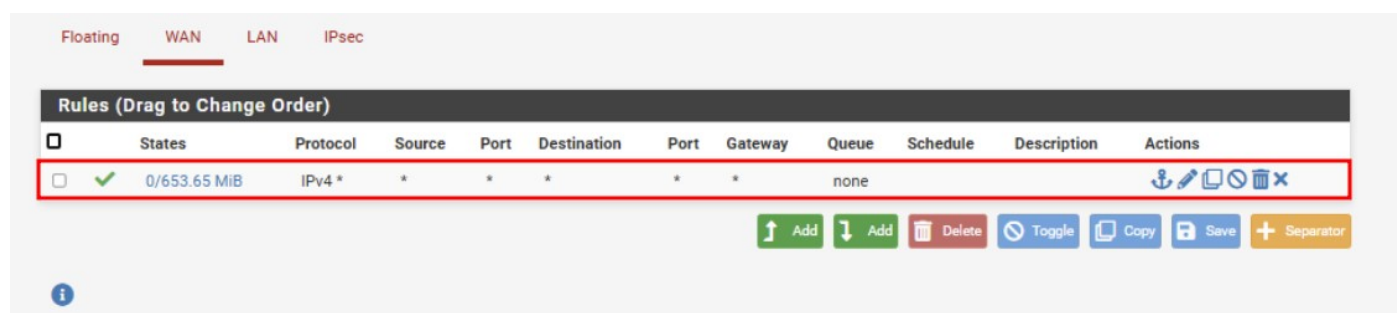


3. Configuration des Règles (Rules)

On se rend dans **Firewall > Rules**.



L'encadré montre une règle autorisant le protocole **IPv4 ICMP** sur l'interface WAN.



Nous allons bloquer toutes les flux de l'interface WAN.

Edit Firewall Rule

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

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

On supprime les règles "portes ouvertes" par défaut du pare-feu pour pouvoir, par la suite, créer ses propres règles beaucoup plus précises et sécurisées

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 11/17.08 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	✓ 9/3.99 GiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

On clique sur le bouton **"Add"** (celui avec la flèche verte pointant vers le bas).

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 3/17.12 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add Add Delete Toggle Copy Save Separator

1. **Action (1)** : On change l'action pour **"Block"**. Cela signifie que le pare-feu va rejeter silencieusement tous les paquets qui correspondent à cette règle.
2. **Protocol (2)** : On sélectionne **"Any"**. La règle s'appliquera donc à absolument tous les types de protocoles (TCP, UDP, ICMP, etc.).
3. **Save (3)** : On clique sur le bouton **"Save"** pour valider et enregistrer cette règle.

Edit Firewall Rule

Action Block 1

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 LAN

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

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol Any 2

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Any Source Address /

Destination

Destination ☐ Invert match Any Destination Address /

Extra Options

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

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

Advanced Options Display Advanced

Save 3

1. **Encadré 1** : On confirme que l'on se trouve bien sur l'onglet de l'interface **LAN**.
2. **Encadré 2** : Ce grand encadré montre la **liste complète et ordonnée des règles** que vous avez créées. Le pare-feu lit cette liste de haut en bas :
 - **Anti-Lockout Rule** : La règle par défaut pour ne pas perdre l'accès à l'interface d'administration.
 - **IPv4 ICMP** : Autorise le "Ping" depuis le LAN vers n'importe où.
 - **IPv4 UDP vers port 67** : Autorise le trafic DHCP vers le contrôleur de domaine (DC_SITE_A).
 - **IPv4 TCP/UDP vers port 53 (DNS)** : Autorise les requêtes DNS.
 - **IPv4 TCP/UDP vers AD_PORTS** : Autorise tous les flux nécessaires à l'Active Directory (en utilisant l'alias de ports créé précédemment).
 - **IPv4 TCP vers SAN_SA** : Autorise le trafic iSCSI vers le réseau de stockage.
 - **La dernière ligne (IPv4 * avec la croix rouge)** : C'est la règle de blocage total que vous avez créée à l'étape précédente. Elle sert de "filet de sécurité" : tout ce qui n'a pas été explicitement autorisé par les règles au-dessus sera bloqué.

Floating **1** LAN IPsec

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	16/20.02 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/3 KiB	IPv4 ICMP any	LAN subnets	*	*	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 UDP	LAN subnets	*	DC_SITE_A	67	*	none			
<input type="checkbox"/>	2/2 KiB	IPv4 TCP/UDP	LAN subnets	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	LAN subnets	*	DC_SITE_A	AD_PORTS	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	*	SAN_SA	ISCSI	*	none			
<input checked="" type="checkbox"/>	0/70 KiB	IPv4 *	*	*	*	*	*	none			

2 Add Add Delete Toggle Copy Save Separator

- Encadré 1 (Haut) :** Vous avez sélectionné l'onglet **IPsec**. Ces règles s'appliquent spécifiquement au trafic qui circule à travers le tunnel VPN entre vos deux sites.
- Encadré 2 (Liste des règles) :** Vous avez défini trois règles cruciales pour la communication inter-sites :
 - **Première règle (AD_PORTS) :** Elle autorise les flux Active Directory entre tous les contrôleurs de domaine (via l'alias DC_ALL) des deux sites. C'est ce qui permet la réplication et l'authentification entre les sites.
 - **Deuxième règle (ICMP) :** Elle autorise le "Ping" (IPv4 ICMP) depuis votre réseau local (LAN subnets) vers le réseau local du site distant (LAN_SITE_B). C'est essentiel pour tester la connectivité entre les deux bureaux.
 - **Troisième règle (La croix rouge) :** C'est une règle de **blocage par défaut**. Elle garantit que tout ce qui n'est pas explicitement autorisé (comme le DNS ou le ping ci-dessus) est interdit de passer par le tunnel VPN.

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

Floating WAN LAN **IPsec** **1**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	DC_ALL	*	DC_ALL	AD_PORTS	*	none			
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	LAN subnets	*	LAN_SITE_B	*	*	none			
<input checked="" type="checkbox"/>	0/8.68 MiB	IPv4 *	*	*	*	*	*	none			

2 Add Add Delete Toggle Copy Save Separator

Répétez l'ensemble de ces étapes sur le second pare-feu (Site B), en adaptant simplement les adresses IP en fonction du plan d'adressage de ce site.

Windows Server Site A

Windows Server Site A

Installation de Windows Server 2022 sur DC1 en mode GUI

Introduction

Ce premier document couvre la procédure d'installation de Windows Server 2022 dans un environnement Proxmox.

1. Préparation d'une VM
2. Installation de Windows
3. Installation des pilotes

Pour ce faire, vous aurez besoin des éléments suivants :

- Image ISO de Windows Server 2022
- Les ressources suivantes disponibles sur votre Hyperviseur
 - processeur 2v
 - 3 Go de RAM
 - 64 Go de stockage
- Une copie des pilotes VirtIO

Pour mener à bien cette procédure, vous devez disposer des accès nécessaires pour créer des Machines Virtuelles dans Proxmox.

1) Préparation d'une VM

Cliquez sur l'option créer une VM dans l'interface d'administration Proxmox.



Sélectionnez ensuite un nom, le pool de ressources approprié pour votre machine, et cliquez sur suivant.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: pve Resource Pool:

VM ID: 113

Name: 1

Start at boot: ☐

Start/Shutdown order: any

Startup delay: default

Shutdown timeout: default

Tags

No Tags +

Help Advanced ☒ Back Next 3

Sur la deuxième page, sélectionnez d'abord votre stockage ISO Proxmox, puis sélectionnez votre ISO de Windows Server déjà préchargée sur votre Hyperviseur. Sélectionnez ensuite les options appropriées dans les paramètres de l'OS Client. Puis, ajoutez l'ISO des drivers en cliquant sur la case à cocher et en sélectionnant l'ISO dans votre bibliothèque.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

☒ Use CD/DVD disc image file (iso)

Storage: ZFS-data 1

ISO image: x64_dvd_4e34897c.iso 2

Guest OS: Microsoft Windows 4

Type: 11/2022/2025 5

Version: 11/2022/2025

☐ Use physical CD/DVD Drive

☐ Do not use any media

☒ Add additional drive for VirtIO drivers 6

Storage: ZFS-data 7

ISO image: virtio-win-0.1.266.iso 8

Advanced ☒ Back Next

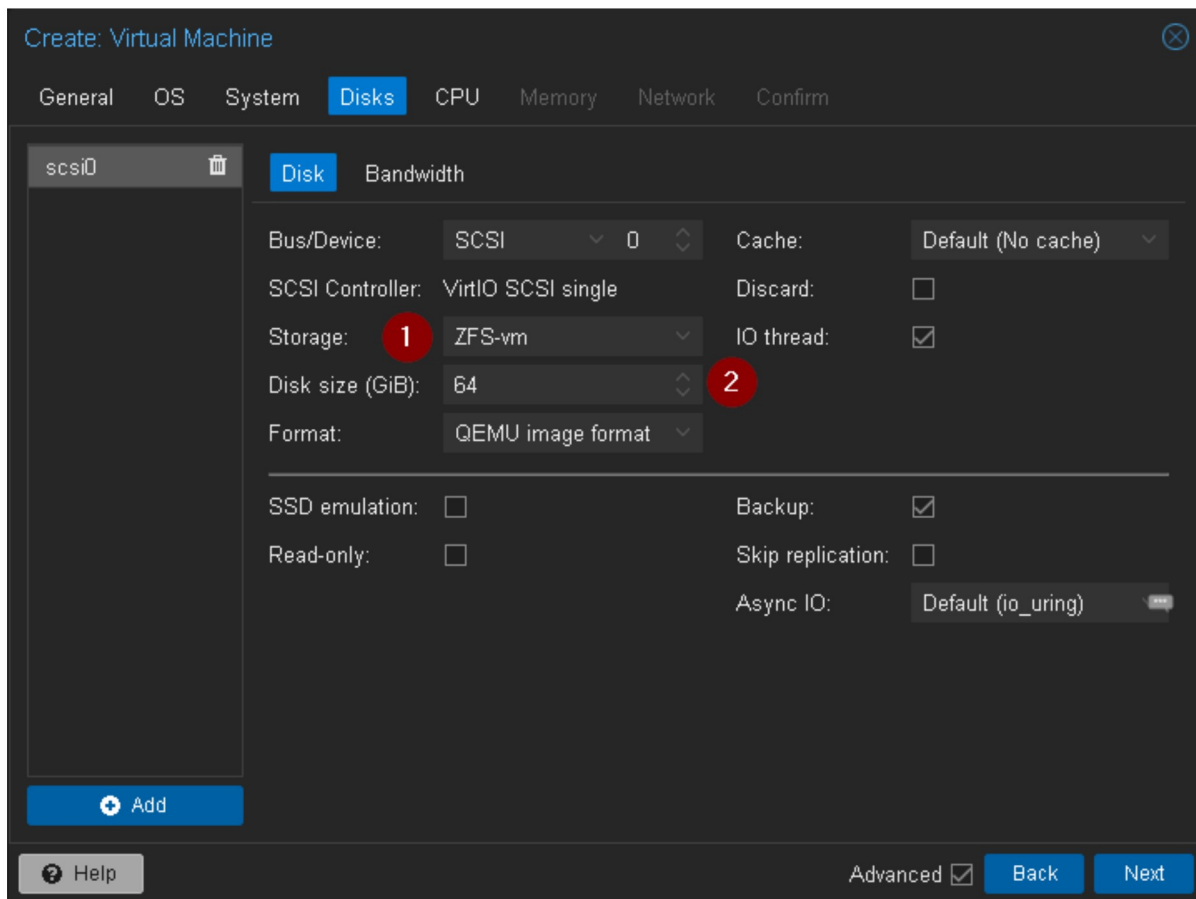
Ajoutez ensuite un espace de Stockage pour la partition EFI et la puce TPM qui sera nécessaire pour l'activation de BitLocker sur vos serveurs. En général, l'espace de stockage est le même que celui utilisé pour stocker l'image disque principale.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'System' tab selected. The 'EFI Storage' dropdown is highlighted with a red circle and the number '1'. The 'TPM Storage' dropdown is highlighted with a red circle and the number '2'. The 'Add TPM' checkbox is checked. The 'Version' dropdown is set to 'v2.0'. The 'Format' dropdown is set to 'QEMU image format (qcow2)'. The 'Pre-Enroll keys' checkbox is checked. The 'Advanced' checkbox is checked. The 'Back' and 'Next' buttons are visible at the bottom right.

Field	Value
Graphic card:	Default
Machine:	q35
SCSI Controller:	VirtIO SCSI single
Qemu Agent:	<input type="checkbox"/>
BIOS:	OVMF (UEFI)
Add TPM:	<input checked="" type="checkbox"/>
EFI Storage:	[Dropdown menu highlighted with red circle 1]
TPM Storage:	[Dropdown menu highlighted with red circle 2]
Version:	v2.0
Format:	QEMU image format (qcow2)
Pre-Enroll keys:	<input checked="" type="checkbox"/>

Help Advanced ☒ Back Next

Dans la page de sélection du disque virtuel principal, choisissez l'emplacement de stockage de l'image disque et augmentez la taille du disque à votre convenance. Cliquez sur "Add" pour ajouter des disques secondaires.



Dans la page CPU, ajoutez un Socket à votre machine virtuelle et sélectionnez le Type "x86-64-v2-AES" s'il n'est pas sélectionné par défaut.

Si votre hyperviseur dispose de deux CPU physiques, vous pouvez activer l'option NUMA.

Create: Virtual Machine

GeneralOSSystemDisksCPUMemoryNetworkConfirm

Sockets: 1 2

Type: 2 x86-64-v2-AES

Cores: 1

Total cores: 2

VCPUs: 2

CPU units: 100

CPU limit: unlimited

Enable NUMA: ☒ 3

CPU Affinity: All Cores

Extra CPU Flags:

Default	-	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	md-clear	Required to let the guest OS know if MDS is mitigated correctly
Default	-	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	pcid	Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default	-	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	spec-ctrl	Allows improved Spectre mitigation with Intel CPUs
Default	-	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	ssbd	Protection for "Speculative Store Bypass" for Intel models
Default	-	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	ibpb	Allows improved Spectre mitigation with AMD CPUs
Default	-	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	virt-ssbd	Basis for "Speculative Store Bypass" protection for AMD models

Help

Advanced ☒

Back

Next

Dans la page Mémoire, sélectionnez un montant de RAM entre 3 et 4 go minimum. En fonction de votre utilisation, il faudra allouer de la mémoire en plus. Sélectionnez ensuite la même quantité de mémoire minimale ou désactivez l'option de Ballooning.

Create: Virtual Machine

General OS System Disks CPU **Memory** Network Confirm

Memory (MiB): 4096 1

Minimum memory (MiB): 4096 2

Shares: Default (1000)

Ballooning Device: ☒ 3

Help Advanced ☒ Back Next

Configurez ensuite la carte réseau selon votre infrastructure. Sélectionnez la carte réseau VirtIO dans la rubrique "Modèle"

Create: Virtual Machine

General OS System Disks CPU Memory **Network** Confirm

☐ No network device

Bridge: 1 vmbri0 Model: 2 VirtIO (paravirtualized)

VLAN Tag: no VLAN MAC address: auto

Firewall: ☒

Disconnect: ☐ Rate limit (MB/s): unlimited

MTU: 1500 (1 = bridge MTU) Multiqueue:

Help Advanced ☒ Back Next

Vérifiez votre configuration et cliquez sur le bouton FINISH.

Create: Virtual Machine

General

OS

System

Disks

CPU

Memory

Network

Confirm

Key ↑	Value
cores	1
cpu	x86-64-v2-AES
ide2	ZFS-data:iso/fr-fr_windows_server_2022_updated_nov_2024_x64_dvd_4e34897c.iso,med...
memory	2048
net0	virtio,bridge=vmbr0,firewall=1
nodename	pve
numa	0
ostype	l26
scsi0	ZFS-retro:32,iotread=on
scsihw	virtio-scsi-single
sockets	1
vmid	113

☐ Start after created

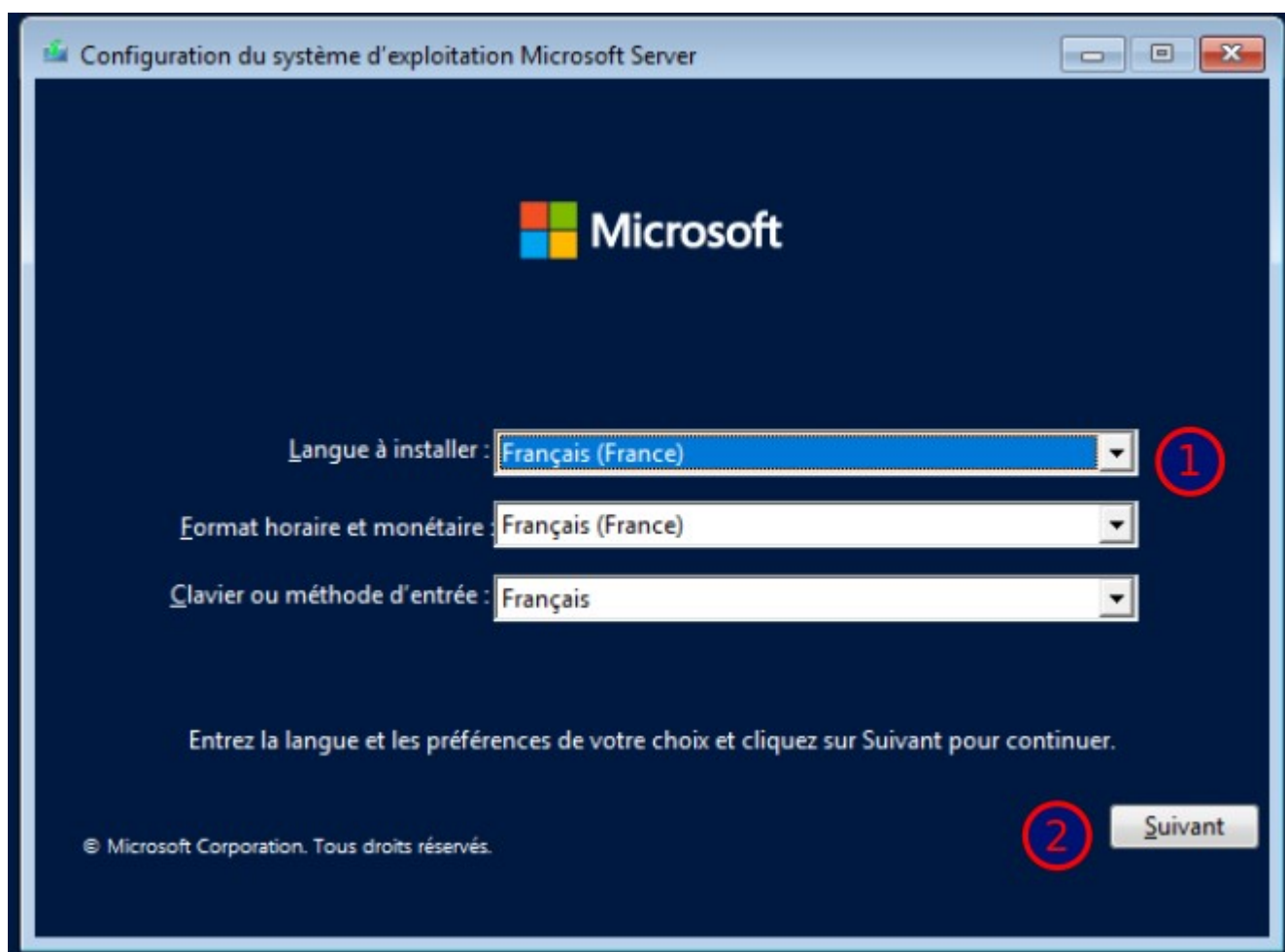
Advanced ☒

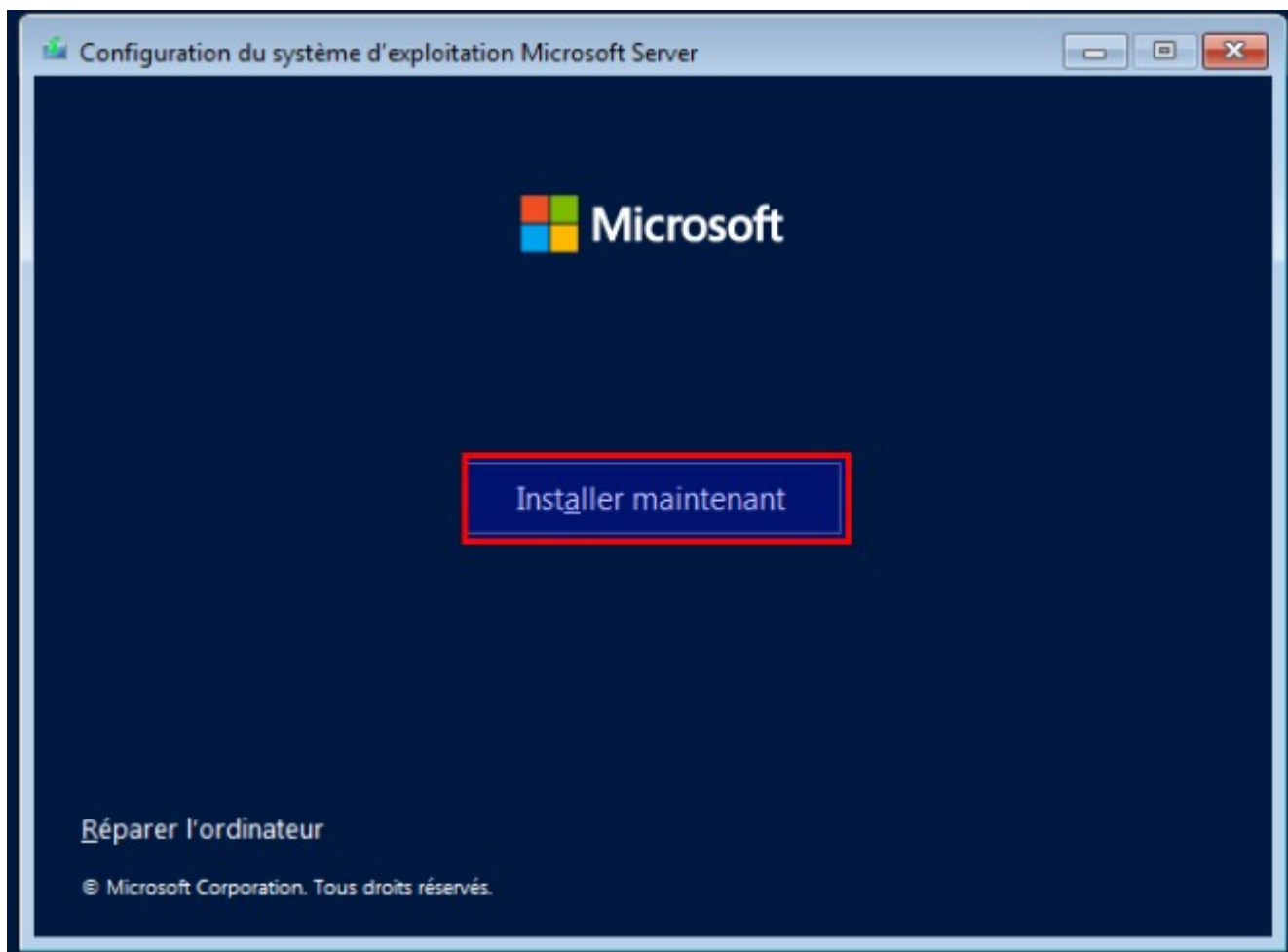
Back

Finish

2) Installation de Windows Server 2022

Une fois la VM lancée sur l'ISO de Windows Server, sélectionnez la langue (Français) et cliquez sur suivant.





Sélectionnez bien "Je n'ai pas de clé de produit"

Activer la configuration du système d'exploitation Microsoft Server

Si vous installez le système d'exploitation Microsoft Server pour la première fois sur cet ordinateur (ou si vous installez une autre édition), vous devez entrer une clé de produit valide pour le système d'exploitation Microsoft Server. Votre clé de produit doit figurer dans le courrier de confirmation que vous avez reçu après l'achat d'une copie numérique du système d'exploitation Microsoft Server ou sur une étiquette fournie dans la zone du système d'exploitation Microsoft Server.

La clé de produit (Product Key) ressemble à ceci : XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Si vous réinstallez le système d'exploitation Microsoft Server, sélectionnez je ne dispose pas d'une clé de produit. Votre copie du système d'exploitation Microsoft Server sera automatiquement



[Déclaration de confidentialité](#)

[Je n'ai pas de clé de produit \(Product Key\)](#)

[Suivant](#)

Sélectionnez « Windows Server 2022 Standard (expérience de bureau) » et continuez

Sélectionner le système d'exploitation à installer

Système d'exploitation	Architecture	Date de modi...
Windows Server 2022 Standard	x64	07/08/2021
Windows Server 2022 Standard (expérience de bureau)	x64	07/08/2021
Windows Server 2022 Datacenter	x64	07/08/2021
Windows Server 2022 Datacenter (expérience de bureau)	x64	07/08/2021

1

Description :

Cette option installe l'environnement graphique Windows complet, qui utilise de l'espace disque supplémentaire. Il peut être utile si vous souhaitez utiliser le bureau Windows ou une application qui en a besoin.

2

Suivant

Avis et conditions du contrat de licence applicables

VOUS DEVEZ ACCEPTER LES TERMES DE LA LICENCE DU LOGICIEL. VOIR CI-APRÈS. Veuillez lire les conditions de licence complètes fournies à l'adresse (aka.ms/useterms).

NOTIFICATION IMPORTANTE

Informations relatives à l'utilisation et au diagnostic. Microsoft recueille ces informations sur Internet pour assurer la sécurité et la mise à jour de Windows, diagnostiquer les problèmes et apporter des améliorations aux produits, et peut associer ces informations à votre organisation. Les systèmes d'exploitation des serveurs Microsoft peuvent être configurés pour désactiver les données de diagnostic, envoyer des données de diagnostic obligatoires ou envoyer des données de diagnostic facultatives. Le réglage par défaut consiste à envoyer les données de diagnostic requises. Les données de diagnostic requises

1

☒ J'accepte les termes du contrat de licence logiciel Microsoft. Si la licence appartient à une organisation, je suis autorisé à agir en son nom.

2

Suivant

Choisissez l'option personnalisée.

Quel type d'installation voulez-vous effectuer ?

Mise à jour : Installer le système d'exploitation Microsoft Server et conserver les fichiers, les paramètres et les applications.

Avec cette option, les fichiers, paramètres et applications sont déplacés vers le nouveau système d'exploitation. Cette option est disponible uniquement lorsqu'une version prise en charge du système d'exploitation est déjà en cours d'exécution sur l'ordinateur.

Personnalisé : installer uniquement le système d'exploitation Microsoft Server (avancé)

Avec cette option, les fichiers, les paramètres et les applications ne sont pas déplacés vers le nouveau système d'exploitation. Pour modifier les partitions et les lecteurs, démarrez l'ordinateur à l'aide du disque d'installation. Nous vous recommandons de sauvegarder vos fichiers avant de continuer.

Où voulez-vous installer le système d'exploitation ?

Nom	Taille totale	Espace libre	Type

 Actualiser Supprimer Formater Nouveau

1

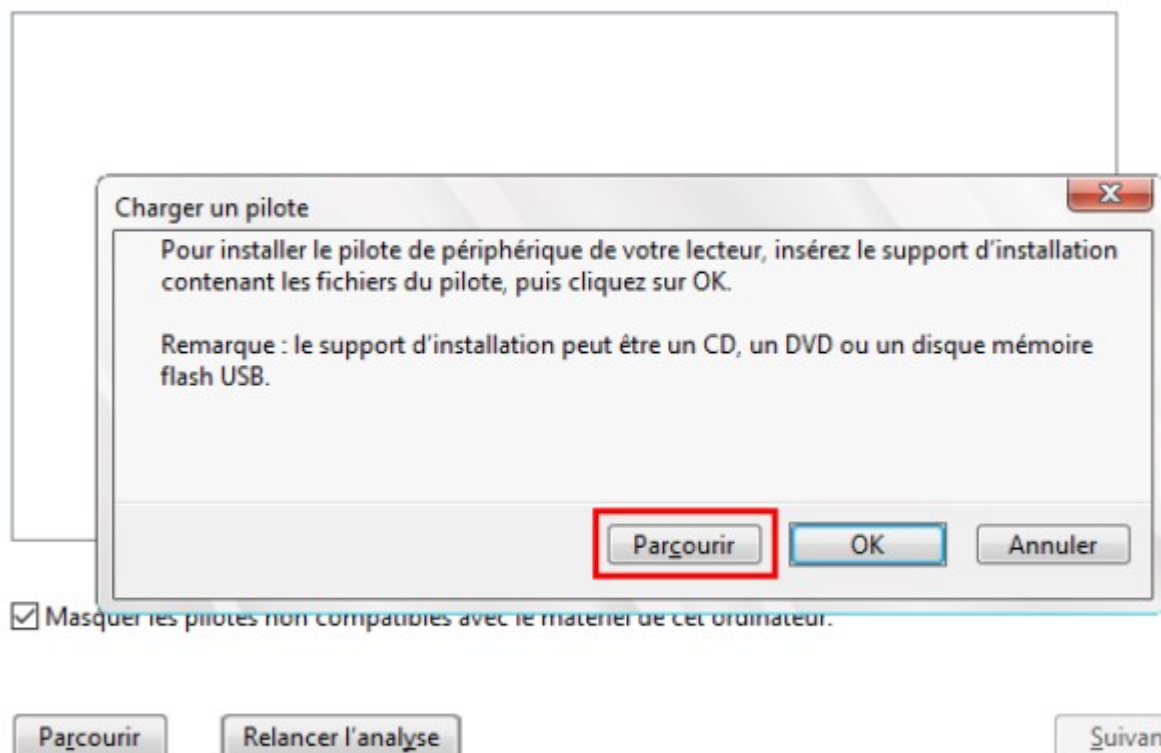
 Charger un pilote Étendre

Nous n'avons trouvé aucun lecteur. Pour obtenir un pilote de stockage, cliquez sur Charger un pilote.

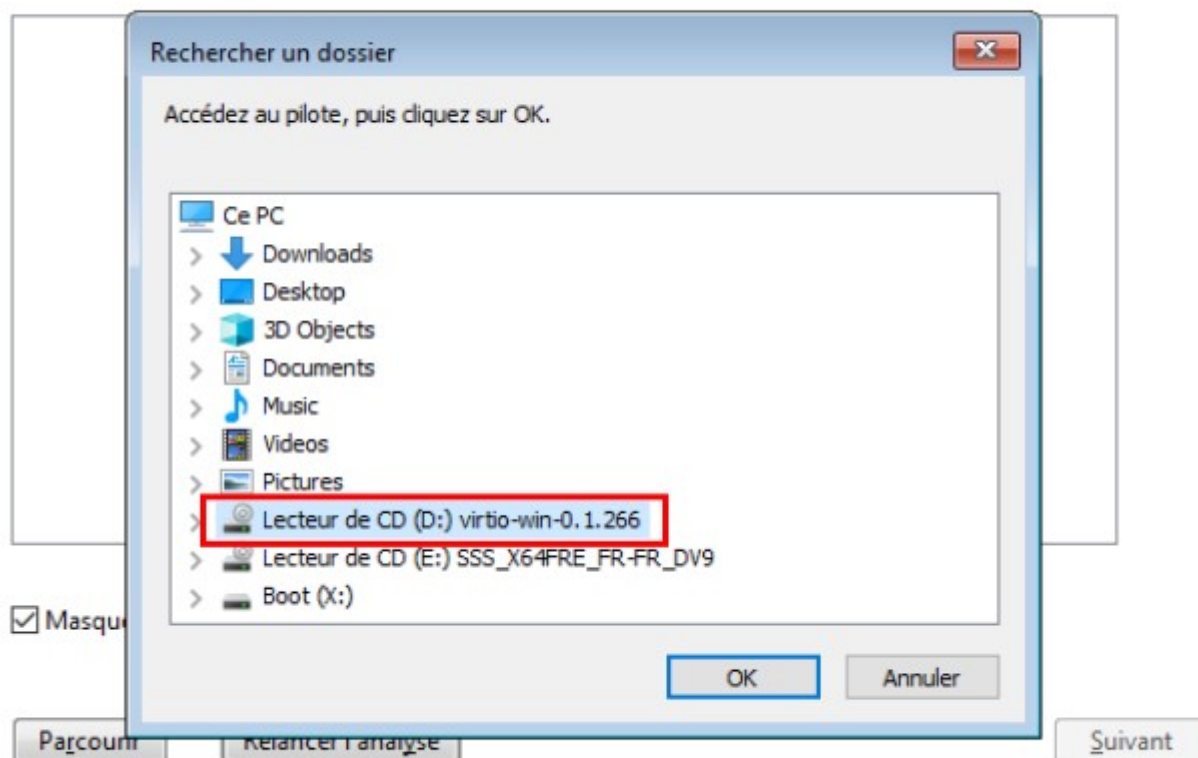
2

Suivant

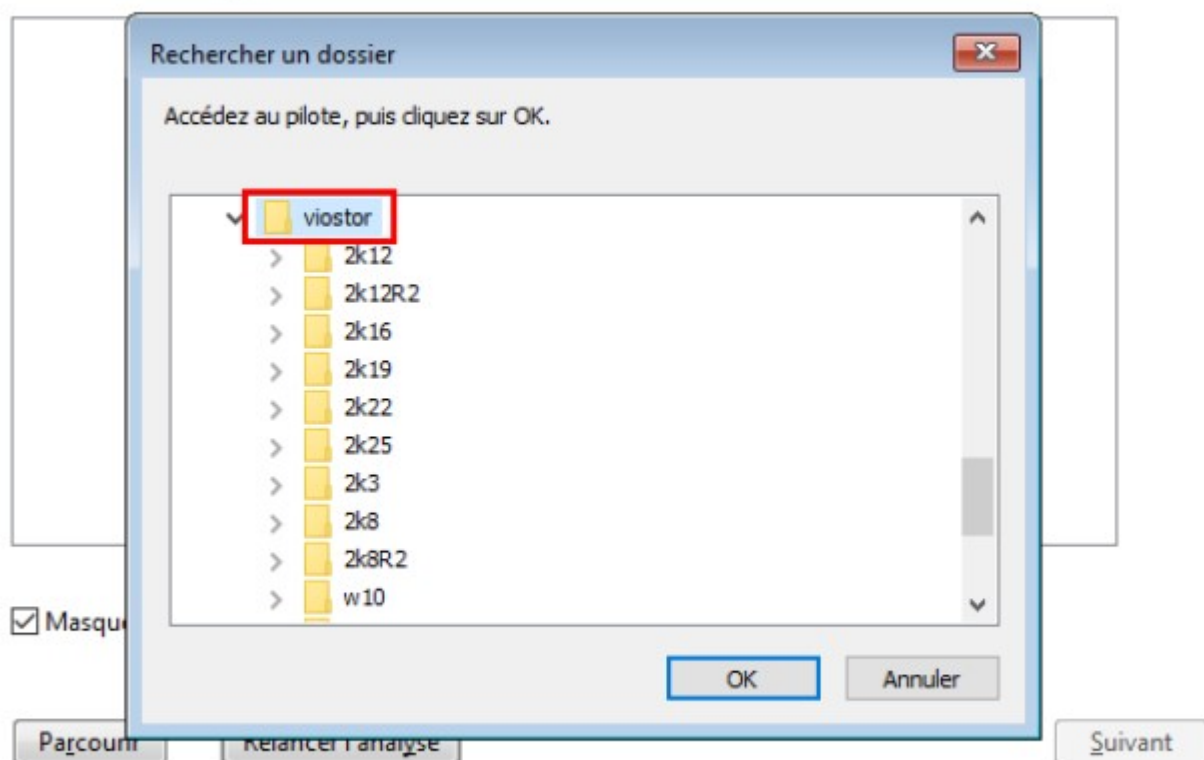
Sélectionner le pilote à installer



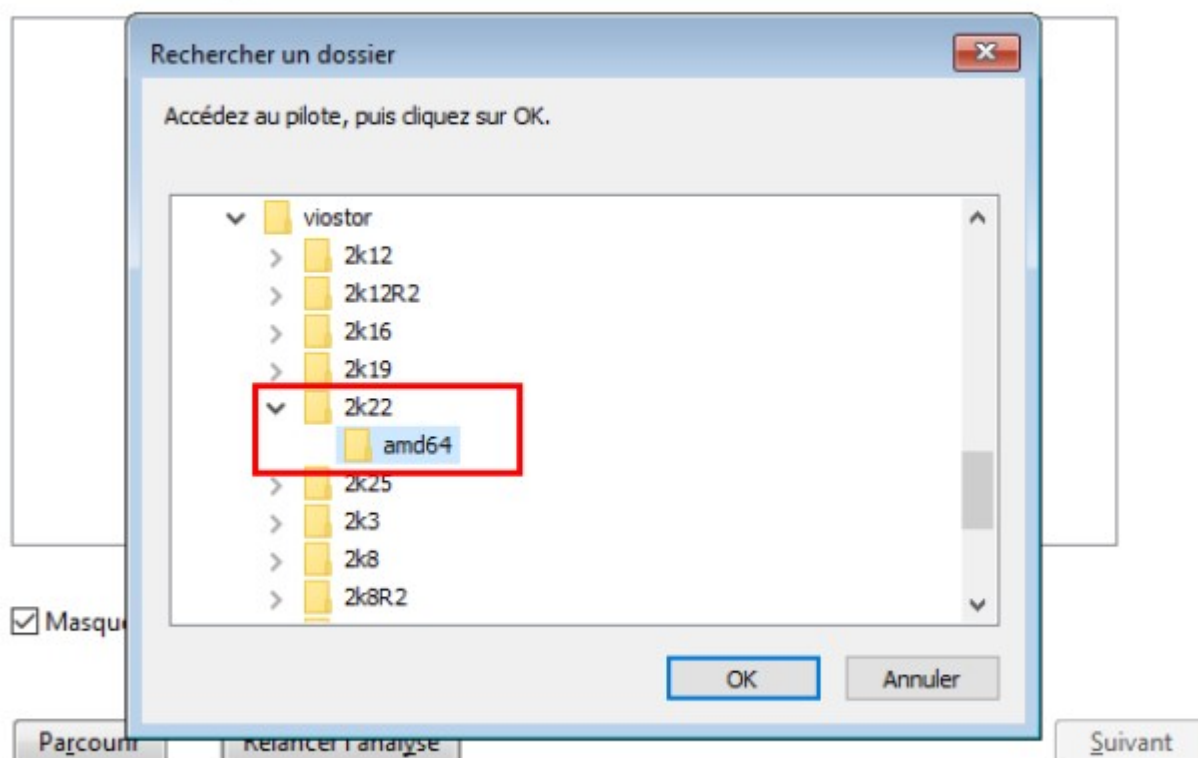
Sélectionner le pilote à installer



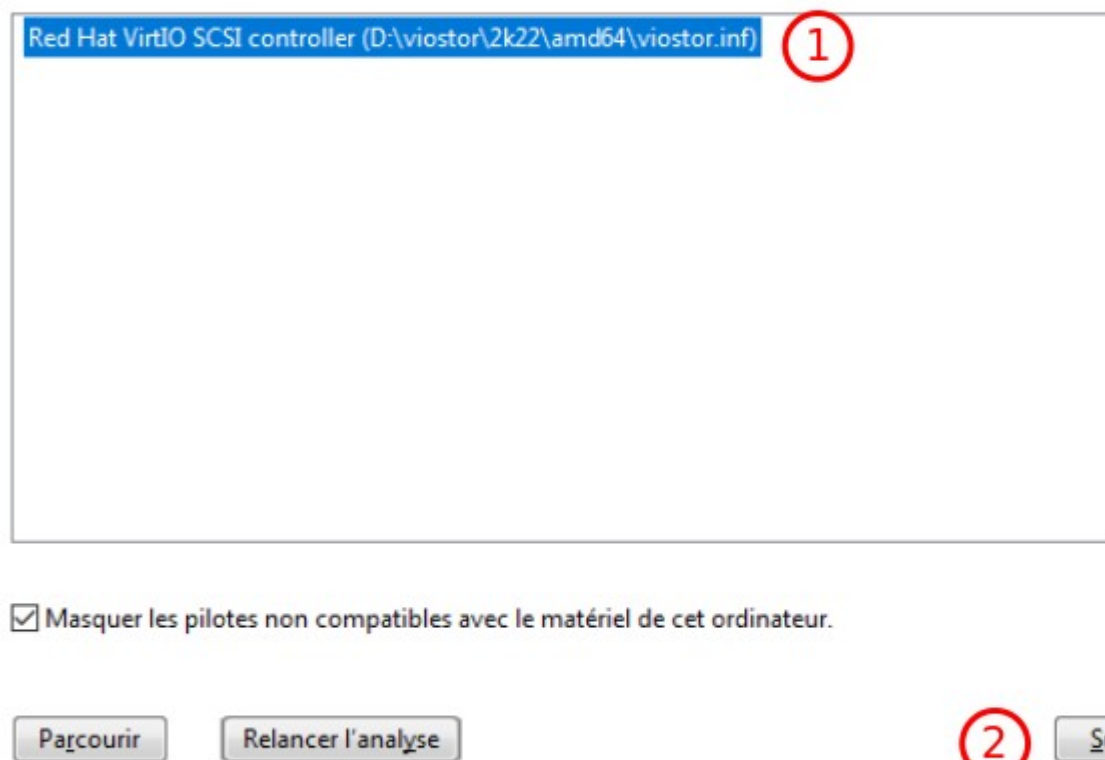
Sélectionner le pilote à installer




Sélectionner le pilote à installer

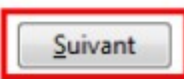


Sélectionner le pilote à installer



Où voulez-vous installer le système d'exploitation ?

	Nom	Taille totale	Espace libre	Type
	Lecteur 0 Espace non alloué	64.0 Go	64.0 Go	

 Actualiser Supprimer Formater Nouveau Charger un pilote Étendre Suivant

Paramètres de personnalisation

Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.

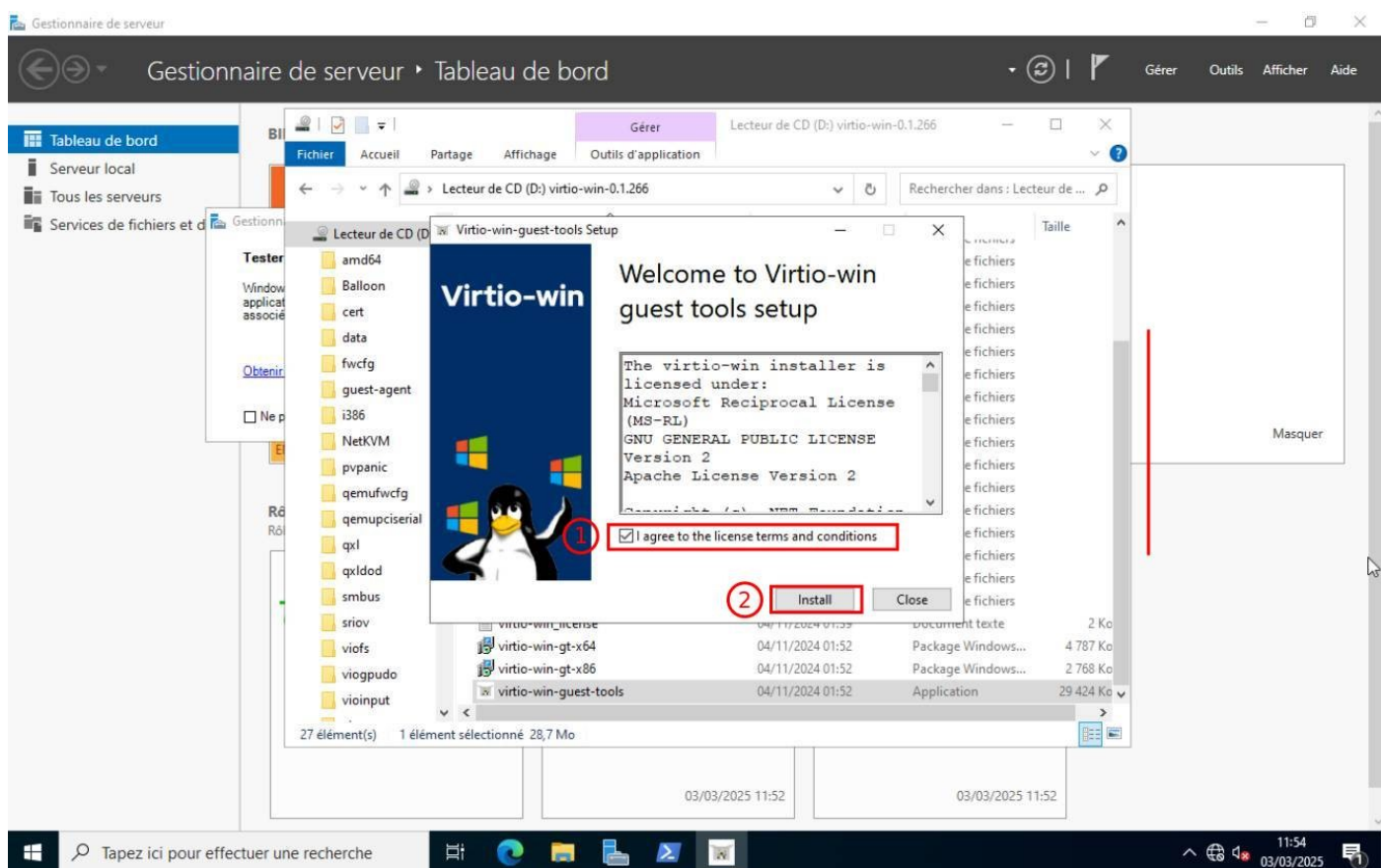
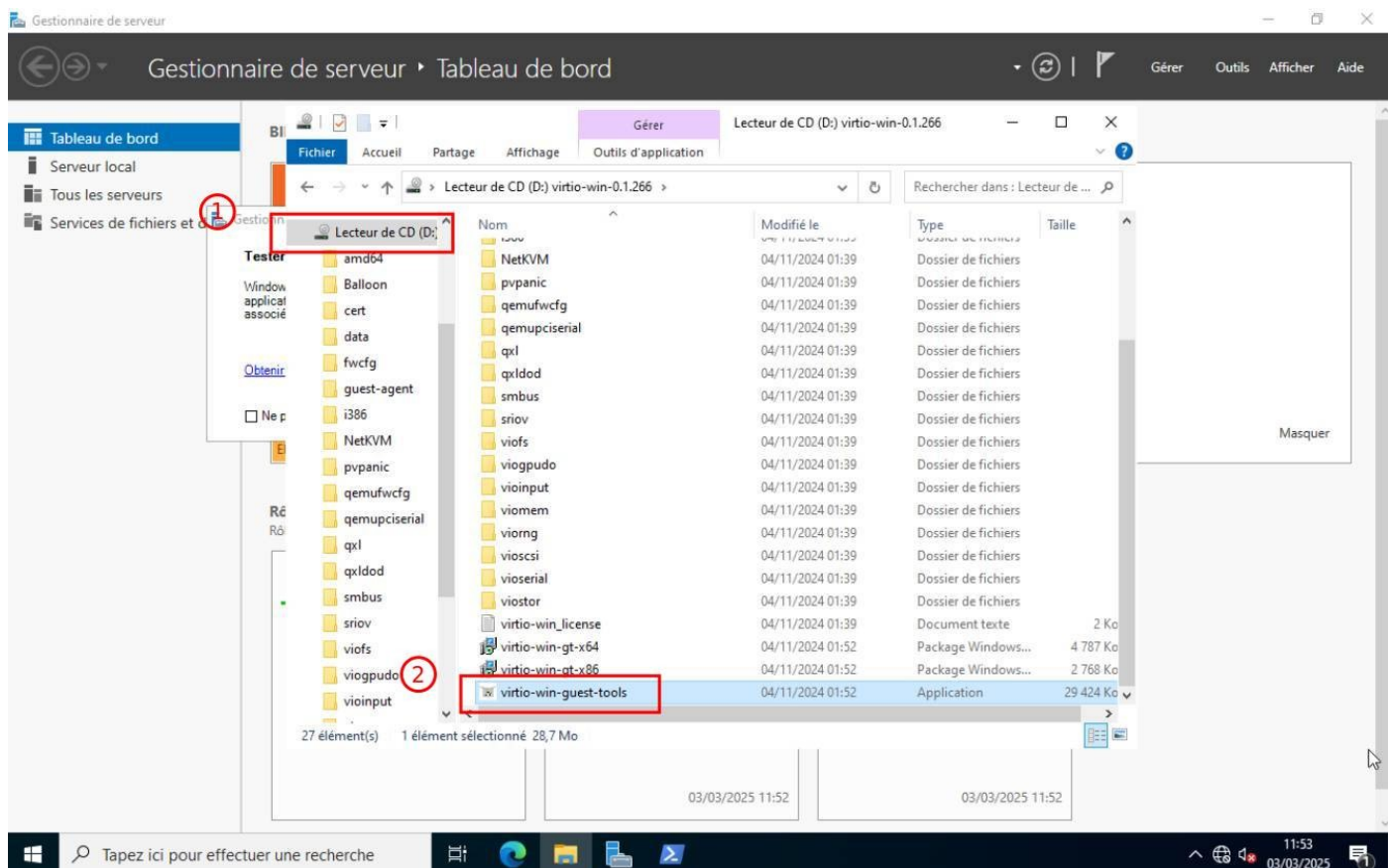
Nom d'utilisateur

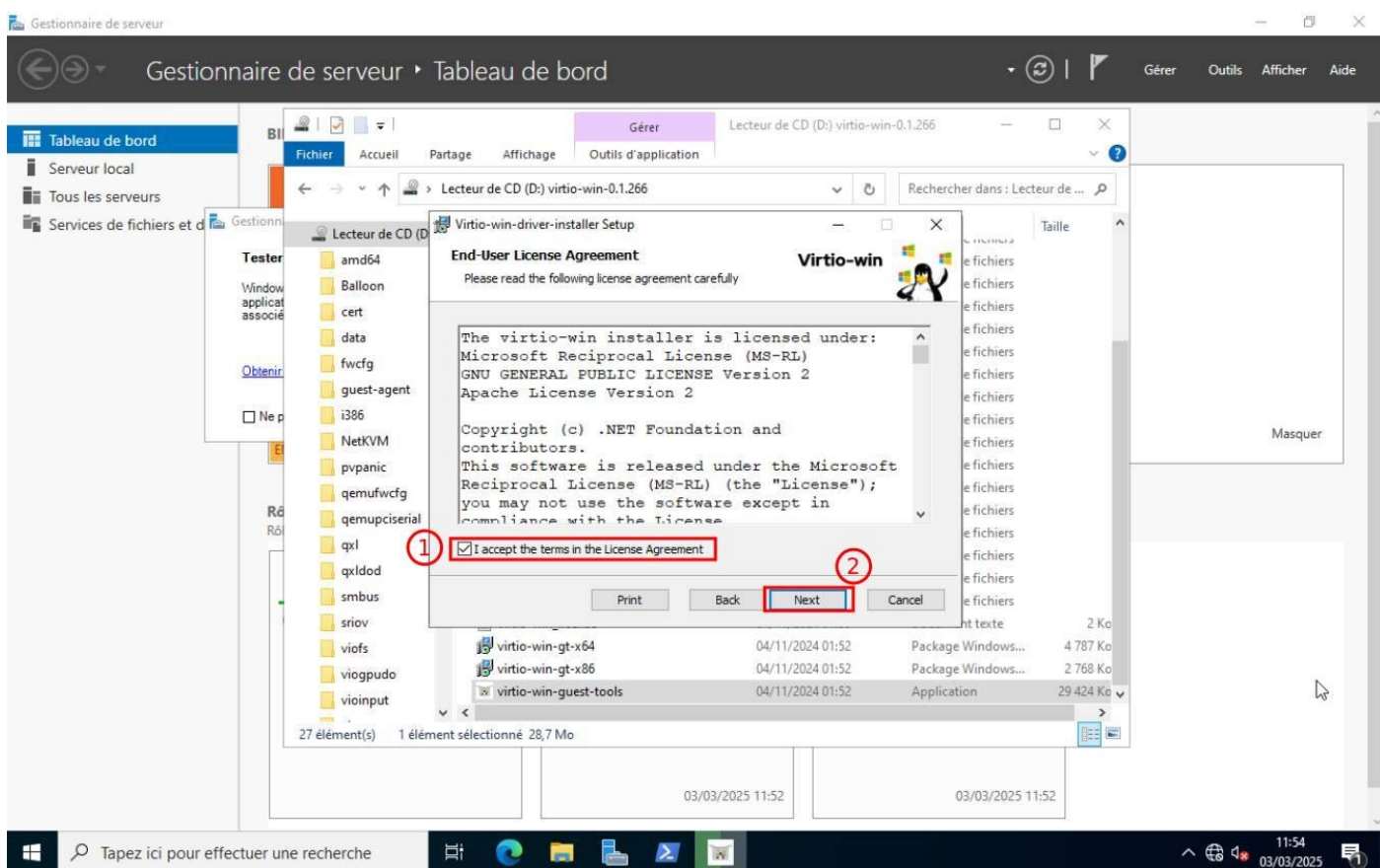
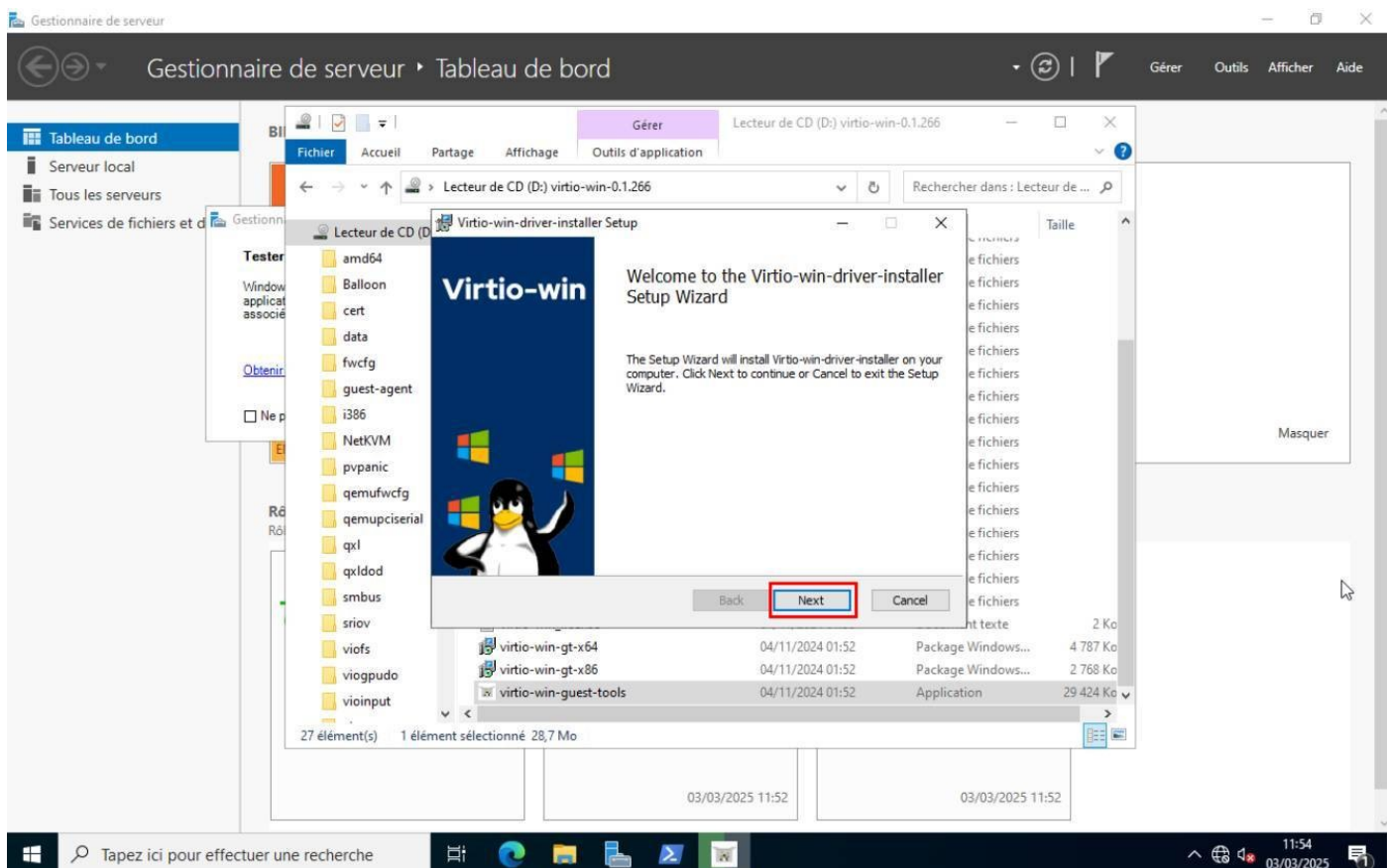
Administrateur

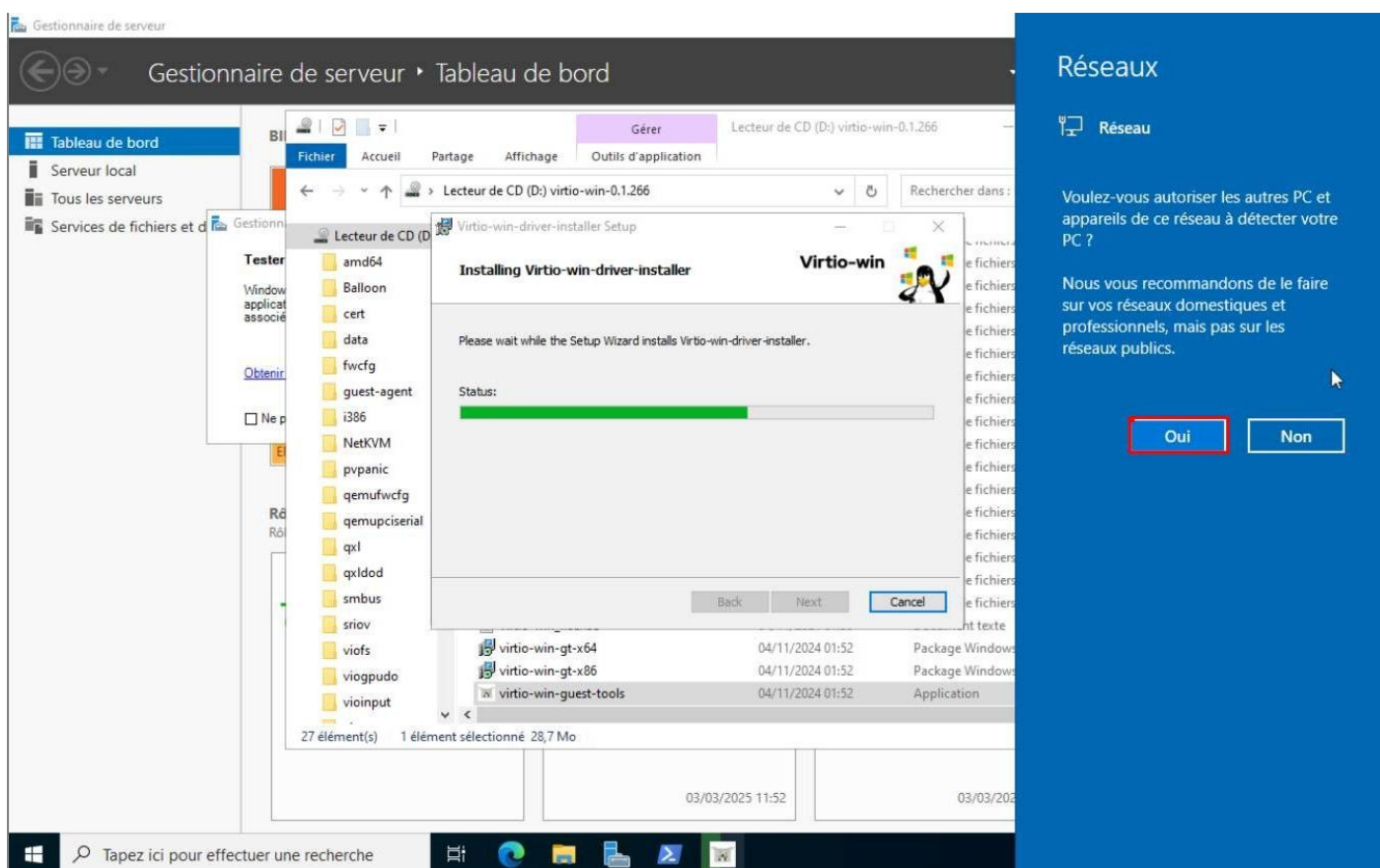
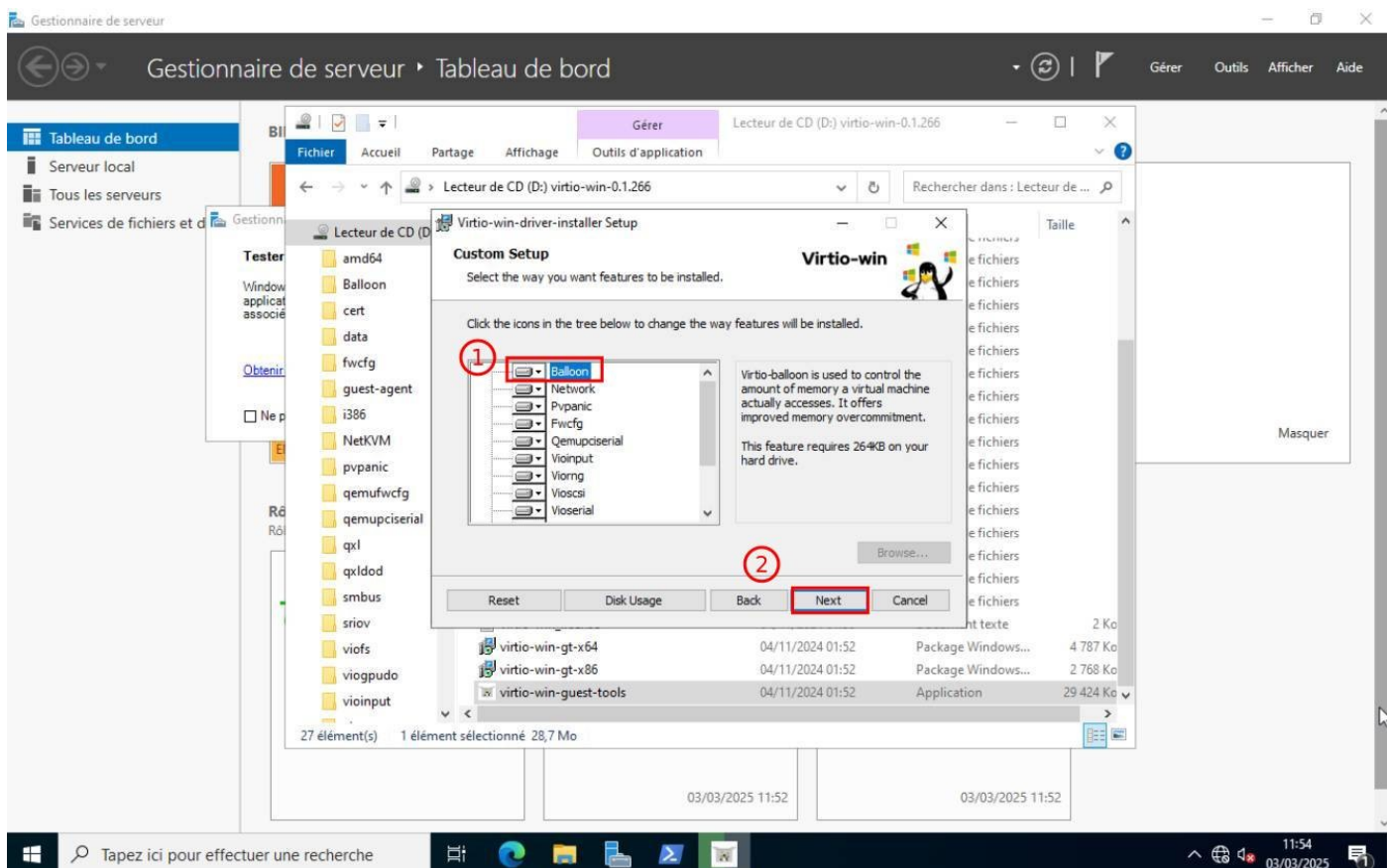
Mot de passe

Entrez de nouveau le
mot de passe

Terminer







Réseaux

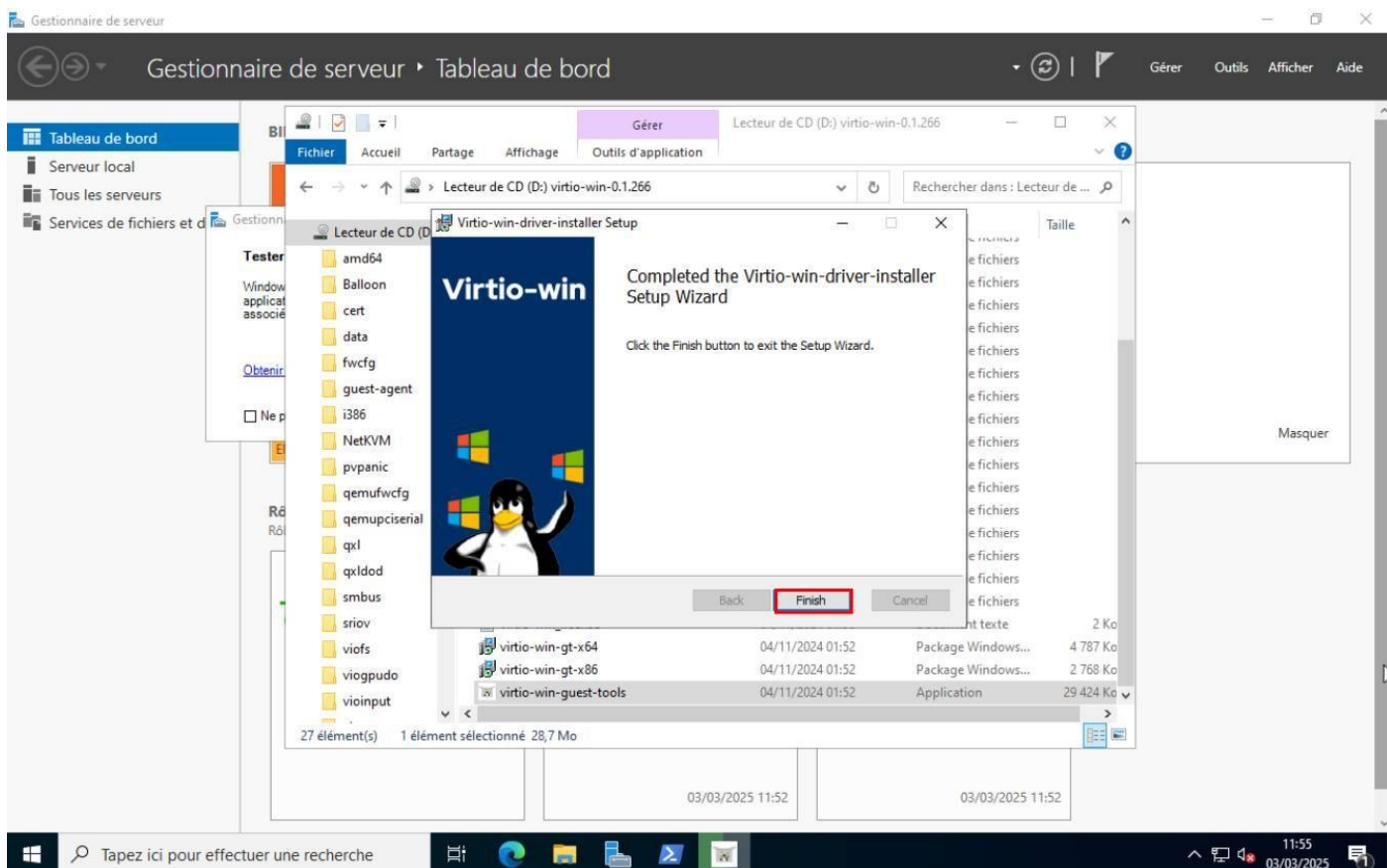
Réseau

Voulez-vous autoriser les autres PC et appareils de ce réseau à détecter votre PC ?

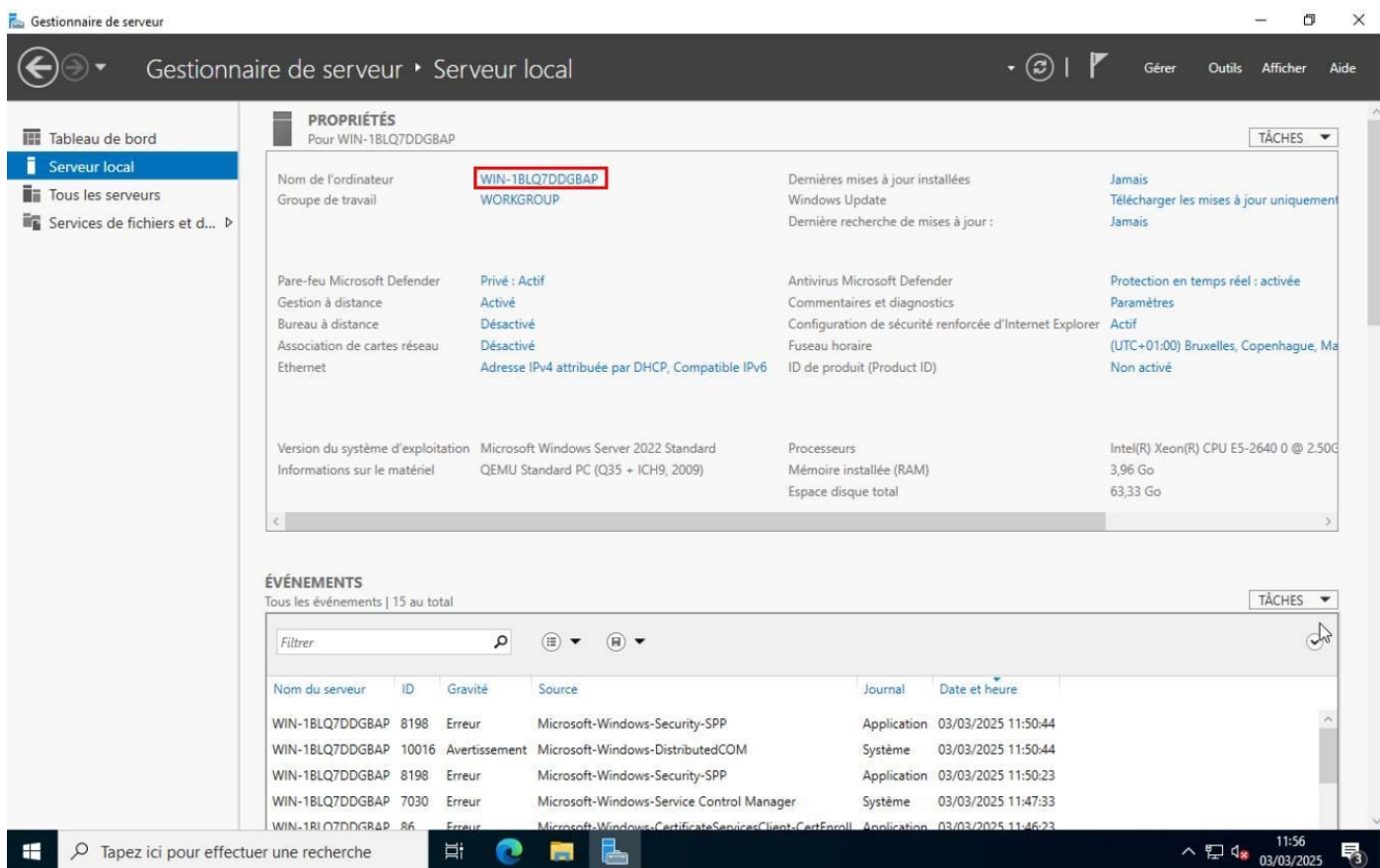
Nous vous recommandons de le faire sur vos réseaux domestiques et professionnels, mais pas sur les réseaux publics.

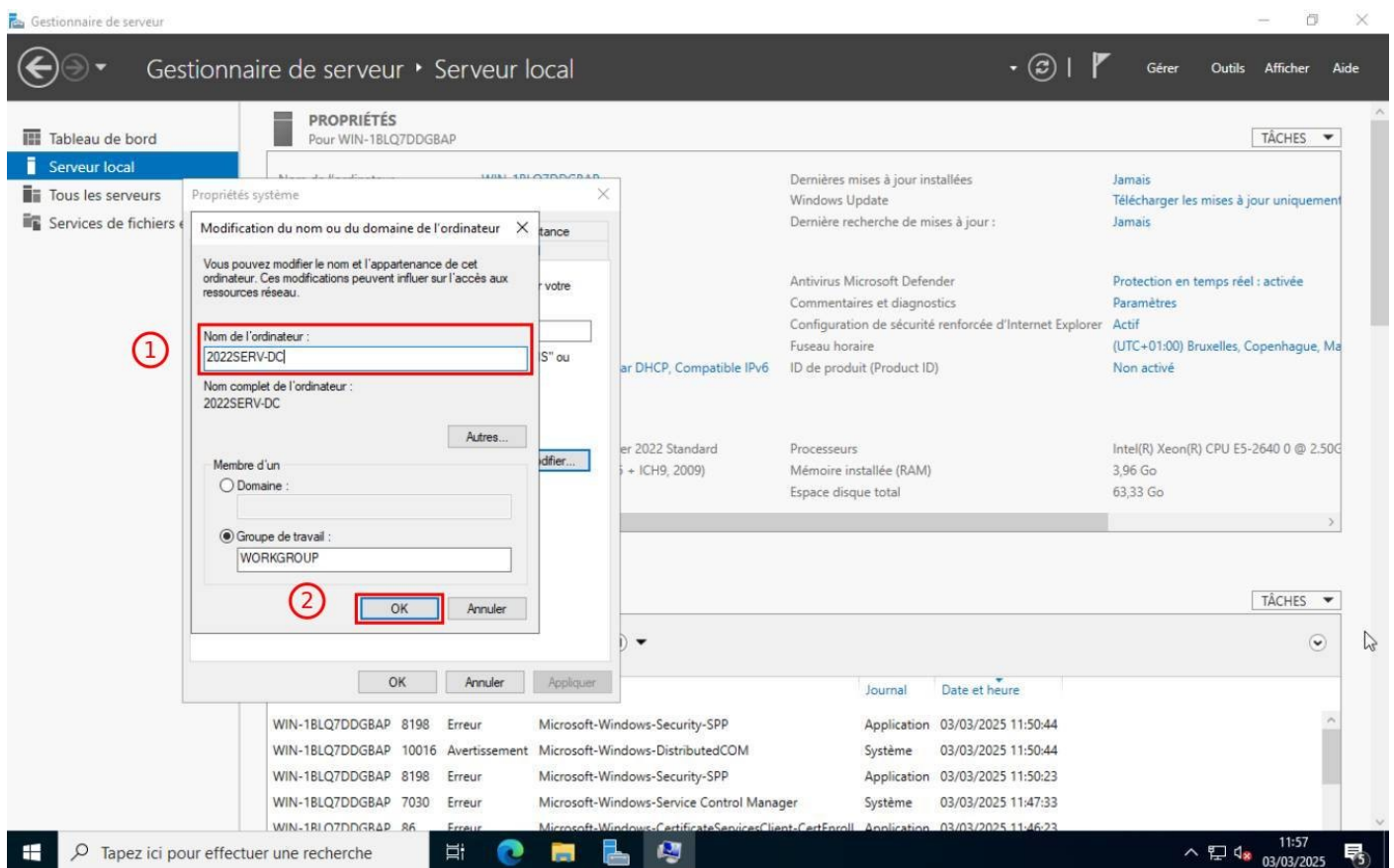
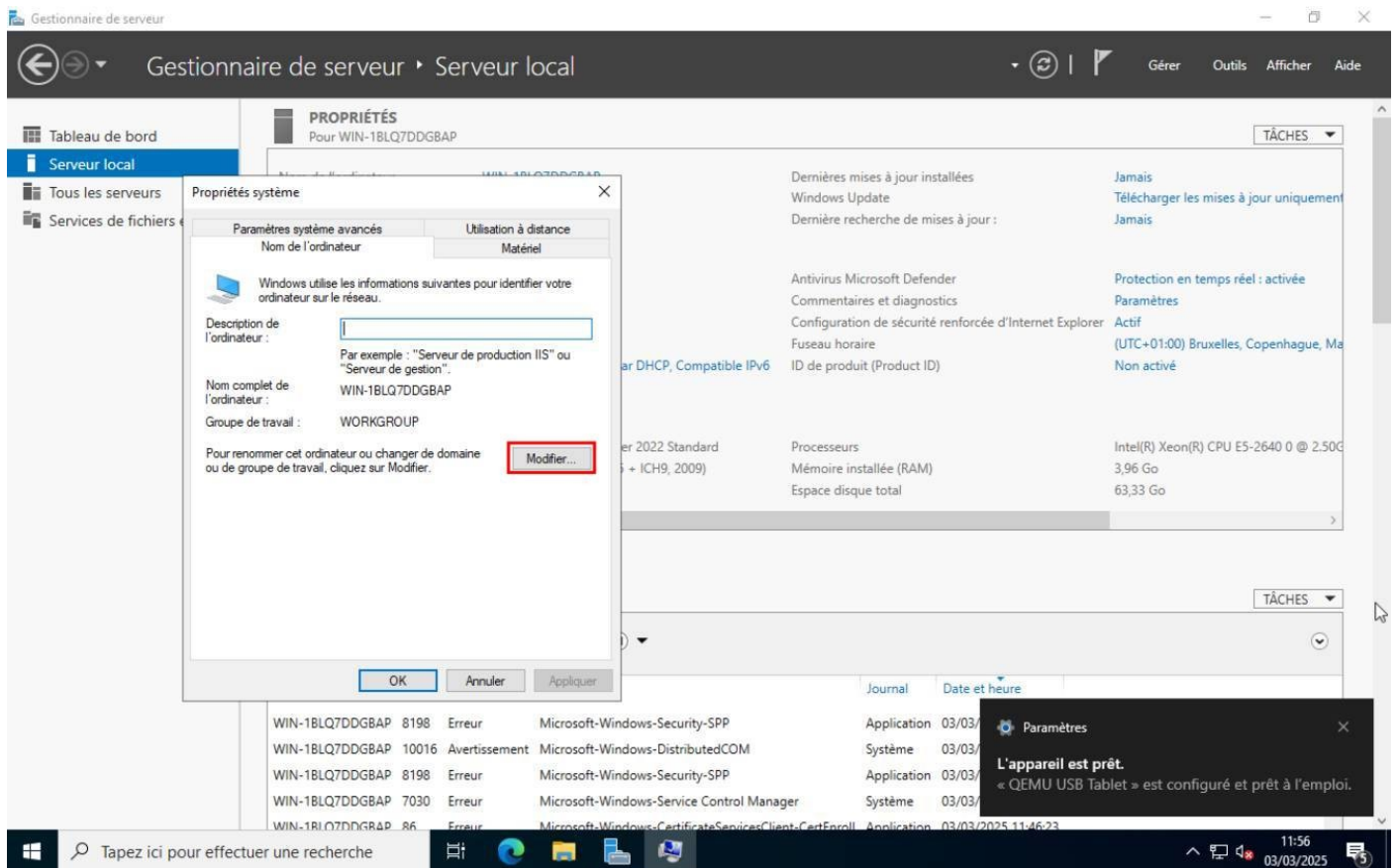
Oui

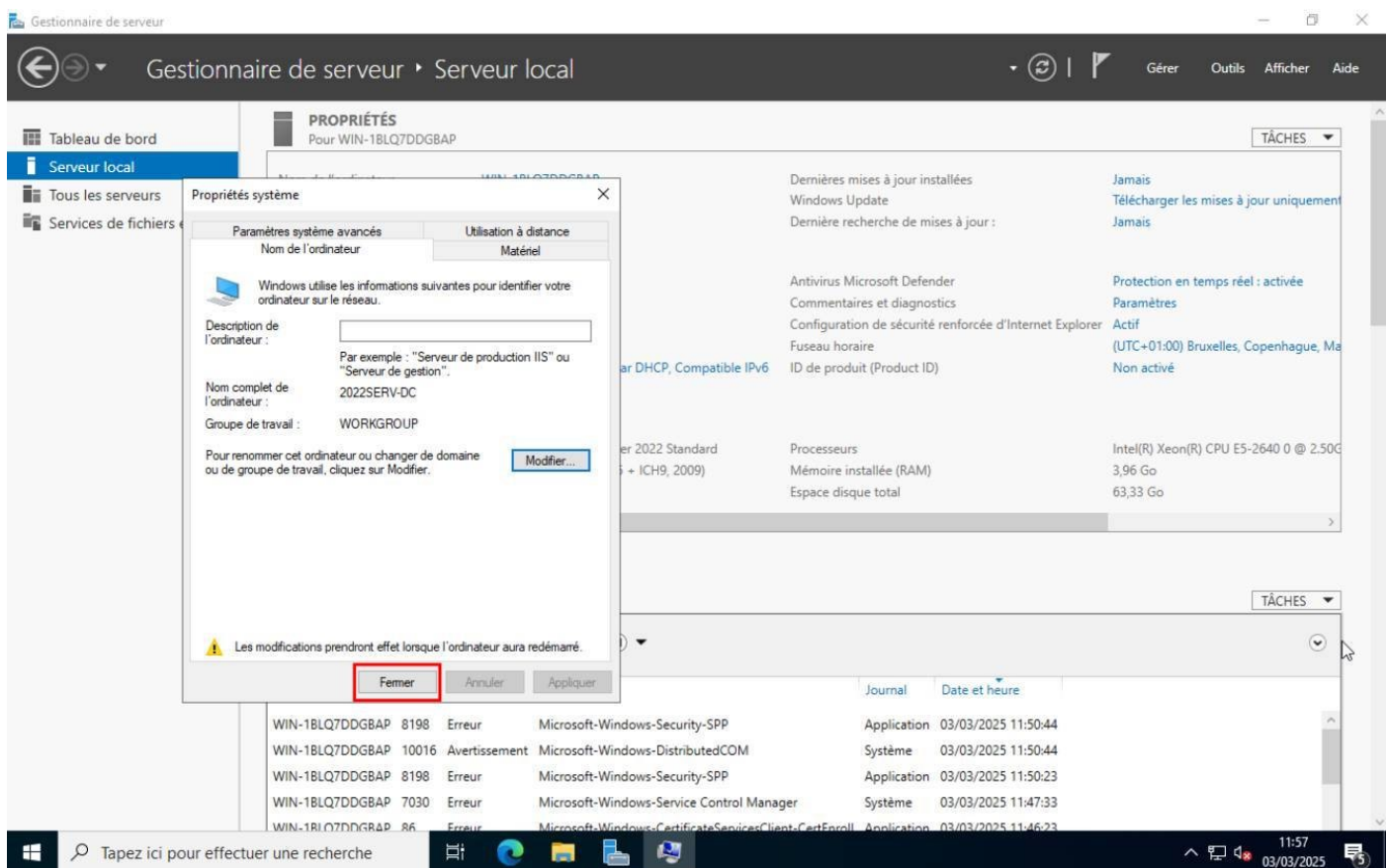
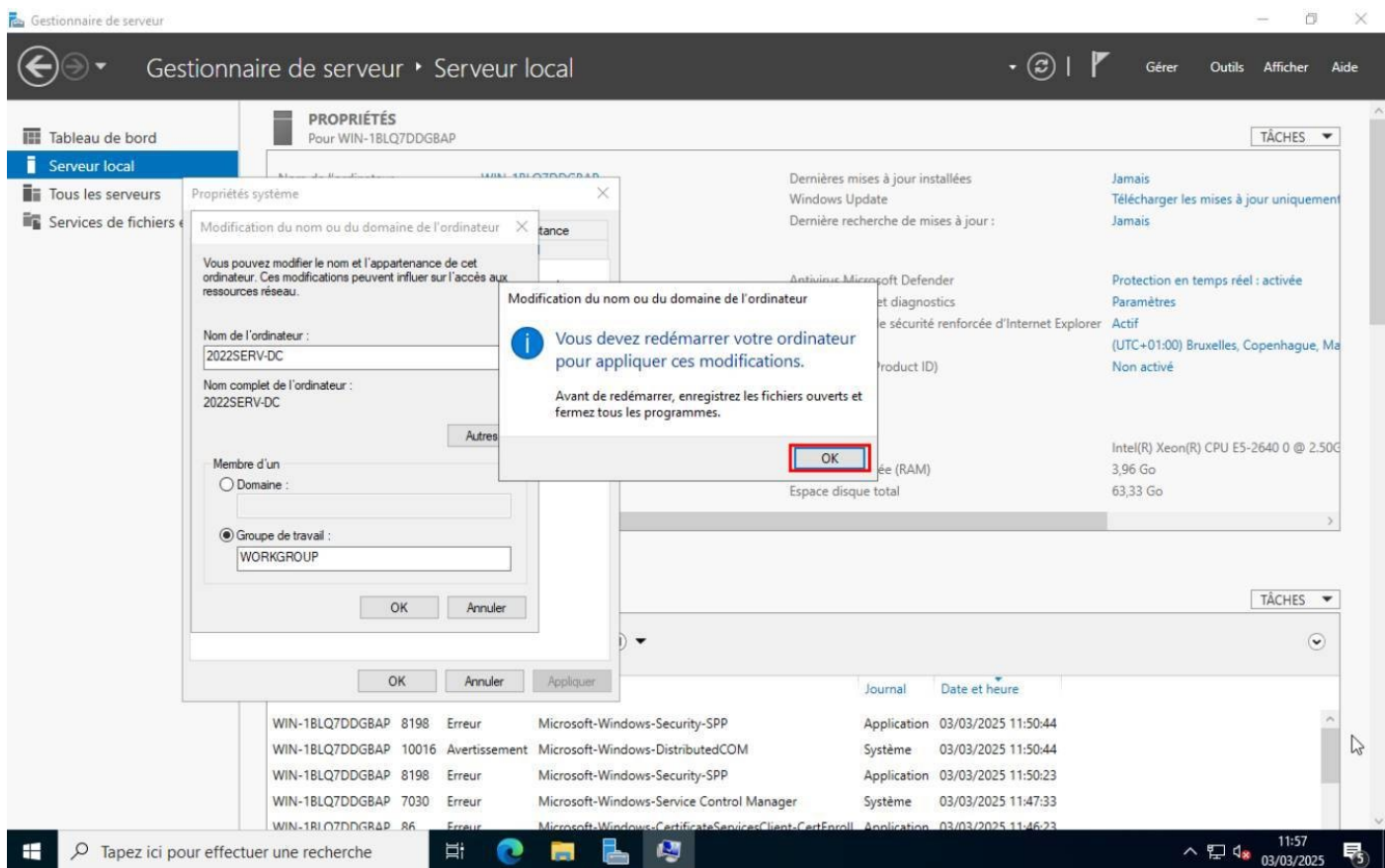
Non



Sélectionnez le nom de l'ordinateur pour le modifier.







Gestionnaire de serveur

Gestionnaire de serveur ▸ Serveur local

Tableau de bord

Serveur local

Tous les serveurs

Services de fichiers et d...

PROPRIÉTÉS

Pour WIN-1BLQ7DDGBAP

Nom de l'ordinateur: WIN-1BLQ7DDGBAP

Groupe de travail: WORKGROUP

Dernières mises à jour installées: Jamais

Windows Update: Télécharger les mises à jour uniquement

Dernière recherche de mises à jour: Jamais

Pare-feu Microsoft Defender: **Activé**

Gestion à distance: Protection en temps réel: activée

Bureau à distance: Paramètres

Association de cartes réseau: Actif (UTC+01:00) Bruxelles, Copenhague, Ma

Ethernet: Non activé

Version du système d'exploitation: Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50G

Informations sur le matériel: 3,96 Go

Espace disque total: 63,33 Go

Microsoft Windows

Vous devez redémarrer votre ordinateur pour appliquer ces modifications.

Avant de redémarrer, enregistrez les fichiers ouverts et fermez tous les programmes.

Redémarrer maintenant

Redémarrer ultérieurement

ÉVÉNEMENTS

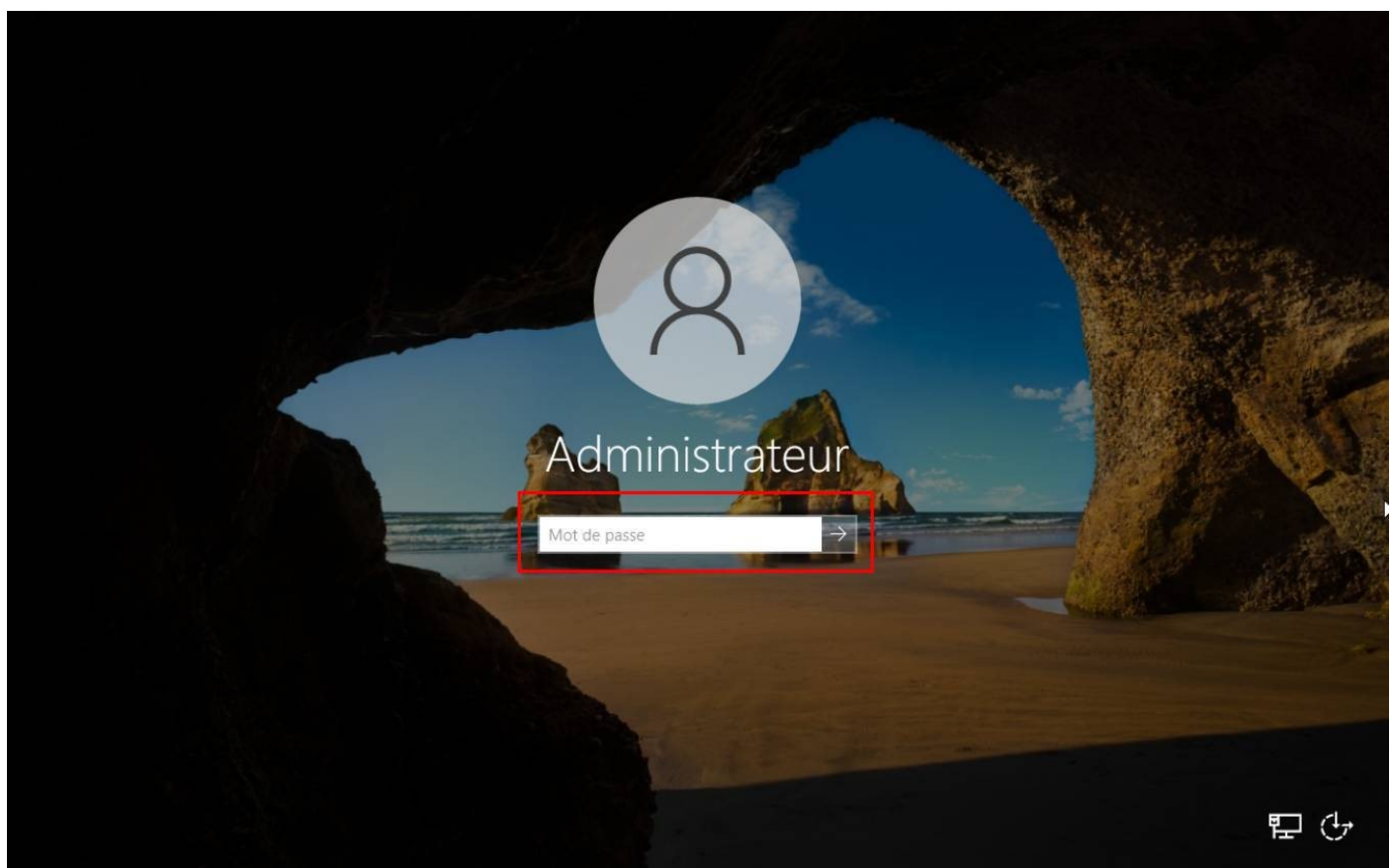
Tous les événements | 15 au total

Filter

Nom du serveur	ID	Gravité	Source	Journal	Date et heure
WIN-1BLQ7DDGBAP	8198	Erreur	Microsoft-Windows-Security-SPP	Application	03/03/2025 11:50:44
WIN-1BLQ7DDGBAP	10016	Avertissement	Microsoft-Windows-DistributedCOM	Système	03/03/2025 11:50:44
WIN-1BLQ7DDGBAP	8198	Erreur	Microsoft-Windows-Security-SPP	Application	03/03/2025 11:50:23
WIN-1BLQ7DDGBAP	7030	Erreur	Microsoft-Windows-Service Control Manager	Système	03/03/2025 11:47:33
WIN-1BLQ7DDGBAP	86	Erreur	Microsoft-Windows-CertificateServicesClient-CertEnroll	Application	03/03/2025 11:46:23

Tapez ici pour effectuer une recherche

11:57 03/03/2025



Windows Server Site A

Installation de Windows Server 2022 sur DC2 en mode CORE

Introduction

Ce premier document couvre la procédure d'installation de Windows Server 2022 dans un environnement Proxmox.

1. Préparation d'une VM
2. Installation de Windows
3. Installation des pilotes

Pour ce faire, vous aurez besoin des éléments suivants :

- Image ISO de Windows Server 2022
- Les ressources suivantes disponibles sur votre Hyperviseur
 - processeur 2v
 - 3 Go de RAM
 - 64 Go de stockage
- Une copie des pilotes VirtIO

Pour mener à bien cette procédure, vous devez disposer des accès nécessaires pour créer des Machines Virtuelles dans Proxmox.

1) Préparation d'une VM

Cliquez sur l'option créer une VM dans l'interface d'administration Proxmox.



Sélectionnez ensuite un nom, le pool de ressources approprié pour votre machine, et cliquez sur suivant.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: pve Resource Pool:

VM ID: 113

Name:

Start at boot: ☐

Start/Shutdown order: any

Startup delay: default

Shutdown timeout: default

Tags

No Tags +

Help Advanced ☒ Back Next

Sur la deuxième page, sélectionnez d'abord votre stockage ISO Proxmox, puis sélectionnez votre ISO de Windows Server déjà préchargée sur votre Hyperviseur. Sélectionnez ensuite les options appropriées dans les paramètres de l'OS Client. Puis, ajoutez l'ISO des drivers en cliquant sur la case à cocher et en sélectionnant l'ISO dans votre bibliothèque.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

☒ Use CD/DVD disc image file (iso)

Storage: ZFS-data

ISO image: x64_dvd_4e34897c.iso

Guest OS: Microsoft Windows

Type: 11/2022/2025

Version: 11/2022/2025

☐ Use physical CD/DVD Drive

☐ Do not use any media

☒ Add additional drive for VirtIO drivers

Storage: ZFS-data

ISO image: virtio-win-0.1.266.iso

Advanced ☒ Back Next

Ajoutez ensuite un espace de Stockage pour la partition EFI et la puce TPM qui sera nécessaire pour l'activation de BitLocker sur vos serveurs. En général, l'espace de stockage est le même que celui utilisé pour stocker l'image disque principale.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'System' tab selected. The 'EFI Storage' dropdown is highlighted with a red circle and the number '1'. The 'TPM Storage' dropdown is highlighted with a red circle and the number '2'. The 'Add TPM' checkbox is checked. The 'Version' dropdown is set to 'v2.0'. The 'Format' dropdown is set to 'QEMU image format (qcow2)'. The 'Pre-Enroll keys' checkbox is checked. The 'Advanced' checkbox is checked. The 'Back' and 'Next' buttons are visible at the bottom right.

Field	Value
Graphic card:	Default
Machine:	q35
SCSI Controller:	VirtIO SCSI single
Qemu Agent:	<input type="checkbox"/>
BIOS:	OVMF (UEFI)
Add TPM:	<input checked="" type="checkbox"/>
EFI Storage:	[Dropdown menu highlighted with red circle 1]
TPM Storage:	[Dropdown menu highlighted with red circle 2]
Version:	v2.0
Format:	QEMU image format (qcow2)
Pre-Enroll keys:	<input checked="" type="checkbox"/>

Help Advanced ☒ Back Next

Dans la page de sélection du disque virtuel principal, choisissez l'emplacement de stockage de l'image disque et augmentez la taille du disque à votre convenance. Cliquez sur "Add" pour ajouter des disques secondaires.

Create: Virtual Machine

General OS System **Disks** CPU Memory Network Confirm

scsi0

Disk Bandwidth

Bus/Device: SCSI 0 Cache: Default (No cache)

SCSI Controller: VirtIO SCSI single Discard: ☐

Storage: **1** ZFS-vm IO thread: ☒

Disk size (GiB): 64 **2**

Format: QEMU image format

SSD emulation: ☐ Backup: ☒

Read-only: ☐ Skip replication: ☐

Async IO: Default (io_uring)

Add

Help Advanced ☒ **Back** **Next**

Dans la page CPU, ajoutez un Socket à votre machine virtuelle et sélectionnez le Type "x86-64-v2-AES" s'il n'est pas sélectionné par défaut.

Si votre hyperviseur dispose de deux CPU physiques, vous pouvez activer l'option NUMA.

Create: Virtual Machine

GeneralOSSystemDisksCPUMemoryNetworkConfirm

Sockets: 1 2

Type: 2 x86-64-v2-AES

Cores: 1

Total cores: 2

VCPUs: 2

CPU units: 100

CPU limit: unlimited

Enable NUMA: ☒ 3

CPU Affinity: All Cores

Extra CPU Flags:

Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	md-clear	Required to let the guest OS know if MDS is mitigated correctly
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	pcid	Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	spec-ctrl	Allows improved Spectre mitigation with Intel CPUs
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	ssbd	Protection for "Speculative Store Bypass" for Intel models
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	ibpb	Allows improved Spectre mitigation with AMD CPUs
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	virt-ssbd	Basis for "Speculative Store Bypass" protection for AMD models

Help

Advanced ☒

Back

Next

Dans la page Mémoire, sélectionnez un montant de RAM entre 3 et 4 go minimum. En fonction de votre utilisation, il faudra allouer de la mémoire en plus. Sélectionnez ensuite la même quantité de mémoire minimale ou désactivez l'option de Ballooning.

Create: Virtual Machine

General OS System Disks CPU **Memory** Network Confirm

Memory (MiB): 4096 1

Minimum memory (MiB): 4096 2

Shares: Default (1000)

Ballooning Device: ☒ 3

Help Advanced ☒ Back Next

Configure the network card according to your infrastructure. Select the VirtIO network card in the "Model" section.

Create: Virtual Machine

General OS System Disks CPU Memory **Network** Confirm

☐ No network device

Bridge: 1 vmbri0 Model: 2 VirtIO (paravirtualized)

VLAN Tag: no VLAN MAC address: auto

Firewall: ☒

Disconnect: ☐ Rate limit (MB/s): unlimited

MTU: 1500 (1 = bridge MTU) Multiqueue:

Help Advanced ☒ Back Next

Vérifiez votre configuration et cliquez sur le bouton FINISH.

Create: Virtual Machine

General

OS

System

Disks

CPU

Memory

Network

Confirm

Key ↑	Value
cores	1
cpu	x86-64-v2-AES
ide2	ZFS-data:iso/fr-fr_windows_server_2022_updated_nov_2024_x64_dvd_4e34897c.iso,med...
memory	2048
net0	virtio,bridge=vmbr0,firewall=1
nodename	pve
numa	0
ostype	l26
scsi0	ZFS-retro:32,ioread=on
scsihw	virtio-scsi-single
sockets	1
vmid	113

☐ Start after created

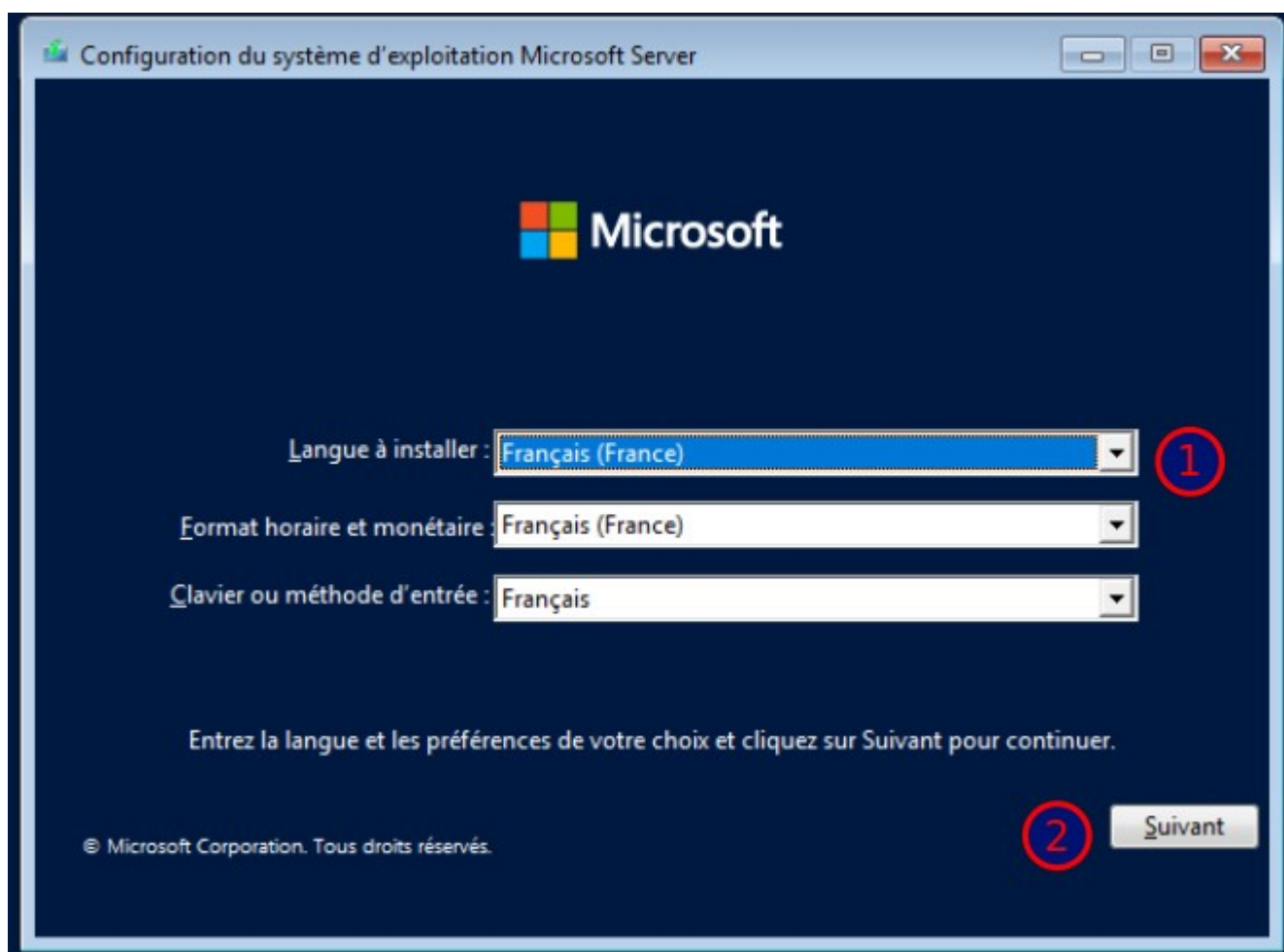
Advanced ☒

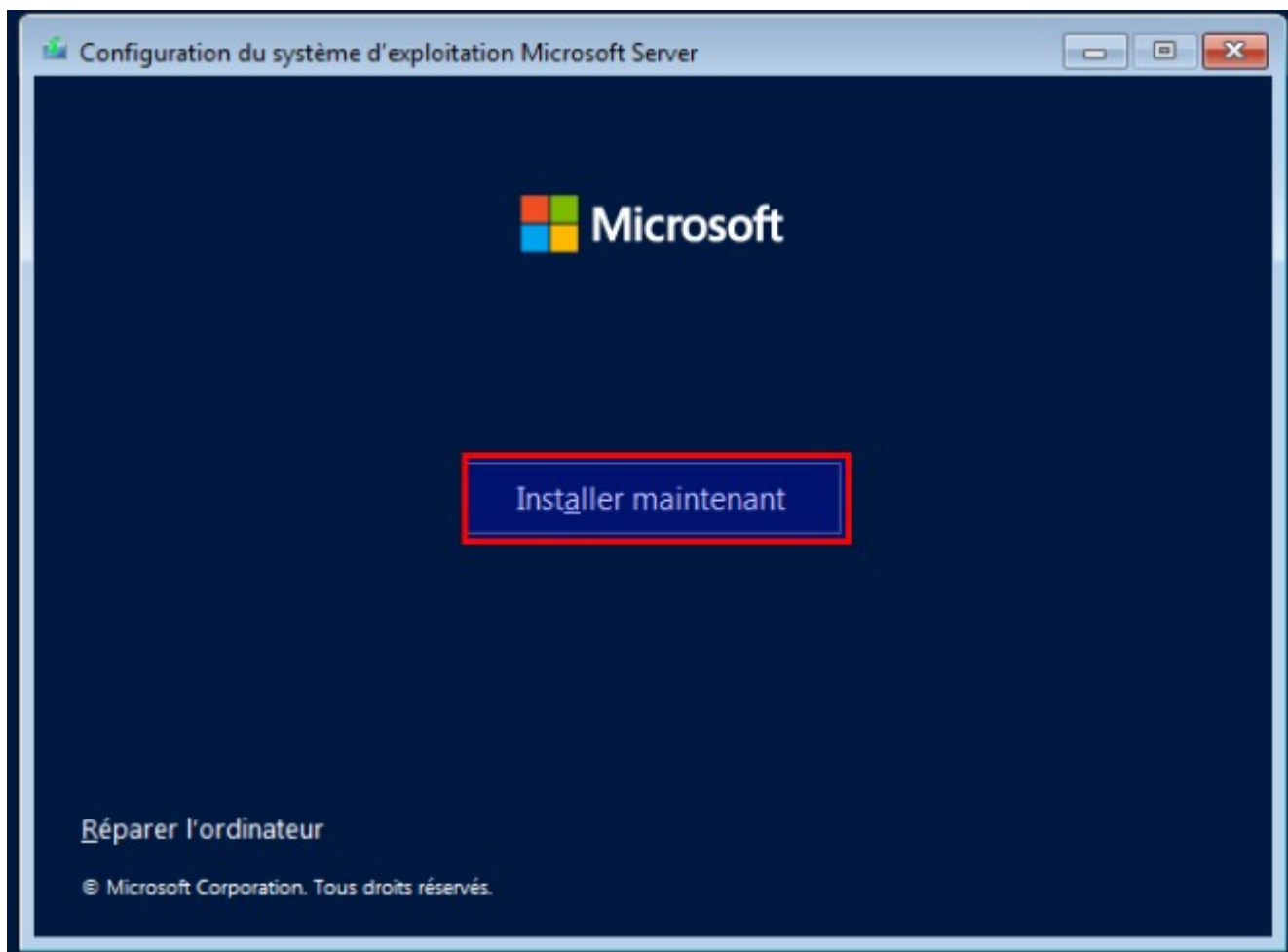
Back

Finish

2) Installation de Windows Server 2022

Une fois la VM lancée sur l'ISO de Windows Server, sélectionnez la langue (Français) et cliquez sur suivant.





Sélectionnez bien "Je n'ai pas de clé de produit"

Activer la configuration du système d'exploitation Microsoft Server

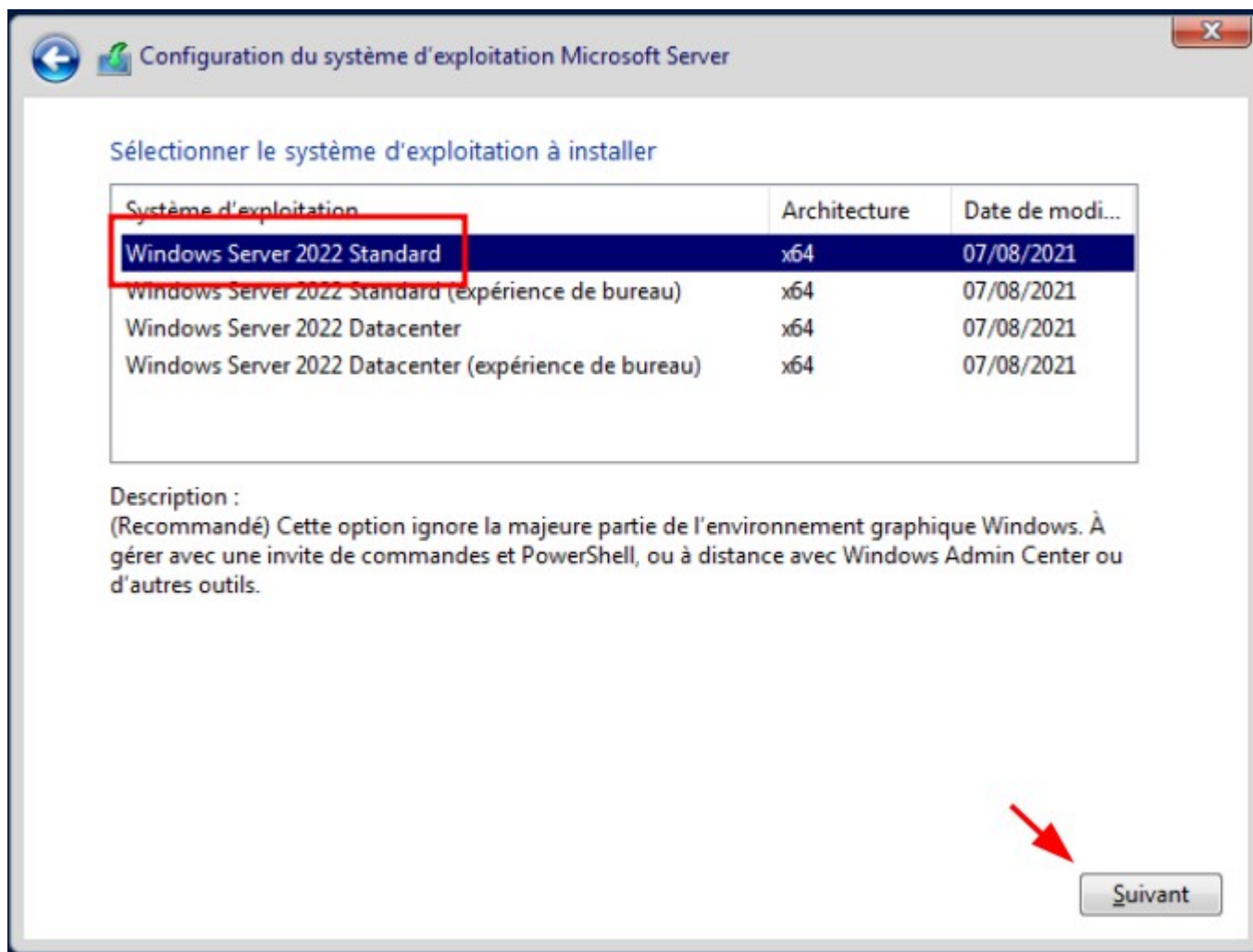
Si vous installez le système d'exploitation Microsoft Server pour la première fois sur cet ordinateur (ou si vous installez une autre édition), vous devez entrer une clé de produit valide pour le système d'exploitation Microsoft Server. Votre clé de produit doit figurer dans le courrier de confirmation que vous avez reçu après l'achat d'une copie numérique du système d'exploitation Microsoft Server ou sur une étiquette fournie dans la zone du système d'exploitation Microsoft Server.

La clé de produit (Product Key) ressemble à ceci : XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Si vous réinstallez le système d'exploitation Microsoft Server, sélectionnez je ne dispose pas d'une clé de produit. Votre copie du système d'exploitation Microsoft Server sera automatiquement

[Déclaration de confidentialité](#)[Je n'ai pas de clé de produit \(Product Key\)](#)[Suivant](#)

Sélectionnez « Windows Server 2022 Standard » et continuez



Avis et conditions du contrat de licence applicables

VOUS DEVEZ ACCEPTER LES TERMES DE LA LICENCE DU LOGICIEL. VOIR CI-APRÈS. Veuillez lire les conditions de licence complètes fournies à l'adresse (aka.ms/userterms).

NOTIFICATION IMPORTANTE

Informations relatives à l'utilisation et au diagnostic. Microsoft recueille ces informations sur Internet pour assurer la sécurité et la mise à jour de Windows, diagnostiquer les problèmes et apporter des améliorations aux produits, et peut associer ces informations à votre organisation. Les systèmes d'exploitation des serveurs Microsoft peuvent être configurés pour désactiver les données de diagnostic, envoyer des données de diagnostic obligatoires ou envoyer des données de diagnostic facultatives. Le réglage par défaut consiste à envoyer les données de diagnostic requises. Les données de diagnostic requises

1



J'accepte les termes du contrat de licence logiciel Microsoft. Si la licence appartient à une organisation, je suis autorisé à agir en son nom.

2

Suivant

Choisissez l'option personnalisée.

Quel type d'installation voulez-vous effectuer ?

Mise à jour : Installer le système d'exploitation Microsoft Server et conserver les fichiers, les paramètres et les applications.

Avec cette option, les fichiers, paramètres et applications sont déplacés vers le nouveau système d'exploitation. Cette option est disponible uniquement lorsqu'une version prise en charge du système d'exploitation est déjà en cours d'exécution sur l'ordinateur.

Personnalisé : installer uniquement le système d'exploitation Microsoft Server (avancé)

Avec cette option, les fichiers, les paramètres et les applications ne sont pas déplacés vers le nouveau système d'exploitation. Pour modifier les partitions et les lecteurs, démarrez l'ordinateur à l'aide du disque d'installation. Nous vous recommandons de sauvegarder vos fichiers avant de continuer.

Où voulez-vous installer le système d'exploitation ?

Nom	Taille totale	Espace libre	Type

 Actualiser Supprimer Formater Nouveau

1

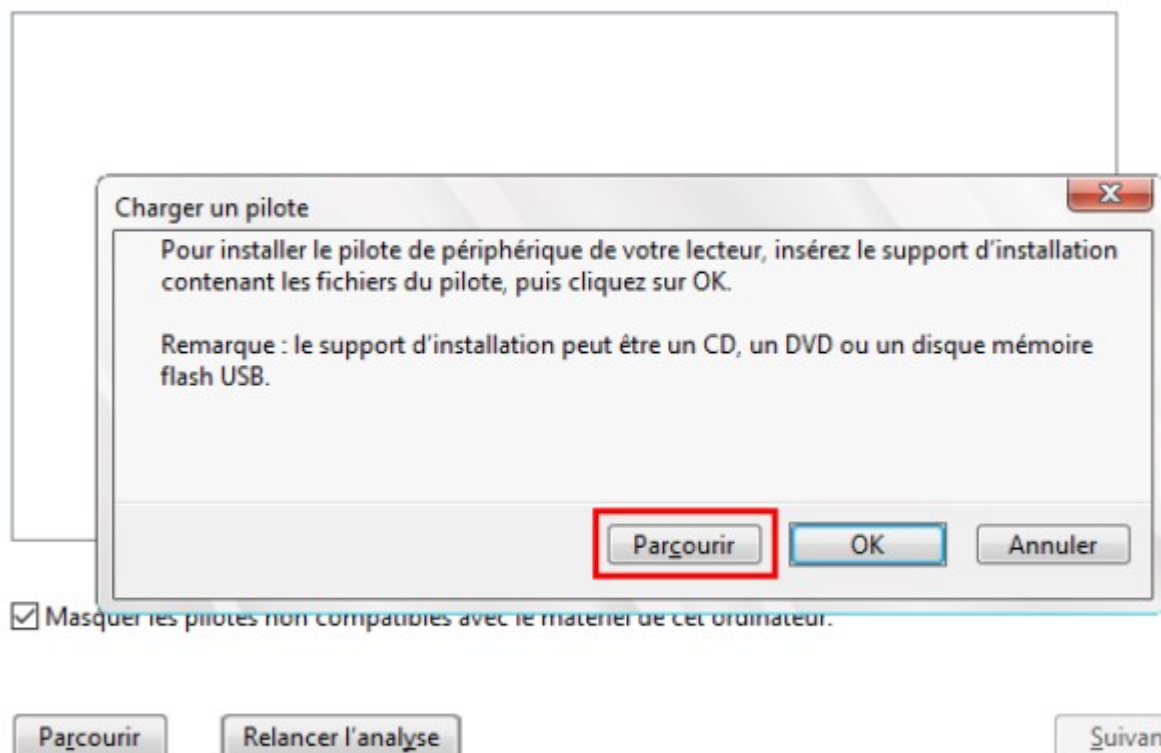
 Charger un pilote Étendre

Nous n'avons trouvé aucun lecteur. Pour obtenir un pilote de stockage, cliquez sur Charger un pilote.

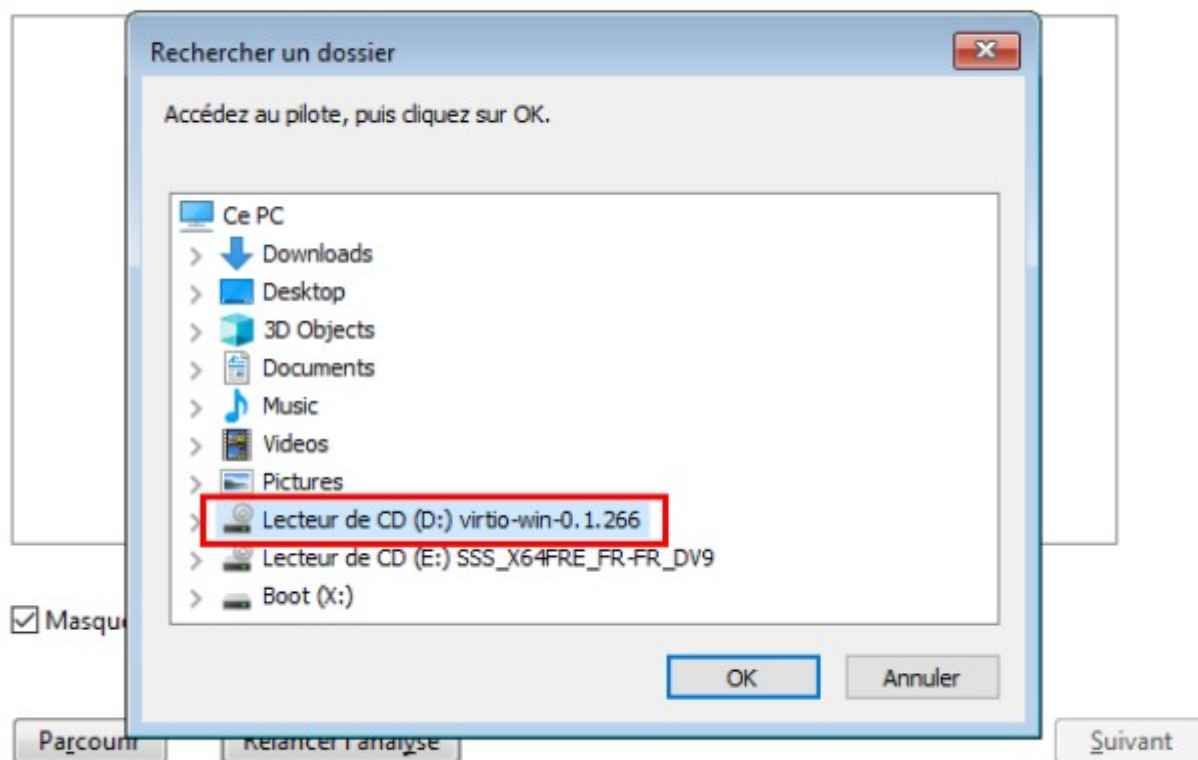
2

Suivant

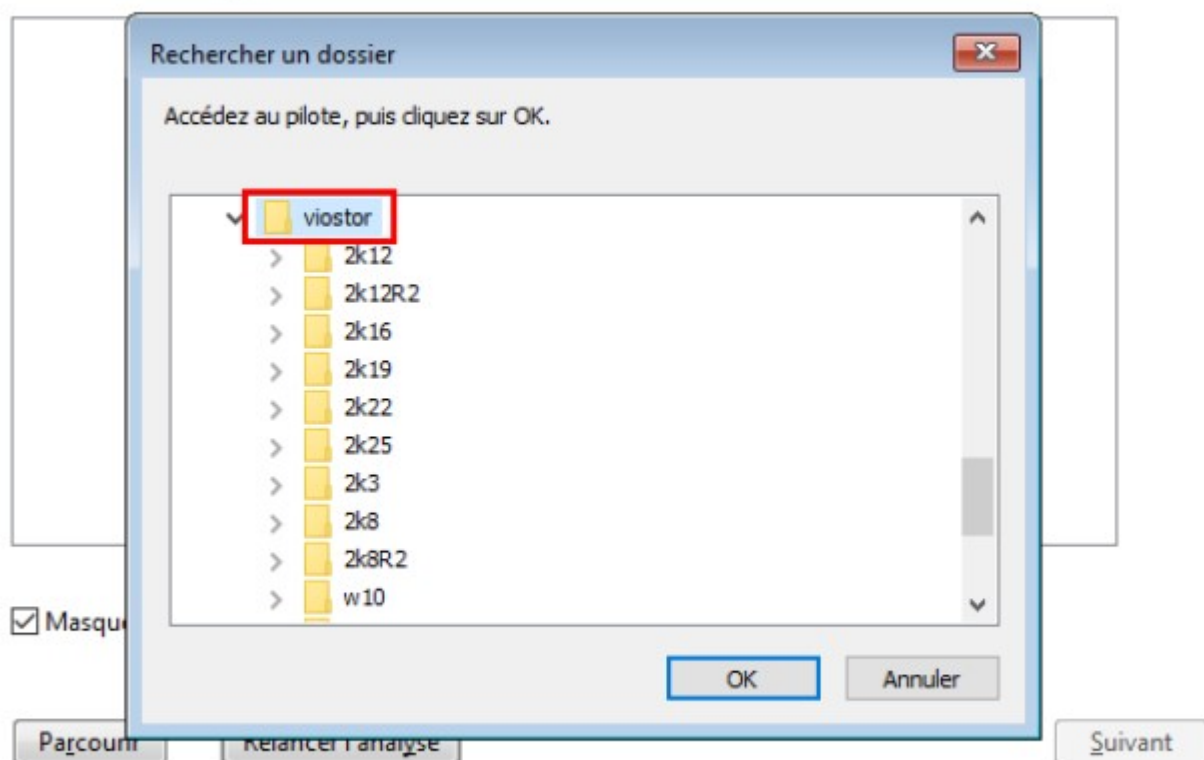
Sélectionner le pilote à installer



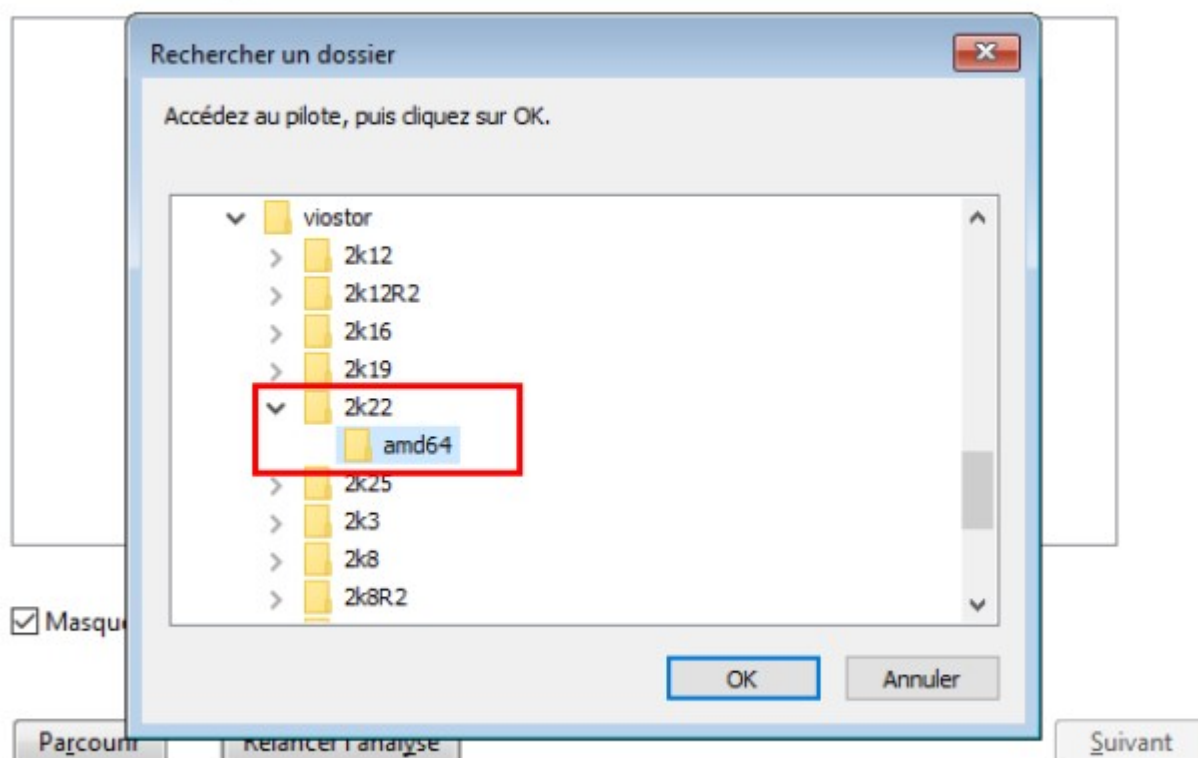
Sélectionner le pilote à installer



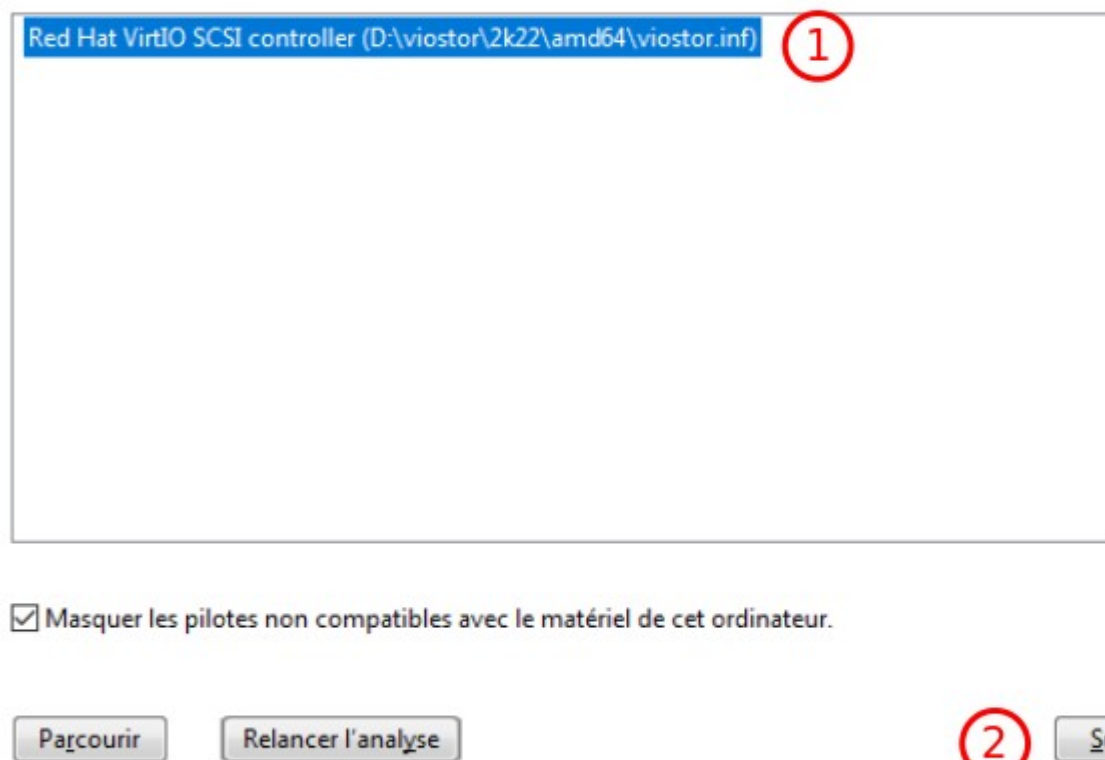
Sélectionner le pilote à installer




Sélectionner le pilote à installer



Sélectionner le pilote à installer

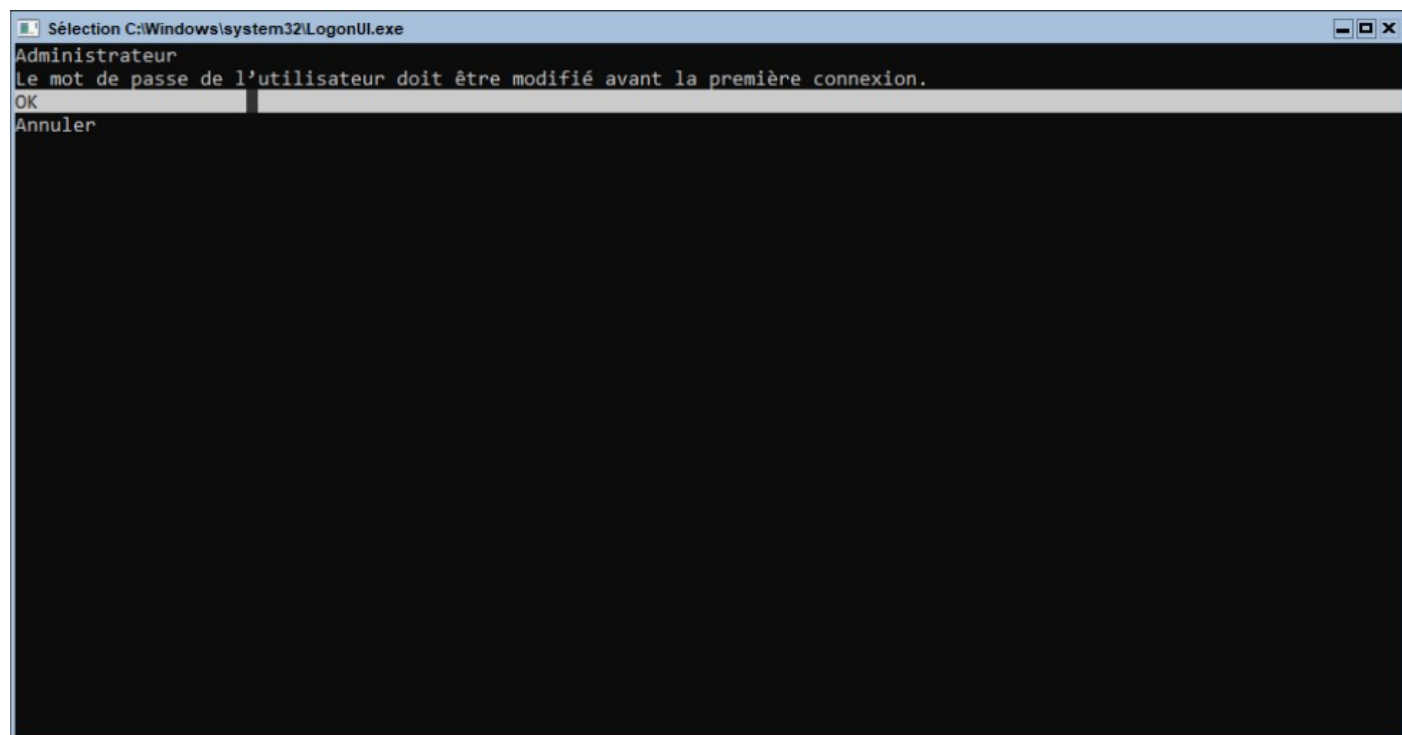


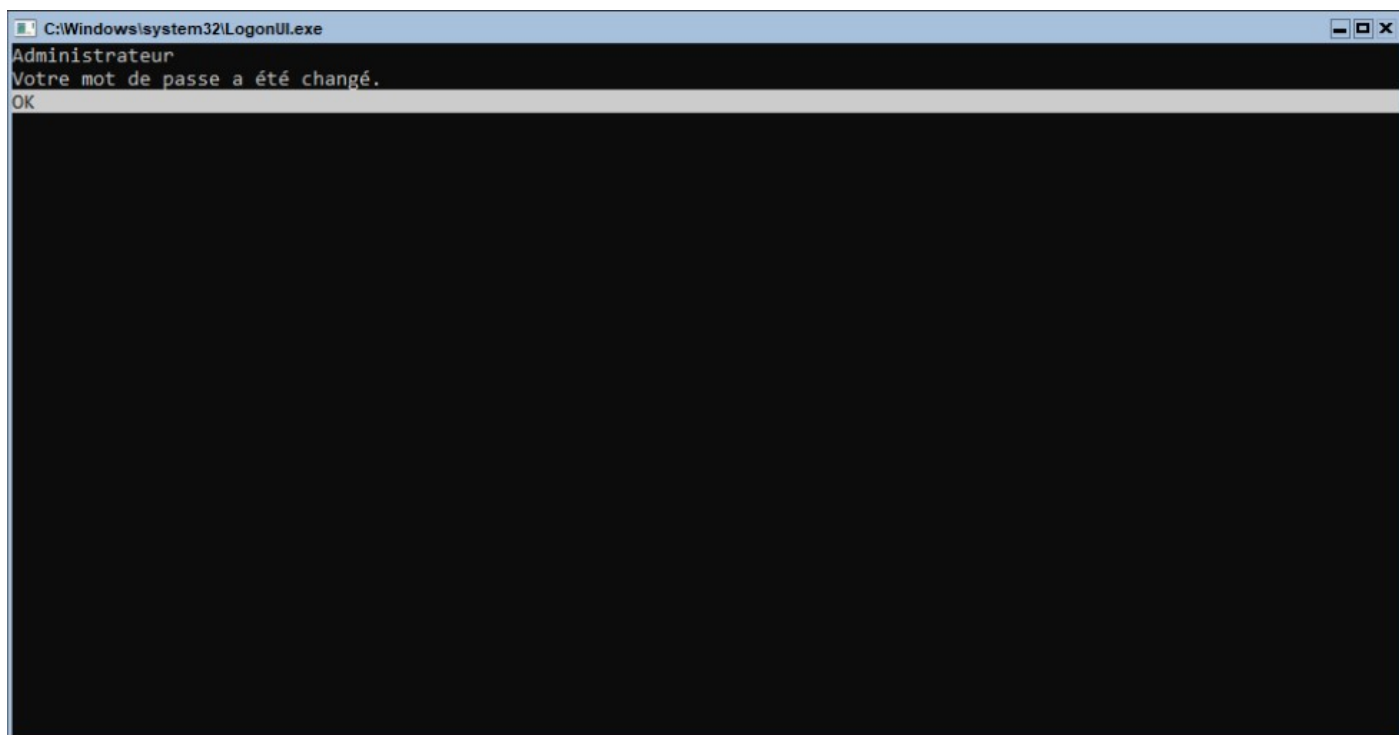
Où voulez-vous installer le système d'exploitation ?

	Nom	Taille totale	Espace libre	Type
	Lecteur 0 Espace non alloué	64.0 Go	64.0 Go	

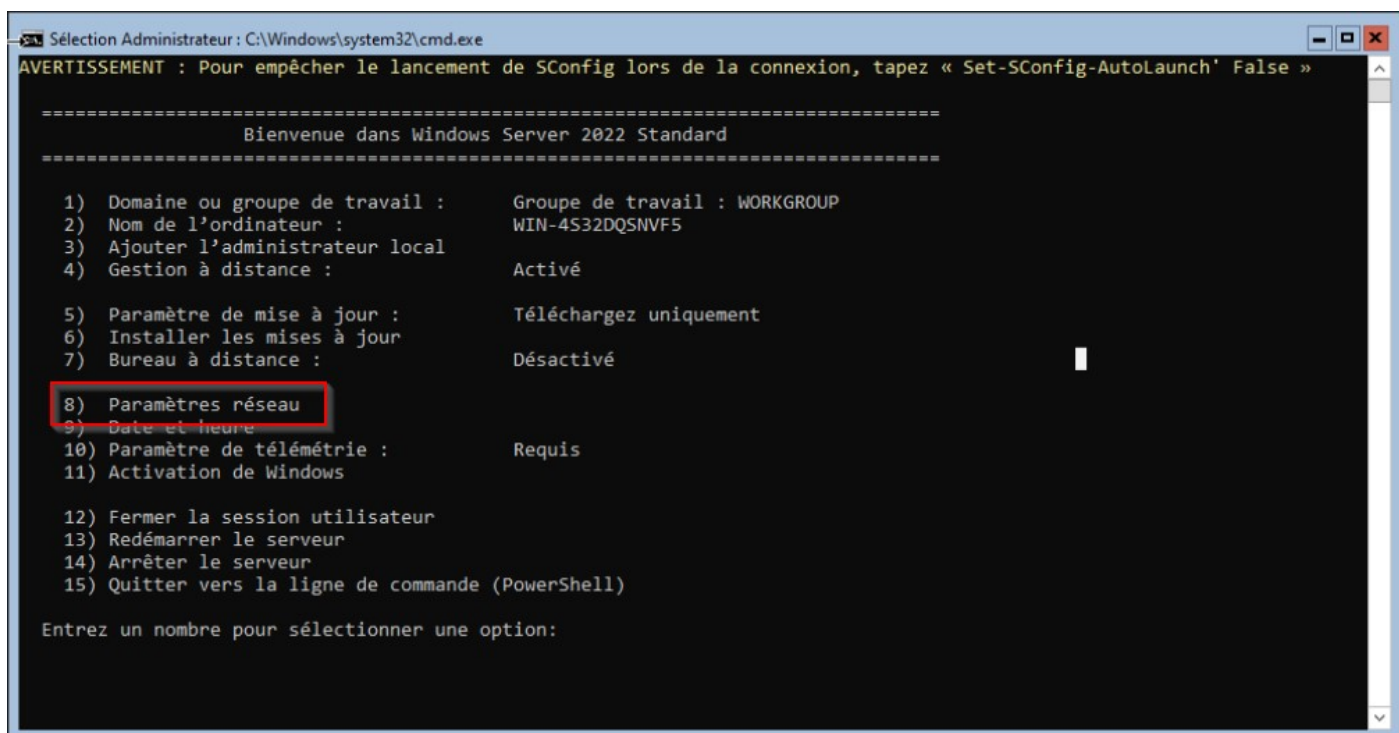
 Actualiser Supprimer Formater Nouveau Charger un pilote Étendre**Suivant**

Une fois l'installation terminée, le serveur va redemarrer. Vous allez devoir changer le MDP





Vous allez ensuite voir apparaître le menu "SConfig". Une fois le menu visible, utilisez l'option 8 pour configurer le réseau



Entrez ensuite le numéro d'index de votre carte


```
Administrateur : C:\Windows\system32\cmd.exe

=====
Paramètres réseau
=====

Cartes réseau disponibles :

Index numéro | Adresse IP      | Description
1            | 192.168.200.10 | Intel(R) PRO/1000 MT Network Connection

Sélectionnez le numéro d'index de la carte réseau (Vide = annuler): _
```

Vous devrez configurer les options 1 et 2, commencez par l'option 1

```
Administrateur : C:\Windows\system32\cmd.exe

=====
Paramètres de carte réseau
=====

Index NIC :          1
Description :        Intel(R) PRO/1000 MT Network Connection
Adresse IP :         192.168.200.10,
                    fe80::e4de:244:1cce:ff28
Masque de sous-réseau : 255.255.255.0
DHCP activé :        True

Passerelle par défaut : 192.168.200.1 fe80::be24:11ff:fe2b:44cd
Serveur DNS préféré :  192.168.200.200
Serveur DNS auxiliaire : 192.168.200.201

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS

Entrez la sélection (Vide = annuler):
```

entrez les paramètres désirés

```

Administrateur : C:\Windows\system32\cmd.exe

=====
Paramètres de carte réseau
=====

Index NIC :          1
Description :        Intel(R) PRO/1000 MT Network Connection
Adresse IP :         192.168.200.10,
                   fe80::e4de:244:1cce:ff28
Masque de sous-réseau : 255.255.255.0
DHCP activé :        True

Passerelle par défaut : 192.168.200.1 fe80::be24:11ff:fe2b:44cd
Serveur DNS préféré :  192.168.200.200
Serveur DNS auxiliaire : 192.168.200.201

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS

Entrez la sélection (Vide = annuler): 1
Sélectionnez le protocole (D)HCP ou l'adresse IP (S)tatique (Vide = annuler): S
Entrez une adresse IP statique : (Vide = annuler): 192.168.200.201
Entrez un masque de sous-réseau (Vide=255.255.255.0):
Entrez la passerelle par défaut (Vide = annuler): 192.168.200.1
Affectation en cours de l'adresse IP statique à la carte réseau... Merci de patienter.
Le bail DHCP a été libéré avec succès.
L'adressage statique a été correctement activé. DHCP n'est pas activé pour cette carte réseau.
La passerelle a été correctement définie.
Définition de l'adresse de la carte réseau effectuée avec succès.
(Appuyez sur ENTRÉE pour continuer):

```

Pour les DNS, vous devez quitter le menu principal avec l'option 15, puis utilisez les commandes suivantes :

```

Set-DnsClientServerAddress -InterfaceIndex 1 -ServerAddresses
192.168.100.200,192.168.100.201,192.168.200.200,192.168.200.201
Get-DnsClientServerAddress -InterfaceIndex 1

```

Utilisez ensuite la commande "ipconfig /all" pour vérifier la configuration des serveurs DNS.

```

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Red Hat VirtIO Ethernet Adapter
Adresse physique . . . . . : BC-24-11-90-EF-98
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::9d31:4d25:df07:a536%4(préféré)
Adresse IPv4. . . . . : 192.168.100.201(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.100.1
IAID DHCPv6 . . . . . : 112993297
DUID de client DHCPv6. . . . . : 00-01-00-01-30-80-26-57-BC-24-11-90-EF-98
Serveurs DNS. . . . . :
192.168.100.200
192.168.100.201
192.168.200.200
192.168.200.201

NetBIOS sur Tcpip. . . . . : Active
PS C:\Users\Administrateur\IEF>

```

tapez ensuite exit dans le terminal pour revenir au menu SConfig, sélectionnez l'option 1 pour rejoindre un domaine

```
Sélection Administrateur : C:\Windows\system32\cmd.exe
AVERTISSEMENT : Pour empêcher le lancement de SConfig lors de la connexion, tapez « Set-SConfig-AutoLaunch' False »

=====
                    Bienvenue dans Windows Server 2022 Standard
=====

1) Domaine ou groupe de travail :   Groupe de travail : WORKGROUP
2) Nom de l'ordinateur :           WIN-4S32DQSNVF5
3) Ajouter l'administrateur local
4) Gestion à distance :            Activé

5) Paramètre de mise à jour :       Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance :             Désactivé

8) Paramètres réseau
9) Date et heure
10) Paramètre de télémétrie :       Requis
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option:
```

Entrez les informations de votre domaine et validez avec "O"

```
Administrateur : C:\Windows\system32\cmd.exe

=====
                    Changer l'appartenance au domaine ou groupe de travail
=====

Actuel groupe de travail : WORKGROUP

Souhaitez-vous adhérer à un (D)omaine ou Groupe de (t)ravail? (Vide = annuler): D
Nom de domaine à joindre (Vide = annuler): ief.local
Spécifier un domaine\utilisateur autorisé: (Vide = annuler): ief\ADM-RCS
Mot de passe de ief\ADM-RCS: *****
Vous rejoignez ief.local... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-4S32DQSNVF5.
Vous avez correctement rejoint le domaine.
Voulez-vous modifier le nom de l'ordinateur avant de redémarrer ? (O)ui ou (N)on:
```

Entrez le nouveau nom pour votre DC, et validez le redémarrage

```
Administrateur : C:\Windows\system32\cmd.exe

=====
Changer l'appartenance au domaine ou groupe de travail
=====

Actuel groupe de travail : WORKGROUP

Souhaitez-vous adhérer à un (D)omaine ou Groupe de (t)ravail? (Vide = annuler): D
Nom de domaine à joindre (Vide = annuler): ief.local
Spécifier un domaine\utilisateur autorisé: (Vide = annuler): ief\ADM-RCS
Mot de passe de ief\ADM-RCS: *****
Vous rejoignez ief.local... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-4S32DQSNVF5.
Vous avez correctement rejoint le domaine.
Voulez-vous modifier le nom de l'ordinateur avant de redémarrer ? (O)ui ou (N)on: o
Entrer un nouveau nom d'ordinateur (Vide = annuler): WS2022-DC2-SB
Mot de passe de ief\ADM-RCS: *****
Modification en cours du nom d'ordinateur... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-4S32DQSNVF5.
Redémarrer maintenant ? (O)ui ou (N)on: _
```

Windows Server Site A

Configuration - Création du domaine AD, configuration initiale du domaine.

Introduction

Ce deuxième document couvre la procédure d'installation des différents rôles nécessaires à la mise en place d'un domaine AD.

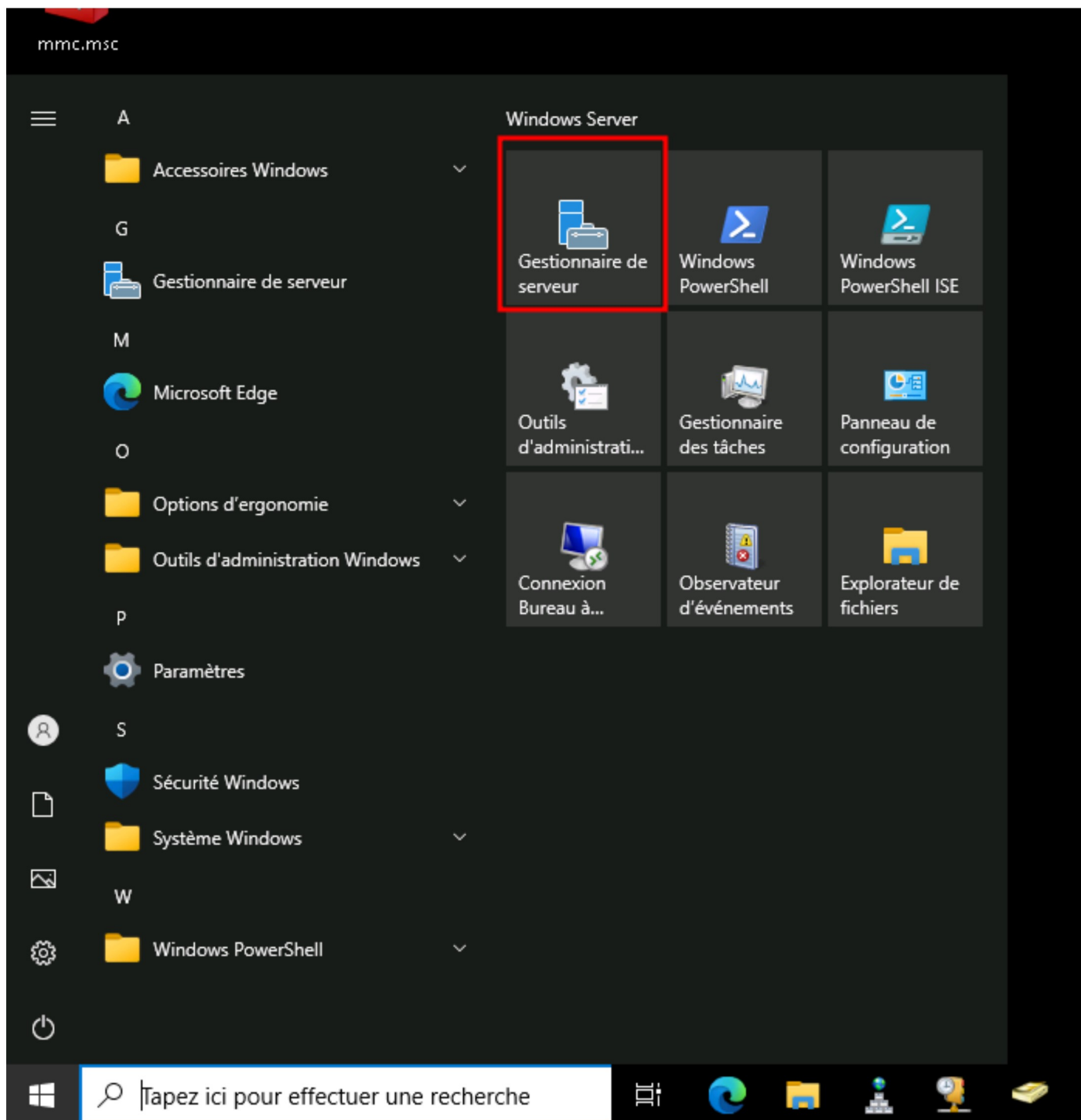
1. Installation des rôles AD, DNS, DHCP.
2. Configuration initiale du domaine

Pour ce faire, vous aurez besoin des éléments suivants :

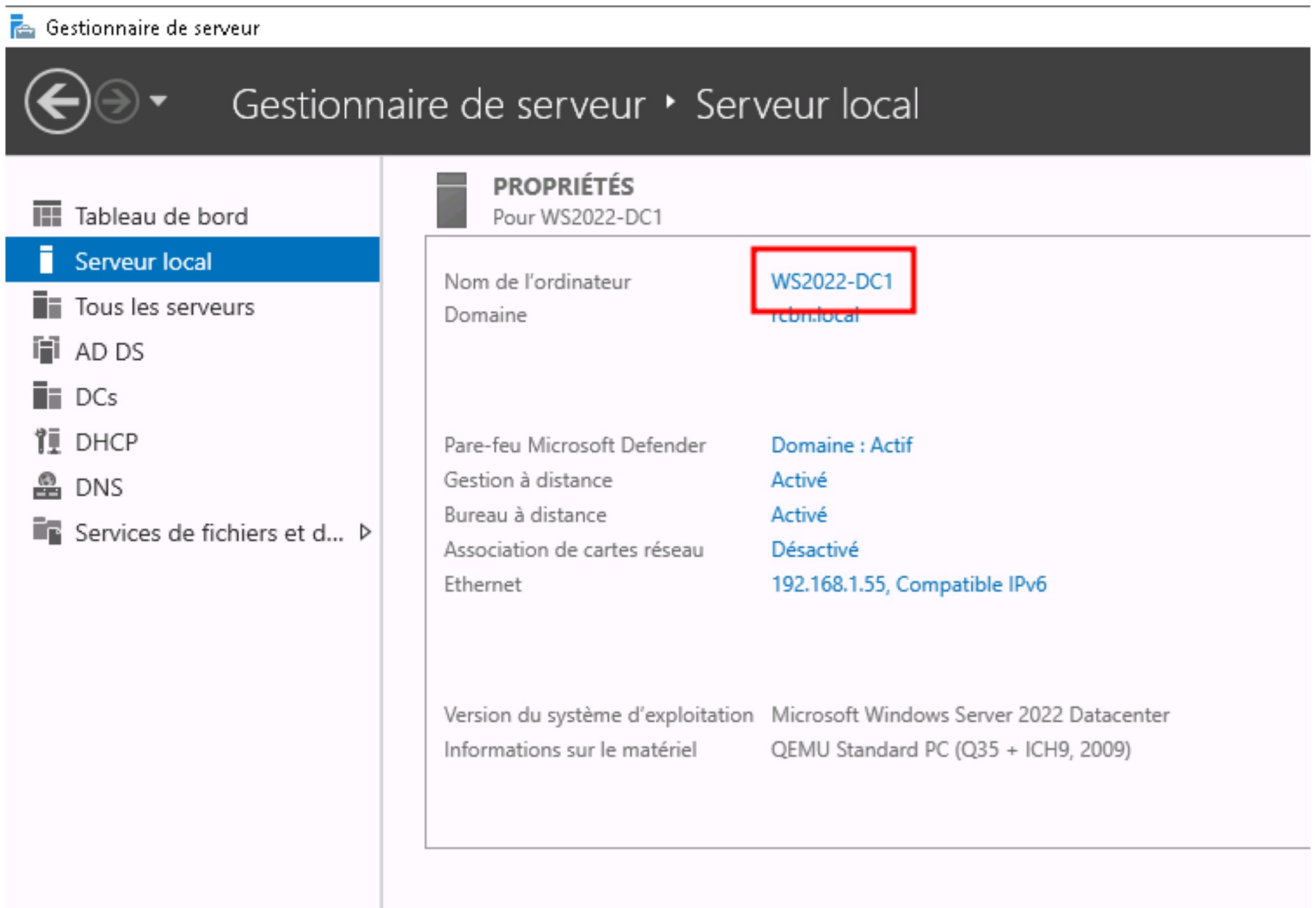
- Machine virtuelle Windows Server 2022
- Compte d'administration du serveur
- Serveur correctement nommé

1) Installation des rôles

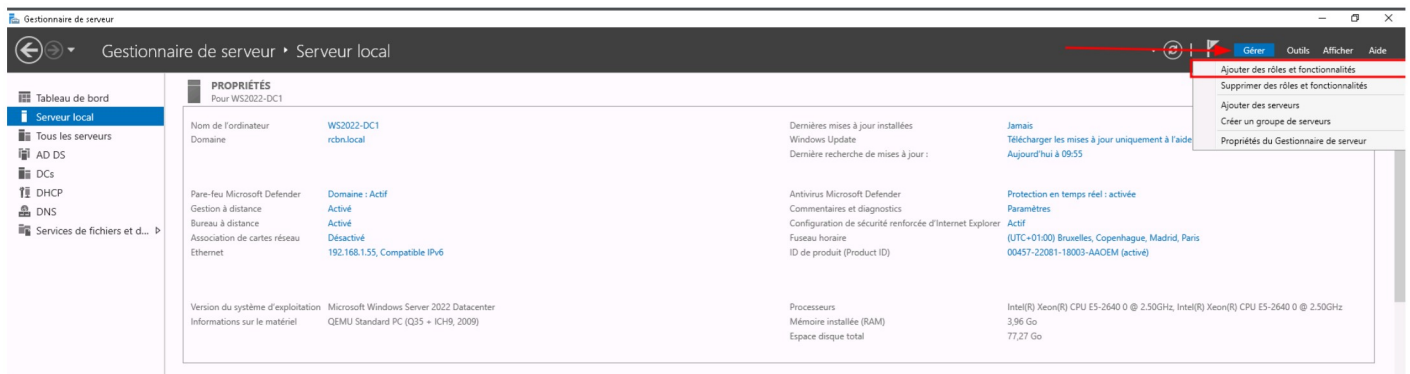
Pour installer des rôles de serveur, vous devez lancer le gestionnaire de serveur, trouvable dans le menu démarrer du serveur.



