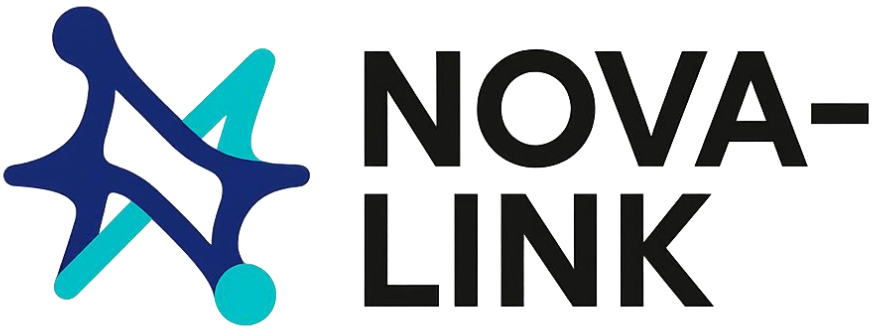
Projet « NOVA-LINK »
-
BTS SIO 2025 Option SISR
-
DOCUMENTAION TECHNIQUE



BTSSIO

CCI campus ALSACE

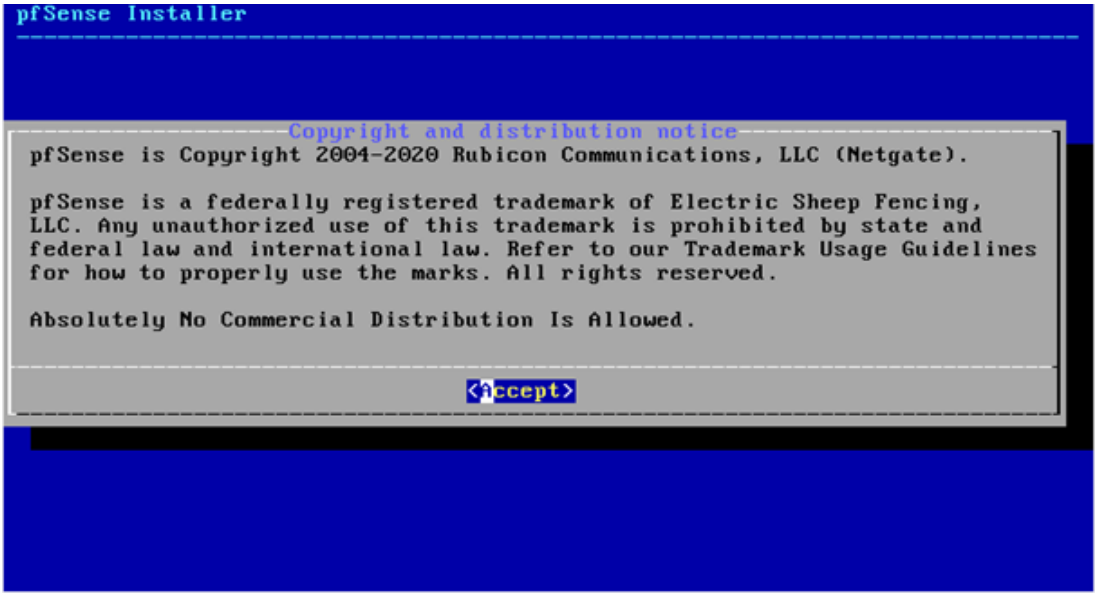
Documentation technique projet NOVA-LINK

Table des matières

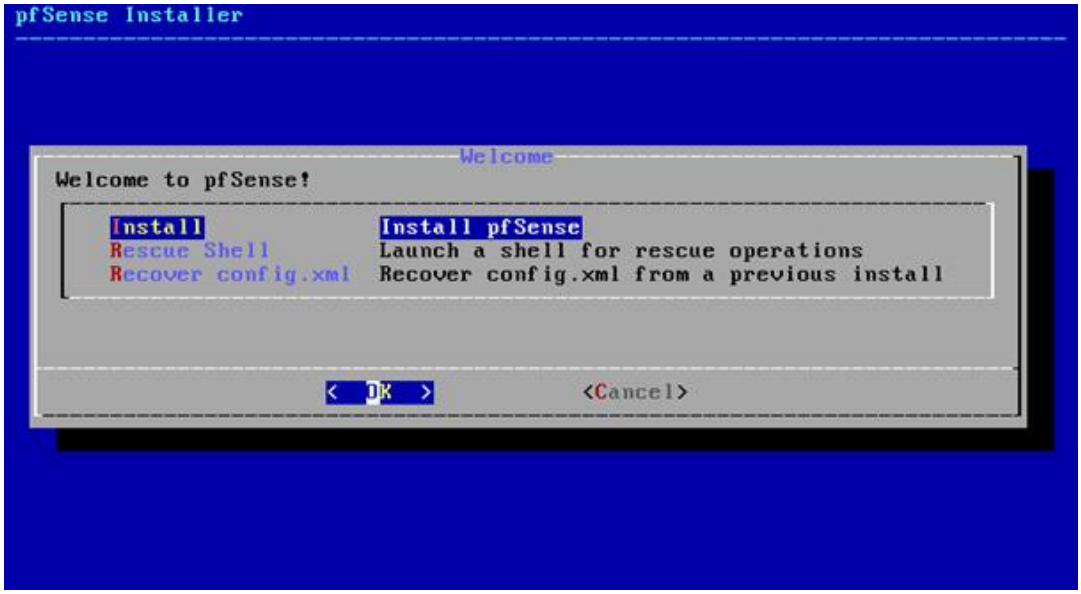
Mise en place de PfSense

Installation

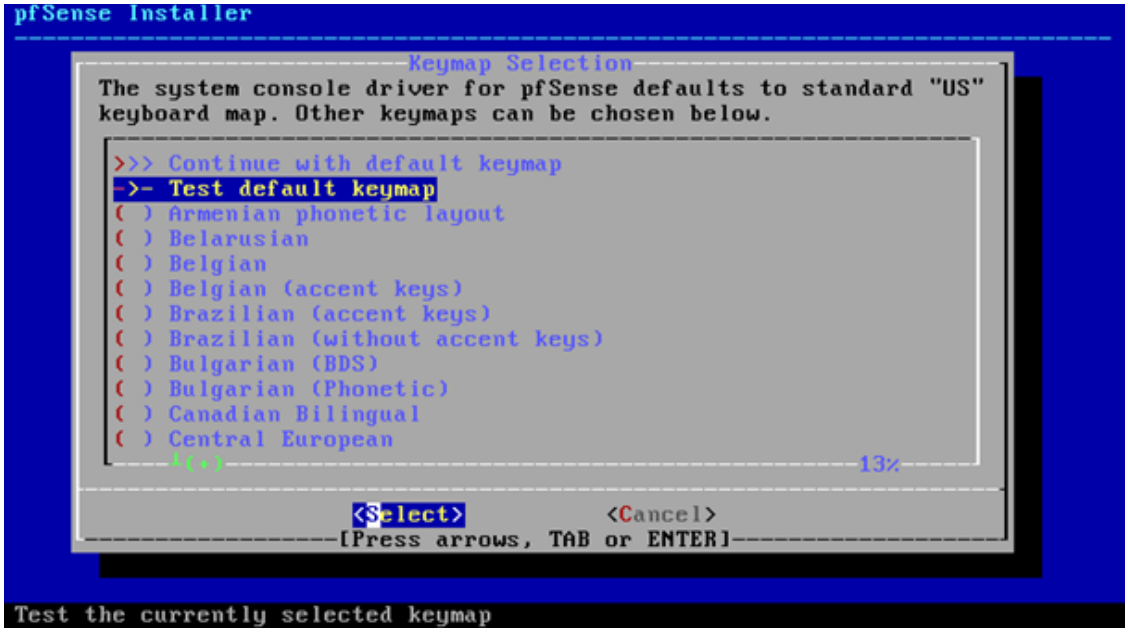
- Au commencement de l'installation, vous pourrez accepter le contrat de licence.



- Installez ensuite la distribution.

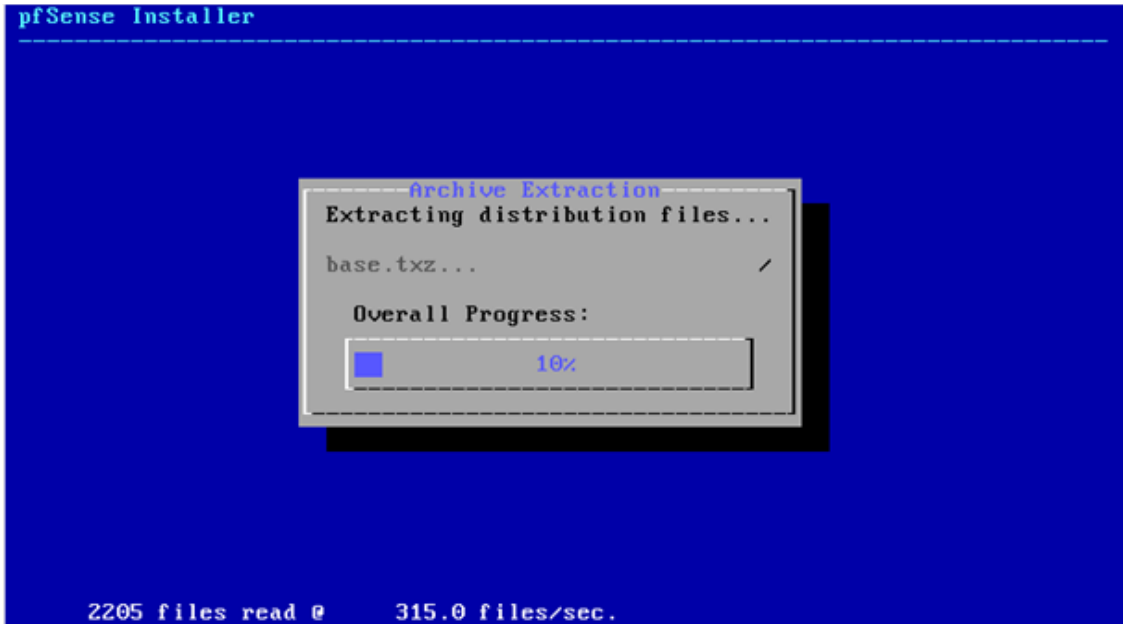


- Choisissez les paramètres linguistiques :

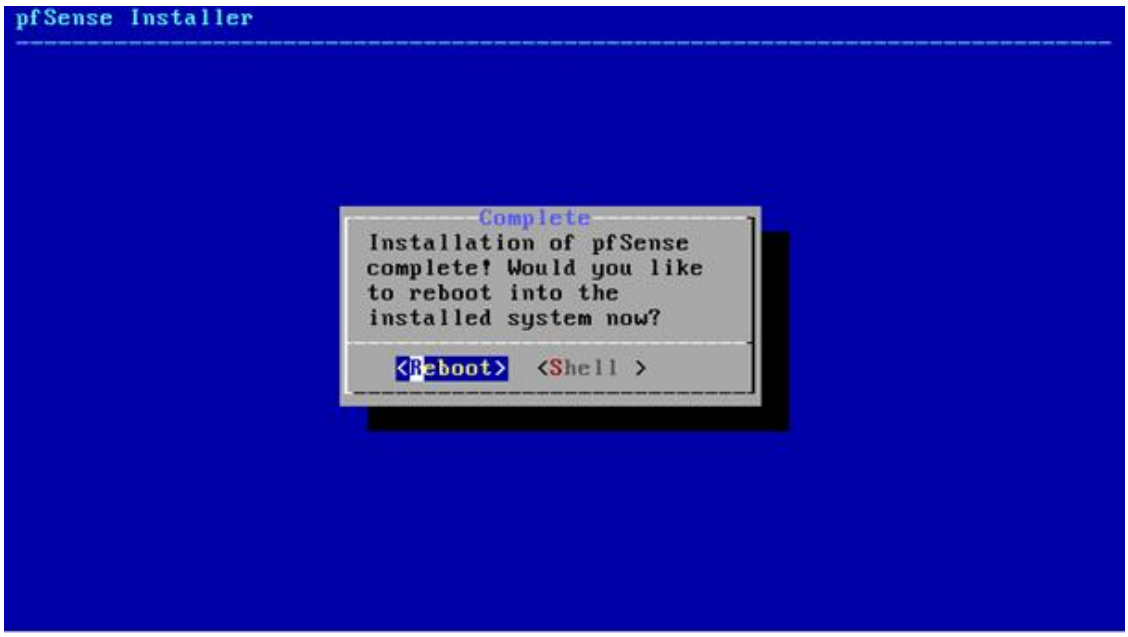


- Choisir la manière de partitionner votre disque. Ici on conservera la méthode par défaut.

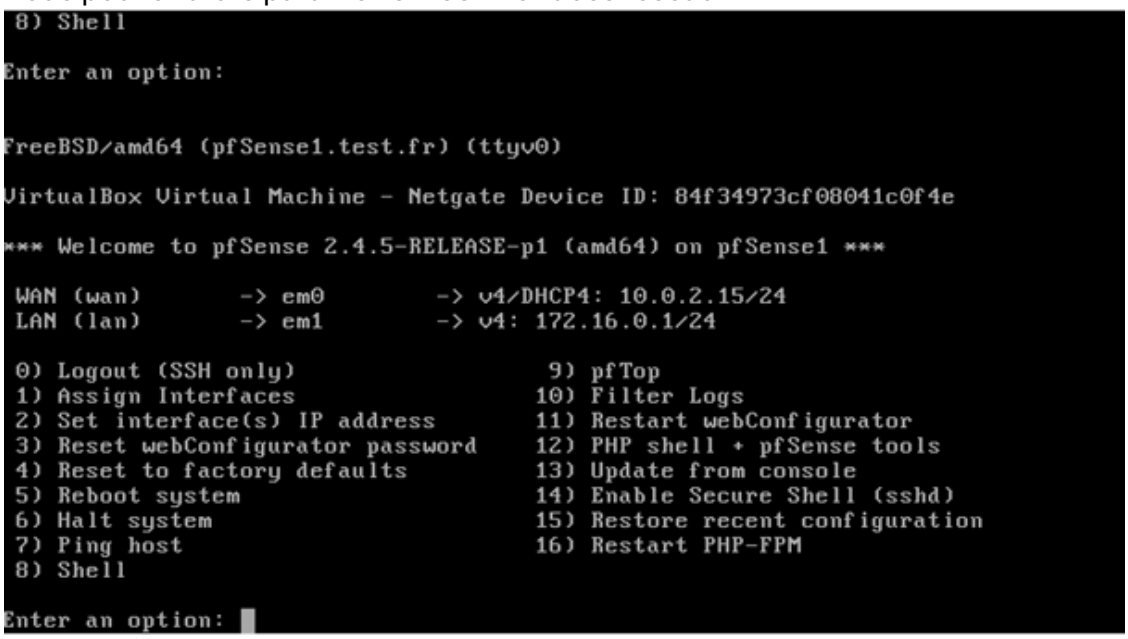
- L'installation va alors se dérouler



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



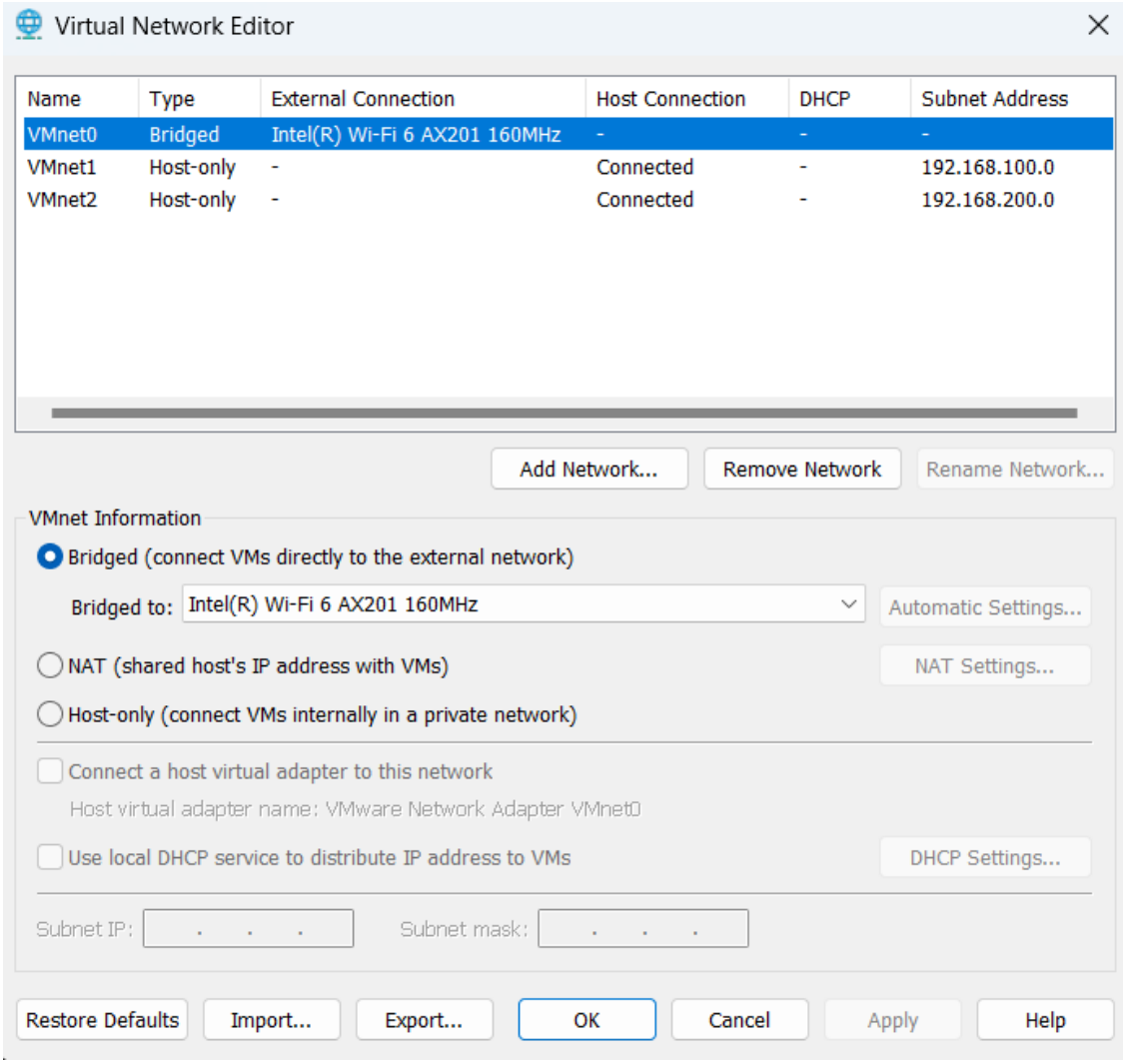
- Vous pouvez alors paramétrer vos interfaces réseau.



Configuration

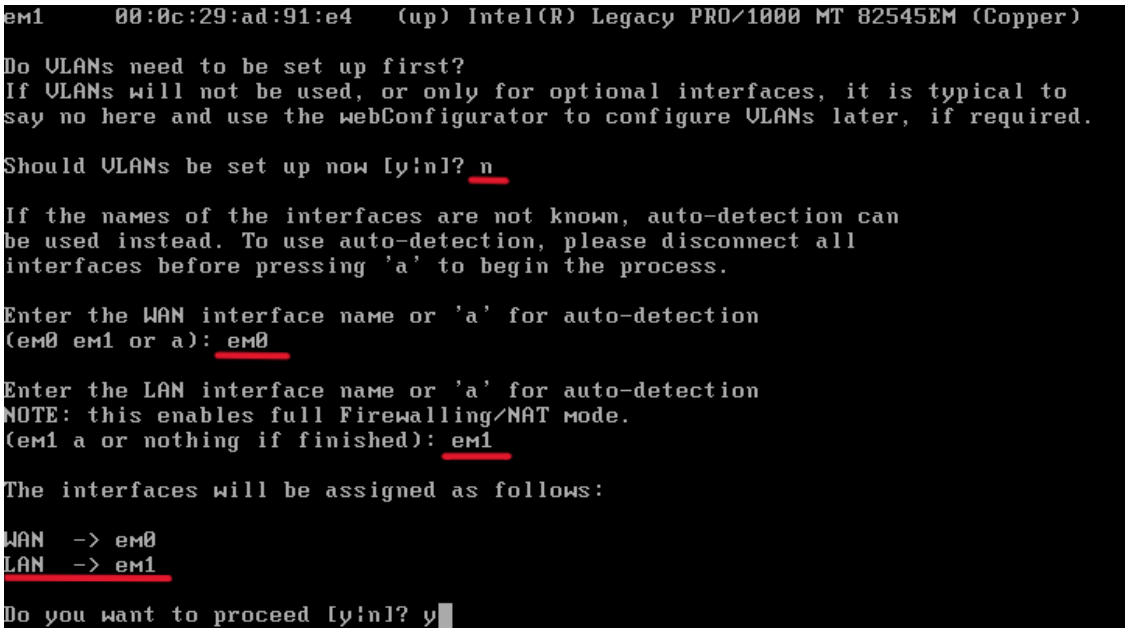
Dans un scénario de VPN site à site, nous avons besoin de deux cartes réseau sur chaque machine pfSense :

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



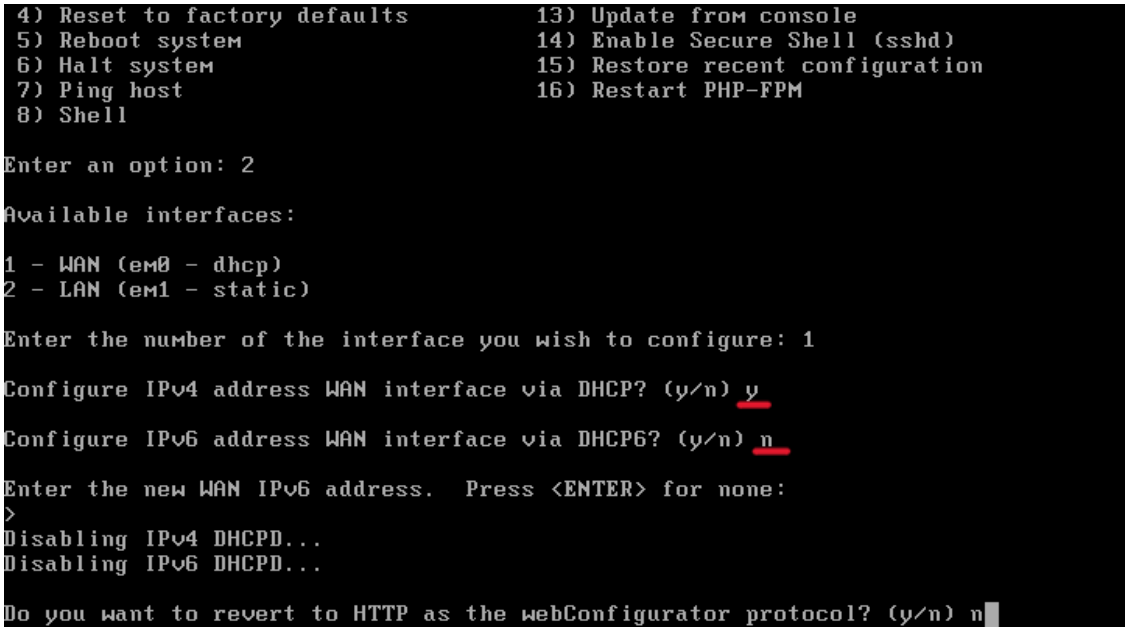
- Pour la **carte réseau 1 (WAN)**, sélectionnez **"Bridged"**. Cela permet à cette interface de se connecter directement au réseau de l'hôte et de recevoir une adresse IP du routeur.
- Pour la **carte réseau 2 (LAN)**, sélectionnez **"Host-only"**. Cela isole cette interface du reste du réseau, la connectant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

- Affecter les interfaces réseaux

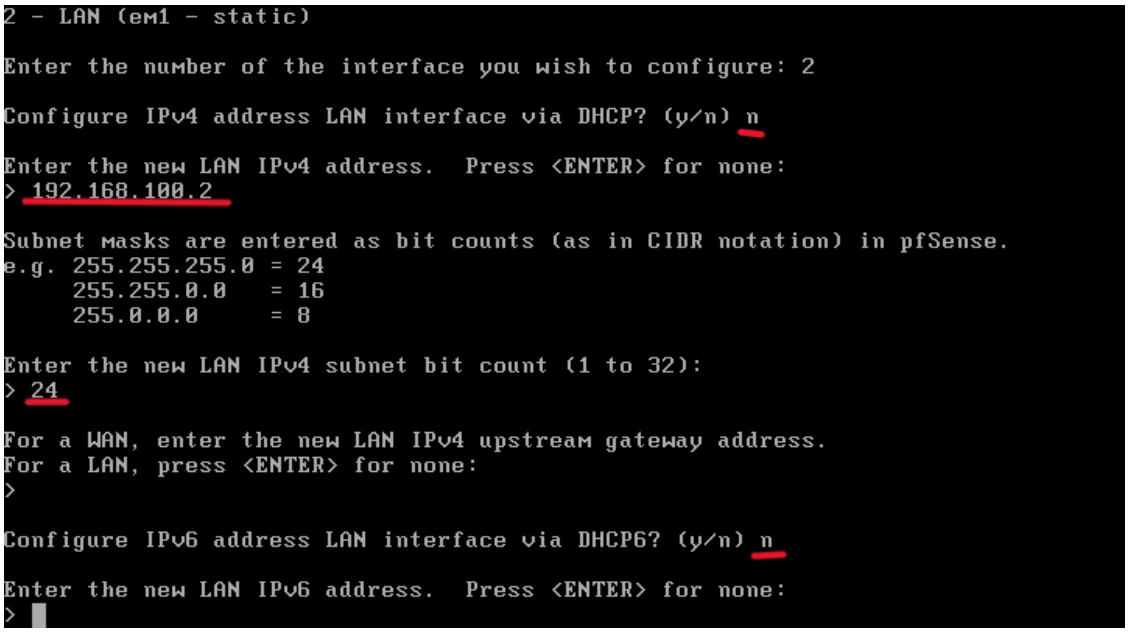


- Par défaut, pfSense va détecter les interfaces réseau. Vous verrez des interfaces appelées **em0**, **em1**, etc., qui correspondent aux adaptateurs réseau que vous avez configurés.
- Attribuez **em0** à l'interface **WAN** et **em1** à l'interface **LAN**.

