

Projet « NOVA-LINK »
-
BTS SIO 2025 Option SISR
-
DOCUMENTAION TECHNIQUE



Documentation technique projet NOVA-LINK

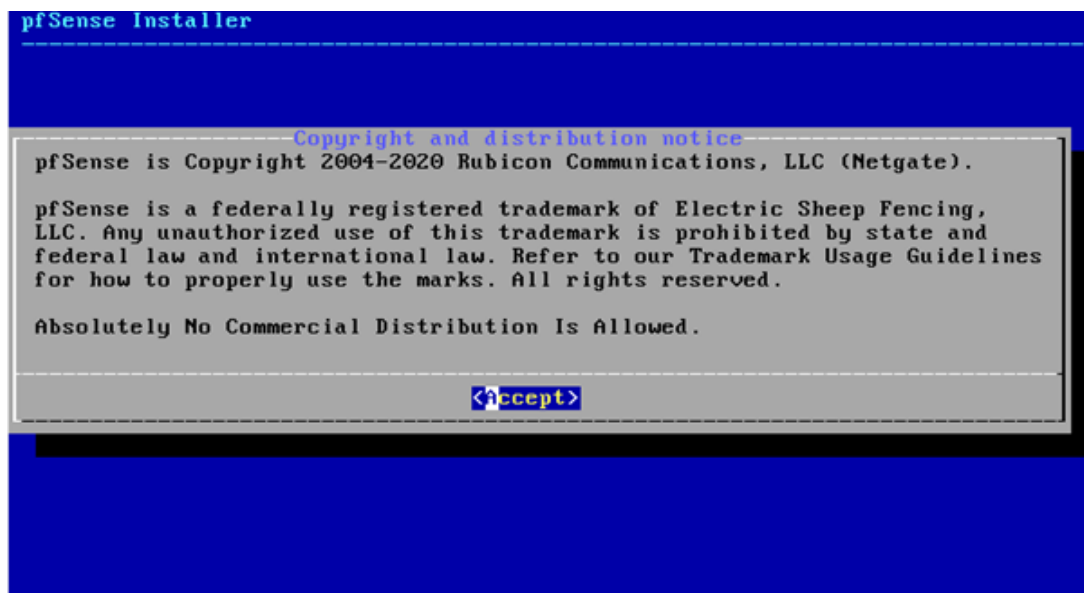
Table des matières

Documentation technique projet M2i	1
Mise en place de PfSense	2
Installation.....	2
Configuration	6
Création du tunnel VPN	9
Configuration du pare-feu.....	14
Installation de l'AD, DNS, DHCP	16
Configuration de l'IP BONDING.....	16
Installation de l'AD	20
Installation du DHCP	28
Installation et configuration de DFS/R	36
Création du partage.....	37
Mise en place des droits sur les dossiers.....	41
Réplication des données	43
Mise en place de TrueNas	48
Installation.....	48
Création du volume	51
Configuration du partage ISCSI	53
Ajout du disque sur le serveur	56
Mise en place de ShadowCopy	57
Mise en place des GPO	59
Mappage des lecteurs	59
Papier peint du bureau	61
Redirection des dossiers personnels.....	65
Interdire l'accès aux paramètres.....	66
Bloquer les ports USB.....	67
Masquer et bloquer le disque C	68
Bloquer l'accès aux consoles Powershell et Invité de commande	69

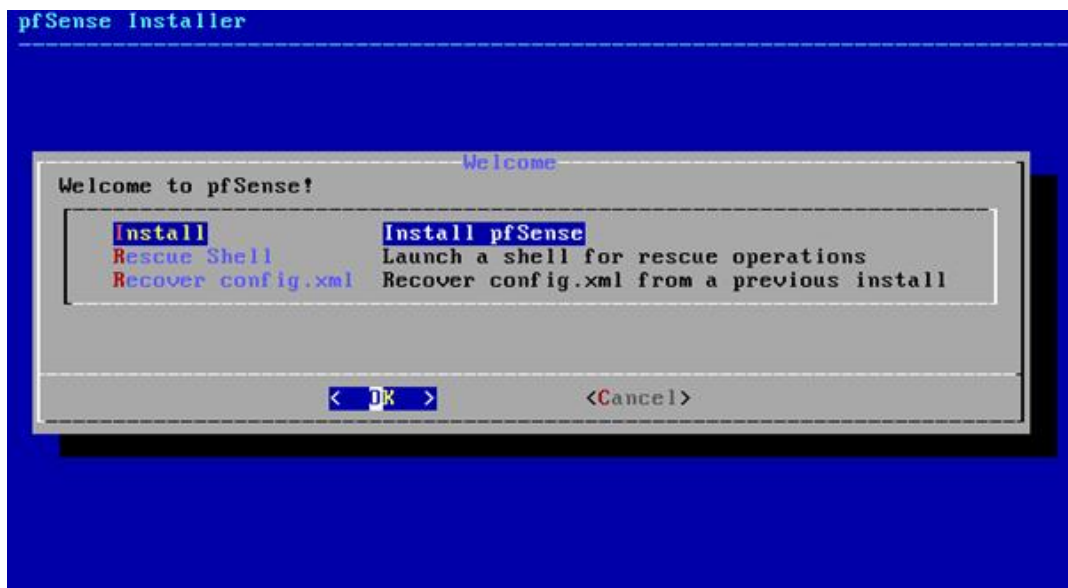
Mise en place de PfSense

Installation

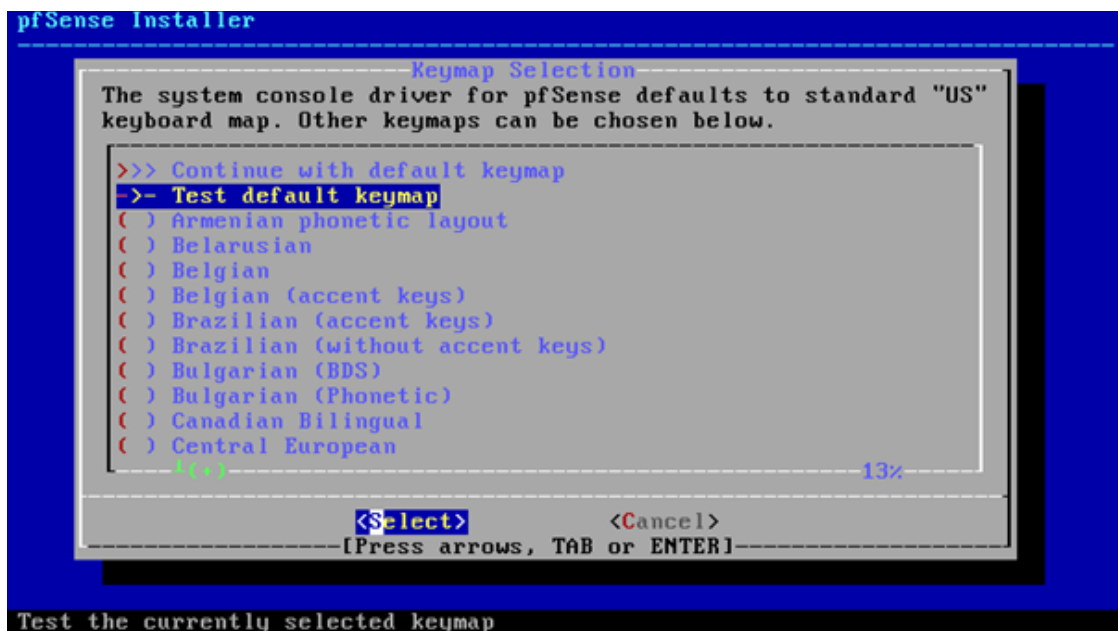
- Au commencement de l'installation, vous pourrez accepter le contrat de licence.



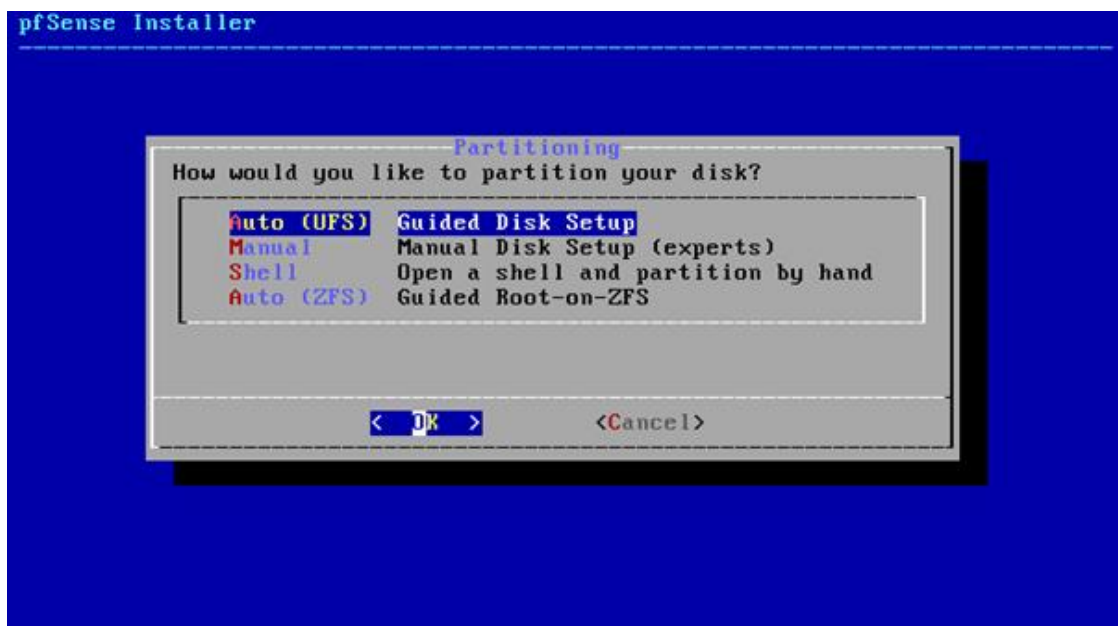
- Installez ensuite la distribution.



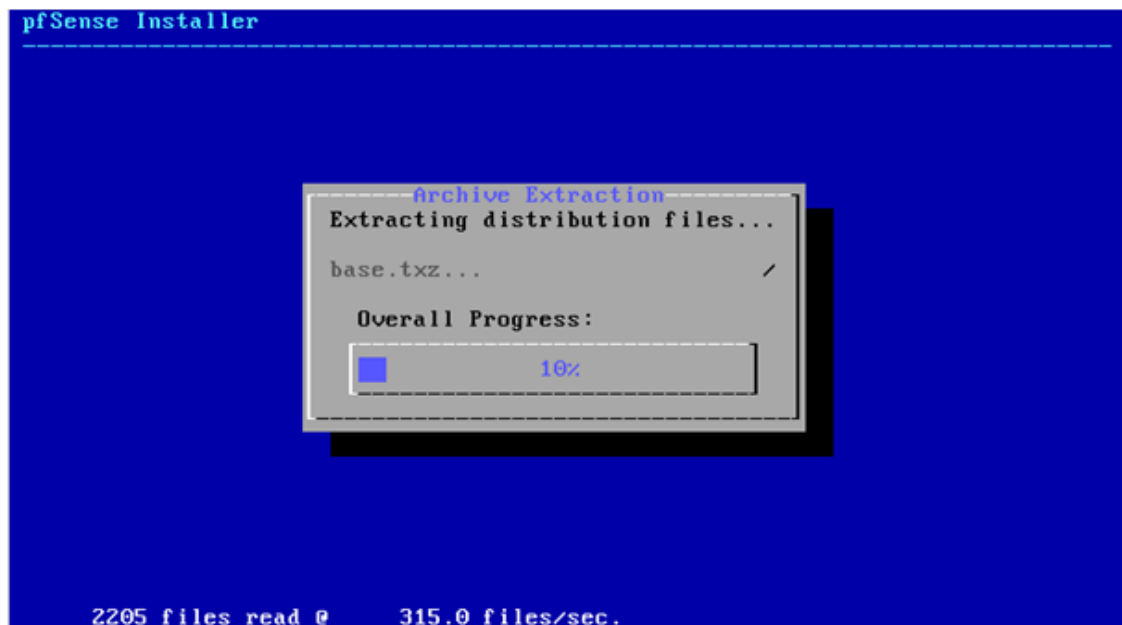
- Choisissez les paramètres linguistiques :



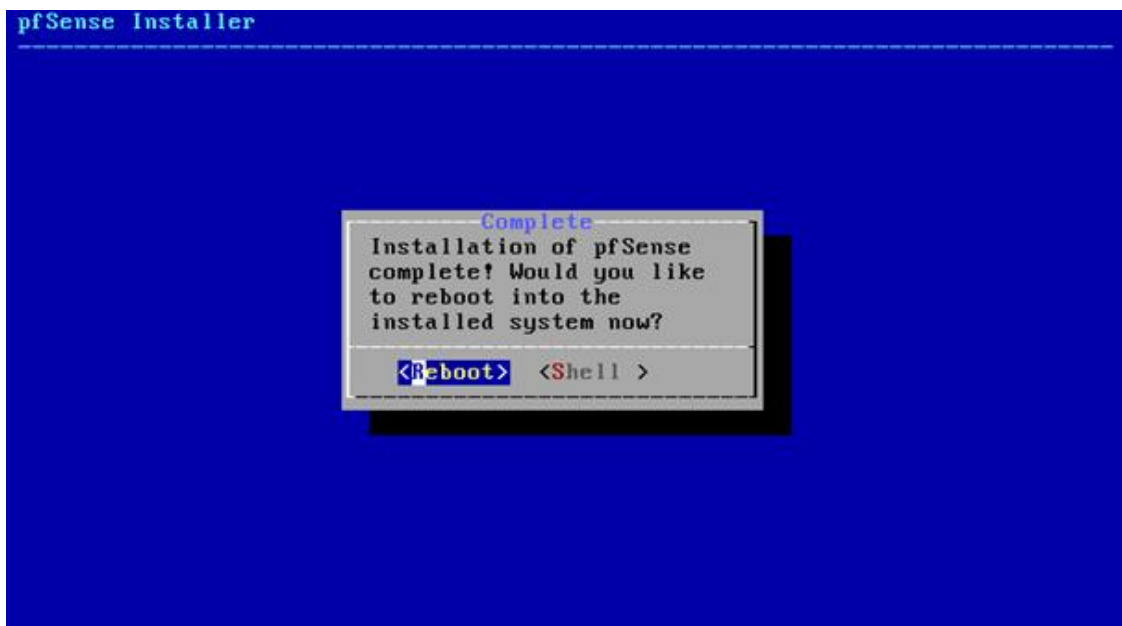
- Choisir la manière de partitionner votre disque. Ici on conservera la méthode par défaut.



- L'installation va alors se dérouler



- Le système devrait vous demander de redémarrer par la suite.



- Vous pouvez alors paramétrer vos interfaces réseau.

```
8) Shell
Enter an option:

FreeBSD/amd64 (pfSense1.test.fr) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 84f34973cf08041c0f4e
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense1 ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 172.16.0.1/24

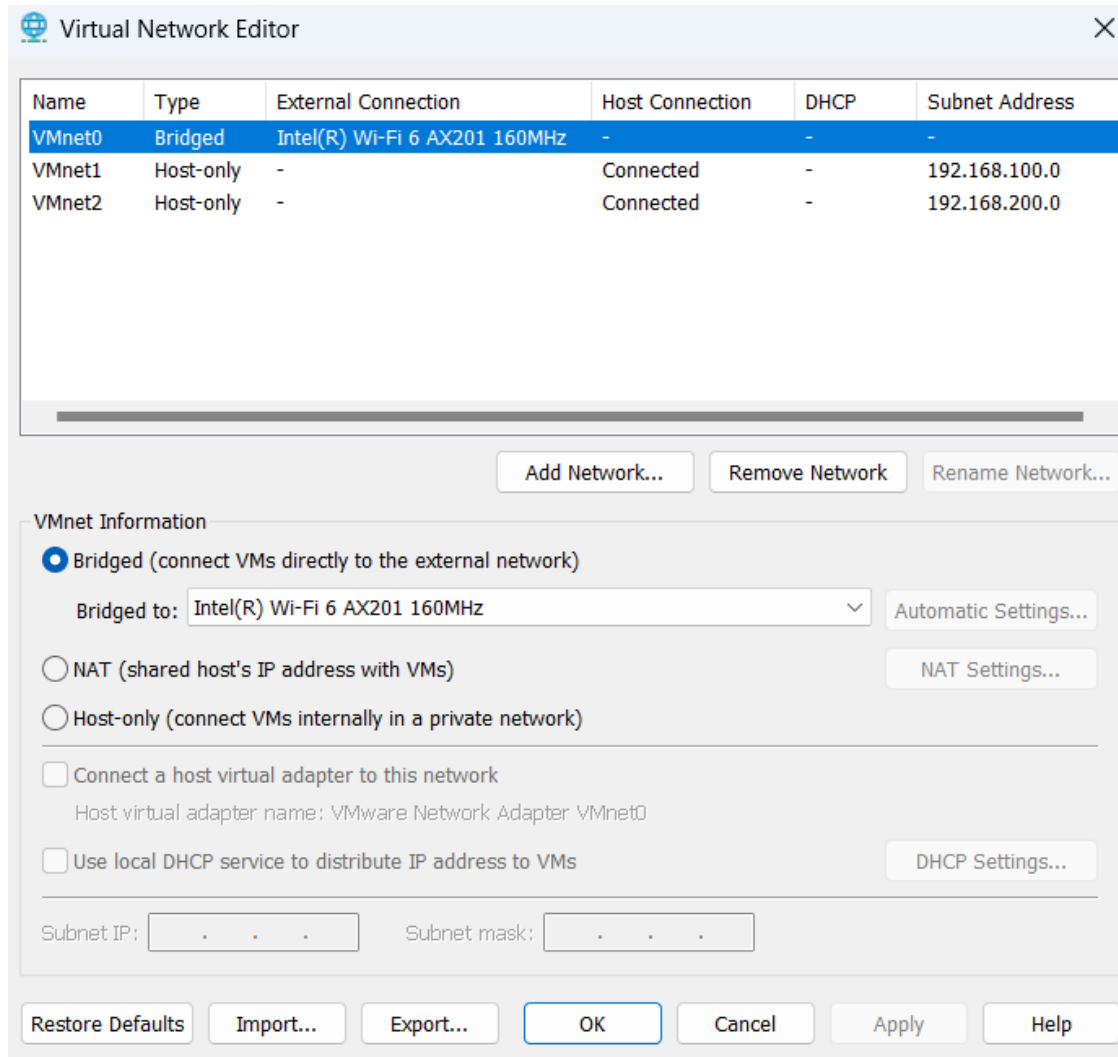
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Configuration

Dans un scénario de VPN site à site, nous avons besoin de deux cartes réseau sur chaque machine pfSense :

- **Carte 1 : Réseau LAN** – Cela simule le réseau interne.
- **Carte 2 : Réseau WAN** – Cela simule l'accès à Internet (ou réseau externe).



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Intel(R) Wi-Fi 6 AX201 160MHz	-	-	-
VMnet1	Host-only	-	Connected	-	192.168.100.0
VMnet2	Host-only	-	Connected	-	192.168.200.0

Buttons: Add Network..., Remove Network, Rename Network...

VMnet Information

☒ Bridged (connect VMs directly to the external network)

Bridged to: Intel(R) Wi-Fi 6 AX201 160MHz Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☐ Host-only (connect VMs internally in a private network)

☐ Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet0

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: . . . Subnet mask: . . .

Buttons: Restore Defaults, Import..., Export..., OK, Cancel, Apply, Help

- Pour la **carte réseau 1 (WAN)**, sélectionnez "**Bridged**". Cela permet à cette interface de se connecter directement au réseau de l'hôte et de recevoir une adresse IP du routeur.
- Pour la **carte réseau 2 (LAN)**, sélectionnez "**Host-only**". Cela isole cette interface du reste du réseau, la connectant uniquement à l'hôte et à d'autres machines virtuelles qui utilisent également une interface **Host-only**.

- Affecter les interfaces réseaux

```
em1      00:0c:29:ad:91:e4    (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed [y!n]? y
```

- Par défaut, pfSense va détecter les interfaces réseau. Vous verrez des interfaces appelées **em0**, **em1**, etc., qui correspondent aux adaptateurs réseau que vous avez configurés.
- Attribuez **em0** à l'interface **WAN** et **em1** à l'interface **LAN**.

- Configuration IP initial

```
4) Reset to factory defaults      13) Update from console
5) Reboot system                  14) Enable Secure Shell (sshd)
6) Halt system                    15) Restore recent configuration
7) Ping host                      16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y
Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

- Pour l'interface **WAN**, laissez la configuration en DHCP (l'interface obtiendra une adresse IP automatiquement du routeur ou du réseau bridgé).

```
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.2

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

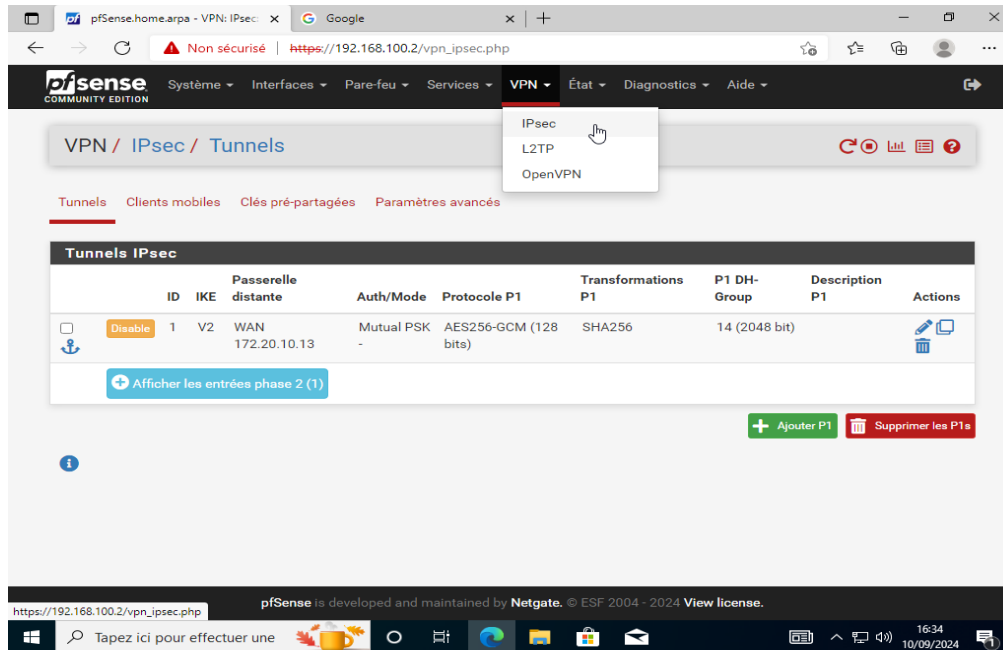
Enter the new LAN IPv6 address. Press <ENTER> for none:
> 
```

- Pour l'interface **LAN**, configurez une IP statique, par exemple **192.168.100.2/24**.

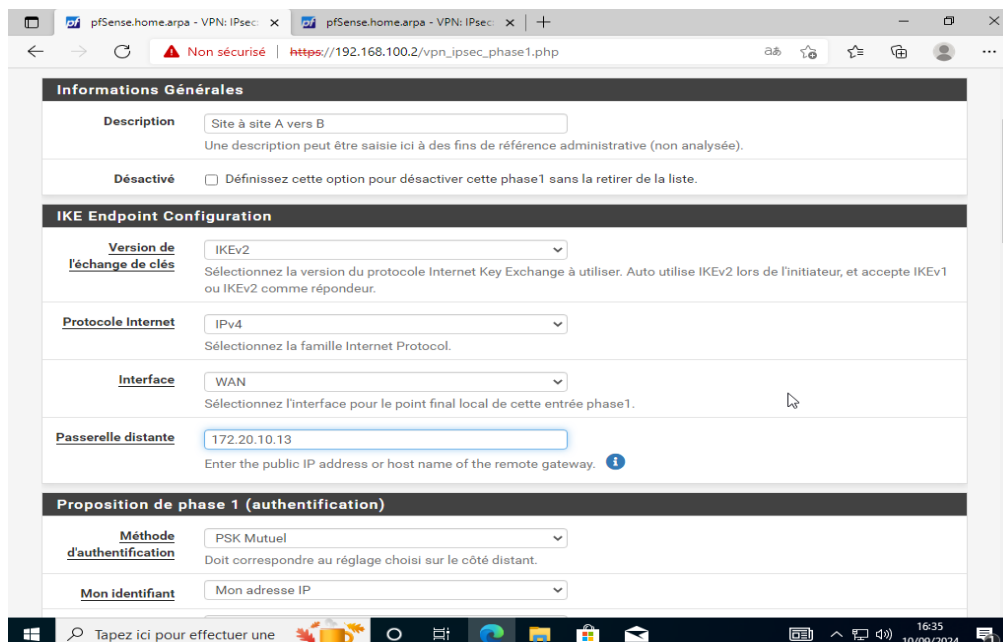
Vous pouvez maintenant accéder à l'interface Web de PfSense via l'adresse **192.168.100.2** depuis une autre machine virtuelle connectée au réseau **Host-only**.

Création du tunnel VPN

- Une fois dans l'interface Web de PfSense, pour créer la connexion VPN il faut se rendre dans l'onglet **VPN -> IPsec**



- Dans le menu **IKE Endpoint Configuration -> Passerelle distante** mettre l'adresse IP WAN de l'autre routeur



- Laisser les paramètres par défaut et enregistrer

Sélectionnez l'interface pour le point final local de cette entrée phase1.

Passerelle distante
172.20.10.13
Enter the public IP address or host name of the remote gateway. ⓘ

Proposition de phase 1 (authentification)

Méthode d'authentification
PSK Mutuel
Doit correspondre au réglage choisi sur le côté distant.

Mon identifiant
Mon adresse IP

Identifiant de pair
Adresse IP distante

***Clé Pré-Partagée**
pfsense
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.
[Generate new Pre-Shared Key](#)

Phase 1 Proposal (Encryption Algorithm)

Algorithme de chiffrement
AES
128 bits
SHA256
14 (2048 bit)
Supprimer

Algorithm
Longueur de la clé
Hash
DH Group

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm
[+ Add Algorithm](#)

Expiration and Replacement

Connexions partagées
☐ Activez ceci pour fractionner les entrées de connexion avec plusieurs configurations de phase 2. Obligatoire pour les points distants qui ne prennent en charge qu'un seul sélecteur de trafic par enfant SA.

PRF Selection
☐ Enable manual Pseudo-Random Function (PRF) selection
Manual PRF selection is typically not required, but can be useful in combination with AEAD Encryption Algorithms such as AES-GCM

Custom IKE/NAT-T Ports
Remote IKE Port
Remote NAT-T Port
UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500).
UDP port for NAT-T on the remote gateway. ⓘ

Détection des pairs morts
☒ Activer DPD
Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKEv1 R_U_THERE messages. Active DPD checking is only enforced if no IKE or ESP/AH packet has been received for the configured DPD delay.

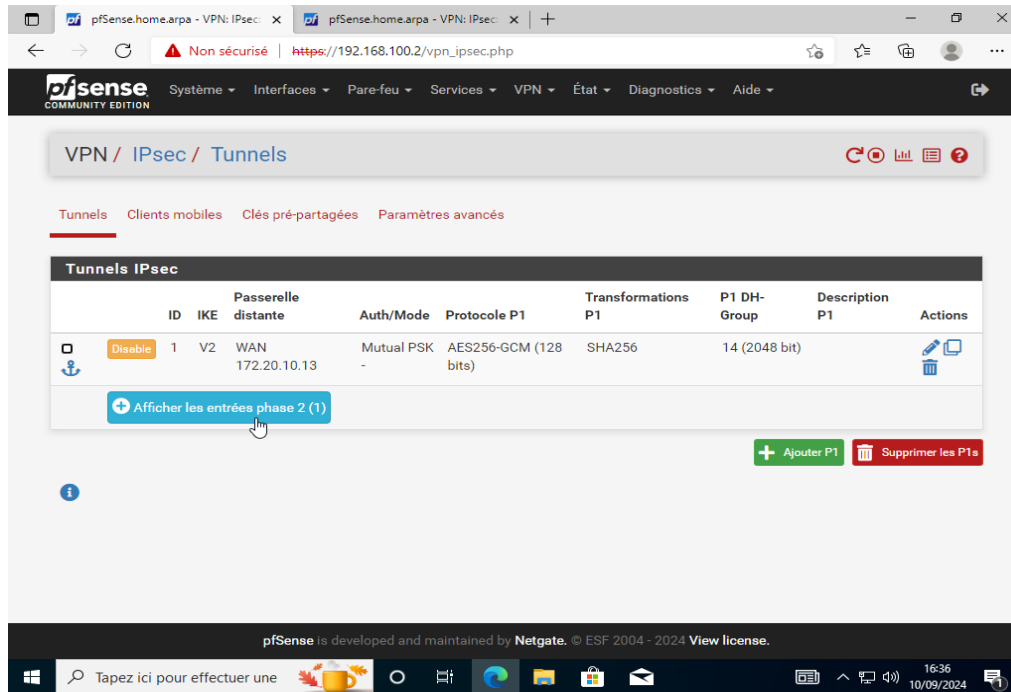
Délai
10
Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.

Échecs maxi
5
Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the [retransmission](#) timeout is used instead.

[Enregistrer](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license.](#)

- Configurer la phase 2 en cliquant sur **Afficher les entrées phase 2** puis **Ajouter P2**



- Dans le menu **réseaux** dans le champs **réseau distant** mettre l'ip du réseau **LAN** de l'autre routeur. Mettre le subnet correspondant, en occurrence **/24**

The screenshot shows the pfSense web interface for configuring a VPN Phase 2. The browser address bar shows the URL: https://192.168.100.2/vpn_ipsec_phase2.php?p2index=66dac01a575ee. The page is titled "Informations Générales".

Informations Générales

- Description:** LAN A vers B. A note below states: "Une description peut être saisie ici à des fins de référence administrative (non analysée)."
- Désactivé:** ☐ Désactivez cette la phase 2 sans la supprimer de la liste.
- Mode:** Tunnel IPv4
- Phase 1:** No description (IKE ID 1)
- P2 reqid:** 1

Réseaux

- Réseau local:** LAN subnet. Type: Adresse. Local network component of this IPsec security association.
- Traduction NAT/BINAT:** Aucun. Type: Adresse. Si NAT/BINAT est requis sur ce réseau, spécifiez l'adresse à traduire.
- Réseau distant:** Réseau. Type: Adresse. Remote network component of this IPsec security association. The address field is set to 192.168.200.0/24.

Proposition de phase 2 (SA/Key Exchange)

- Sélectionner algorithme de chiffrement **AES256-GCM**

The screenshot shows the "Proposition de phase 2 (SA/Key Exchange)" section of the pfSense web interface. The browser address bar shows the URL: https://192.168.100.2/vpn_ipsec_phase2.php?p2index=66dac01a575ee.

Proposition de phase 2 (SA/Key Exchange)

- Protocole:** ESP. Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.
- Algorithmes de chiffrement:**
 - ☐ AES (Auto)
 - ☐ AES128-GCM (Auto)
 - ☐ AES192-GCM (Auto)
 - ☒ AES256-GCM (128 bits)
 - ☐ CHACHA20-POLY1305
- Algorithmes de hachage:**
 - ☐ SHA1
 - ☐ SHA256
 - ☐ SHA384
 - ☐ SHA512
 - ☐ AES-XCBC

Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.
- Groupe de clés PFS:** 14 (2048 bit). Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Expiration and Replacement

- Life Time:** 3600. Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty,

- Enregistrer tout et le résultat devrais être le suivant

pfSense.home.arpa - VPN: IPsec x pfSense.home.arpa - VPN: IPsec x +

Non sécurisé | https://192.168.100.2/vpn_ipsec_phase2.php?p2index=66dac01a575ee

to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.

Rekey Time

Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.

Rand Time

A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Keep Alive

Pinger automatiquement l'hôte

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.

[Enregistrer](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license.](#)

Tapez ici pour effectuer une

pfSense.home.arpa - VPN: IPsec x pfSense.home.arpa - VPN: IPsec x +

Non sécurisé | https://192.168.100.2/vpn_ipsec.php

pfSense COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

VPN / IPsec / Tunnels

Tunnels Clients mobiles Clés pré-partagées Paramètres avancés

Tunnels IPsec

	ID	IKE	Passerelle distante	Auth/Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions
☐ Disable	1	V2	WAN 172.20.10.13	Mutual PSK -	AES256-GCM (128 bits)	SHA256	14 (2048 bit)		Éditer Copier Supprimer

	ID	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Description	Actions
☐ Disable	1	tunnel	LAN	192.168.200.0/24	ESP	AES256-GCM (128 bits)			Éditer Copier Supprimer

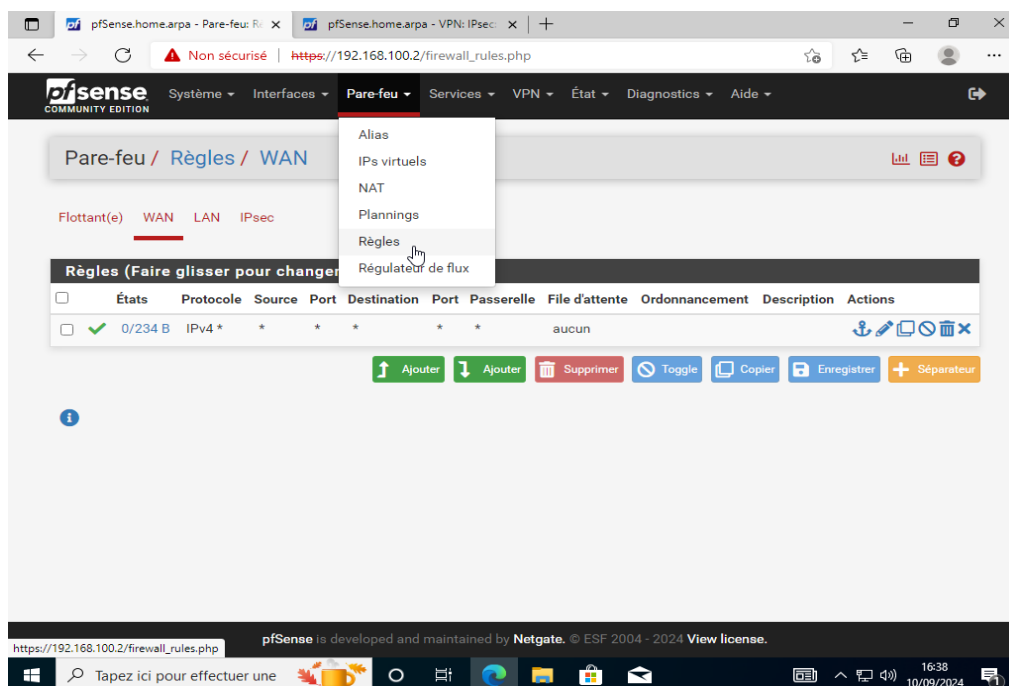
[+ Ajouter P2](#)

[+ Ajouter P1](#) [Supprimer les P1s](#)

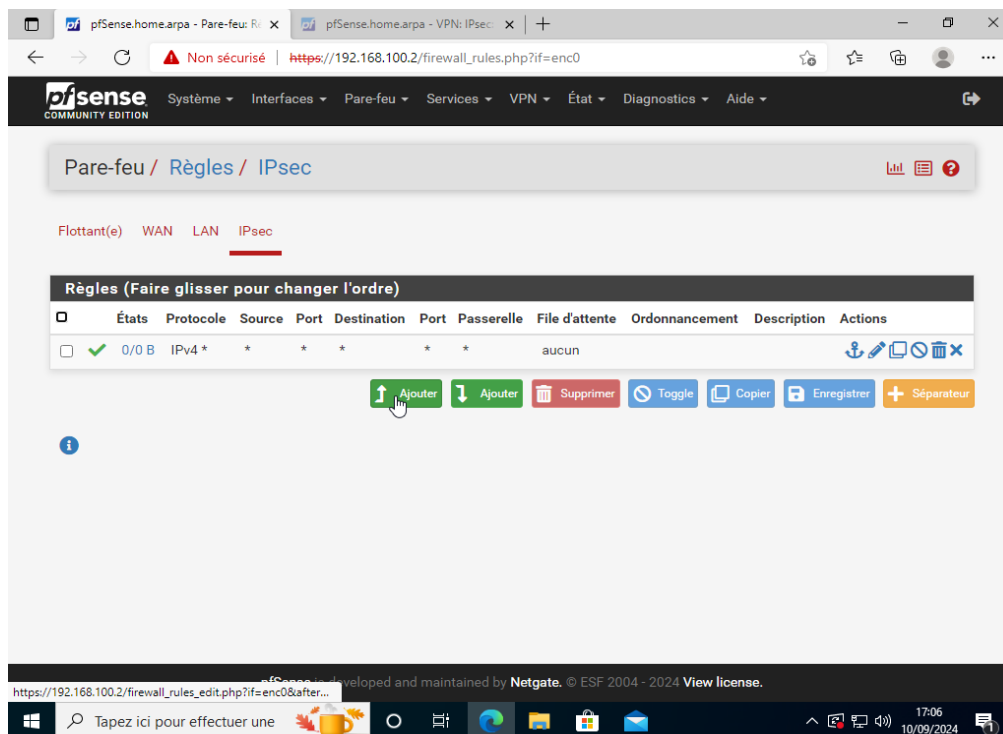
Le tunnel VPN est créé, maintenant il faut se rendre sur le second routeur et refaire la même configuration en mettant les adresses IP du premier serveur.