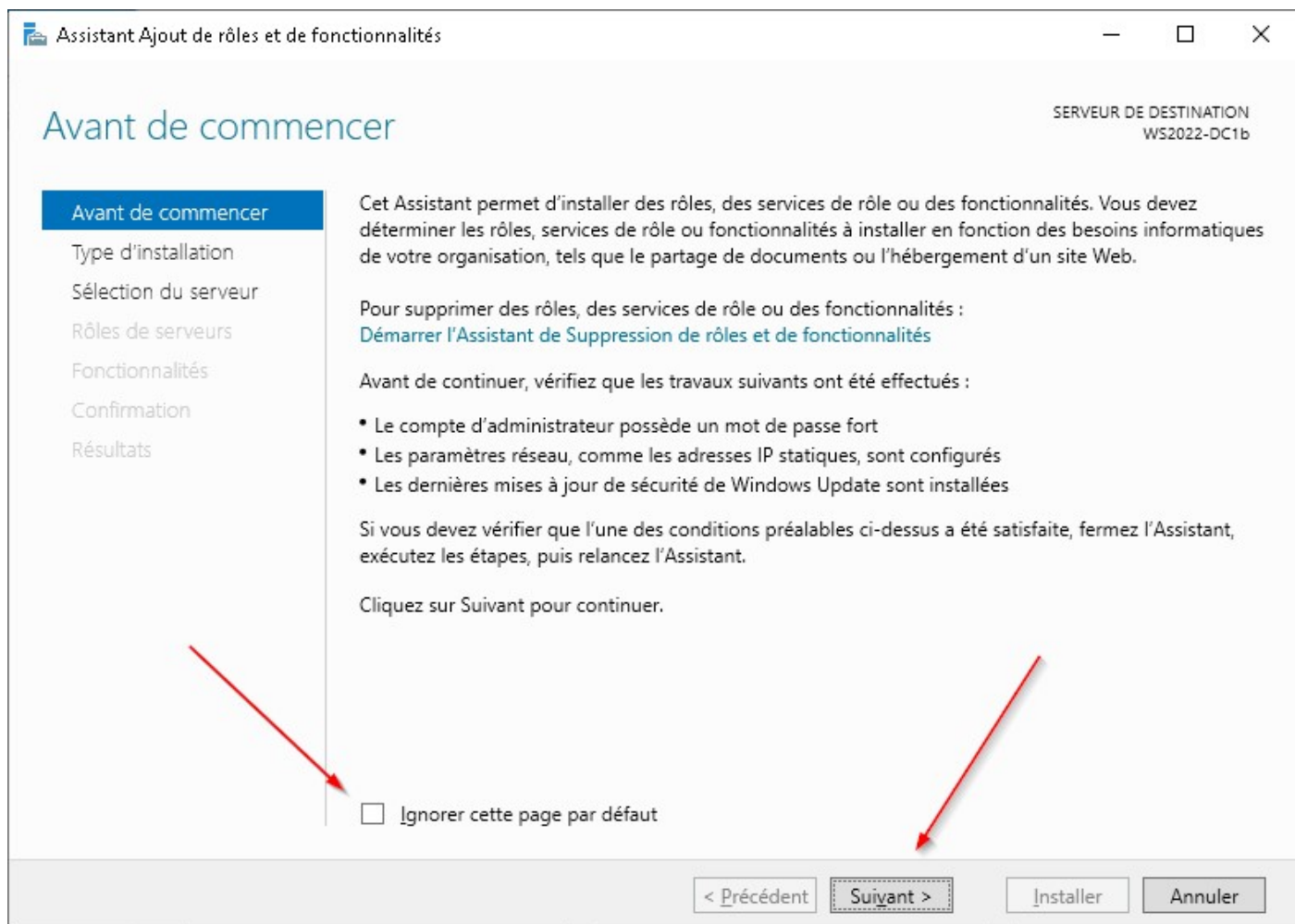
Avant de commencer, vérifiez que votre serveur est correctement nommé. Une fois le domaine créé, il faudra réaliser des actions spécifiques dans le cas où vous voudriez renommer votre serveur par la suite.



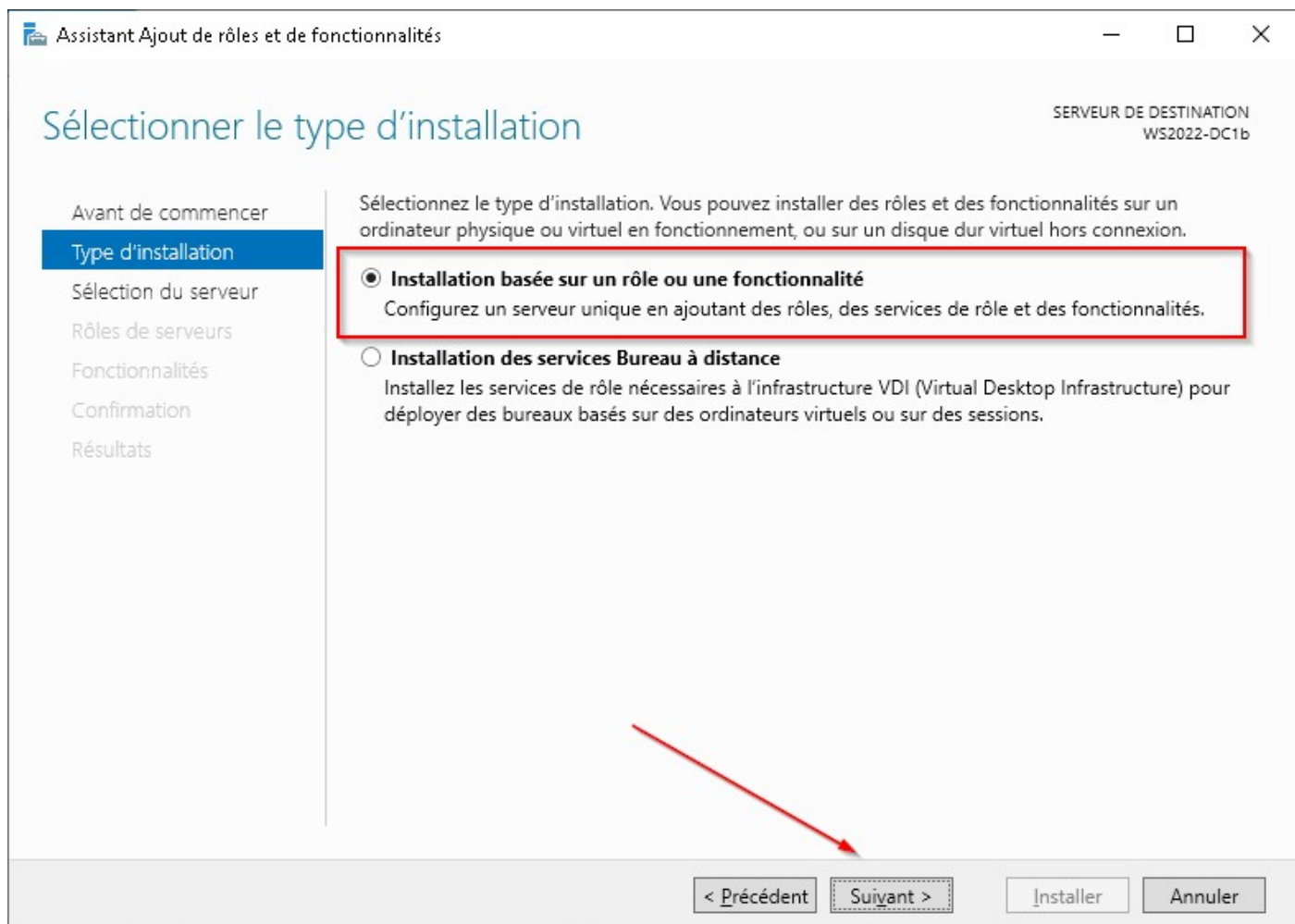
Cliquez ensuite sur gérer, puis "Ajouter des rôles et des fonctionnalités"



Vous voici sur la page d'accueil de l'assistant. Vous pouvez cocher (ou non) la case pour ignorer l'introduction de l'assistant. Cliquez ensuite sur suivant.



Vérifiez ensuite que la première option est bien celle cochée dans la fenêtre qui suit



Sélectionnez les paramètres régionaux de votre machine, et cliquez sur suivant

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
WS2022-DC1b

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

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

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

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
WS2022-DC1b	192.168.1.10	Microsoft Windows Server 2022 Standard

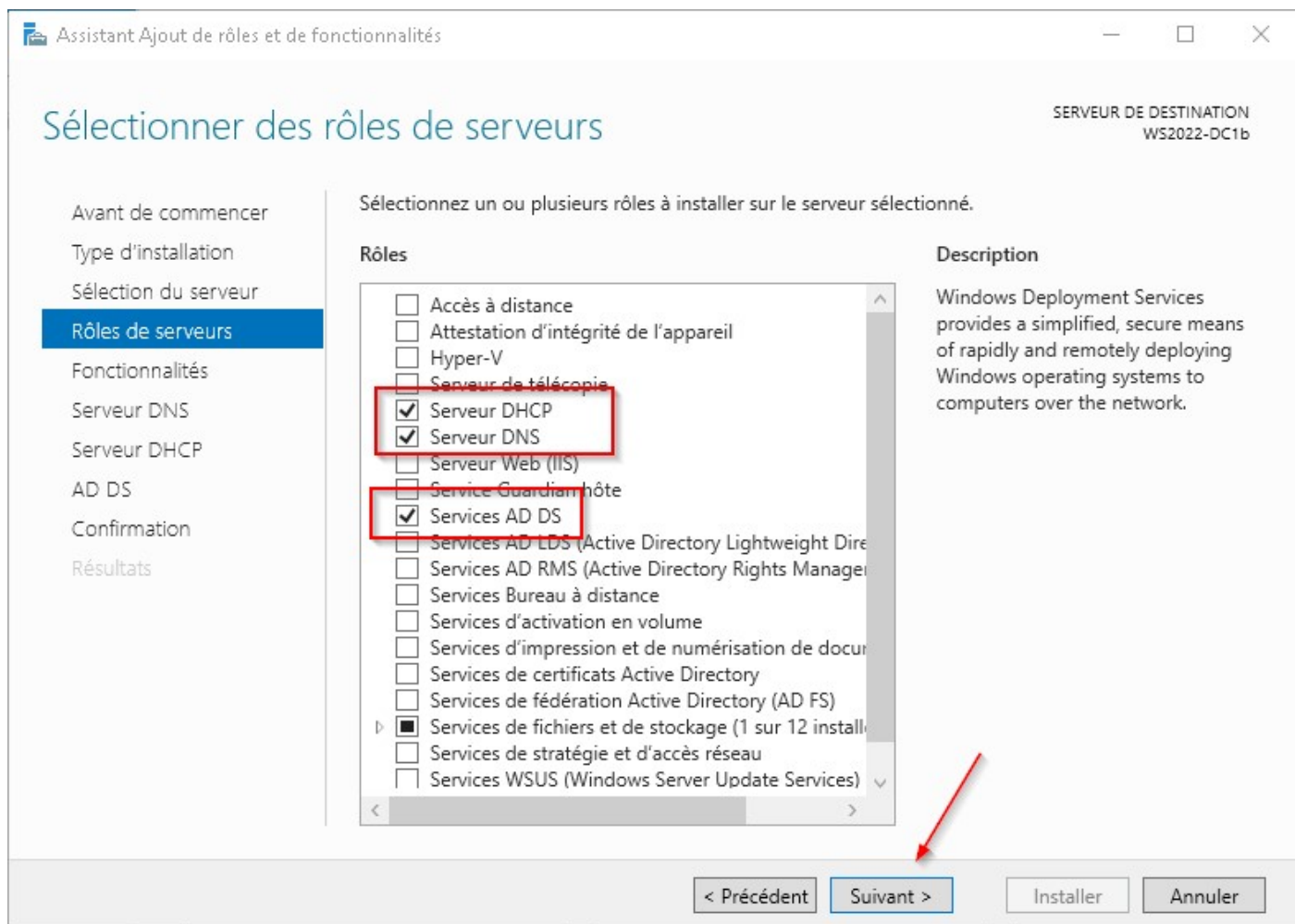
1 ordinateur(s) trouvé(s)

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

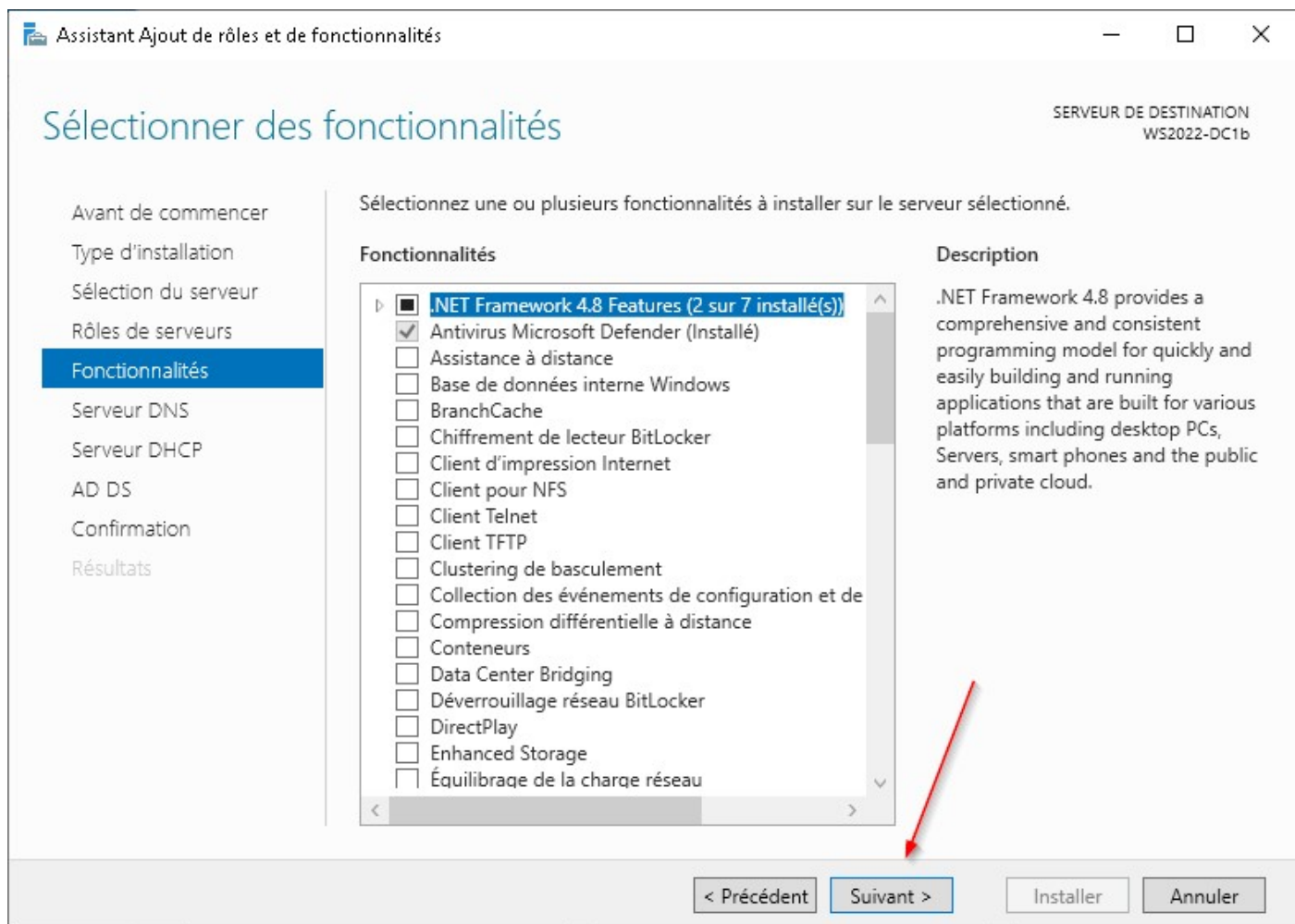
< Précédent Suivant > Installer Annuler

Si votre machine fait partie d'un Pool de Serveurs, pensez à vérifier son nom pour être sûr d'agir sur la bonne machine.

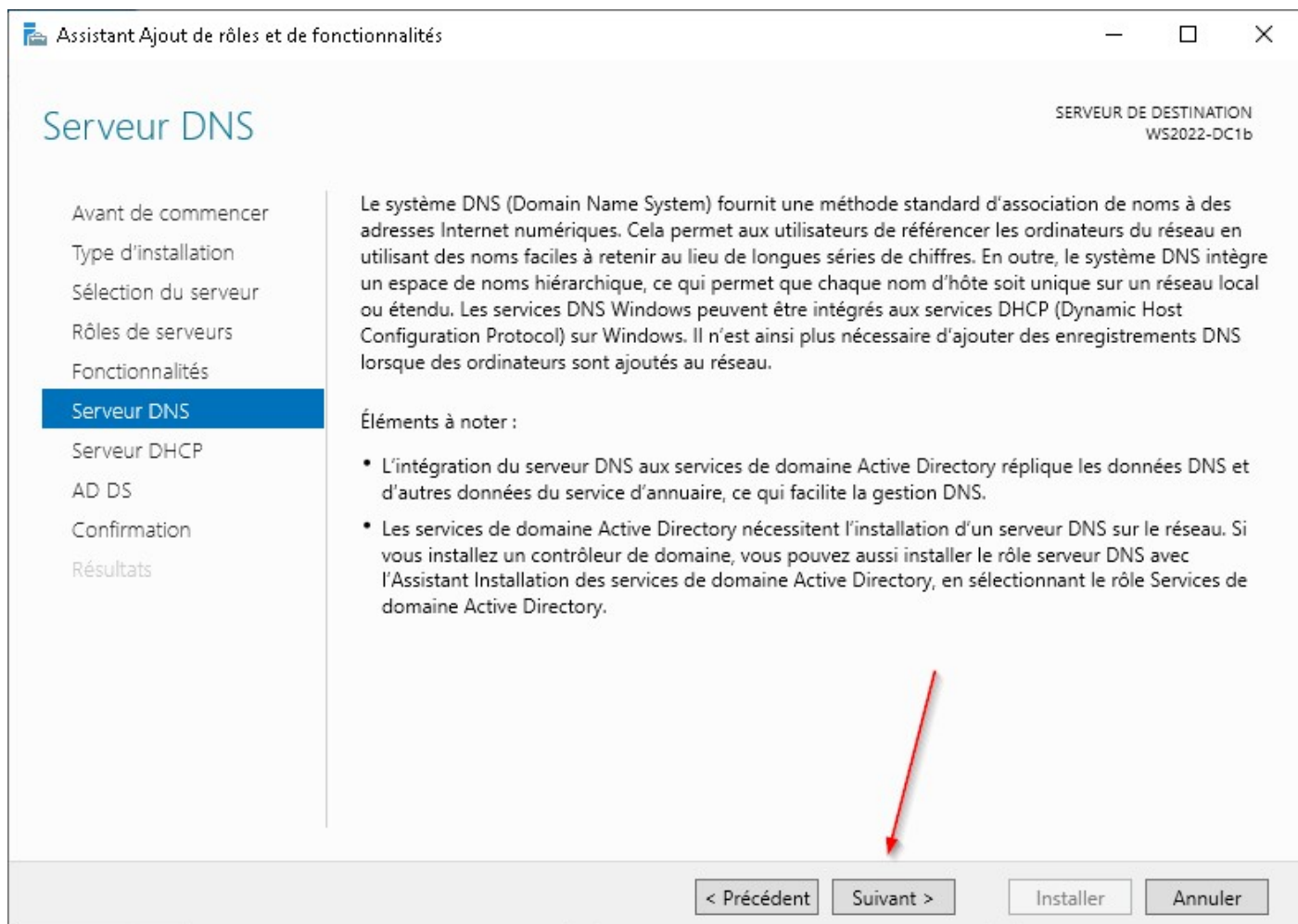
Sélectionnez les rôles nécessaires. Dans notre cas, nous allons utiliser notre serveur pour AD et DHCP, il faut donc activer les rôles DNS, DHCP et AD DS.

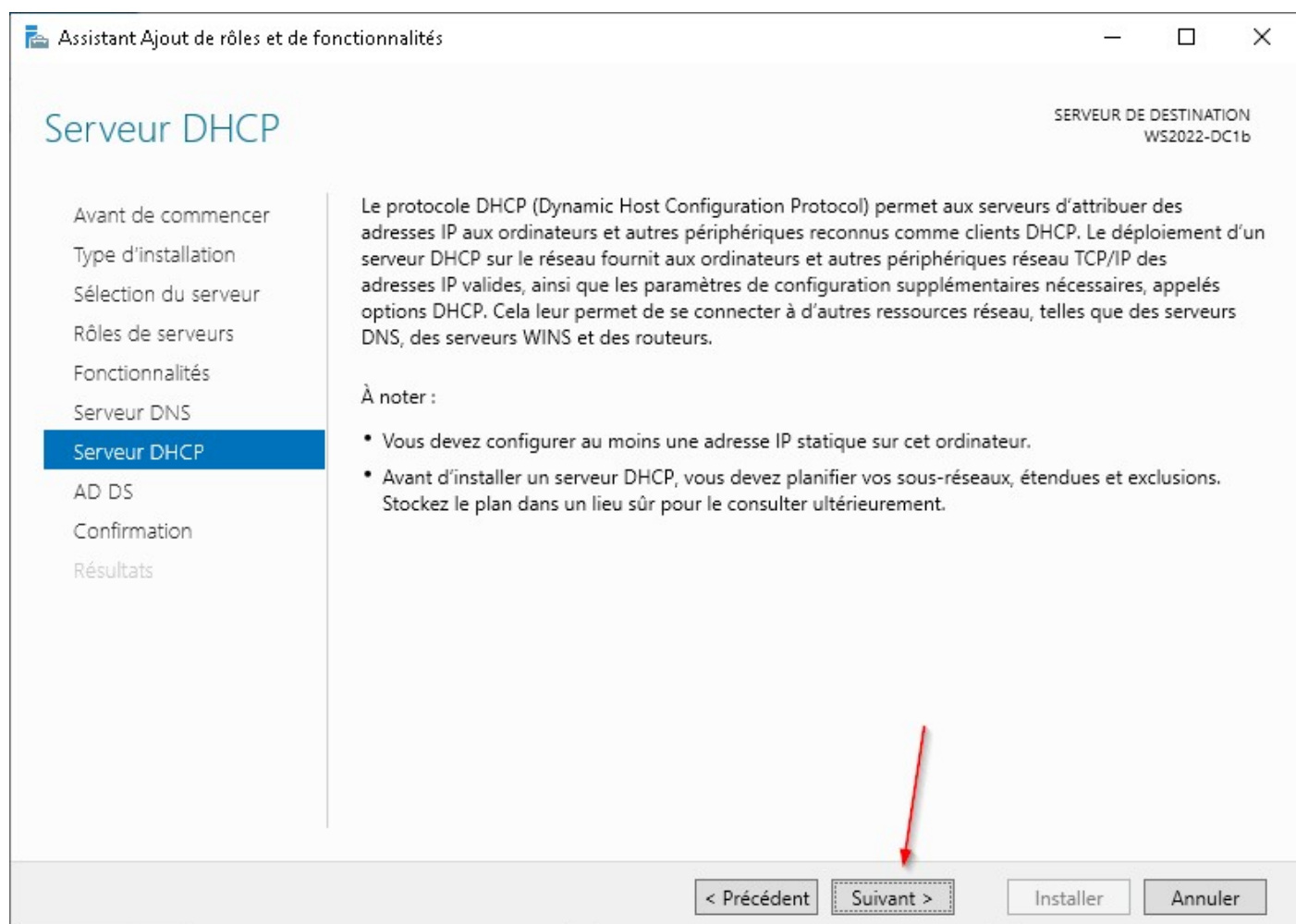


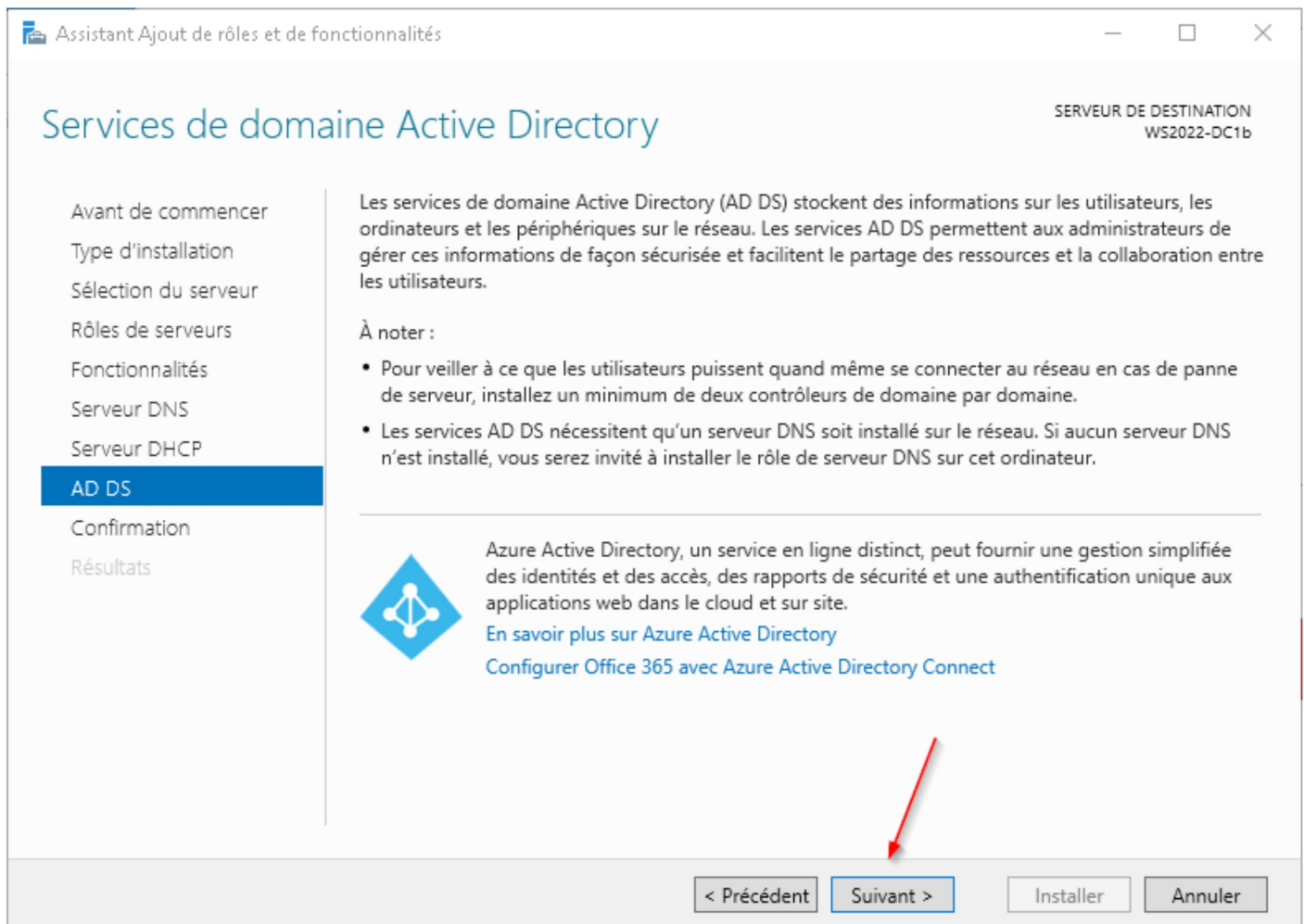
Aucun besoin d'ajouter des fonctionnalités, elles ont déjà été auto-sélectionnées par Windows lors de la sélection des rôles.



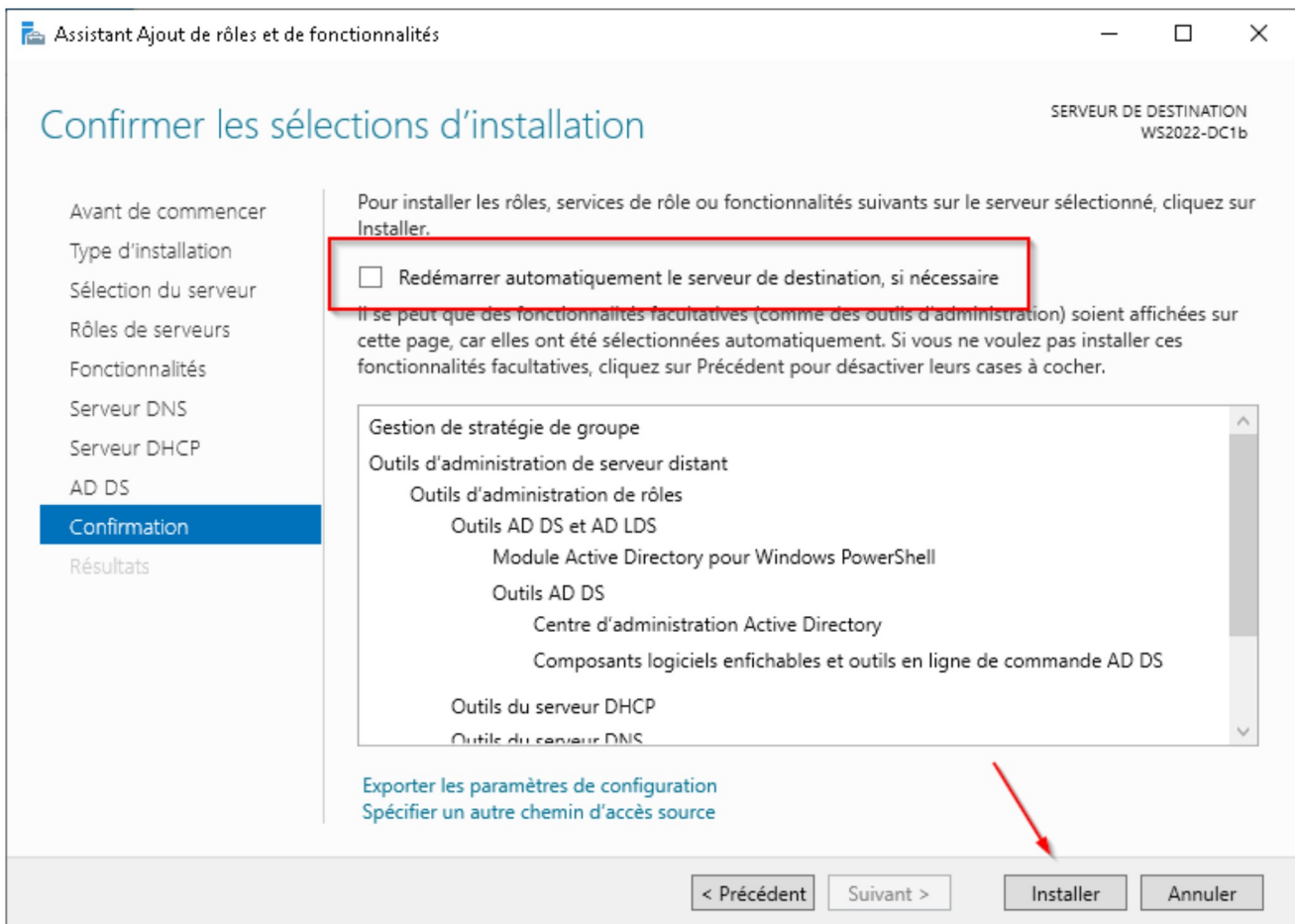
3 fenêtres d'information vont se suivre.



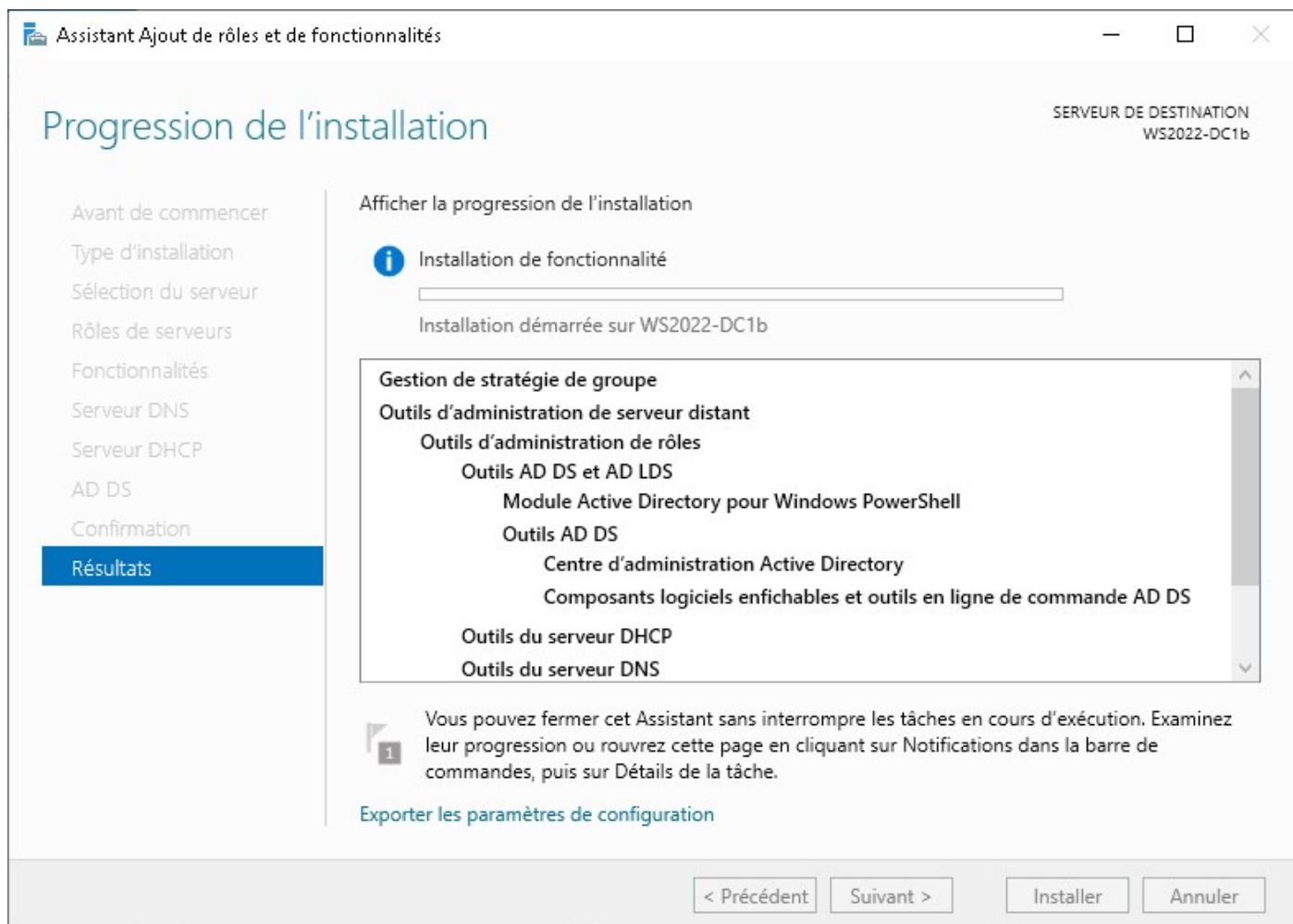




Décochez ensuite la case pour redémarrer la machine, et cliquez sur installer

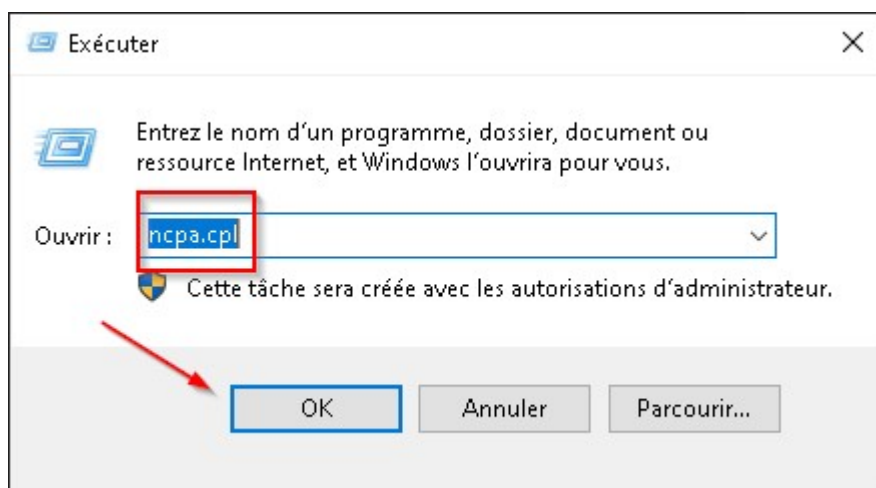


L'installation démarre.

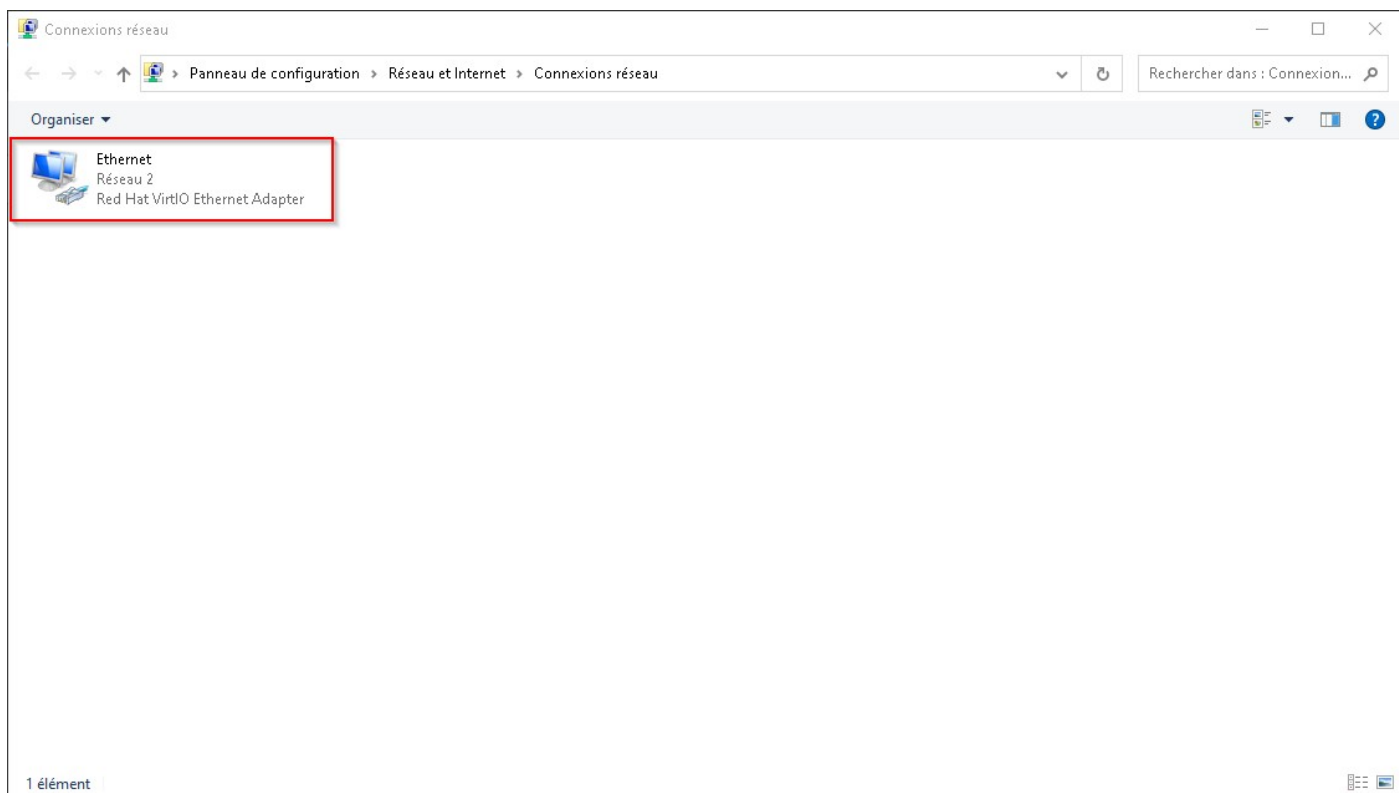


Pendant que les rôles s'installent, nous allons configurer une adresse IP statique sur notre serveur

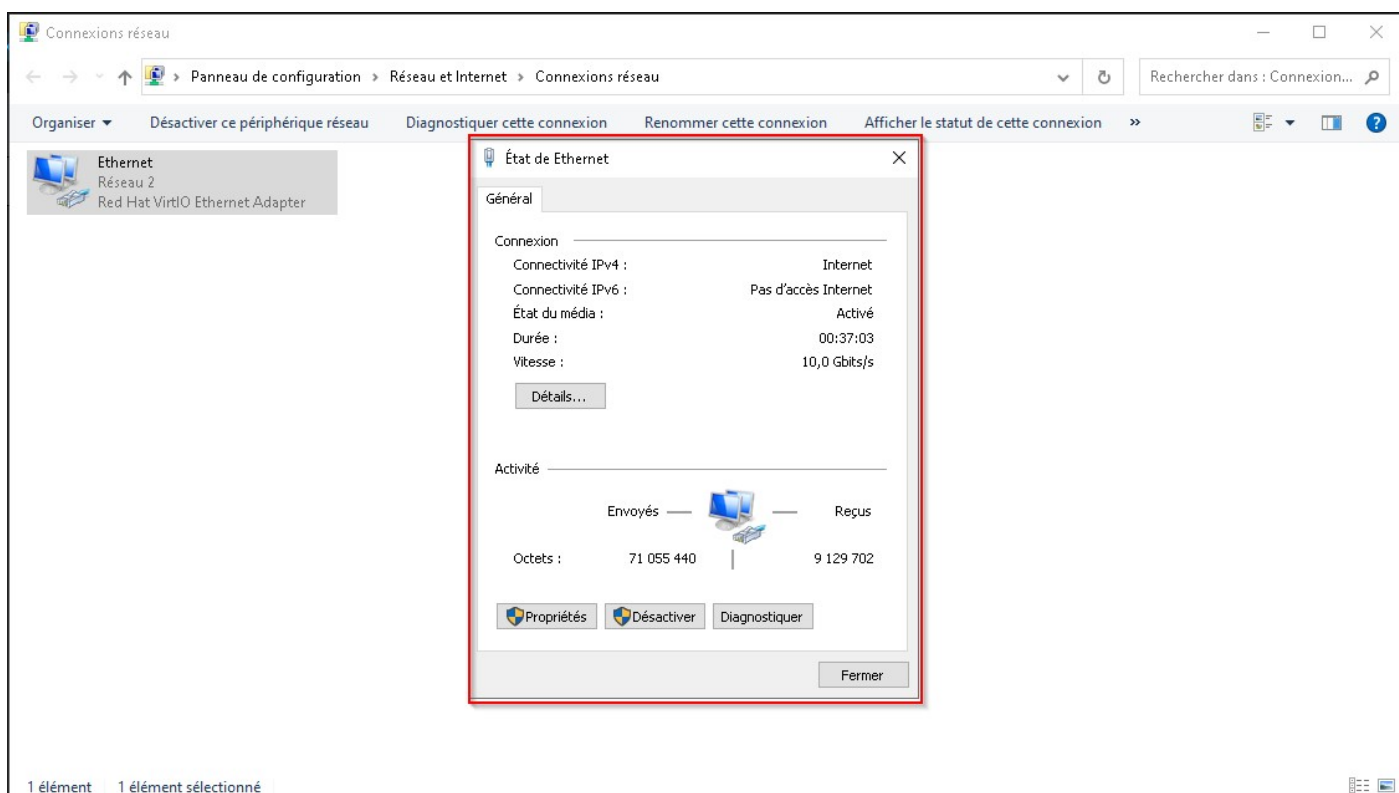
Pour se faire, ouvrez le dialogue d'exécution de Windows via le raccourci "Win+R" et tapez "ncpa.cpl"



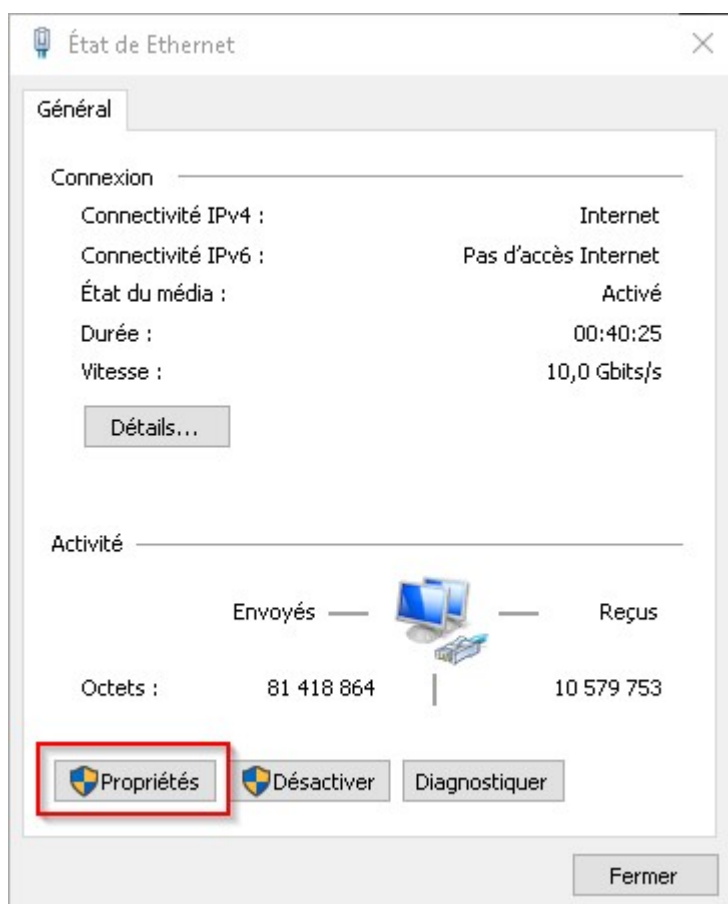
Cela ouvrira le panneau de configuration des adaptateurs réseau. Double-cliquez sur votre interface réseau.



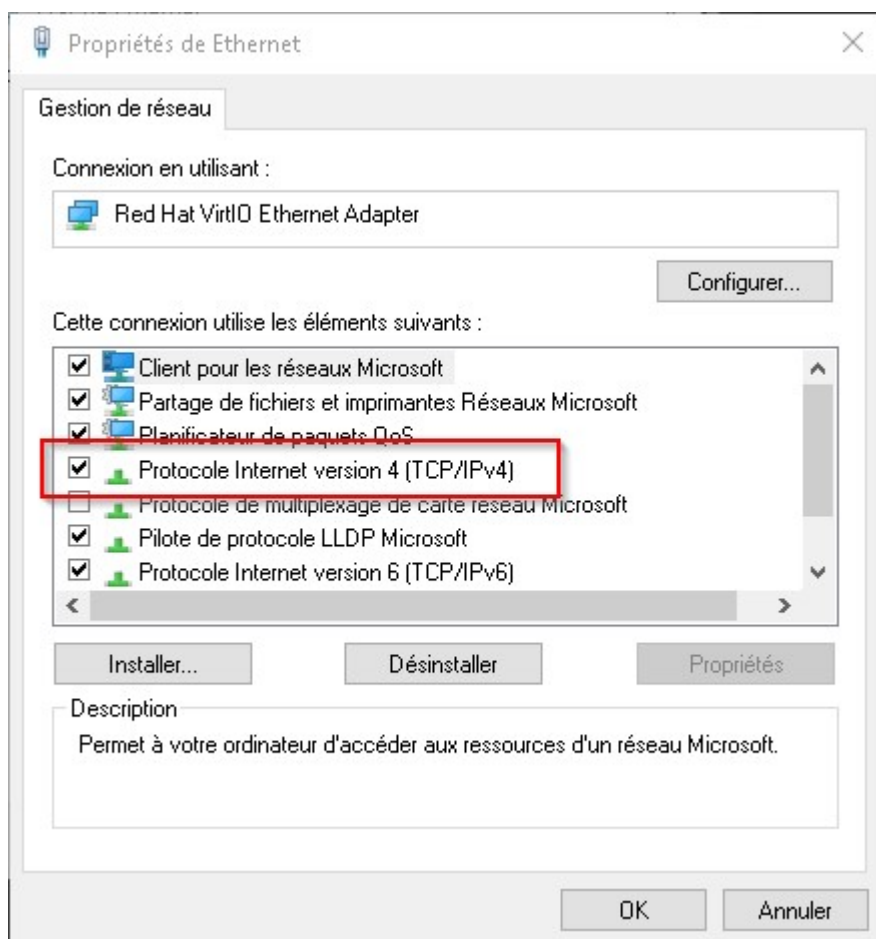
Une fenêtre de propriété apparaît



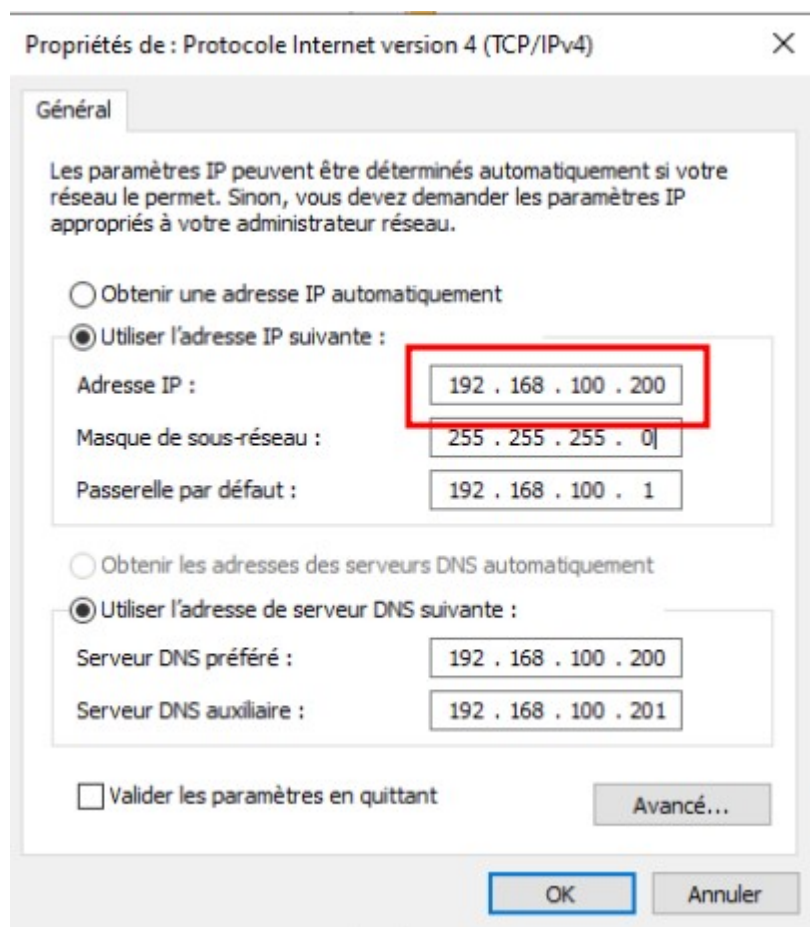
Cliquez ensuite sur "Propriétés"



Double-cliquez sur "Protocole internet version 4"



Configurez ensuite le réseau selon votre environnement, pensez à utiliser l'adresse loopback sur le serveur primaire de votre contrôleur de domaine principal.

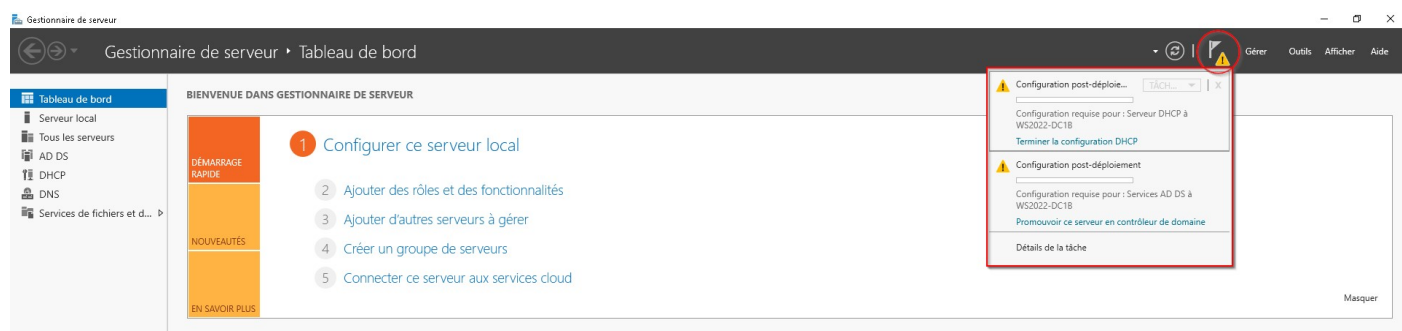


Validez en cliquant sur OK aux fenêtres deux contextuelles et Fermer sur l'interface de propriétés.

Vous pouvez ensuite redémarrer votre machine.

2) Configuration des rôles.

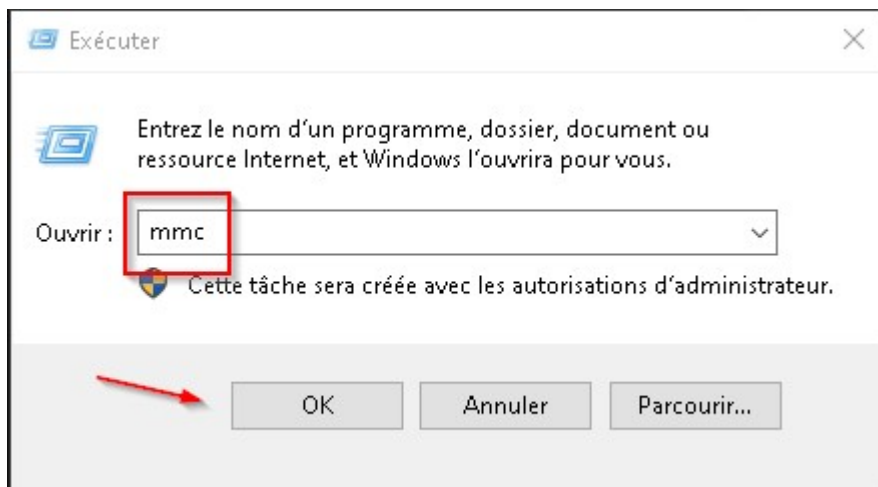
Une fois redémarré, lancez le gestionnaire de serveur, et cliquez sur le drapeau en haut à droite.



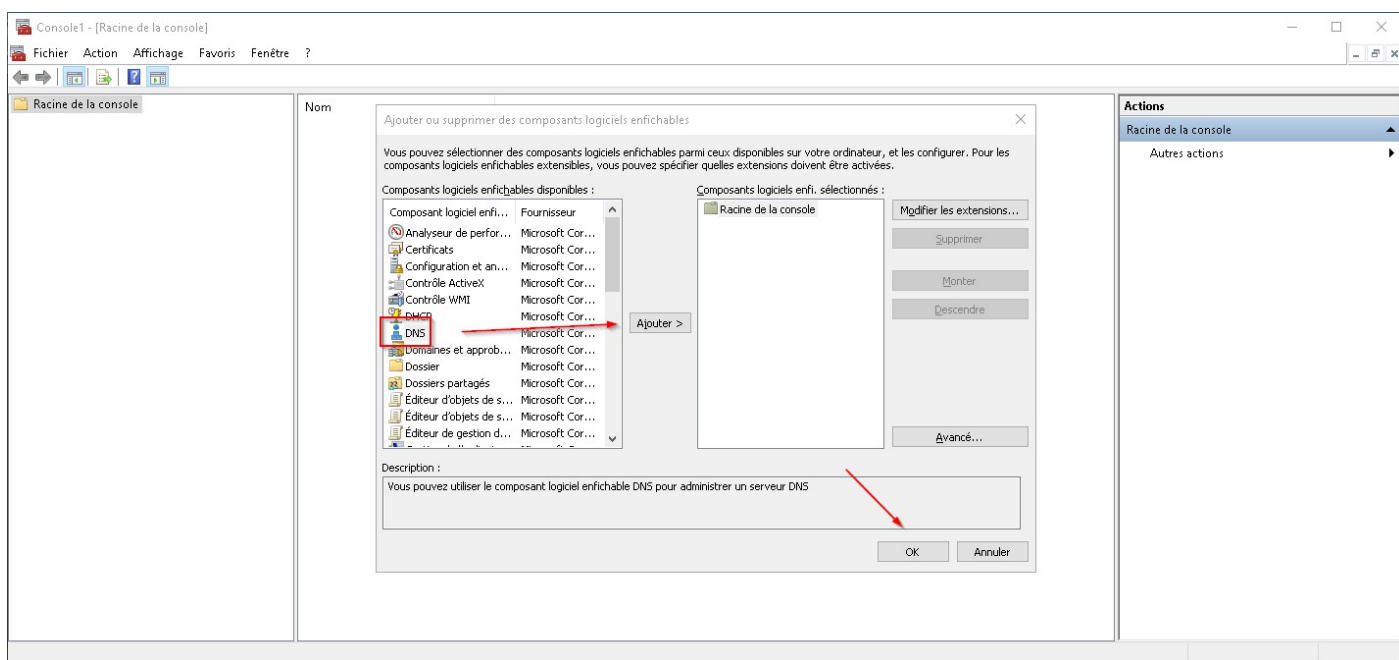
Vous verrez les taches de configuration en suspens.

A. Configuration du DNS.

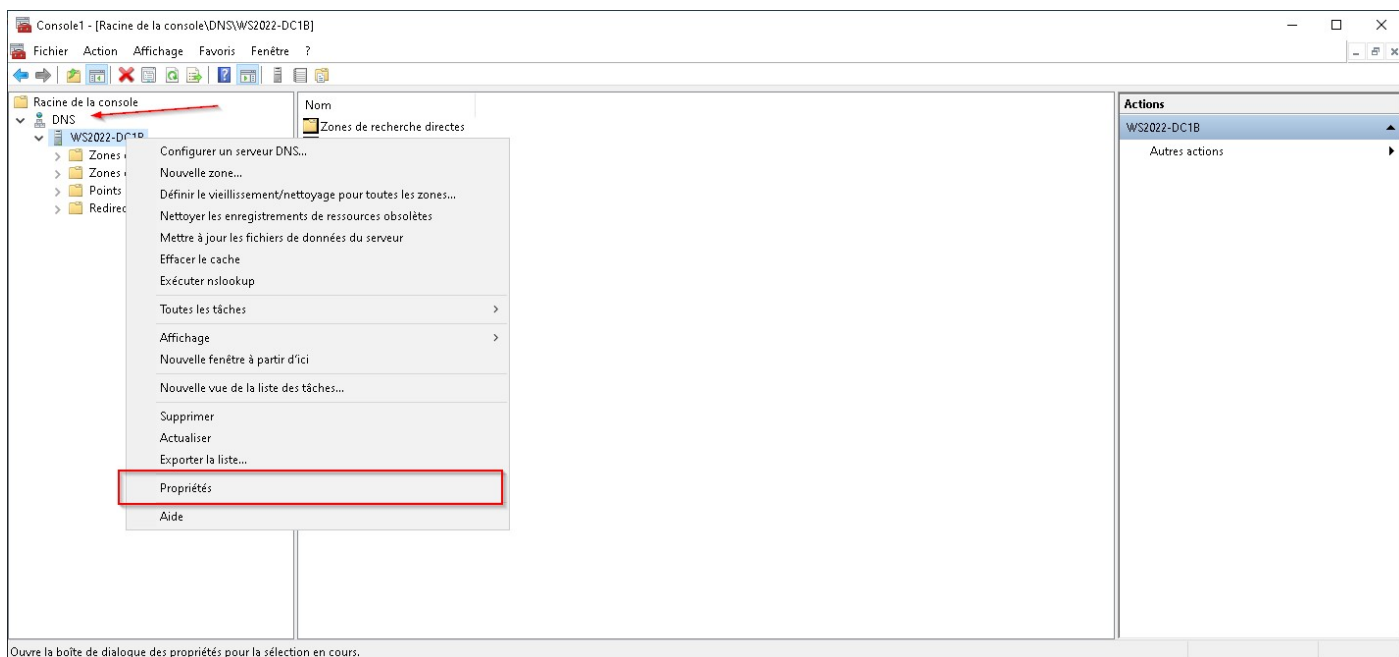
Avant de les effectuer, lancez la console DNS via la console MMC



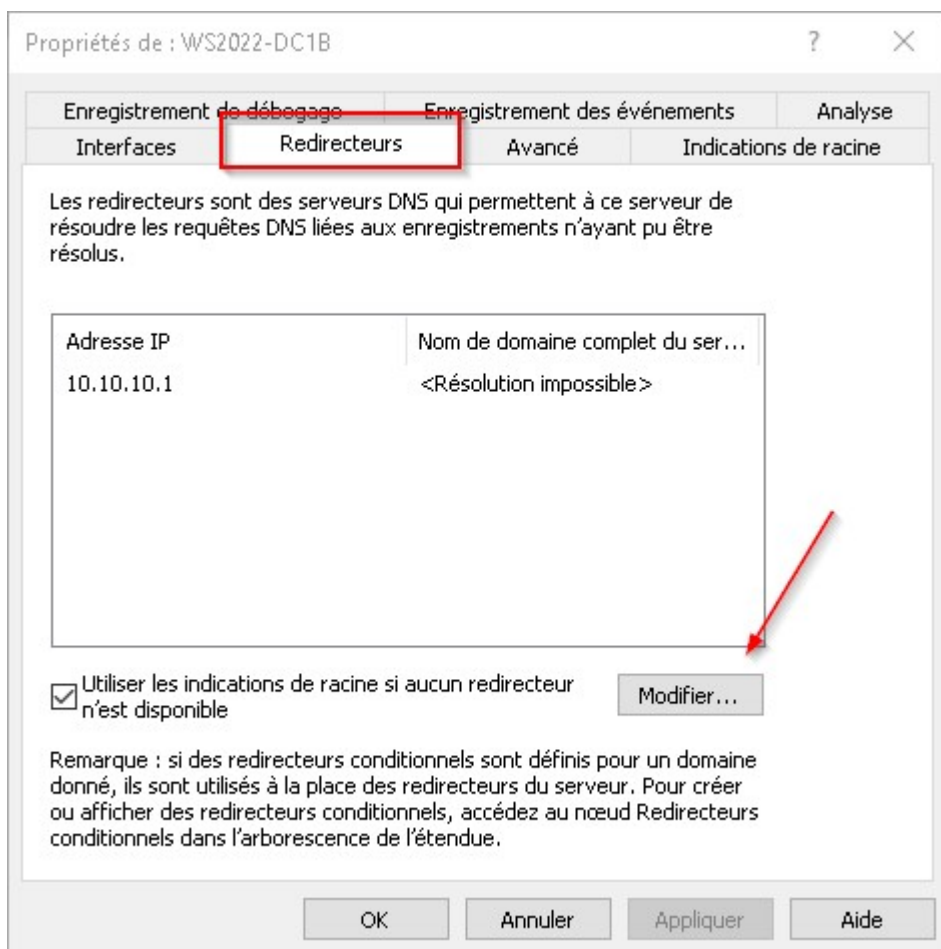
Une fois la console lancée, appuyez sur le raccourci "Ctrl+M" et activez le DNS de la console, et validez avec OK.



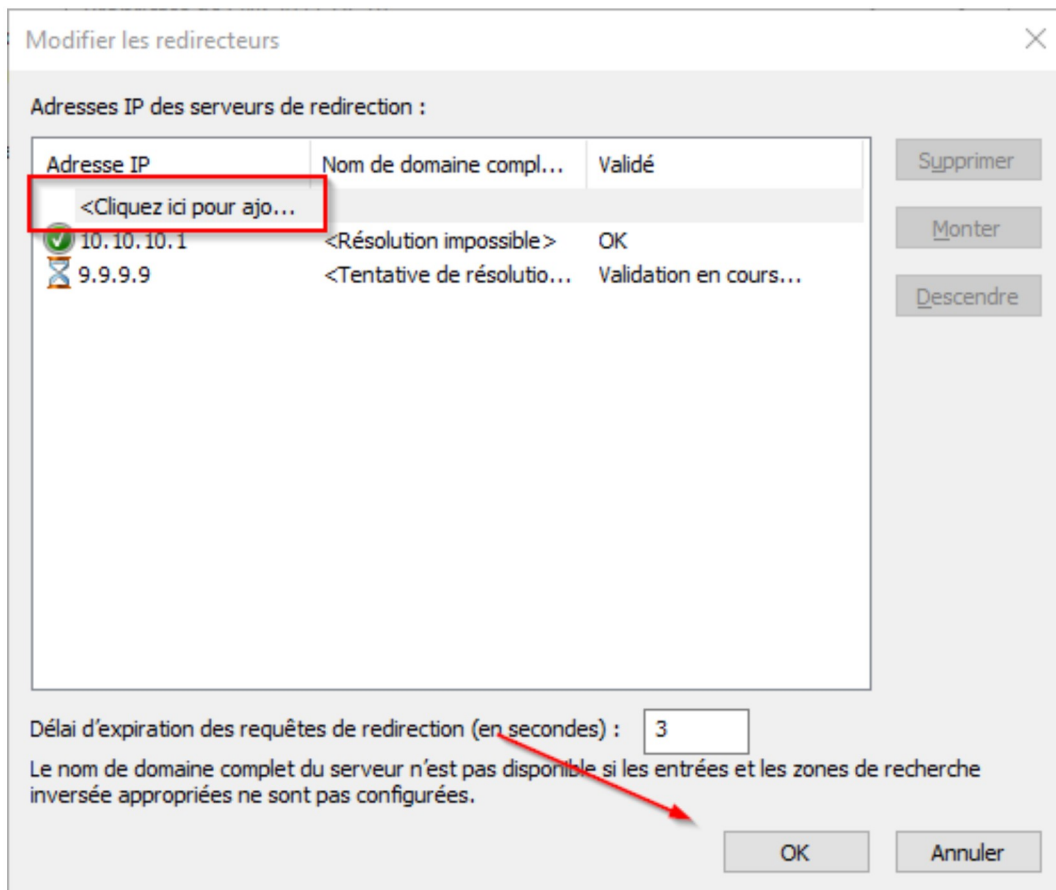
Faites un clic droit sur votre serveur et choisissez les propriétés.



Allez ensuite sur l'onglet redirecteurs, puis sur modifier.



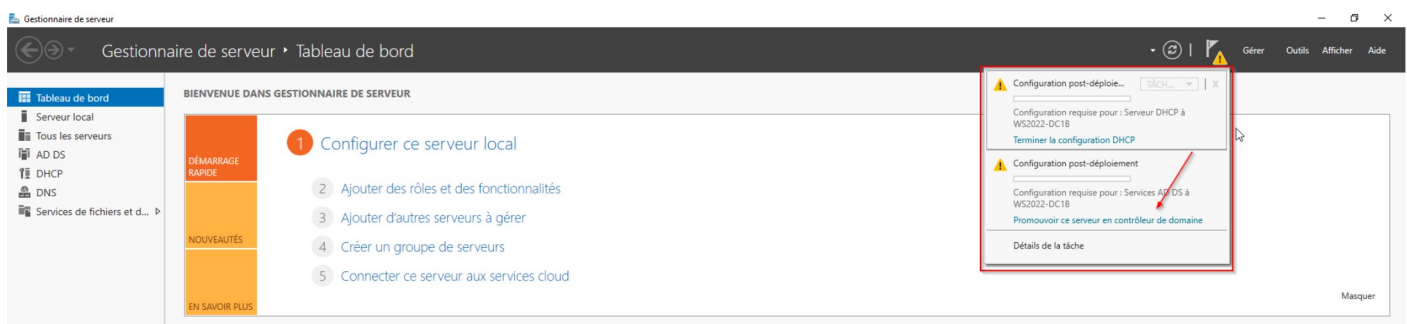
Ajoutez ensuite un ou plusieurs serveurs DNS pour toutes les requêtes sortant des zones DNS que vous gérez.



Validez avec OK sur les deux fenêtres.

B. Configuration d'AD DS.

Revenez dans le menu déroulant sous le drapeau du gestionnaire de serveur, et cliquez sur "Promouvoir ce serveur en contrôleur de domaine"



Vous devrez ensuite créer une nouvelle forêt pour laquelle vous devrez choisir le nom.

Le choix du nom de domaine AD est important. Ce nom doit respecter les restrictions de formatage pour les noms de domaine de l'ICANN. Il est préférable de disposer du contrôle total du domaine, aussi bien sur votre réseau, que via les registrars si vous comptez utiliser des TLD résolubles (.fr ; .com ; .net).

Autrement, vous pouvez utiliser un nom de domaine interne, comme .local ou .lan. A noter que le choix du domaine n'a aucune influence sur la fonctionnalité d'Active Directory.

Assistant Configuration des services de domaine Active Directory

— □ ×

SERVEUR CIBLE
W2022-DC1-SA

Configuration de déploiement

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

Sélectionner l'opération de déploiement

- ☐ Ajouter un contrôleur de domaine à un domaine existant
- ☐ Ajouter un nouveau domaine à une forêt existante
- ☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

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

< Précédent Suivant > Installer Annuler

Vous devez ensuite choisir le niveau fonctionnel de la forêt. Laissez le niveau sur le plus récent si votre réseau n'intègre pas d'autres domaines et forêts AD. Choisissez ensuite un mot de passe pour la restauration AD, gardez-le en lieu et place sur, il sera nécessaire en cas de problème sur l'intégrité de l'annuaire.

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SERVEUR CIBLE
WS2022-DC1b

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

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

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

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

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

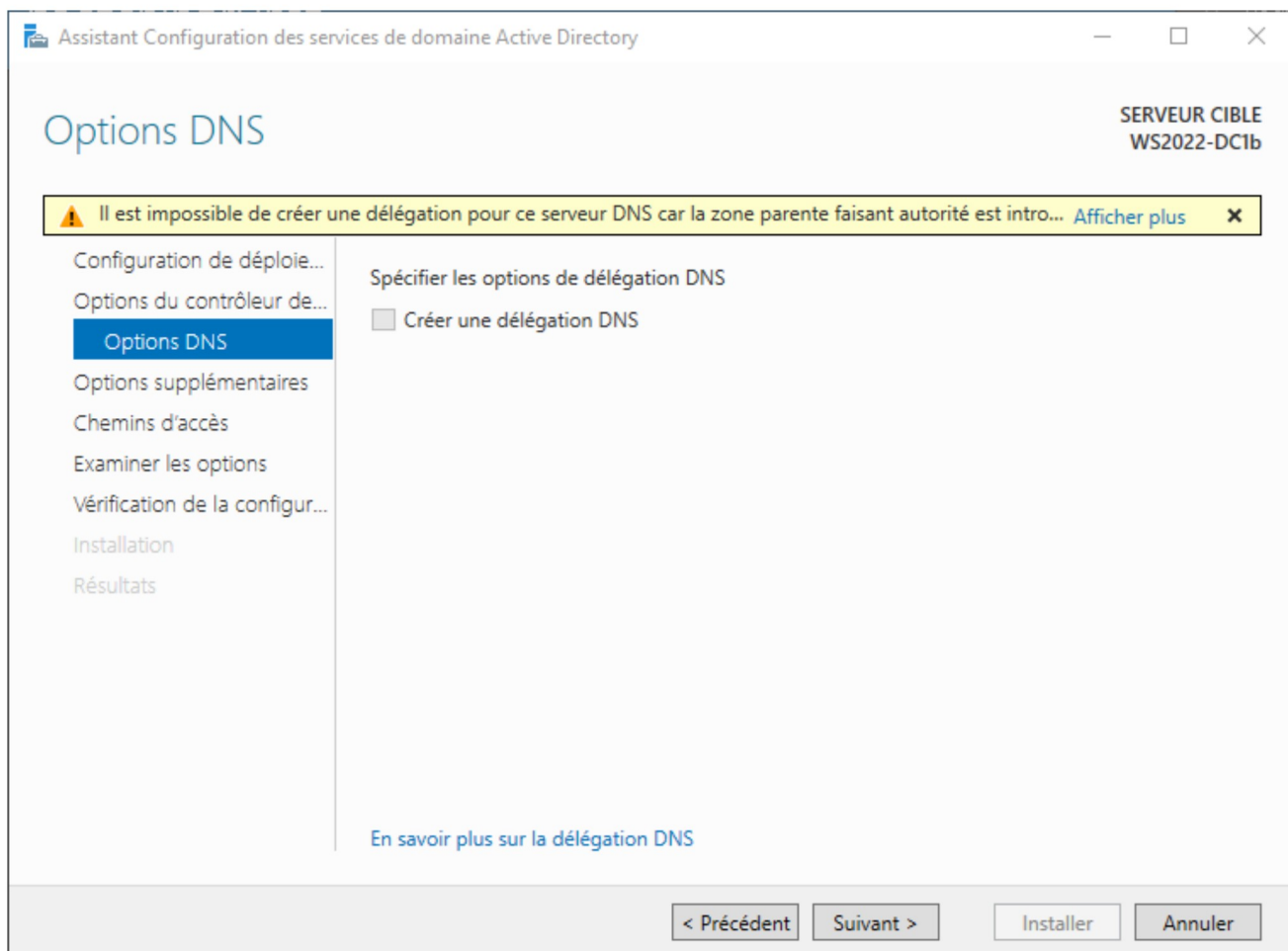
Mot de passe : *

Confirmer le mot de passe : *

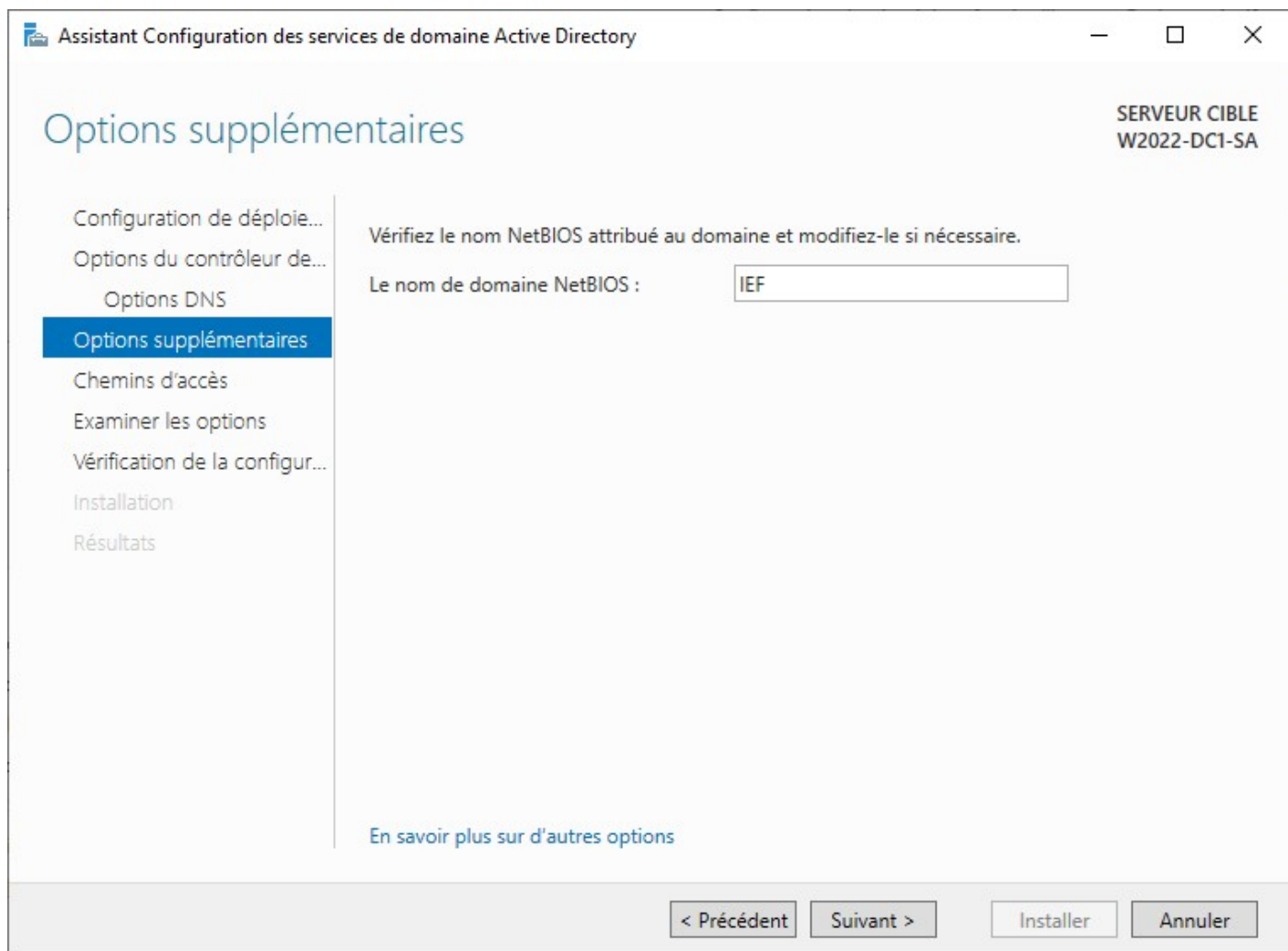
[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent Suivant > Installer Annuler

Une fois validé, le dialogue affichera suivant un message d'erreur. Pour une nouvelle forêt, vous pouvez l'ignorer.



Vous pourrez ensuite changer votre nom NetBIOS,



Vous pourrez ensuite choisir le dossier d'installation de la base de données du serveur. Il est recommandé de mettre l'instance du domaine sur un disque secondaire, redondé.

Assistant Configuration des services de domaine Active Directory

SERVEUR CIBLE
WS2022-DC1b

Chemins d'accès

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

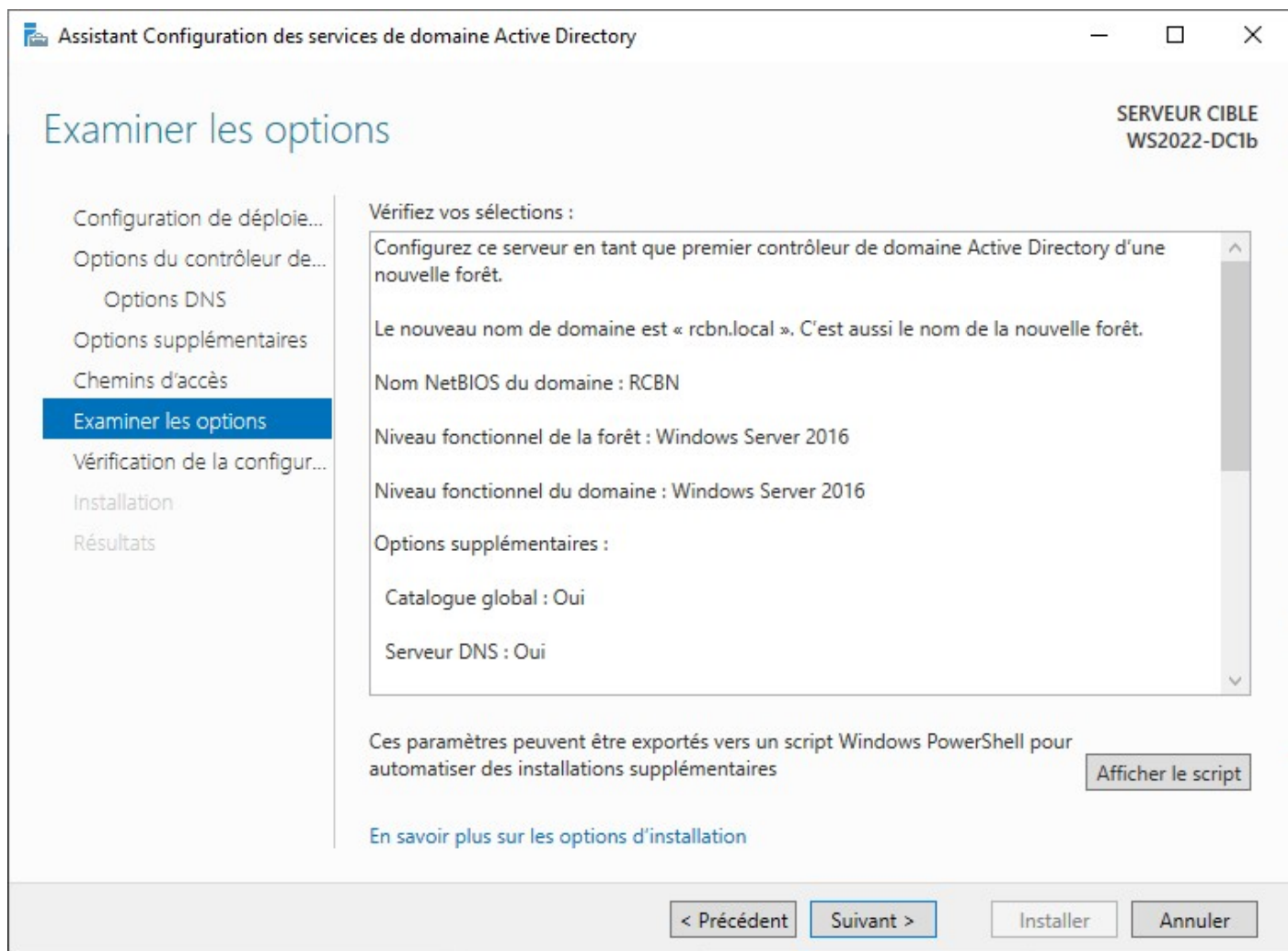
Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

Dossier de la base de données :	D:\NTDS	...
Dossier des fichiers journaux :	D:\NTDS	...
Dossier SYSVOL :	D:\SYSVOL	...

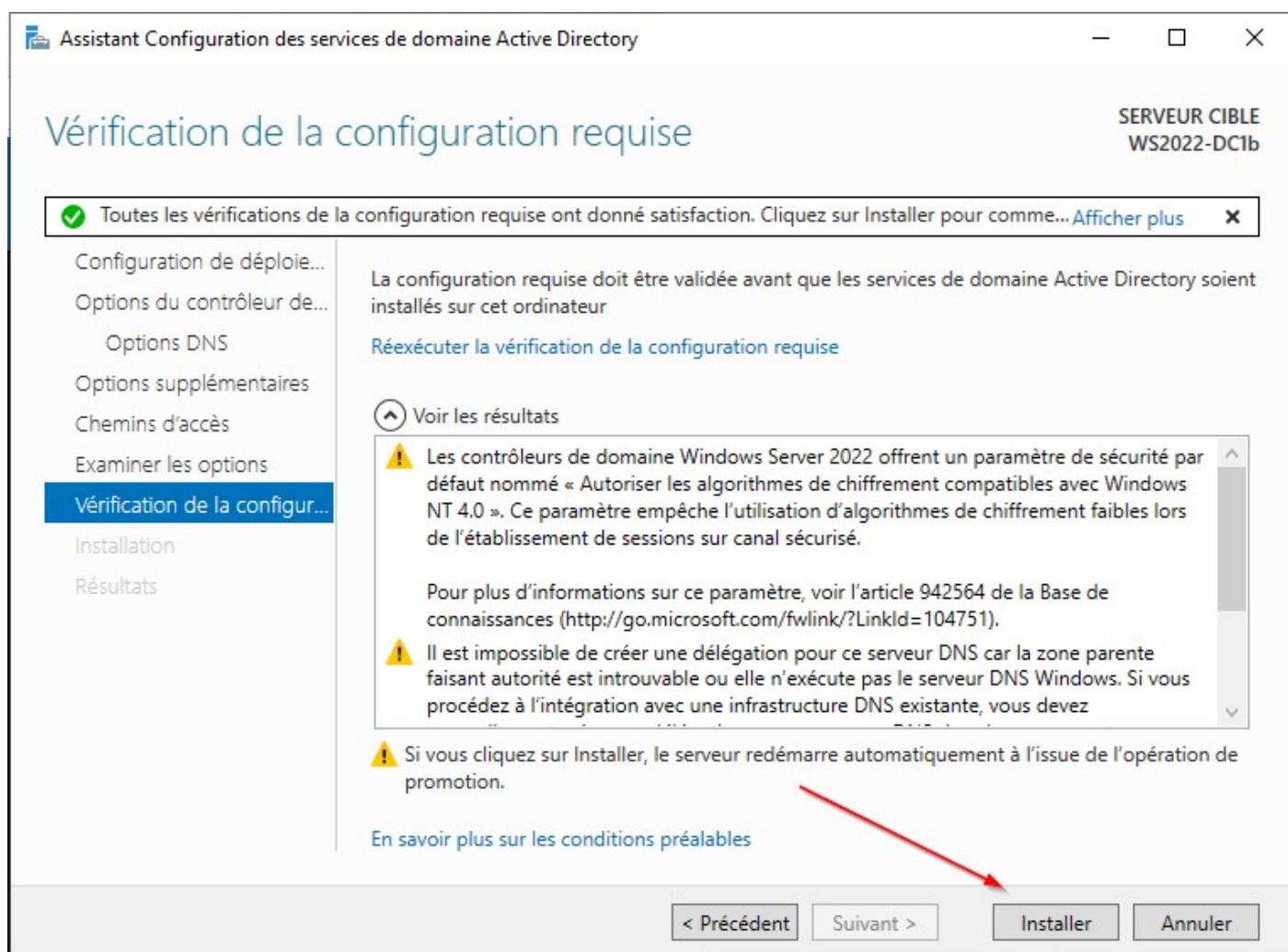
[En savoir plus sur les chemins d'accès Active Directory](#)

< Précédent Suivant > Installer Annuler

Un récapitulatif de la configuration du domaine vous sera présenté, Vérifiez les informations et appuyez sur suivant



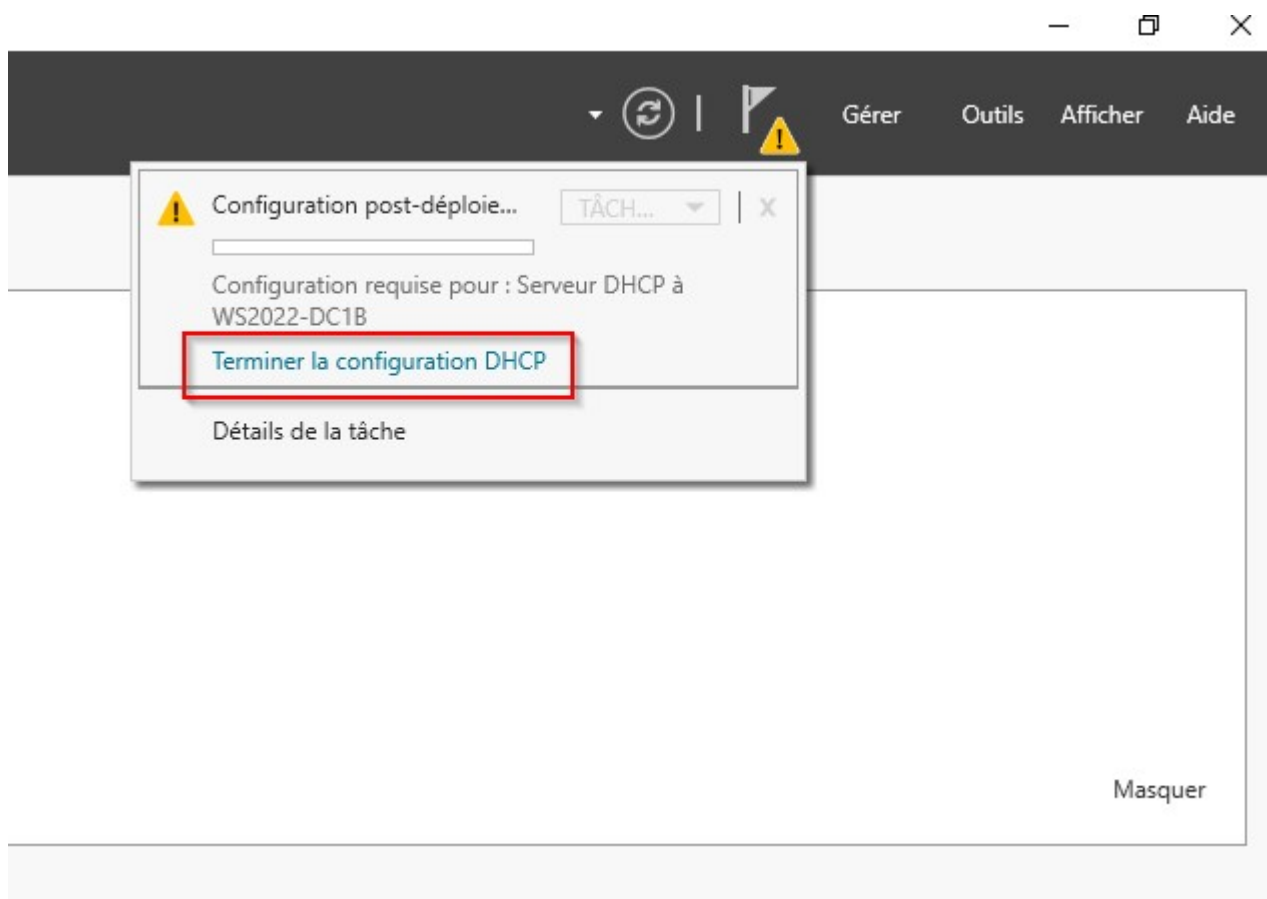
Windows Vérifiez ensuite la configuration de votre machine, et vous proposera de corriger certains problèmes pour vous. Une fois tous les prérequis validés, vous pourrez finalement terminer l'installation du domaine.



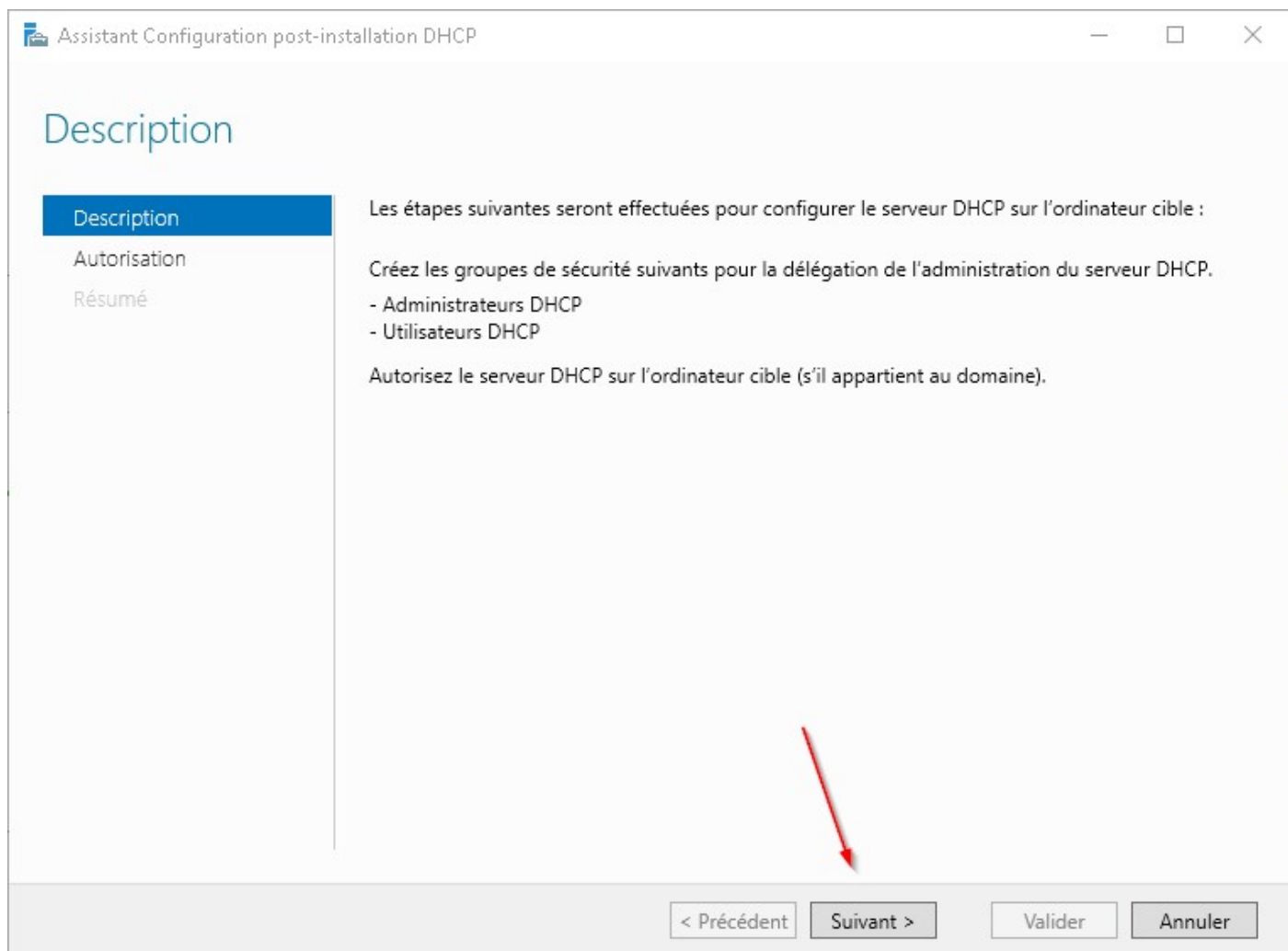
Votre serveur va redémarrer pour finaliser l'installation.

C. Installation du DHCP.

Cliquez sur le panneau en haut à droite puis sur "Terminer la configuration DHCP".



Une fenêtre va s'ouvrir avec des instructions.



Renseignez bien votre nom d'utilisateur et valider ensuite.

Assistant Configuration post-installation DHCP

Autorisation

Description

Autorisation

Résumé

Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.

☒ Utiliser les informations d'identification de l'utilisateur suivant


Nom d'utilisateur : RCBN\Administrateur

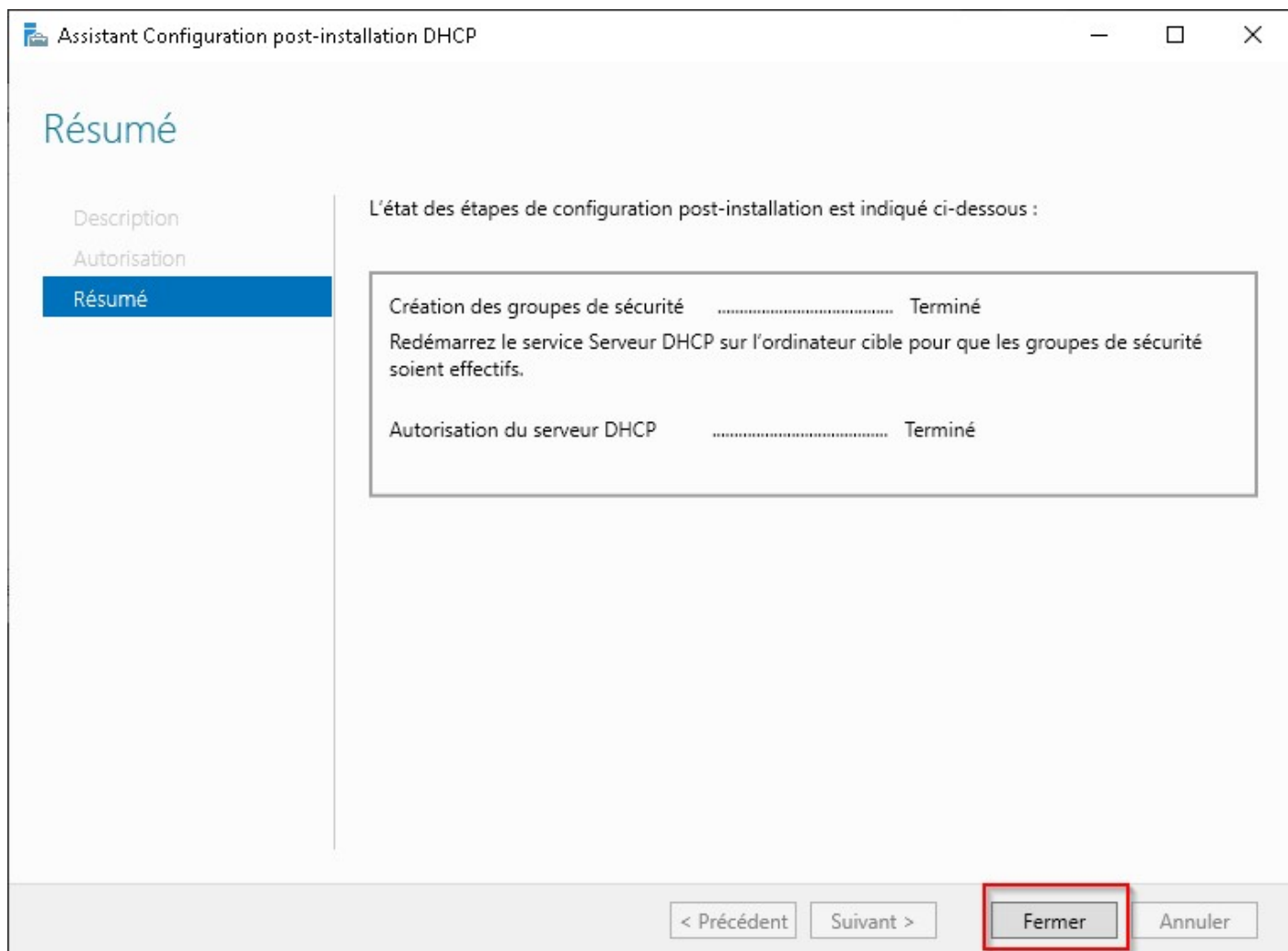
☐ Utiliser d'autres informations d'identification

Nom d'utilisateur :

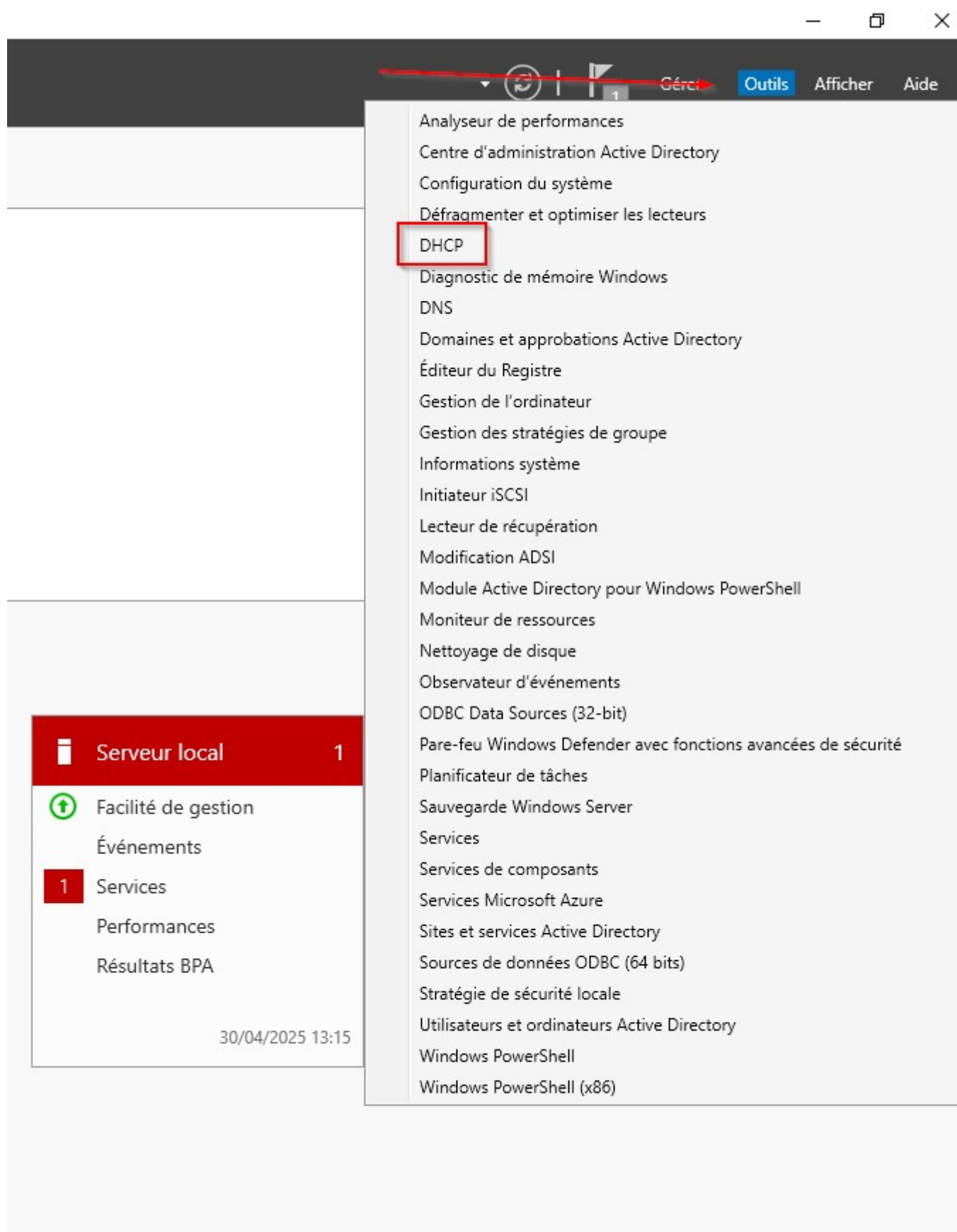
☐ Ignorer l'autorisation AD

< Précédent Suivant > Valider Annuler

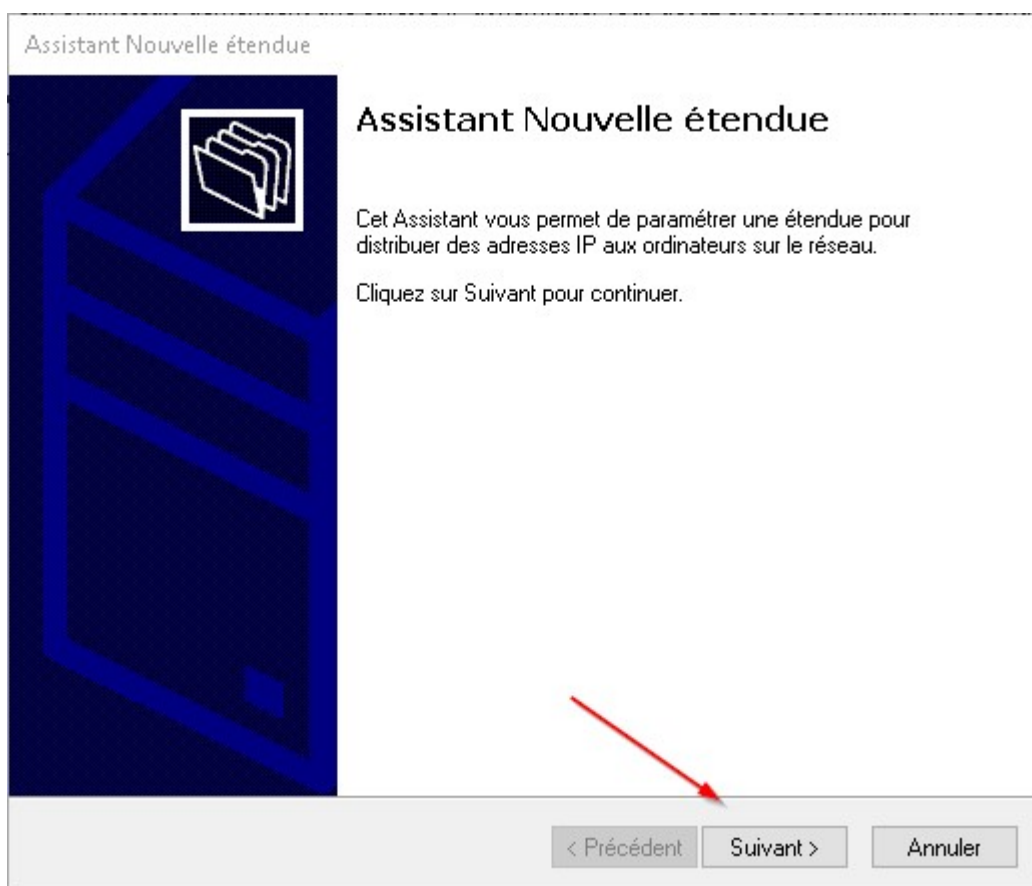
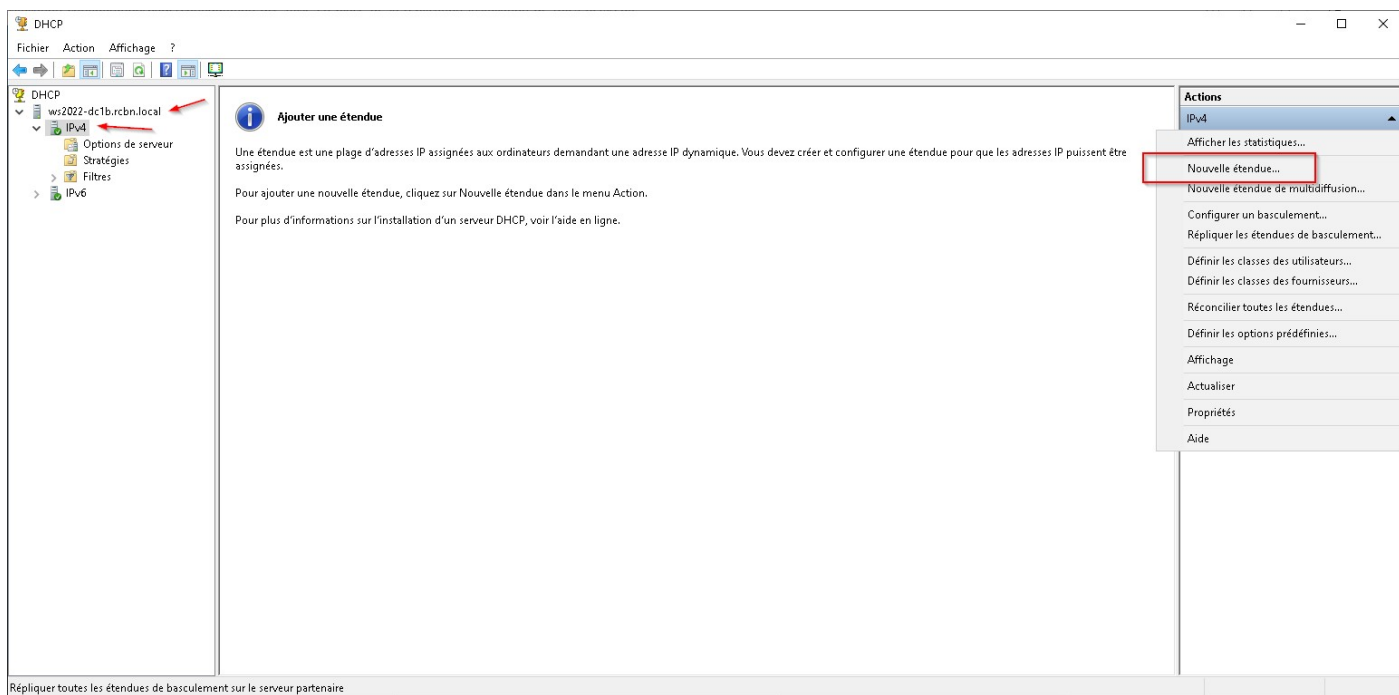




Maintenant on va ajouter une nouvelle extension au DHCP, pour cela aller dans outils puis DHCP.



Ouvrez le dossier IPv4 puis cliquez droit dessus et sélectionnez ensuite « Nouvelle étendue ».



Ajouter un nom ainsi qu'une description.

Assistant Nouvelle étendue

Nom de l'étendue

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.

Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom :

Description :

< Précédent Suivant > Annuler

Complétez la plage d'adresse IP de l'étendue avec une adresse IP de début et de fin pour le serveur DHCP ainsi que la longueur du masque de sous réseau.

Assistant Nouvelle étendue

Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP

Longueur :

Masque de sous-réseau :

< Précédent Suivant > Annuler

Assistant Nouvelle étendue

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCP OFFER.

Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début : Adresse IP de fin :

Plage d'adresses exclue :

Retard du sous-réseau en millisecondes :

Assistant Nouvelle étendue

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

Cochez la première option puis cliquez sur suivante.

Assistant Nouvelle étendue

Configuration des paramètres DHCP

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.

Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

☒ Oui, je veux configurer ces options maintenant

☐ Non, je configurerai ces options ultérieurement

< Précédent Suivant > Annuler

Ajoutez l'adresse IP du routeur.

Assistant Nouvelle étendue

Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.

Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

Ajouter

Supprimer

Monter

Descendre

< Précédent Suivant > Annuler

Ajoutez d'abord le nom du domaine parent et ensuite l'adresse IP des serveurs DNS.

Assistant Nouvelle étendue

Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.

Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :

Adresse IP :

Assistant Nouvelle étendue

Serveurs WINS

Les ordinateurs fonctionnant avec Windows peuvent utiliser les serveurs WINS pour convertir les noms NetBIOS d'ordinateurs en adresses IP.

Entrer les adresses IP ici permet aux clients Windows d'interroger WINS avant d'utiliser la diffusion pour s'enregistrer et résoudre les noms NetBIOS.

Nom du serveur :

Adresse IP :

Pour modifier ce comportement pour les clients DHCP Windows, modifiez l'option 046, type de nœud WINS/NBT, dans les options de l'étendue.

Sélectionnez la première option.

Assistant Nouvelle étendue

Activer l'étendue
Les clients ne peuvent obtenir des baux d'adresses que si une étendue est activée.

Voulez-vous activer cette étendue maintenant ?

☒ Oui, je veux activer cette étendue maintenant

☐ Non, j'activerai cette étendue ultérieurement

< Précédent Suivant > Annuler

Assistant Nouvelle étendue

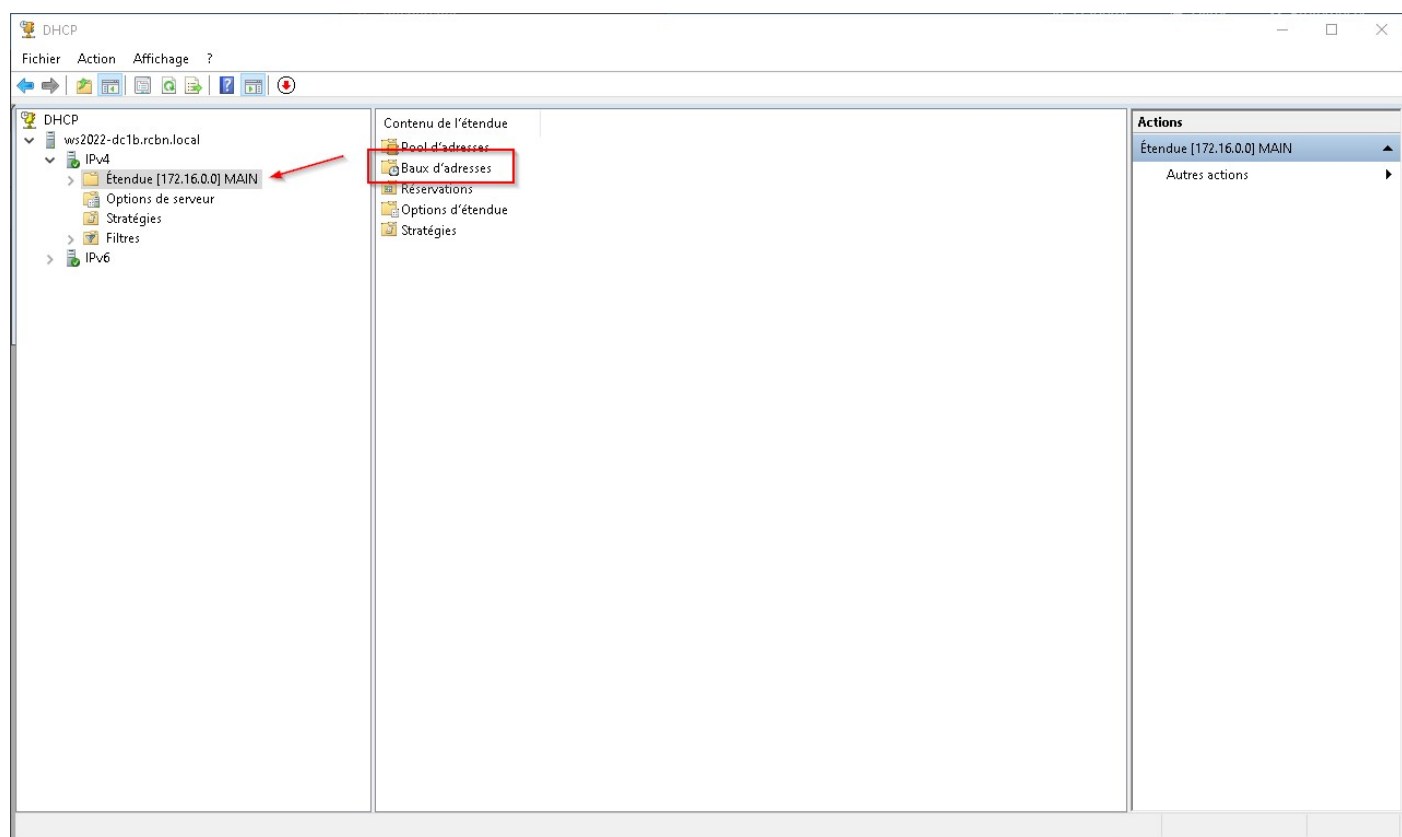
Fin de l'Assistant Nouvelle étendue
L'Assistant Nouvelle étendue s'est terminé correctement.

Pour offrir une haute disponibilité pour cette étendue, configurez le basculement pour l'étendue nouvellement ajoutée en cliquant avec le bouton droit sur l'étendue, puis en cliquant sur Configurer un basculement.

Pour fermer cet Assistant, cliquez sur Terminer.

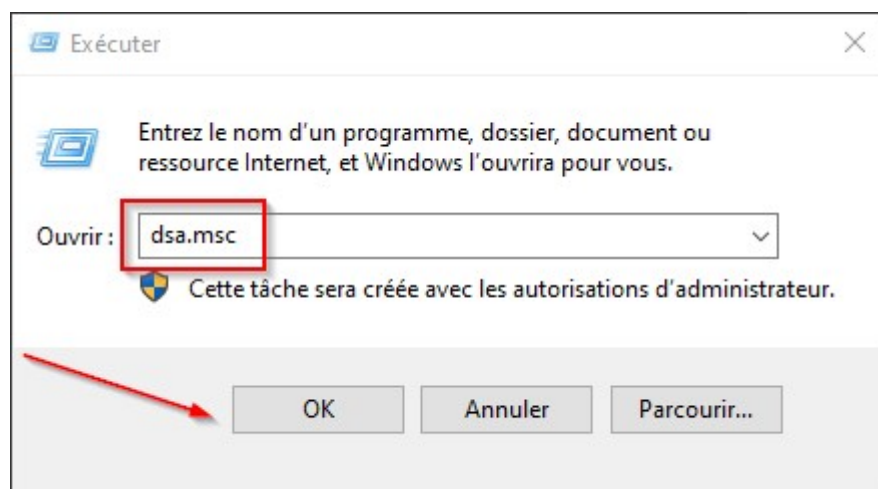
< Précédent Terminer Annuler

Maintenant dans le dossier IPv4 on aperçoit l'étendue qu'on vient de créer.

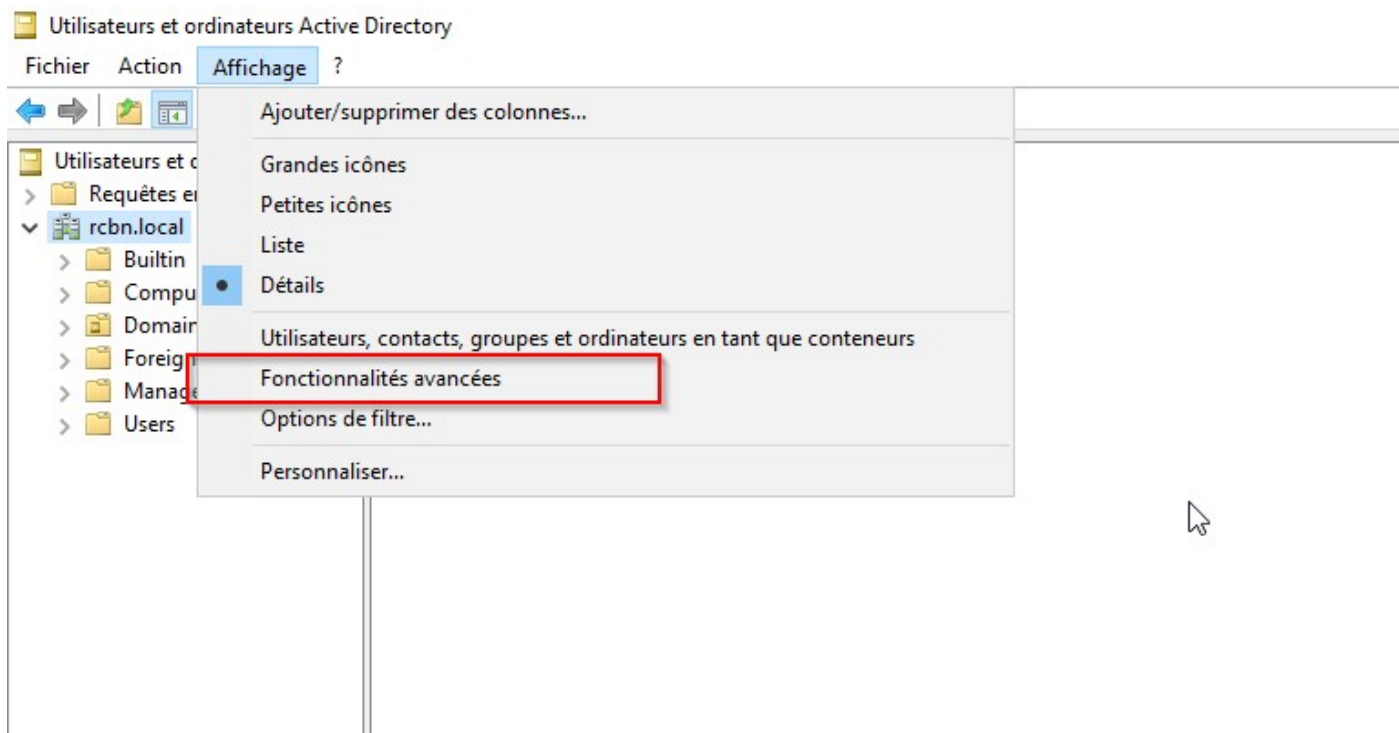


3) Préparation à l'exploitation du domaine.

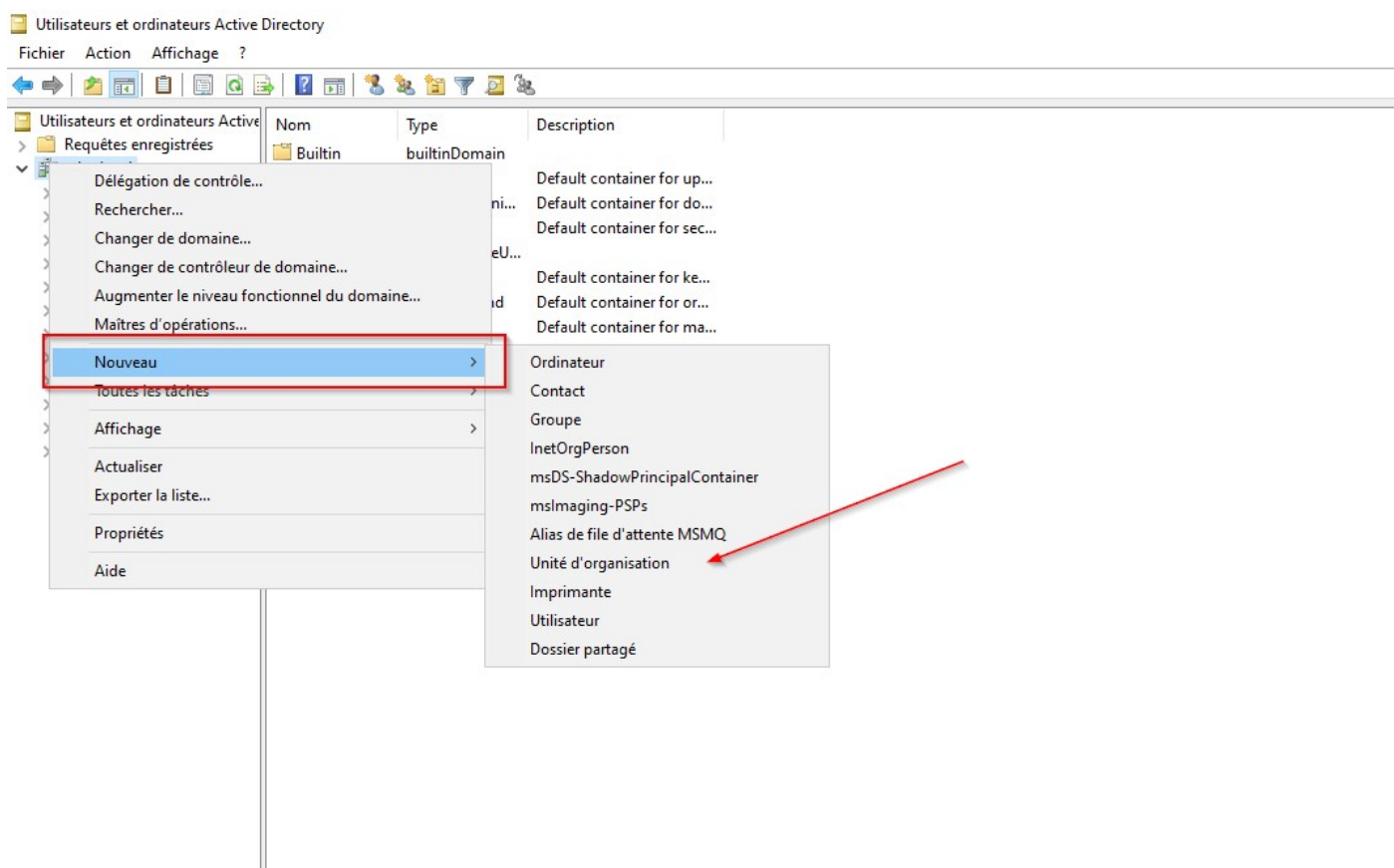
Une fois relancé, nous allons créer certains objets dans la Console "Utilisateurs et Ordinateurs Active Directory". Pour la lancer, tapez "dsa.msc" dans la fenêtre "Exécuter".



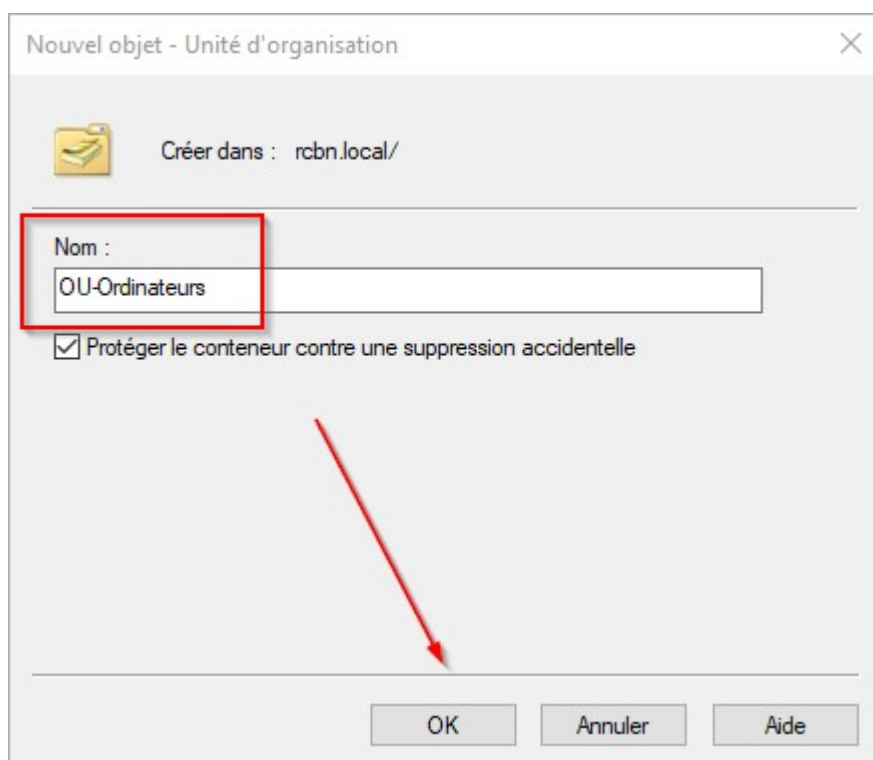
Une fois la console lancée, cliquez sur "Affichage" et activez les Fonctionnalités avancées.



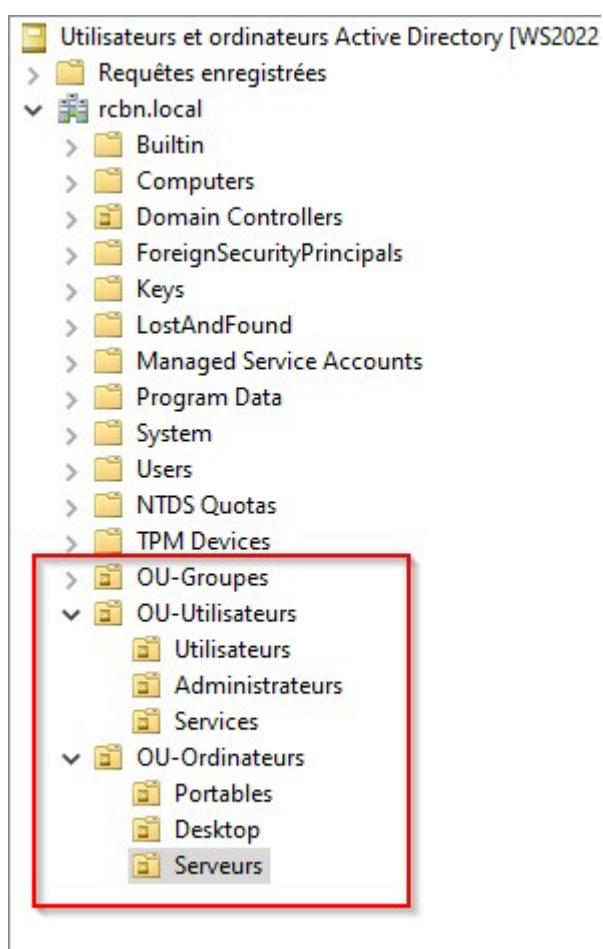
Faites ensuite un clic droit sur l'icône du domaine, puis dans le menu "Nouveau" choisissez "Unité d'Organisation".



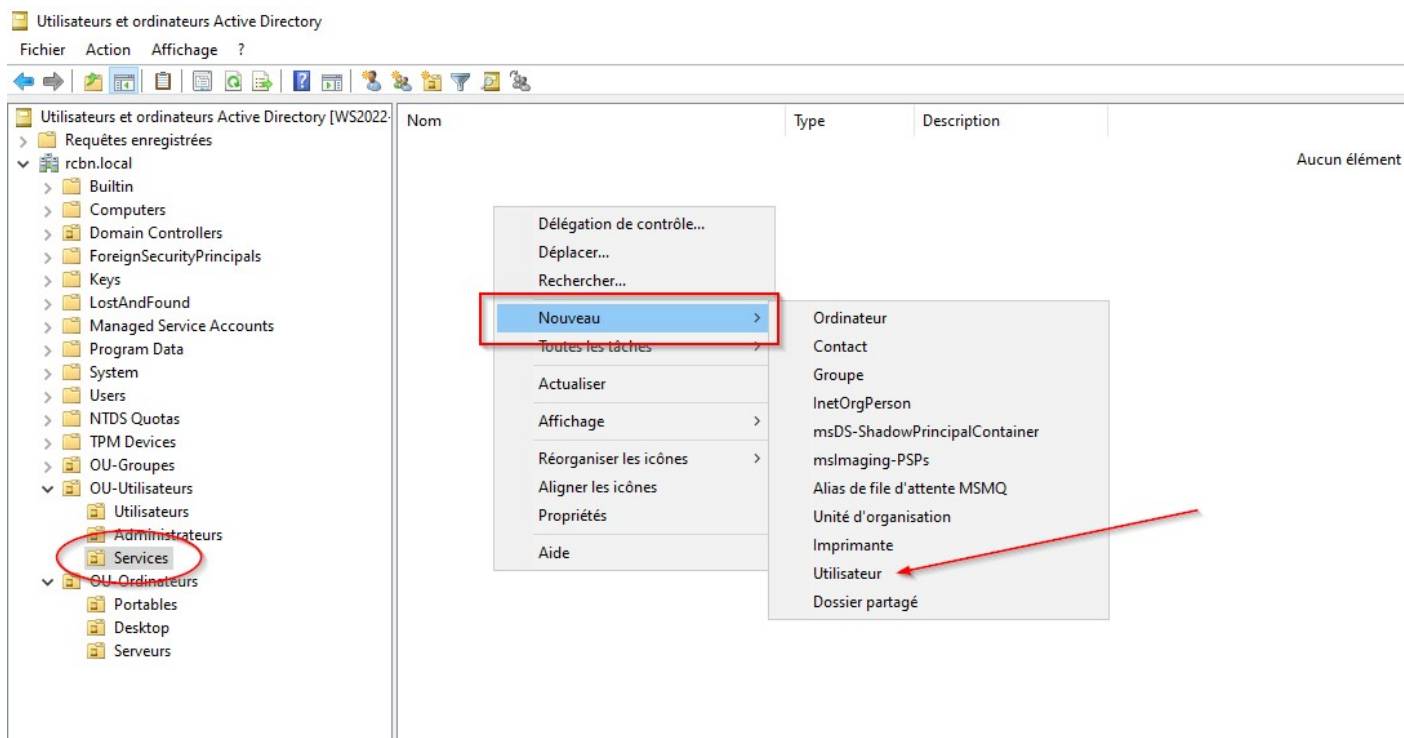
Vous serez ensuite invité à nommer votre OU.



Créez des OU, pour arriver à un schéma comme suit :



Dans l'OU-Utilisateurs > Services, créez un utilisateur en faisant un clic droit, puis en sélectionnant les utilisateurs dans le menu "nouveau"



Nommez cet utilisateur "join". Ce sera utilisateur celui qui sera utiliser pour joindre les machines au domaine.

The screenshot shows the 'Nouvel objet - Utilisateur' (New Object - User) dialog box. The 'Créer dans' (Create in) field is set to 'rcbn.local/OU-Utilisateurs/Services'. The 'Prénom' (First name) and 'Initiales' (Initials) fields are empty. The 'Nom' (Name) field is set to 'join'. The 'Nom complet' (Full name) field is set to 'join'. The 'Nom d'ouverture de session de l'utilisateur' (User logon name) field is set to 'join' and the domain dropdown is set to '@rcbn.local'. The 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)' (User logon name (pre-Windows 2000)) field is set to 'RCBN\join'. The 'Suivant' (Next) button is highlighted.

Utilisez un mot de passe fort, et cochez les cases comme ci dessous.

Nouvel objet - Utilisateur

Créer dans : rcbn.local/OU-Utilisateurs/Services

Mot de passe :

Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

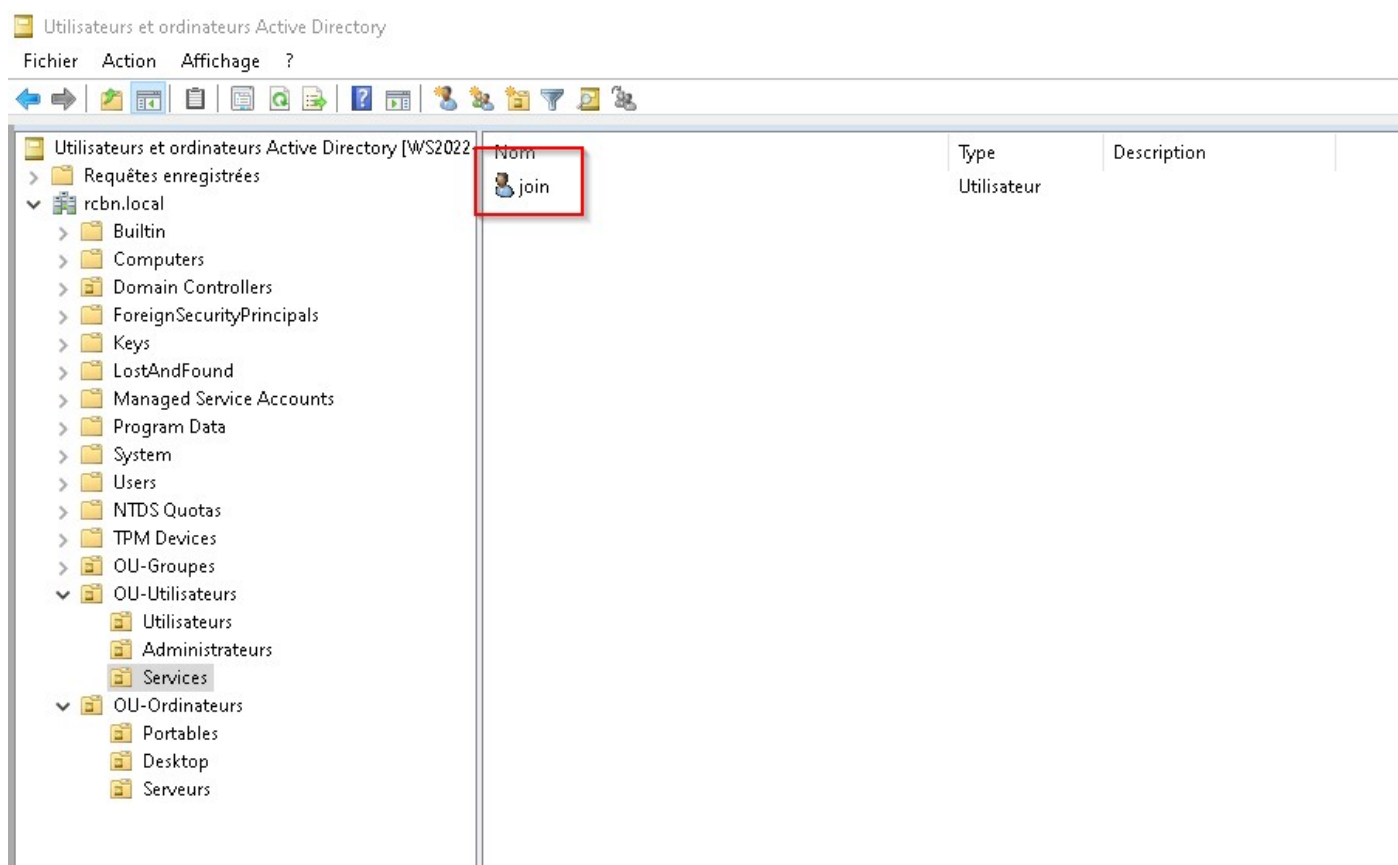
☒ L'utilisateur ne peut pas changer de mot de passe

☒ Le mot de passe n'expire jamais

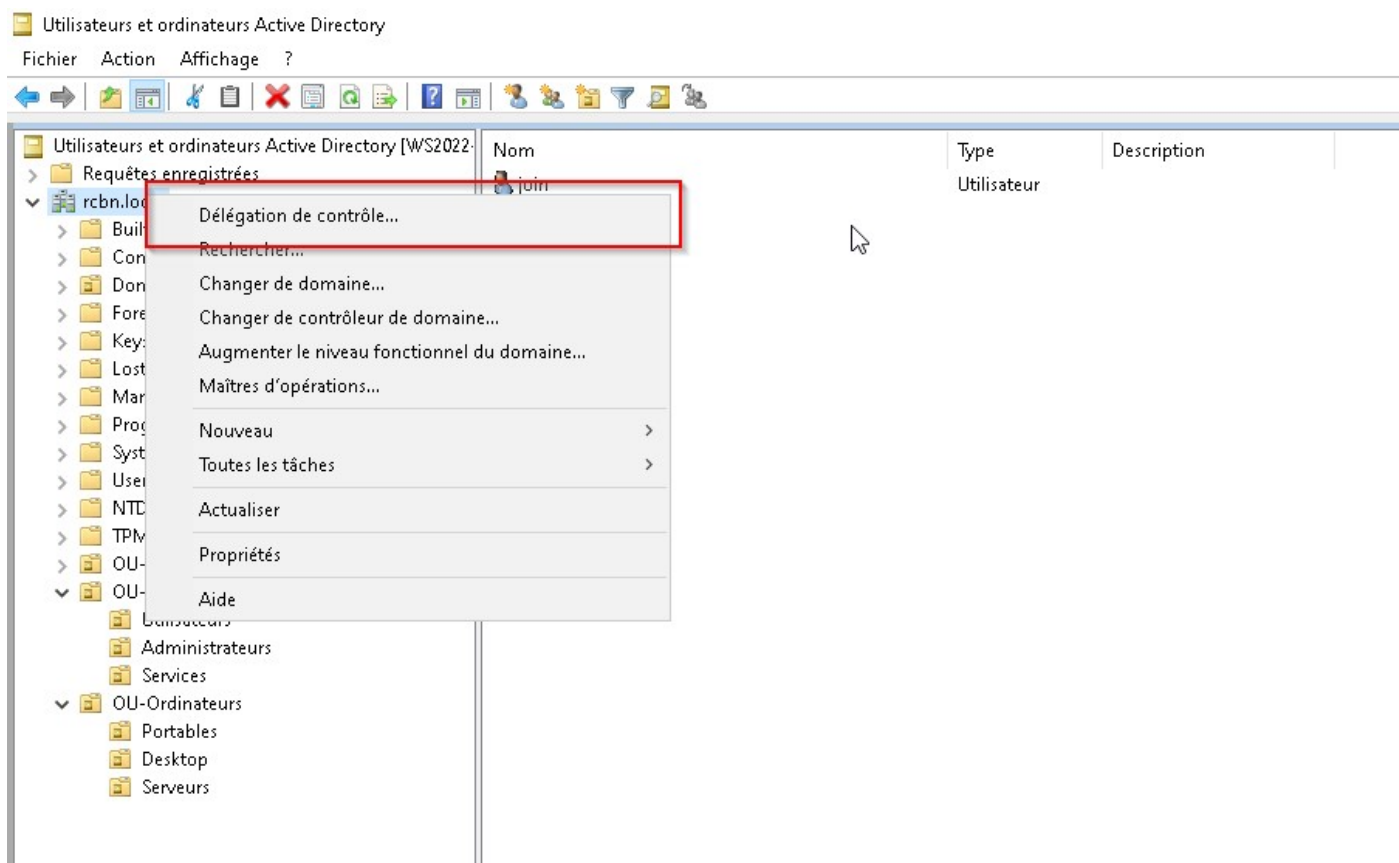
☐ Le compte est désactivé

< Précédent Suivant > Annuler

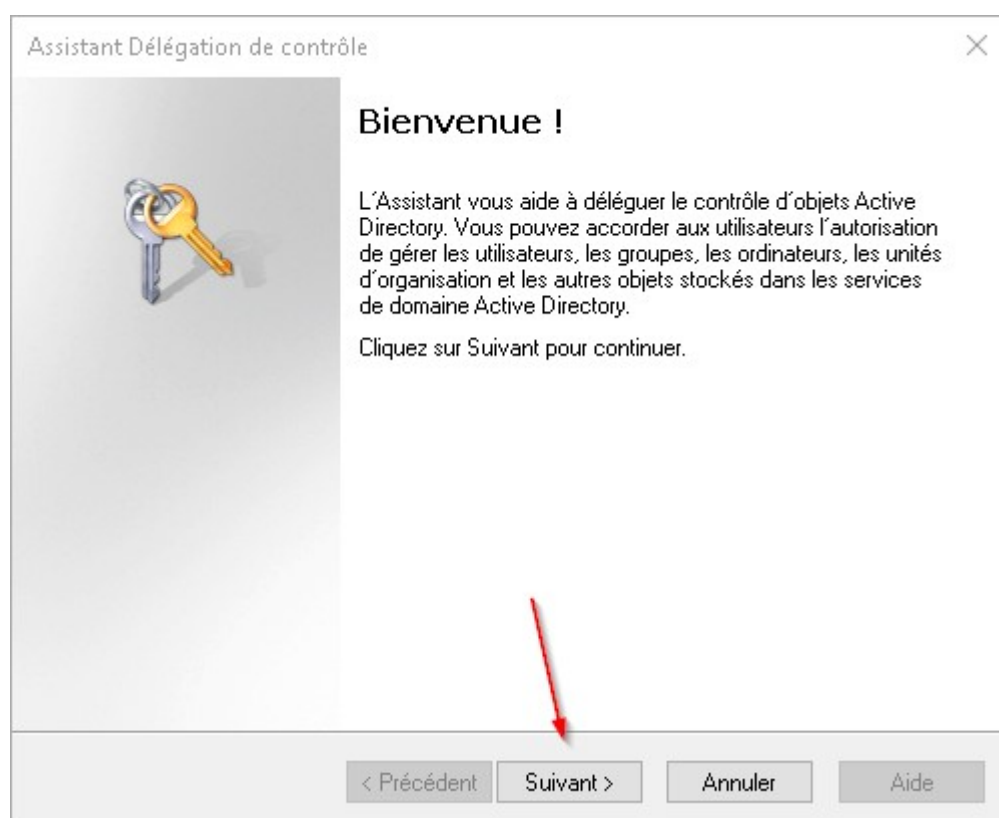
Il apparaîtra ensuite dans l'OU.



Créez ensuite une délégation pour l'utilisateur, en faisant un clic droit sur l'icône du domaine.



Une page d'introduction apparaît, cliquez sur suivant



Ajoutez l'utilisateur "join" dans la liste, cliquez sur suivant

Assistant Délégation de contrôle

Utilisateurs ou groupes
Sélectionnez un ou plusieurs groupes ou utilisateurs auxquels vous voulez déléguer le contrôle.

Utilisateurs et groupes sélectionnés :

join (join@rcbn.local)

Ajouter... Supprimer

< Précédent Suivant > Annuler Aide

Cochez "Joindre un ordinateur au domaine"

Assistant Délégation de contrôle

Tâches à déléguer
Vous pouvez sélectionner des tâches communes ou personnaliser vos propres tâches.

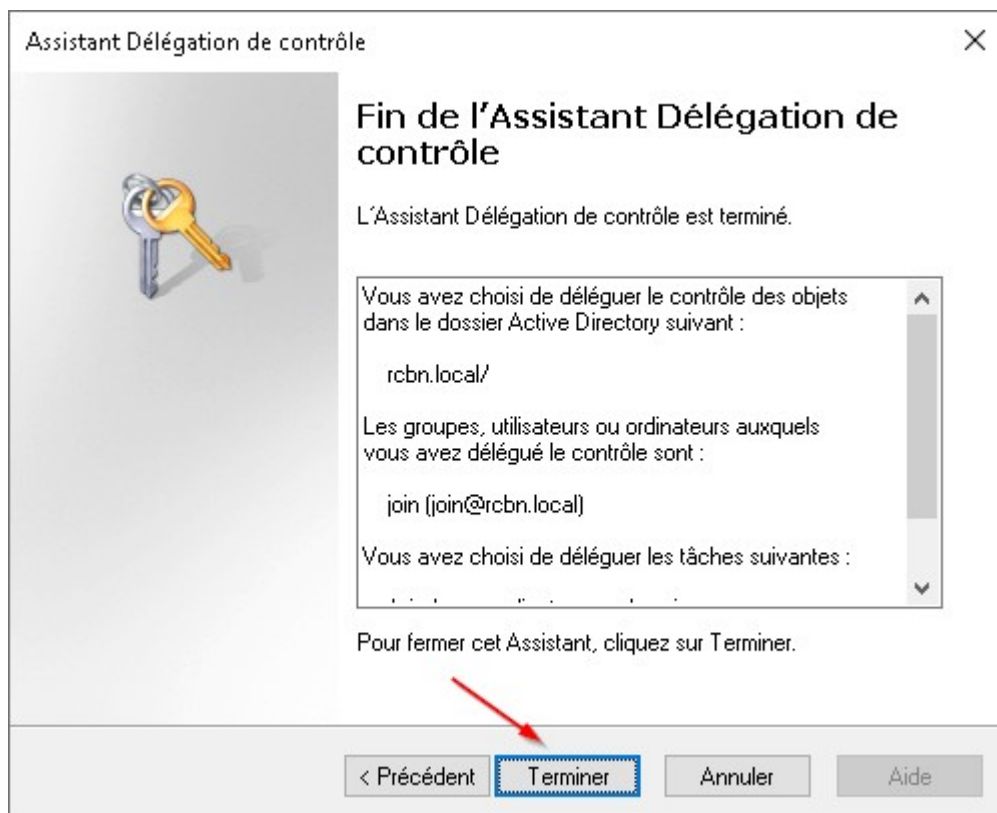
☒ Déléguer les tâches courantes suivantes :

- ☐ Créer, supprimer et gérer les comptes d'utilisateurs
- ☐ Réinitialiser les mots de passe utilisateur et forcer le changement de m
- ☐ Lire toutes les informations sur l'utilisateur
- ☐ Modifier l'appartenance à un groupe
- ☒ Joindre un ordinateur au domaine
- ☐ Gérer les liens de stratégie de groupe
- ☐ Générer le jeu de stratégie résultant (Planification)

☐ Créer une tâche personnalisée à déléguer

< Précédent Suivant > Annuler Aide

Un récapitulatif de la délégation apparaît.



Votre domaine devrait désormais être prêt à l'exploitation.

Windows Server Site A

Configuration - Jonction au domaine AD, mise en place des rôles DC2

Introduction

Ce deuxième document couvre la procédure d'installation des différents rôles nécessaires à la mise en place d'un domaine AD.

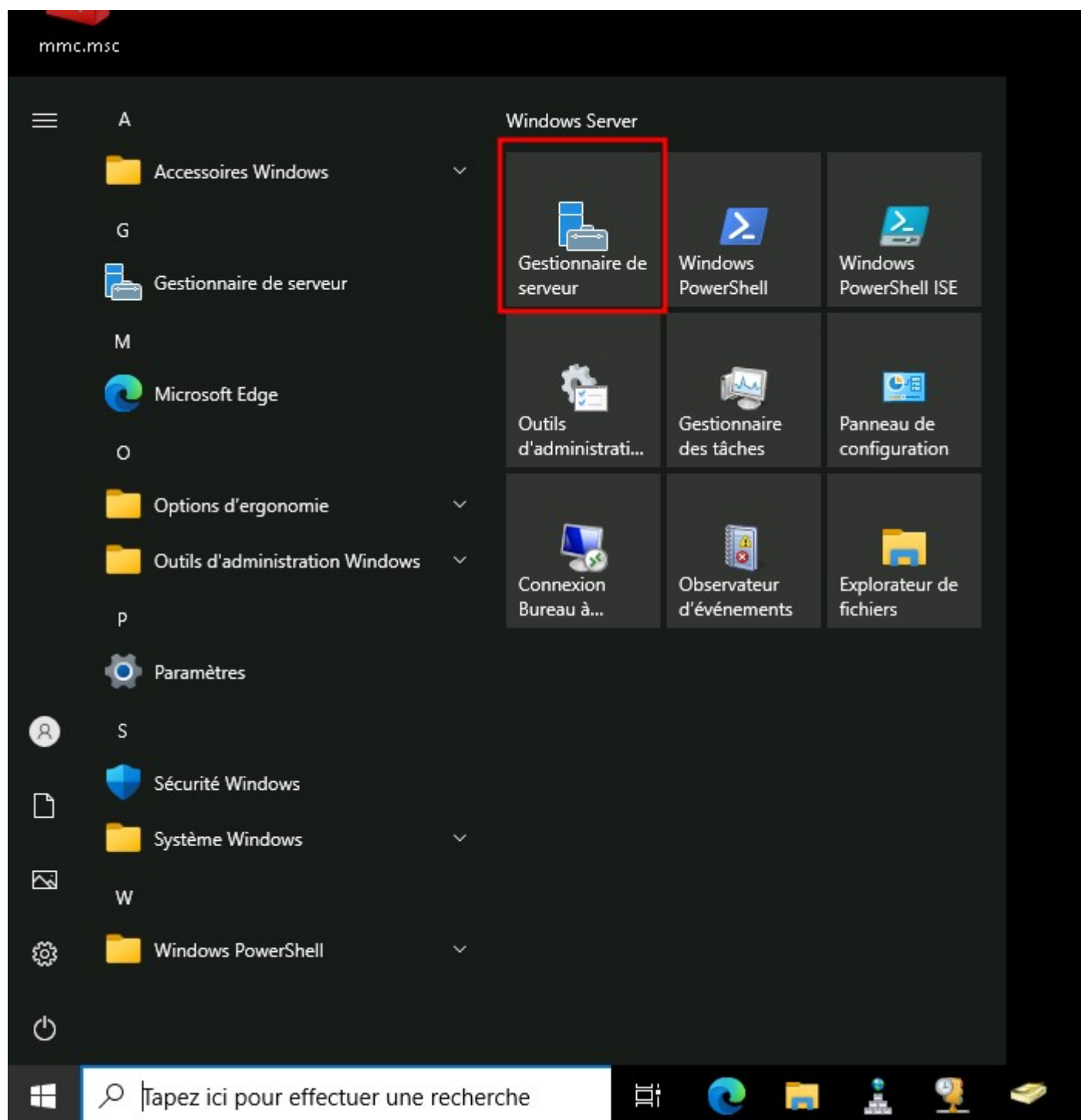
1. Installation des rôles AD, DNS, DHCP.
2. Configuration initiale du domaine

Pour ce faire, vous aurez besoin des éléments suivants :

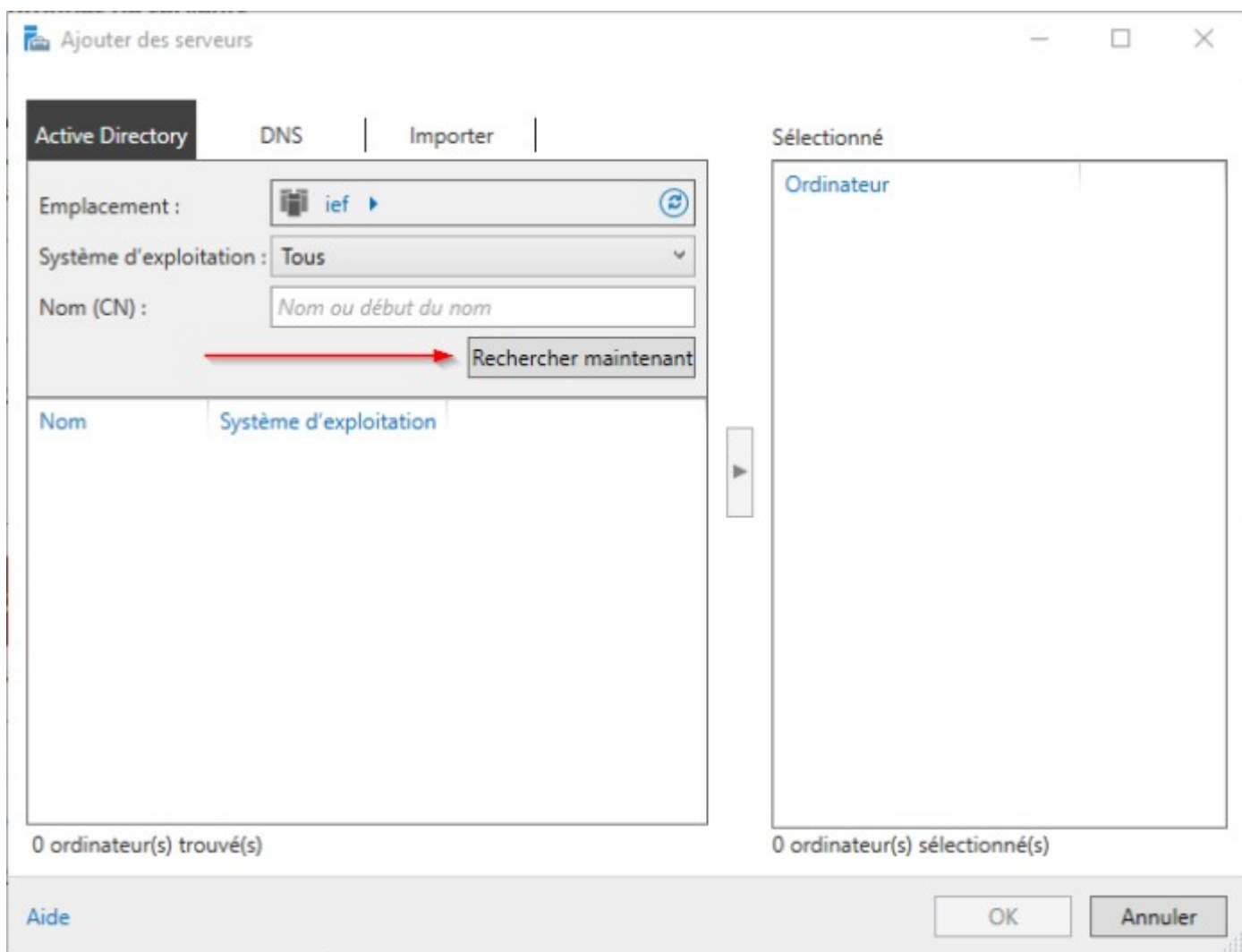
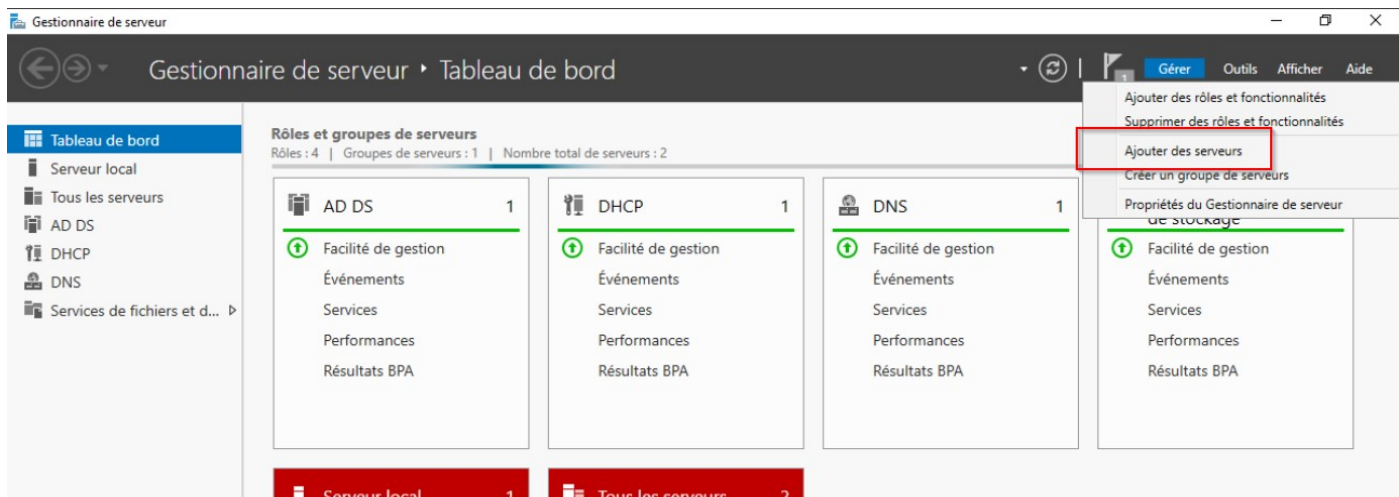
- Machine virtuelle Windows Server 2022
- Compte d'administration du serveur
- Serveur correctement nommé

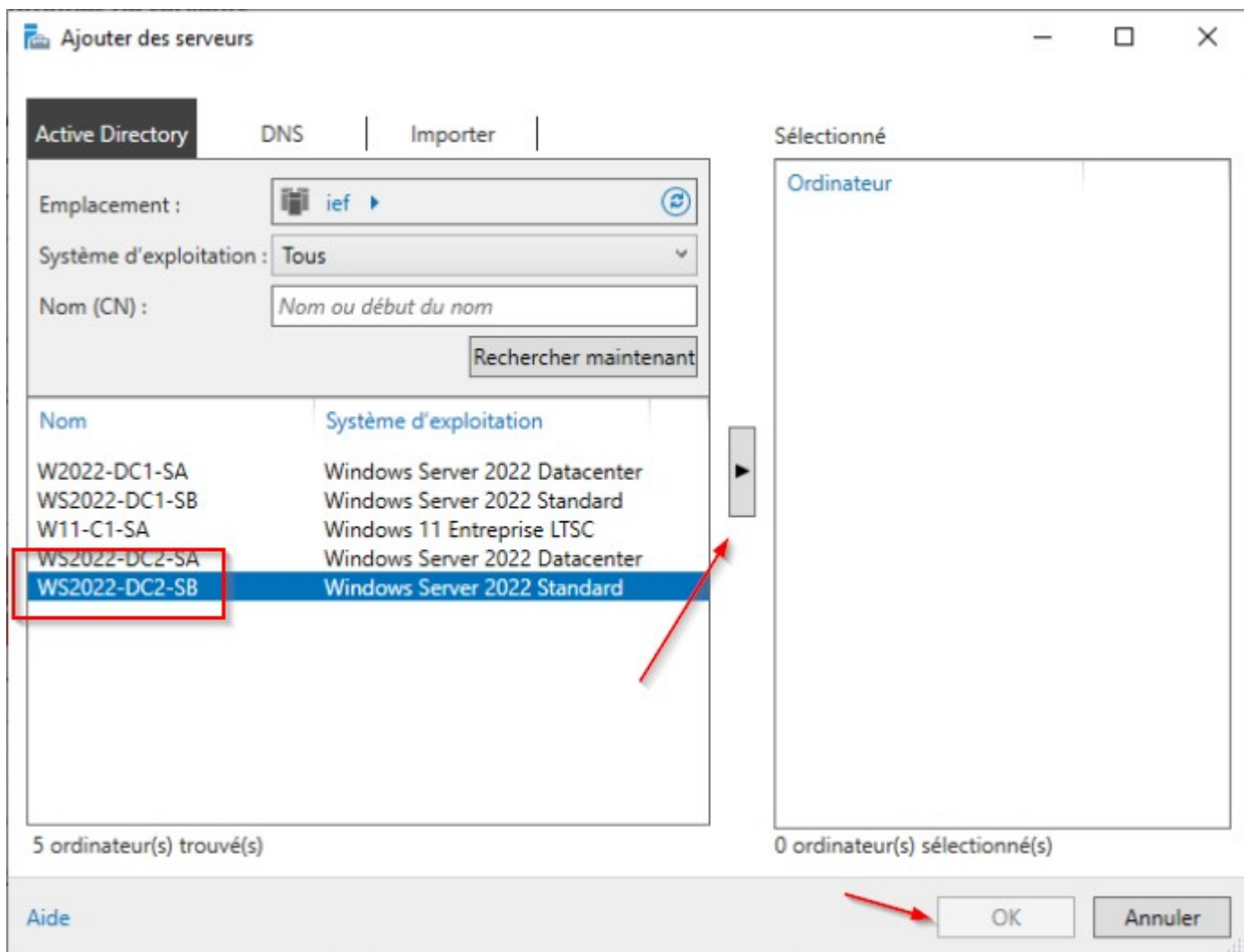
1) Installation des rôles

Pour installer des rôles de serveur, vous devez lancer le gestionnaire de serveur, trouvable dans le menu démarrer du serveur.