- Cnfiguration IP initial



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

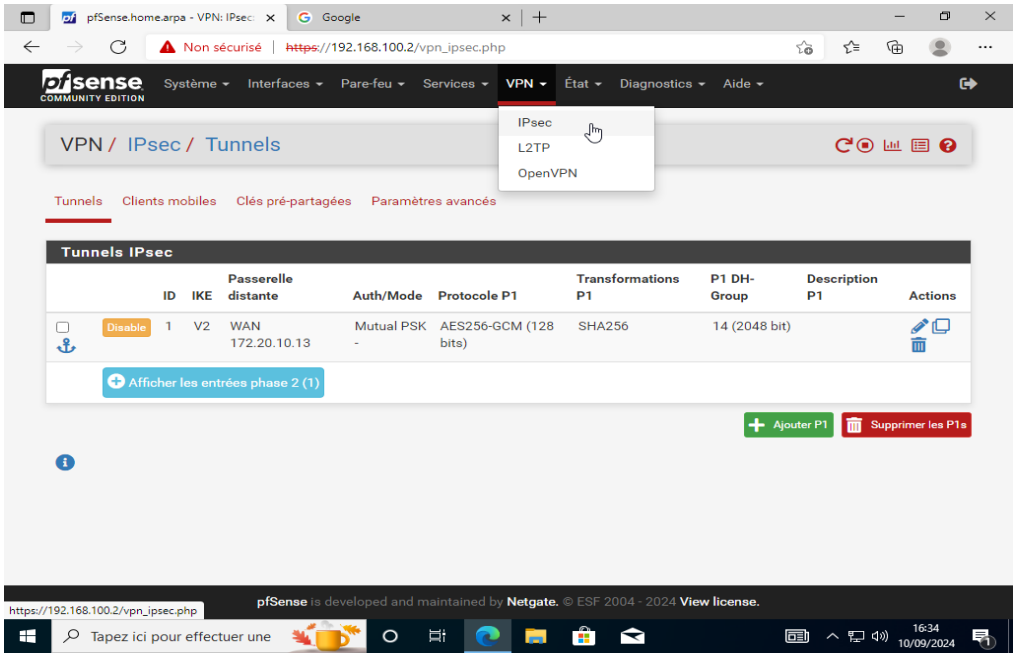


- Pour l'interface **LAN**, configurez une IP statique, par exemple **192.168.100.2/24**.

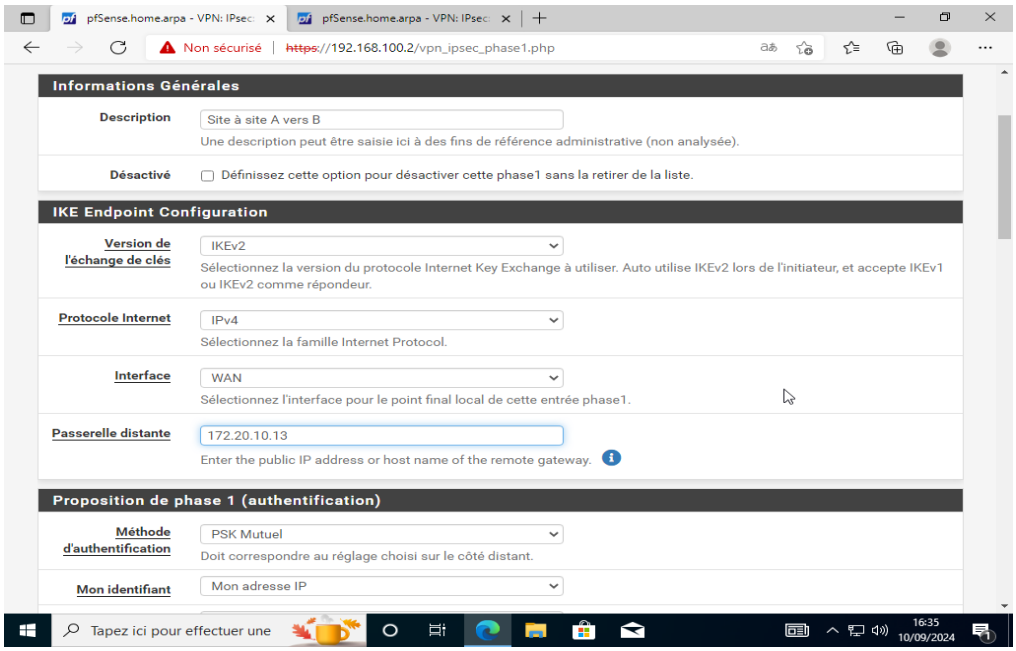
Vous pouvez maintenant accéder à l'interface Web de PfSense via l'adresse **192.168.100.2** depuis une autre machine virtuelle connectée au réseau **Host-only**.

Création du tunnel VPN

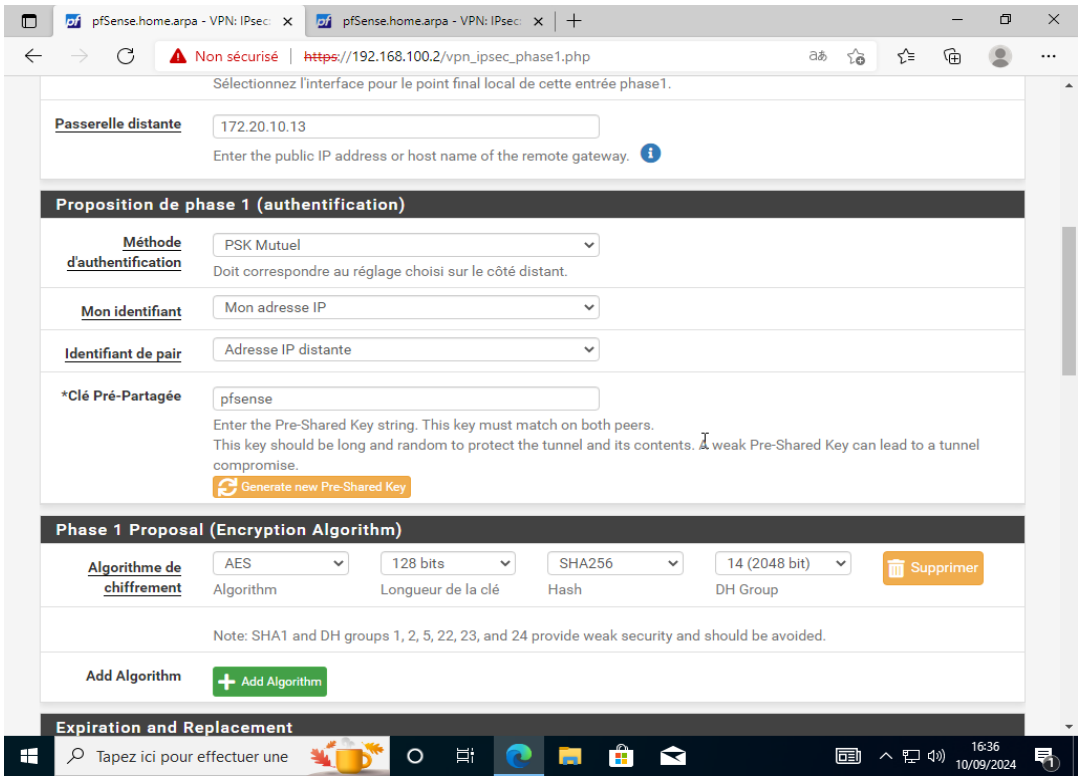
- Une fois dans l'interface Web de PfSense, pour créer la connexion VPN il faut ce rendre dans l'onglet **VPN** -> **IPsec**

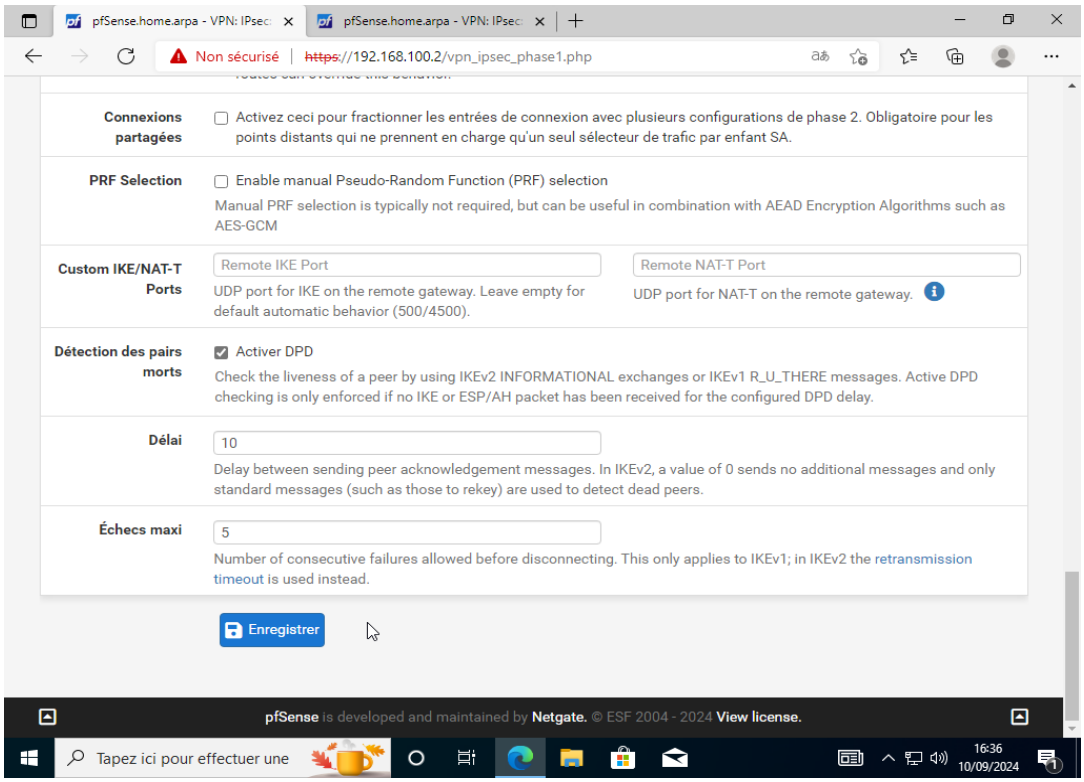


- Dans le menu **IKE Endpoint Configuration** -> **Passerelle distante** mettre l'adresse IP WAN de l'autre routeur

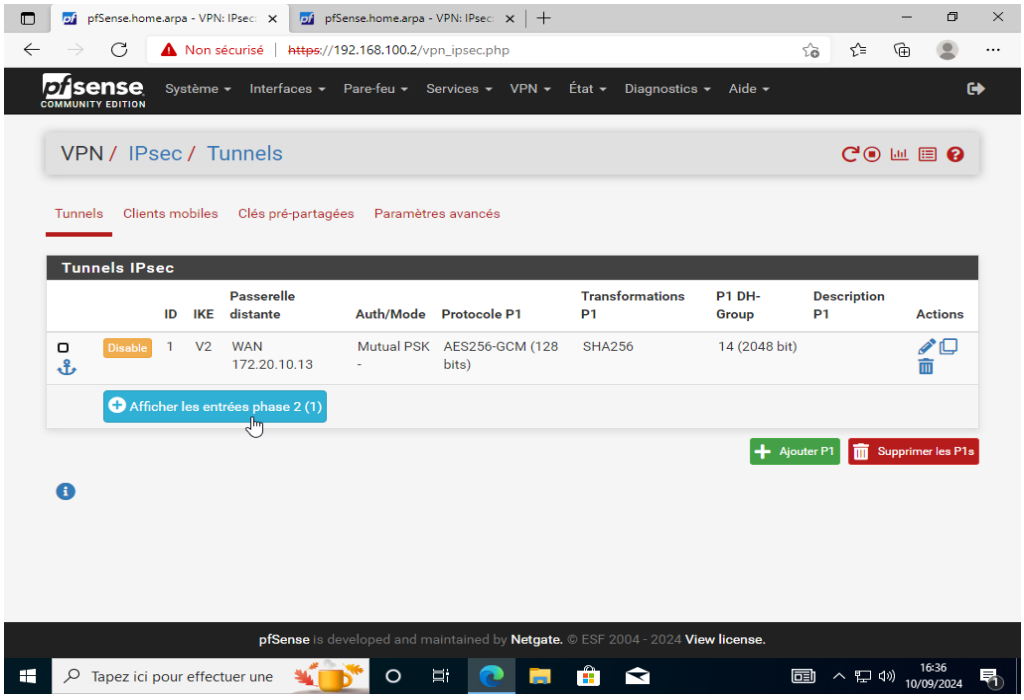


- Laisser les paramètres par défauts et enregistrer

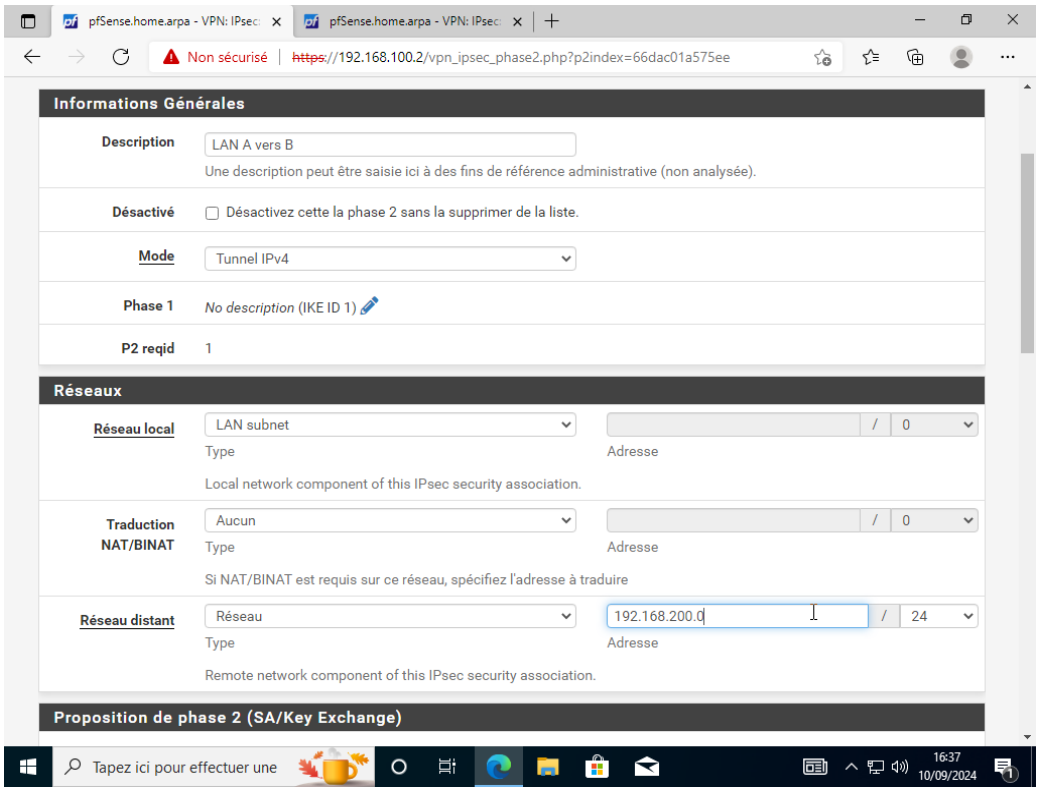




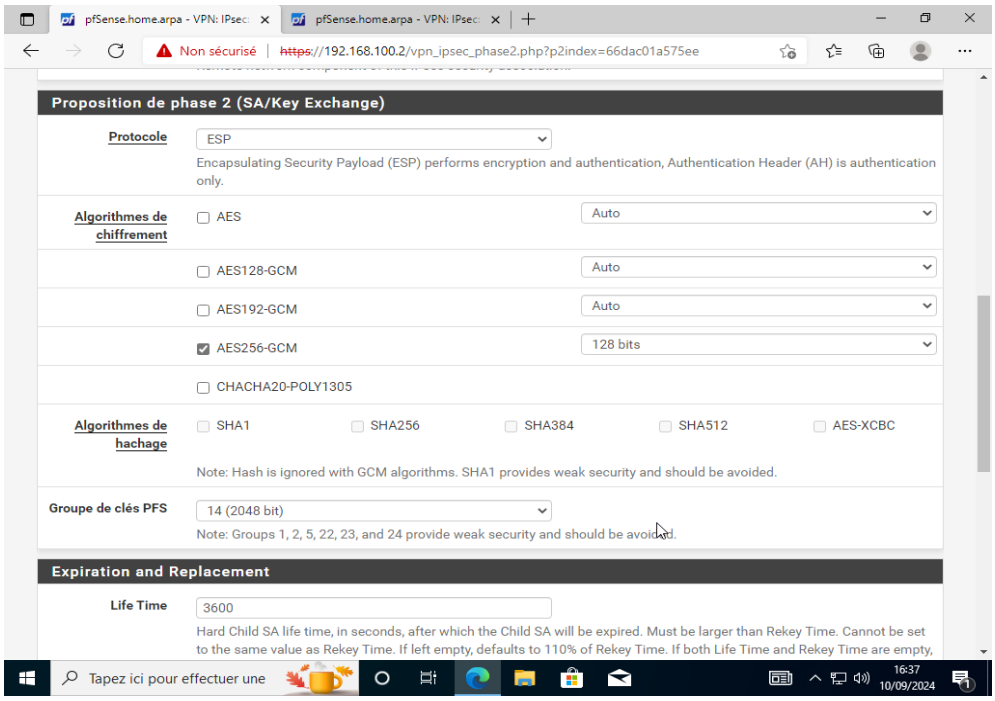
- Configurer la phase 2 en cliquant sur **Afficher les entrées phase 2** puis **Ajouter P2**



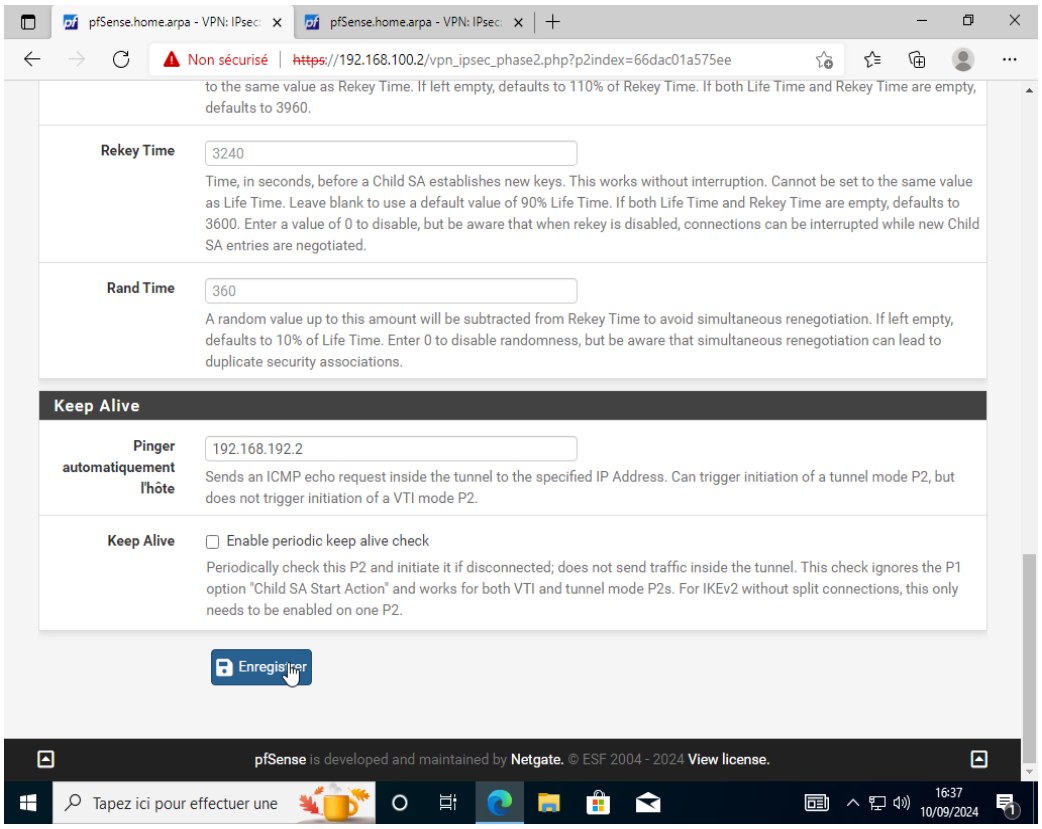
- Dans le menu **réseaux** dans le champs **réseau distant** mettre l'ip du réseau **LAN** de l'autre routeur. Mettre le subnet correspondant, en occurrence **/24**