Configuration du pare-feu

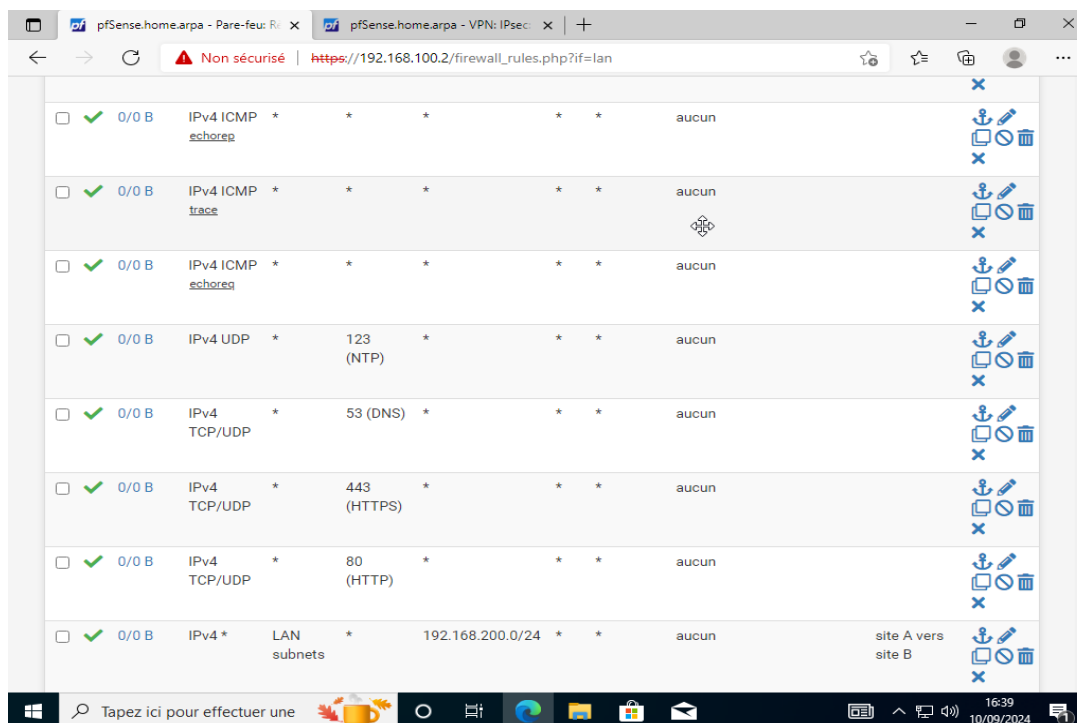
- Pour configurer les règles du pare-feu il faut se rendre dans le menu **Pare-feu** -> **Règles**



- Aller dans l'onglet **IPsec** et ajouter une règle qui autorise toutes les connexions.



- Aller dans l'onglet **LAN** et configurer les règles suivantes



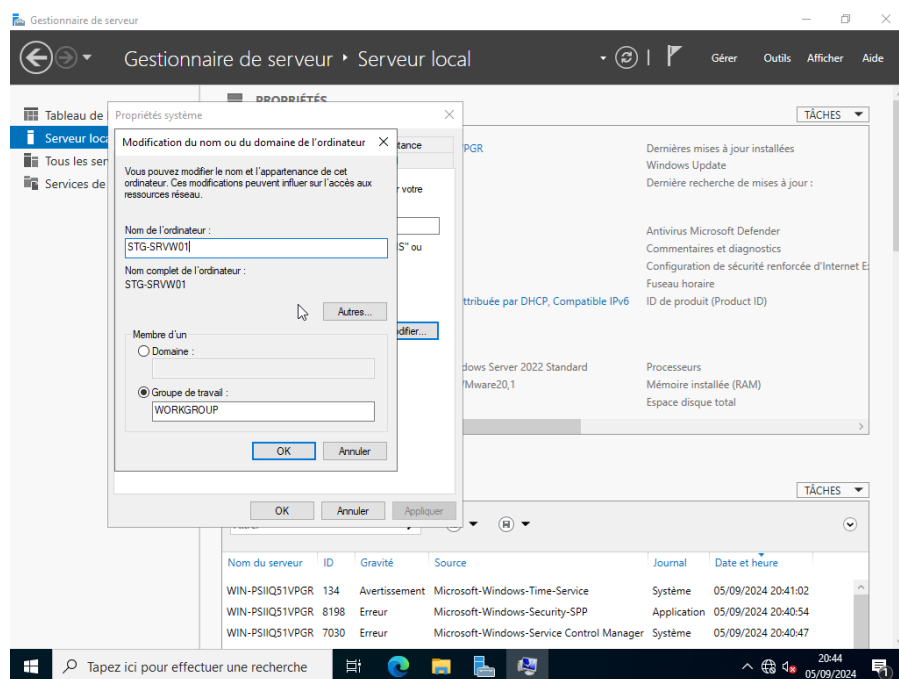
- Répéter les mêmes règles pare feu sur le second serveur.

Les routeurs sont maintenant prêts à l'emploi.

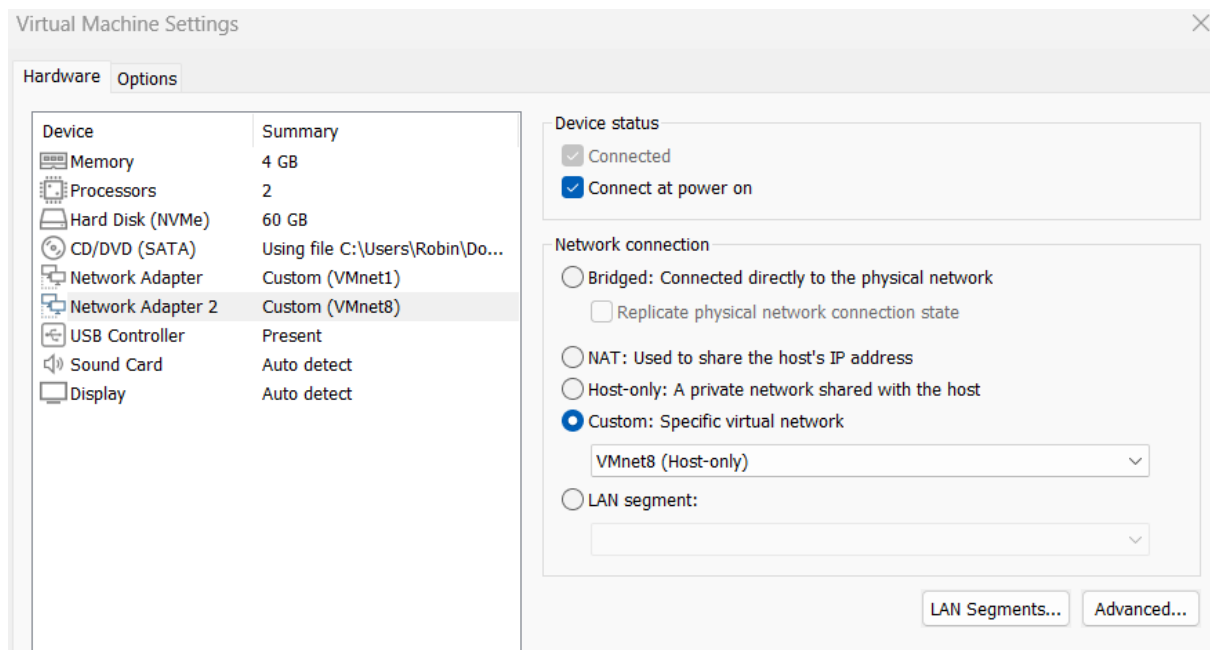
Installation de l'AD, DNS, DHCP

Configuration de l'IP BONDING

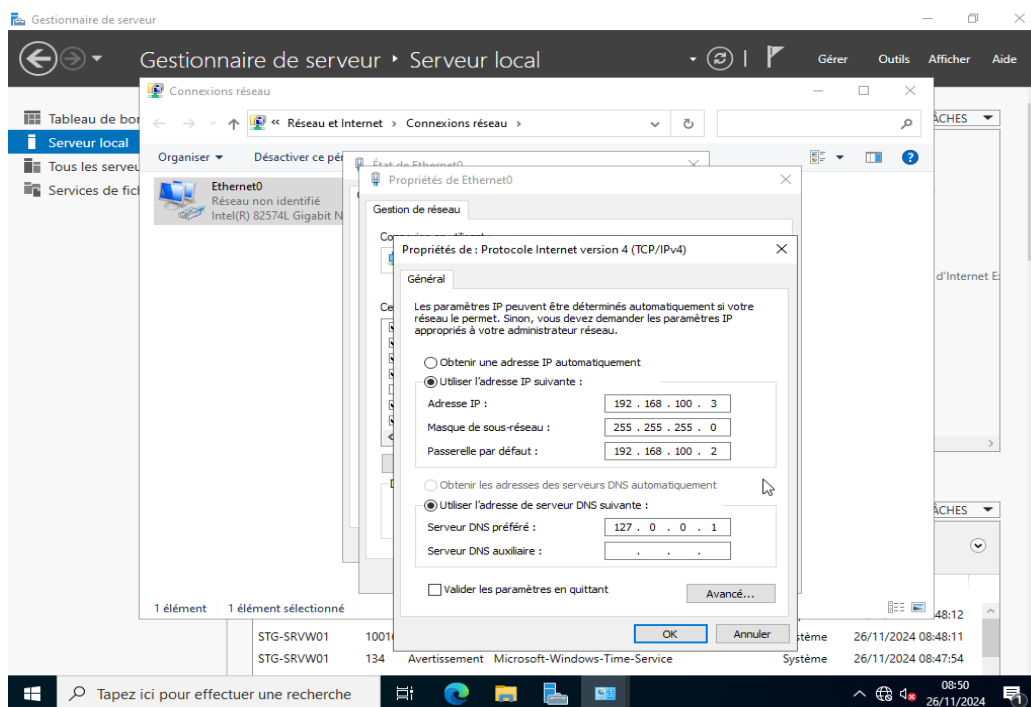
- Renommer le serveur



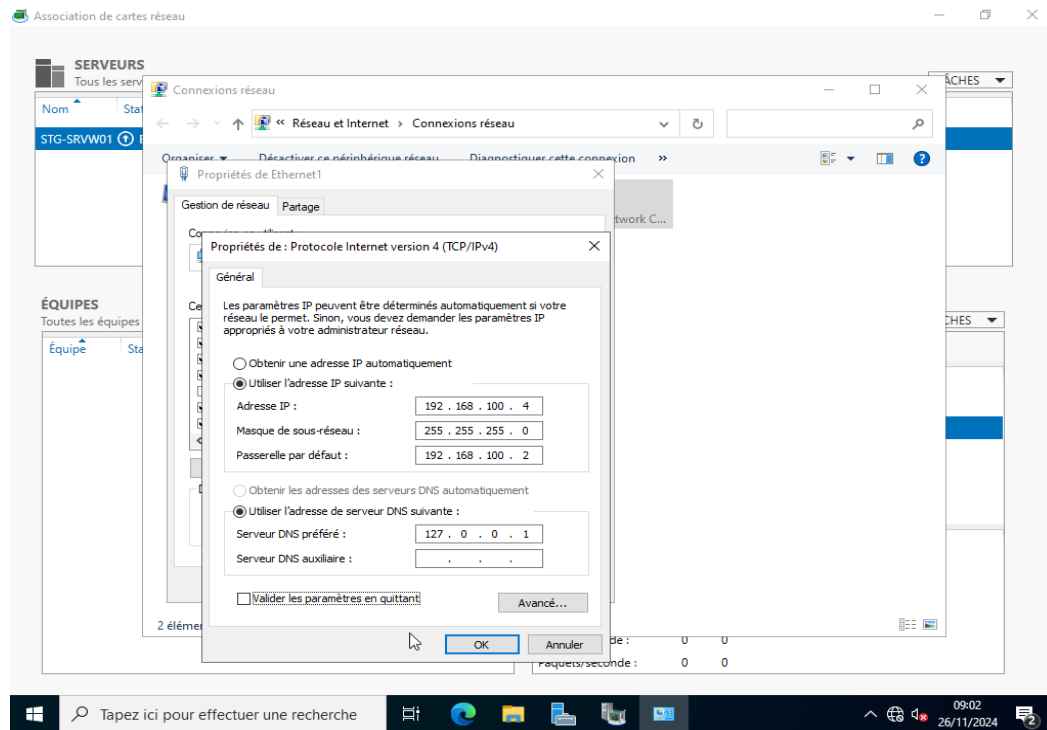
- Ajouter une deuxième carte réseau



- Configuration de la première carte réseau

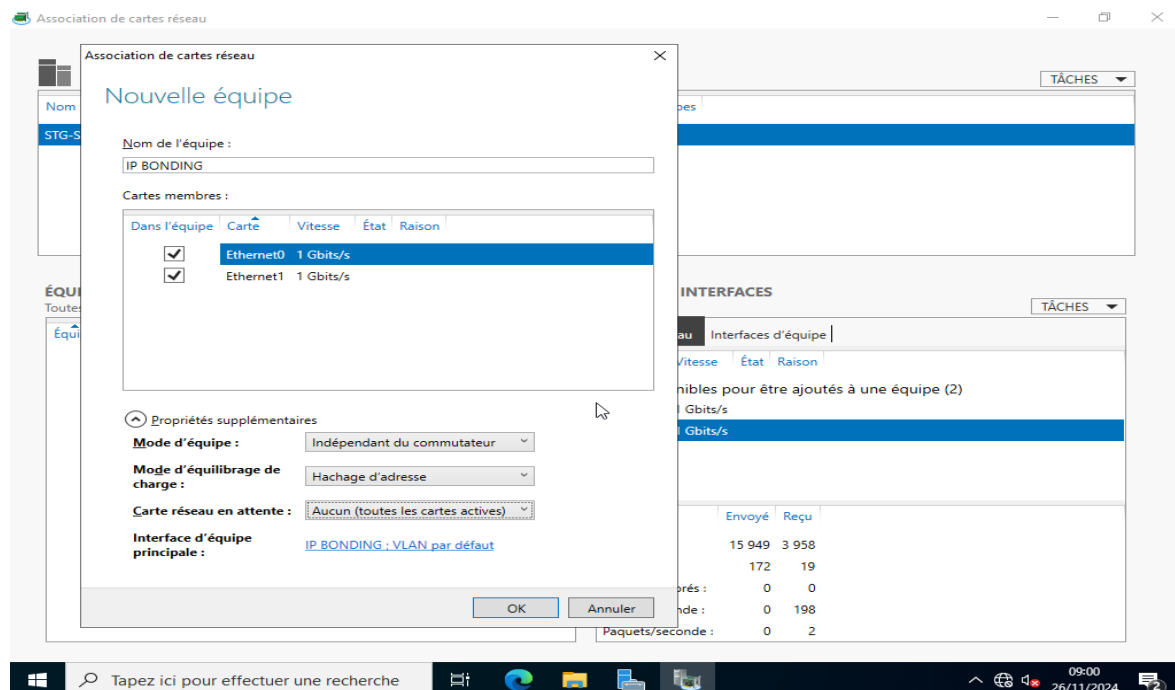


- Configuration de la deuxième carte réseau



- Configuration de l'IP Bonding -> se rendre dans association des cartes réseaux puis ajouter une nouvelle équipe et sélectionner les deux cartes réseaux

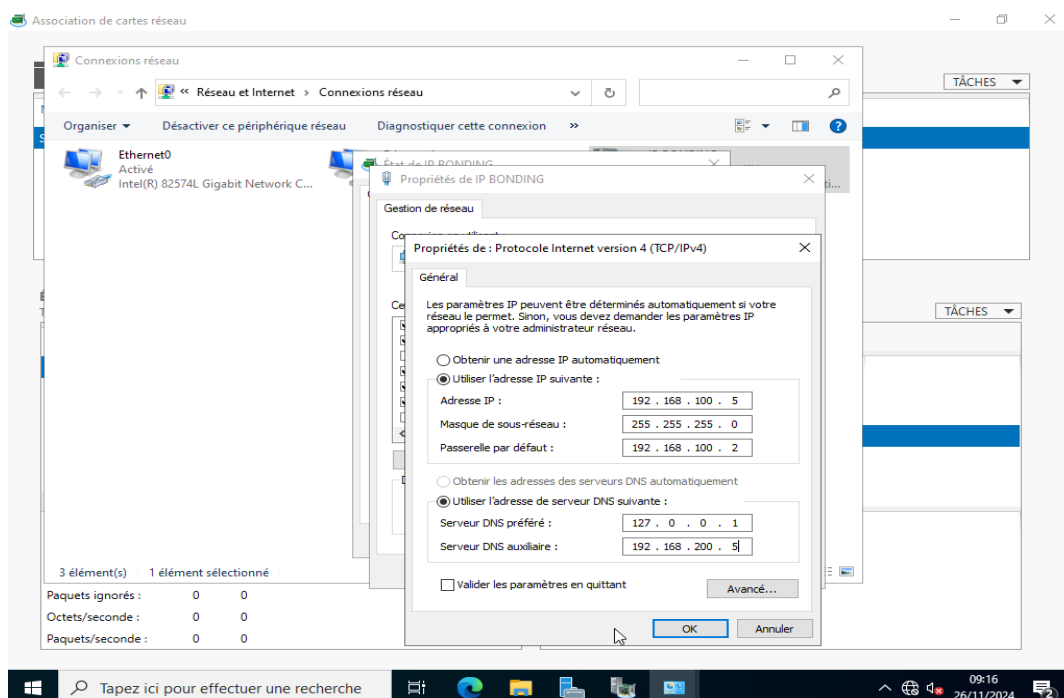
Dans les propriétés supplémentaires configurer le mode d'équilibrage de charge en hachage d'adresse.



- Une fois fait le résultat est le suivant, les deux interfaces à l'état actif

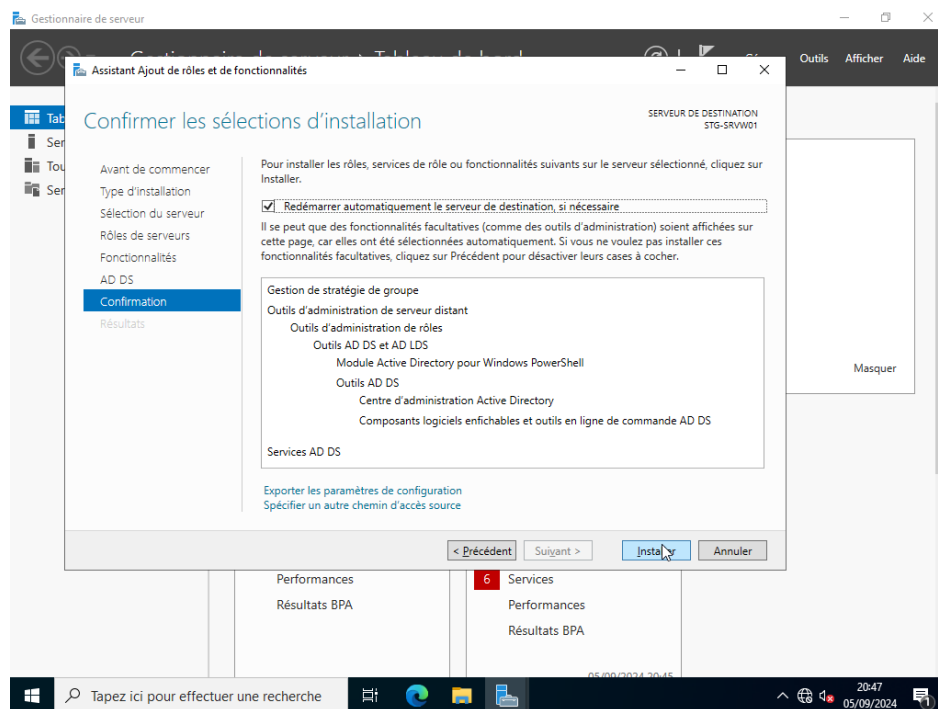
CARTES ET INTERFACES			
TÂCHES ▼			
Cartes réseau Interfaces d'équipe			
Carte	Vitesse	État	Raison
IP BONDING (2)			
Ethernet0	1 Gbits/s	Actif	
Ethernet1	1 Gbits/s	Actif	
Nom	Envoyé	Reçu	
Octets :	16 690	12 302	
Paquets :	203	62	
Paquets ignorés :	0	0	
Octets/seconde :	0	0	
Paquets/seconde :	0	0	

- Configuration de la carte réseau créer avec l'IP Bonding

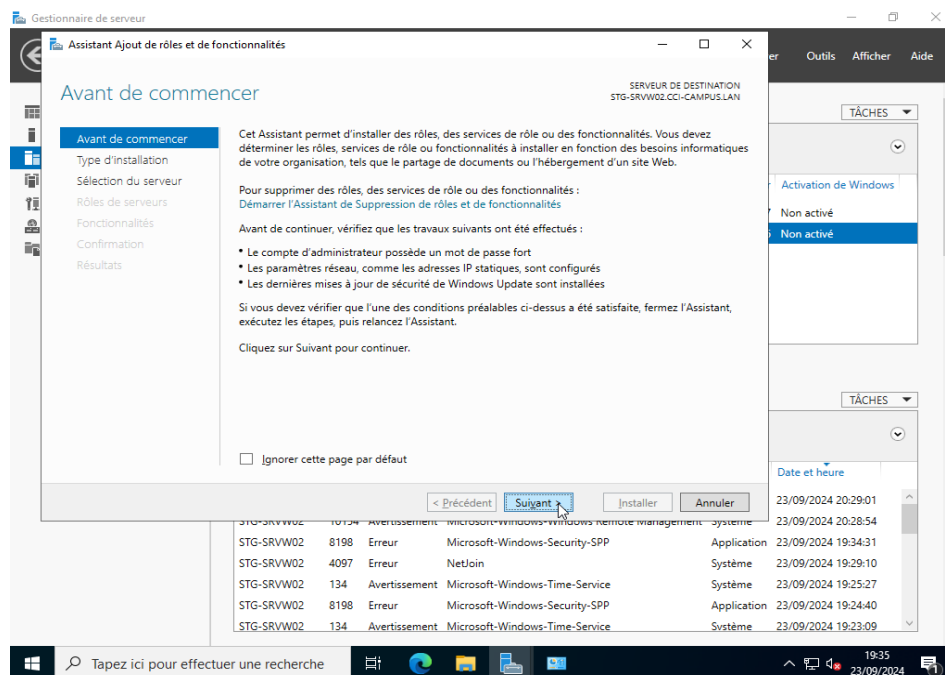


Installation de l'AD

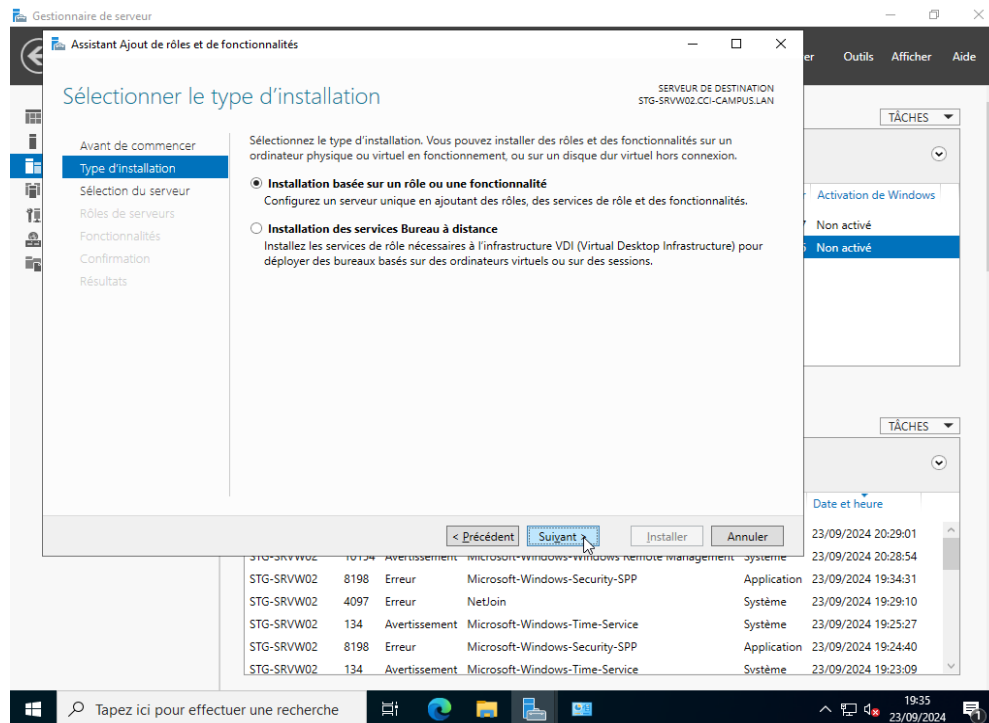
- Cliquer sur **ajout des rôles et fonctionnalités**



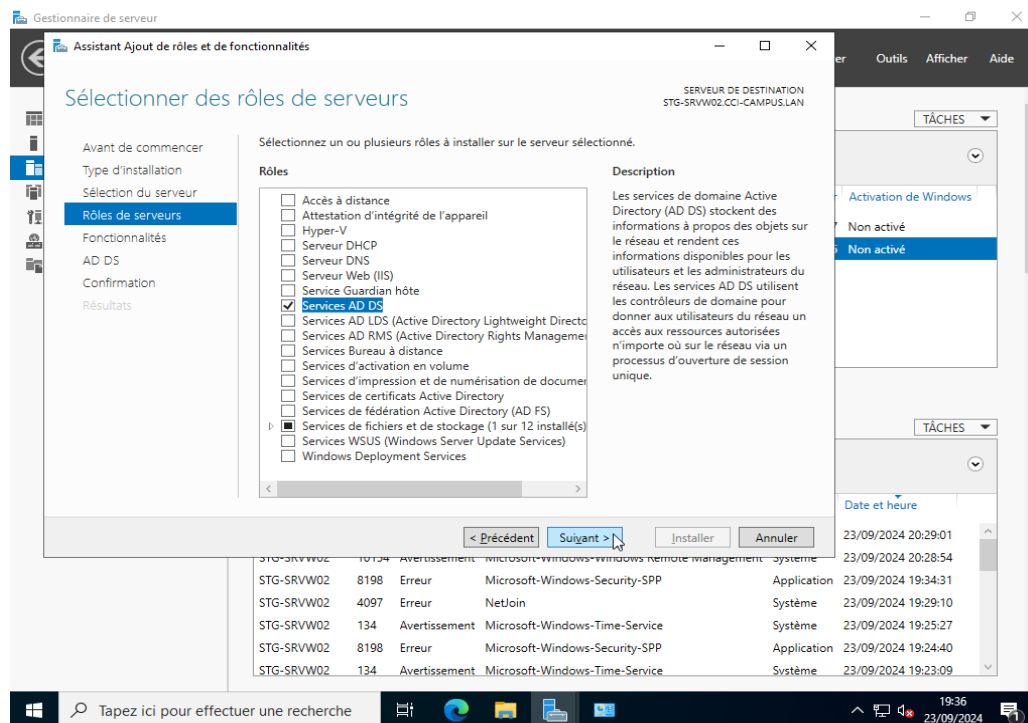
- Puis cliquer sur **suivant**



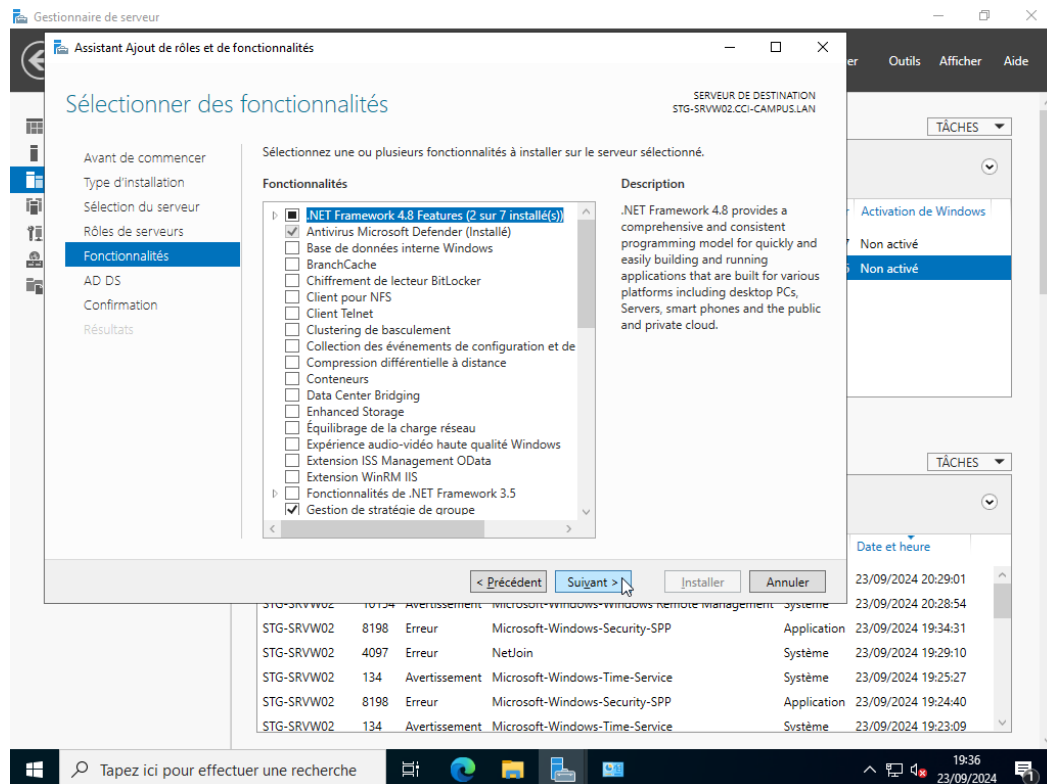
- Encore sur **suivant**



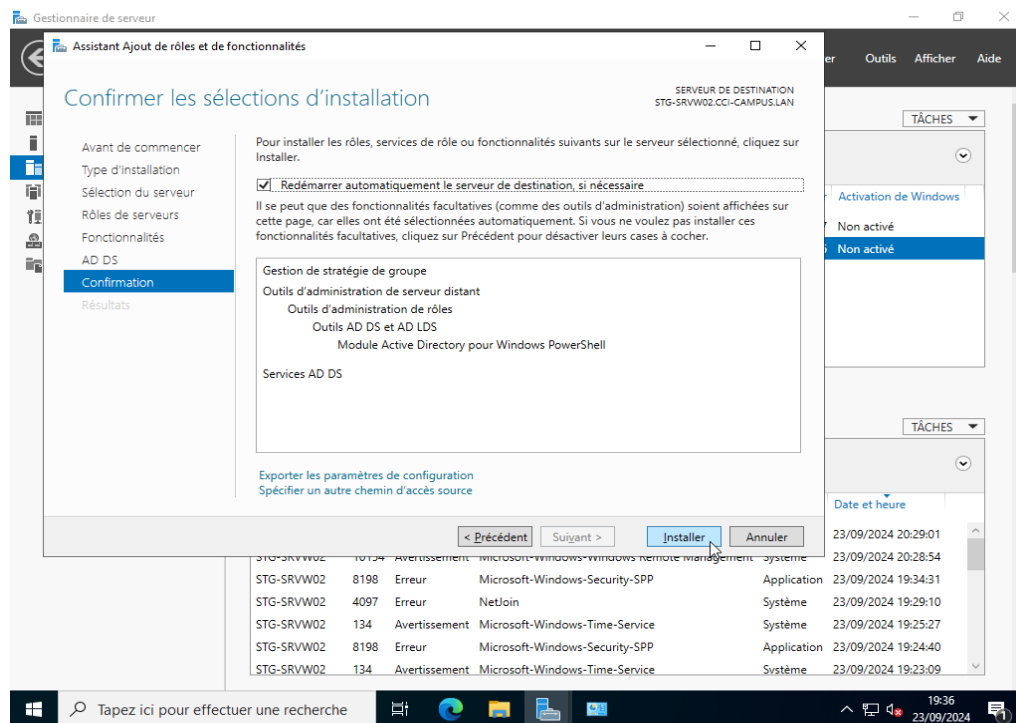
- Sélectionner **Services AD DS**



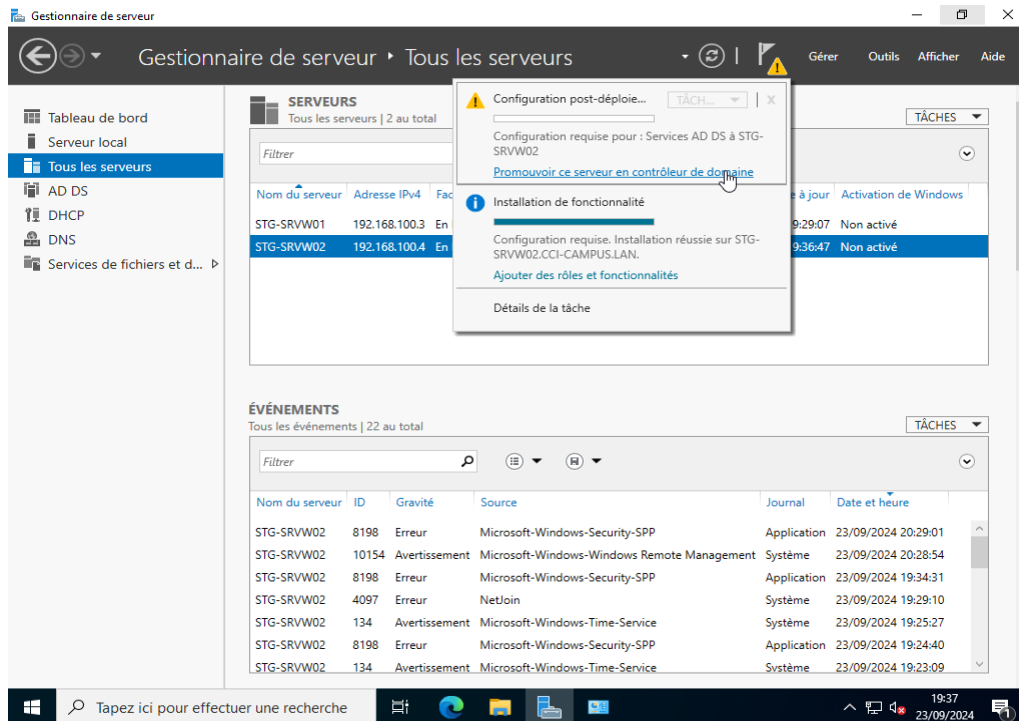
- Cliquer sur **suivant**



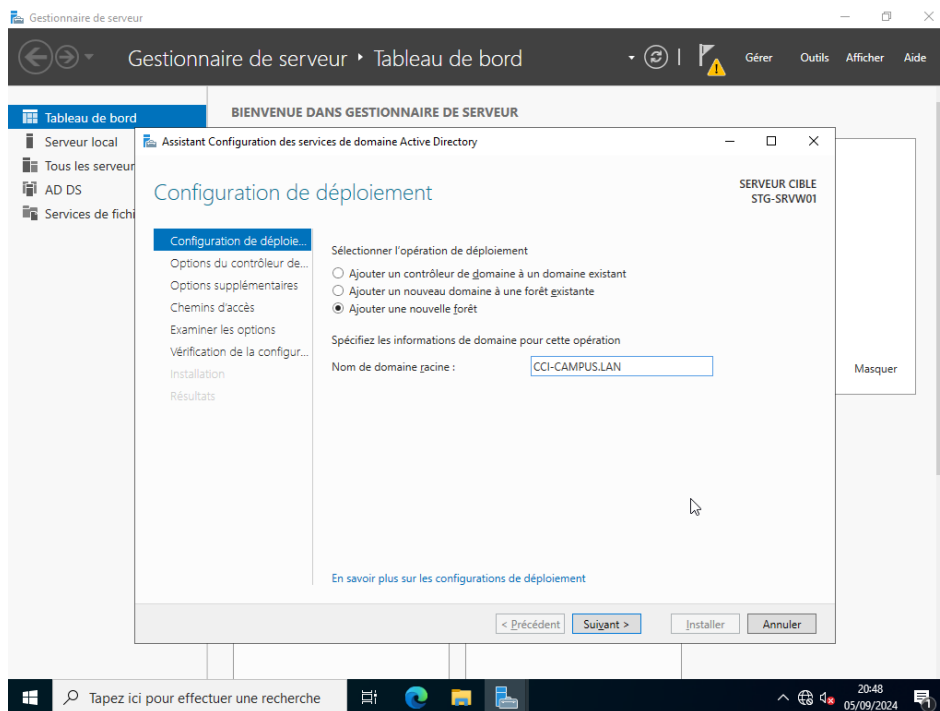
- Installer le rôle



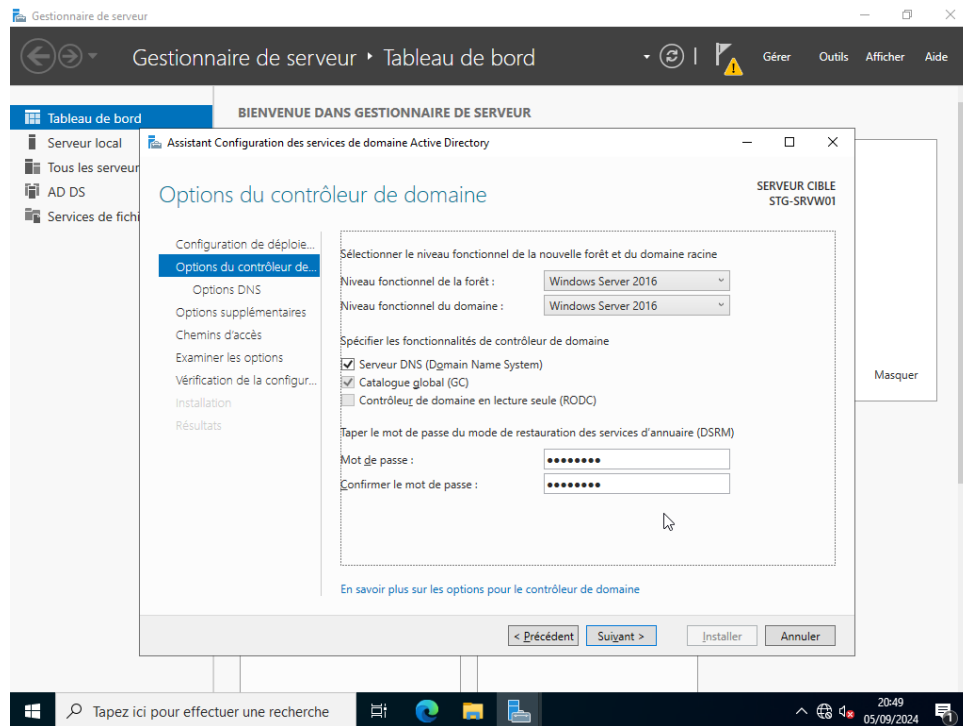
- Ensuite, cliquer sur le drapeau en haut à droite, puis sur **Promouvoir ce serveur en contrôleur de domaine**