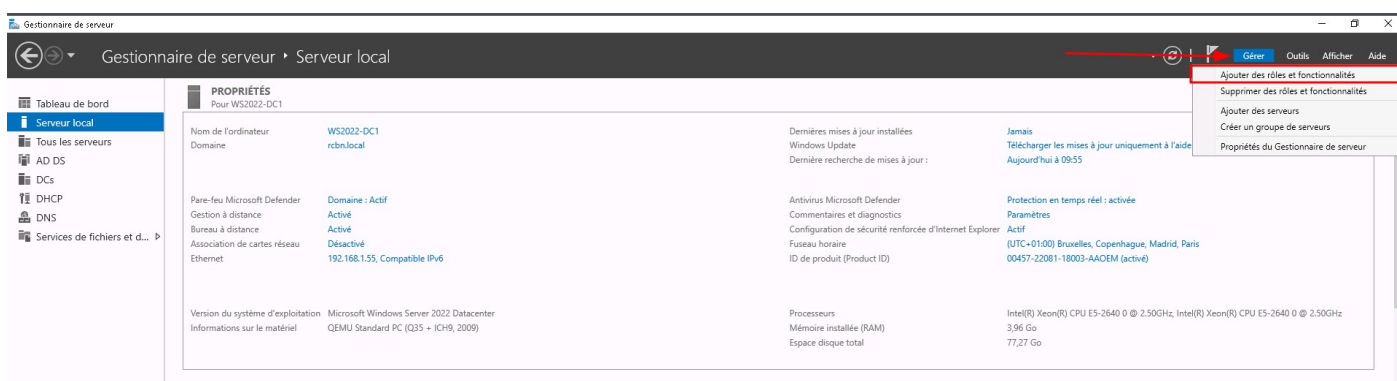


Vous devez ajouté le serveur nouvellement ajouté au domaine dans le gestionnaire de serveur pour installer des rôles dessus

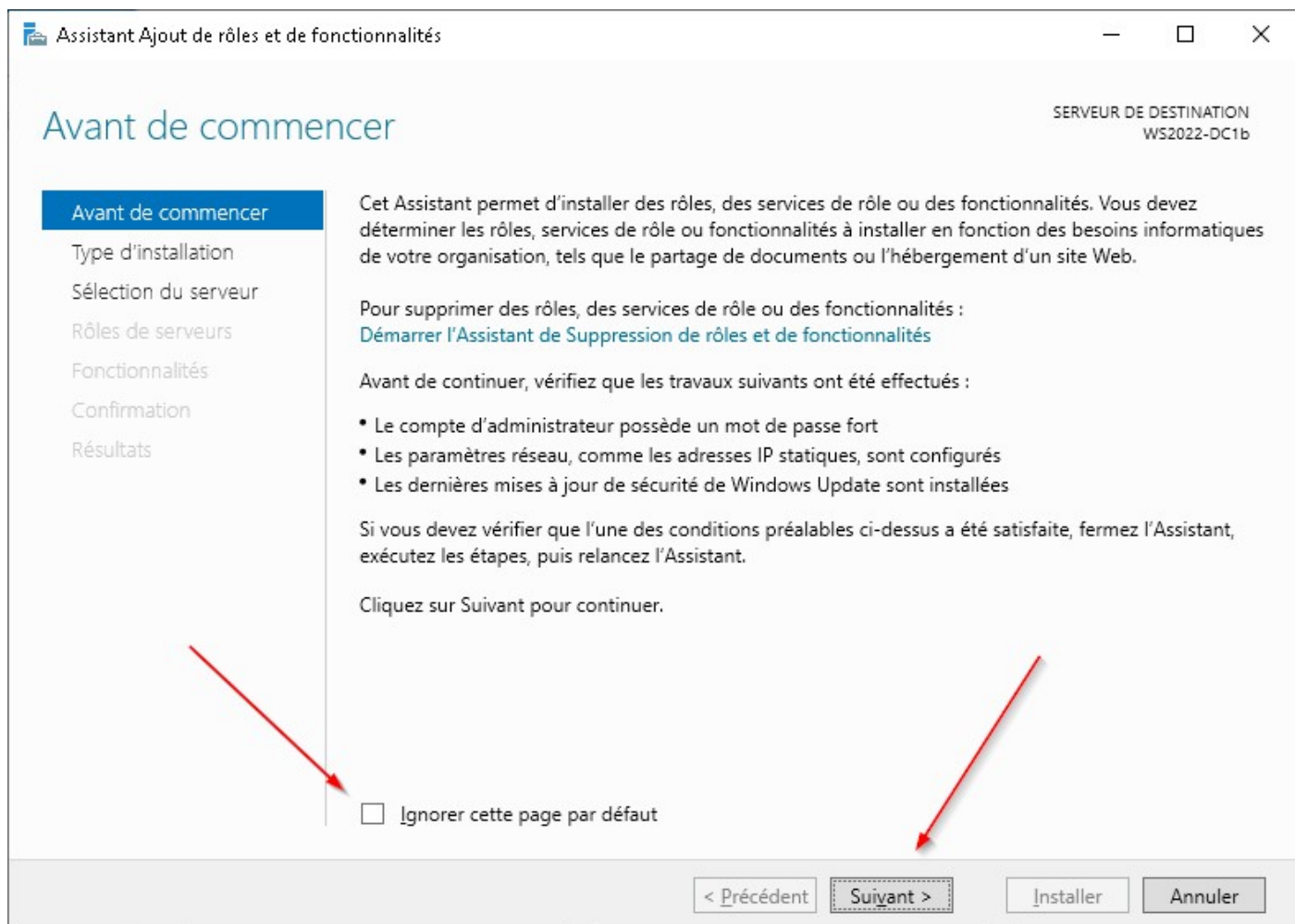




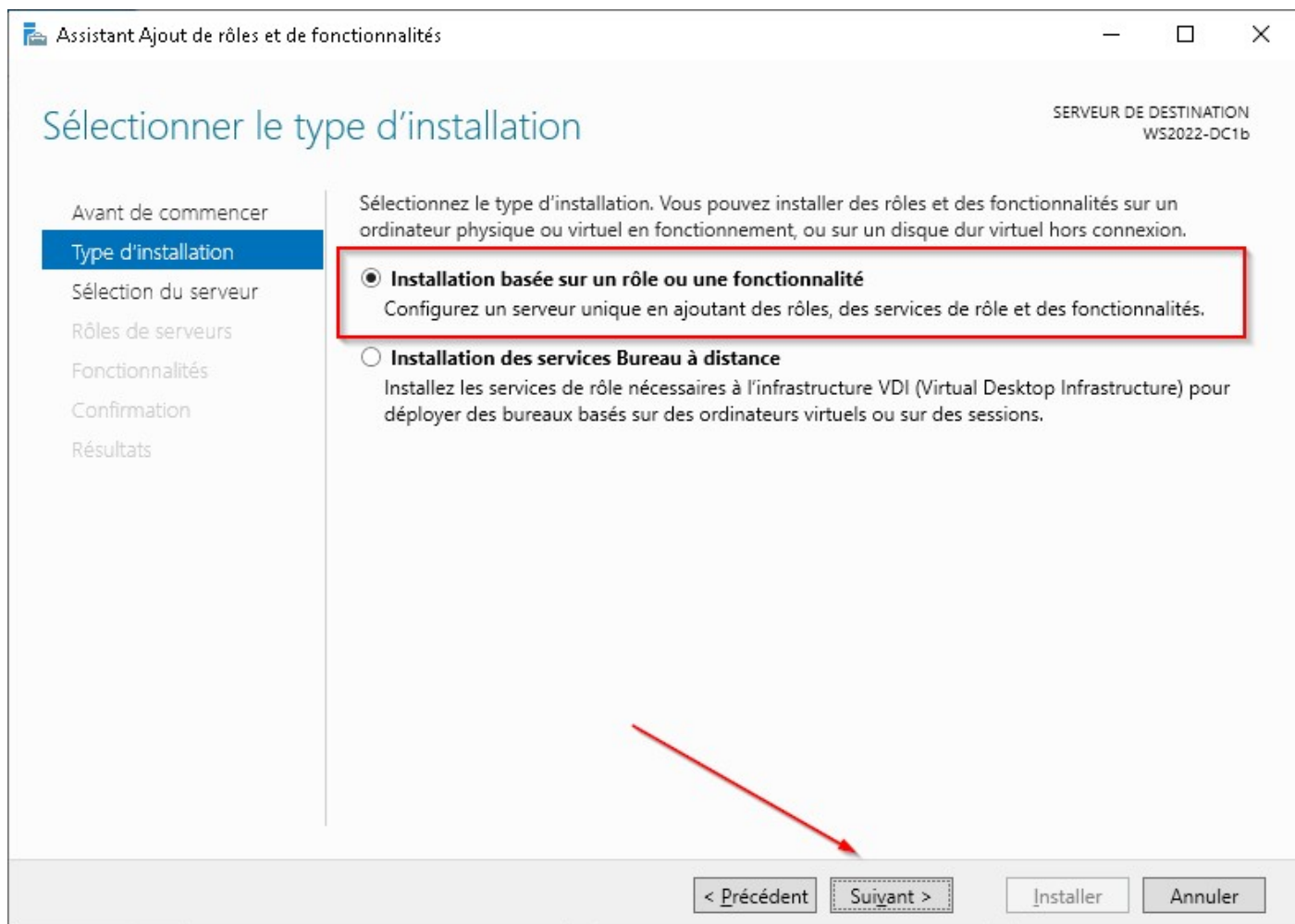
Cliquez ensuite sur gérer, puis "Ajouter des rôles et des fonctionnalités"



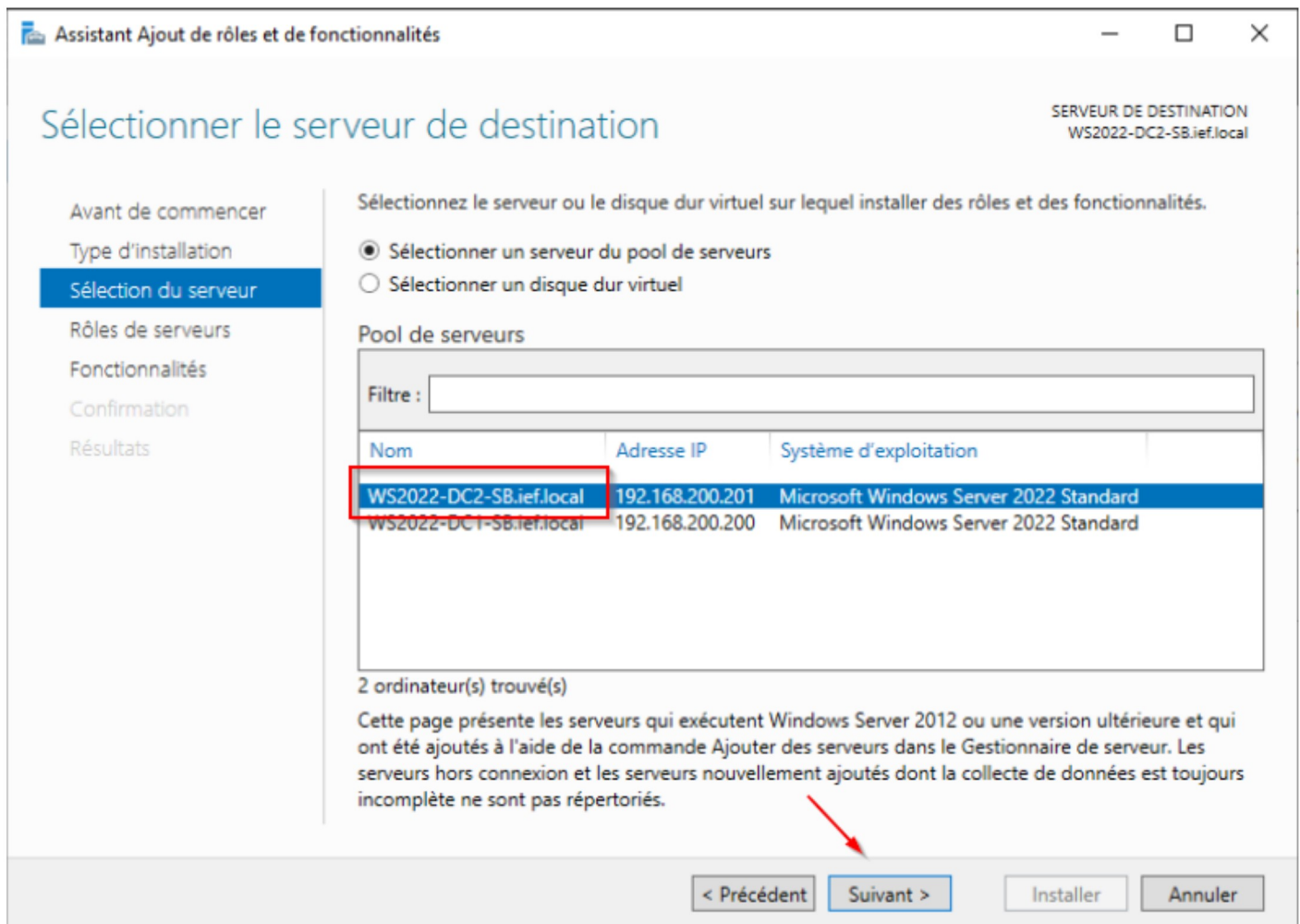
Vous voici sur la page d'accueil de l'assistant. Vous pouvez cocher (ou non) la case pour ignorer l'introduction de l'assistant. Cliquez ensuite sur suivant.



Vérifiez ensuite que la première option est bien celle cochée dans la fenêtre qui suit

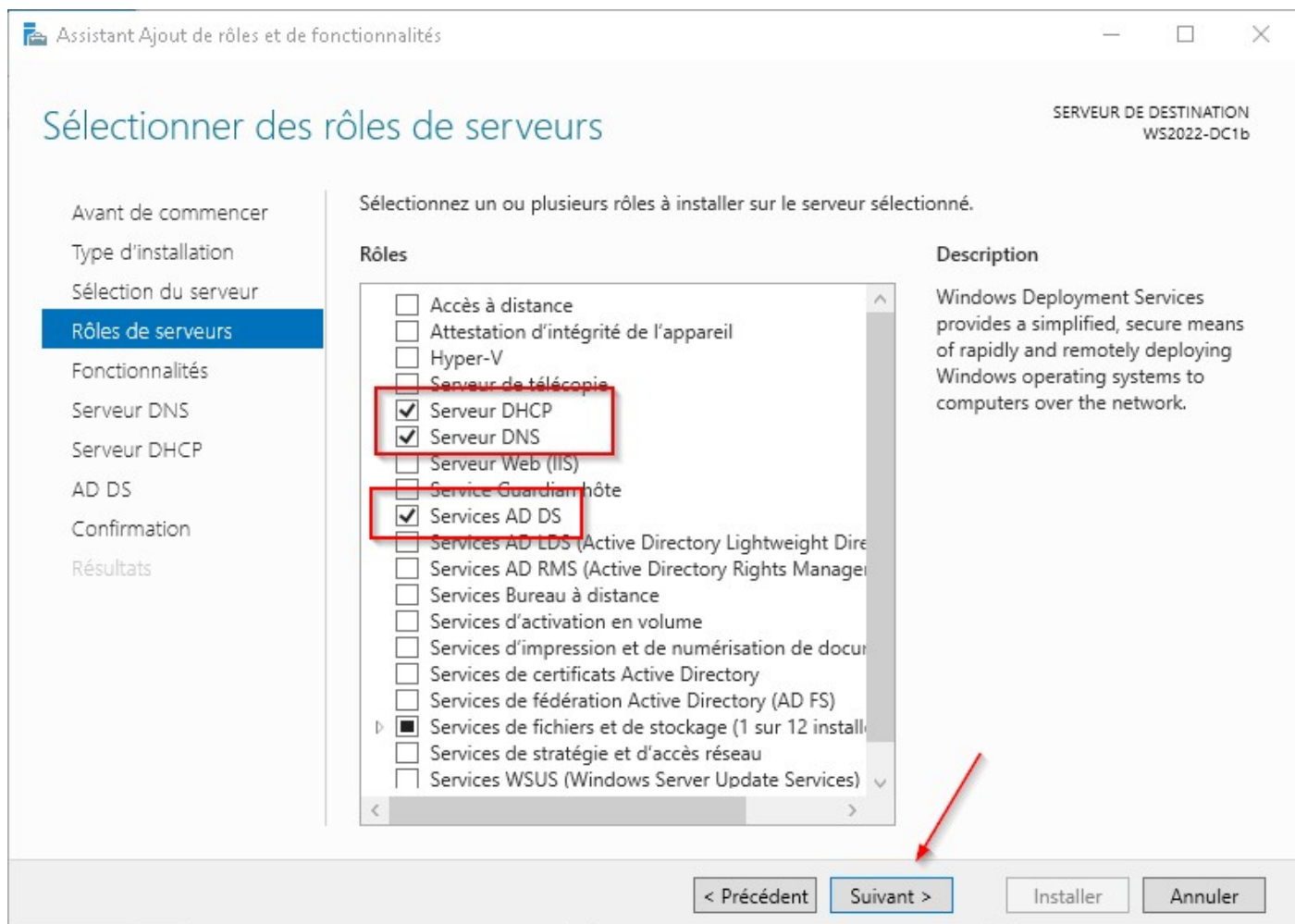


Sélectionnez les paramètres régionaux de votre machine, et cliquez sur suivant

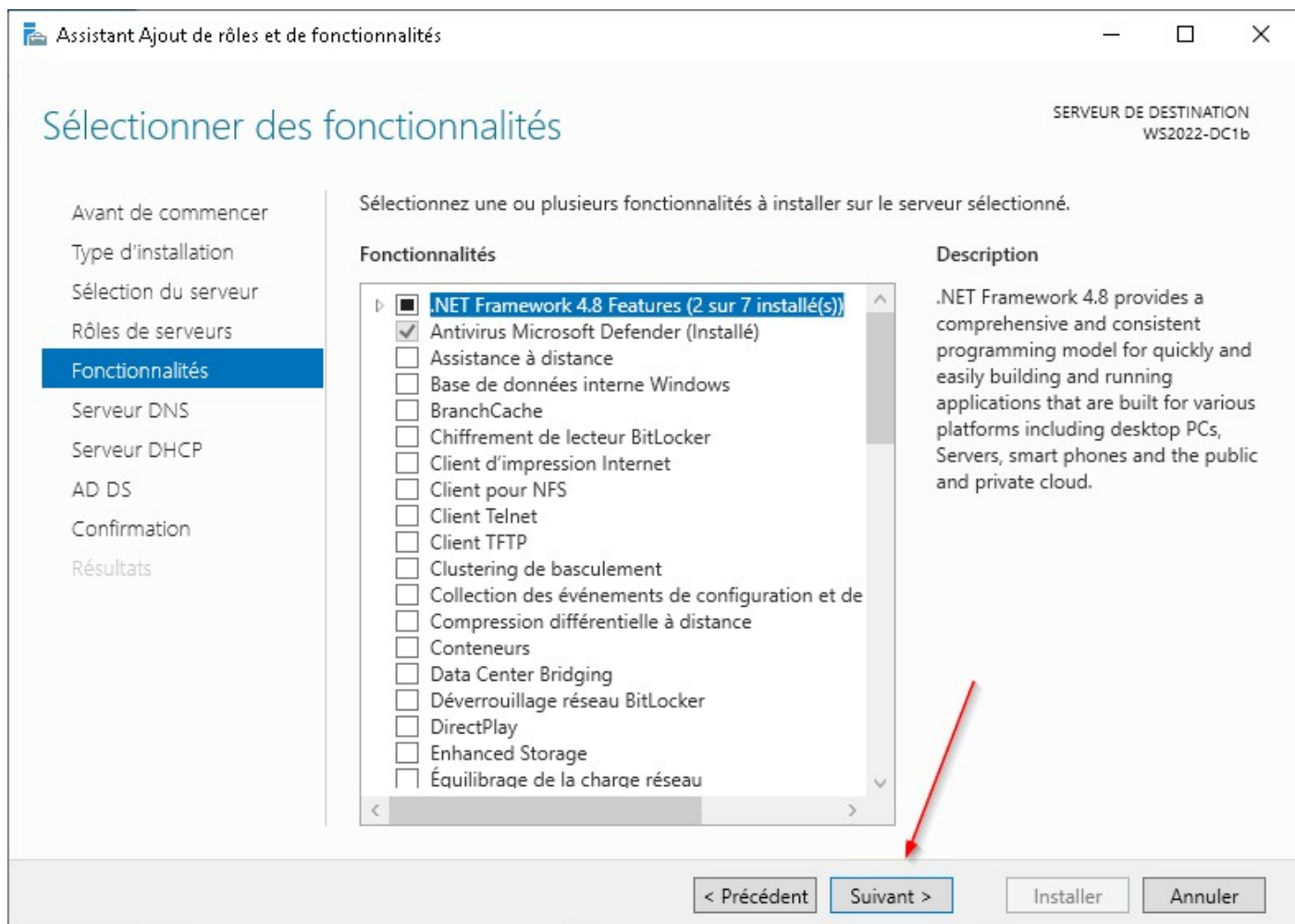


Si votre machine fait partie d'un Pool de Serveurs, pensez à vérifier son nom pour être sûr d'agir sur la bonne machine.

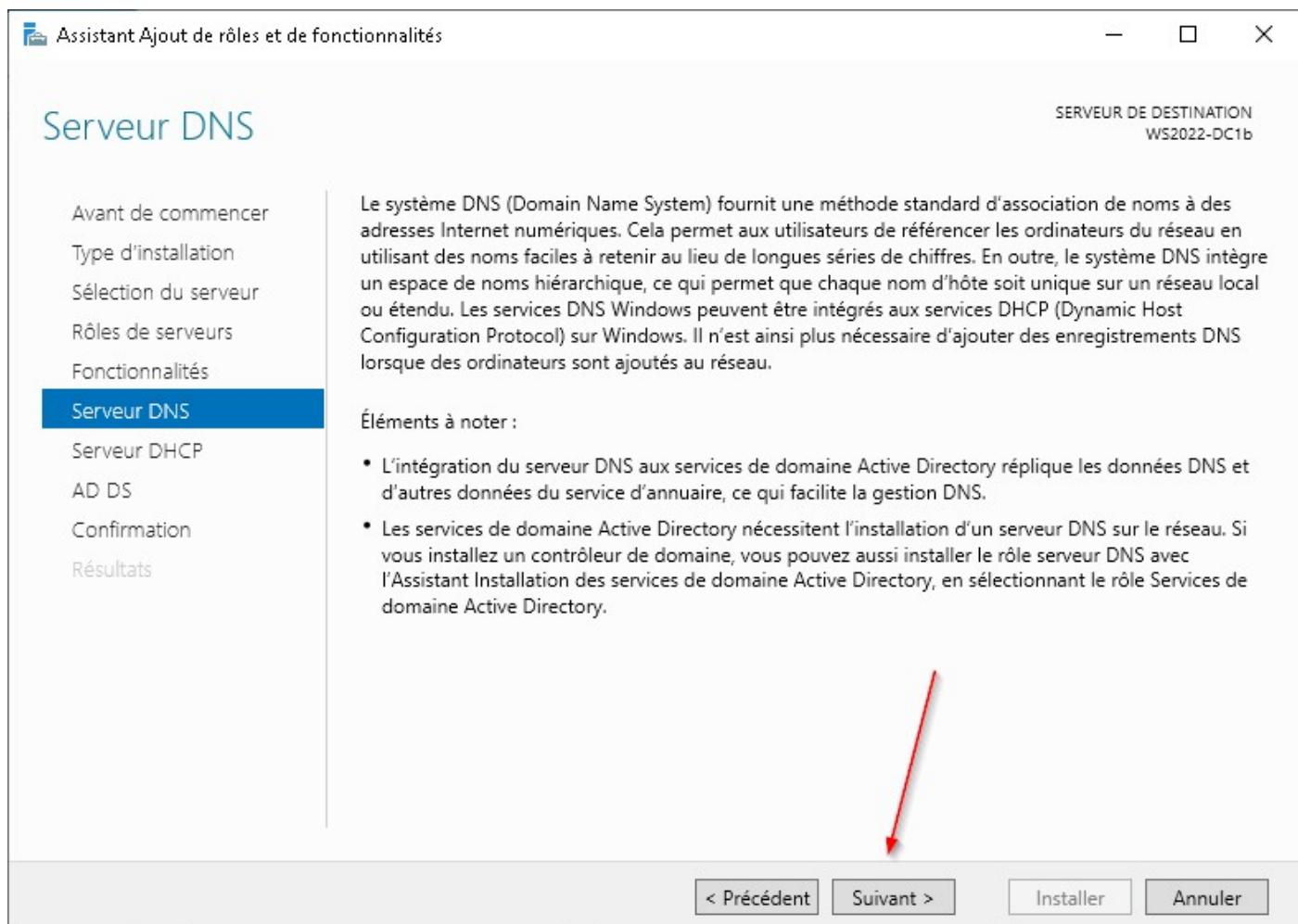
Sélectionnez les rôles nécessaires. Dans notre cas, nous allons utiliser notre serveur pour AD et DHCP, Il faut donc activer les rôles DNS, DHCP et AD DS.

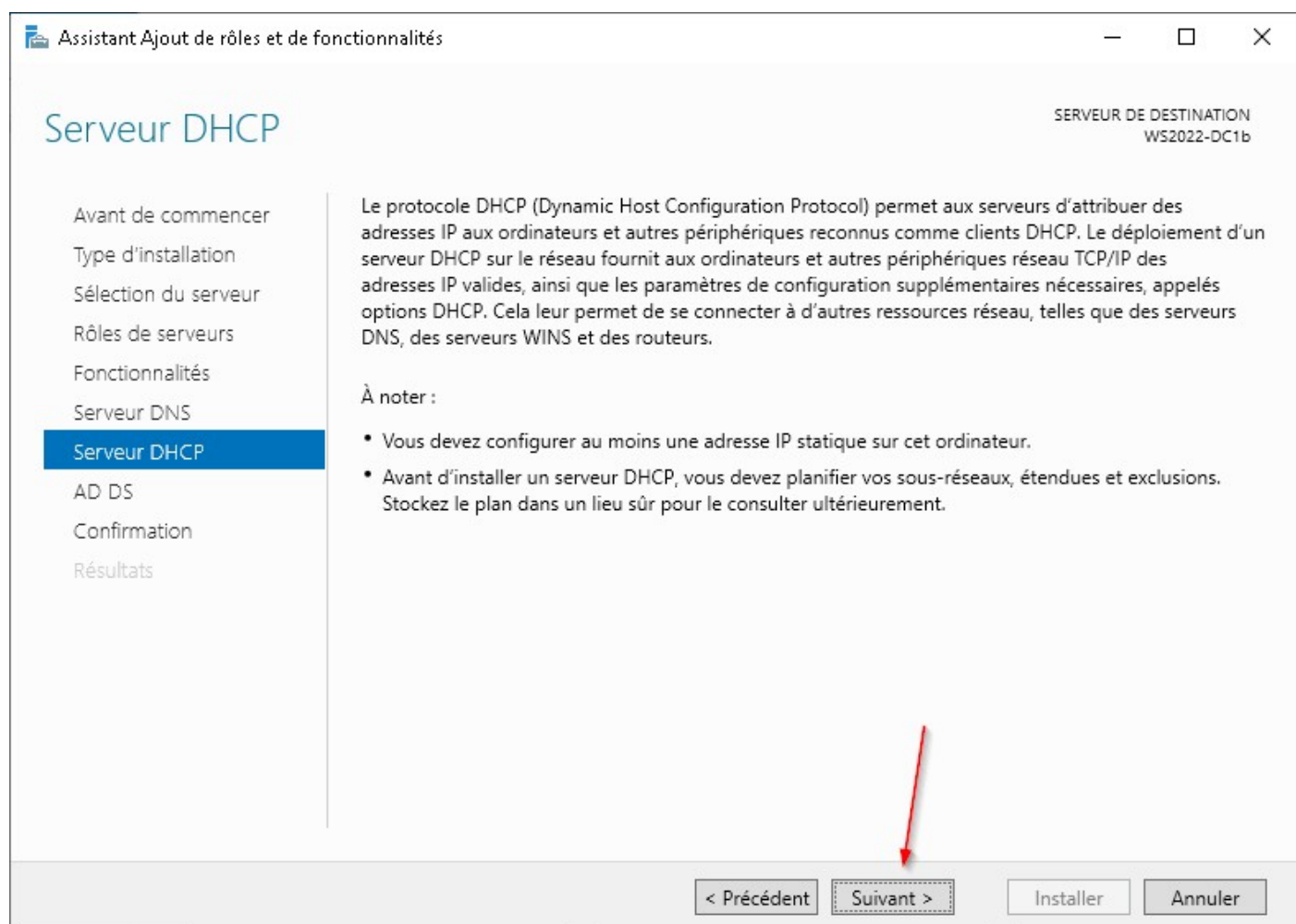


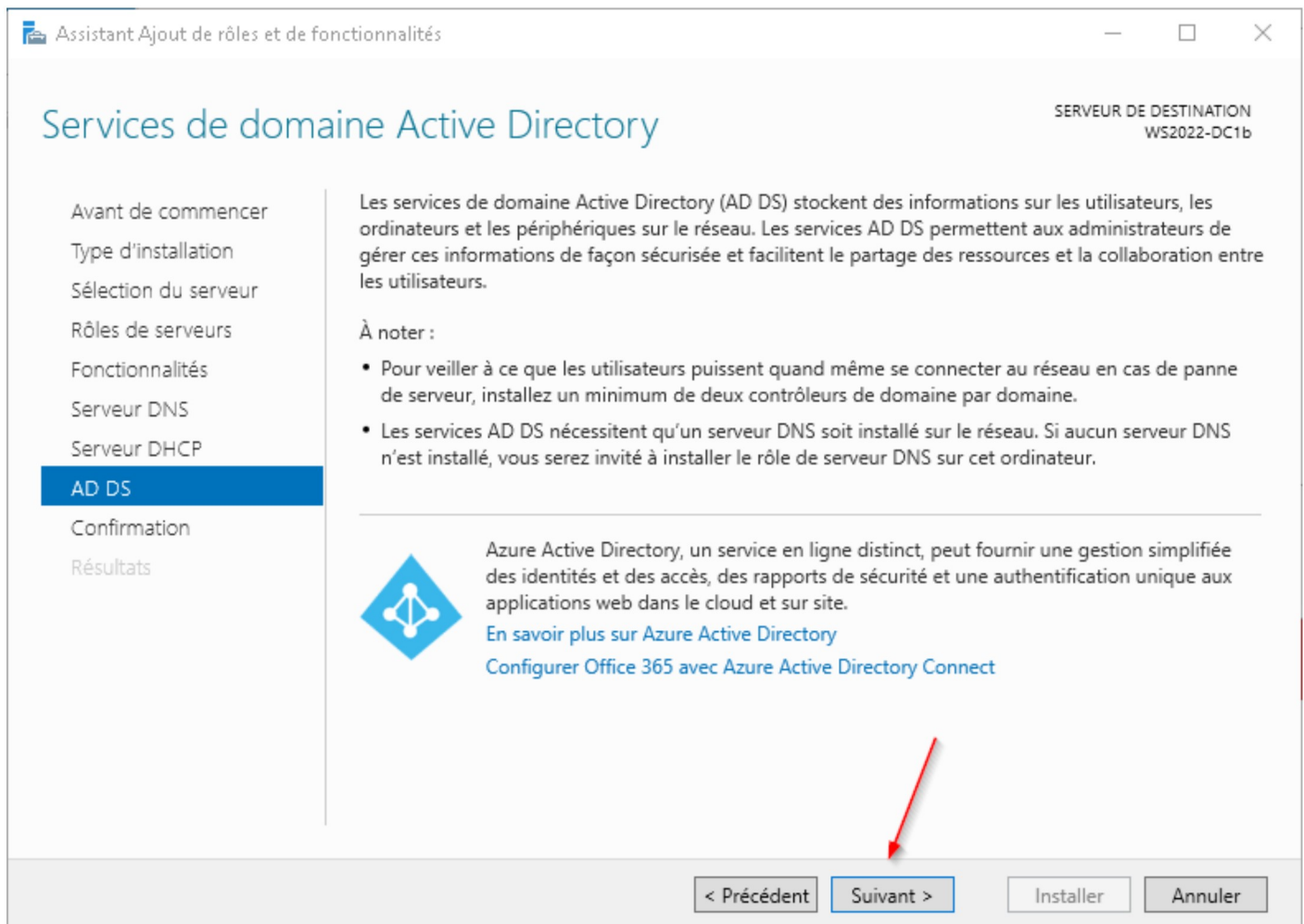
Aucun besoin d'ajouter des fonctionnalités, elles ont déjà été auto-sélectionnées par Windows lors de la sélection des rôles.



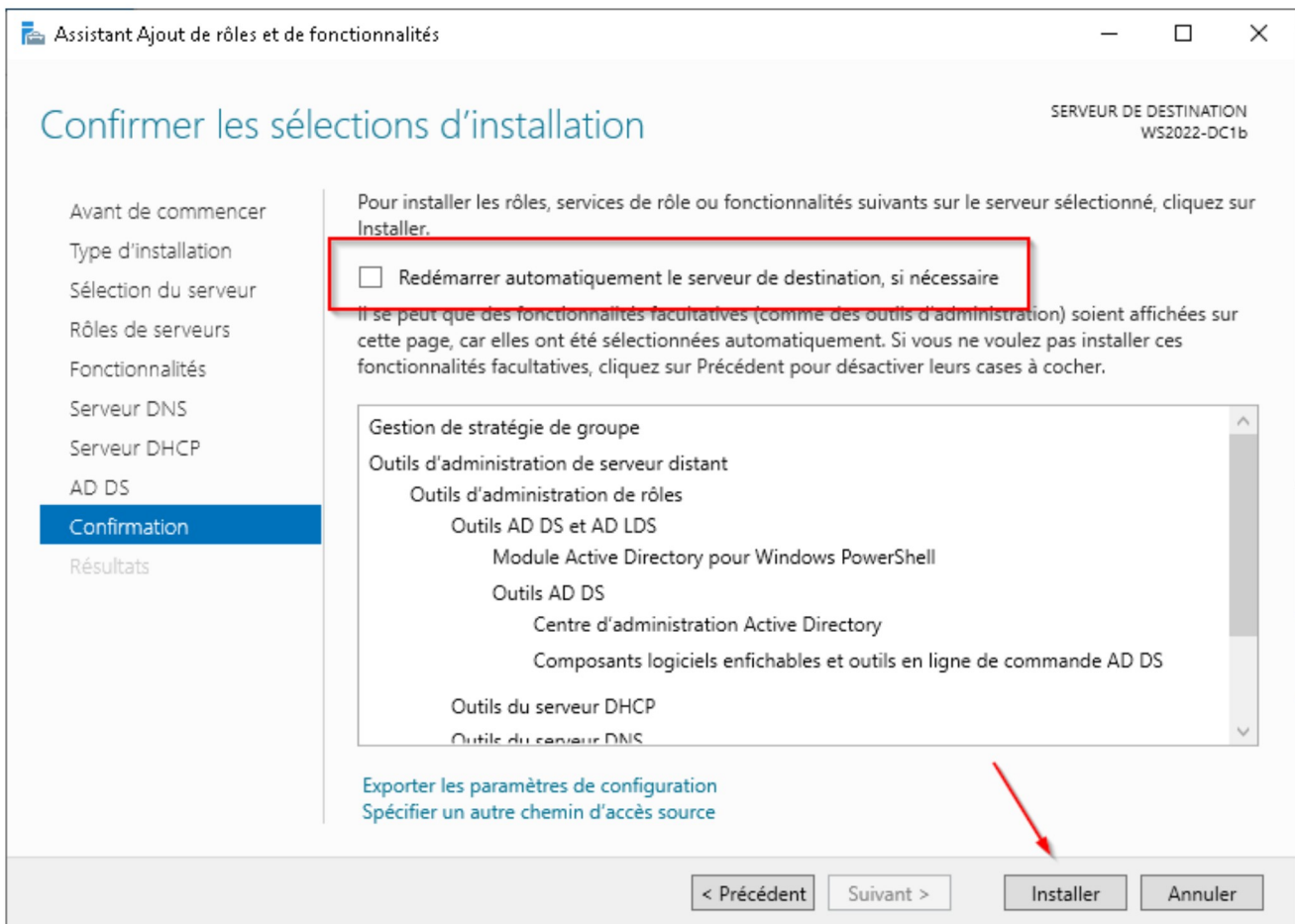
3 fenêtres d'information vont se suivre.



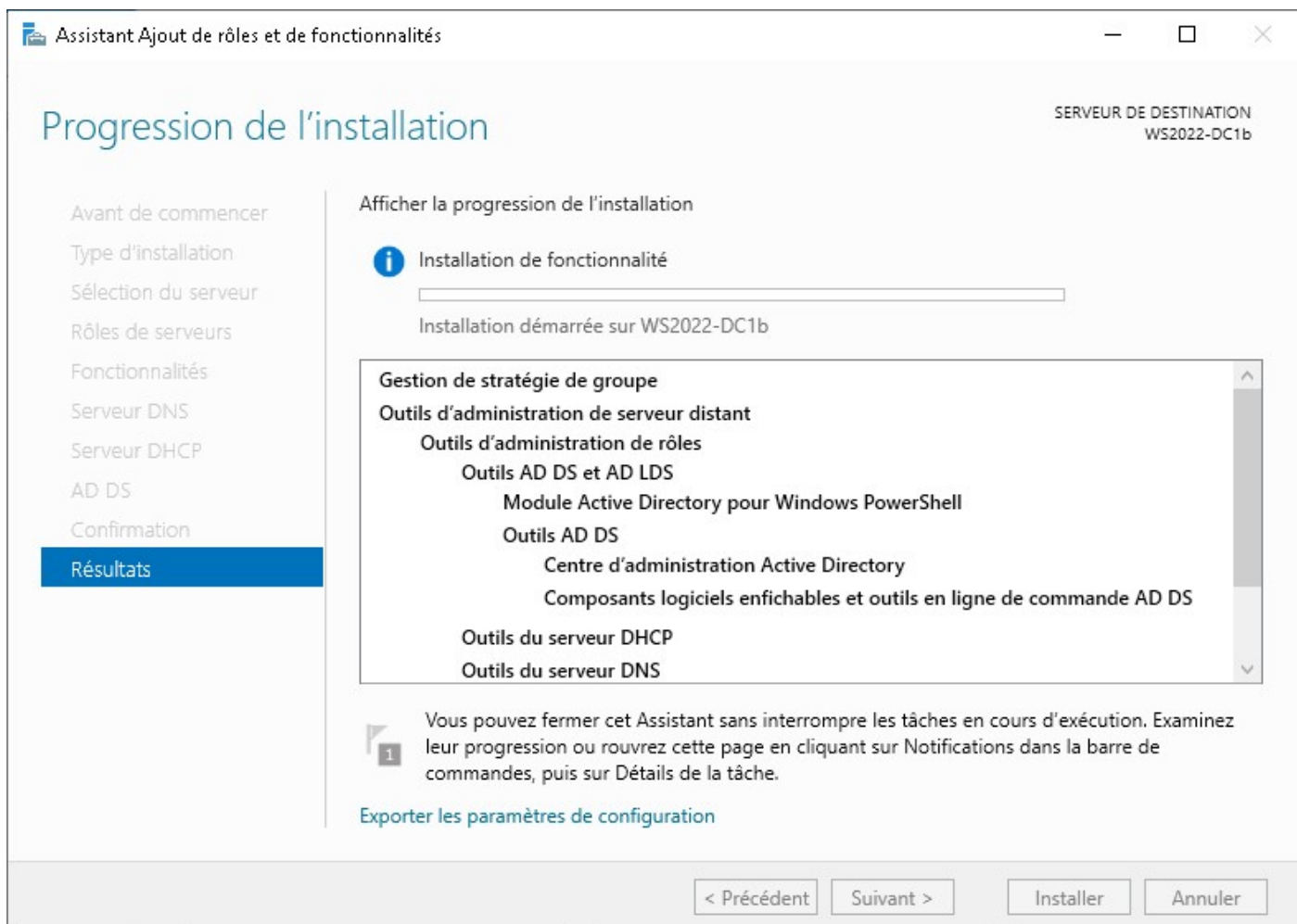




Décochez ensuite la case pour redémarrer la machine, et cliquez sur installer

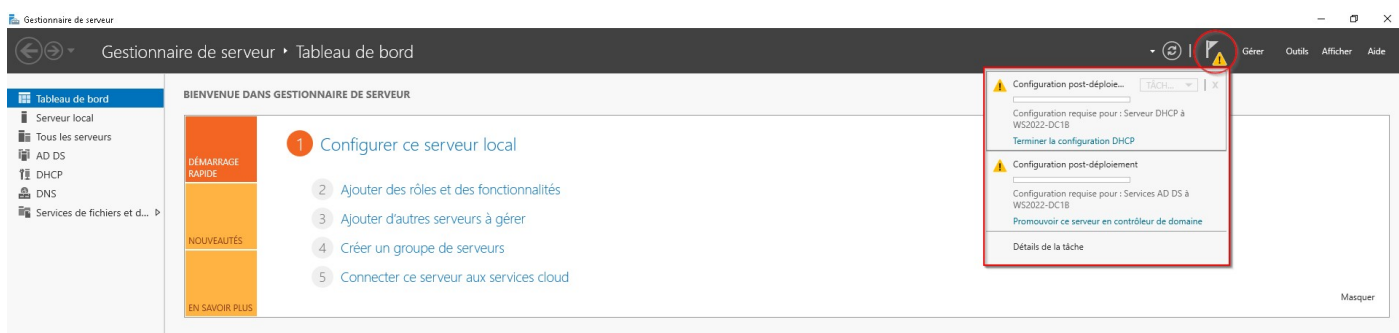


L'installation démarre.



2) Configuration des rôles.

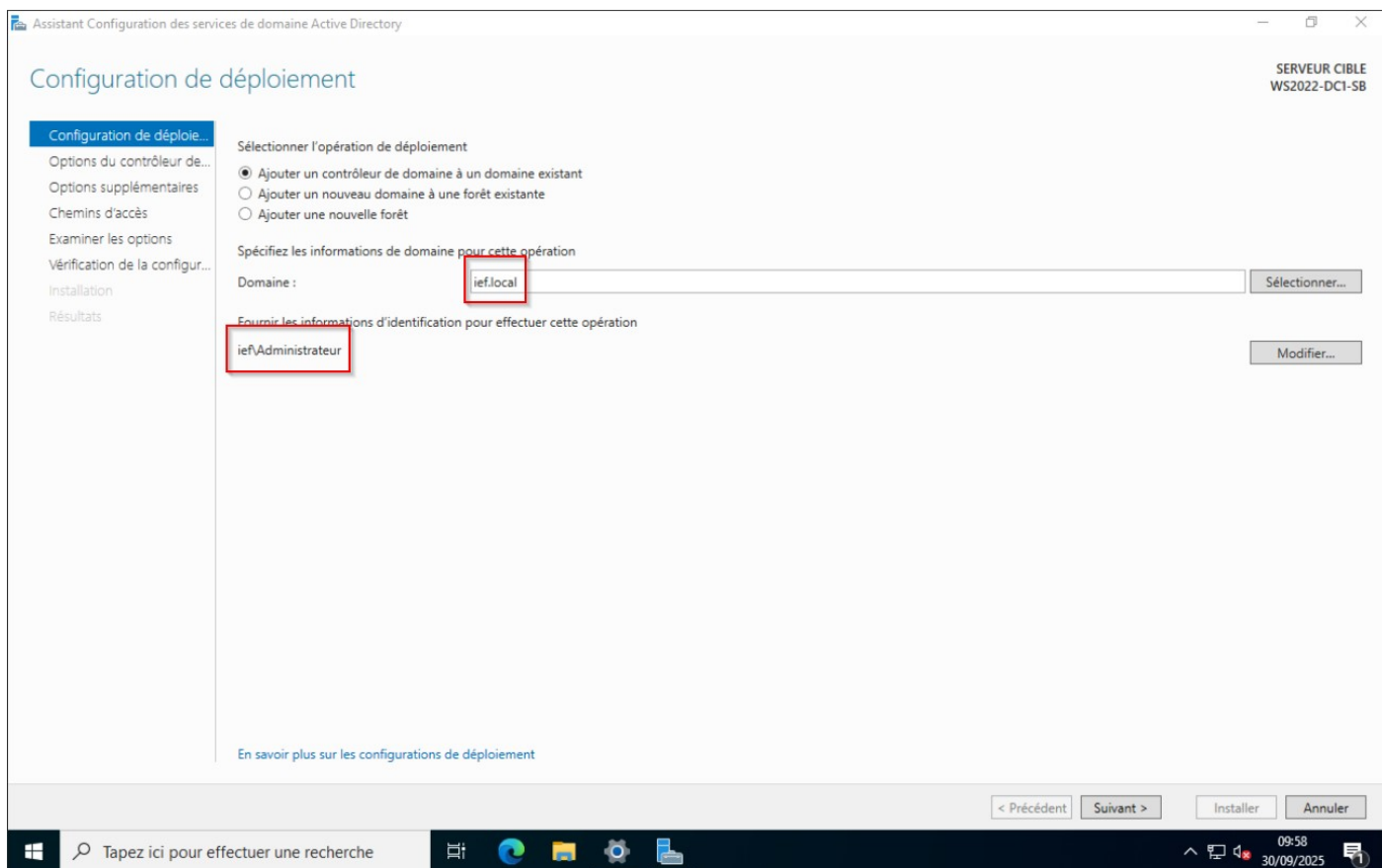
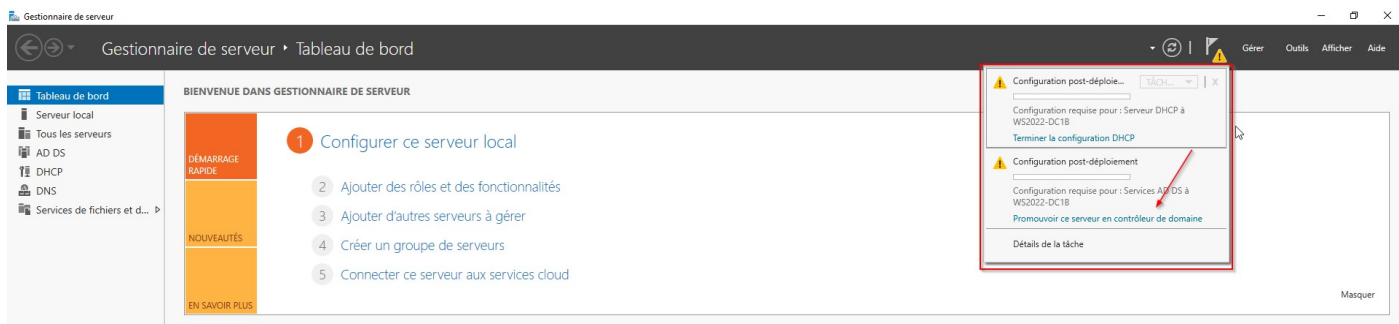
Une fois redémarré, lancez le gestionnaire de serveur, et cliquez sur le drapeau en haut à droite.

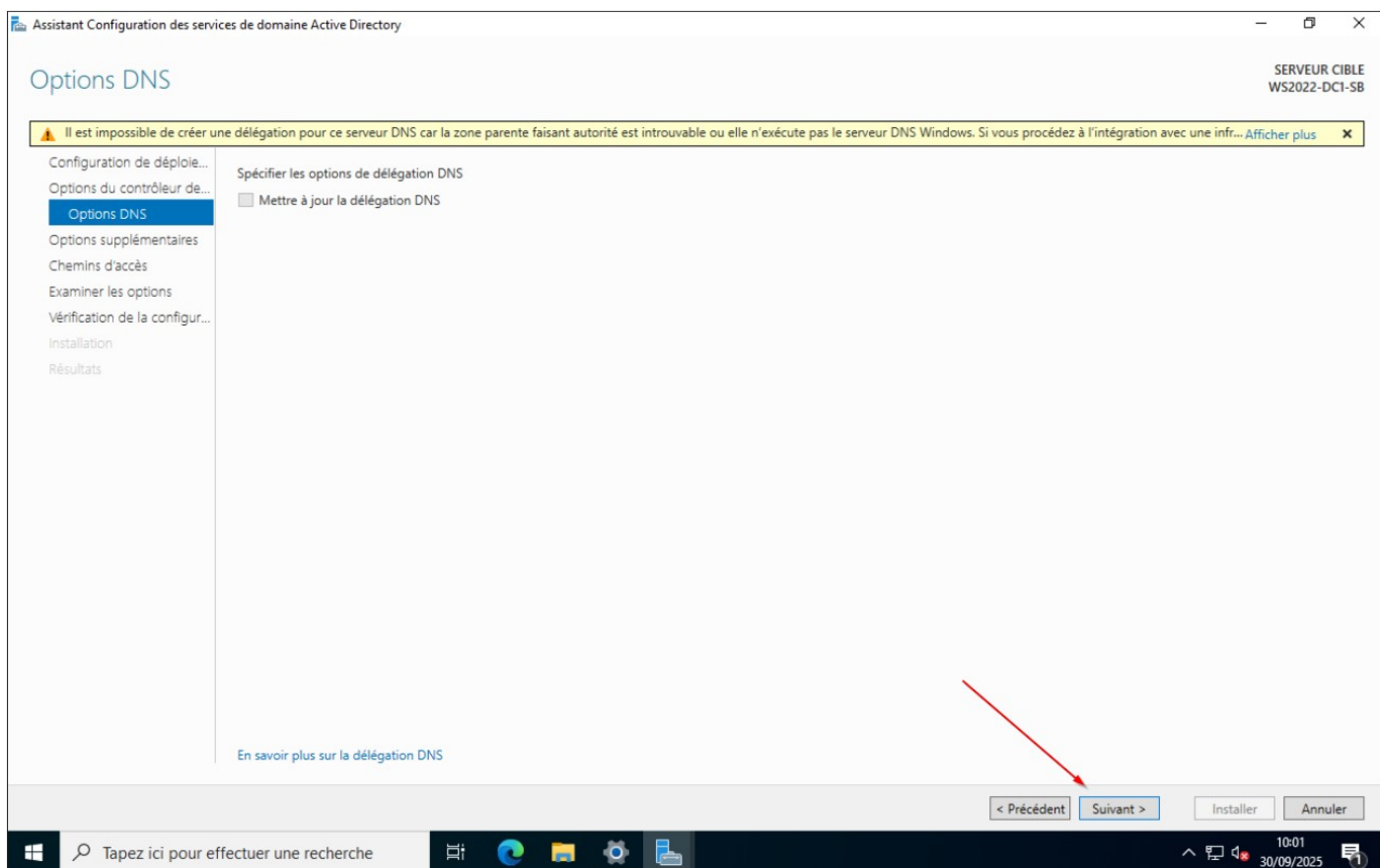
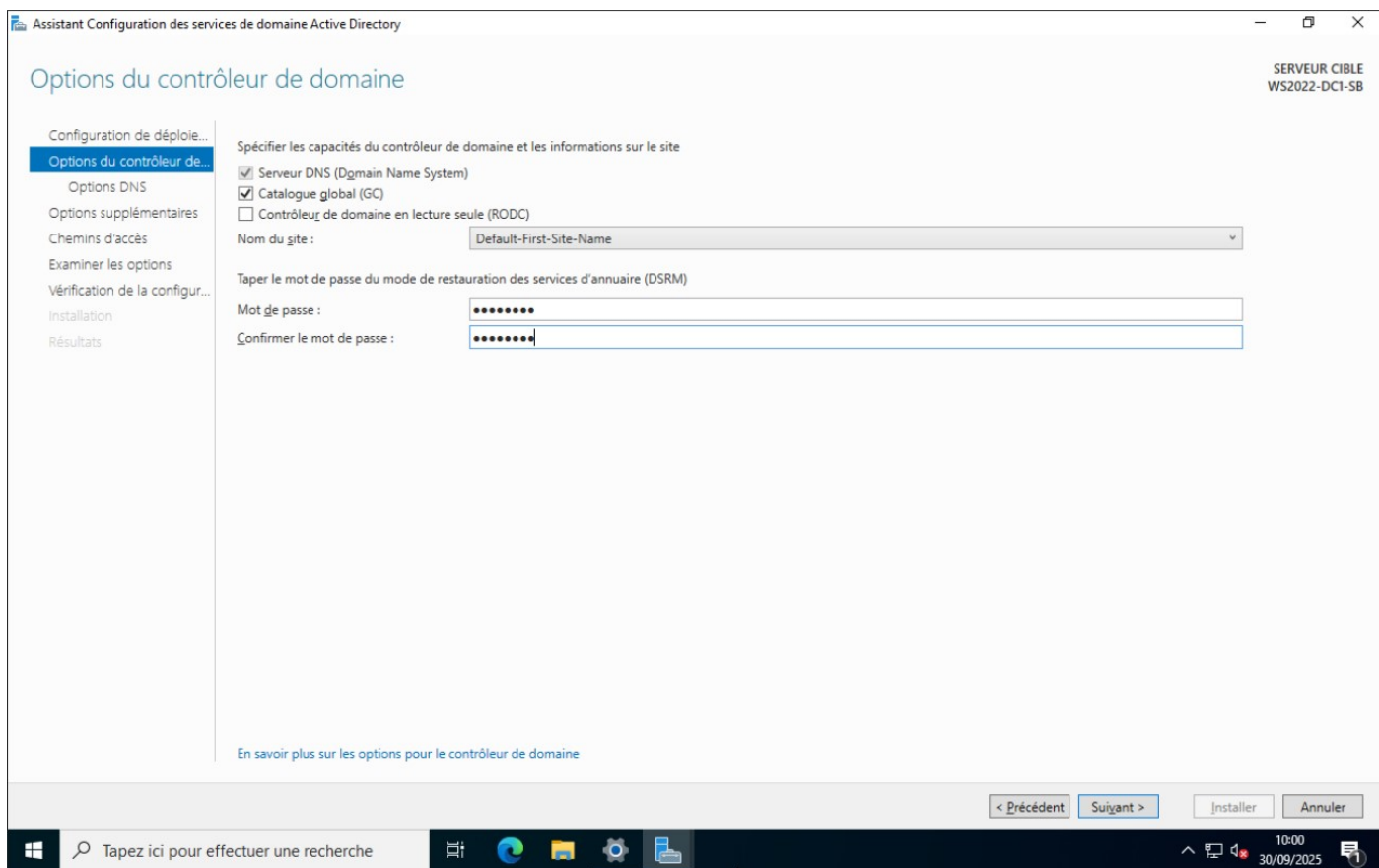


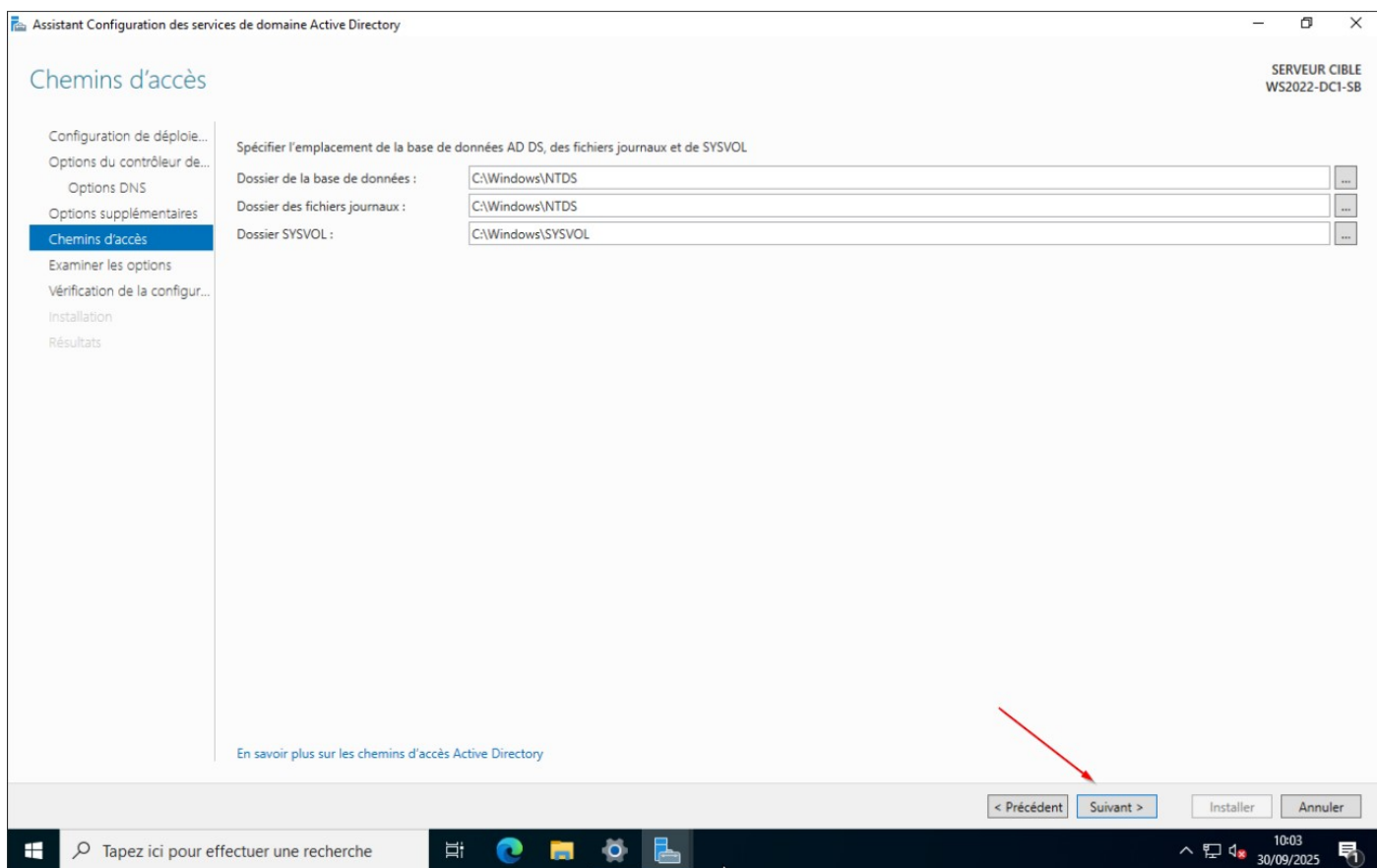
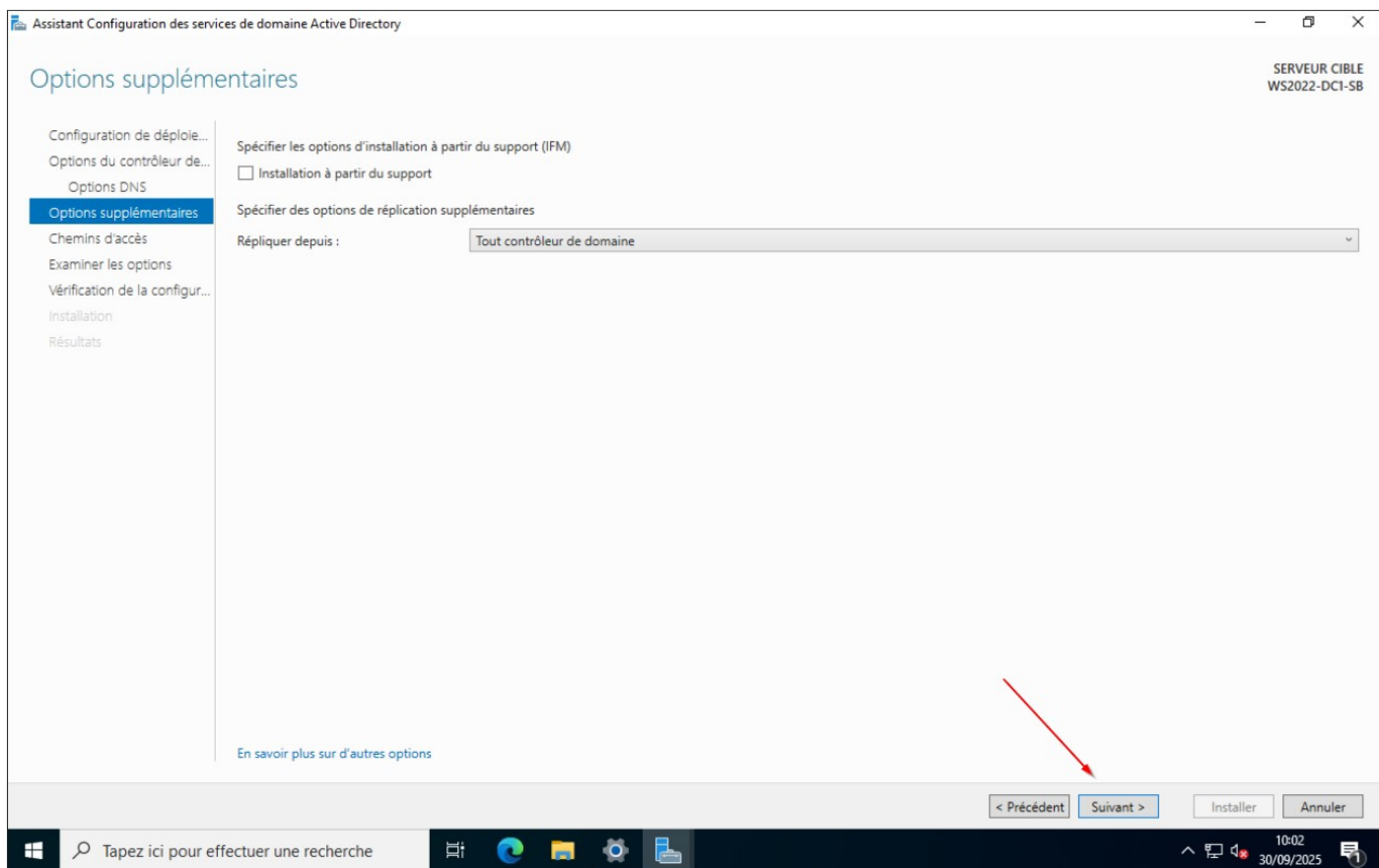
Vous verrez les taches de configuration en suspens.

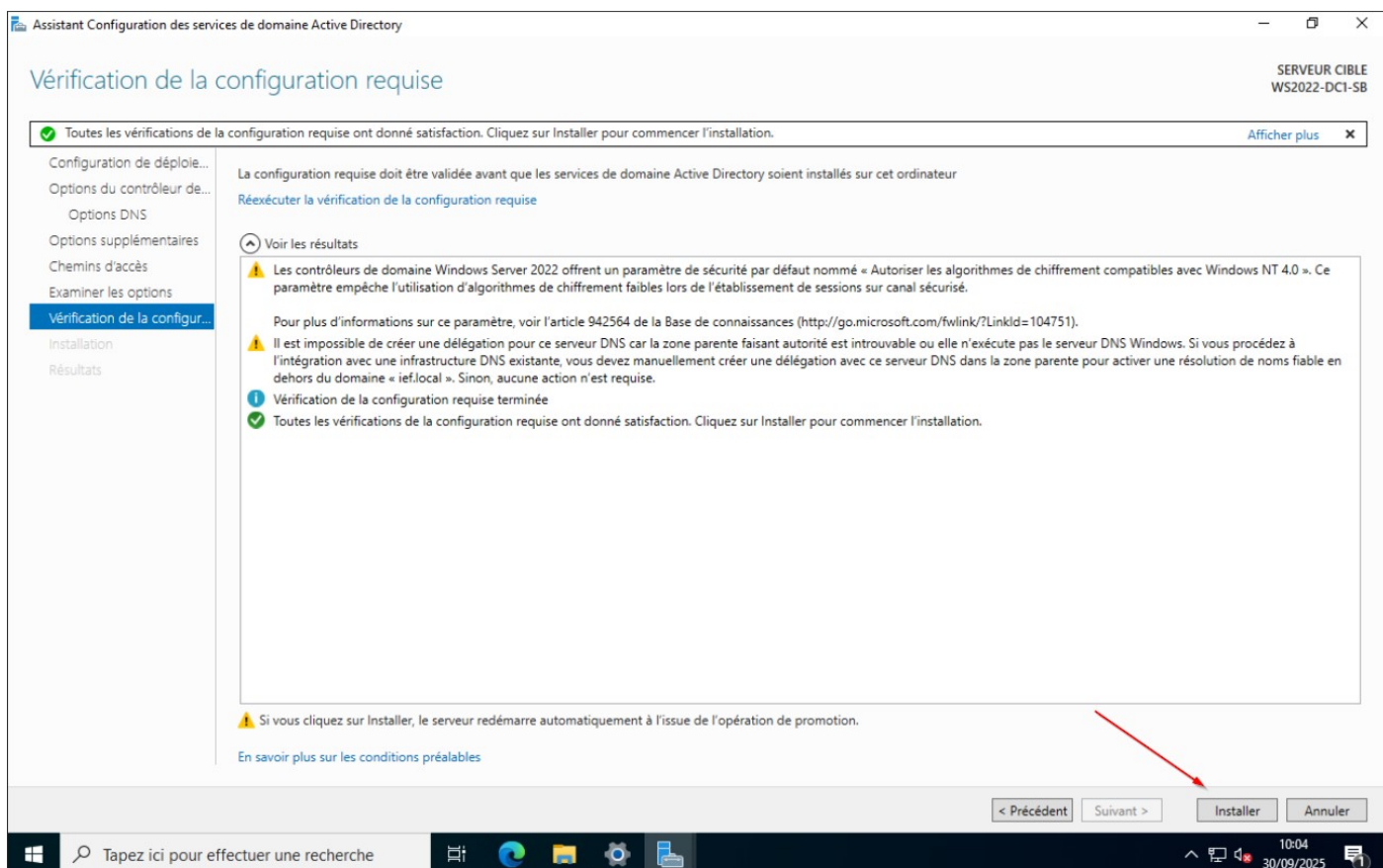
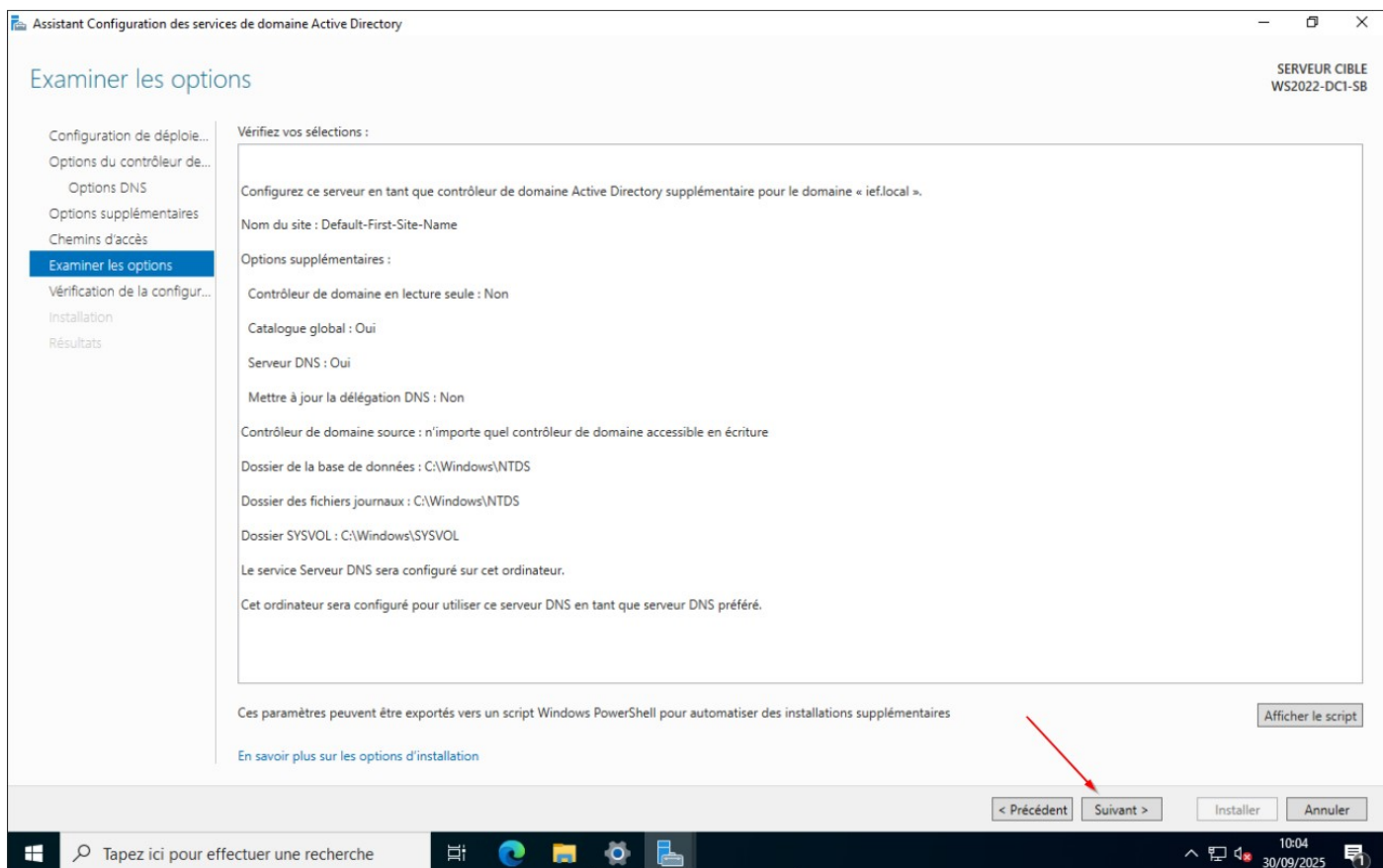
A. Configuration d'AD DS et jonction au domaine

Revenez dans le menu déroulant sous le drapeau du gestionnaire de serveur, et cliquez sur "Promouvoir ce serveur en contrôleur de domaine"



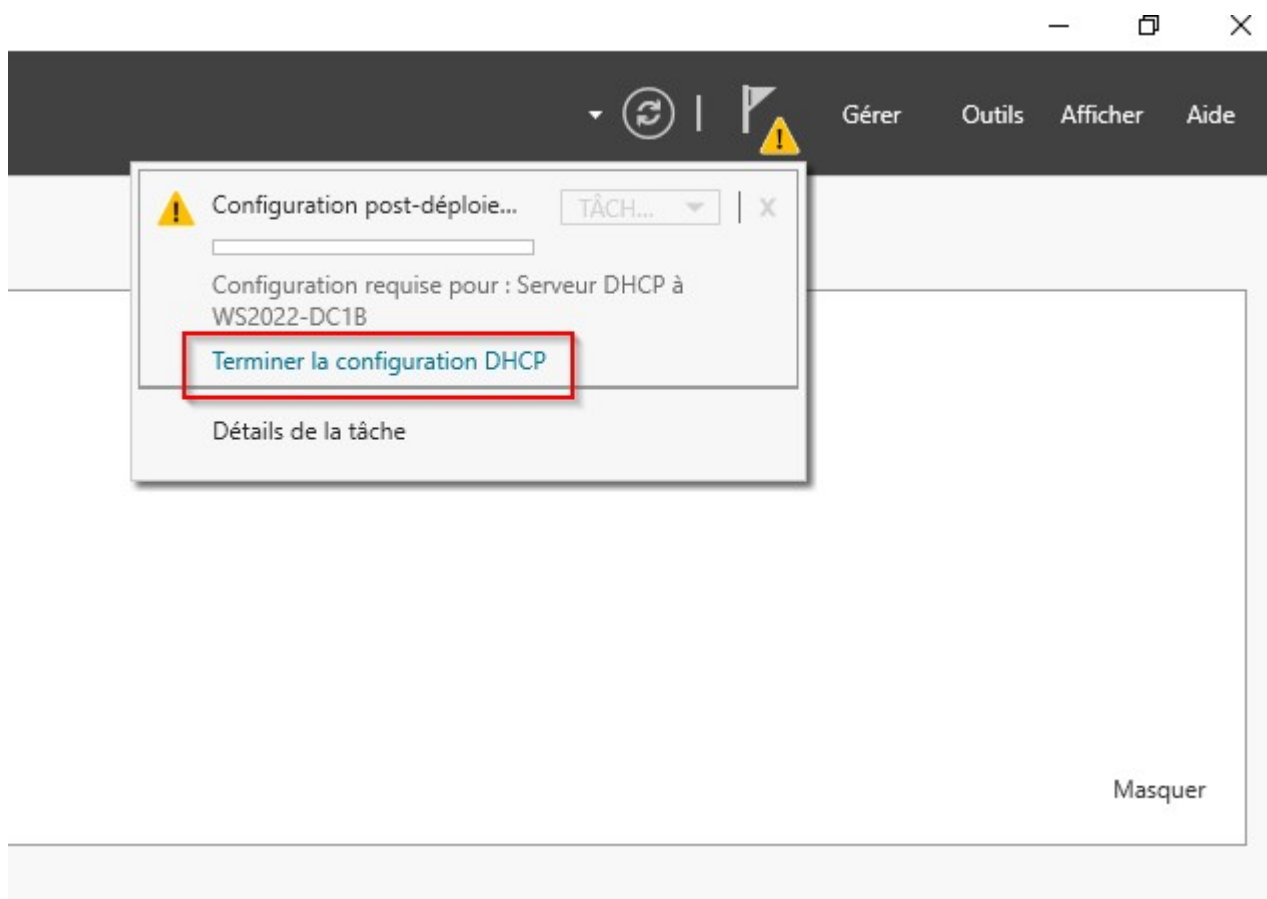




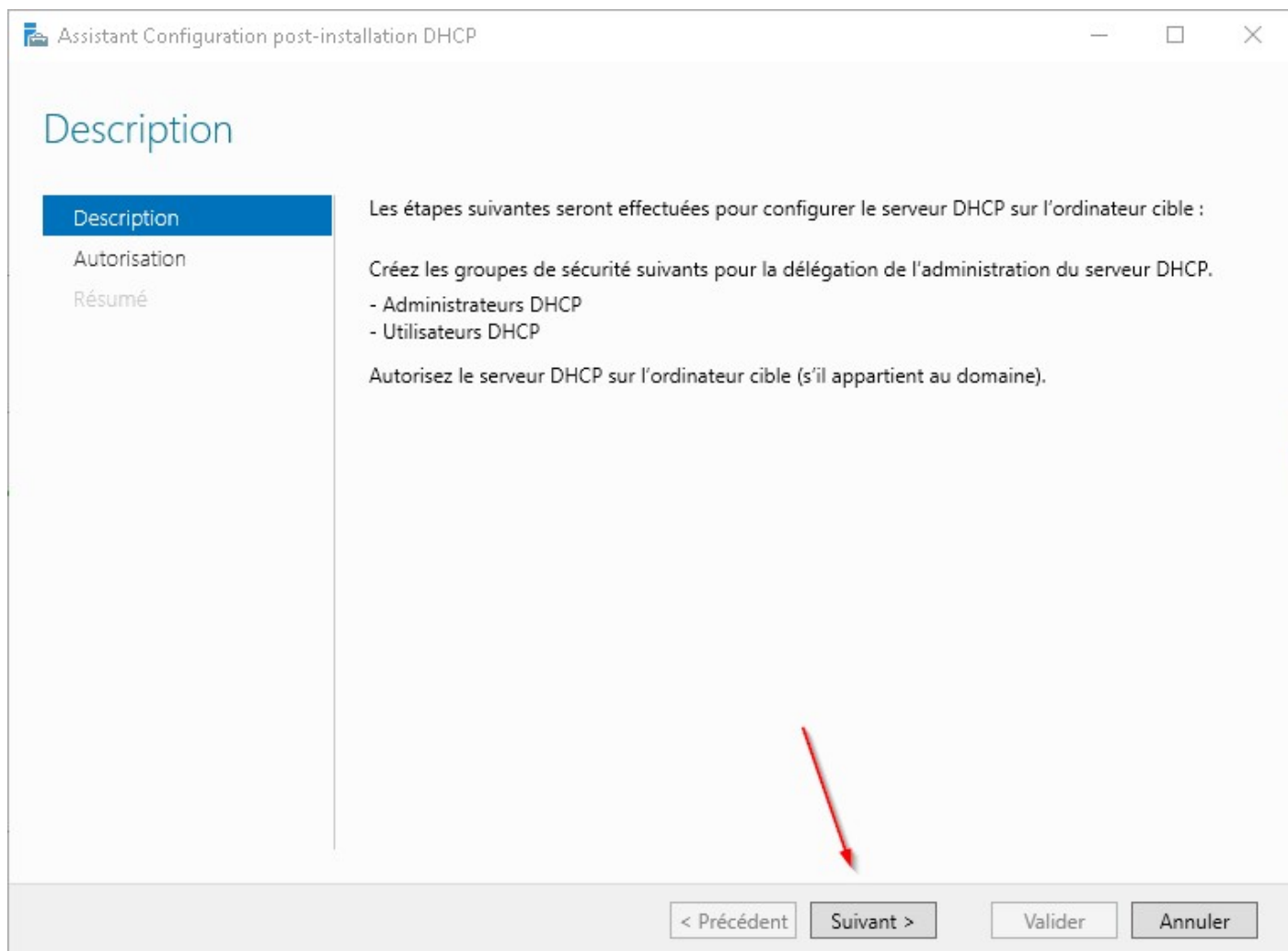


B. Installation du DHCP.

Cliquez sur le panneau en haut à droite puis sur "Terminer la configuration DHCP".



Une fenêtre va s'ouvrir avec des instructions.



Renseignez bien votre nom d'utilisateur et valider ensuite.

Assistant Configuration post-installation DHCP

Autorisation

Description

Autorisation

Résumé

Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.

☒ Utiliser les informations d'identification de l'utilisateur suivant


Nom d'utilisateur : RCBN\Administrateur

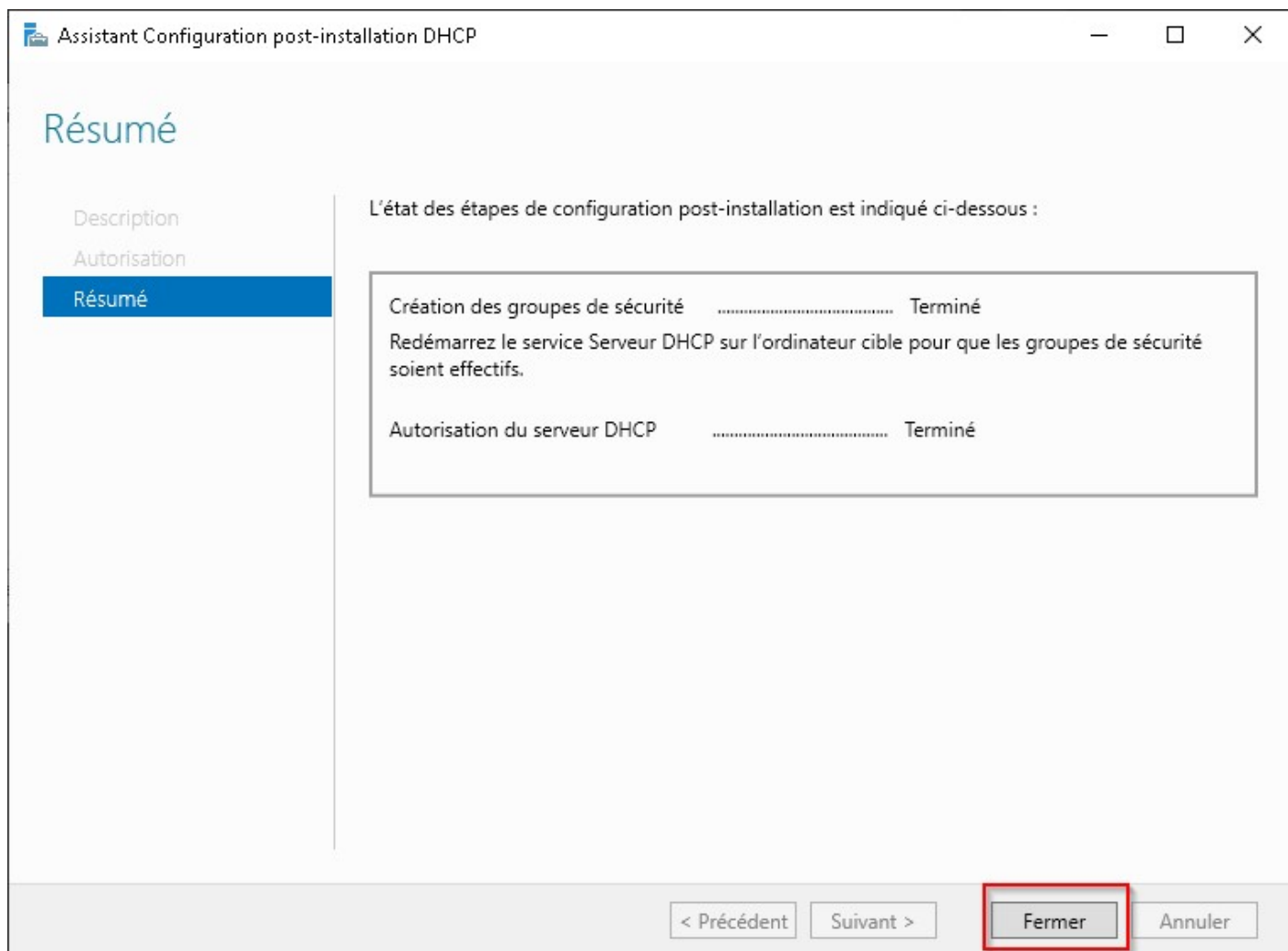
☐ Utiliser d'autres informations d'identification

Nom d'utilisateur :

☐ Ignorer l'autorisation AD

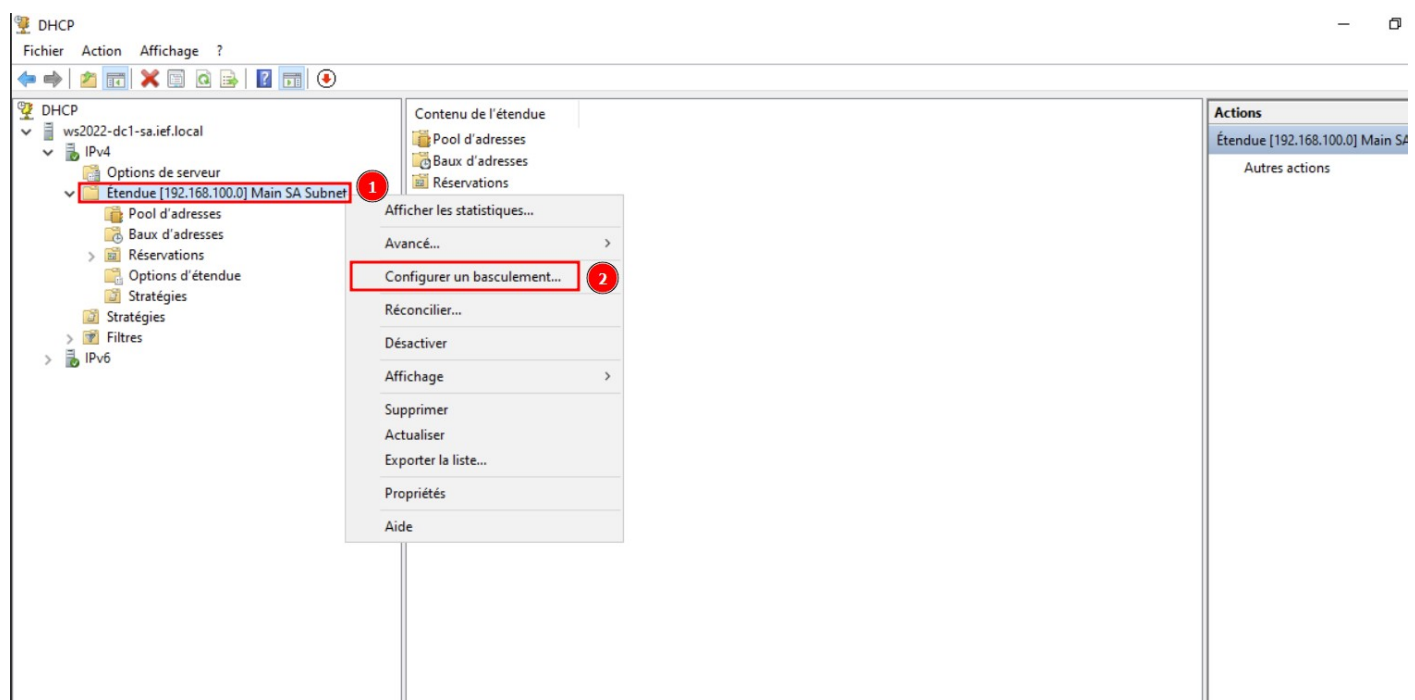
< Précédent Suivant > Valider Annuler





C. Configuration du DHCP Failover

Sur le DC primaire de votre site, crée un basculement sur votre étendu DHCP





Il faut désormais sélectionner le serveur de basculement qui sera le DC2 de votre site, dans notre cas cela sera le DC2-SA

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement



Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :

Ajouter un serveur

☐ Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

< Précédent

Suivant >

Annuler

Ajouter un serveur ? X

Sélectionnez un serveur que vous voulez ajouter à votre console.

☐ Ce serveur :

Parcourir...


☒ Ce serveur DHCP autorisé 1

Nom	Adresse IP
192.168.200.200	192.168.200.200
ws2022-dc1-sa.ief.local	192.168.100.200
ws2022-dc2-sa.ief.local	192.168.100.201 2
ws2022-dc2-sb.ief.local	192.168.200.201

3 OK Annuler

Configurer un basculement


Spécifier le serveur partenaire à utiliser pour le basculement



Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.


Serveur partenaire : 

☐ Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

Il faut désormais configurer les options du basculement, dans notre cas, nous allons uniquement changer le mode et le passer en mode "Serveur de secours" puis mettez un secret partagé afin de chiffrer la communication entre les deux serveurs dhcp pour qu'il ne soit pas en clair sur le réseau.

Configurer un basculement

Créer une relation de basculement



Créer une relation de basculement avec le partenaire ws2022-dc2-sa.ief.local

Nom de la relation :

Délai de transition maximal du client (MCLT) : heures minutes

Mode : 1

Configuration du serveur de secours

Rôle du serveur partenaire :

Adresses réservées pour le serveur de secours : %


☐ Intervalle de basculement d'état : minutes

☒ Activer l'authentification du message

Secret partagé : 2

3

Configurer un basculement



Un basculement va être configuré entre ws2022-dc1-sa.ief.local et ws2022-dc2-sa.ief.local avec les paramètres suivants.

Étendues :

192.168.100.0

Nom de la relation :	ws2022-dc1-sa
Délai de transition maximal du client (MCLT) :	1 h 0 min
Mode :	Serveur de sec
Intervalle de basculement d'état :	Désactivé

< >

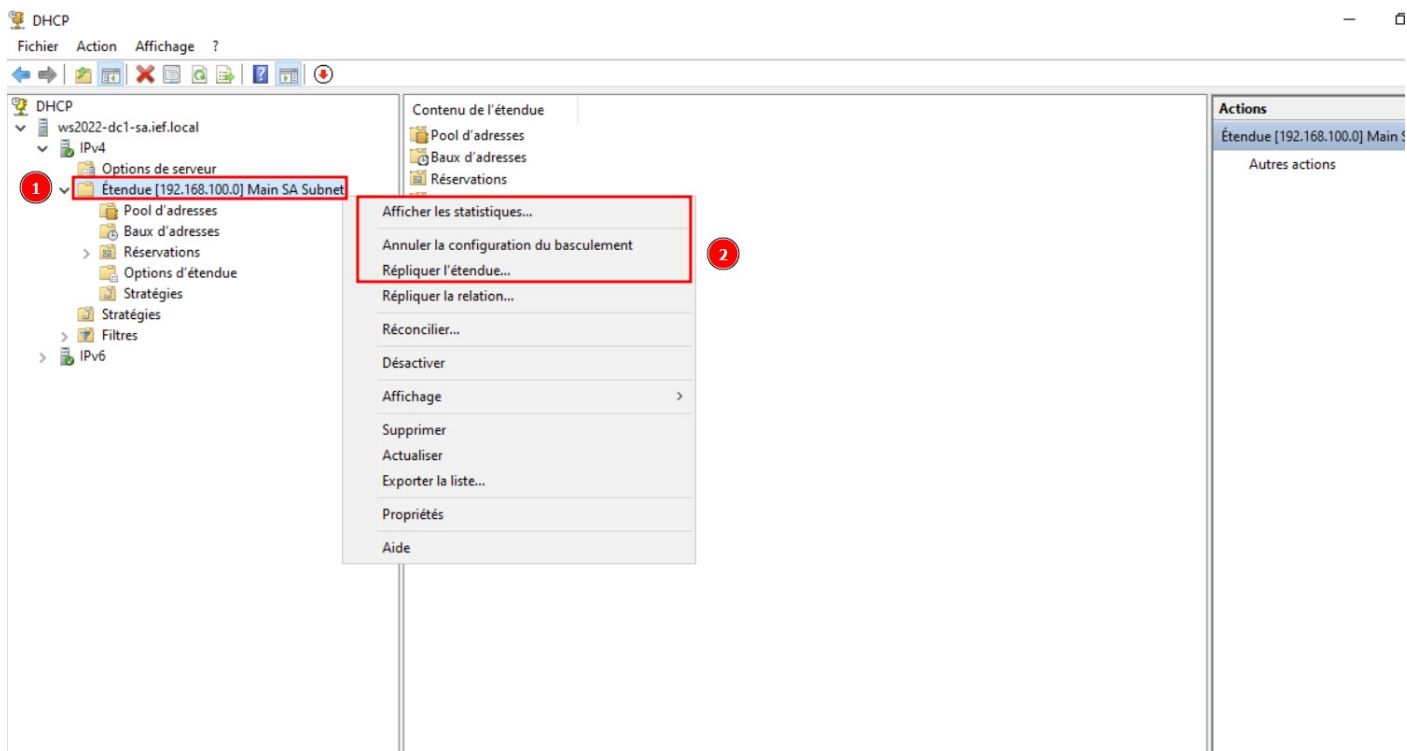
Configuration du serveur de secours

Rôle du serveur partenaire : Veille

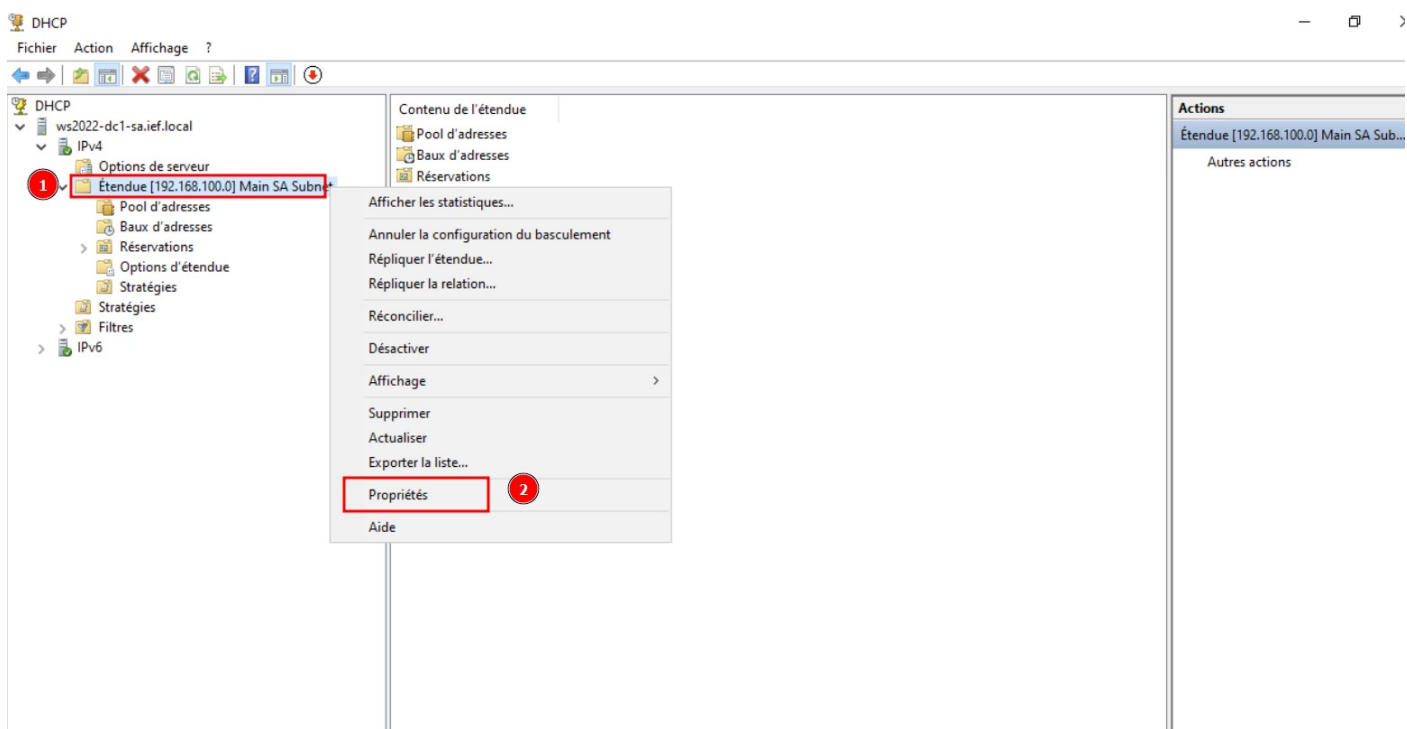
Adresses réservées pour le serveur 5 %

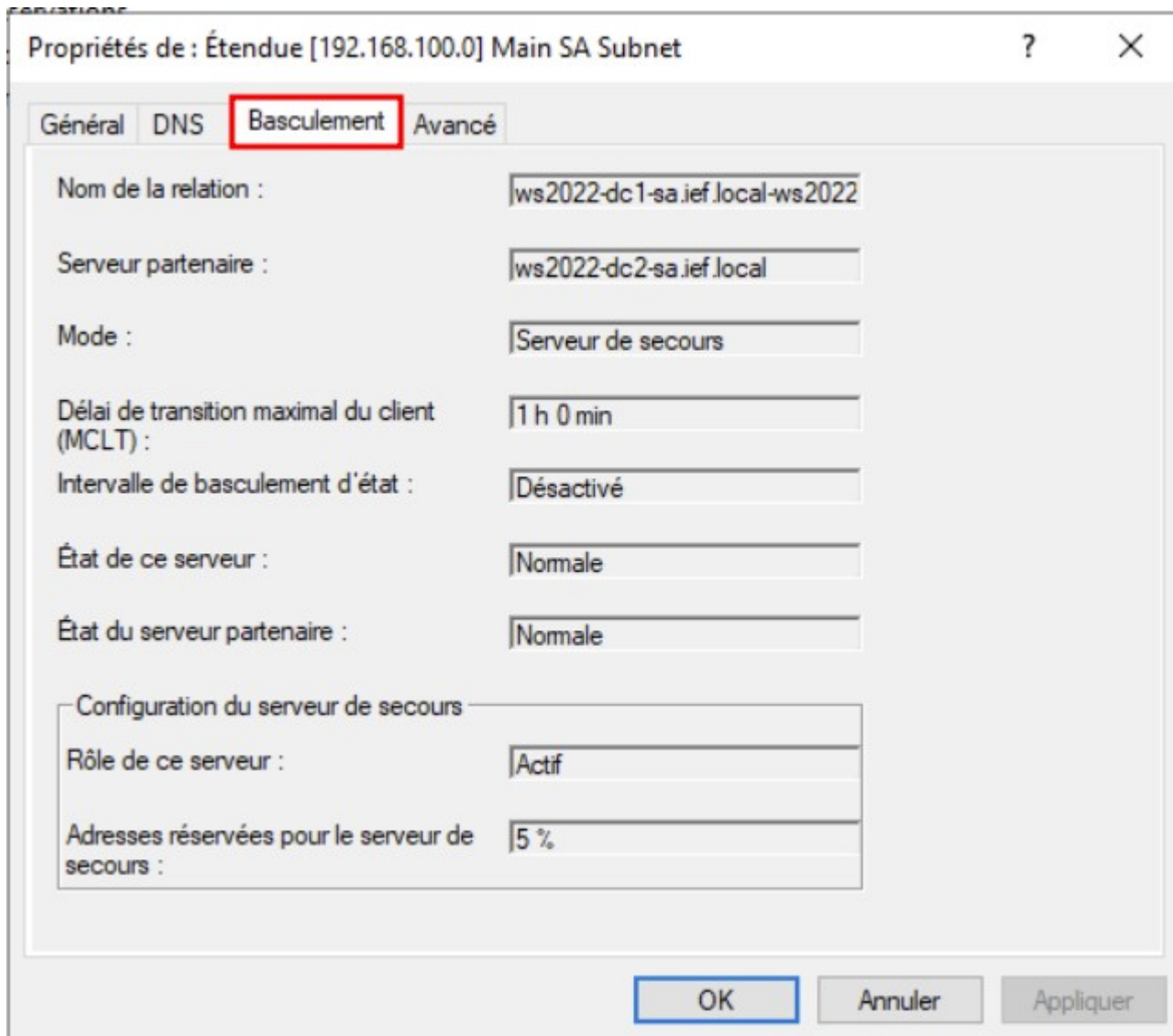
< Précédent **Terminer** Annuler

Sur votre étendue, vous pouvez constater plusieurs options, la première permet d'afficher les statistiques des 2 serveurs dhcp, la deuxième permet d'annuler le basculement, pour refaire la configuration il faudrait l'annuler et la refaire à nouveau. Puis nous pouvons répliquer l'étendu si nous faisons des modifications sur le DHCP primaire.

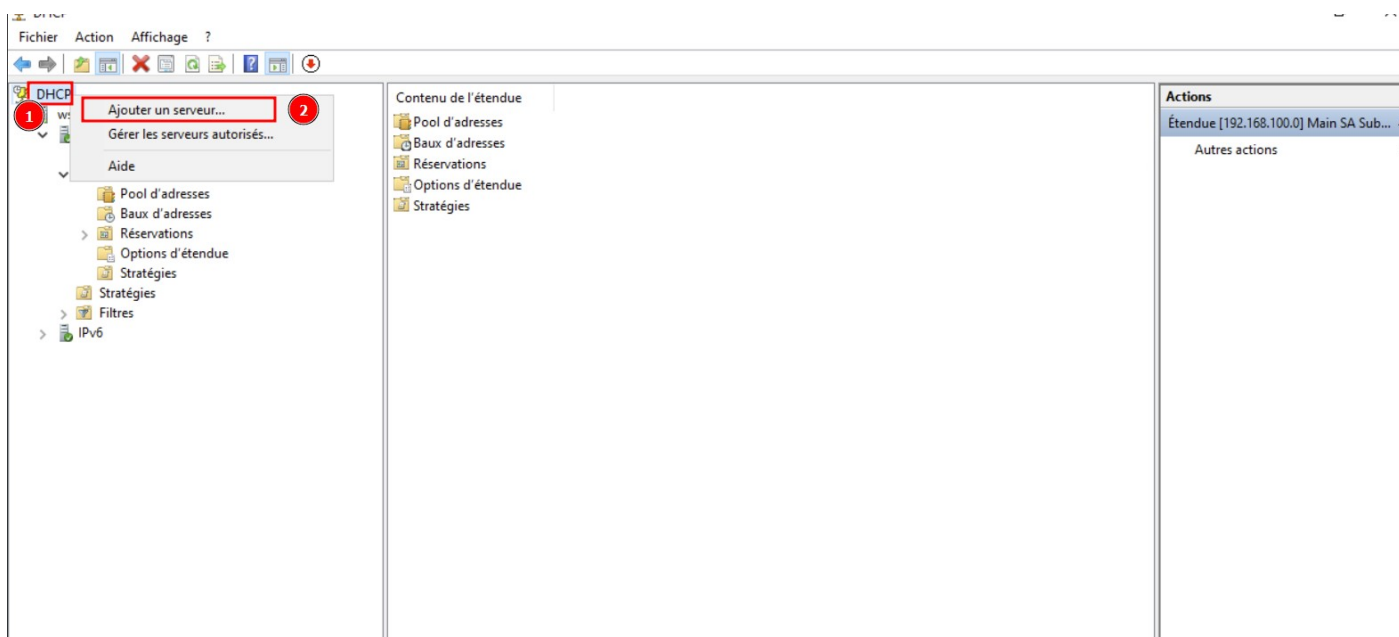


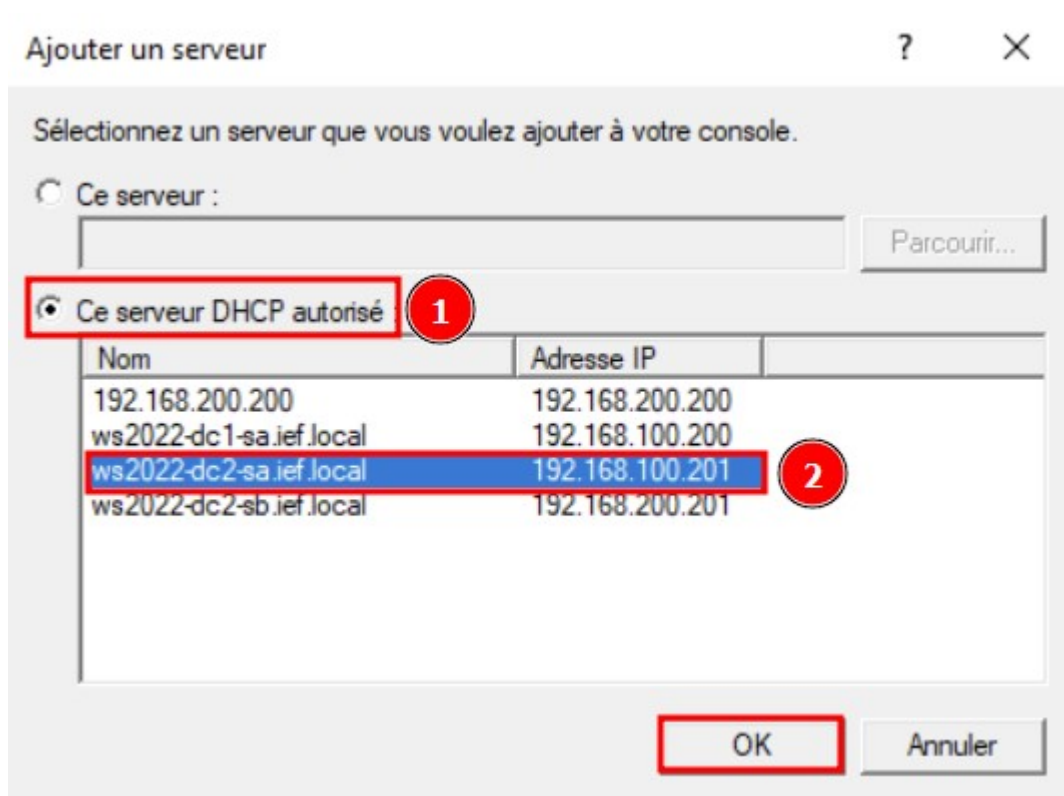
Dans les propriété puis dans Basculement nous avons aussi les détails de la relation entre les deux serveurs DHCP.



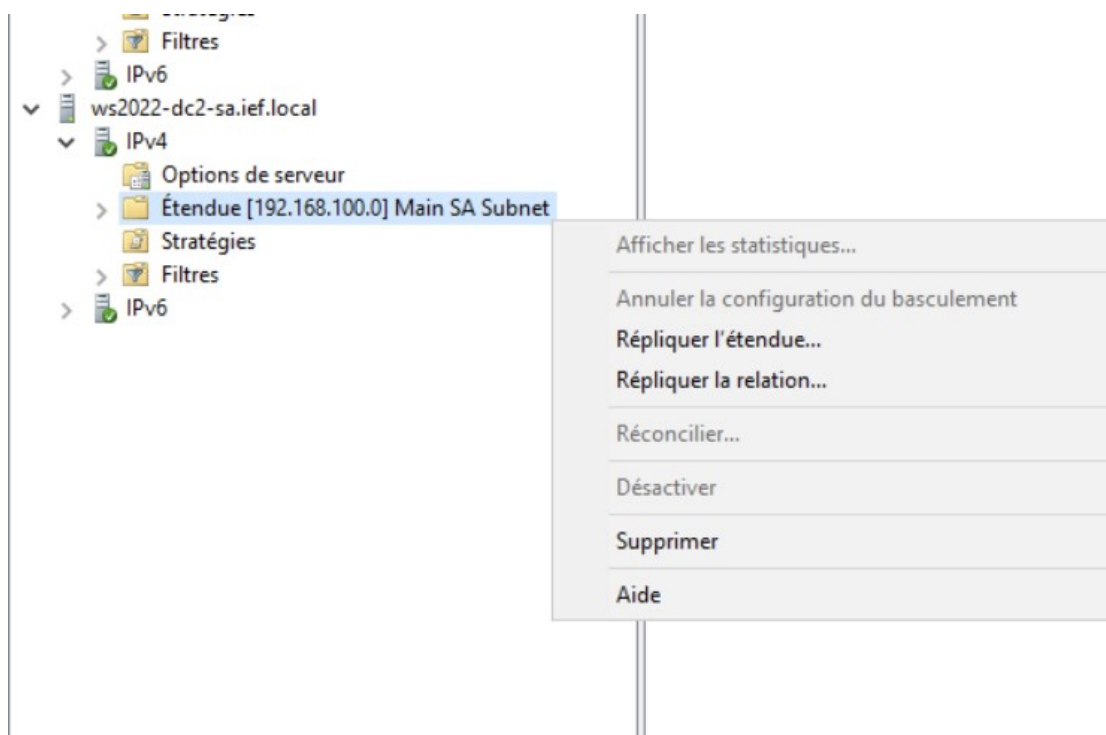


Dans votre panneau DHCP, nous pouvons également ajouter le serveur partenaire afin de pouvoir l'administrer également en cas de soucis. Attention, la relation entre les deux est unidirectionnelle ce qui signifie que si on modifie le DHCP du DC2 rien ne va se passer pour le primaire alors que le primaire écrase la configuration du secondaire.





Nous pouvons voir que le serveur DHCP failover à bel est bien pris la configuration du DHCP primaire.



Windows Server Site B

Windows Server Site B

Installation de Windows Server 2022 sur DC1 en mode GUI

Introduction

Ce premier document couvre la procédure d'installation de Windows Server 2022 dans un environnement Proxmox.

1. Préparation d'une VM
2. Installation de Windows
3. Installation des pilotes

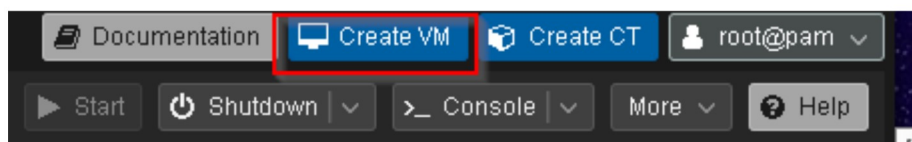
Pour ce faire, vous aurez besoin des éléments suivants :

- Image ISO de Windows Server 2022
- Les ressources suivantes disponibles sur votre Hyperviseur
 - processeur 2v
 - 3 Go de RAM
 - 64 Go de stockage
- Une copie des pilotes VirtIO

Pour mener à bien cette procédure, vous devez disposer des accès nécessaires pour créer des Machines Virtuelles dans Proxmox.

1) Préparation d'une VM

Cliquez sur l'option créer une VM dans l'interface d'administration Proxmox.



Sélectionnez ensuite un nom, le pool de ressources approprié pour votre machine, et cliquez sur suivant.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: pve Resource Pool:

VM ID: 113

Name: 1

Start at boot: ☐

Start/Shutdown order: any

Startup delay: default

Shutdown timeout: default

Tags

No Tags +

Help Advanced ☒ Back Next 3

Sur la deuxième page, sélectionnez d'abord votre stockage ISO Proxmox, puis sélectionnez votre ISO de Windows Server déjà préchargée sur votre Hyperviseur. Sélectionnez ensuite les options appropriées dans les paramètres de l'OS Client. Puis, ajoutez l'ISO des drivers en cliquant sur la case à cocher et en sélectionnant l'ISO dans votre bibliothèque.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

☒ Use CD/DVD disc image file (iso)

Storage: ZFS-data 1

ISO image: x64_dvd_4e34897c.iso 2

Guest OS: Microsoft Windows 4

Type: 11/2022/2025 5

Version: 11/2022/2025 5

☐ Use physical CD/DVD Drive

☐ Do not use any media

☒ Add additional drive for VirtIO drivers 6

Storage: ZFS-data 7

ISO image: virtio-win-0.1.266.iso 8

Advanced ☒ Back Next 3

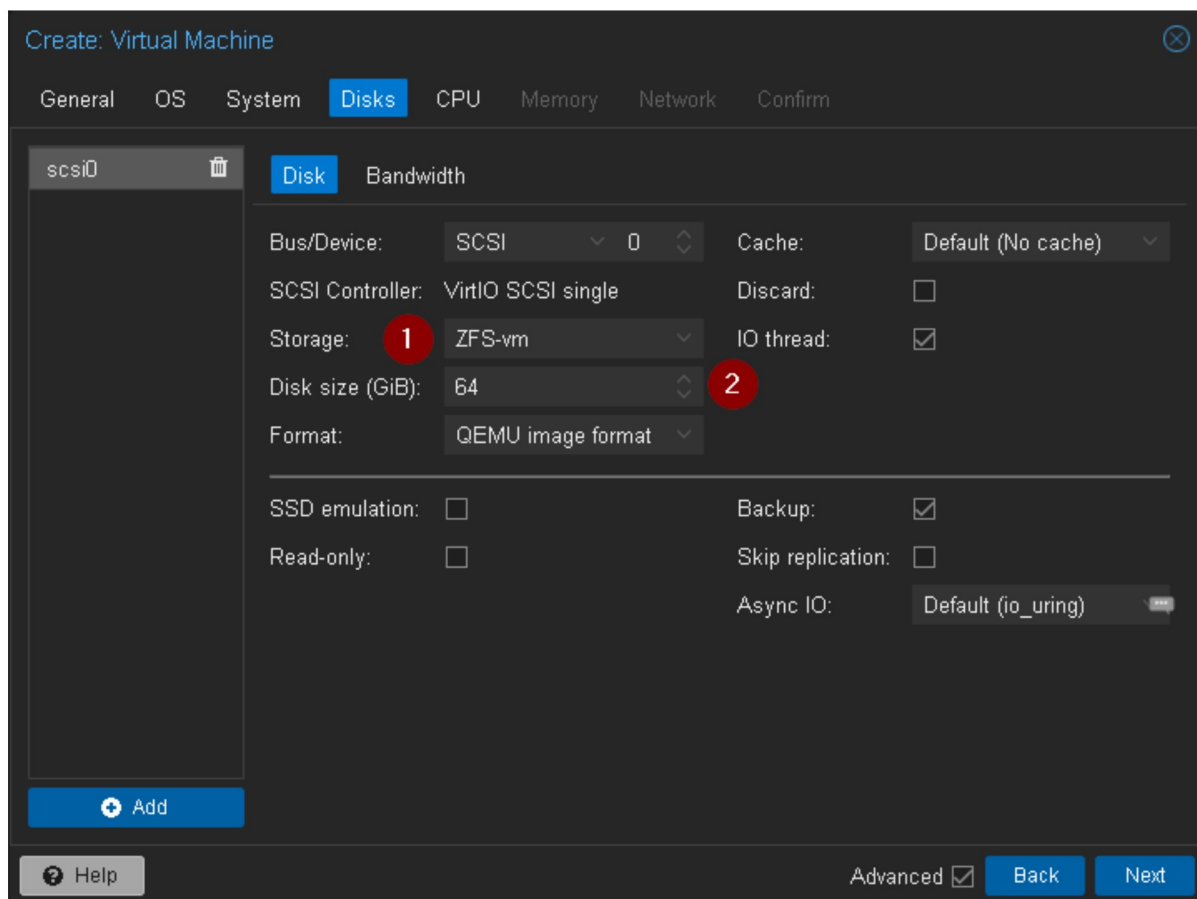
Ajoutez ensuite un espace de Stockage pour la partition EFI et la puce TPM qui sera nécessaire pour l'activation de BitLocker sur vos serveurs. En général, l'espace de stockage est le même que celui utilisé pour stocker l'image disque principale.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'System' tab selected. The 'EFI Storage' dropdown is highlighted with a red circle and the number '1'. The 'TPM Storage' dropdown is highlighted with a red circle and the number '2'. The 'Add TPM' checkbox is checked. The 'Version' dropdown is set to 'v2.0'. The 'Format' dropdown is set to 'QEMU image format (qcow2)'. The 'Pre-Enroll keys' checkbox is checked. The 'Advanced' checkbox is checked. The 'Back' and 'Next' buttons are visible at the bottom right.

Field	Value
Graphic card:	Default
Machine:	q35
SCSI Controller:	VirtIO SCSI single
Qemu Agent:	<input type="checkbox"/>
BIOS:	OVMF (UEFI)
Add TPM:	<input checked="" type="checkbox"/>
EFI Storage:	[Dropdown menu highlighted with red circle 1]
TPM Storage:	[Dropdown menu highlighted with red circle 2]
Version:	v2.0
Format:	QEMU image format (qcow2)
Pre-Enroll keys:	<input checked="" type="checkbox"/>

Help Advanced ☒ Back Next

Dans la page de sélection du disque virtuel principal, choisissez l'emplacement de stockage de l'image disque et augmentez la taille du disque à votre convenance. Cliquez sur "Add" pour ajouter des disques secondaires.



Dans la page CPU, ajoutez un Socket à votre machine virtuelle et sélectionnez le Type "x86-64-v2-AES" s'il n'est pas sélectionné par défaut.

Si votre hyperviseur dispose de deux CPU physiques, vous pouvez activer l'option NUMA.

Create: Virtual Machine

GeneralOSSystemDisksCPUMemoryNetworkConfirm

Sockets: 1 2

Type: 2 x86-64-v2-AES

Cores: 1

Total cores: 2

VCPUs: 2

CPU units: 100

CPU limit: unlimited

Enable NUMA: ☒ 3

CPU Affinity: All Cores

Extra CPU Flags:

Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	md-clear	Required to let the guest OS know if MDS is mitigated correctly
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	pcid	Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	spec-ctrl	Allows improved Spectre mitigation with Intel CPUs
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	ssbd	Protection for "Speculative Store Bypass" for Intel models
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	ibpb	Allows improved Spectre mitigation with AMD CPUs
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	virt-ssbd	Basis for "Speculative Store Bypass" protection for AMD models

Help

Advanced ☒

Back

Next

Dans la page Mémoire, sélectionnez un montant de RAM entre 3 et 4 go minimum. En fonction de votre utilisation, il faudra allouer de la mémoire en plus. Sélectionnez ensuite la même quantité de mémoire minimale ou désactivez l'option de Ballooning.

Create: Virtual Machine

General OS System Disks CPU **Memory** Network Confirm

Memory (MiB): 4096 1

Minimum memory (MiB): 4096 2

Shares: Default (1000)

Ballooning Device: ☒ 3

Help Advanced ☒ Back Next

Configurez ensuite la carte réseau selon votre infrastructure. Sélectionnez la carte réseau VirtIO dans la rubrique "Modèle"

Create: Virtual Machine

General OS System Disks CPU Memory **Network** Confirm

☐ No network device

Bridge: 1 vmbri0 Model: 2 VirtIO (paravirtualized)

VLAN Tag: no VLAN MAC address: auto

Firewall: ☒

Disconnect: ☐

Rate limit (MB/s): unlimited

MTU: 1500 (1 = bridge MTU) Multiqueue:

Help Advanced ☒ Back Next

Vérifiez votre configuration et cliquez sur le bouton FINISH.

Create: Virtual Machine

General

OS

System

Disks

CPU

Memory

Network

Confirm

Key ↑	Value
cores	1
cpu	x86-64-v2-AES
ide2	ZFS-data:iso/fr-fr_windows_server_2022_updated_nov_2024_x64_dvd_4e34897c.iso,med...
memory	2048
net0	virtio,bridge=vmbr0,firewall=1
nodename	pve
numa	0
ostype	l26
scsi0	ZFS-retro:32,iotthread=on
scsihw	virtio-scsi-single
sockets	1
vmid	113

☐ Start after created

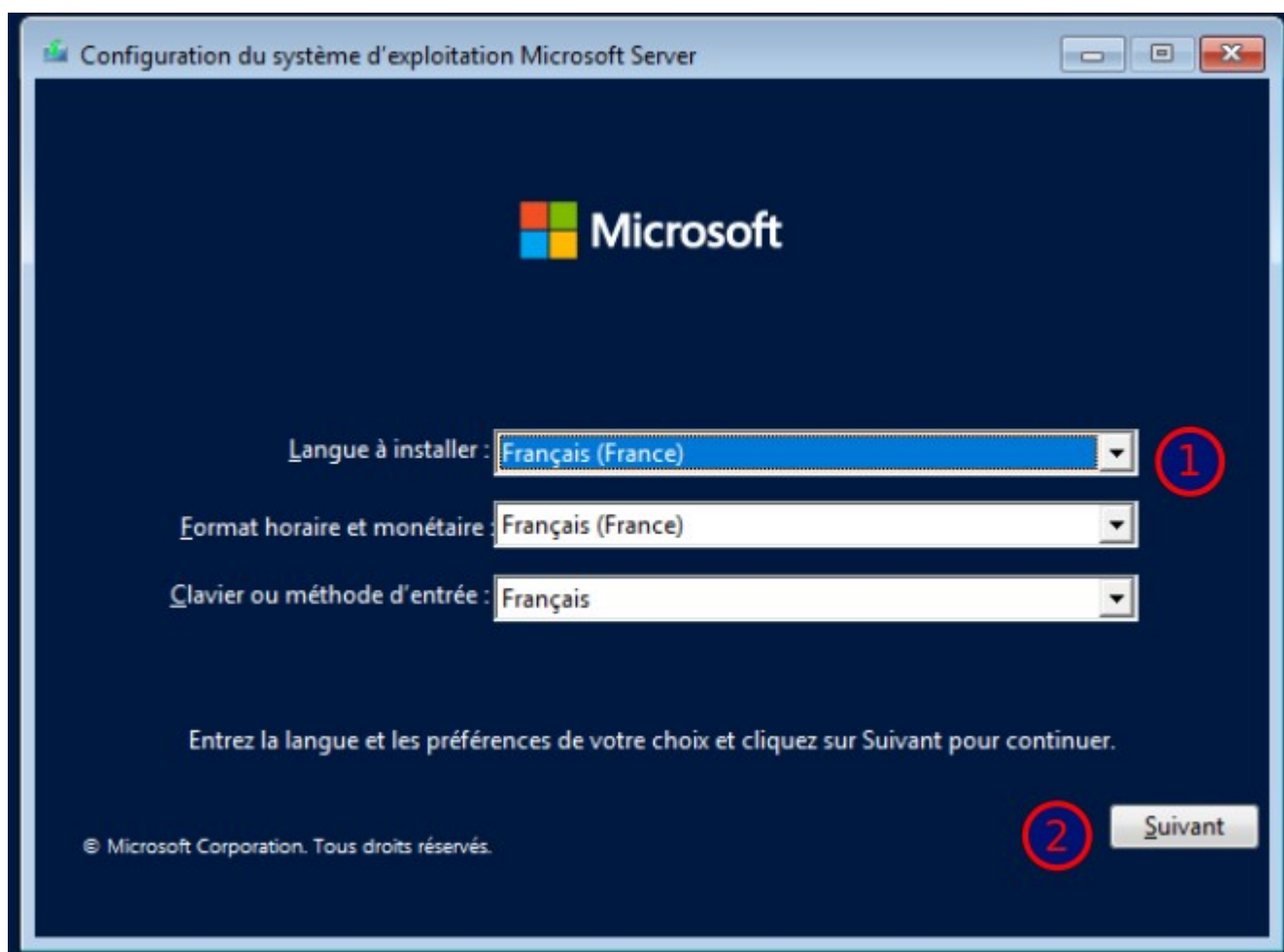
Advanced ☒

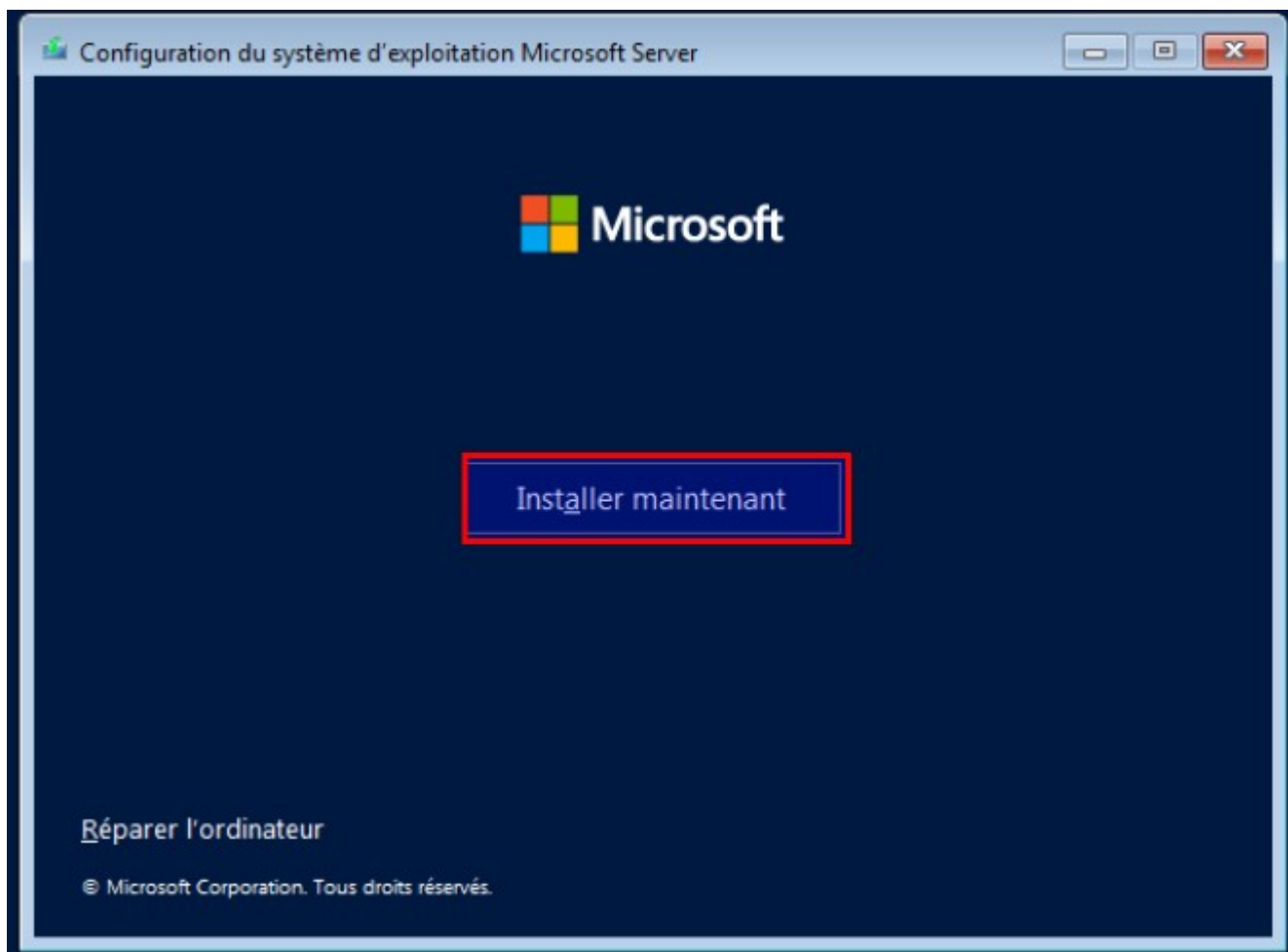
Back

Finish

2) Installation de Windows Server 2022

Une fois la VM lancée sur l'ISO de Windows Server, sélectionnez la langue (Français) et cliquez sur suivant.





Sélectionnez bien "Je n'ai pas de clé de produit"

Activer la configuration du système d'exploitation Microsoft Server

Si vous installez le système d'exploitation Microsoft Server pour la première fois sur cet ordinateur (ou si vous installez une autre édition), vous devez entrer une clé de produit valide pour le système d'exploitation Microsoft Server. Votre clé de produit doit figurer dans le courrier de confirmation que vous avez reçu après l'achat d'une copie numérique du système d'exploitation Microsoft Server ou sur une étiquette fournie dans la zone du système d'exploitation Microsoft Server.

La clé de produit (Product Key) ressemble à ceci : XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Si vous réinstallez le système d'exploitation Microsoft Server, sélectionnez je ne dispose pas d'une clé de produit. Votre copie du système d'exploitation Microsoft Server sera automatiquement



[Déclaration de confidentialité](#)

[Je n'ai pas de clé de produit \(Product Key\)](#)

[Suivant](#)

Sélectionnez « Windows Server 2022 Standard (expérience de bureau) » et continuez

Sélectionner le système d'exploitation à installer

Système d'exploitation	Architecture	Date de modi...
Windows Server 2022 Standard	x64	07/08/2021
Windows Server 2022 Standard (expérience de bureau)	x64	07/08/2021
Windows Server 2022 Datacenter	x64	07/08/2021
Windows Server 2022 Datacenter (expérience de bureau)	x64	07/08/2021

1

Description :

Cette option installe l'environnement graphique Windows complet, qui utilise de l'espace disque supplémentaire. Il peut être utile si vous souhaitez utiliser le bureau Windows ou une application qui en a besoin.

2

Suivant

Avis et conditions du contrat de licence applicables

VOUS DEVEZ ACCEPTER LES TERMES DE LA LICENCE DU LOGICIEL. VOIR CI-APRÈS. Veuillez lire les conditions de licence complètes fournies à l'adresse (aka.ms/useterms).

NOTIFICATION IMPORTANTE

Informations relatives à l'utilisation et au diagnostic. Microsoft recueille ces informations sur Internet pour assurer la sécurité et la mise à jour de Windows, diagnostiquer les problèmes et apporter des améliorations aux produits, et peut associer ces informations à votre organisation. Les systèmes d'exploitation des serveurs Microsoft peuvent être configurés pour désactiver les données de diagnostic, envoyer des données de diagnostic obligatoires ou envoyer des données de diagnostic facultatives. Le réglage par défaut consiste à envoyer les données de diagnostic requises. Les données de diagnostic requises

1

☒ J'accepte les termes du contrat de licence logiciel Microsoft. Si la licence appartient à une organisation, je suis autorisé à agir en son nom.

2

Suivant

Choisissez l'option personnalisée.

Quel type d'installation voulez-vous effectuer ?

Mise à jour : Installer le système d'exploitation Microsoft Server et conserver les fichiers, les paramètres et les applications.

Avec cette option, les fichiers, paramètres et applications sont déplacés vers le nouveau système d'exploitation. Cette option est disponible uniquement lorsqu'une version prise en charge du système d'exploitation est déjà en cours d'exécution sur l'ordinateur.

Personnalisé : installer uniquement le système d'exploitation Microsoft Server (avancé)


Avec cette option, les fichiers, les paramètres et les applications ne sont pas déplacés vers le nouveau système d'exploitation. Pour modifier les partitions et les lecteurs, démarrez l'ordinateur à l'aide du disque d'installation. Nous vous recommandons de sauvegarder vos fichiers avant de continuer.

Où voulez-vous installer le système d'exploitation ?

Nom	Taille totale	Espace libre	Type

 Actualiser Supprimer Formater Nouveau

1

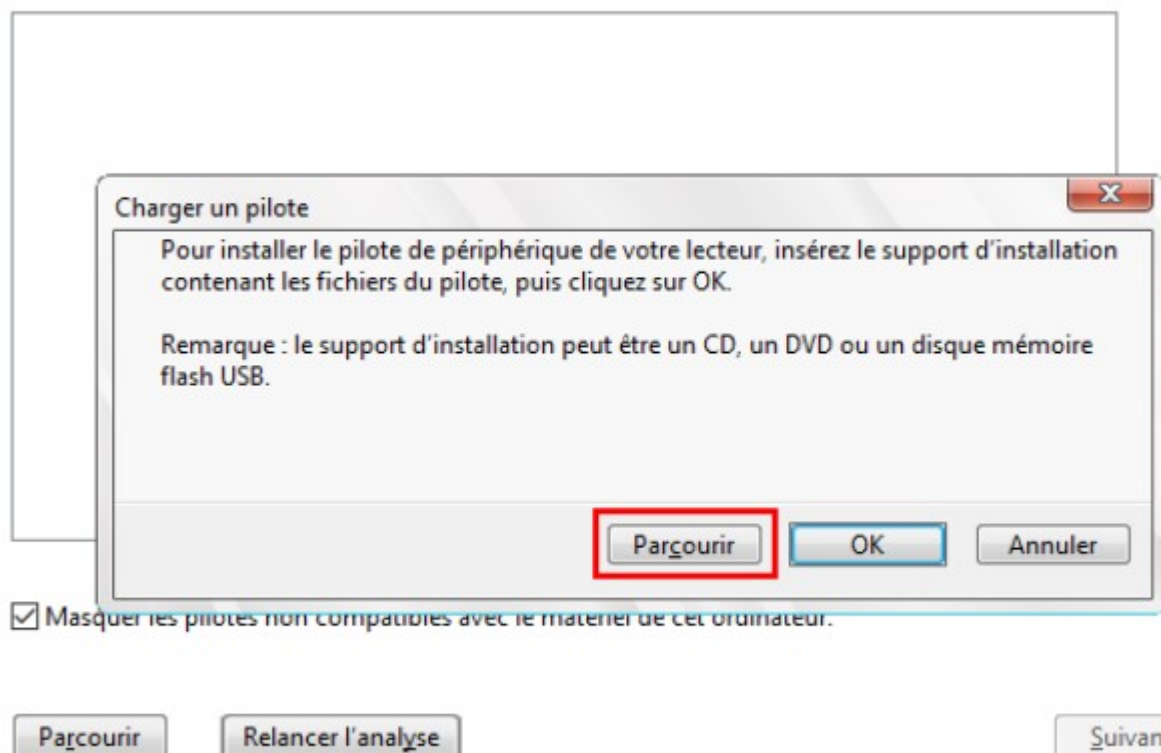
 Charger un pilote Étendre

Nous n'avons trouvé aucun lecteur. Pour obtenir un pilote de stockage, cliquez sur Charger un pilote.

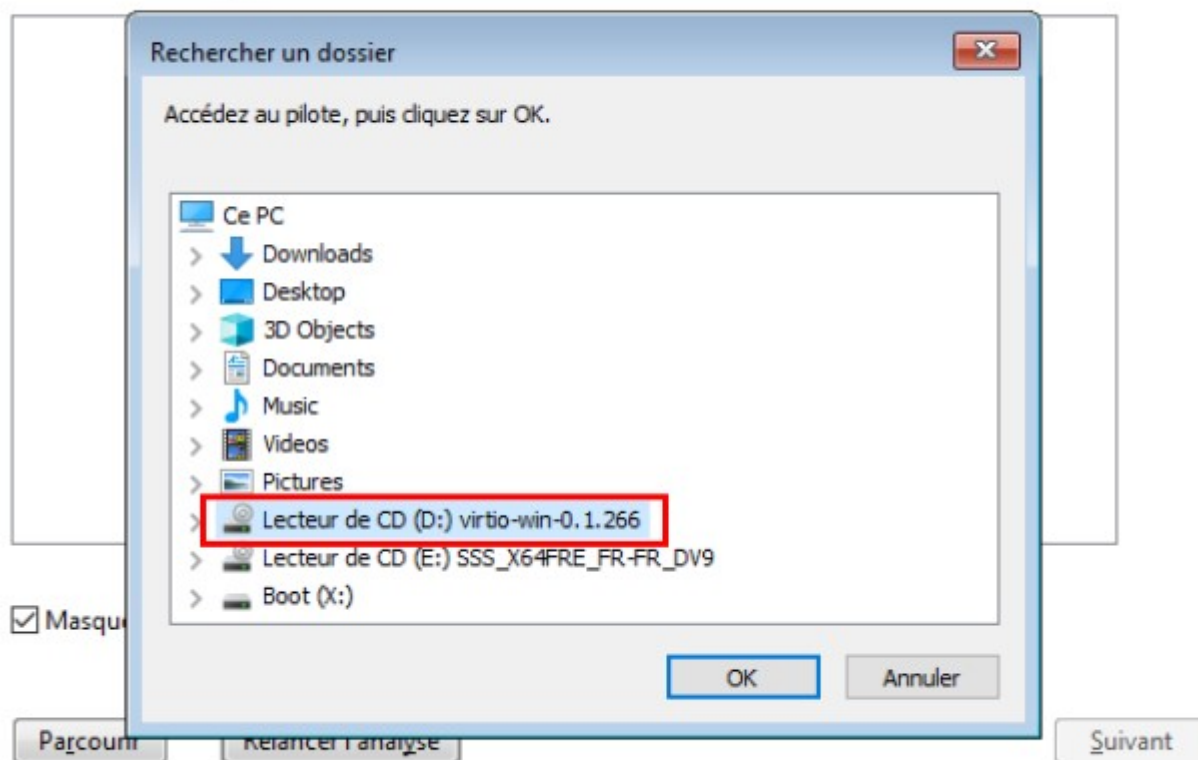
2

Suivant

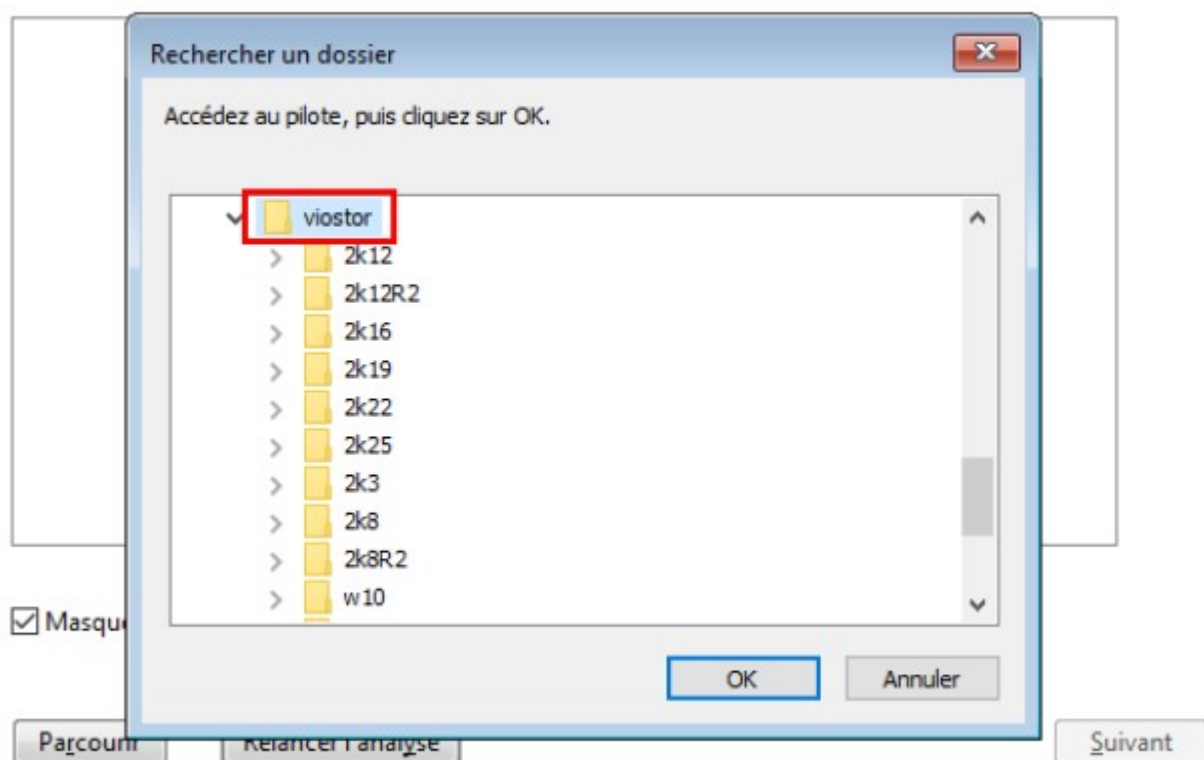
Sélectionner le pilote à installer



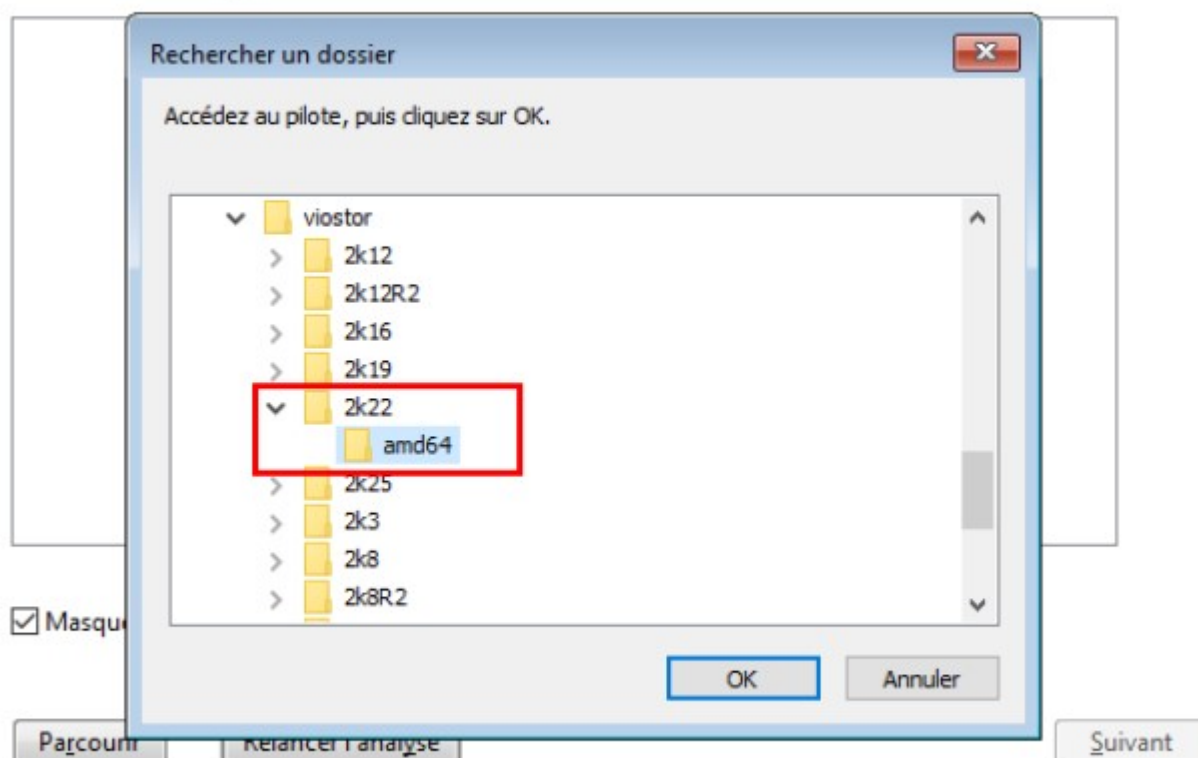
Sélectionner le pilote à installer



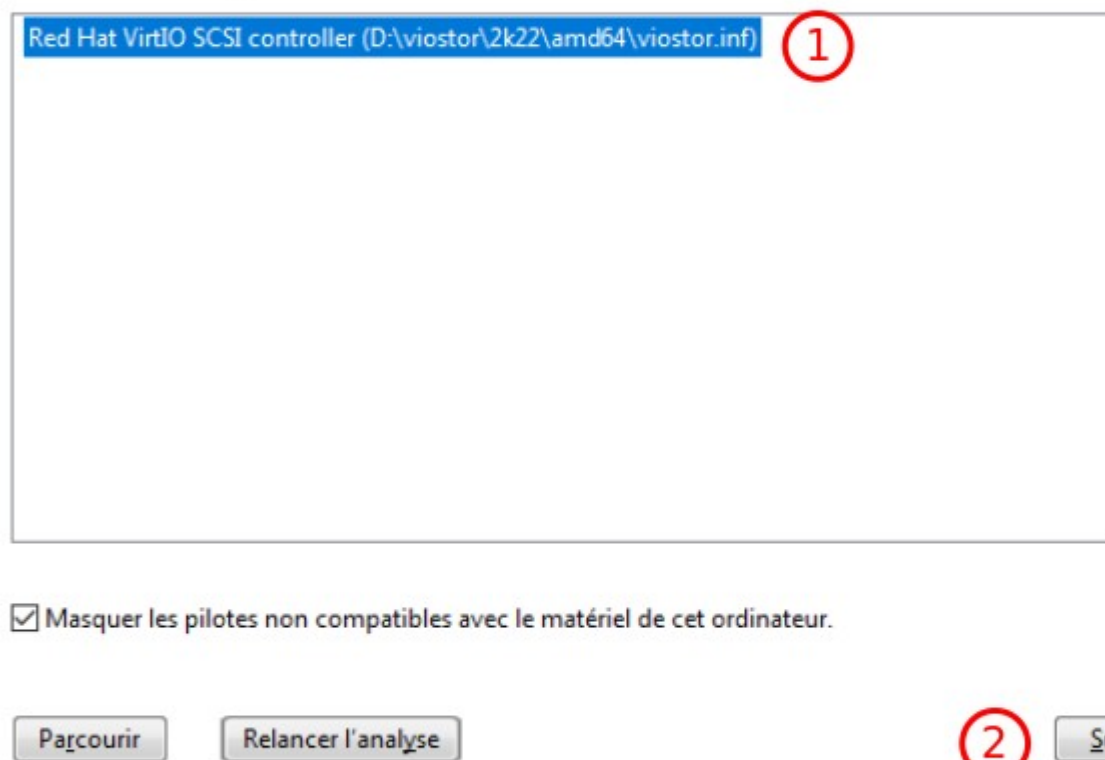
Sélectionner le pilote à installer




Sélectionner le pilote à installer

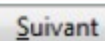


Sélectionner le pilote à installer



Où voulez-vous installer le système d'exploitation ?

	Nom	Taille totale	Espace libre	Type
	Lecteur 0 Espace non alloué	64.0 Go	64.0 Go	

 Actualiser Supprimer Formater Nouveau Charger un pilote Étendre Suivant

Paramètres de personnalisation

Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.