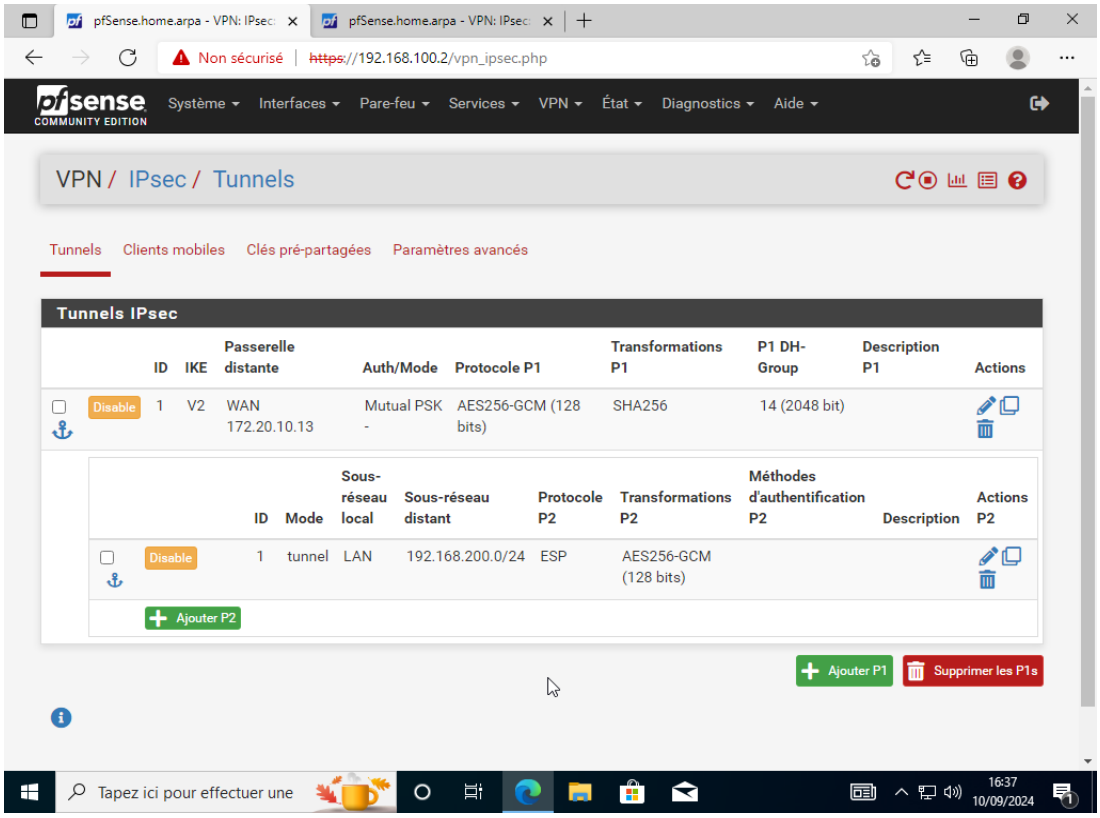


- Sélectionner algorithme de chiffrement **AES256-GCM**



- Enregistrer tout et le résultat devrais être le suivant

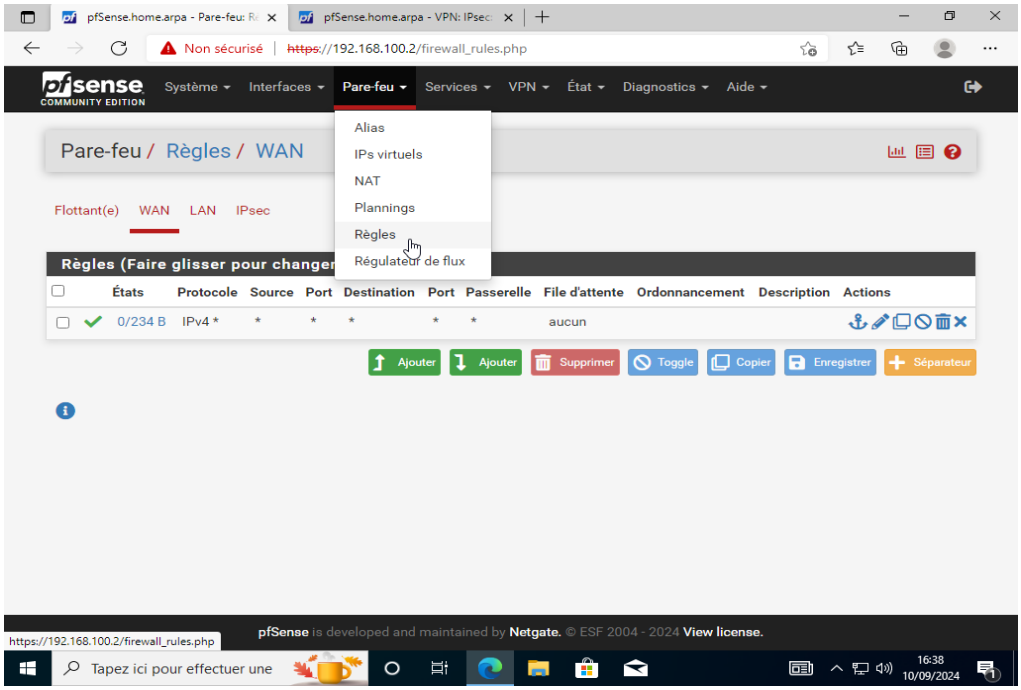

pfSense.home.arpa - VPN: IPsec
Non sécurisé | https://192.168.100.2/vpn_ipsec_phase2.php?p2index=66dac01a575ee
to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.
Rekey Time
3240
Time, in seconds, before a Child 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
360
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
192.168.192.2
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
16:37
10/09/2024


pfSense.home.arpa - VPN: IPsec
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)
ID
Mode
Sous-réseau local
Sous-réseau distant
Protocole P2
Transformations P2
Méthodes d'authentification P2
Description
Actions P2
Disable
1
tunnel
LAN
192.168.200.0/24
ESP
AES256-GCM (128 bits)
Ajouter P2
Ajouter P1
Supprimer les P1s
Tapez ici pour effectuer une
16:37
10/09/2024

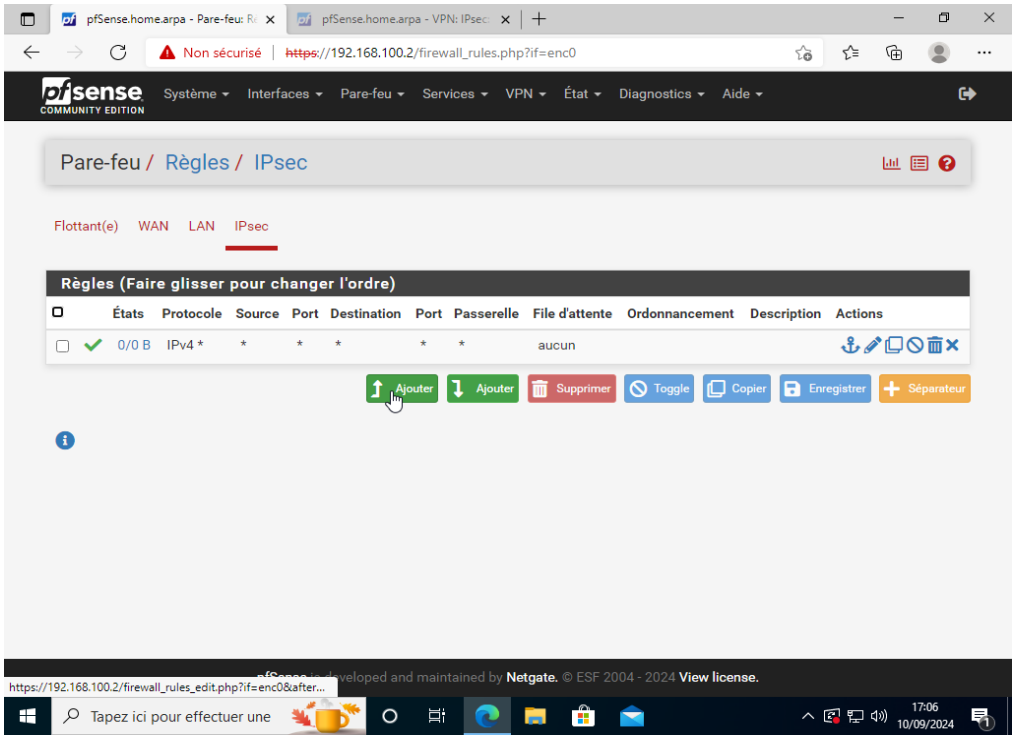
Le tunnel VPN est créer, maintenant il faut se rendre sur le second routeur et refaire la même configuration en mettant les adresses ip du premier serveur.

Configuration du pare-feu

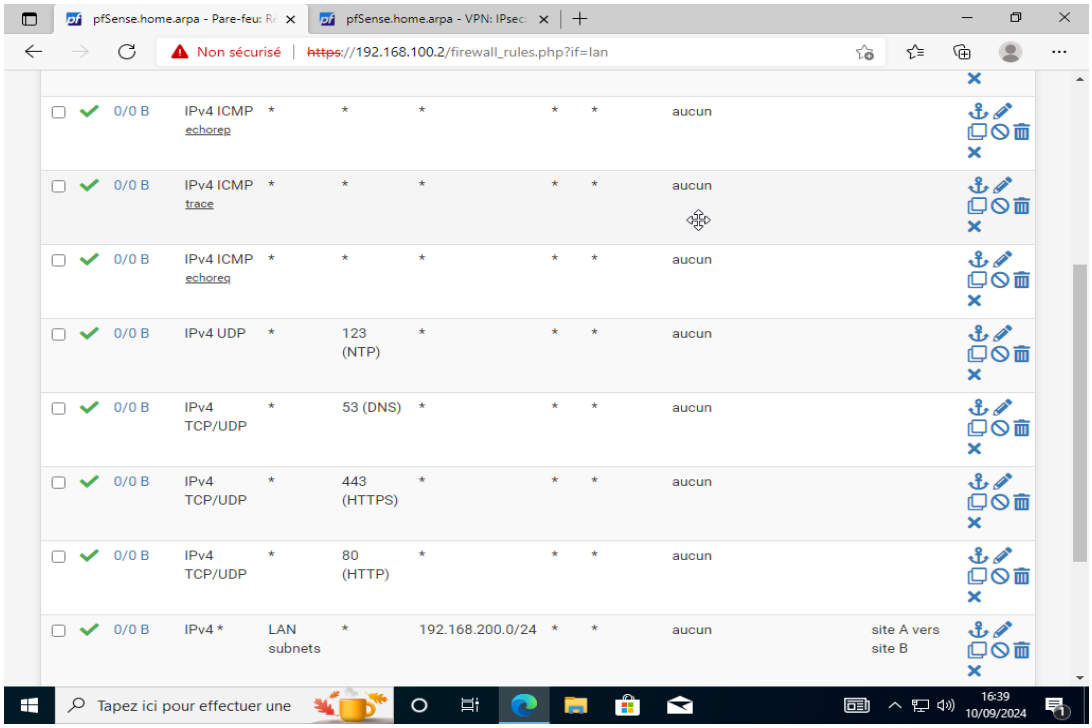
- Pour configurer les règles du pare-feu il faut se rendre dans le menu **Pare-feu** -> **Règles**



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



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



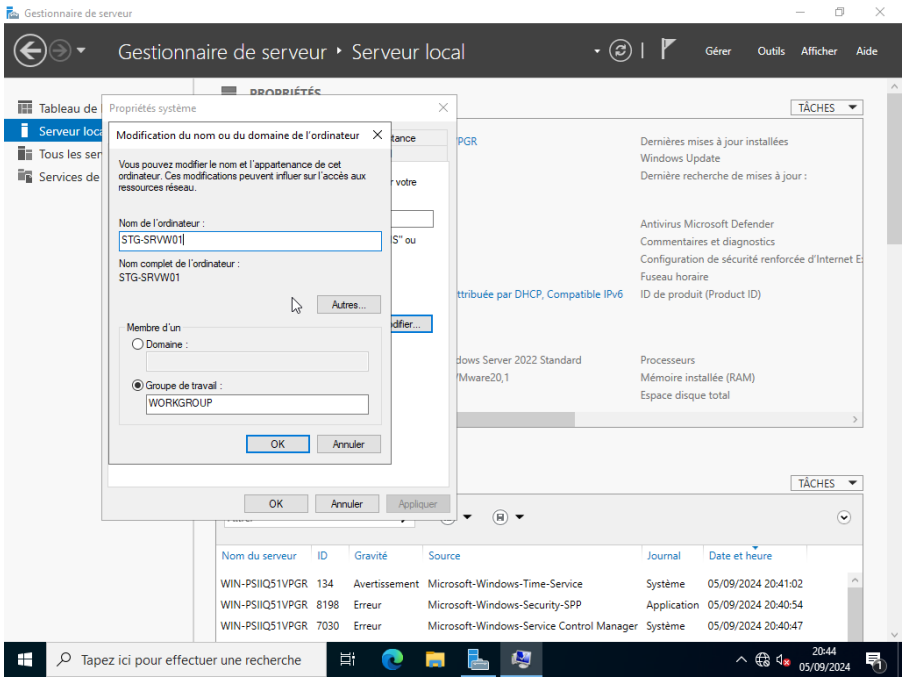
- Répéter les mêmes règles pare feu sur le second serveur.

Les routeurs sont maintenant prêts à l'emploie.

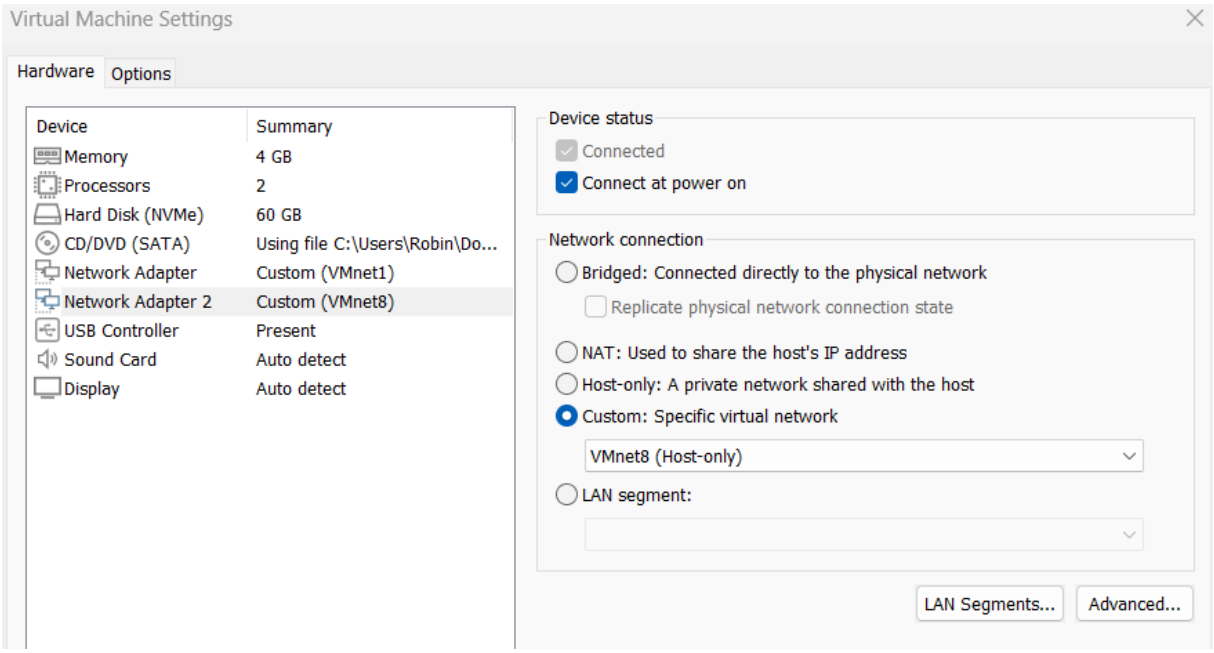
Installation de l'AD, DNS, DHCP

Configuration de l'IP BONDING

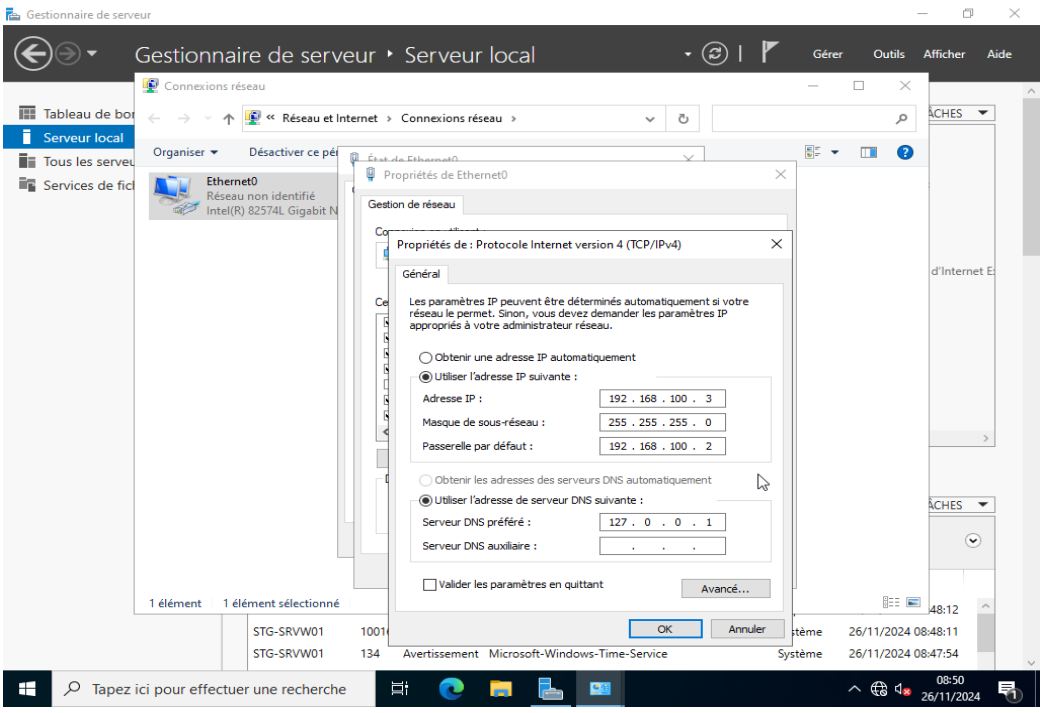
- Renommer le serveur



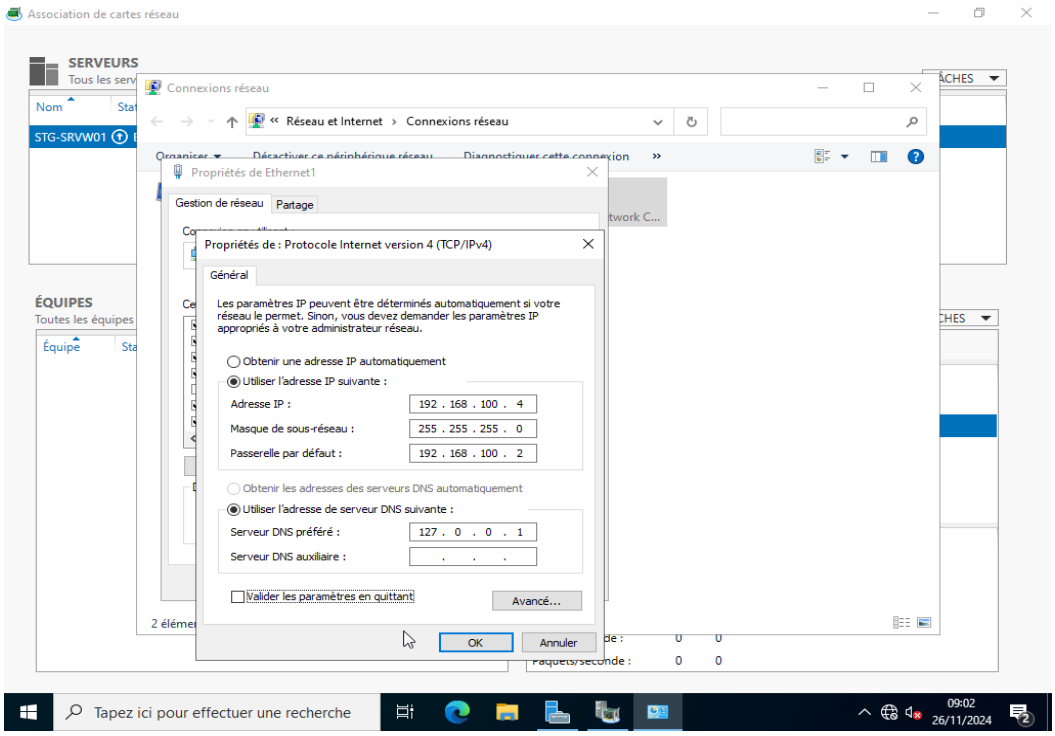
- Ajouter une deuxième carte réseau



- Configuration de la première carte réseau

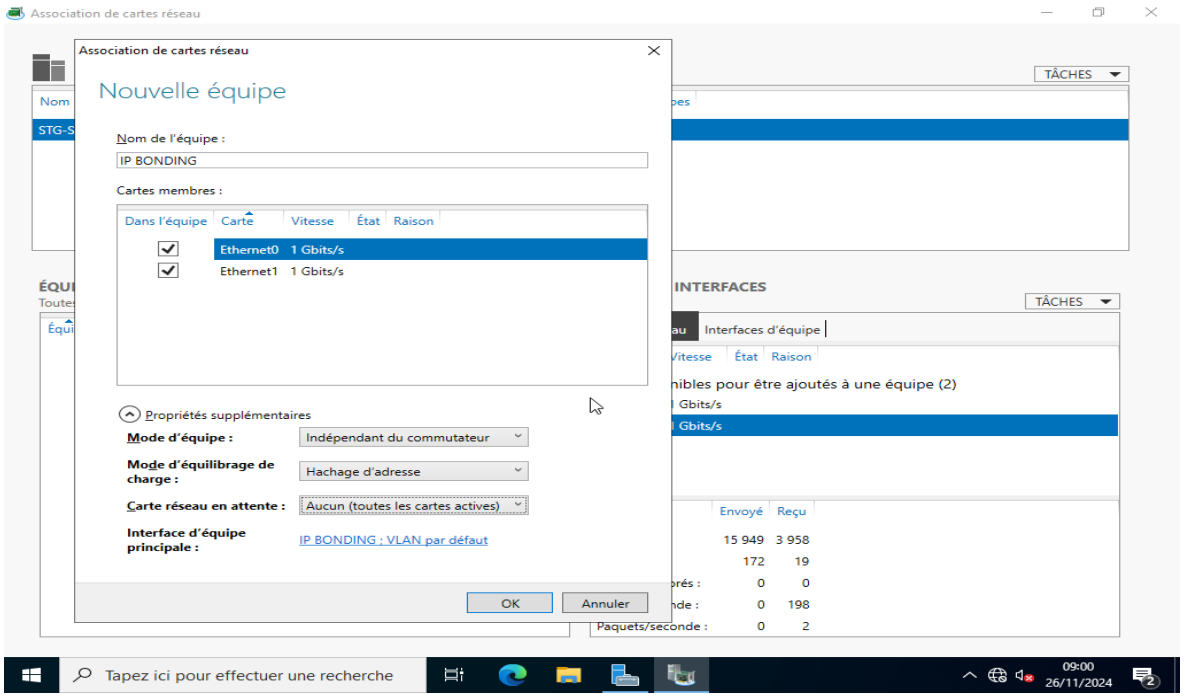


- Configuration de la deuxième carte réseau

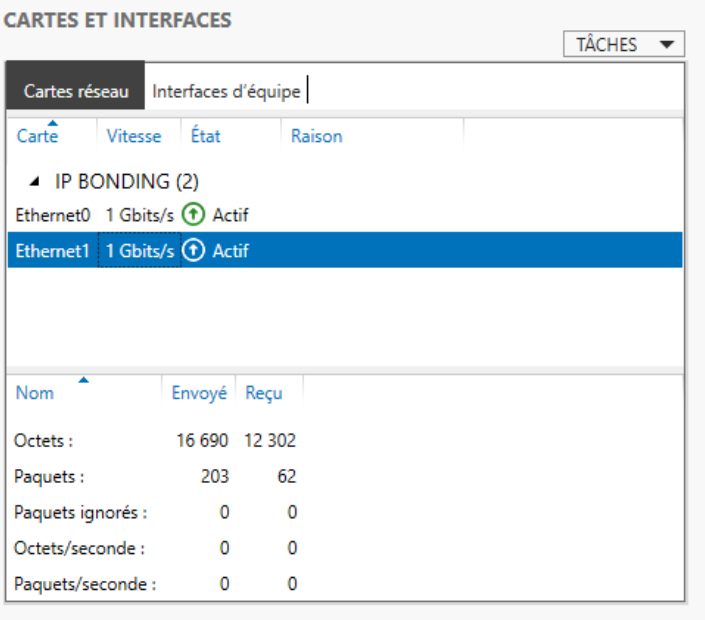


- Configuration de l'IP Bonding -> se rendre dans association des cartes réseaux puis ajouter une nouvelle équipe et sélectionner les deux cartes réseaux

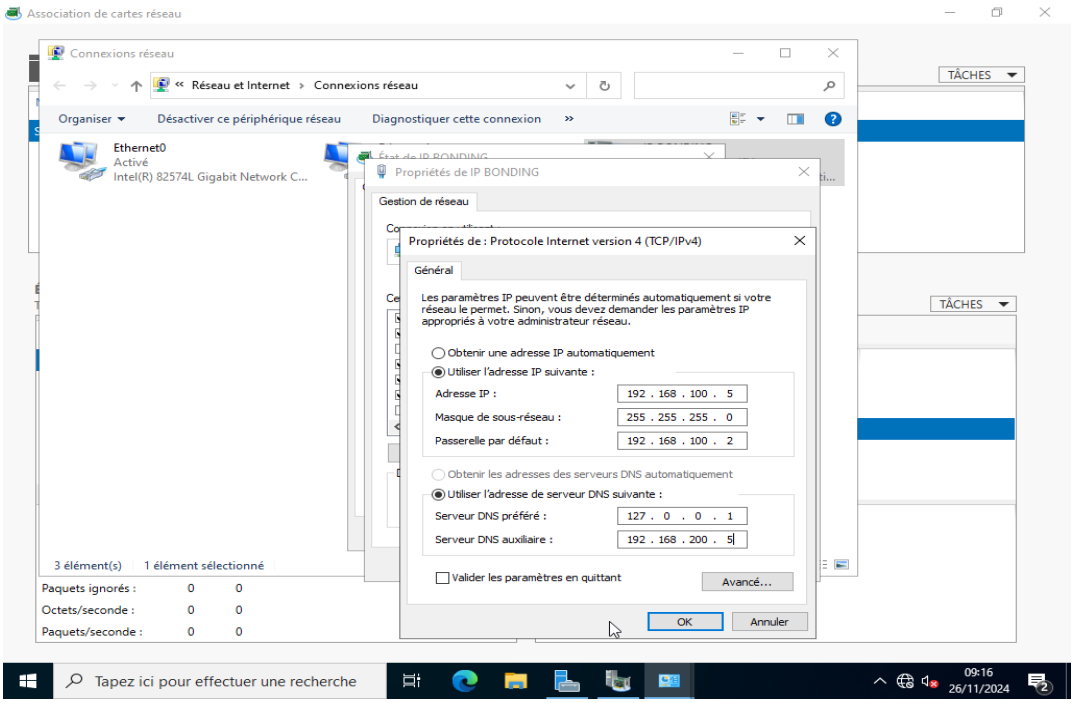
Dans les propriétés supplémentaires configurer le mode d'équilibrage de charge en hachage d'adresse.