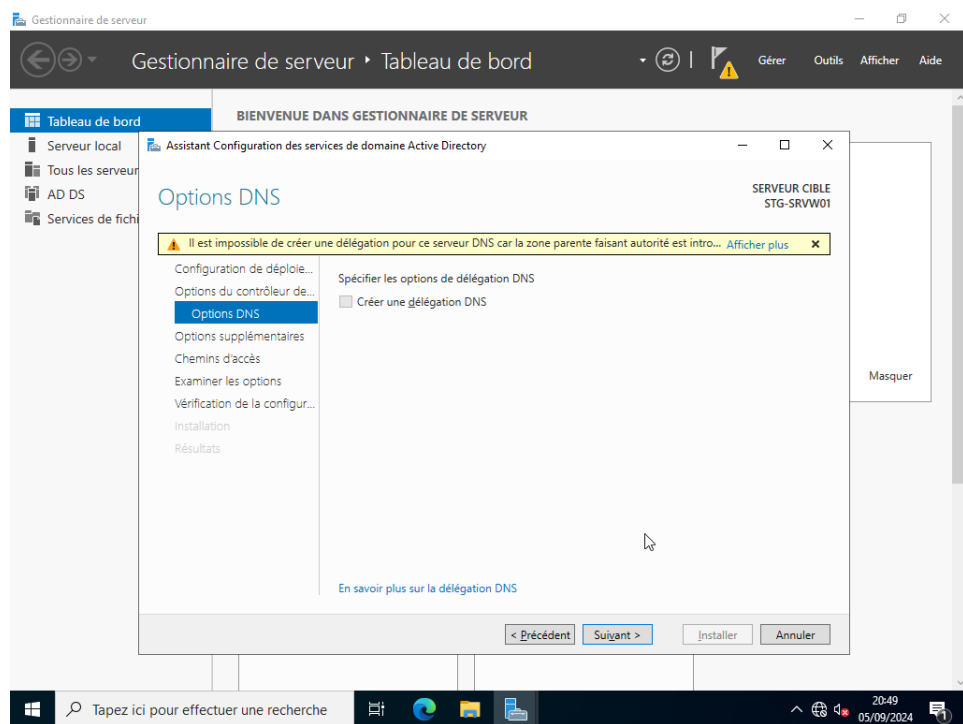
- Spécifier le nom du domaine

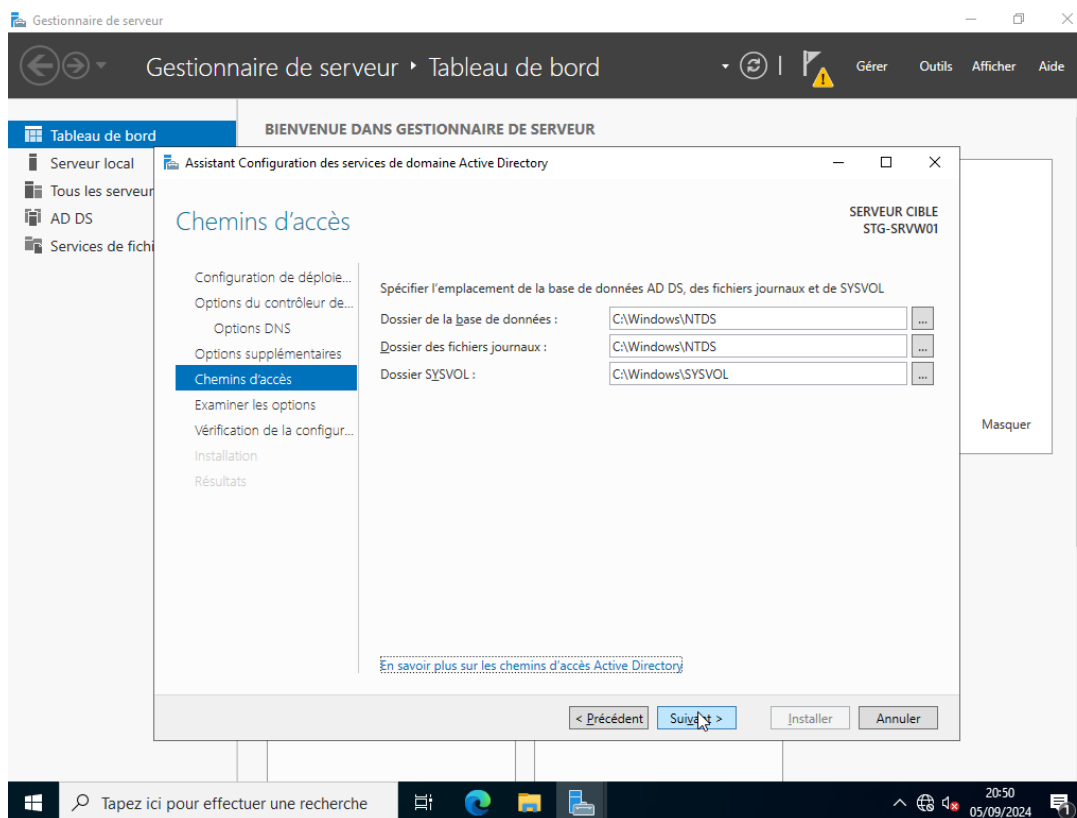
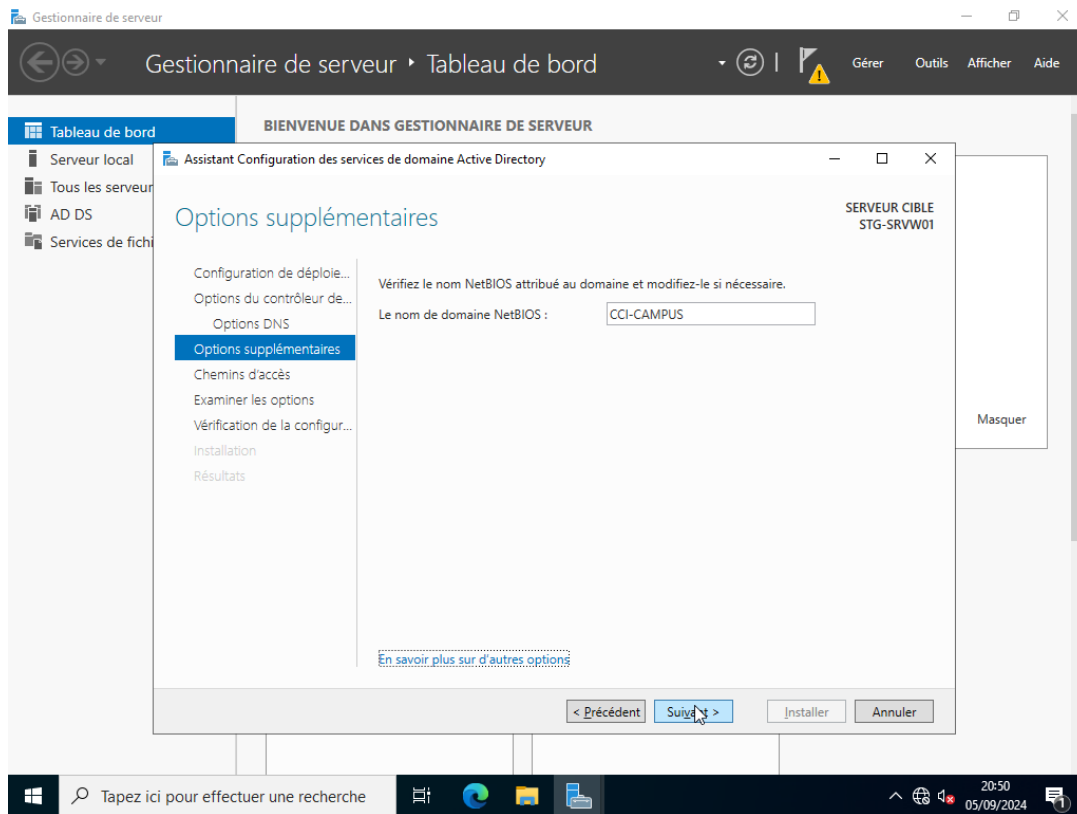


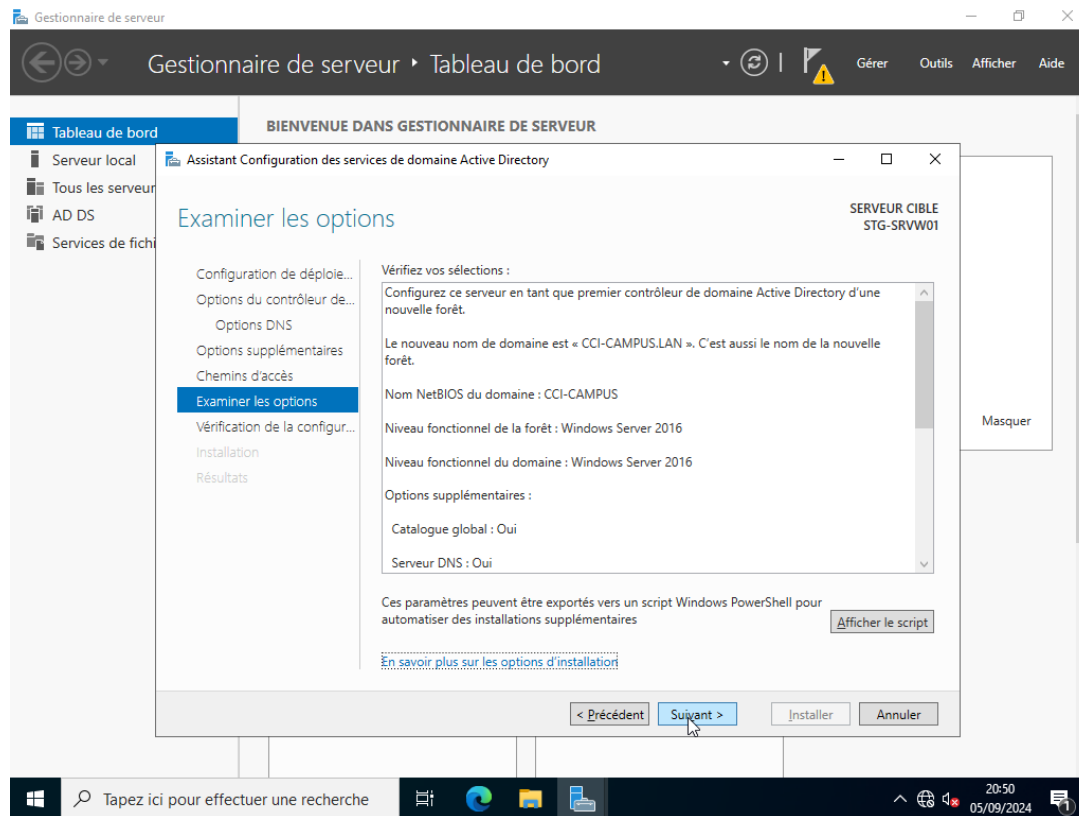
- Renter un mot de passe de restauration



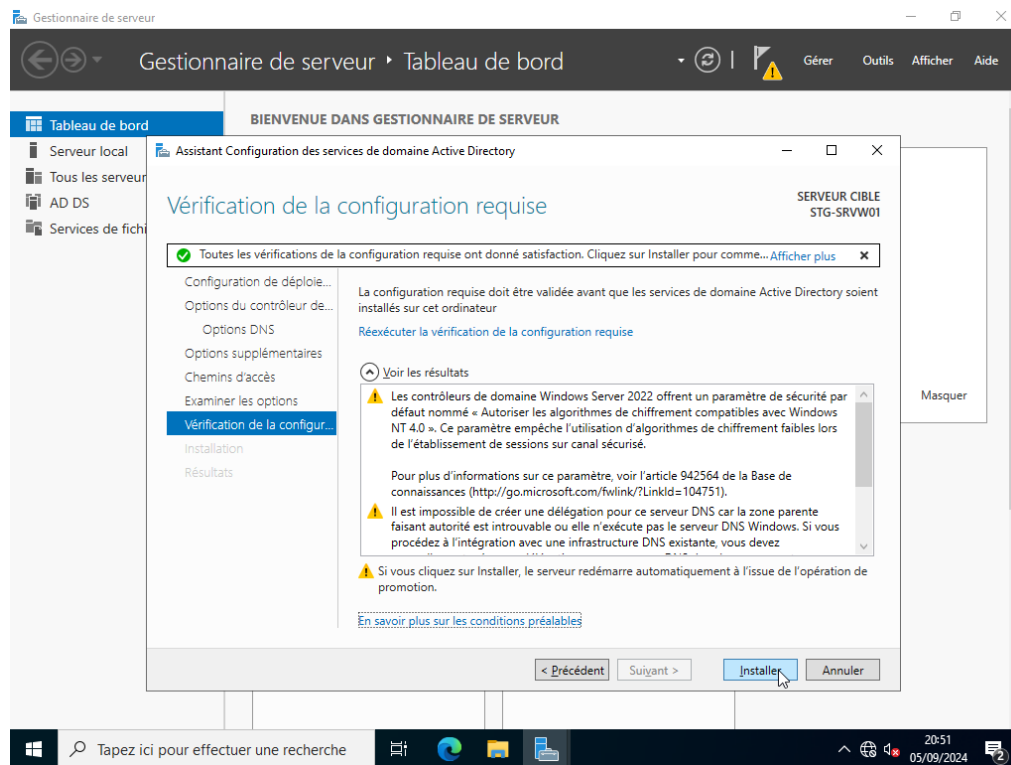
- Cliquer sur **suivant**



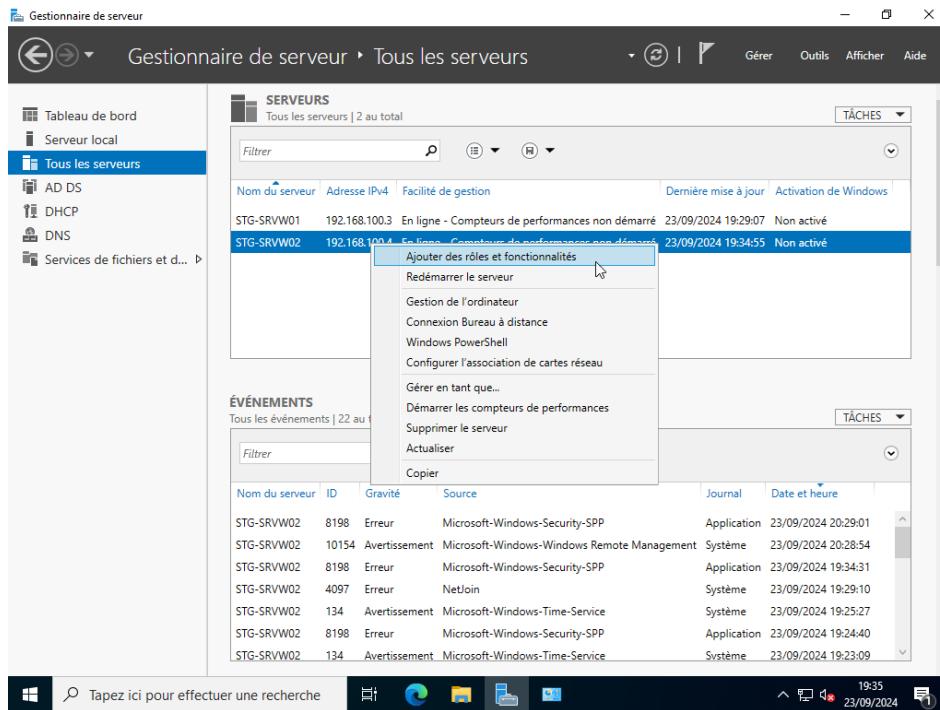




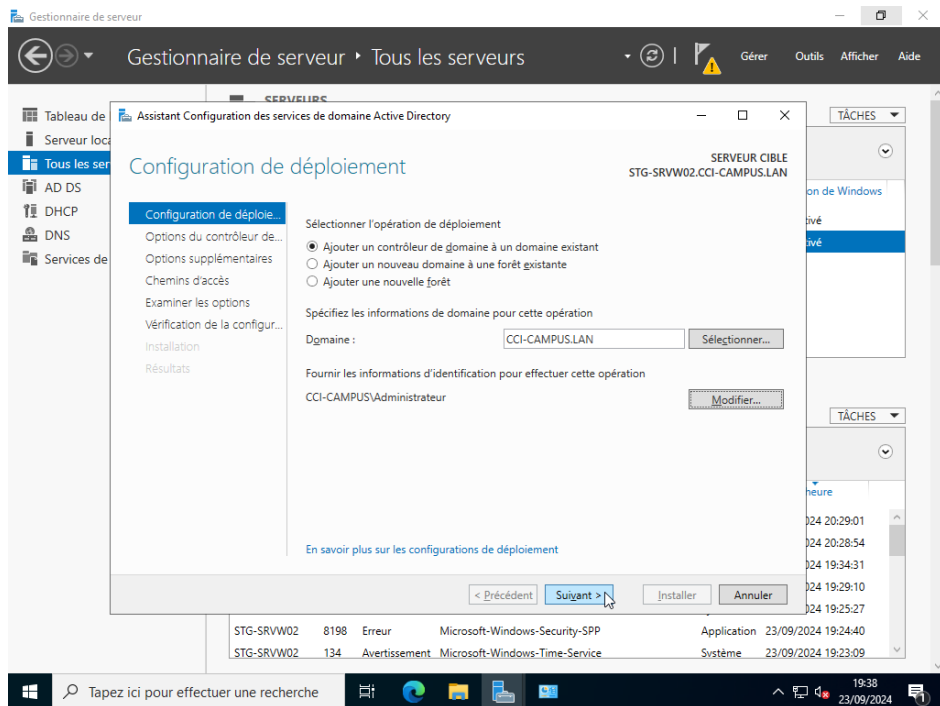
- Puis installer



- Le rôle AD DS est maintenant installé et configuré en tant que contrôleur de domaine principale sur le STG-SRVW01
- Faire de même sur le serveur secondaire

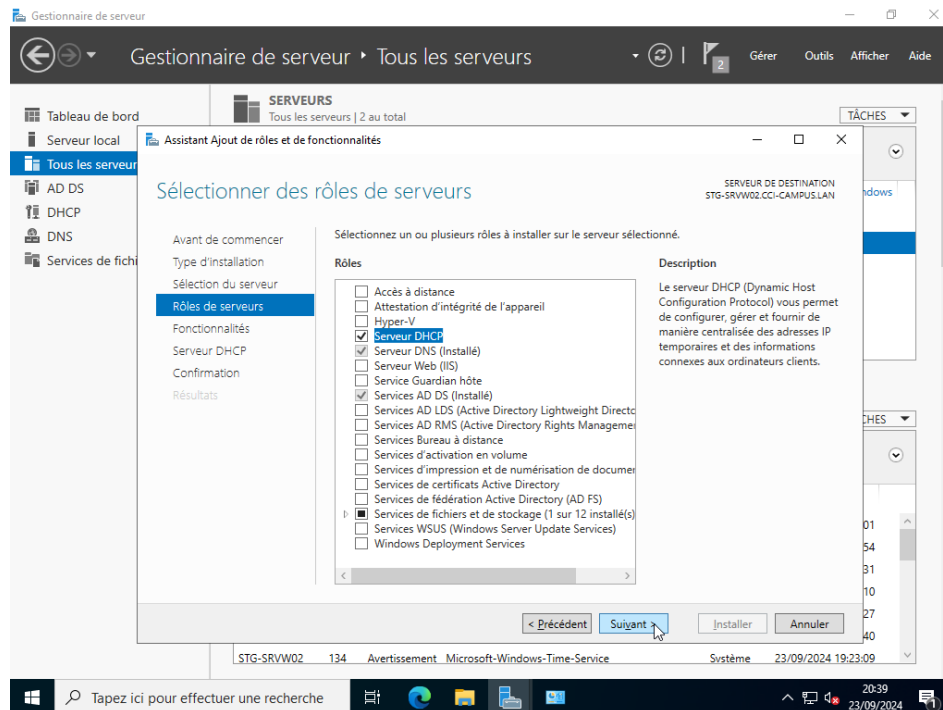


- Ajouter un contrôleur de domaine à un domaine existant

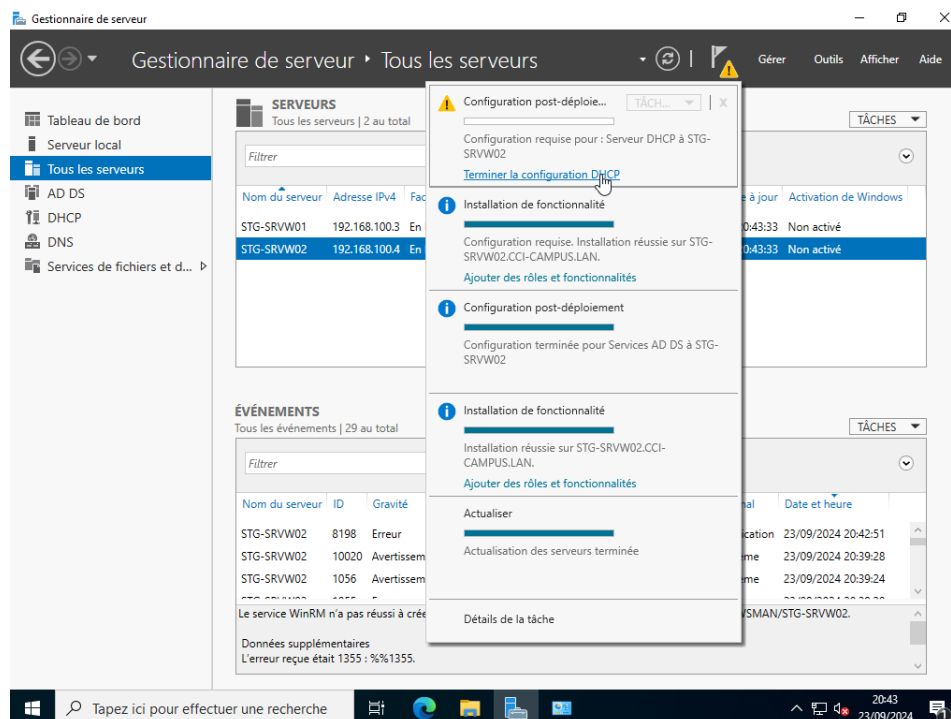


Installation du DHCP

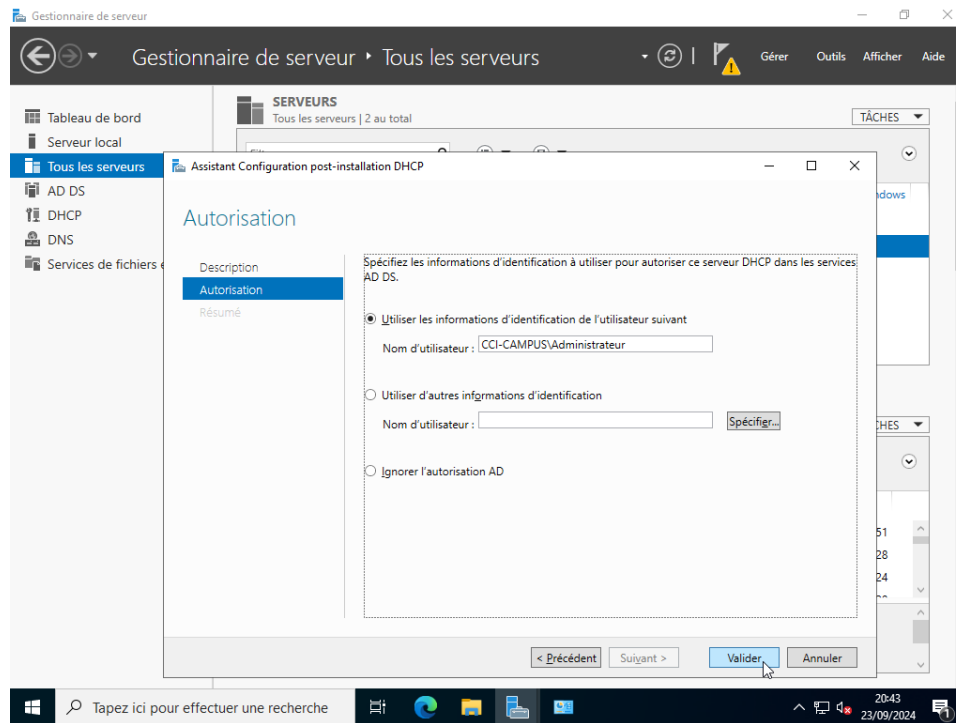
- Installer le rôle DHCP



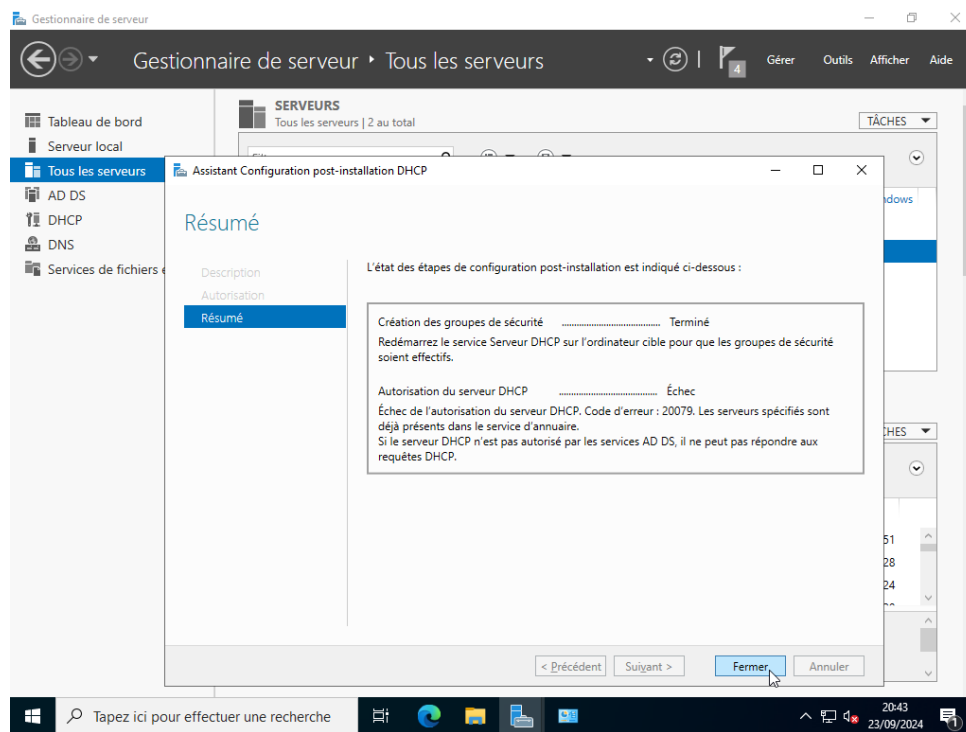
- Faire terminer la configuration DHCP



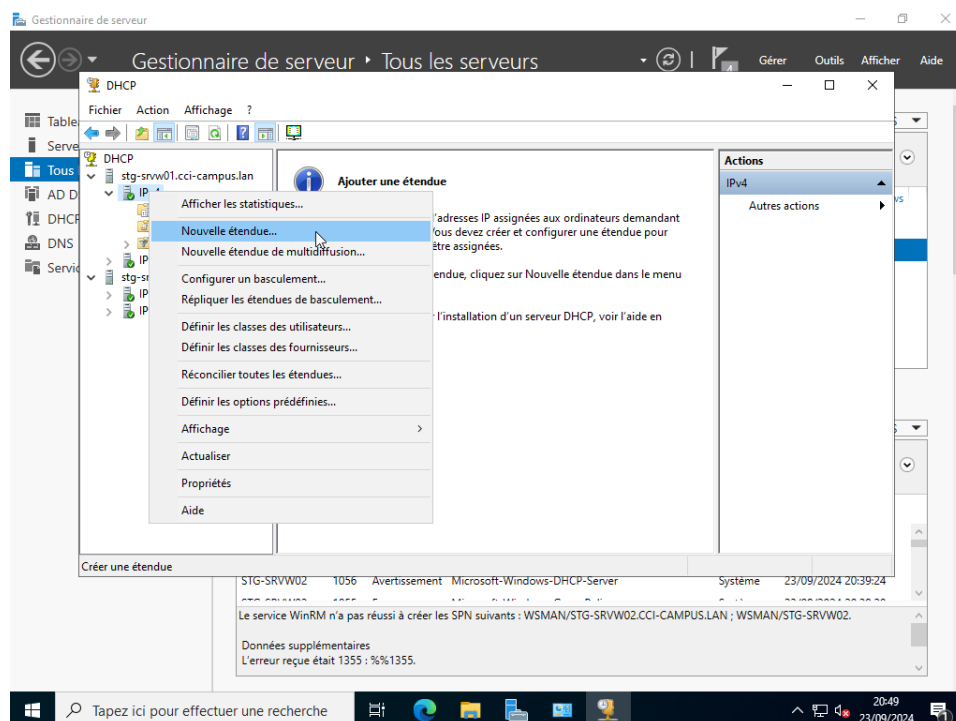
- Faire valider



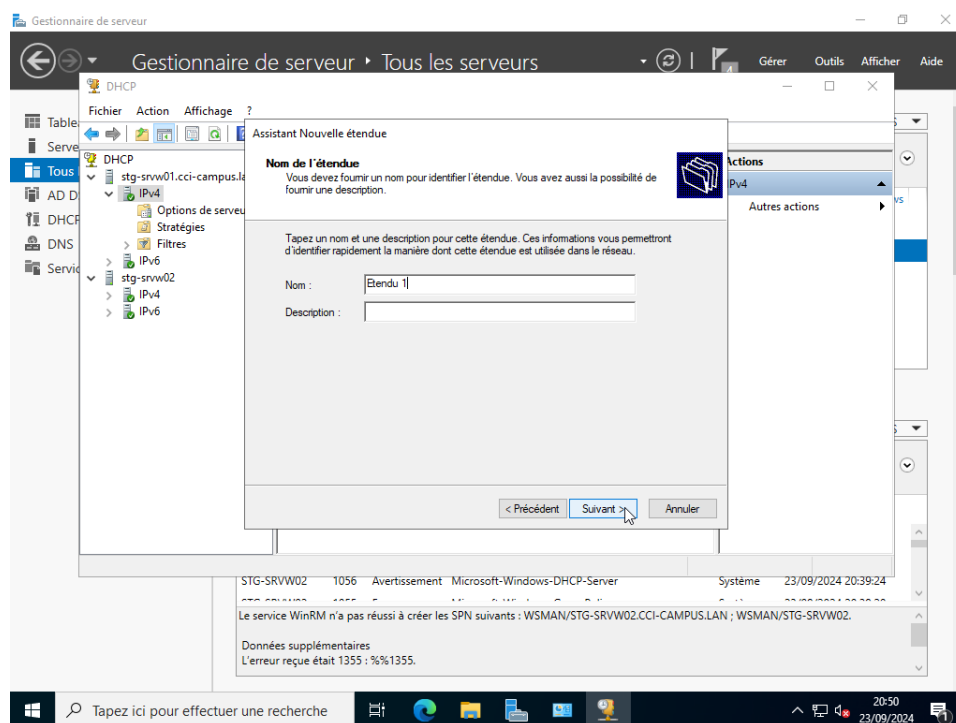
- Et fermer



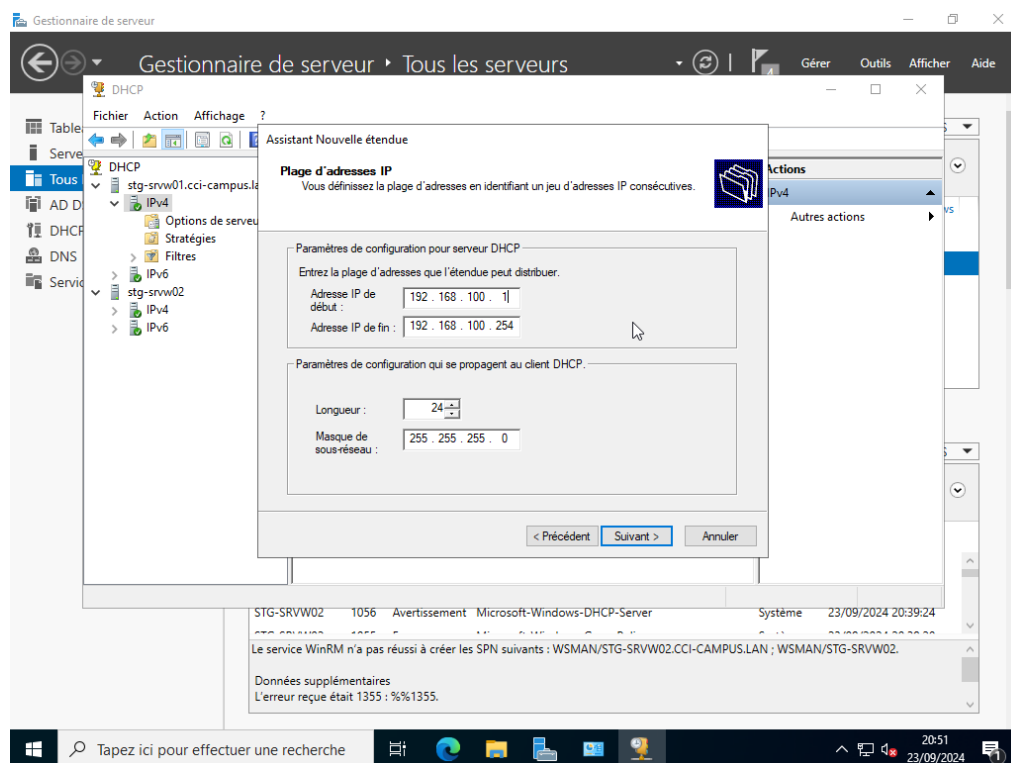
- Aller dans le **gestionnaire DHCP** et **configurer une nouvelle étendue**