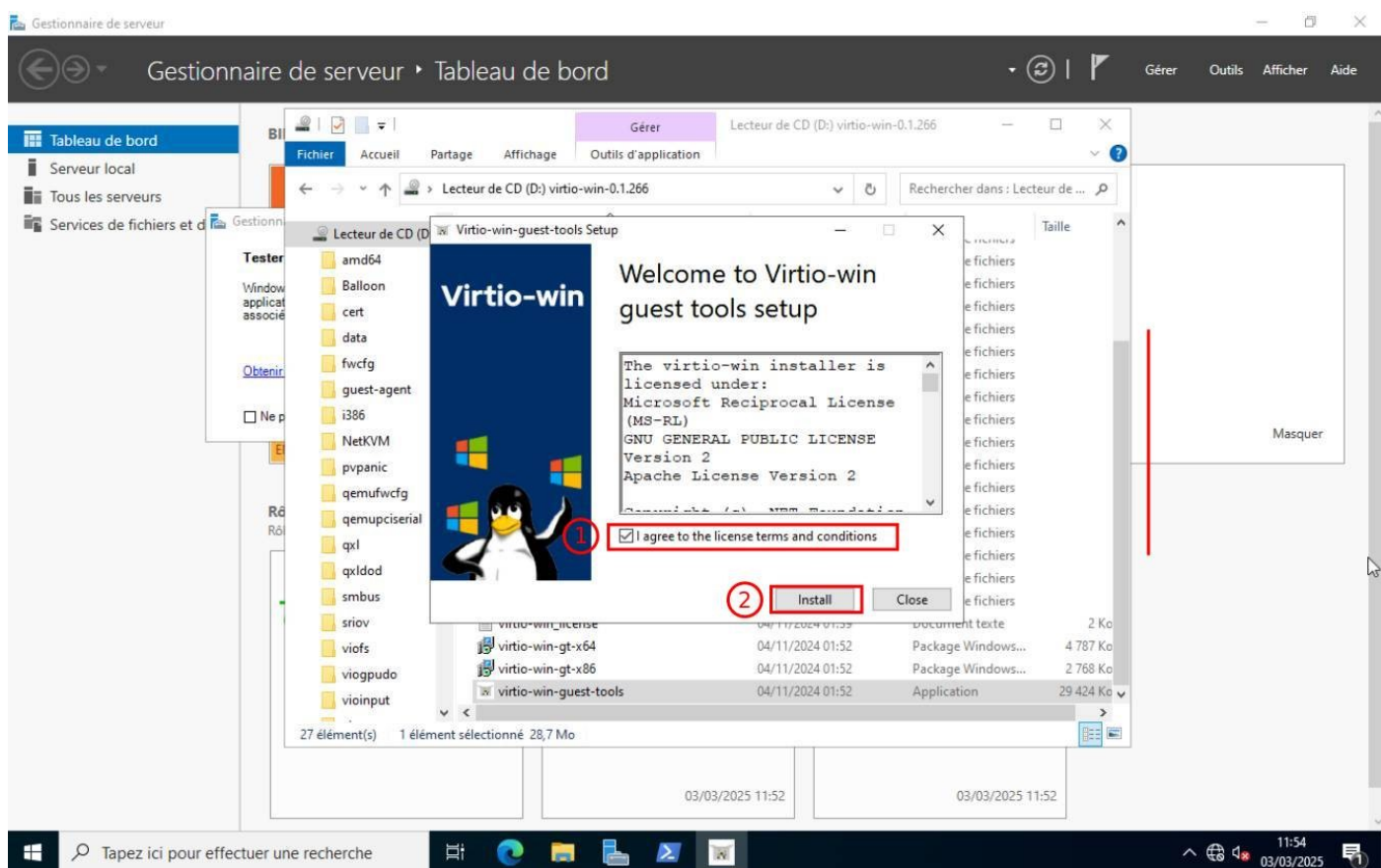
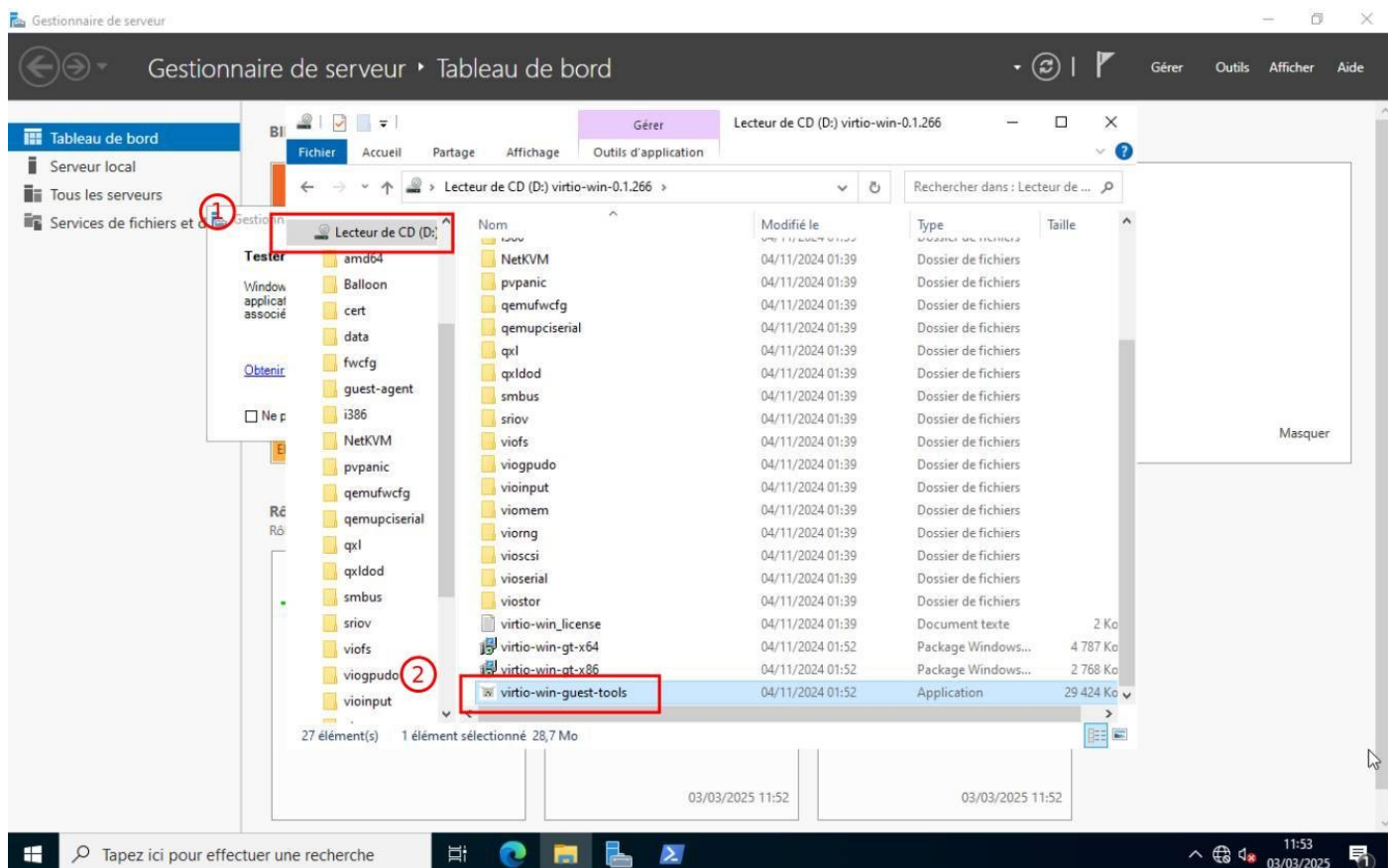
Nom d'utilisateur

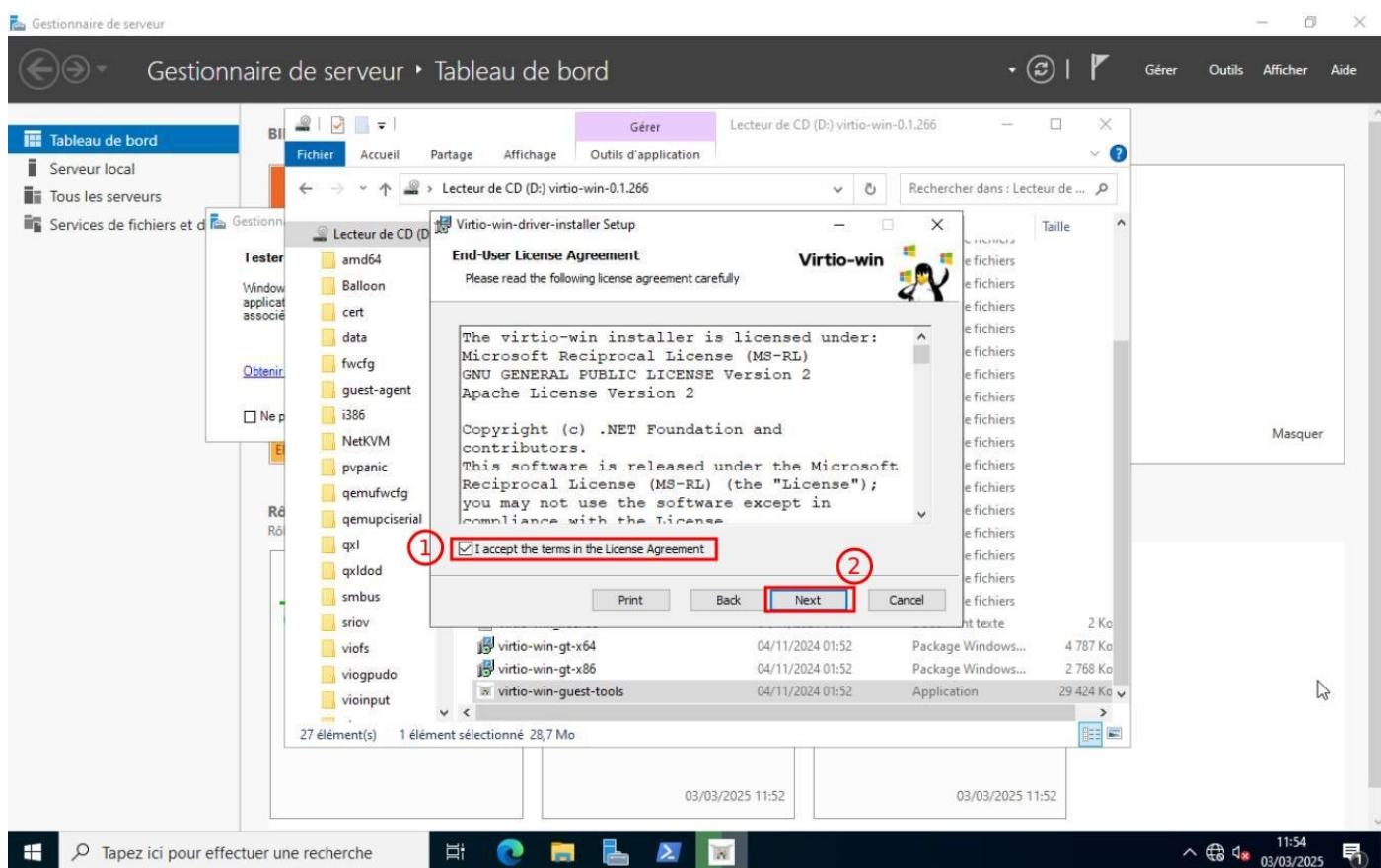
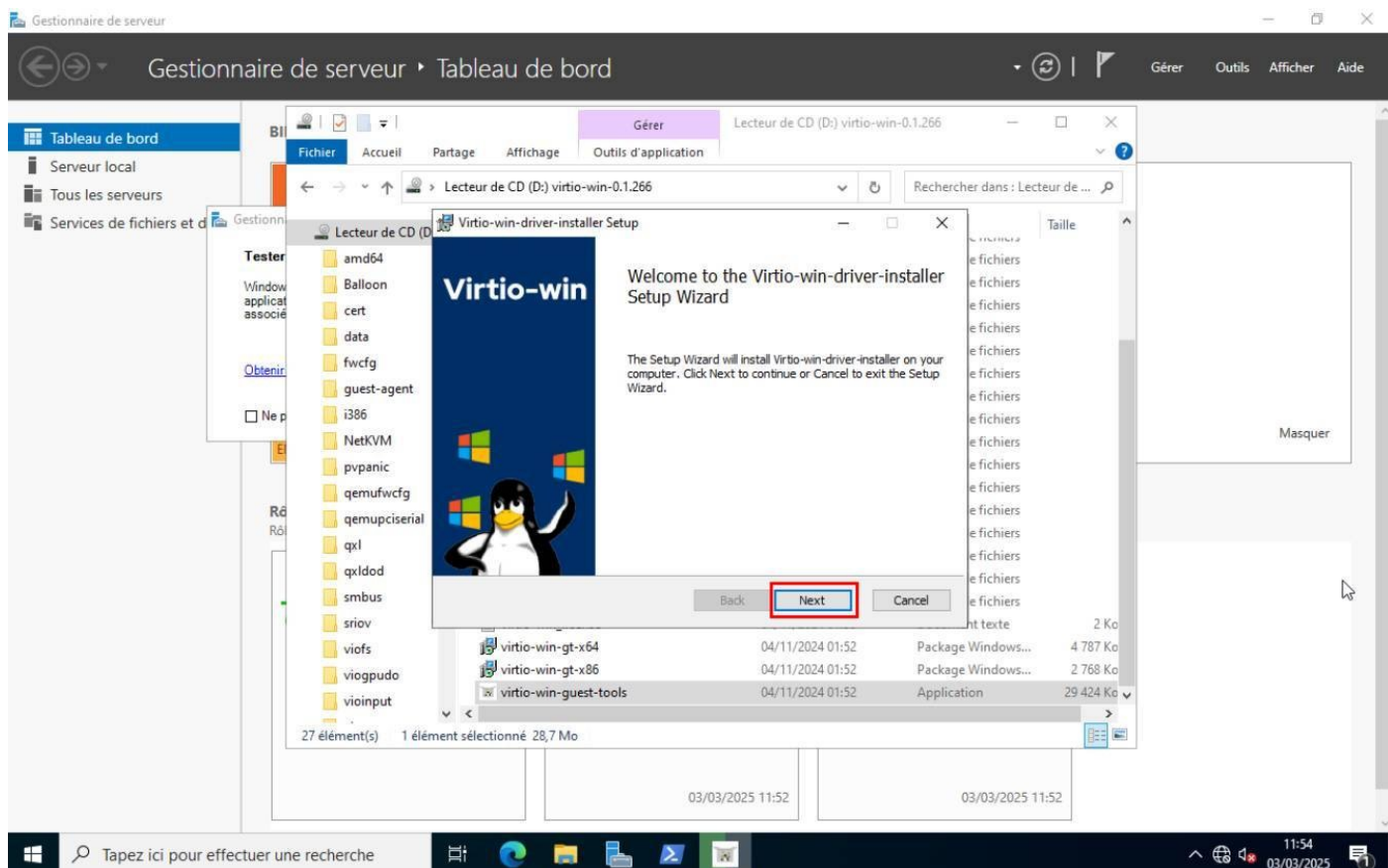
Administrateur

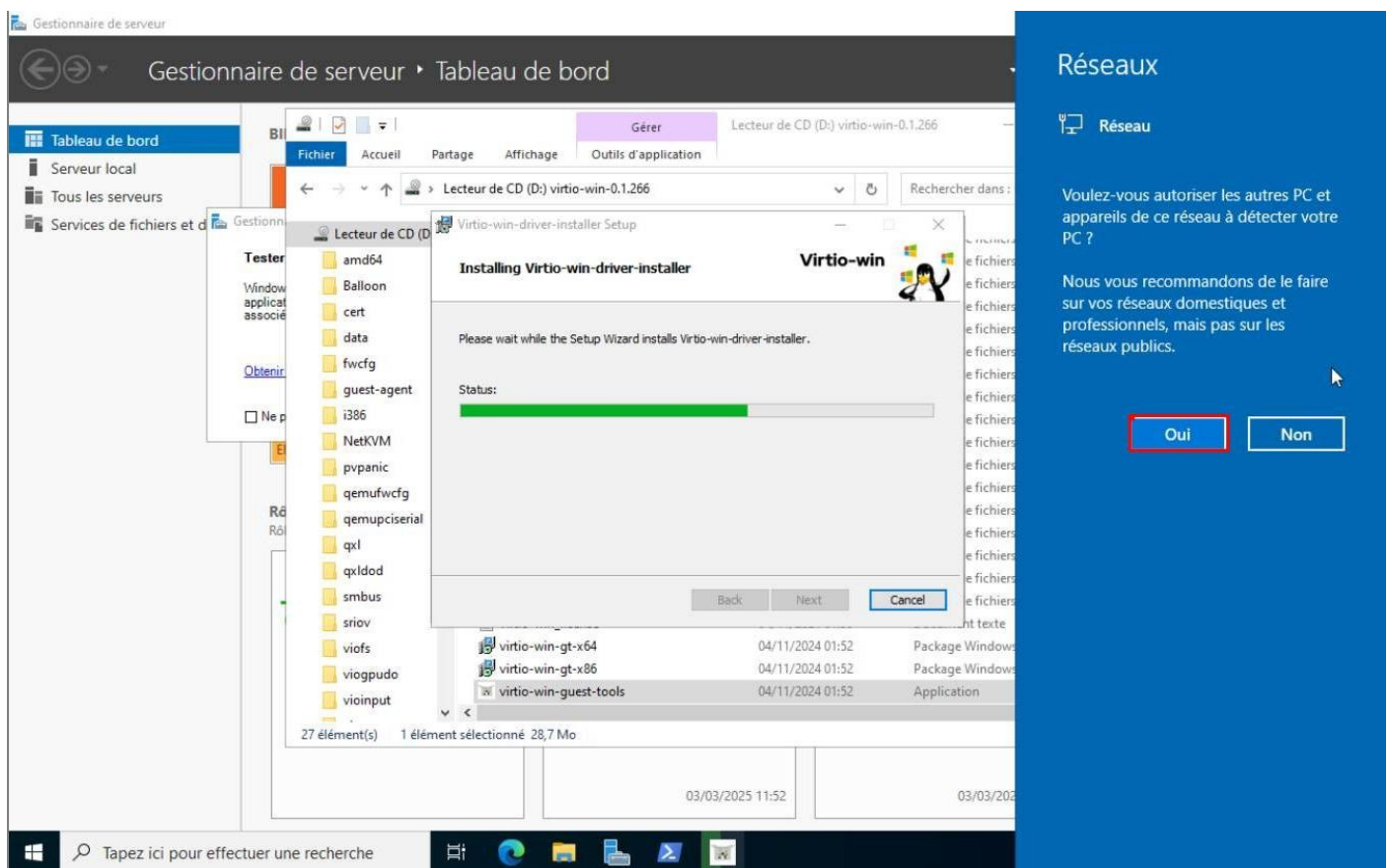
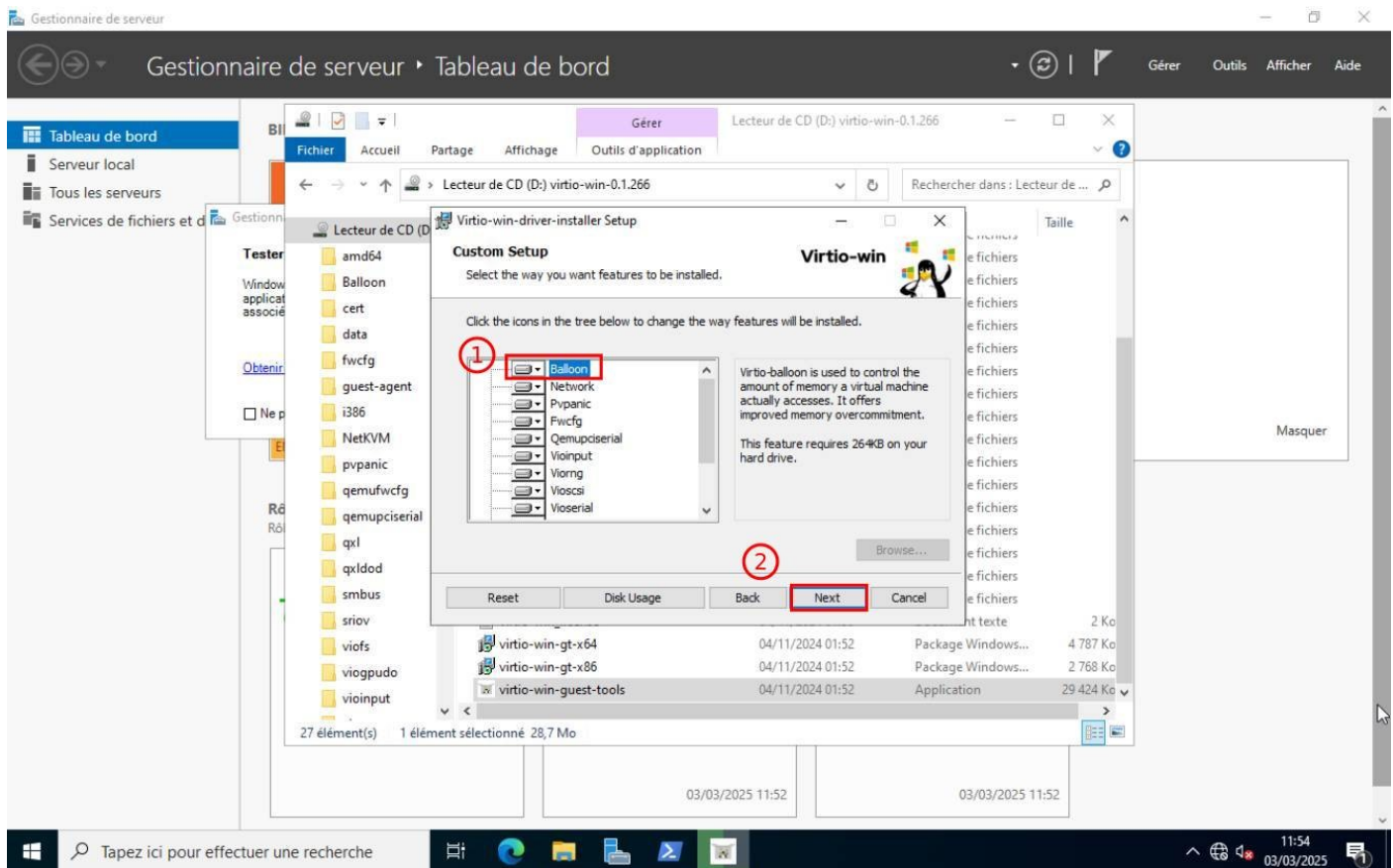
Mot de passe

Entrez de nouveau le
mot de passe

Terminer







Réseaux

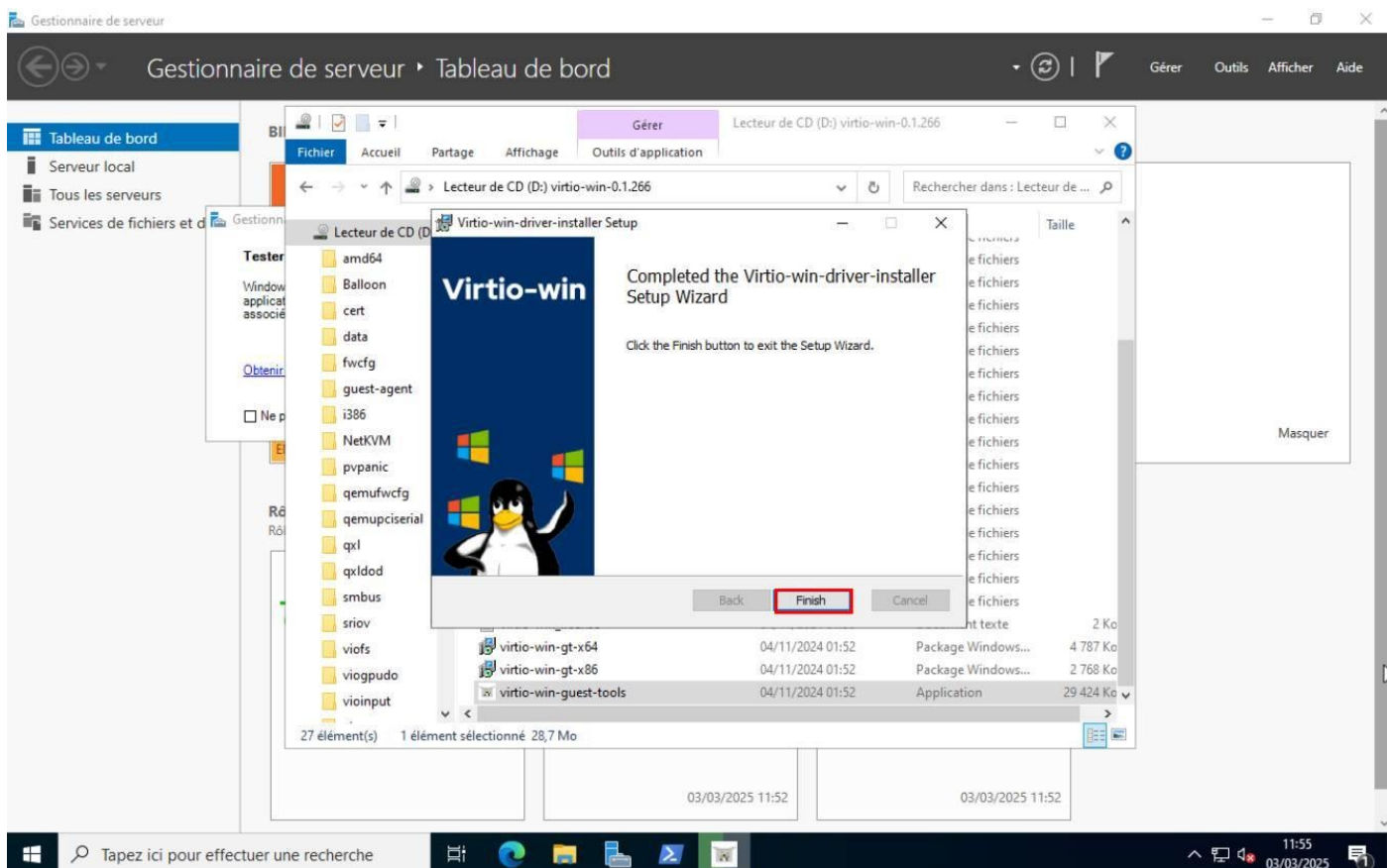
Réseau

Voulez-vous autoriser les autres PC et appareils de ce réseau à détecter votre PC ?

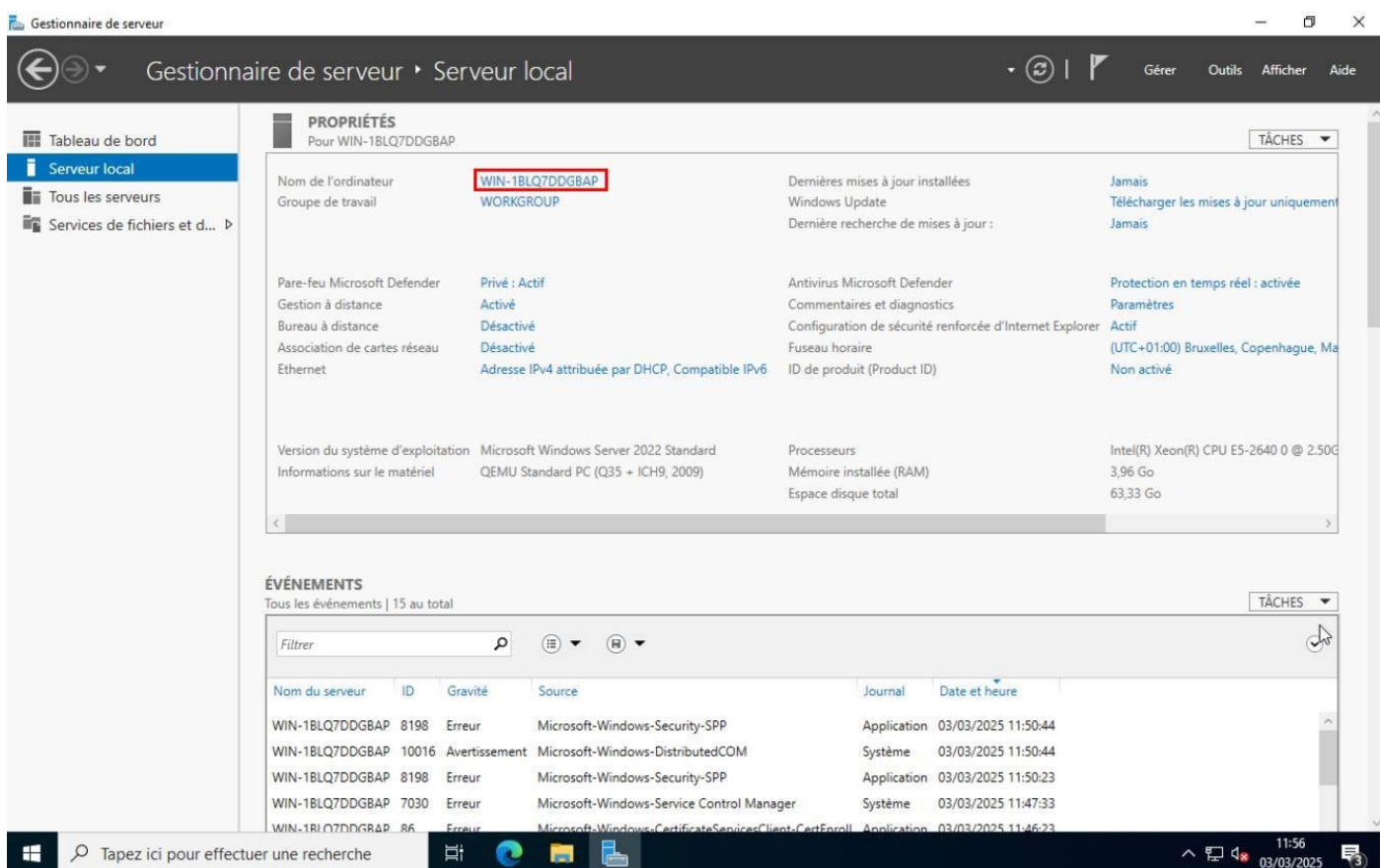
Nous vous recommandons de le faire sur vos réseaux domestiques et professionnels, mais pas sur les réseaux publics.

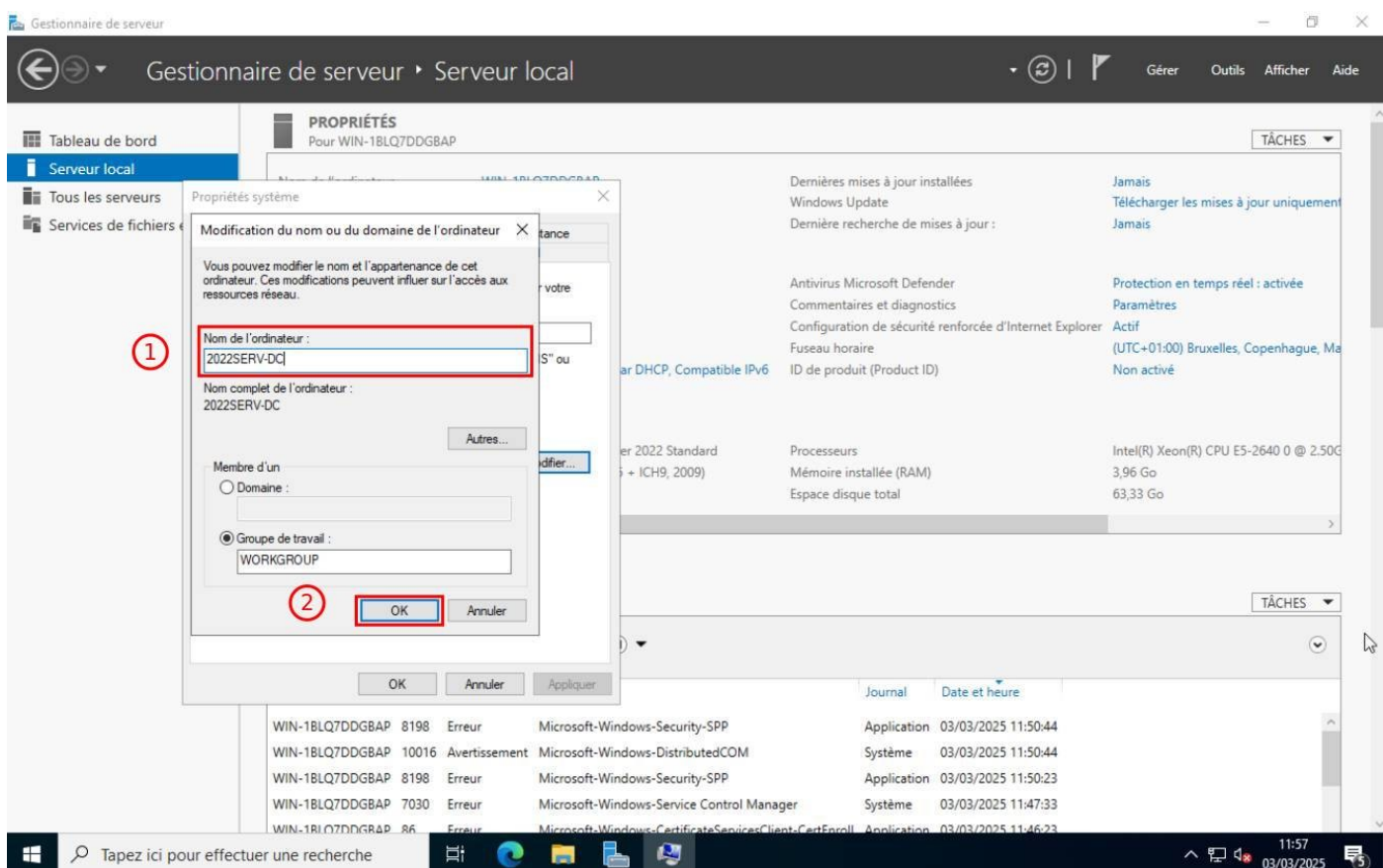
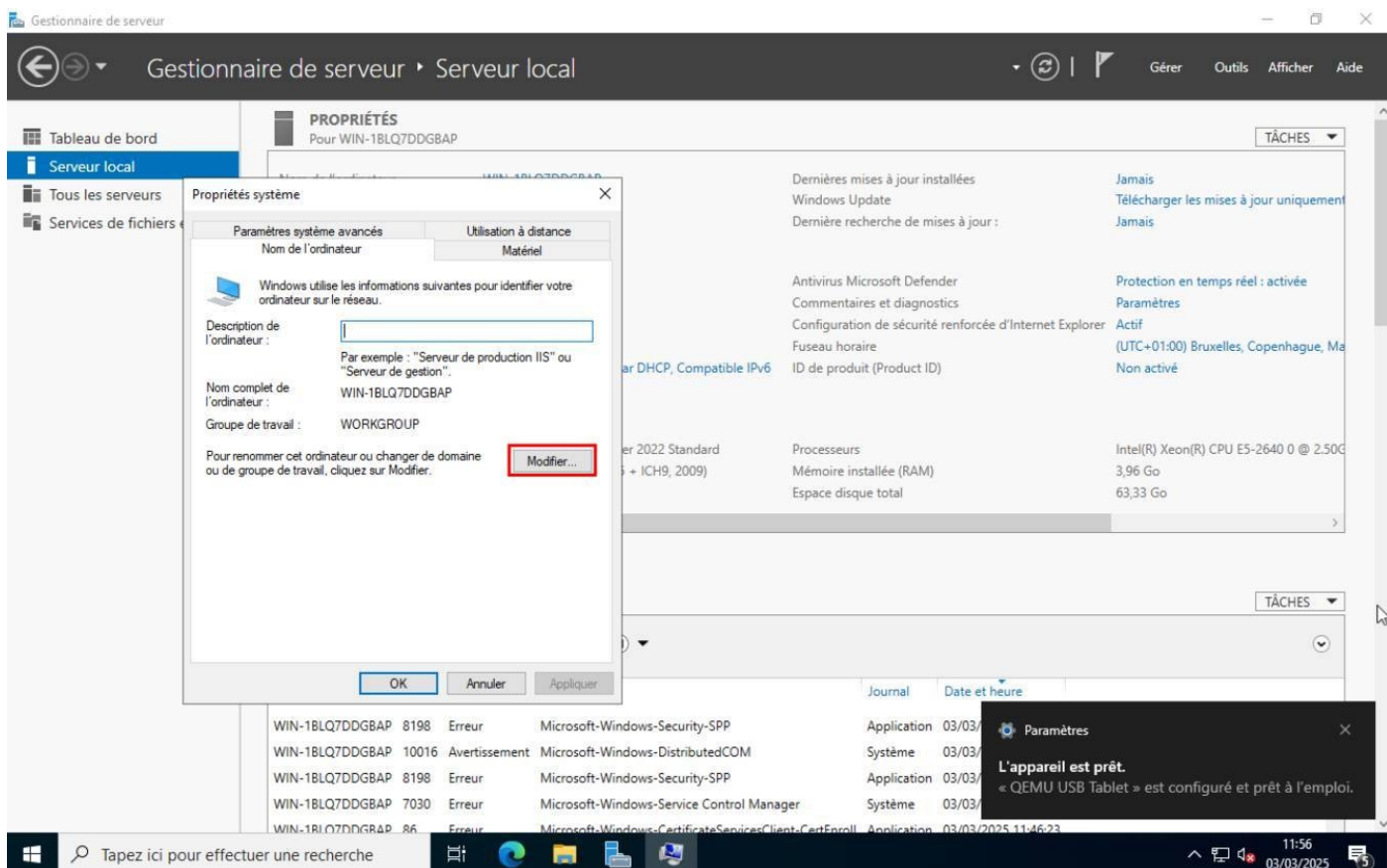
Oui

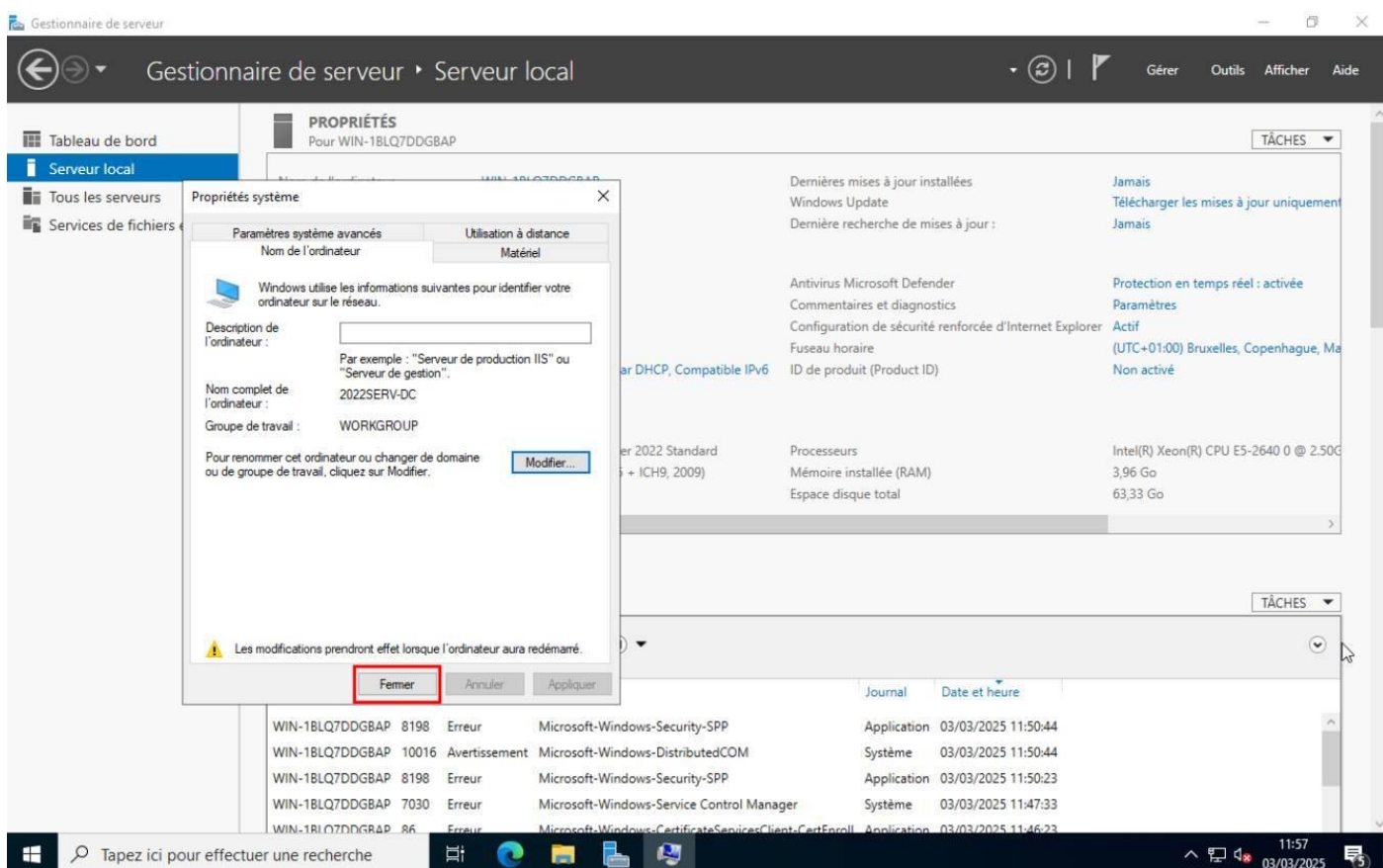
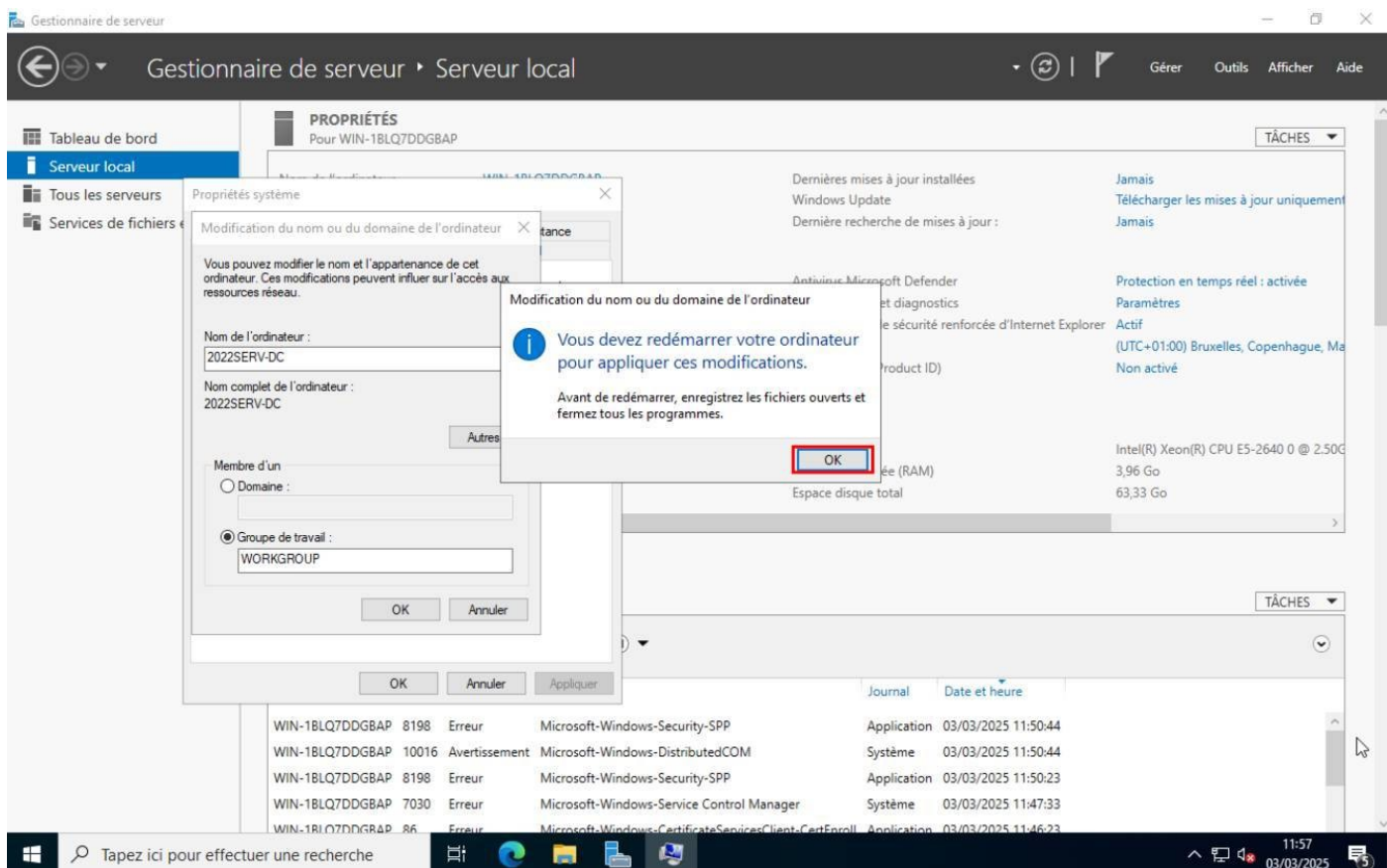
Non



Sélectionnez le nom de l'ordinateur pour le modifier.







Gestionnaire de serveur

Gestionnaire de serveur ▸ Serveur local

Tableau de bord

Serveur local

Tous les serveurs

Services de fichiers et d...

PROPRIÉTÉS
Pour WIN-1BLQ7DDGBAP

Nom de l'ordinateur: WIN-1BLQ7DDGBAP
Groupe de travail: WORKGROUP

Dernières mises à jour installées: Jamais
Windows Update: Télécharger les mises à jour uniquement
Dernière recherche de mises à jour: Jamais

Pare-feu Microsoft Defender: **Activé**
Gestion à distance: Paramètres
Bureau à distance: Actif
Association de cartes réseau: (UTC+01:00) Bruxelles, Copenhague, Ma
Ethernet: Non activé

Version du système d'exploitation: Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50G
Informations sur le matériel: 3,96 Go
Espace disque total: 63,33 Go

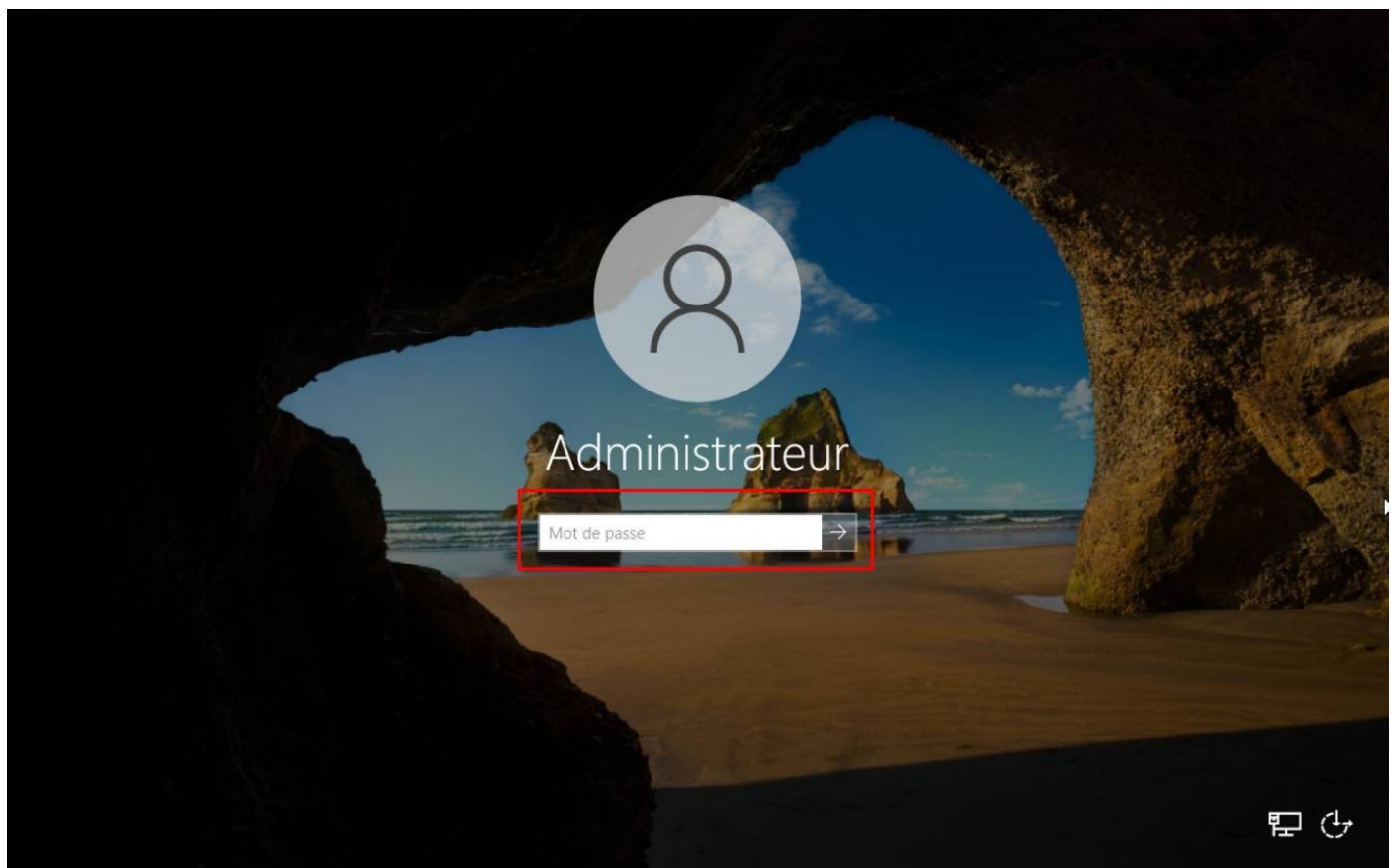
ÉVÉNEMENTS
Tous les événements | 15 au total

Filter

Nom du serveur	ID	Gravité	Source	Journal	Date et heure
WIN-1BLQ7DDGBAP	8198	Erreur	Microsoft-Windows-Security-SPP	Application	03/03/2025 11:50:44
WIN-1BLQ7DDGBAP	10016	Avertissement	Microsoft-Windows-DistributedCOM	Système	03/03/2025 11:50:44
WIN-1BLQ7DDGBAP	8198	Erreur	Microsoft-Windows-Security-SPP	Application	03/03/2025 11:50:23
WIN-1BLQ7DDGBAP	7030	Erreur	Microsoft-Windows-Service Control Manager	Système	03/03/2025 11:47:33
WIN-1BLQ7DDGBAP	86	Erreur	Microsoft-Windows-CertificateServicesClient-CertEnroll	Application	03/03/2025 11:46:23

Tapez ici pour effectuer une recherche

11:57
03/03/2025



Windows Server Site B

Installation de Windows Server 2022 sur DC2 en mode CORE

Introduction

Ce premier document couvre la procédure d'installation de Windows Server 2022 dans un environnement Proxmox.

1. Préparation d'une VM
2. Installation de Windows
3. Installation des pilotes

Pour ce faire, vous aurez besoin des éléments suivants :

- Image ISO de Windows Server 2022
- Les ressources suivantes disponibles sur votre Hyperviseur
 - processeur 2v
 - 3 Go de RAM
 - 64 Go de stockage
- Une copie des pilotes VirtIO

Pour mener à bien cette procédure, vous devez disposer des accès nécessaires pour créer des Machines Virtuelles dans Proxmox.

1) Préparation d'une VM

Cliquez sur l'option créer une VM dans l'interface d'administration Proxmox.



Sélectionnez ensuite un nom, le pool de ressources approprié pour votre machine, et cliquez sur suivant.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: pve Resource Pool:

VM ID: 113

Name: 1

Start at boot: ☐

Start/Shutdown order: any

Startup delay: default

Shutdown timeout: default

Tags

No Tags +

Help Advanced ☒ Back Next 3

Sur la deuxième page, sélectionnez d'abord votre stockage ISO Proxmox, puis sélectionnez votre ISO de Windows Server déjà préchargée sur votre Hyperviseur. Sélectionnez ensuite les options appropriées dans les paramètres de l'OS Client. Puis, ajoutez l'ISO des drivers en cliquant sur la case à cocher et en sélectionnant l'ISO dans votre bibliothèque.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

☒ Use CD/DVD disc image file (iso) Guest OS:

1 Storage: ZFS-data 4 Type: Microsoft Windows

2 ISO image: x64_dvd_4e34897c.iso 5 Version: 11/2022/2025

☐ Use physical CD/DVD Drive 6 ☒ Add additional drive for VirtIO drivers

☐ Do not use any media 7 Storage: ZFS-data

8 ISO image: virtio-win-0.1.266.iso

Advanced ☒ Back Next 3

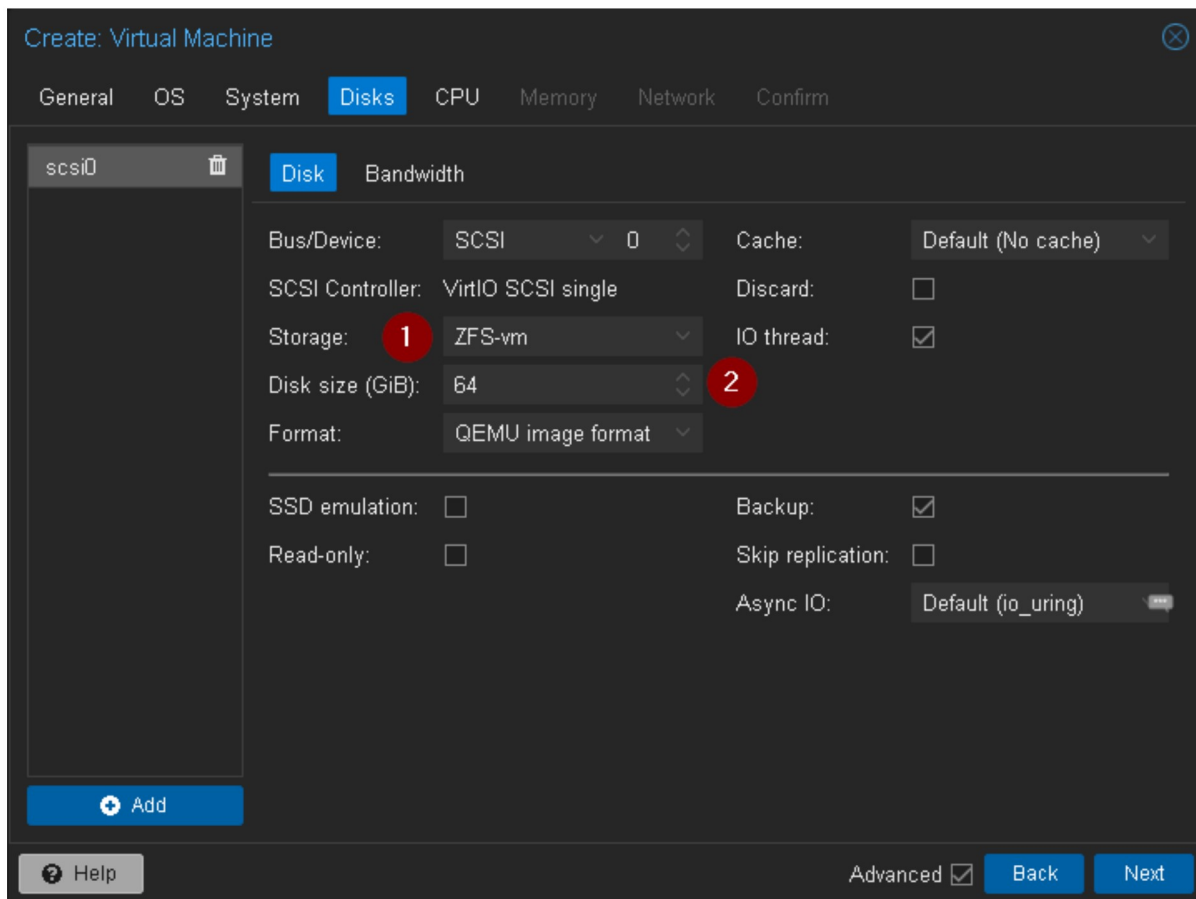
Ajoutez ensuite un espace de Stockage pour la partition EFI et la puce TPM qui sera nécessaire pour l'activation de BitLocker sur vos serveurs. En général, l'espace de stockage est le même que celui utilisé pour stocker l'image disque principale.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'System' tab selected. The 'EFI Storage' dropdown is highlighted with a red circle and the number '1'. The 'TPM Storage' dropdown is highlighted with a red circle and the number '2'. The 'Add TPM' checkbox is checked. The 'Version' dropdown is set to 'v2.0'. The 'Format' dropdown is set to 'QEMU image format (qcow2)'. The 'Pre-Enroll keys' checkbox is checked. The 'Advanced' checkbox is checked. The 'Back' and 'Next' buttons are visible at the bottom right.

Field	Value
Graphic card:	Default
Machine:	q35
SCSI Controller:	VirtIO SCSI single
Qemu Agent:	<input type="checkbox"/>
BIOS:	OVMF (UEFI)
Add TPM:	<input checked="" type="checkbox"/>
EFI Storage:	[Dropdown menu highlighted with red circle 1]
TPM Storage:	[Dropdown menu highlighted with red circle 2]
Version:	v2.0
Format:	QEMU image format (qcow2)
Pre-Enroll keys:	<input checked="" type="checkbox"/>

Help Advanced ☒ Back Next

Dans la page de sélection du disque virtuel principal, choisissez l'emplacement de stockage de l'image disque et augmentez la taille du disque à votre convenance. Cliquez sur "Add" pour ajouter des disques secondaires.



Dans la page CPU, ajoutez un Socket à votre machine virtuelle et sélectionnez le Type "x86-64-v2-AES" s'il n'est pas sélectionné par défaut.

Si votre hyperviseur dispose de deux CPU physiques, vous pouvez activer l'option NUMA.

Create: Virtual Machine

GeneralOSSystemDisksCPUMemoryNetworkConfirm

Sockets: 1 2

Type: 2 x86-64-v2-AES

Cores: 1

Total cores: 2

VCPUs: 2

CPU units: 100

CPU limit: unlimited

Enable NUMA: ☒ 3

CPU Affinity: All Cores

Extra CPU Flags:

Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	md-clear	Required to let the guest OS know if MDS is mitigated correctly
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	pcid	Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	spec-ctrl	Allows improved Spectre mitigation with Intel CPUs
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	ssbd	Protection for "Speculative Store Bypass" for Intel models
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	ibpb	Allows improved Spectre mitigation with AMD CPUs
Default	- <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> +	virt-ssbd	Basis for "Speculative Store Bypass" protection for AMD models

Help

Advanced ☒

Back

Next

Dans la page Mémoire, sélectionnez un montant de RAM entre 3 et 4 go minimum. En fonction de votre utilisation, il faudra allouer de la mémoire en plus. Sélectionnez ensuite la même quantité de mémoire minimale ou désactivez l'option de Ballooning.

Create: Virtual Machine

General OS System Disks CPU **Memory** Network Confirm

Memory (MiB): 4096 1

Minimum memory (MiB): 4096 2

Shares: Default (1000)

Ballooning Device: ☒ 3

Help Advanced ☒ Back Next

Configurez ensuite la carte réseau selon votre infrastructure. Sélectionnez la carte réseau VirtIO dans la rubrique "Modèle"

Create: Virtual Machine

General OS System Disks CPU Memory **Network** Confirm

☐ No network device

Bridge: 1 vmbri0 Model: 2 VirtIO (paravirtualized)

VLAN Tag: no VLAN MAC address: auto

Firewall: ☒

Disconnect: ☐ Rate limit (MB/s): unlimited

MTU: 1500 (1 = bridge MTU) Multiqueue:

Help Advanced ☒ Back Next

Vérifiez votre configuration et cliquez sur le bouton FINISH.

Create: Virtual Machine

General

OS

System

Disks

CPU

Memory

Network

Confirm

Key ↑	Value
cores	1
cpu	x86-64-v2-AES
ide2	ZFS-data:iso/fr-fr_windows_server_2022_updated_nov_2024_x64_dvd_4e34897c.iso,med...
memory	2048
net0	virtio,bridge=vmbr0,firewall=1
nodename	pve
numa	0
ostype	l26
scsi0	ZFS-retro:32,ioread=on
scsihw	virtio-scsi-single
sockets	1
vmid	113

☐ Start after created

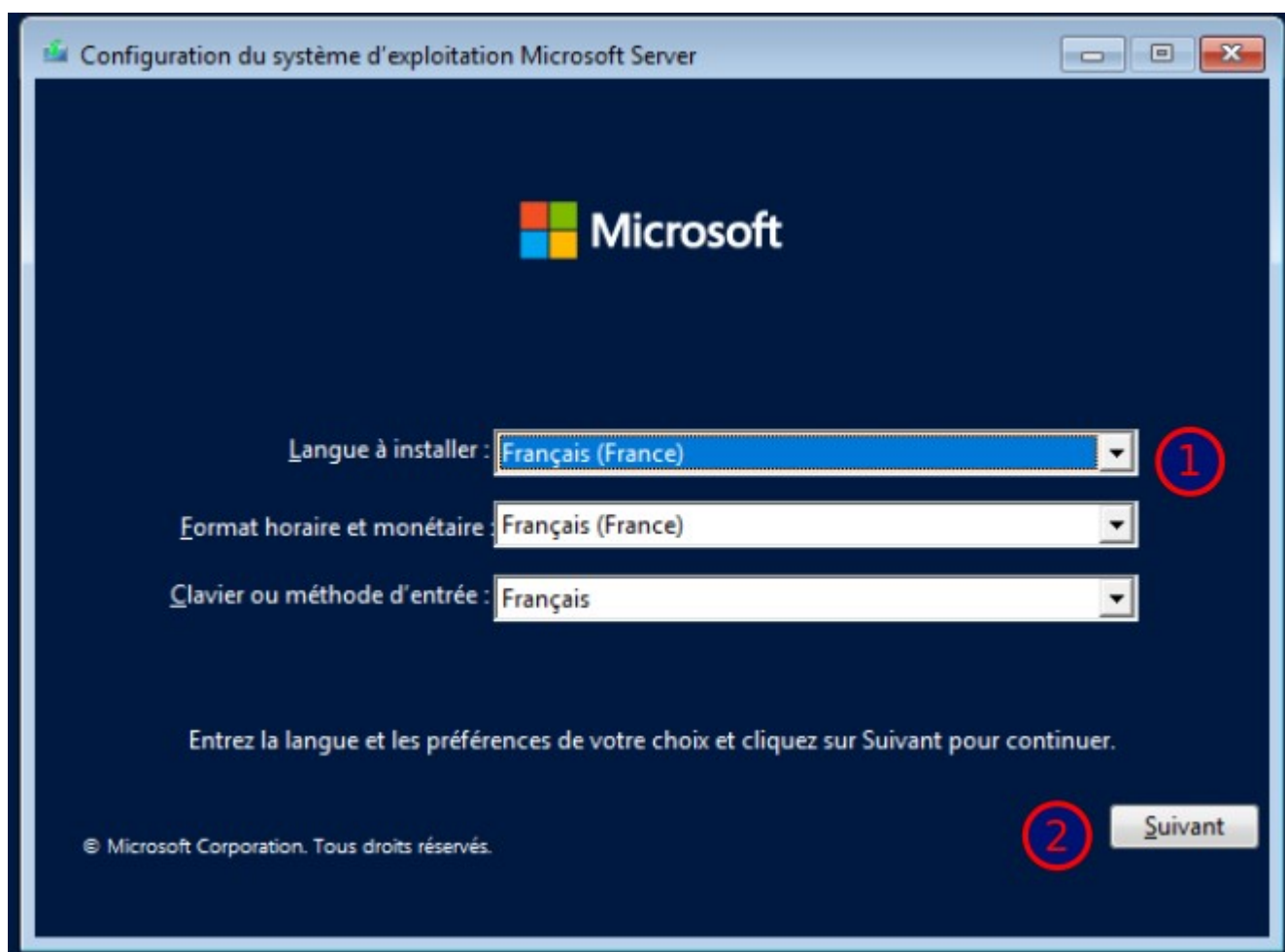
Advanced ☒

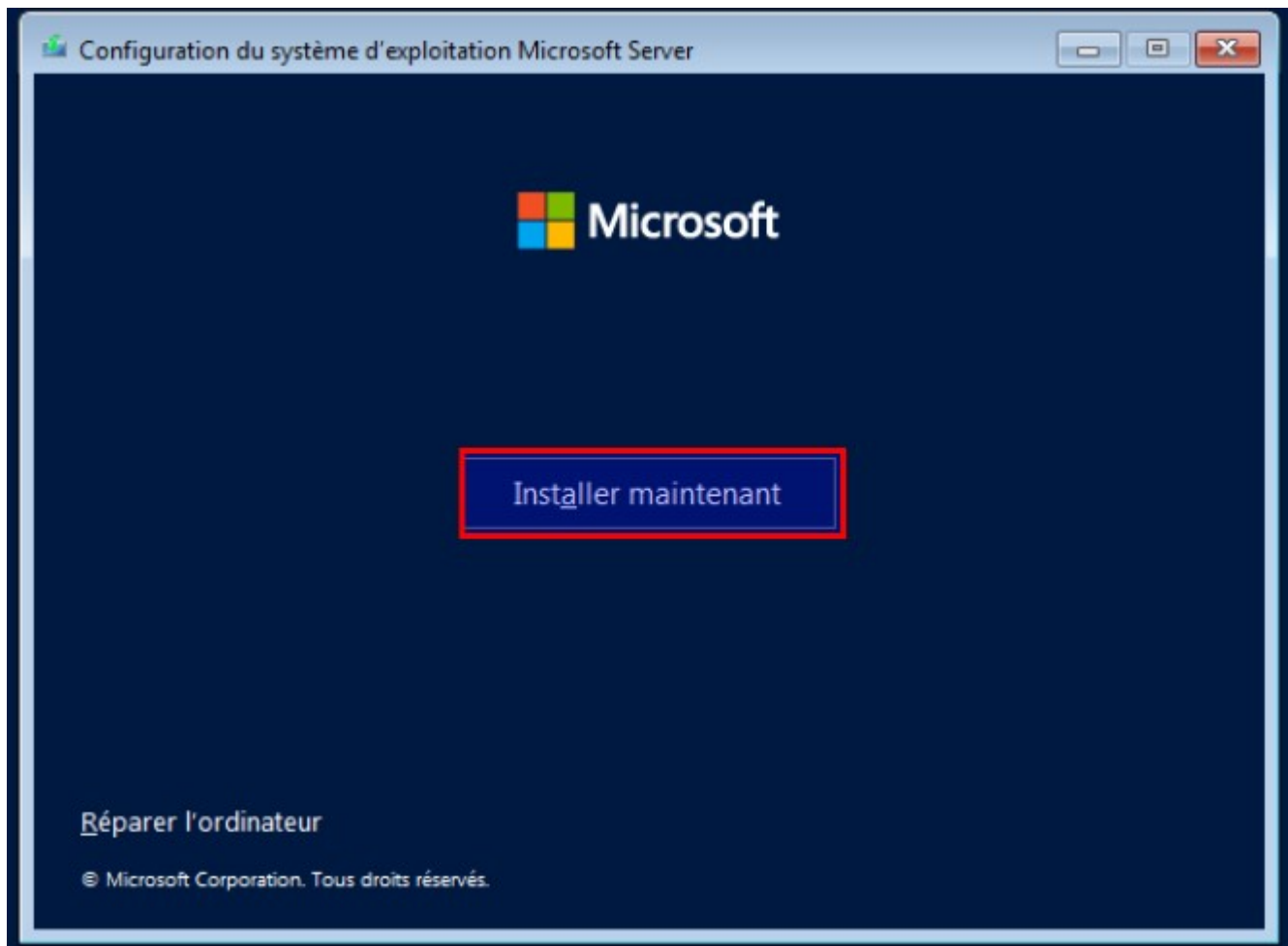
Back

Finish

2) Installation de Windows Server 2022

Une fois la VM lancée sur l'ISO de Windows Server, sélectionnez la langue (Français) et cliquez sur suivant.





Sélectionnez bien "Je n'ai pas de clé de produit"

Activer la configuration du système d'exploitation Microsoft Server

Si vous installez le système d'exploitation Microsoft Server pour la première fois sur cet ordinateur (ou si vous installez une autre édition), vous devez entrer une clé de produit valide pour le système d'exploitation Microsoft Server. Votre clé de produit doit figurer dans le courrier de confirmation que vous avez reçu après l'achat d'une copie numérique du système d'exploitation Microsoft Server ou sur une étiquette fournie dans la zone du système d'exploitation Microsoft Server.

La clé de produit (Product Key) ressemble à ceci : XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Si vous réinstallez le système d'exploitation Microsoft Server, sélectionnez je ne dispose pas d'une clé de produit. Votre copie du système d'exploitation Microsoft Server sera automatiquement

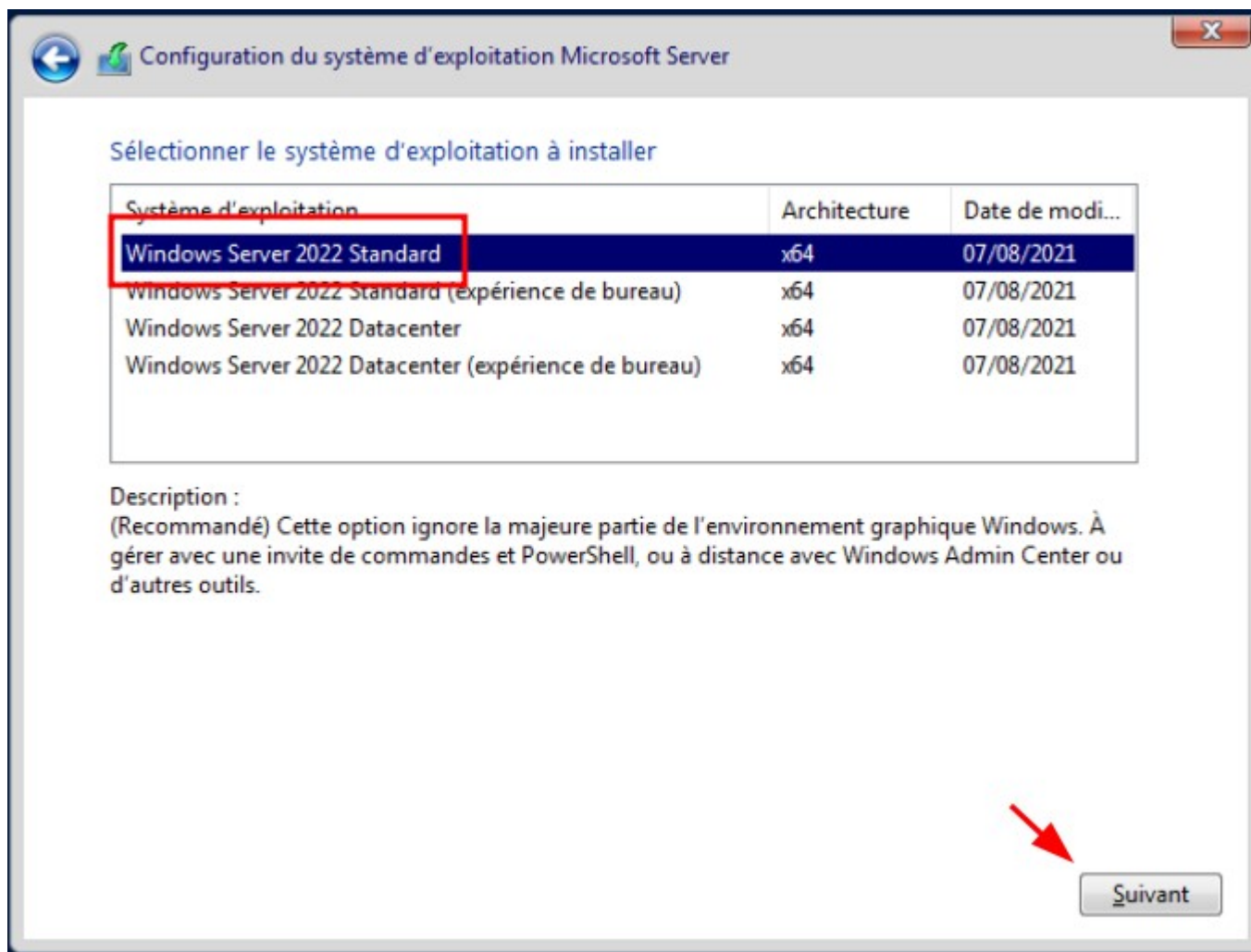
 

[Déclaration de confidentialité](#)

[Je n'ai pas de clé de produit \(Product Key\)](#)

[Suivant](#)

Sélectionnez « Windows Server 2022 Standard » et continuez



Avis et conditions du contrat de licence applicables

VOUS DEVEZ ACCEPTER LES TERMES DE LA LICENCE DU LOGICIEL. VOIR CI-APRÈS. Veuillez lire les conditions de licence complètes fournies à l'adresse (aka.ms/useterms).

NOTIFICATION IMPORTANTE

Informations relatives à l'utilisation et au diagnostic. Microsoft recueille ces informations sur Internet pour assurer la sécurité et la mise à jour de Windows, diagnostiquer les problèmes et apporter des améliorations aux produits, et peut associer ces informations à votre organisation. Les systèmes d'exploitation des serveurs Microsoft peuvent être configurés pour désactiver les données de diagnostic, envoyer des données de diagnostic obligatoires ou envoyer des données de diagnostic facultatives. Le réglage par défaut consiste à envoyer les données de diagnostic requises. Les données de diagnostic requises

1



J'accepte les termes du contrat de licence logiciel Microsoft. Si la licence appartient à une organisation, je suis autorisé à agir en son nom.

2

Suivant

Choisissez l'option personnalisée.

Quel type d'installation voulez-vous effectuer ?

Mise à jour : Installer le système d'exploitation Microsoft Server et conserver les fichiers, les paramètres et les applications.

Avec cette option, les fichiers, paramètres et applications sont déplacés vers le nouveau système d'exploitation. Cette option est disponible uniquement lorsqu'une version prise en charge du système d'exploitation est déjà en cours d'exécution sur l'ordinateur.

Personnalisé : installer uniquement le système d'exploitation Microsoft Server (avancé)

Avec cette option, les fichiers, les paramètres et les applications ne sont pas déplacés vers le nouveau système d'exploitation. Pour modifier les partitions et les lecteurs, démarrez l'ordinateur à l'aide du disque d'installation. Nous vous recommandons de sauvegarder vos fichiers avant de continuer.

Où voulez-vous installer le système d'exploitation ?

Nom	Taille totale	Espace libre	Type

 Actualiser Supprimer Formater Nouveau

1

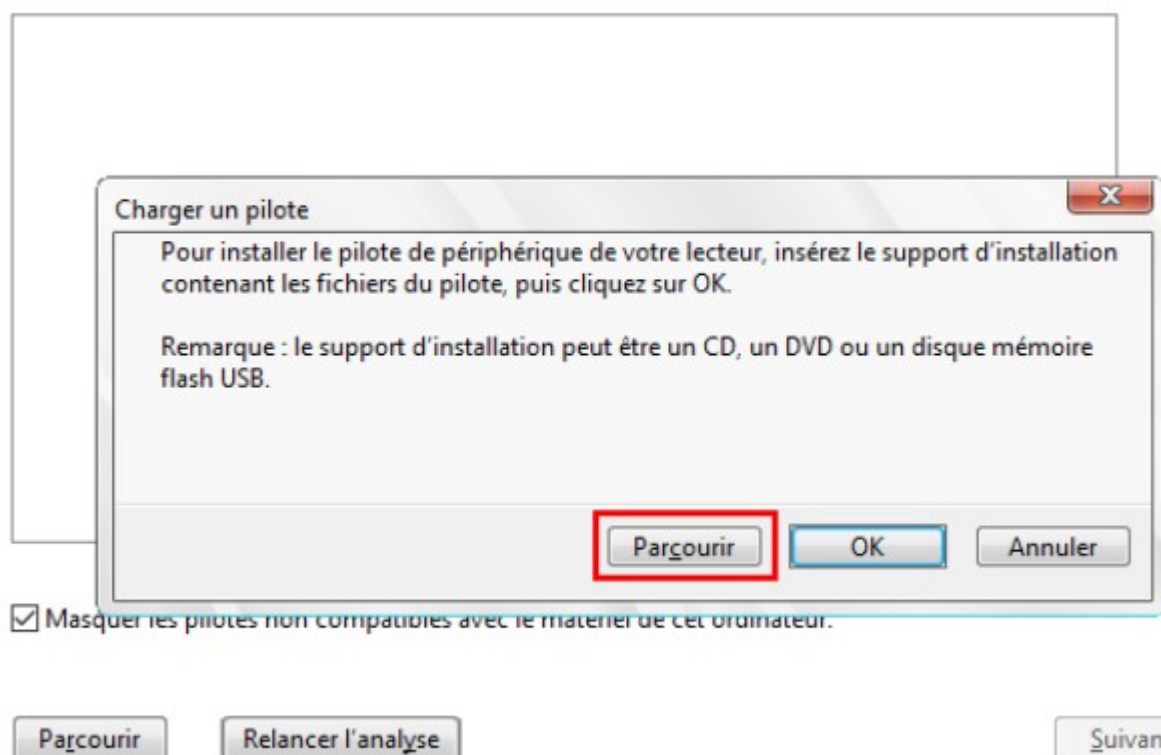
 Charger un pilote Étendre

Nous n'avons trouvé aucun lecteur. Pour obtenir un pilote de stockage, cliquez sur Charger un pilote.

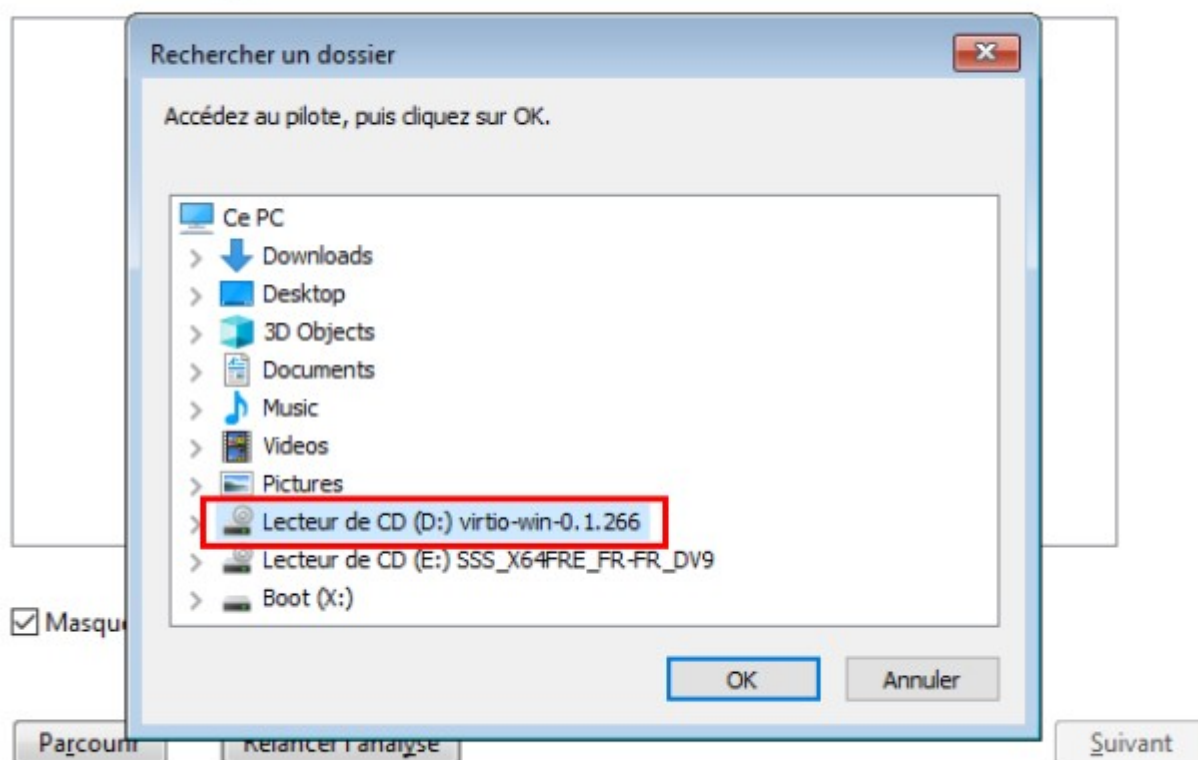
2

Suivant

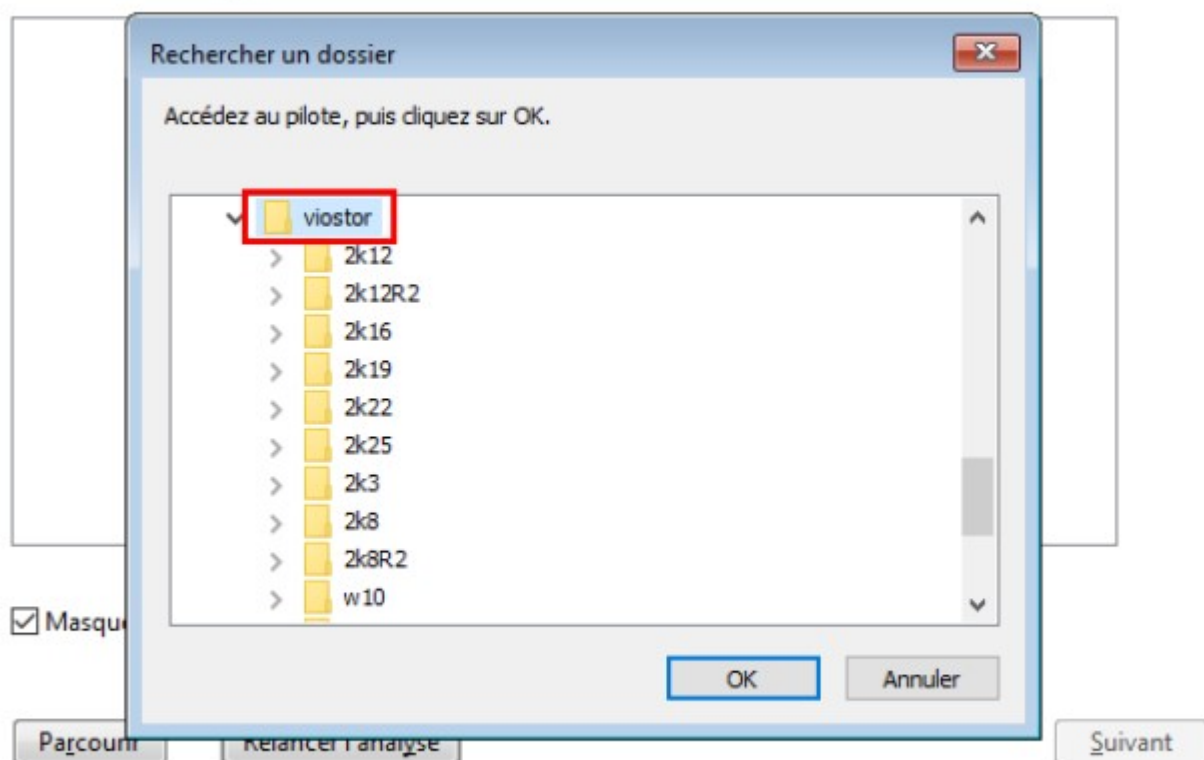
Sélectionner le pilote à installer



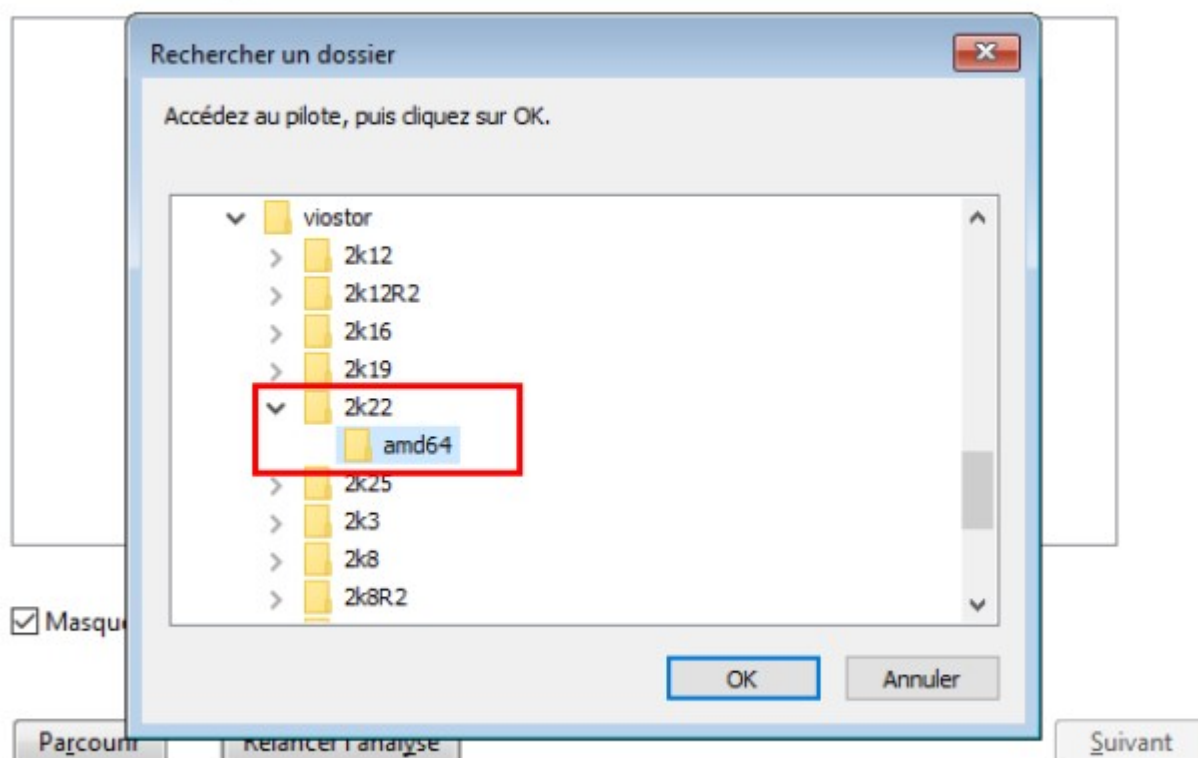
Sélectionner le pilote à installer



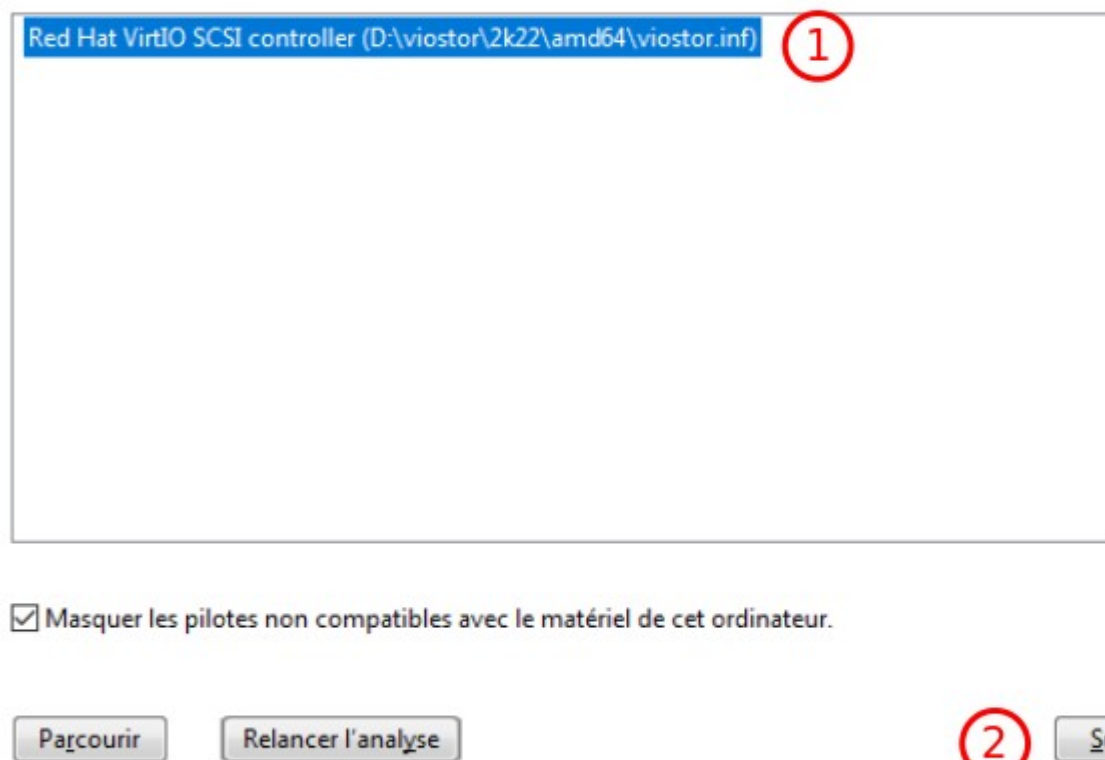
Sélectionner le pilote à installer




Sélectionner le pilote à installer



Sélectionner le pilote à installer



Où voulez-vous installer le système d'exploitation ?

	Nom	Taille totale	Espace libre	Type
	Lecteur 0 Espace non alloué	64.0 Go	64.0 Go	

 Actualiser

 Supprimer

 Formater

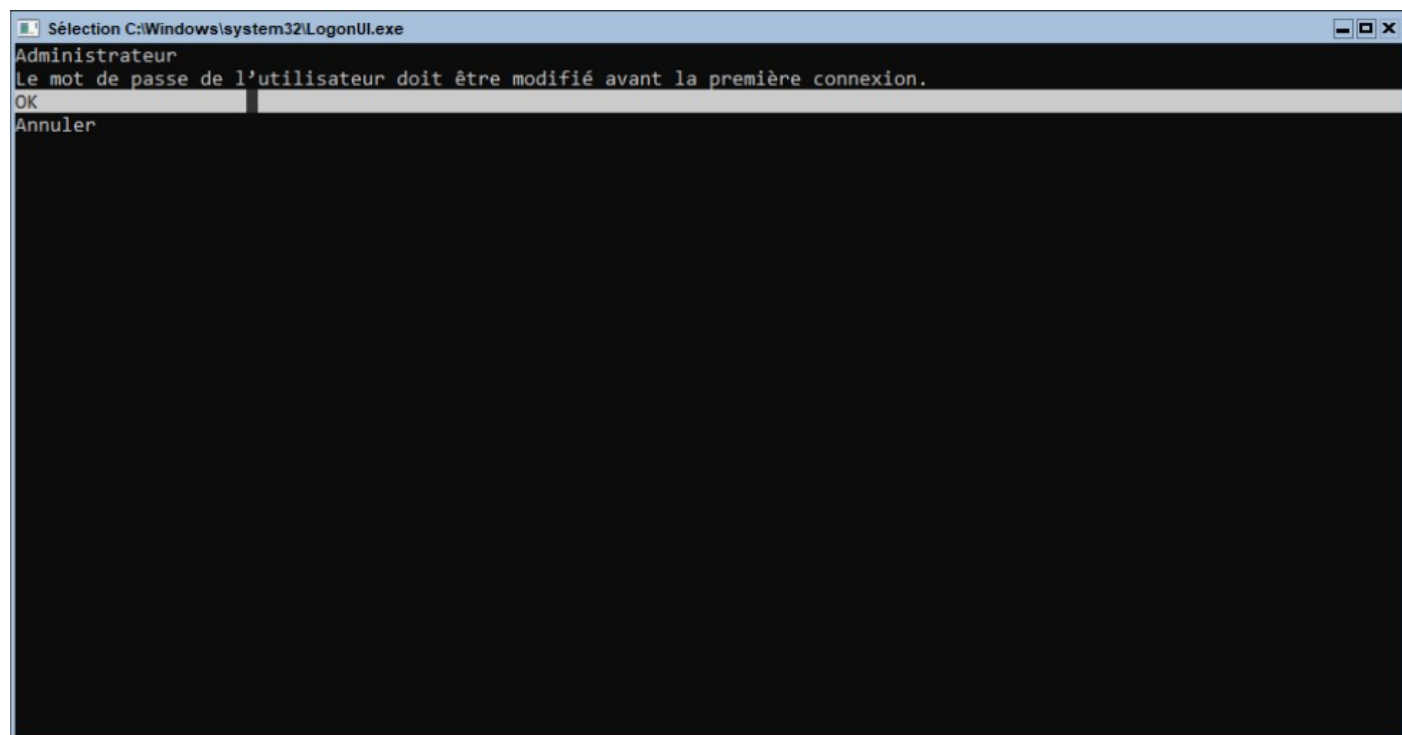
 Nouveau

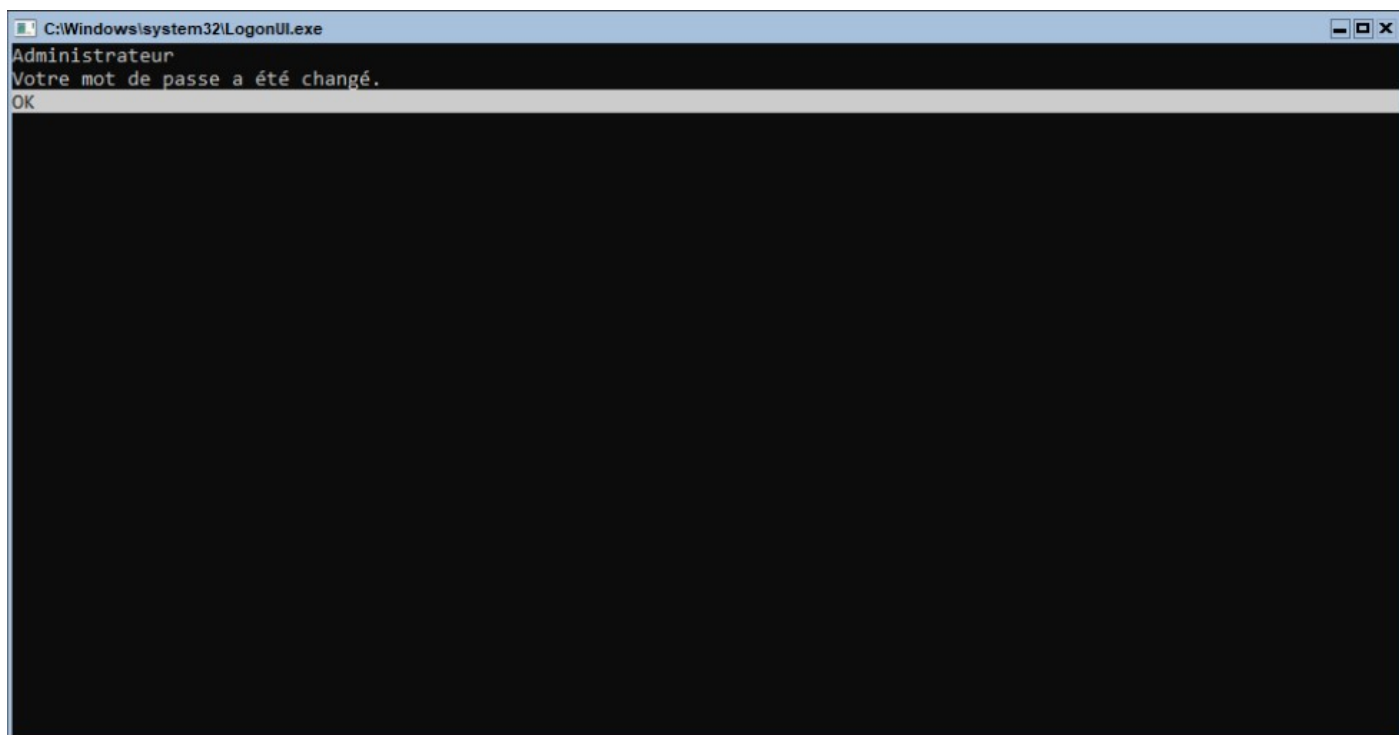
 Charger un pilote

 Étendre

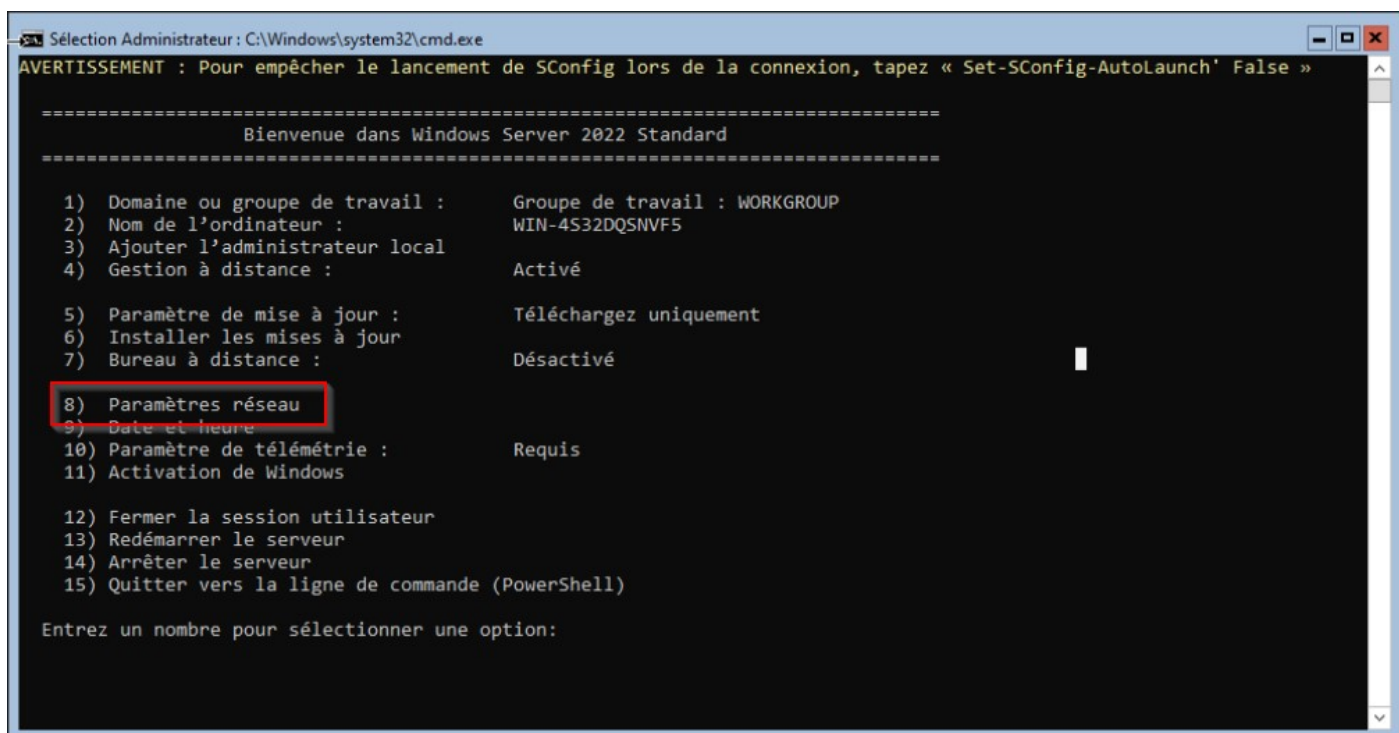
Suivant

Une fois l'installation terminée, le serveur va redemarrer. Vous allez devoir changer le MDP





Vous allez ensuite voir apparaître le menu "SConfig". Une fois le menu visible, utilisez l'option 8 pour configurer le réseau



Entrez ensuite le numéro d'index de votre carte


```
Administrateur : C:\Windows\system32\cmd.exe

=====
Paramètres réseau
=====

Cartes réseau disponibles :

Index numéro | Adresse IP      | Description
1            | 192.168.200.10 | Intel(R) PRO/1000 MT Network Connection

Sélectionnez le numéro d'index de la carte réseau (Vide = annuler):
```

Vous devrez configurer les options 1 et 2, commencez par l'option 1

```
Administrateur : C:\Windows\system32\cmd.exe

=====
Paramètres de carte réseau
=====

Index NIC :          1
Description :         Intel(R) PRO/1000 MT Network Connection
Adresse IP :          192.168.200.10,
                     fe80::e4de:244:1cce:ff28
Masque de sous-réseau : 255.255.255.0
DHCP activé :         True

Passerelle par défaut : 192.168.200.1 fe80::be24:11ff:fe2b:44cd
Serveur DNS préféré :  192.168.200.200
Serveur DNS auxiliaire : 192.168.200.201

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS

Entrez la sélection (Vide = annuler):
```

entrez les paramètres désirés

```

Administrateur : C:\Windows\system32\cmd.exe

=====
Paramètres de carte réseau
=====

Index NIC :          1
Description :        Intel(R) PRO/1000 MT Network Connection
Adresse IP :         192.168.200.10,
                   fe80::e4de:244:1cce:ff28
Masque de sous-réseau : 255.255.255.0
DHCP activé :        True

Passerelle par défaut : 192.168.200.1 fe80::be24:11ff:fe2b:44cd
Serveur DNS préféré :  192.168.200.200
Serveur DNS auxiliaire : 192.168.200.201

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS

Entrez la sélection (Vide = annuler): 1
Sélectionnez le protocole (D)HCP ou l'adresse IP (S)tatique (Vide = annuler): S
Entrez une adresse IP statique : (Vide = annuler): 192.168.200.201
Entrez un masque de sous-réseau (Vide=255.255.255.0):
Entrez la passerelle par défaut (Vide = annuler): 192.168.200.1
Affectation en cours de l'adresse IP statique à la carte réseau... Merci de patienter.
Le bail DHCP a été libéré avec succès.
L'adressage statique a été correctement activé. DHCP n'est pas activé pour cette carte réseau.
La passerelle a été correctement définie.
Définition de l'adresse de la carte réseau effectuée avec succès.
(Appuyez sur ENTRÉE pour continuer):

```

Pour les DNS, vous devez quitter le menu principal avec l'option 15, puis utilisez les commandes suivantes :

```

Set-DnsClientServerAddress -InterfaceIndex 1 -ServerAddresses
192.168.200.200,192.168.200.201,192.168.100.200,192.168.100.201
Get-DnsClientServerAddress -InterfaceIndex 1

```

Utilisez ensuite la commande "ipconfig /all" pour vérifier la configuration des serveurs DNS.

```

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Red Hat VirtIO Ethernet Adapter
Adresse physique . . . . . : BC-24-11-90-EF-98
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::9d31:4d25:df07:a536%4(préféré)
Adresse IPv4. . . . . : 192.168.100.201(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.100.1
IAID DHCPv6 . . . . . : 112993297
DUID de client DHCPv6. . . . . : 00-01-00-01-30-80-26-57-BC-24-11-90-EF-98
Serveurs DNS. . . . . :
                        192.168.100.200
                        192.168.100.201
                        192.168.200.200
                        192.168.200.201

NetBIOS sur Tcpip. . . . . : Active
PS C:\Users\Administrateur\IEF>

```

tapez ensuite exit dans le terminal pour revenir au menu SConfig, sélectionnez l'option 1 pour rejoindre un domaine

une fois revenu dans le menu SConfig, sélectionnez l'option 1 pour rejoindre un domaine

```
Sélection Administrateur : C:\Windows\system32\cmd.exe
AVERTISSEMENT : Pour empêcher le lancement de SConfig lors de la connexion, tapez « Set-SConfig-AutoLaunch' False »

=====
                    Bienvenue dans Windows Server 2022 Standard
=====

1) Domaine ou groupe de travail :      Groupe de travail : WORKGROUP
2) Nom de l'ordinateur :               WIN-4S32DQSNVF5
3) Ajouter l'administrateur local
4) Gestion à distance :                Activé

5) Paramètre de mise à jour :          Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance :                Désactivé

8) Paramètres réseau
9) Date et heure
10) Paramètre de télémétrie :          Requis
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option:
```

Entrez les informations de votre domaine et validez avec "O"

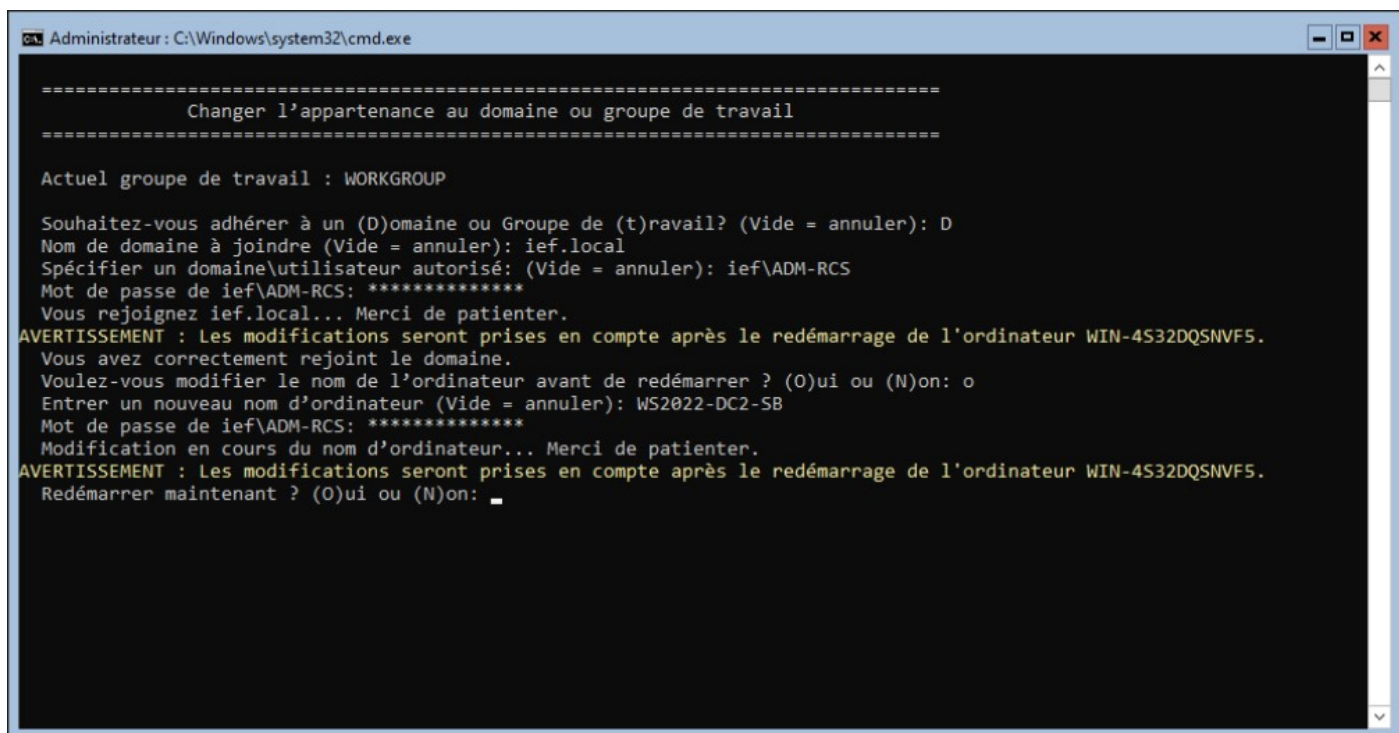
```
Administrateur : C:\Windows\system32\cmd.exe

=====
                    Changer l'appartenance au domaine ou groupe de travail
=====

Actuel groupe de travail : WORKGROUP

Souhaitez-vous adhérer à un (D)omaine ou Groupe de (t)ravail? (Vide = annuler): D
Nom de domaine à joindre (Vide = annuler): ief.local
Spécifier un domaine/utilisateur autorisé: (Vide = annuler): ief\ADM-RCS
Mot de passe de ief\ADM-RCS: *****
Vous rejoignez ief.local... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-4S32DQSNVF5.
Vous avez correctement rejoint le domaine.
Voulez-vous modifier le nom de l'ordinateur avant de redémarrer ? (O)ui ou (N)on:
```

Entrez le nouveau nom pour votre DC, et validez le redémarrage



```
Administrateur : C:\Windows\system32\cmd.exe

=====
Changer l'appartenance au domaine ou groupe de travail
=====

Actuel groupe de travail : WORKGROUP

Souhaitez-vous adhérer à un (D)omaine ou Groupe de (t)ravail? (Vide = annuler): D
Nom de domaine à joindre (Vide = annuler): ief.local
Spécifier un domaine/utilisateur autorisé: (Vide = annuler): ief\ADM-RCS
Mot de passe de ief\ADM-RCS: *****
Vous rejoignez ief.local... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-4S32DQSNVF5.
Vous avez correctement rejoint le domaine.
Voulez-vous modifier le nom de l'ordinateur avant de redémarrer ? (O)ui ou (N)on: o
Entrer un nouveau nom d'ordinateur (Vide = annuler): WS2022-DC2-SB
Mot de passe de ief\ADM-RCS: *****
Modification en cours du nom d'ordinateur... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-4S32DQSNVF5.
Redémarrer maintenant ? (O)ui ou (N)on: _
```

Windows Server Site B

Configuration - Jonction au domaine AD, mise en place des rôles DC1

Introduction

Ce deuxième document couvre la procédure d'installation des différents rôles nécessaires à la mise en place d'un domaine AD.

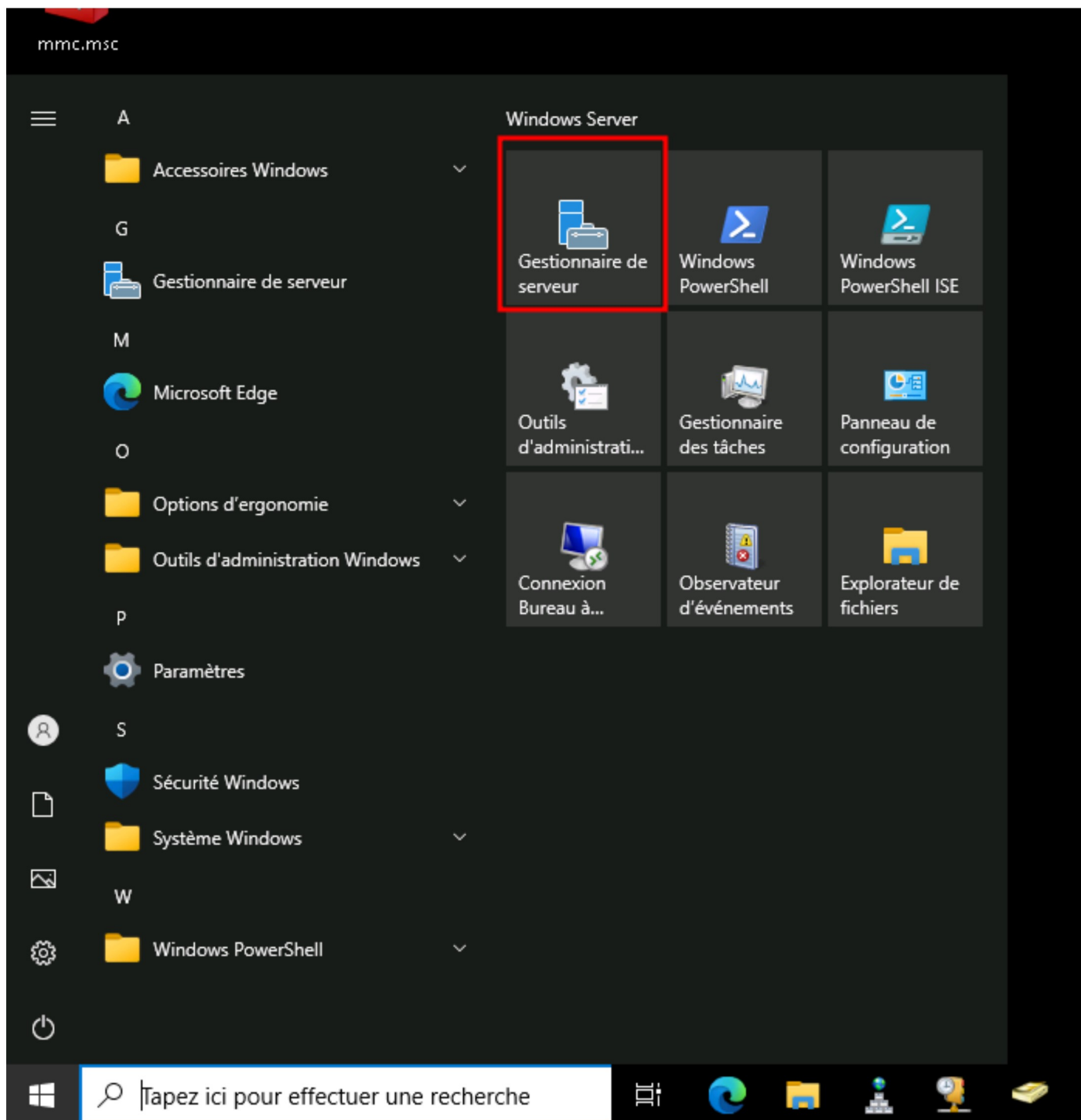
1. Installation des rôles AD, DNS, DHCP.
2. Configuration initiale du domaine

Pour ce faire, vous aurez besoin des éléments suivants :

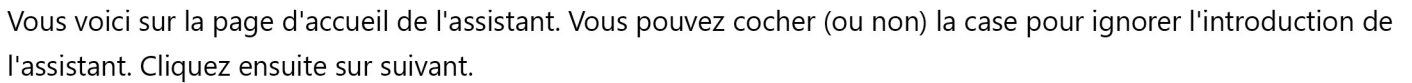
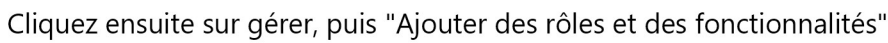
- Machine virtuelle Windows Server 2022
- Compte d'administration du serveur
- Serveur correctement nommé

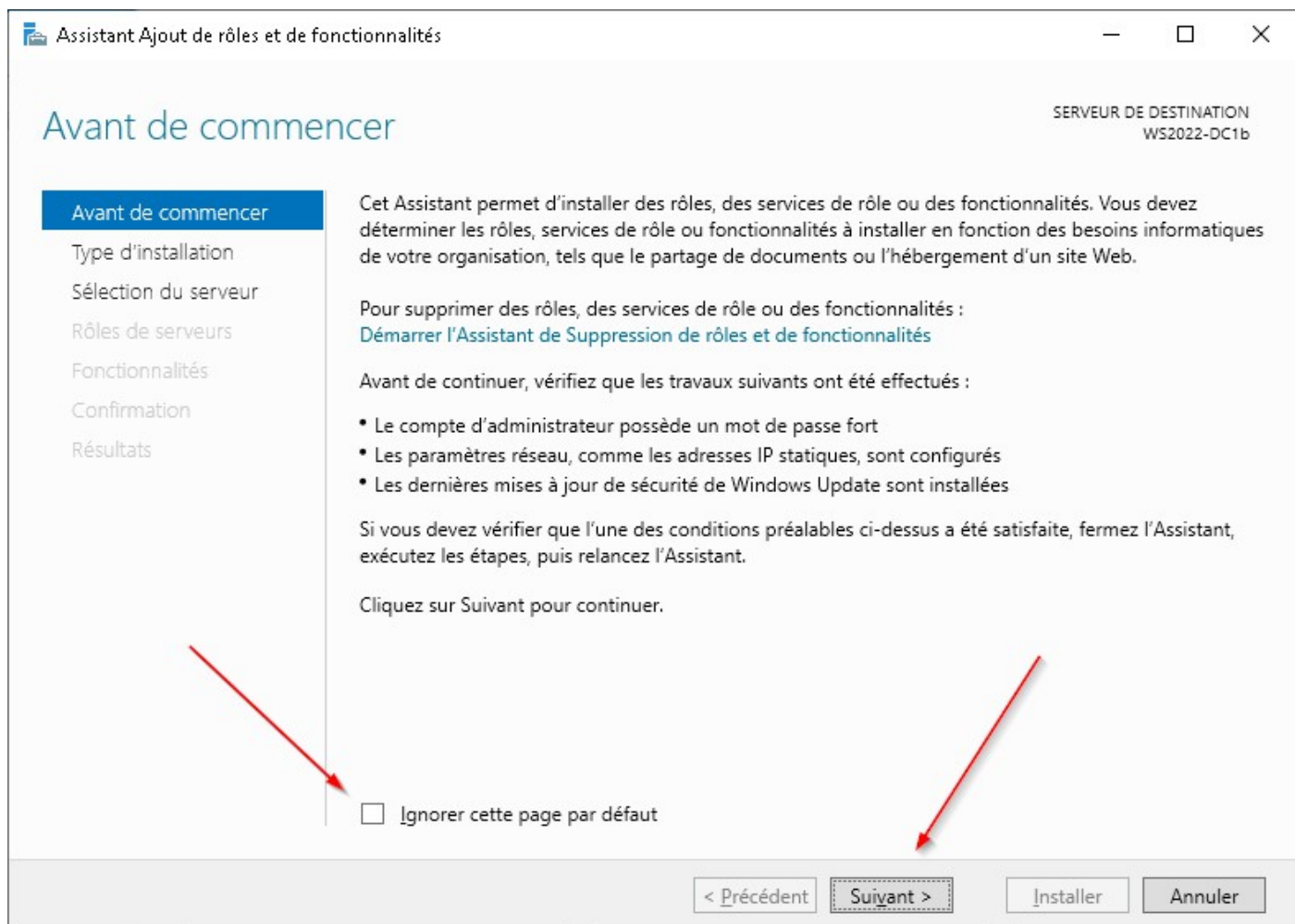
1) Installation des rôles

Pour installer des rôles de serveur, vous devez lancer le gestionnaire de serveur, trouvable dans le menu démarrer du serveur.

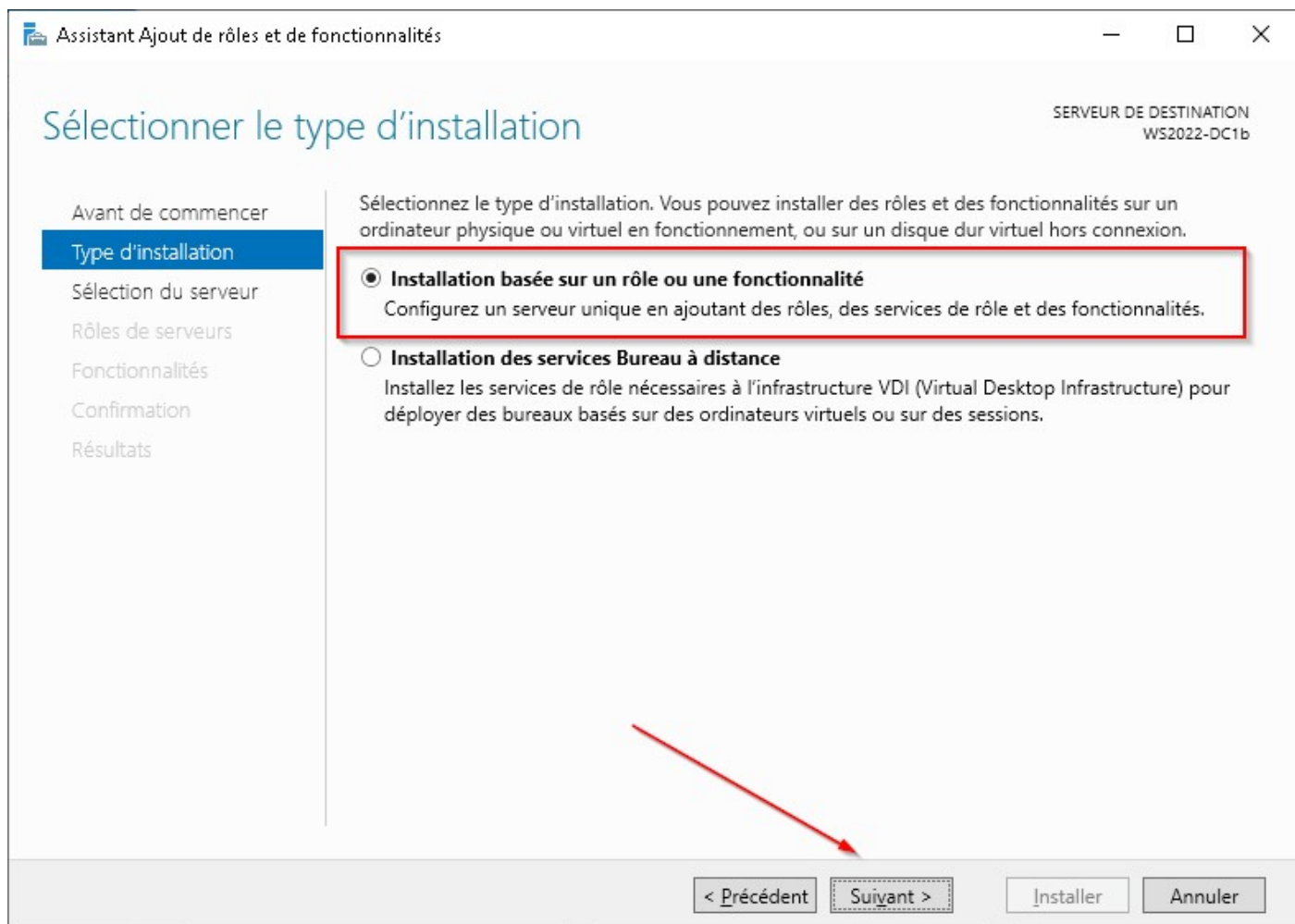


Avant de commencer, vérifiez que votre serveur est correctement nommé. Une fois le domaine créé, il faudra réaliser des actions spécifiques dans le cas où vous voudriez renommer votre serveur par la suite.





Vérifiez ensuite que la première option est bien celle cochée dans la fenêtre qui suit



Sélectionnez les paramètres régionaux de votre machine, et cliquez sur suivant

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
WS2022-DC1b

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

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

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

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
WS2022-DC1b	192.168.1.10	Microsoft Windows Server 2022 Standard

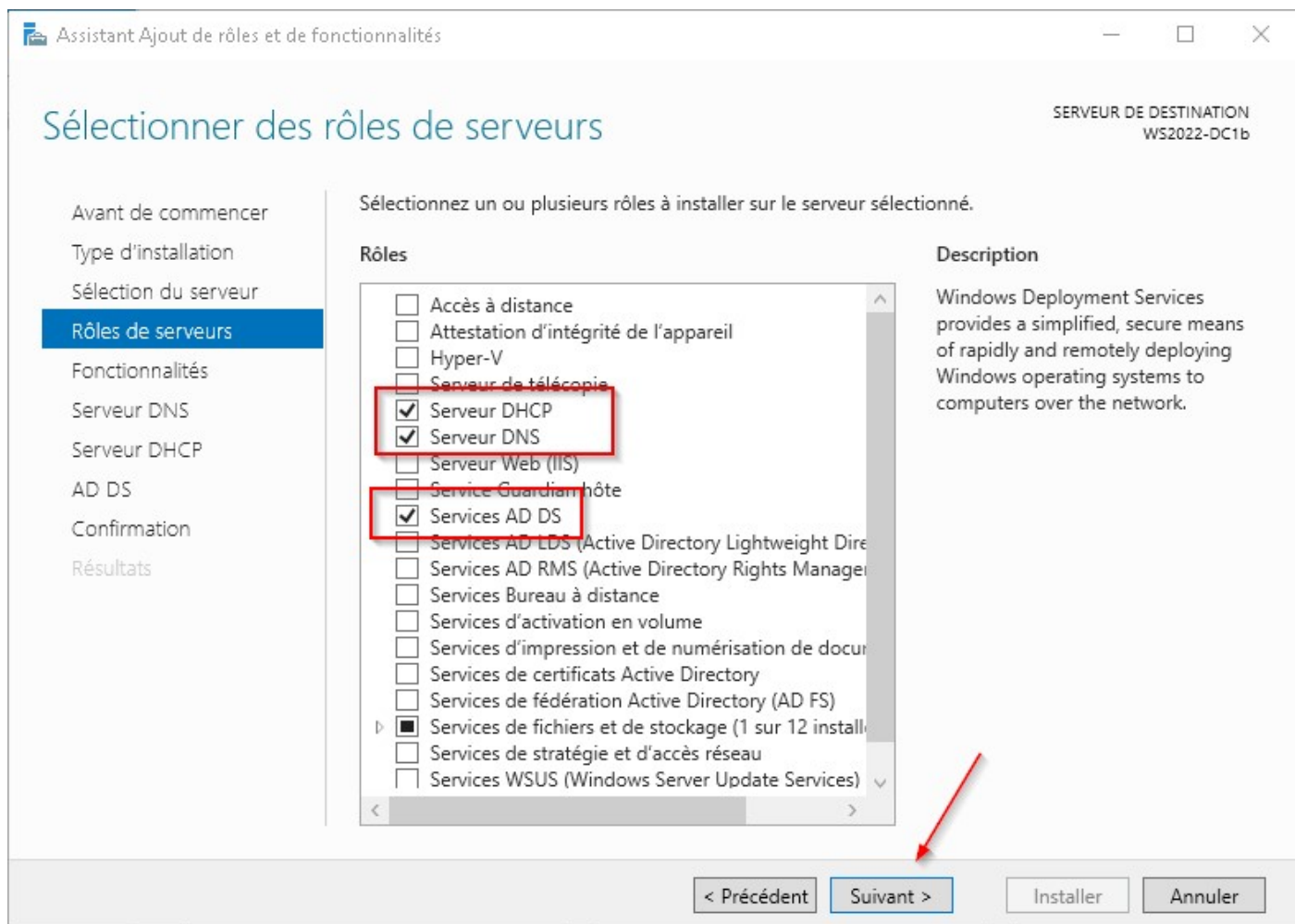
1 ordinateur(s) trouvé(s)

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

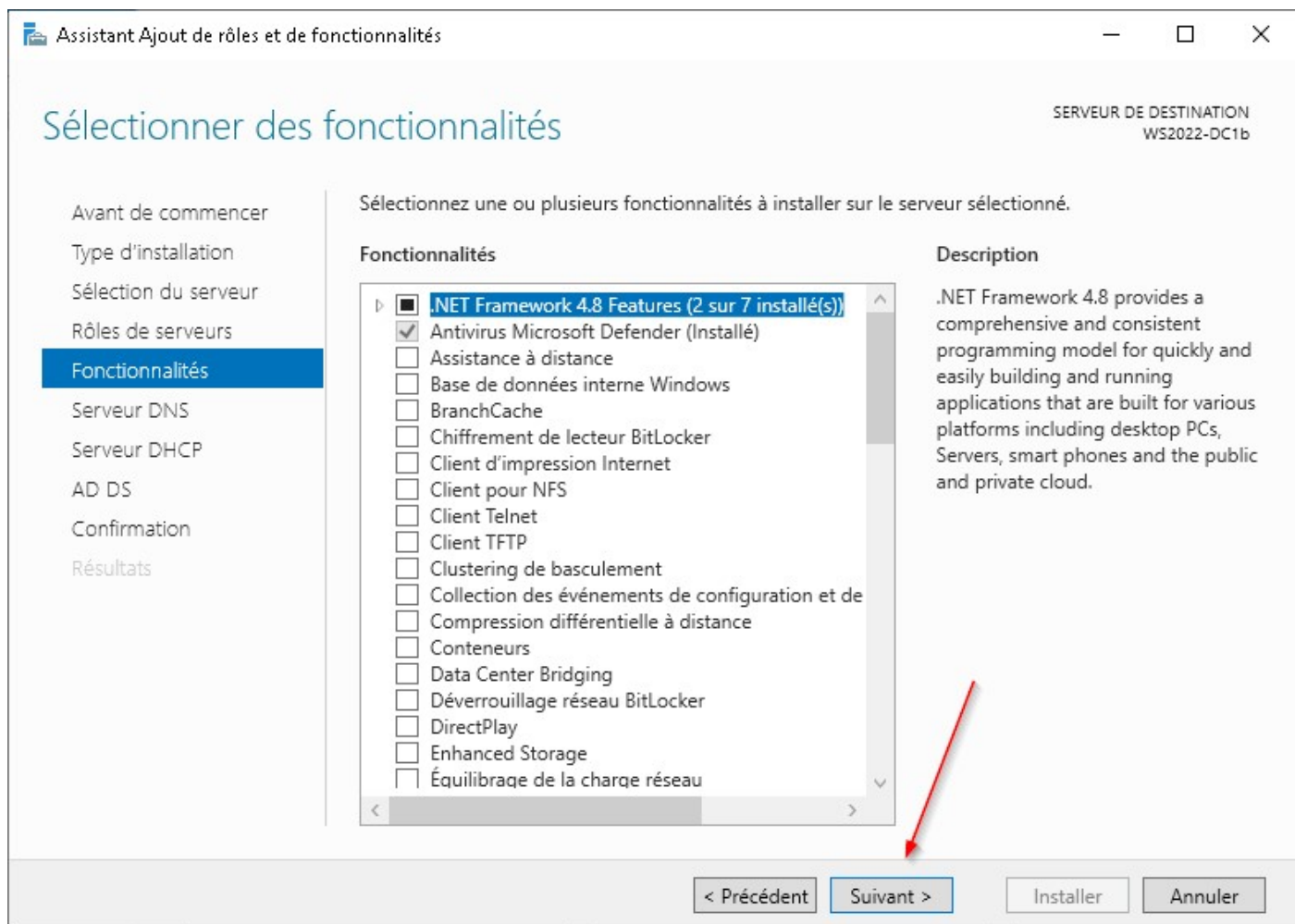
< Précédent Suivant > Installer Annuler

Si votre machine fait partie d'un Pool de Serveurs, pensez à vérifier son nom pour être sûr d'agir sur la bonne machine.

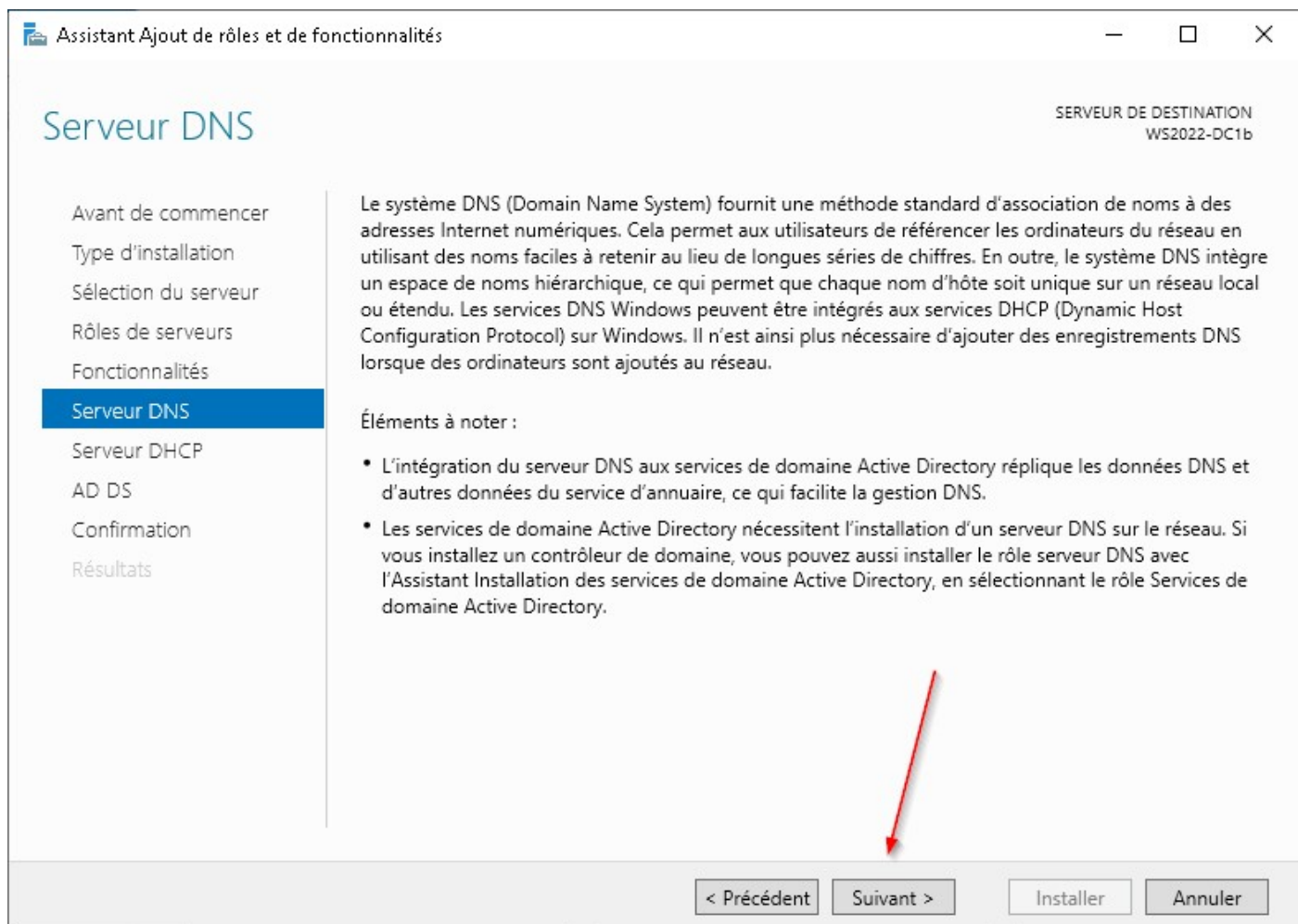
Sélectionnez les rôles nécessaires. Dans notre cas, nous allons utiliser notre serveur pour AD et DHCP, Il faut donc activer les rôles DNS, DHCP et AD DS.

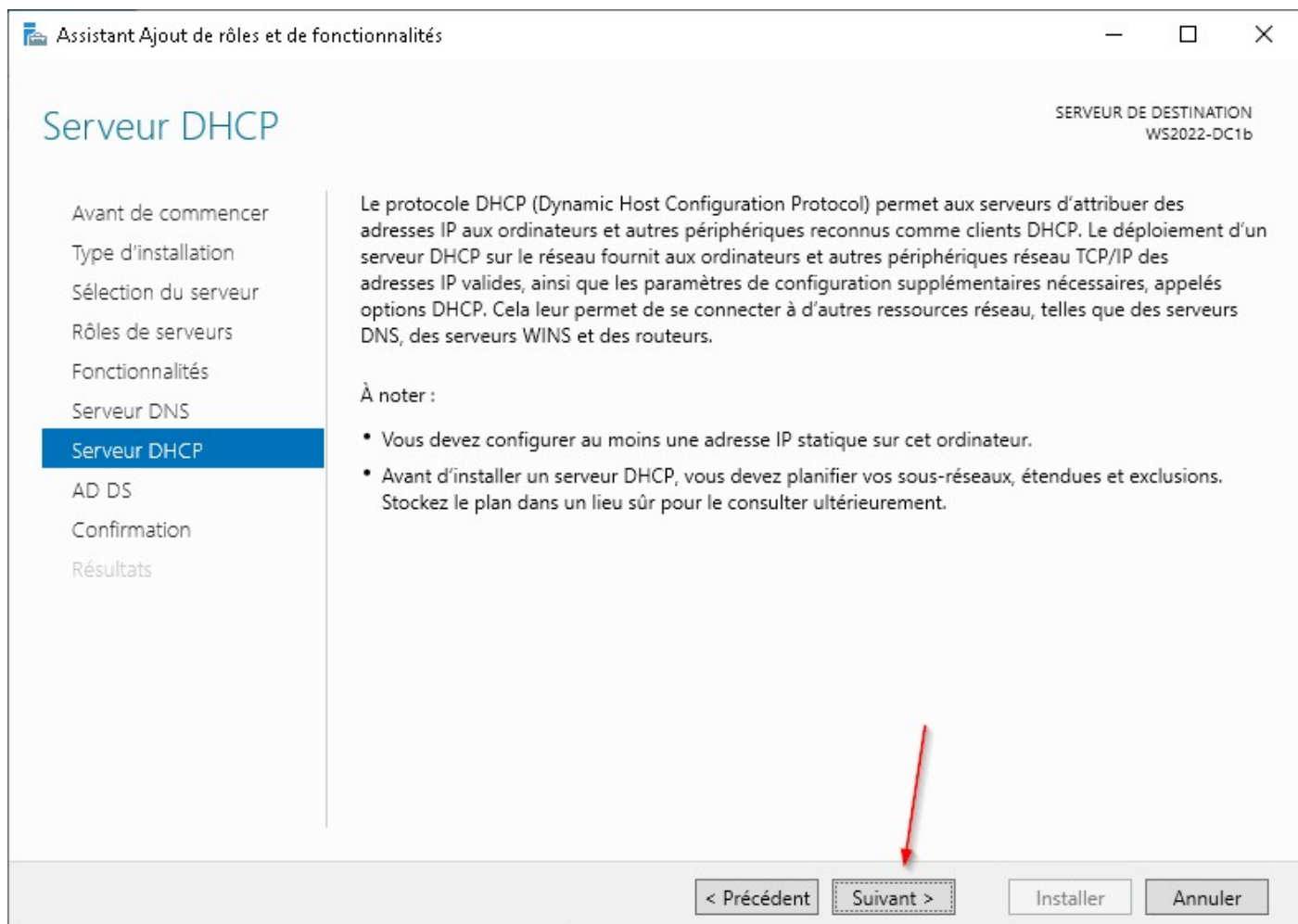


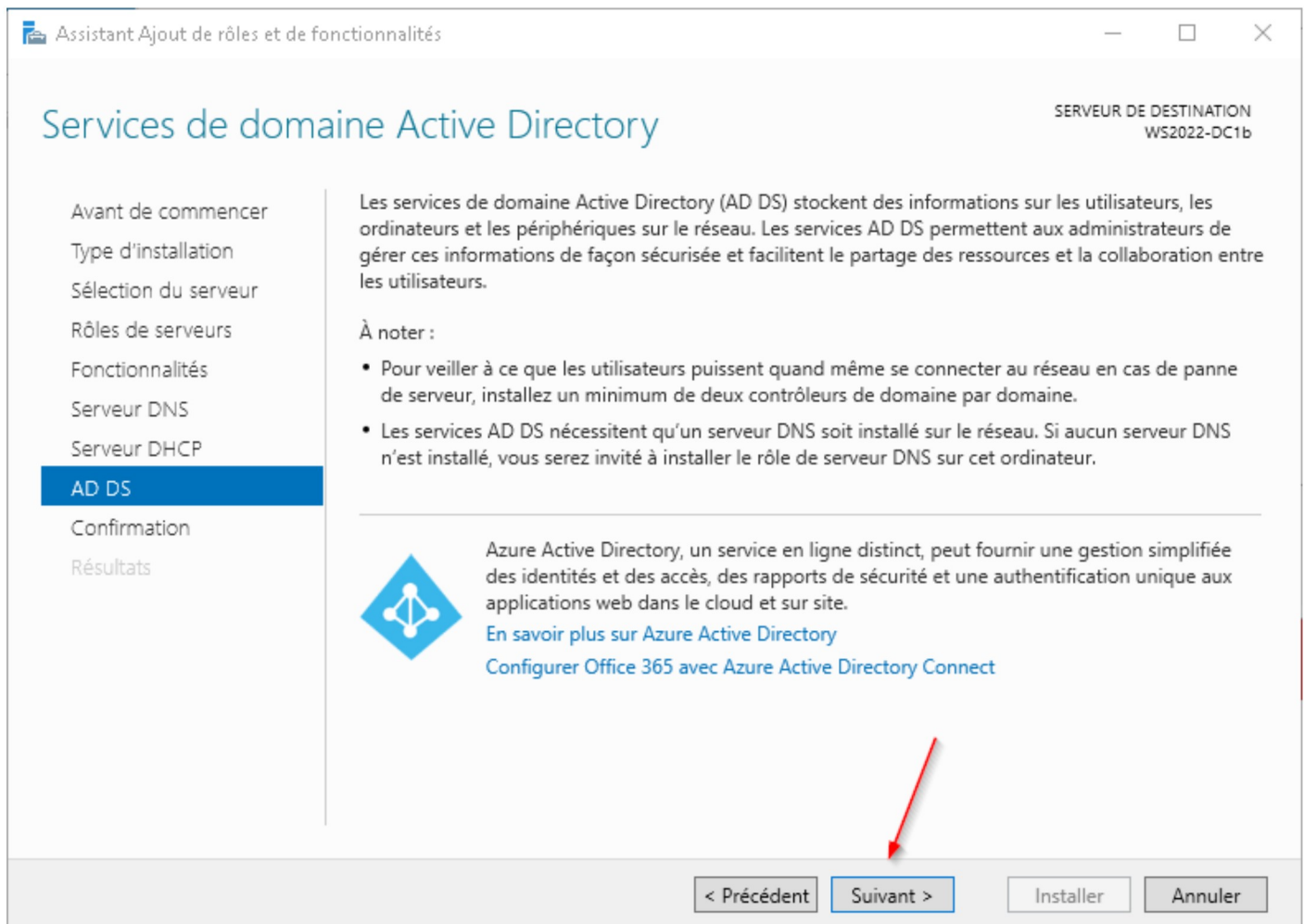
Aucun besoin d'ajouter des fonctionnalités, elles ont déjà été auto-sélectionnées par Windows lors de la sélection des rôles.



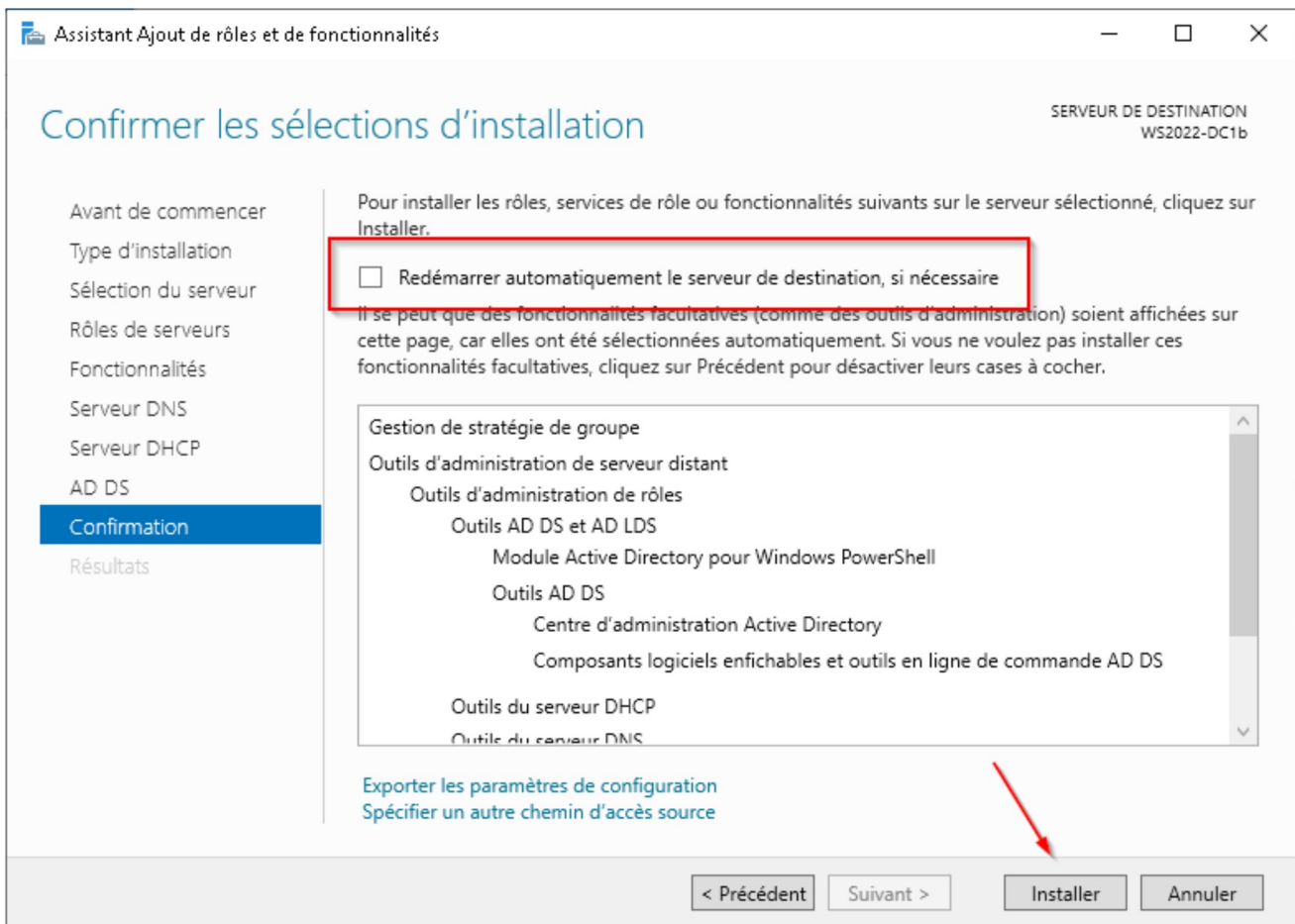
3 fenêtres d'information vont se suivre.



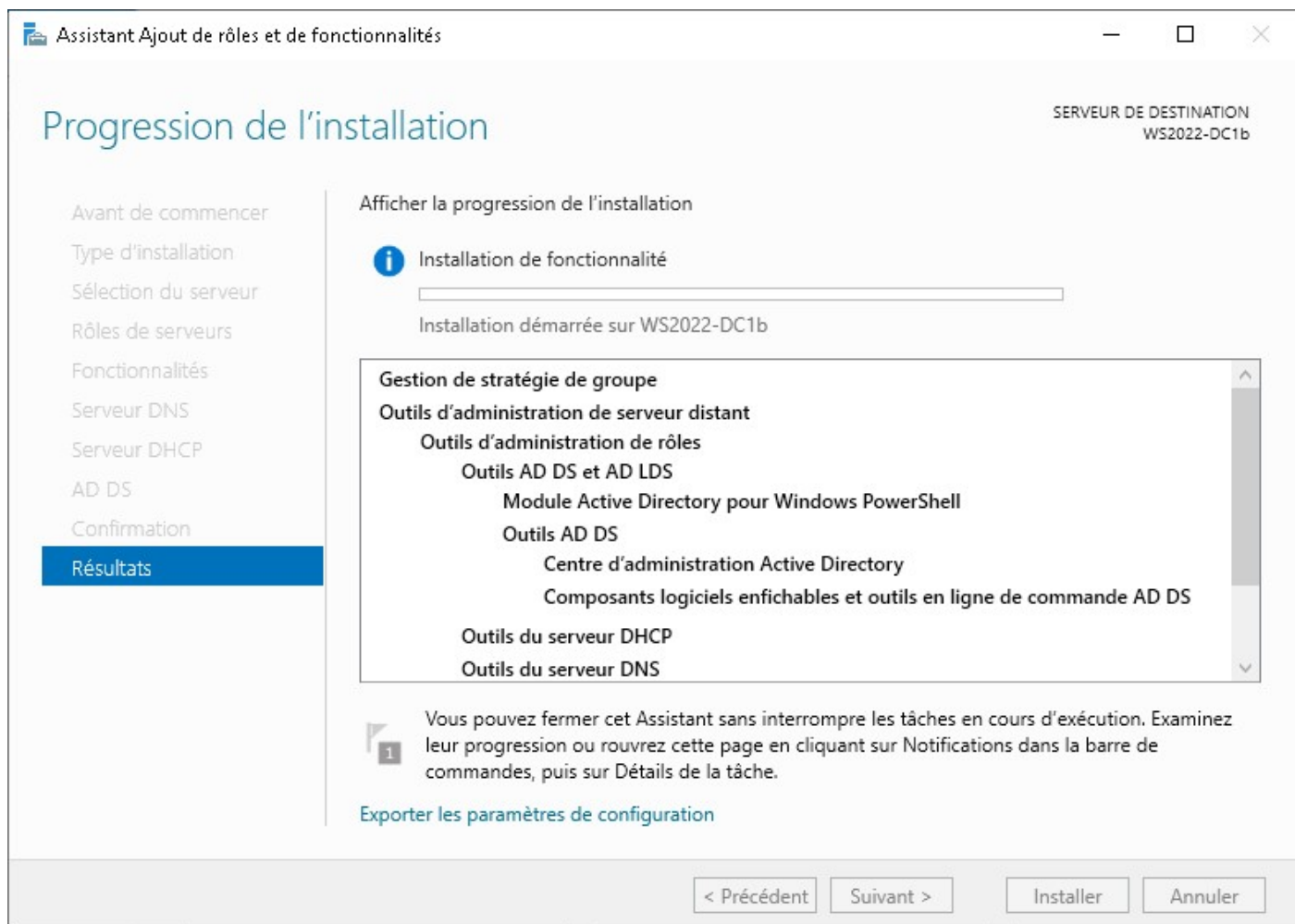




Décochez ensuite la case pour redémarrer la machine, et cliquez sur installer

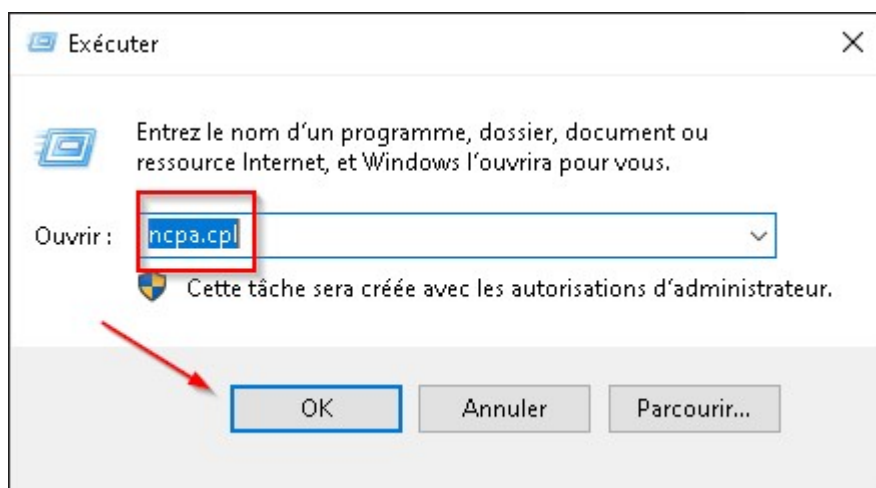


L'installation démarre.

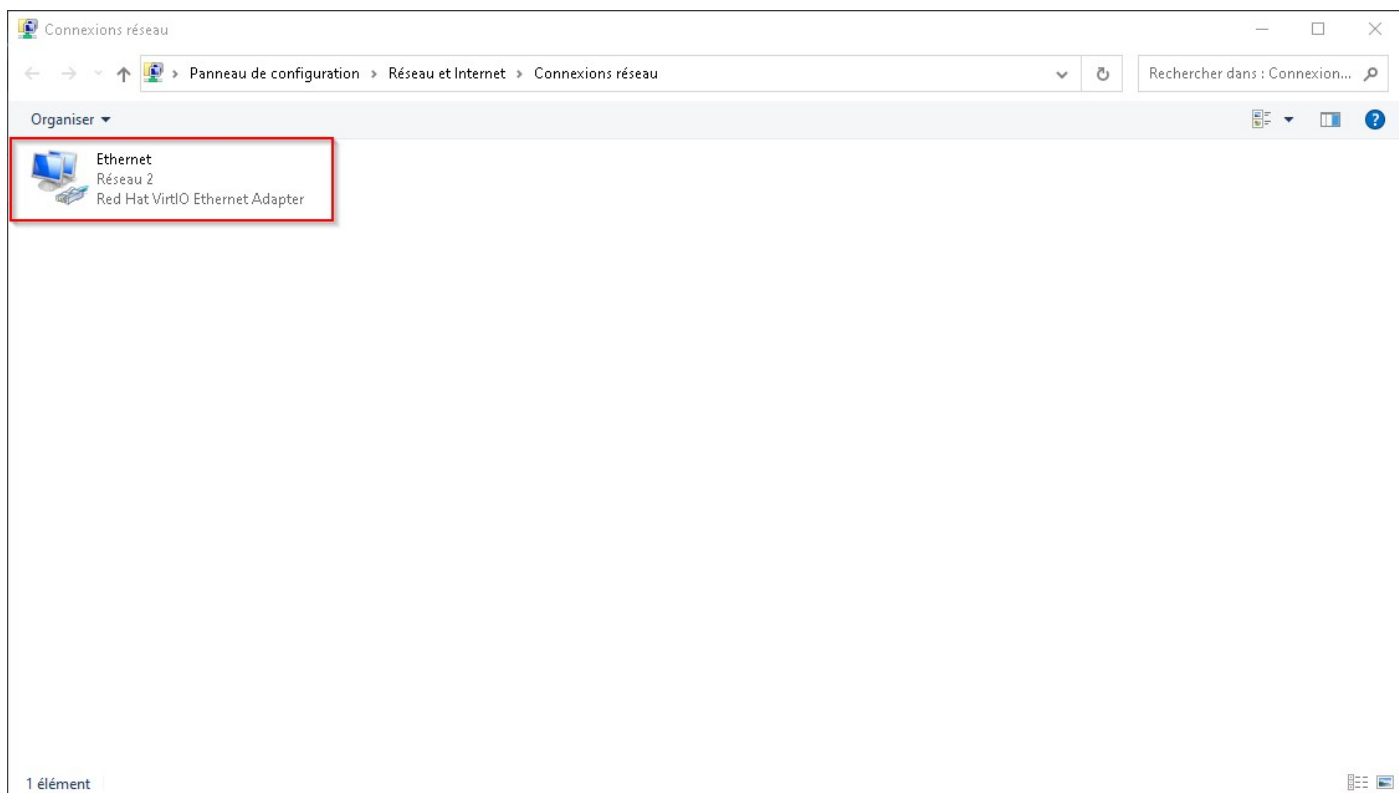


Pendant que les rôles s'installent, nous allons configurer une adresse IP statique sur notre serveur

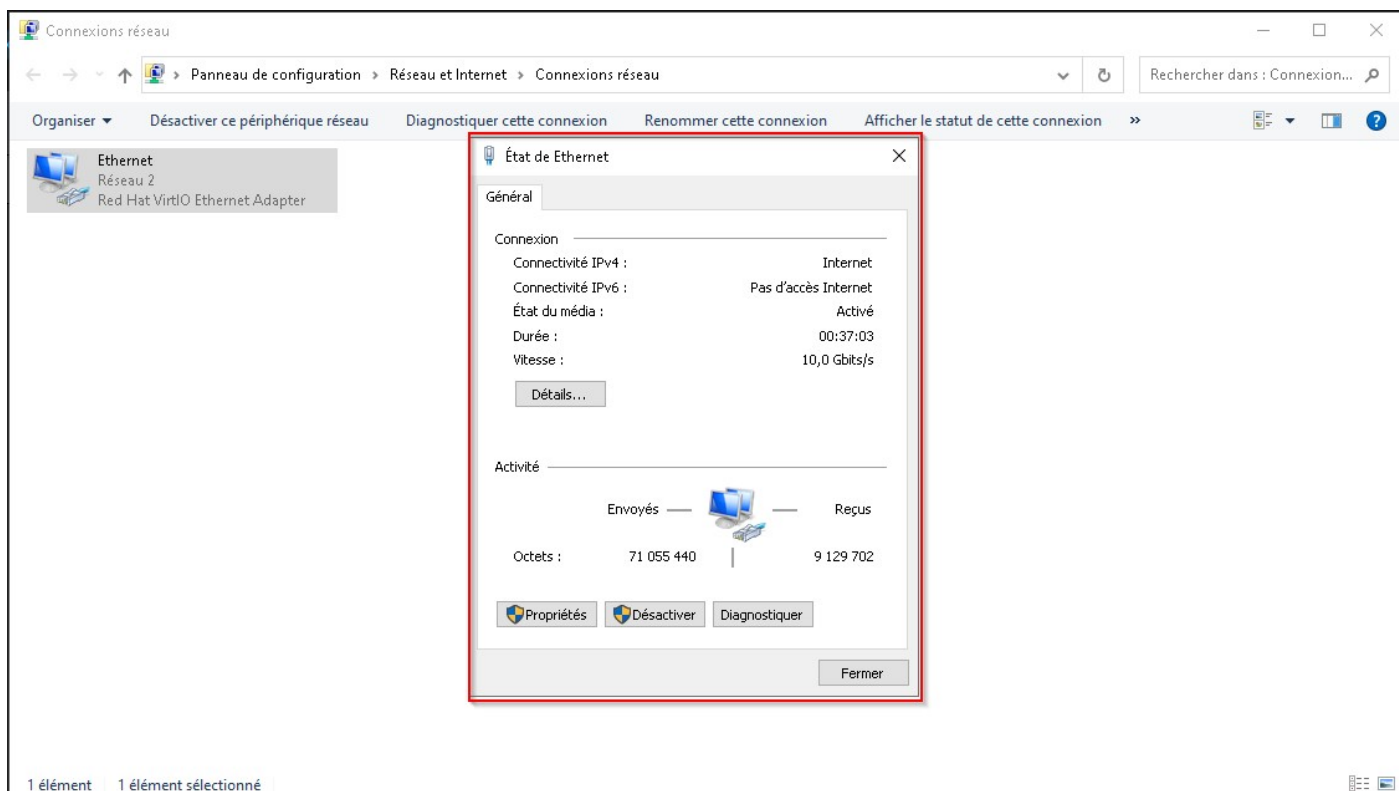
Pour se faire, ouvrez le dialogue d'exécution de Windows via le raccourci "Win+R" et tapez "ncpa.cpl"



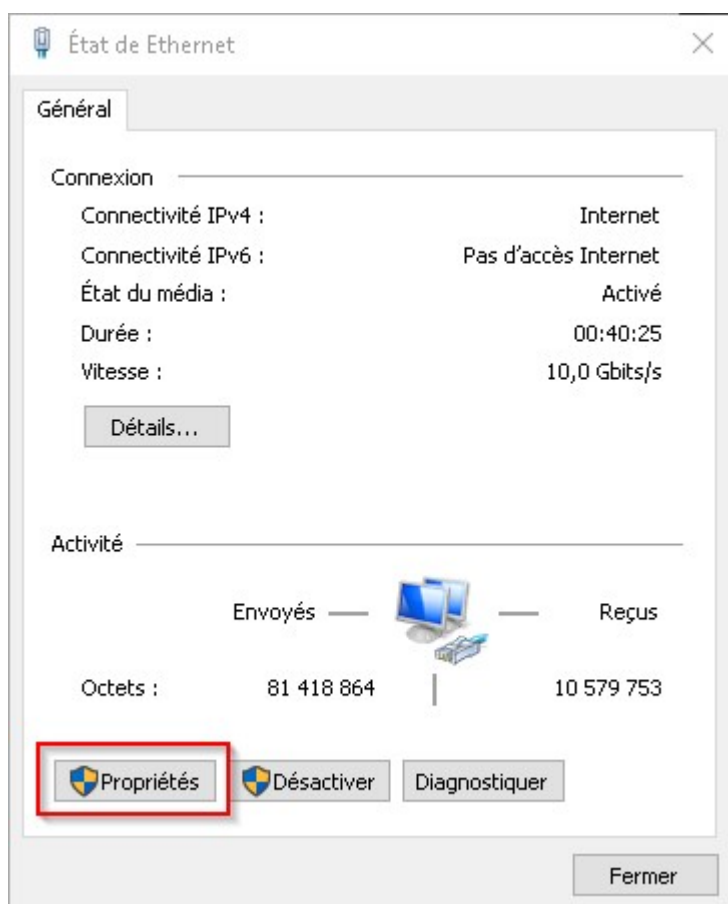
Cela ouvrira le panneau de configuration des adaptateurs réseau. Double-cliquez sur votre interface réseau.