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

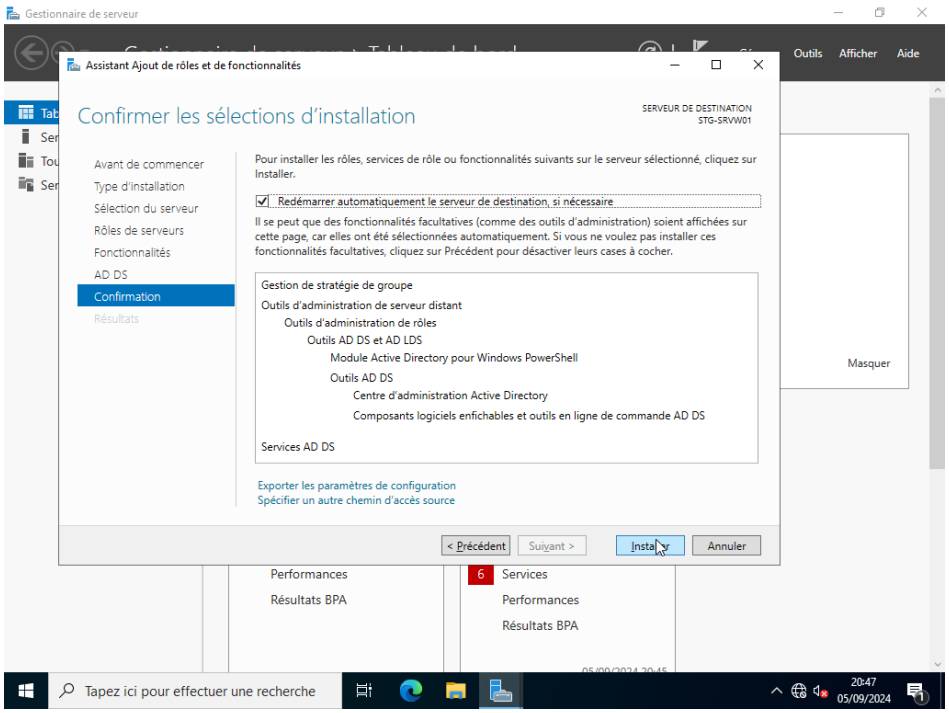


- Configuration de la carte réseau créer avec l'IP Bonding

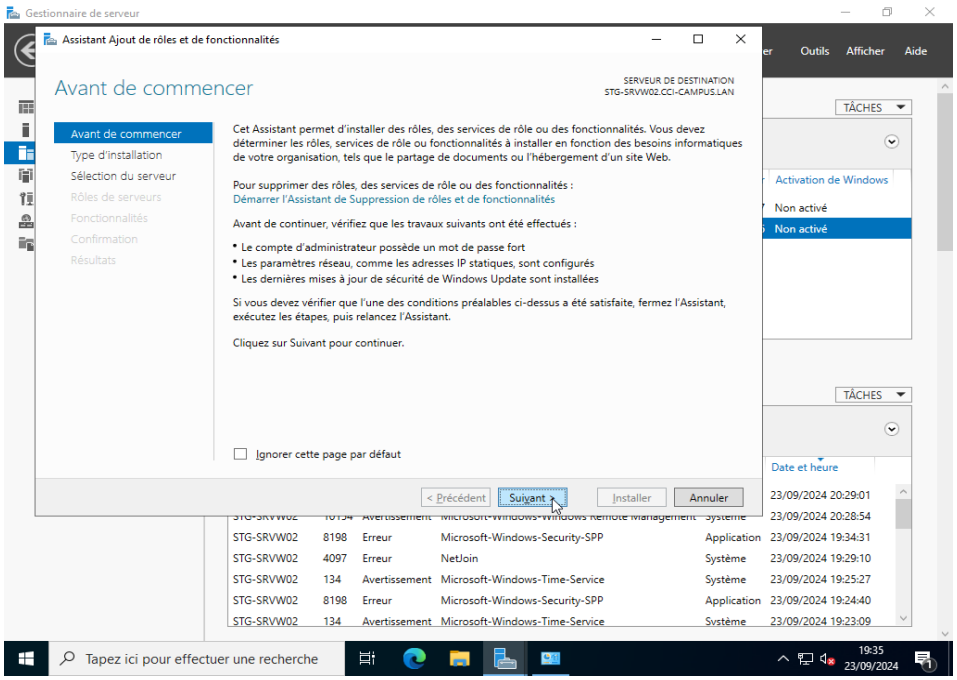


Installation de l'AD

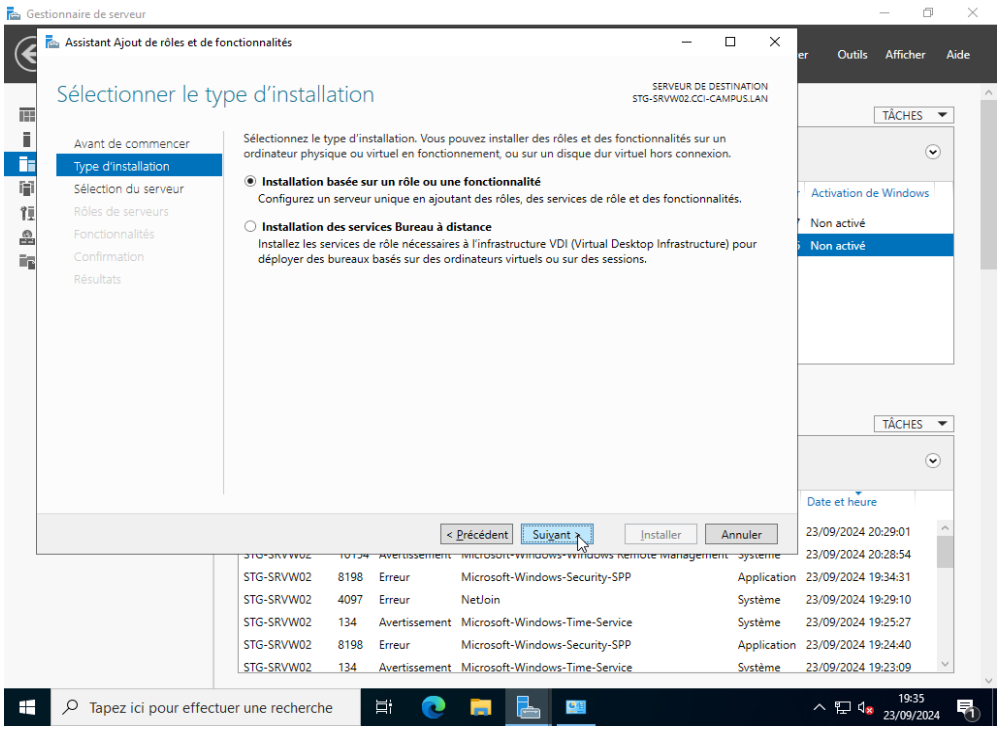
- Cliquer sur **ajout des rôles et fonctionnalités**



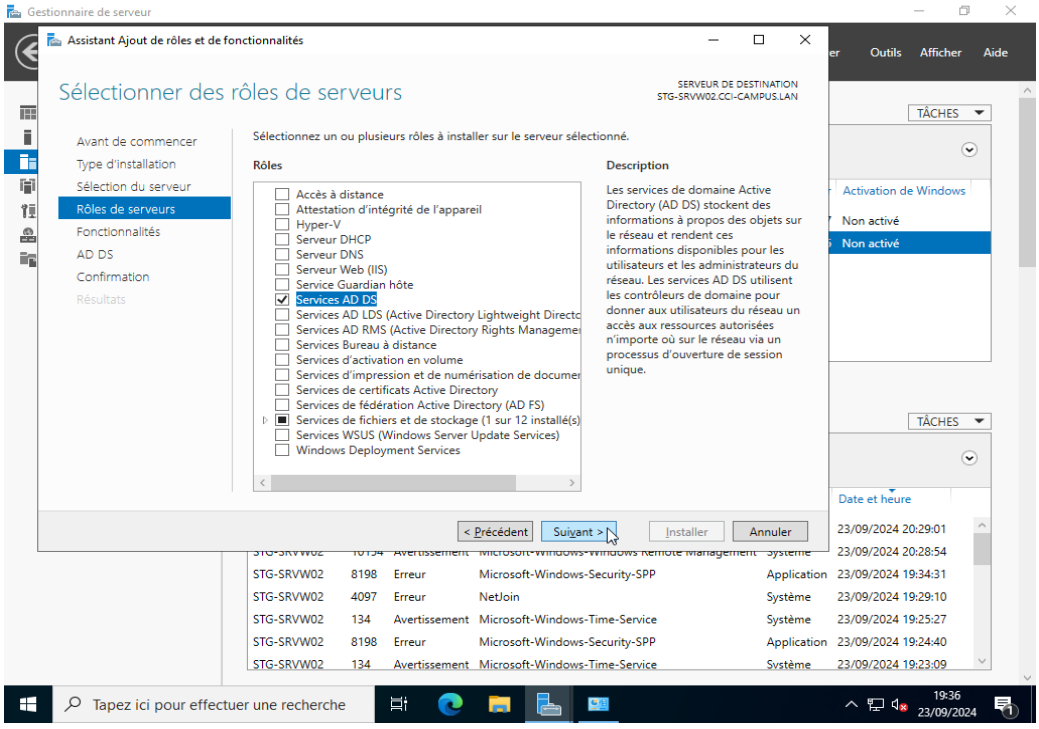
- Puis cliquer sur **suivant**



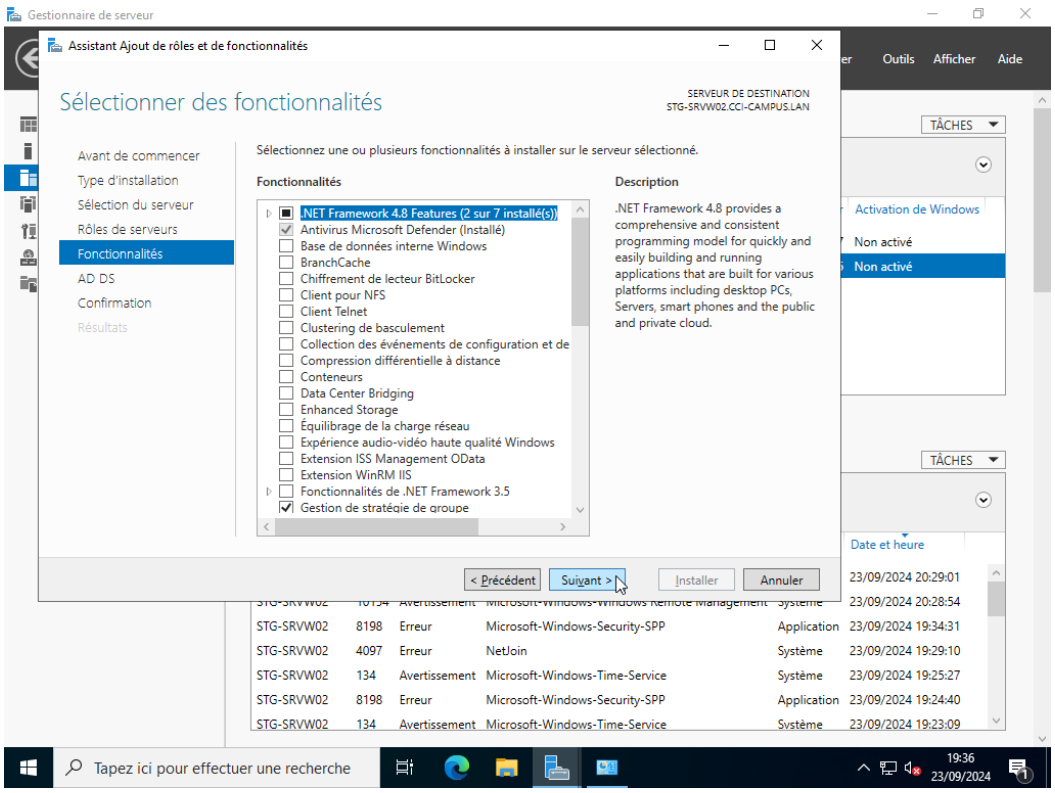
- Encore sur **suivant**



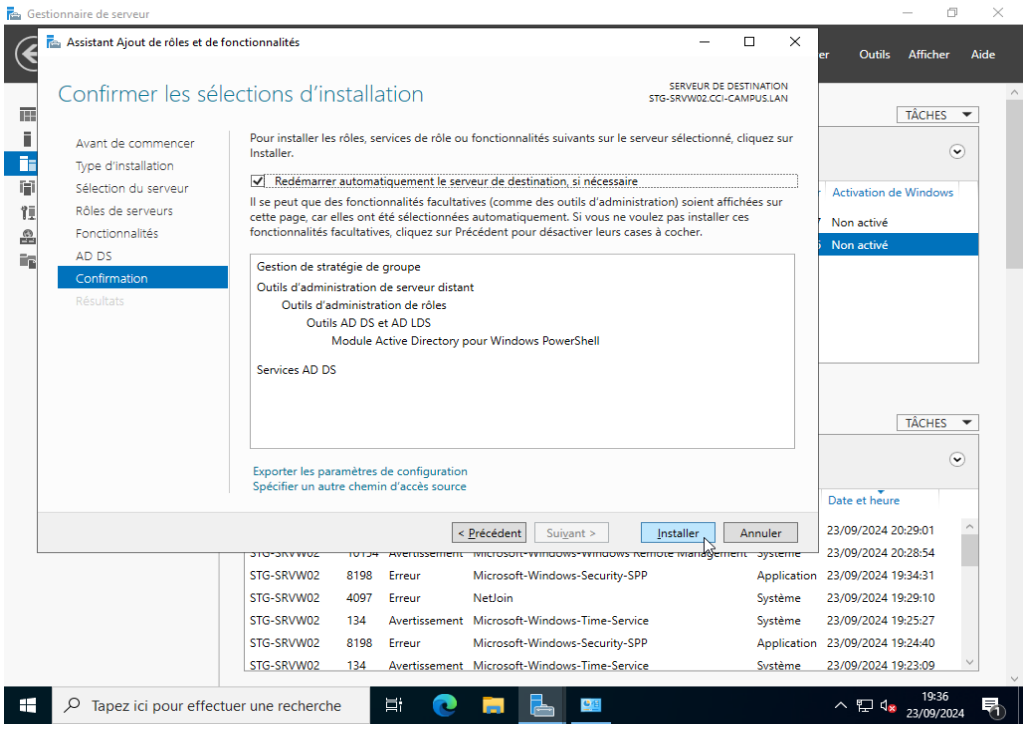
- Sélectionner **Services AD DS**



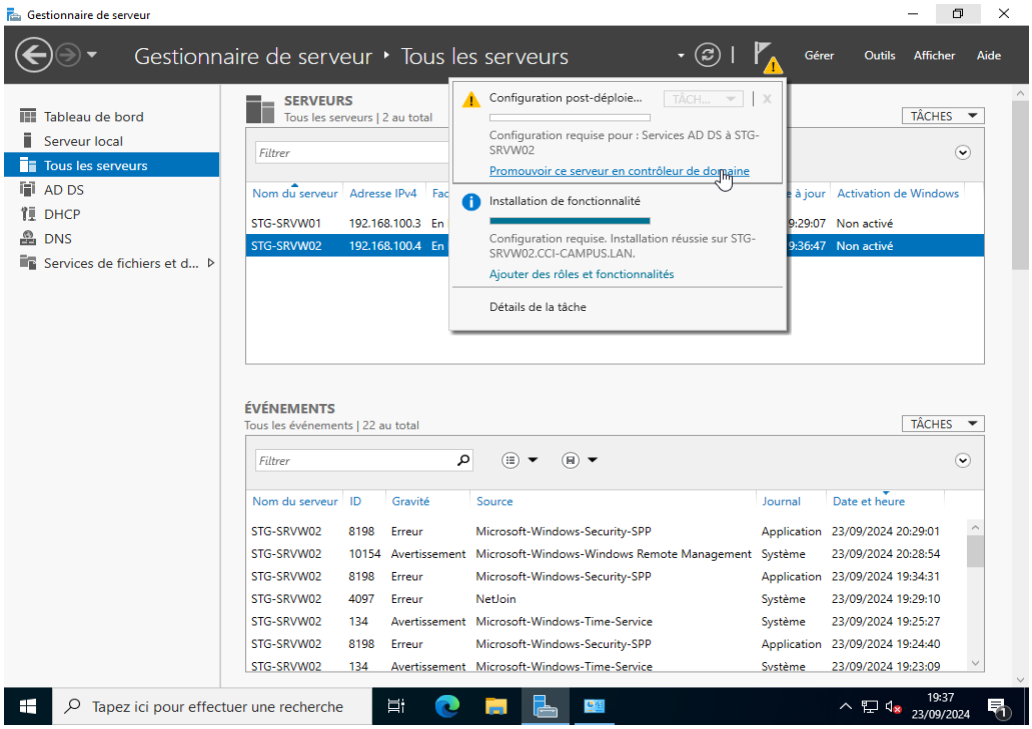
- Cliquer sur **suivant**



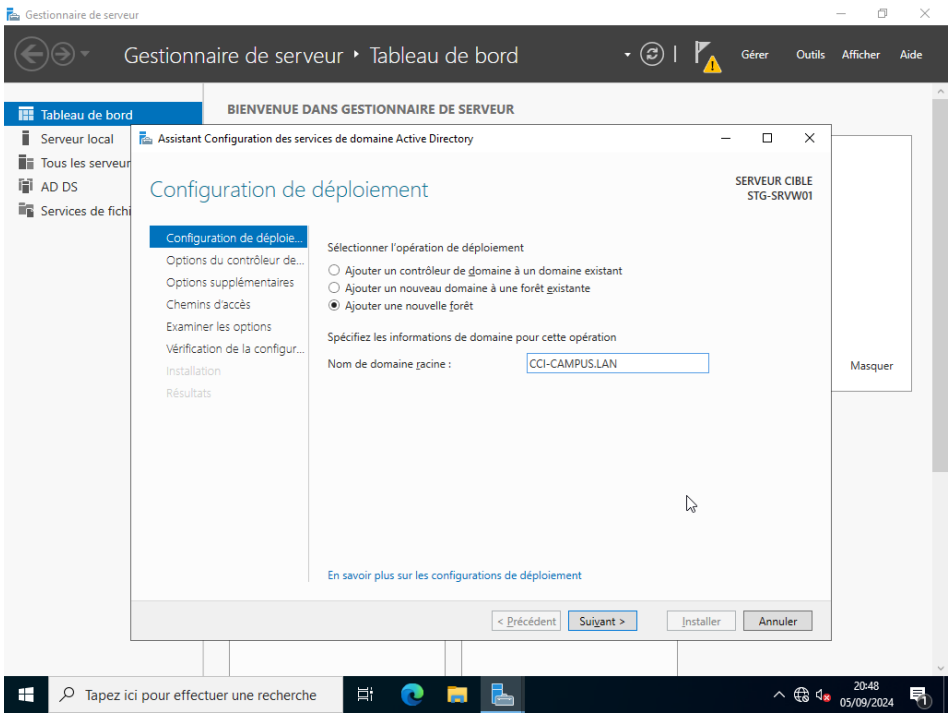
- Installer le rôle



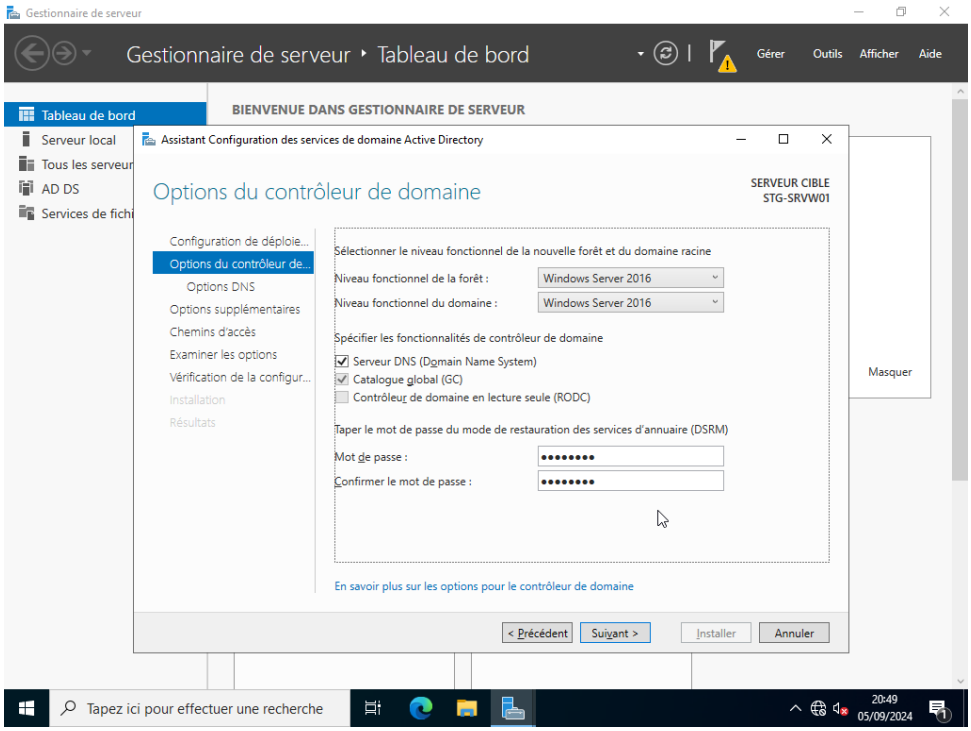
- Ensuite, cliquer sur le drapeau en haut à droite, puis sur **Promouvoir ce serveur en contrôleur de domaine**