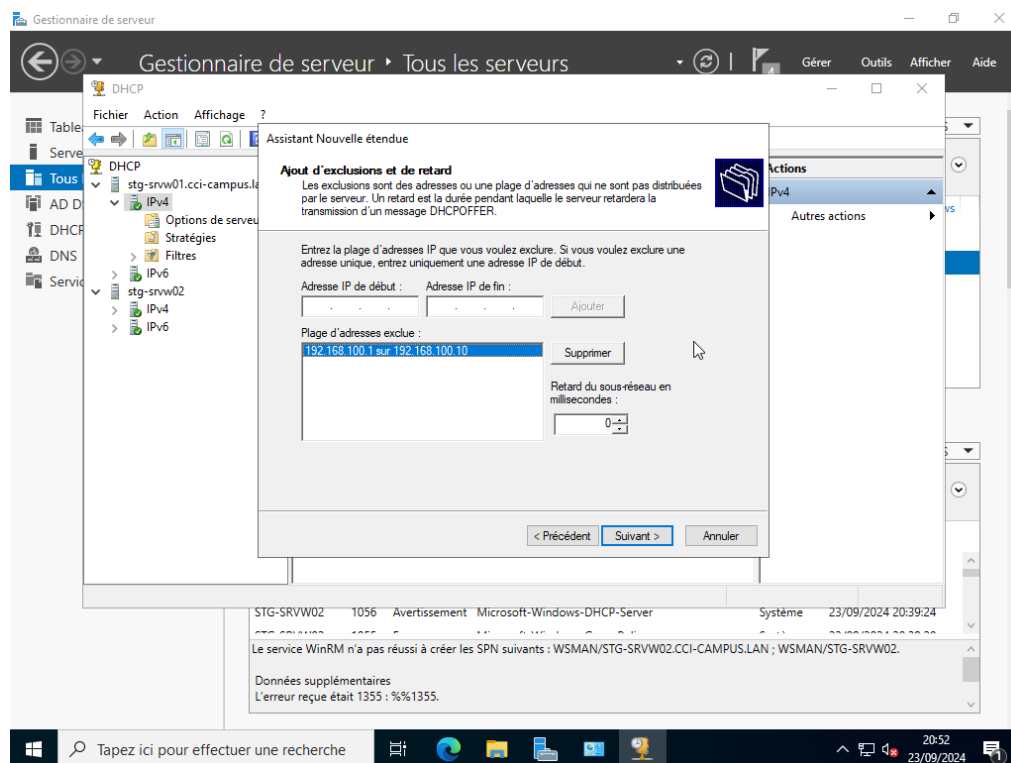
- Mettre un nom à l'étendue



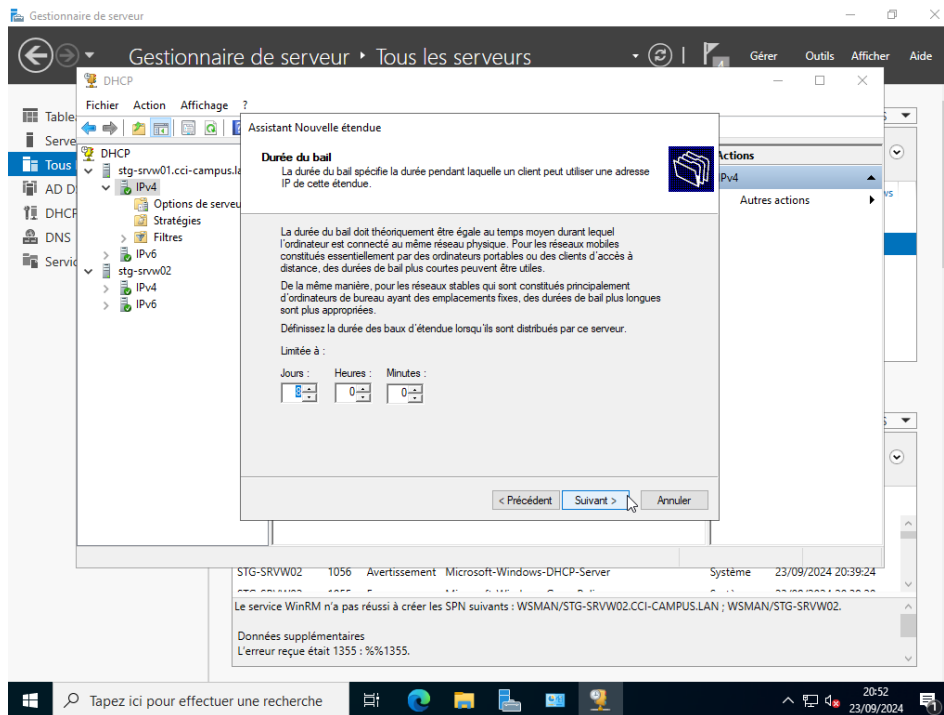
- Configurer une plage d'adresse IP



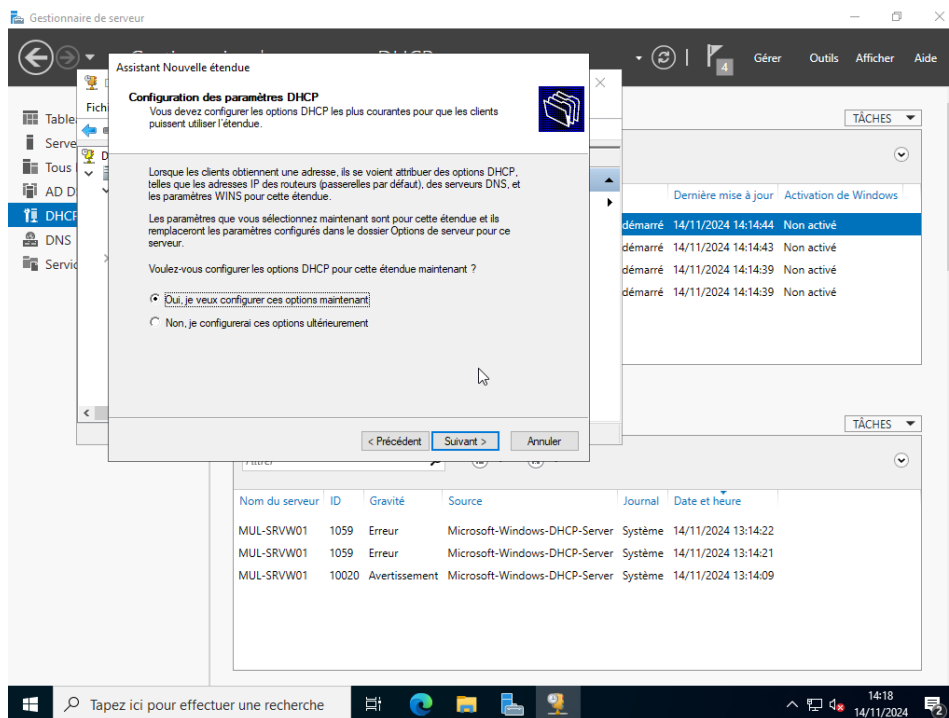
- Sélectionner une plage d'exclusion



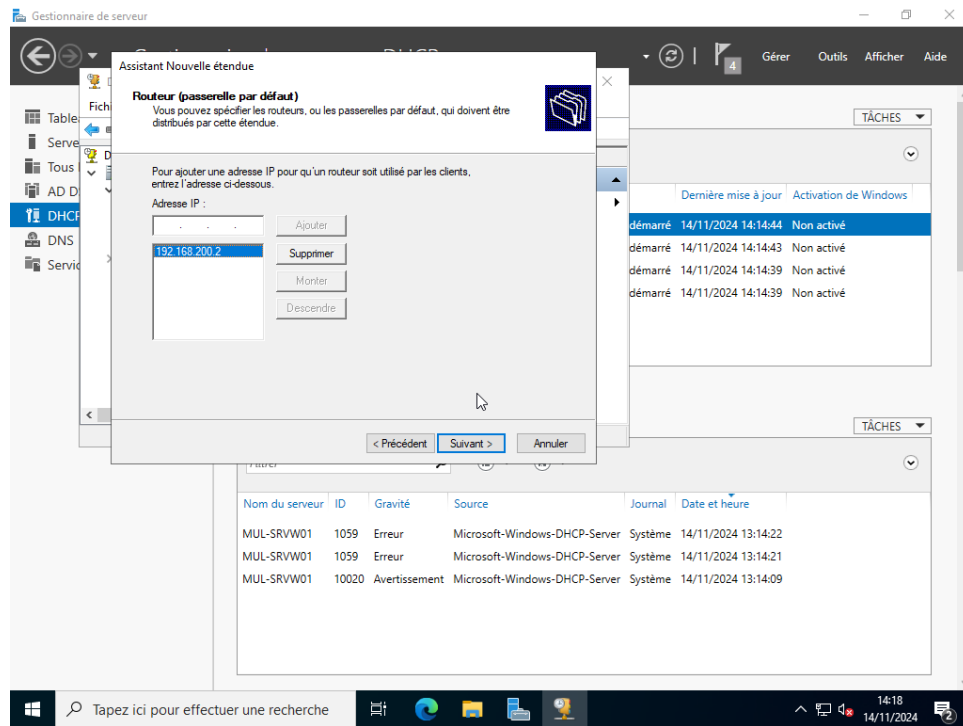
- Sélectionner la durée du bail



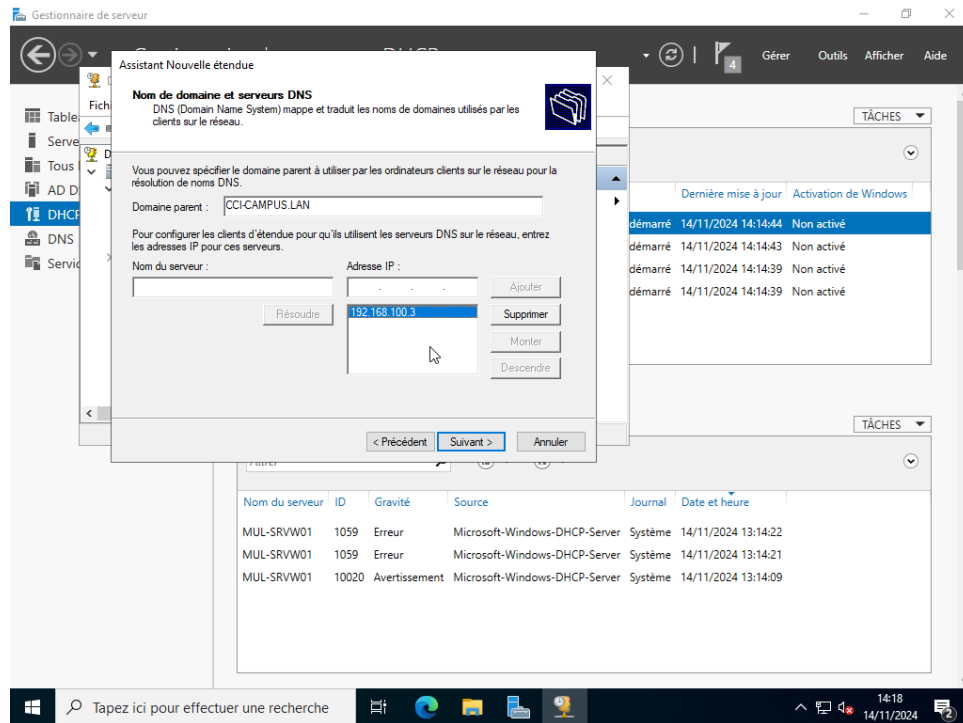
- Configurer maintenant



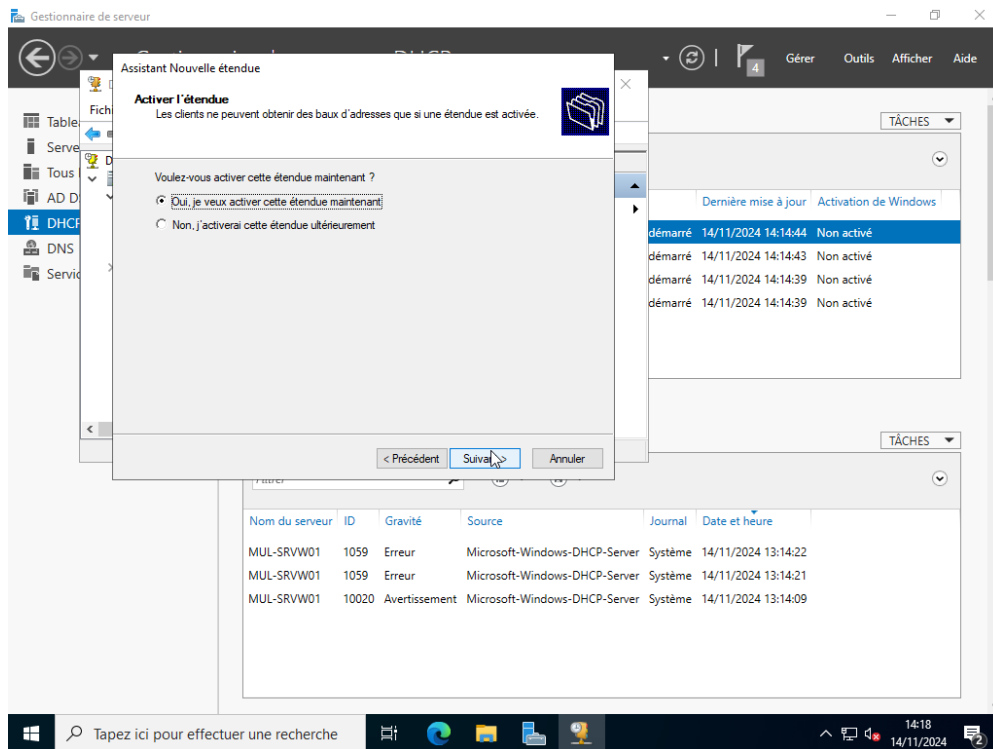
- Ajouter le routeur



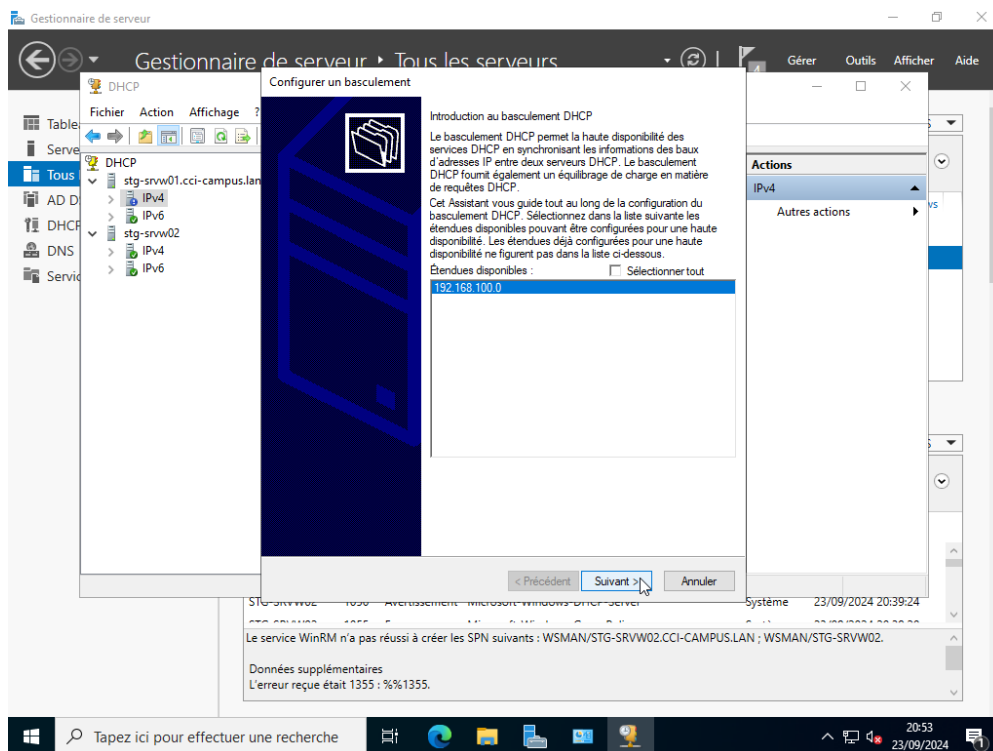
- Ajouter le serveur DNS qui est le serveur principale



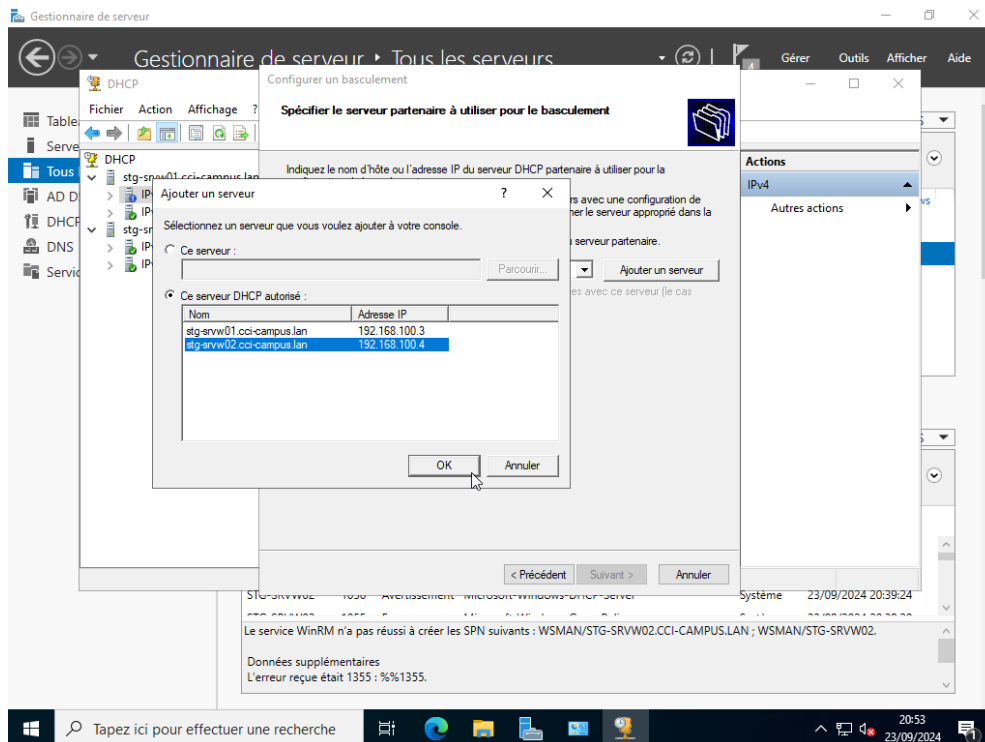
- Activer l'étendue



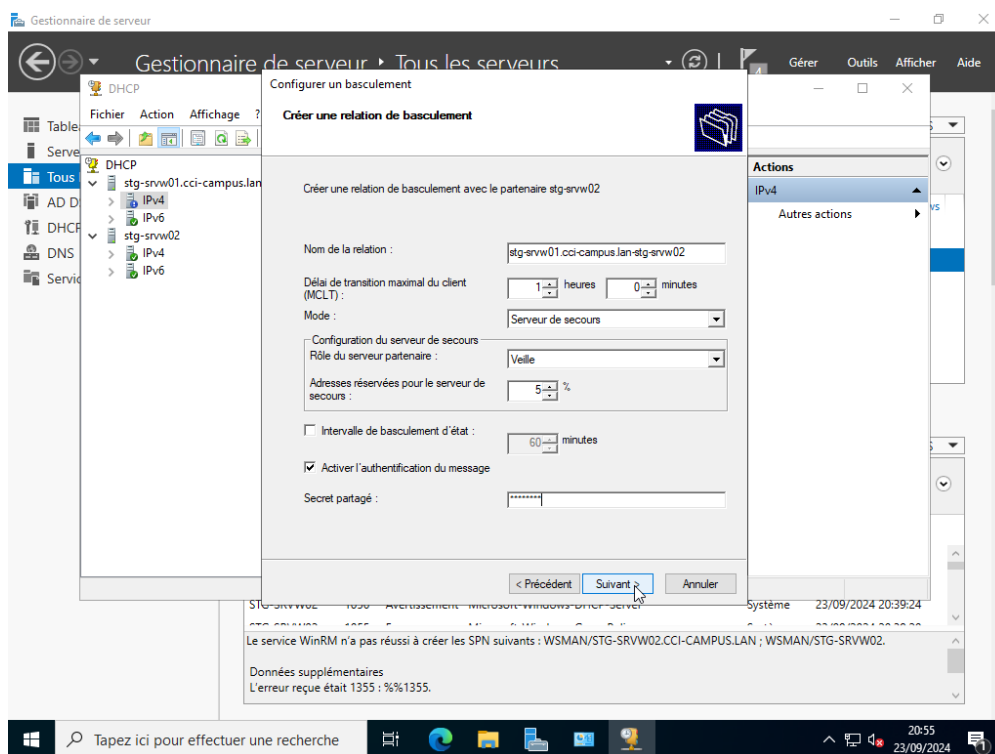
- Ensuite configurer un basculement sur l'étendue qui vient d'être créée



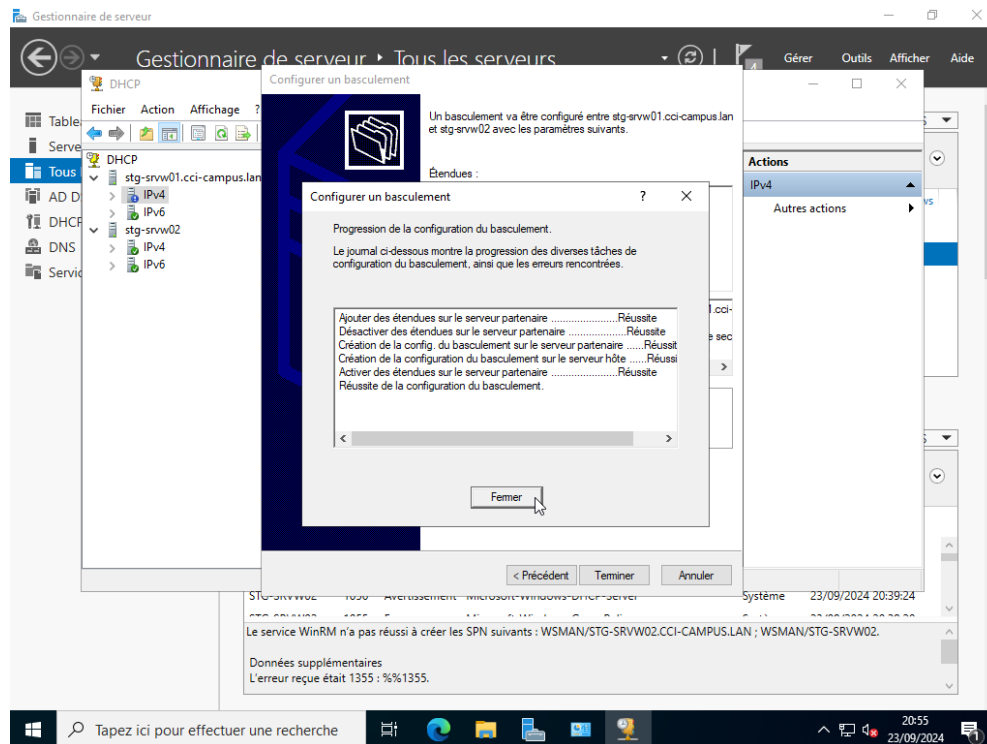
- Sélectionner le serveur DHCP



- Configurer la relation de basculement, mettre en mode serveur de secours



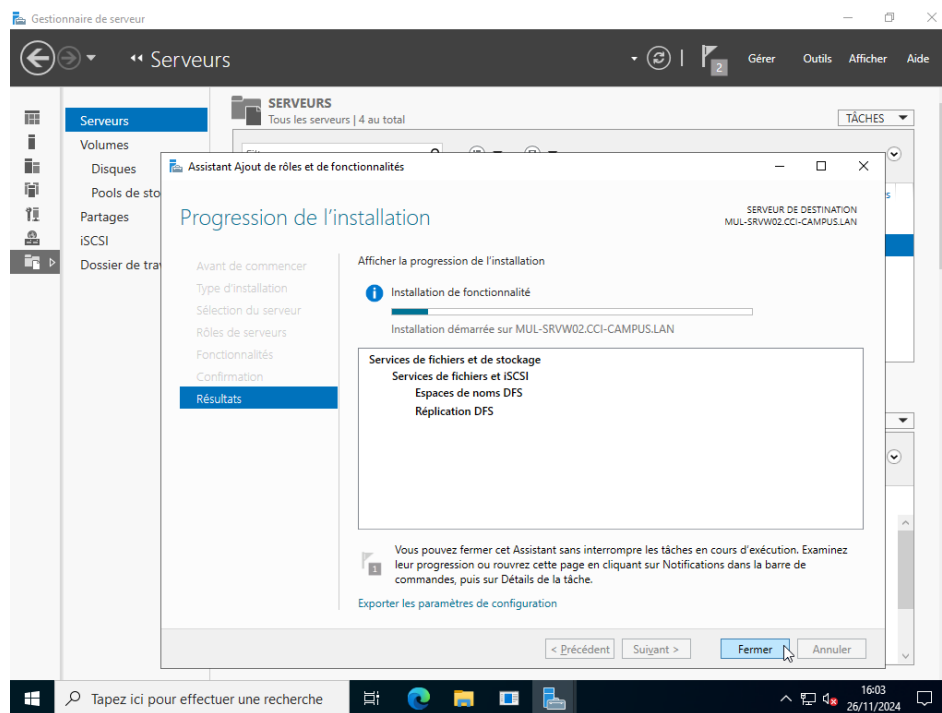
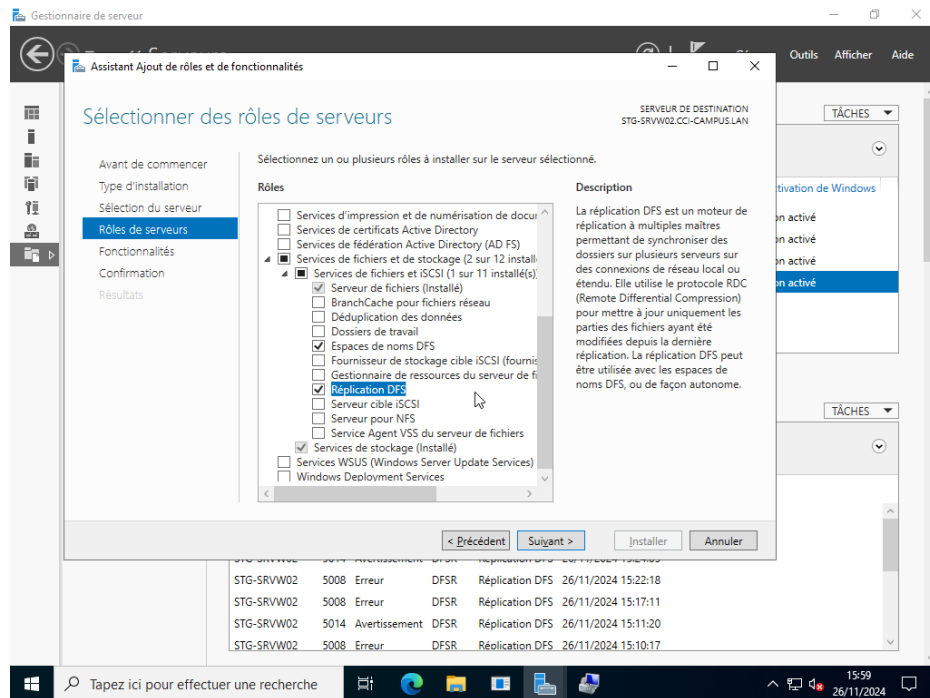
- Puis terminer



- Faire de même pour les autres serveurs en modifiant les adresses IP en conséquence

Installation et configuration de DFS/R

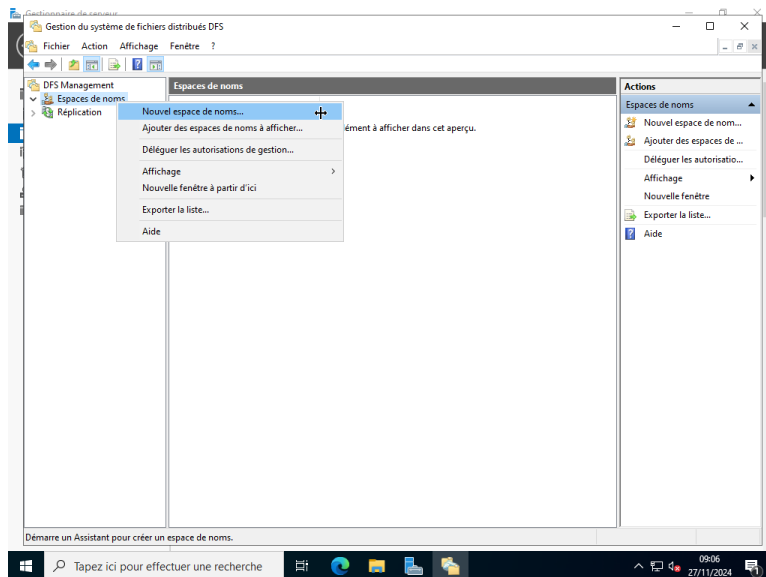
- Installation des rôles **Espaces de noms DFS** et **Réplication DFS** sur les différents serveurs



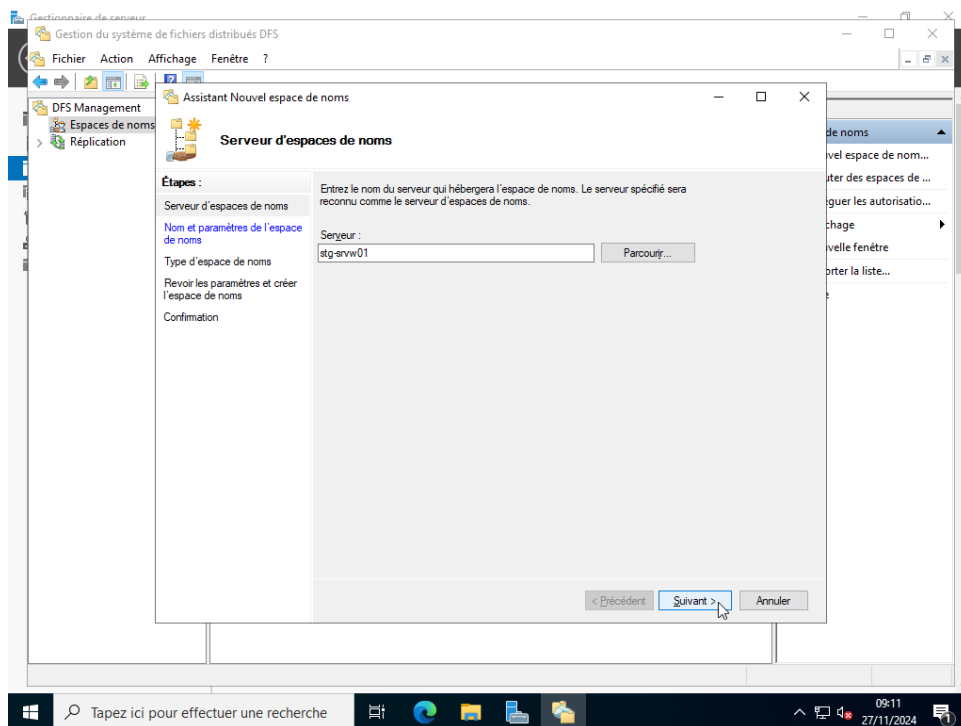
Création du partage

- Se rendre dans le menu **outils** dans le gestionnaire de serveur et aller dans **Gestion du système de fichiers distribués DFS**

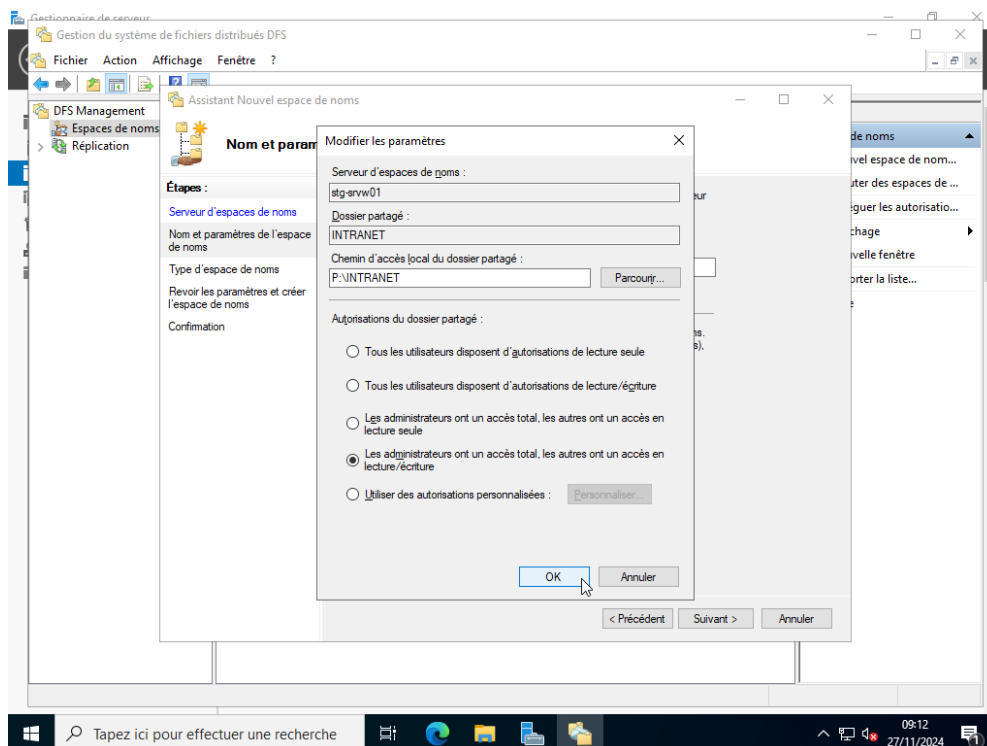
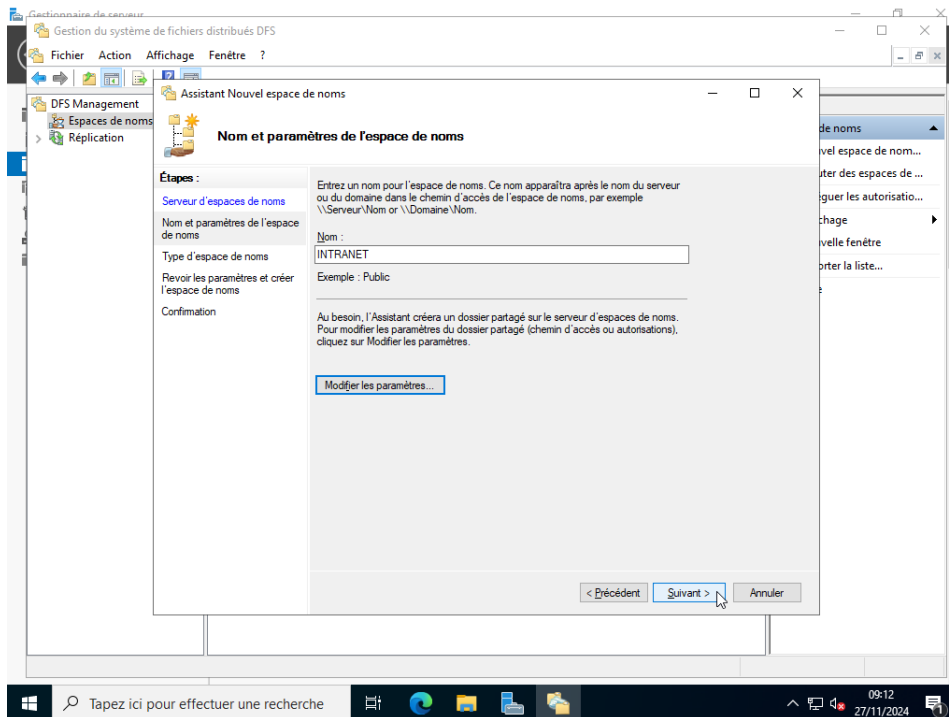
- Sur le menu **Espaces de noms** faire un clique droit et créer un nouvel espace de noms



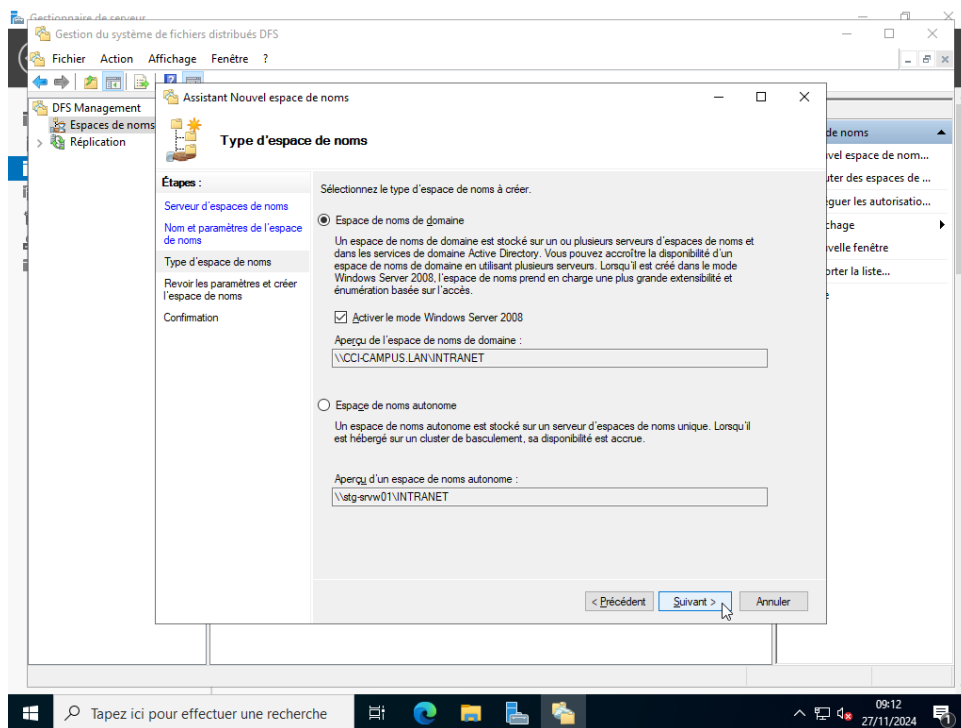
- Sélectionner le serveur qui hébergera les fichiers



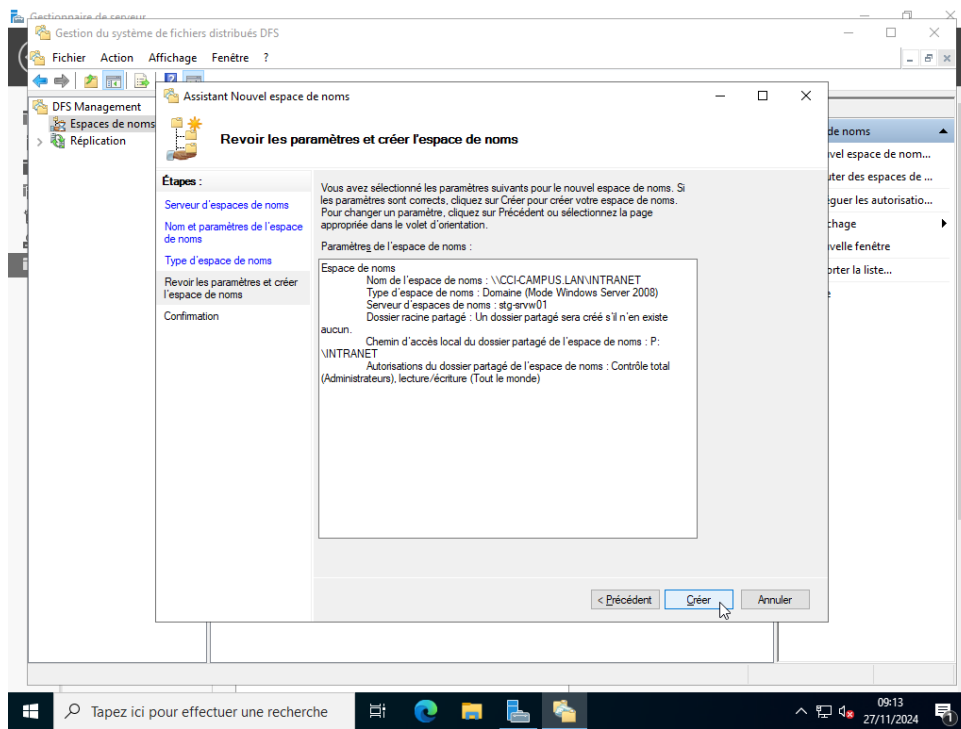
- L'espace de nom s'appelle ici **INTRANET**. Sélectionner la case autorisant l'accès total aux administrateurs et l'accès lecture/écriture aux autres en accédant aux paramètres



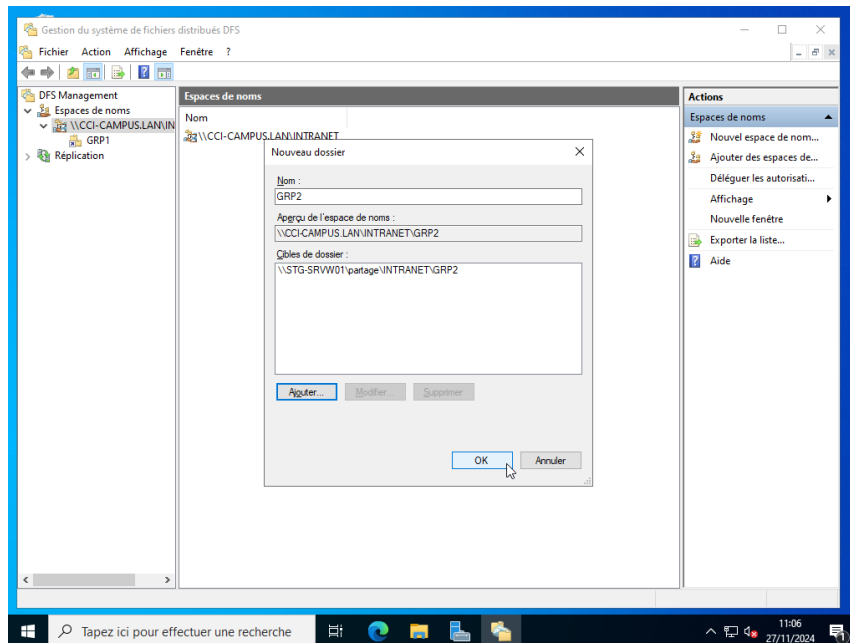
- Sélectionner **espace de noms de domaine**