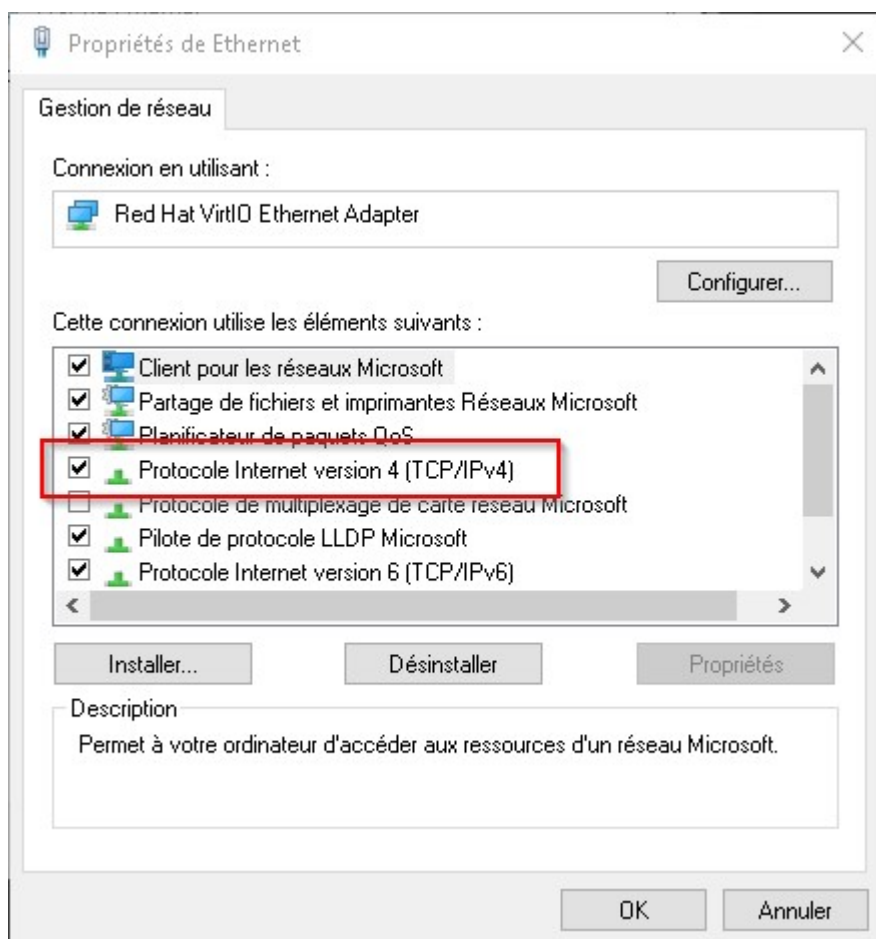
Une fenêtre de propriété apparaît



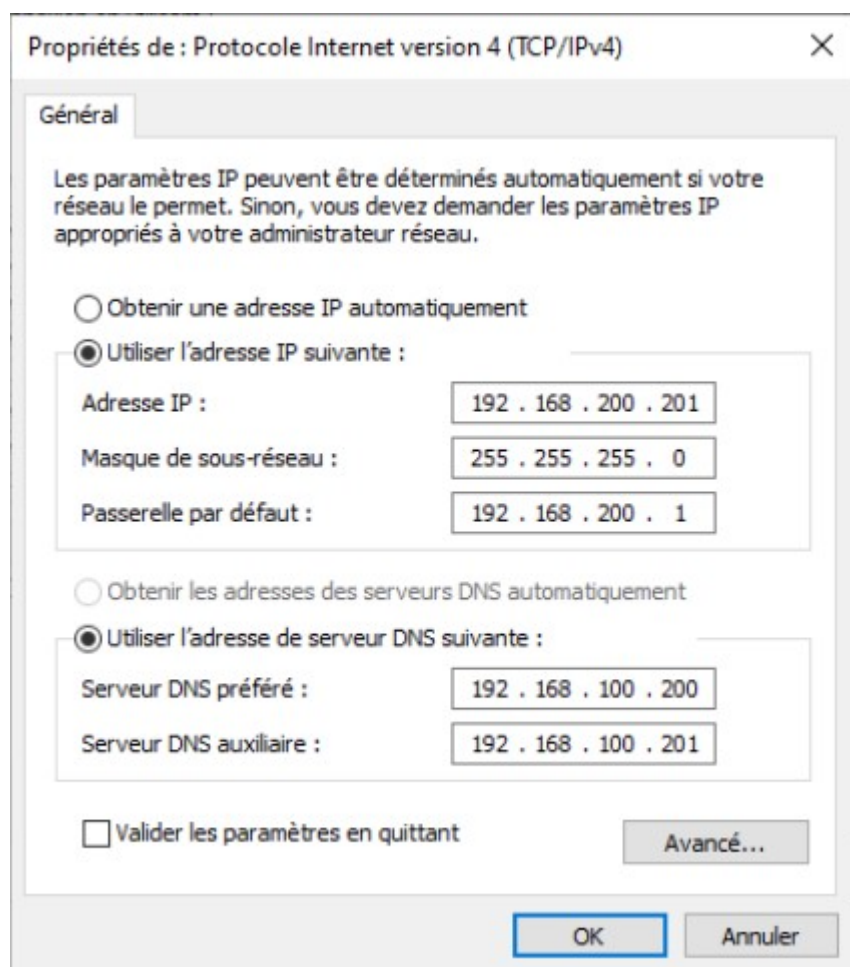
Cliquez ensuite sur "Propriétés"



Double-cliquez sur "Protocole internet version 4"



Configurez ensuite le réseau selon votre environnement, dans notre cas, les DNS seront dans un premier temps les DNS du site afin de pouvoir rejoindre le domaine existant, ils devront être changés pour les DC locaux dans le futur.

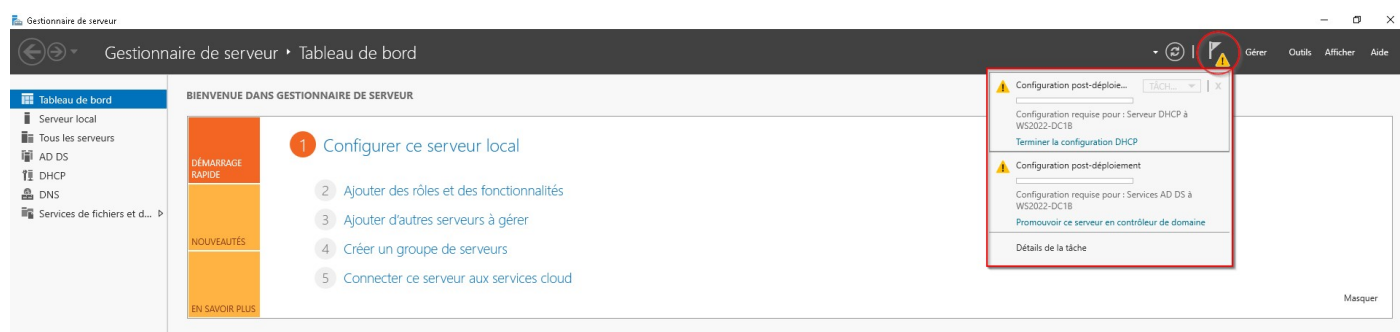


Validez en cliquant sur OK aux fenêtres deux contextuelles et Fermer sur l'interface de propriétés.

Vous pouvez ensuite redémarrer votre machine.

2) Configuration des rôles.

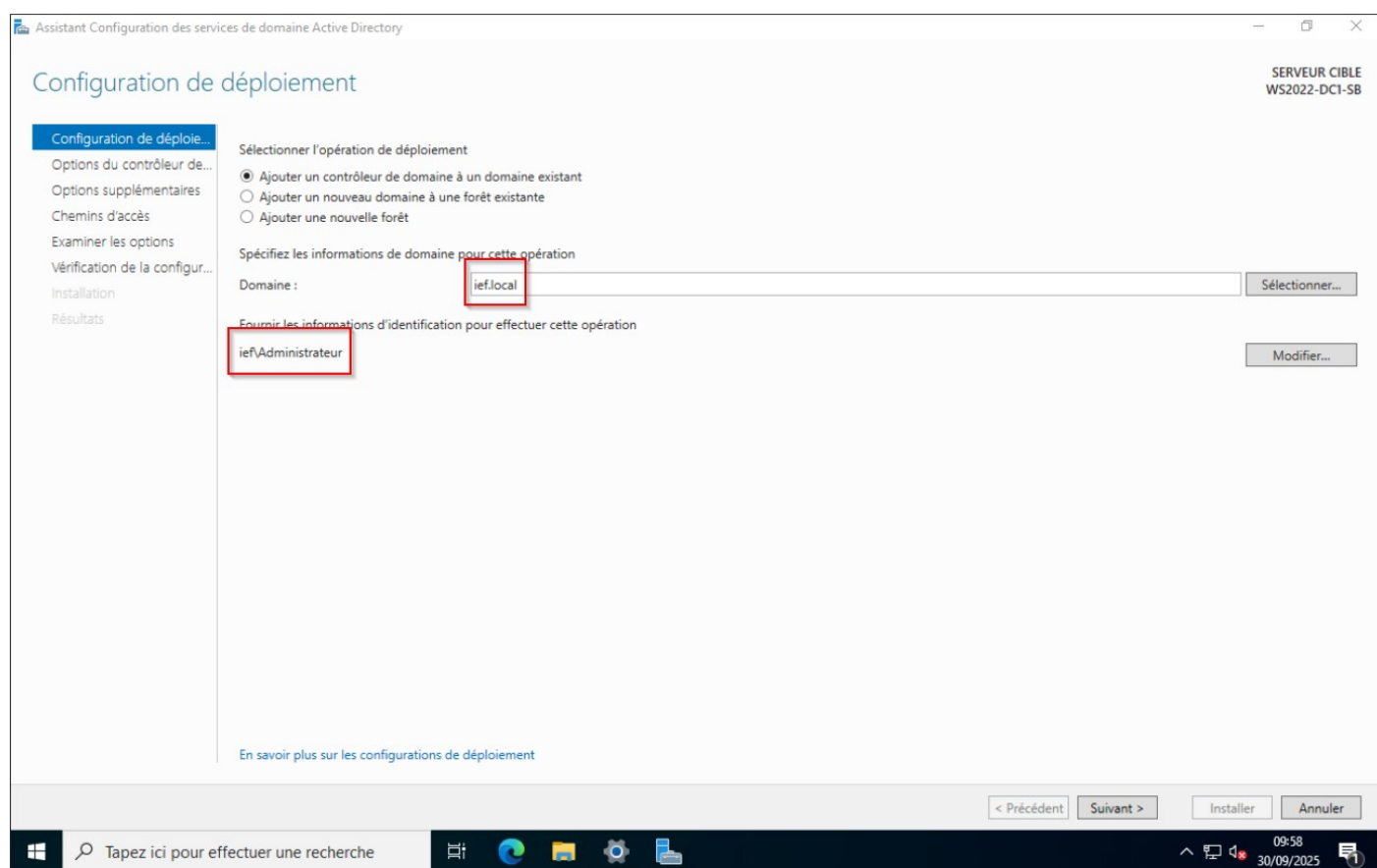
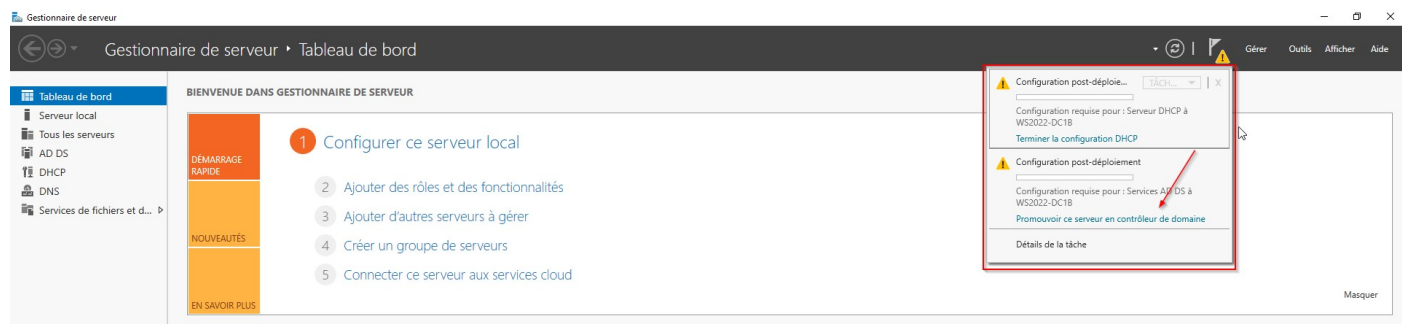
Une fois redémarré, lancez le gestionnaire de serveur, et cliquez sur le drapeau en haut à droite.

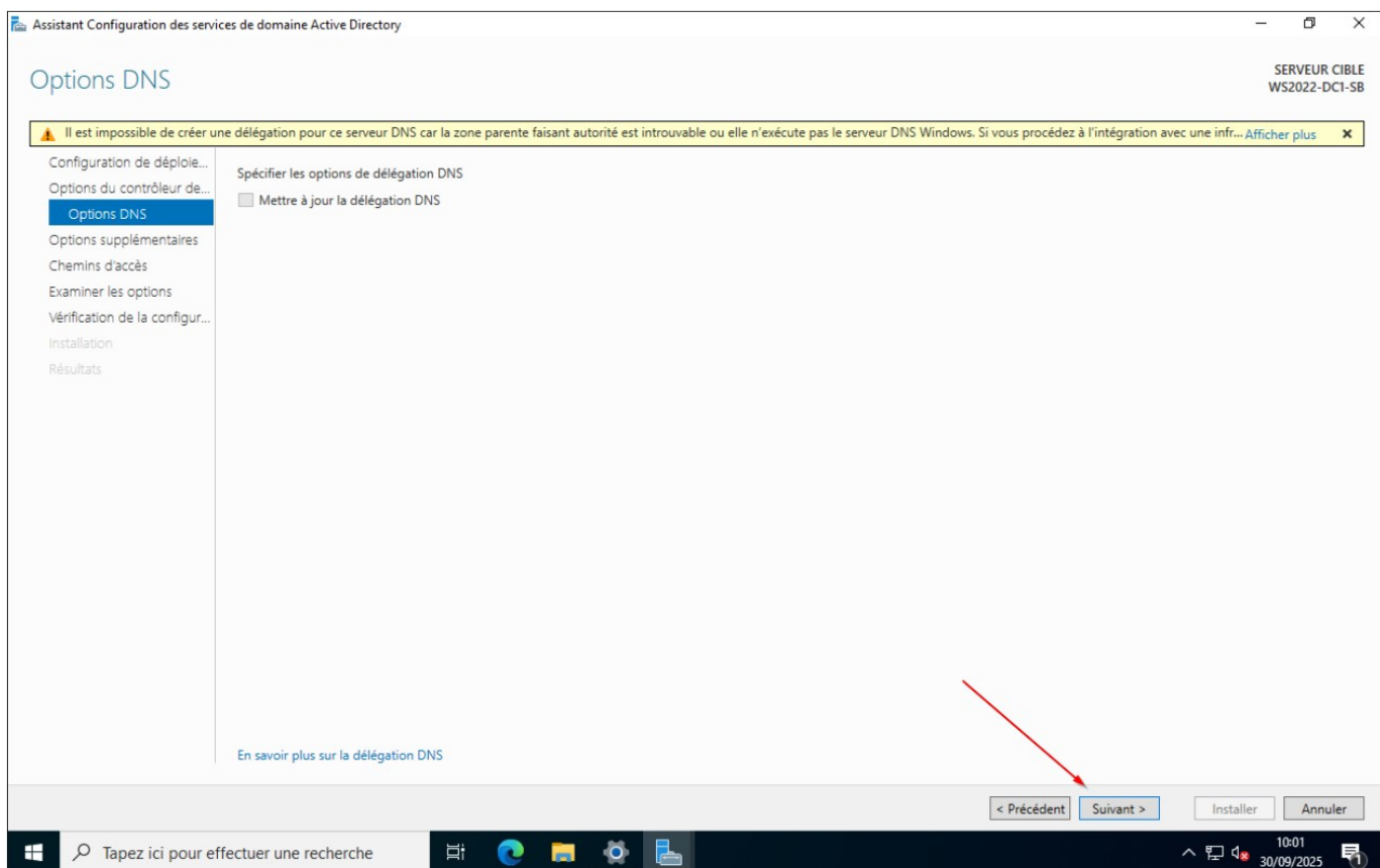
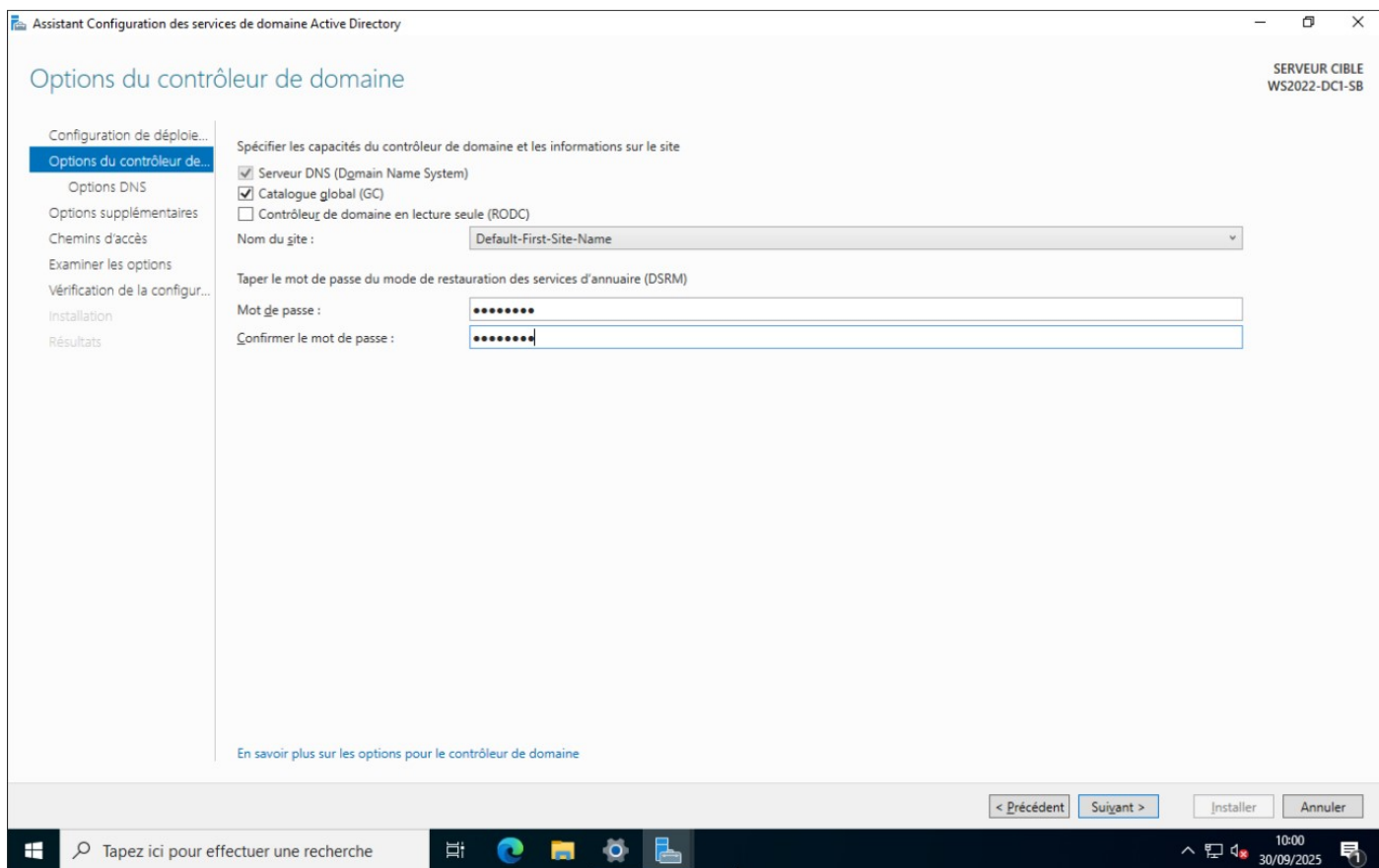


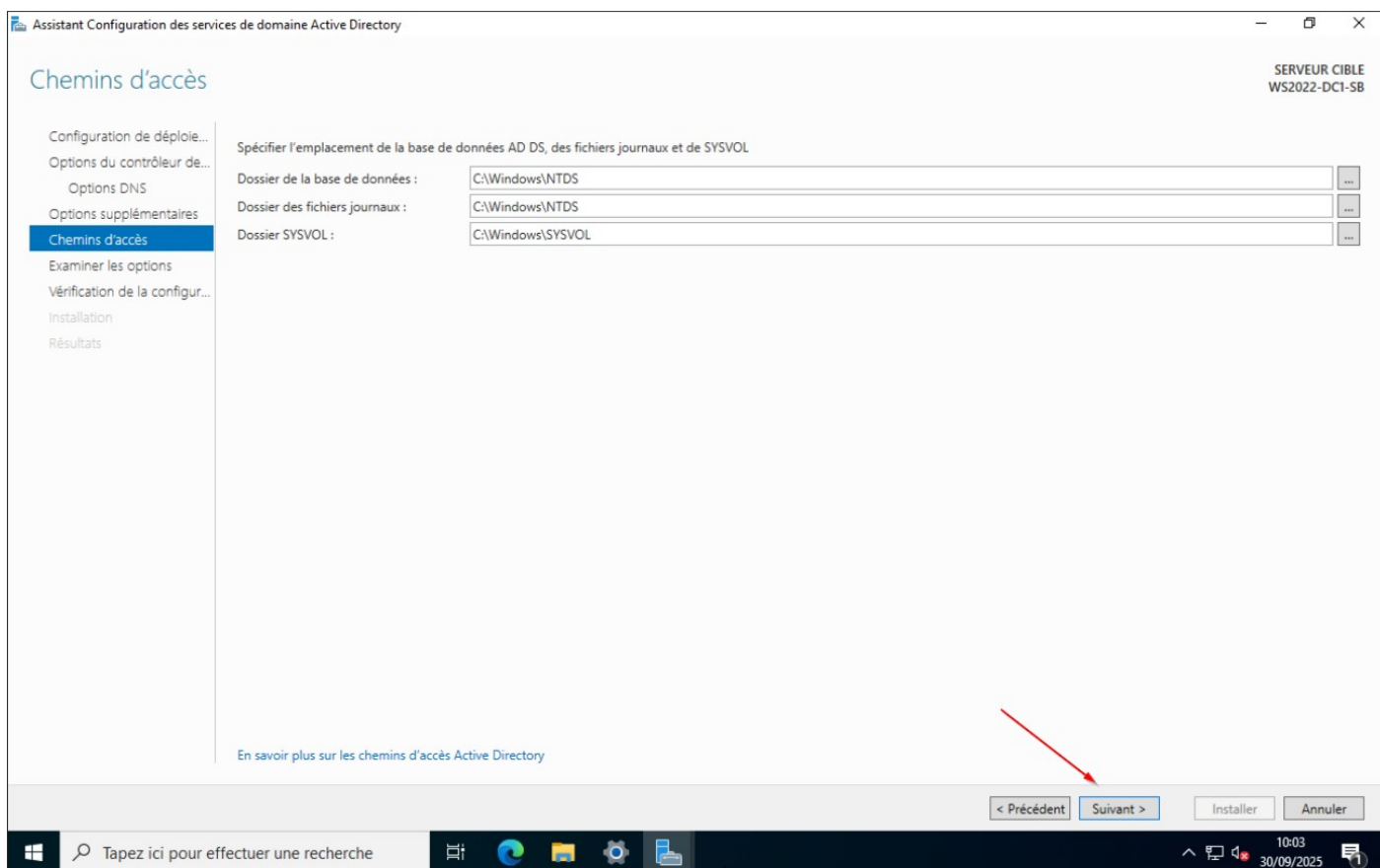
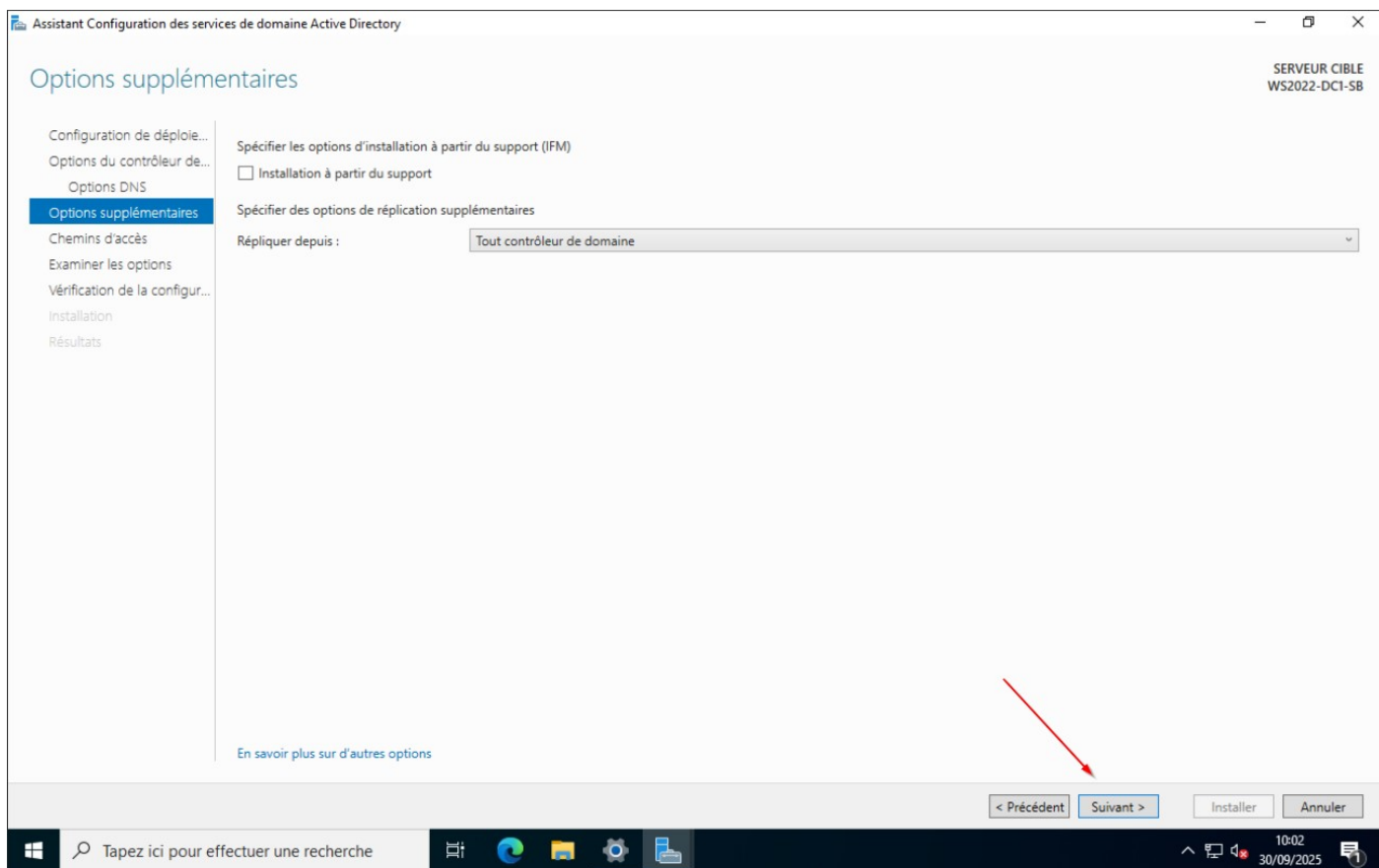
Vous verrez les tâches de configuration en suspens.

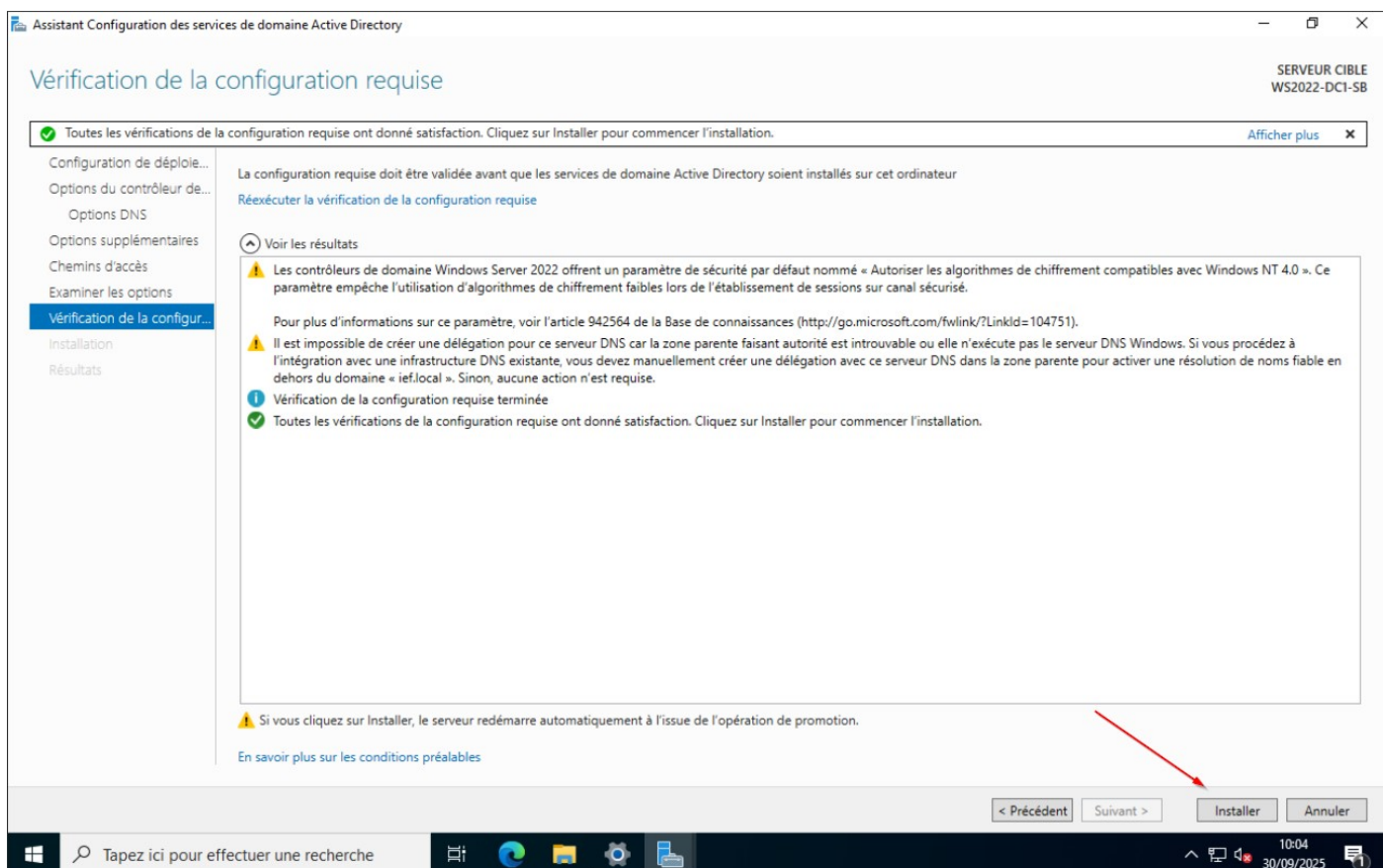
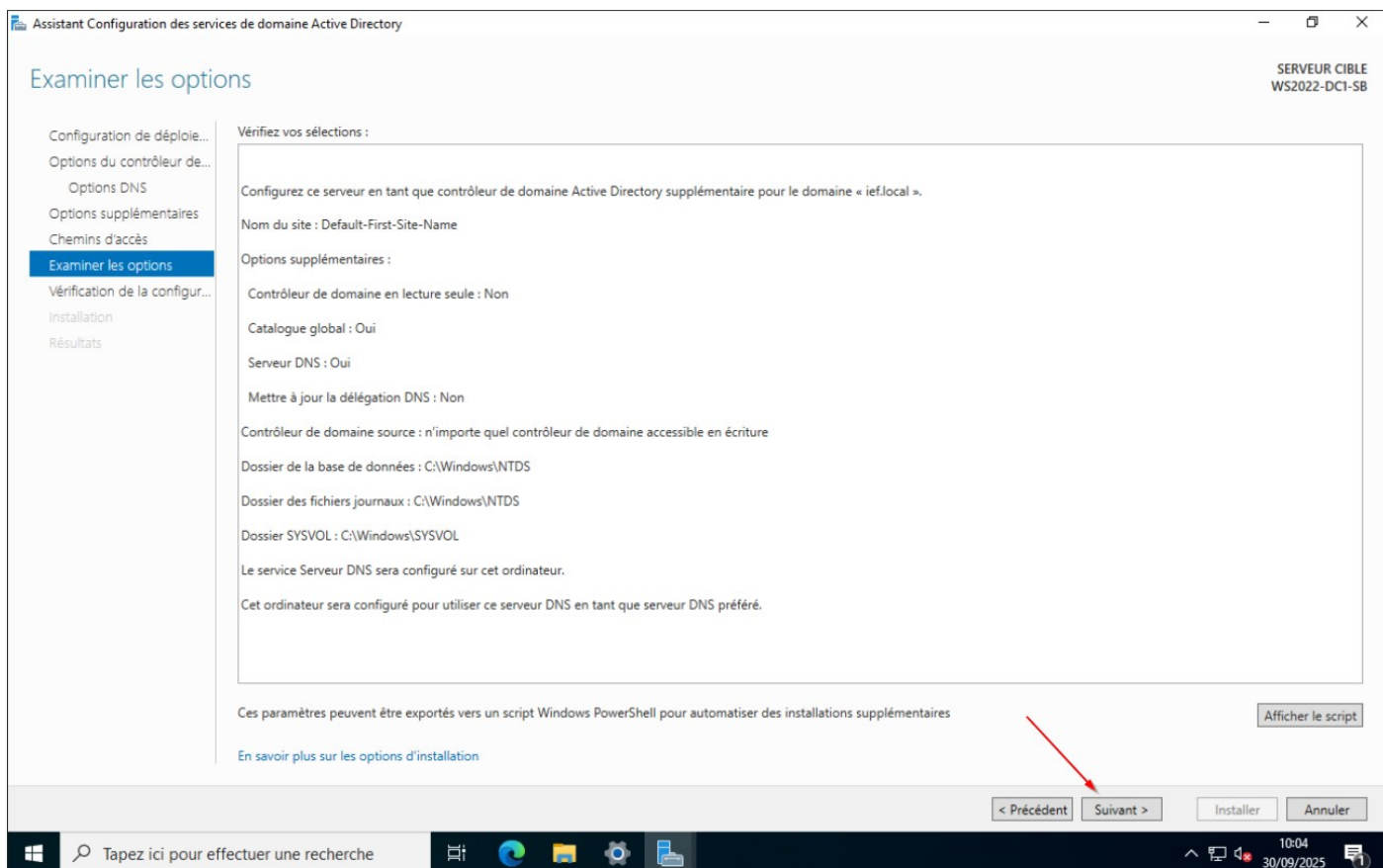
A. Configuration d'AD DS et jonction au domaine

Revenez dans le menu déroulant sous le drapeau du gestionnaire de serveur, et cliquez sur "Promouvoir ce serveur en contrôleur de domaine"



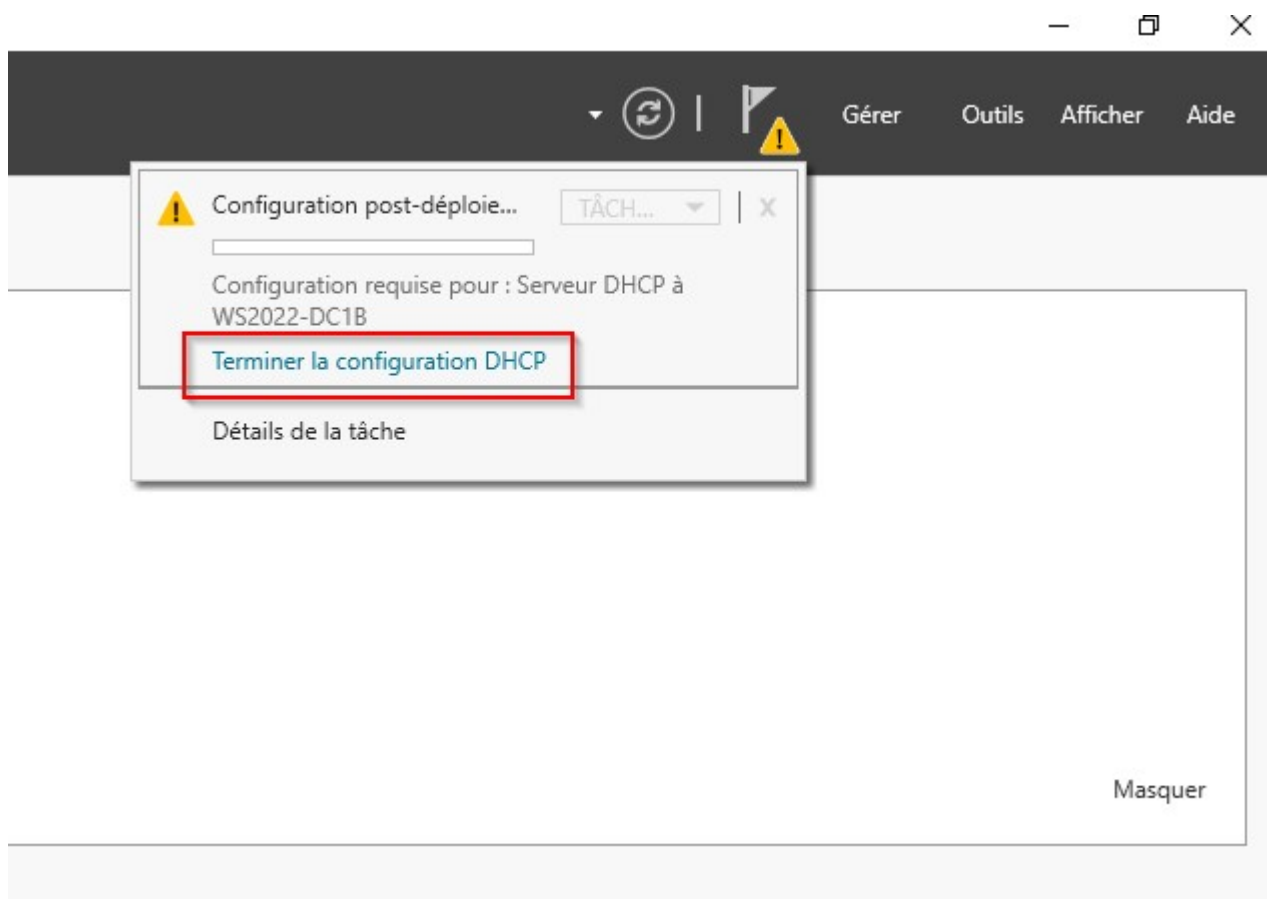




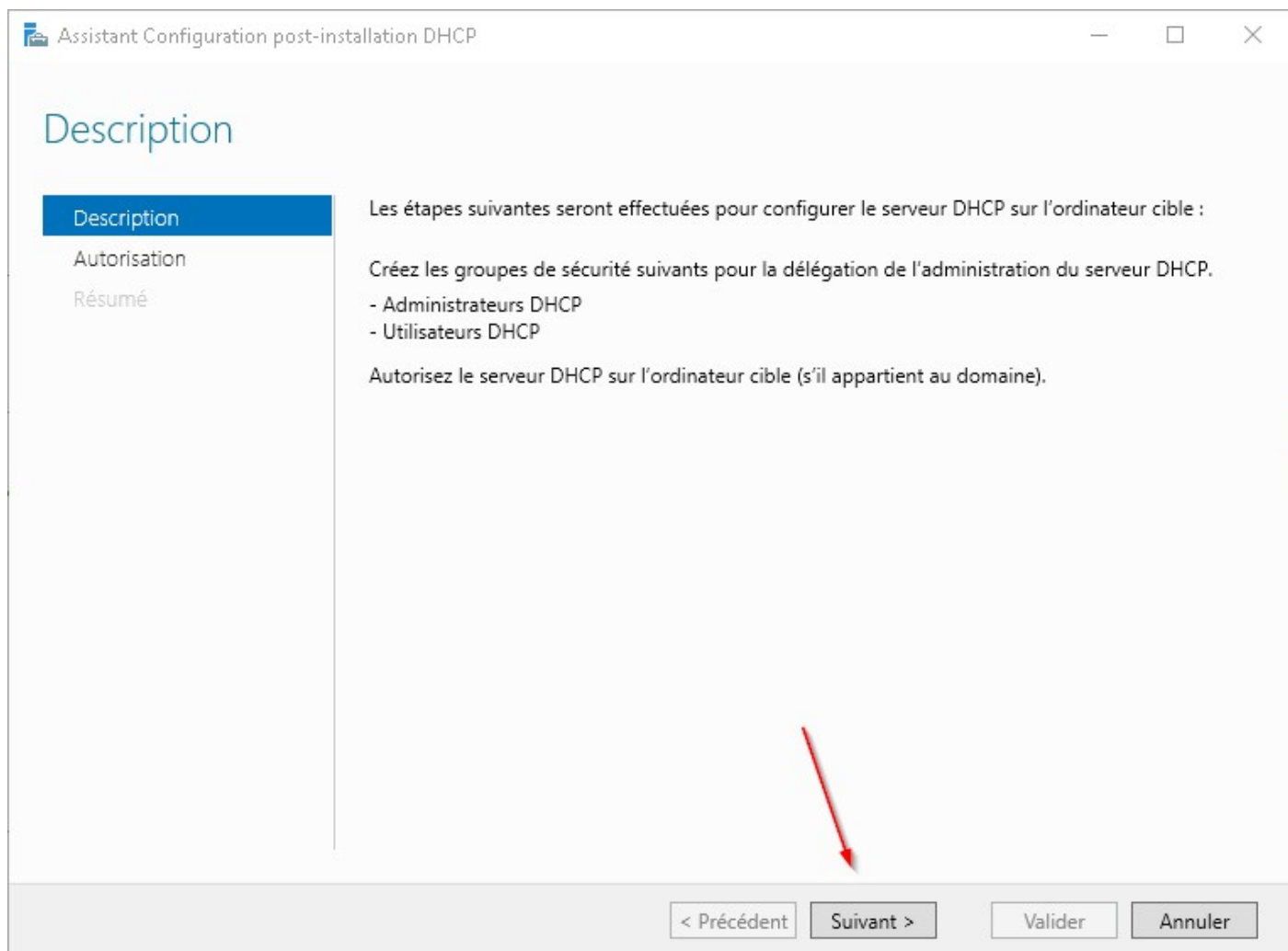


C. Installation du DHCP.

Cliquez sur le panneau en haut à droite puis sur "Terminer la configuration DHCP".



Une fenêtre va s'ouvrir avec des instructions.



Renseignez bien votre nom d'utilisateur et valider ensuite.

Assistant Configuration post-installation DHCP

Autorisation

Description

Autorisation

Résumé

Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.

☒ Utiliser les informations d'identification de l'utilisateur suivant


Nom d'utilisateur :

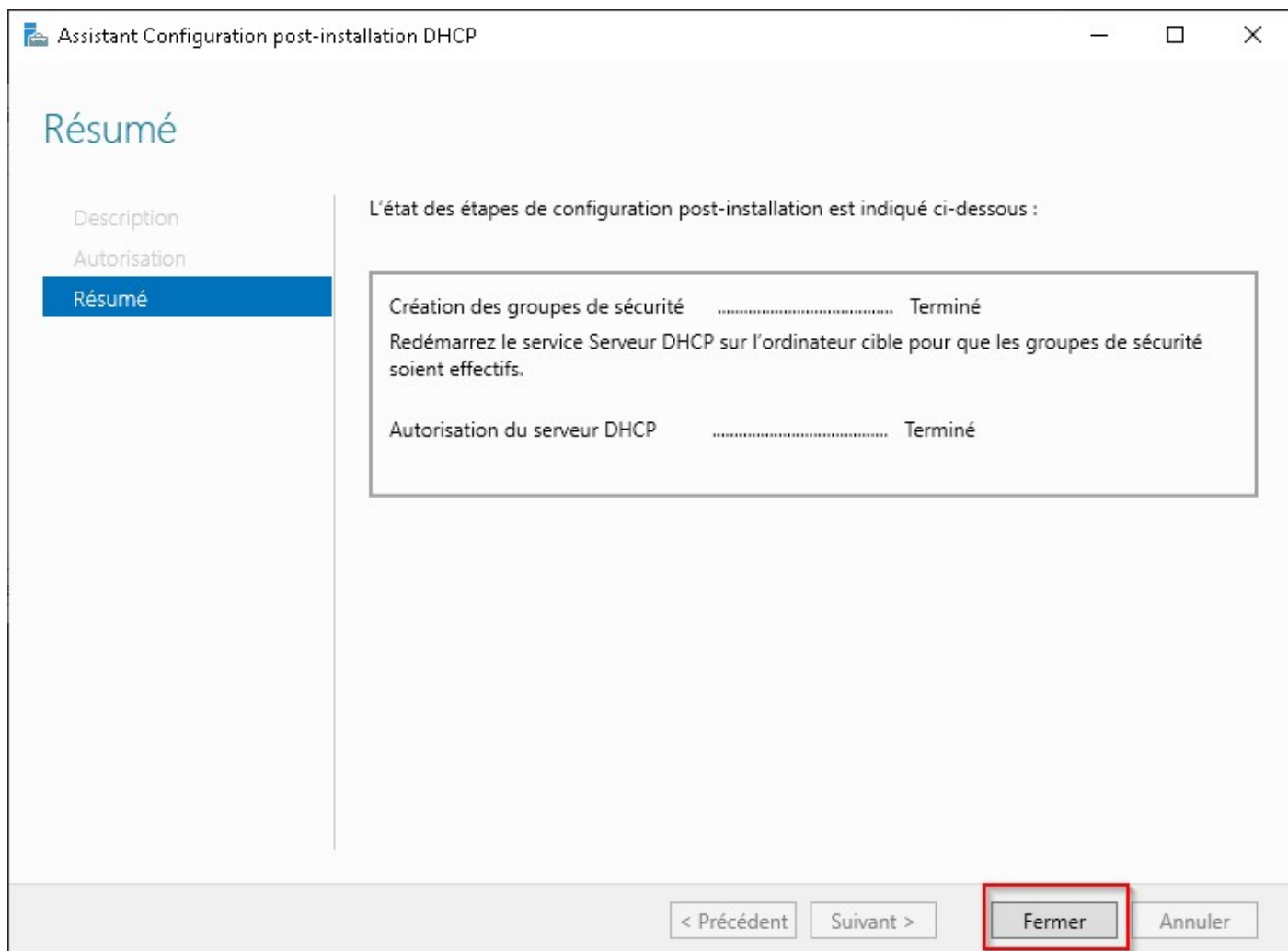
☐ Utiliser d'autres informations d'identification

Nom d'utilisateur :

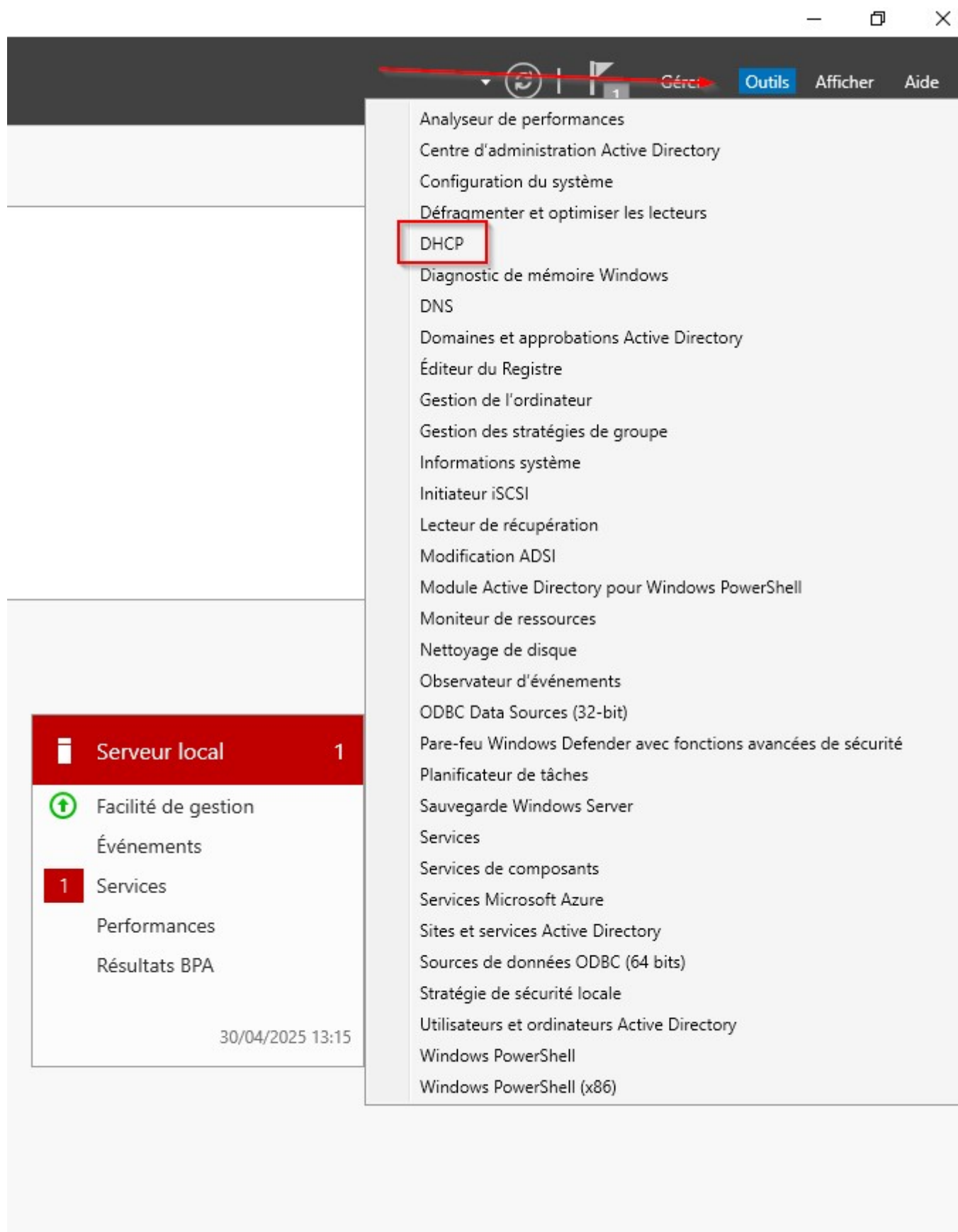
☐ Ignorer l'autorisation AD

< Précédent Suivant > Valider Annuler

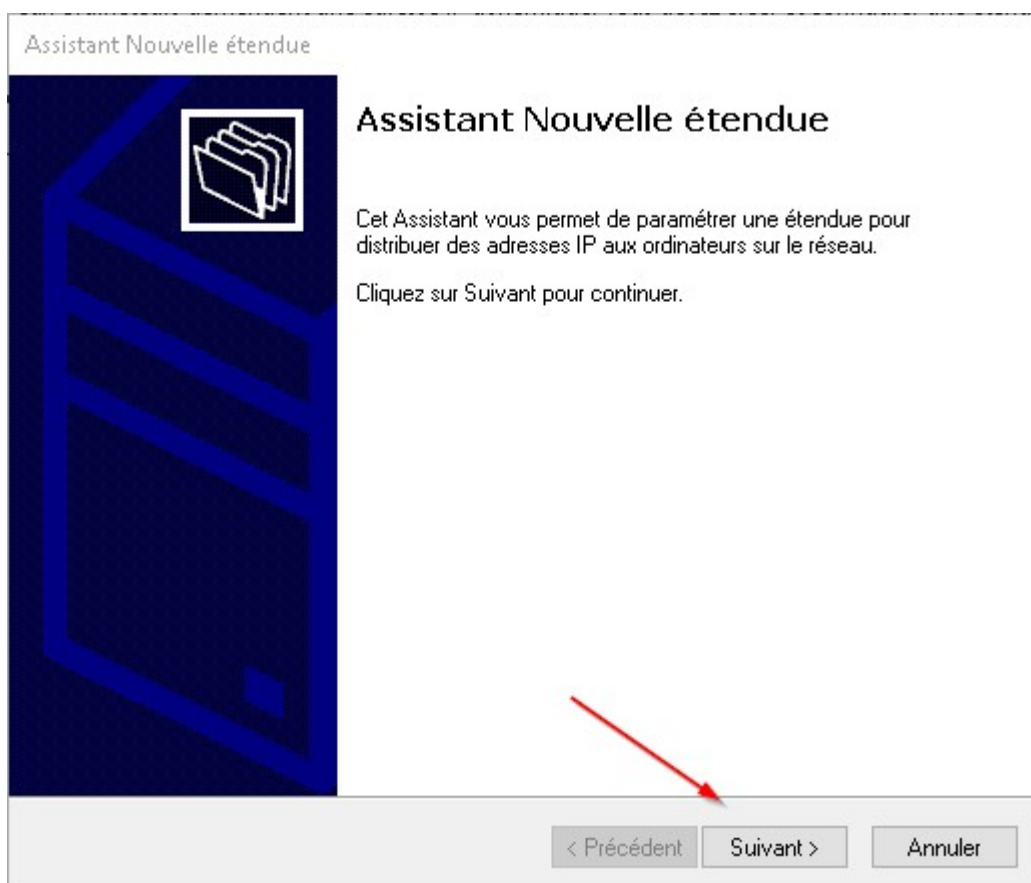
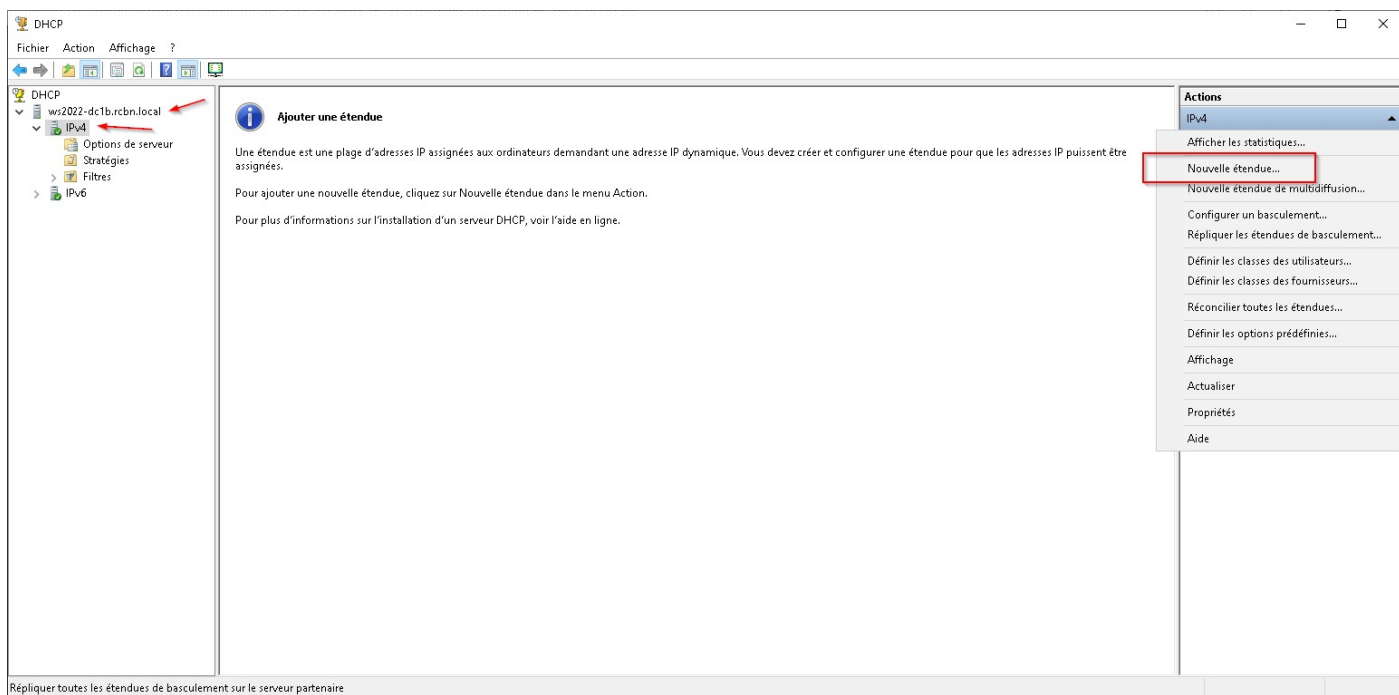




Maintenant on va ajouter une nouvelle extension au DHCP, pour cela aller dans outils puis DHCP.



Ouvrez le dossier IPv4 puis cliquez droit dessus et sélectionnez ensuite « Nouvelle étendue ».



Ajouter un nom ainsi qu'une description.

Assistant Nouvelle étendue

Nom de l'étendue

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.

Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom : MAIN

Description : main DHCP range

< Précédent Suivant > Annuler

Complétez la plage d'adresse IP de l'étendue avec une adresse IP de début et de fin pour le serveur DHCP ainsi que la longueur du masque de sous réseau.

Assistant Nouvelle étendue

Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début : 192 . 168 . 200 . 10

Adresse IP de fin : 192 . 168 . 200 . 199

Paramètres de configuration qui se propagent au client DHCP

Longueur : 24

Masque de sous-réseau : 255 . 255 . 255 . 0

< Précédent Suivant > Annuler

Assistant Nouvelle étendue

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCP OFFER.

Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début : Adresse IP de fin :

Plage d'adresses exclue :

Retard du sous-réseau en millisecondes :

Assistant Nouvelle étendue

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

Cochez la première option puis cliquez sur suivante.

Assistant Nouvelle étendue

Configuration des paramètres DHCP

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.

Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

☒ Oui, je veux configurer ces options maintenant

☐ Non, je configurerai ces options ultérieurement

< Précédent Suivant > Annuler

Ajoutez l'adresse IP du routeur.

Assistant Nouvelle étendue

Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.

Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

Ajouter

Supprimer

Monter

Descendre

< Précédent Suivant > Annuler

Ajoutez d'abord le nom du domaine parent et ensuite l'adresse IP des serveurs DNS.

Assistant Nouvelle étendue

Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.

Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :	Adresse IP :	
<input type="text"/>	<input type="text" value=" . . ."/>	Ajouter
<input type="button" value="Résoudre"/>	192.168.200.200 192.168.200.201	Supprimer
		Monter
		Descendre

< Précédent Suivant > Annuler

Assistant Nouvelle étendue

Serveurs WINS

Les ordinateurs fonctionnant avec Windows peuvent utiliser les serveurs WINS pour convertir les noms NetBIOS d'ordinateurs en adresses IP.

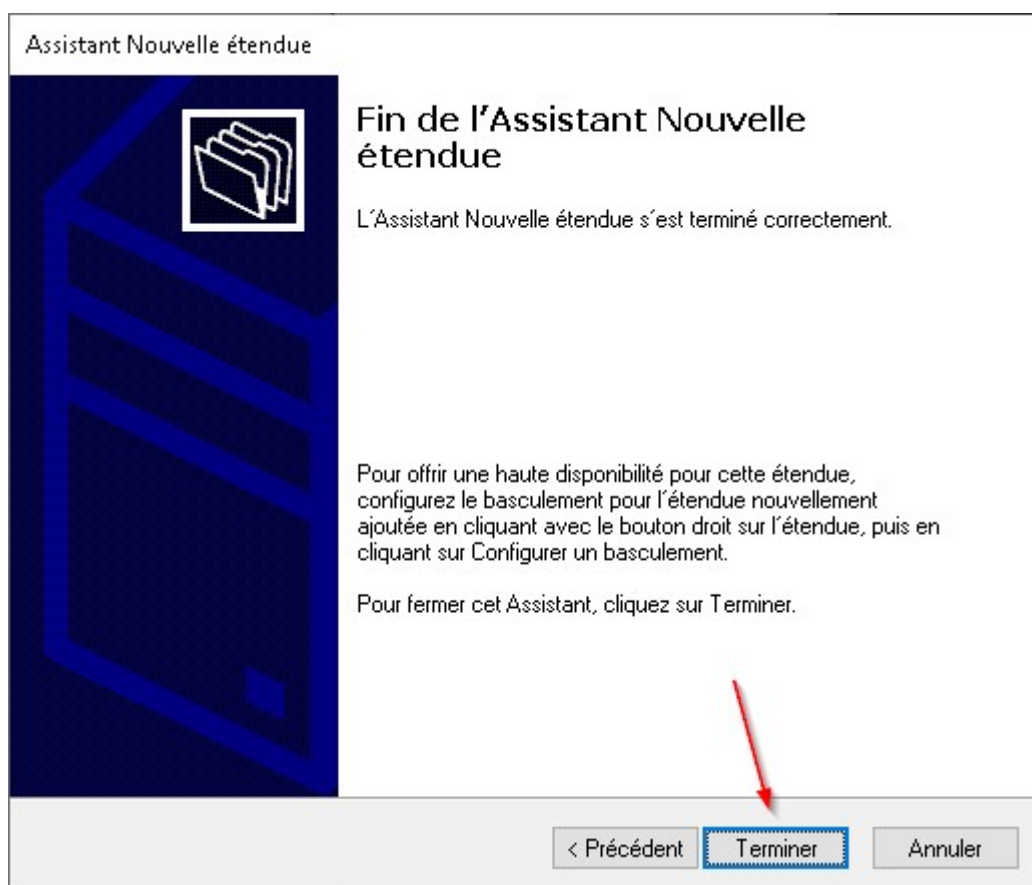
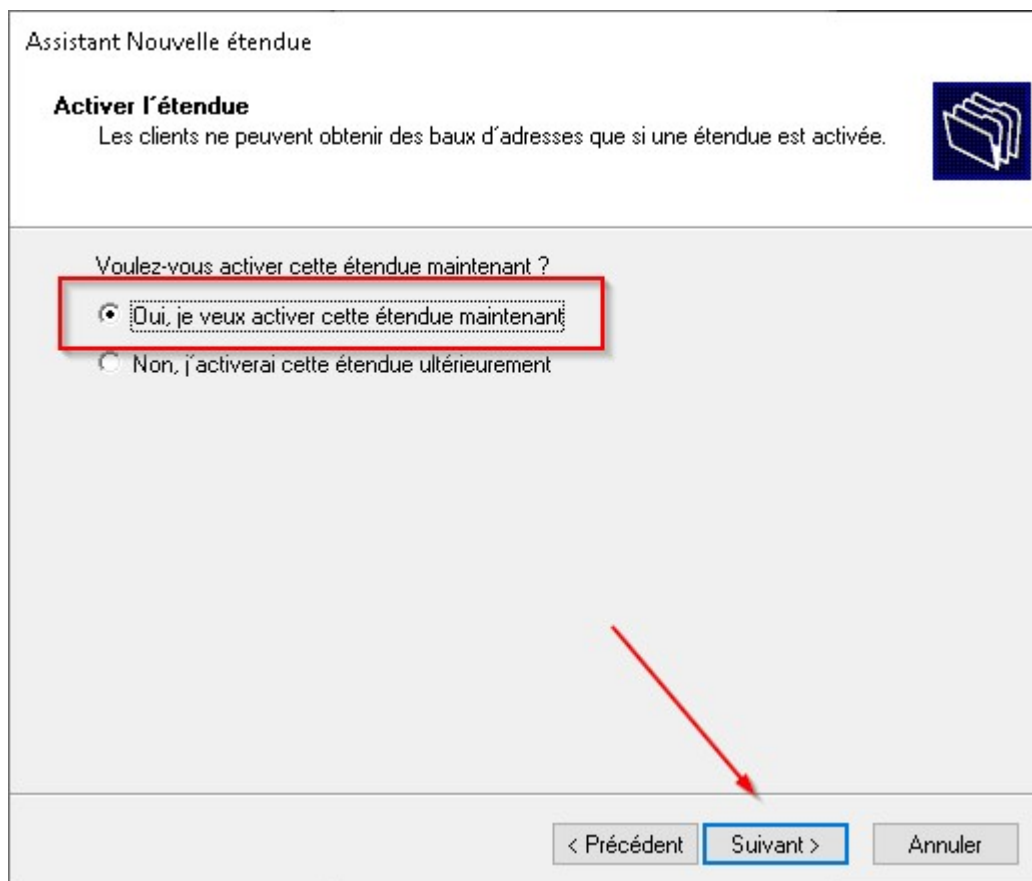
Entrer les adresses IP ici permet aux clients Windows d'interroger WINS avant d'utiliser la diffusion pour s'enregistrer et résoudre les noms NetBIOS.

Nom du serveur :	Adresse IP :	
<input type="text"/>	<input type="text" value=" . . ."/>	Ajouter
<input type="button" value="Résoudre"/>		Supprimer
		Monter
		Descendre

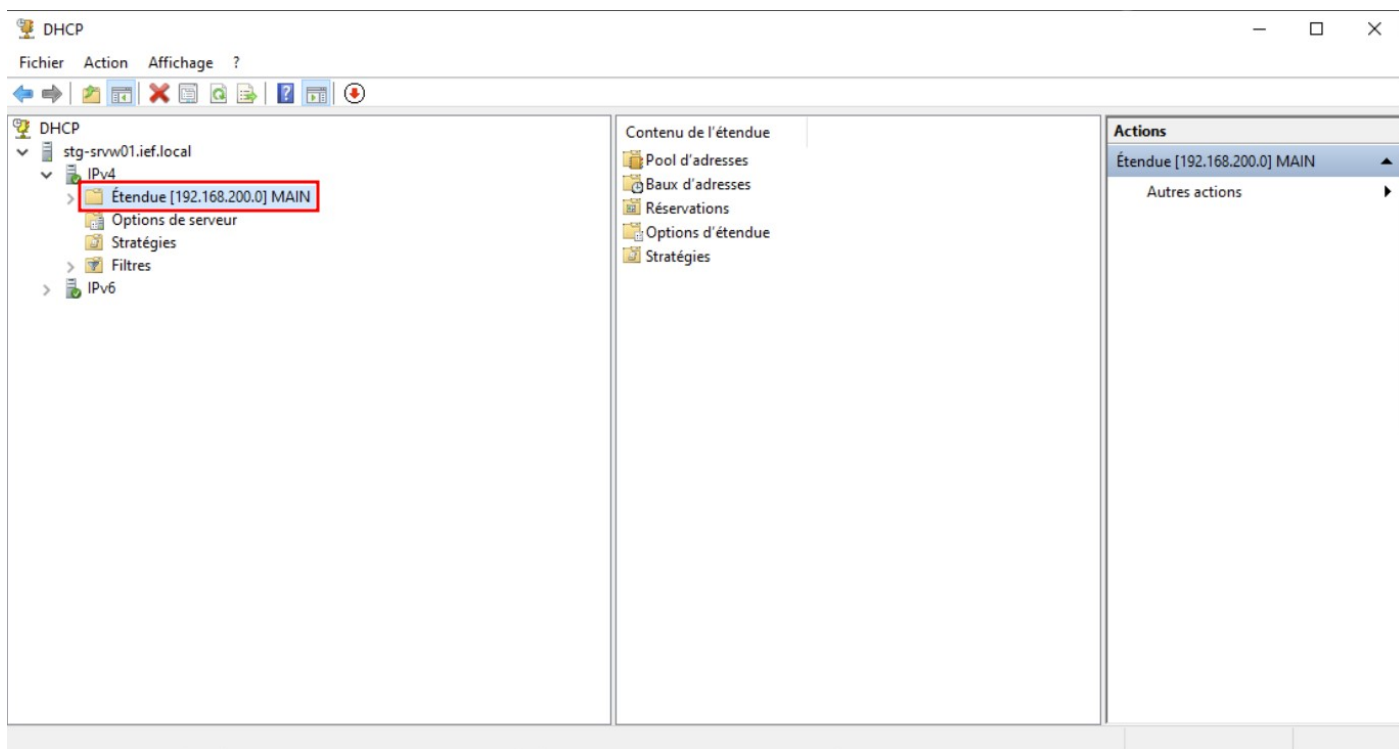
Pour modifier ce comportement pour les clients DHCP Windows, modifiez l'option 046, type de nœud WINS/NBT, dans les options de l'étendue.

< Précédent **Suivant >** Annuler

Sélectionnez la première option.



Maintenant dans le dossier IPv4 on aperçoit l'étendue qu'on vient de créer.



Windows Server Site B

Configuration - Jonction au domaine AD, mise en place des rôles DC2

Introduction

Ce deuxième document couvre la procédure d'installation des différents rôles nécessaires à la mise en place d'un domaine AD.

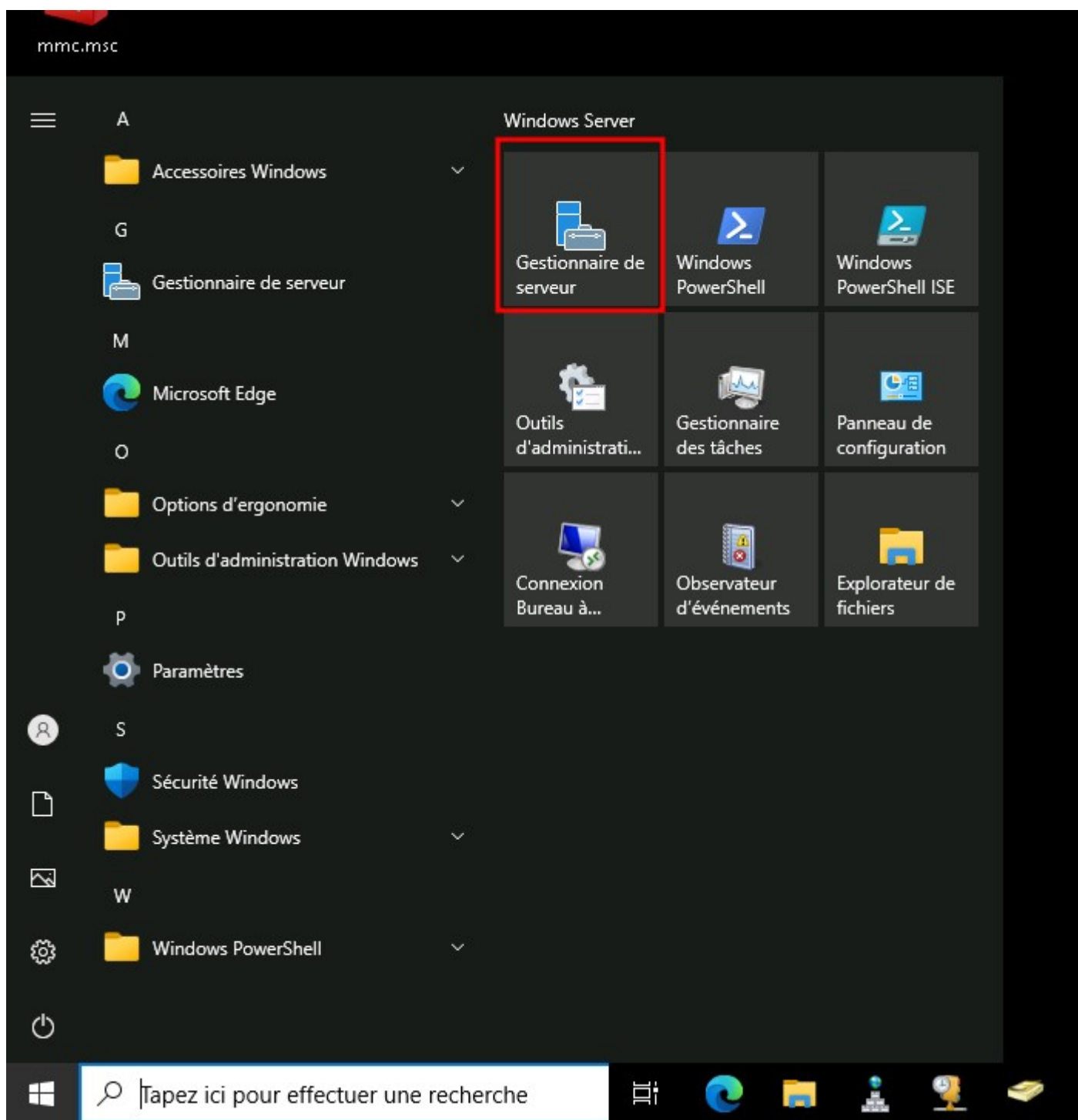
1. Installation des rôles AD, DNS, DHCP.
2. Configuration initiale du domaine

Pour ce faire, vous aurez besoin des éléments suivants :

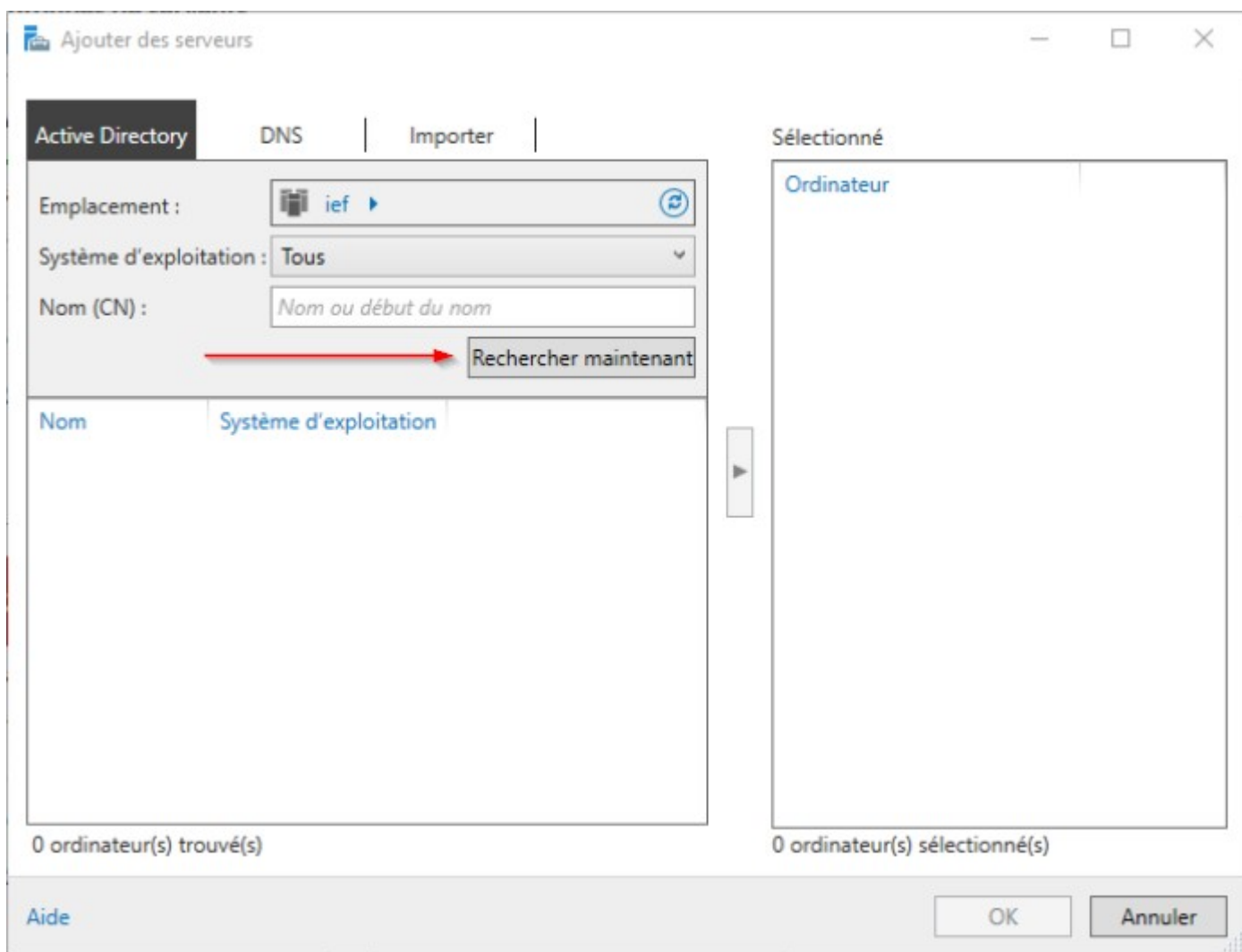
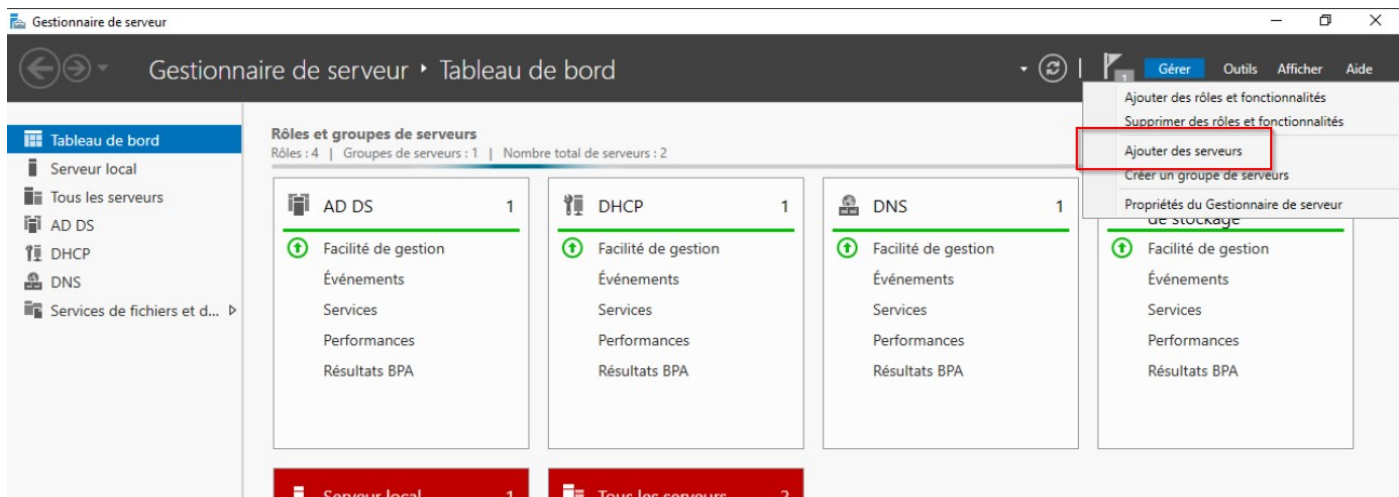
- Machine virtuelle Windows Server 2022
- Compte d'administration du serveur
- Serveur correctement nommé

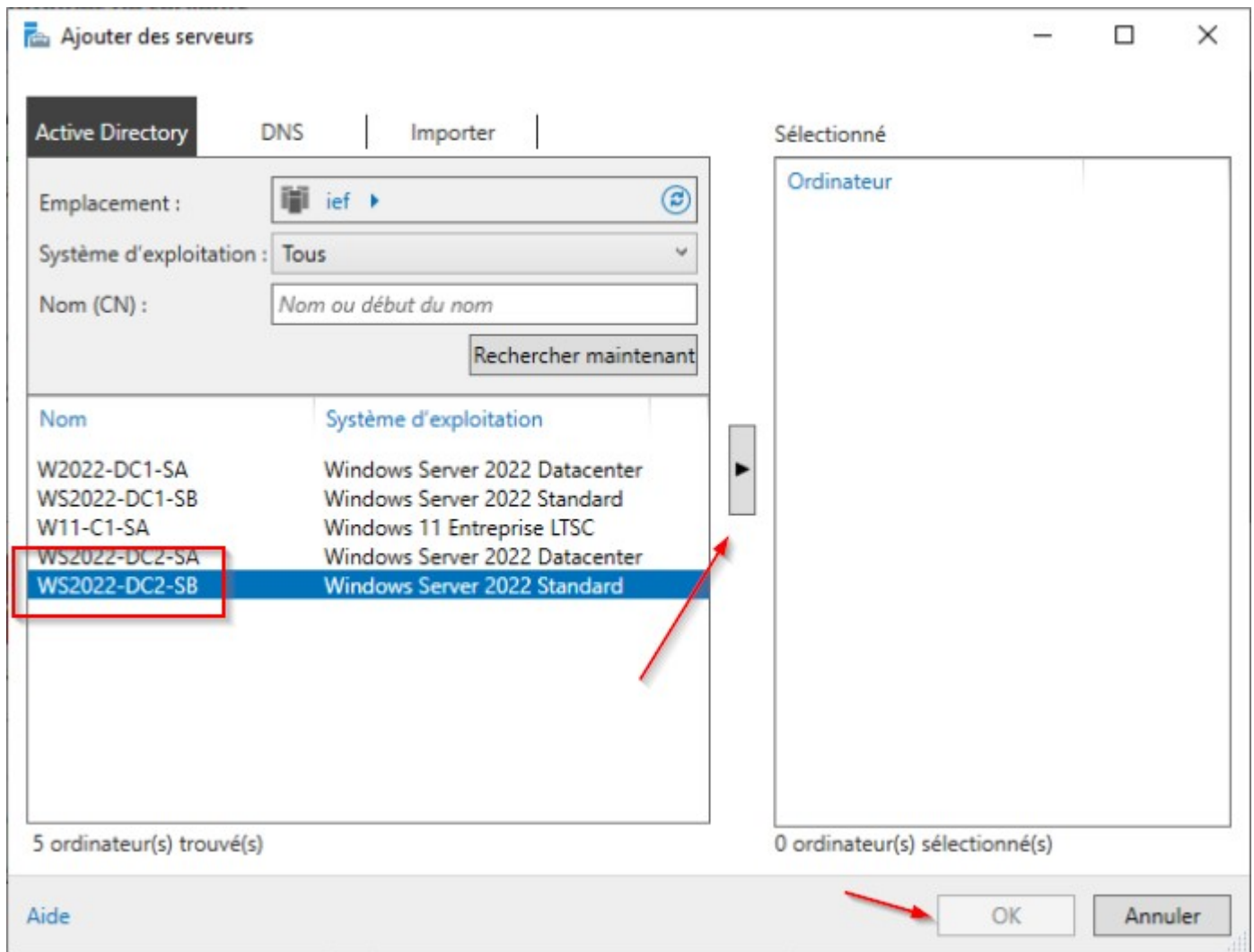
1) Installation des rôles

Pour installer des rôles de serveur, vous devez lancer le gestionnaire de serveur, trouvable dans le menu démarrer du serveur.

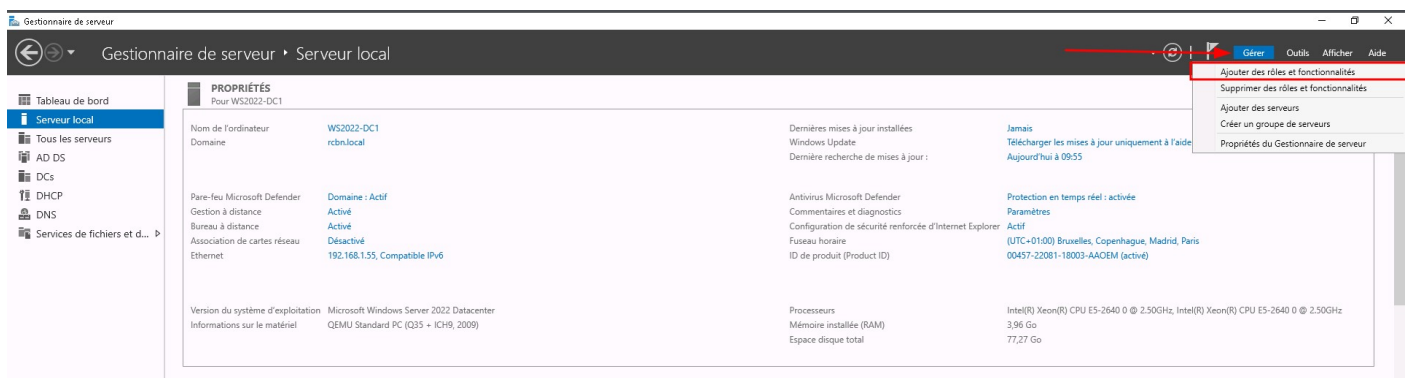


Vous devez ajouté le serveur nouvellement ajouté au domaine dans le gestionnaire de serveur pour installer des rôles dessus

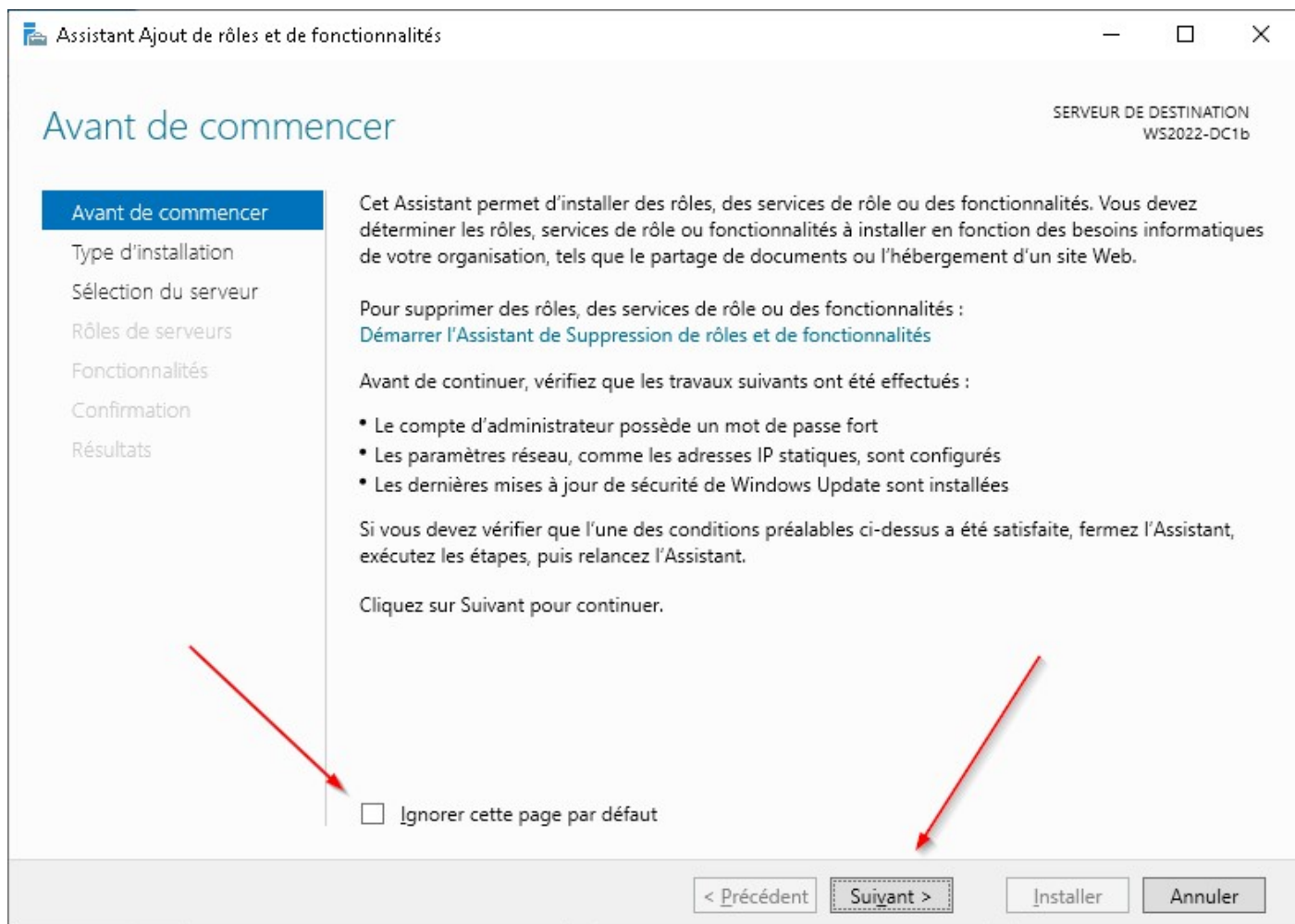




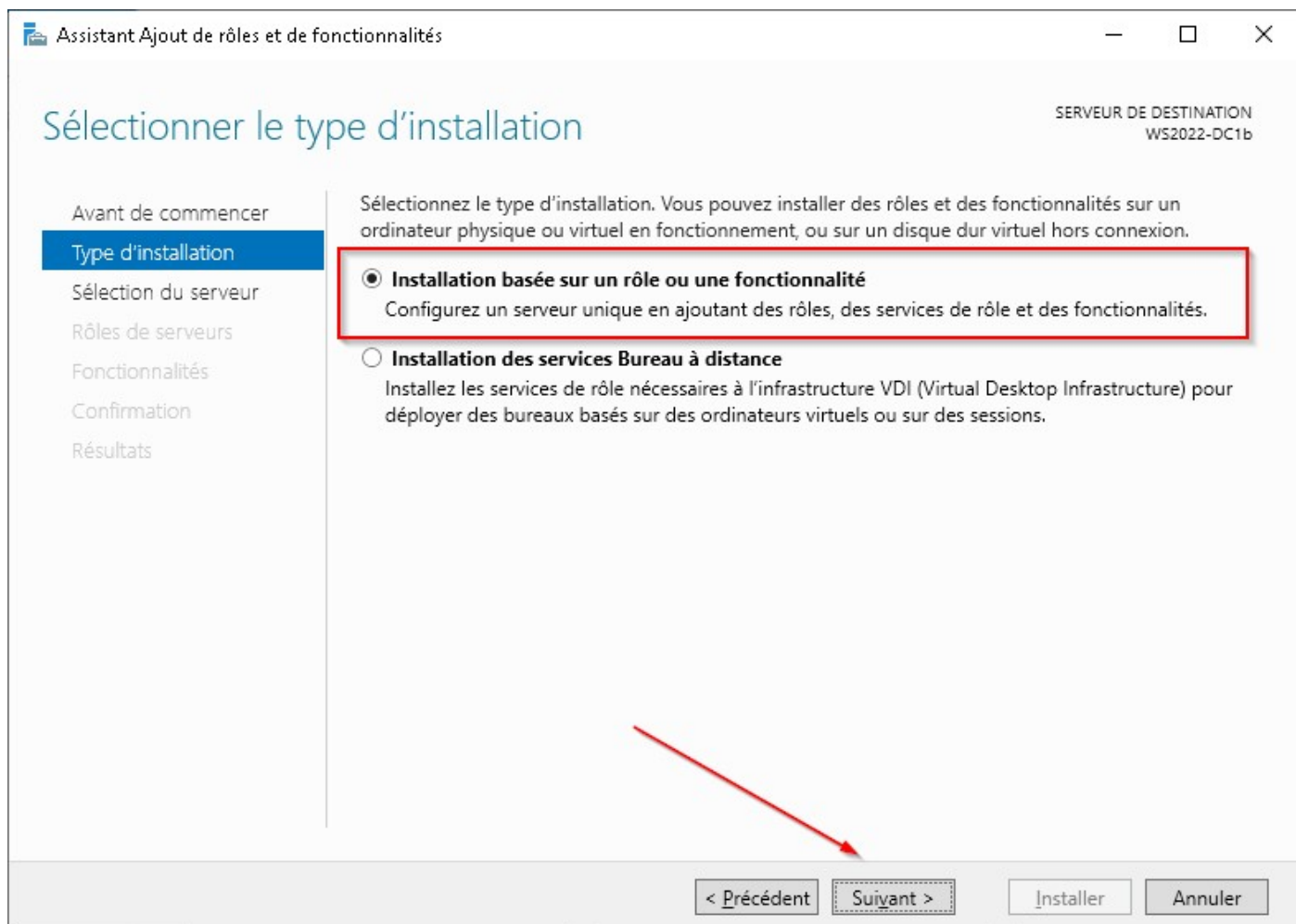
Cliquez ensuite sur gérer, puis "Ajouter des rôles et des fonctionnalités"



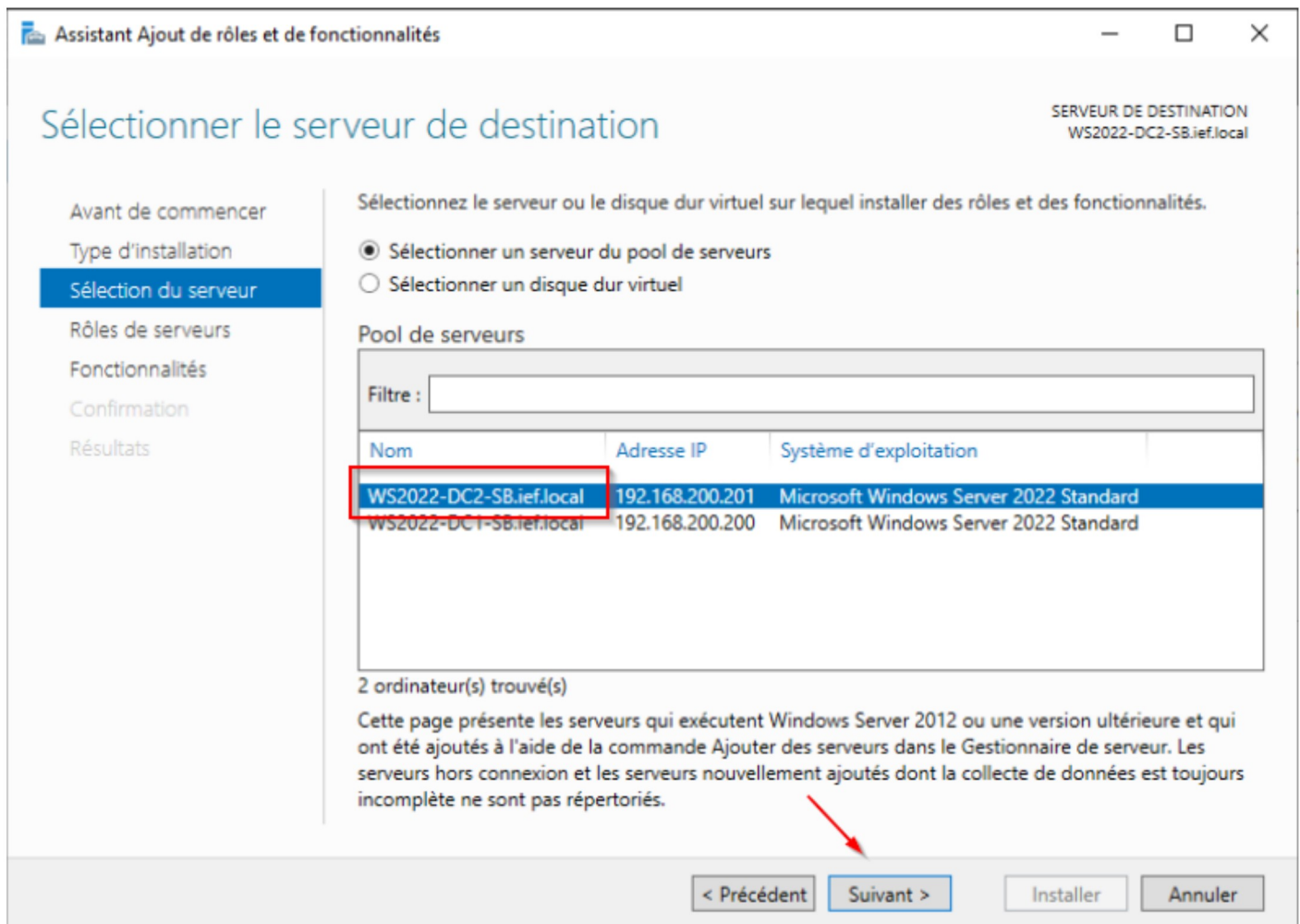
Vous voici sur la page d'accueil de l'assistant. Vous pouvez cocher (ou non) la case pour ignorer l'introduction de l'assistant. Cliquez ensuite sur suivant.



Vérifiez ensuite que la première option est bien celle cochée dans la fenêtre qui suit

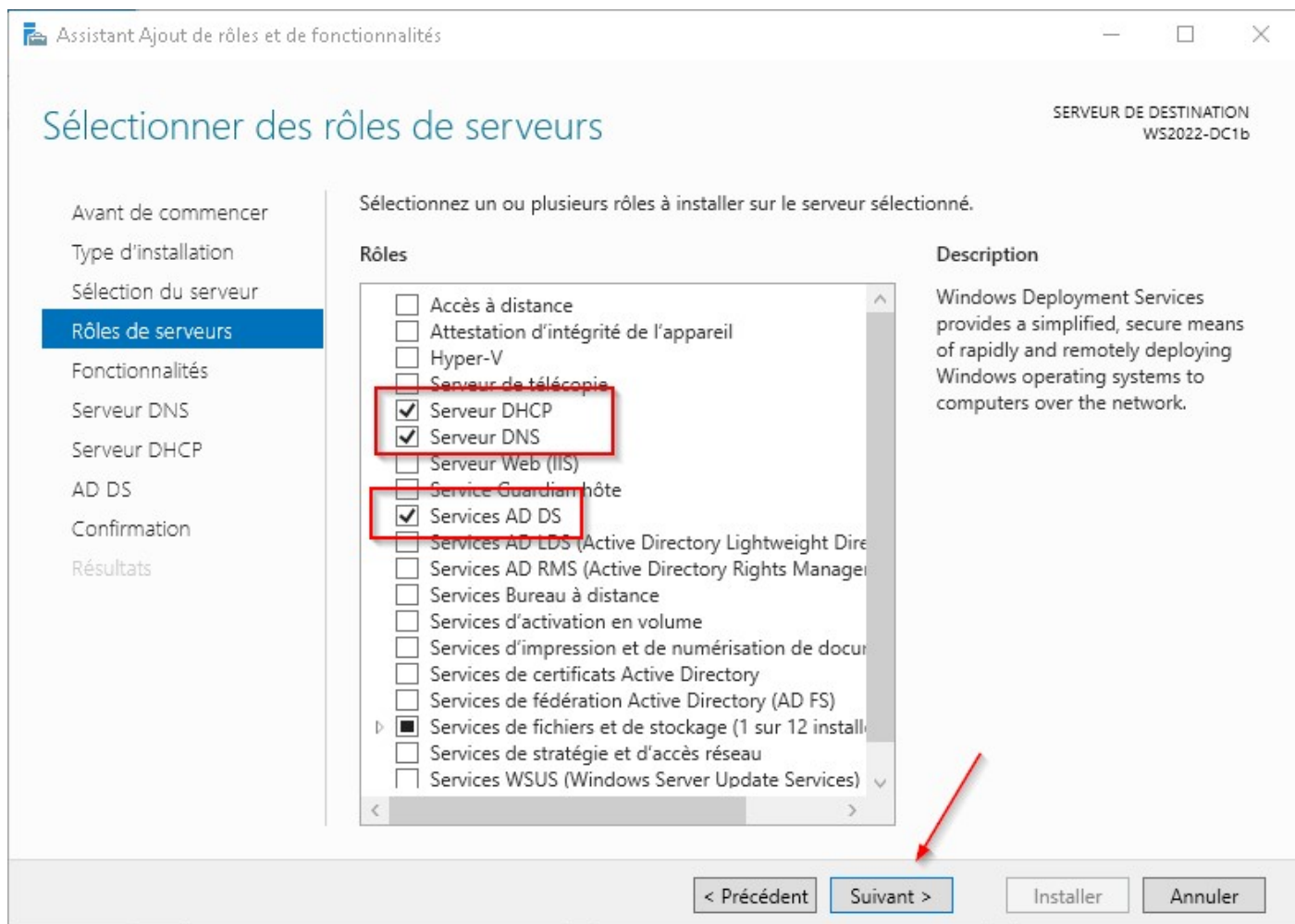


Sélectionnez les paramètres régionaux de votre machine, et cliquez sur suivant

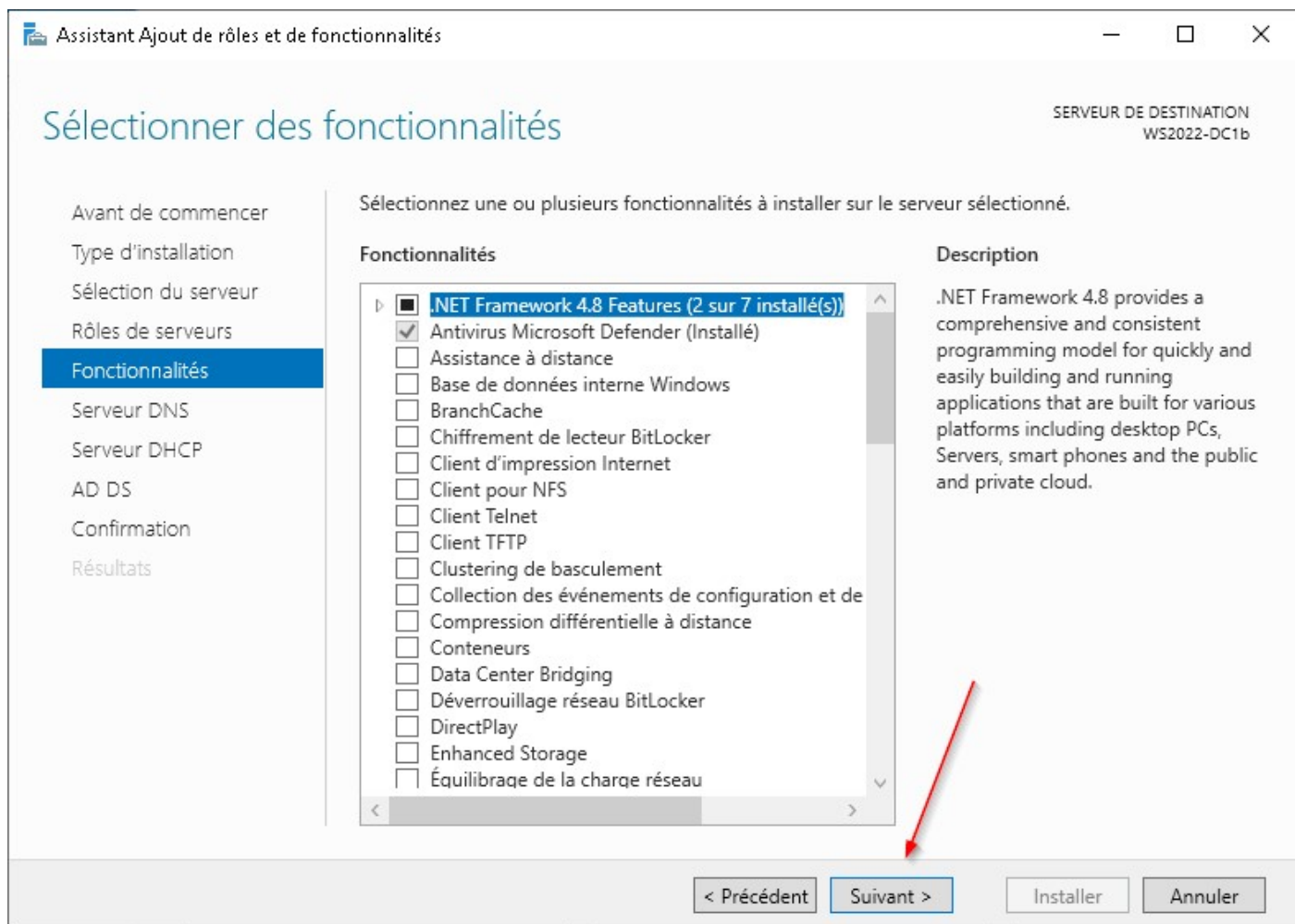


Si votre machine fait partie d'un Pool de Serveurs, pensez à vérifier son nom pour être sûr d'agir sur la bonne machine.

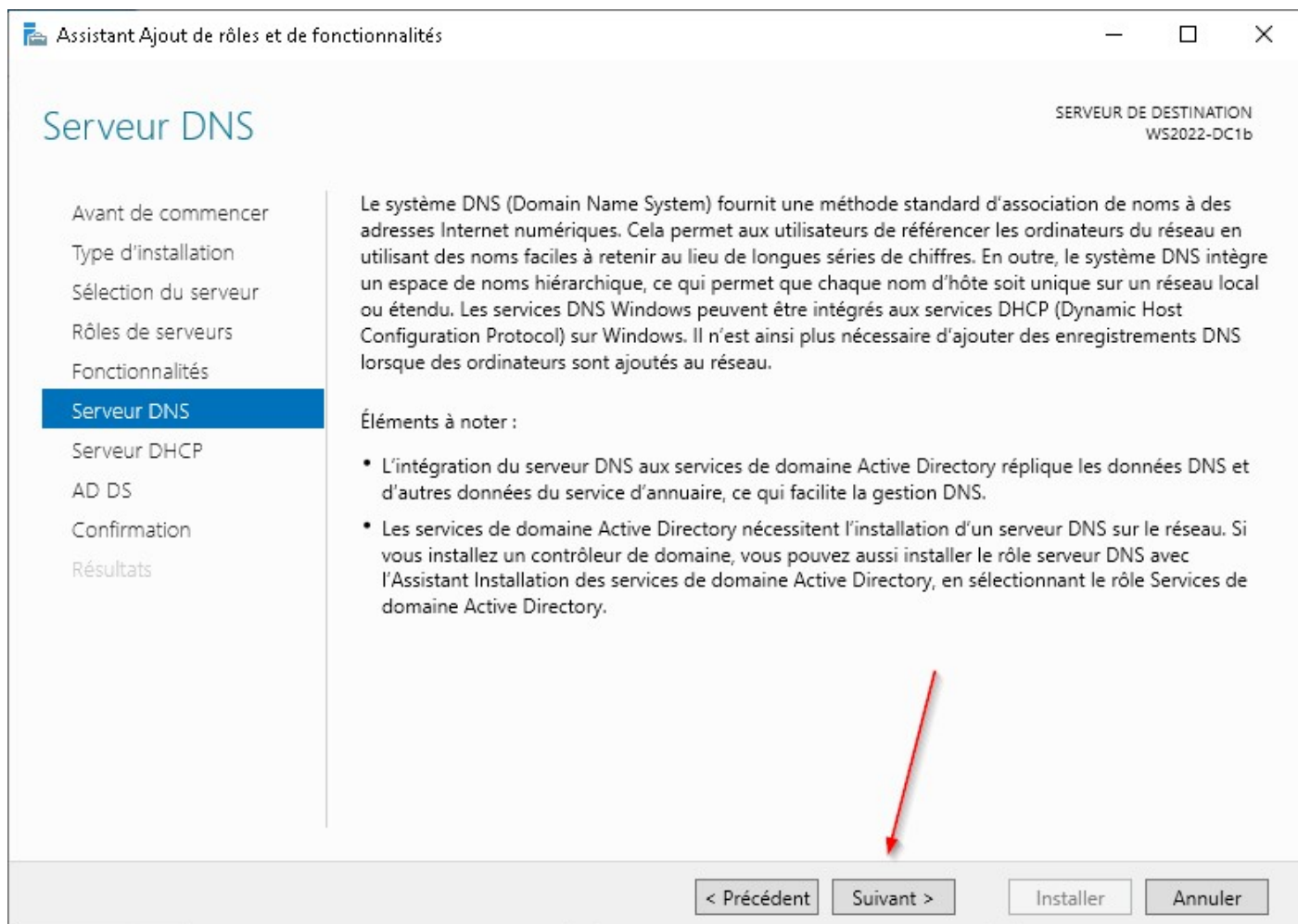
Sélectionnez les rôles nécessaires. Dans notre cas, nous allons utiliser notre serveur pour AD et DHCP, Il faut donc activer les rôles DNS, DHCP et AD DS.

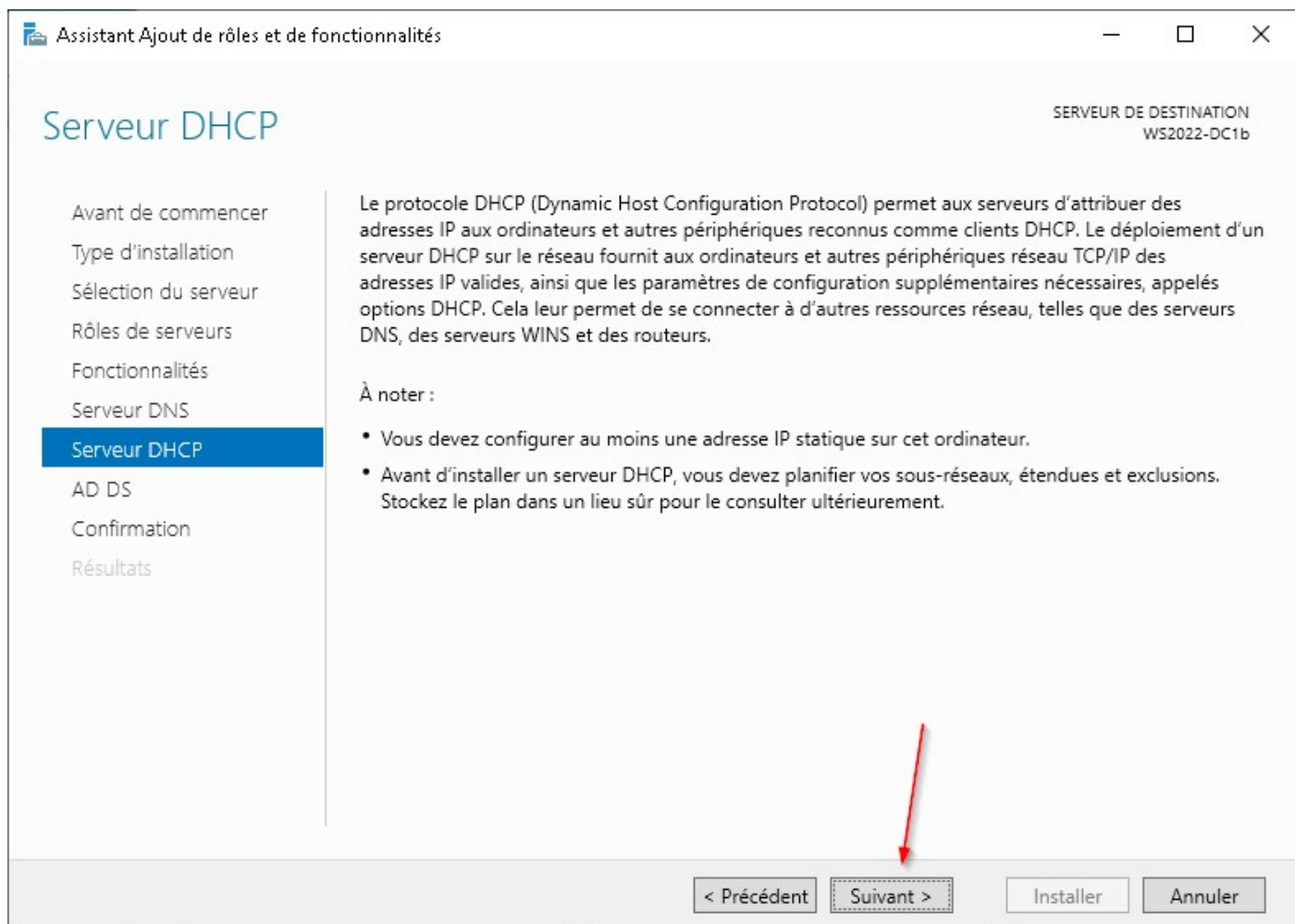


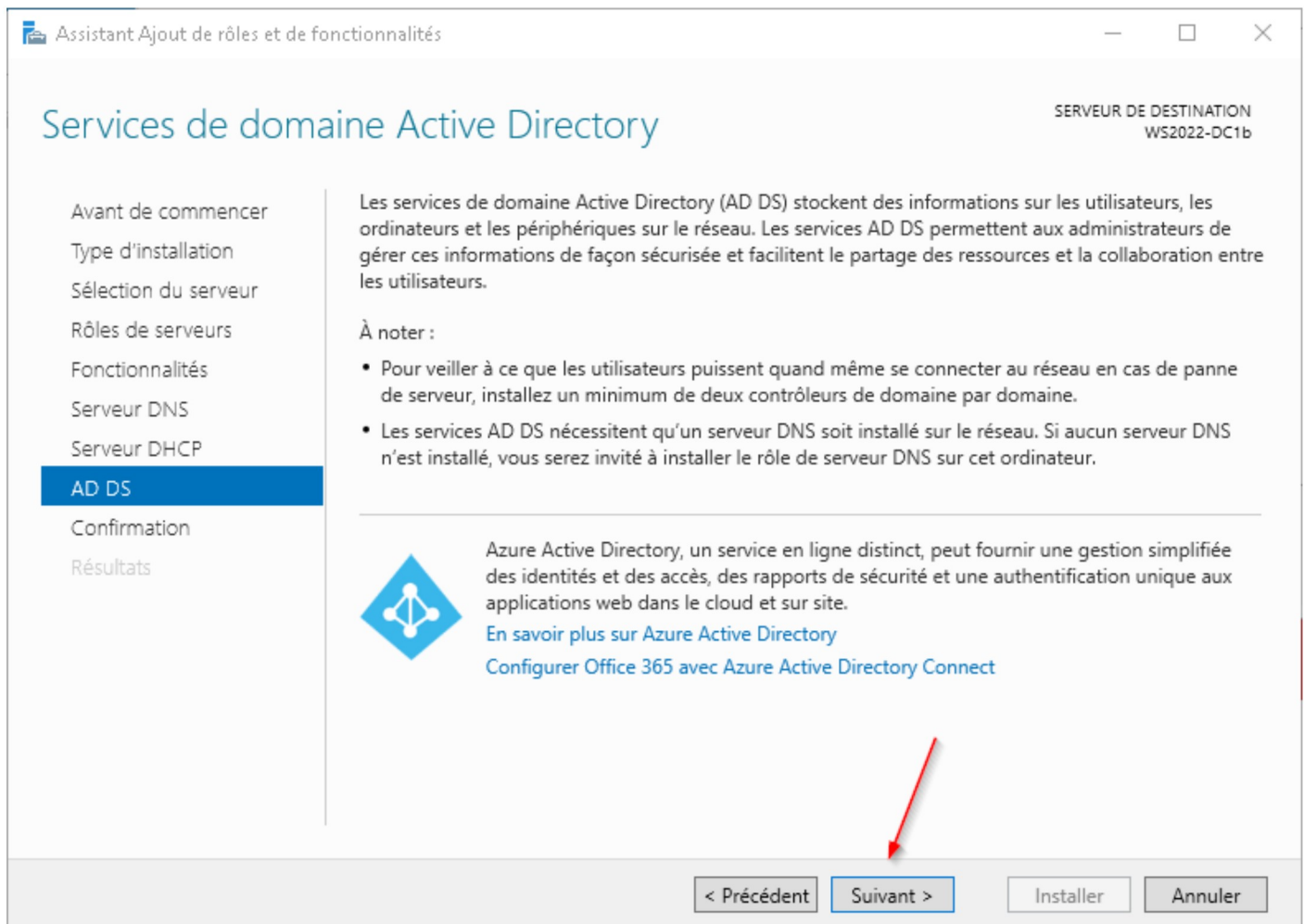
Aucun besoin d'ajouter des fonctionnalités, elles ont déjà été auto-sélectionnées par Windows lors de la sélection des rôles.



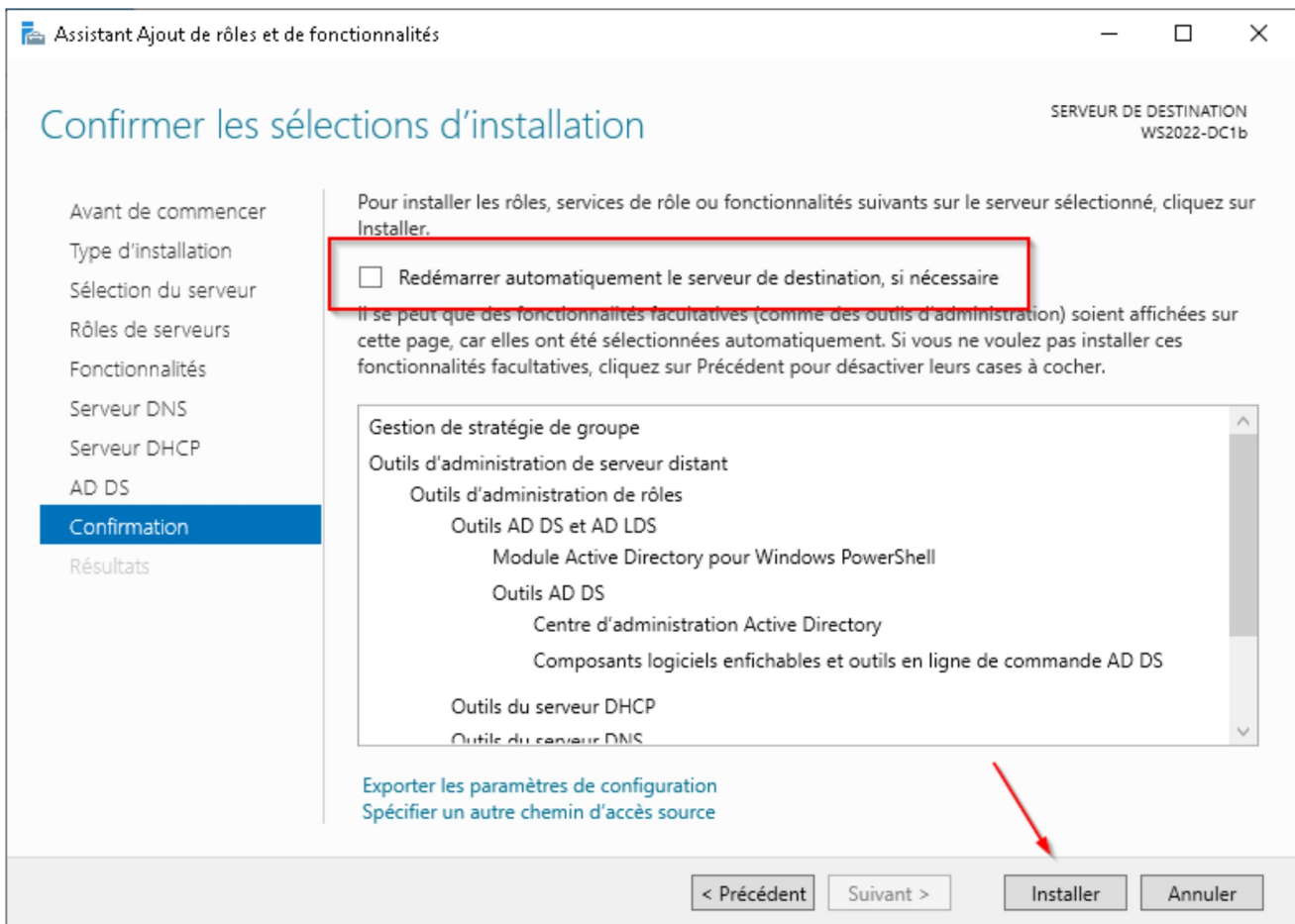
3 fenêtres d'information vont se suivre.



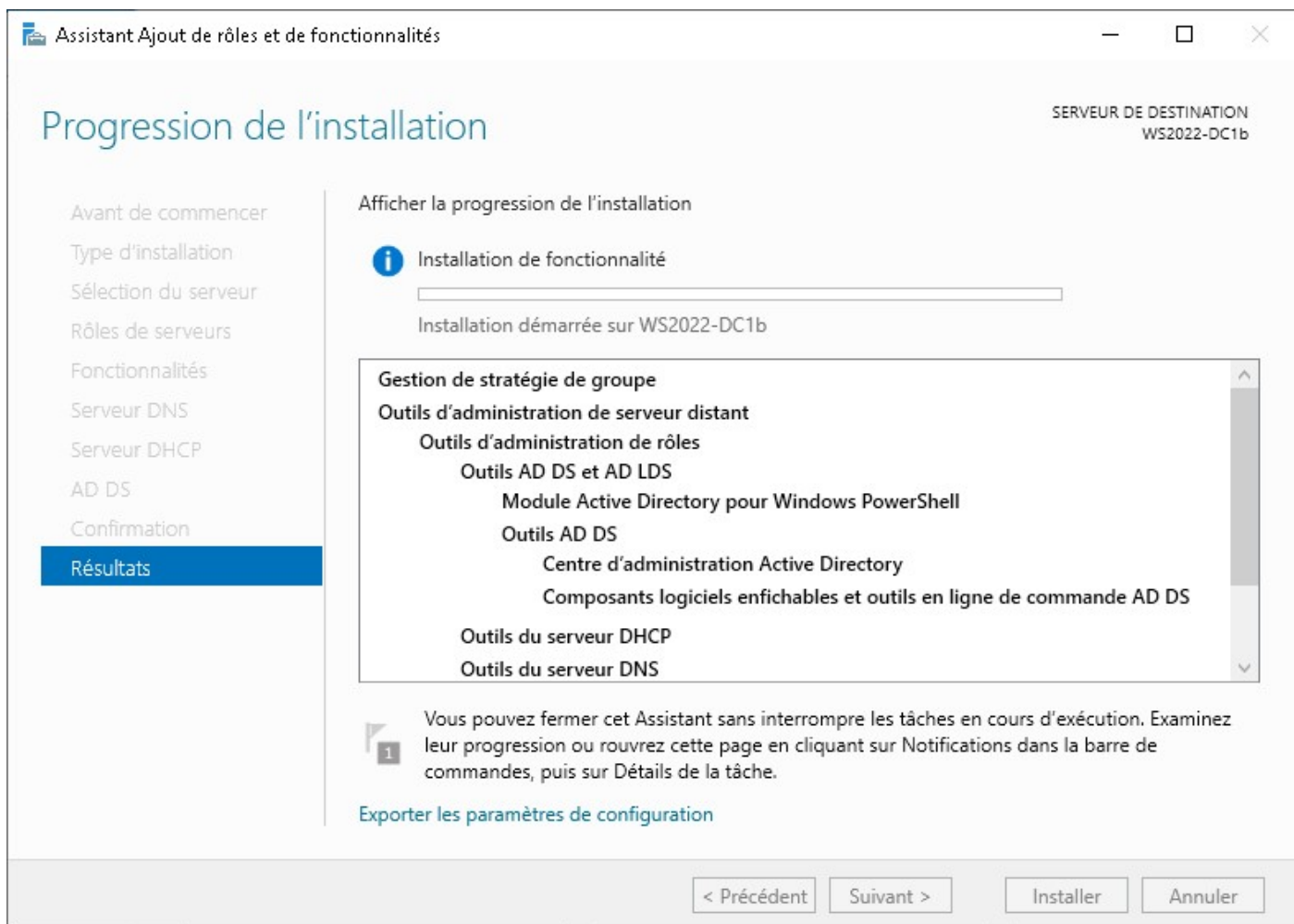




Décochez ensuite la case pour redémarrer la machine, et cliquez sur installer

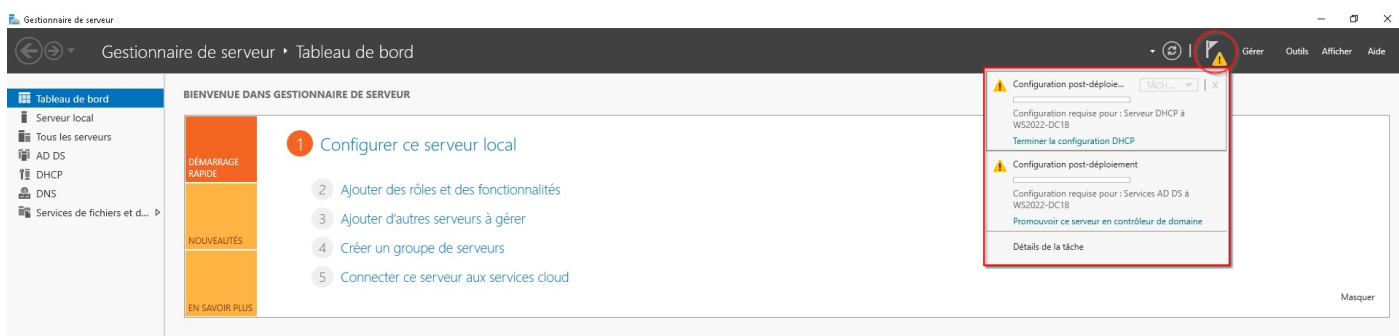


L'installation démarre.



2) Configuration des rôles.

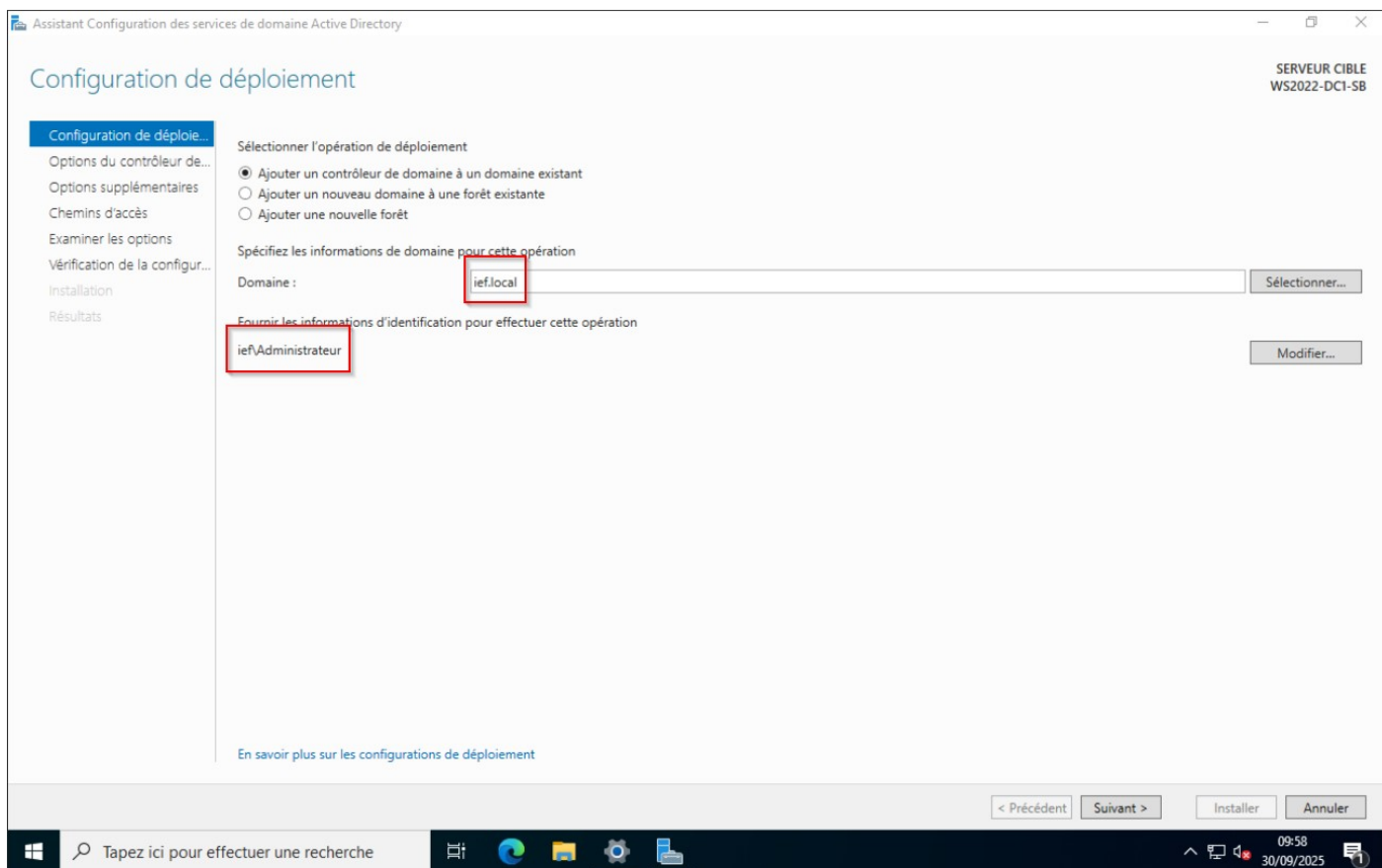
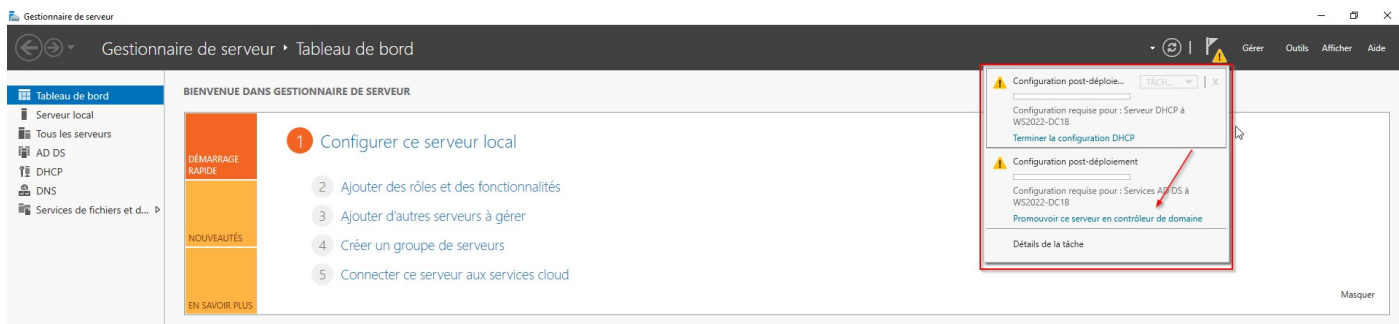
Une fois redémarré, lancez le gestionnaire de serveur, et cliquez sur le drapeau en haut à droite.

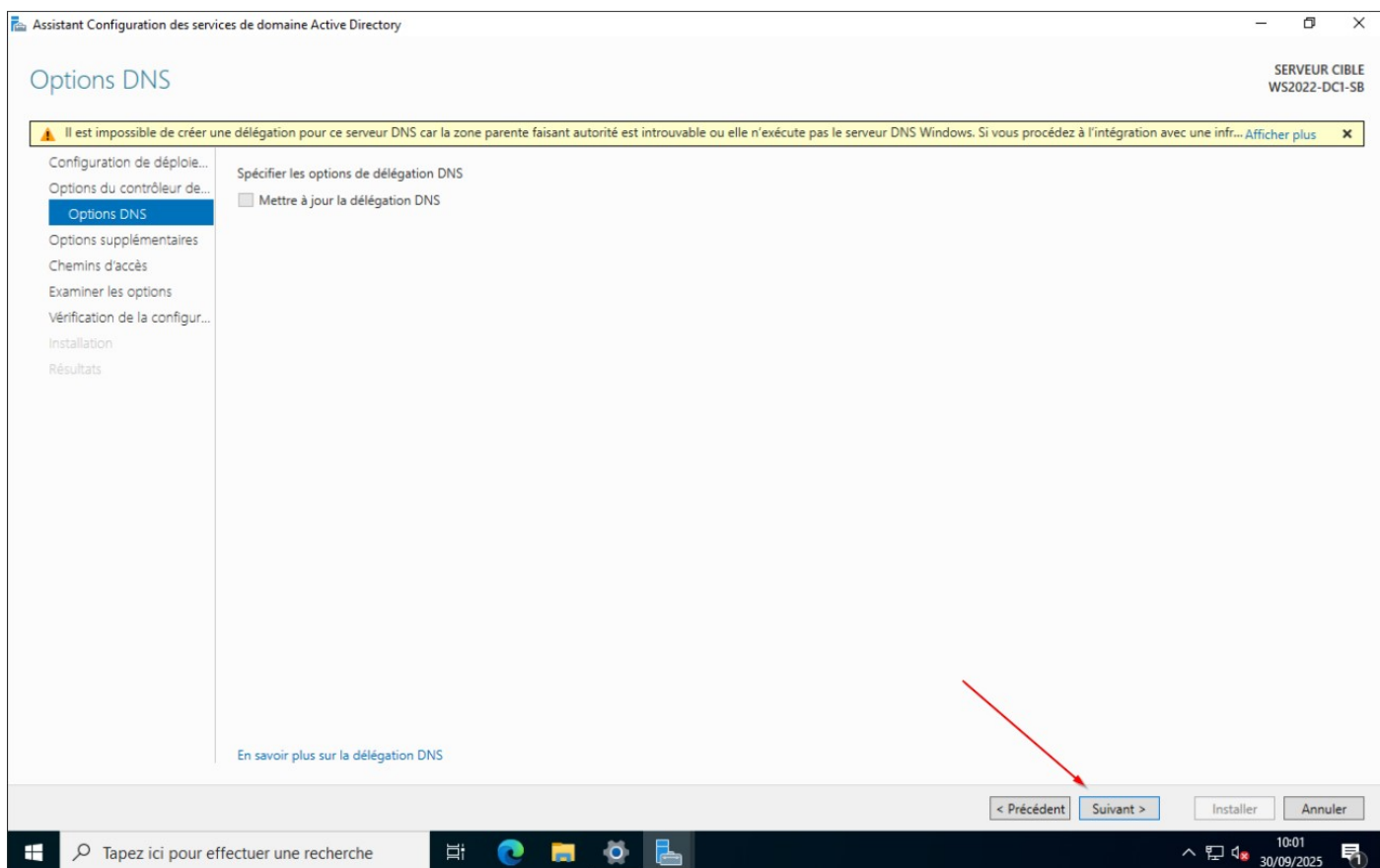
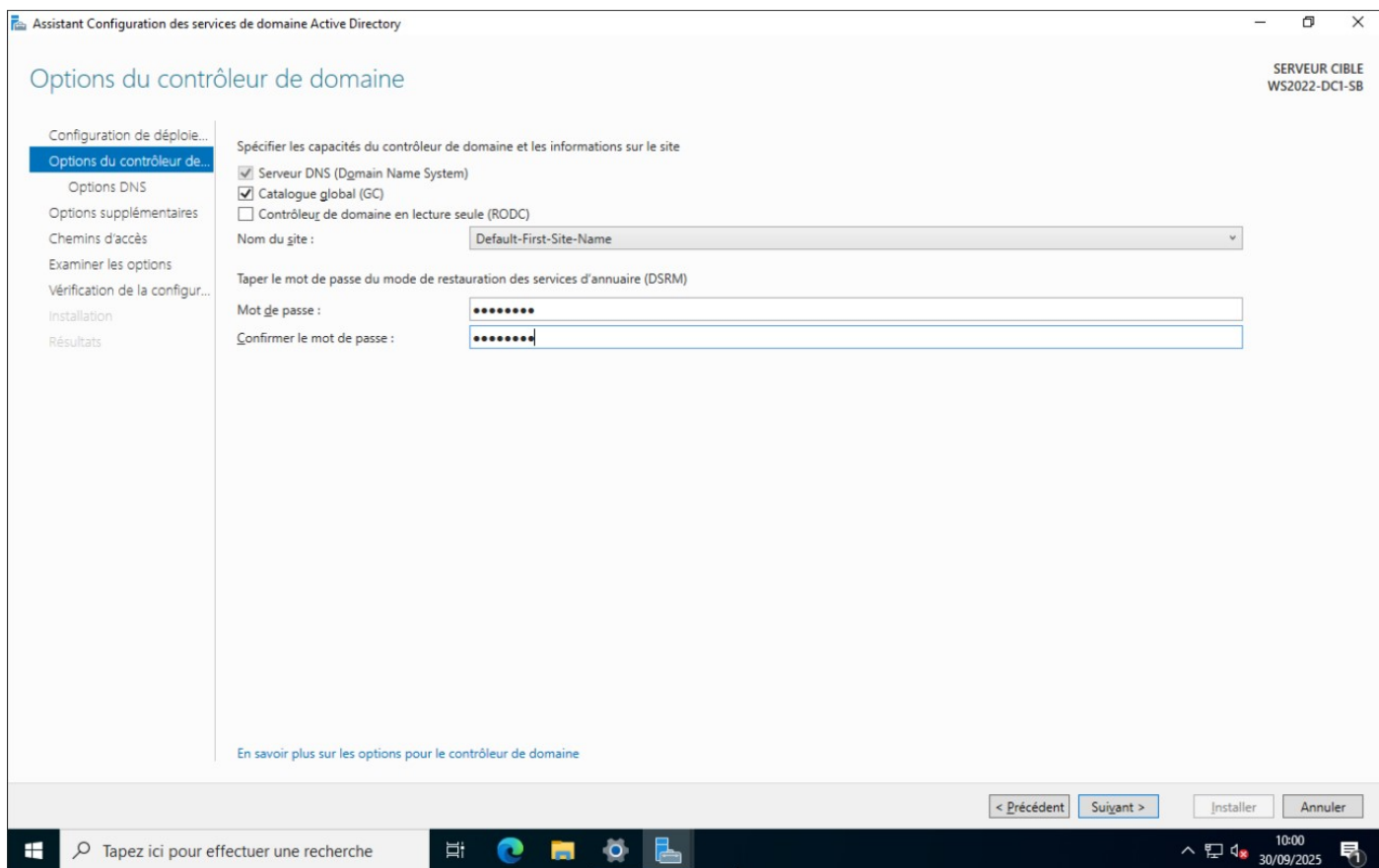


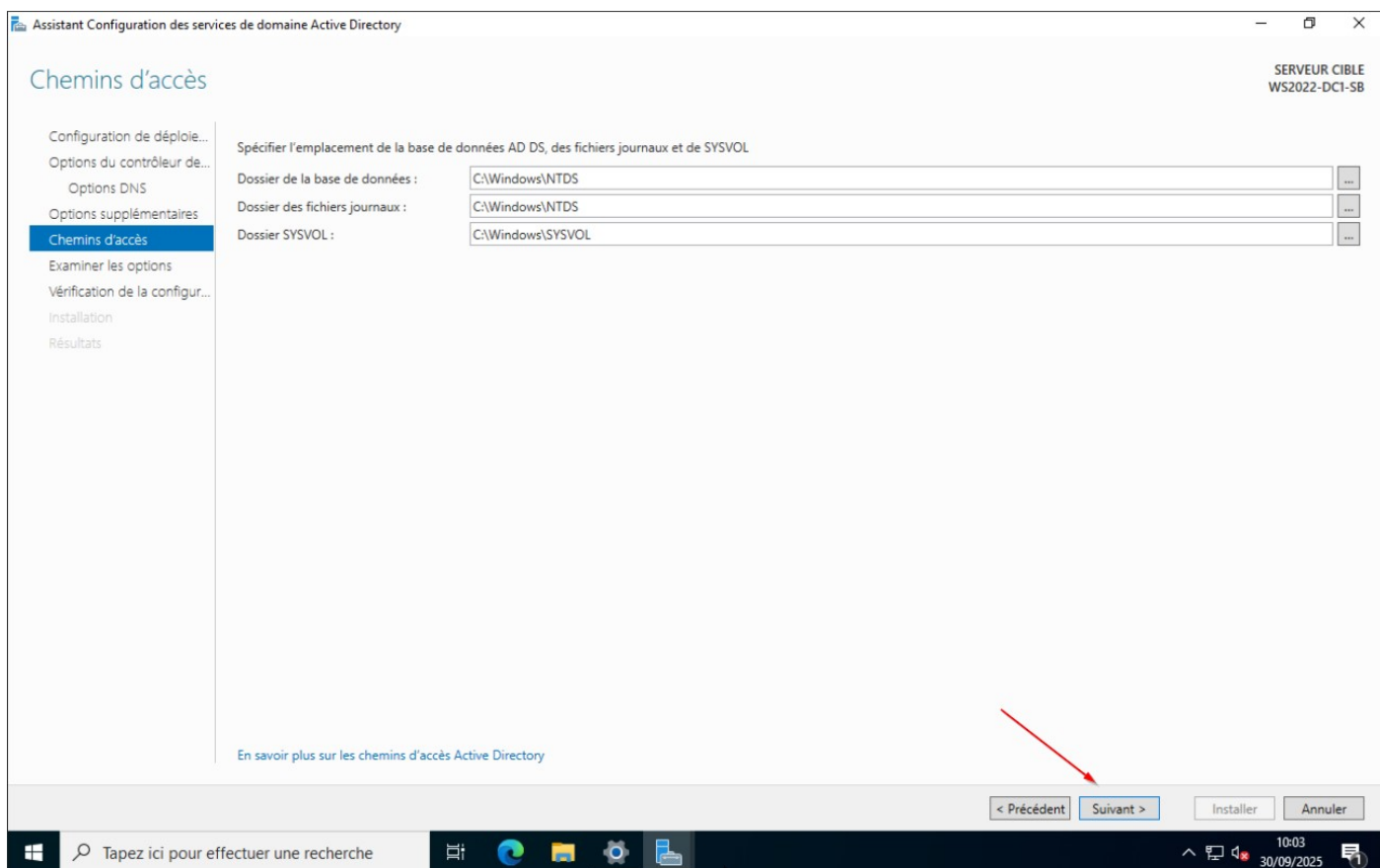
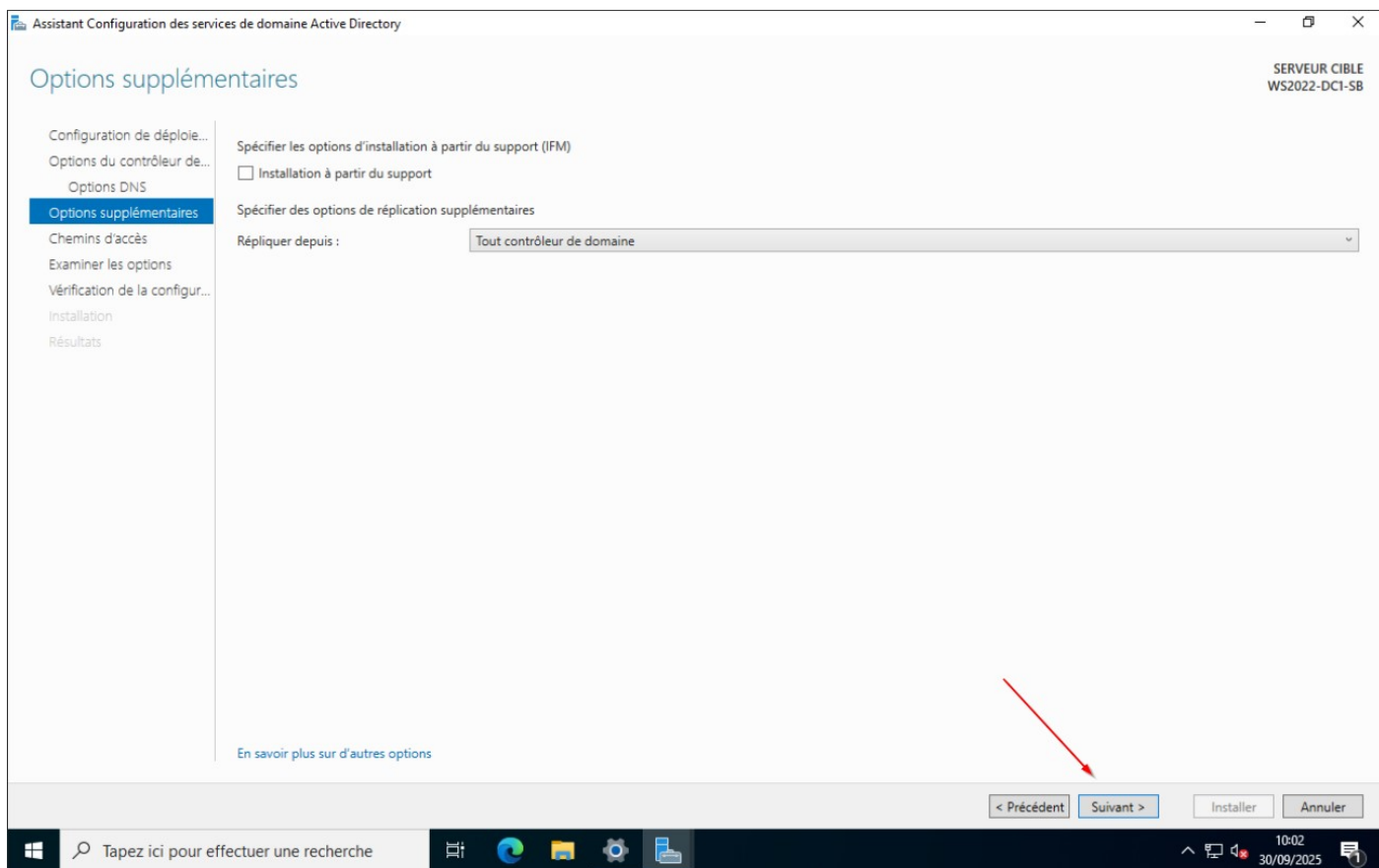
Vous verrez les tâches de configuration en suspens.

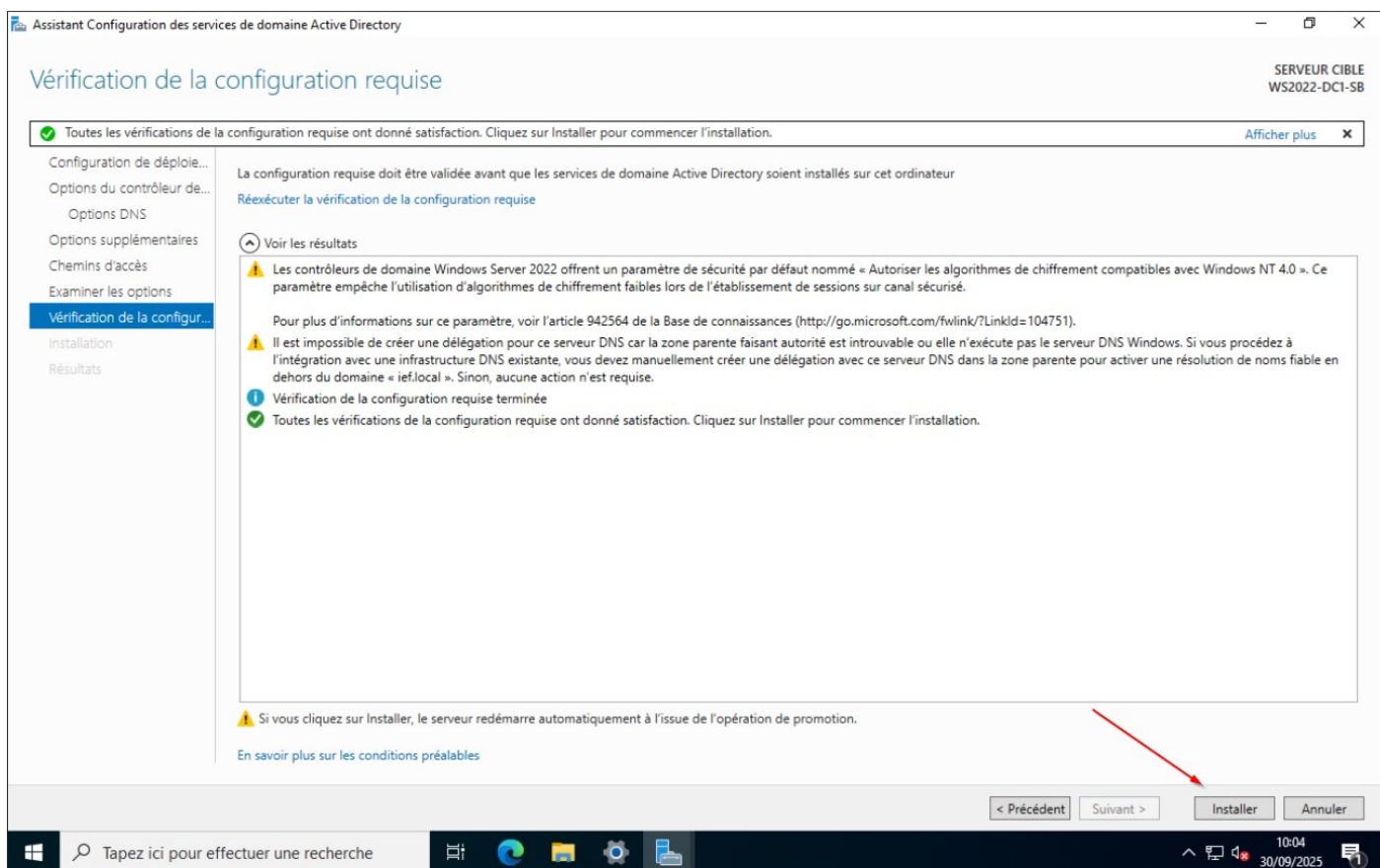
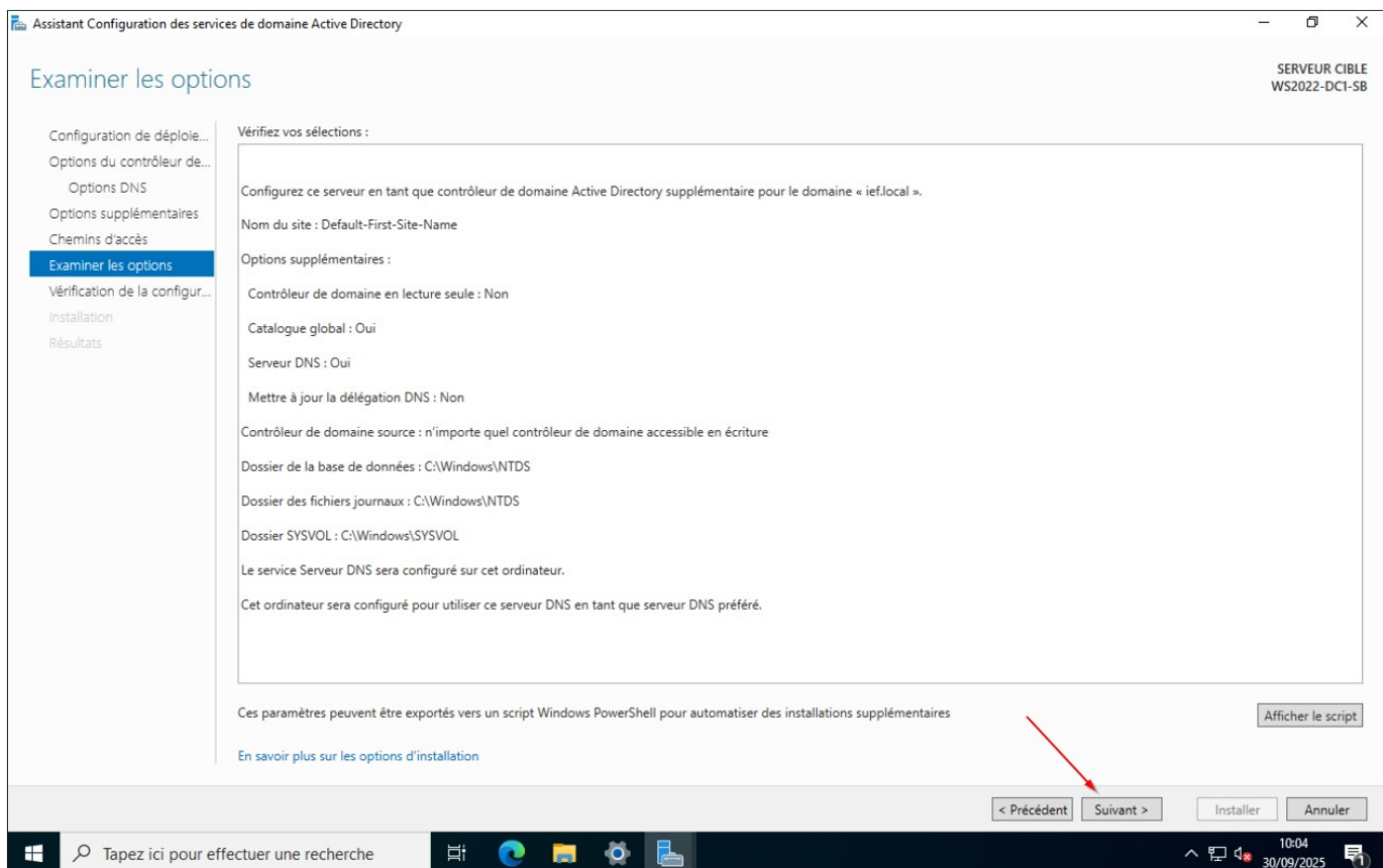
A. Configuration d'AD DS et jonction au domaine

Revenez dans le menu déroulant sous le drapeau du gestionnaire de serveur, et cliquez sur "Promouvoir ce serveur en contrôleur de domaine"



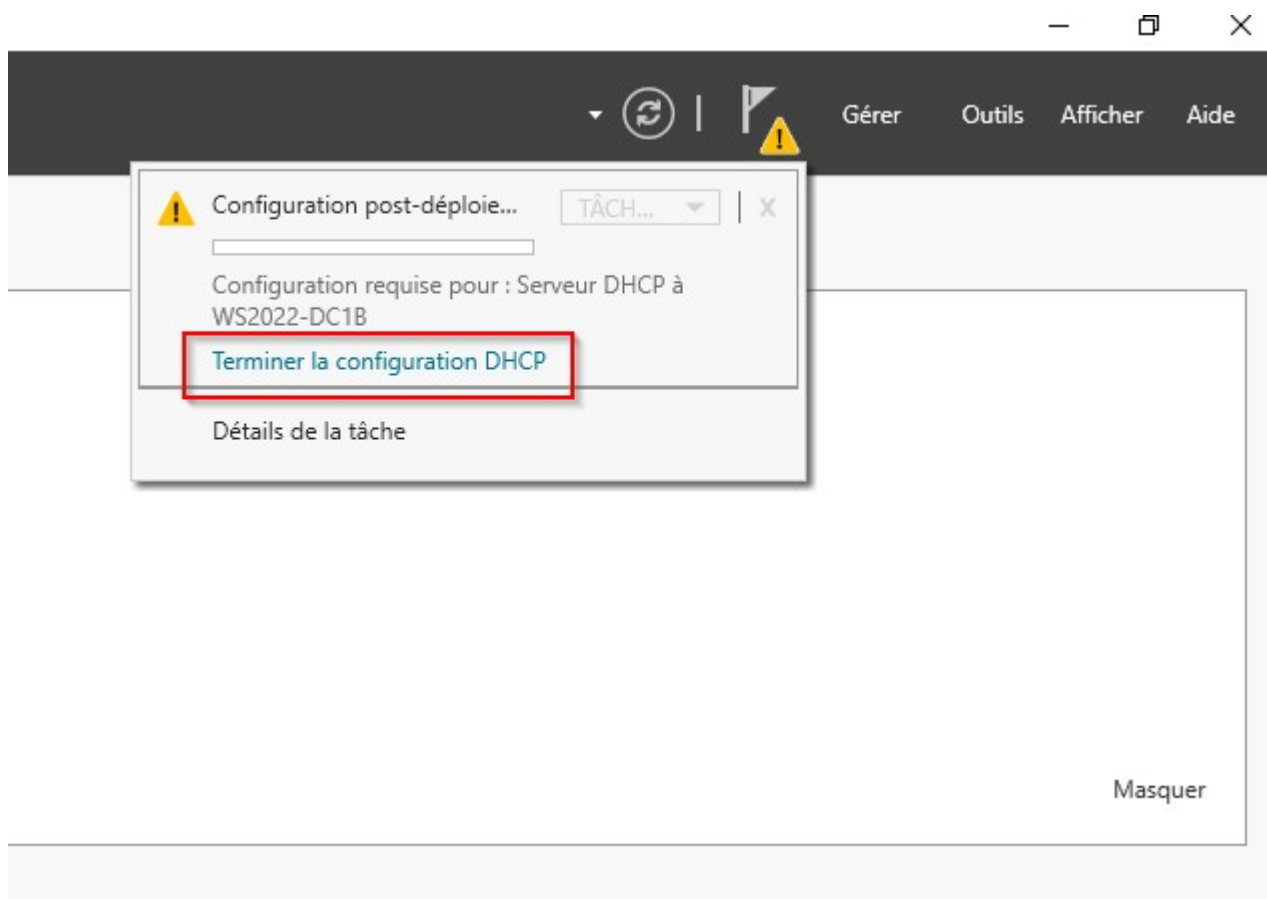




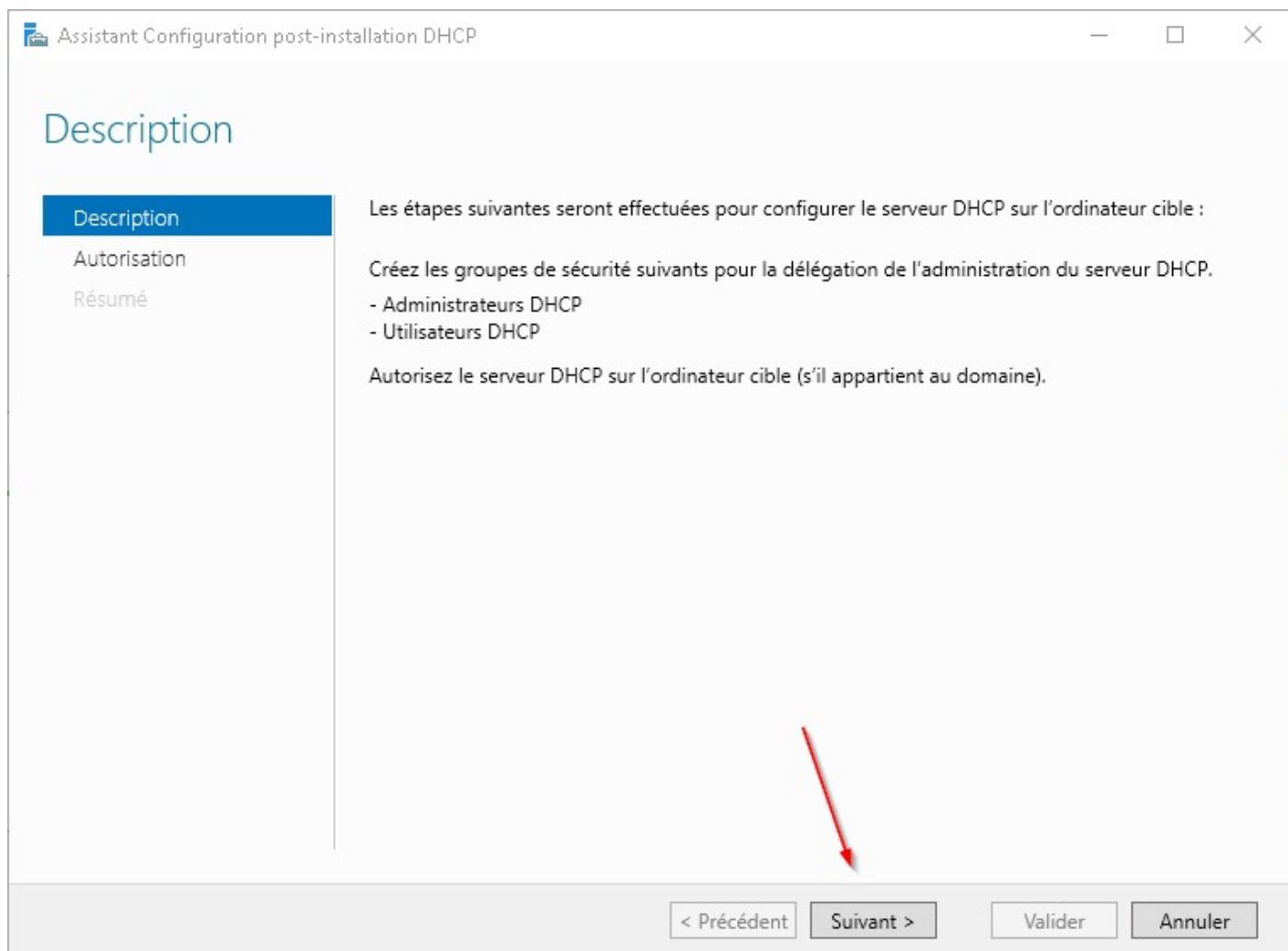


C. Installation du DHCP.

Cliquez sur le panneau en haut à droite puis sur "Terminer la configuration DHCP".