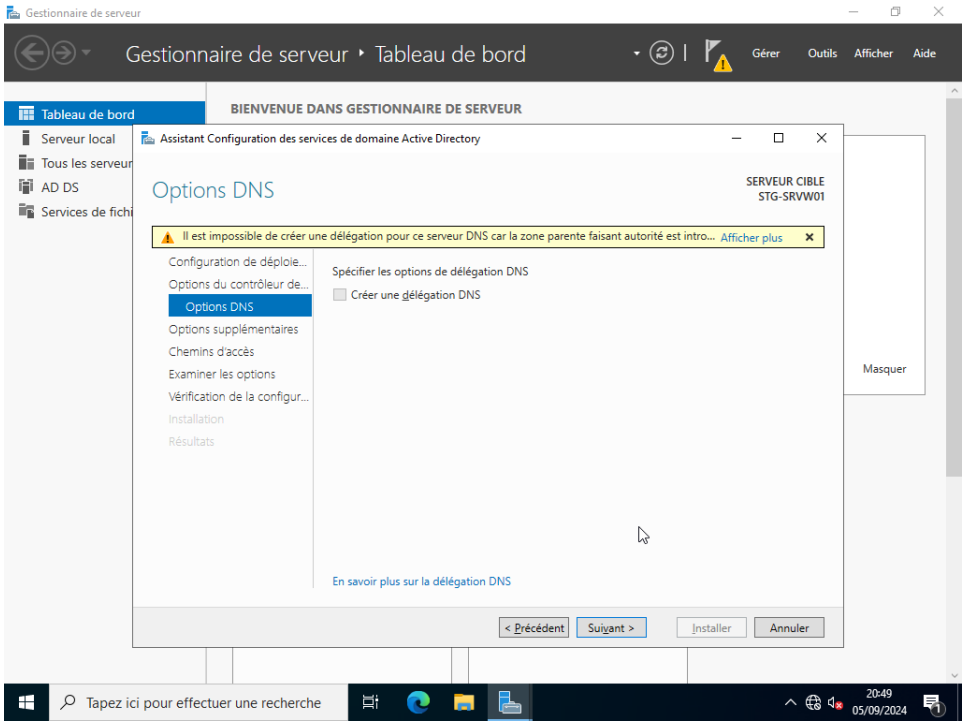
- Spécifier le nom du domaine

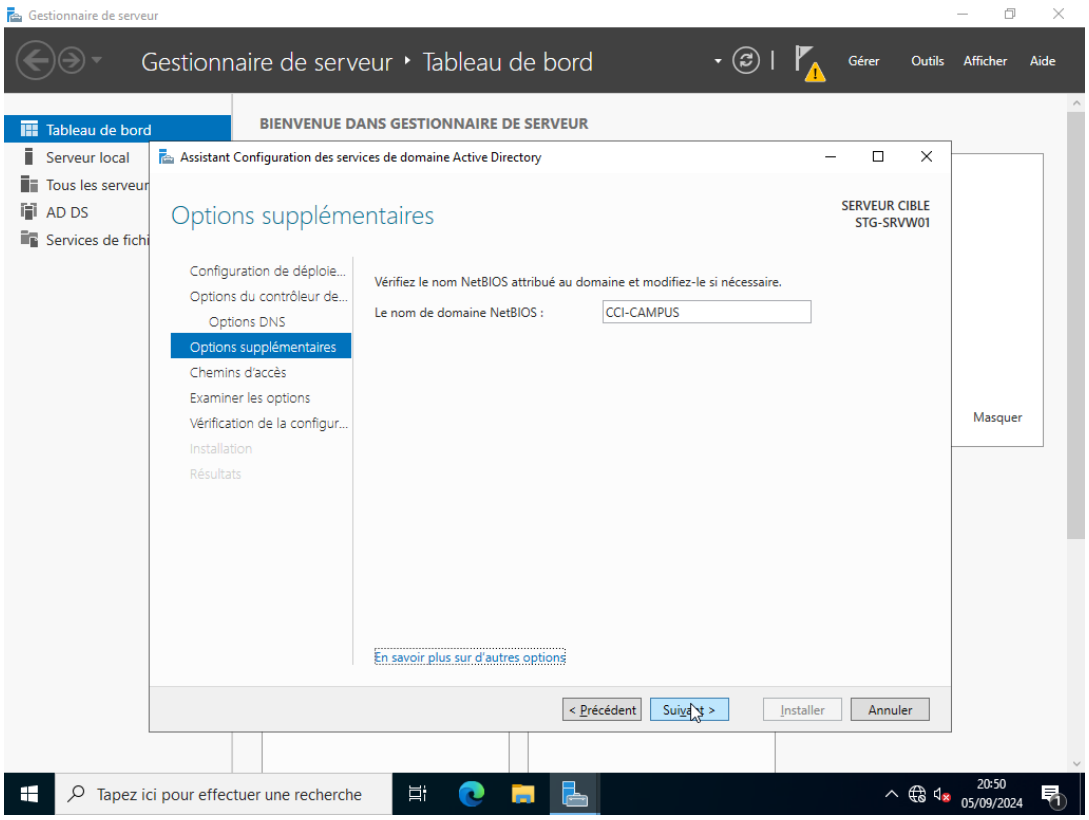


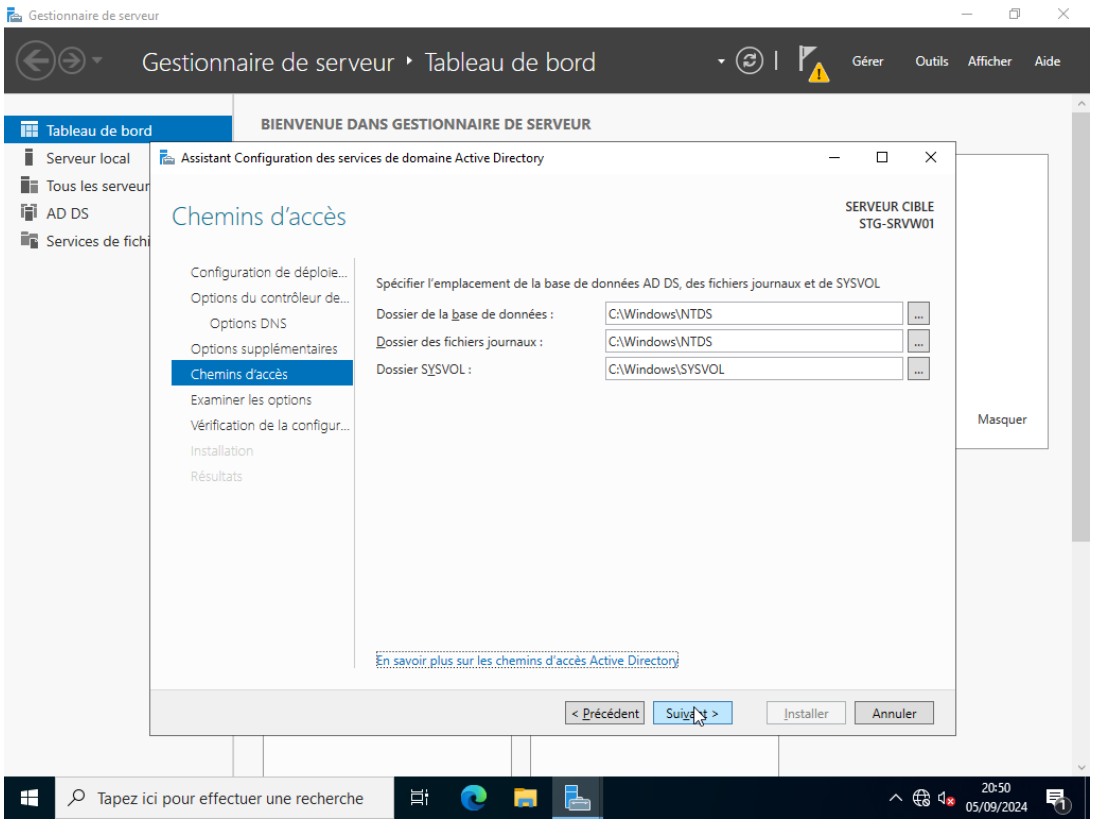
- Renter un mot de passe de restauration

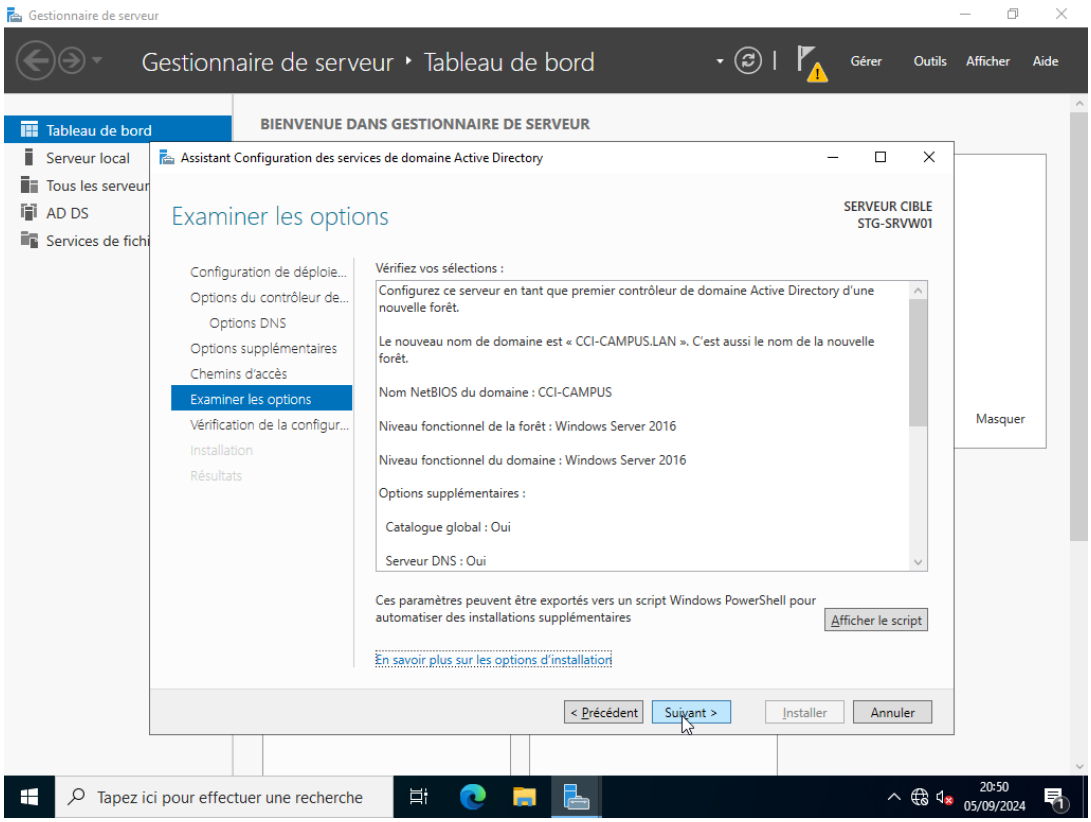


- Cliquer sur **suivant**

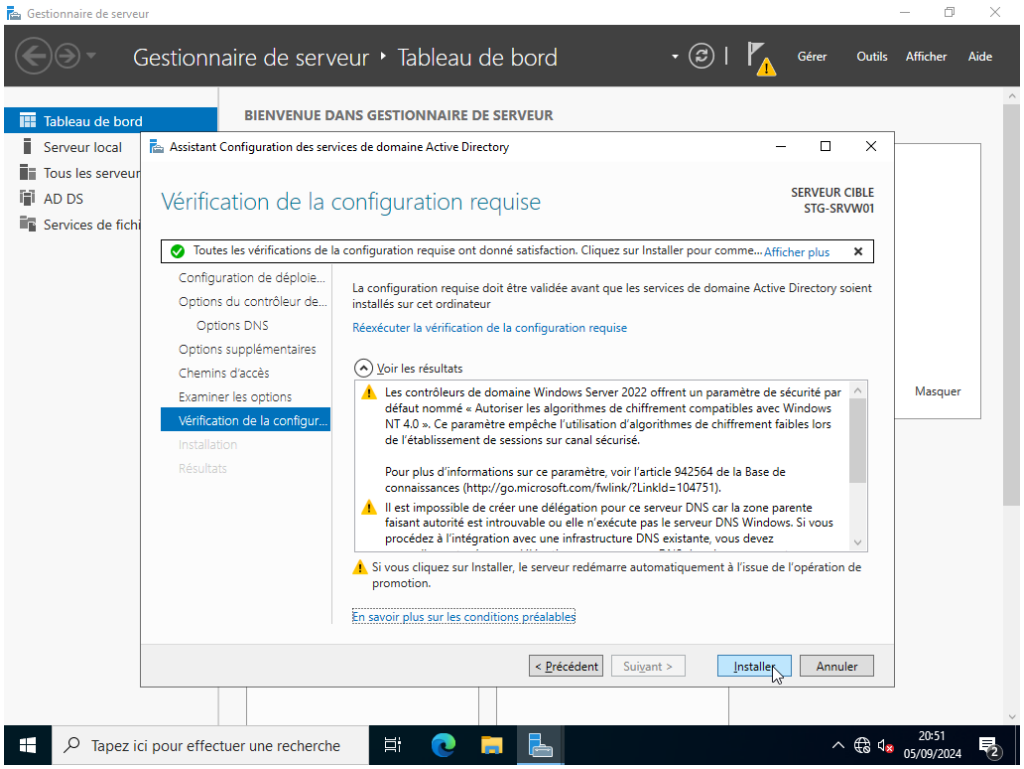



Gestionnaire de serveur
Gestionnaire de serveur ‣ Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveur
AD DS
Services de fichi
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
Masquer
Assistant Configuration des services de domaine Active Directory
Options supplémentaires
SERVEUR CIBLE
STG-SRVW01
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.
Le nom de domaine NetBIOS :
CCI-CAMPUS
En savoir plus sur d'autres options
< Précédent
Suivant >
Installer
Annuler
Tapez ici pour effectuer une recherche
20:50
05/09/2024


Gestionnaire de serveur
Gestionnaire de serveur ‣ Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveur
AD DS
Services de fichi
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
Masquer
Assistant Configuration des services de domaine Active Directory
Chemins d'accès
SERVEUR CIBLE
STG-SRVW01
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 :
C:\Windows\NTDS
Dossier des fichiers journaux :
C:\Windows\NTDS
Dossier SYSVOL :
C:\Windows\SYSVOL
En savoir plus sur les chemins d'accès Active Directory
< Précédent
Suivant >
Installer
Annuler
Tapez ici pour effectuer une recherche
20:50
05/09/2024

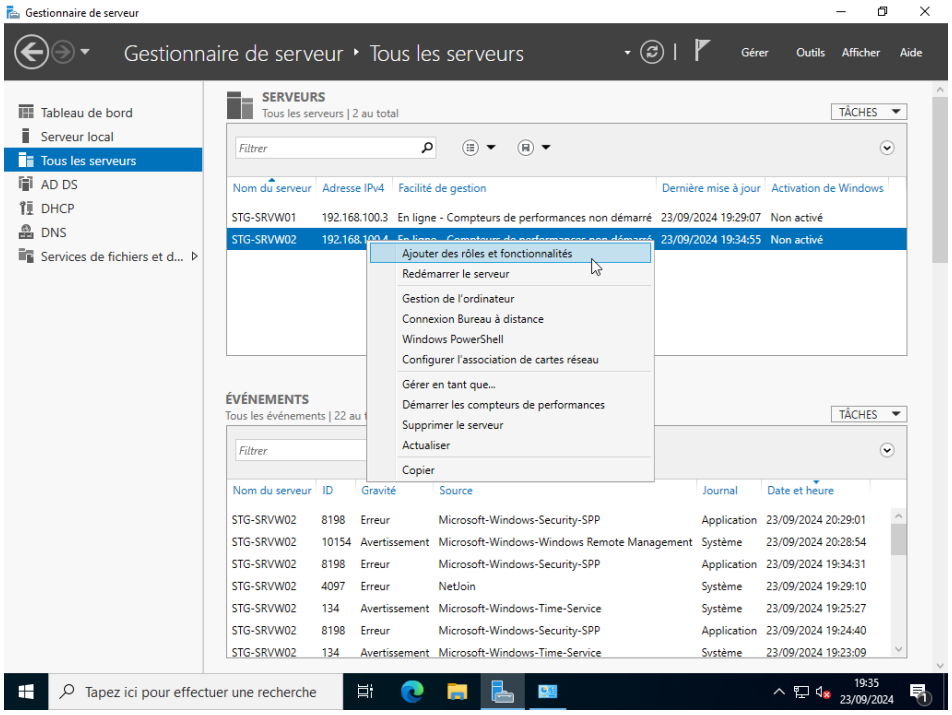


- Puis **installer**

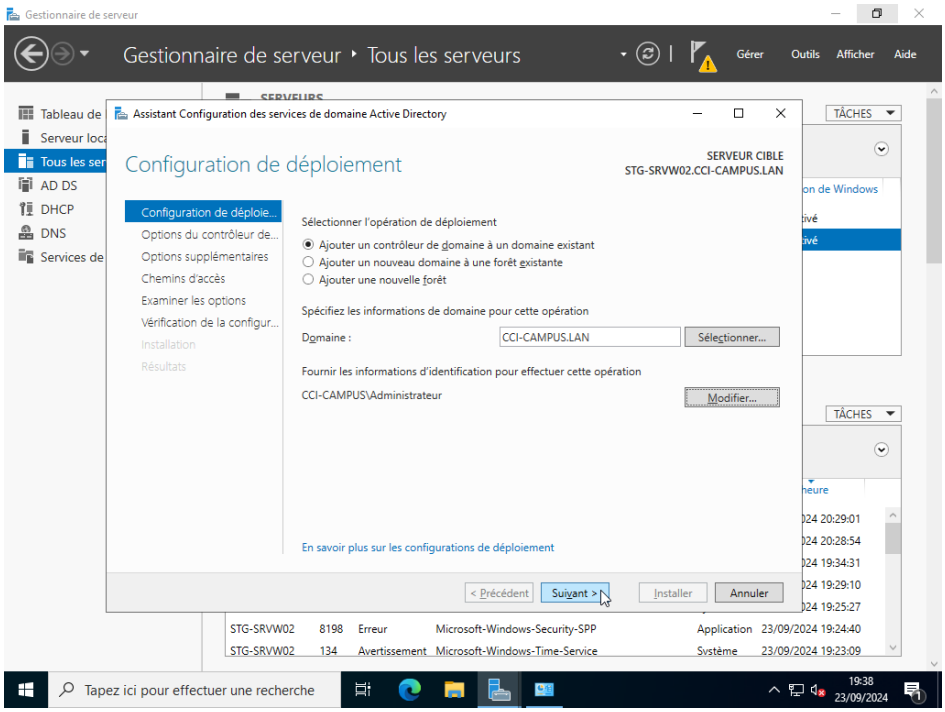


- Le rôle AD DS est maintenant installé et configuré en tant que contrôleur de domaine principale sur le STG-SRVW01

- Faire de même sur le serveur secondaire

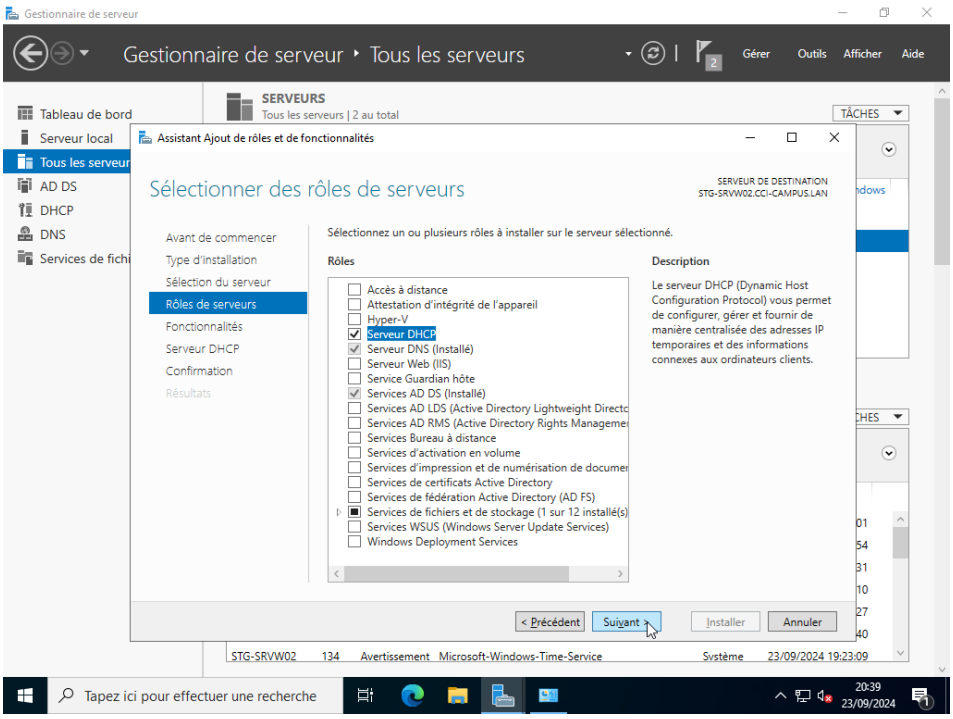


- Ajouter un contrôleur de domaine à un domaine existant

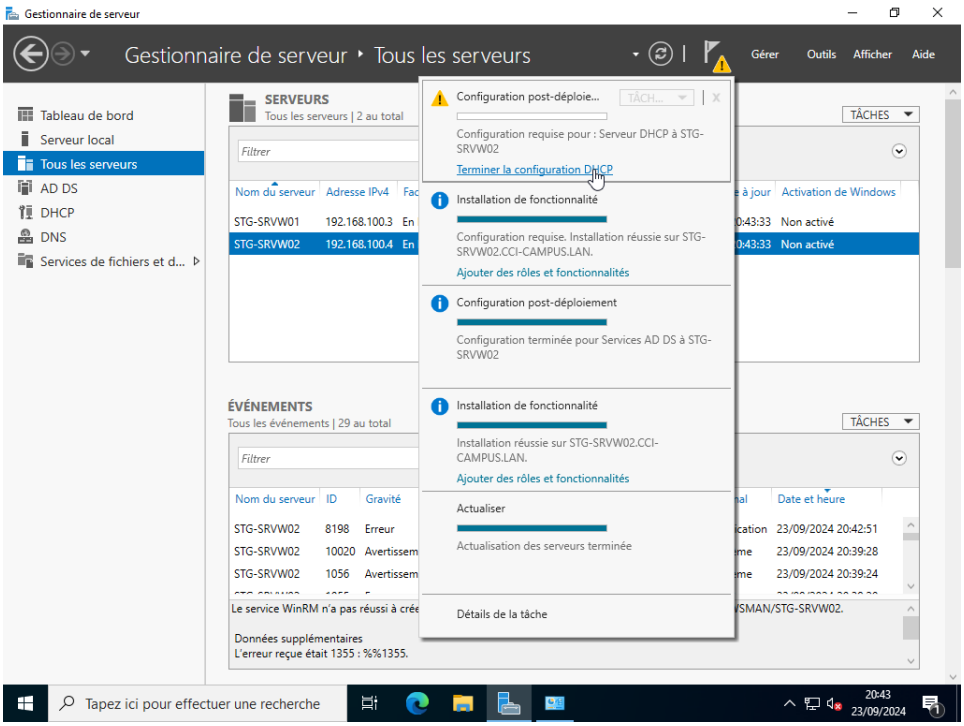


Installation du DHCP

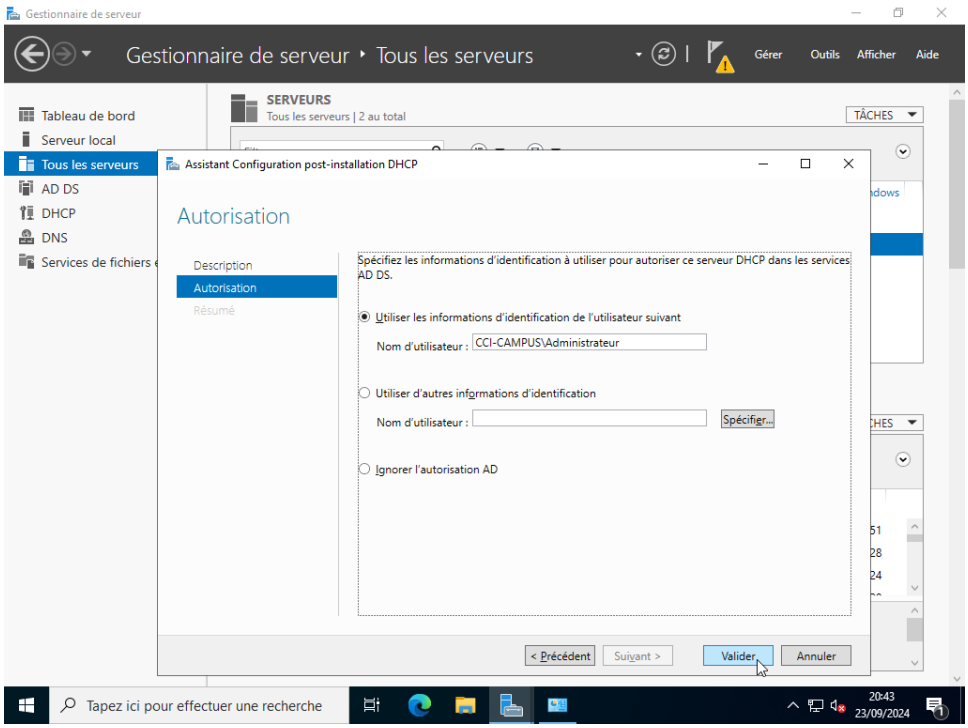
- Installer le rôle DHCP



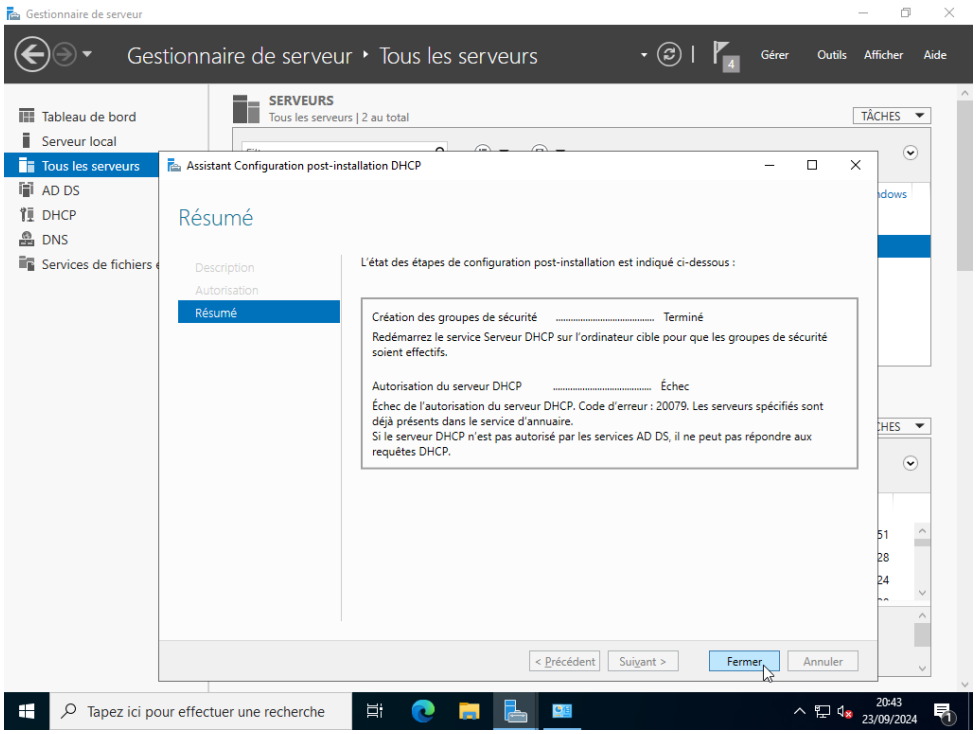
- Faire **terminer la configuration DHCP**