- Créer l'espace de noms



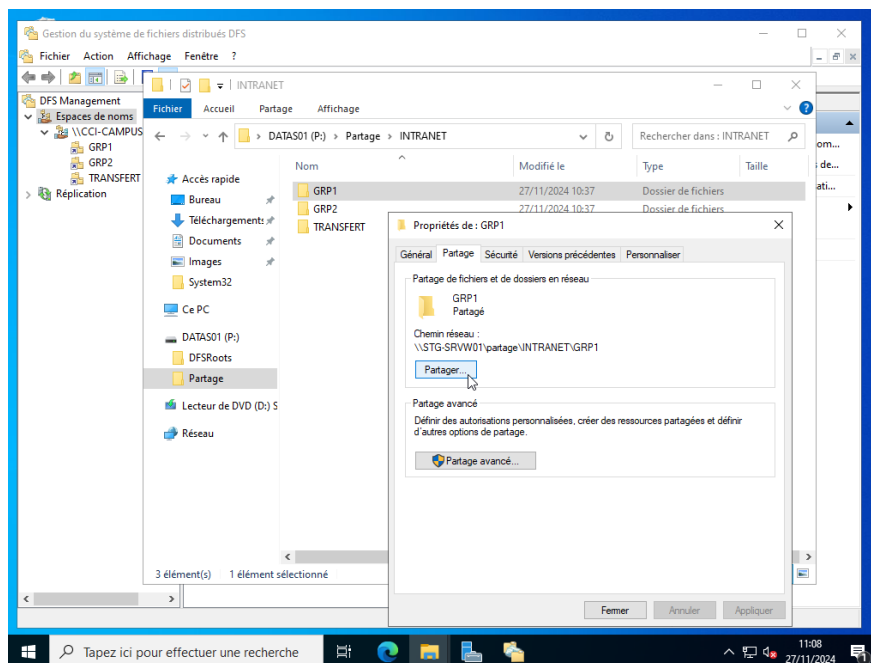
- Une fois l'espace de noms créer, ajouter un nouveau dossier en faisant un clic droit sur l'espace de noms. Ajouter un nom au dossier puis sélectionner la cible (l'endroit où est stocké le dossier)



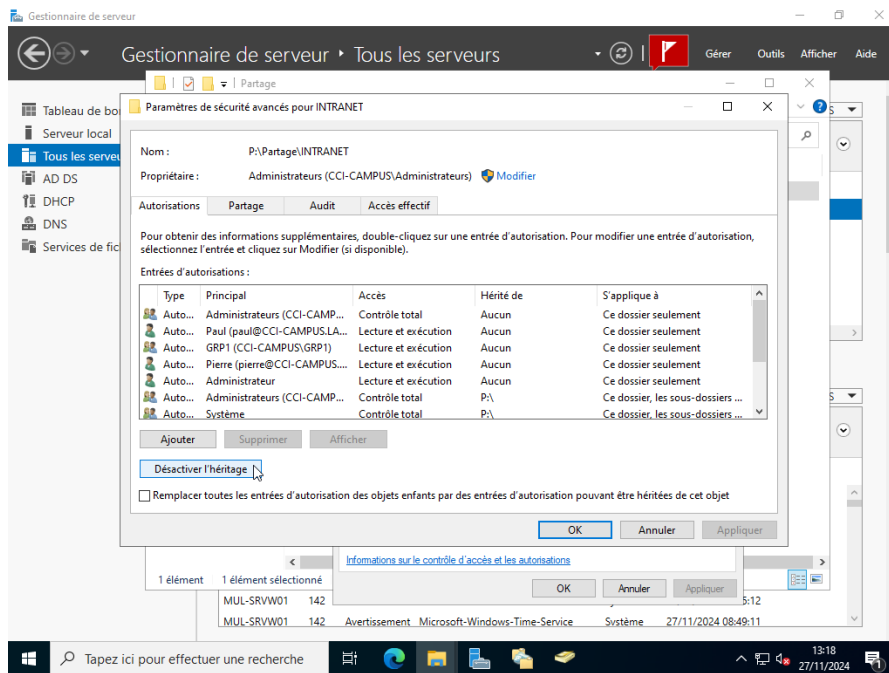
Ta mère

Mise en place des droits sur les dossiers

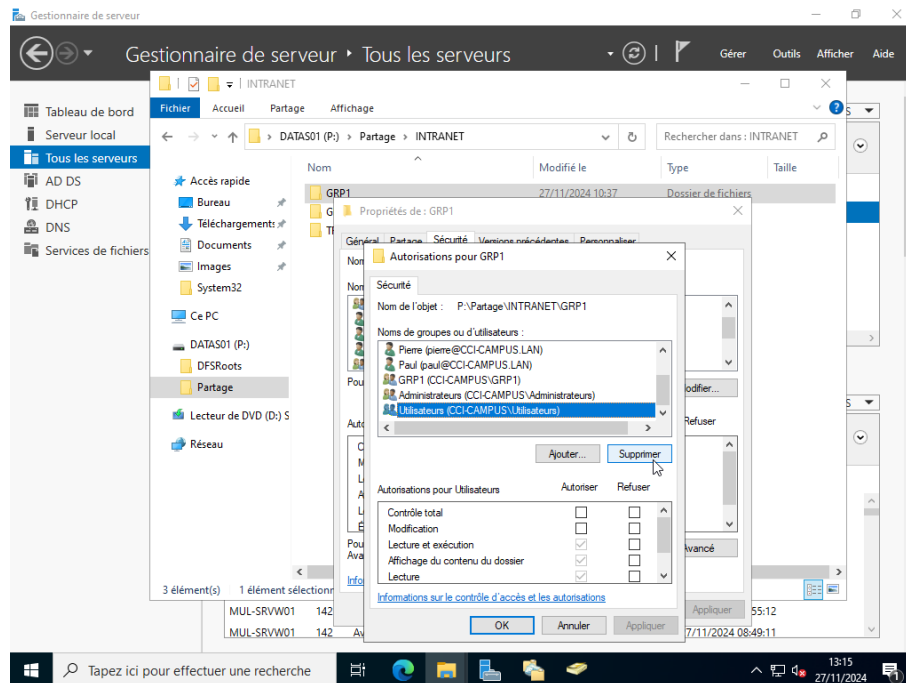
- Aller dans le répertoire où se trouve les dossiers. Dans les **propriétés** se rendre dans l'onglet **partage** puis **partage avancé**



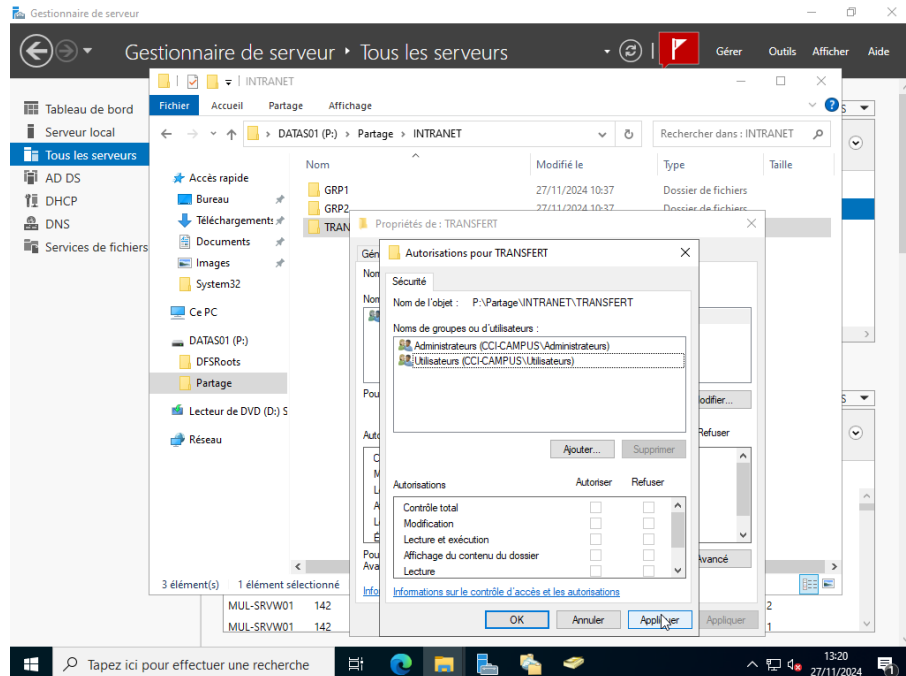
- Désactivé l'héritage



- Ensuite aller dans l'onglet **sécurité** puis supprimer l'accès à tous les utilisateurs et ajouter l'accès total aux administrateurs et en lecture/écriture aux ayant droit donc dans l'exemple au groupe 1. Faire la même chose pour le dossier **GRP2** et adapter les droits pour les répertoires personnels

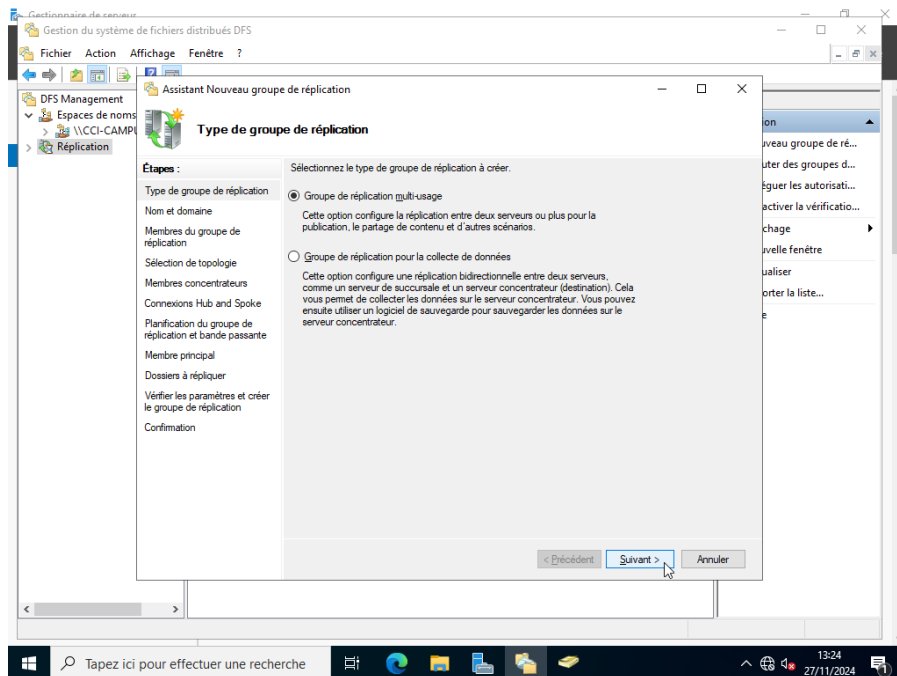


- Pour le dossier **TRANSFERT**, ajouter l'accès total aux administrateurs et en lecture/écriture pour tous les autres utilisateurs

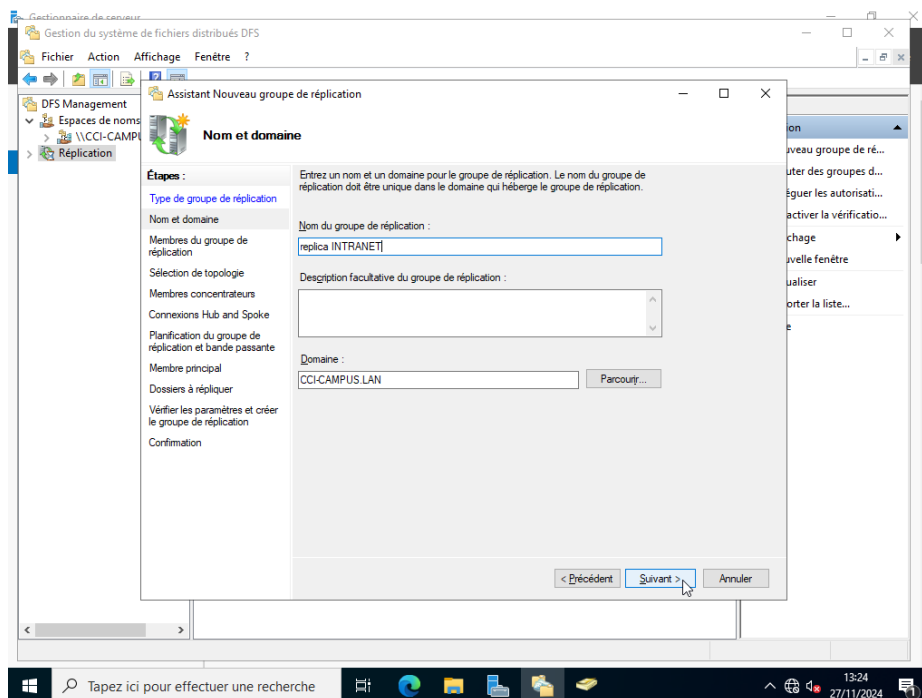


Réplication des données

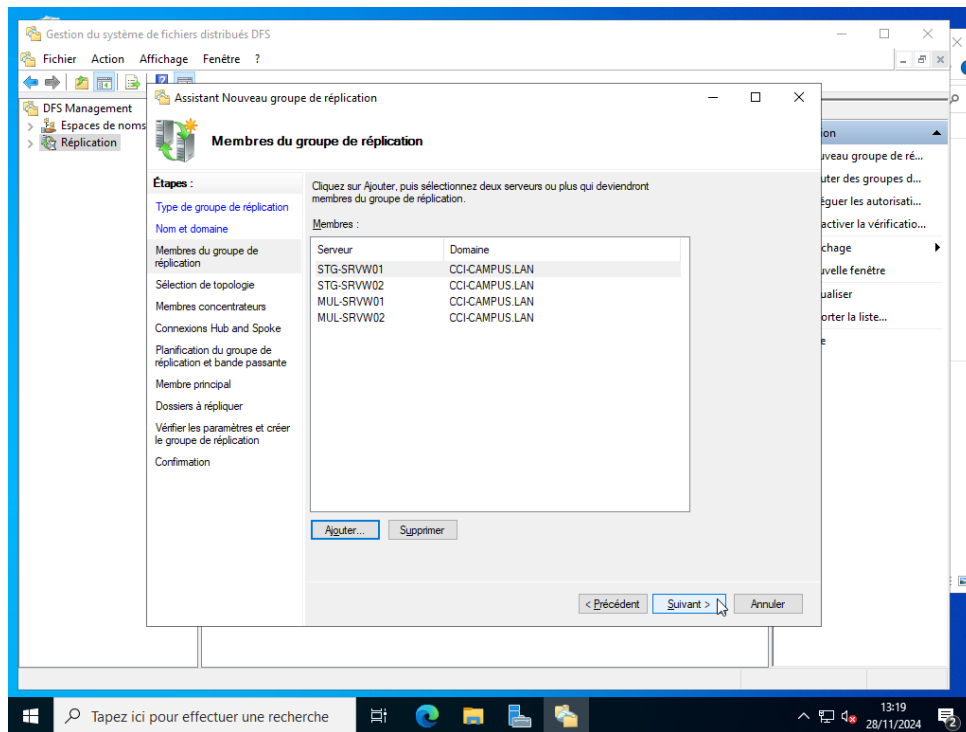
- Faire un clic droit sur réplication puis ajouter un nouveau **groupe de réplication multi-usage**



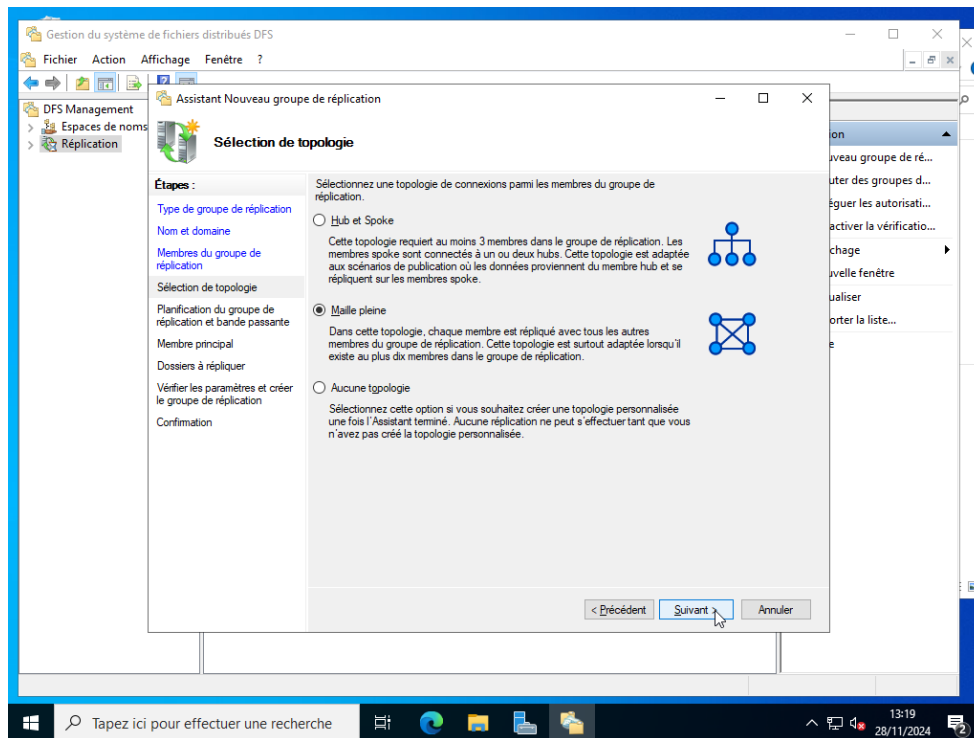
- Sélectionner le domaine



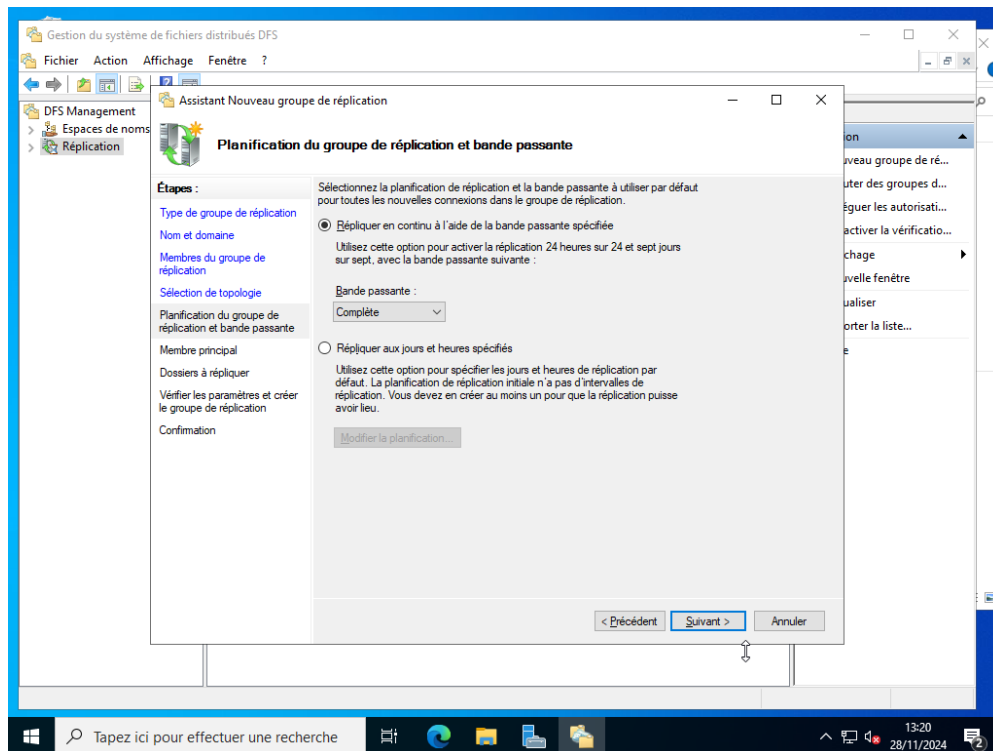
- Ajouter tous les serveurs comme membre du groupe de réplication



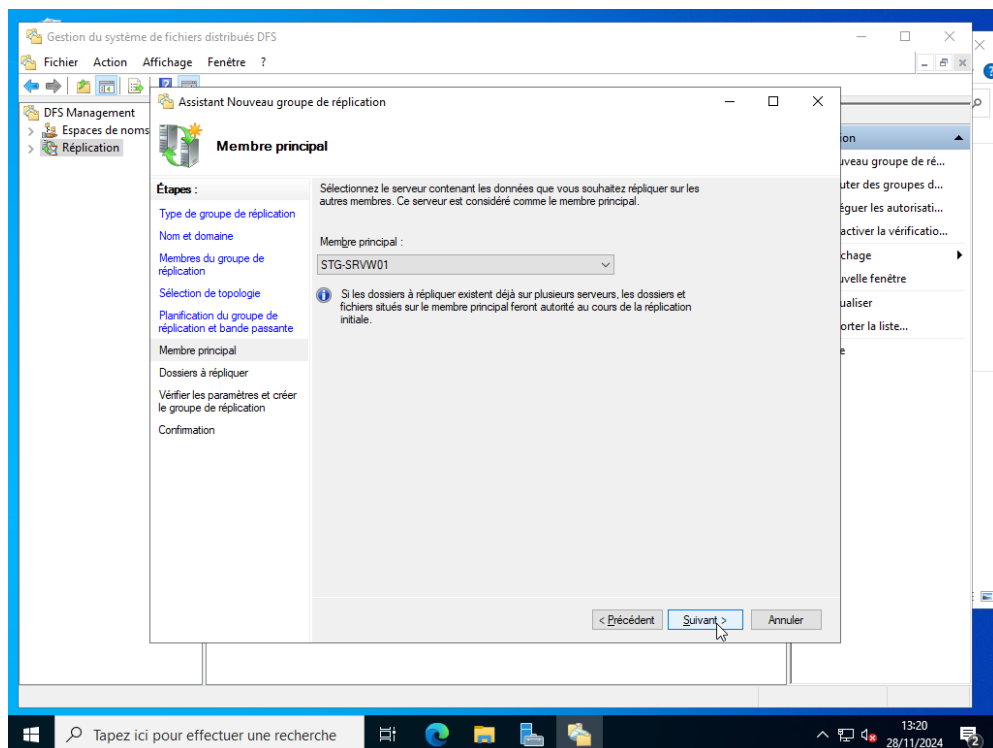
- Sélectionner **maille pleine** en topologie



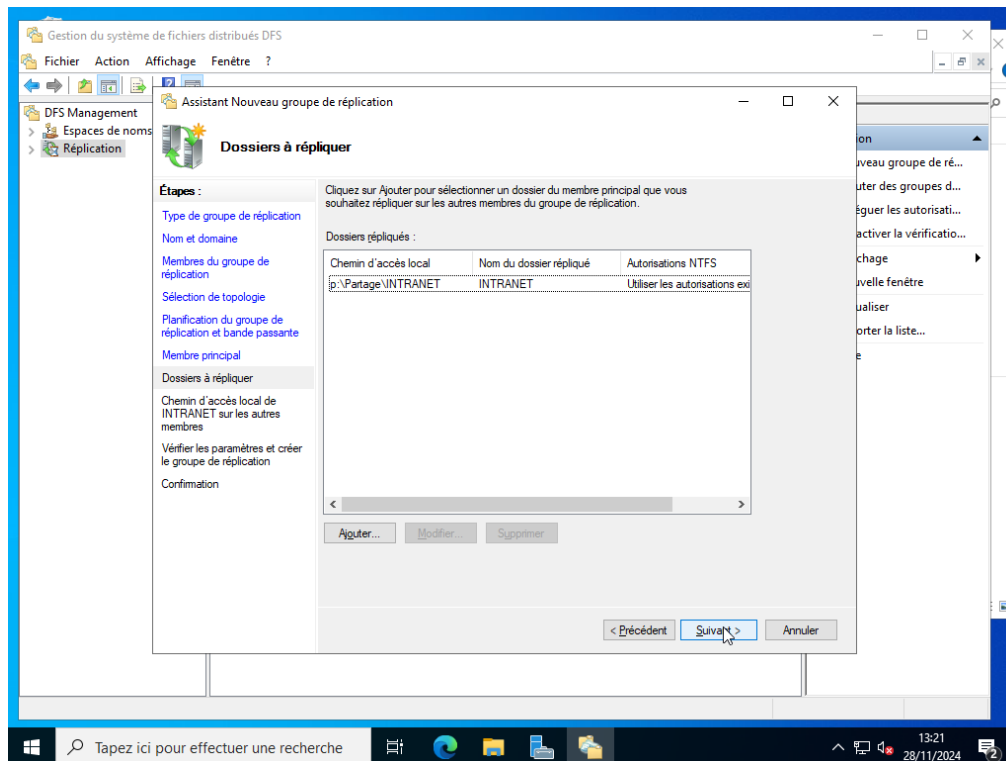
- Répliquer le contenu avec une bande passante complète



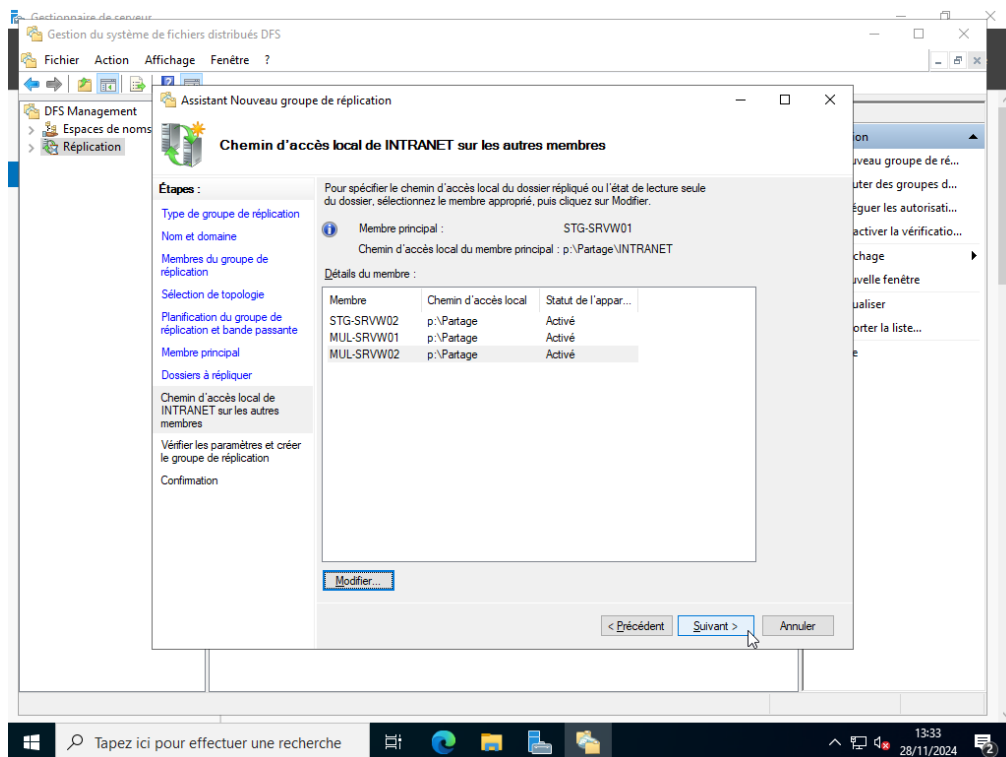
- Sélectionner le serveur principal



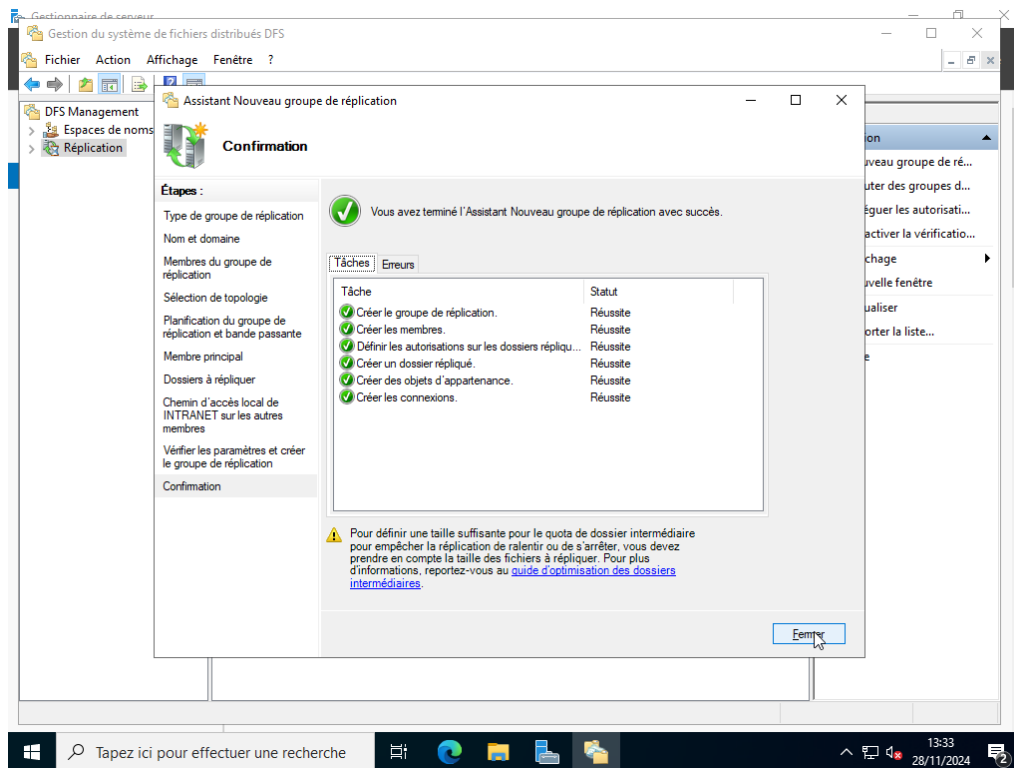
- Sélectionner le dossier **INTRANET** à répliquer



- Ajouter le chemin d'accès des autres serveurs



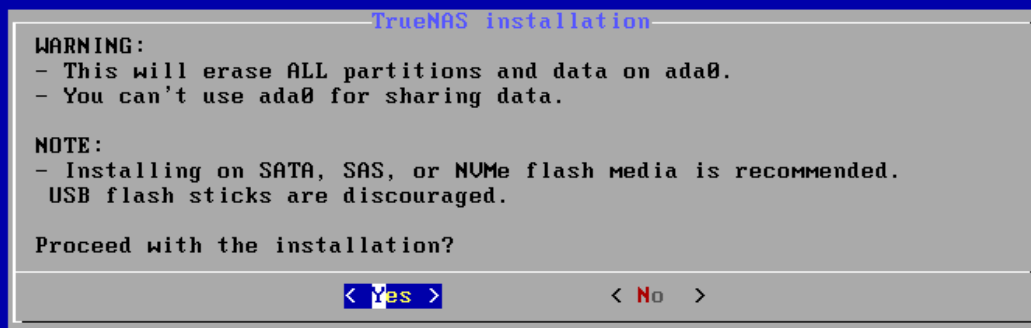
- La réplication est maintenant effective



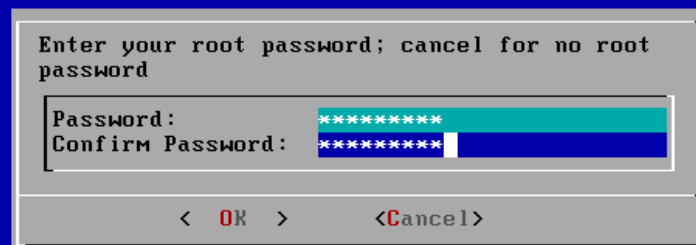
Mise en place de TrueNas

Installation

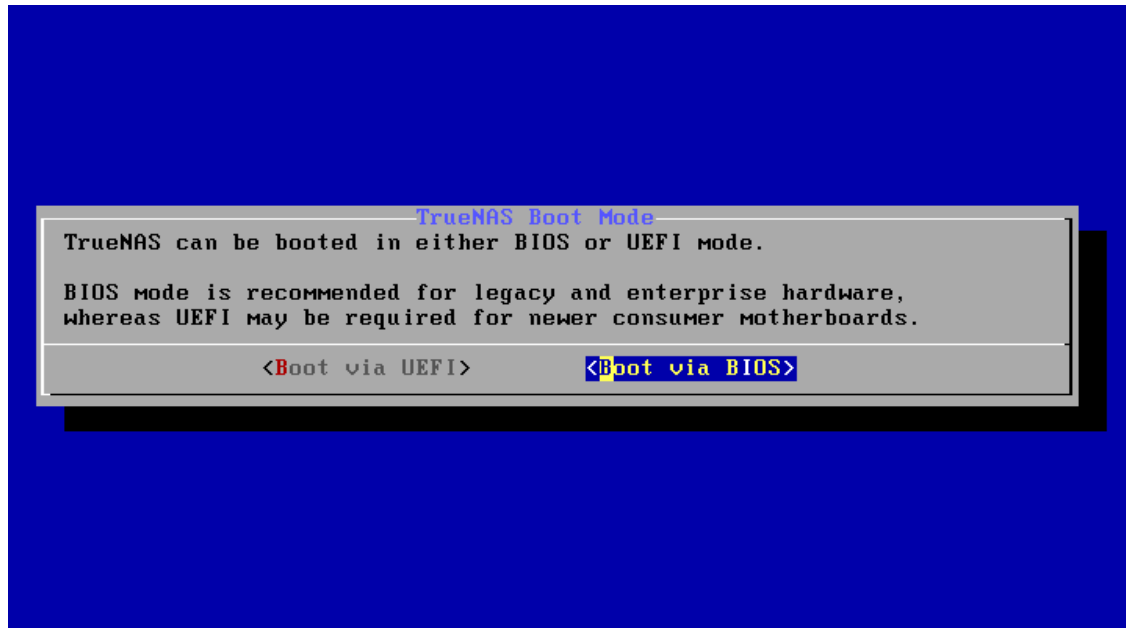
- Au début de l'installation cliquer sur **yes**