Une fenêtre va s'ouvrir avec des instructions.



Renseignez bien votre nom d'utilisateur et valider ensuite.

Assistant Configuration post-installation DHCP

Autorisation

Description

Autorisation

Résumé

Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.


☒ Utiliser les informations d'identification de l'utilisateur suivant

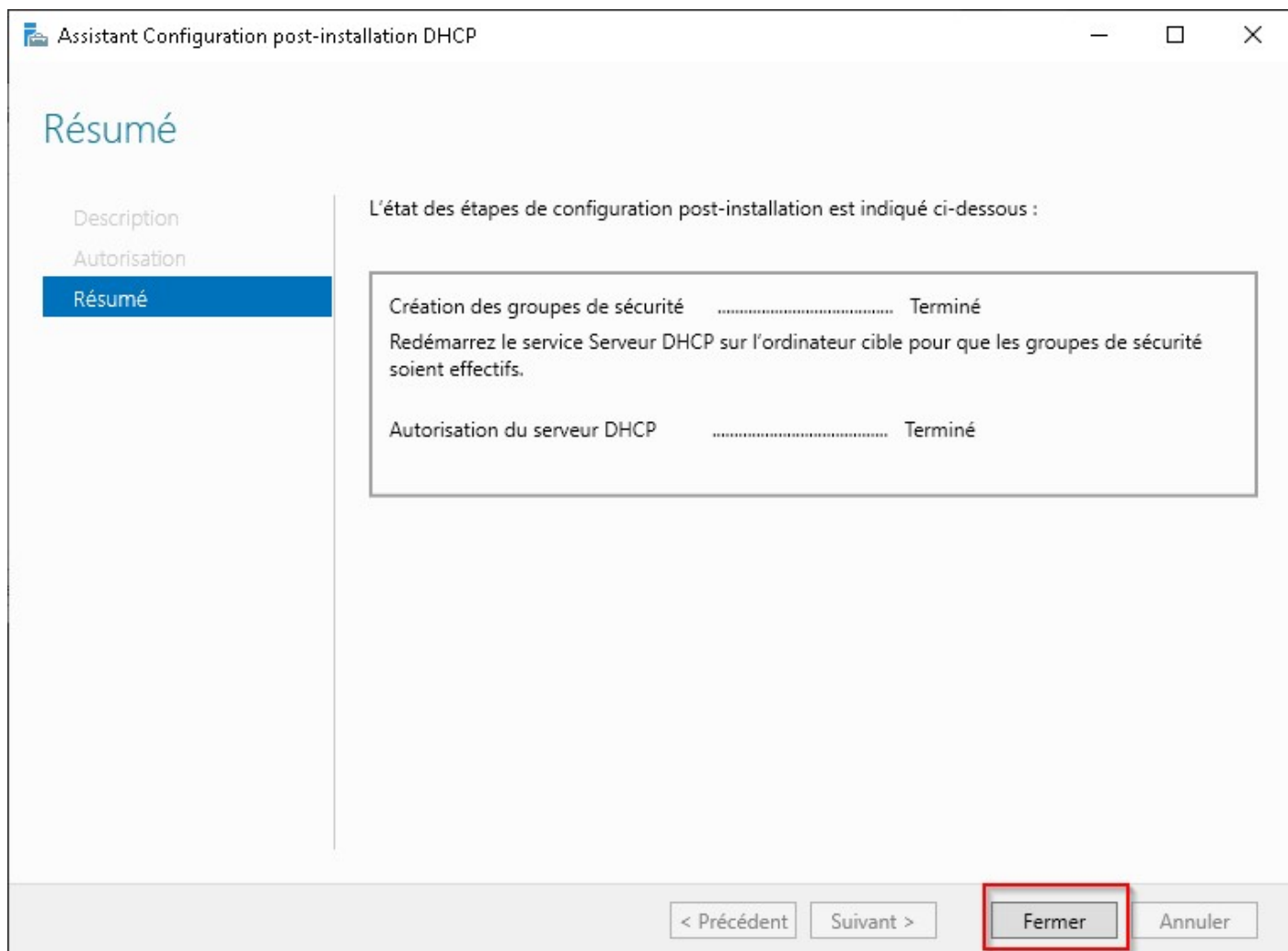
Nom d'utilisateur : RCBN\Administrateur

☐ Utiliser d'autres informations d'identification

Nom d'utilisateur :

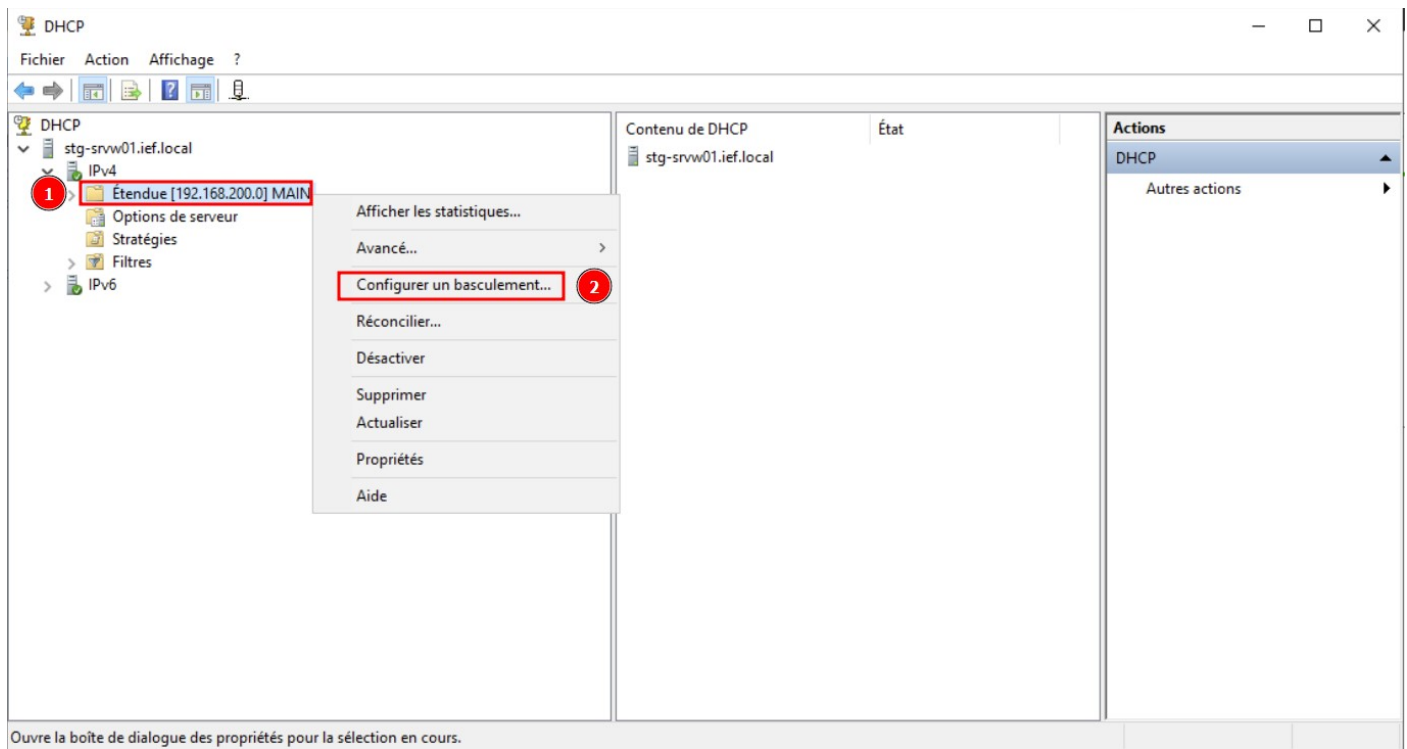
☐ Ignorer l'autorisation AD





D. Configuration du DHCP Failover

Sur le DC primaire de votre site, crée un basculement sur votre étendu DHCP





Il faut désormais sélectionner le serveur de basculement qui sera le DC2 de votre site, dans notre cas cela sera le DC2-SB

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement



Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :

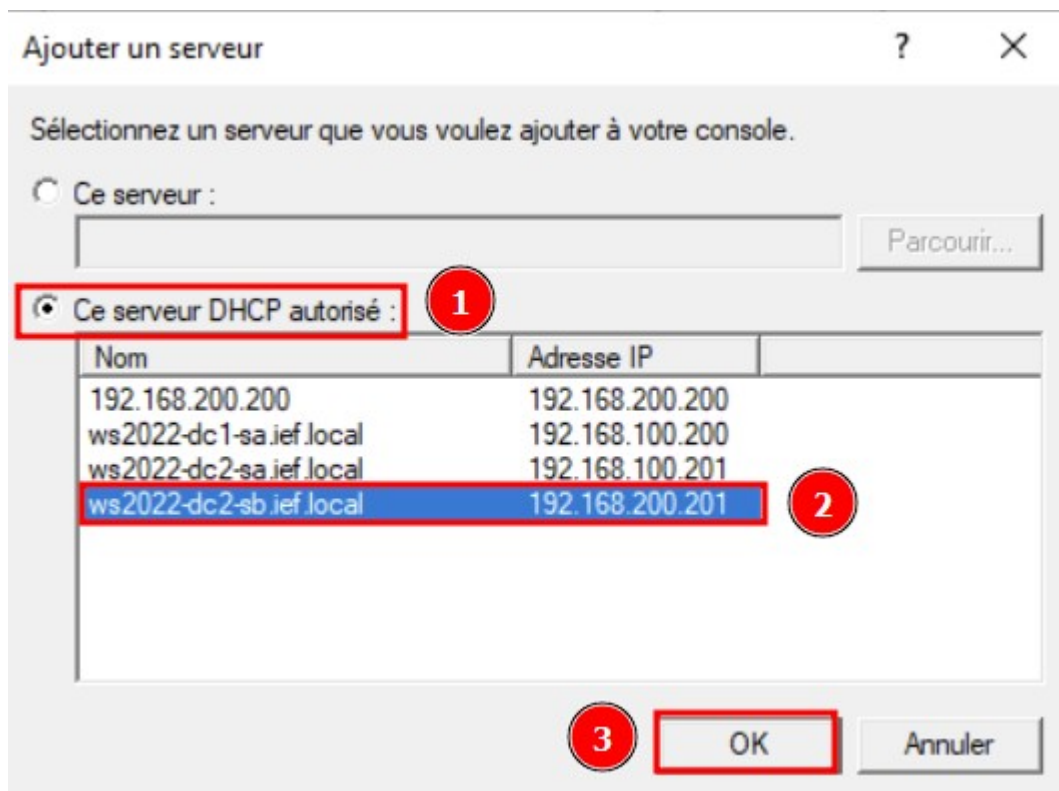
Ajouter un serveur

☐ Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

< Précédent


Suivant >

Annuler



Configurer un basculement


Spécifier le serveur partenaire à utiliser pour le basculement



Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.


Serveur partenaire : 

☐ Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

Il faut désormais configurer les options du basculement, dans notre cas, nous allons uniquement changer le mode et le passer en mode "Serveur de secours" puis mettez un secret partagé afin de chiffrer la communication entre les deux serveurs dhcp pour qu'il ne soit pas en clair sur le réseau.

Configurer un basculement

Créer une relation de basculement



Créer une relation de basculement avec le partenaire ws2022-dc2-sa.ief.local

Nom de la relation :

Délai de transition maximal du client (MCLT) : heures minutes

Mode : 1

Configuration du serveur de secours

Rôle du serveur partenaire :

Adresses réservées pour le serveur de secours : %

☐ Intervalle de basculement d'état : minutes

☒ Activer l'authentification du message

Secret partagé : 2

3

Configurer un basculement

Un basculement va être configuré entre stg-srvw01.jef.local et ws2022-dc2-sb.jef.local avec les paramètres suivants.

Étendues :

192.168.200.0

Nom de la relation :	stg-srvw01.jef.l
Délai de transition maximal du client (MCLT) :	1 h 0 min
Mode :	Serveur de sec
Intervalle de basculement d'état :	Désactivé

< >

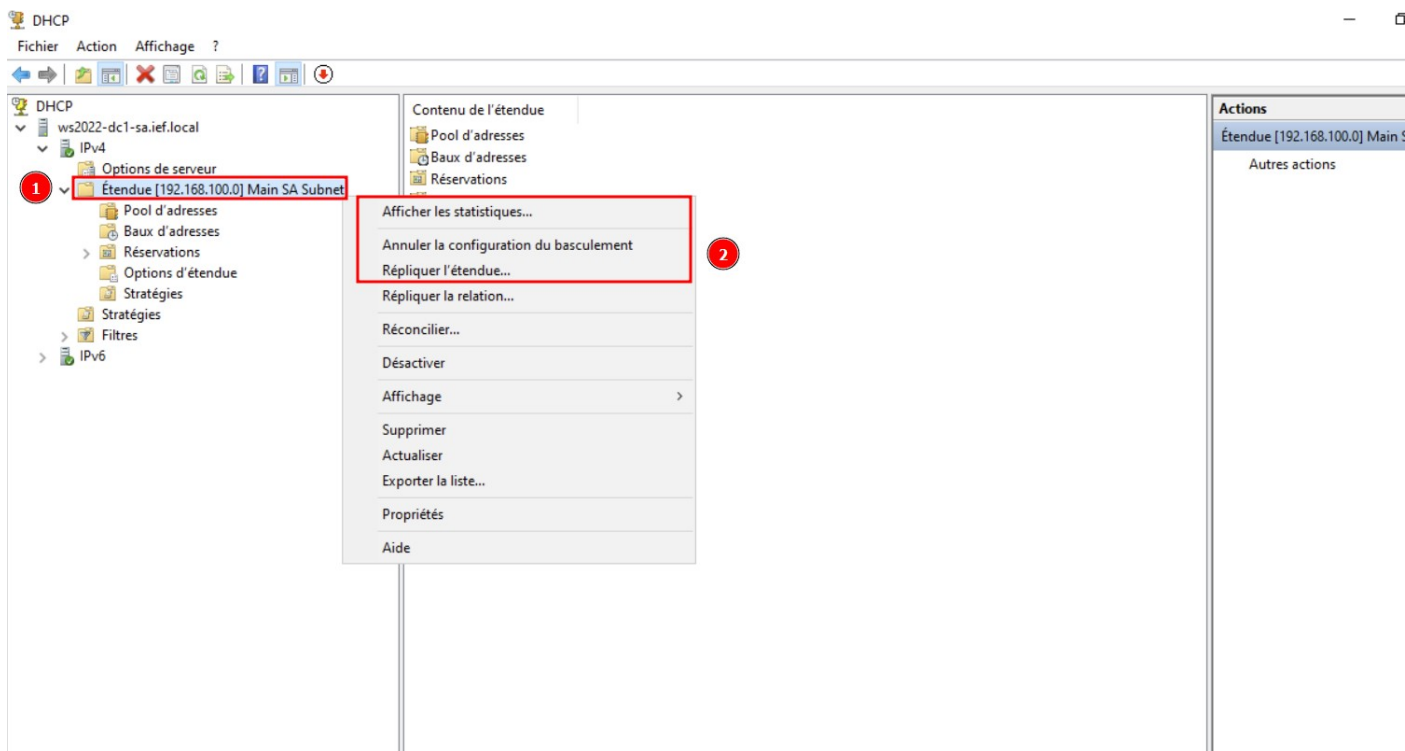
Configuration du serveur de secours

Rôle du serveur partenaire : Veille

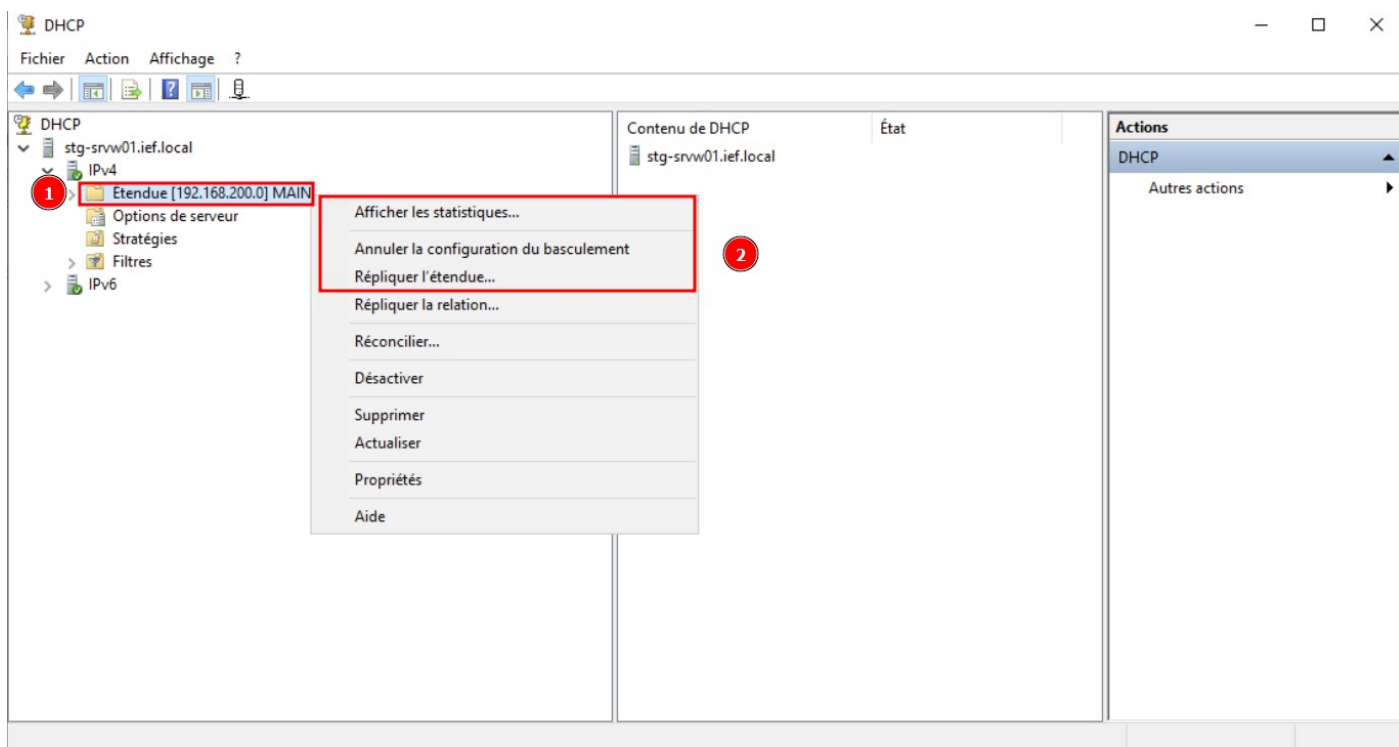
Adresses réservées pour le serveur 5 %

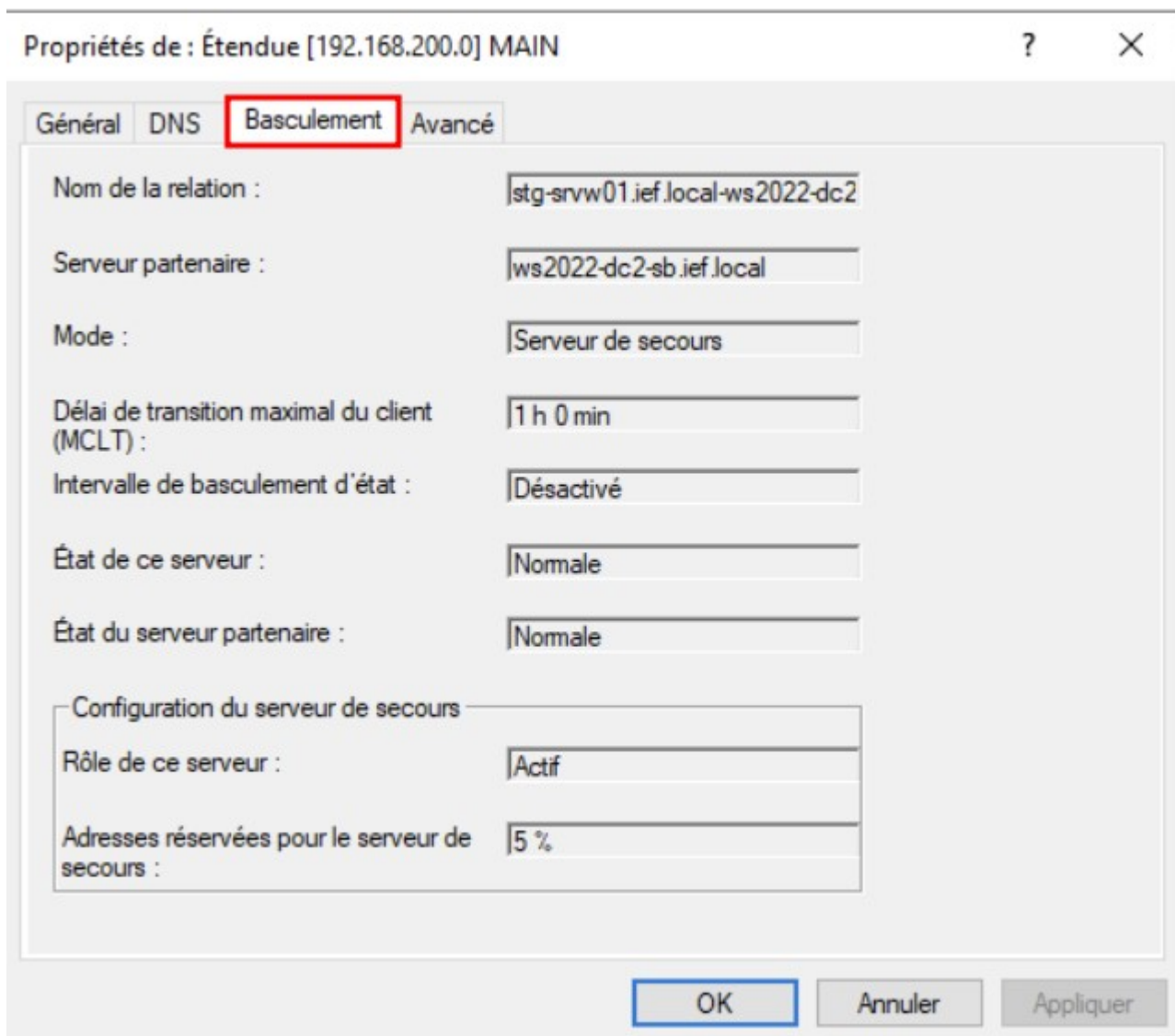
< Précédent **Terminer** Annuler

Sur votre étendue, vous pouvez constater plusieurs options, la première permet d'afficher les statistiques des 2 serveurs dhcp, la deuxième permet d'annuler le basculement, pour refaire la configuration il faudrait l'annuler et la refaire à nouveau. Puis nous pouvons répliquer l'étendu si nous faisons des modifications sur le DHCP primaire.

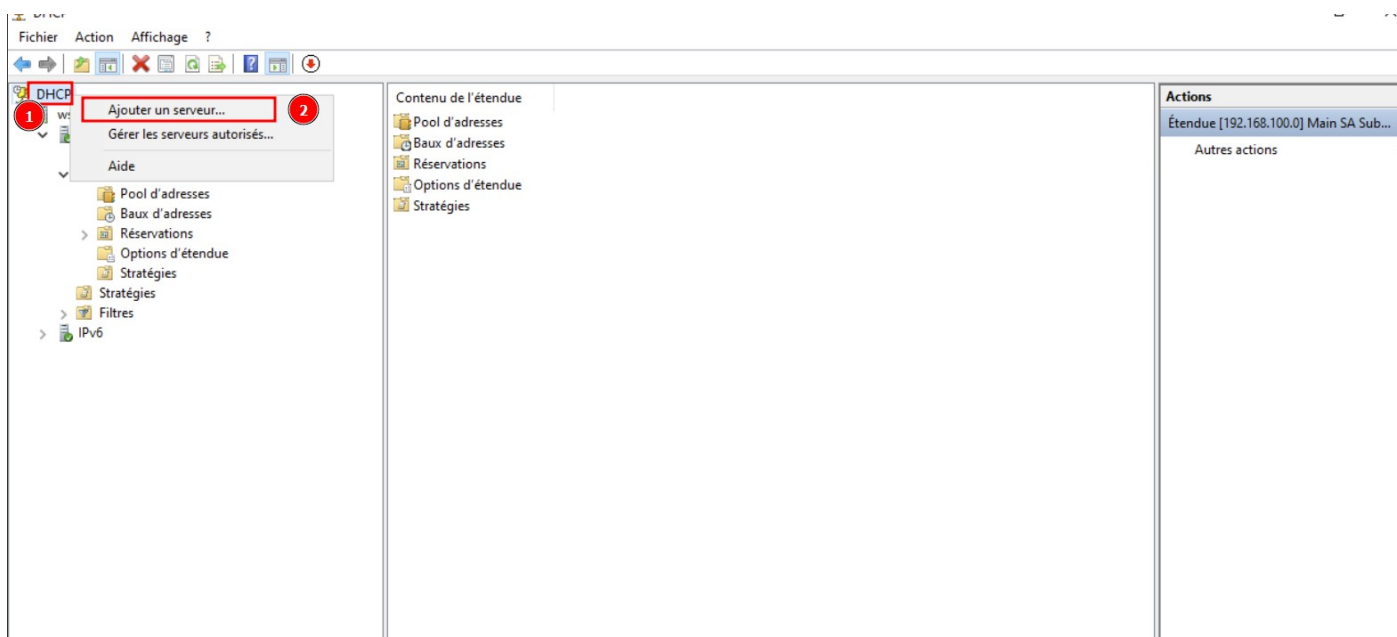


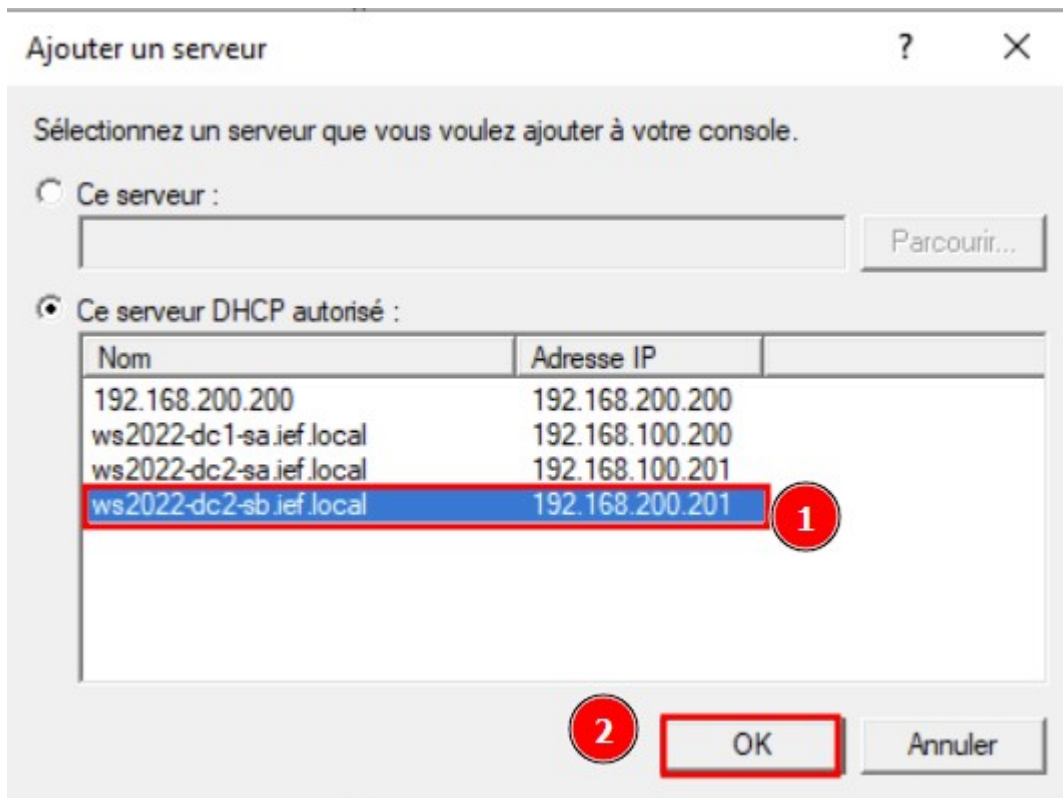
Dans les propriétés puis dans Basculement nous avons aussi les détails de la relation entre les deux serveurs DHCP.



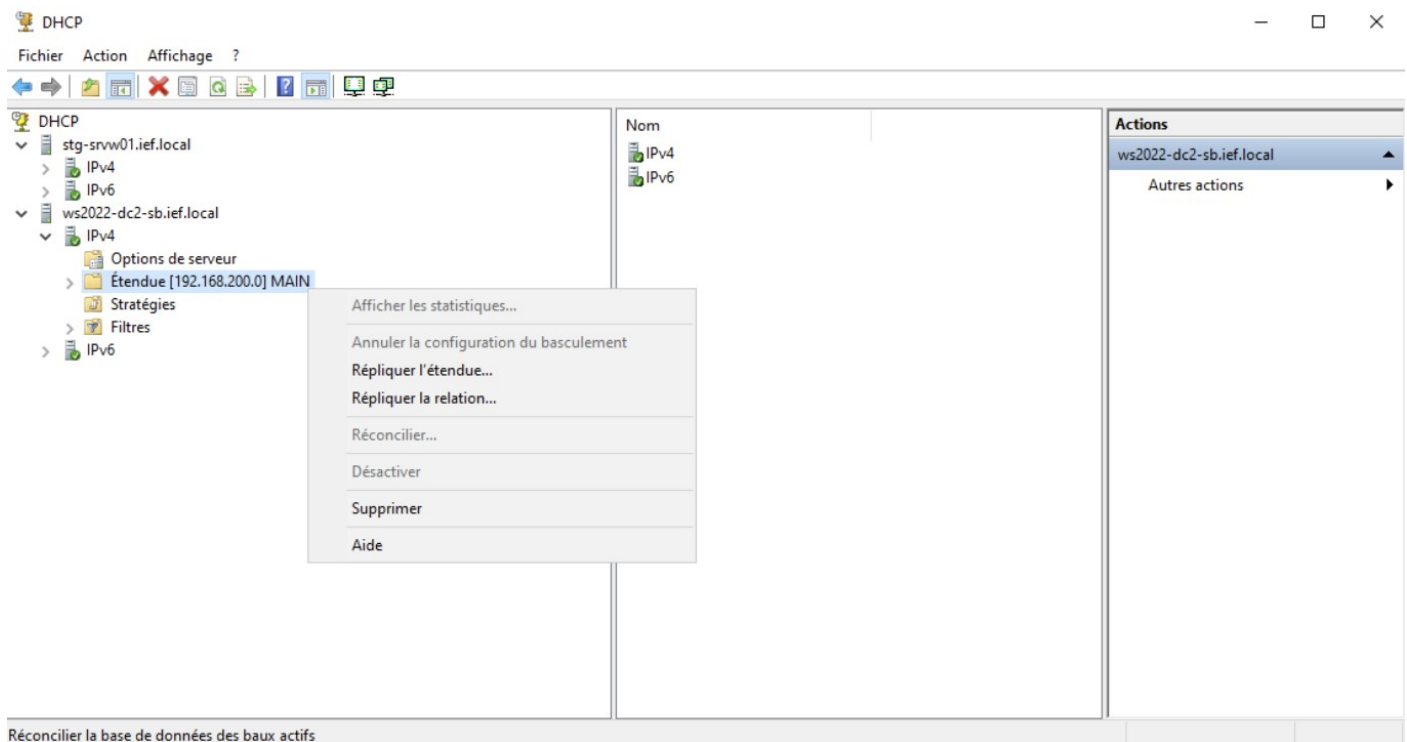


Dans votre pannel DHCP, nous pouvons également ajouter le serveur partenaire afin de pouvoir l'administrer également en cas de soucis. Attention, la relation entre les deux est unidirectionnelle ce qui signifie que si on modifie le DHCP du DC2 rien ne va se passer pour le primaire alors que le primaire écrase la configuration du secondaire.





Nous pouvons voir que le serveur DHCP failover à bel est bien pris la configuration du DHCP primaire.



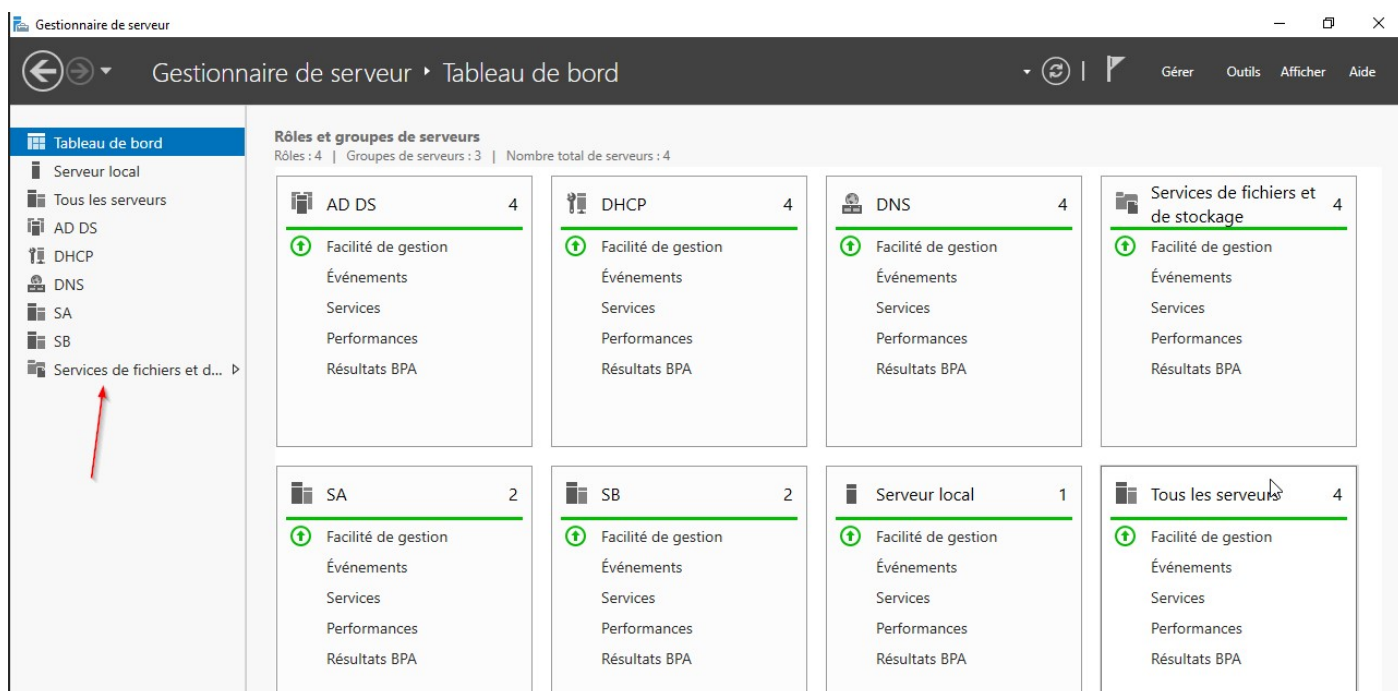
DFS

DFS

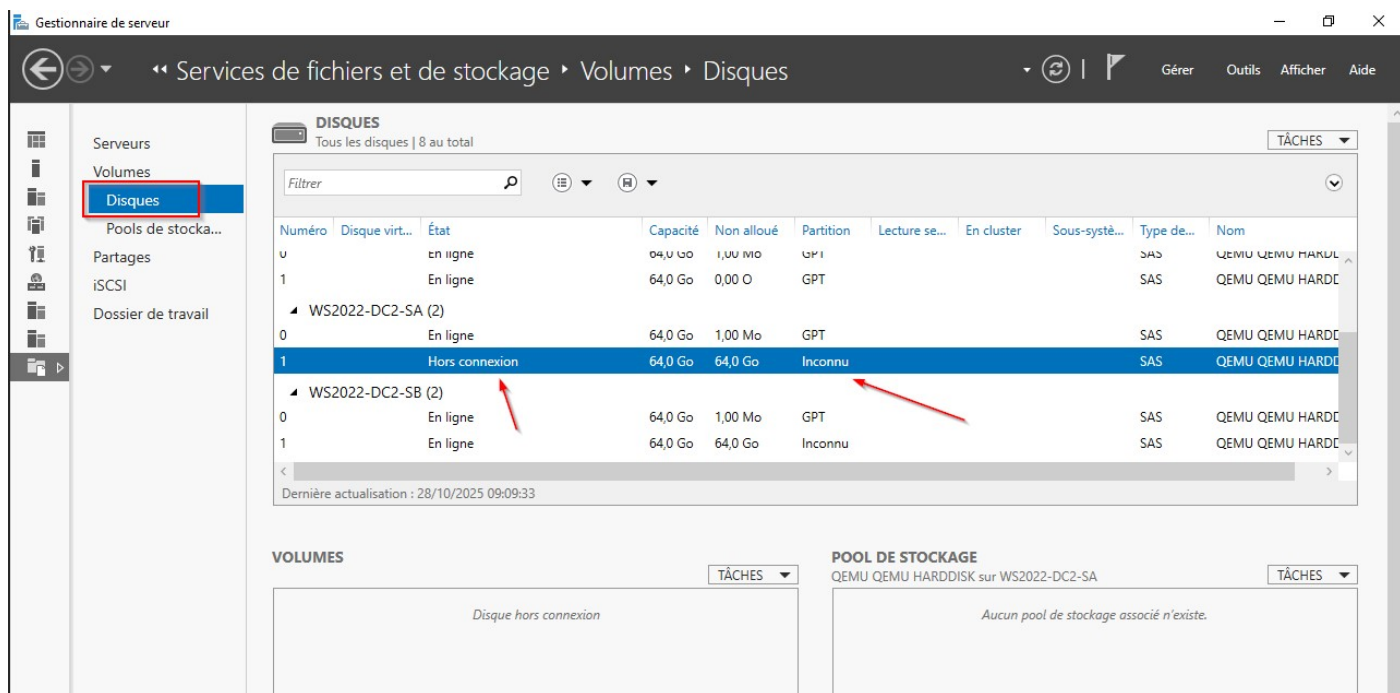
Préparation des disques et partages

1. Initialisation du Disque

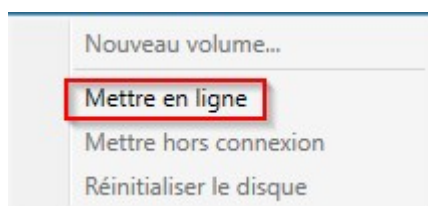
Allez dans "Services de fichiers et de stockage" sur le dashboard du serveur.



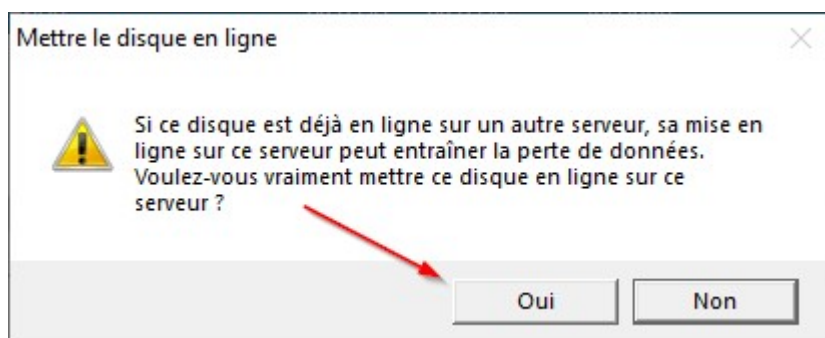
- Encadré rouge (à gauche) :** Vous avez sélectionné la section **Disques** dans le menu "Services de fichiers et de stockage" du Gestionnaire de serveur. C'est ici que l'on gère le matériel de stockage physique ou virtuel relié au serveur.
- Flèches rouges et surbrillance bleue (au centre) :** Vous ciblez un disque spécifique de **64 Go** sur le serveur WS2022-DC2-SA.
 - On remarque que l'état du disque est "**Hors connexion**" et que son type de partition est "**Inconnu**".



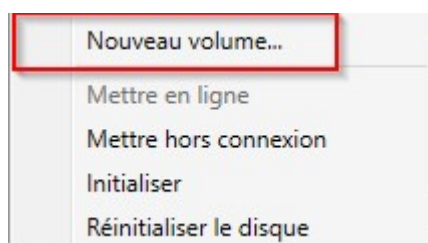
Vous faites un clic droit sur le disque et sélectionnez **"Mettre en ligne"**. C'est l'action qui permet au système d'exploitation de commencer à utiliser le disque physique.



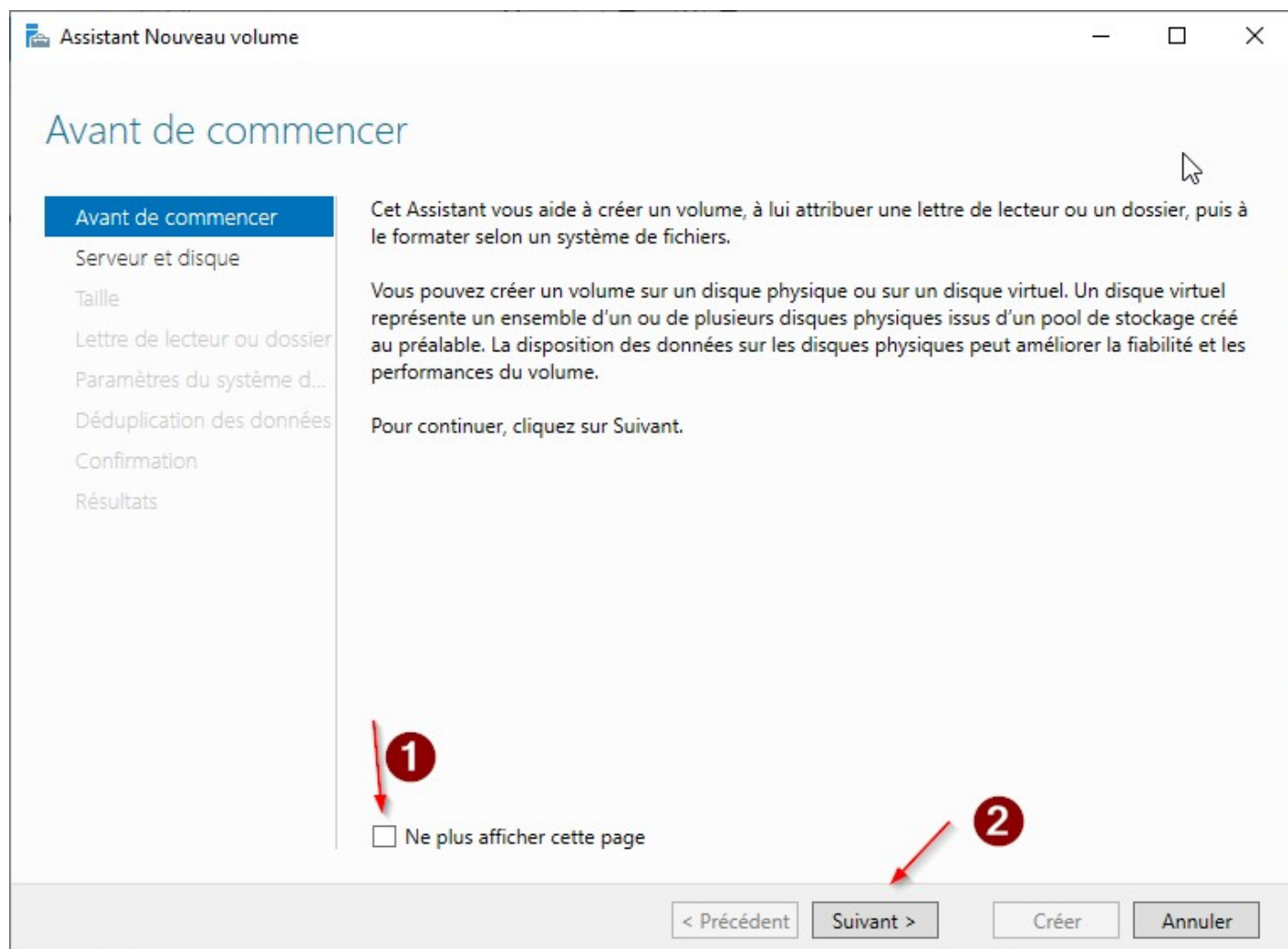
Une fenêtre de confirmation apparaît pour vous prévenir des risques potentiels (si le disque était utilisé ailleurs). Vous cliquez sur **"Oui"** pour valider la mise en ligne.



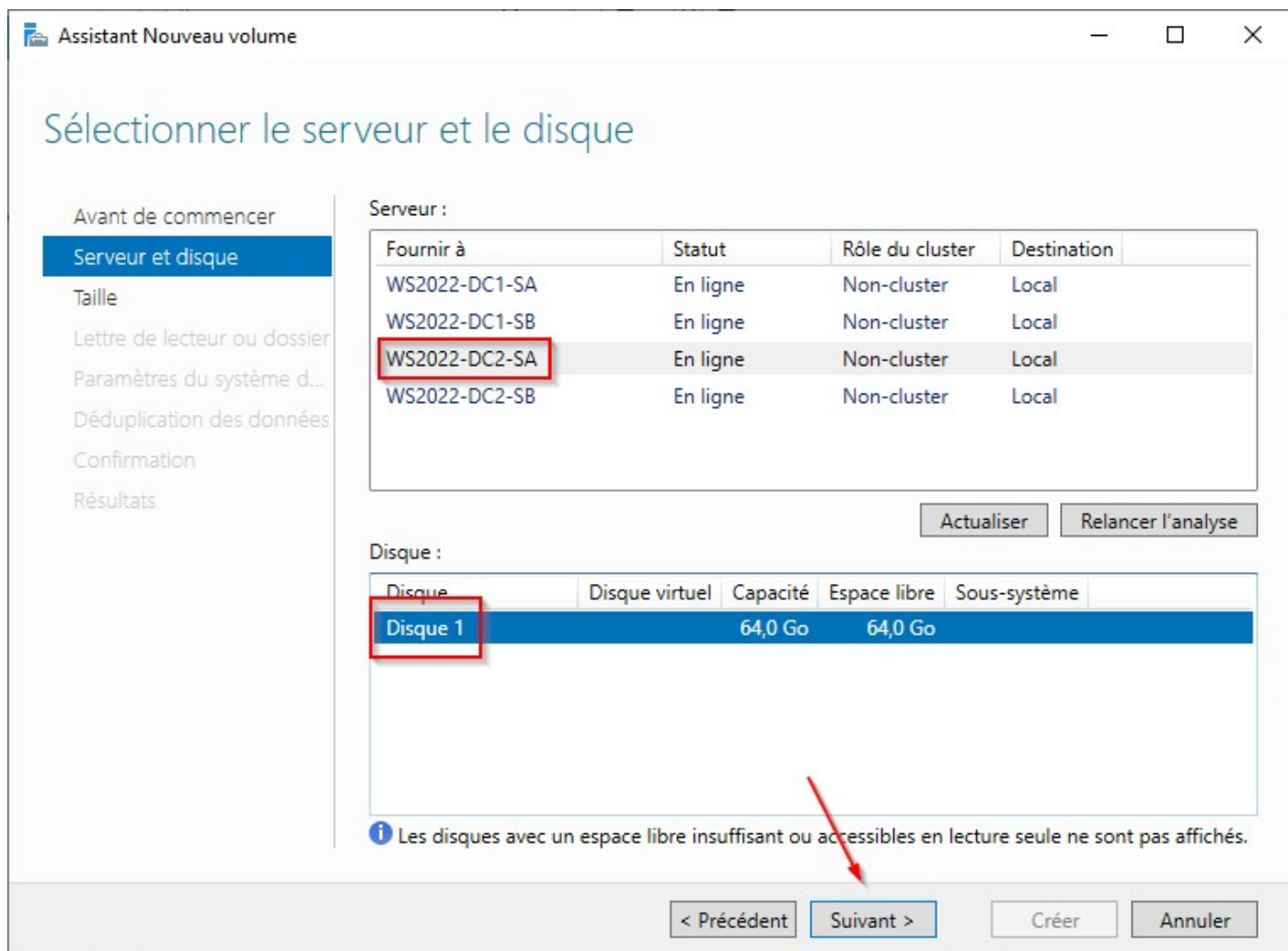
Une fois le disque en ligne, vous faites à nouveau un clic droit et sélectionnez **"Nouveau volume..."**. Cette action lance l'assistant qui va vous permettre de partitionner le disque et de lui attribuer une lettre.



Vous passez simplement l'écran d'introduction de l'assistant en cliquant sur le bouton « **Suivant >** ». La flèche 1 montre la case à cocher pour ne plus afficher cet avertissement à l'avenir.

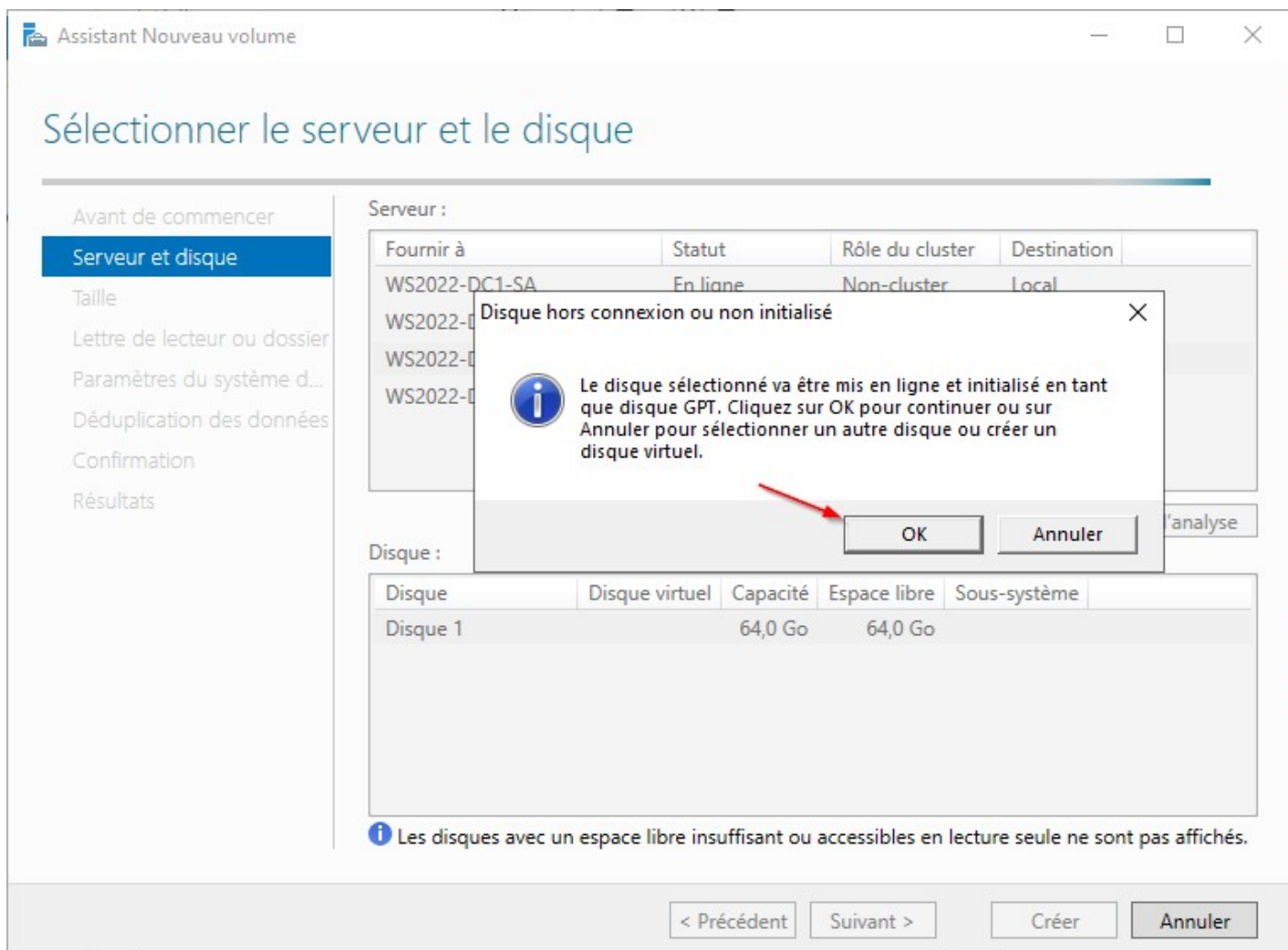


- **Premier encadré rouge** : Vous sélectionnez le serveur cible sur lequel le disque est rattaché, ici le serveur **WS2022-DC2-SA**.
- **Deuxième encadré rouge** : Vous sélectionnez le disque physique sur lequel vous allez créer le volume. Ici, il s'agit du « **Disque 1** » d'une capacité de 64 Go (celui que vous avez mis en ligne précédemment).
- **Flèche rouge** : Une fois le serveur et le disque bien sélectionnés, vous cliquez sur le bouton « **Suivant >** » pour passer à l'étape de définition de la taille du volume.



Vous cliquez sur le bouton « **OK** » dans la fenêtre d'avertissement.

- **Ce que cela fait** : Cela confirme que le disque va être initialisé avec un style de partition **GPT** (GUID Partition Table). C'est l'étape nécessaire pour que Windows puisse réellement écrire des données sur ce nouveau disque.



- On voit que la « Taille du volume » est réglée par défaut sur la capacité maximale disponible (**64 Go**).
- **Flèche rouge** : Vous cliquez sur le bouton « **Suivant** > ».
 - **Ce que cela fait** : Vous décidez d'utiliser l'intégralité de l'espace disque pour créer une seule et unique partition.

Assistant Nouveau volume

Spécifier la taille du volume

Avant de commencer

Serveur et disque

Taille

Lettre de lecteur ou dossier

Paramètres du système d...

Déduplication des données

Confirmation

Résultats

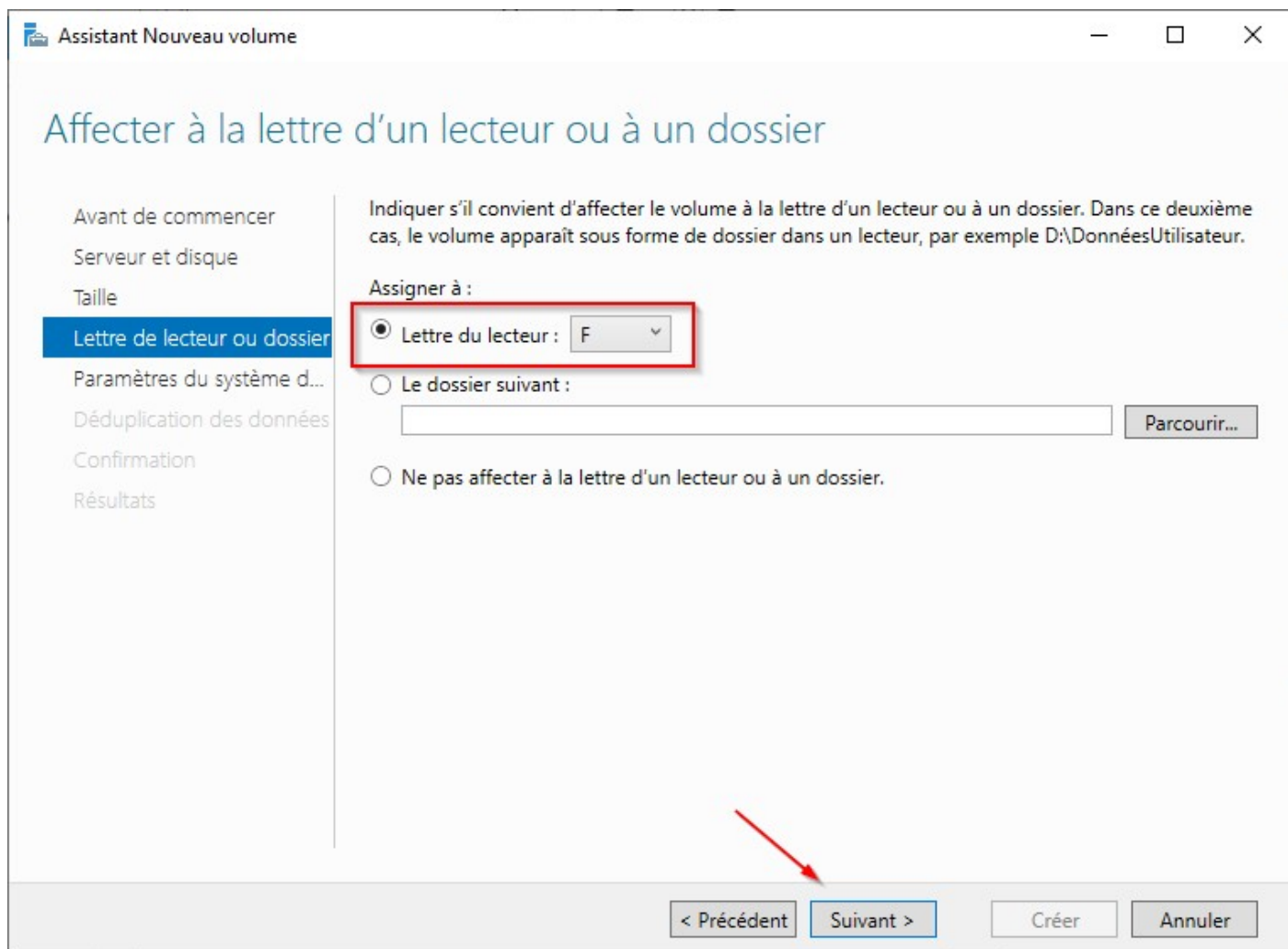
Capacité disponible : 64,0 Go

Taille minimale : 8,00 Mo

Taille du volume : 64,0 Go

< Précédent Suivant > Créer Annuler

- **Encadré rouge** : Vous choisissez d'assigner une lettre au lecteur. Ici, vous sélectionnez la lettre « **F** ». C'est sous cette lettre que le disque apparaîtra dans l'Explorateur de fichiers.
- **Flèche rouge** : Vous cliquez sur « **Suivant** » pour valider ce choix.



- **Encadré rouge** : Vous donnez un nom explicite au disque dans le champ « Nom de volume ». Ici, vous saisissez « **DATAS03** ». Cela permet d'identifier facilement à quoi sert ce stockage parmi les autres disques.
- **Flèche rouge** : Vous cliquez sur « **Suivant** » pour valider le nom et passer à la suite (le formatage se fera en NTFS par défaut).

Assistant Nouveau volume

Sélectionner les paramètres du système de fichiers

Avant de commencer
Serveur et disque
Taille
Lettre de lecteur ou dossier
Paramètres du système d...
Déduplication des données
Confirmation
Résultats

Système de fichiers : NTFS

Taille d'unité d'allocation : Par défaut

Nom de volume : DATAS03

☐ Générer des noms de fichiers courts (déconseillé)

Les noms de fichier courts (8 caractères plus 3 caractères pour l'extension) sont obligatoires pour certaines applications 16 bits s'exécutant sur les ordinateurs clients, mais ralentissent les opérations sur les fichiers.

< Précédent Suivant > Créer Annuler

- **Encadré rouge** : Vous activez la déduplication sur ce nouveau volume en choisissant le profil « **Serveur de fichiers à usage général** ».
 - À quoi ça sert ? Cela permet de gagner de l'espace disque en ne stockant qu'une seule copie des fichiers identiques. Ici, on voit que le système commencera à dédoubler les fichiers ayant plus de 3 jours.
- **Flèche rouge** : Vous cliquez sur le bouton « **Suivant** > » pour passer au résumé final.

Assistant Nouveau volume

Activer la déduplication des données

Avant de commencer
Serveur et disque
Taille
Lettre de lecteur ou dossier
Paramètres du système d...
Déduplication des données
Confirmation
Résultats

La déduplication des données économise de l'espace disque en stockant une seule copie de données identiques sur le volume. Spécifiez l'ancienneté des fichiers à dédupliquer, les extensions de fichier à exclure et quand planifier la déduplication.

Déduplication des données :

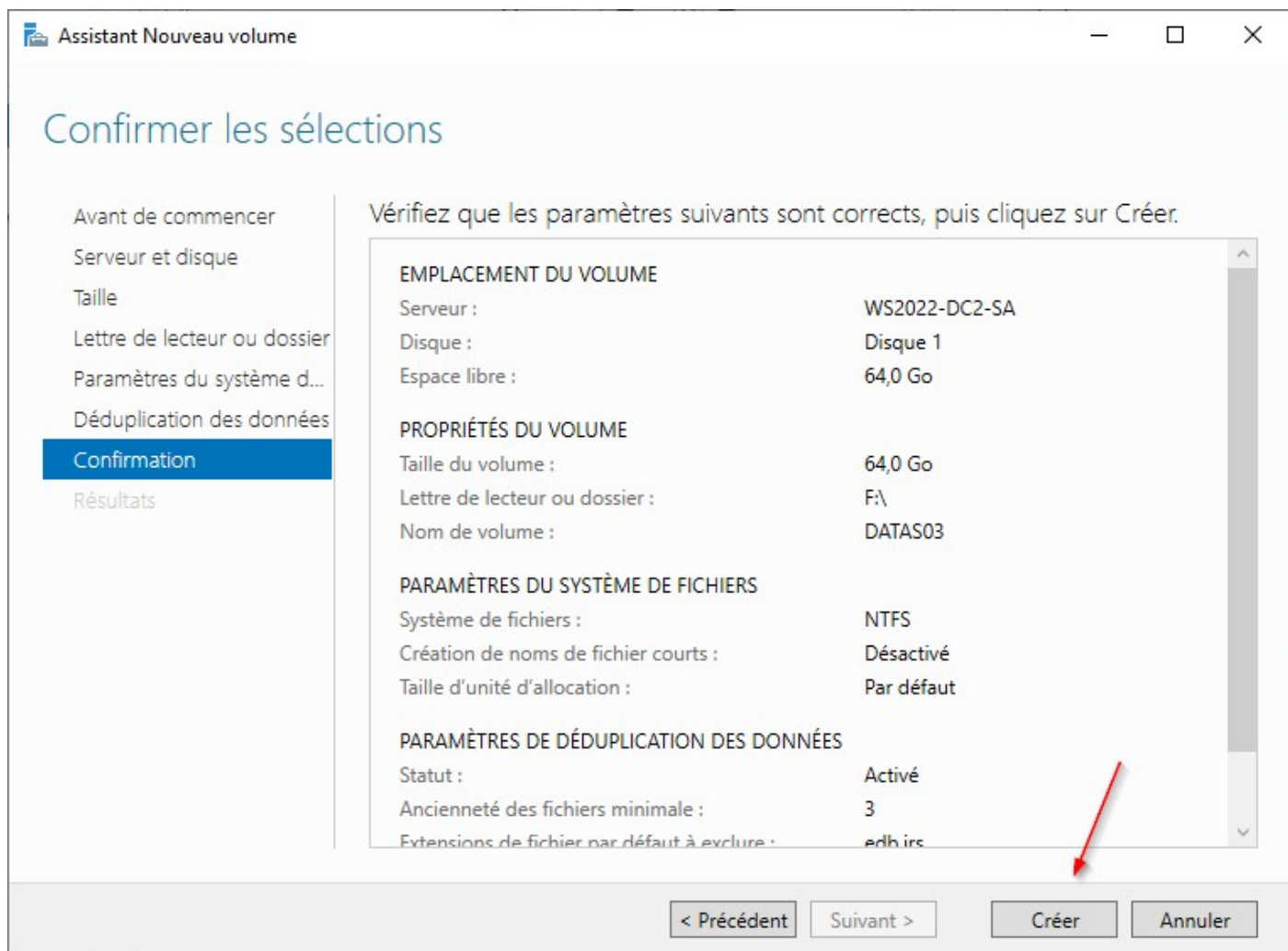
Dédupliquer les fichiers de plus de (en jours) :

Tapez les extensions de fichier que vous souhaitez exclure de la déduplication des données, en séparant les extensions à l'aide d'une virgule. Par exemple : doc,txt,png

Extensions de fichier par défaut à exclure :

Extensions de fichier personnalisées à exclure :

- **Contenu** : Cet écran affiche le récapitulatif complet de votre configuration (Serveur WS2022-DC2-SA, Disque 1 de 64 Go, Lettre de lecteur **F:**, Nom **DATAS03** et Déduplication activée).
- **Flèche rouge** : Vous cliquez sur le bouton « **Créer** ».



Encadré rouge : Dans le menu de gauche du Gestionnaire de serveur, vous cliquez sur l'onglet « **Partages** ».

RESSOURCES PARTAGÉES
Tous les partages | 8 au total

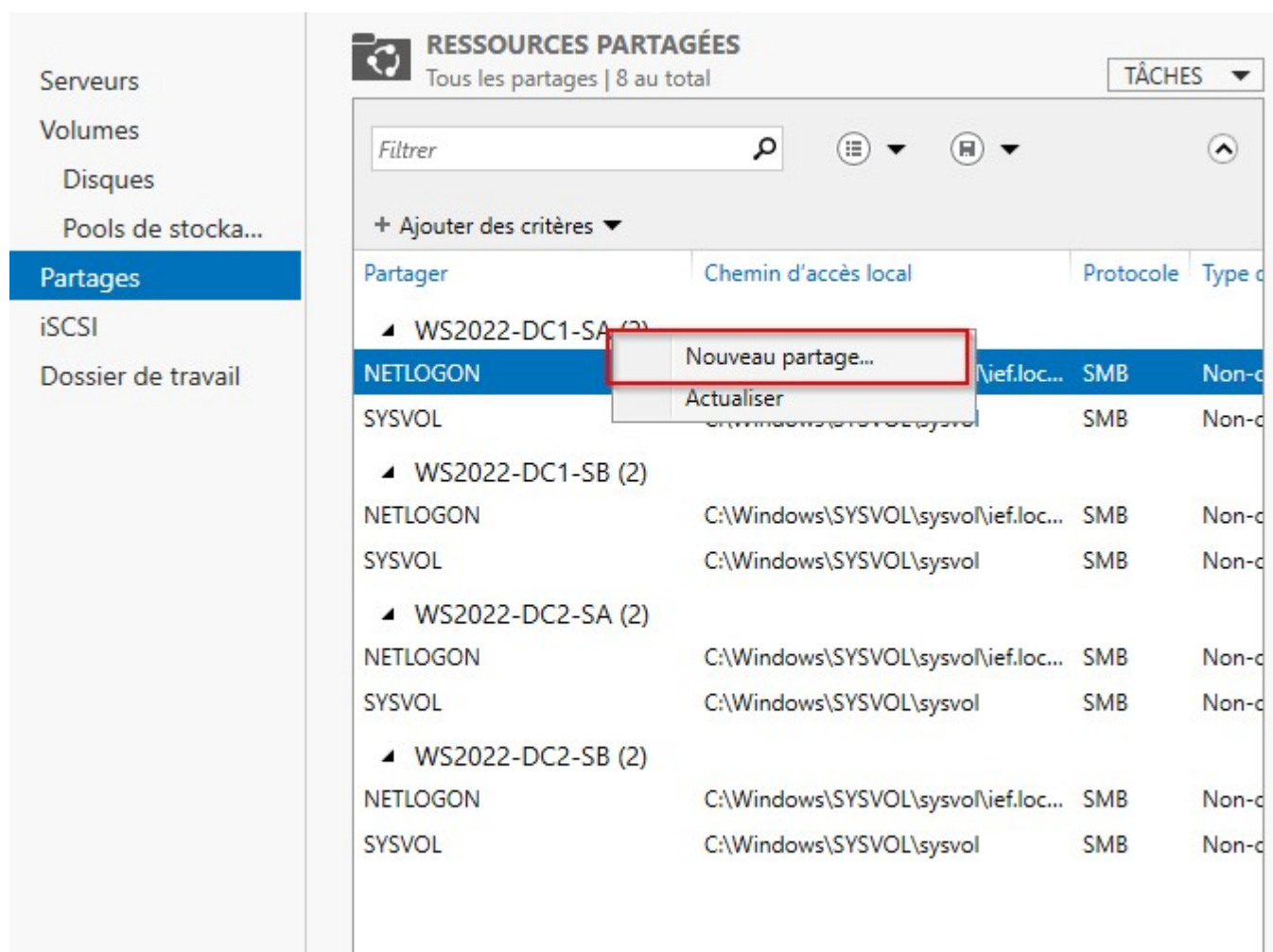
TÂCHES ▼

Filtrer 🔍

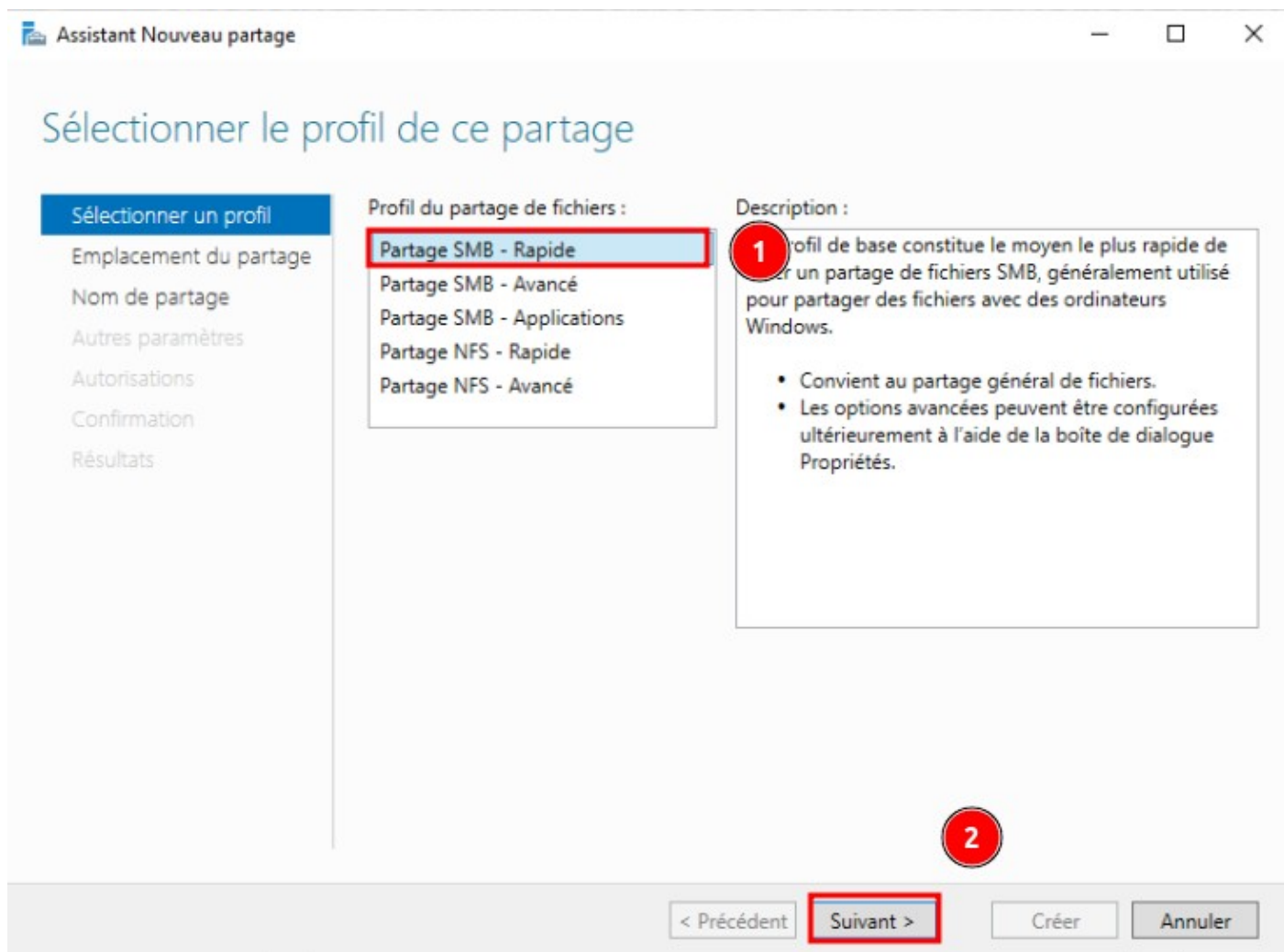
+ Ajouter des critères ▼

Partager	Chemin d'accès local	Protocole	Type de partage
WS2022-DC1-SA (2)			
NETLOGON	C:\Windows\SYSVOL\sysvol\ief.loc...	SMB	Non-caché
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-caché
WS2022-DC1-SB (2)			
NETLOGON	C:\Windows\SYSVOL\sysvol\ief.loc...	SMB	Non-caché
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-caché
WS2022-DC2-SA (2)			
NETLOGON	C:\Windows\SYSVOL\sysvol\ief.loc...	SMB	Non-caché
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-caché
WS2022-DC2-SB (2)			
NETLOGON	C:\Windows\SYSVOL\sysvol\ief.loc...	SMB	Non-caché
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-caché

Encadré rouge : Vous faites un clic droit dans la zone vide de la liste des ressources partagées et vous sélectionnez « **Nouveau partage...** ».



- **Encadré 1** : On sélectionne le profil « **Partage SMB - Rapide** ». C'est l'option standard et la plus rapide pour créer un partage de fichiers compatible avec les ordinateurs Windows.
- **Encadré 2** : On clique sur le bouton « **Suivant** > » pour passer à l'étape suivante.



- **Encadré 1** : On choisit l'emplacement physique du partage. Ici, on sélectionne le volume « **F:** » (le disque de 64 Go préparé précédemment). Windows créera automatiquement un dossier nommé "Shares" sur ce disque pour y stocker le partage.
- **Encadré 2** : On clique sur « **Suivant** > » pour continuer.

Assistant Nouveau partage

Sélectionner le serveur et le chemin d'accès au partage

Sélectionner un profil

Emplacement du partage

Nom de partage

Autres paramètres

Autorisations

Confirmation

Résultats

Serveur :

Nom du serveur	Statut	Rôle du cluster	Noeud propriétaire
WS2022-DC1-SA	En ligne	Non-cluster	
WS2022-DC1-SB	En ligne	Non-cluster	
WS2022-DC2-SA	En ligne	Non-cluster	
WS2022-DC2-SB	En ligne	Non-cluster	

Emplacement du partage :

☒ Sélectionner par volume :

Volume	Espace libre	Capacité	Système de fichiers
C:	40,1 Go	63,3 Go	NTFS
F:	63,2 Go	64,0 Go	NTFS

L'emplacement du partage de fichiers sera un nouveau dossier du répertoire \Shares sur le volume sélectionné.

☐ Tapez un chemin personnalisé :

Parcourir...

< Précédent **Suivant >** Créer Annuler

- **Encadré 1** : On saisit le nom que les utilisateurs verront sur le réseau. Ici, vous avez tapé « **DATAS01** ».
 - On remarque juste en dessous le **chemin d'accès distant** (le lien réseau) qui sera généré : \WS2022-DC1-SA\DATAS01.
- **Encadré 2** : On clique sur « **Suivant >** » pour valider le nom et passer au paramétrage de la sécurité.

Assistant Nouveau partage

Indiquer le nom de partage

Sélectionner un profil
Emplacement du partage
Nom de partage
Autres paramètres
Autorisations
Confirmation
Résultats

Nom du partage : **DATAS01** **1**

Description du partage :

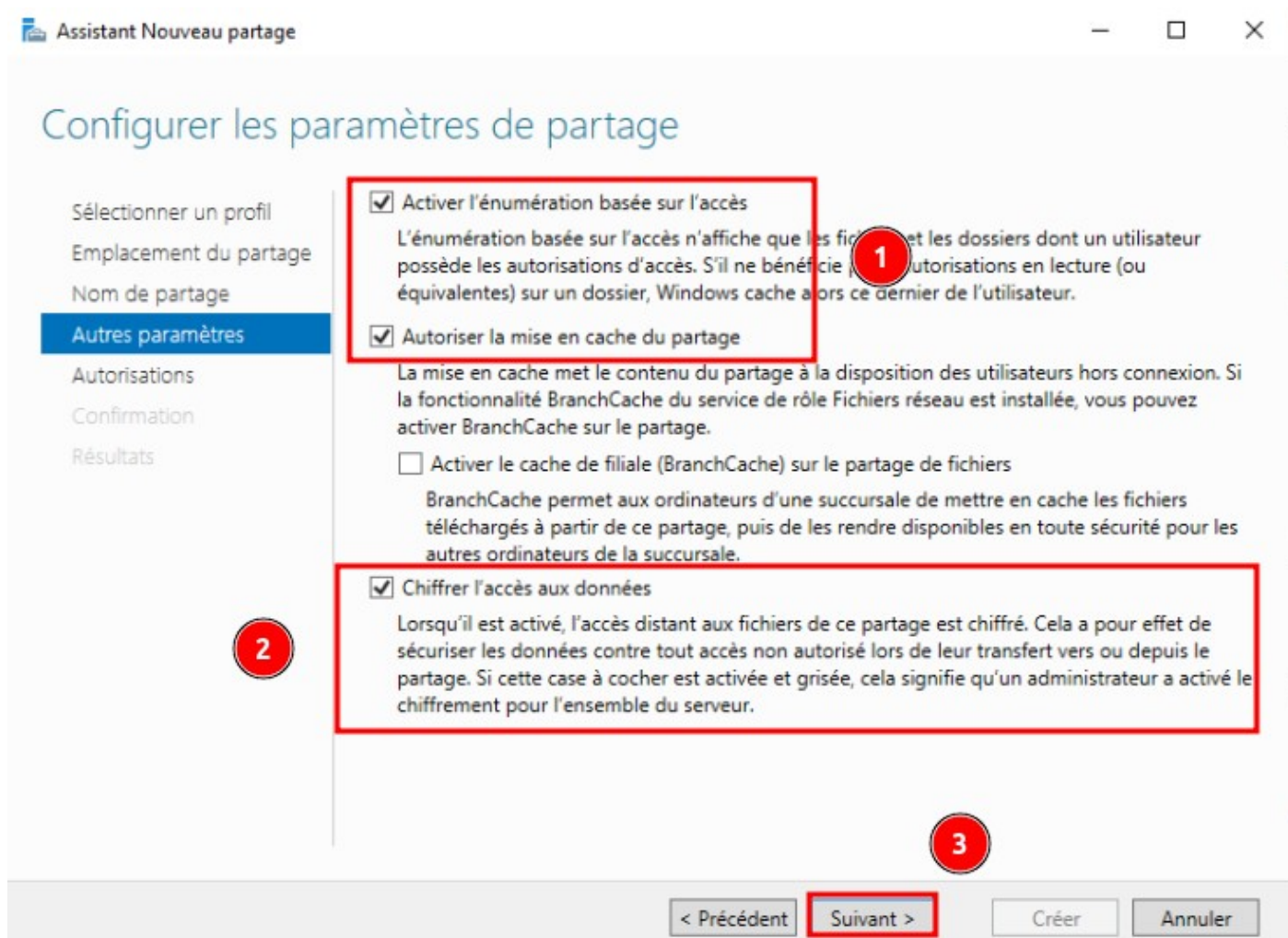
Chemin d'accès local au partage : F:\Shares\DATAS01
i Si le dossier n'existe pas, il est créé.

Chemin d'accès distant au partage : \\WS2022-DC1-SA\DATAS01

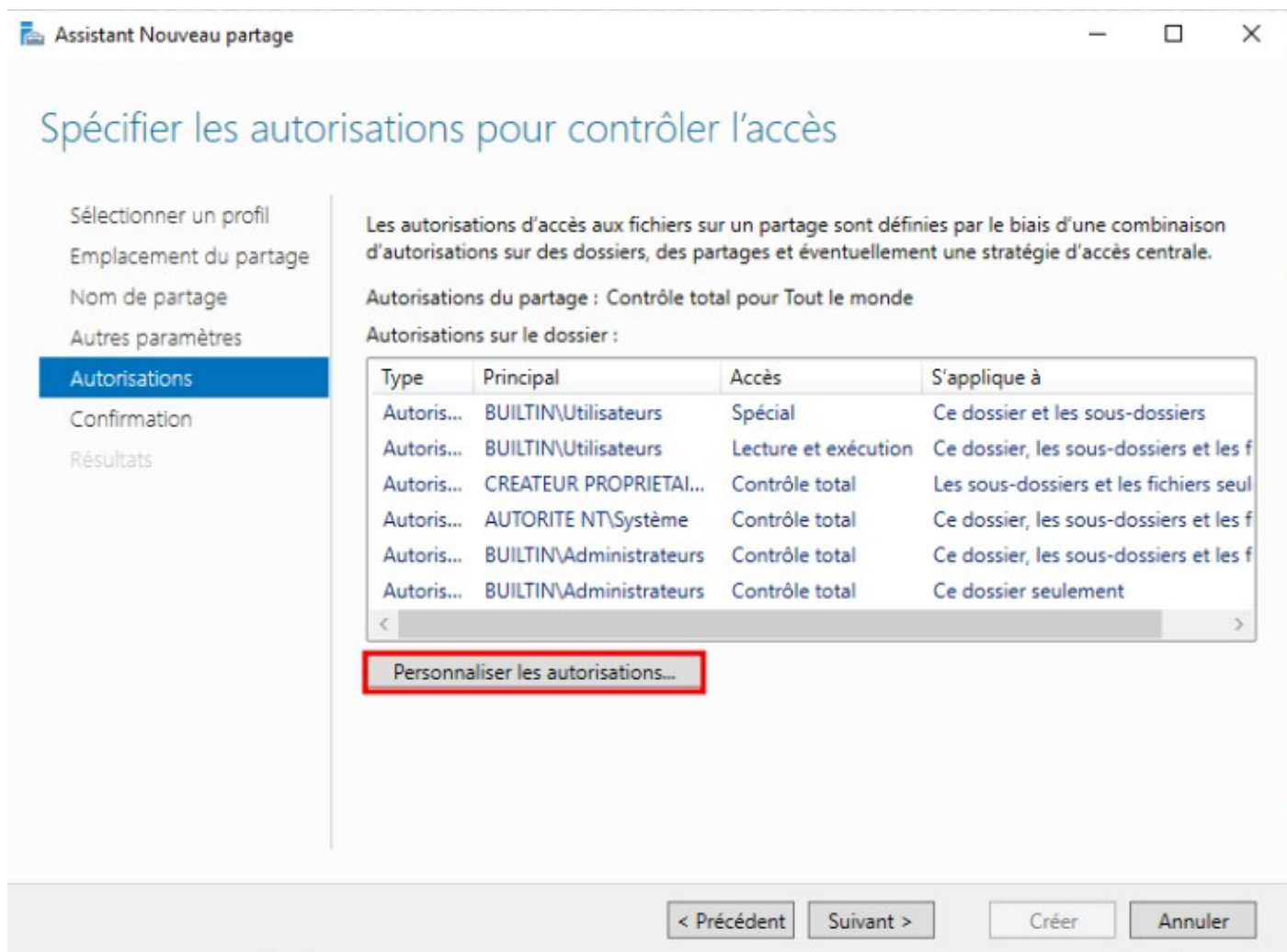
2

< Précédent **Suivant >** Créer Annuler

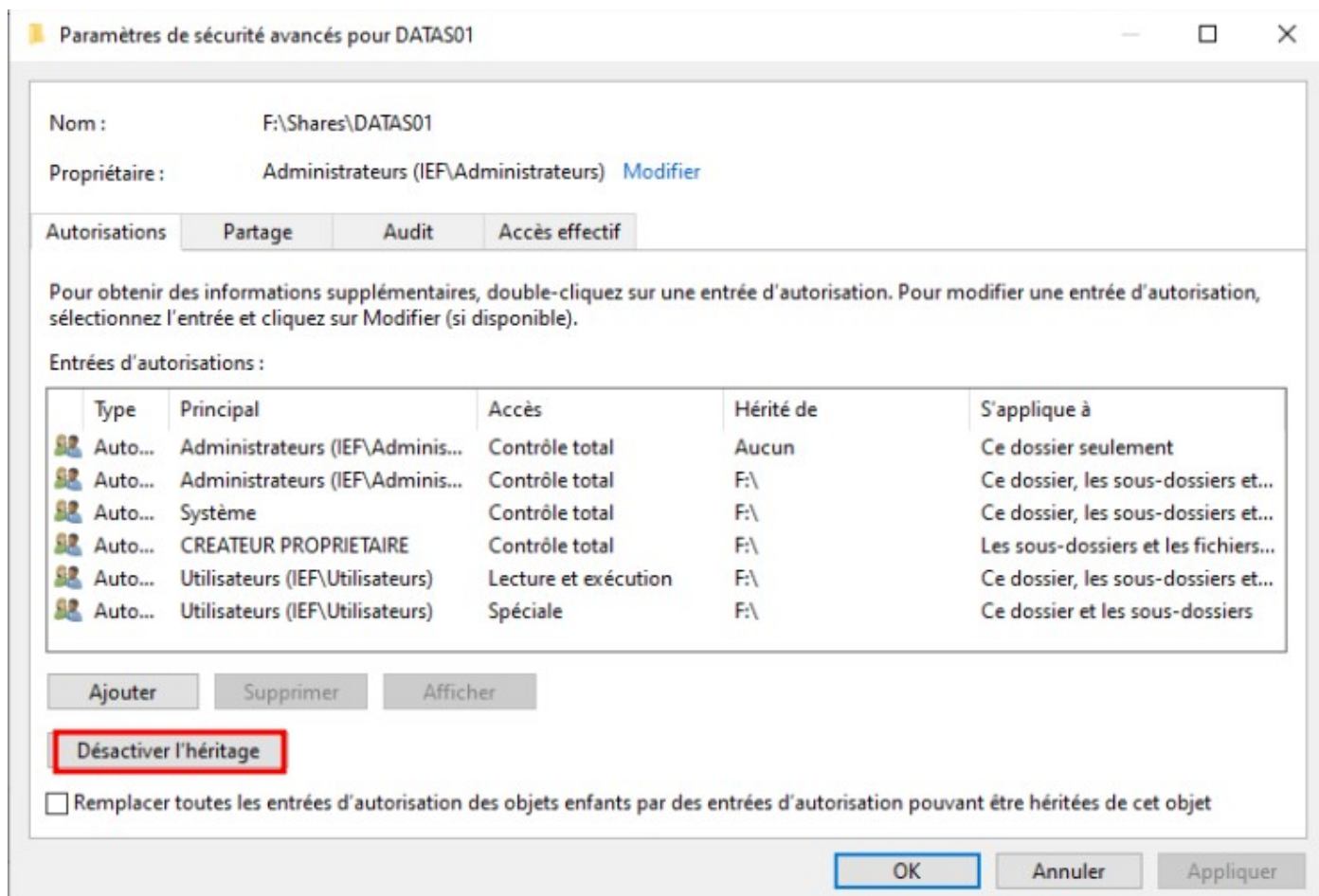
- **Encadré 1** : On coche deux options de sécurité et de confort :
 - **Activer l'énumération basée sur l'accès** : Les utilisateurs ne verront que les dossiers et fichiers pour lesquels ils ont une autorisation. S'ils n'ont pas accès à un dossier, il sera invisible pour eux.
 - **Autoriser la mise en cache** : Permet un accès plus fluide et la consultation hors connexion.
- **Encadré 2** : On coche « **Chiffrer l'accès aux données** ». Cela sécurise les transferts de fichiers sur le réseau en les rendant illisibles pour toute personne tentant d'intercepter le trafic.
- **Encadré 3** : On clique sur « **Suivant >** » pour passer aux réglages des droits d'accès.



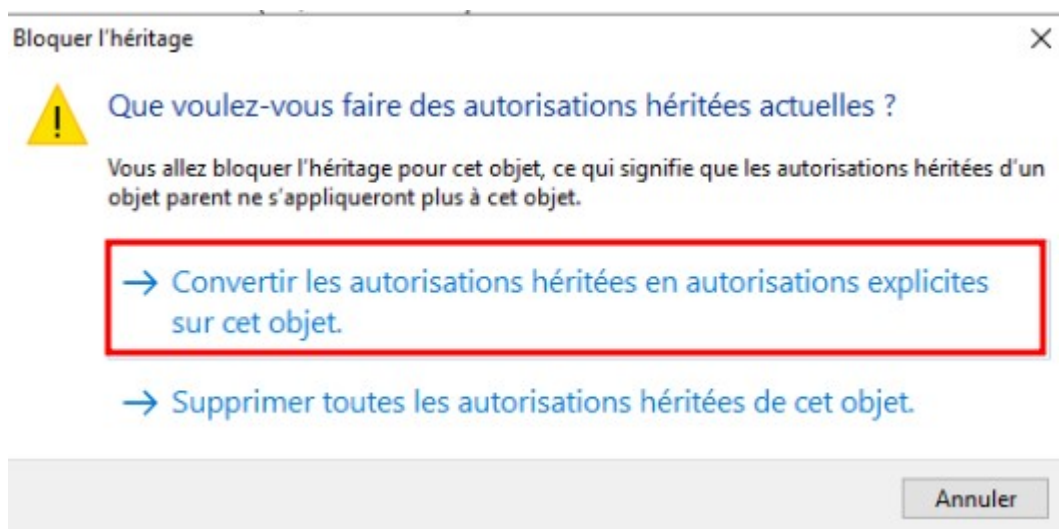
Encadré rouge : On clique sur le bouton « **Personnaliser les autorisations...** ».



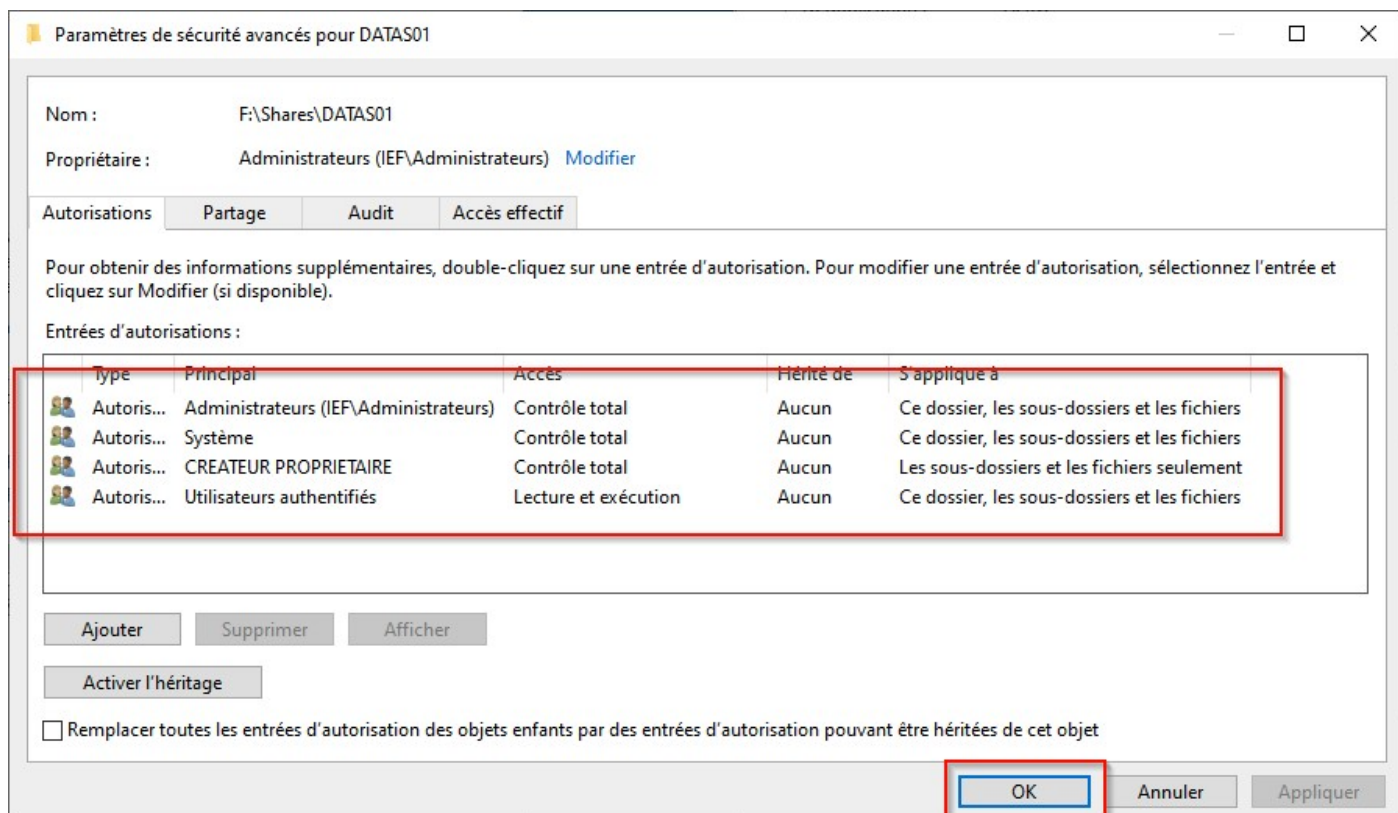
Encadré rouge : On clique sur le bouton « **Désactiver l'héritage** ».



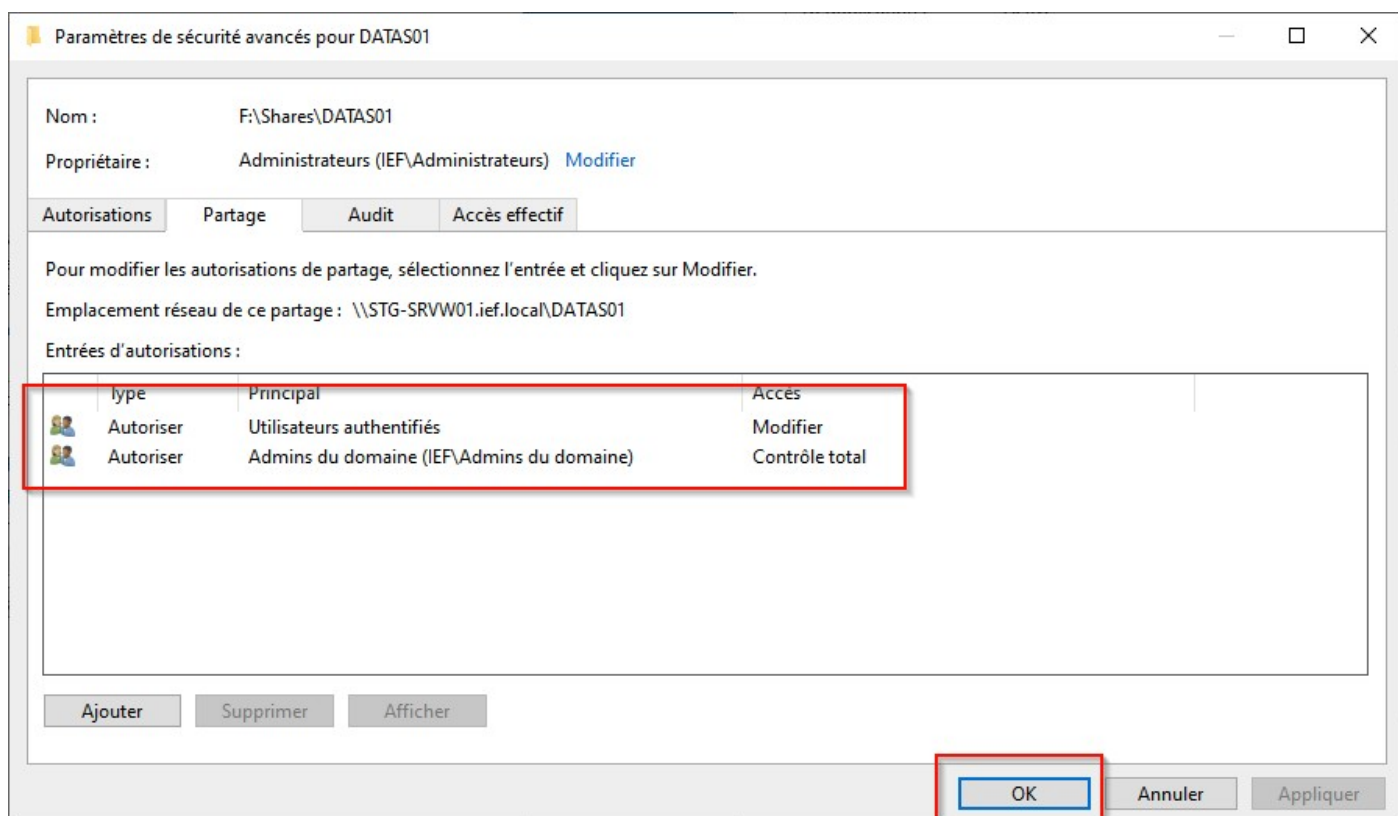
Encadré rouge : Vous cliquez sur « **Convertir les autorisations héritées en autorisations explicites sur cet objet** ».



- **Grand encadré rouge :** On voit la liste des accès au dossier qui ont été "convertis" (Administrateurs, Système, Créateur propriétaire, Utilisateurs authentifiés).
- **Petit encadré rouge :** Vous cliquez sur « **OK** » pour valider cette liste de sécurité pour le dossier physique.



- **Grand encadré rouge** : Vous définissez ici les droits d'accès **via le réseau**. On voit que :
 - Les **Utilisateurs authentifiés** ont un droit de « Modifier ».
 - Les **Admins du domaine** ont le « Contrôle total ».
- **Petit encadré rouge** : Vous cliquez sur « **OK** » pour enregistrer ces droits de partage.



- C'est le résumé final de l'assistant montrant le nom (DATAS01), le protocole (SMB), et les options de sécurité activées (Énumération basée sur l'accès et Chiffrement).

- **Encadré rouge** : Vous cliquez sur le bouton « **Créer** ».

Assistant Nouveau partage

Confirmer les sélections

Sélectionner un profil
Emplacement du partage
Nom de partage
Autres paramètres
Autorisations
Confirmation
Résultats

Vérifiez que les paramètres suivants sont corrects, puis cliquez sur Créer.

EMPLACEMENT DU PARTAGE
Serveur : WS2022-DC1-SA
Rôle du cluster : Non-cluster
Chemin d'accès local : F:\Shares\DATAS01

PROPRIÉTÉS DU PARTAGE
Nom du partage : DATAS01
Protocole : SMB
Énumération basée sur l'accès : Activé
Mise en cache : Activé
BranchCache : Désactivé
Chiffrer les données : Activé

< Précédent Suivant > **Créer** Annuler

L'encadré rouge : Il affiche le résultat final de toutes les étapes précédentes. On confirme que le nouveau partage, nommé **DATAS01**, est désormais actif sur le serveur **WS2022-DC1-SA** et qu'il est correctement lié au dossier local F:\Shares\DATAS01.

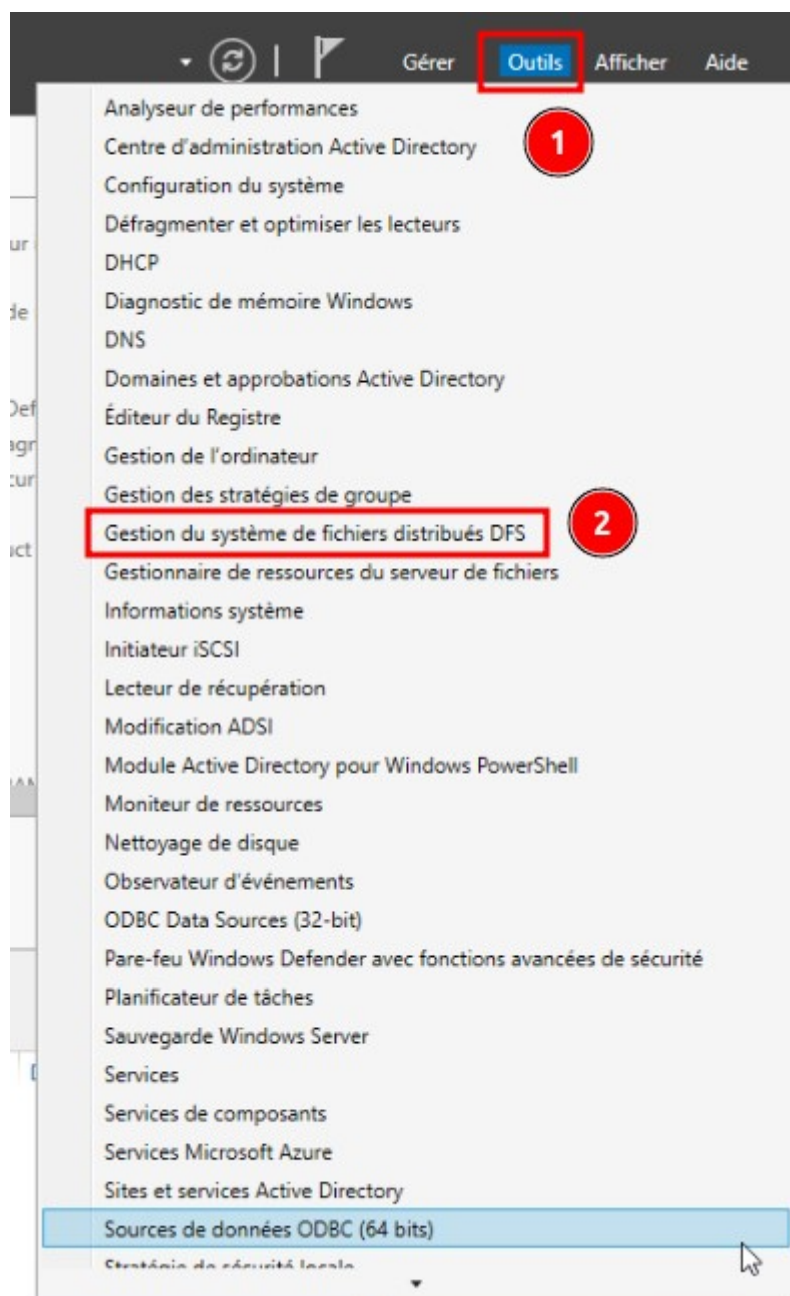
WS2022-DC1-SA (3)		
WS2022-DC1-SA	NETLOGON	C:\Windows\SYSVOL\sysvol\
WS2022-DC1-SA	SYSVOL	C:\Windows\SYSVOL\sysvol
WS2022-DC1-SA	DATAS01	F:\Shares\DATAS01

Reproduisez exactement la même procédure sur les autres contrôleurs de domaine (DC), en prenant soin d'incrémenter le nom du volume et du partage (DATAS02, DATAS03, etc.) pour chaque nouveau serveur.

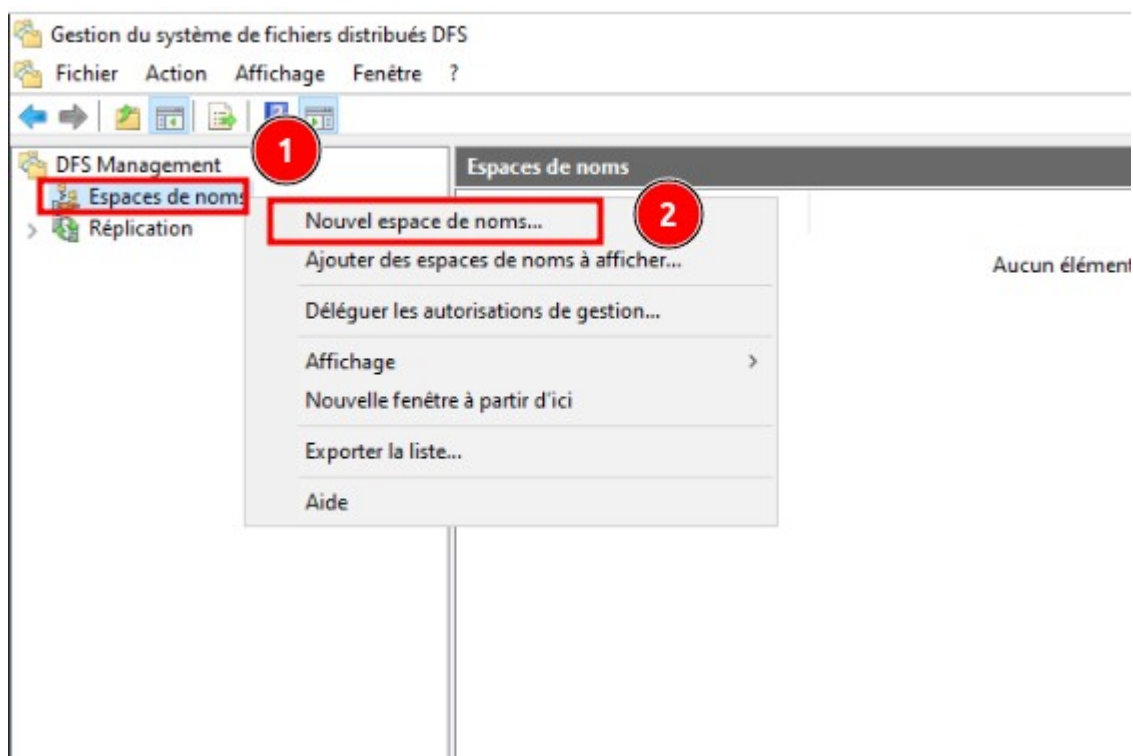
DFS

Configuration de DFS

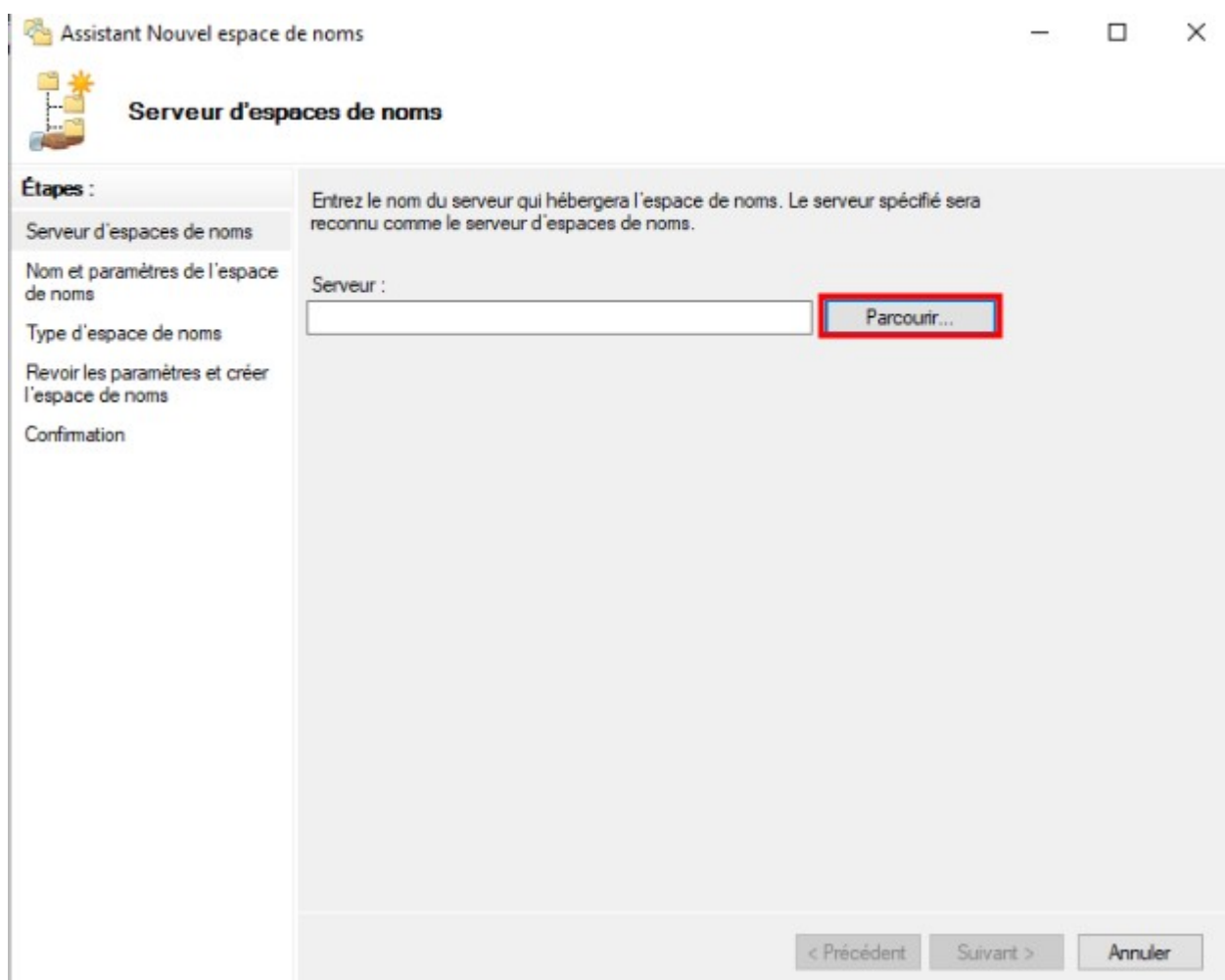
- **Encadré 1** : Dans le Gestionnaire de serveur, vous cliquez sur le menu « **Outils** ».
- **Encadré 2** : Dans la liste qui s'affiche, vous sélectionnez « **Gestion du système de fichiers distribués DFS** ». C'est l'outil qui permet de regrouper plusieurs dossiers partagés (situés sur différents serveurs) sous un seul chemin d'accès réseau unique.



- **Encadré 1** : Dans la console de gestion DFS, vous faites un clic droit sur le dossier « **Espaces de noms** ».
- **Encadré 2** : Vous choisissez l'option « **Nouvel espace de noms...** » pour lancer l'assistant de configuration.



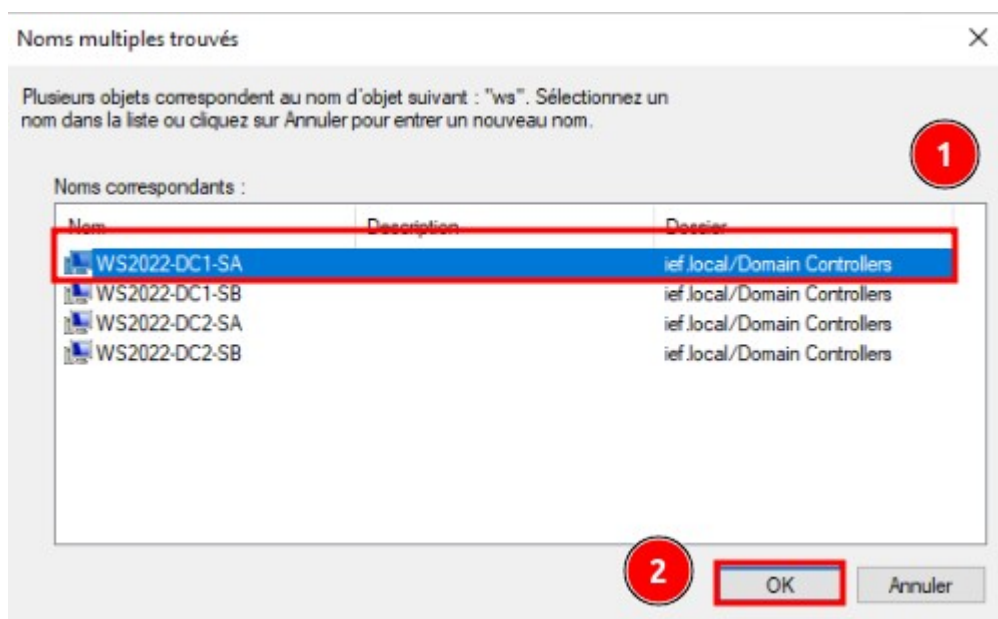
Encadré rouge : Dans l'assistant qui s'est ouvert, à l'étape "Serveur d'espaces de noms", vous cliquez sur le bouton « **Parcourir...** ».



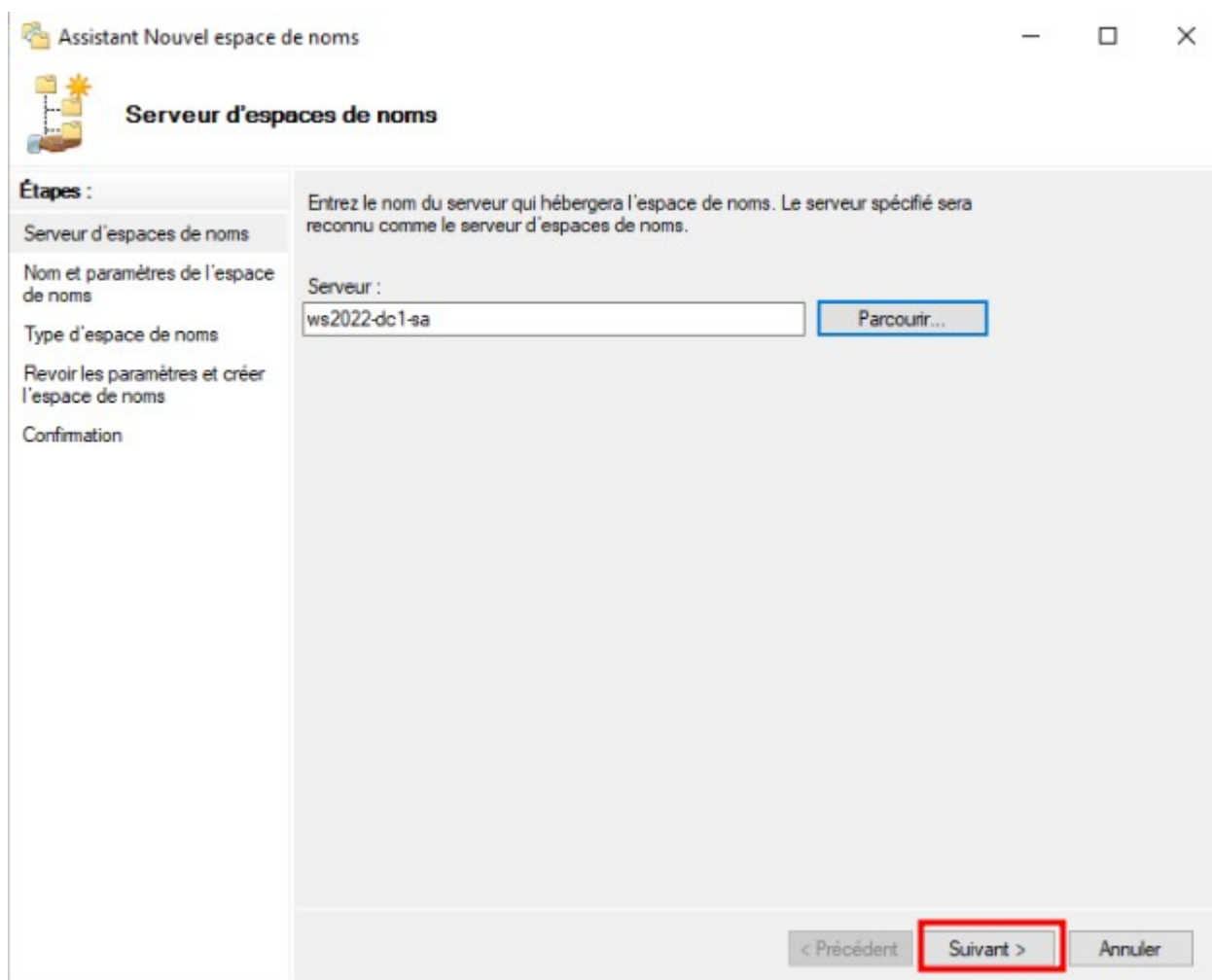
- **Encadré 1 :** Dans la liste des serveurs trouvés, vous sélectionnez le serveur **WS2022-DC1-SA**. C'est lui

qui servira de point d'entrée pour les utilisateurs.

- **Encadré 2** : Vous cliquez sur le bouton « **OK** » pour valider votre choix et revenir à l'assistant.



- **Encadré rouge** : Une fois le serveur ws2022-dc1-sa sélectionné, vous cliquez sur « **Suivant >** » pour passer à l'étape suivante de l'assistant.



- **Encadré 1** : Dans le champ « Nom », vous saisissez « **Intranet** ». C'est le nom qui apparaîtra dans le

chemin réseau final (ex: \\Domaine\Intranet).

- **Encadré 2** : Vous cliquez sur le bouton « **Modifier les paramètres...** » pour configurer l'emplacement local et les droits d'accès au dossier racine du DFS.

Assistant Nouvel espace de noms

Nom et paramètres de l'espace de noms

Étapes :

- Serveur d'espaces de noms
- Nom et paramètres de l'espace de noms**
- Type d'espace de noms
- Revoir les paramètres et créer l'espace de noms
- Confirmation

Entrez un nom pour l'espace de noms. Ce nom apparaîtra après le nom du serveur ou du domaine dans le chemin d'accès de l'espace de noms, par exemple \\Serveur\Nom or \\Domaine\Nom.

Nom :

Exemple : Public

Au besoin, l'Assistant créera un dossier partagé sur le serveur d'espaces de noms. Pour modifier les paramètres du dossier partagé (chemin d'accès ou autorisations), cliquez sur Modifier les paramètres.

< Précédent Suivant > Annuler

- **Encadré 1** : Vous définissez le chemin d'accès local où sera créé le dossier racine : **F:\Shares\DFS\$**. Le signe \$ rend le dossier racine "caché" si quelqu'un explore directement le disque.
- **Encadré 2** : Vous sélectionnez l'option de sécurité : « **Les administrateurs ont un accès total, les autres ont un accès en lecture seule** ». Cela protège la structure de votre DFS contre les modifications accidentelles par les utilisateurs.
- **Encadré 3** : Vous cliquez sur « **OK** » pour valider ces réglages.

Modifier les paramètres

Serveur d'espaces de noms :
ws2022-dc1-sa

Dossier partagé : **1**
Intranet

Chemin d'accès local du dossier partagé :
F:\Shares\DFS\$ Parcourir...

Autorisations du dossier partagé :

☐ Tous les utilisateurs disposent d'autorisations de lecture seule

2 ☒ Tous les utilisateurs disposent d'autorisations de lecture/écriture

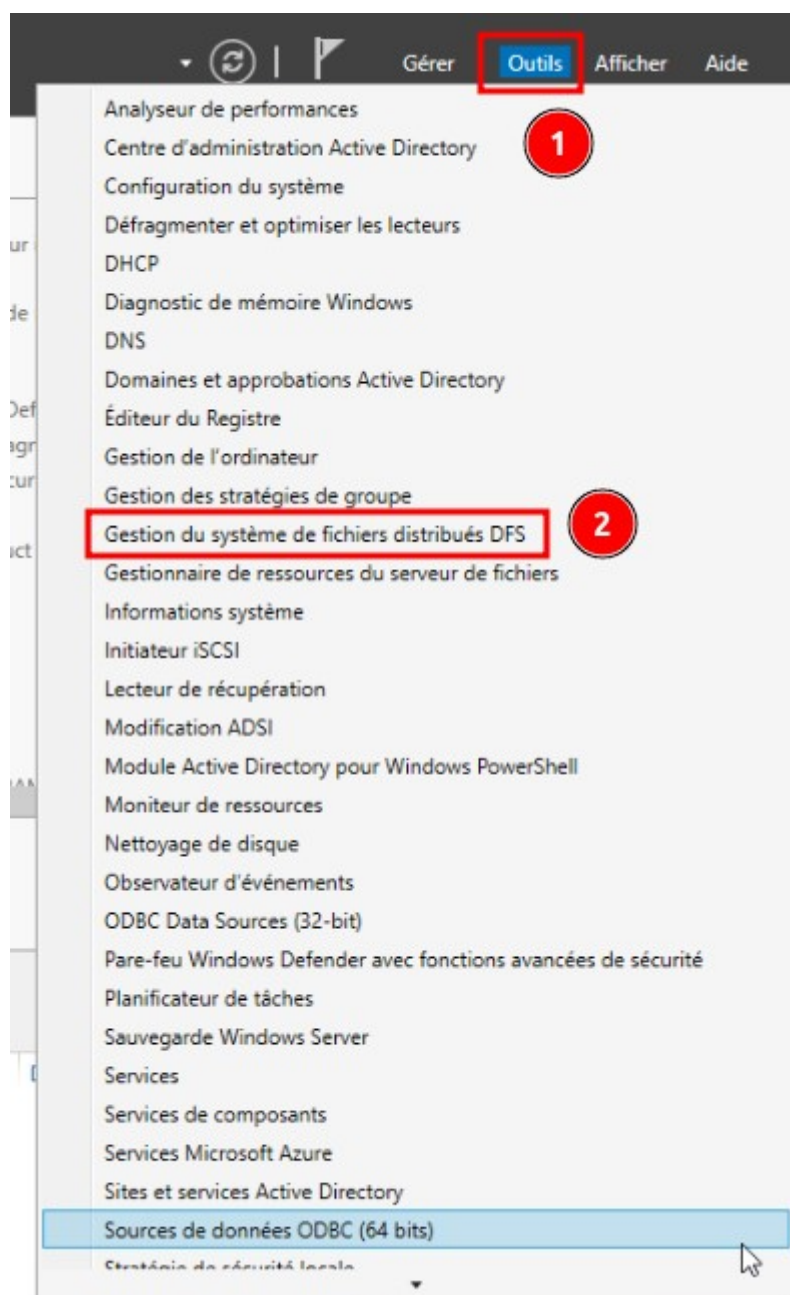
☒ Les administrateurs ont un accès total, les autres ont un accès en lecture seule

☐ Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture

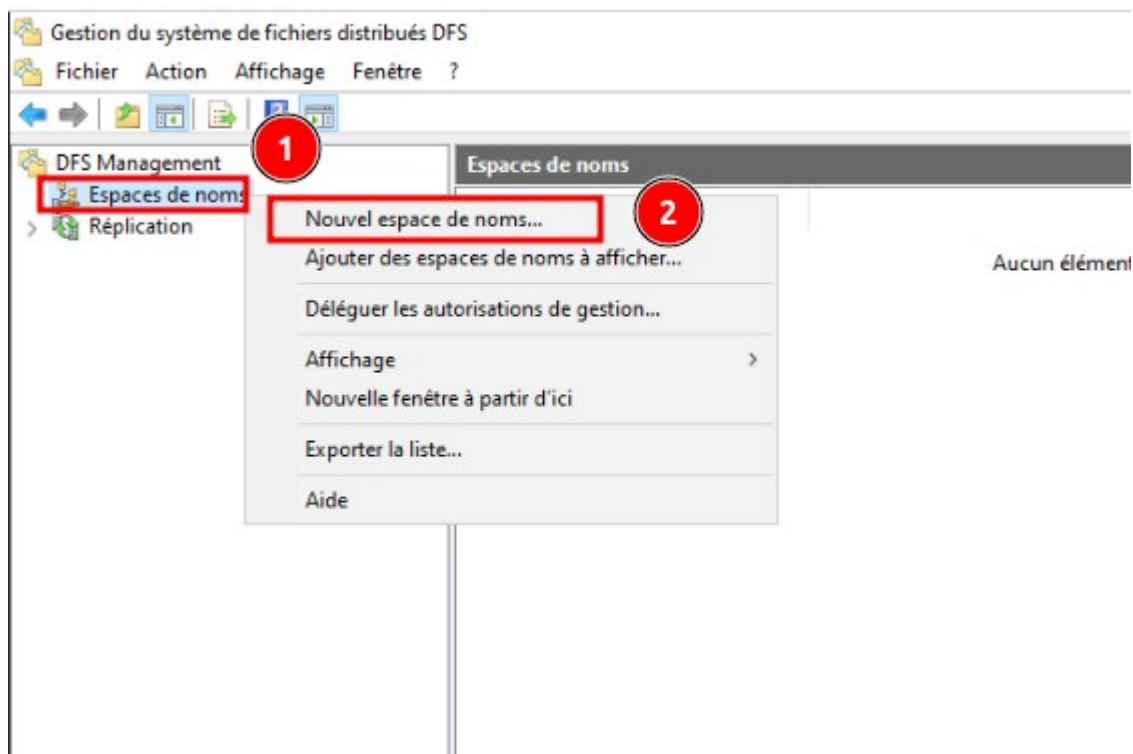
☐ Utiliser des autorisations personnalisées : Personnaliser...

3 OK Annuler

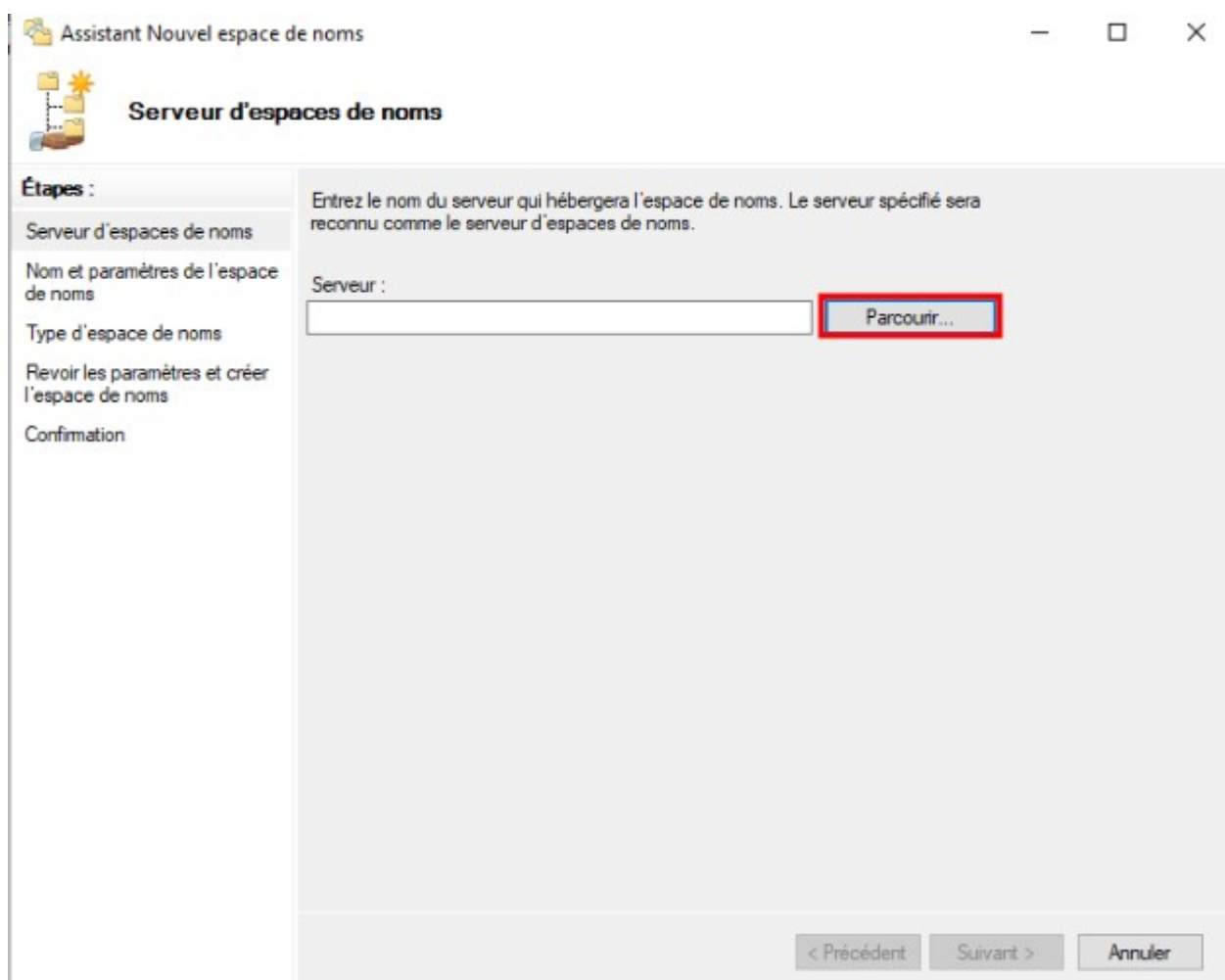
- **Encadré 1 & 2** : Cette image montre simplement comment revenir à la console si nécessaire via le menu « **Outils** » puis « **Gestion du système de fichiers distribués DFS** ».



- **Encadré 1** : Dans la console de gestion DFS, vous faites un clic droit sur « **Espaces de noms** ».
- **Encadré 2** : Vous sélectionnez « **Nouvel espace de noms...** » pour démarrer la configuration.

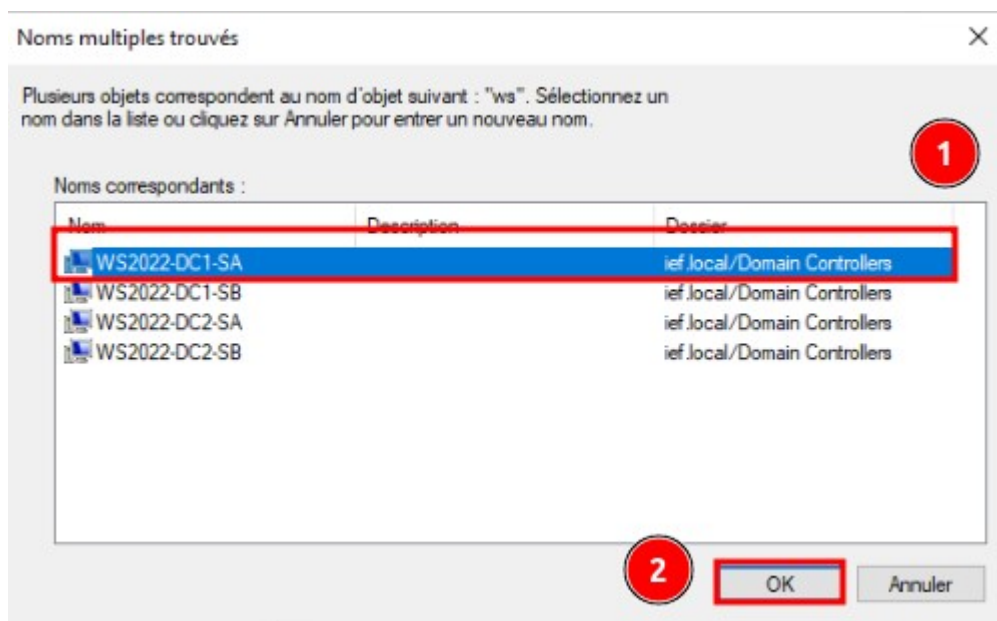


- **Encadré rouge** : À la première étape de l'assistant ("Serveur d'espaces de noms"), vous cliquez sur le bouton « **Parcourir...** ». L'objectif est de désigner le serveur qui va gérer cet espace de noms.

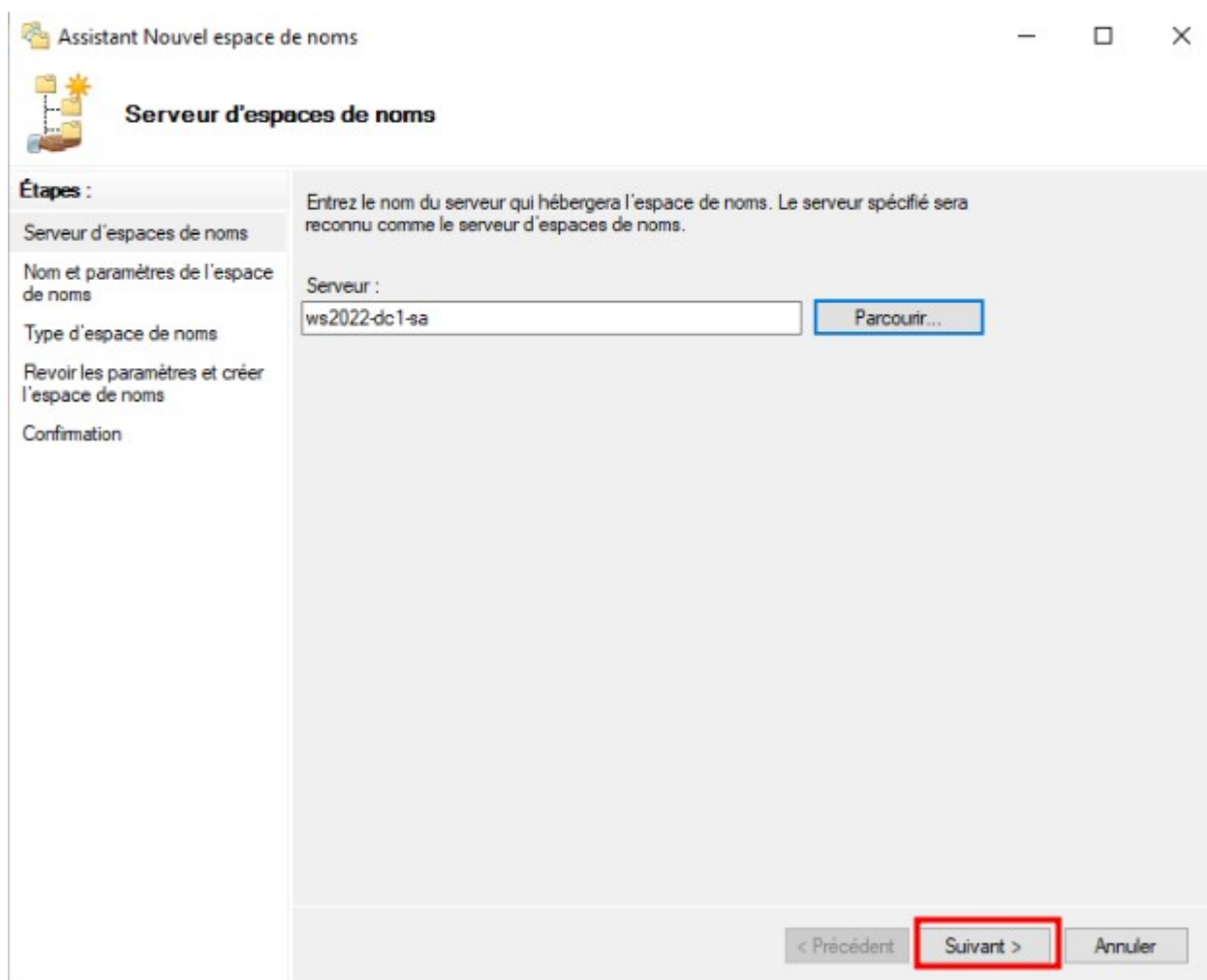


- **Encadré 1** : Dans les résultats de la recherche, vous sélectionnez le serveur **WS2022-DC1-SA**.

- **Encadré 2** : Vous cliquez sur le bouton « **OK** » pour valider ce choix.



- **Encadré rouge** : Le nom du serveur apparaît désormais dans le champ prévu. Vous cliquez sur le bouton « **Suivant** > » pour passer à l'étape du nommage de votre espace de noms.



- **Encadré 1** : Vous saisissez le nom « **Intranet** » dans le champ "Nom". C'est ce nom qui sera utilisé par les utilisateurs dans leur barre d'adresse réseau (ex: \\domaine.local\Intranet).

- **Encadré 2** : Vous cliquez sur le bouton « **Modifier les paramètres...** ». Cela permet de définir le chemin local sur le disque du serveur et de régler les autorisations de partage pour la racine du DFS.

- **Encadré rouge** : Une fois le nom saisi et les paramètres réglés, vous cliquez sur le bouton « **Suivant >** ».

The screenshot shows a Windows XP-style window titled 'Assistant Nouvel espace de noms'. The window has a standard title bar with minimize, maximize, and close buttons. Below the title bar is a toolbar with a folder icon and a sun icon. The main content area is divided into two panes. The left pane, titled 'Étapes :', contains a list of steps: 'Serveur d'espaces de noms' (highlighted in blue), 'Nom et paramètres de l'espace de noms' (current step), 'Type d'espace de noms', 'Revoir les paramètres et créer l'espace de noms', and 'Confirmation'. The right pane, titled 'Nom et paramètres de l'espace de noms', contains instructions: 'Entrez un nom pour l'espace de noms. Ce nom apparaîtra après le nom du serveur ou du domaine dans le chemin d'accès de l'espace de noms, par exemple \\Serveur\Nom or \\Domaine\Nom.' Below this is a text box labeled 'Nom :' containing the word 'Intranet'. Below the text box is an example: 'Exemple : Public'. At the bottom of the right pane is a button labeled 'Modifier les paramètres...'. At the bottom of the window are three buttons: '< Précédent', 'Suivant >' (highlighted with a red rectangle), and 'Annuler'.

Assistant Nouvel espace de noms

Nom et paramètres de l'espace de noms

Étapes :

- Serveur d'espaces de noms
- Nom et paramètres de l'espace de noms
- Type d'espace de noms
- Revoir les paramètres et créer l'espace de noms
- Confirmation

Entrez un nom pour l'espace de noms. Ce nom apparaîtra après le nom du serveur ou du domaine dans le chemin d'accès de l'espace de noms, par exemple \\Serveur\Nom or \\Domaine\Nom.

Nom : Intranet

Exemple : Public

Au besoin, l'Assistant créera un dossier partagé sur le serveur d'espaces de noms. Pour modifier les paramètres du dossier partagé (chemin d'accès ou autorisations), cliquez sur Modifier les paramètres.

Modifier les paramètres...

< Précédent Suivant > Annuler

- **Contexte** : Vous avez laissé l'option « **Espace de noms de domaine** » sélectionnée par défaut. Cela permet de stocker la configuration dans l'Active Directory et assure une haute disponibilité si vous ajoutez d'autres serveurs plus tard.
- **Encadré rouge** : Vous cliquez sur le bouton « **Suivant** > ».

Assistant Nouvel espace de noms

Type d'espace de noms

Étapes :

- Serveur d'espaces de noms
- Nom et paramètres de l'espace de noms
- Type d'espace de noms
- Revoir les paramètres et créer l'espace de noms
- Confirmation

Sélectionnez le type d'espace de noms à créer.

☒ Espace de noms de domaine

Un espace de noms de domaine est stocké sur un ou plusieurs serveurs d'espaces de noms et dans les services de domaine Active Directory. Vous pouvez accroître la disponibilité d'un espace de noms de domaine en utilisant plusieurs serveurs. Lorsqu'il est créé dans le mode Windows Server 2008, l'espace de noms prend en charge une plus grande extensibilité et énumération basée sur l'accès.

☒ Activer le mode Windows Server 2008

Aperçu de l'espace de noms de domaine :

\\ief.local\Intranet

☐ Espace de noms autonome

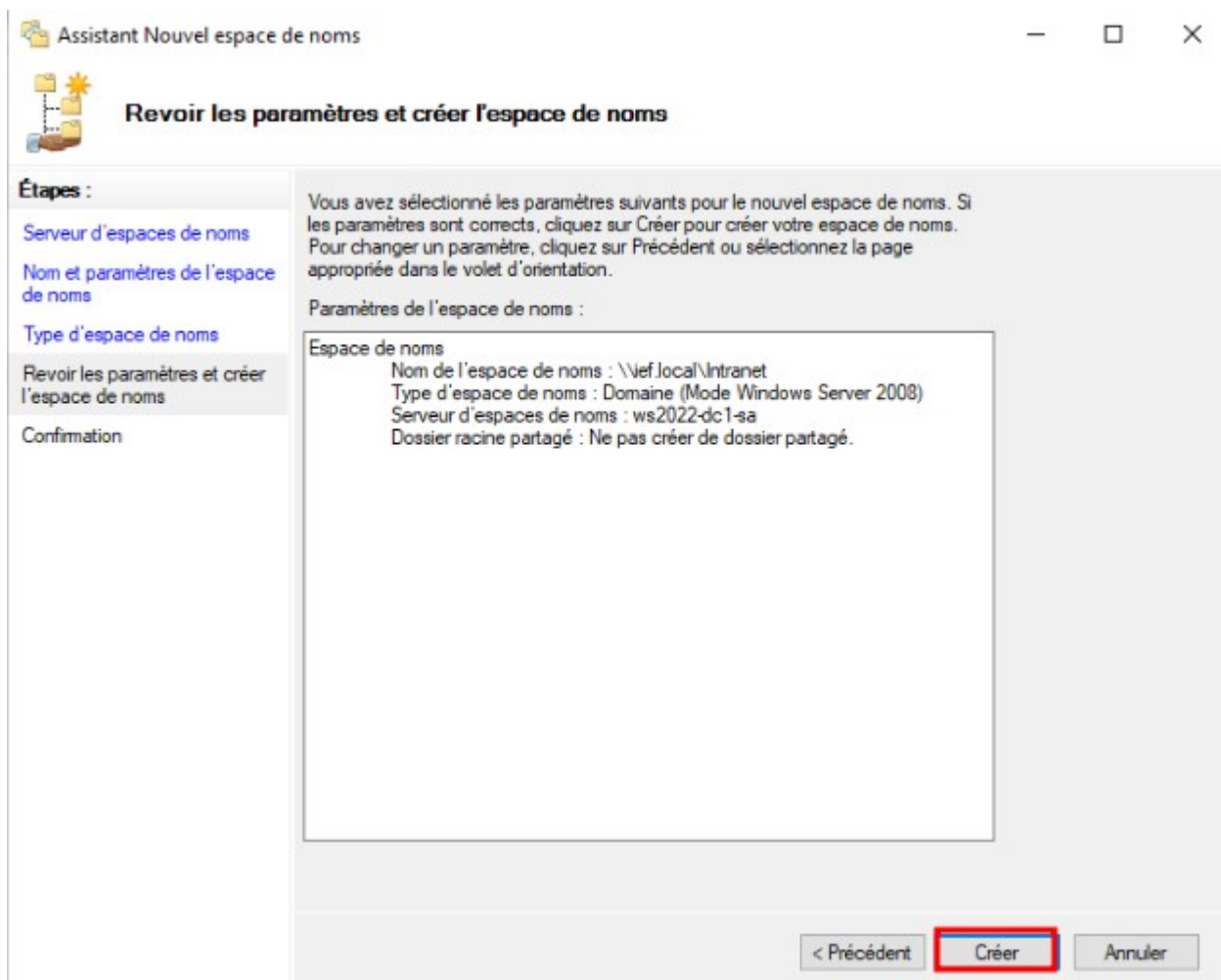
Un espace de noms autonome est stocké sur un serveur d'espaces de noms unique. Lorsqu'il est hébergé sur un cluster de basculement, sa disponibilité est accrue.

Aperçu d'un espace de noms autonome :

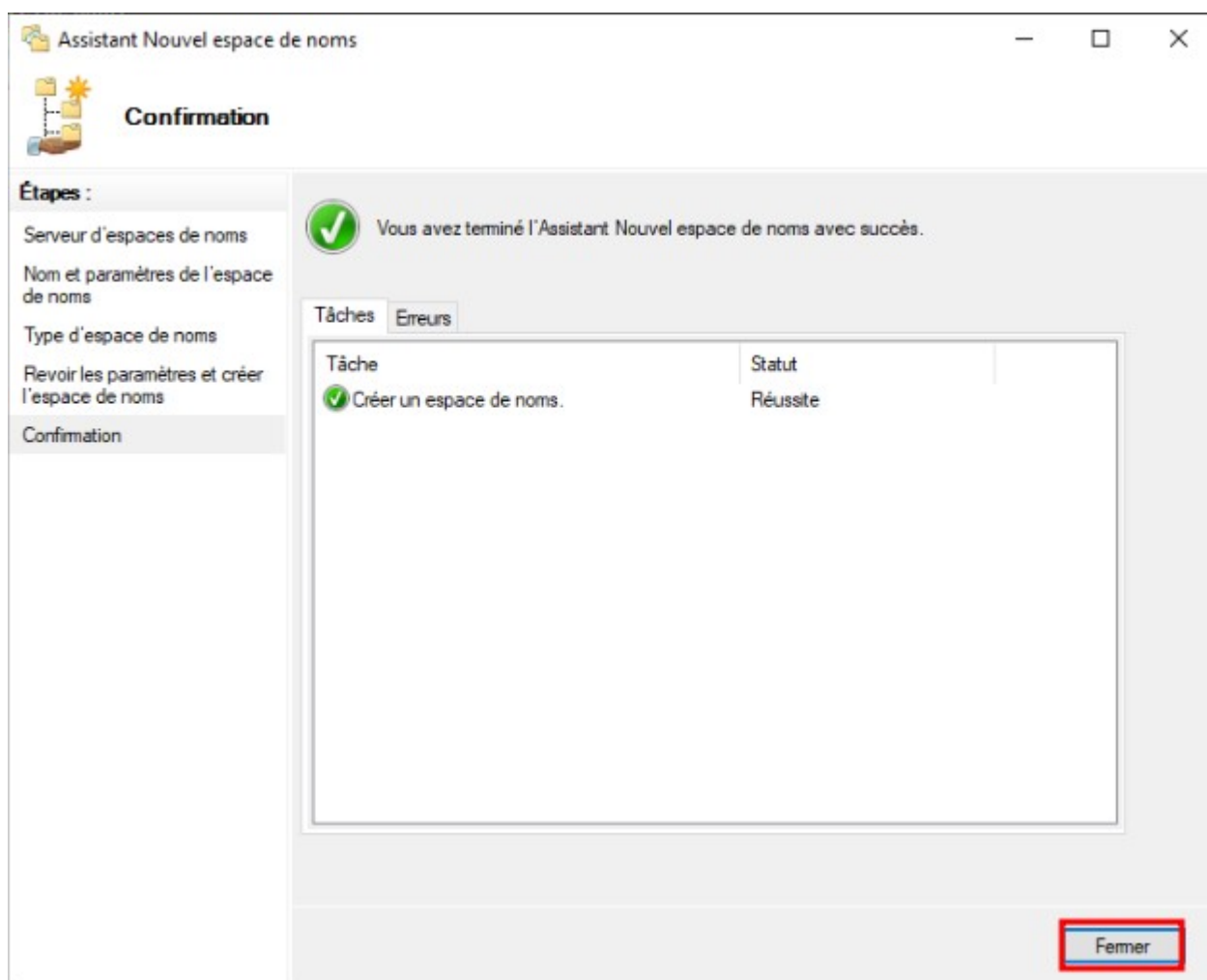
\\ws2022-dc1-sa\Intranet

< Précédent **Suivant >** Annuler

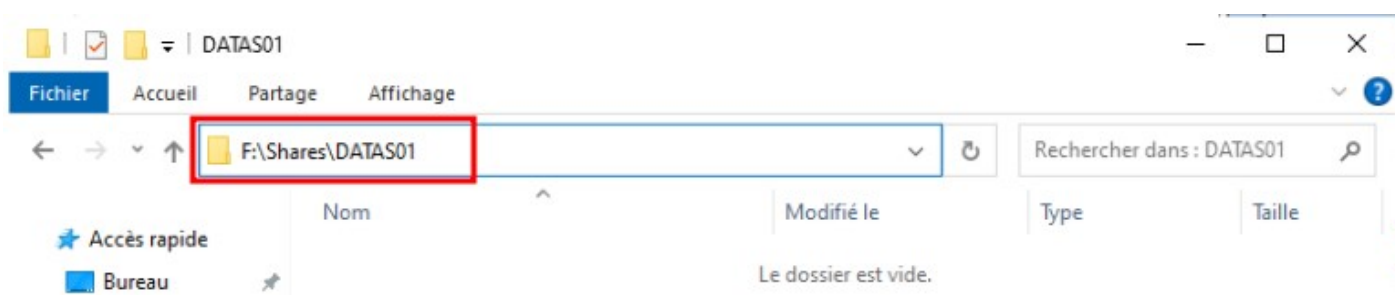
- **Contenu :** Cet écran affiche le résumé de vos choix : Nom (\\ief.local\Intranet), Type (Domaine) et Serveur hôte (ws2022-dc1-sa).
- **Encadré rouge :** Vous cliquez sur le bouton « **Créer** ». C'est l'action finale qui génère réellement l'espace de noms sur le serveur.



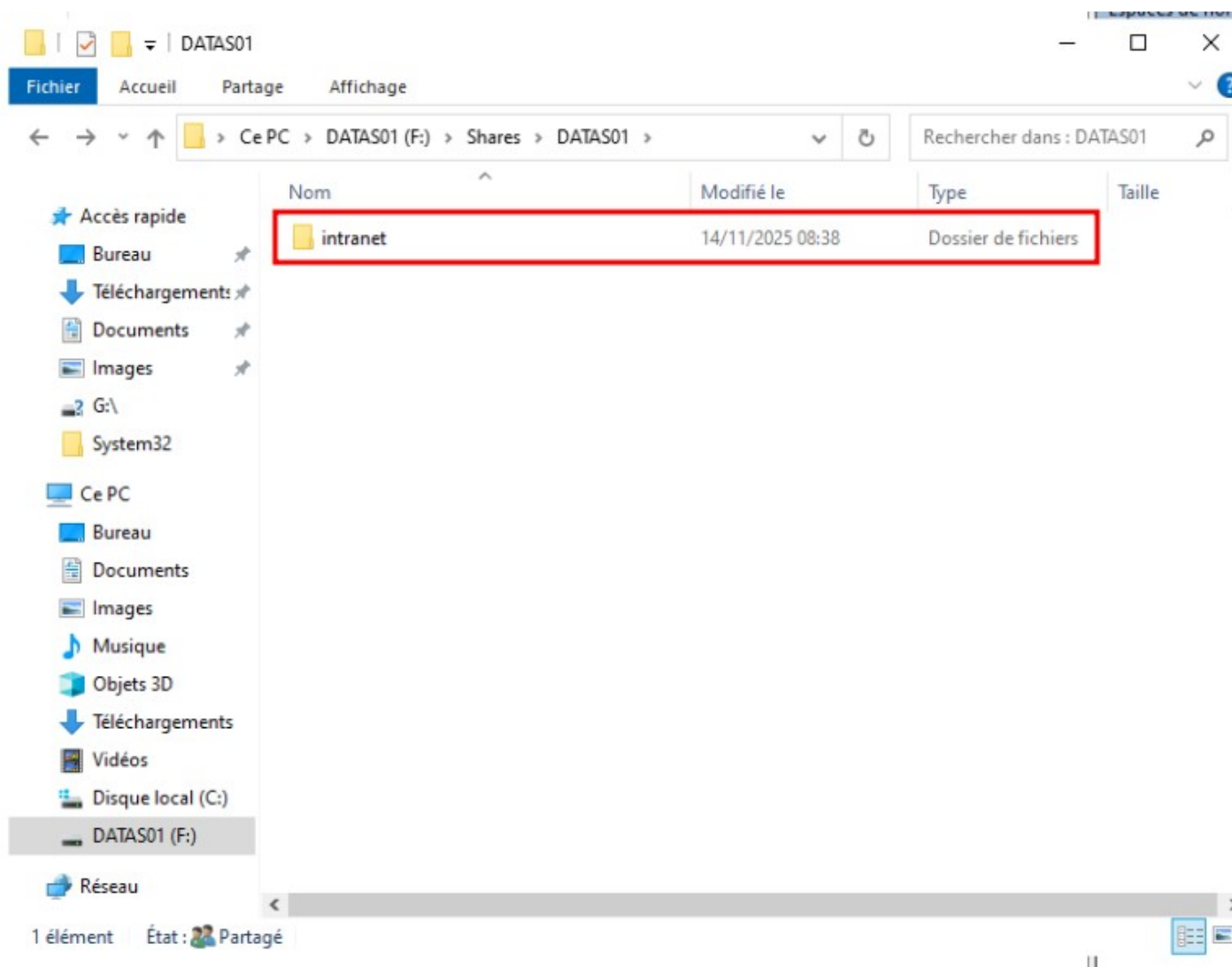
- **Encadré rouge** : L'assistant confirme que la création de l'espace de noms a réussi. Vous cliquez sur le bouton « **Fermer** » pour quitter la fenêtre.