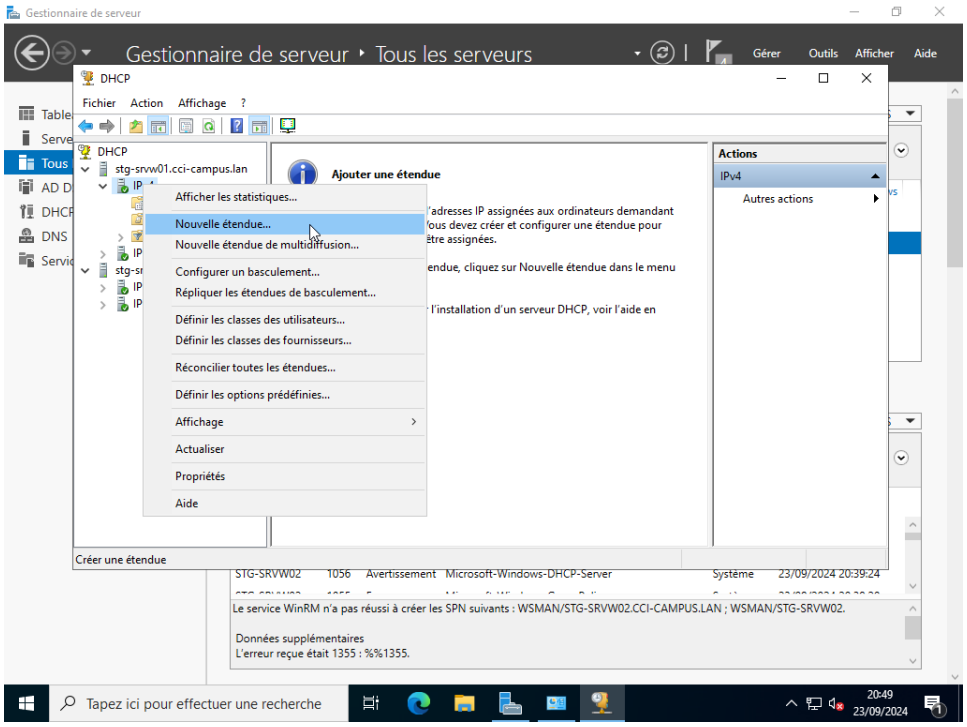
- Faire valider


Gestionnaire de serveur
Gestionnaire de serveur ‣ Tous les serveurs
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
AD DS
DHCP
DNS
Services de fichiers
SERVEURS
Tous les serveurs | 2 au total
TÂCHES
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 : CCI-CAMPUS\Administrateur
Utiliser d'autres informations d'identification
Nom d'utilisateur :
Spécifier...
Ignorer l'autorisation AD
< Précédent
Suivant >
Valider
Annuler
Tapez ici pour effectuer une recherche
20:43
23/09/2024

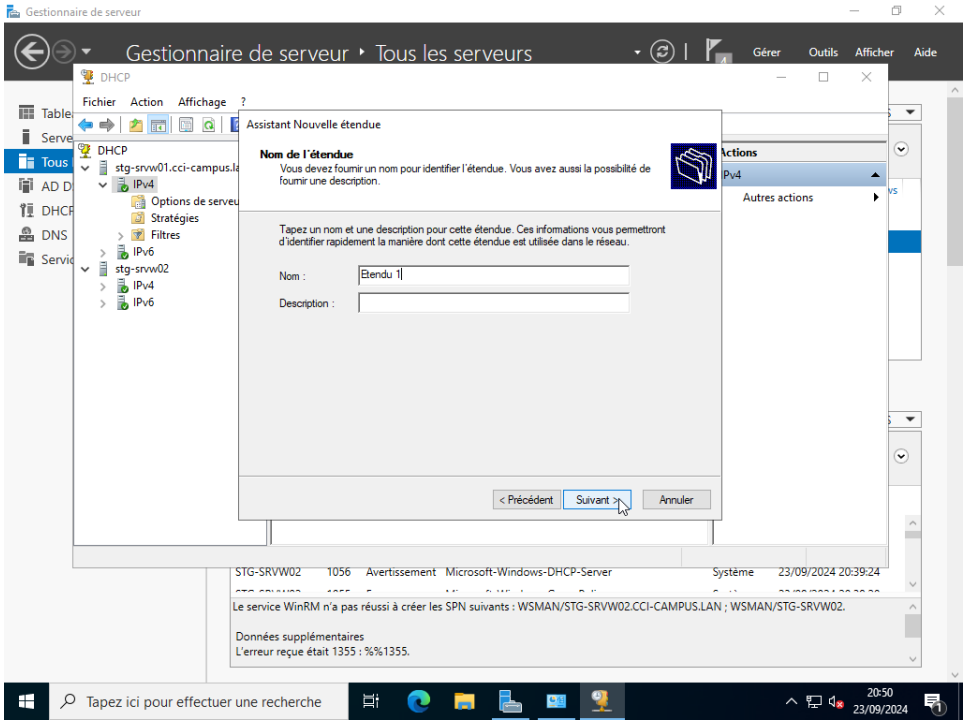
- Et fermer


Gestionnaire de serveur
Gestionnaire de serveur ‣ Tous les serveurs
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
AD DS
DHCP
DNS
Services de fichiers
SERVEURS
Tous les serveurs | 2 au total
TÂCHES
Assistant Configuration post-installation DHCP
Résumé
Description
Autorisation
Résumé
L'état des étapes de configuration post-installation est indiqué ci-dessous :
Création des groupes de sécurité ..... Terminé
Redémarrez le service Serveur DHCP sur l'ordinateur cible pour que les groupes de sécurité soient effectifs.
Autorisation du serveur DHCP ..... Échec
Échec de l'autorisation du serveur DHCP. Code d'erreur : 20079. Les serveurs spécifiés sont déjà présents dans le service d'annuaire.
Si le serveur DHCP n'est pas autorisé par les services AD DS, il ne peut pas répondre aux requêtes DHCP.
< Précédent
Suivant >
Fermer
Annuler
Tapez ici pour effectuer une recherche
20:43
23/09/2024

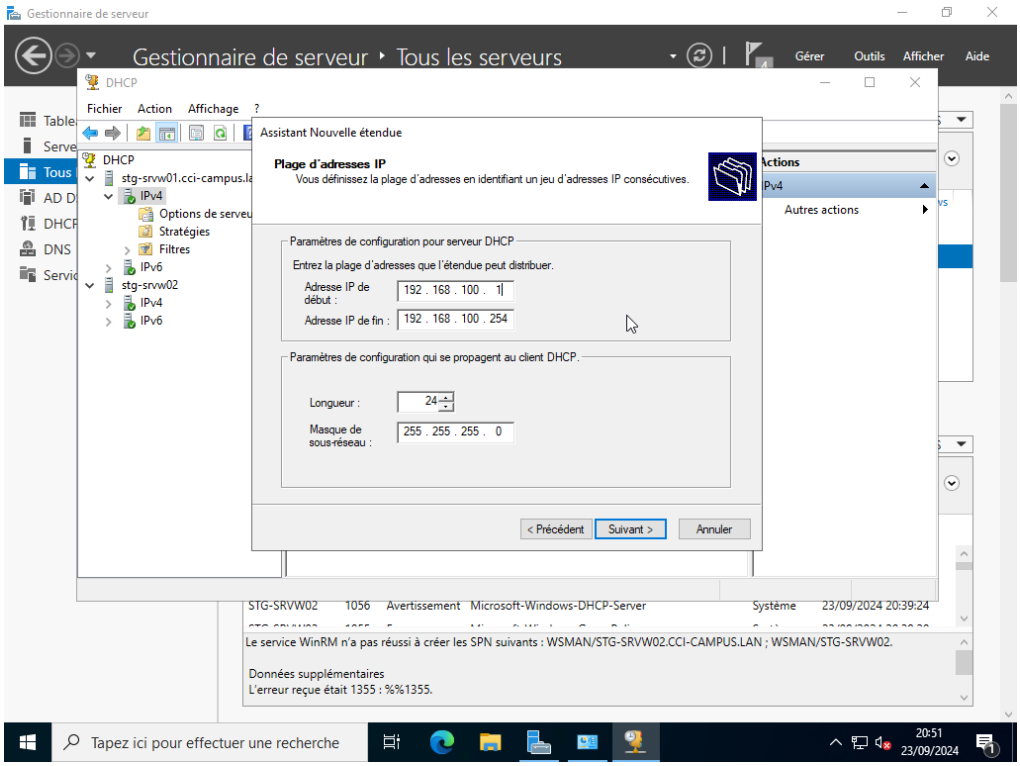
- Aller dans le **gestionnaire DHCP** et **configurer une nouvelle étendue**