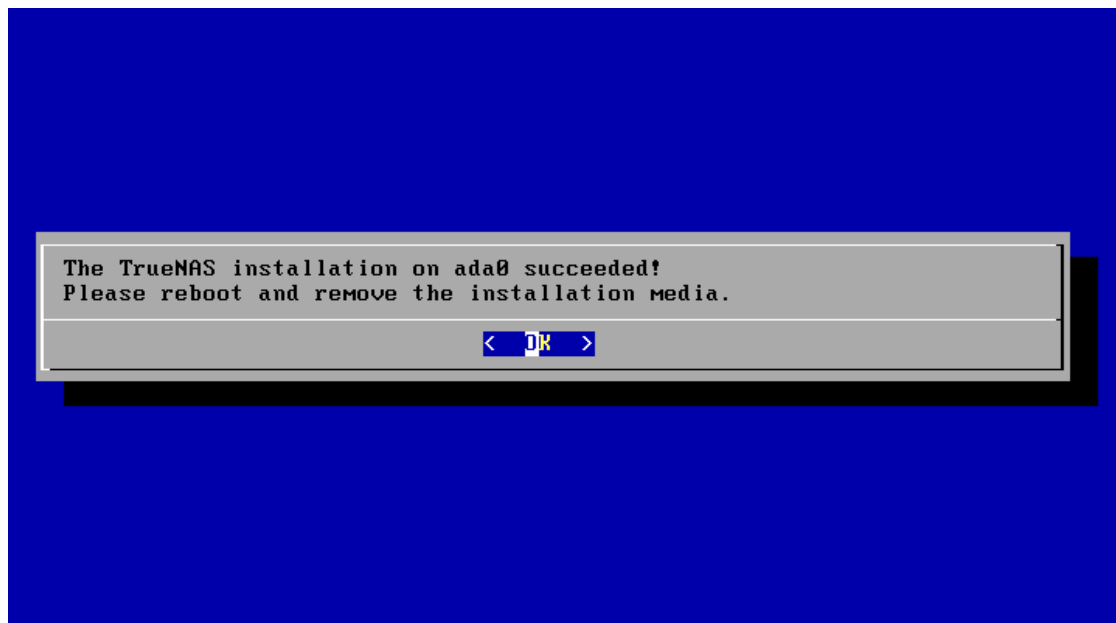
- Choisissez un mot de passe



- Sélectionner **boot via BIOS**

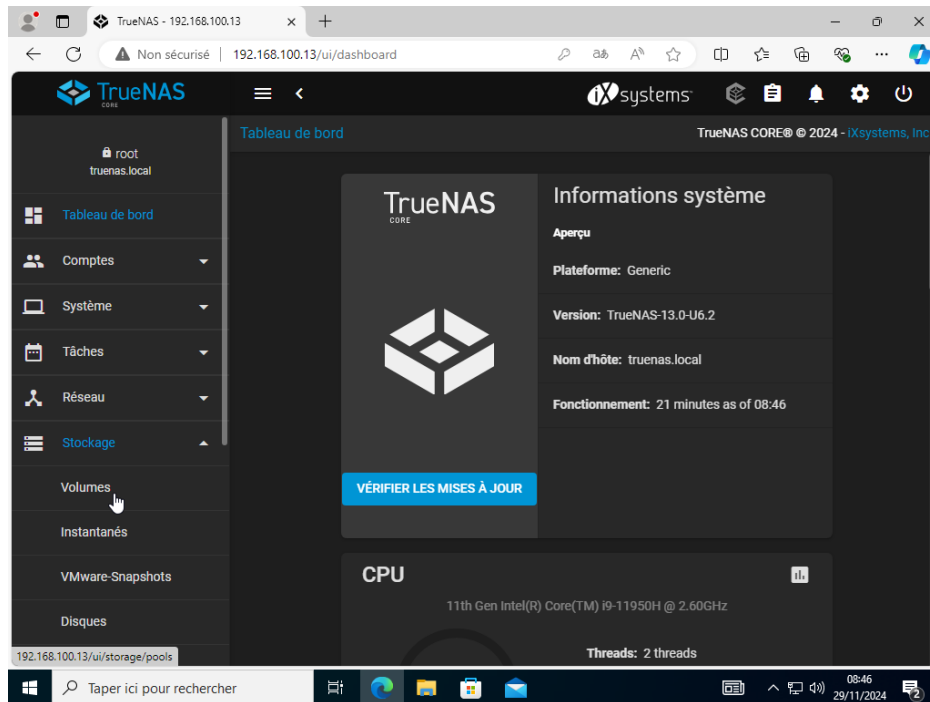


- Redémarrer le système

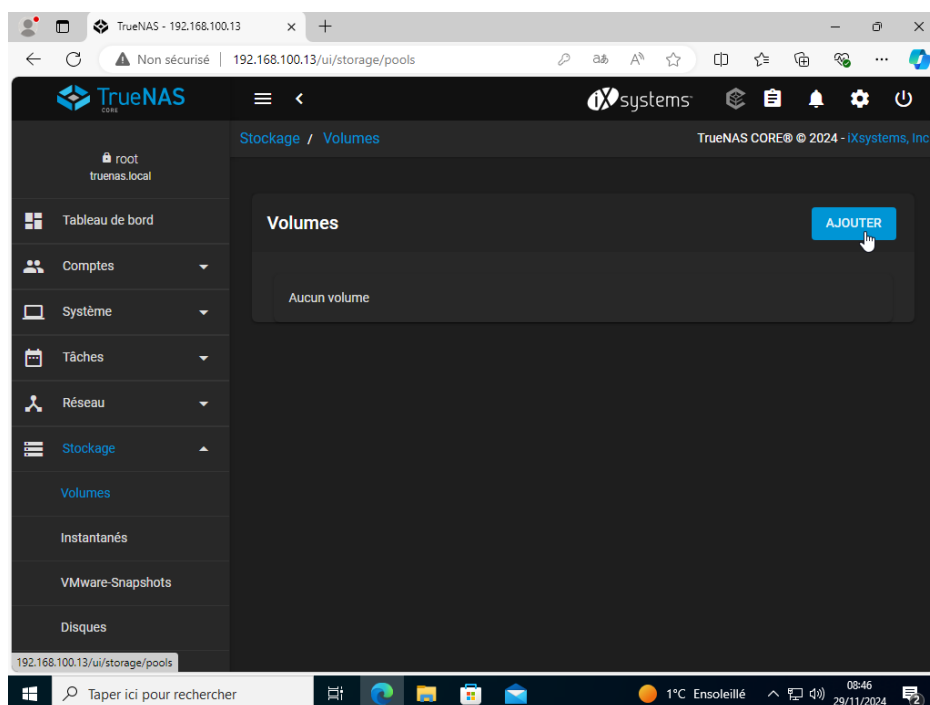


Création du volume

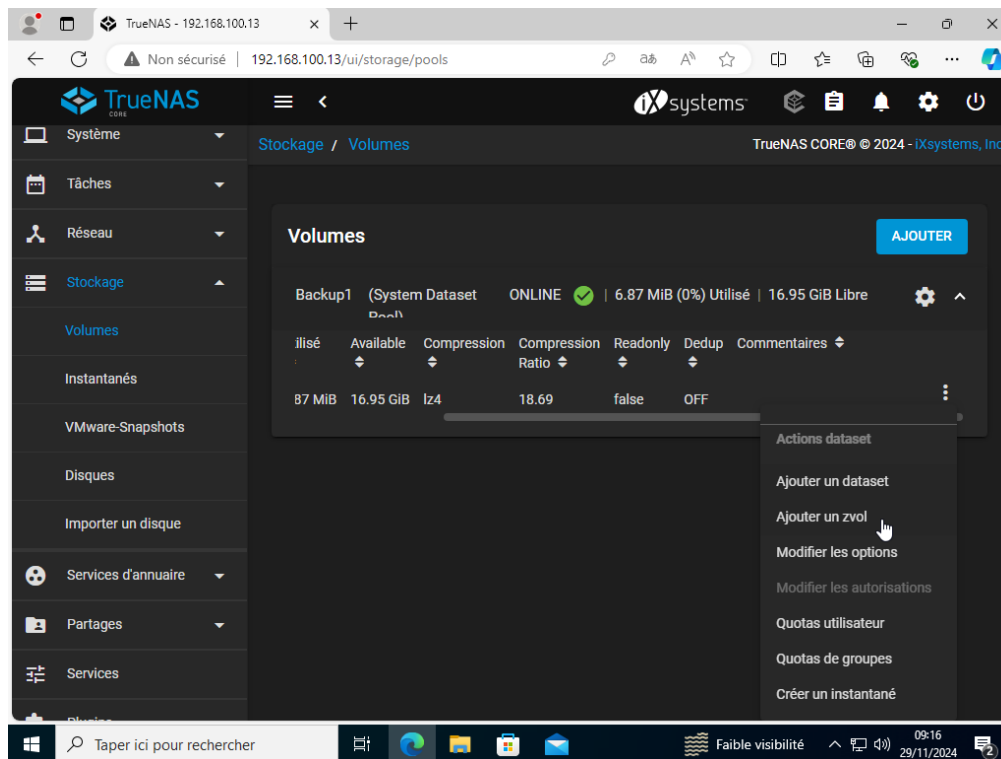
- Une fois redémarré on accède au tableau de bord, puis se rendre dans l'onglet **stockage -> volumes**



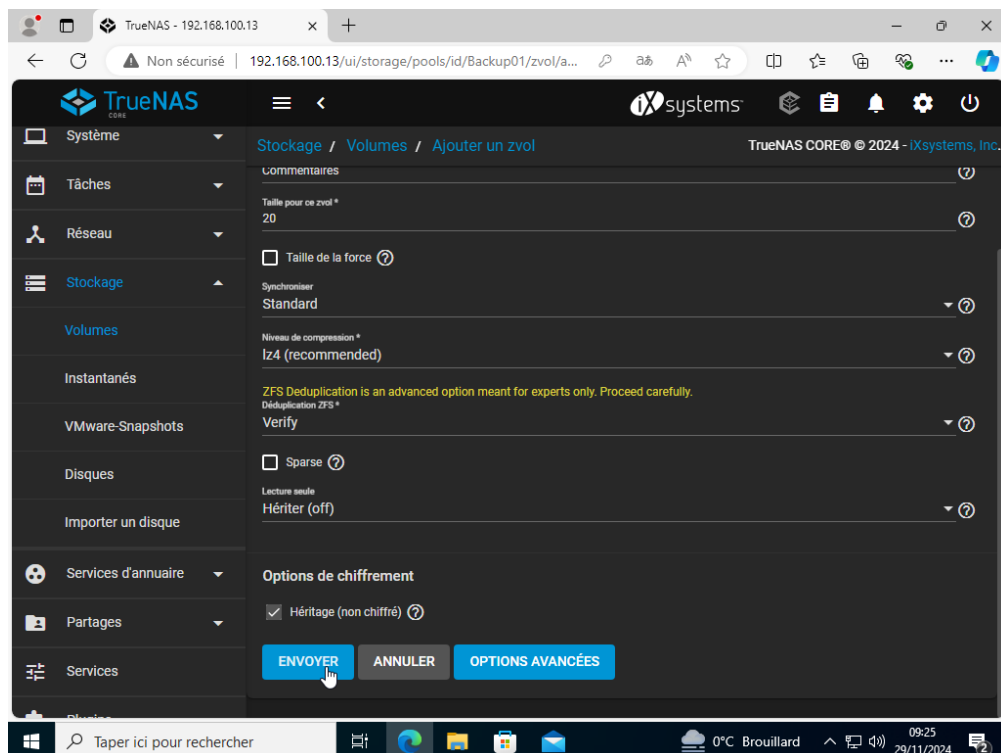
- Ajouter un nouveau volume



- Une fois le volume créer, ajouter un zvol

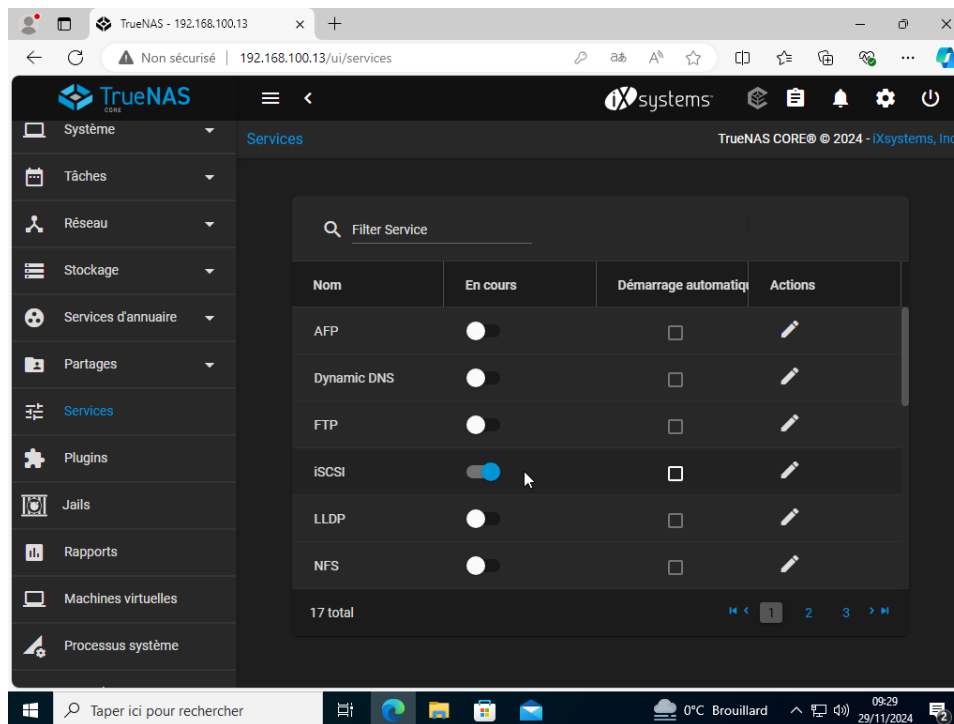


- Confirmer la création du zvol

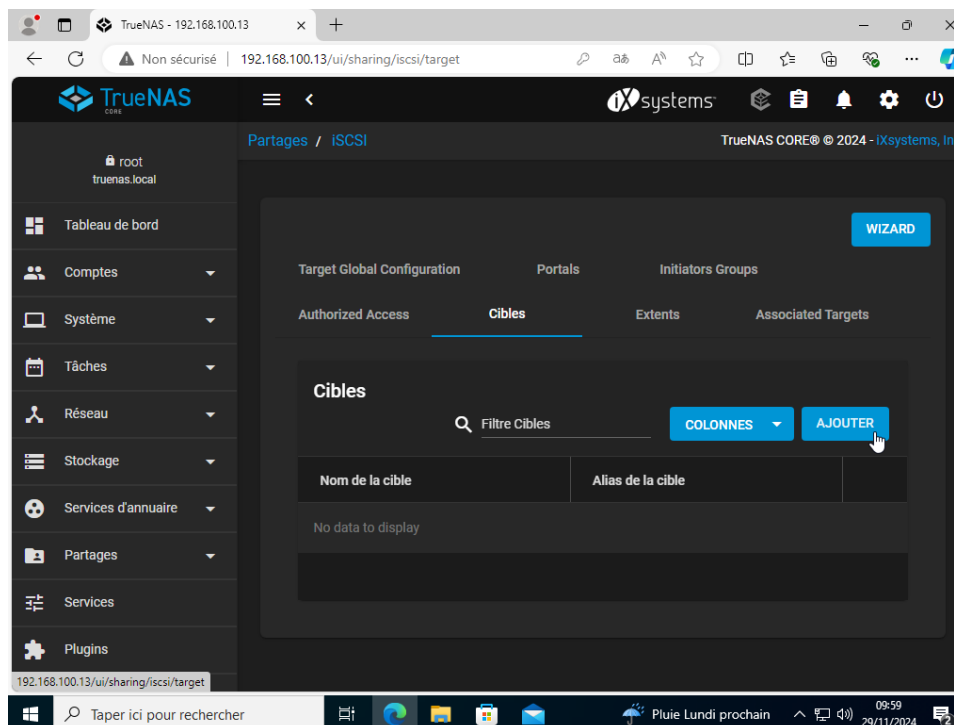


Configuration du partage ISCSI

- Dans l'onglet **services**, activé le service **ISCSI**



- Dans **partage -> ISCSI** ajouter une nouvelle cible



- Choisissez un nom et un id pour la cible

The screenshot shows the TrueNAS web interface at the URL `192.168.100.13/ui/sharing/iscsi/target/add`. The left sidebar contains a navigation menu with items like 'Tableau de bord', 'Comptes', 'Système', 'Tâches', 'Réseau', 'Stockage', 'Services d'annuaire', 'Partages', 'Services', and 'Plugins'. The main content area is titled 'Partages / iSCSI / Cibles / Ajouter'. It contains a form with the following fields: 'Nom de la cible *' (filled with 'Backup01_target'), 'Alias de la cible', 'groupe iSCSI' (filled with '1'), 'ID de groupe du portail *' (filled with '1'), 'ID de groupe de l'initiateur', 'Méthode d'Authentification' (filled with 'Aucun'), and 'Numéro du groupe d'authentification'. There are 'ENVOYER' and 'ANNULER' buttons at the bottom left, and an 'AJOUTER' button at the bottom right. The TrueNAS logo and 'TrueNAS CORE © 2024 - iXsystems, Inc.' are visible at the top.

- Ajouter un extents

The screenshot shows the TrueNAS web interface at the URL `192.168.100.13/ui/sharing/iscsi/extent`. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Partages / iSCSI'. It features a 'WIZARD' button at the top right. Below it, there are tabs for 'Target Global Configuration', 'Portals', 'Initiators Groups', 'Authorized Access', 'Cibles', 'Extents', and 'Associated Targets'. The 'Extents' tab is selected. It contains a search bar 'Filtre Extents', a 'COLONNES' dropdown, and an 'AJOUTER' button. Below these is a table with the following columns: 'Nom de l'étendue', 'Description', 'Numéro de série', 'NAA', and 'Acti'. The table is currently empty, showing 'No data to display'.

- Sélectionner le disque ISCSI

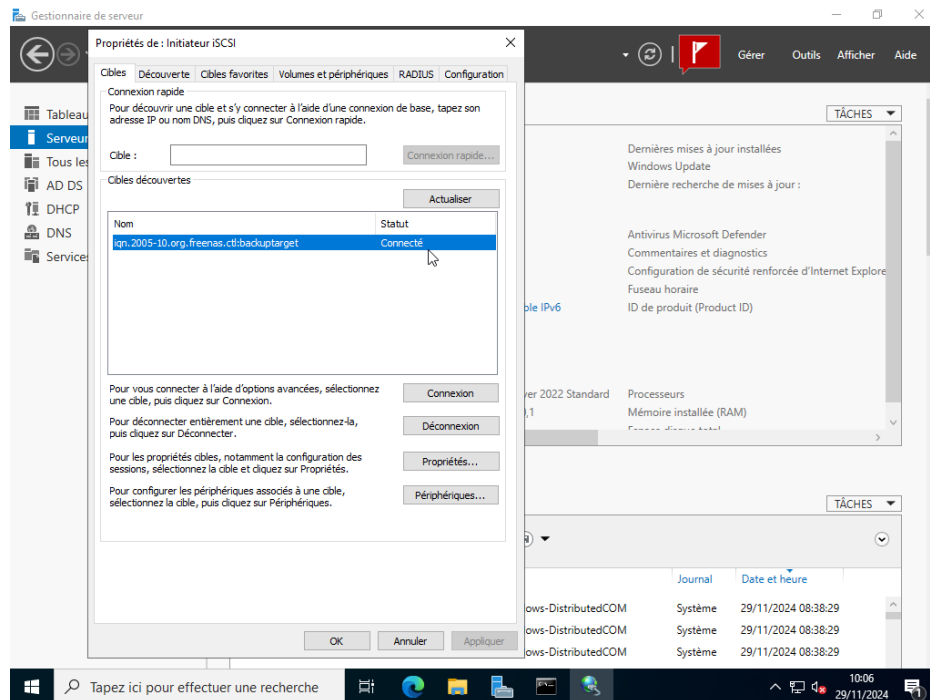
The screenshot shows the TrueNAS web interface at the URL `192.168.100.13/ui/sharing/iscsi/extent/add`. The left sidebar contains a navigation menu with options like 'Tableau de bord', 'Comptes', 'Système', 'Tâches', 'Réseau', 'Stockage', 'Services d'annuaire', and 'Partages'. The 'Partages' section is expanded, showing 'Partages Apple (AFP)', 'Partages Block (iSCSI)', 'Partages Unix (NFS)', and 'Partages WebDAV'. The main content area is titled 'Partages / iSCSI / Extents / Ajouter'. It displays configuration fields for a new iSCSI extent: 'Type' (Périphérique), 'Périphérique*' (Backup01/Backup01 (16K)), 'Taille du bloc logique' (512), 'Désactiver le rapport sur la taille des blocs physiques' (unchecked), 'Seuil d'espace disponible (%)' (empty), 'Compatibility' (Activé TPC checked, Mode compat d'initiateur Xen unchecked), 'NPM LUN' (SSD), and 'Lecture seule' (unchecked). At the bottom, there are 'ENVOYER' and 'ANNULER' buttons. The Windows taskbar at the bottom shows the time as 10:02 on 29/11/2024.

- Configurer l'association de cible

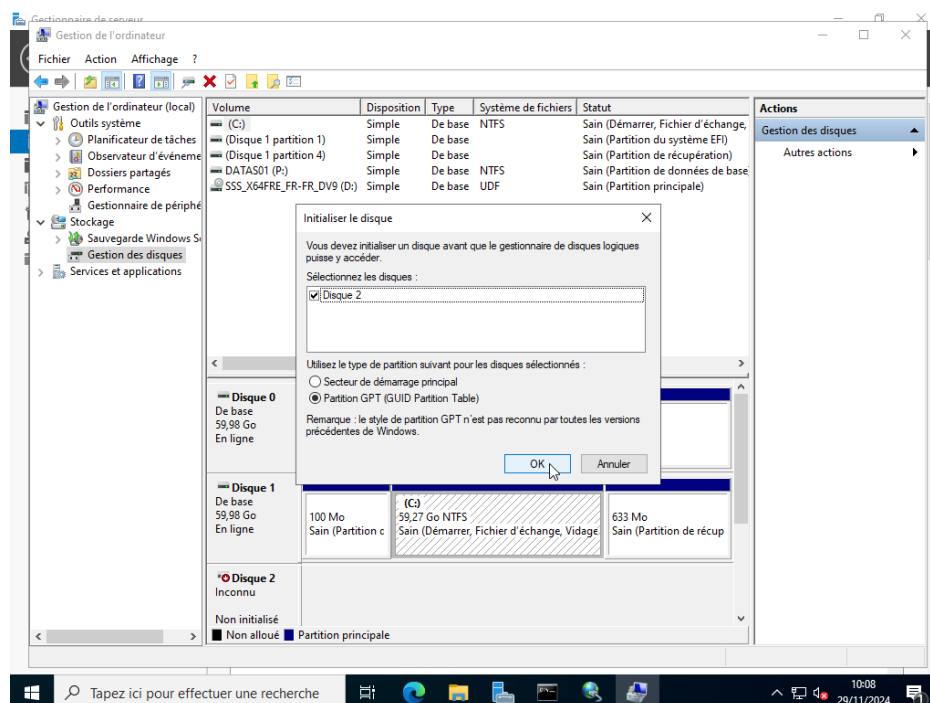
The screenshot shows the TrueNAS web interface at the URL `192.168.100.13/ui/sharing/iscsi/associatedtarget/add`. The left sidebar is identical to the previous screenshot. The main content area is titled 'Partages / iSCSI / Associated Targets / Ajouter'. It displays configuration fields for a new associated target: 'Cible associée' (backuptarget), 'ID LUN' (empty), and 'Etendue*' (Backup01). At the bottom, there are 'ENVOYER' and 'ANNULER' buttons. The Windows taskbar at the bottom shows the time as 10:03 on 29/11/2024.

Ajout du disque sur le serveur

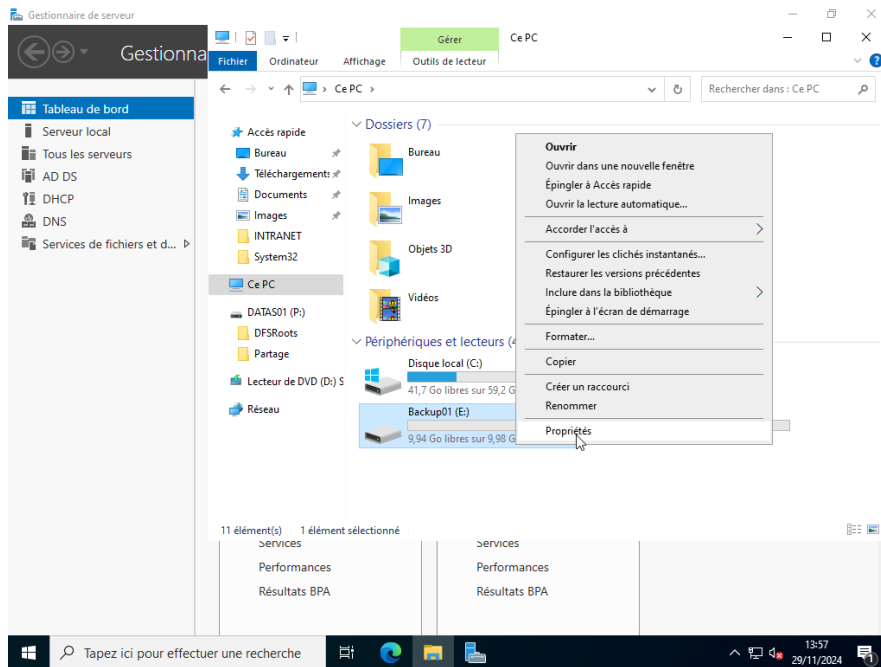
- Ouvrir l'**initiateur iSCSI** et dans le champ cible entrer l'adresse IP de TrueNas



- Une fois le disque connecté, aller dans le **gestionnaire de disque** puis **initialiser le disque** et le **formater** au format NTFS

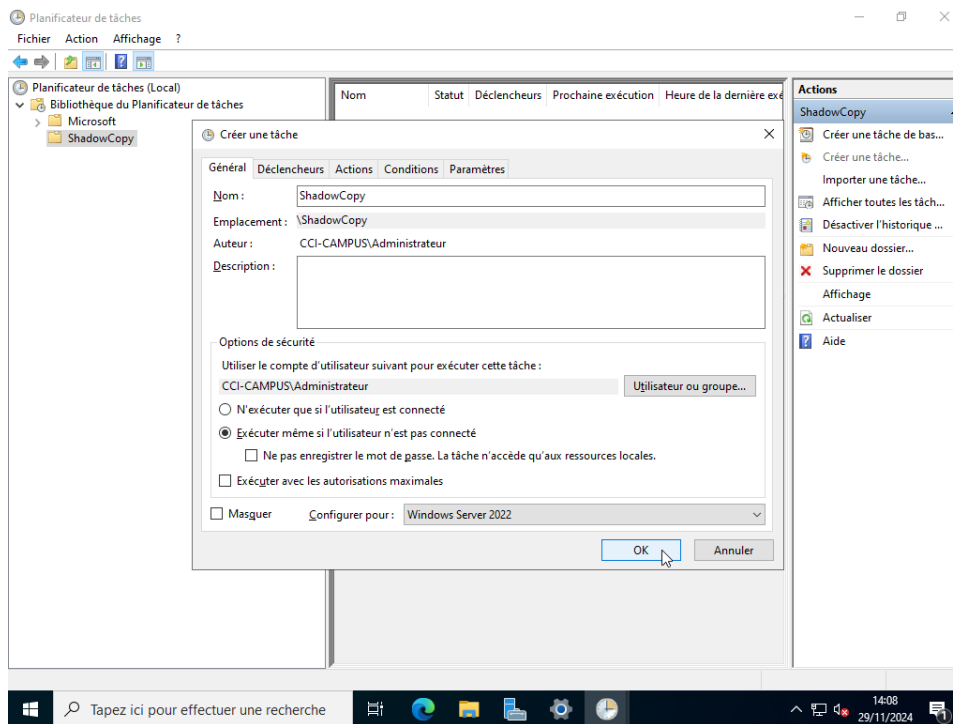


- Le disque est maintenant créé et disponible dans l'explorateur de fichier



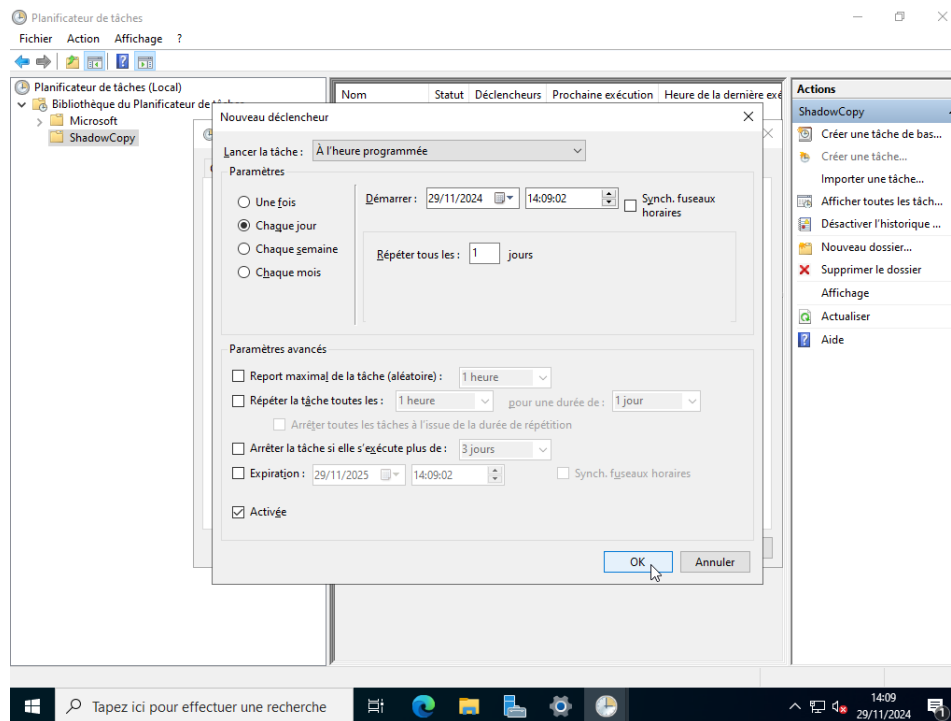
Mise en place de ShadowCopy

- Créer une tâche

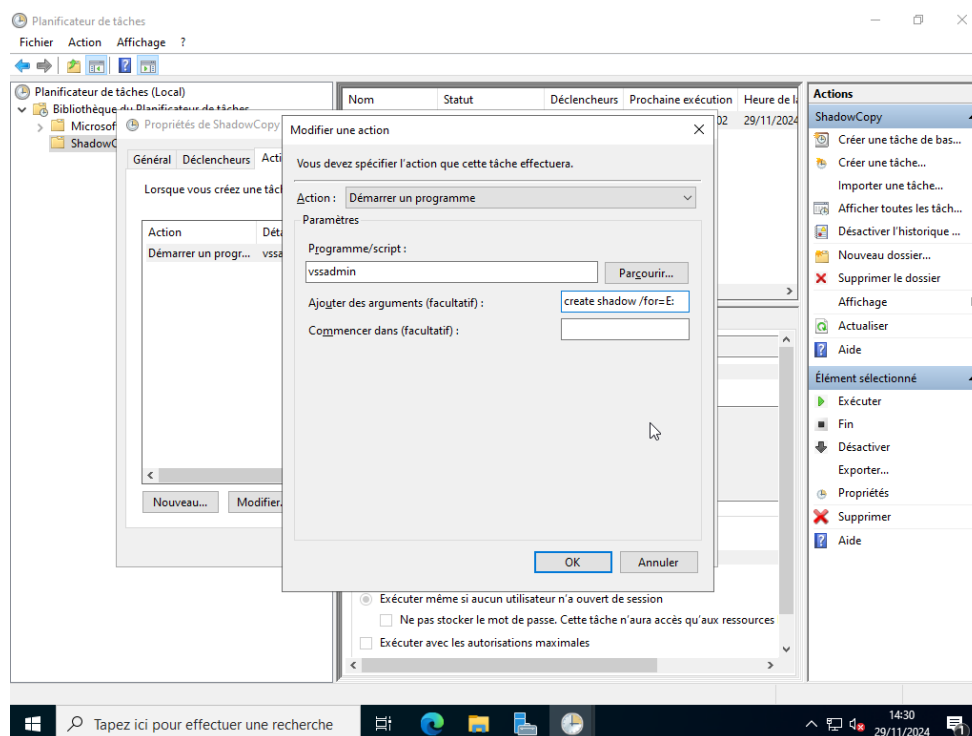


- Activé la

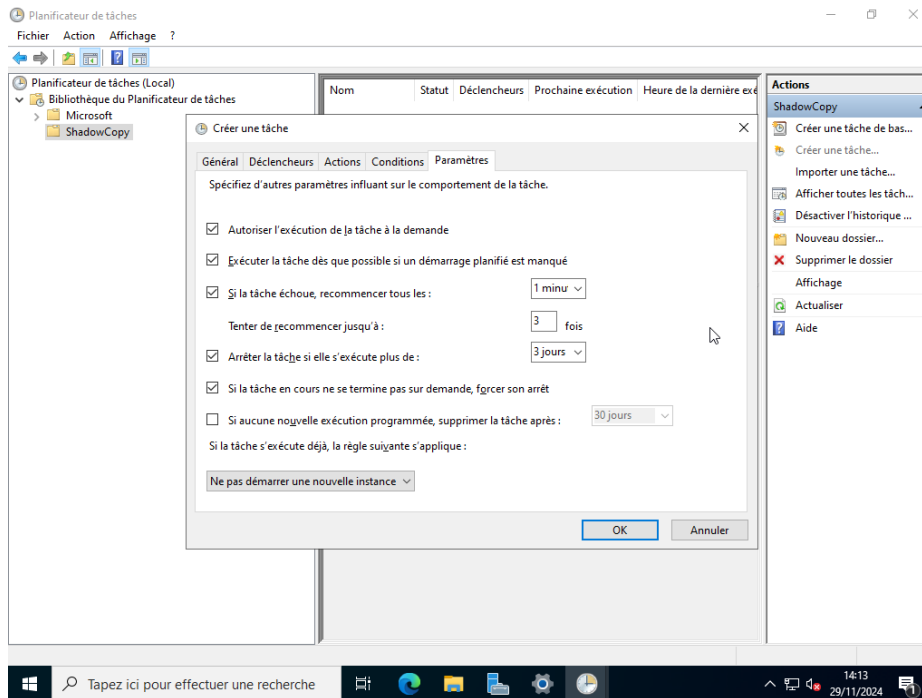
tâche tous les jours à une certaine heure



- Définir l'action de la tâche



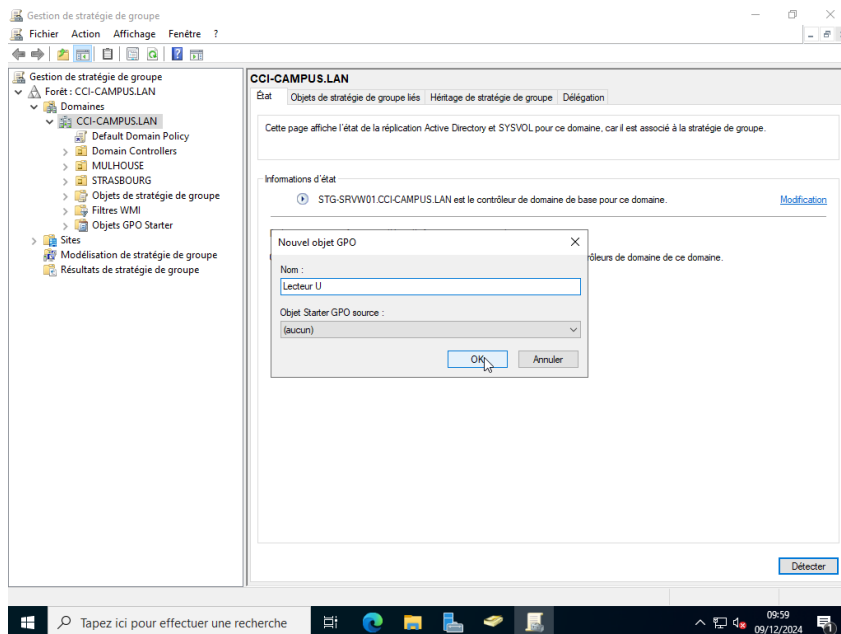
- Cocher les mêmes paramètres ci-dessous



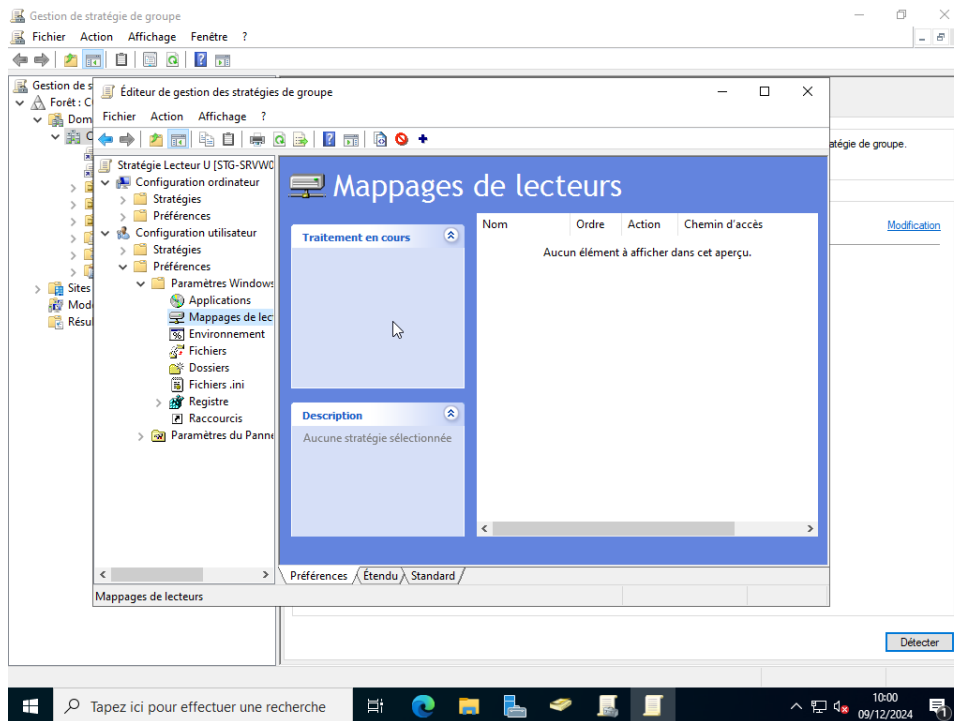
Mise en place des GPO

Mappage des lecteurs

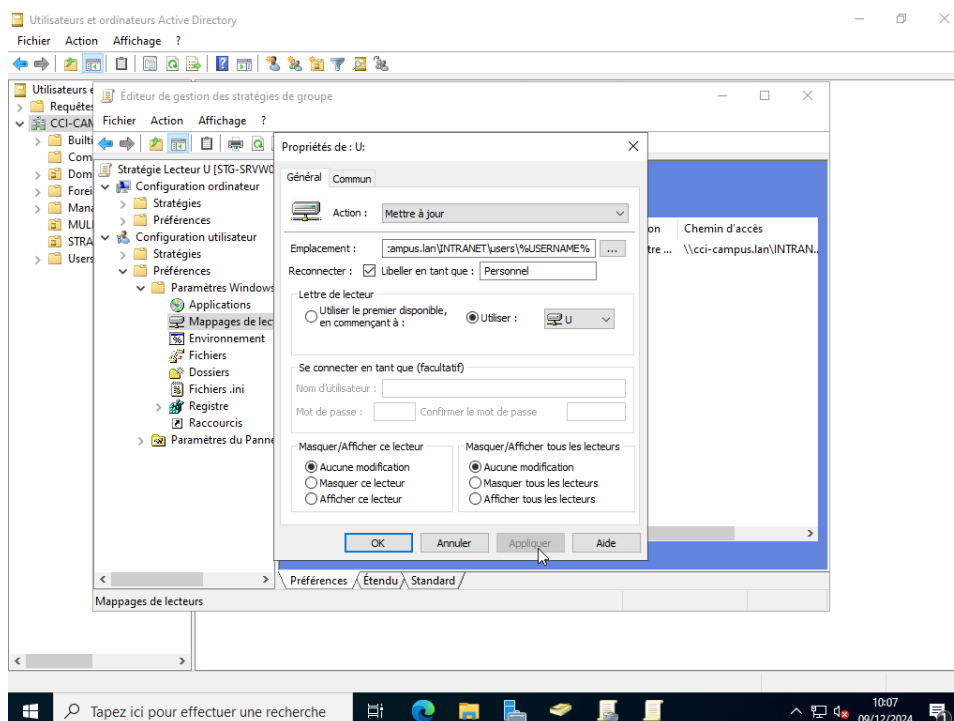
- Dans le gestionnaire de stratégie de groupe créer une nouvelle GPO



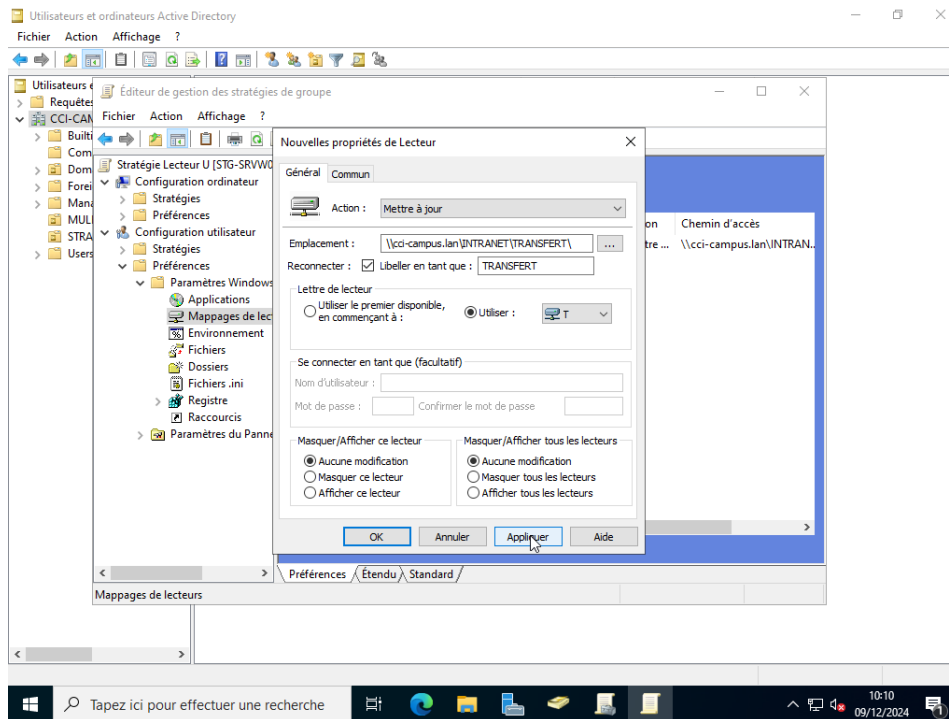
- Faire un clic droit -> **modifier** sur la GPO puis se rendre dans **Configuration utilisateur -> Préférences -> Paramètres Windows -> Mappages de lecteurs**