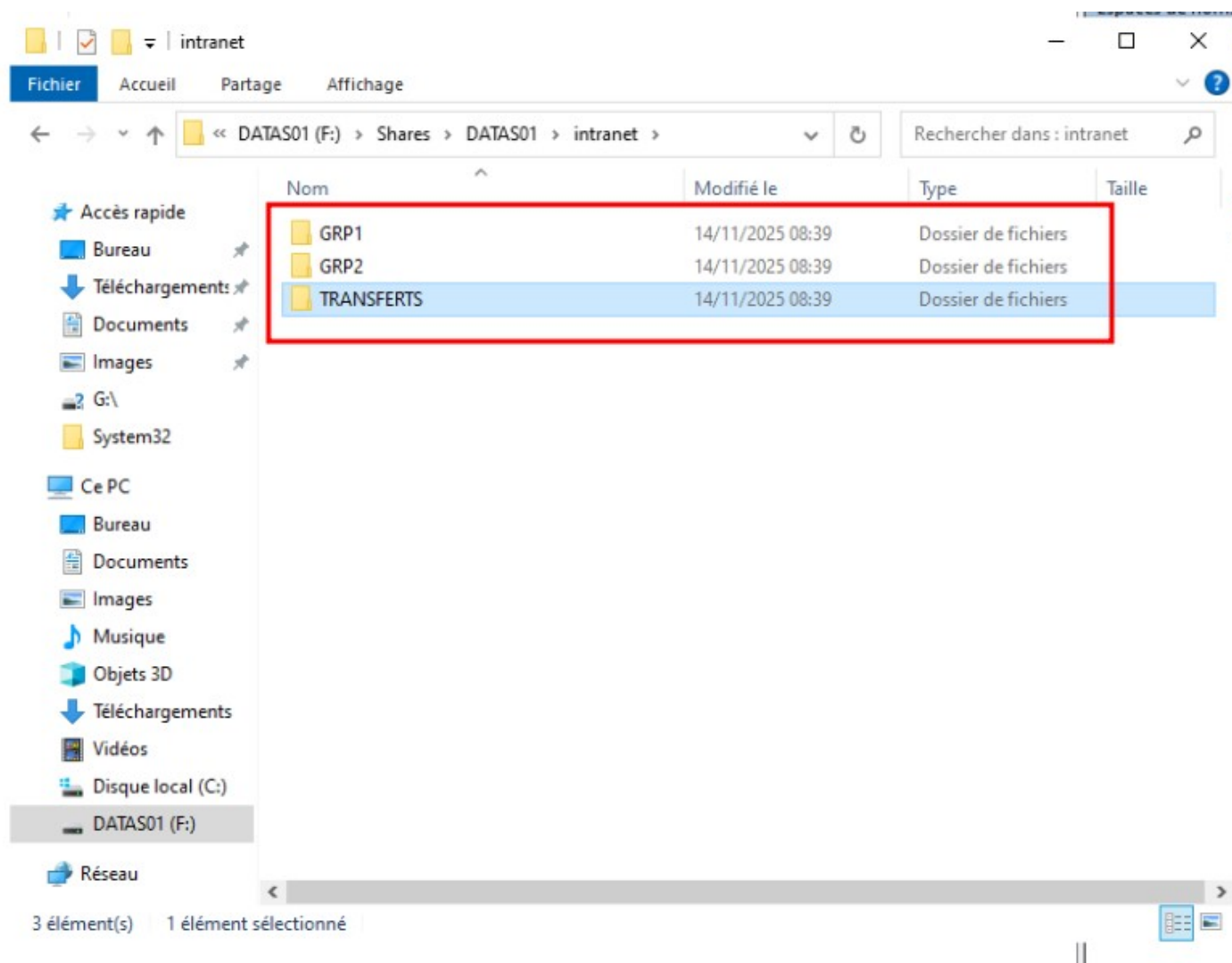
- **Encadré rouge** : Vous ouvrez l'Explorateur de fichiers et vous vous rendez dans le chemin local **F:\Shares\DATAS01**. C'est le volume de 64 Go que vous avez préparé au tout début.



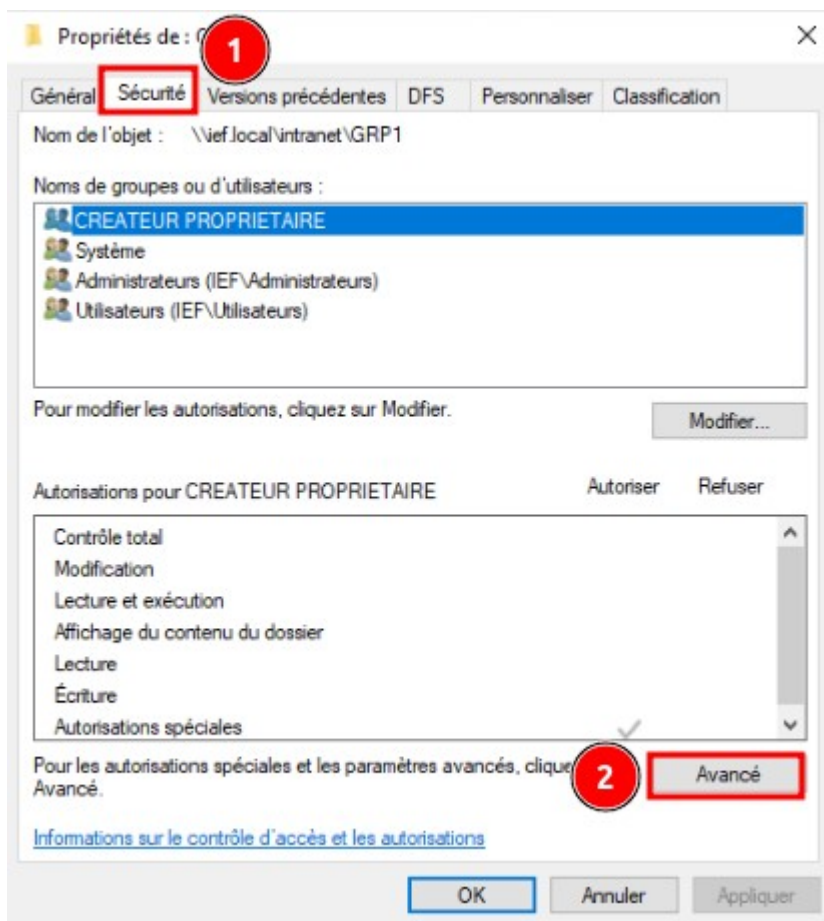
Encadré rouge : À l'intérieur de DATAS01, vous créez un nouveau dossier nommé « **intranet** ».



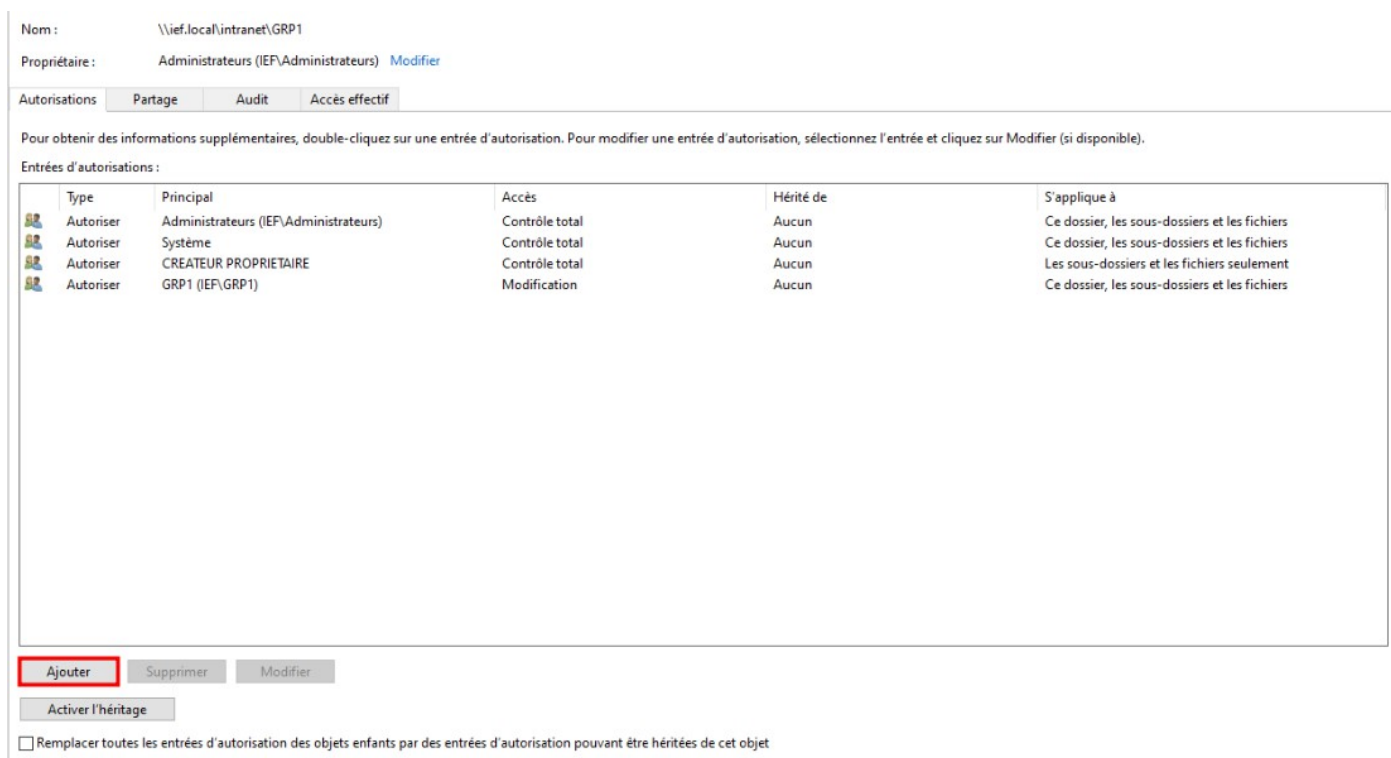
- **Encadré rouge** : À l'intérieur du dossier "intranet", vous créez la structure cible pour vos utilisateurs :
 - **GRP1** : pour un premier groupe de service.
 - **GRP2** : Pour un second groupe.
 - **TRANSFERTS** : Un dossier destiné aux échanges de fichiers entre utilisateurs.



- **Encadré 1 :** On se rend dans l'onglet « **Sécurité** » du dossier.
- **Encadré 2 :** On clique sur le bouton « **Avancé** » pour ouvrir la gestion fine des droits.



- **Encadré rouge** : On clique sur le bouton « **Ajouter** » pour créer une nouvelle règle d'accès spécifique à ce dossier.



- **Encadré 1** : On a sélectionné le groupe d'utilisateurs concerné : **GRP1 (IEF\GRP1)**.
- **Encadré 2** : On définit les droits précis. Ici, on coche les cases pour permettre la lecture, l'affichage et l'écriture de données, tout en restreignant certaines actions (comme le contrôle total).

- **Encadré 3** : On clique sur « **OK** » pour valider ces permissions.

Autorisations pour GRP1

Principal : GRP1 (IEF\GRP1) Sélectionnez un principal 1

Type : Autoriser

S'applique à : Ce dossier, les sous-dossiers et les fichiers

Autorisations avancées :

<input type="checkbox"/> Contrôle total	<input type="checkbox"/> Attributs d'écriture
<input checked="" type="checkbox"/> Parcours du dossier/exécuter le fichier	<input type="checkbox"/> Écriture d'attributs étendus
<input checked="" type="checkbox"/> Liste du dossier/lecture de données	<input checked="" type="checkbox"/> Suppression de sous-dossier et fichier
<input checked="" type="checkbox"/> Attributs de lecture	<input type="checkbox"/> Suppression
<input checked="" type="checkbox"/> Lecture des attributs étendus	<input checked="" type="checkbox"/> Autorisations de lecture
<input checked="" type="checkbox"/> Création de fichier/écriture de données	<input checked="" type="checkbox"/> Modifier les autorisations
<input checked="" type="checkbox"/> Création de dossier/ajout de données	<input checked="" type="checkbox"/> Appropriation

☐ Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

Effacer tout

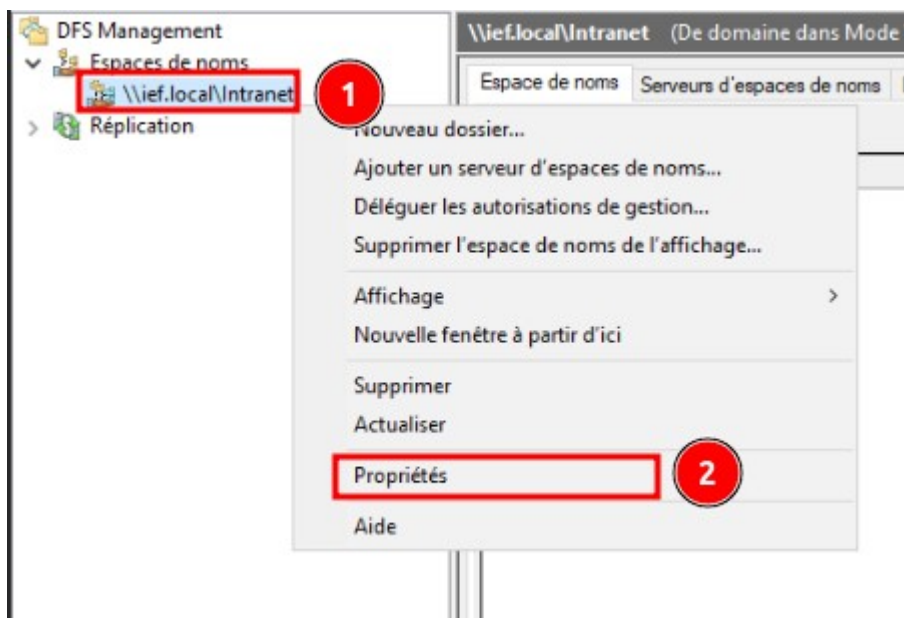
Ajoutez une condition pour limiter l'accès. Les autorisations spécifiées ne seront accordées au principal que si les conditions sont remplies.

Ajouter une condition

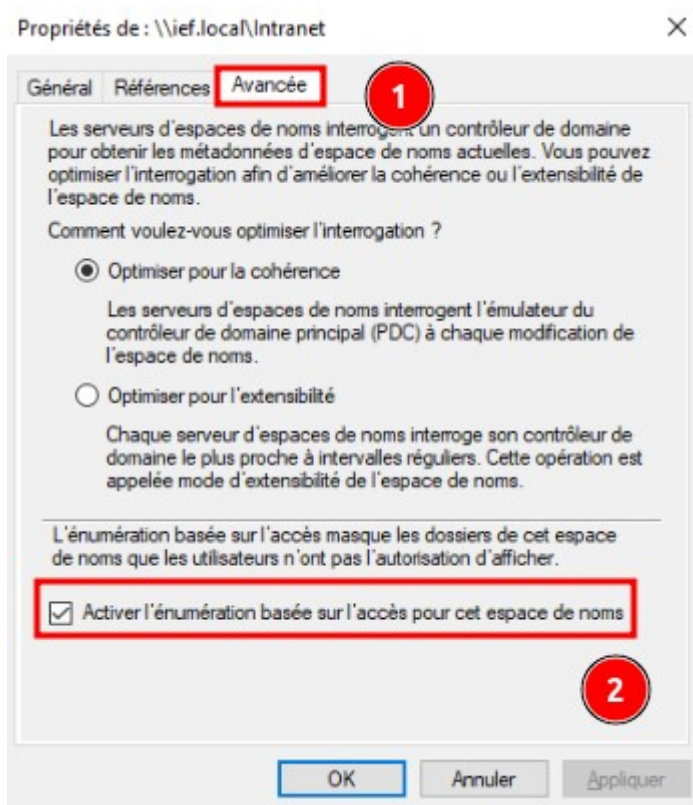
OK Annuler

Faire pareil pour le dossier groupe 2.

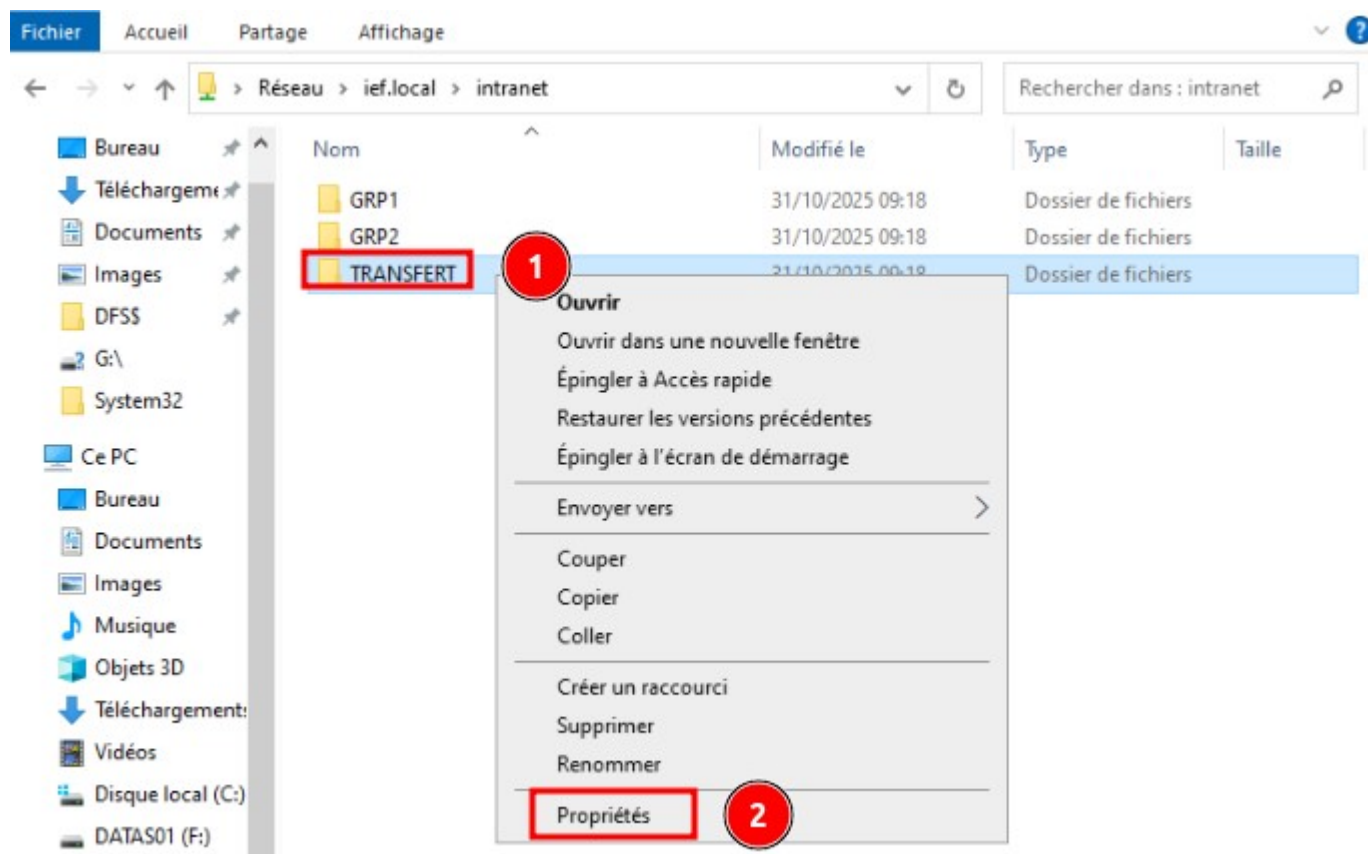
- **Encadré 1** : Dans la console DFS Management, on effectue un clic droit sur l'espace de noms créé précédemment : **\\ief.local\Intranet**.
- **Encadré 2** : On sélectionne l'option « **Propriétés** » dans le menu contextuel.
 - Objectif : Probablement pour vérifier la configuration de l'espace de noms ou pour y ajouter des dossiers cibles dans les étapes suivantes.



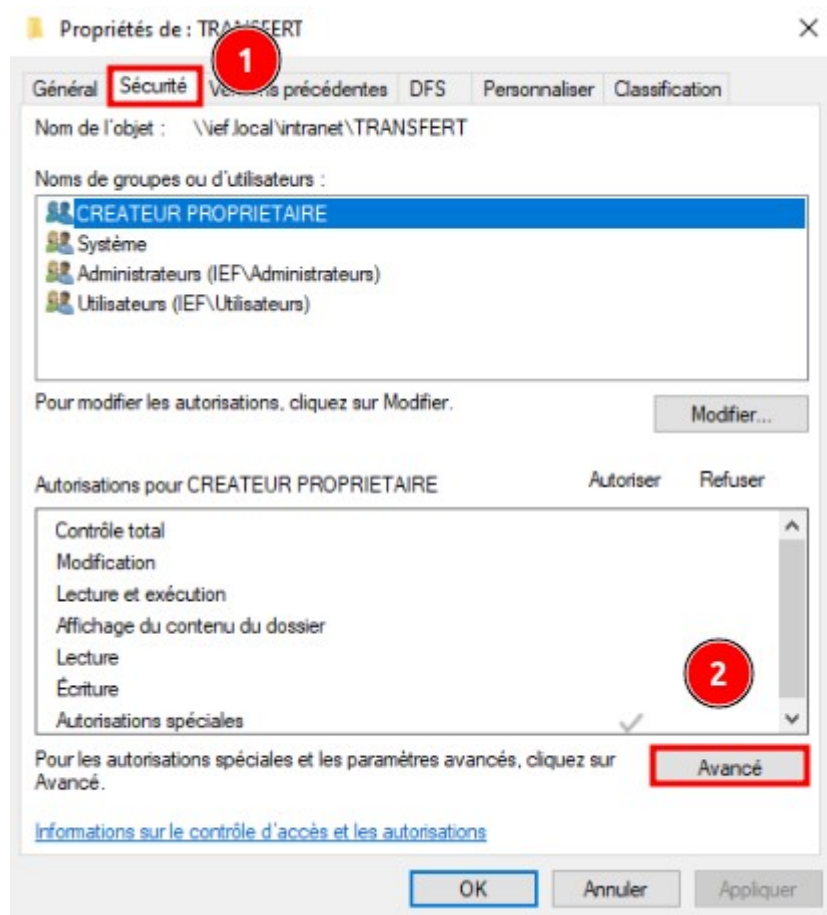
- **Encadré 1** : Dans les propriétés de l'espace de noms, on se trouve sur l'onglet « **Avancé** ».
- **Encadré 2** : On coche la case « **Activer l'énumération basée sur l'accès pour cet espace de noms** ».



- **Encadré 1** : On effectue un clic droit sur le dossier « **TRANSFERT** » que l'on a créé précédemment.
- **Encadré 2** : On sélectionne l'option « **Propriétés** » dans le menu.



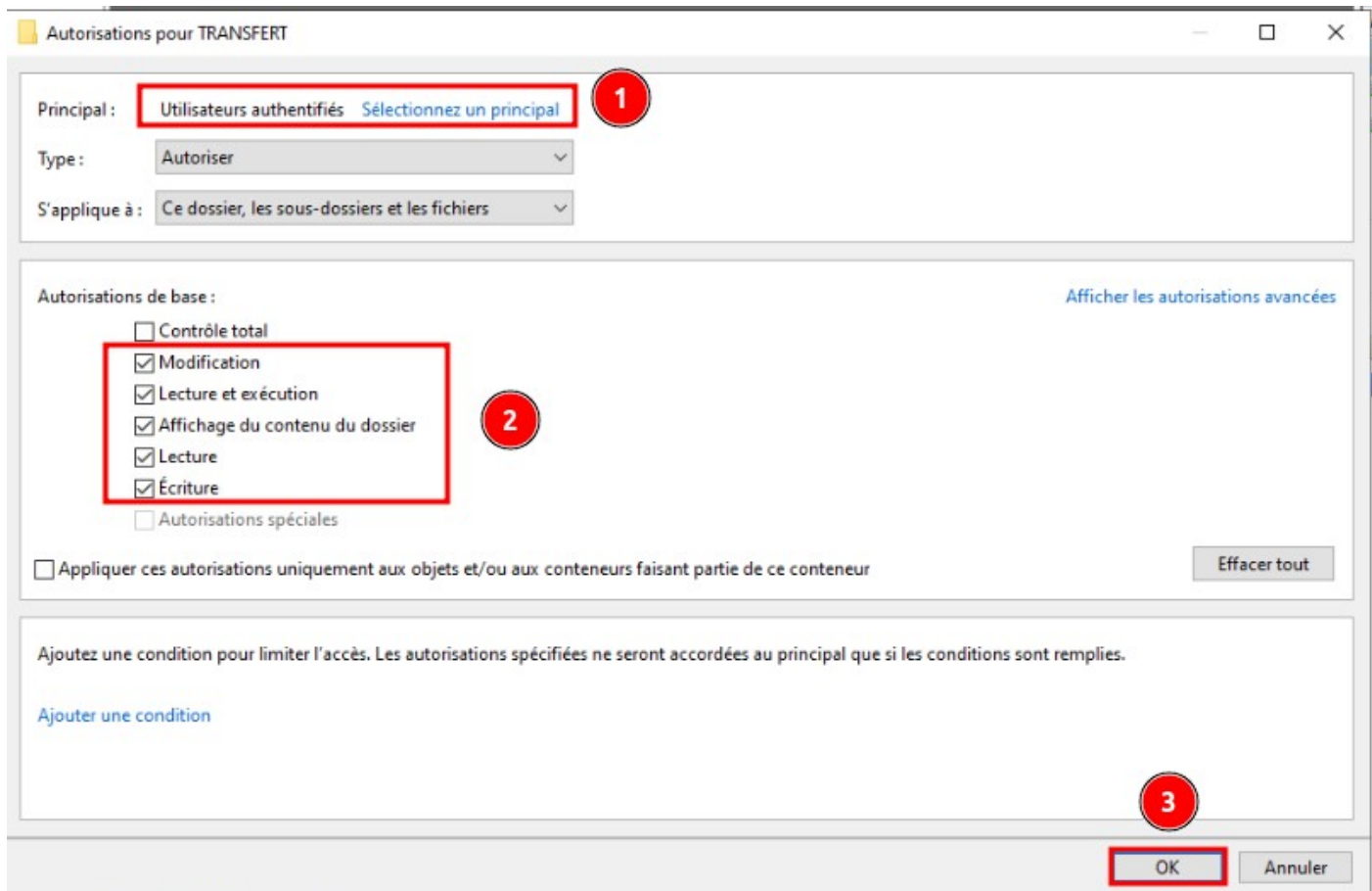
- **Encadré 1** : On se rend sur l'onglet « **Sécurité** ».
- **Encadré 2** : On clique sur le bouton « **Avancé** » pour modifier les entrées d'autorisation.



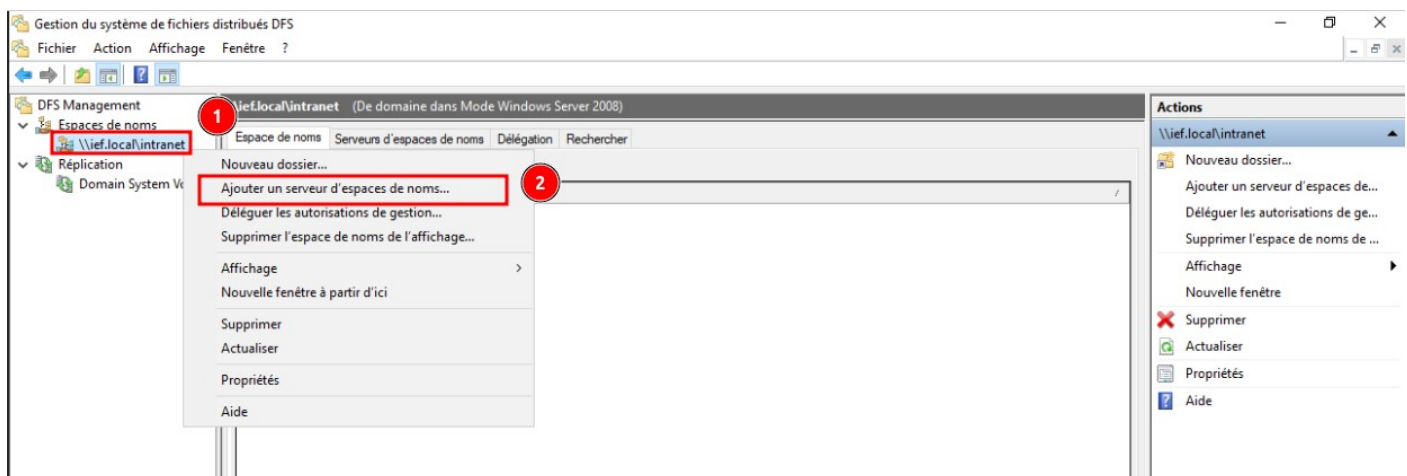
- **Encadré 1** : On a sélectionné le principal « **Utilisateurs authentifiés** » (ce qui regroupe toutes les

personnes ayant une session sur le domaine).

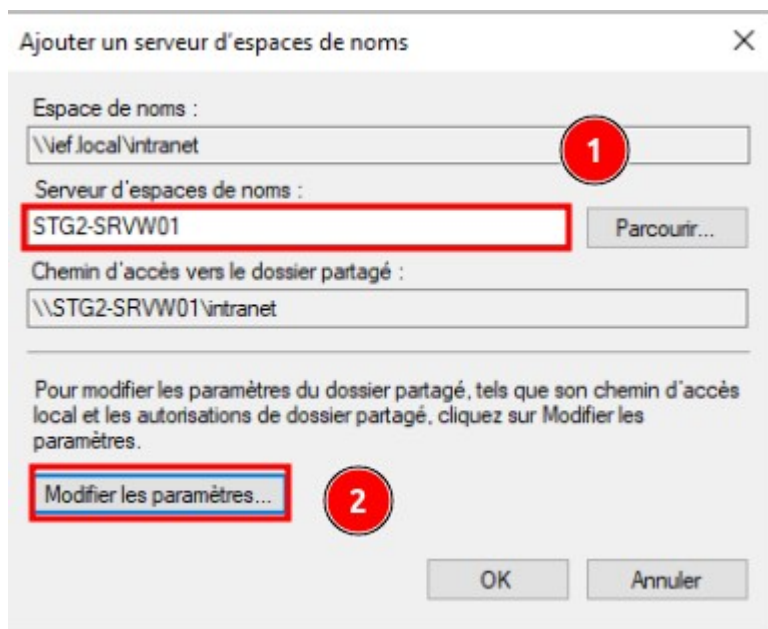
- **Encadré 2** : On définit les droits pour ce dossier d'échange. On coche les cases « **Modification** », « **Lecture et exécution** », « **Affichage du contenu** », « **Lecture** » et « **Écriture** ».
 - **Objectif** : Comme c'est un dossier de transfert, tout le monde doit pouvoir y déposer, lire et modifier des fichiers.
- **Encadré 3** : On clique sur « **OK** » pour valider et appliquer ces droits



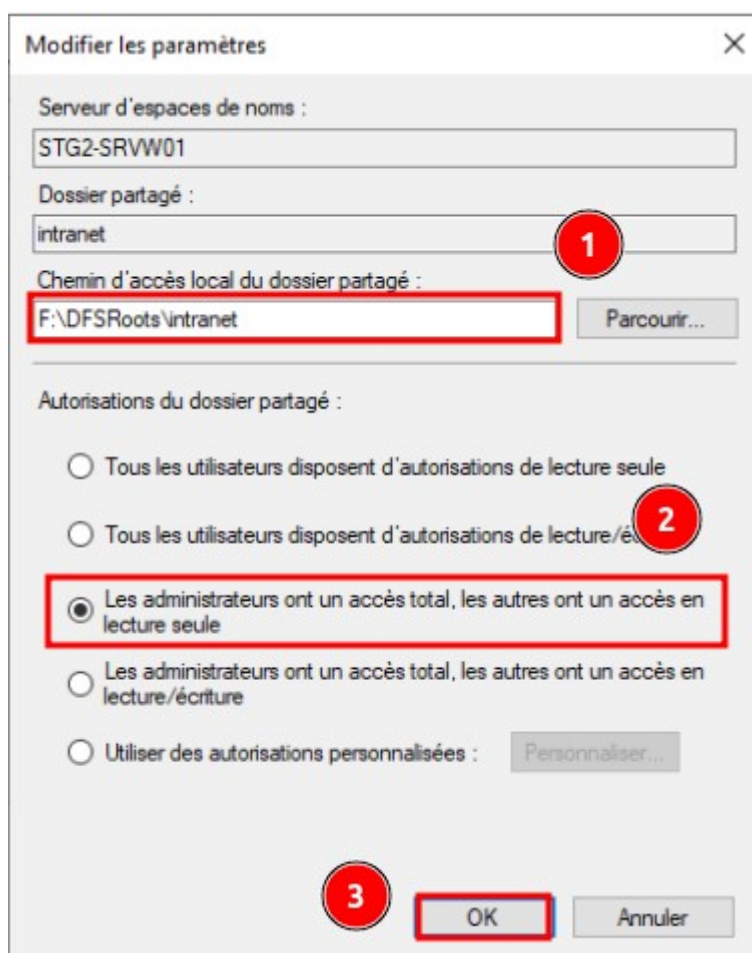
Vous faites un clic droit sur votre espace de noms et choisissez « **Ajouter un serveur d'espaces de noms...** » (Encadré 2).



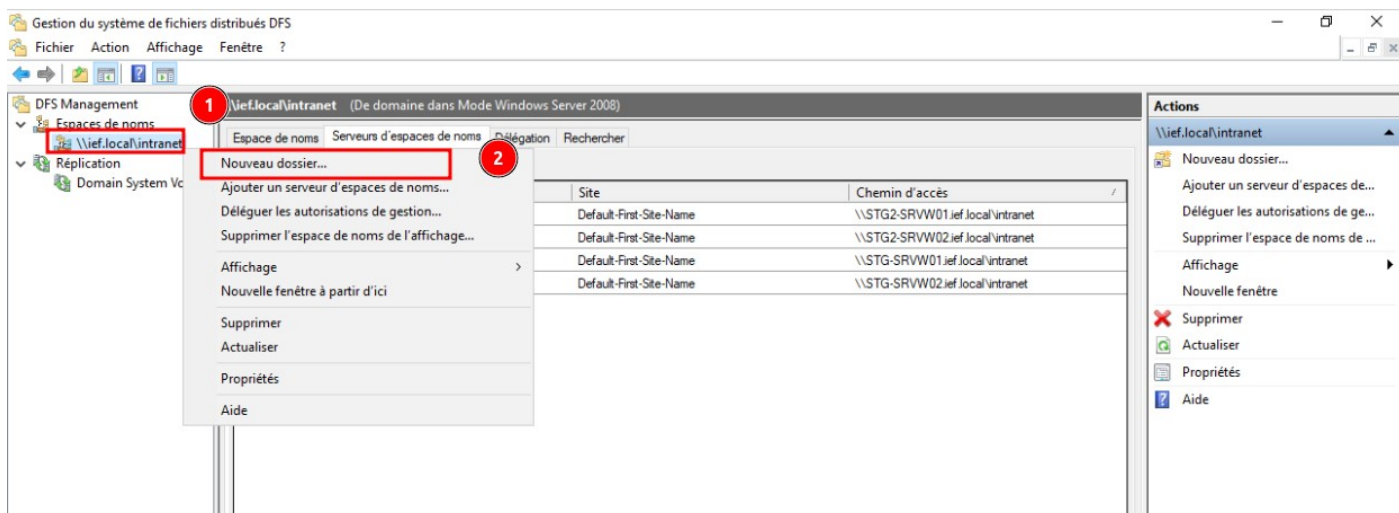
Vous renseignez le nom du deuxième serveur, ici **STG2-SRVW01** (Encadré 1), puis vous cliquez sur « **Modifier les paramètres...** » (Encadré 2).



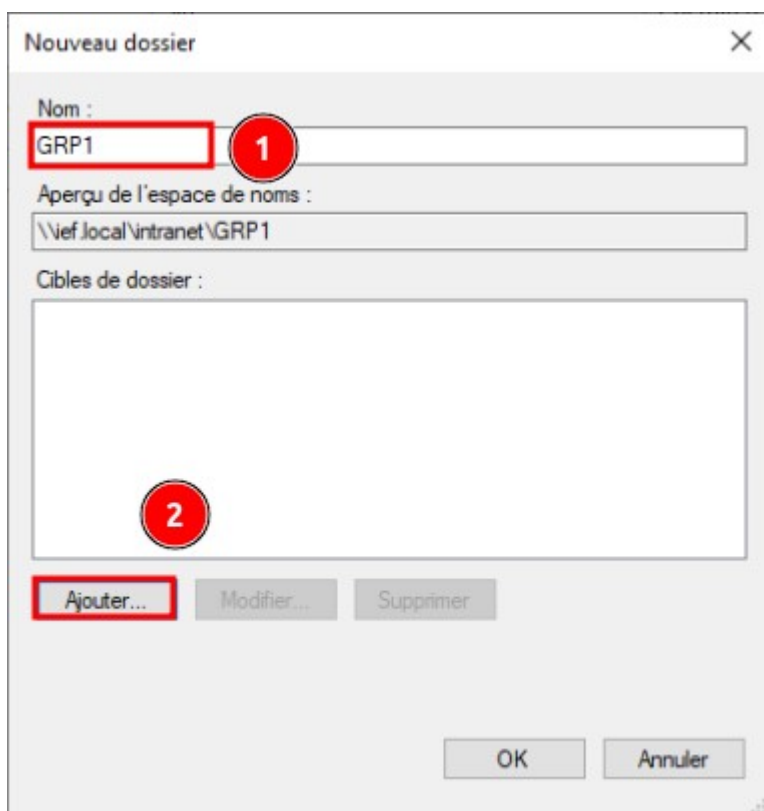
Vous définissez le chemin local sur ce second serveur, **F:\DFSRoots\intranet** (Encadré 1), et vous remettez les mêmes sécurités (Lecture seule pour les utilisateurs, Encadré 2) avant de valider par « **OK** » (Encadré 3).



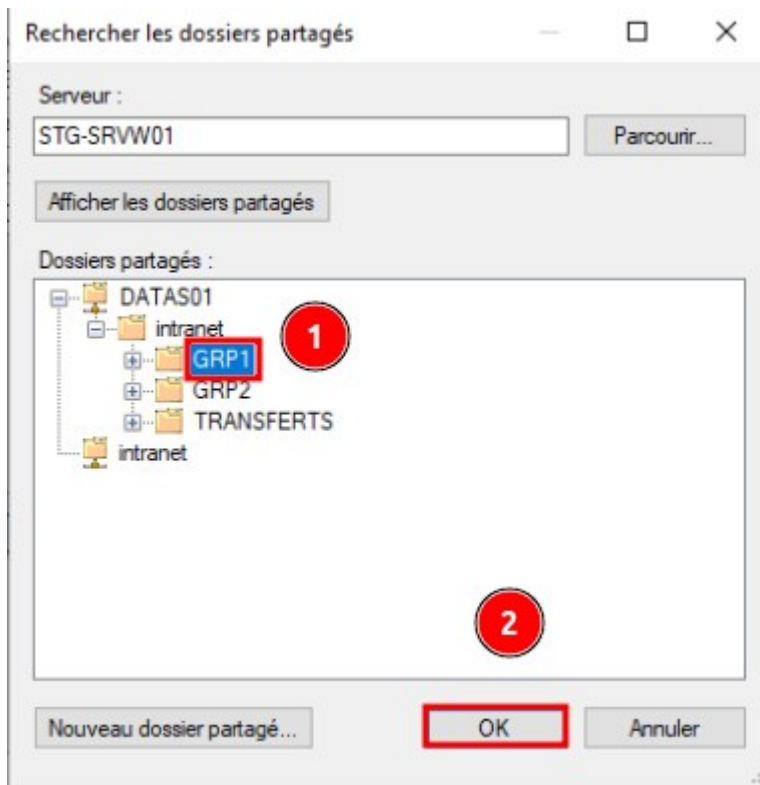
Vous faites à nouveau un clic droit sur l'espace de noms et sélectionnez cette fois « **Nouveau dossier...** » (Encadré 2).



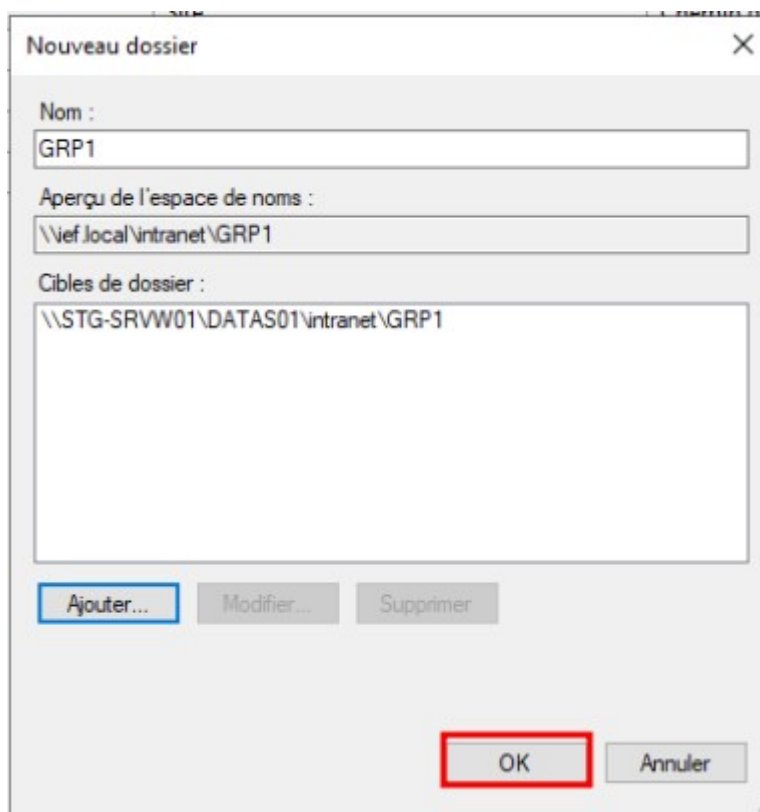
- **Encadré 1** : Vous nommez ce dossier « **GRP1** ». C'est le nom qui apparaîtra sous `\\ief.local\\intranet\\GRP1`.
- **Encadré 2** : Vous cliquez sur le bouton « **Ajouter...** ».



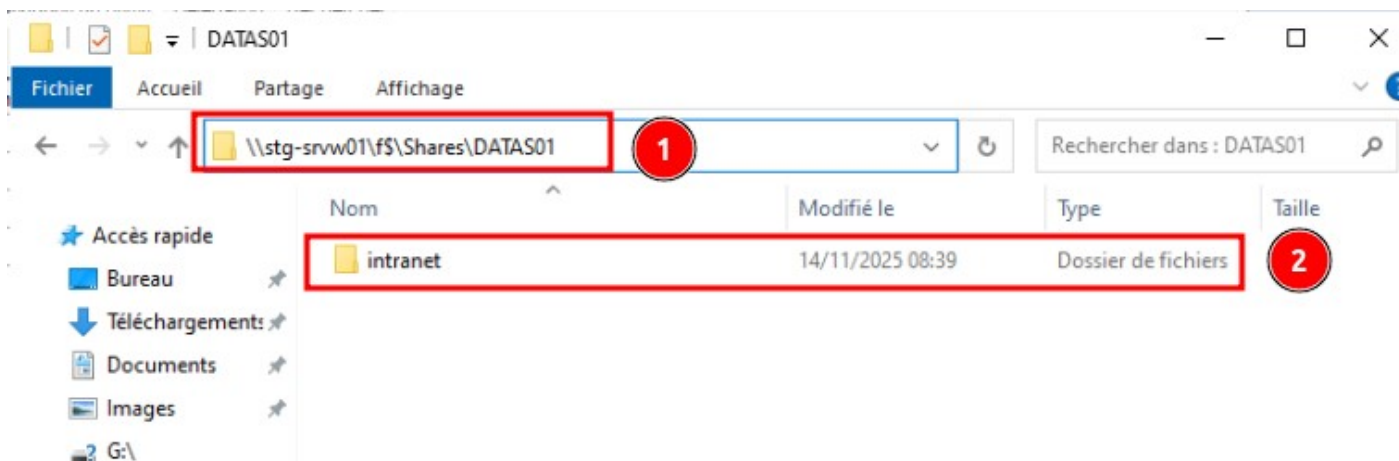
Dans la fenêtre de recherche, vous sélectionnez le dossier physique « **GRP1** » situé sur le premier serveur (Encadré 1), puis vous validez en cliquant sur « **OK** » (Encadré 2).



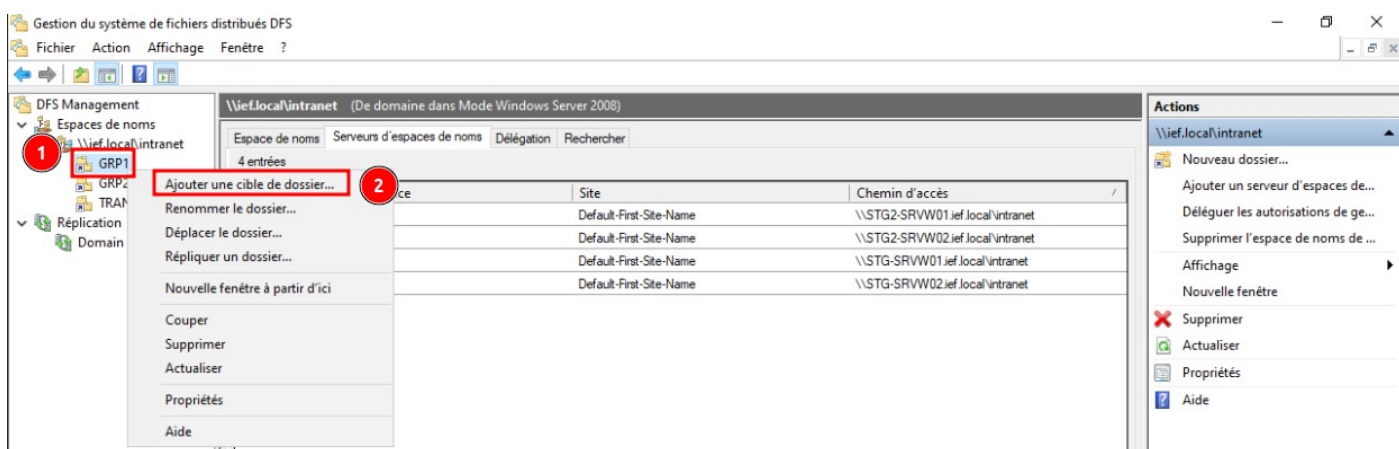
Vous confirmez la création du lien DFS pour le groupe 1 en cliquant sur le bouton « **OK** ».



- **Encadré 1** : Vous utilisez l'explorateur pour accéder au partage administratif du second serveur (\\stg-srvw01\\f\$\\...).
- **Encadré 2** : Vous y collez le dossier « **intranet** » (qui contient GRP1, GRP2 et TRANSFERTS).
 - Pourquoi ? Pour que le DFS puisse lier un seul nom logique à plusieurs emplacements physiques identiques sur différents serveurs.

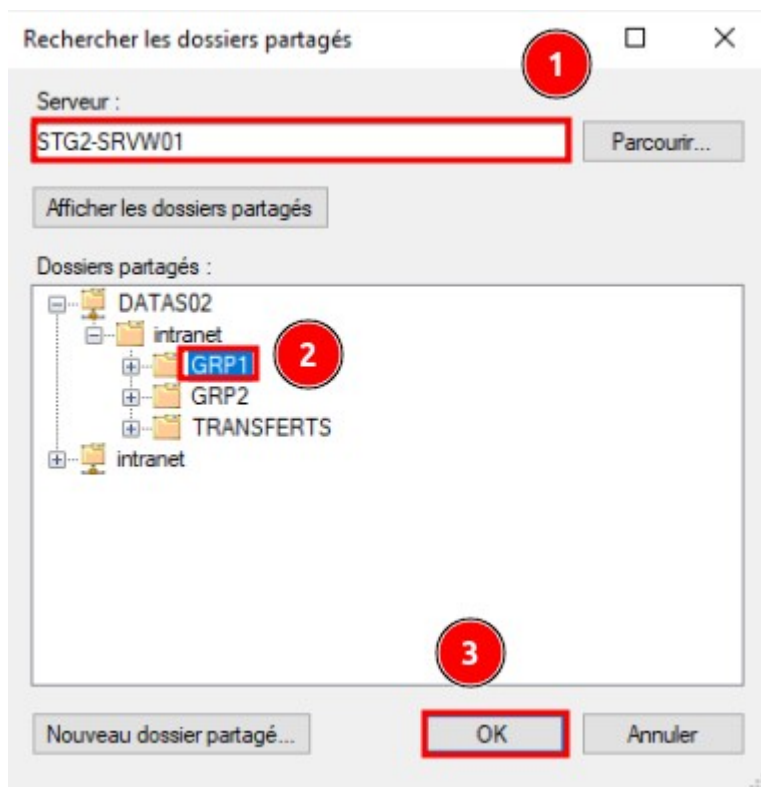


Dans la console DFS, vous faites un clic droit sur le dossier logique « **GRP1** » (Encadré 1) et vous sélectionnez « **Ajouter une cible de dossier...** » (Encadré 2).



Vous allez désigner le même dossier mais sur le **deuxième serveur**.

- **Encadré 1** : Vous saisissez le nom du serveur partenaire : **STG2-SRVW01**.
- **Encadré 2** : Vous sélectionnez le dossier « **GRP1** » correspondant sur ce nouveau serveur.
- **Encadré 3** : Vous validez par « **OK** ».

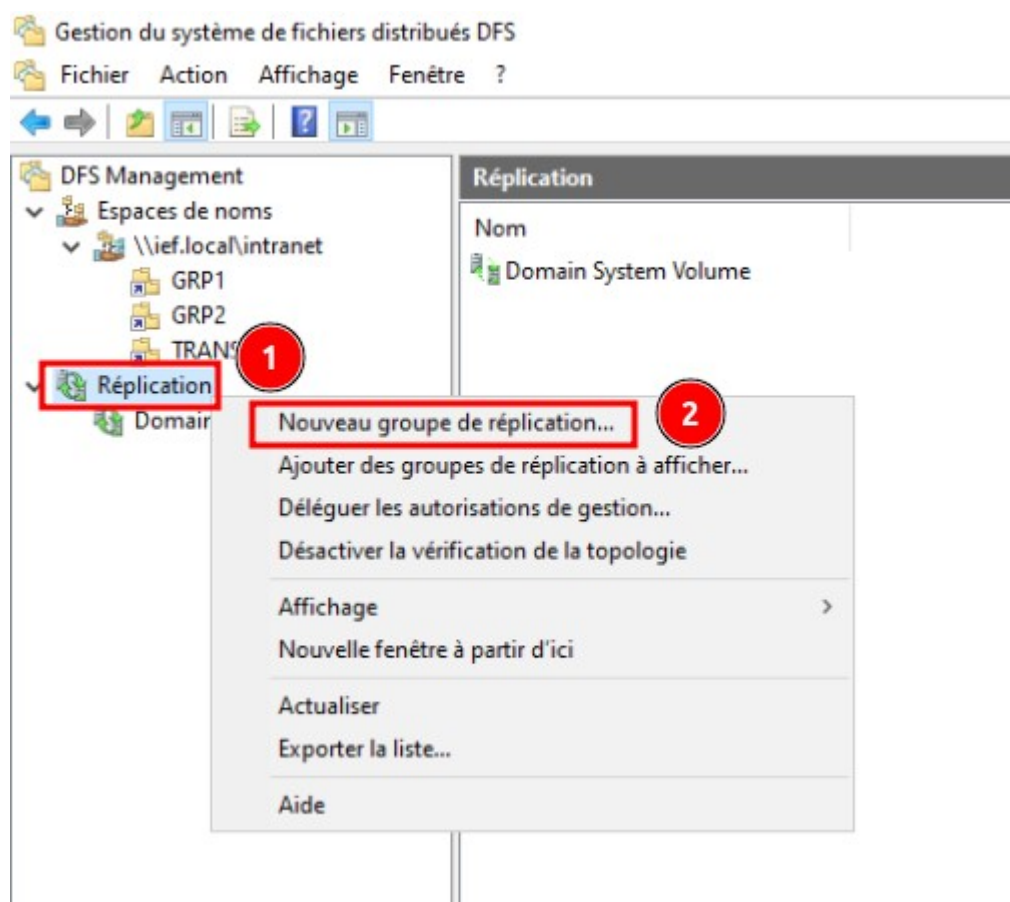


Maintenant il faut faire de même pour tous les dossier et ajouter tous les serveurs sur chacun des dossiers.

DFS

Configuration de la replication DFS

- **Encadré 1** : Dans la console DFS, vous sélectionnez l'onglet « **Réplication** ».
- **Encadré 2** : Vous faites un clic droit et sélectionnez « **Nouveau groupe de réplication...** ».



- **Encadré 1** : Vous sélectionnez « **Groupe de réplication multi-usage** ». C'est le choix standard pour synchroniser des fichiers entre plusieurs serveurs de fichiers classiques.
- **Encadré 2** : Vous cliquez sur le bouton « **Suivant >** ».

Assistant Nouveau groupe de réplication

Type de groupe de réplication

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Membres concentrateurs
- Connexions Hub and Spoke
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Sélectionnez le type de groupe de réplication à créer.

☒ Groupe de réplication multi-usage

Cette option configure la réplication entre deux serveurs ou plus pour la publication, le partage de contenu et d'autres scénarios.

☐ Groupe de réplication pour la collecte de données

Cette option configure une réplication bidirectionnelle entre deux serveurs, comme un serveur de succursale et un serveur concentrateur (destination). Cela vous permet de collecter les données sur le serveur concentrateur. Vous pouvez ensuite utiliser un logiciel de sauvegarde pour sauvegarder les données sur le serveur concentrateur.


< Précédent

Suivant >

Annuler

- **Encadré 1** : Vous donnez un nom à ce groupe de synchronisation. Ici, vous avez saisi « **PRINCIPAL** ».
- **Encadré 2** : Vous cliquez sur le bouton « **Suivant** > ».

Assistant Nouveau groupe de réplication

 **Nom et domaine**

Étapes :

- Type de groupe de réplication
- Nom et domaine**
- Membres du groupe de réplication
- Sélection de topologie
- Membres concentrateurs
- Connexions Hub and Spoke
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Entrez un nom et un domaine pour le groupe de réplication. Le nom du groupe de réplication doit être unique dans le domaine qui héberge le groupe de réplication.

Nom du groupe de réplication : **1**

Description facultative du groupe de réplication :

Domaine :

2

Encadré rouge : Vous cliquez sur le bouton « **Ajouter...** ».

Assistant Nouveau groupe de réplication

Membres du groupe de réplication

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication**
- Sélection de topologie
- Membres concentrateurs
- Connexions Hub and Spoke
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Cliquez sur **Ajouter**, puis sélectionnez deux serveurs ou plus qui deviendront membres du groupe de réplication.

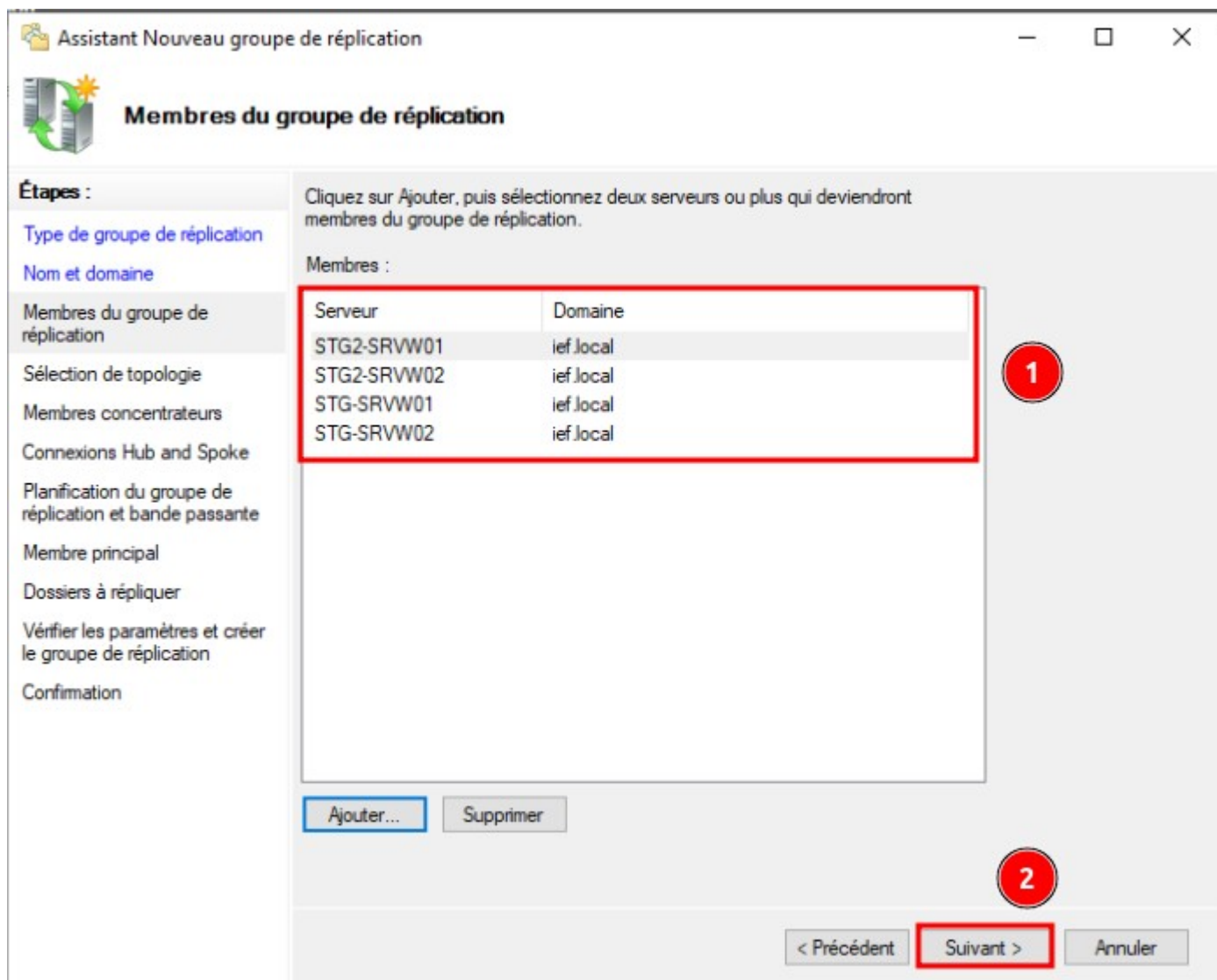
Membres :

Serveur	Domaine
---------	---------

Ajouter... Supprimer

< Précédent Suivant > Annuler

- **Encadré 1** : Vous avez ajouté la liste de tous les serveurs qui participeront à la réplication : STG1-SRVW01, STG2-SRVW01, STG1-SRVW02 et STG2-SRVW02.
- **Encadré 2** : Vous cliquez sur « **Suivant** » après avoir validé votre sélection de serveurs membres.



- **Encadré 1** : Vous sélectionnez l'option « **Maille pleine** » (Full mesh).
 - **Ce que cela signifie** : Chaque serveur du groupe se synchronisera avec tous les autres serveurs. C'est la configuration idéale pour garantir que les données sont identiques partout rapidement dans un petit parc de serveurs.
- **Encadré 2** : Vous cliquez sur « **Suivant** > ».

Assistant Nouveau groupe de réplication

Sélection de topologie


Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie**
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Sélectionnez une topologie de connexions parmi les membres du groupe de réplication.


☐ Hub et Spoke

Cette topologie requiert au moins 3 membres dans le groupe de réplication. Les membres spoke sont connectés à un ou deux hubs. Cette topologie est adaptée aux scénarios de publication où les données proviennent du membre hub et se répliquent sur les membres spoke.



☒ Maille pleine

Dans cette topologie, chaque membre est répliqué avec tous les autres membres du groupe de réplication. Cette topologie est surtout adaptée lorsqu'il existe au plus dix membres dans le groupe de réplication.



☐ Aucune topologie

Sélectionnez cette option si vous souhaitez créer une topologie personnalisée une fois l'Assistant terminé. Aucune réplication ne peut s'effectuer tant que vous n'avez pas créé la topologie personnalisée.

1

2

< Précédent **Suivant >** Annuler

Encadré rouge : Vous cliquez sur « **Suivant** > ».

Assistant Nouveau groupe de réplication

Planification du groupe de réplication et bande passante

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Planification du groupe de réplication et bande passante**
- Membre principal
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Sélectionnez la planification de réplication et la bande passante à utiliser par défaut pour toutes les nouvelles connexions dans le groupe de réplication.

☒ Répliquer en continu à l'aide de la bande passante spécifiée

Utilisez cette option pour activer la réplication 24 heures sur 24 et sept jours sur sept, avec la bande passante suivante :

Bande passante : Complète

☐ Répliquer aux jours et heures spécifiés

Utilisez cette option pour spécifier les jours et heures de réplication par défaut. La planification de réplication initiale n'a pas d'intervalles de réplication. Vous devez en créer au moins un pour que la réplication puisse avoir lieu.

Modifier la planification...

< Précédent **Suivant >** Annuler

- **Encadré 1** : Vous désignez **STG1-SRVW01** comme **membre principal**.
 - **C'est une étape cruciale** : Lors de la toute première synchronisation, les fichiers présents sur ce serveur seront considérés comme la "référence" et seront copiés vers tous les autres serveurs du groupe.
- **Encadré 2** : Vous cliquez sur « **Suivant >** ».

Assistant Nouveau groupe de réplication

Membre principal

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Membre principal**
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Sélectionnez le serveur contenant les données que vous souhaitez répliquer sur les autres membres. Ce serveur est considéré comme le membre principal.

Membre principal :

STG-SRVW01

1


i Si les dossiers à répliquer existent déjà sur plusieurs serveurs, les dossiers et fichiers situés sur le membre principal feront autorité au cours de la réplication initiale.

2

< Précédent Suivant > Annuler

Encadré rouge : Vous cliquez sur le bouton « **Ajouter...** ».

Assistant Nouveau groupe de réplication

 **Dossiers à répliquer**

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer**
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Cliquez sur **Ajouter** pour sélectionner un dossier du membre principal que vous souhaitez répliquer sur les autres membres du groupe de réplication.

Dossiers répliqués :

Chemin d'accès local	Nom du dossier répliqué	Autorisations NT...
----------------------	-------------------------	---------------------

Ajouter... Modifier... Supprimer

< Précédent Suivant > Annuler

- **Encadré 1** : Vous renseignez le chemin local du dossier à synchroniser sur le serveur maître : **F:\Shares\DATAS01\intranet**.
- **Encadré 2** : Vous cochez « **Autorisations personnalisées** ».
 - Pourquoi ? Cela permet de conserver les droits NTFS (GRP1, GRP2, etc.) que vous avez configurés avec précision précédemment.
- **Encadré 3** : Vous validez par « **OK** ».

Ajouter un dossier à répliquer

Membre :
STG-SRVW01

Chemin d'accès local du dossier à répliquer :
F:\Shares\DATAS01\intranet

Exemple : C:\Documents

Sélectionnez ou entrez un nom représentant ce dossier sur tous les membres du groupe de réplication. Ce nom est reconnu comme le nom du dossier répliqué.

☒ Utiliser le nom en fonction du chemin d'accès :
intranet

☐ Utiliser un nom personnalisé :
Exemple : Documents

Sélectionnez les autorisations NTFS pour le dossier répliqué :

☐ Autorisations existantes

☒ Autorisations personnalisées :
Modifier...

Autorisations << OK Annuler

- **Encadré rouge** : Le dossier est maintenant ajouté à la liste des dossiers à répliquer. Vous cliquez sur « **Suivant** > ».

Assistant Nouveau groupe de réplication

Dossiers à répliquer

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer**
- Chemin d'accès local de intranet sur les autres membres
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Cliquez sur **Ajouter** pour sélectionner un dossier du membre principal que vous souhaitez répliquer sur les autres membres du groupe de réplication.

Dossiers répliqués :

Chemin d'accès local	Nom du dossier répliqué	Autorisations NT...
F:\Shares\DATAS01\intranet	intranet	Personnalisée

Ajouter... **Modifier...** **Supprimer**

< Précédent **Suivant >** Annuler

- **Encadré 1** : On voit que pour les autres serveurs (membres), le statut est par défaut « **Désactivé** ». Vous sélectionnez un serveur dans la liste.
- **Encadré 2** : Vous cliquez sur le bouton « **Modifier...** » pour activer la réplication sur ce serveur et désigner son dossier local.

Assistant Nouveau groupe de réplication

Chemin d'accès local de intranet sur les autres membres

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Chemin d'accès local de intranet sur les autres membres**
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Pour spécifier le chemin d'accès local du dossier répliqué ou l'état de lecture seule du dossier, sélectionnez le membre approprié, puis cliquez sur Modifier.

Membre principal : STG-SRVW01
Chemin d'accès local du membre principal : F:\Shares\DATAS01\intranet

Détails du membre :

Membre	Chemin d'accès local	Statut de l'appar...
STG2-SRVW01	<Non défini>	Désactivé
STG2-SRVW02	<Non défini>	Désactivé
STG-SRVW02	<Non défini>	Désactivé

Modifier...

< Précédent Suivant > Annuler

- **Encadré 1 :** Vous cochez la case « **Activé** ». Cela autorise ce serveur à recevoir et envoyer les fichiers du groupe de réplication.
- **Encadré 2 :** Vous indiquez le chemin local sur ce serveur spécifique.
 - Attention : Comme l'indique votre petite note textuelle, il faut adapter le chemin selon le serveur (par exemple **F:\Shares\DATAS02\intranet** pour le serveur 2).
- **Encadré 3 :** Vous validez par « **OK** ».

Modifier

Général

Membre :
STG2-SRVW01

Sélectionnez l'état initial du dossier répliqué sur ce membre.

Statut de l'appartenance :

☐ Désactivé
Le dossier répliqué ne sera pas stocké sur ce membre.

☒ **Activé**
Garder le dossier suivant synchronisé avec les autres membres. 1

Chemin d'accès local du dossier :
F:\Shares\DATAS02\intranet 2
Exemple : C:\Données

☐ Placez en lecture seule le dossier répliqué sélectionné sur ce membre.

OK 3 Annuler

- **Contenu** : On voit maintenant que tous les serveurs ont le statut « **Activé** » et que chacun possède son propre chemin local configuré.
- **Encadré rouge** : Vous cliquez sur « **Suivant** > » pour terminer l'assistant.

Assistant Nouveau groupe de réplication

Chemin d'accès local de intranet sur les autres membres

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Chemin d'accès local de intranet sur les autres membres**
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Pour spécifier le chemin d'accès local du dossier répliqué ou l'état de lecture seule du dossier, sélectionnez le membre approprié, puis cliquez sur Modifier.

Membre principal : STG-SRVW01
Chemin d'accès local du membre principal : F:\Shares\DATAS01\intranet

Détails du membre :

Membre	Chemin d'accès local	Statut de l'appar...
STG2-SRVW01	F:\Shares\DATAS02\intranet	Activé
STG2-SRVW02	F:\Shares\DATAS04\intranet	Activé
STG-SRVW02	F:\Shares\DATAS03\intranet	Activé

Modifier...

< Précédent **Suivant >** Annuler

Encadré rouge : Vous cliquez sur le bouton « **Créer** ».

Assistant Nouveau groupe de réplication

Vérifier les paramètres et créer le groupe de réplication

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Chemin d'accès local de intranet sur les autres membres
- Vérifier les paramètres et créer le groupe de réplication**
- Confirmation

Vous avez sélectionné les paramètres suivants pour le nouveau groupe de réplication. Si les paramètres sont corrects, cliquez sur Créer pour créer le groupe de réplication. Pour changer un paramètre, cliquez sur Précédent ou sélectionnez la page appropriée dans le volet d'orientation.

Paramètres du groupe de réplication :

Nom du groupe de réplication :
PRINCIPAL

Description du groupe de réplication :

Domaine du groupe de réplication :
ief.local

Membres du groupe de réplication (4) :

- STG2-SRVW01
- STG2-SRVW02
- STG-SRVW01
- STG-SRVW02

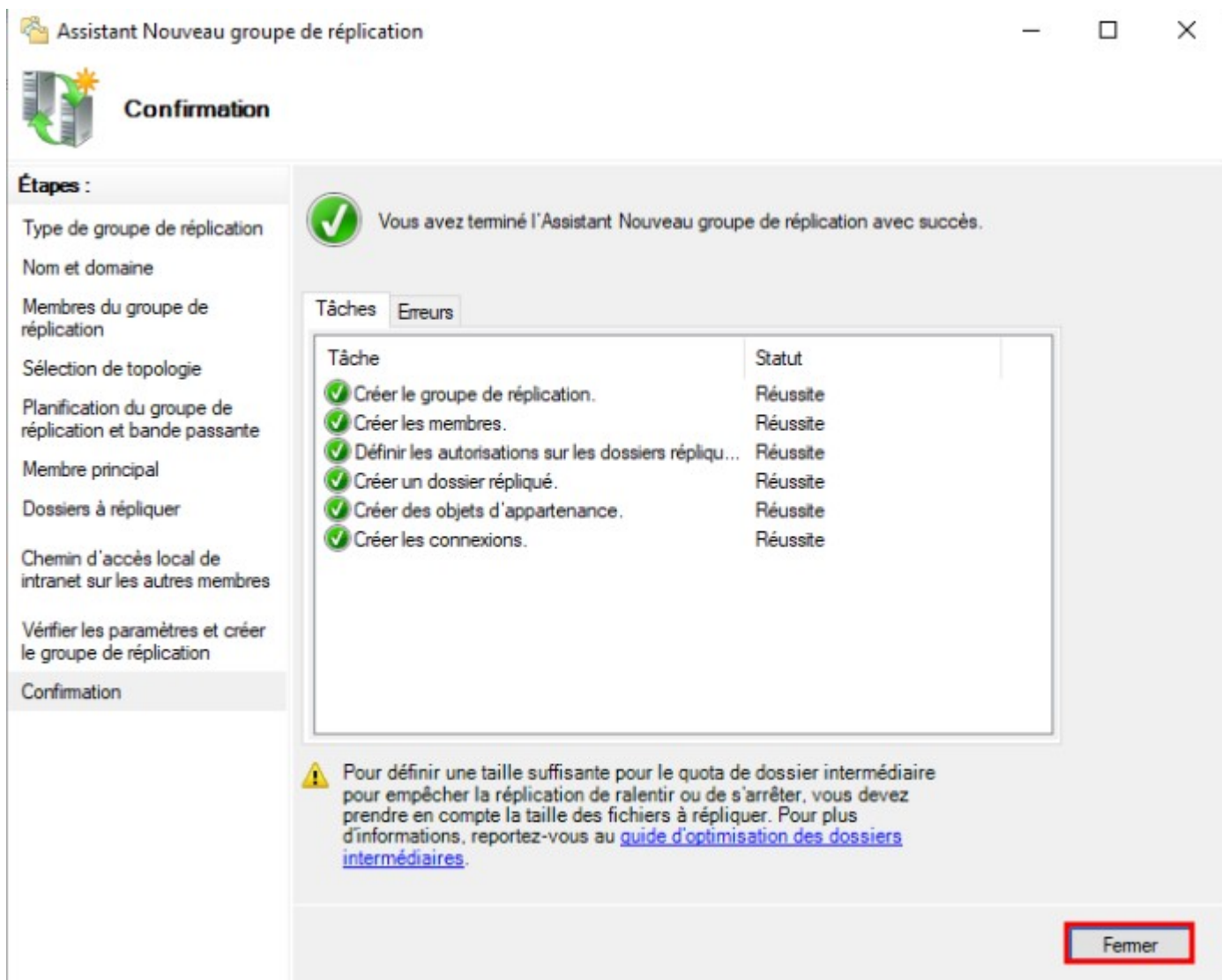
Type de topologie :
Maille pleine

Liste des connexions (12) :

- STG2-SRVW02 -> STG2-SRVW01
- STG2-SRVW01 -> STG2-SRVW02
- STG-SRVW01 -> STG2-SRVW01
- STG2-SRVW01 -> STG-SRVW01

< Précédent **Créer** Annuler

Encadré rouge : Vous cliquez sur le bouton « **Fermer** ».



Maintenant nous pouvons tester pour voir si la réplication fonctionne, pour cela crée un fichier dans un des dossiers sur un des serveurs et le voir si il apparait sur l'autre serveur.

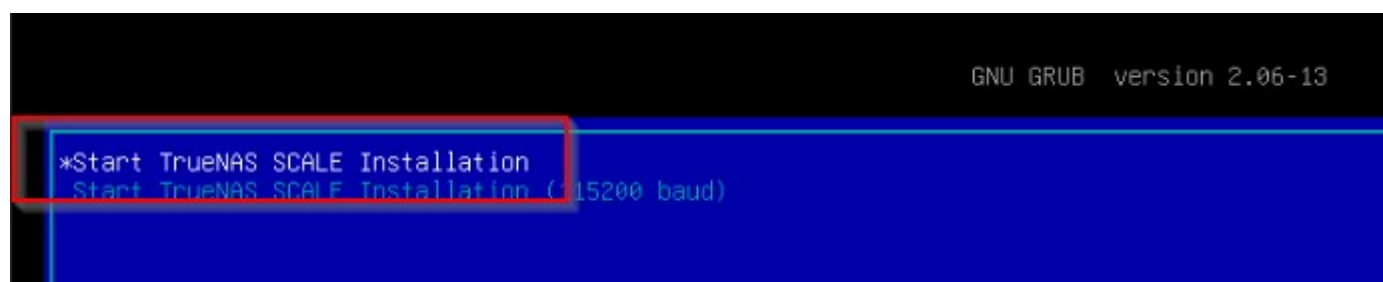
SAN

SAN

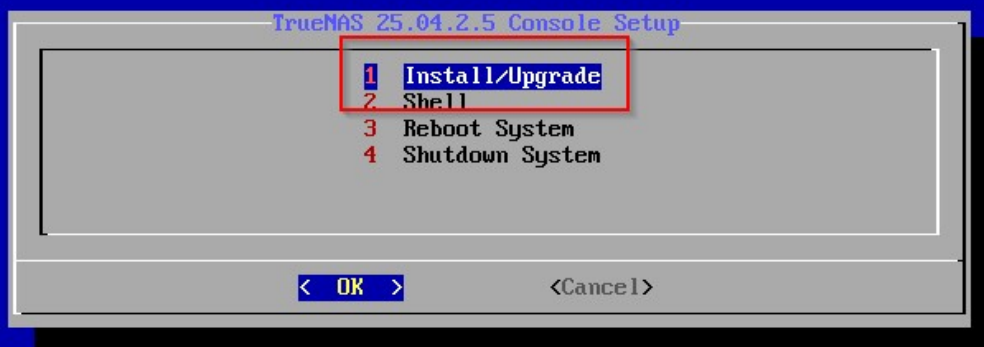
Installation de TrueNAS

1. Installation de TrueNAS

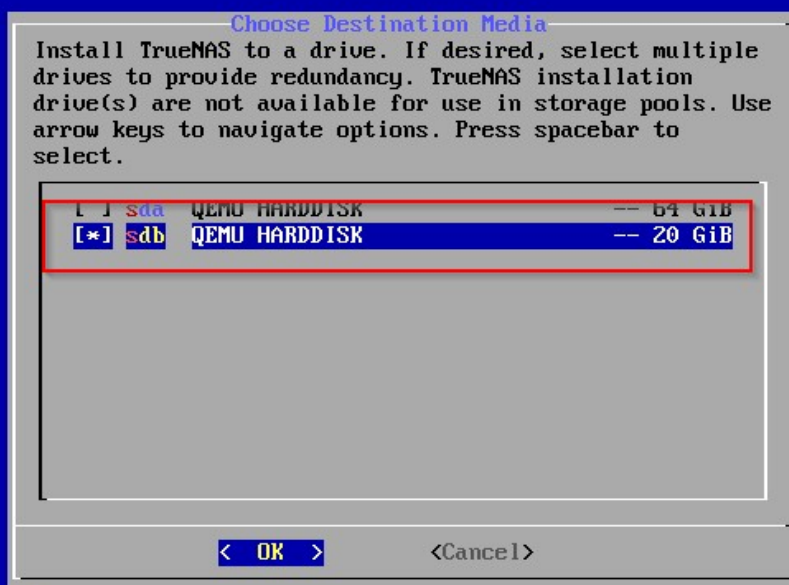
Encadré rouge : On sélectionne la première option : « **Start TrueNAS SCALE Installation** ».



Encadré rouge : On choisit l'option « **1 Install/Upgrade** ».



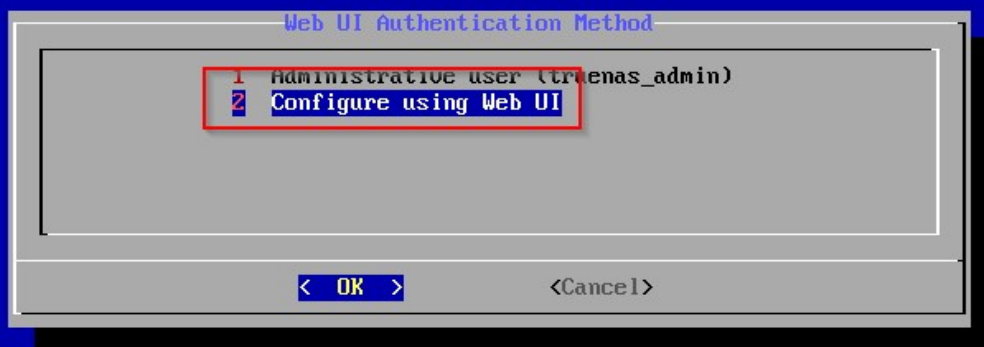
Encadré rouge : On sélectionne le disque dur sur lequel le système d'exploitation sera installé. Ici, c'est le disque « **sda** » de **20 GiB**.



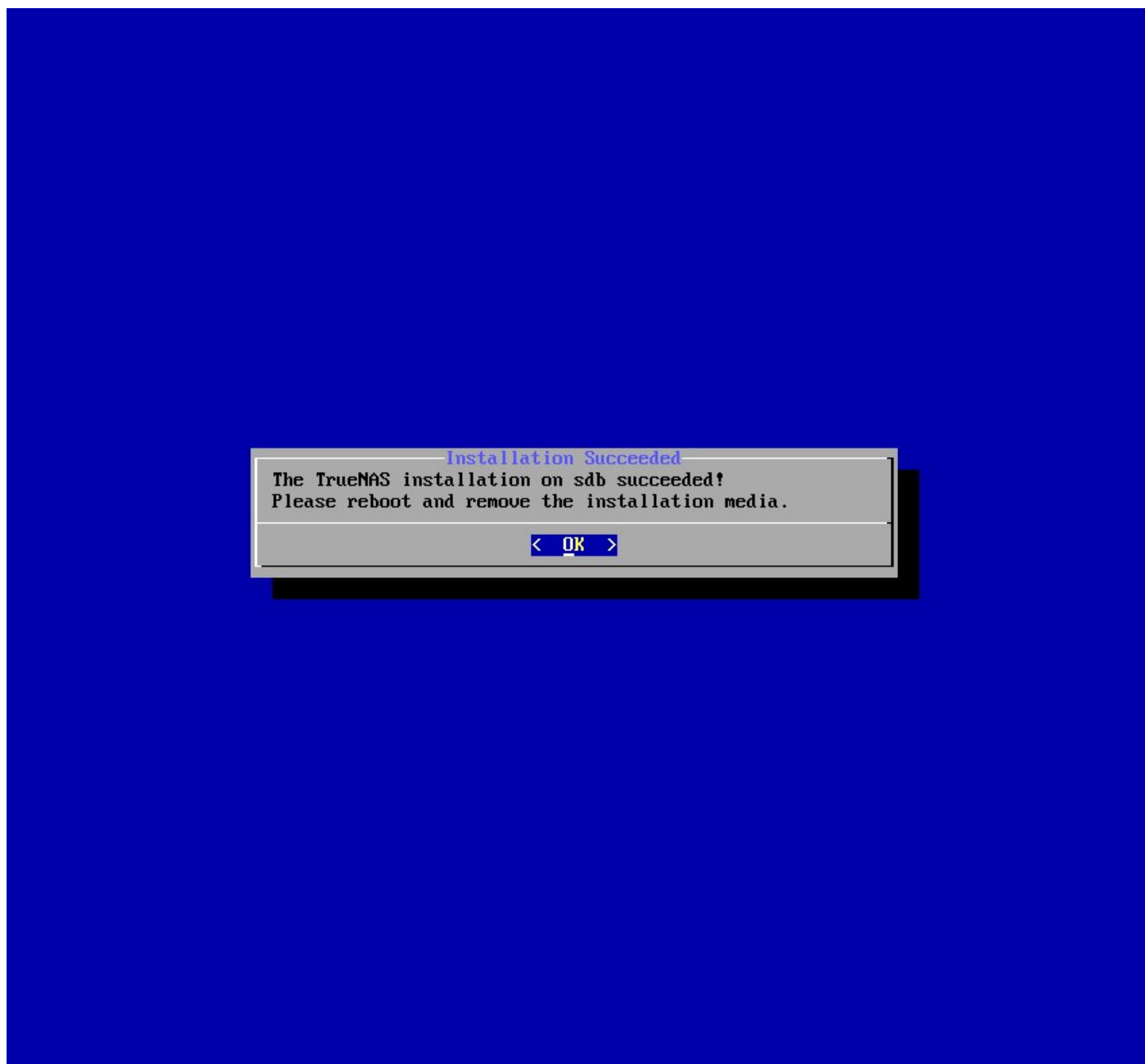
Encadré rouge : On sélectionne « < **Yes** > » pour répondre à la question "Proceed with the installation?".



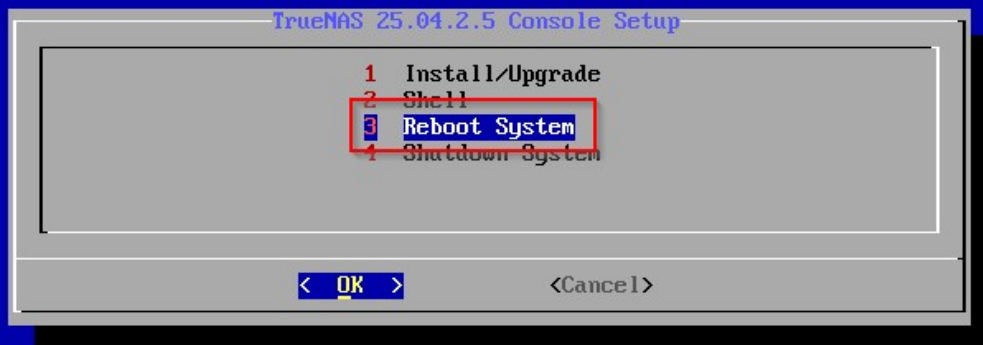
Encadré rouge : On sélectionne l'option « **2 Configure using Web UI** ».



L'installation est terminée avec succès. On clique sur « **OK** » pour confirmer le message informant qu'il faut retirer le support d'installation et redémarrer.

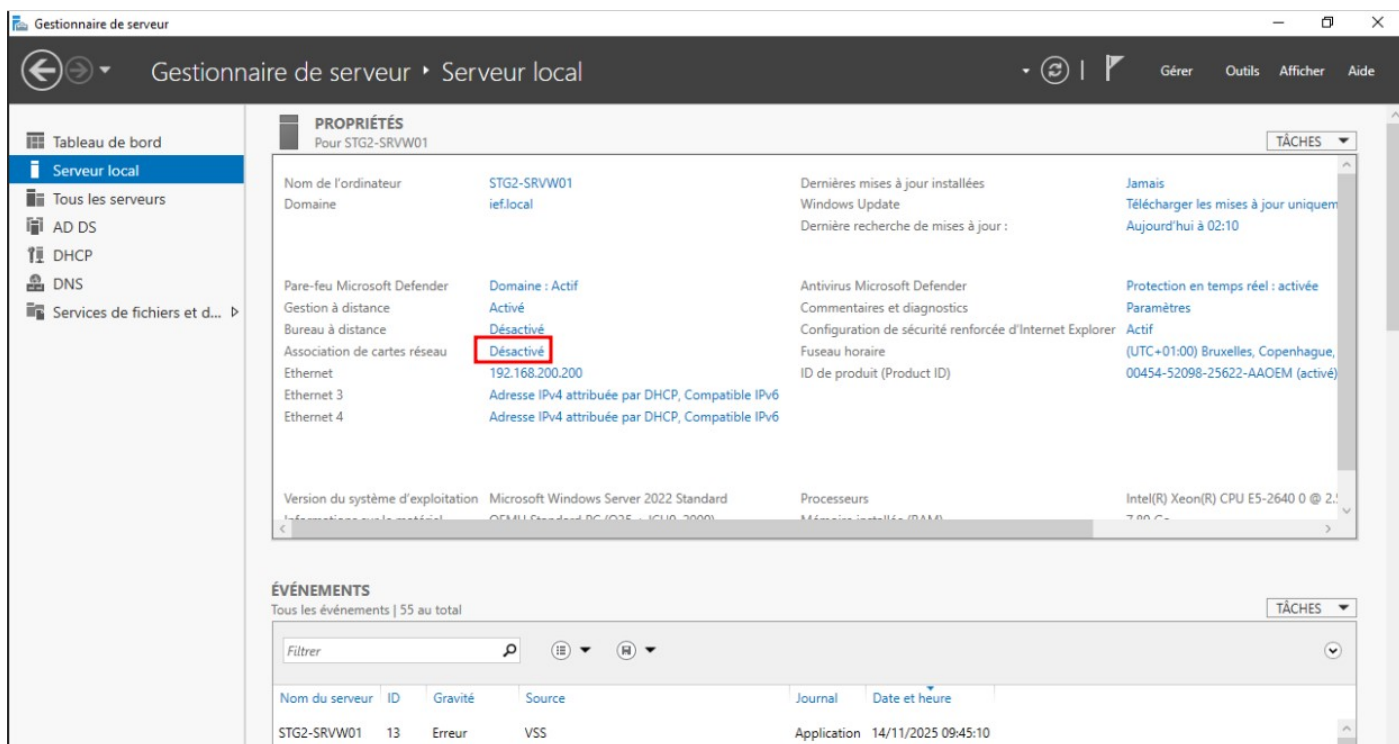


Dans le menu de configuration de la console, on sélectionne l'option « **3 Reboot System** » pour redémarrer la machine et lancer le système TrueNAS fraîchement installé.

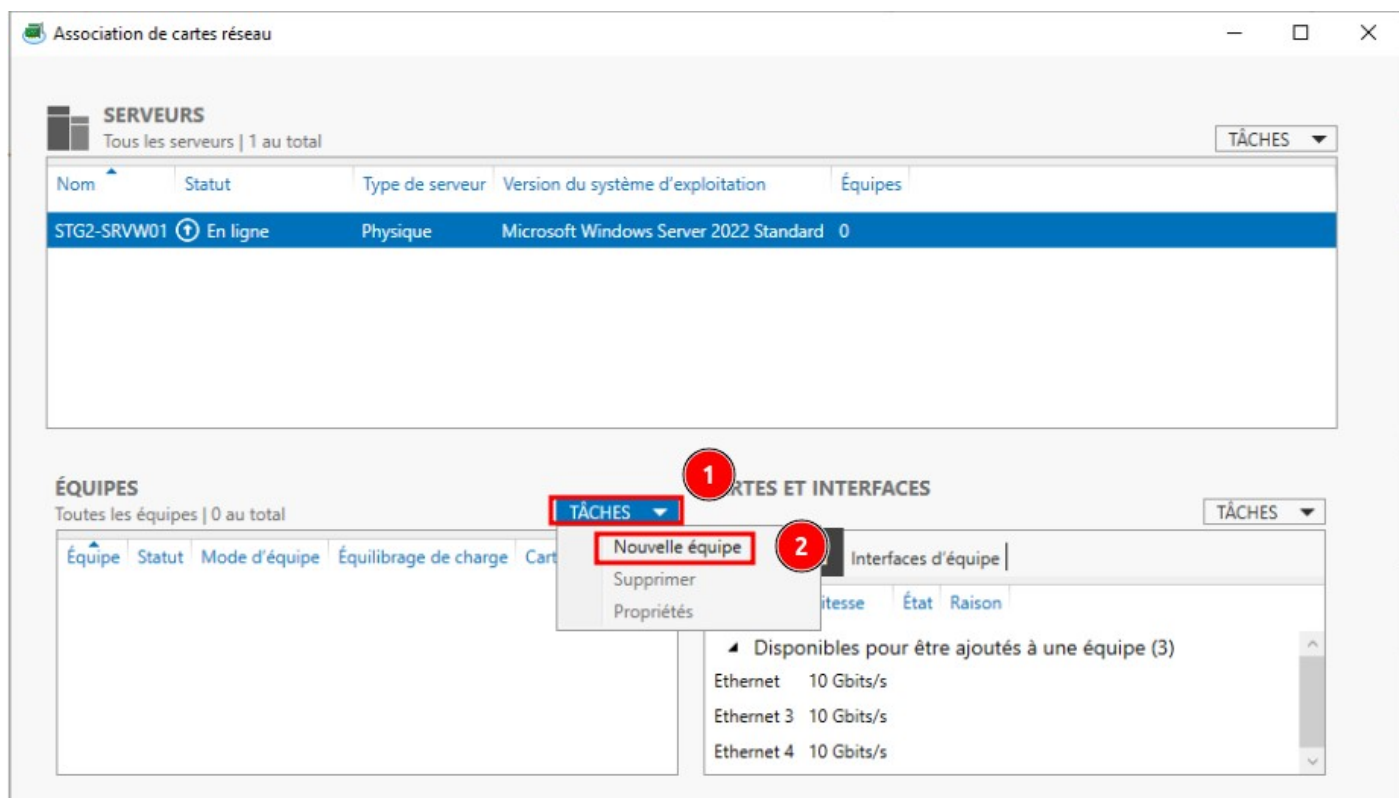


2. Configuration du NIC Teaming sur Windows Server

Dans les propriétés du serveur local, on clique sur le statut « **Désactivé** » en face de "Association de cartes réseau" (NIC Teaming) pour ouvrir la fenêtre de configuration.



Dans la section "Équipes", on clique sur le menu « **Tâches** » (1) puis sur « **Nouvelle équipe** » (2).



1. **Nom de l'équipe (1)** : On nomme l'agrégation « **VMLAG1** ».
2. **Cartes membres (2)** : On coche les deux cartes réseau physiques que l'on souhaite regrouper, ici **Ethernet 2** et **Ethernet 3** (10 Gbps chacune).
3. **Mode d'équilibrage (3)** : On sélectionne « **Hachage d'adresse** » comme mode de répartition de la charge.
4. **Validation (4)** : On clique sur « **OK** » pour créer l'interface virtuelle.

Association de cartes réseau

Nouvelle équipe

Nom de l'équipe :

Cartes membres :

Dans l'équipe	Carte	Vitesse	État	Raison
<input type="checkbox"/>	Ethernet	10 Gbits/s		
<input checked="" type="checkbox"/>	Ethernet 3	10 Gbits/s		
<input checked="" type="checkbox"/>	Ethernet 4	10 Gbits/s		

Propriétés supplémentaires

Mode d'équipe : Indépendant du commutateur

Mode d'équilibrage de charge : Hachage d'adresse

Carte réseau en attente : Aucun (toutes les cartes actives)

Interface d'équipe principale : [LINKAGG : VLAN par défaut](#)

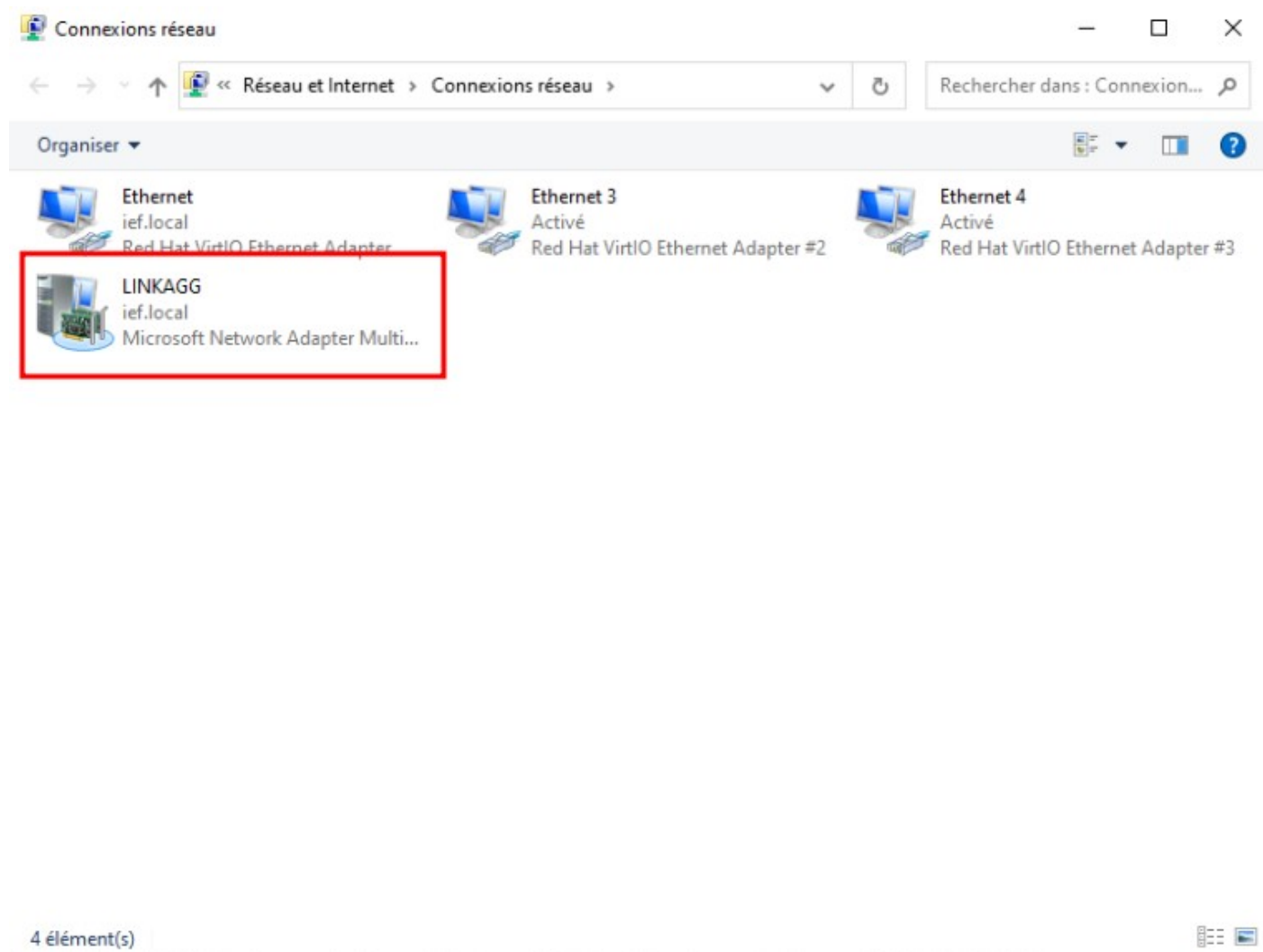
OK Annuler

De retour dans le Gestionnaire de serveur, on constate que l'association est active et affiche bien une vitesse cumulée de **20 Gbps** (10+10).

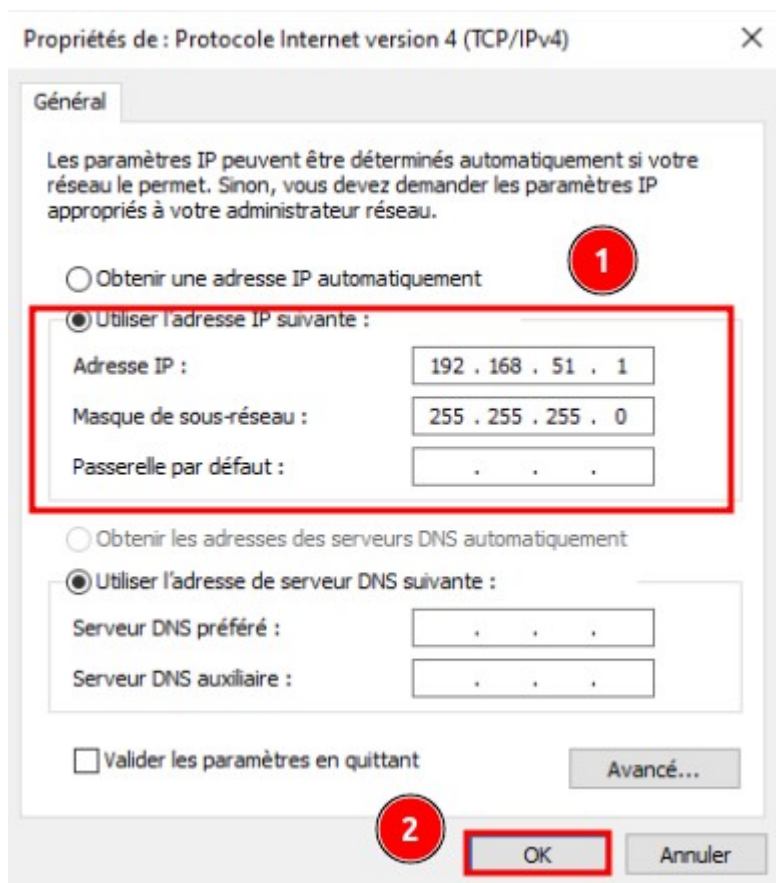
Nom de l'ordinateur	STG2-SRVW01	Dernières mises à jour installées	Jamais
Domaine	ief.local	Windows Update	Télécharger les mises à jour uniquement
		Dernière recherche de mises à jour :	Aujourd'hui à 02:10
Pare-feu Microsoft Defender	Domaine : Actif, Public : Actif	Antivirus Microsoft Defender	Protection en temps réel : activée
Gestion à distance	Activé	Commentaires et diagnostics	Paramètres
Bureau à distance	Désactivé	Configuration de sécurité renforcée d'Internet Explorer	Actif
Association de cartes réseau	Activé	Fuseau horaire	(UTC+01:00) Bruxelles, Copenhague, ...
Ethernet	192.168.200.200	ID de produit (Product ID)	00454-52098-25622-AAOEM (activé)
LINKAGG	Adresse IPv4 attribuée par DHCP, Compatible IPv6		
Version du système d'exploitation	Microsoft Windows Server 2022 Standard	Processeurs	Intel(R) Xeon(R) CPU E5-2640 0 @ 2.5
Informations sur le matériel	QEMU Standard PC (Q35 + ICH9, 2009)	Mémoire installée (RAM)	7,89 Go
		Espace disque total	137,31 Go

Dans le panneau de configuration réseau de Windows, on voit apparaître la nouvelle carte réseau logique «

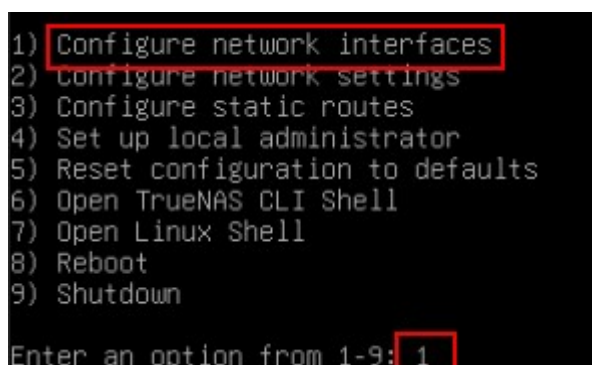
LINKAGG» qui représente le groupe de cartes fusionnées.



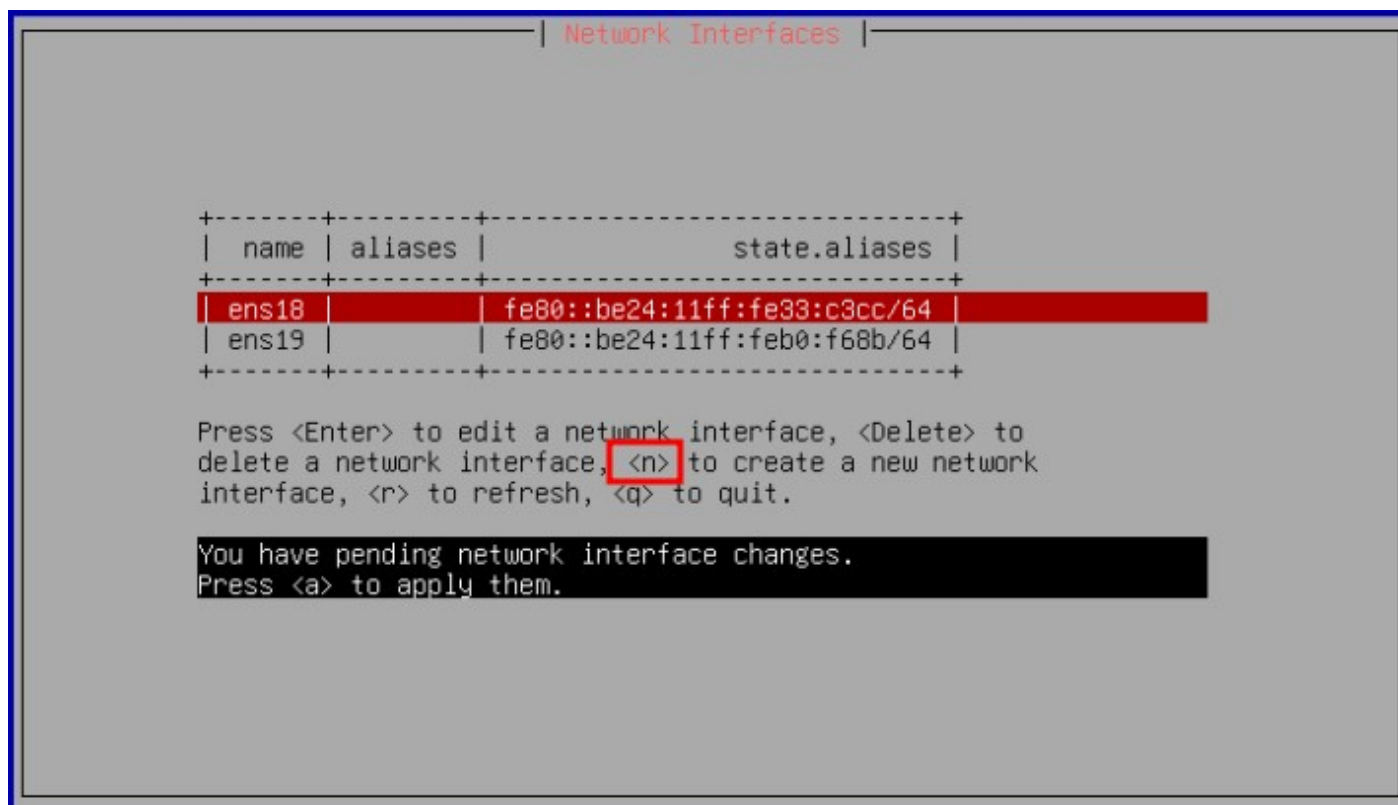
- **Encadré 1 :** Dans les propriétés TCP/IPv4, vous définissez une adresse IP statique pour le serveur Windows :
 - Adresse IP : **192.168.51.1**
 - Masque de sous-réseau : **255.255.255.0**
- **Encadré 2 :** Vous cliquez sur « **OK** » pour valider cette configuration. Ce serveur sera le point de contact (51.1) pour communiquer avec le TrueNAS.



- **Encadré 1** : Dans le menu de la console TrueNAS, vous ciblez l'option « **1) Configure network interfaces** ».
- **Encadré 2** : Vous saisissez le chiffre « **1** » pour accéder aux réglages des cartes réseau.



Encadré rouge : L'interface affiche la liste des cartes physiques (ens18, ens19). Vous suivez l'instruction en bas de l'écran en appuyant sur la touche « **n** » (create a new network interface).



- **Encadré 1 (Interface Settings)** : Vous configurez les détails de l'interface agrégée :
 - **Type** : LINK_AGGREGATION
 - **Nom** : bond0
 - **Aliases (IP)** : Vous lui attribuez l'adresse **192.168.51.2/24**. (Cela place le TrueNAS dans le même réseau que le serveur Windows configuré à l'étape 1).
 - **LAG Settings** : Vous choisissez le protocole LOADBALANCE et vous sélectionnez les deux cartes physiques membres : **ens18** et **ens19**.
- **Encadré 2** : Vous sélectionnez le bouton « **<Save>** » et validez pour enregistrer cette nouvelle interface bond0.

Create Network Interface

Interface Settings

type: LINK_AGGREGATION
name: bond0
description: LINKAGG
ipv4_dhcp: No
ipv6_auto: No
aliases: 192.168.50.2/24

Link Aggregation Settings

lag_protocol: LOADBALANCE
lag_ports: ens18, ens19
xmit_hash_policy: <default: None>
lacpdu_rate: <default: None>

Other Settings

mtu: <default: <not set>>

1

2

<Save>

<Back>

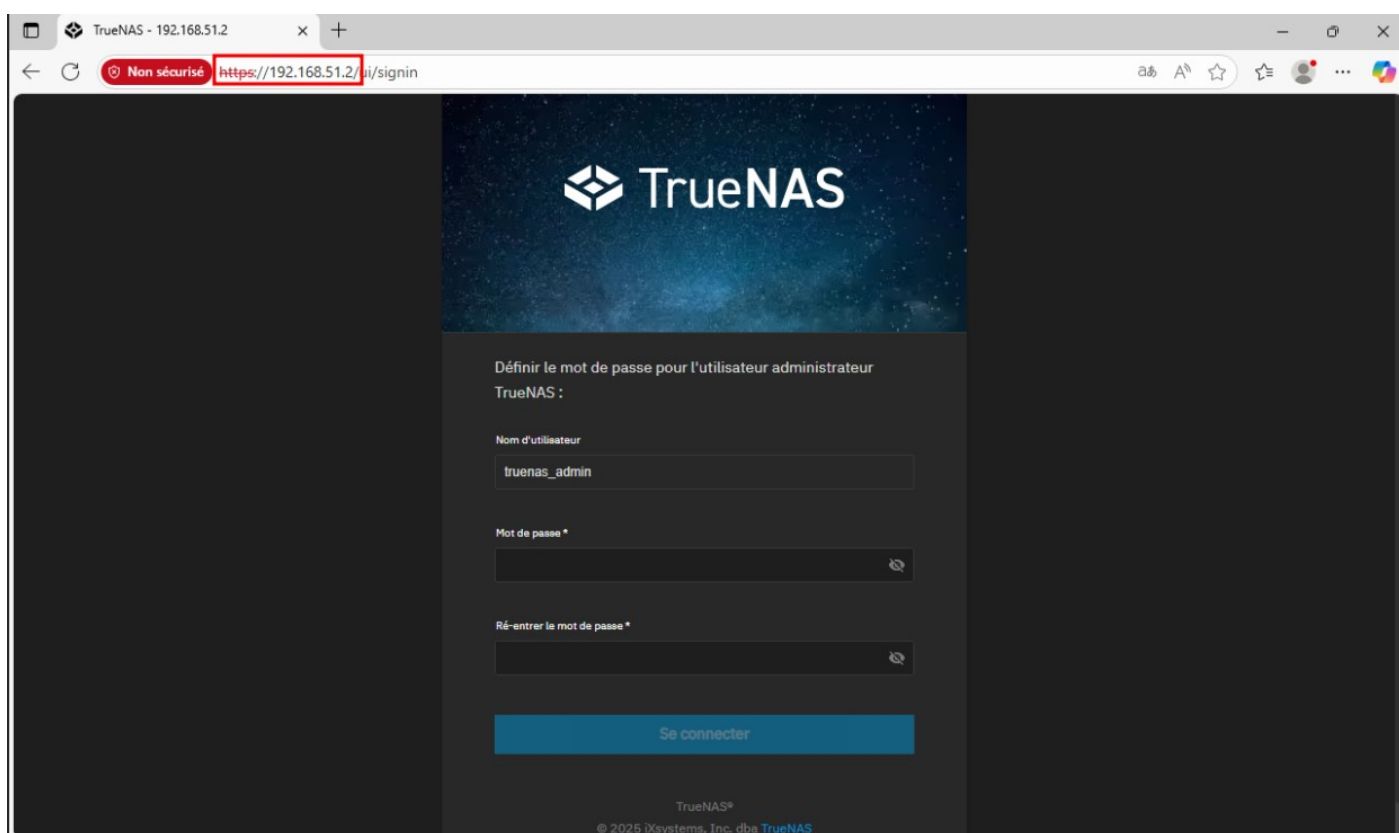
Faite exactement pareil pour l'autre SAN du site B en changeant l'adressage IP.

SAN

Configuration de TrueNAS via l'interface Web

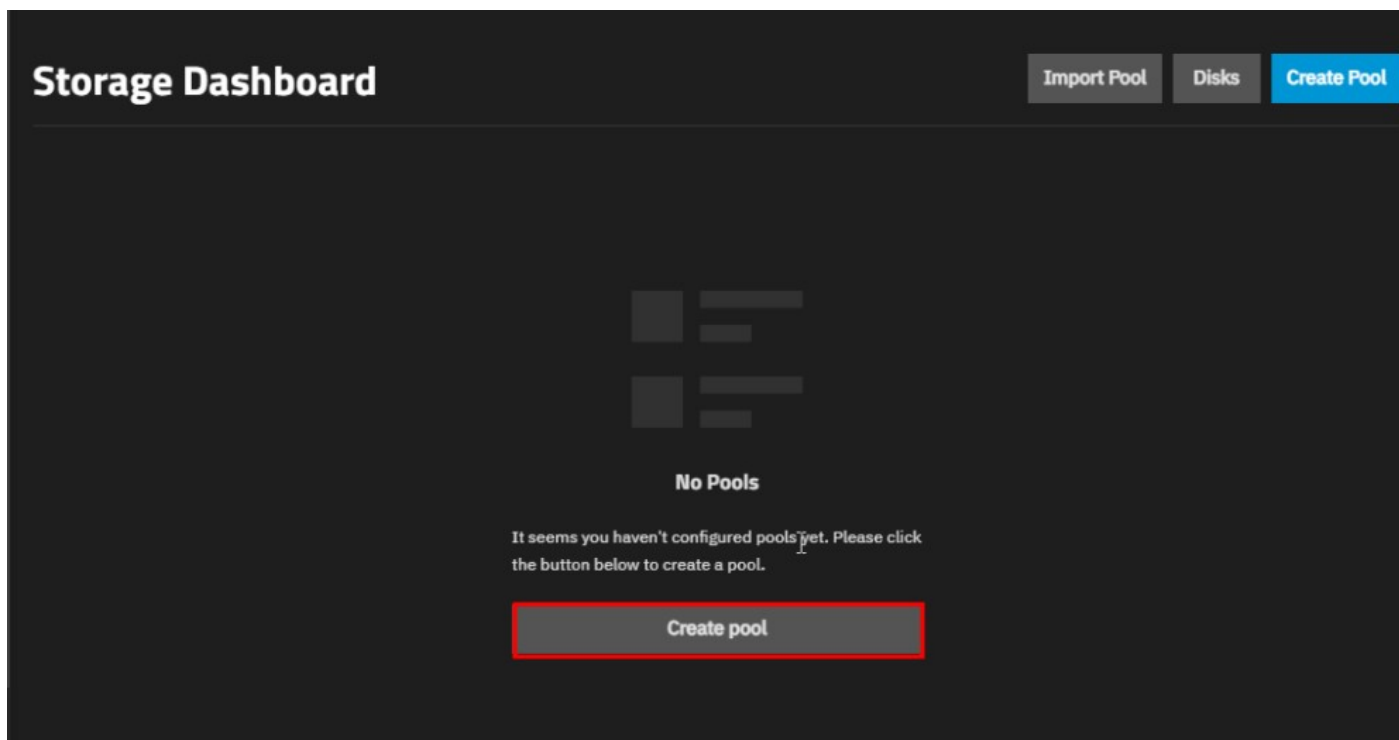
1. Accès à l'interface d'administration

On utilise un navigateur web pour se connecter à l'interface graphique de TrueNAS en saisissant l'adresse IP configurée à l'étape précédente : **192.168.51.2**.

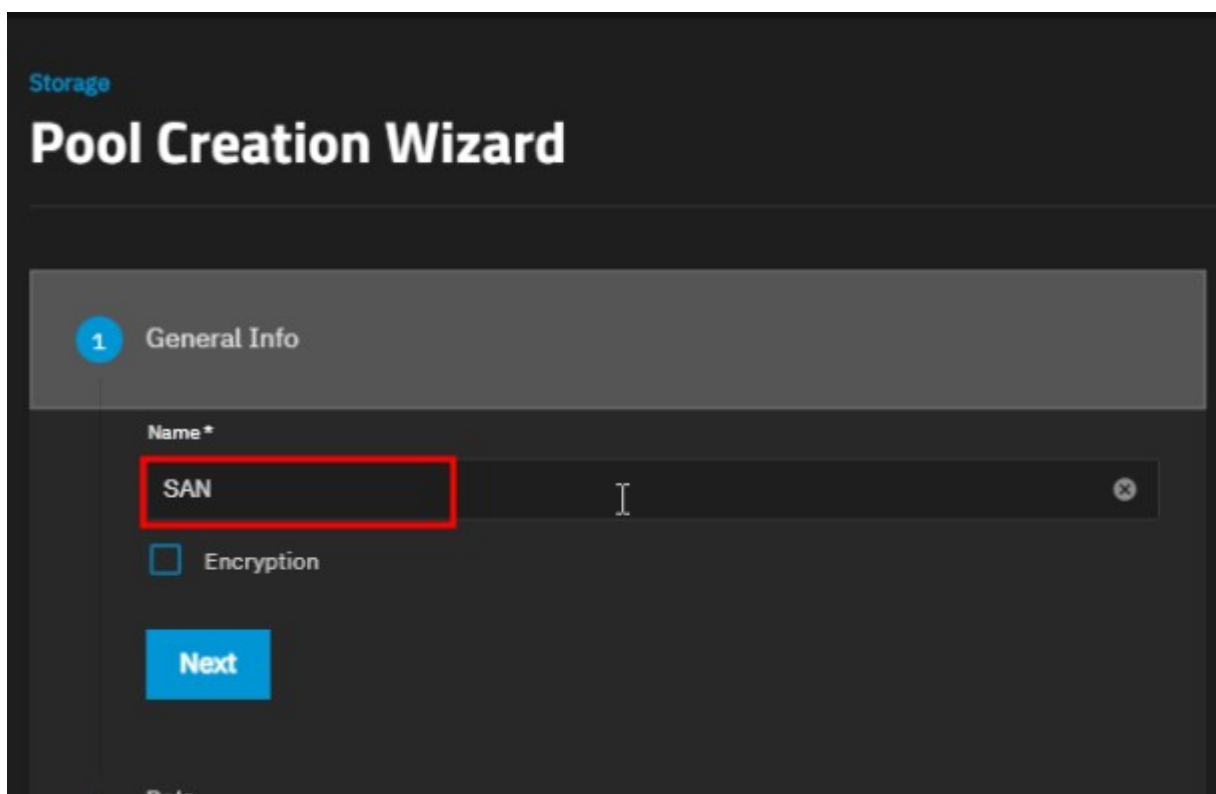


Les identifiants par défaut (truenas_admin / admin) et d'ajouter des disques virtuels dans Proxmox pour la suite.

Encadré rouge : Dans le "Storage Dashboard" (Tableau de bord de stockage), on clique sur le bouton « **Create pool** ».



Encadré rouge : Dans la première étape de l'assistant ("General Info"), on donne un nom au pool. Ici, on saisit « SAN ».



Encadré rouge : Dans la section "Data", on sélectionne le mode de disposition (**Layout**) des disques. On choisit « **Mirror** » (Miroir).

2

Data

Normal VDEV type, used for primary storage operations. ZFS pools always have at least one DATA VDEV.

Layout * ?

Mirror

Automated Disk Selection

Disk Size *

64 GiB (HDD)

☐ Treat Disk Size as Minimum

?

Width *

2

Number of VDEVs *

1

Advanced Options

Manual disk selection allows you to create VDEVs and add disks to those VDEVs individually.

Manual Disk Selection

Encadré rouge : On clique sur le bouton « **Create Pool** ».

8

Review

General Info

Pool Name

SAN

Topology Summary

Details

Data

1 × MIRROR | 2 × 64 GiB (HDD)

Est. Usable Raw Capacity

64 GiB

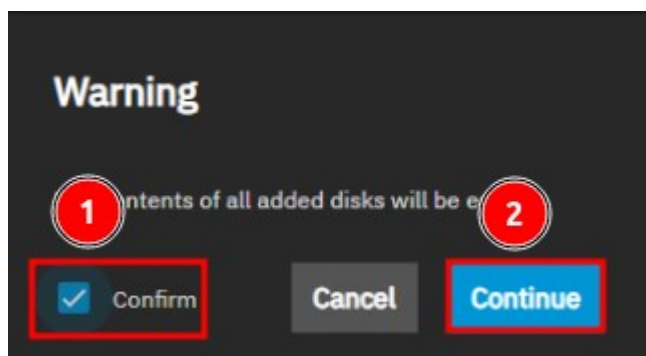
Back

Inspect VDEVs

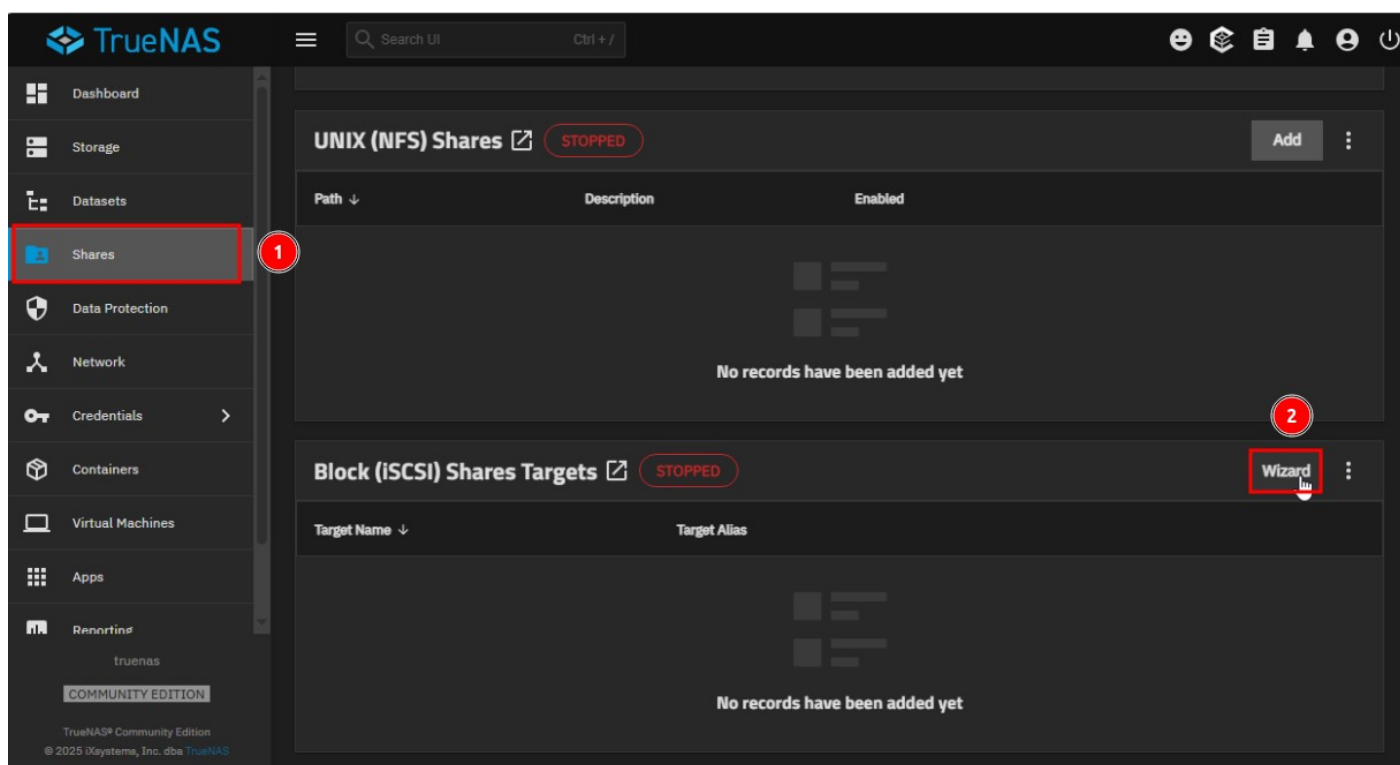
Start Over

Create Pool

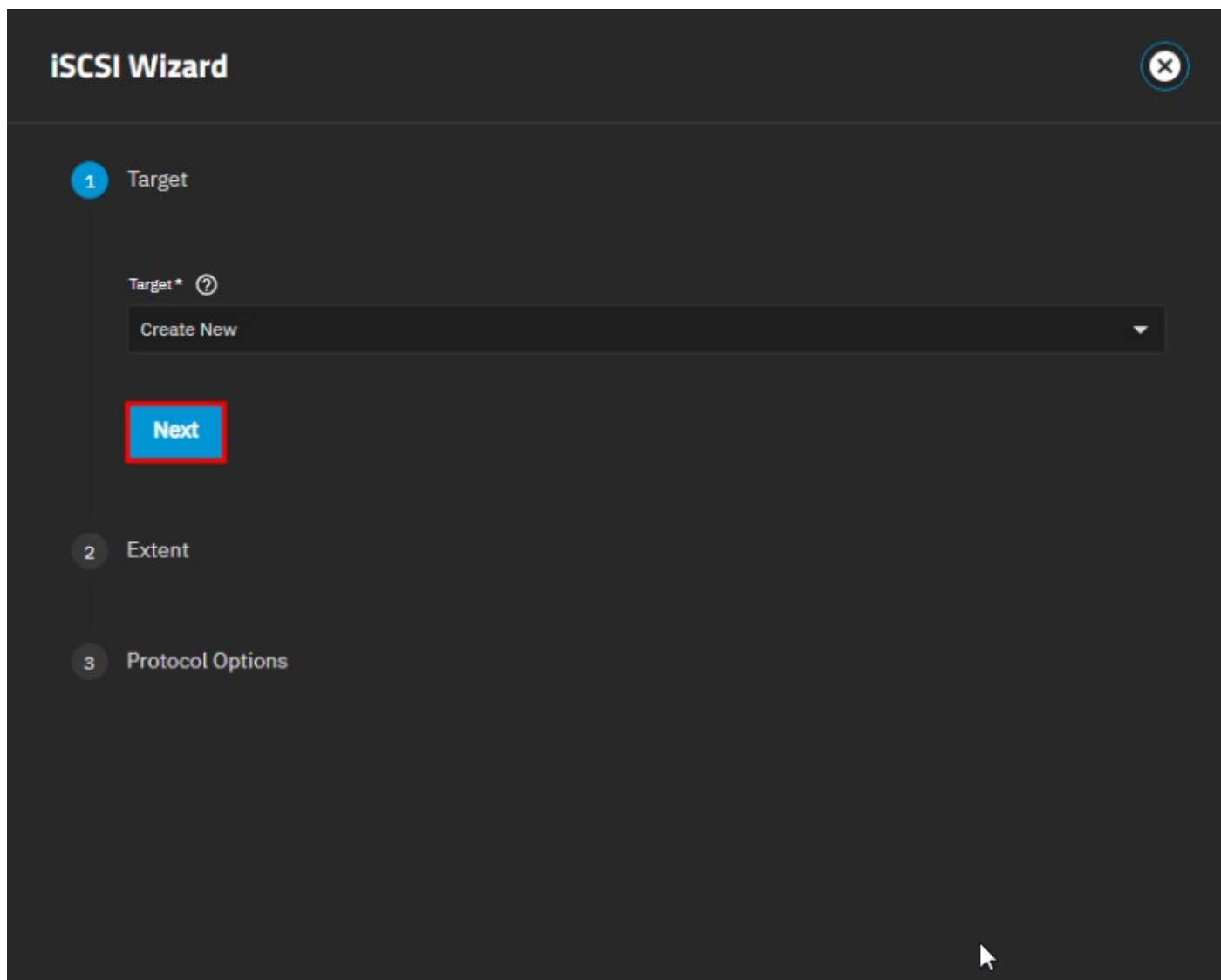
- **Encadré 1** : On coche la case « **Confirm** ».
- **Encadré 2** : On clique sur le bouton « **Continue** ».



- **Encadré 1** : Dans le menu latéral de gauche, on clique sur l'onglet « **Shares** » (Partages).
- **Encadré 2** : Dans la section "Block (iSCSI) Shares Targets", on clique sur le bouton « **Wizard** » (Assistant).



Encadré rouge : On clique sur le bouton « **Next** ».



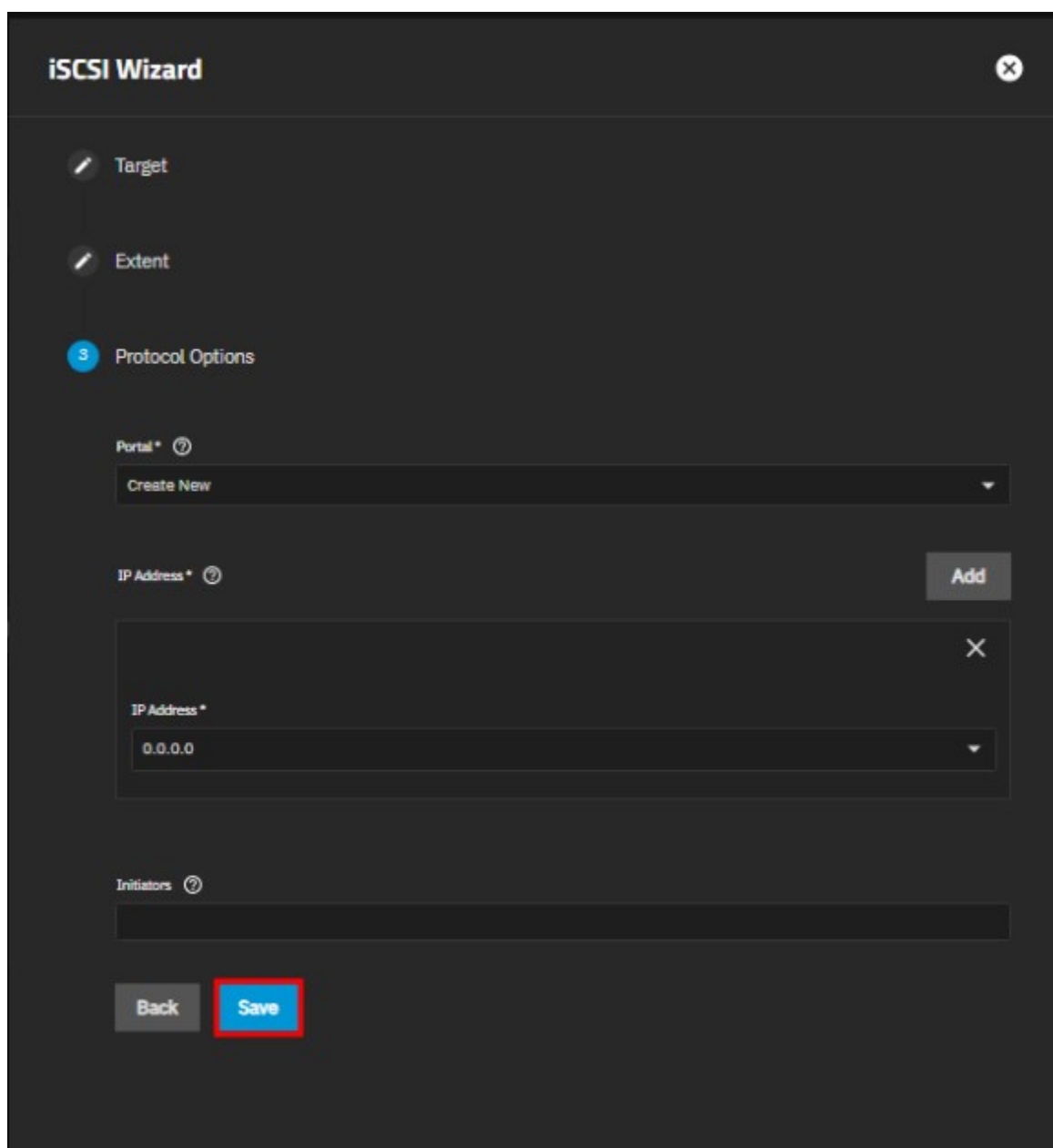
- **Encadré 1 (Name)** : Vous nommez cet espace de stockage virtuel « **backup02** ».
- **Encadré 2 (Device)** : Vous choisissez « **Create New** » pour créer un nouveau périphérique de type bloc (zvol).
- **Encadré 3 (Pool/Dataset)** : Vous sélectionnez l'emplacement physique où ce disque sera créé, ici sur votre pool nommé « **SAN** » (/mnt/SAN).
- **Encadré 4 (Size)** : Vous fixez la taille de ce disque virtuel à **20 GiB**.
- **Encadré 5** : Vous cliquez sur « **Next** » pour passer aux options finales.

The image shows the 'iSCSI Wizard' configuration window. It has a dark theme and a close button in the top right. The configuration fields are as follows:

- Name ***: A text input field containing 'backup02'. A red box highlights the input, and a red circle with the number '1' is next to it.
- Extent Type ***: A dropdown menu with 'Device' selected.
- Device ***: A dropdown menu with 'Create New' selected. A red box highlights the 'Create New' option, and a red circle with the number '2' is next to it.
- Pool/Dataset ***: A tree view showing a hierarchy. The root is '/mnt/SAN'. Below it is '/mnt', and under '/mnt' is 'SAN'. A red box highlights the entire tree view, and a red circle with the number '3' is next to it. A 'Create Dataset' button is visible on the right side of the tree view.
- Size ***: A text input field containing '20 GiB'. A red box highlights the input, and a red circle with the number '4' is next to it.
- Sharing Platform ***: A dropdown menu with 'VMware: Extent block size 512b, TPC enabled, no Xen compat mode, SSD speed' selected.
- Buttons**: At the bottom, there are 'Back' and 'Next' buttons. The 'Next' button is highlighted with a red box, and a red circle with the number '5' is next to it.

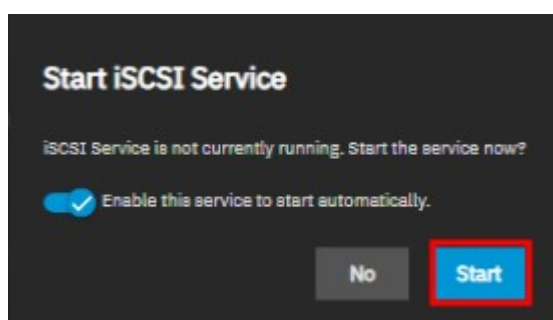
At the bottom left, there is a tab labeled '3 Protocol Options'.

Encadré rouge : Vous cliquez sur le bouton « **Save** ».



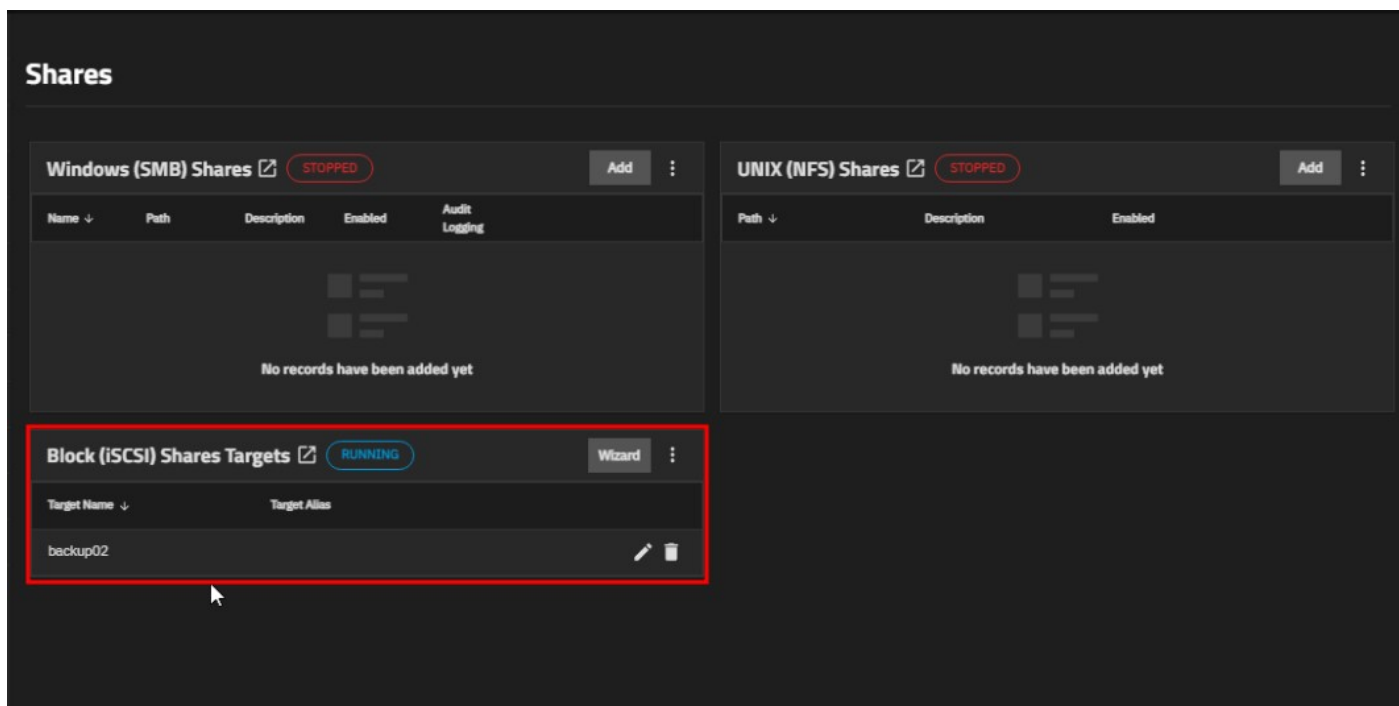
The image shows the 'iSCSI Wizard' window, specifically the 'Protocol Options' step. The wizard has three steps: 'Target', 'Extent', and 'Protocol Options', with the third step being the active one. The 'Portal' dropdown is set to 'Create New'. The 'IP Address' field is set to '0.0.0.0'. There is an 'Add' button next to the IP Address field. At the bottom, there are 'Back' and 'Save' buttons. The 'Save' button is highlighted with a red rectangle.

Encadré rouge : Une fenêtre surgissante vous propose de démarrer le service iSCSI. Vous cliquez sur « **Start** ».

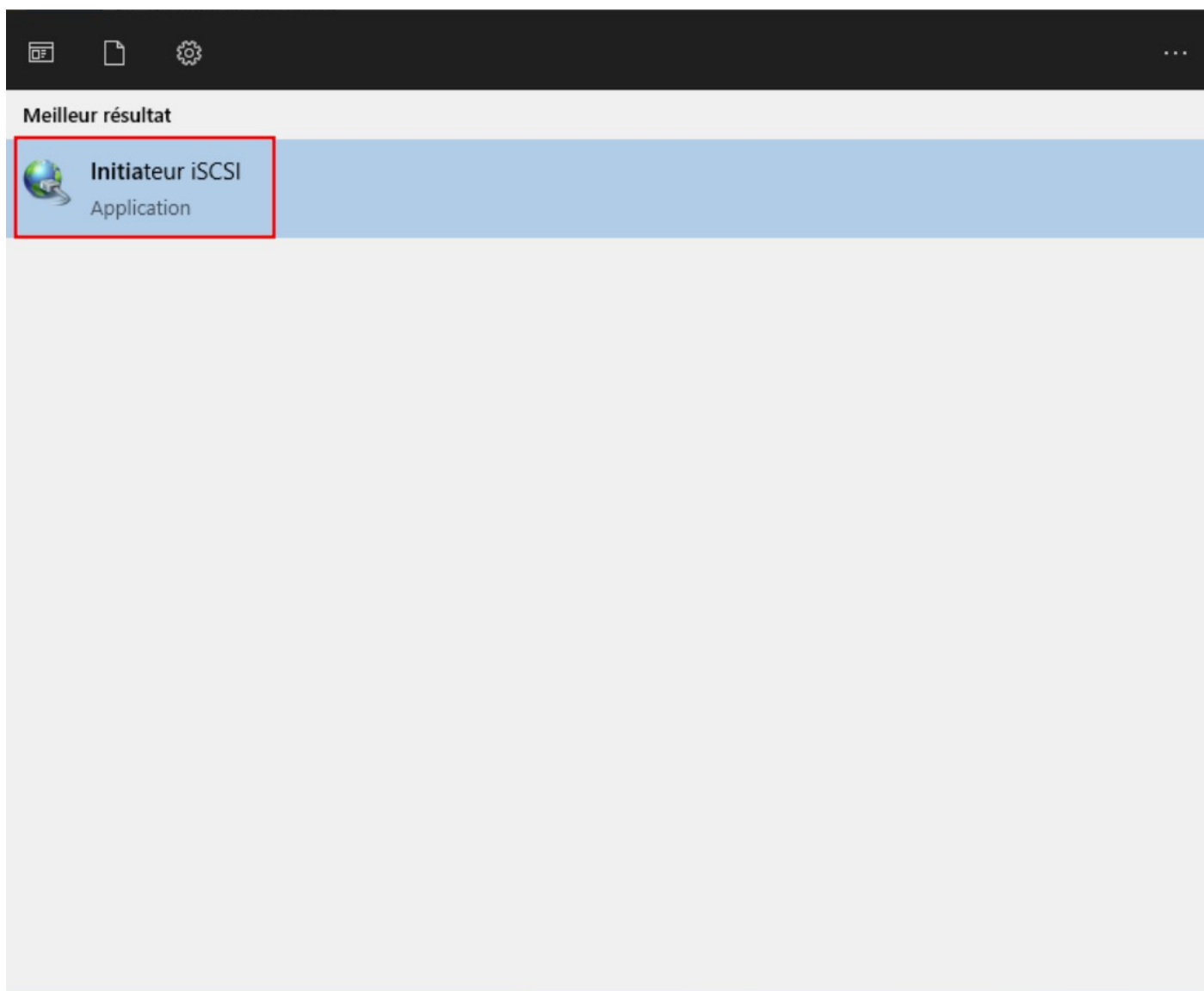


The image shows a 'Start iSCSI Service' dialog box. It contains the text 'iSCSI Service is not currently running. Start the service now?'. Below this text is a toggle switch that is turned on, with the label 'Enable this service to start automatically.'. At the bottom, there are 'No' and 'Start' buttons. The 'Start' button is highlighted with a red rectangle.

Encadré rouge : Dans le tableau de bord des partages, on voit maintenant que la section « **Block (iSCSI) Shares Targets** » est marquée comme « **RUNNING** » (En cours d'exécution).



Encadré rouge : Vous recherchez et lancez l'application « **Initiateur iSCSI** » dans le menu Démarrer de Windows.



- **Encadré 1** : Dans le champ « Cible », vous saisissez l'adresse IP de votre serveur TrueNAS : **192.168.50.2**.
- **Encadré 2** : Vous cliquez sur le bouton « **Connexion rapide...** ».

Propriétés de : Initiateur iSCSI



Cibles Découverte Cibles favorites Volumes et périphériques RADIUS Configuration

Connexion rapide

Pour découvrir une cible et s'y connecter à l'aide d'une connexion de base, tapez son adresse IP ou nom DNS, puis cliquez sur Connexion rapide.

Cible :

192.168.50.2

Connexion rapide...

Cibles découvertes

Actualiser

Nom

Statut

Pour vous connecter à l'aide d'options avancées, sélectionnez une cible, puis cliquez sur Connexion.

Connexion

Pour déconnecter entièrement une cible, sélectionnez-la, puis cliquez sur Déconnecter.

Déconnexion

Pour les propriétés cibles, notamment la configuration des sessions, sélectionnez la cible et cliquez sur Propriétés.

Propriétés...

Pour configurer les périphériques associés à une cible, sélectionnez la cible, puis cliquez sur Périphériques.

Périphériques...

OK

Annuler

Appliquer

Windows a trouvé la cible nommée iqn.2005-10.org.freenas.ctl:backup01. Le statut indique déjà « **Connecté** ».

Connexion rapide

Les cibles qui sont disponibles pour la connexion à l'adresse IP ou au nom DNS fourni sont répertoriées ci-après. Si plusieurs cibles sont disponibles, vous devez connecter chaque cible individuellement.

Les connexions établies ici seront ajoutées à la liste des cibles favorites et une tentative de restauration sera effectuée à chaque redémarrage de l'ordinateur.

Cibles découvertes

Nom	Statut
iqn.2005-10.org.freenas.ctl:backup01	Connecté

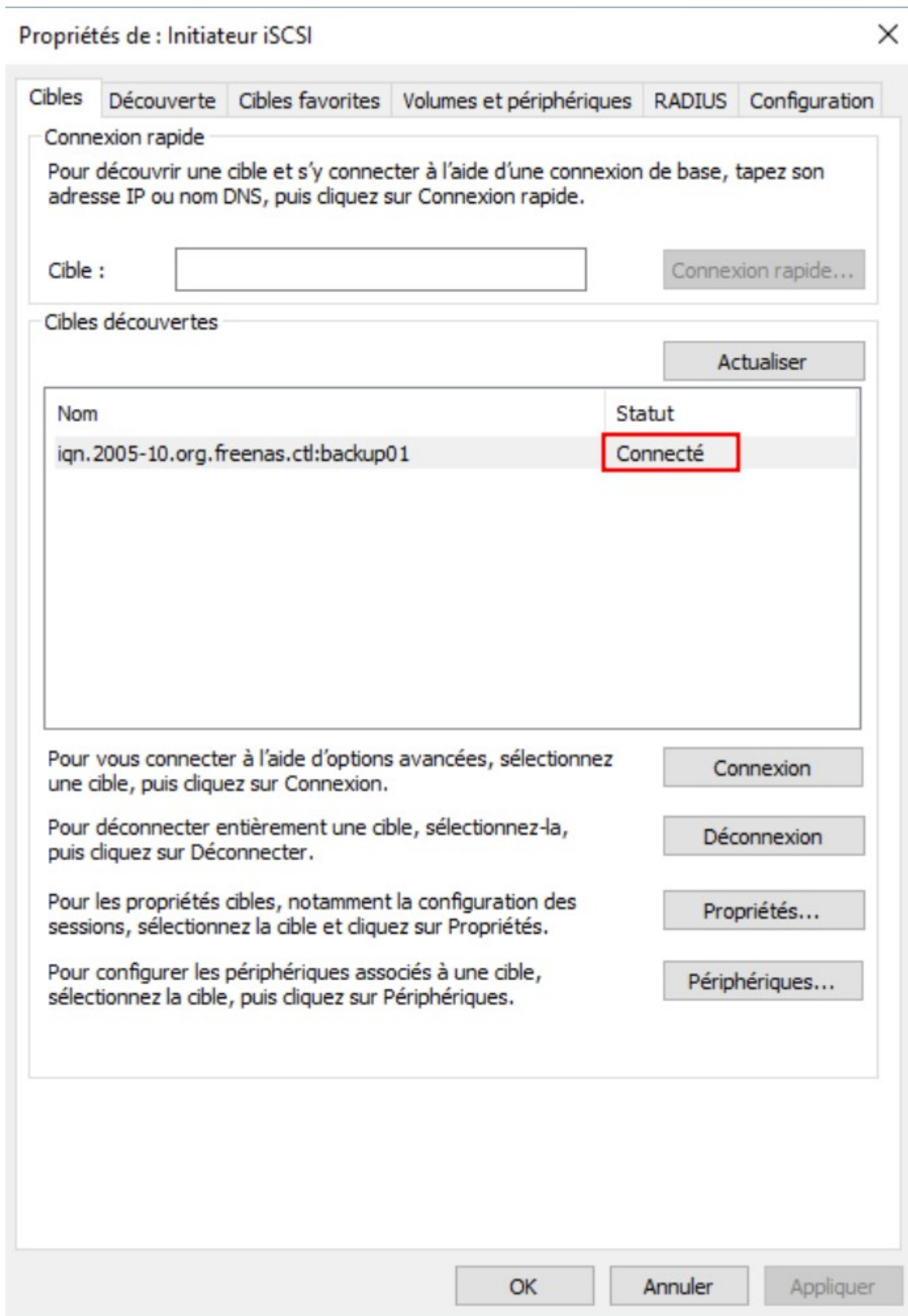
Rapport de progression

Connexion immédiate réussie.Échec de la connexion persistante, la cible ne sera pas disponible après le redémarrage du système.

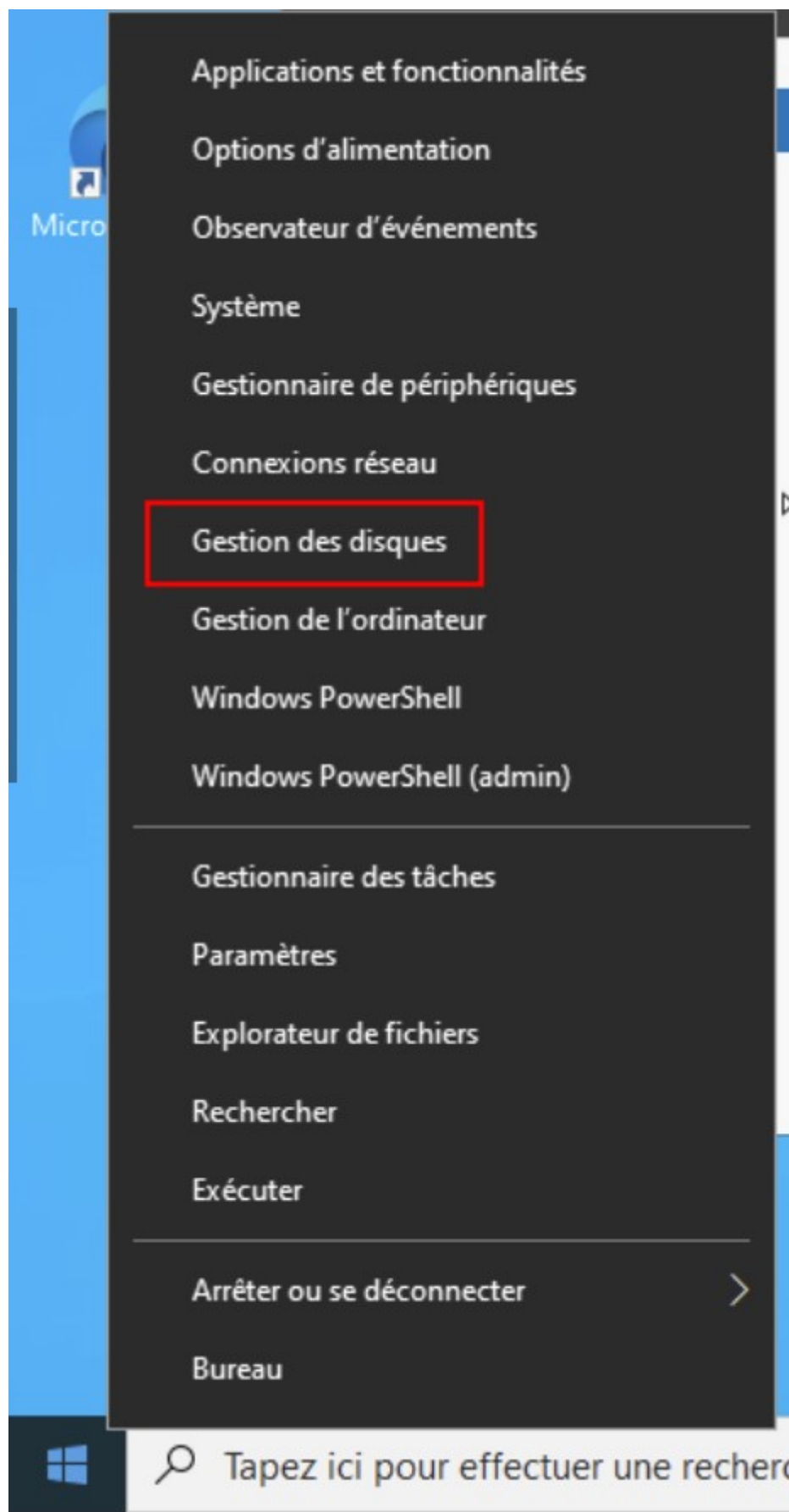
Connexion

Terminer

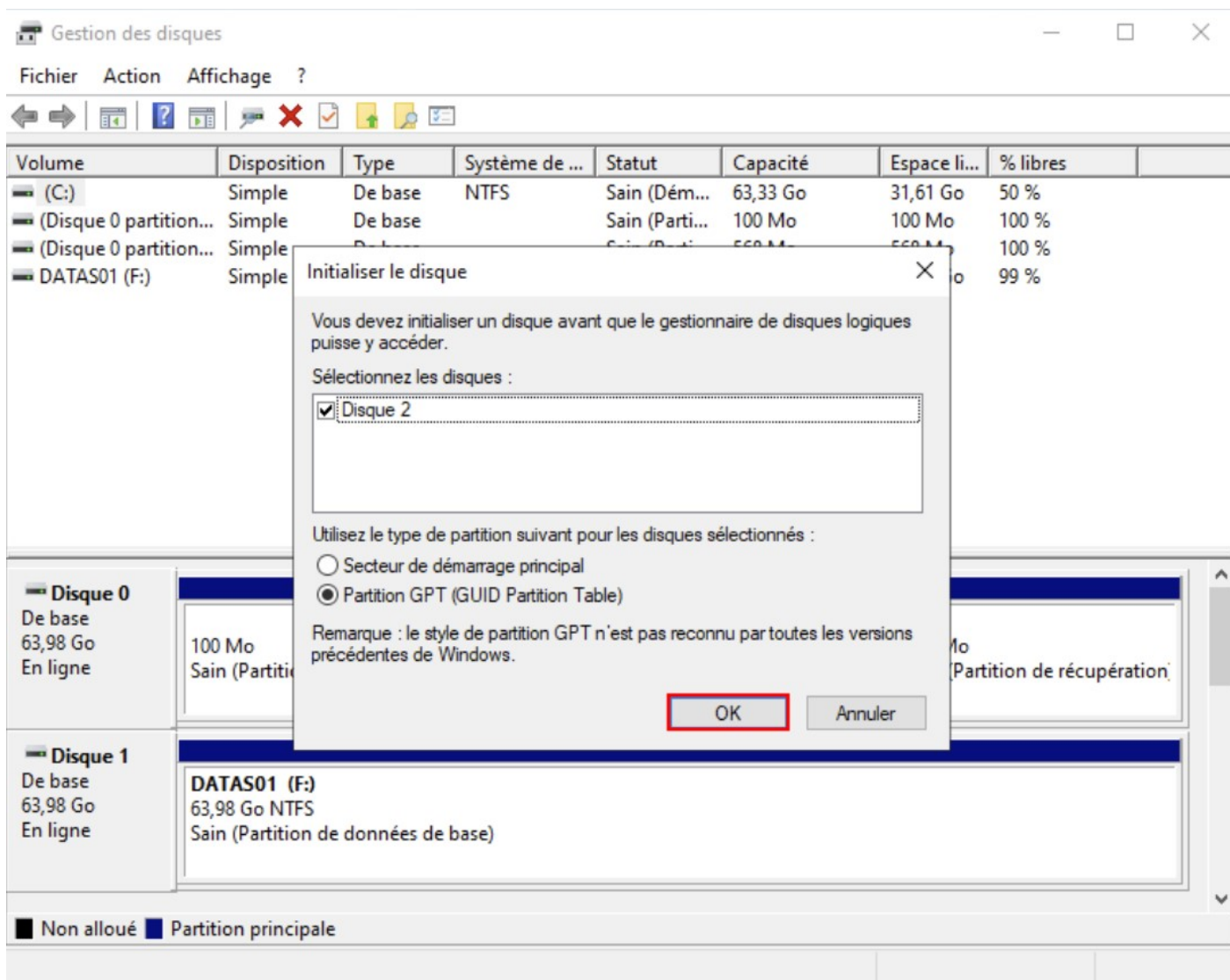
Dans la liste des cibles découvertes, vous vérifiez que le statut de votre disque est bien marqué comme « **Connecté** ».