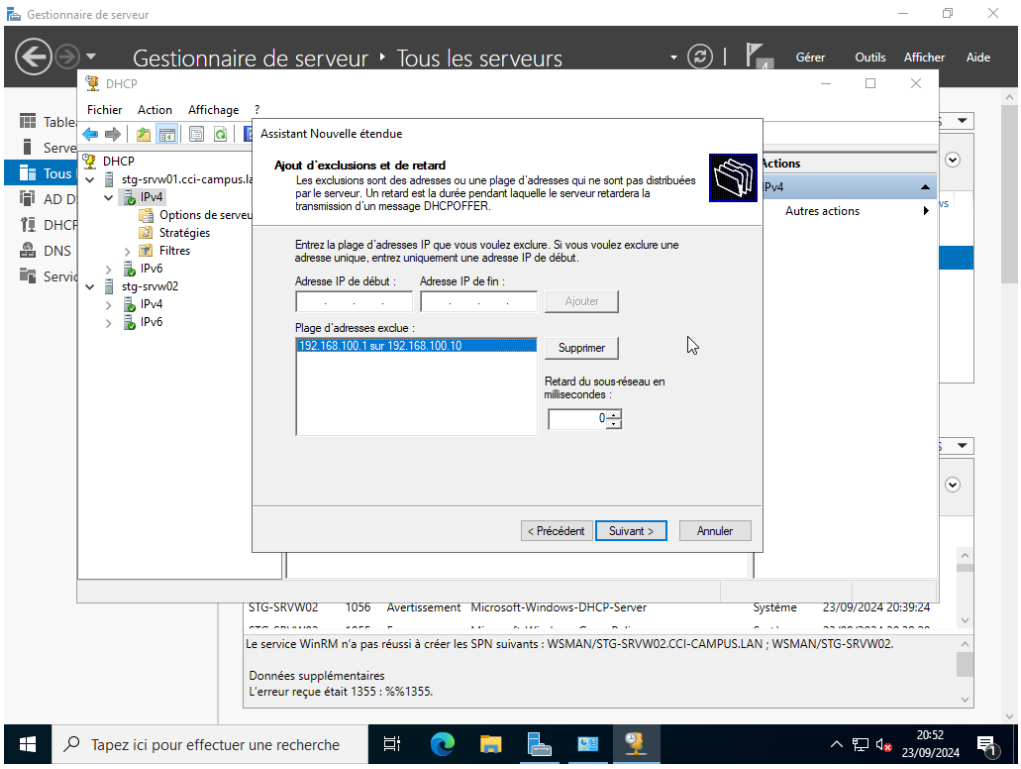
- Mettre un nom à l'étendue



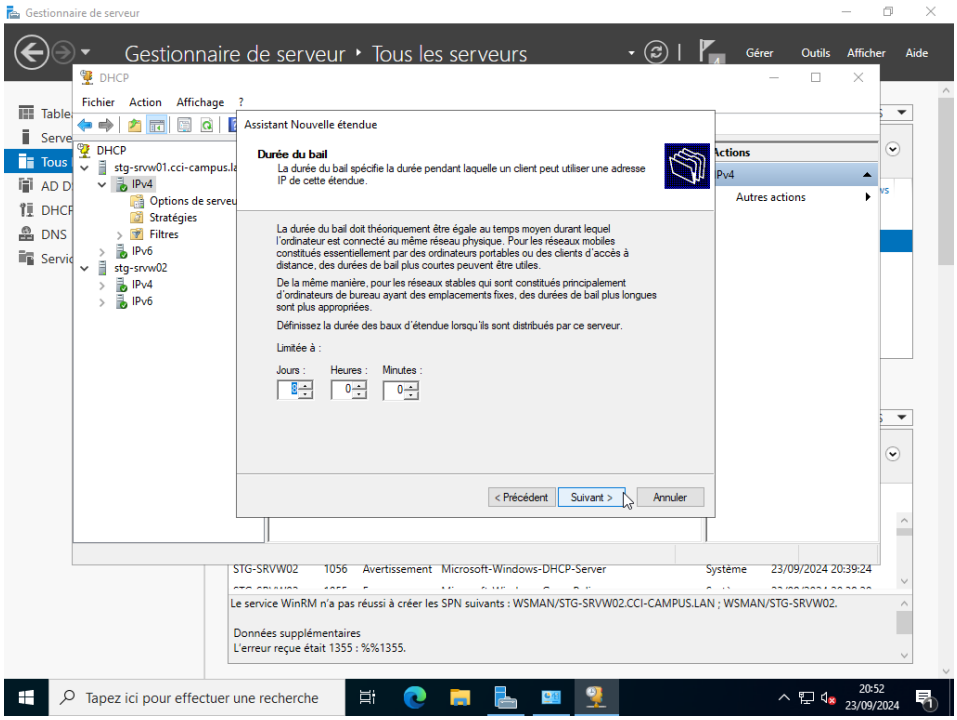
- Configurer une plage d'adresse IP



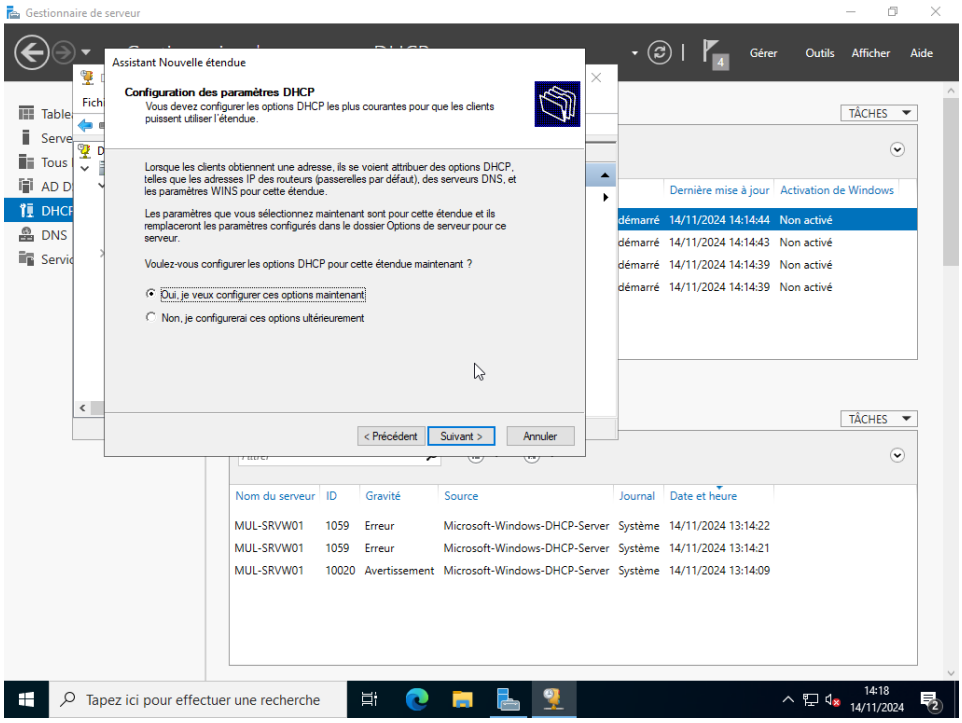
- Sélectionner une plage d'exclusion



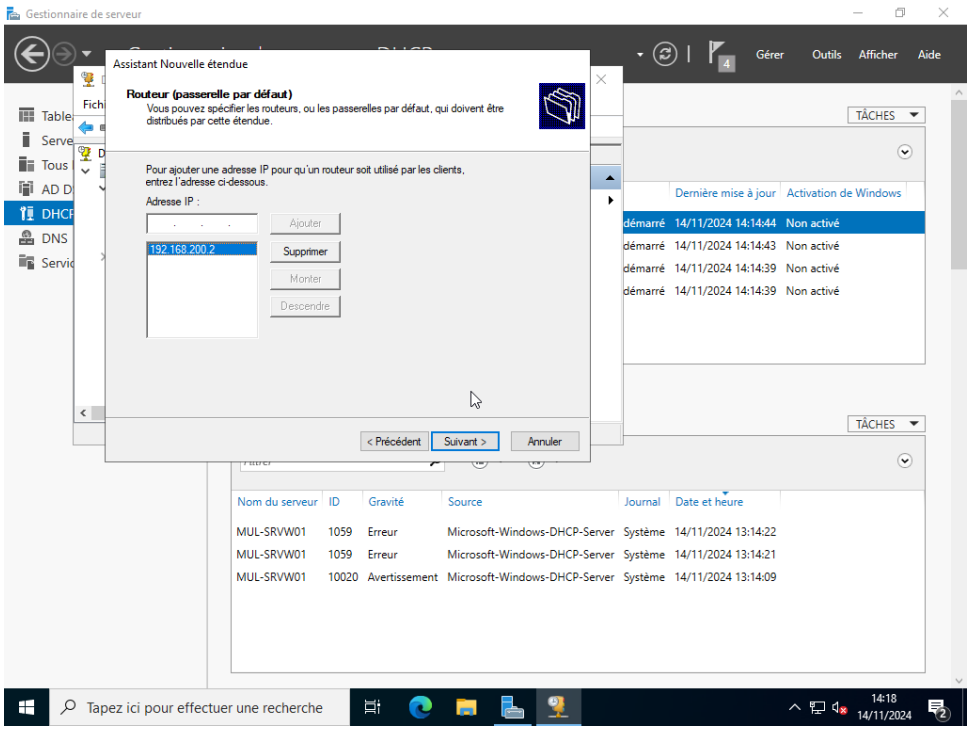
- Sélectionner la durée du bail



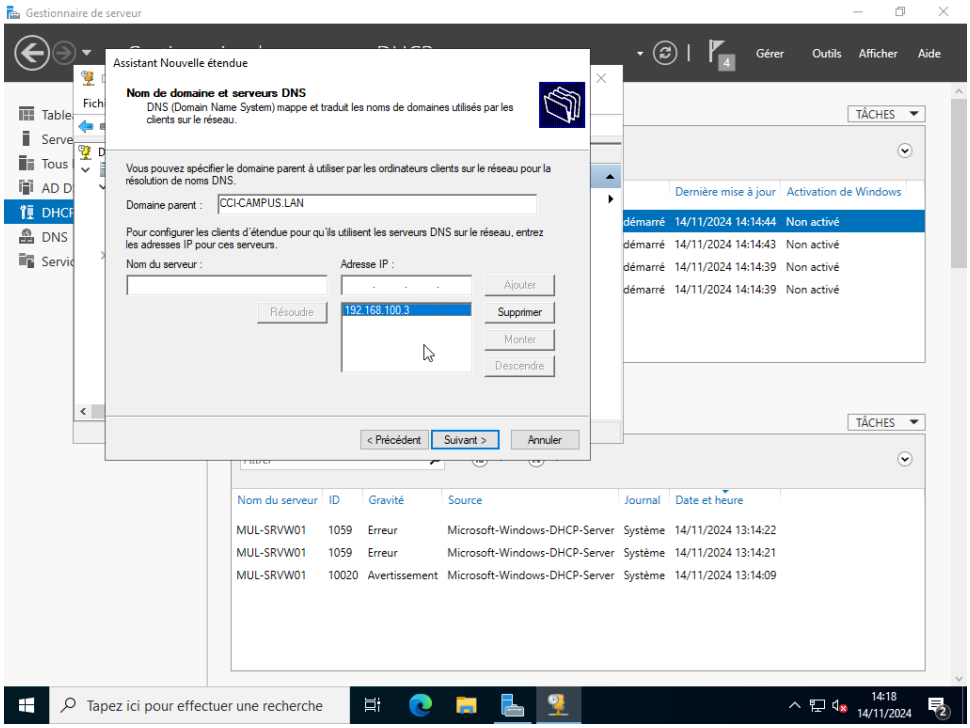
- Configurer maintenant



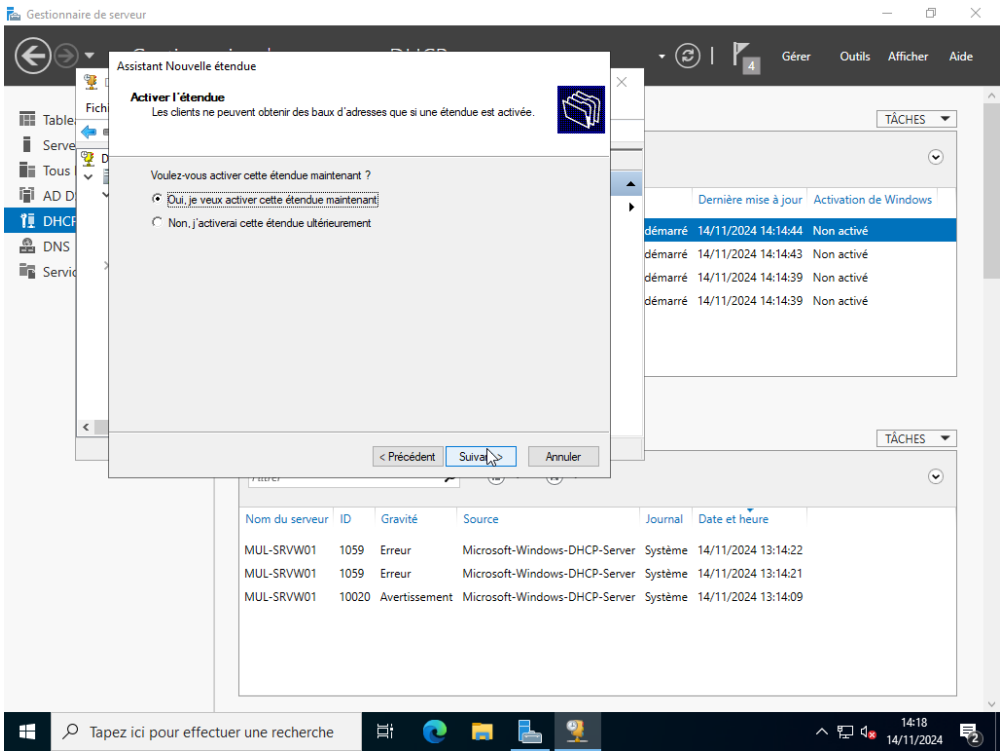
- Ajouter le routeur



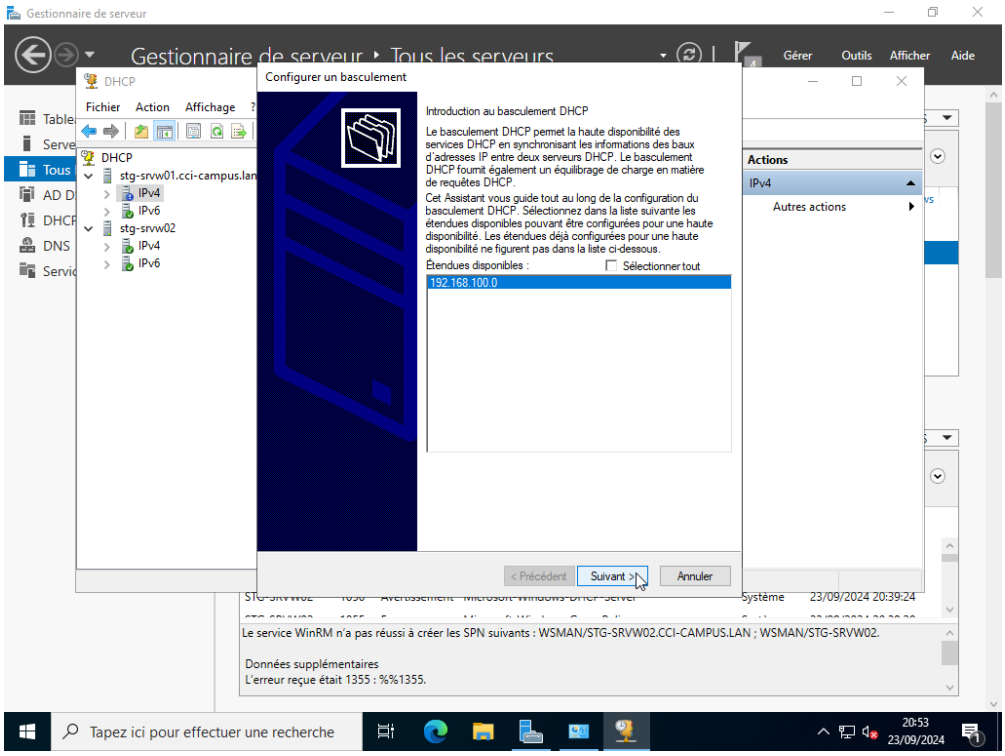
- Ajouter le serveur DNS qui est le serveur principale



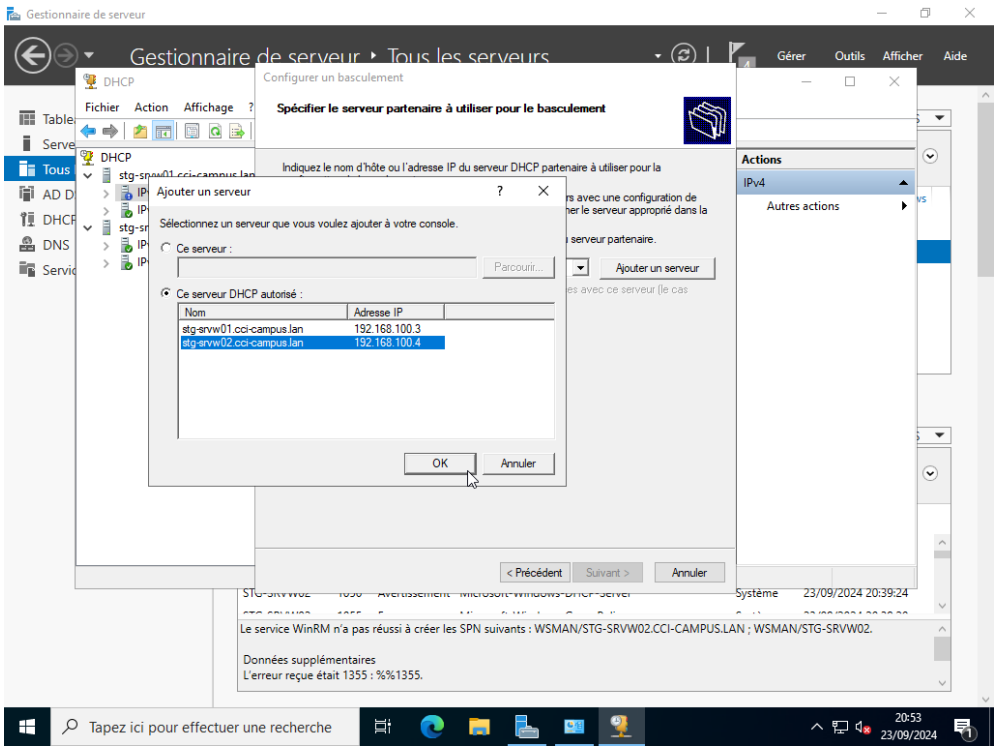
- Activer l'étendue



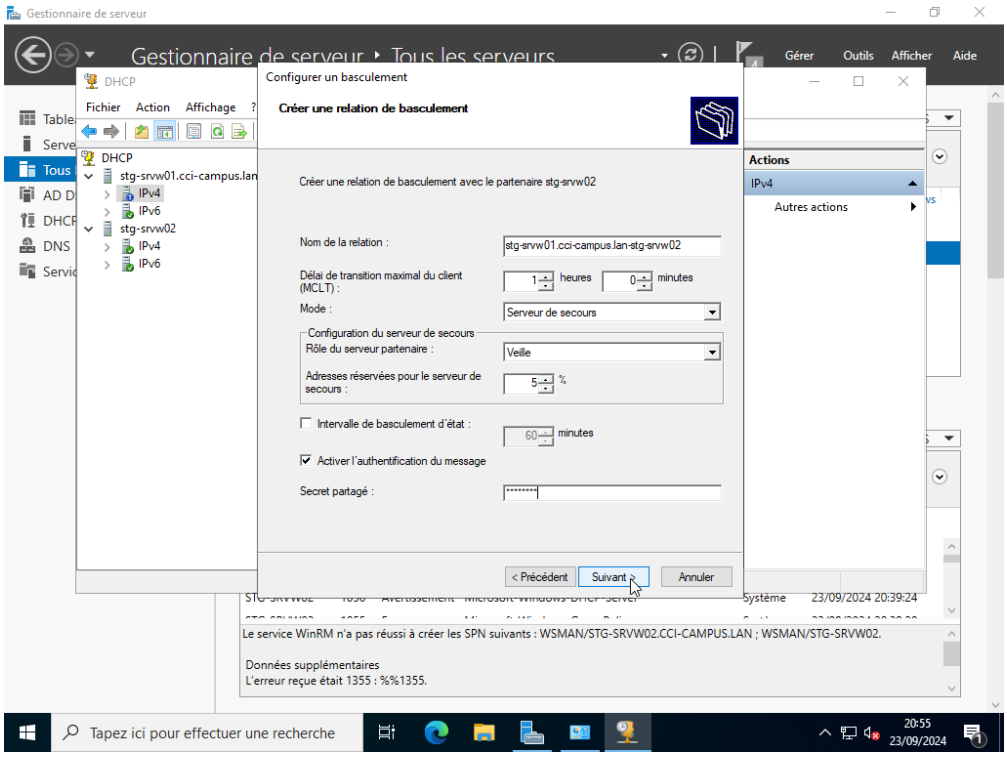
- Ensuite configurer un basculement sur l'étendue qui vient d'être crée



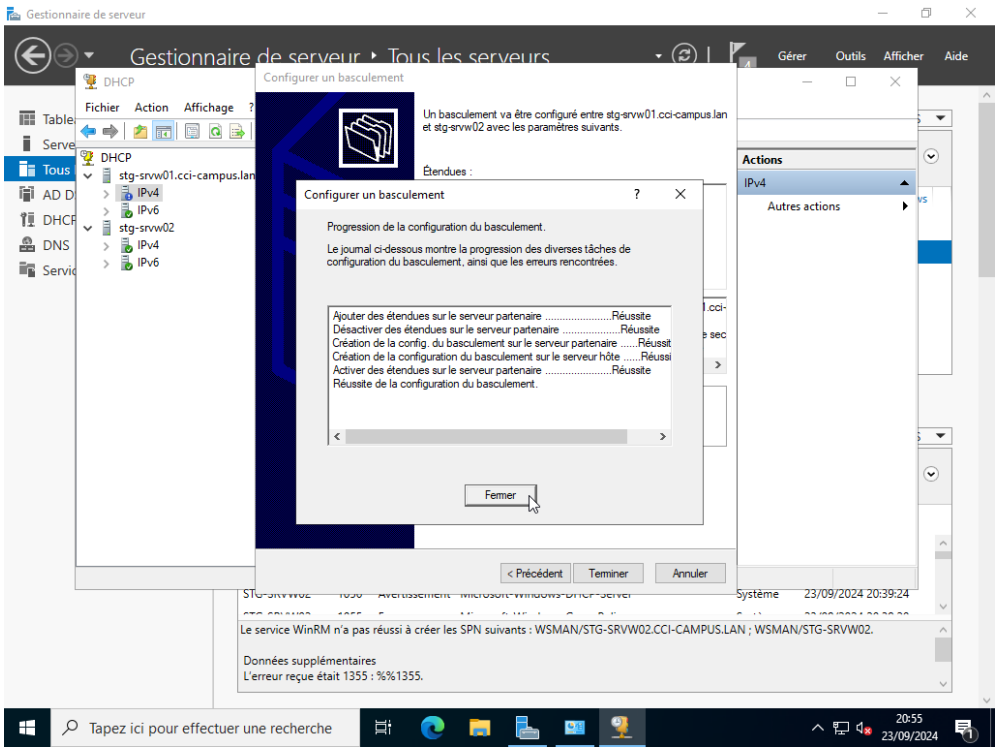
- Sélectionner le serveur DHCP



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



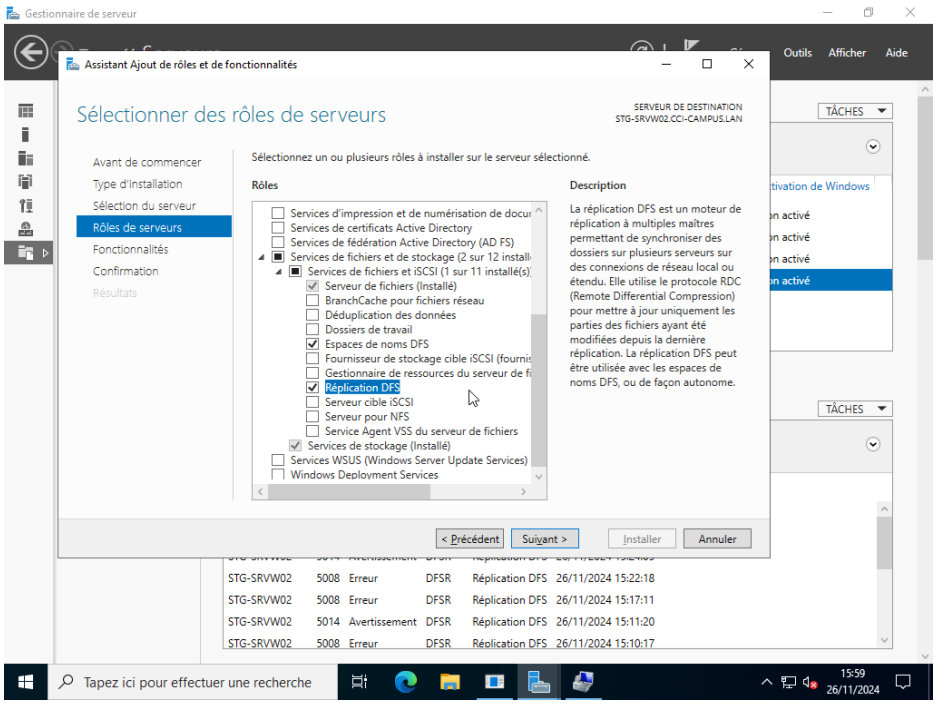
- Puis terminer

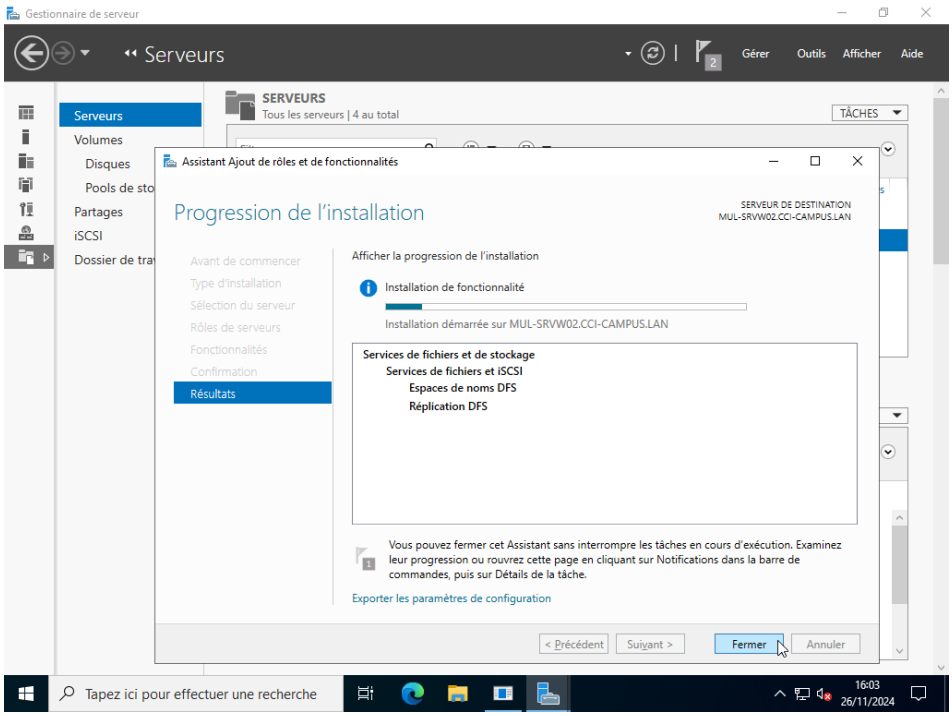


- Faire de même pour les autres serveurs en modifiant les adresses IP en conséquence

Installation et configuration de DFS/R

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

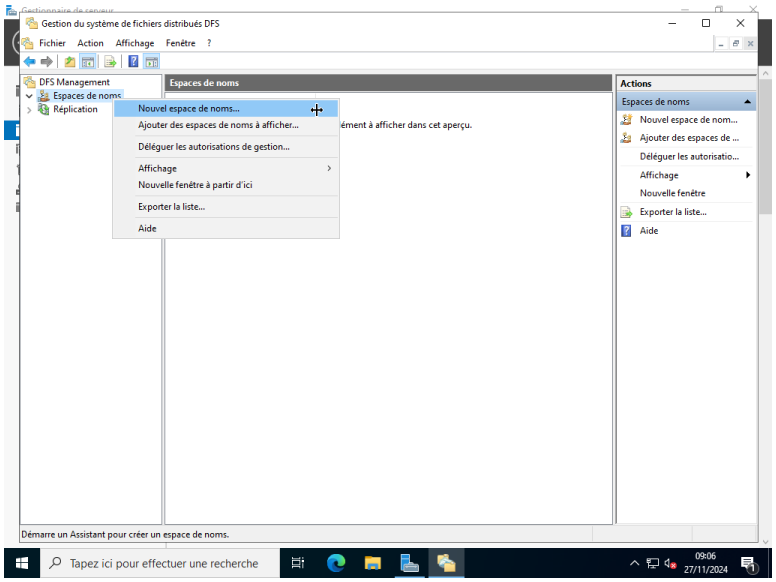




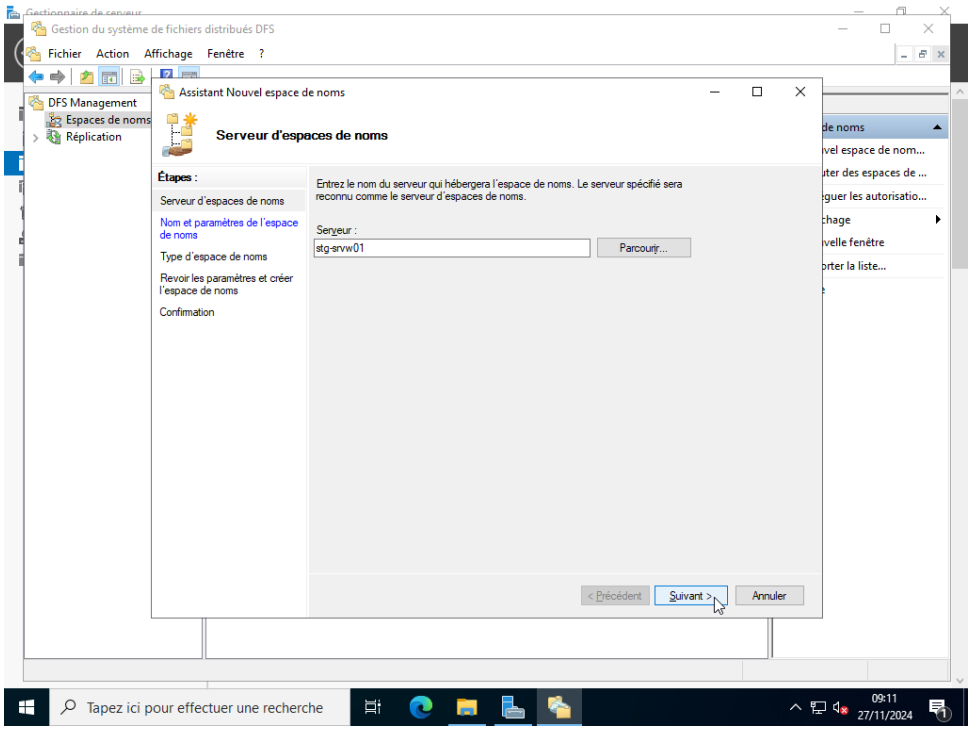
Création du partage

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

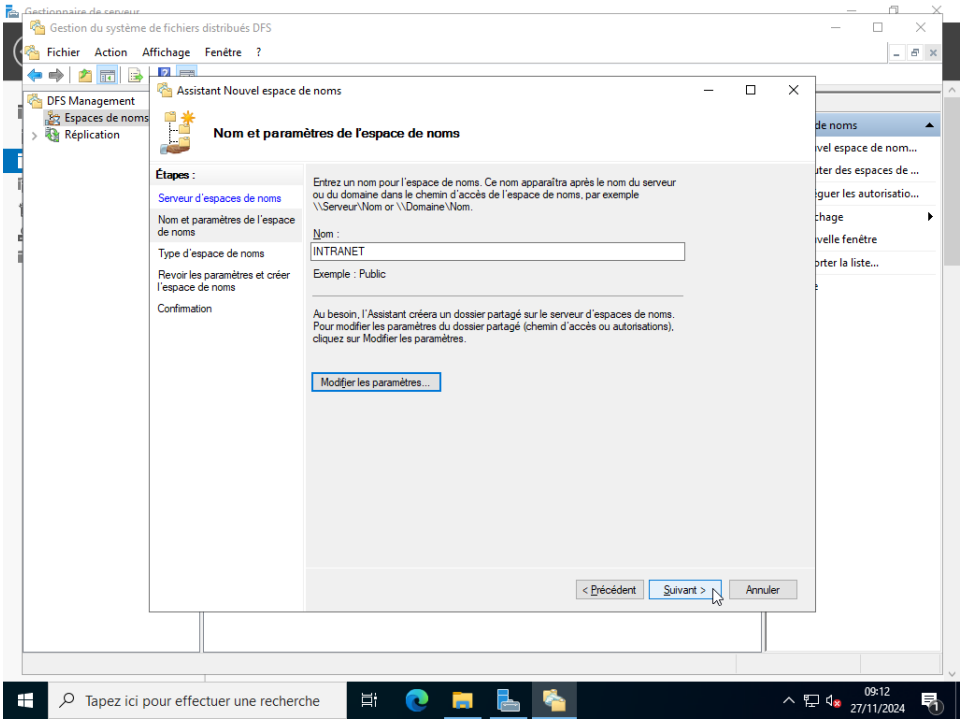
- Sur le menu **Espaces de noms** faire un clique droit et créer un nouvel espace de noms