- Ajouter le lecteur U, dans emplacement saisir le chemin d'accès : **cci-campus.lan\INTRANET\users\%USERNAME%**

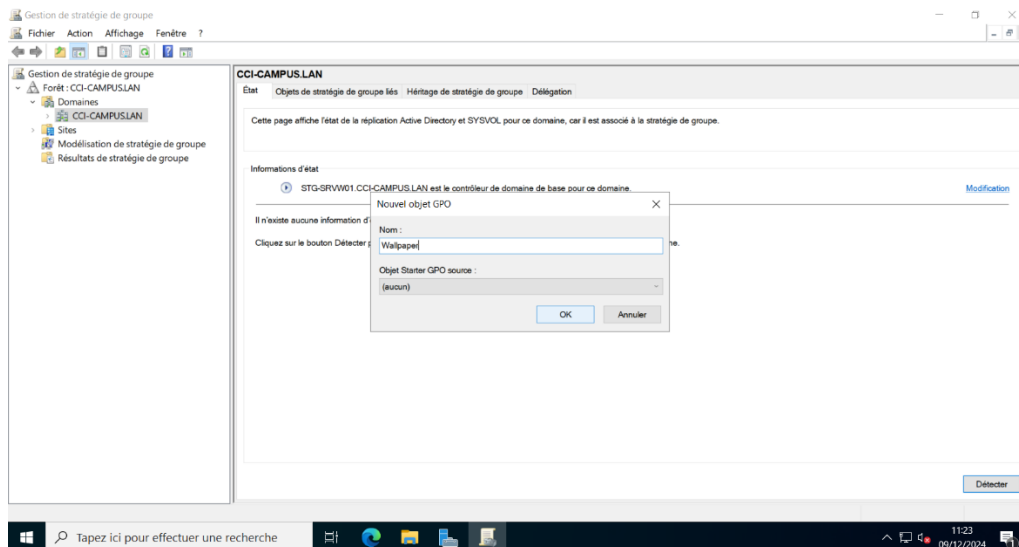


- Faire de même pour le lecteur TRANSFERT

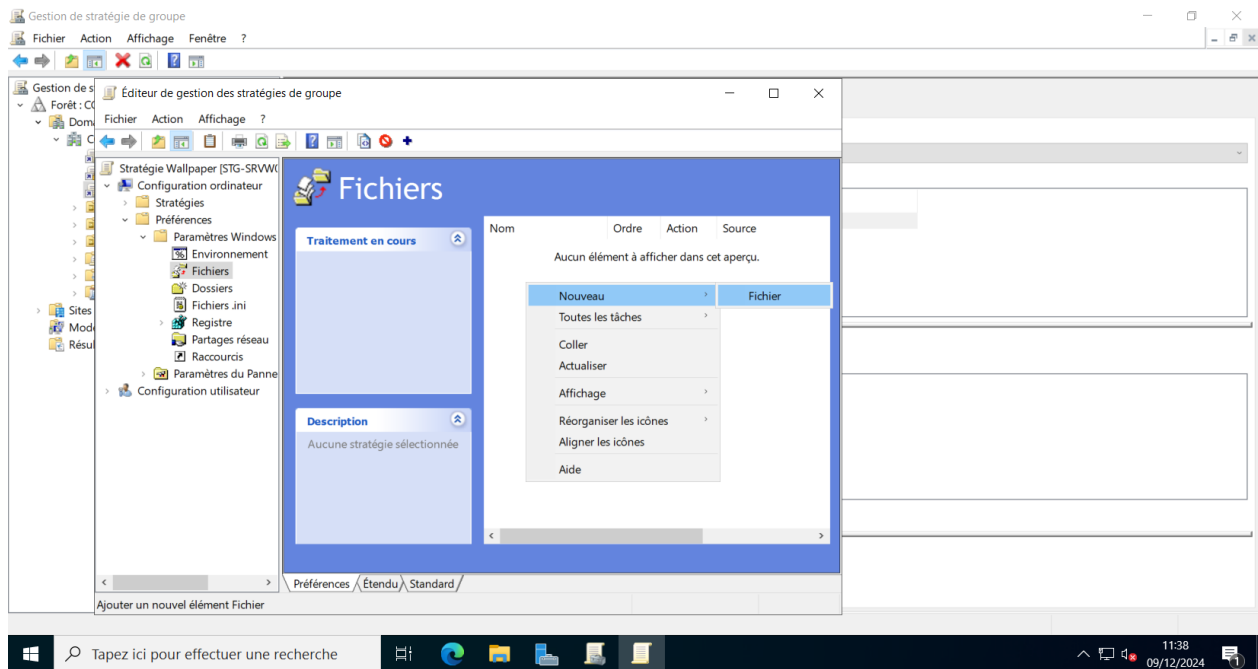


Papier peint du bureau

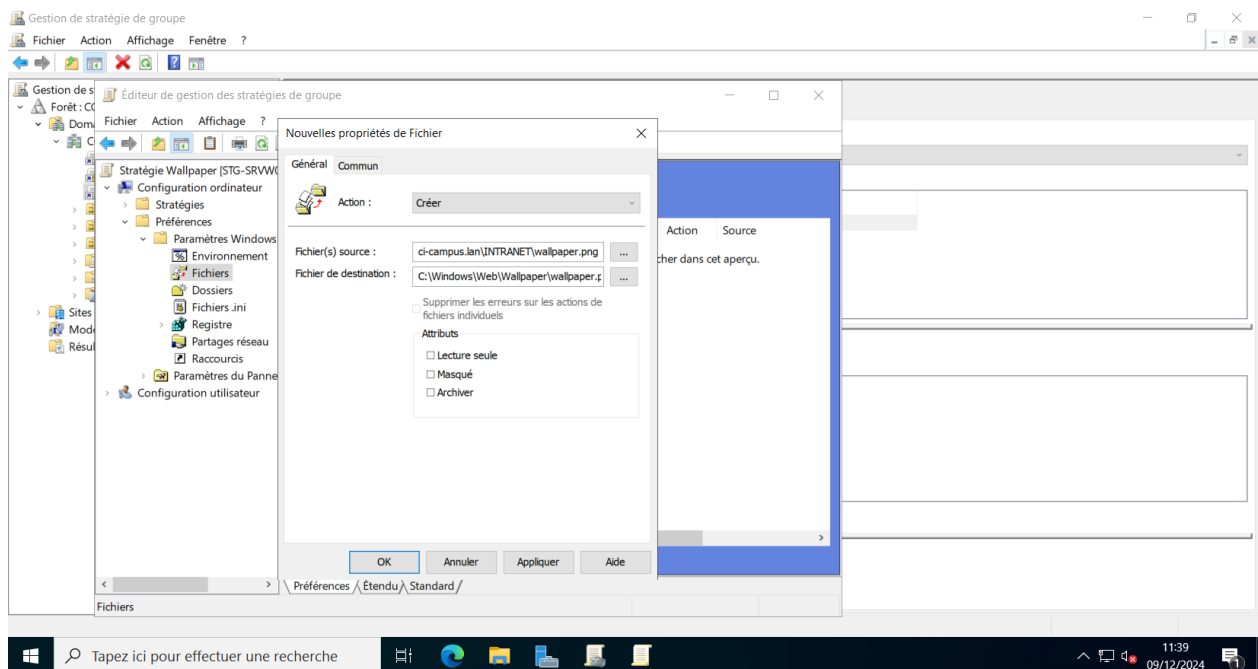
- Créer une GPO à la racine du domaine



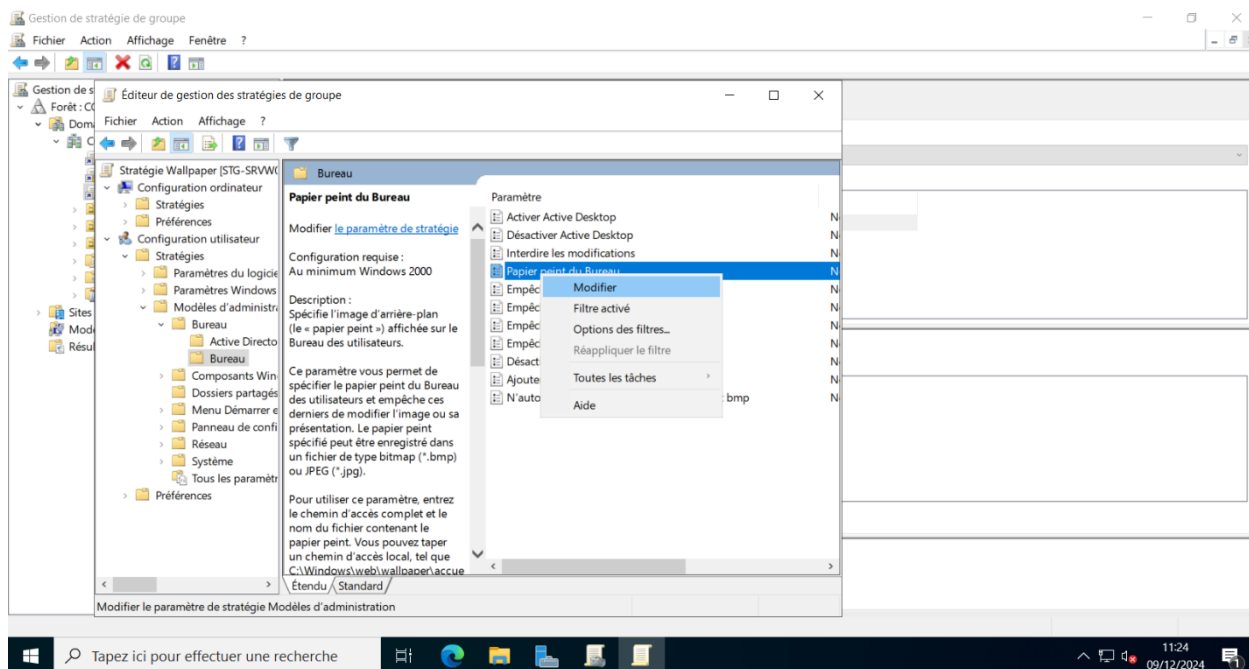
- Se rendre dans **Configuration ordinateur -> Préférences -> Paramètres Windows -> Fichiers**. Ajouter un nouveau fichier



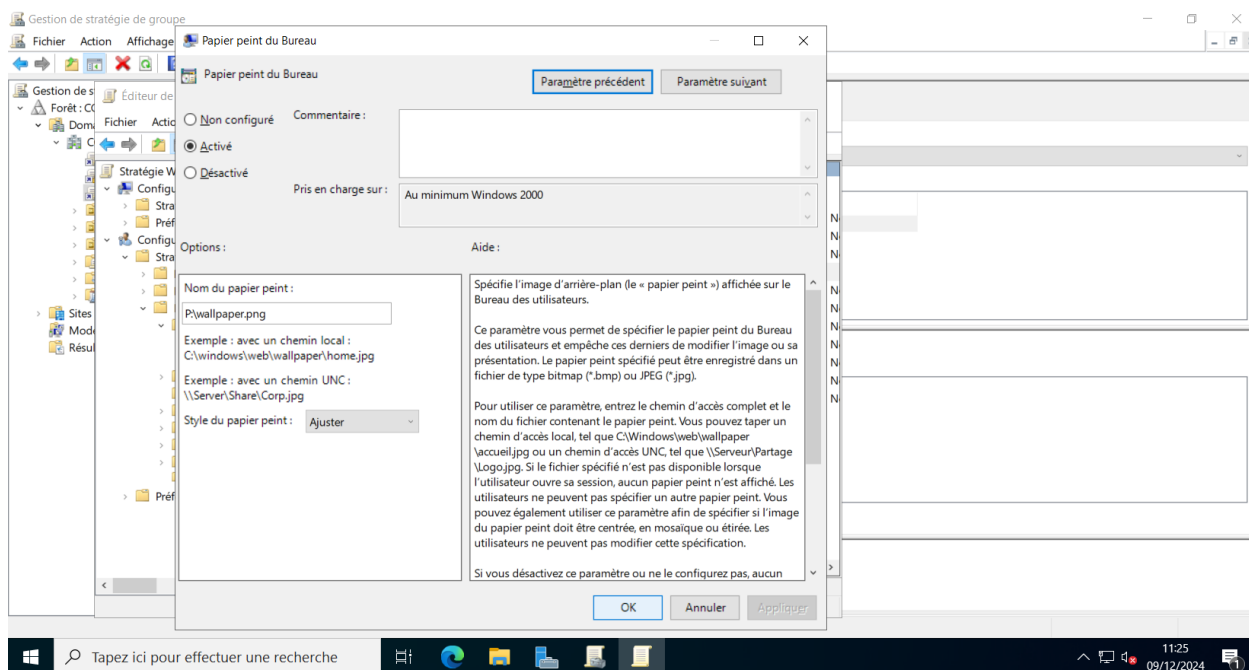
- Sélectionner le fichier source, c'est-à-dire la où se trouve le fichier sur le réseau et un fichier de destination la où sera copier le fichier sur le client afin de pouvoir y accéder.



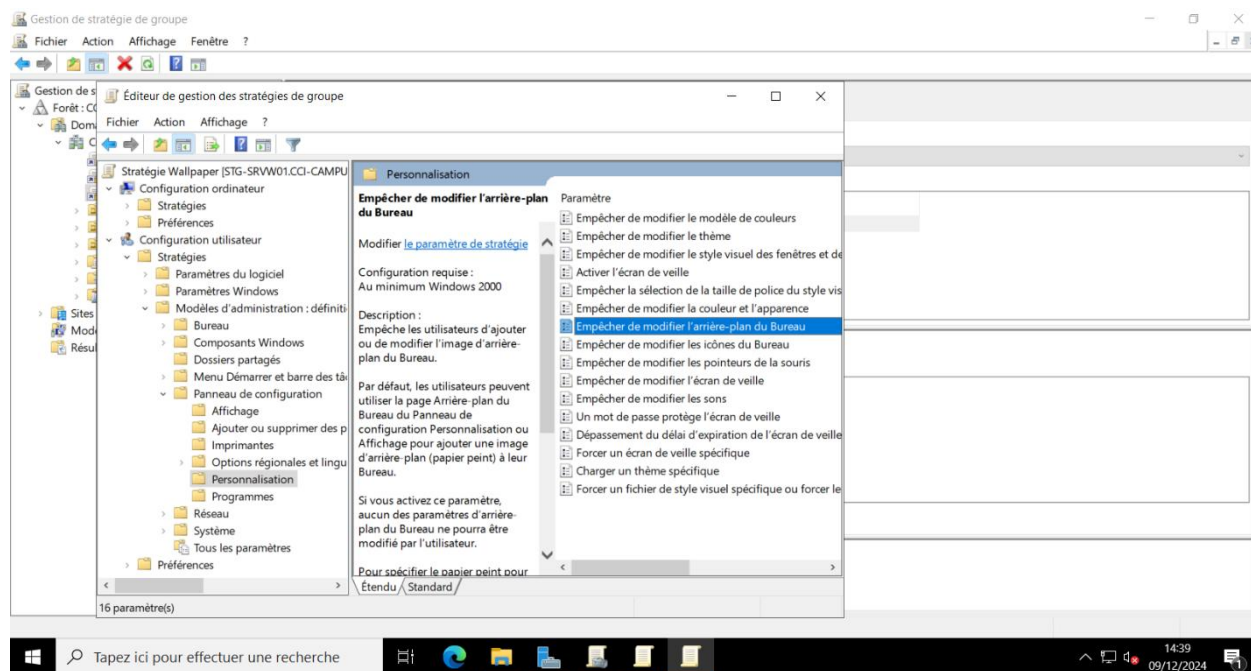
- Ensuite se rendre dans **Configuration utilisateur -> Stratégies -> Modèles d'administration -> Bureau -> Bureau.**



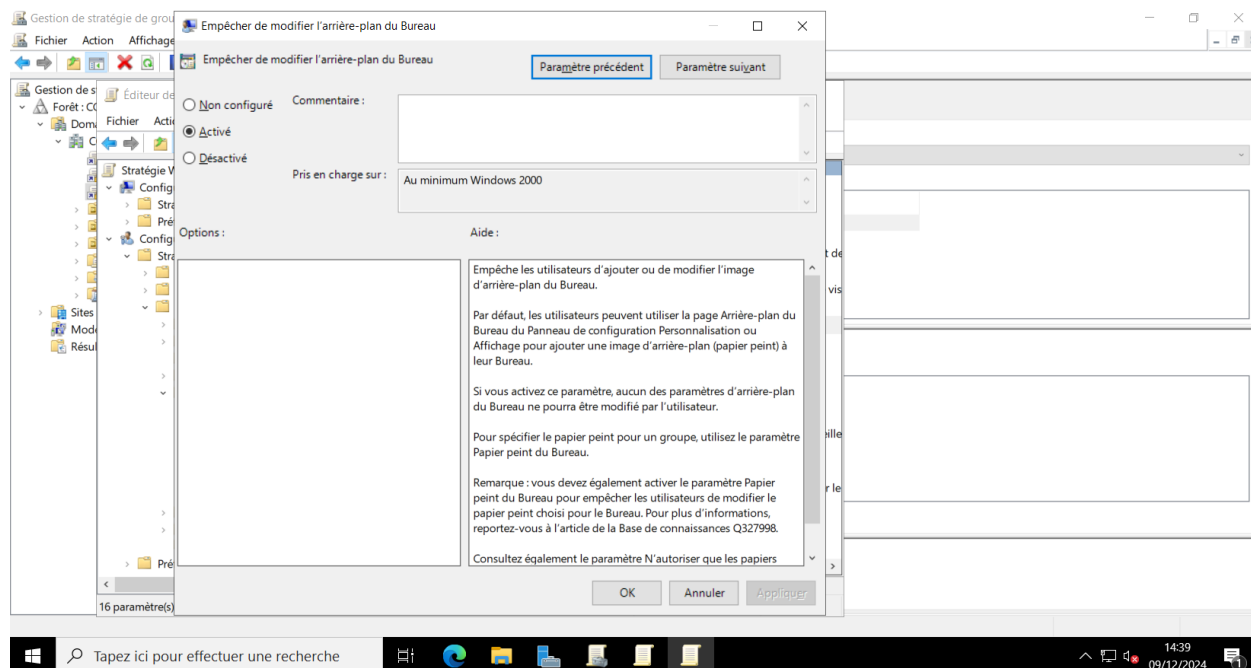
- Ajouter le chemin du fichier du fond d'écran



- Ajouter une règle empêchant de modifier l'arrière-plan dans **Configuration utilisateur -> Stratégies -> Modèles d'administration -> Panneau de configuration -> Personnalisation.**

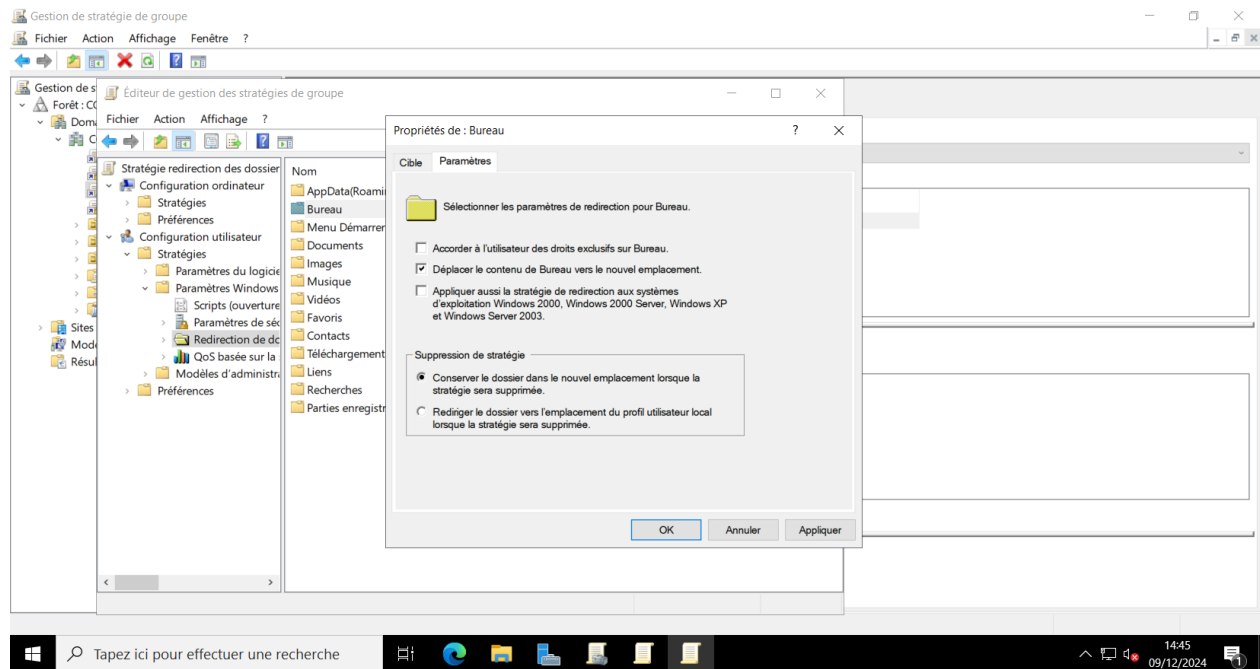


- Activer la GPO

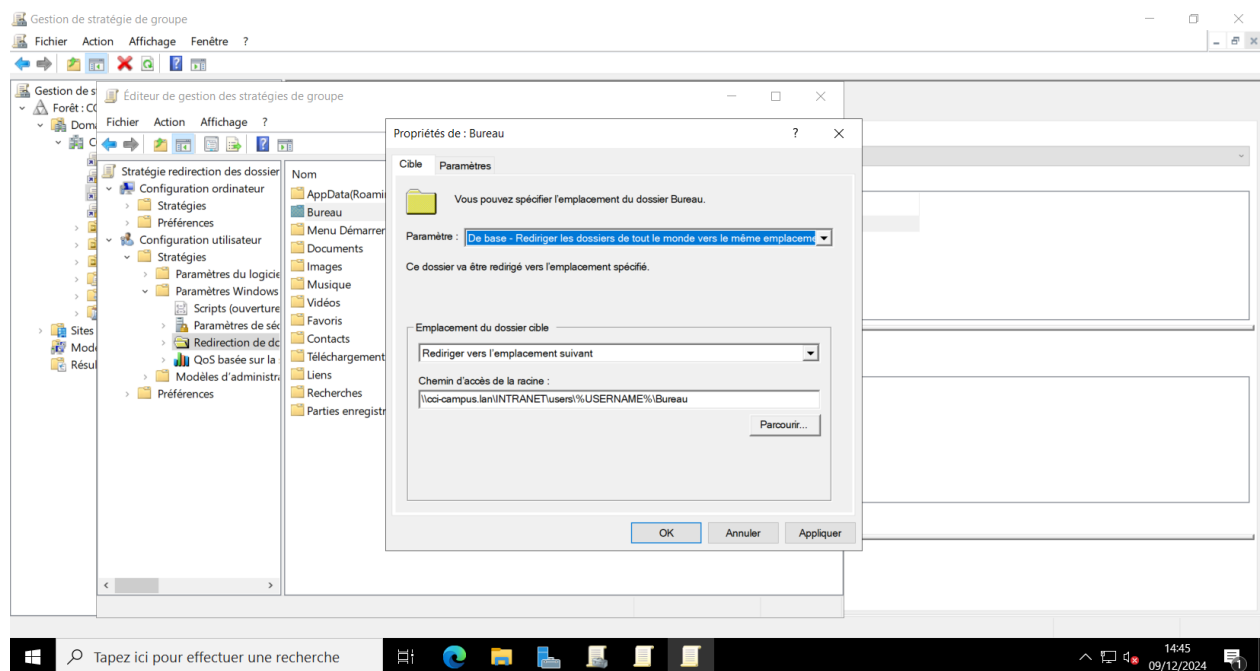


Redirection des dossiers personnels

- Se rendre dans **Configuration utilisateur -> Stratégies -> Paramètres Windows -> Redirection des dossiers**. Sélectionner les dossiers à rediriger et cocher la case **Déplacer le contenu vers le nouvel emplacement**

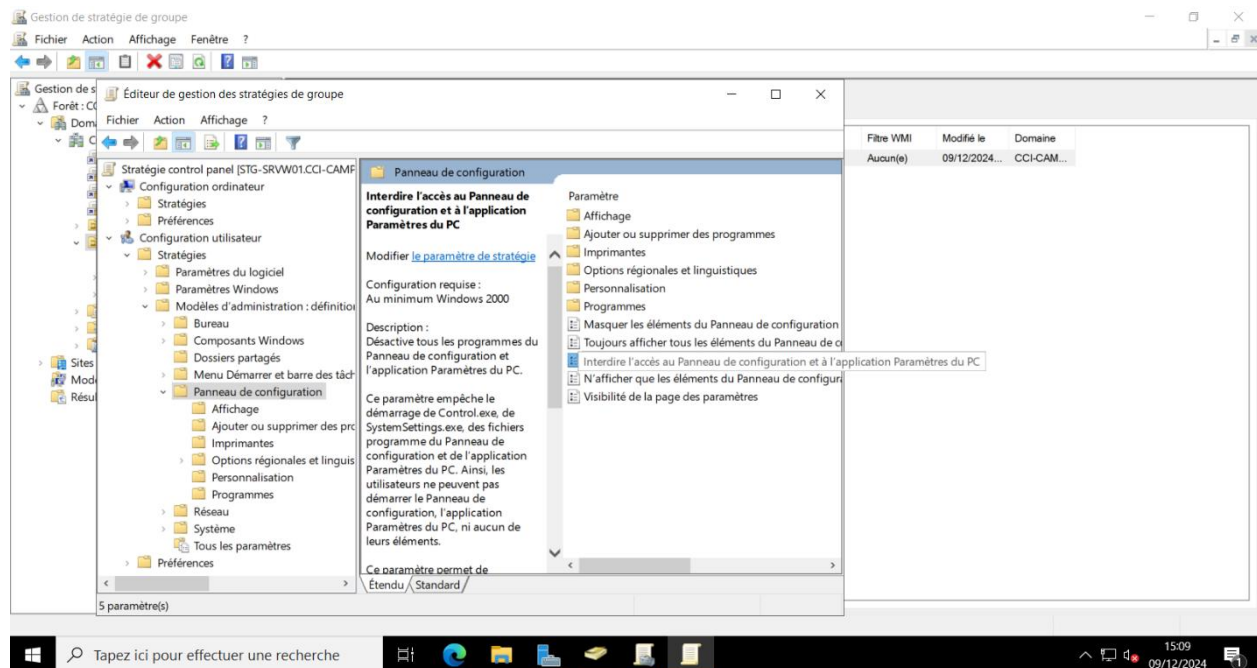


- Choisir l'emplacement vers lequel sera redirigé le dossier

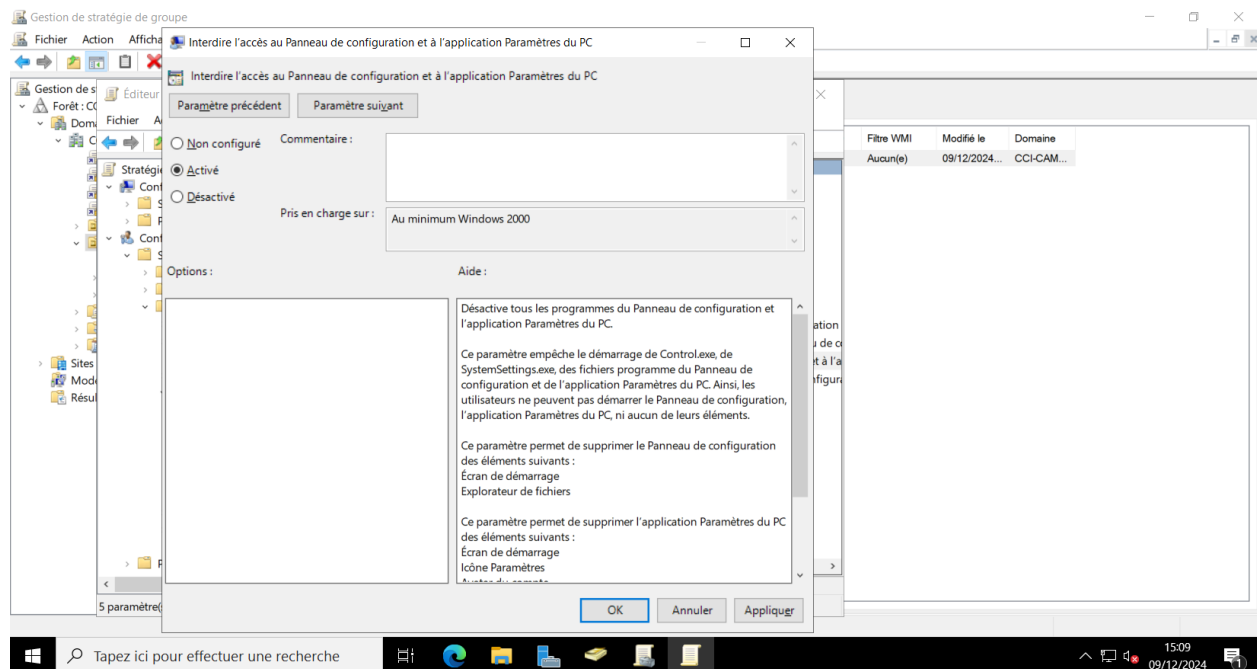


Interdire l'accès aux paramètres

- Se rendre dans **Configuration utilisateur -> Stratégies -> Modèles d'administration -> panneau de configuration.**

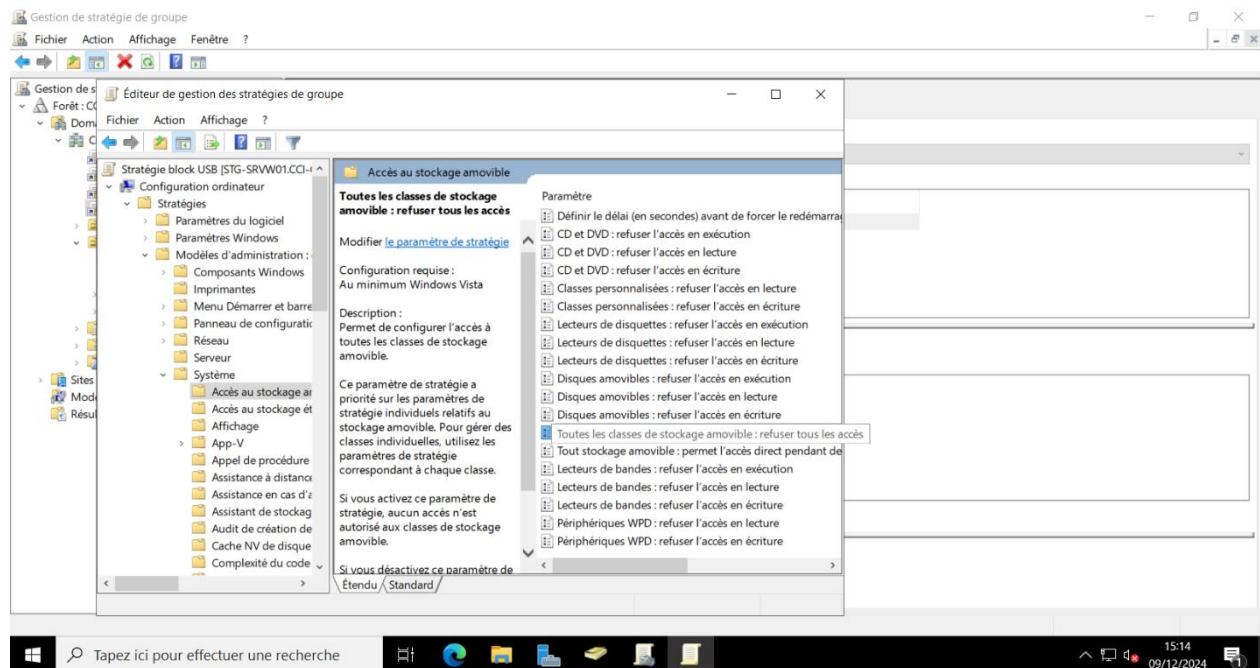


- **Activer la GPO**

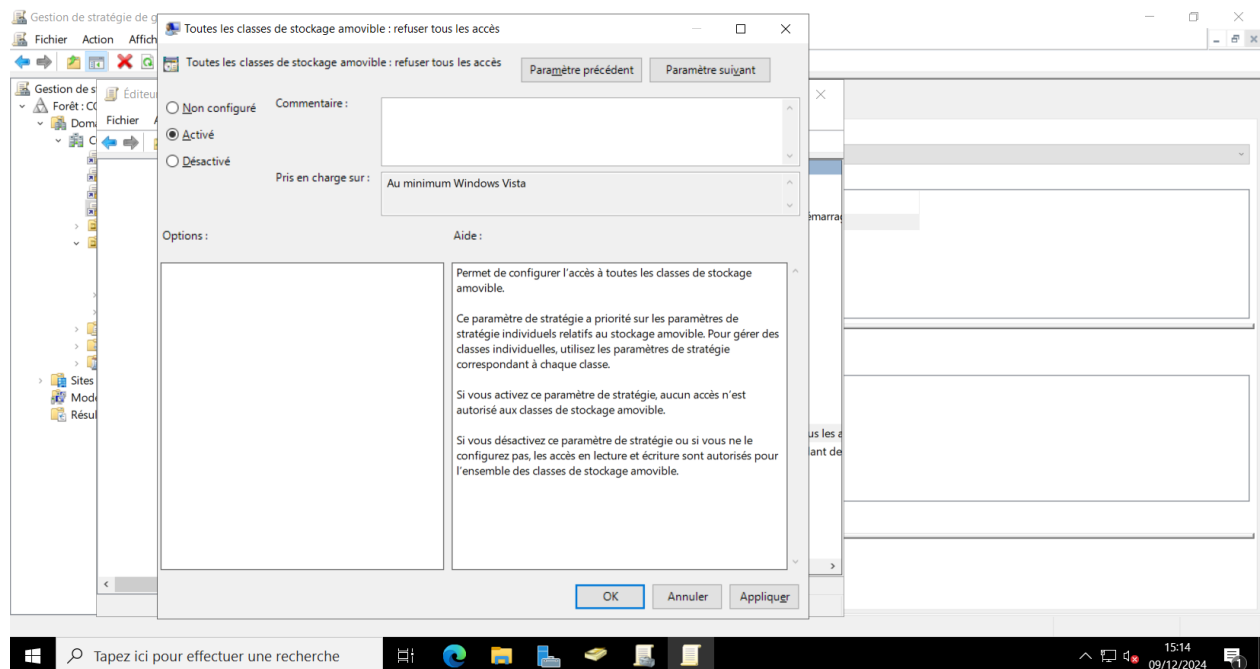


Bloquer les ports USB

- Se rendre dans **Configuration ordinateur -> Stratégies -> Modèles d'administration -> Système -> Accès au stockage amovible.**