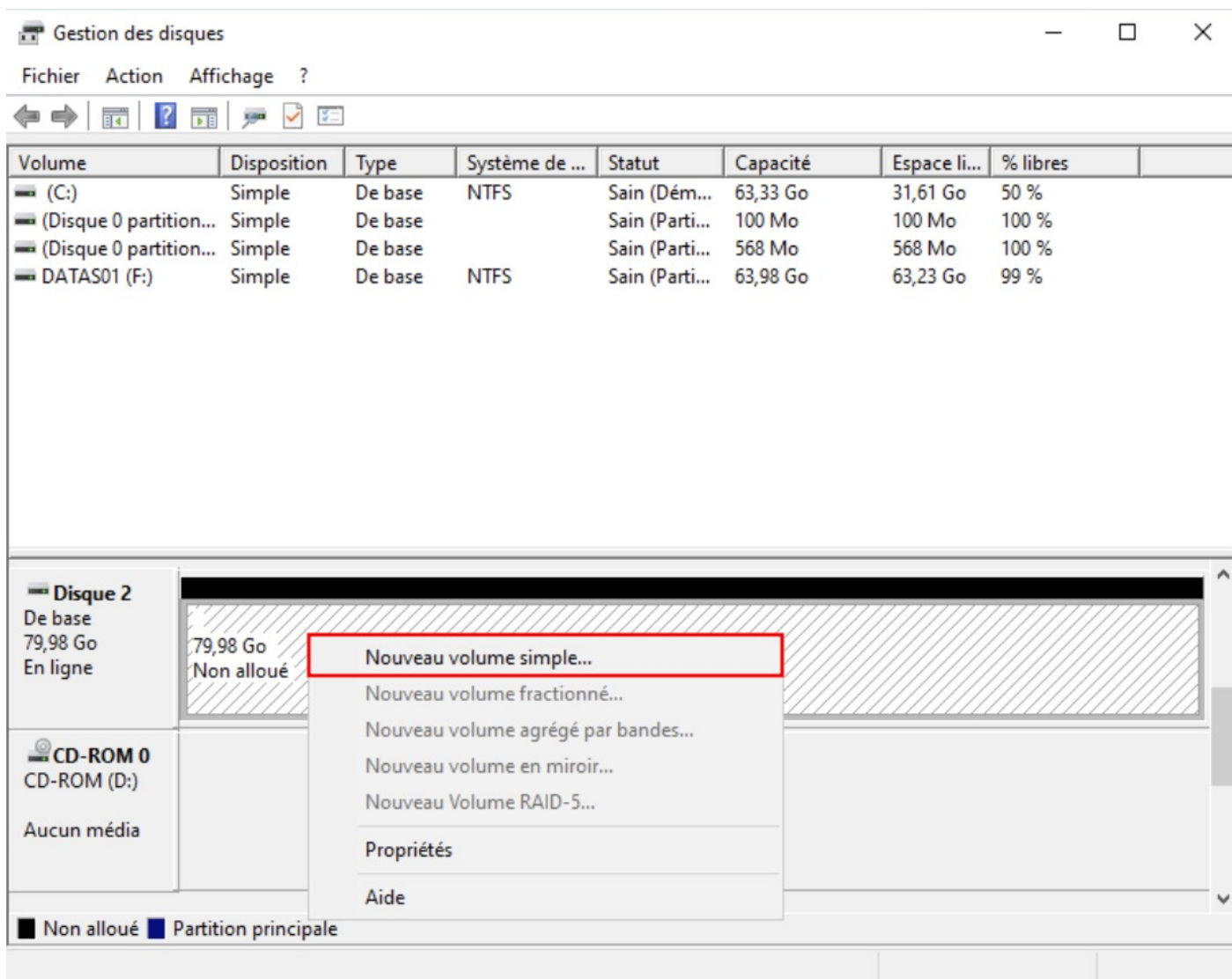
Encadré rouge : Vous faites un clic droit sur le bouton Démarrer de Windows et sélectionnez « **Gestion des disques** ».



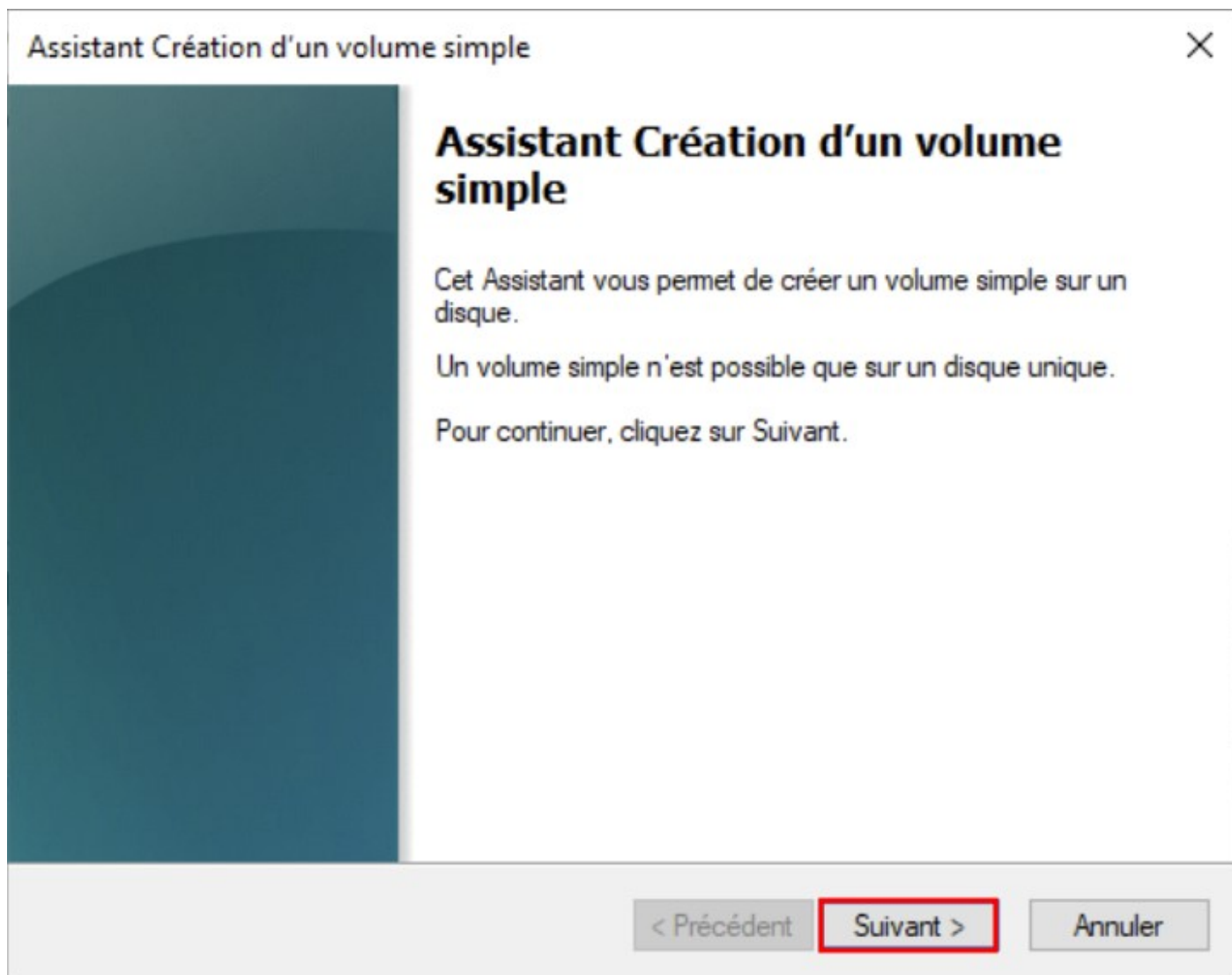
Encadré rouge : Vous cliquez sur le bouton « **OK** » en laissant l'option **GPT** sélectionnée.



Encadré rouge : Dans la partie basse de la fenêtre, vous faites un clic droit sur la zone hachurée ("Non alloué") du Disque 2 et choisissez « **Nouveau volume simple...** ».



Vous cliquez sur « **Suivant** > » pour commencer la configuration.



Vous cliquez sur « **Suivant** > » pour utiliser la totalité de l'espace disponible (environ 20 Go).

Assistant Création d'un volume simple

×

Spécifier la taille du volume
Choisir une taille de volume comprise entre la taille maximale et la taille minimale.

Espace disque maximal en Mo :

81902

Espace disque minimal en Mo :

8

Taille du volume simple en Mo :

81902

▲▼

< Précédent

Suivant >

Annuler

Vous cliquez sur « **Suivant** > » pour accepter l'attribution automatique d'une lettre de lecteur.

Assistant Création d'un volume simple

Attribuer une lettre de lecteur ou de chemin d'accès
Pour un accès plus facile, vous pouvez assigner une lettre de lecteur ou un chemin d'accès au lecteur sur votre partition.

☒ Attribuer la lettre de lecteur suivante : K ▾

☐ Monter dans le dossier NTFS vide suivant : Parcourir...

☐ Ne pas attribuer de lettre de lecteur ni de chemin d'accès de lecteur

< Précédent **Suivant >** Annuler

- **Encadré 1** : Dans l'étape « Formater une partition », vous donnez un nom explicite au disque en saisissant « **SAN** » dans le champ **Nom de volume**.
- **Encadré 2** : Vous cliquez sur le bouton « **Suivant >** ».

Assistant Création d'un volume simple

×

Formater une partition

Pour stocker des données sur cette partition, vous devez d'abord la formater.

Indiquez si vous voulez formater cette partition, et le cas échéant, les paramètres que vous voulez utiliser.

☐

Ne pas formater ce volume

☒

Formater ce volume avec les paramètres suivants :

Système de fichiers :

NTFS

Taille d'unité d'allocation :

Par défaut

Nom de volume :

SAN

☒ Effectuer un formatage rapide

☐ Activer la compression des fichiers et dossiers

1

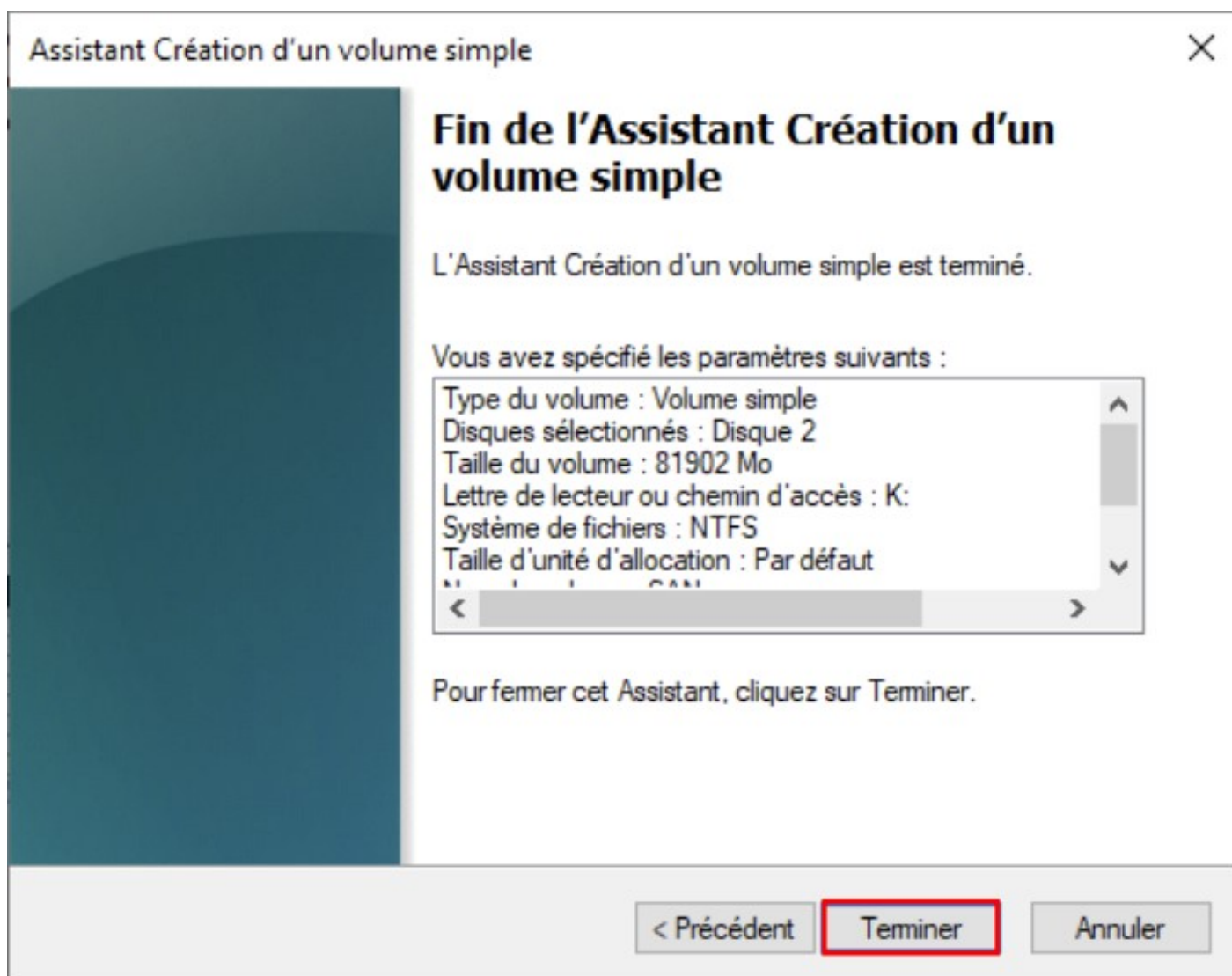
2

< Précédent

Suivant >

Annuler

Encadré rouge : Vous cliquez sur le bouton « **Terminer** ».



- **Encadré rouge** : On voit le résultat final dans la liste des volumes.
 - Le lecteur est maintenant actif sous le nom **SAN (K:)**.
 - Il est bien au format **NTFS** et son statut est « **Sain** ».
 - On constate que sa capacité totale est disponible à 100%.

Gestion des disques

Fichier Action Affichage ?

← → 📅 ? 📅 🗨️ 📄 📄

Volume	Disposition	Type	Système de ...	Statut	Capacité	Espace li...	% libres
(C:)	Simple	De base	NTFS	Sain (Dém...	63,33 Go	31,61 Go	50 %
(Disque 0 partition...	Simple	De base		Sain (Parti...	100 Mo	100 Mo	100 %
(Disque 0 partition...	Simple	De base		Sain (Parti...	568 Mo	568 Mo	100 %
DATAS01 (F:)	Simple	De base	NTFS	Sain (Parti...	63,98 Go	63,23 Go	99 %
SAN (K:)	Simple	De base	NTFS	Sain (Parti...	79,98 Go	79,89 Go	100 %

Disque 2
De base
79,98 Go
En ligne

SAN (K:)
79,98 Go NTFS
Sain (Partition de données de base)

CD-ROM 0
CD-ROM (D:)
Aucun média

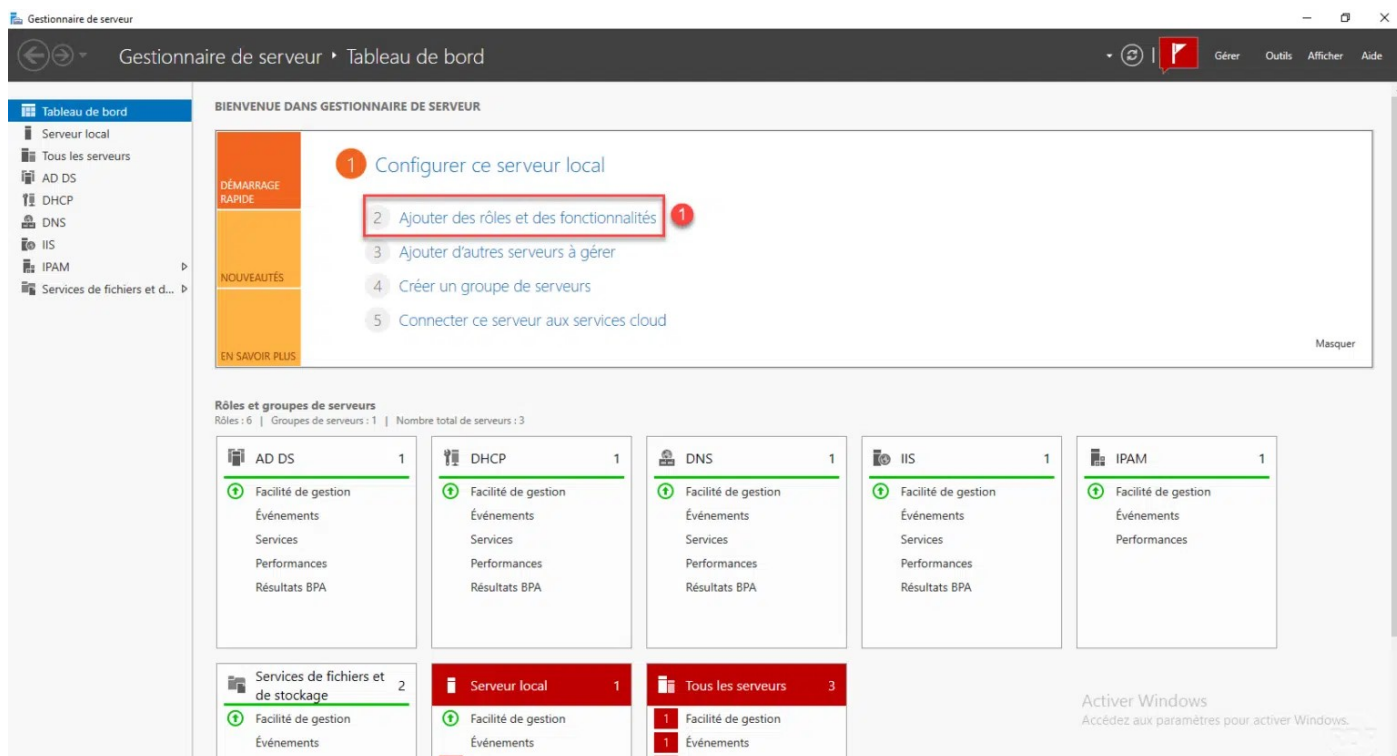
■ Non alloué ■ Partition principale

BACKUP

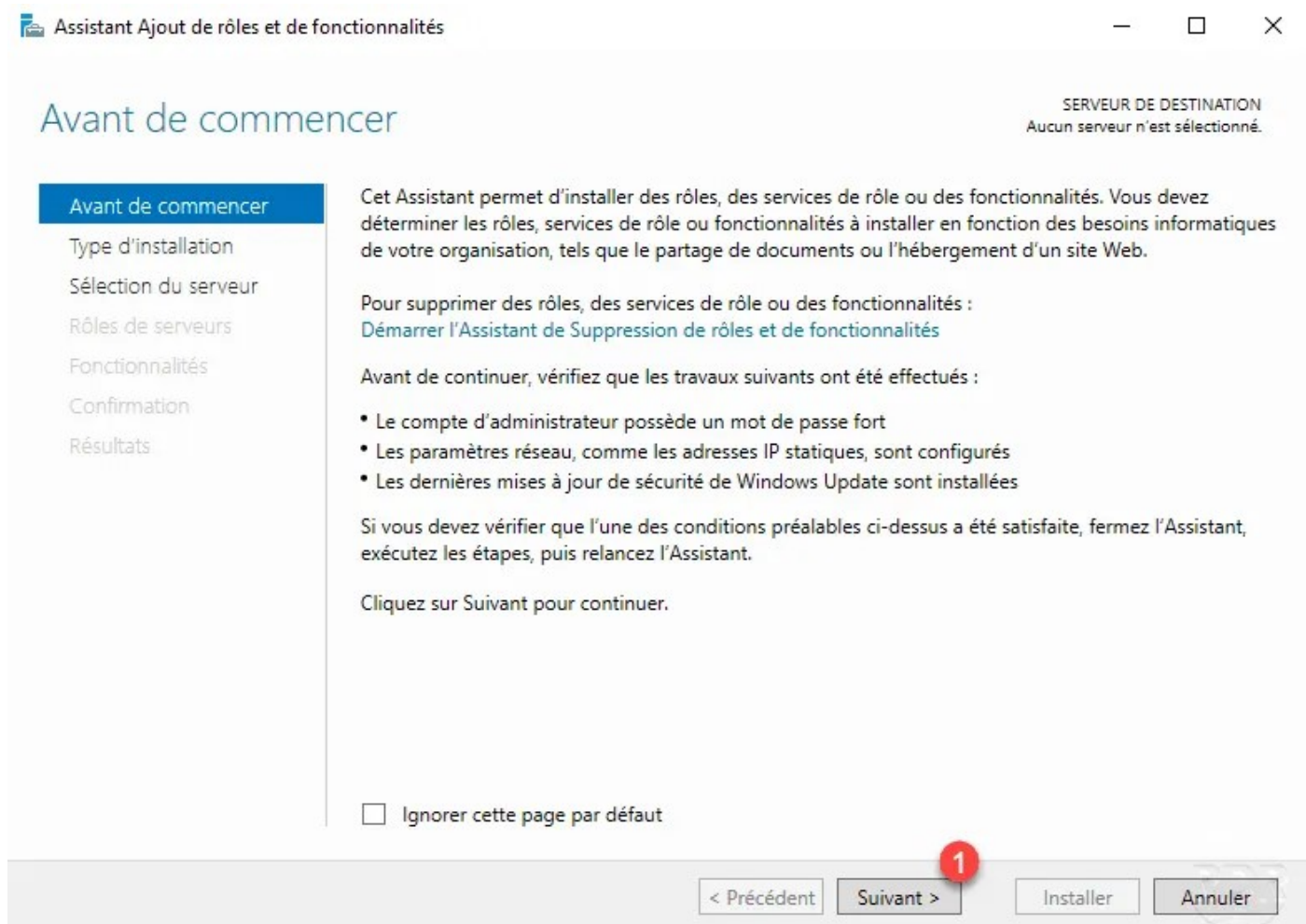
BACKUP

Configuration de Windows BackUp

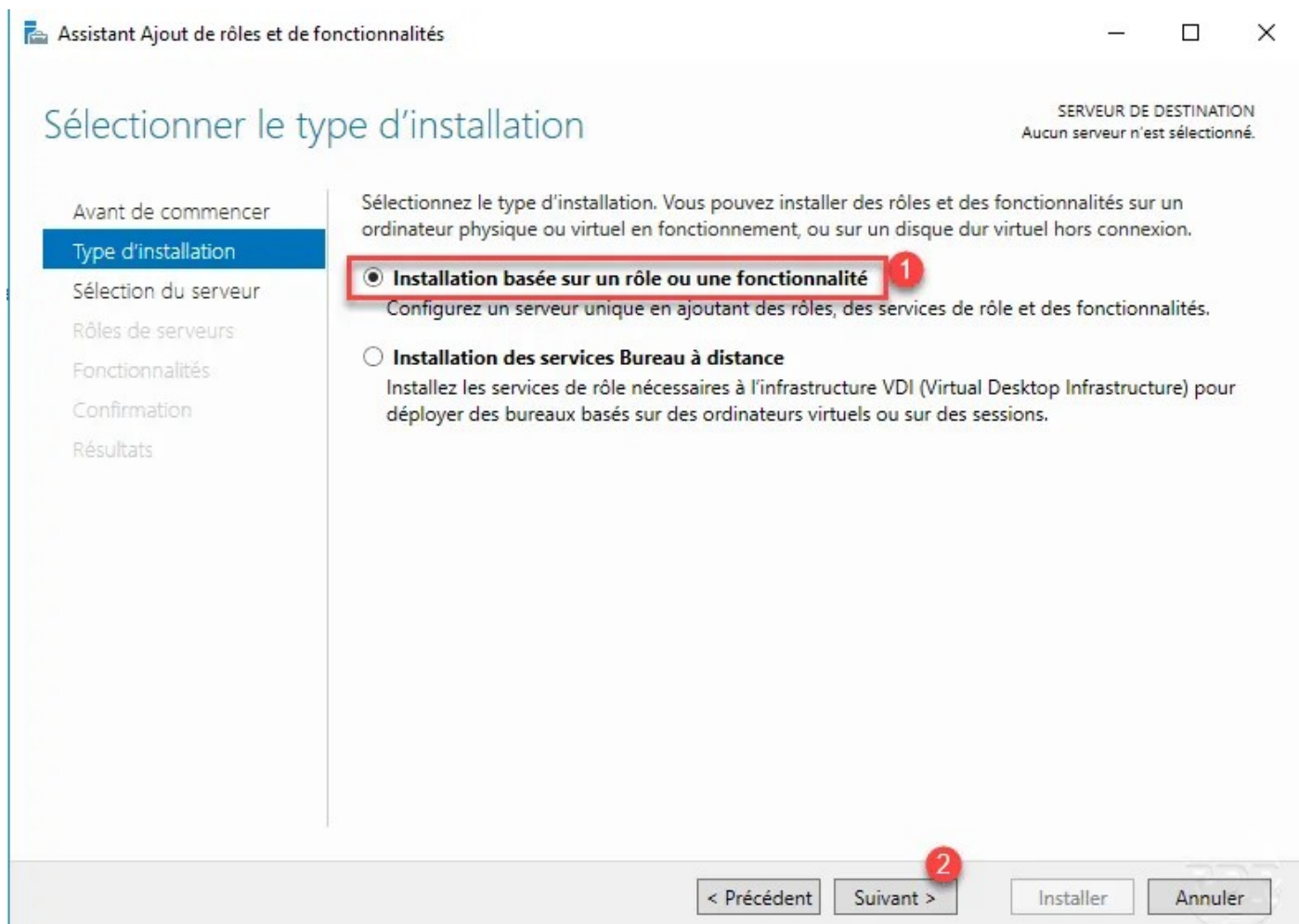
Encadré rouge : Dans le tableau de bord du Gestionnaire de serveur, on clique sur le lien « **2. Ajouter des rôles et des fonctionnalités** ».



Encadré rouge : On clique sur le bouton « **Suivant >** ».



- **Encadré 1** : On sélectionne l'option par défaut « **Installation basée sur un rôle ou une fonctionnalité** ».
- **Encadré 2** : On clique sur le bouton « **Suivant >** ».



- **Encadré rouge** : On sélectionne dans la liste le serveur cible, ici nommé **WS2022-DC1B**.
- **Flèche rouge** : On clique sur le bouton « **Suivant** > ».

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
WS2022-DC1b

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

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

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

Pool de serveurs

Filtre :

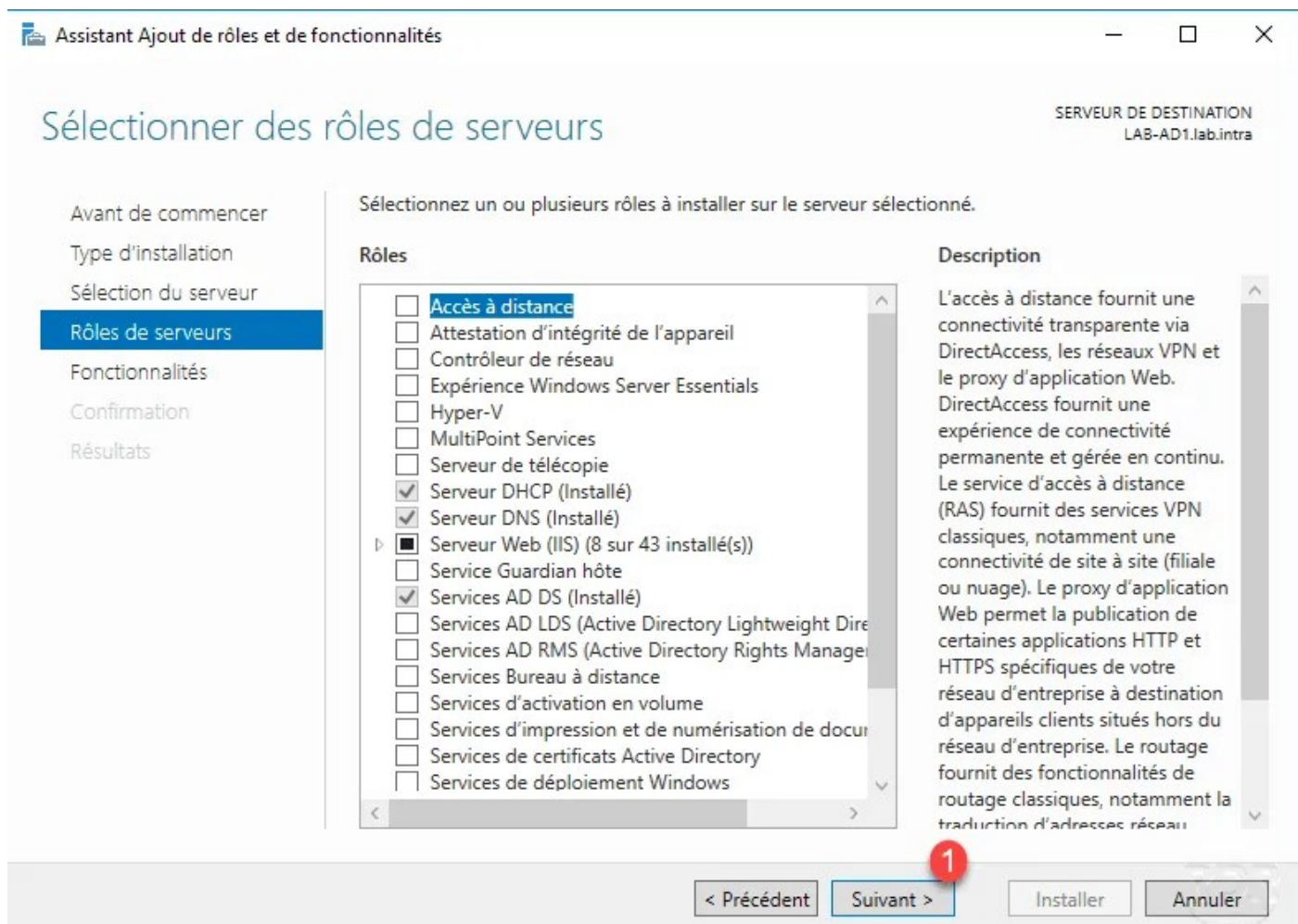
Nom	Adresse IP	Système d'exploitation
WS2022-DC1b	192.168.1.10	Microsoft Windows Server 2022 Standard

1 ordinateur(s) trouvé(s)

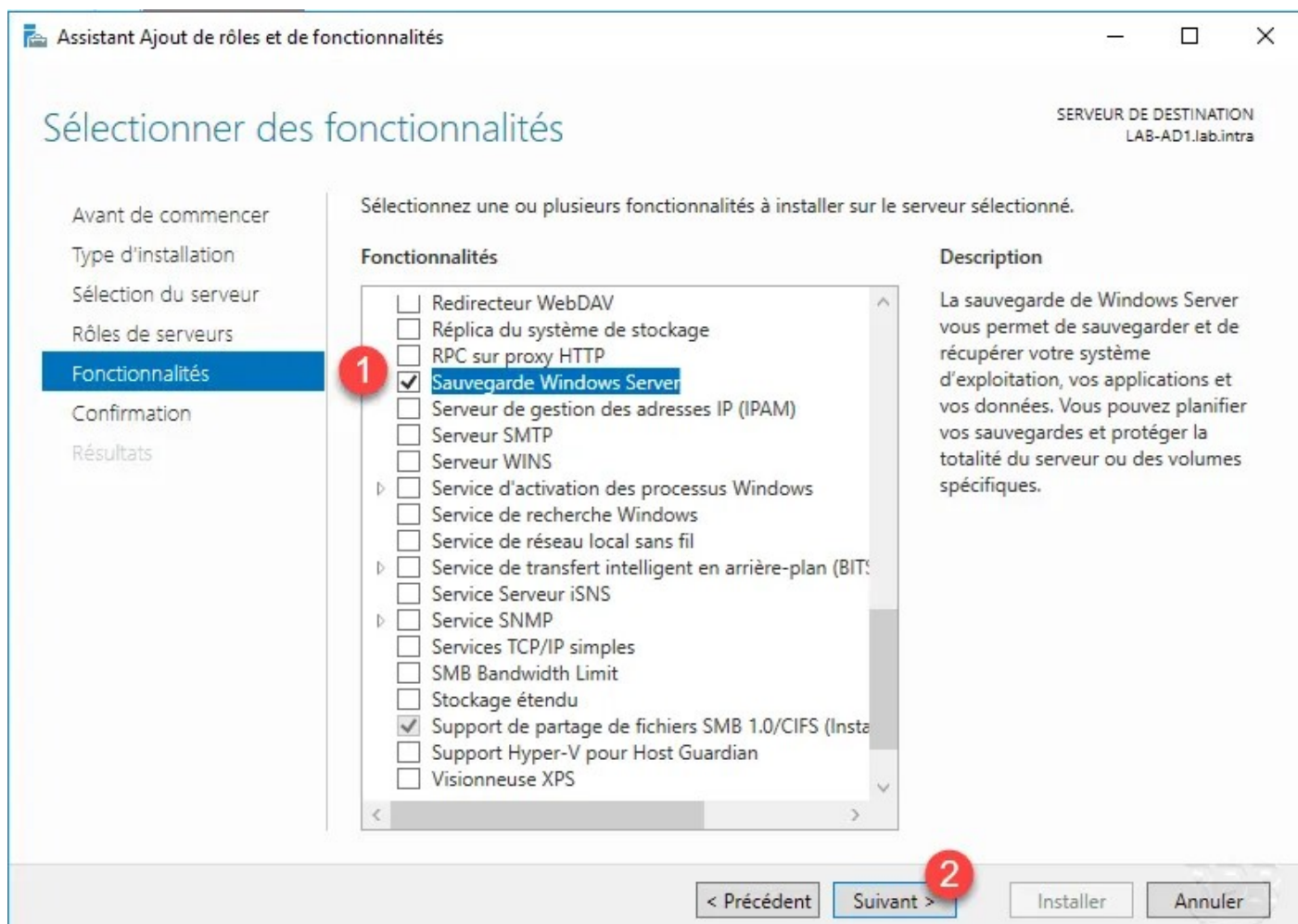
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète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

< Précédent **Suivant >** Installer Annuler

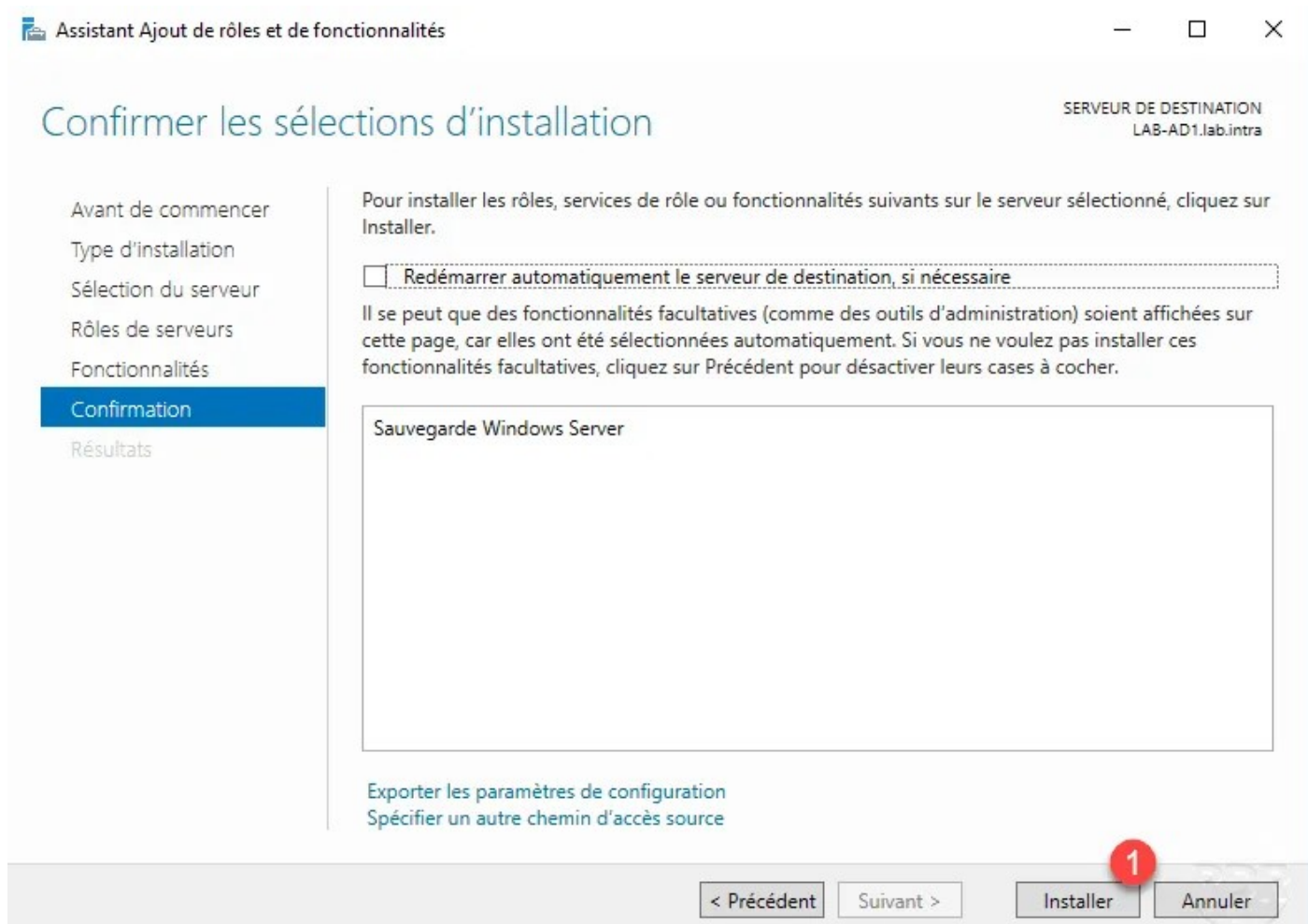
Encadré rouge : On clique sur le bouton « **Suivant >** ».



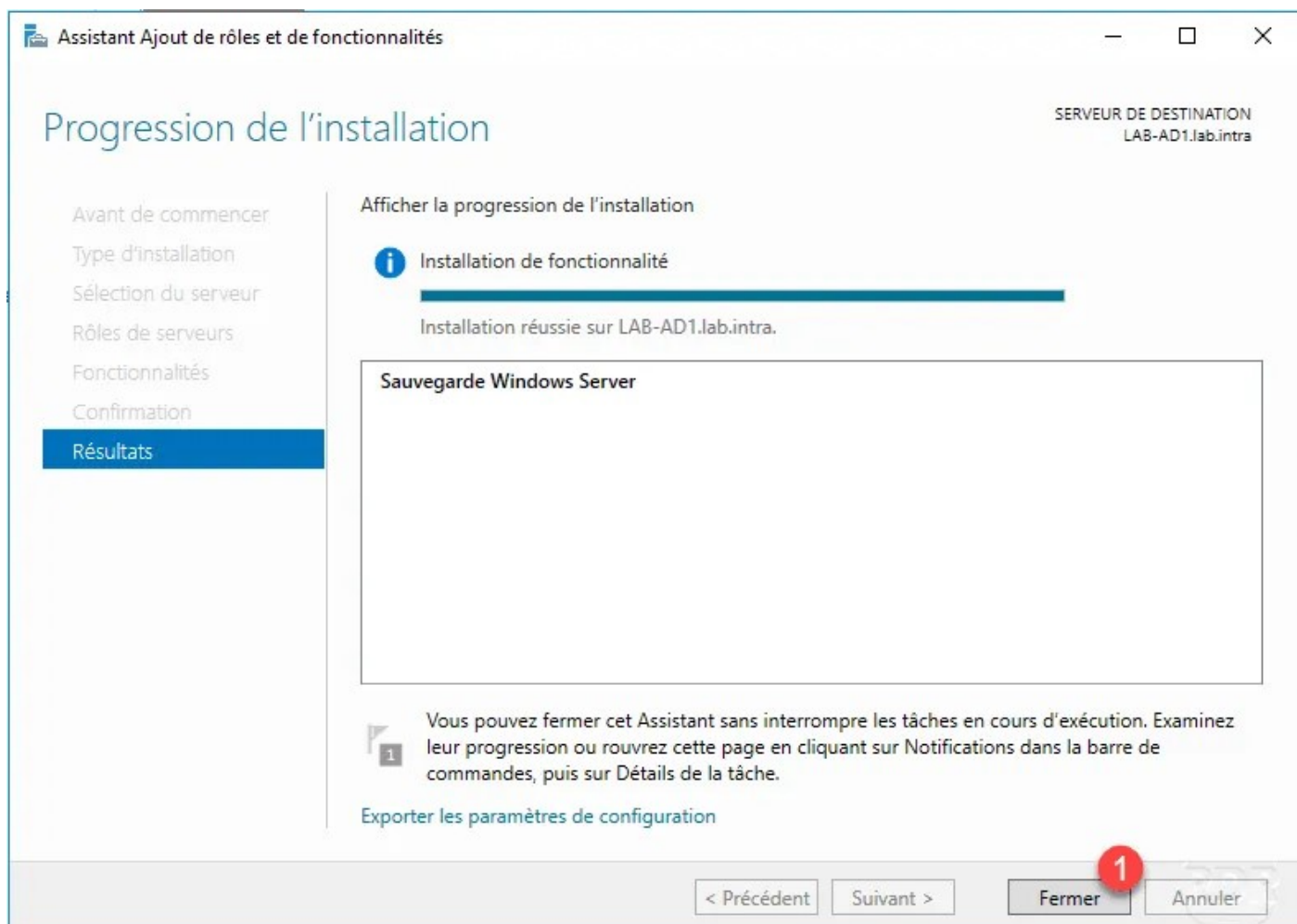
- **Encadré 1** : Dans la liste des fonctionnalités, vous cochez la case « **Sauvegarde Windows Server** ».
 - **Action** : Vous choisissez d'installer l'outil natif de Microsoft permettant de réaliser des sauvegardes complètes ou partielles du serveur.
- **Encadré 2** : Vous cliquez sur le bouton « **Suivant >** ».



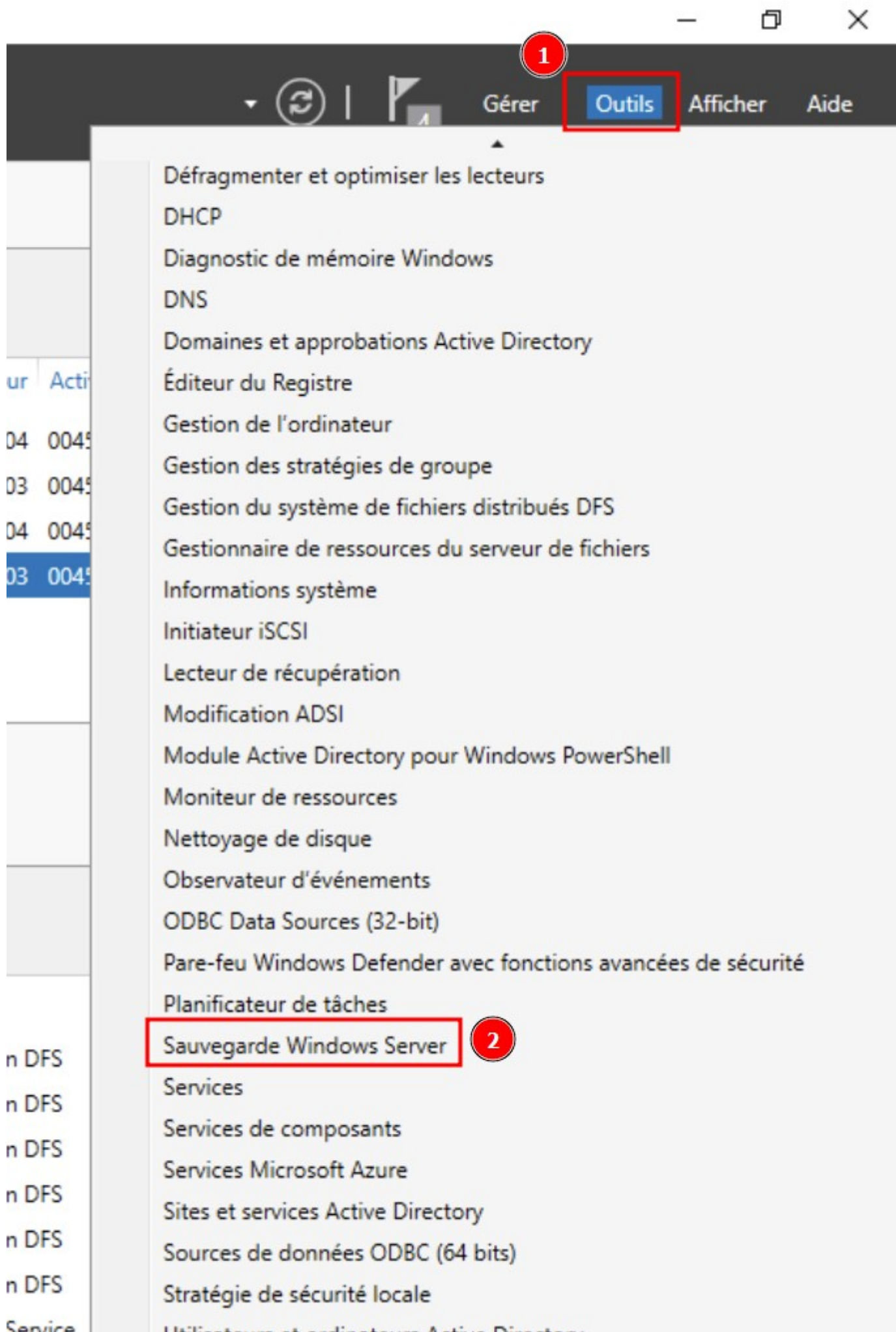
Encadré rouge : Vous cliquez sur le bouton « **Installer** ».



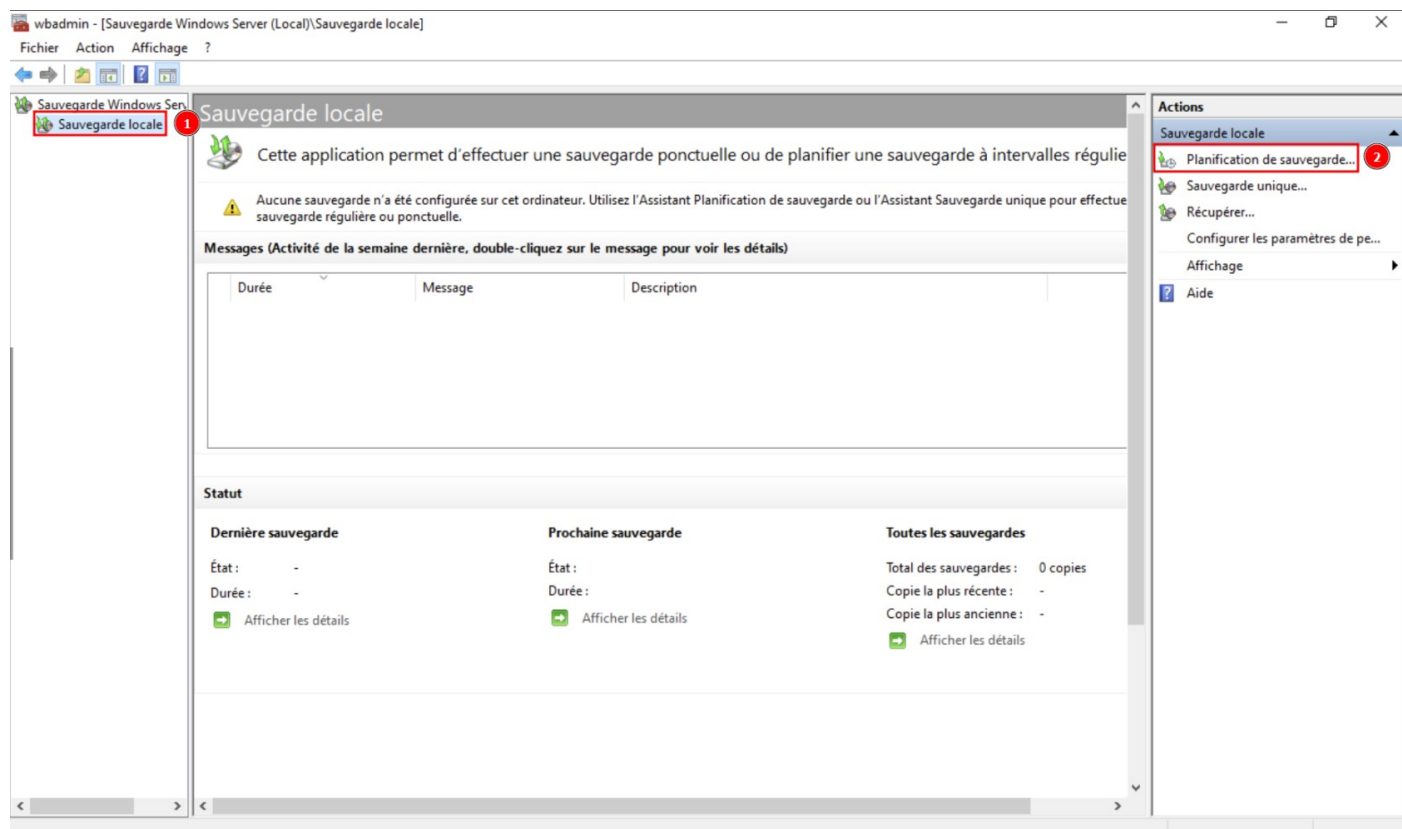
Encadré rouge : Une fois que la barre de progression indique que l'installation est réussie, vous cliquez sur le bouton « **Fermer** ».



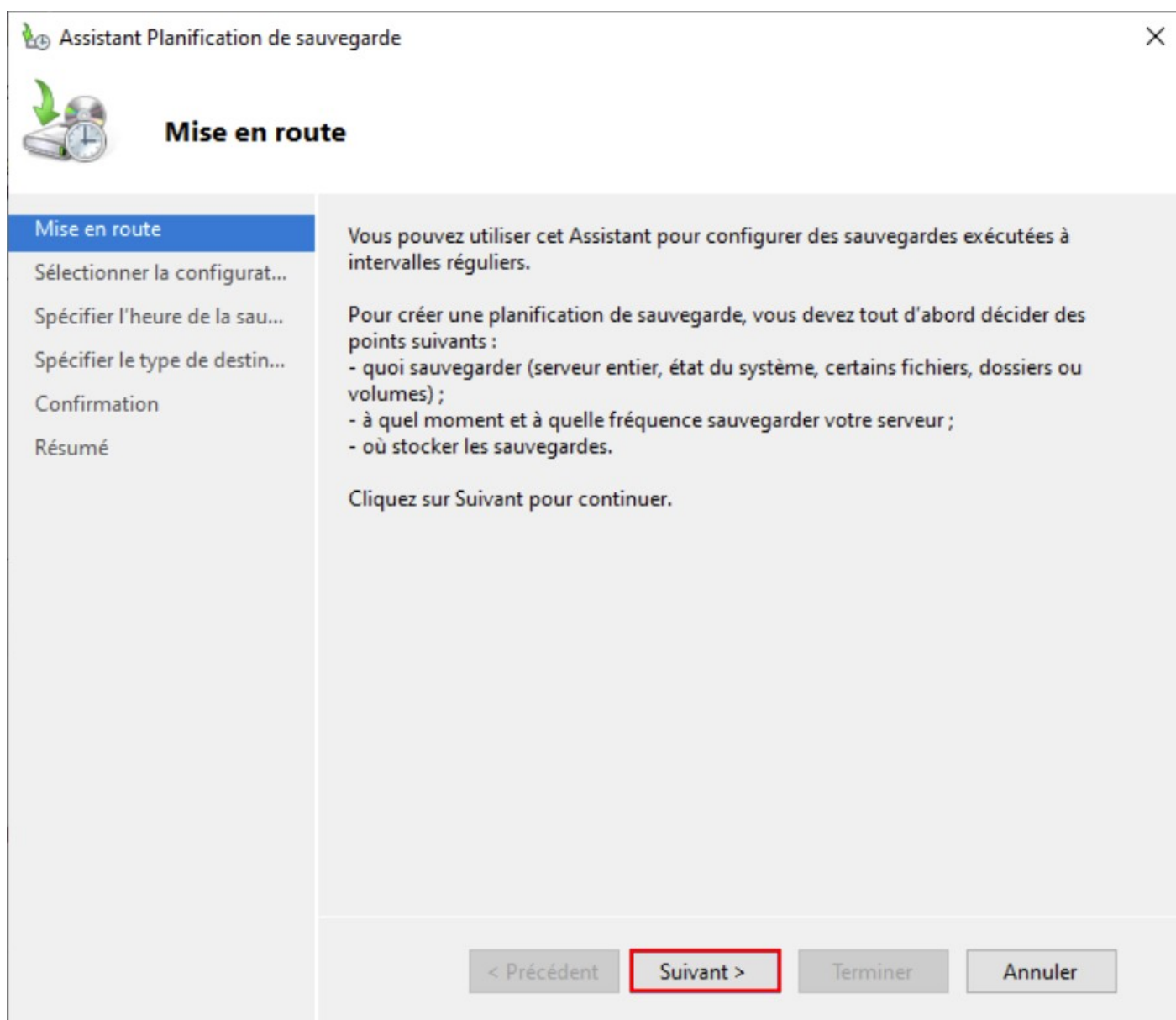
- **Encadré 1** : Dans le menu supérieur du Gestionnaire de serveur, vous cliquez sur l'onglet « **Outils** ».
- **Encadré 2** : Dans la liste déroulante, vous sélectionnez « **Sauvegarde Windows Server** ».



Encadré rouge : Dans le volet "Actions" à droite de la console, vous cliquez sur « **Planification de sauvegarde...** ».



Encadré rouge : Vous cliquez sur le bouton « **Suivant >** ».



Encadré rouge : Vous cliquez sur le bouton « **Suivant >** ».



Sélectionner la configuration de la sauvegarde

Mise en route

Sélectionner la configurat...

Spécifier l'heure de la sau...

Spécifier le type de destin...

Confirmation

Résumé

Quel type de configuration voulez-vous planifier ?

☒ Serveur complet (recommandé)

Je veux sauvegarder toutes les données et les applications présentes sur le serveur, ainsi que l'état du système.

Taille de la sauvegarde : 14,29 Go

☐ Personnalisé

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

< Précédent

Suivant >

Terminer

Annuler

- **Encadré 1** : Vous définissez la fréquence de la sauvegarde. Vous choisissez « **Tous les jours** » et réglez l'heure sur « **21:00** ».
- **Encadré 2** : Vous cliquez sur le bouton « **Suivant >** ».

Assistant Planification de sauvegarde

Spécifier l'heure de la sauvegarde

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

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

☒ Tous les jours
Sélectionnez une heure : 21:00

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

Temps disponible :

00:00	↑
00:30	
01:00	
01:30	
02:00	
02:30	
03:00	
03:30	
04:00	
04:30	↓

Ajouter >

< Supprimer

Heure planifiée : 21:00

2

< Précédent Suivant > Terminer Annuler

Encadré rouge : Vous cliquez sur le bouton « **Suivant** > ».

Assistant Planification de sauvegarde

Spécifier le type de destination

Mise en route

Sélectionner la configurat...

Spécifier l'heure de la sau...

Spécifier le type de destin...

Sélectionner le disque de ...

Confirmation

Résumé

Où voulez-vous stocker les sauvegardes ?

☒ Sauvegarder vers un disque dur dédié aux sauvegardes (recommandé)

Sélectionnez cette option pour stocker de la manière la plus sûre les sauvegardes. Le disque dur utilisé sera formaté, puis utilisé uniquement pour stocker les sauvegardes.

☐ Sauvegarder vers un volume

Sélectionnez cette option si vous ne pouvez pas dédier tout un disque à la sauvegarde. Notez que cette option peut réduire les performances du volume de 200 pour cent durant le stockage des sauvegardes. Il est recommandé de ne pas stocker d'autres données de serveur sur le même volume.

☐ Sauvegarder sur un dossier réseau partagé

Sélectionnez cette option uniquement si vous ne voulez pas stocker les sauvegardes sur le serveur lui-même. Notez que vous ne disposerez que d'une sauvegarde à la fois lorsque vous créez une nouvelle sauvegarde, car celle-ci remplace la précédente.


< Précédent


Suivant >

Terminer

Annuler

- **Encadré rouge** : Comme aucun disque n'apparaît dans la liste, vous cliquez sur le bouton « **Afficher tous les disques disponibles...** ».

 Assistant Planification de sauvegarde ✕

 **Sélectionner le disque de destination**

Mise en route

Sélectionner la configurat...

Spécifier l'heure de la sau...

Spécifier le type de destin...

Sélectionner le disque de ...

Confirmation


Résumé

Sélectionnez un ou plusieurs disques pour stocker vos sauvegardes. Vous pouvez utiliser plusieurs disques de sauvegarde si vous souhaitez stocker des disques hors site.

Disques disponibles :

Disque	Nom	Taille	Espace uti...	Volumes prés...
--------	-----	--------	---------------	-----------------

Afficher tous les disques disponibles...

 Aucun disque externe ou connecté à un port USB (Universal Serial Bus) ou IEEE 1394 n'a été trouvé.

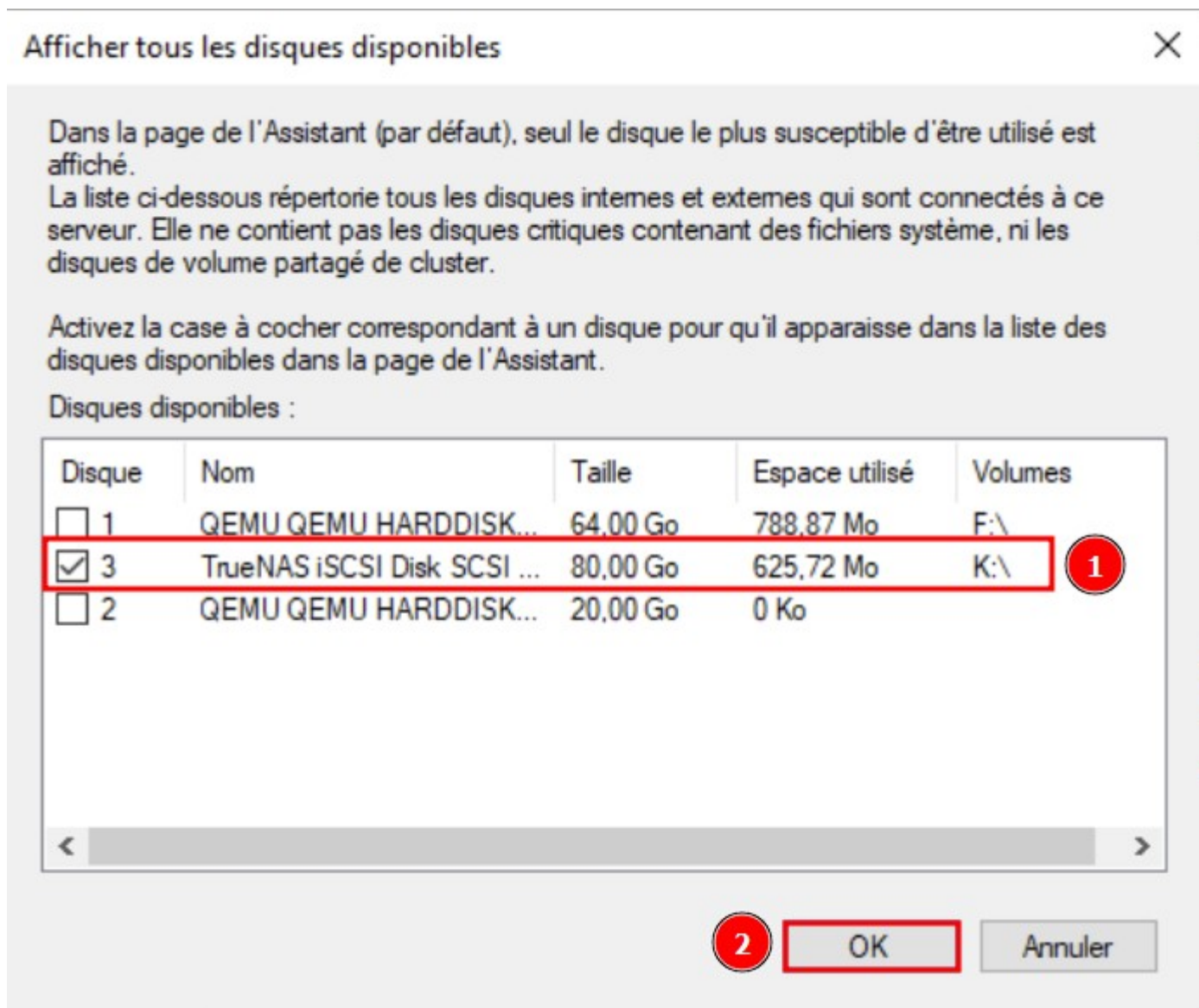
< Précédent

Suivant >

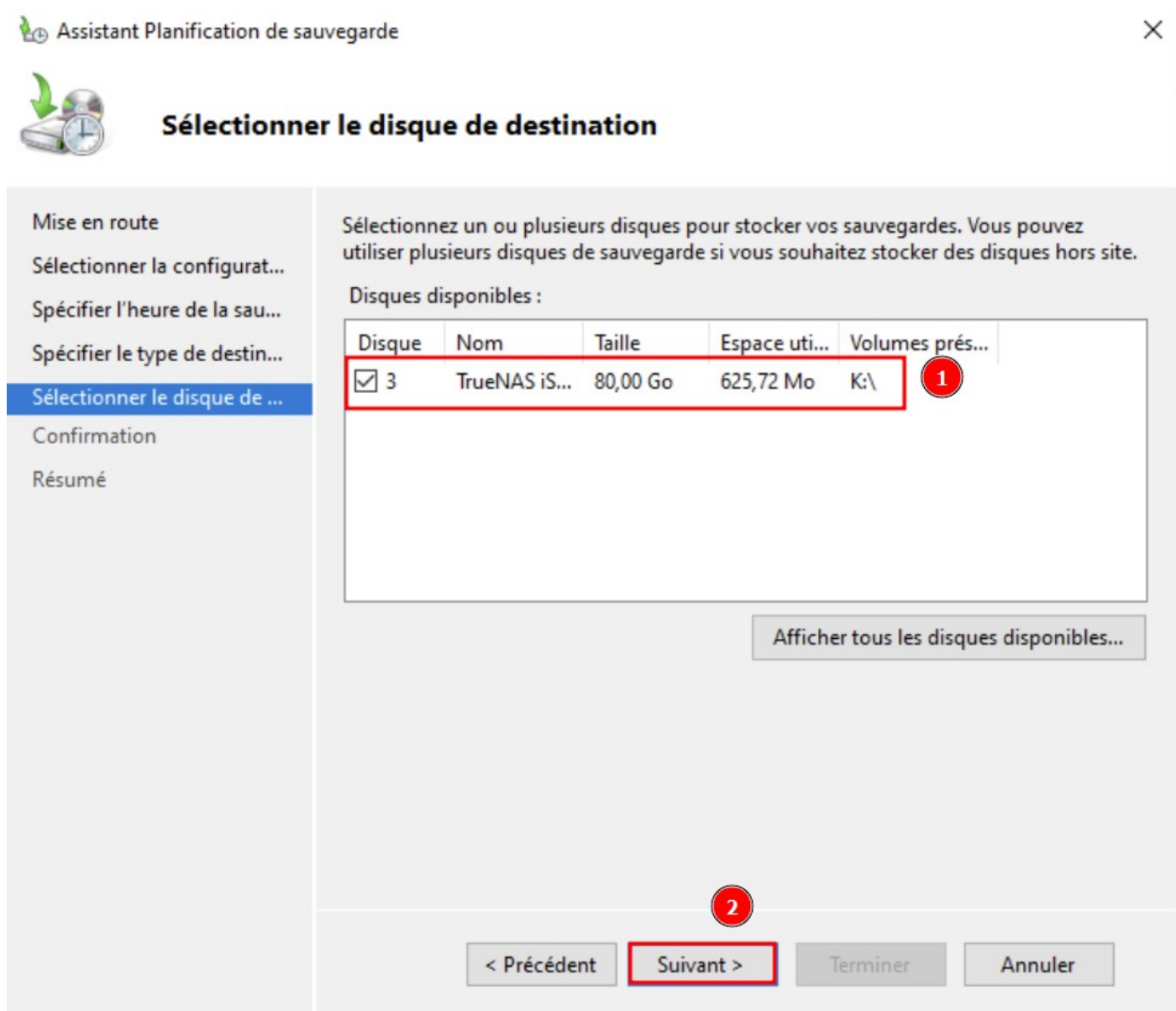
Terminer

Annuler

- **Encadré 1** : Dans la liste qui s'affiche, vous cochez la case du **Disque 2** (nommé "TrueNAS iSCSI Disk..."). C'est le disque distant de 80 Go que vous avez connecté via le réseau précédemment.
- **Encadré 2** : Vous cliquez sur « **OK** ».



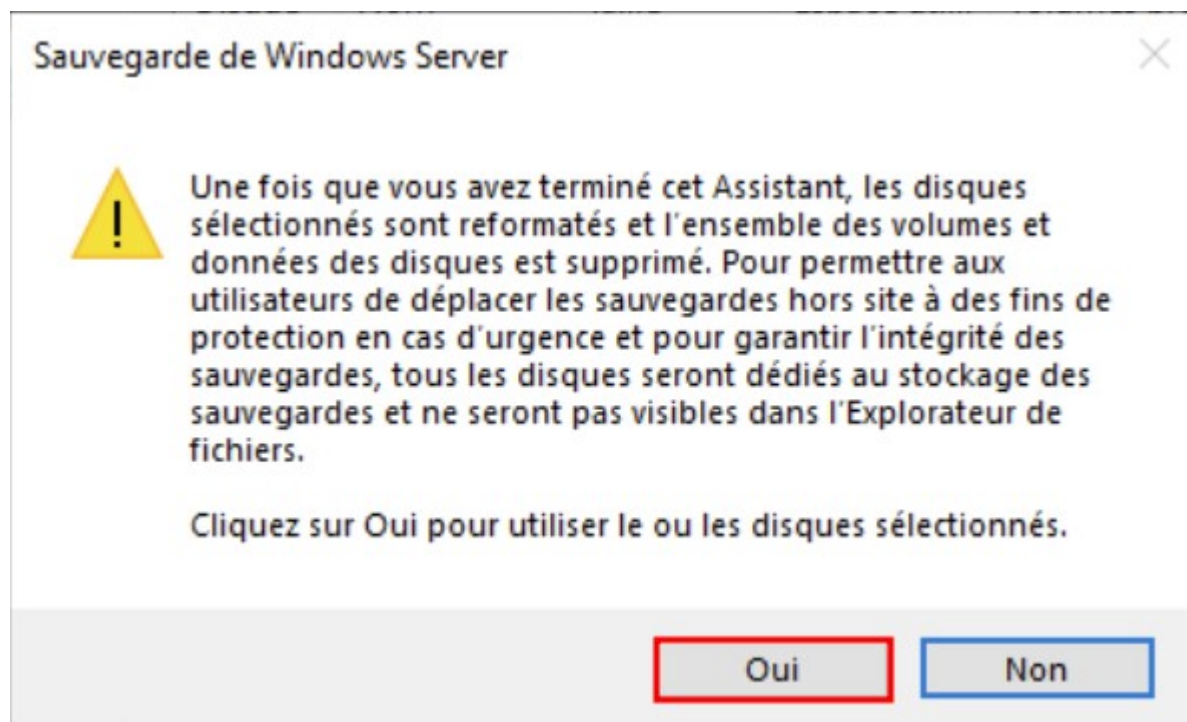
- **Encadré 1** : Le disque TrueNAS apparaît maintenant dans la liste principale. Vous cochez la case pour confirmer sa sélection.
- **Encadré 2** : Vous cliquez sur le bouton « **Suivant** > ».



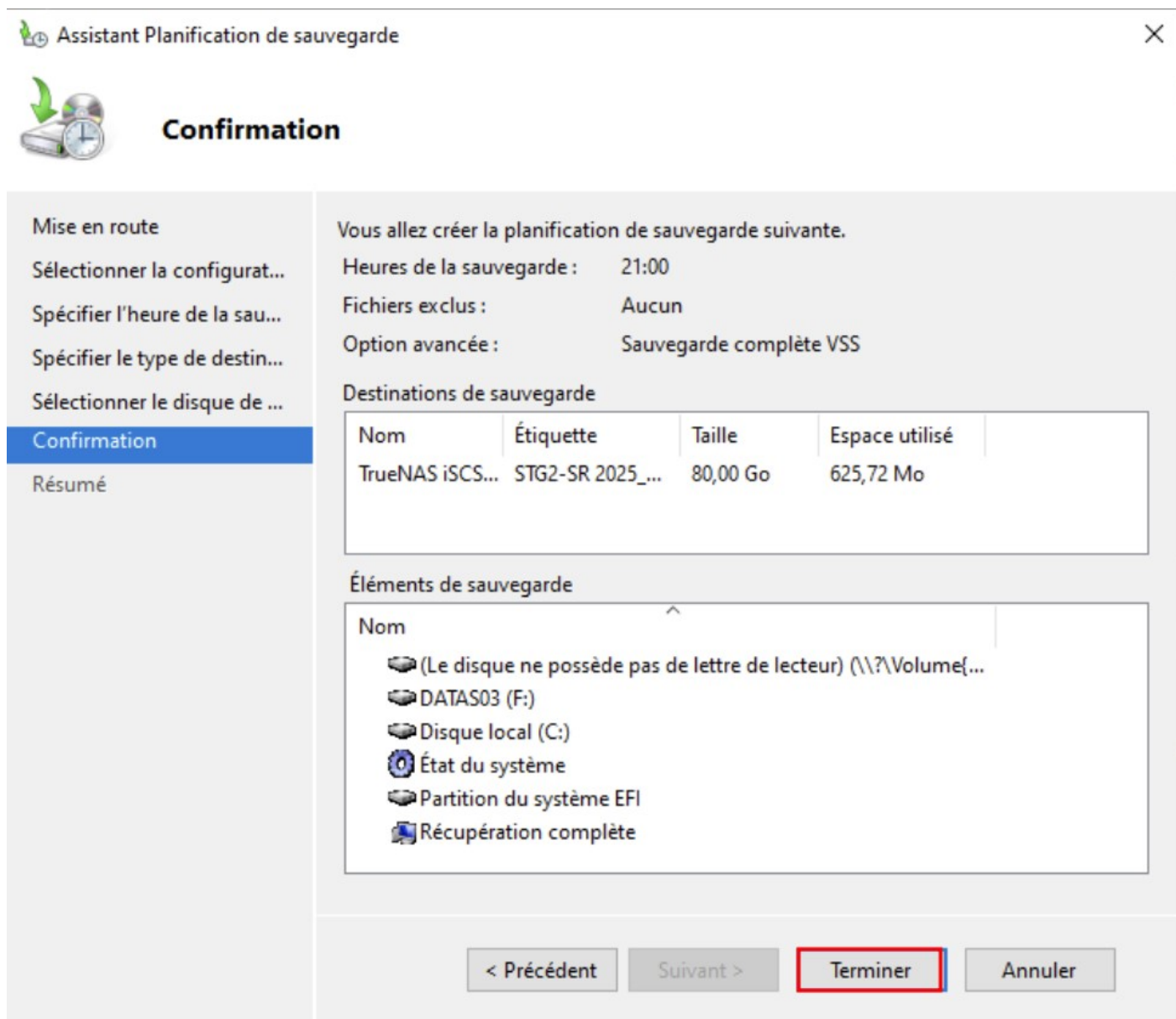
- **Encadré rouge** : Une fenêtre vous avertit que vous tentez de sauvegarder un volume (le SAN K:) qui se trouve sur le même disque physique que la destination. Vous cliquez sur « **OK** » pour accepter que ce volume soit exclu de la sauvegarde (on ne peut pas sauvegarder un disque sur lui-même).



Encadré rouge : Un dernier message d'avertissement crucial vous informe que **le disque sélectionné va être formaté** et que toutes les données présentes dessus seront supprimées. Vous cliquez sur « **Oui** » pour confirmer.




Encadré rouge : Vous cliquez sur le bouton « **Terminer** ».



Encadré rouge : Vous cliquez sur le bouton « **Terminer** ».

Assistant Planification de sauvegarde



Résumé

Mise en route	Statut : La planification de sauvegarde a bien été créée.
Sélectionner la configurat...	Votre première sauvegarde planifiée aura lieu à 15/11/2025 21:00.
Spécifier l'heure de la sau...	Vérifiez que les disques utilisés pour stocker les sauvegardes planifiées sont connectés à cet ordinateur et accessibles.
Spécifier le type de destin...	
Sélectionner le disque de ...	
Confirmation	
Résumé	

< Précédent Suivant > **Fermer** Annuler

On voit ici le tableau de bord principal de la **Sauvegarde Windows Server** mis à jour.

- Dans la partie basse (**Sauvegarde planifiée**), tous les détails apparaissent : la fréquence quotidienne, l'heure de début, et la destination sur le disque distant.
- Le serveur est désormais protégé de manière autonome.

wbadmin - [Sauvegarde Windows Server (Local)\Sauvegarde locale]

Fichier Action Affichage ?

Sauvegarde Windows Serv
Sauvegarde locale

Statut

Dernière sauvegarde	Prochaine sauvegarde	Toutes les sauvegardes
État : -	État : Planifiée	Total des sauvegardes : 0 copies
Durée : -	Durée : 15/11/2025 21:00	Copie la plus récente : -
Afficher les détails	Afficher les détails	Copie la plus ancienne : -
		Afficher les détails

Sauvegarde planifiée

Une sauvegarde planifiée à intervalles réguliers est configurée pour ce serveur.

Paramètres		Utilisation de la destination
Éléments de sauvegarde :	Récupération complète; État du système; Partition d...	Nom : STG2-SR 2025_11_15 16:26 DISK_01
Fichier exclus :	Aucun	Capacité : 79,86 Go
Option avancée :	Sauvegarde complète VSS	Espace utilisé : 0 Go
Destination :	STG2-SR 2025_11_15 16:26 DISK_01	Sauvegardes disponibles : 0 copies
Heure de la sauvegarde :	Tous les jours 21:00	Afficher les détails
		Actualiser les informations

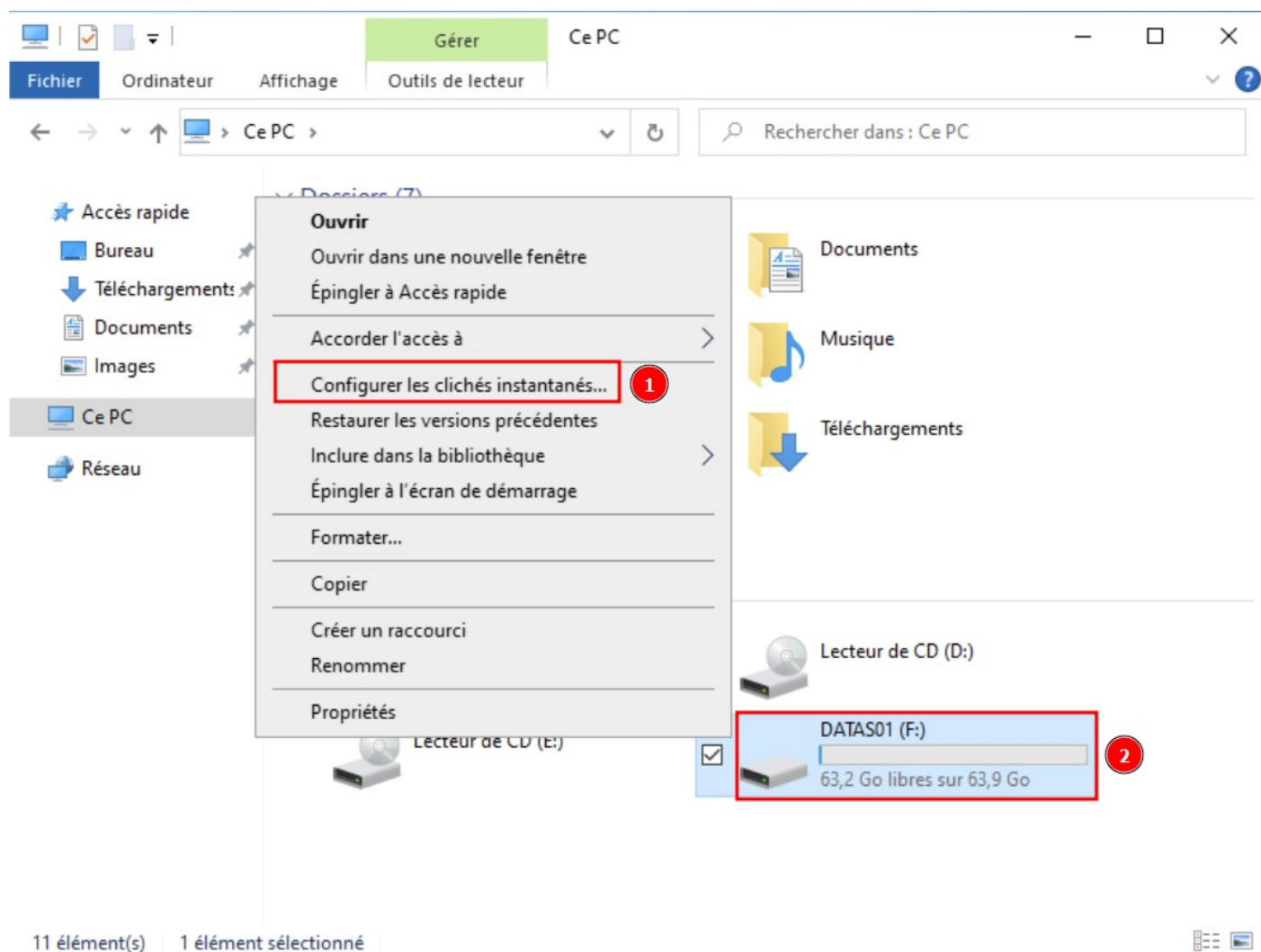
Actions

- Sauvegarde locale ▲
- Planification ...
- Sauvegarde u...
- Récupérer...
- Configurer le...
- Affichage ▶
- Aide

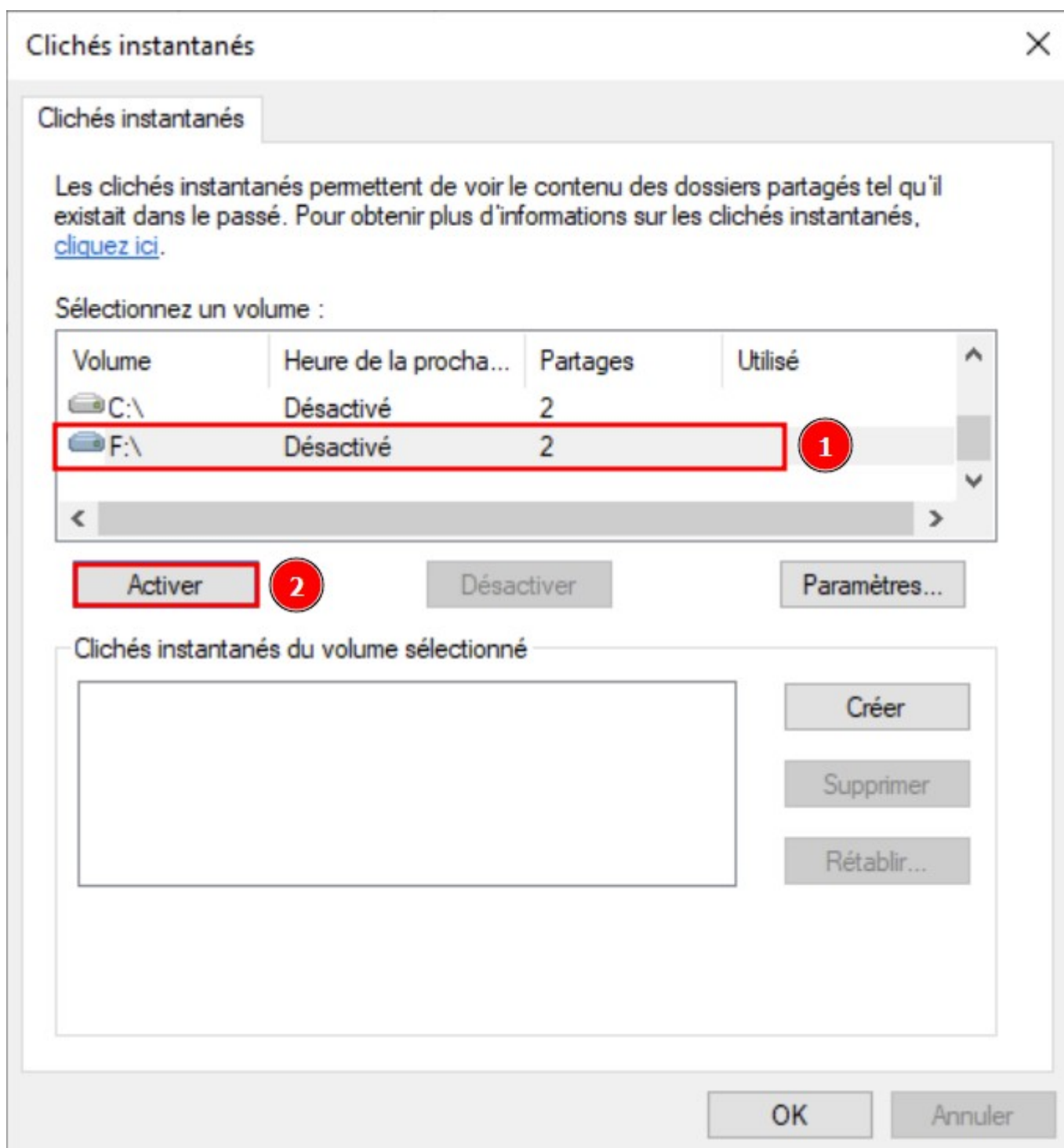
BACKUP

Configuration de Shadow Copy

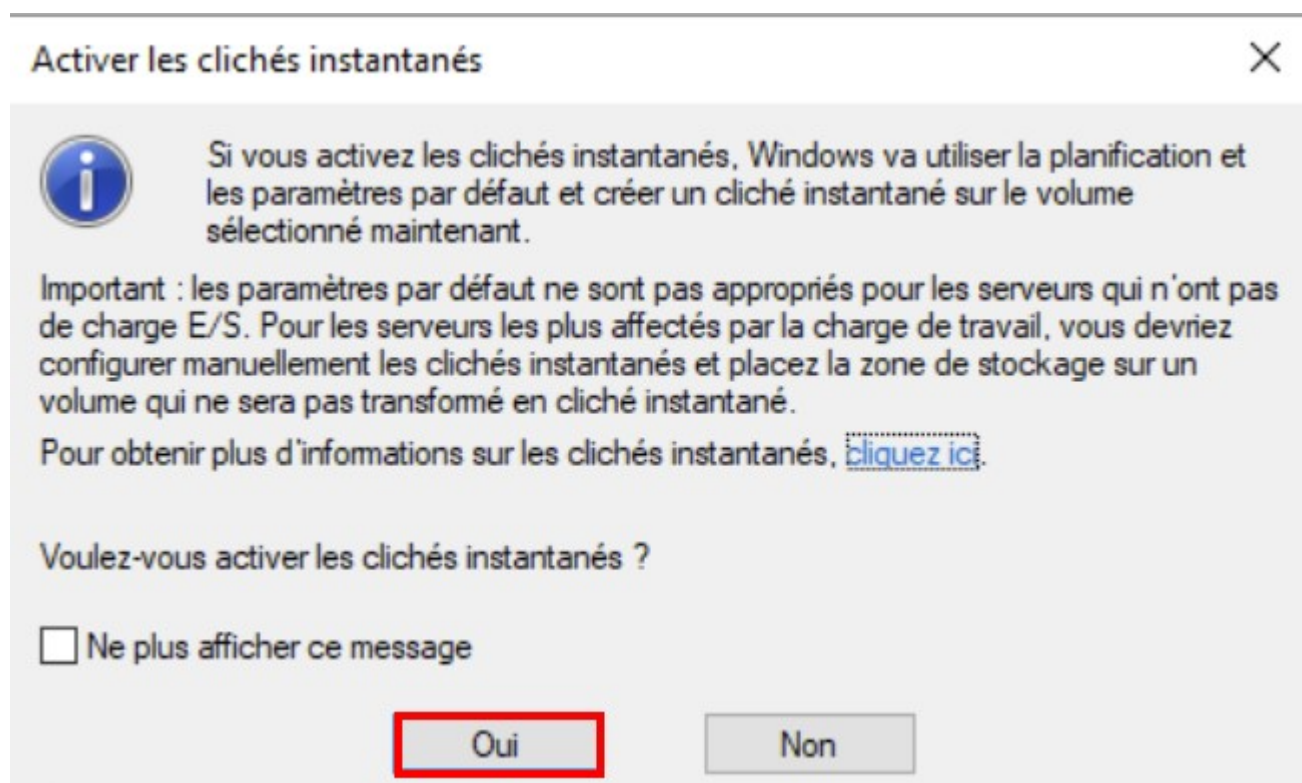
- **Encadré 2** : Dans l'Explorateur de fichiers (« Ce PC »), vous ciblez le lecteur de données **DATAS01 (F:)**.
- **Encadré 1** : Vous faites un clic droit sur ce lecteur et sélectionnez l'option « **Configurer les clichés instantanés...** ».



- **Encadré 1** : Dans la fenêtre qui s'ouvre, vous sélectionnez le volume *F:* dans la liste des lecteurs disponibles.
- **Encadré 2** : Vous cliquez sur le bouton « **Activer** ».



Encadré rouge : Une fenêtre d'avertissement s'affiche pour confirmer l'activation. Vous cliquez sur le bouton « **Oui** ».

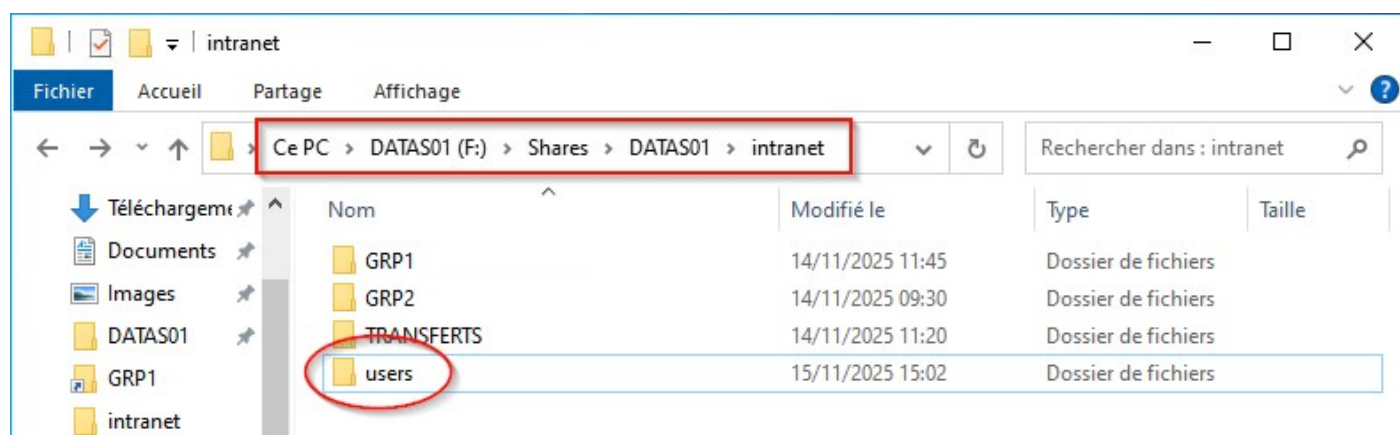


GPO et parametres pour clients

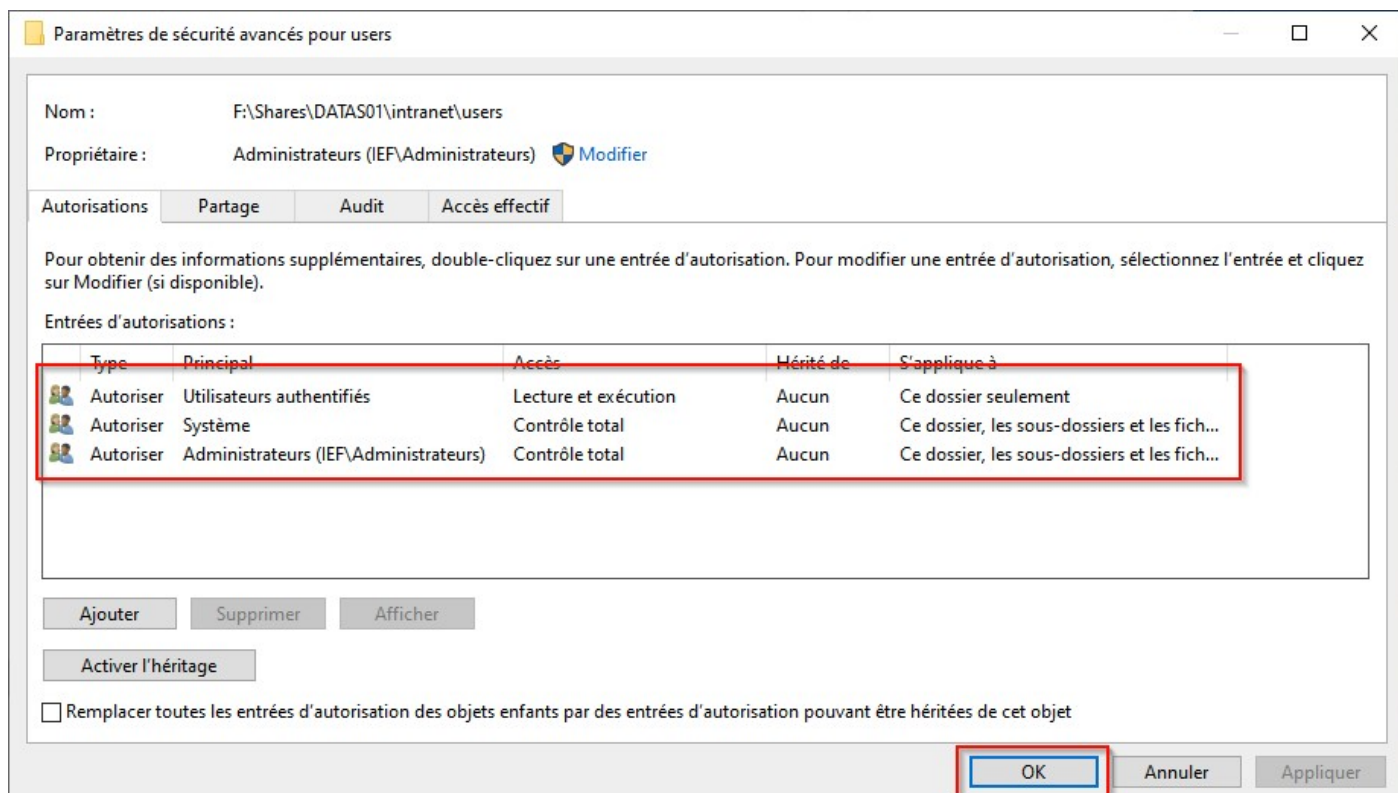
GPO et paramètres pour clients

Mise en place des disques réseau utilisateurs

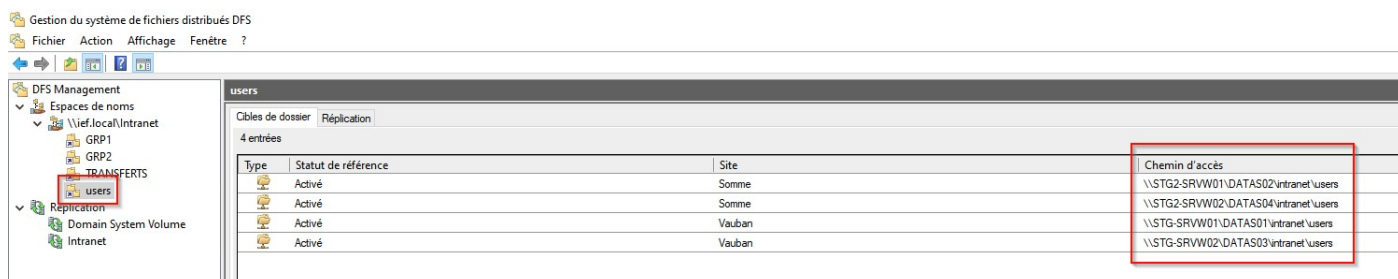
- **Encadré 1 (Chemin)** : On se rend dans le dossier racine du DFS sur le disque physique : F:\Shares\DATAS01\intranet.
- **Cercle 2 (Dossier)** : On crée un nouveau dossier nommé « **users** ». C'est ici que seront regroupés tous les dossiers personnels individuels de chaque employé.



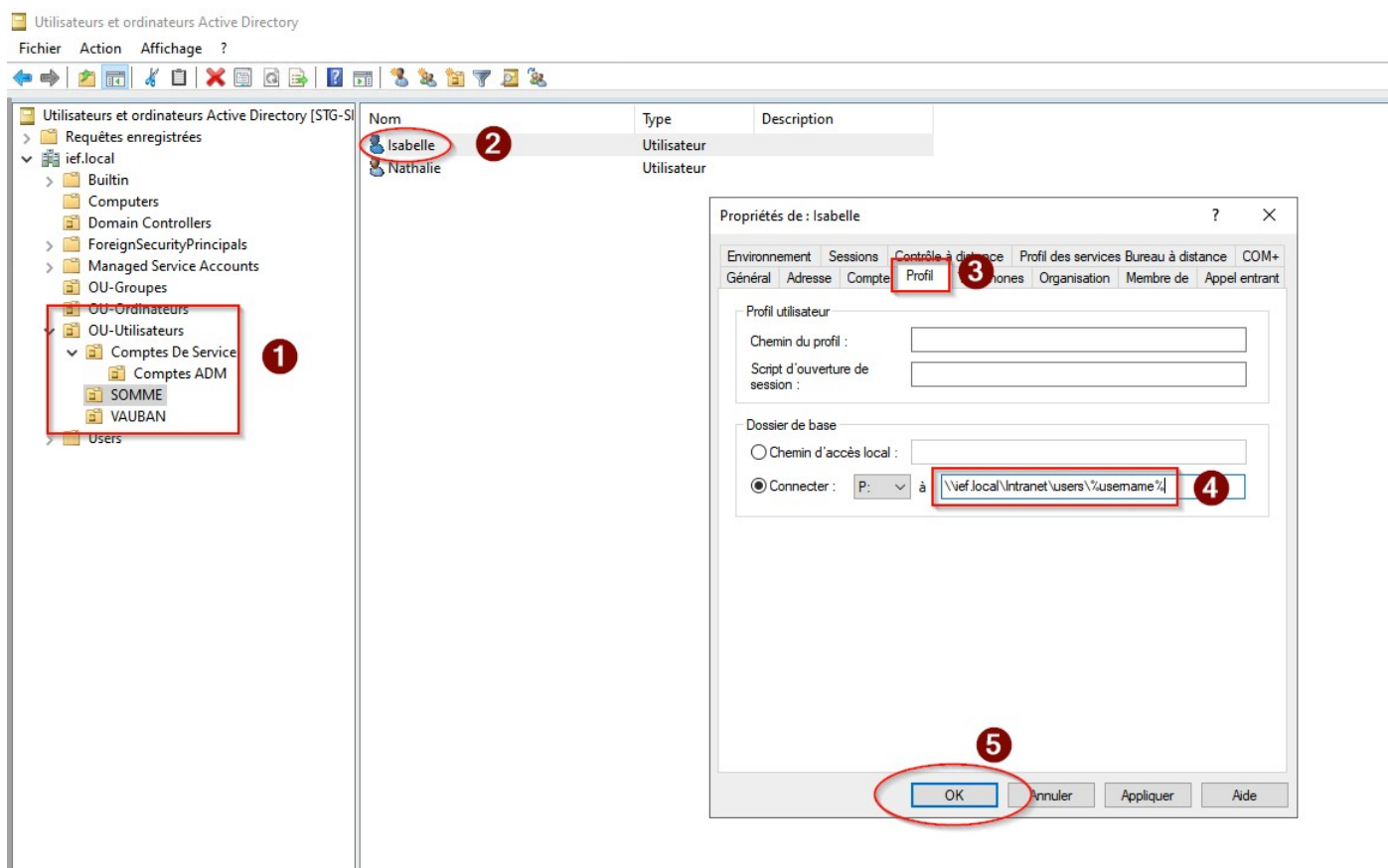
- **Encadré 1 (Autorisations)** : On définit des droits d'accès spécifiques sur le dossier "users" :
 - Les **Utilisateurs authentifiés** n'ont que des droits de « Lecture et exécution » sur « Ce dossier seulement ». Cela leur permet de traverser ce dossier pour atteindre le leur, sans voir le contenu des dossiers des collègues.
 - Le **Système** et les **Administrateurs** conservent le « Contrôle total ».
- **Encadré 2** : On clique sur « **OK** » pour valider ces paramètres de sécurité restreints.



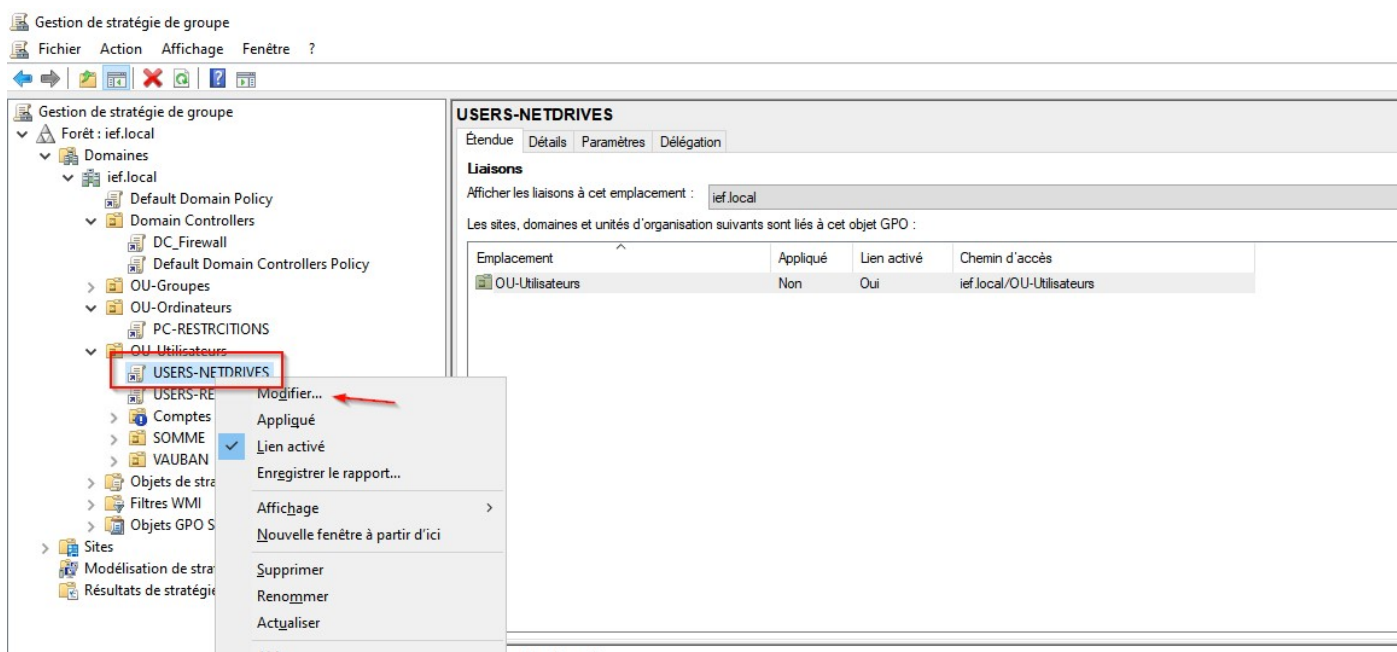
- **Encadré rouge** : Dans la console de gestion DFS, on ajoute des « Cibles de dossier » pour le dossier virtuel "users".
 - **Action** : On lie ce nom unique à quatre emplacements physiques différents répartis sur quatre serveurs (SRVW01 et SRVW02 des deux sites). Cela garantit que les dossiers personnels restent accessibles même si plusieurs serveurs tombent en panne.



- **Encadré 1** : On se trouve dans l'unité d'organisation (OU-Utilisateurs) contenant les comptes des employés.
- **Cercle 2 & Encadré 3** : On ouvre les propriétés de l'utilisateur (ici SOMME) et on va sur l'onglet « Profil ».
- **Encadré 4 (Dossier de base)** : On configure le montage automatique d'un lecteur réseau personnel :
 - On coche « Connecter », on choisit la lettre **U**: et on saisit le chemin réseau : \ief.local\intranet\users\%username%.
 - **Astuce** : La variable %username% sera automatiquement remplacée par le nom de session de l'utilisateur (créant ainsi dynamiquement le dossier users\SOMME).
- **Cercle 5** : On clique sur « OK » pour appliquer.

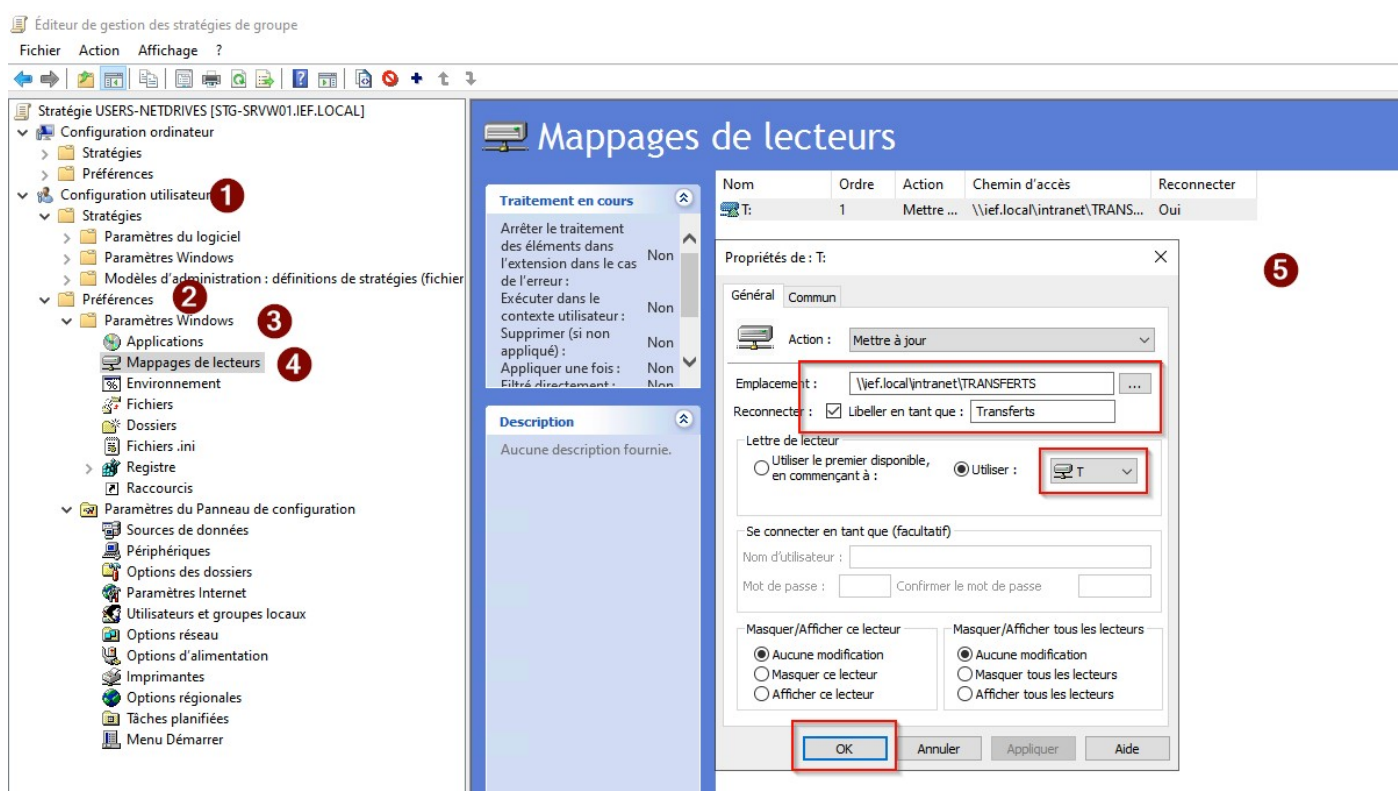


- **Encadré 1** : On a créé une stratégie de groupe (GPO) nommée « **USERS-NETDRIVES** ».
- **Encadré 2** : On fait un clic droit et on sélectionne « **Modifier...** ».



- **1 - Configuration utilisateur** : La règle s'appliquera à la session de l'utilisateur, peu importe l'ordinateur qu'il utilise.
- **2 - Préférences** : On utilise les préférences car elles sont plus souples que les stratégies classiques.
- **3 - Paramètres Windows** : Section regroupant les réglages de base du système.
- **4 - Mappages de lecteurs** : C'est ici que l'on définit les disques réseaux qui doivent "monter" automatiquement.

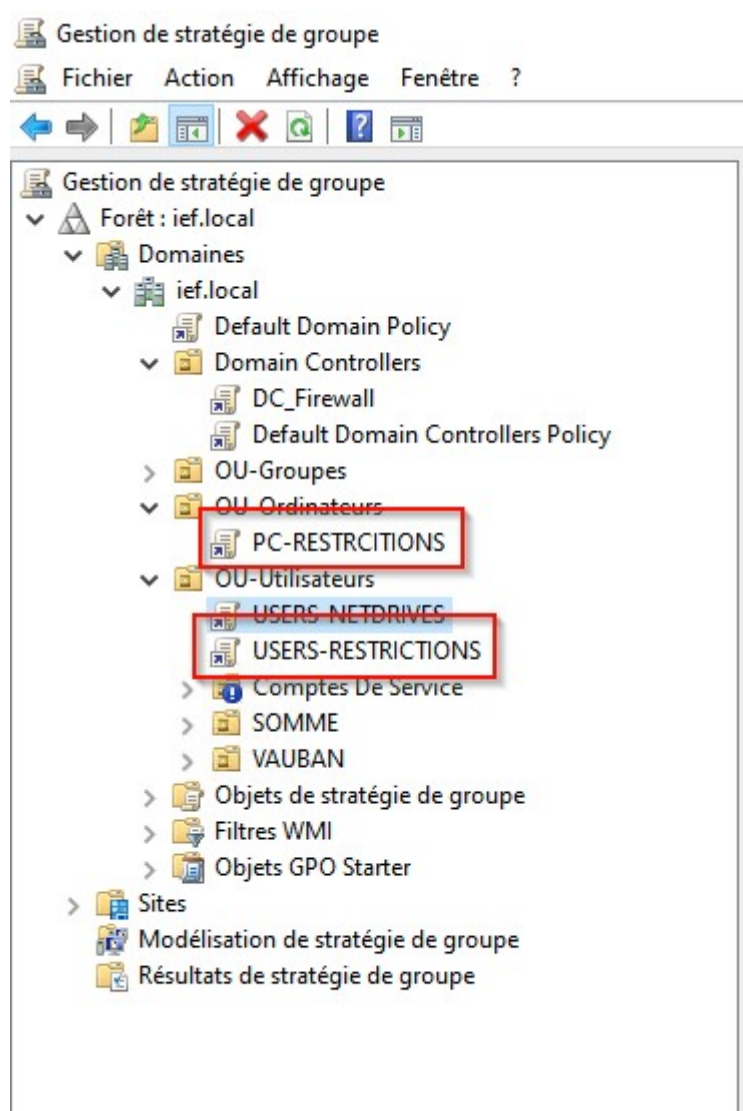
- Définie sur « **Mettre à jour** » (Update). Cela permet de créer le lecteur s'il n'existe pas ou de le mettre à jour s'il a été modifié.
- **Encadré rouge du haut (Emplacement et Libellé) :**
 - **Emplacement :** Vous saisissez le chemin DFS unique : **\\ief.local\intranet\TRANSFERTS**. Grâce au DFS, l'utilisateur aura accès à ses fichiers même si un serveur tombe en panne.
 - **Libeller en tant que :** Vous donnez le nom « **Transferts** » au lecteur pour qu'il soit facilement identifiable dans l'Explorateur de fichiers.
 - **Reconnecter :** La case est cochée pour que le lecteur revienne automatiquement à chaque nouvelle session.
- **Encadré rouge du milieu (Lettre de lecteur) :**
 - Vous imposez l'utilisation de la lettre **T** pour ce partage (T comme Transferts). Cela permet d'avoir une arborescence uniforme pour tous les employés de l'entreprise.
- **Encadré rouge du bas (OK) :**
 - Vous cliquez sur « **OK** » pour enregistrer cette règle de mappage.



GPO et paramètres pour clients

Création des GPO de restrictions

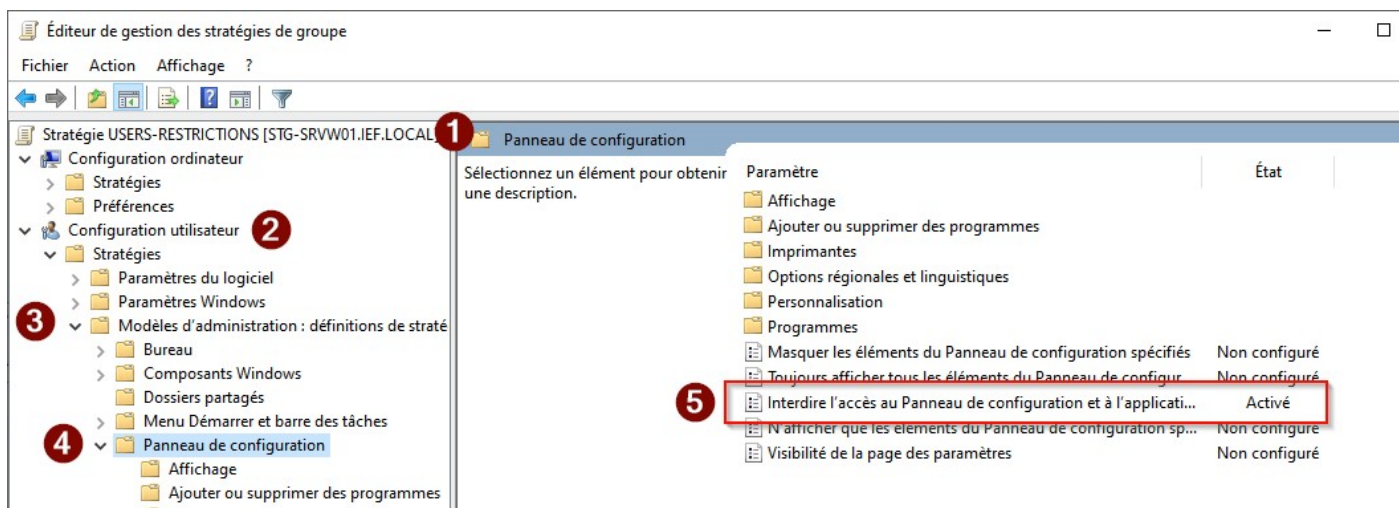
- **Encadrés rouges** : Vous avez créé deux objets de stratégie de groupe distincts et les avez liés à leurs unités d'organisation (OU) respectives :
 - **PC-RESTRICTIONS** : Liée à l'OU des ordinateurs pour appliquer des réglages sur les machines.
 - **USERS-RESTRICTIONS** : Liée à l'OU des utilisateurs pour restreindre les droits des employés sur leurs sessions.



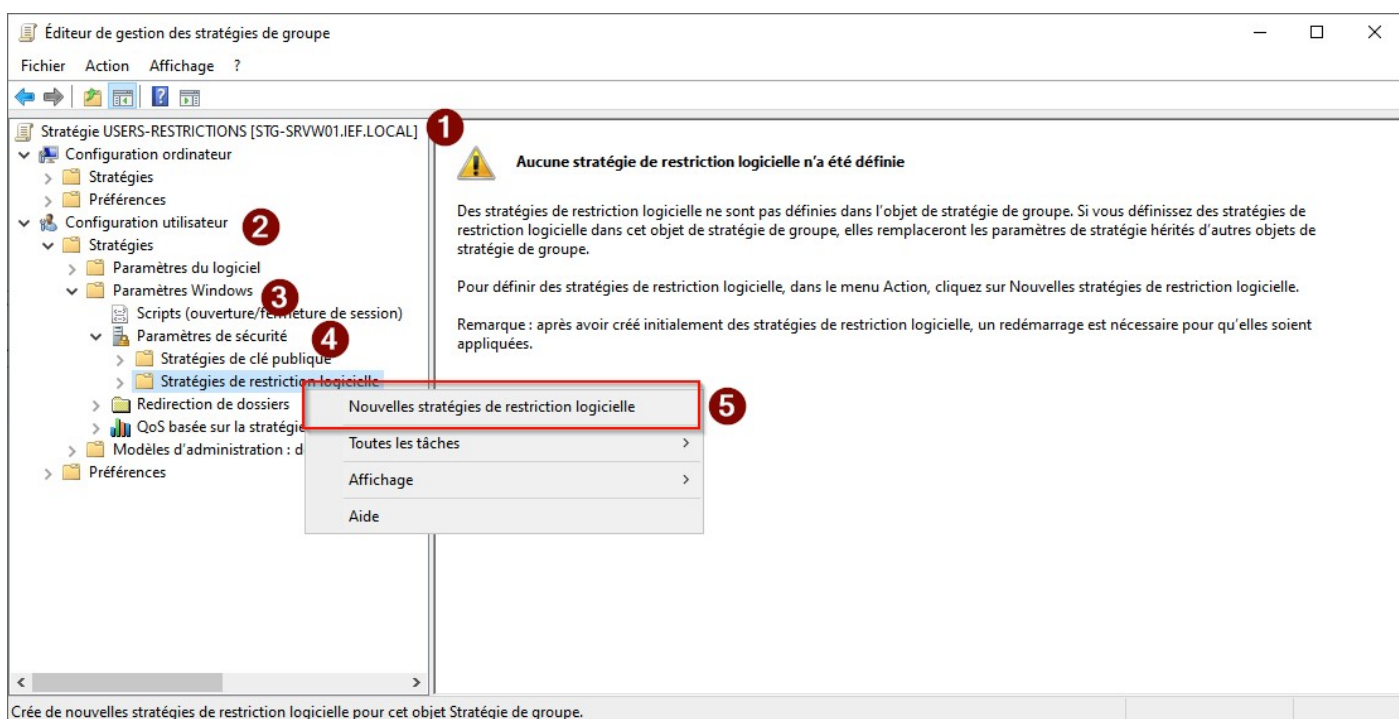
Vous vous rendez dans Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration.

Vous avez activé (**Activé**) le paramètre « **Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC** ».

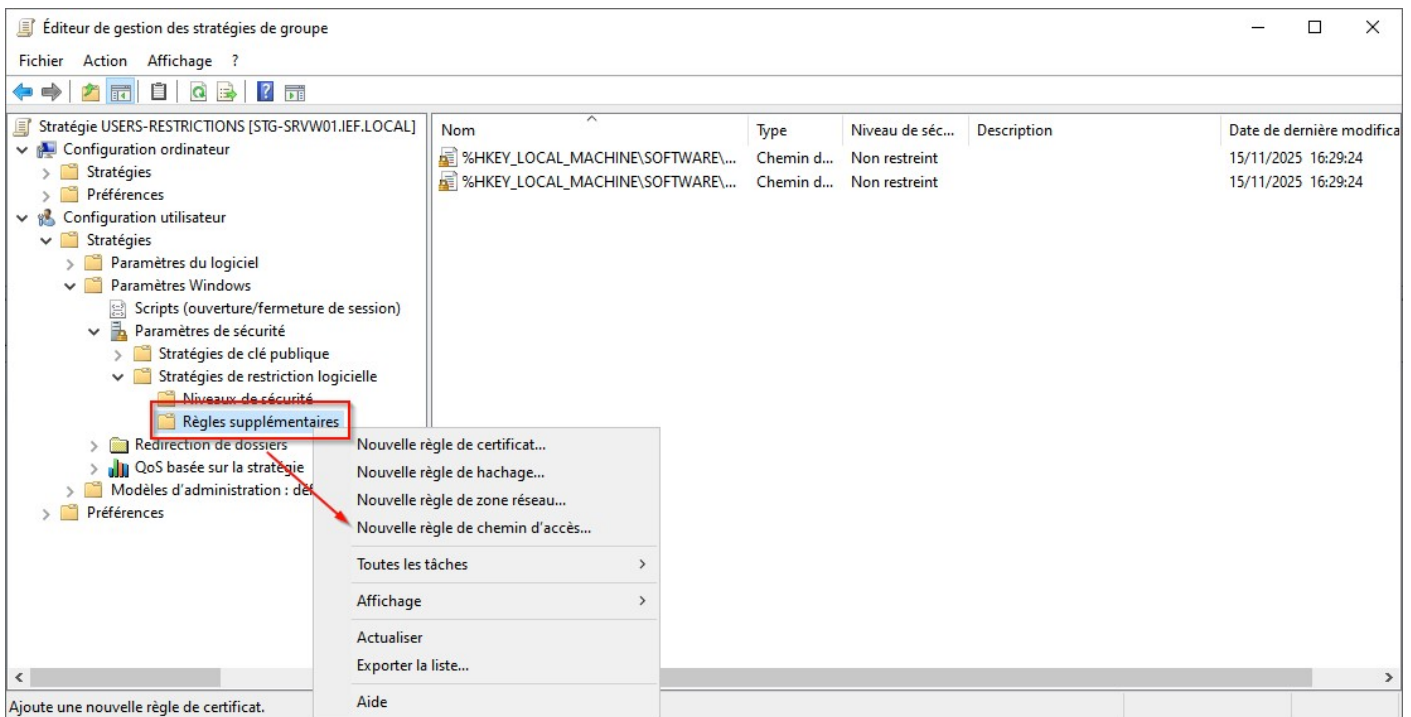
- **Objectif** : Empêcher les utilisateurs de modifier les réglages du système, garantissant ainsi la stabilité des postes de travail.



Dans Paramètres de sécurité, vous faites un clic droit sur « **Stratégies de restriction logicielle** » et sélectionnez « **Nouvelle stratégie...** » pour activer le service.

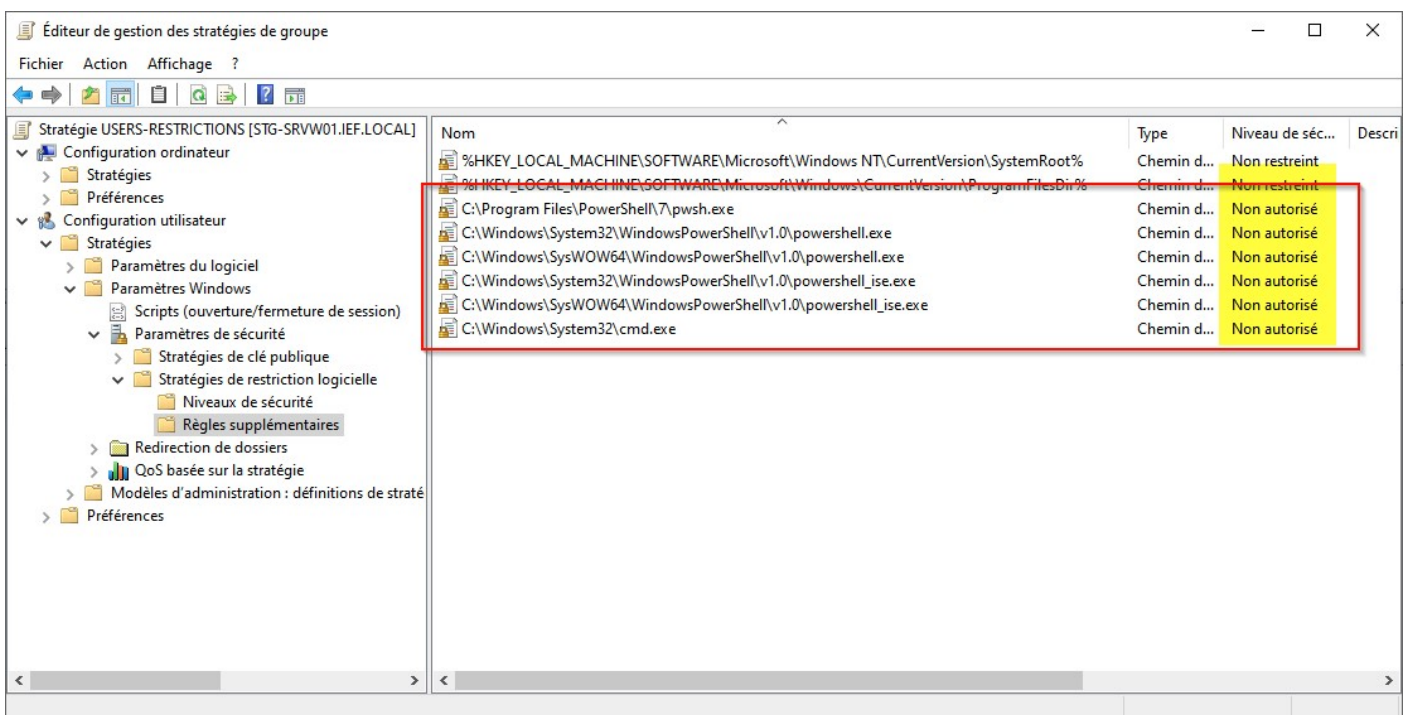


Vous faites un clic droit sur « Règles supplémentaires » pour créer une « **Nouvelle règle de chemin d'accès...** ».



Vous avez créé une liste de règles pour interdire l'exécution de programmes pouvant être utilisés pour contourner la sécurité. On voit dans l'encadré que les fichiers suivants sont marqués comme « **Non autorisé** » :

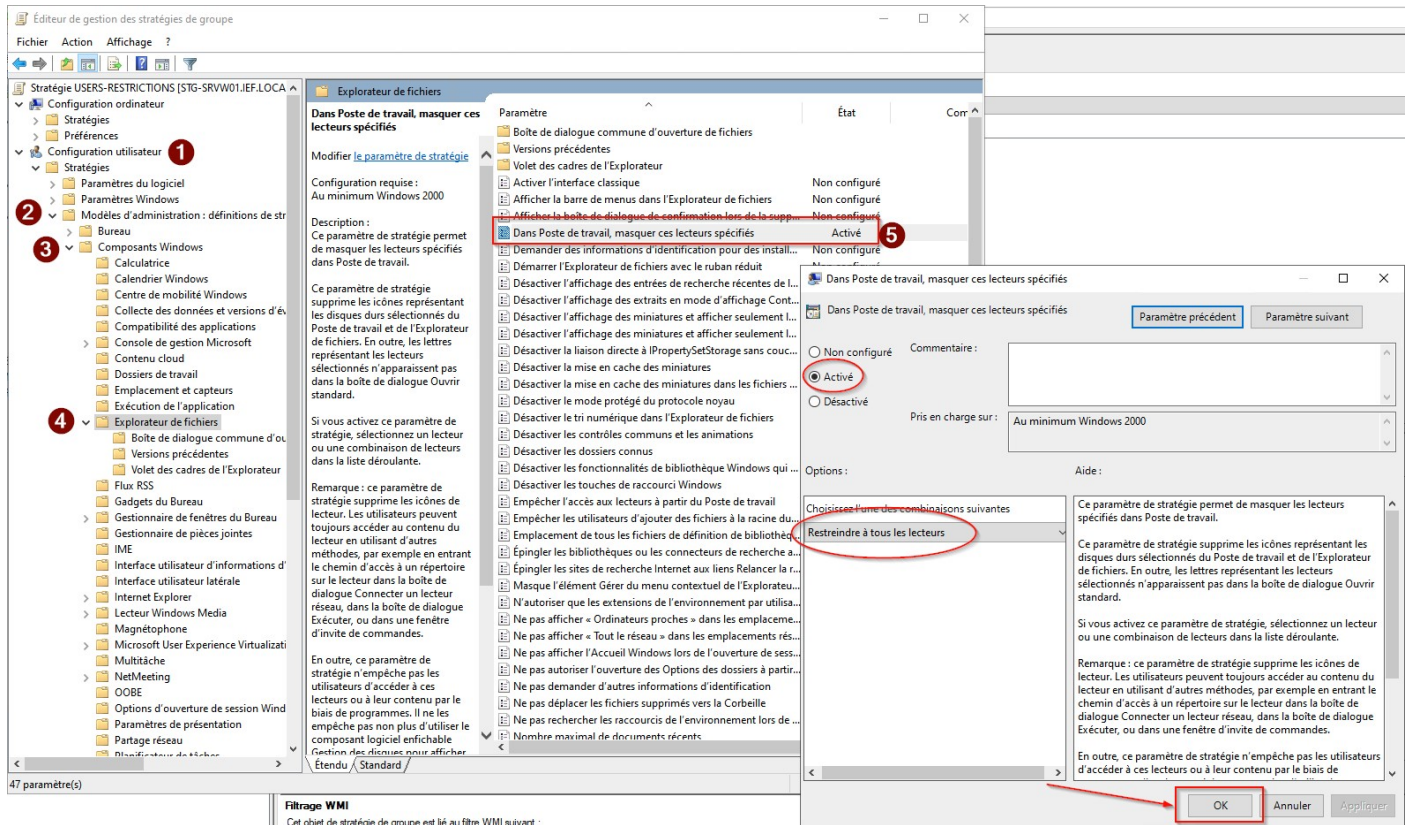
```
C:\Program Files\PowerShell\7\pwsh.exe  
C:\windows\system32\windowsPowerShell\v1.0\powershell.exe  
C:\windows\SysWOW64\windowsPowerShell\v1.0\powershell.exe  
C:\windows\system32\windowsPowerShell\v1.0\powershell_ise.exe  
C:\windows\SysWOW64\windowsPowerShell\v1.0\powershell_ise.exe  
C:\windows\system32\cmd.exe
```



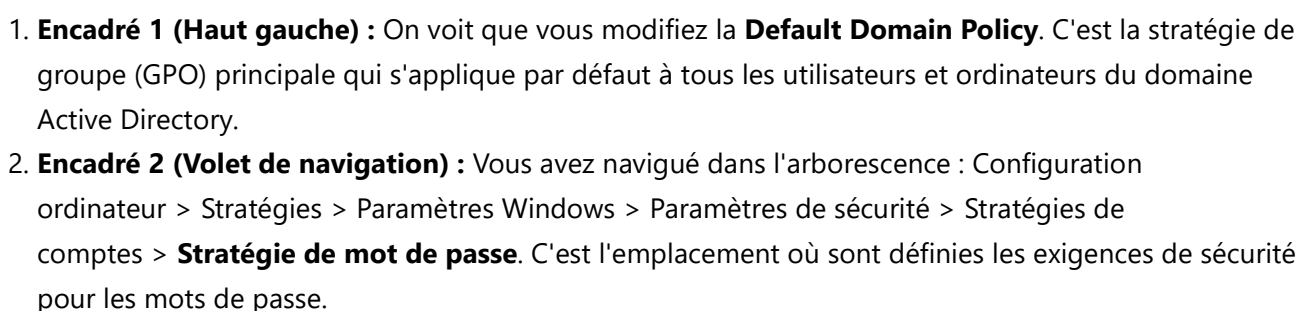
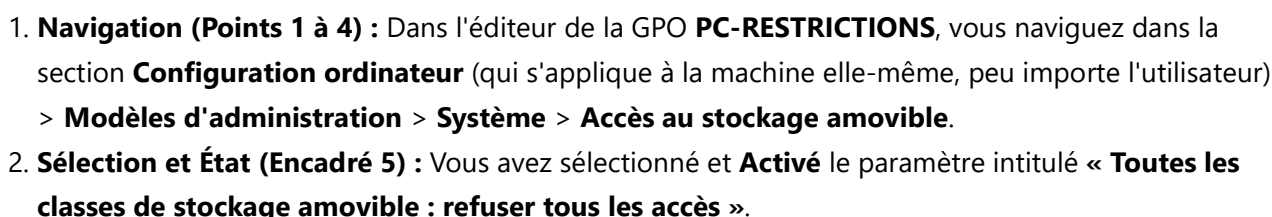
1. **Navigation (Points 1 à 4) :** Dans l'éditeur de la GPO USERS-RESTRICTIONS, vous avez navigué dans le menu suivant : Configuration utilisateur > Stratégies > Modèles d'administration > Composants

Windows > Explorateur de fichiers.

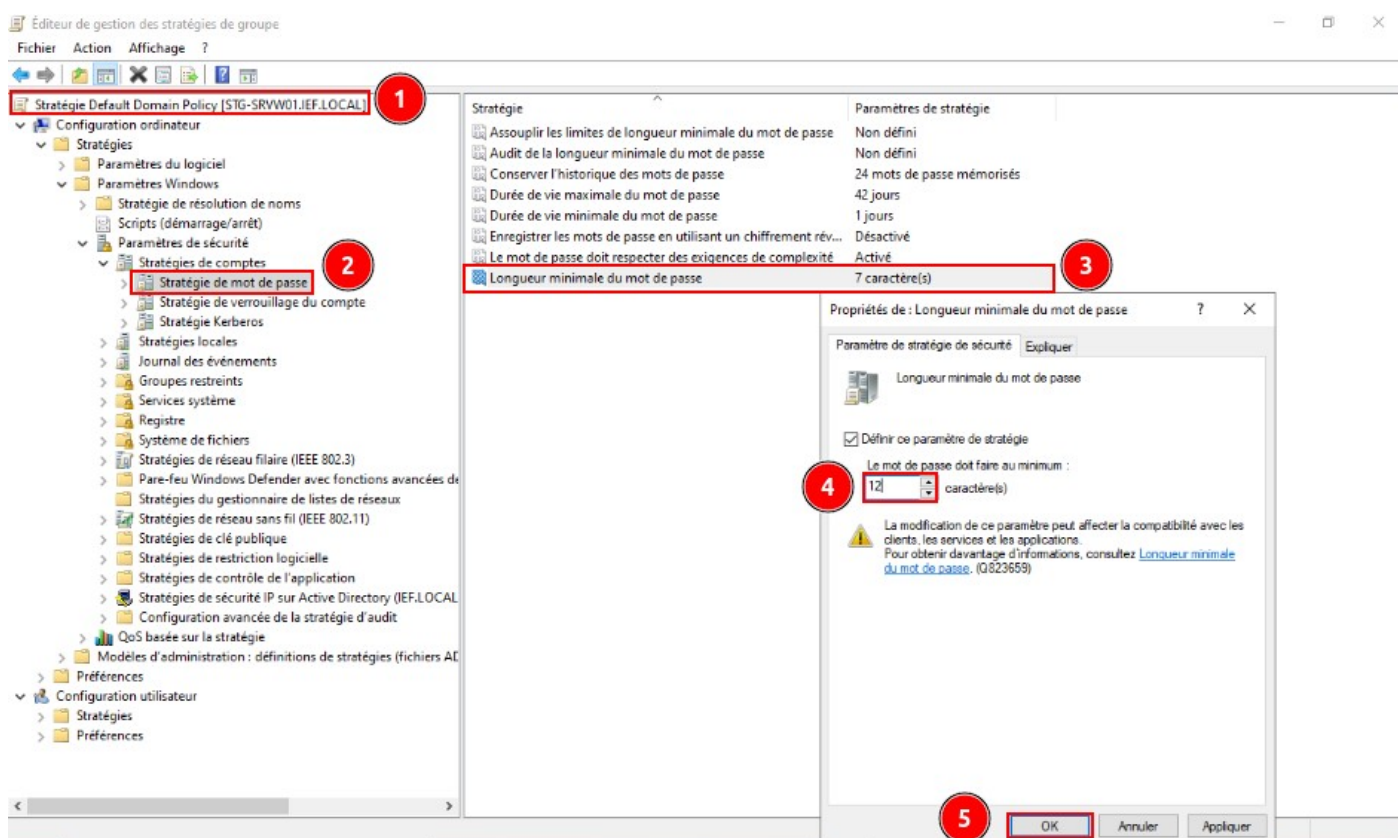
- Sélection du paramètre (Encadré 5) :** Vous avez sélectionné la stratégie nommée « **Dans Poste de travail, masquer ces lecteurs spécifiés** ».
- Configuration de la restriction (Fenêtre au premier plan) :**
 - Vous avez coché l'option « **Activé** ».
 - Dans le menu déroulant des options, vous avez choisi « **Restreindre à tous les lecteurs** ».
- Validation (Encadré en bas à droite) :** Vous cliquez sur le bouton « **OK** » pour enregistrer et appliquer cette restriction.



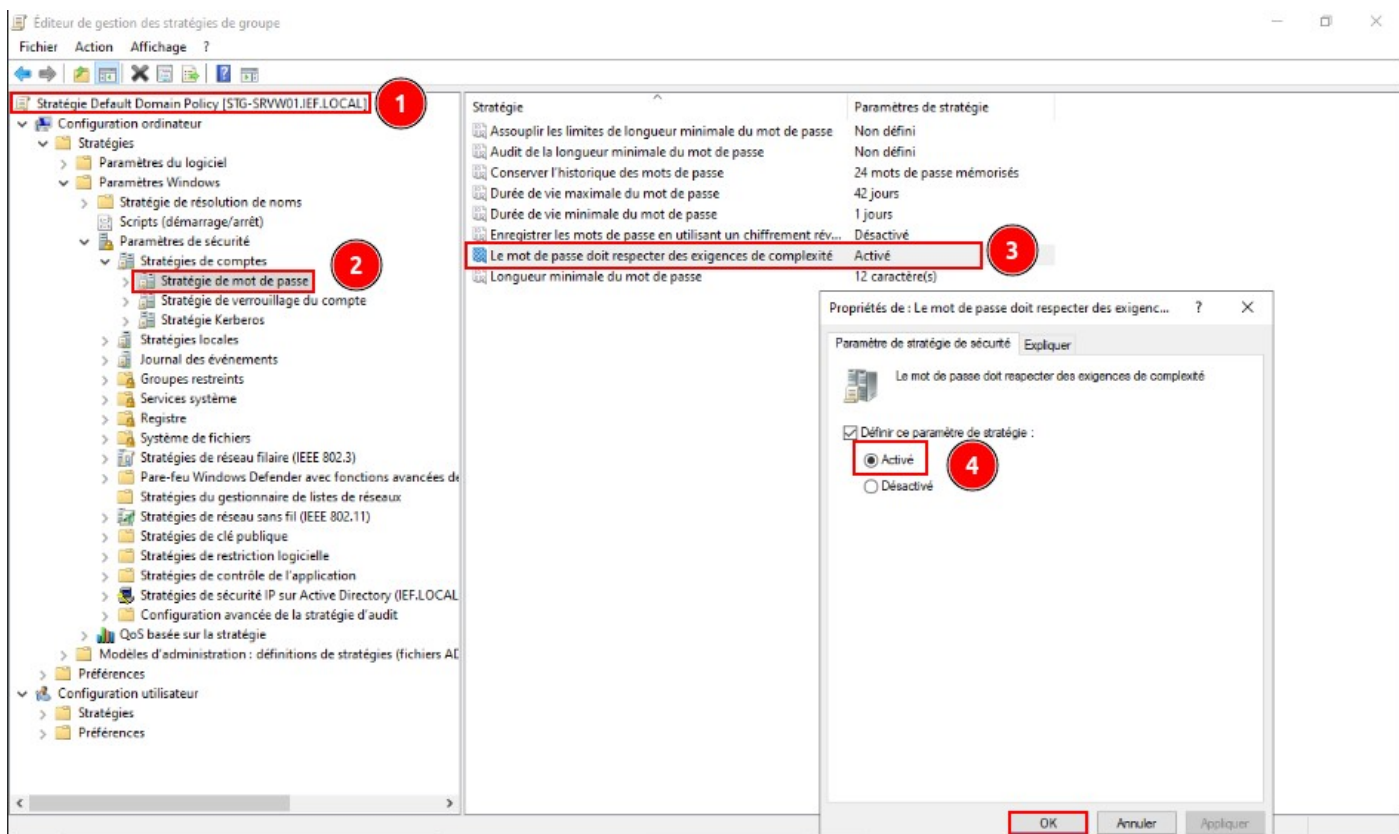
- Navigation (Points 1 à 5) :** Vous vous trouvez toujours dans le même menu de la GPO USERS-RESTRICTIONS : Configuration utilisateur > Stratégies > Modèles d'administration > Composants Windows > Explorateur de fichiers.
- Sélection du paramètre (Encadré 6) :** Vous avez sélectionné la stratégie « **Empêcher l'accès aux lecteurs à partir du Poste de travail** ».
- Configuration de l'interdiction (Fenêtre au premier plan) :**
 - Vous avez coché l'option « **Activé** ».
 - Dans le menu déroulant des options, vous avez choisi « **Restreindre aux lecteurs A, B, C et D uniquement** ».
- Validation (Encadré en bas à droite) :** Vous cliquez sur le bouton « **OK** » pour enregistrer cette règle de sécurité.



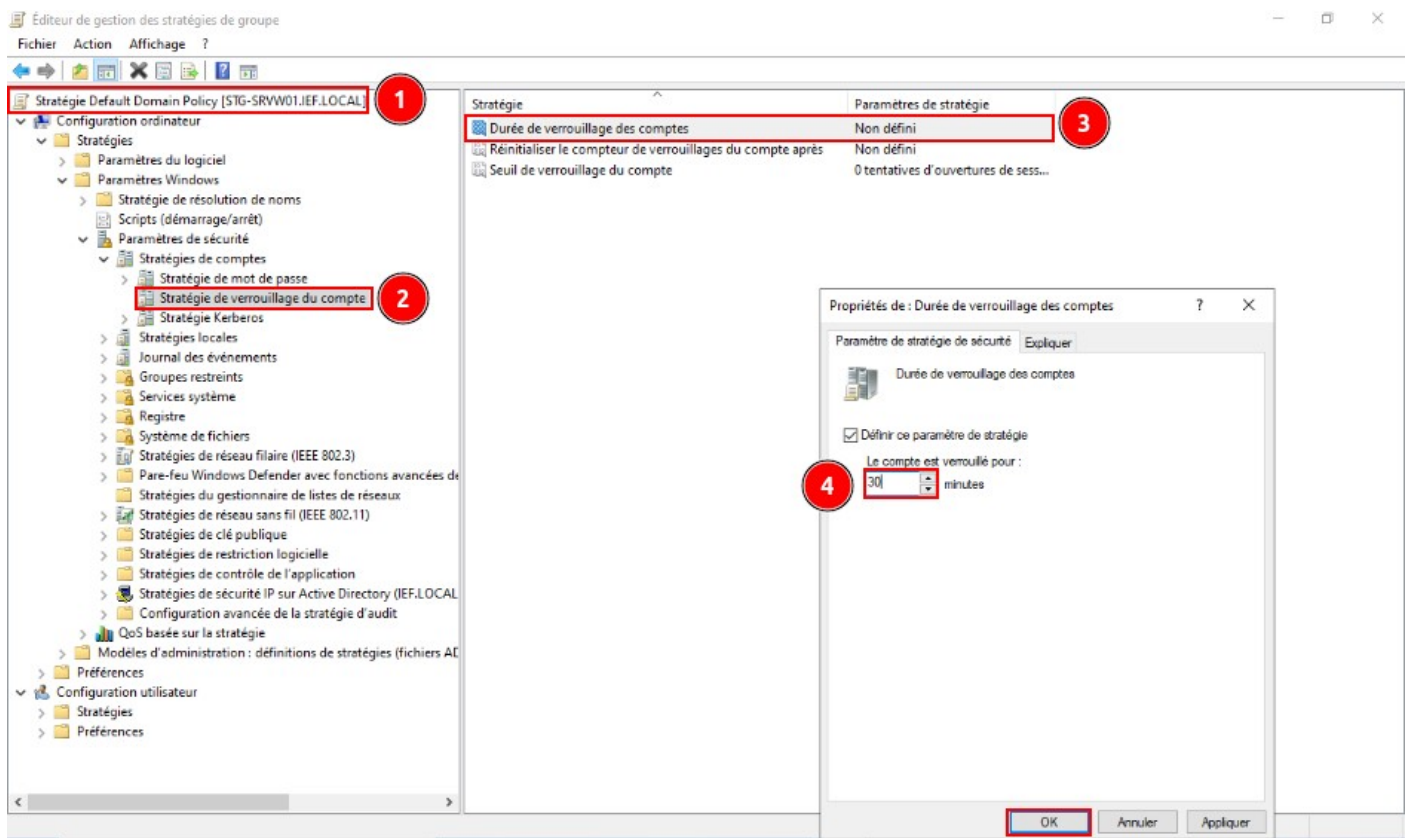
3. **Encadré 3 (Volet central)** : Vous avez sélectionné le paramètre « **Longueur minimale du mot de passe** ». On constate que la valeur actuelle est de **7 caractères** (le réglage par défaut de Windows).
4. **Encadré 4 (Fenêtre de propriétés)** : Dans la fenêtre qui s'est ouverte, vous avez saisi la valeur « **12** ».
5. **Encadré 5 (Bas)** : Vous cliquez sur le bouton « **OK** » pour enregistrer et appliquer officiellement cette nouvelle règle de sécurité à l'ensemble du domaine.



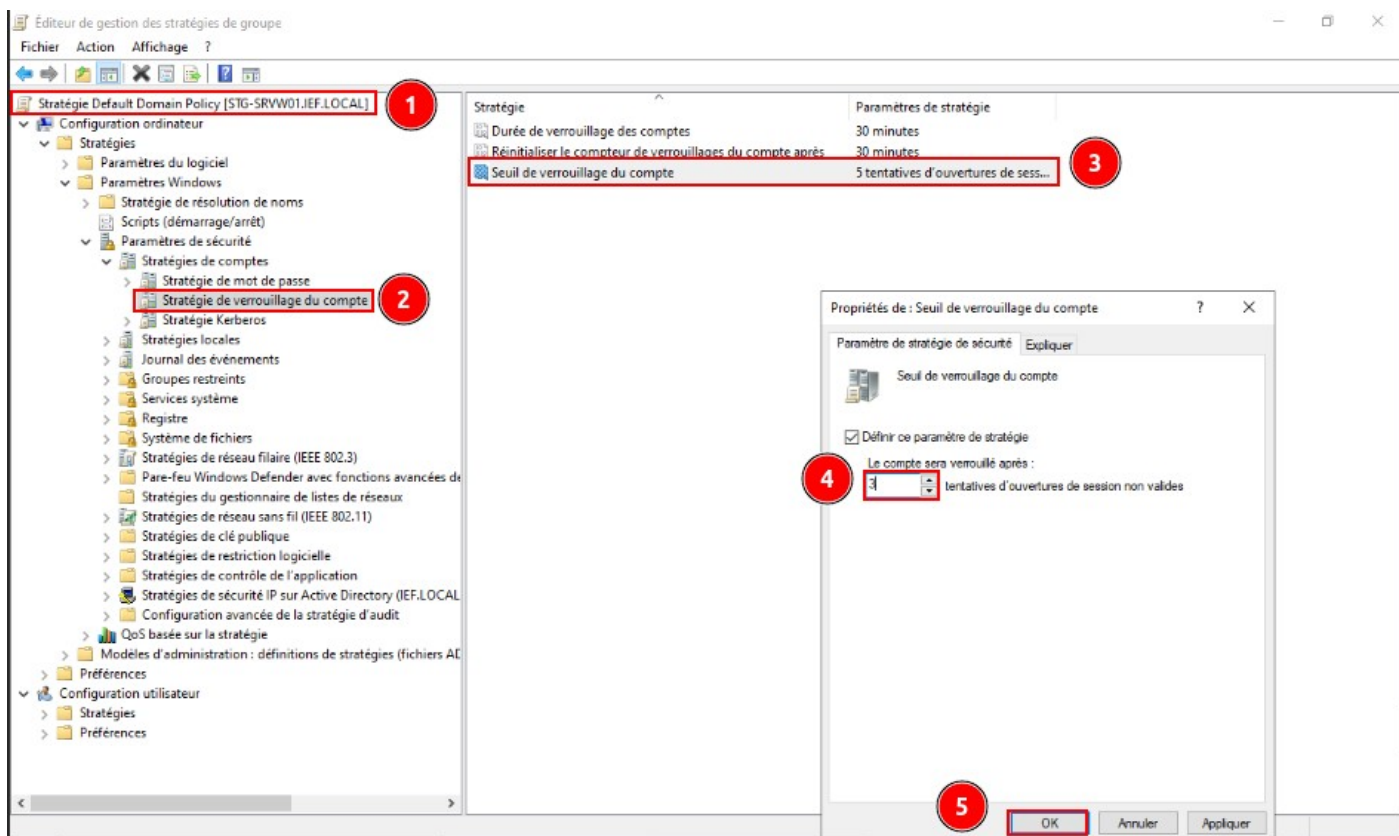
1. **Encadré 1 (Haut gauche)** : On confirme que vous travaillez toujours sur la **Default Domain Policy**, la stratégie qui s'applique à l'ensemble du domaine.
2. **Encadré 2 (Navigation)** : Vous êtes toujours dans la section « **Stratégie de mot de passe** » (sous Paramètres de sécurité > Stratégies de comptes).
3. **Encadré 3 (Volet central)** : Vous avez sélectionné le paramètre intitulé « **Le mot de passe doit respecter des exigences de complexité** ». On voit qu'il est actuellement sur l'état « **Activé** ».
4. **Encadré 4 (Propriétés)** : Dans la fenêtre de réglage, vous avez coché l'option « **Activé** ».



1. **Encadré 1 (Haut gauche)** : Vous travaillez sur la **Default Domain Policy**, la stratégie qui s'applique par défaut à l'ensemble du domaine.
2. **Encadré 2 (Navigation)** : Vous avez navigué dans l'arborescence : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > **Stratégie de verrouillage du compte**.
3. **Encadré 3 (Volet central)** : Vous avez sélectionné le paramètre « **Durée de verrouillage des comptes** ». On voit qu'il était auparavant sur l'état « **Non défini** ».
4. **Encadré 4 (Propriétés)** : Dans la fenêtre qui s'est ouverte, vous saisissez la valeur « **30** ».



1. **Encadré 1 (Haut gauche)** : On confirme que vous modifiez la **Default Domain Policy**, la stratégie qui s'applique à tous les utilisateurs du domaine.
2. **Encadré 2 (Navigation)** : Vous êtes dans la section « **Stratégie de verrouillage du compte** ».
3. **Encadré 3 (Volet central)** : Vous avez sélectionné le paramètre « **Seuil de verrouillage du compte** ». On voit que la valeur précédente était de **5 tentatives**.
4. **Encadré 4 (Fenêtre de propriétés)** : Vous modifiez cette valeur pour la passer à **3**.
5. **Encadré 5 (Bas)** : Vous cliquez sur le bouton « **OK** » pour enregistrer et appliquer ce nouveau seuil de sécurité.



GPO et parametres pour clients

Personnalisation des postes clients

- **Navigation (1 à 4) :** Vous naviguez dans Configuration utilisateur > Stratégies > Modèles d'administration > Bureau > **Bureau**.
- **Sélection (5) :** Vous avez sélectionné le paramètre « **Papier peint du Bureau** ».
- **Configuration (6) :** Vous avez activé (**Activé**) cette stratégie.
- **Paramètres (7) :** Vous avez renseigné le chemin réseau (UNC) vers l'image officielle de l'entreprise : \\ief.local\SYSVOL\ief.local\wallpaper.jpg. Le style est réglé sur "Ajuster".

The screenshot displays the Group Policy Editor interface. On the left, the navigation tree shows the path: Configuration utilisateur > Stratégies > Modèles d'administration > Bureau > **Bureau**. The main pane shows the 'Papier peint du Bureau' policy. The policy is configured with the following settings:

- État:** Activé
- Commentaire:** Non
- Pris en charge sur:** Au minimum Windows 2000
- Options:** Non configuré
- Aide:** Spécifie l'image d'arrière-plan (le « papier peint ») affichée sur le Bureau des utilisateurs.

The configuration window for 'Papier peint du Bureau' is open, showing the 'Activé' radio button selected. The 'Pris en charge sur' dropdown is set to 'Au minimum Windows 2000'. The 'Options' section is set to 'Non configuré'. The 'Aide' section provides detailed instructions on how to use the policy, including examples of local and UNC paths.

Exemple : avec un chemin local : C:\windows\web\wallpaper\home.jpg

Exemple : avec un chemin UNC : \\Server\Share\Corp.jpg

Style du papier peint : Ajuster

- **Navigation (1 à 5) :** Vous naviguez dans Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration > **Personnalisation**.
- **Action (6) :** Vous avez activé le paramètre « **Empêcher de modifier l'arrière-plan du Bureau** ».
 - **Objectif :** Faire en sorte que les utilisateurs ne puissent pas changer le fond d'écran que vous avez imposé à l'étape précédente (l'option sera grisée dans leurs paramètres).
- **Action (7) :** Vous avez activé le paramètre « **Empêcher de modifier le thème** ».

Stratégie USERS-PERSONALISATION 1 SRVV

Configuration ordinateur

Stratégies

Préférences

Configuration utilisateur 2

Stratégies

Paramètres du logiciel

Paramètres Windows

Modèles d'administration : définition 3

Bureau

Composants Windows

Dossiers partagés

Menu Démarrer et barre des tâches

Panneau de configuration 4

Affichage

Ajouter ou supprimer des pro

Imprimantes

Options régionales et linguisti

Personnalisation 5

Programmes

Réseau

Système

Tous les paramètres

Préférences

Personnalisation

Sélectionnez un élément pour obtenir une description.

Paramètre	État	Commentaire
Empêcher de modifier le modèle de couleurs	Non configuré	Non
Empêcher de modifier le thème	Activé 7	Non
Empêcher de modifier le style visuel des fenêtres et des boutons	Non configuré	Non
Activer l'écran de veille	Non configuré	Non
Empêcher la sélection de la taille de police du style visuel	Non configuré	Non
Empêcher de modifier la couleur et l'apparence	Non configuré	Non
Empêcher de modifier l'arrière-plan du Bureau	Activé 6	Non
Empêcher de modifier les icônes du Bureau	Non configuré	Non
Empêcher de modifier les pointeurs de la souris	Non configuré	Non
Empêcher de modifier l'écran de veille	Non configuré	Non
Empêcher de modifier les sons	Non configuré	Non
Un mot de passe protège l'écran de veille	Non configuré	Non
Dépassement du délai d'expiration de l'écran de veille	Non configuré	Non
Forcer un écran de veille spécifique	Non configuré	Non
Charger un thème spécifique	Non configuré	Non
Forcer un fichier de style visuel spécifique ou forcer le style Windows Cla...	Non configuré	Non

Étendu Standard

16 paramètre(s)

Dépannage

Dépannage

Dépannage

1. RESEAU ET TUNNEL VPN (PFSENSE)

Le tunnel IPsec ne s'établit pas (Statut "Down")

- Vérifier que les identifiants (FQDN) correspondent exactement aux noms dans les certificats (FW-SA.ief.local).
- S'assurer que l'algorithme de chiffrement (AES256-GCM) est identique sur les deux pare-feux.
- Vérifier que l'autorité de certification (CA) du site distant a bien été importée dans l'onglet "Authorities".

Le tunnel est "Up" mais le trafic ne passe pas

- Vérifier dans Firewall > Rules > IPsec : une règle doit autoriser le flux "Any" ou au moins le protocole ICMP.
- Vérifier que les passerelles par défaut des clients pointent bien sur l'IP LAN du pare-feu respectif.

2. SERVICES ACTIVE DIRECTORY, DNS ET DHCP

Impossible de joindre le DC2 au domaine

- Cause : Le DC2 ne parvient pas à résoudre le nom du domaine.
- Solution : Vérifier que l'adresse DNS primaire de la carte réseau du DC2 est bien l'IP du DC1 (192.168.100.200).

Le basculement (Failover) DHCP ne se synchronise pas

- Vérifier que le "Secret partagé" saisi lors de la configuration est strictement identique sur les deux serveurs.
- Vérifier que les deux serveurs peuvent communiquer sur les ports UDP 67 et 68.

Résolution de noms Internet impossible sur les clients

- Vérifier dans la console DNS (mmc) que les "Redirecteurs" sont bien configurés avec des DNS valides (ex: 9.9.9.9 ou 1.1.1.1).

3. STOCKAGE ISCSI ET SERVICES DE FICHIERS (DFS)

Le disque distant TrueNAS n'apparaît pas sur le serveur Windows

- Vérifier dans l'Initiateur iSCSI que le statut est bien "Connecté".
- Vérifier la connectivité IP sur le réseau SAN (Ping entre 192.168.51.1 et 192.168.51.2).
- S'assurer que le service iSCSI sur TrueNAS est bien sur "RUNNING".

La réplication DFS ne fonctionne pas entre les sites

- Vérifier qu'un "Membre principal" a été défini pour la première synchronisation.
- Vérifier que les droits NTFS sur les dossiers physiques (F:\Shares\...) autorisent le groupe "Utilisateurs authentifiés" en modification.

L'énumération basée sur l'accès (ABE) ne cache pas les dossiers

- S'assurer que l'option a été cochée à deux endroits : dans les paramètres du partage SMB ET dans les propriétés avancées de l'espace de noms DFS.

4. SAUVEGARDE ET MAINTENANCE

Échec de la planification Windows Server Backup

- Vérifier que le disque de destination (Disque iSCSI) est bien initialisé en mode GPT et non MBR.
- Attention : Le disque de destination est formaté lors de la première sauvegarde, toutes les données précédentes seront perdues.

Problème de performance ou détection matérielle (Proxmox)

- Si un disque ou une carte réseau n'est pas vu par Windows, vérifier que les pilotes VirtIO ont été installés depuis l'ISO (dossiers vioscsi et NetKVM).
- Vérifier que le mode de CPU dans Proxmox est réglé sur "Host" pour une performance optimale.

5. COMMANDES DE DIAGNOSTIC RAPIDE (POWERSHELL / CMD)

- Tester la connectivité : ping [IP_CIBLE]
- Tester la résolution DNS : nslookup [NOM_DU_DOMAINE]
- Vérifier les ports ouverts : Test-NetConnection [IP] -Port 445 (pour le partage de fichiers)
- Forcer la réplication AD : repadmin /syncall /adeP
- Vérifier la configuration IP complète : ipconfig /all