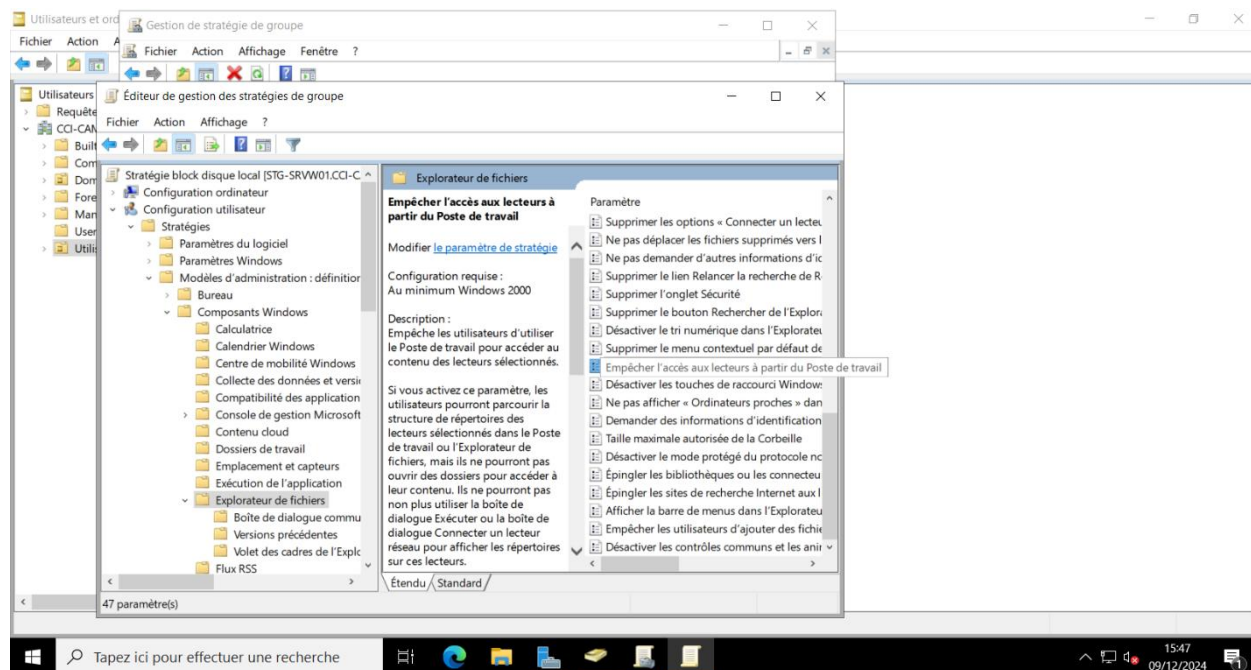


- Activer la GPO

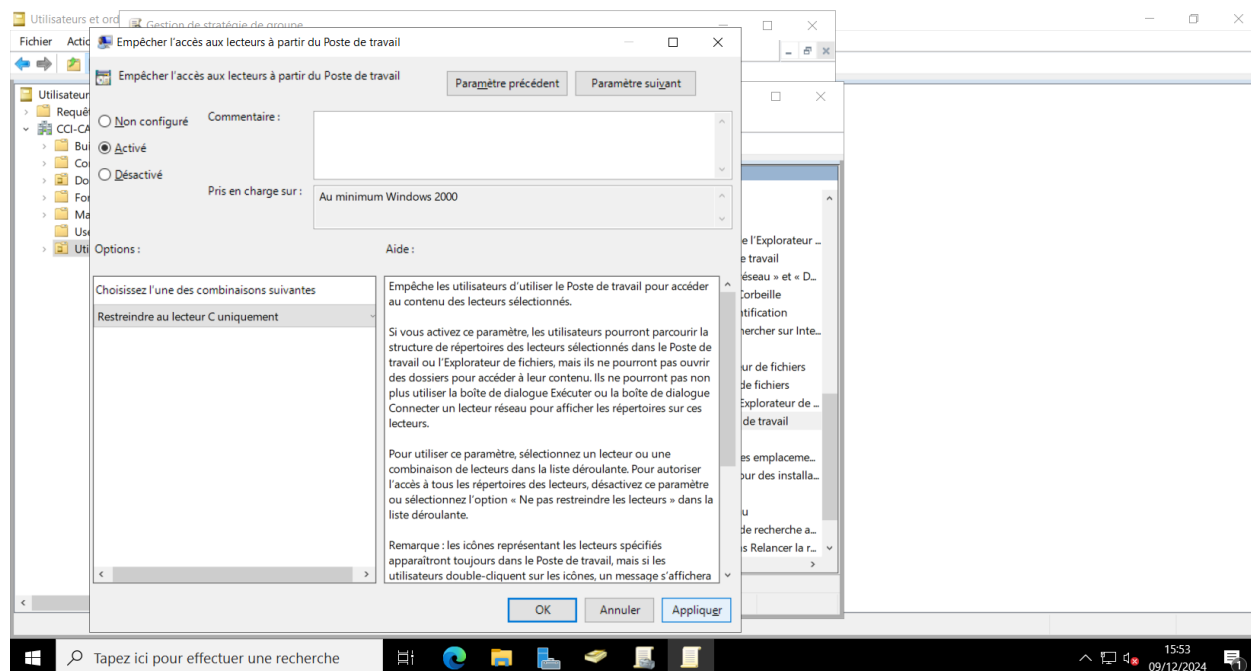


Masquer et bloquer le disque C

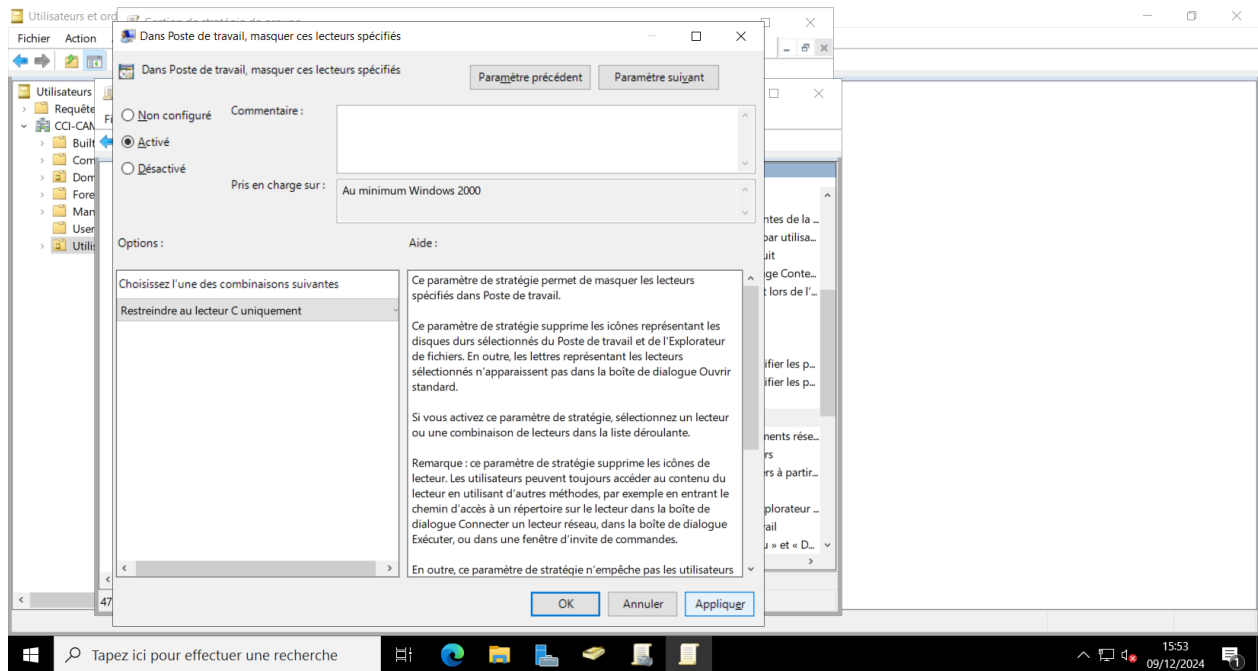
- Pour masquer le disque C, se rendre dans **Configuration utilisateur -> Stratégies -> Modèles d'administration -> Composant Windows -> Explorateur de fichiers.**



- Activer la GPO en choisissant de restreindre l'accès au lecteur C

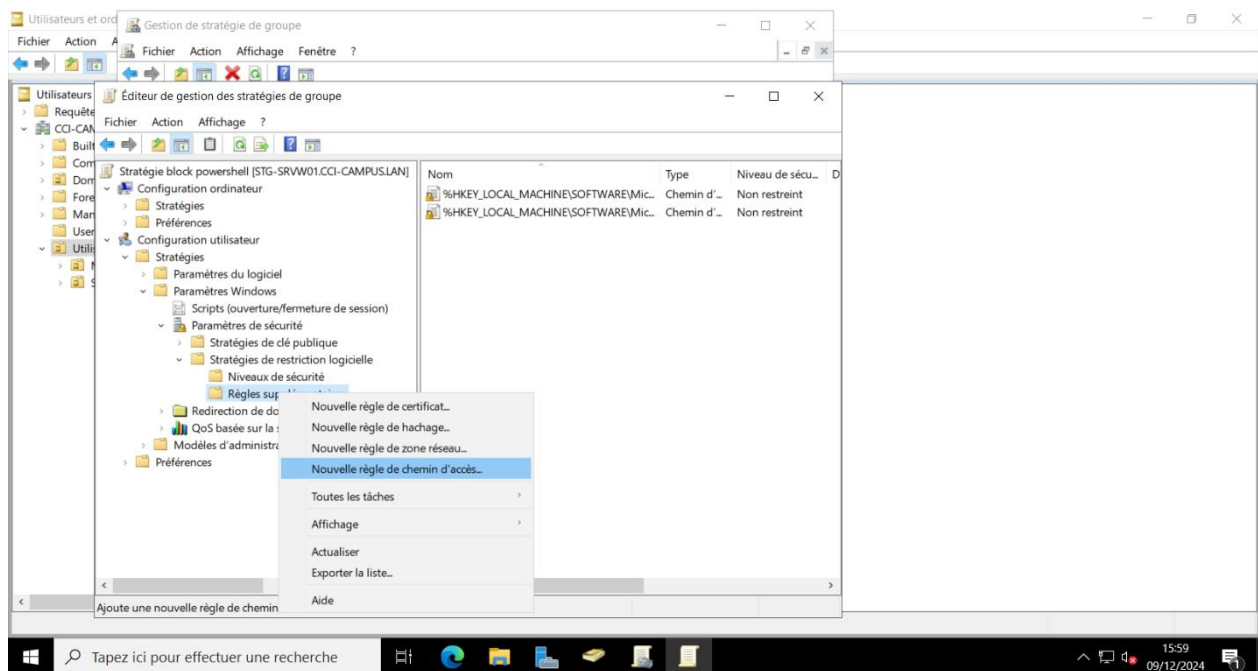


- Faire de même pour masquer le lecteur C

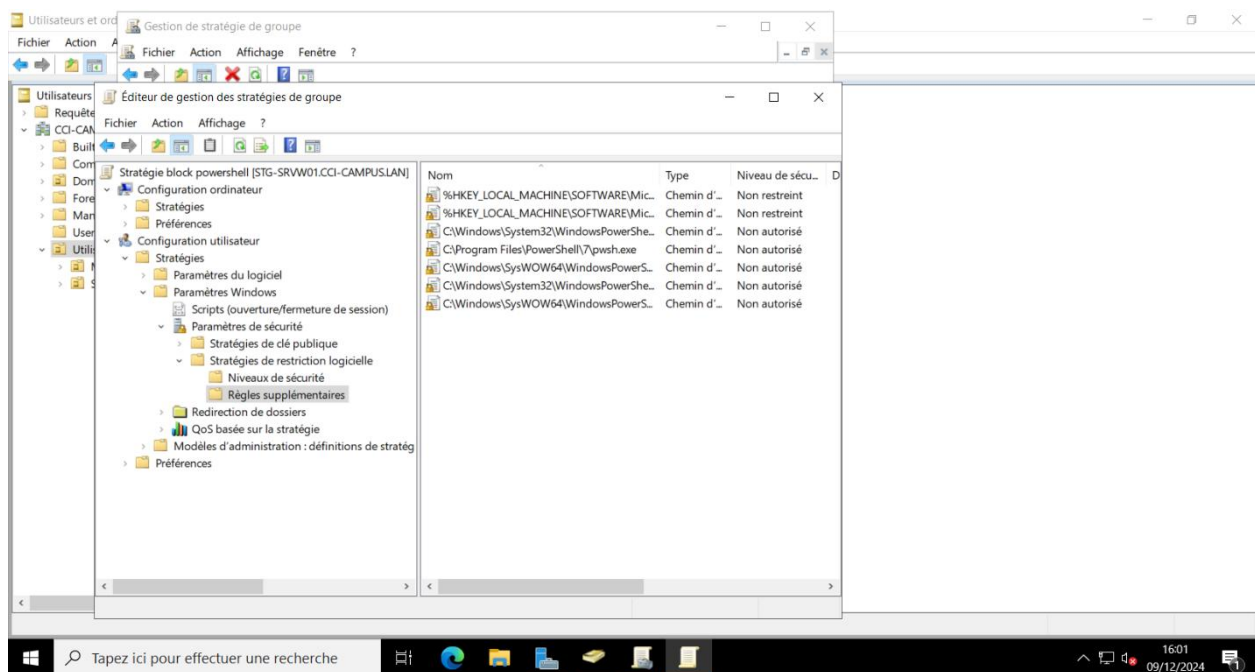
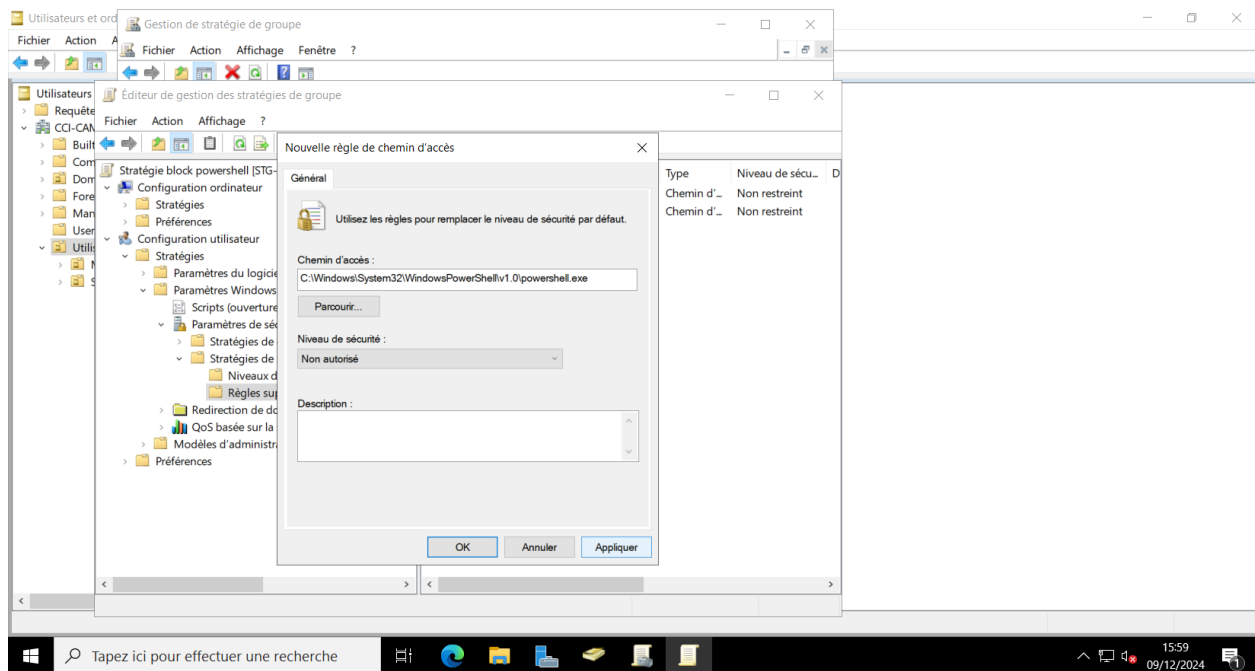


Bloquer l'accès aux consoles Powershell et Invité de commande

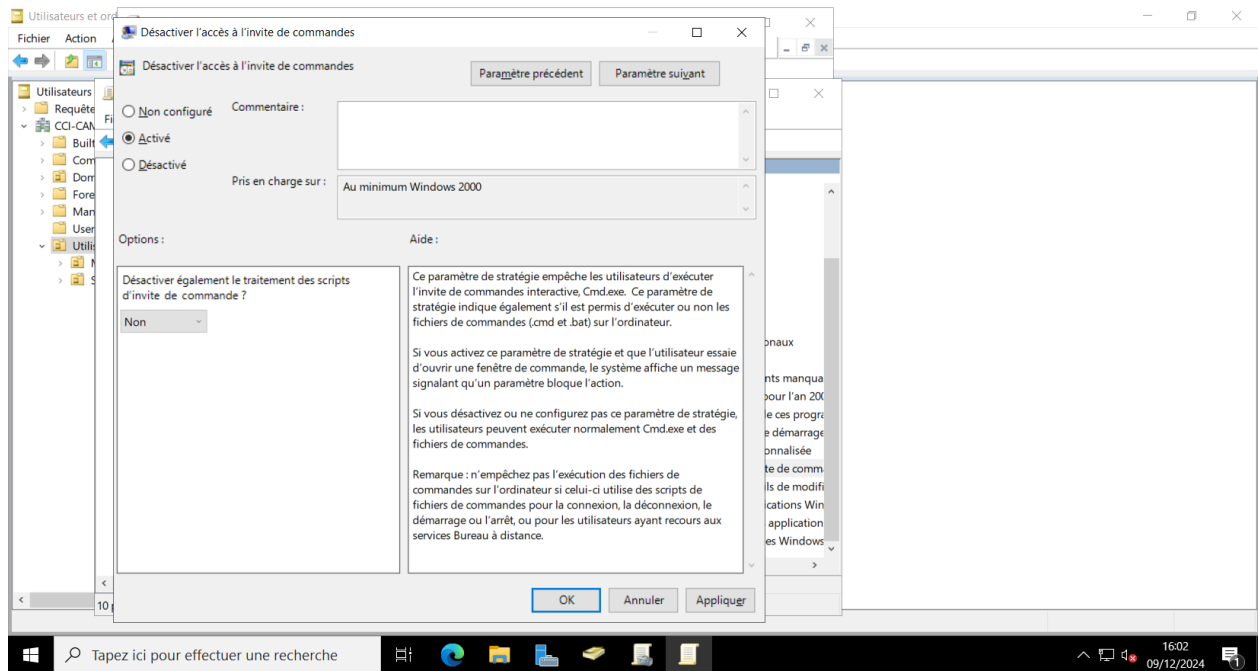
- Créer une règle de restriction de logicielle dans **Configuration utilisateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégies de restriction logicielle -> Règle supplémentaire.**



- Créer ensuite une nouvelle règle en bloquant les chemins d'accès de powershell

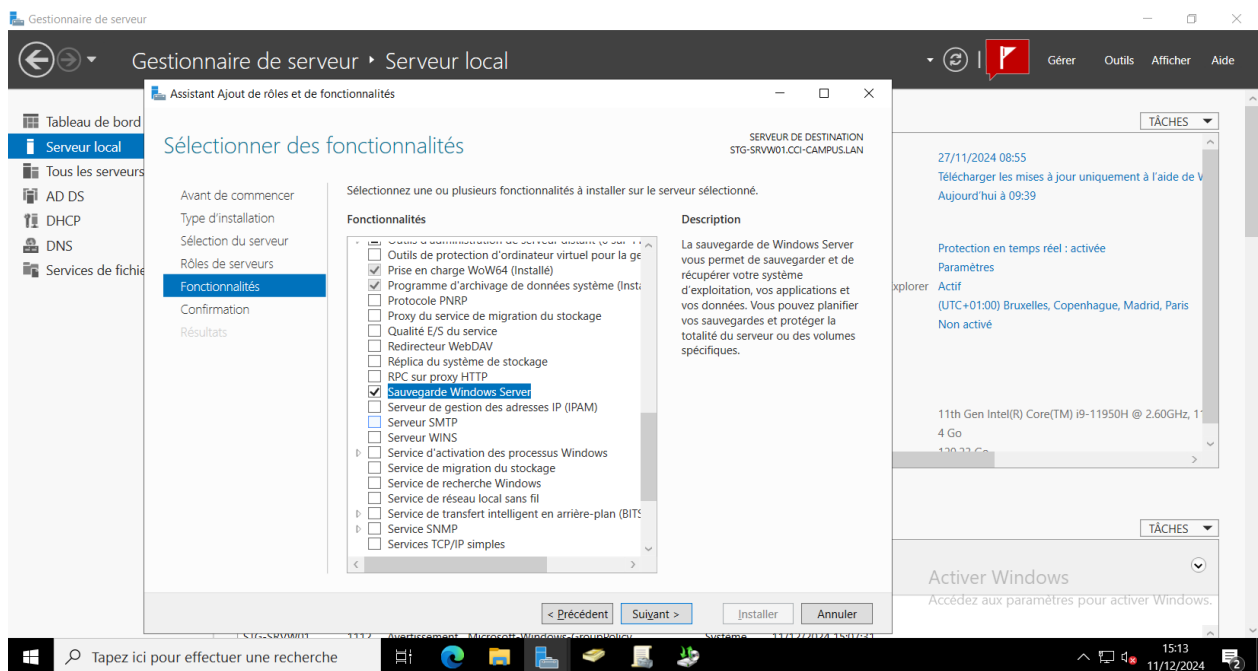


- Activé la GPO bloquant l'accès à l'invite de commande

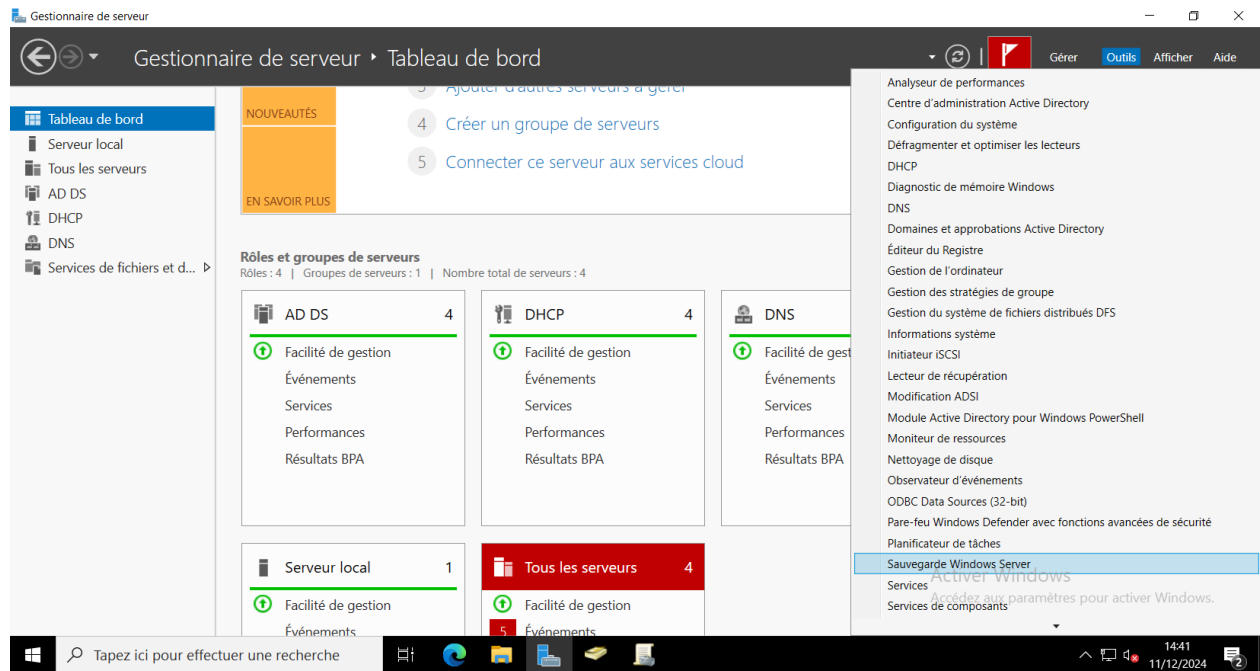


Mise en place de la sauvegarde Windows serveur

- Installer le rôle

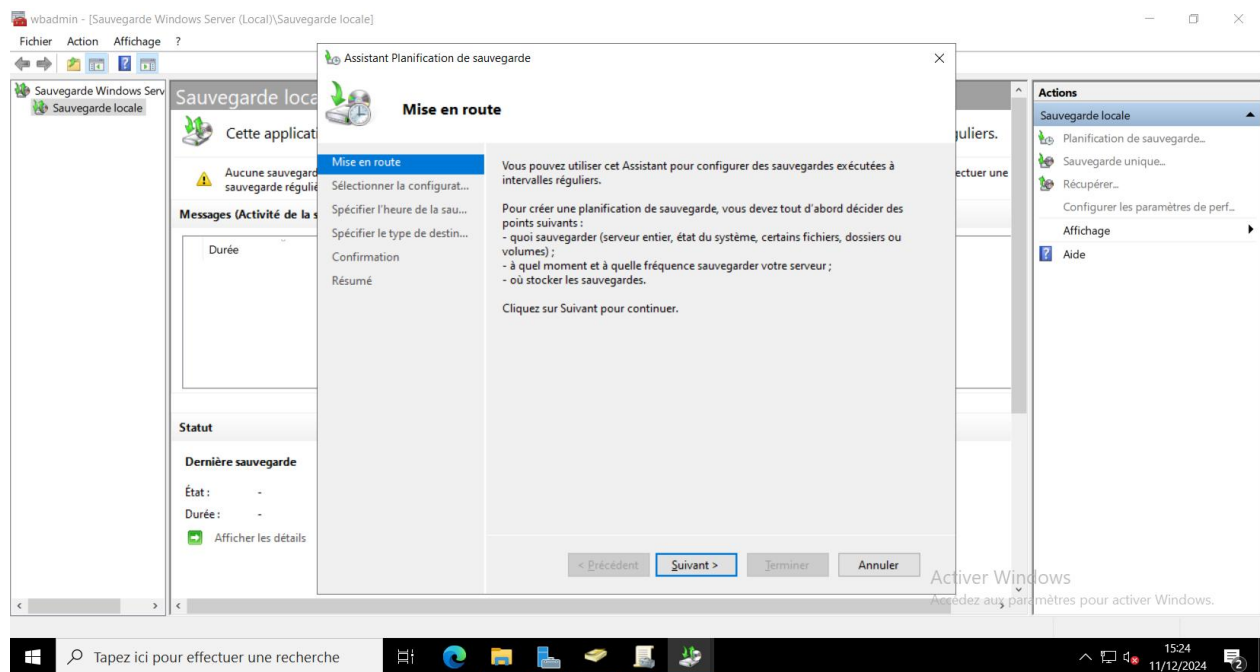


- Ensuite se rendre dans le gestionnaire de sauvegarde

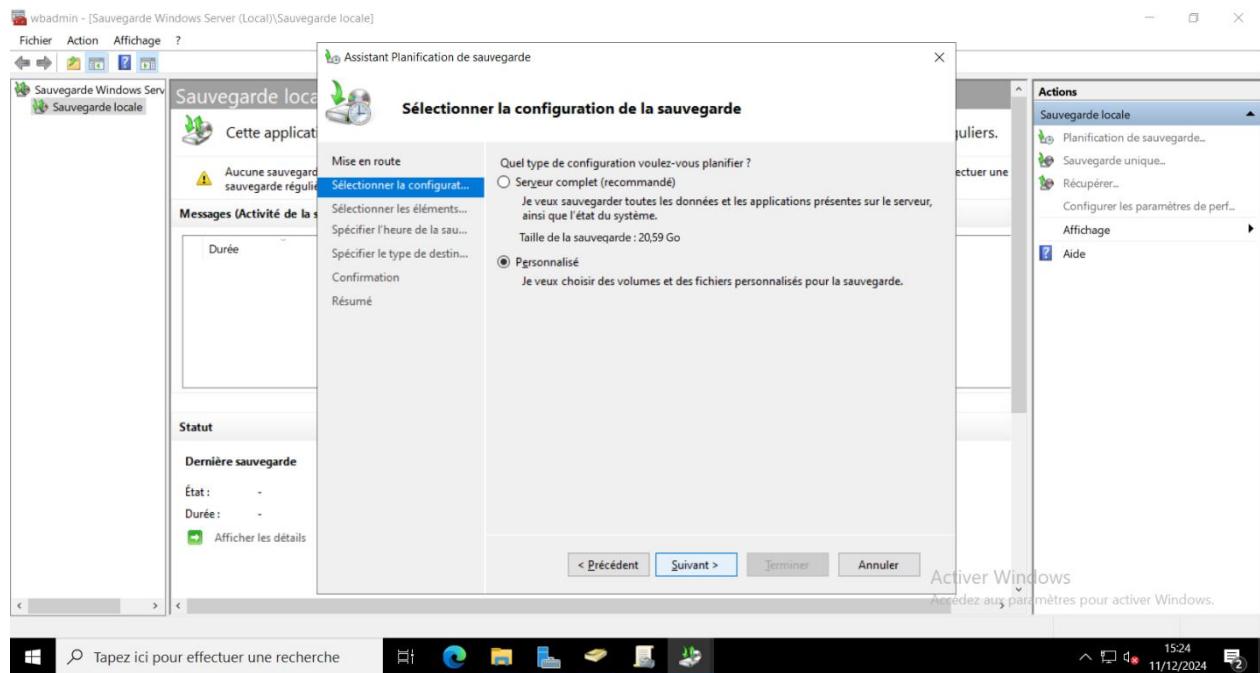


&é

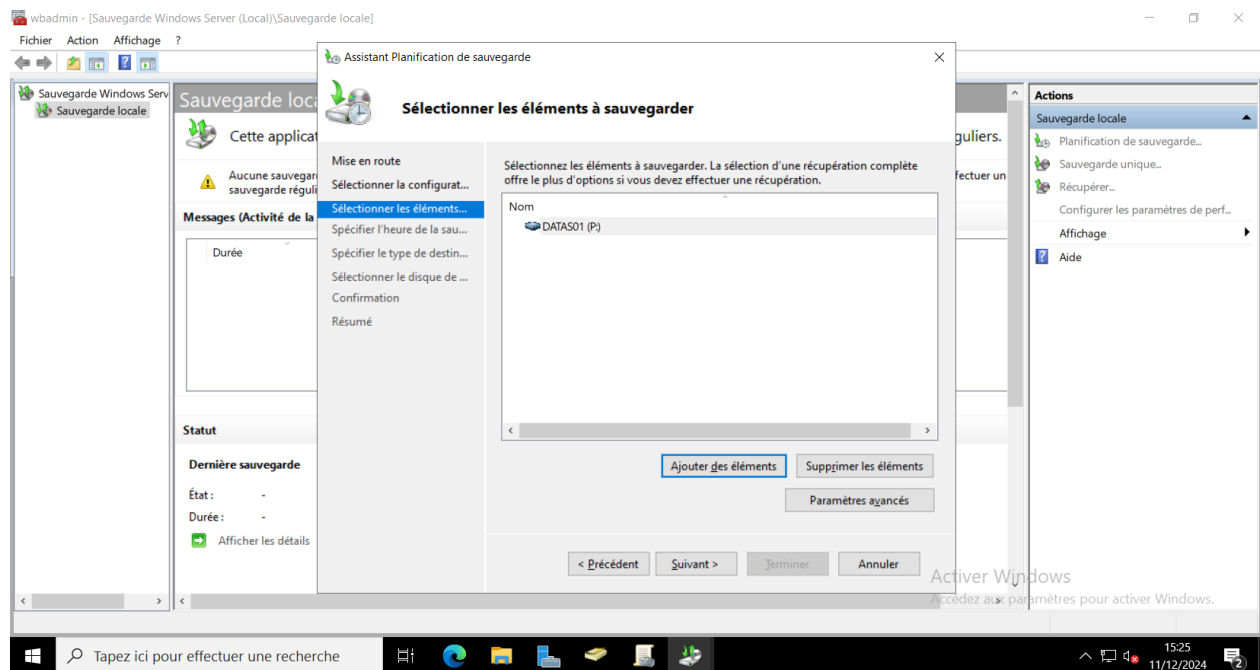
- Créer une nouvelle planification de sauvegarde



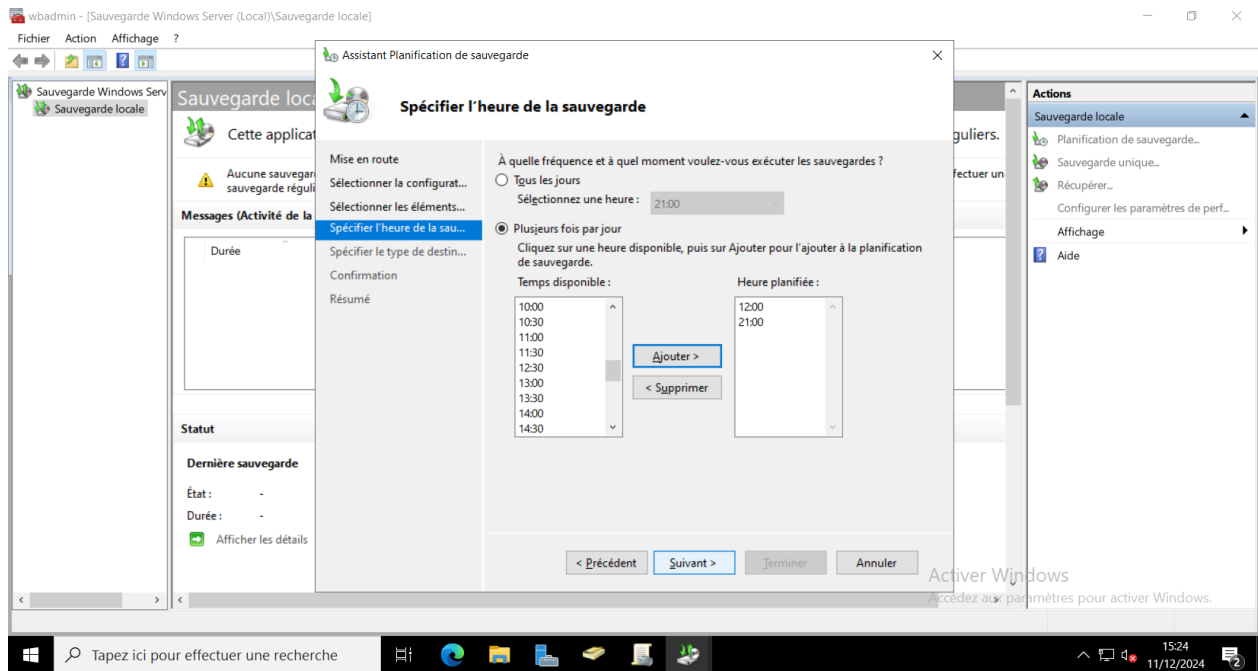
- Sélectionner une configuration personnalisée



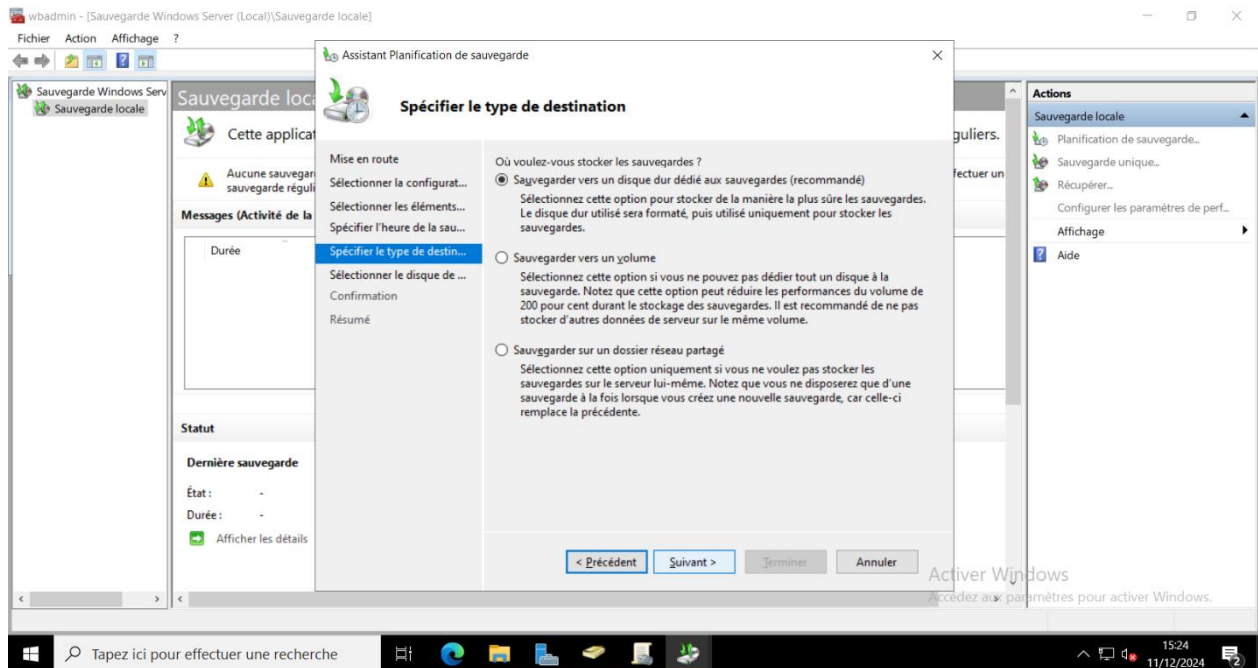
- Sélectionner le disque à sauvegarder



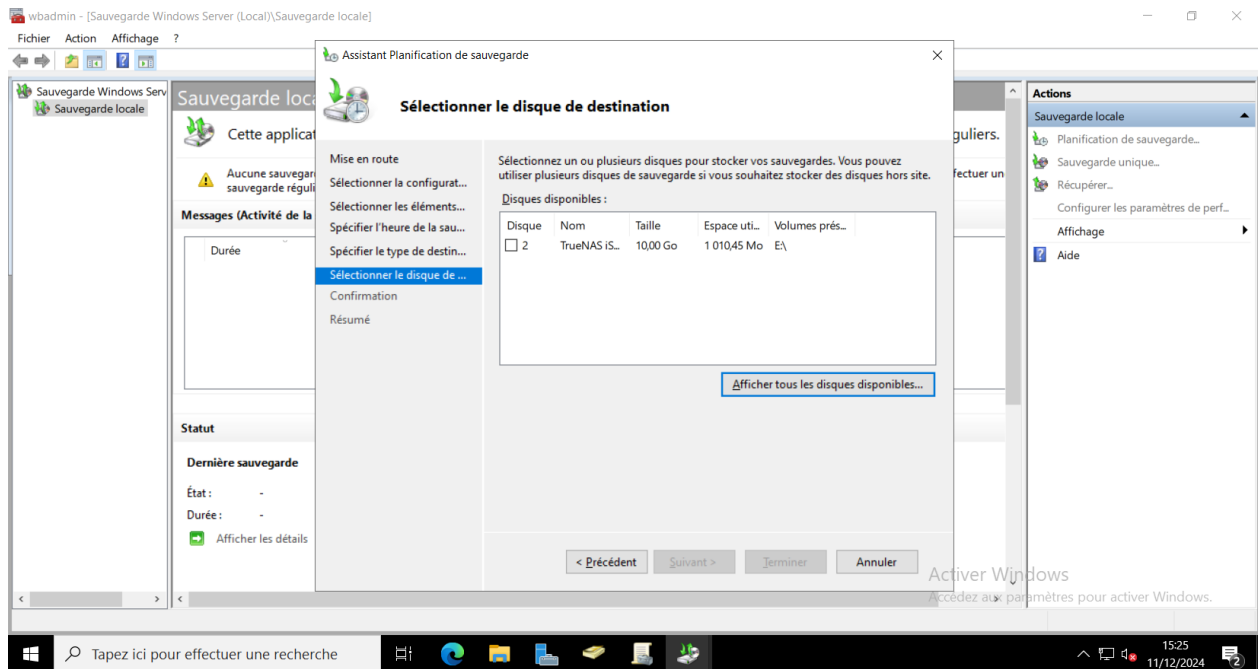
- Ajouter une sauvegarde à une heure régulière



- Sauvegarder vers un disque dur dédié aux sauvegardes



- Sélectionner le disque de sauvegarde TrueNAS ISCSI comme disque de destination



- Confirmer le tout et la sauvegarde est maintenant effective