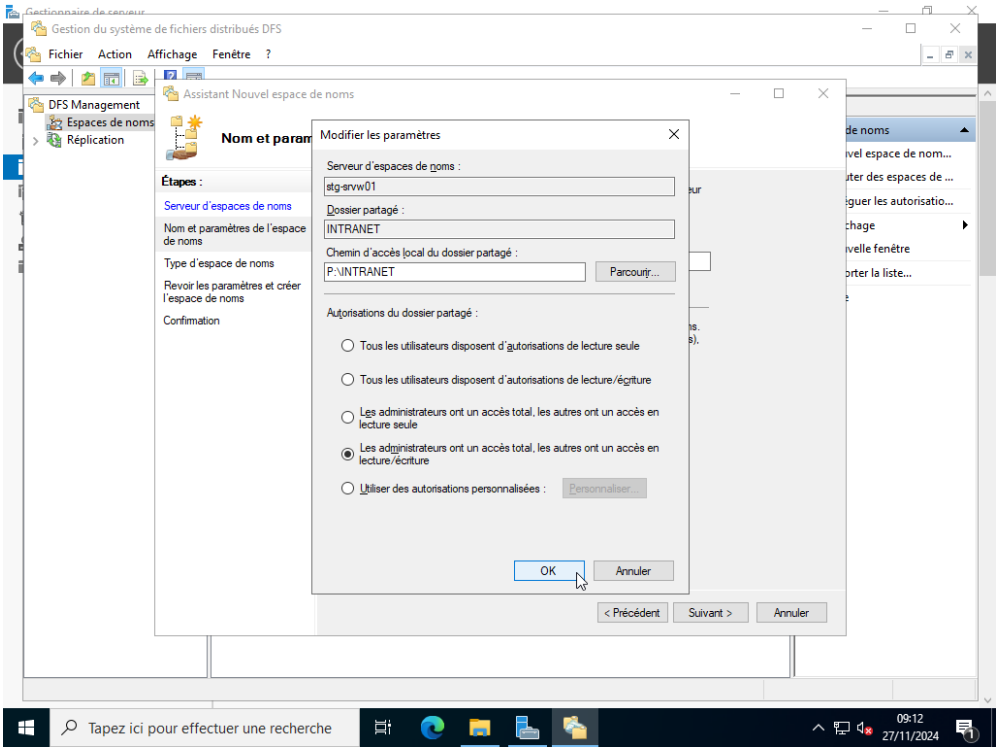


- Sélectionner le serveur qui hébergera les fichiers

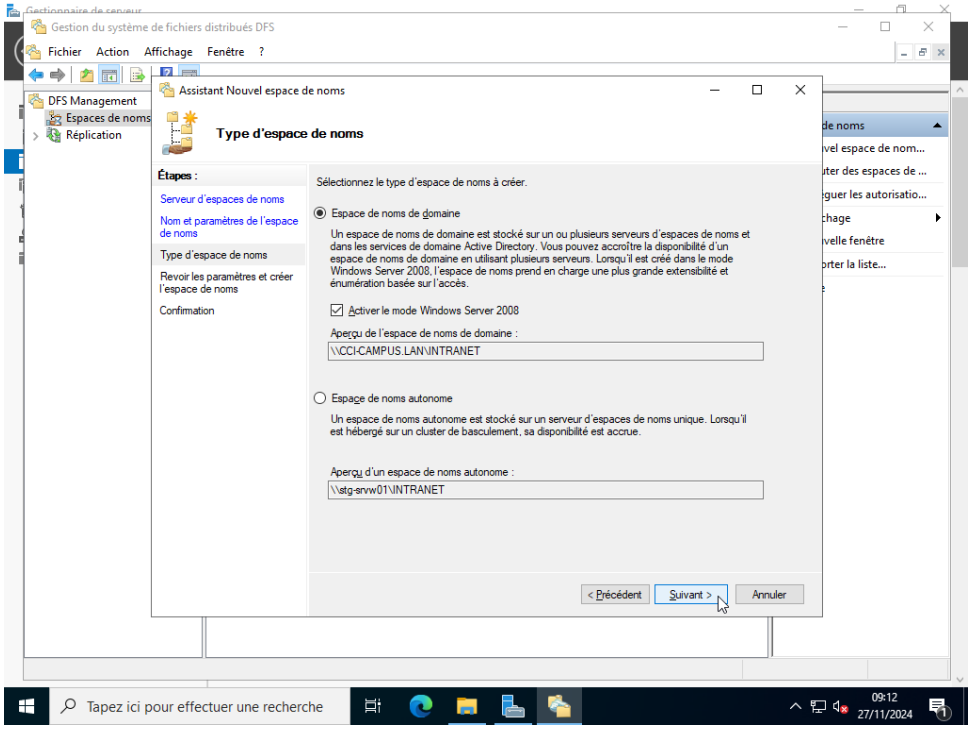


- L'espace de nom s'appelle ici **INTRANET**. Sélectionner la case autorisant l'accès total aux administrateurs et l'accès lecture/écriture aux autres en accédant aux paramètres

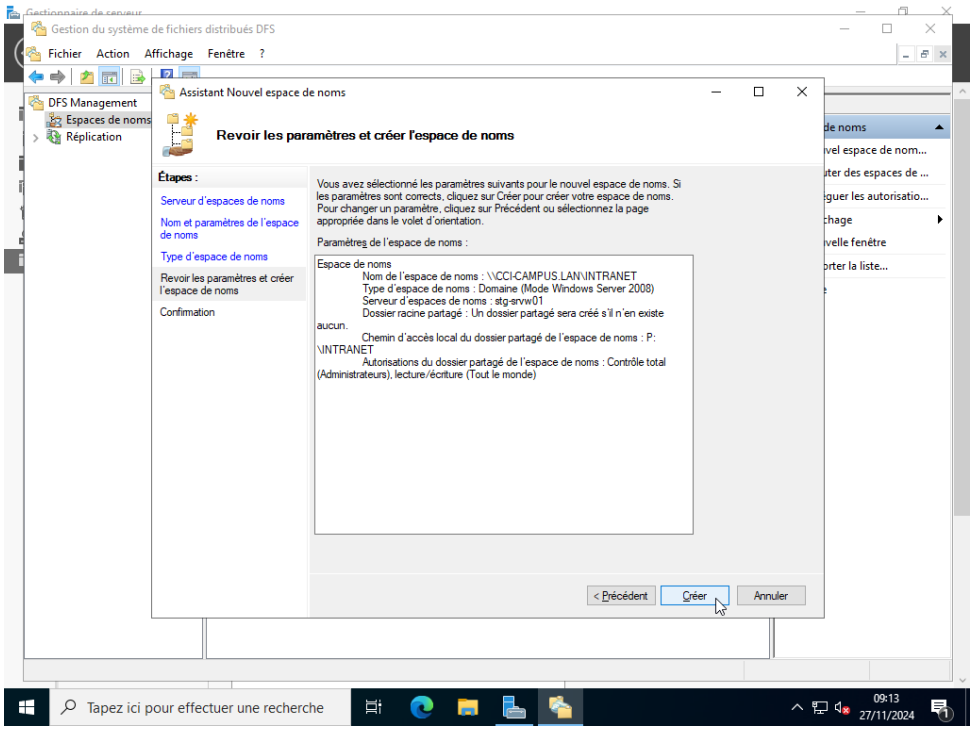




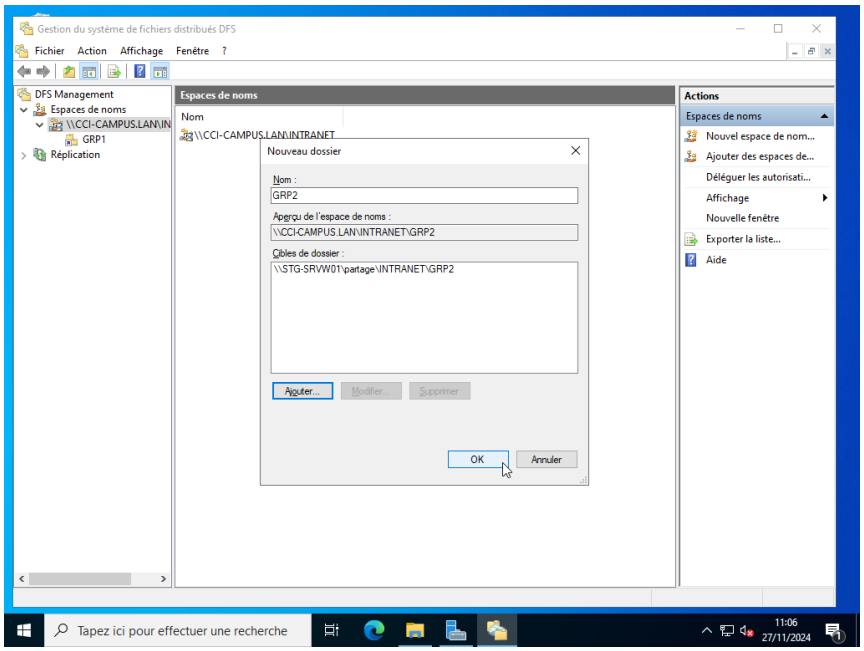
- Sélectionner **espace de noms de domaine**



- Créer l'espace de noms



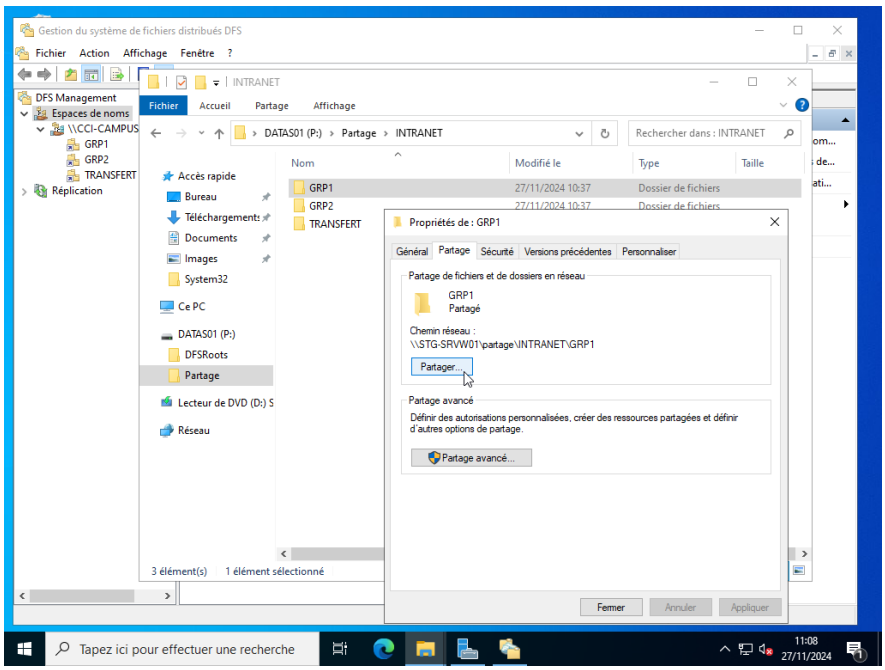
- Une fois l'espace de noms créer, ajouter un nouveau dossier en faisant un clique droit sur l'espace de noms. Ajouter un nom au dossier puis sélectionner la cible (l'endroit où est stocké le dossier)



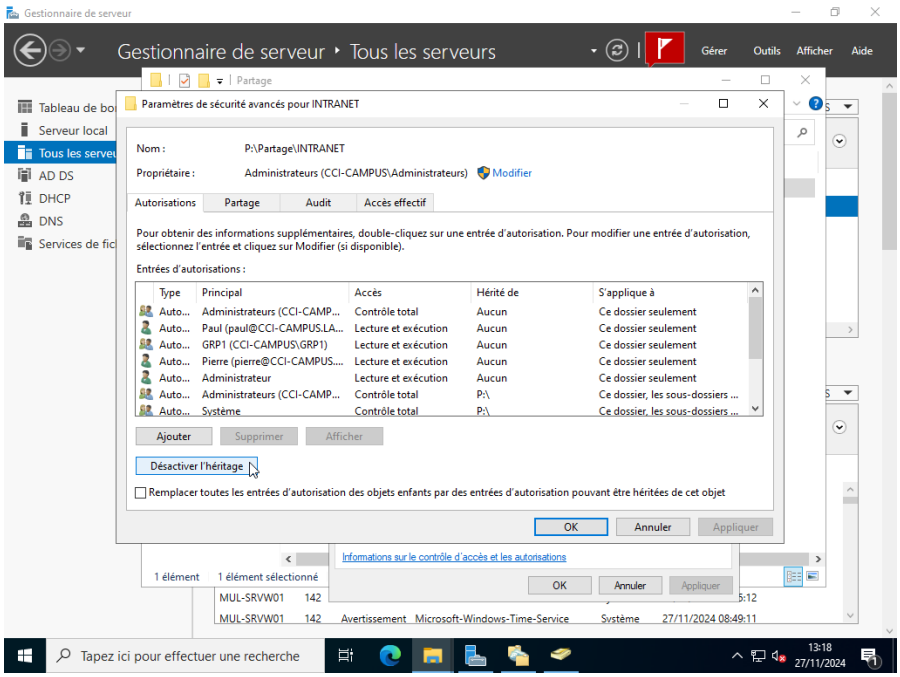
Ta mère

Mise en place des droits sur les dossiers

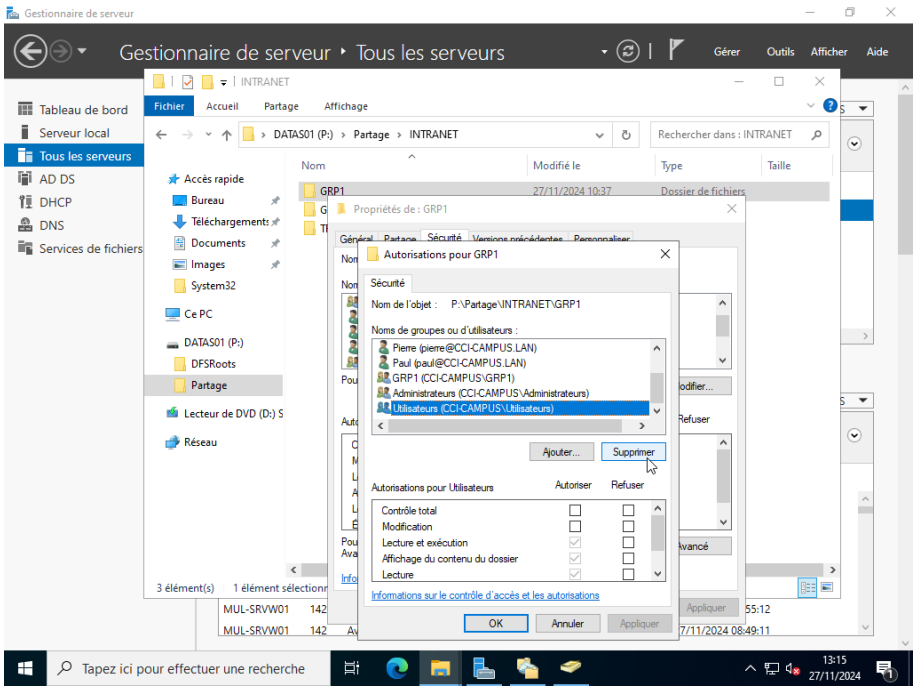
- Aller dans le répertoire où se trouve les dossiers. Dans les **propriétés** se rendre dans l'onglet **partage** puis **partage avancé**



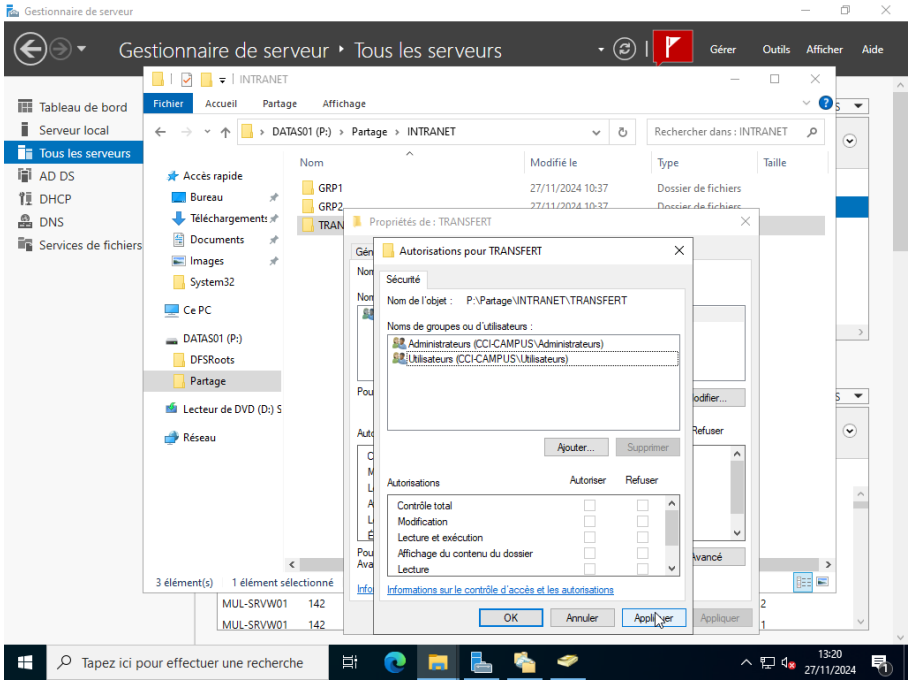
- Désactivé l'héritage



- 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

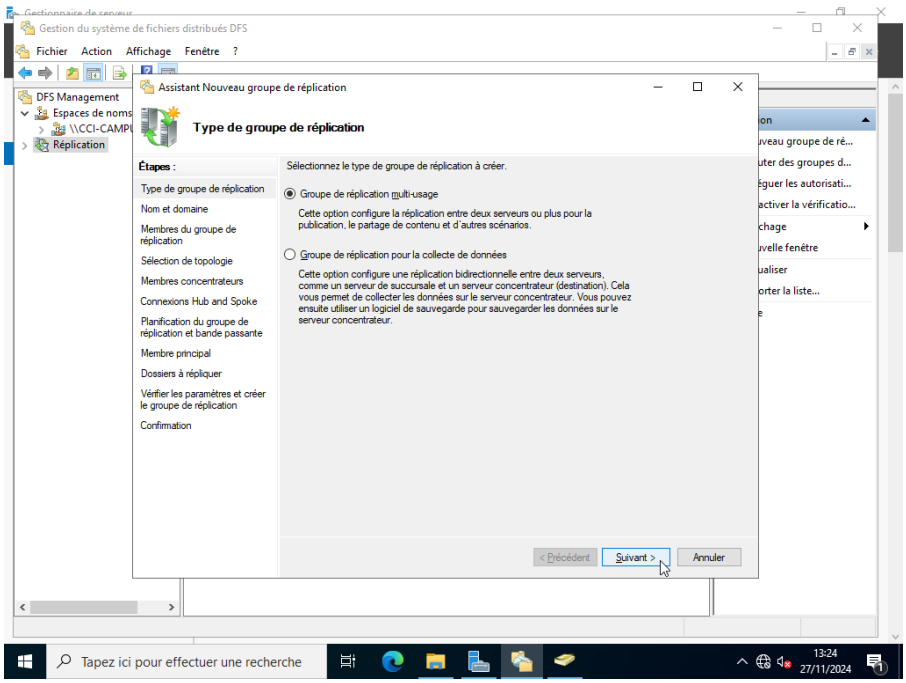


- Pour le dossier **TRANSFERT**, ajouter l'accès total aux administrateurs et en lecture/écriture pour tous les autres utilisateurs

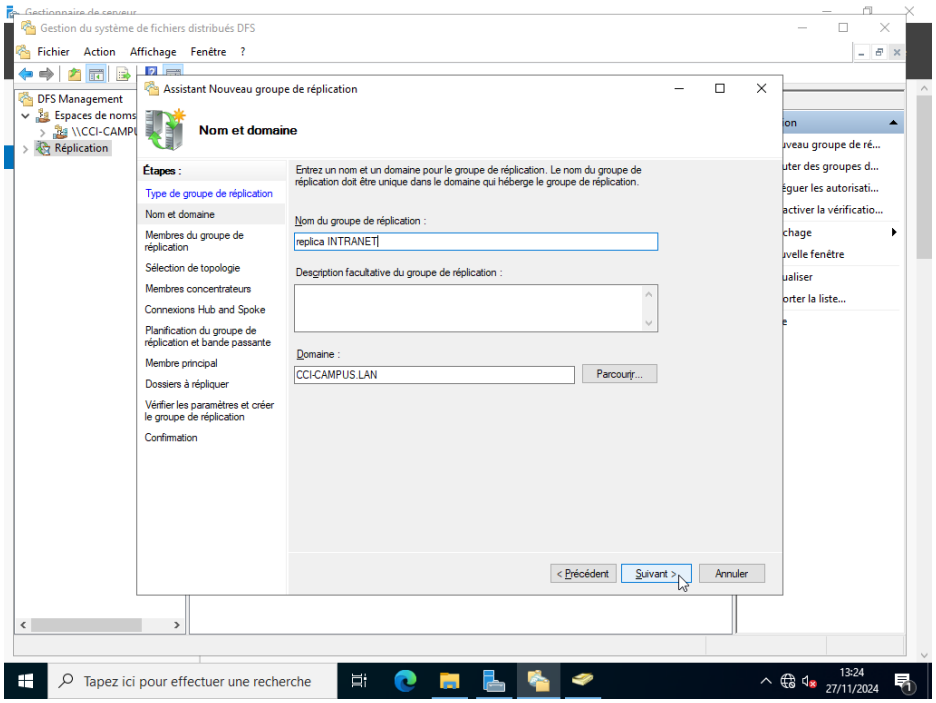


Réplication des données

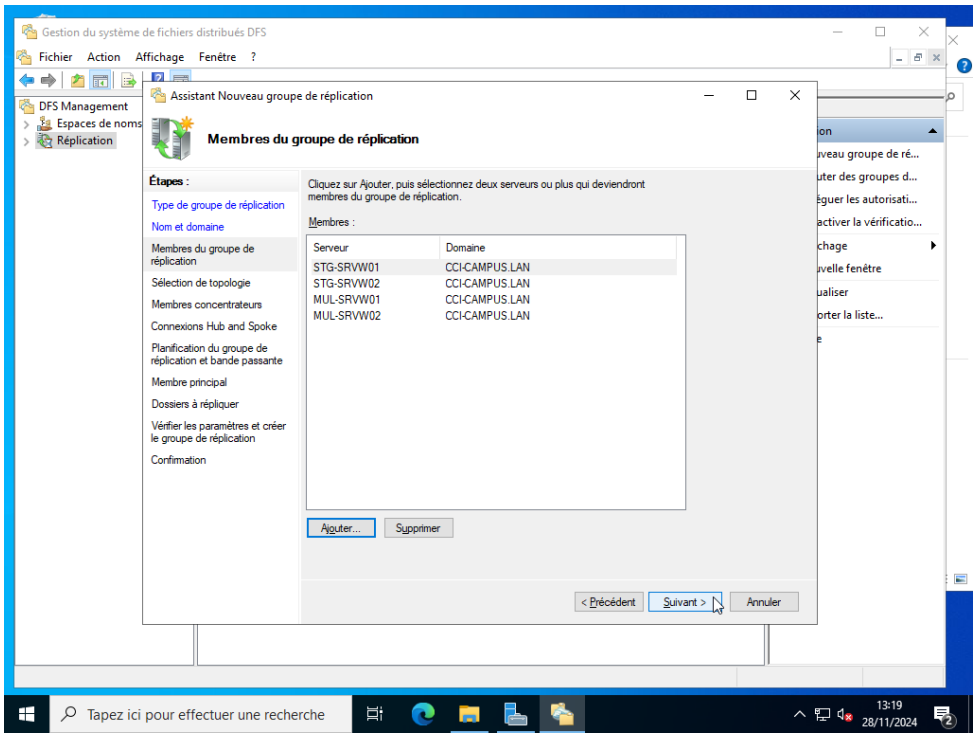
- Faire un clique droit sur réplication puis ajouter un nouveau **groupe de réplication multi-usage**



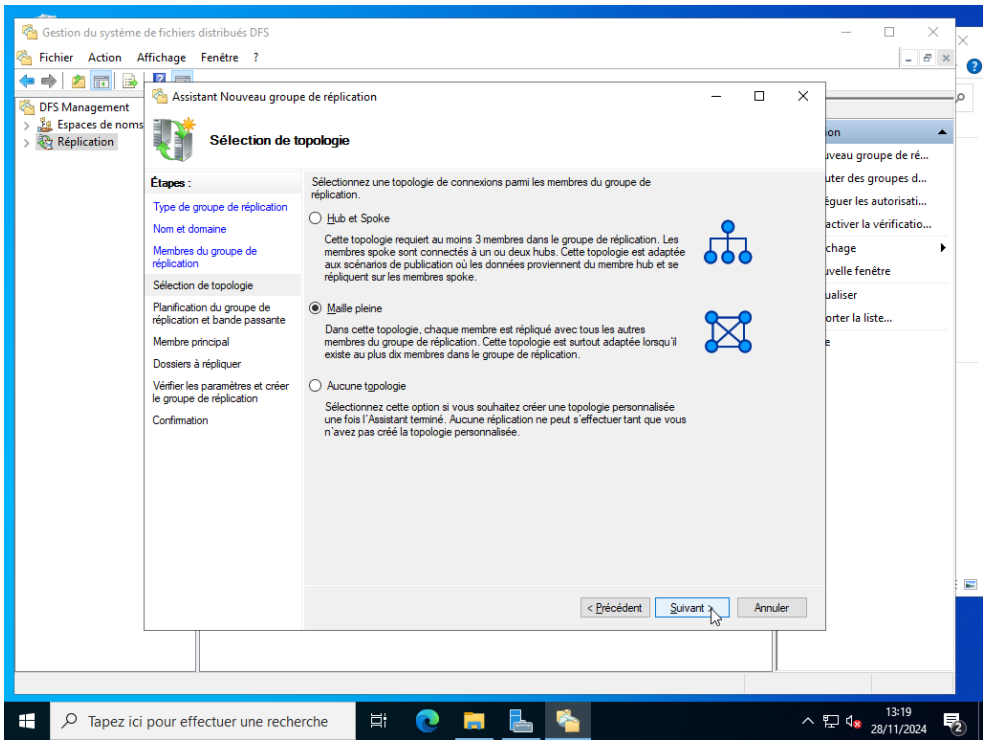
- Sélectionner le domaine



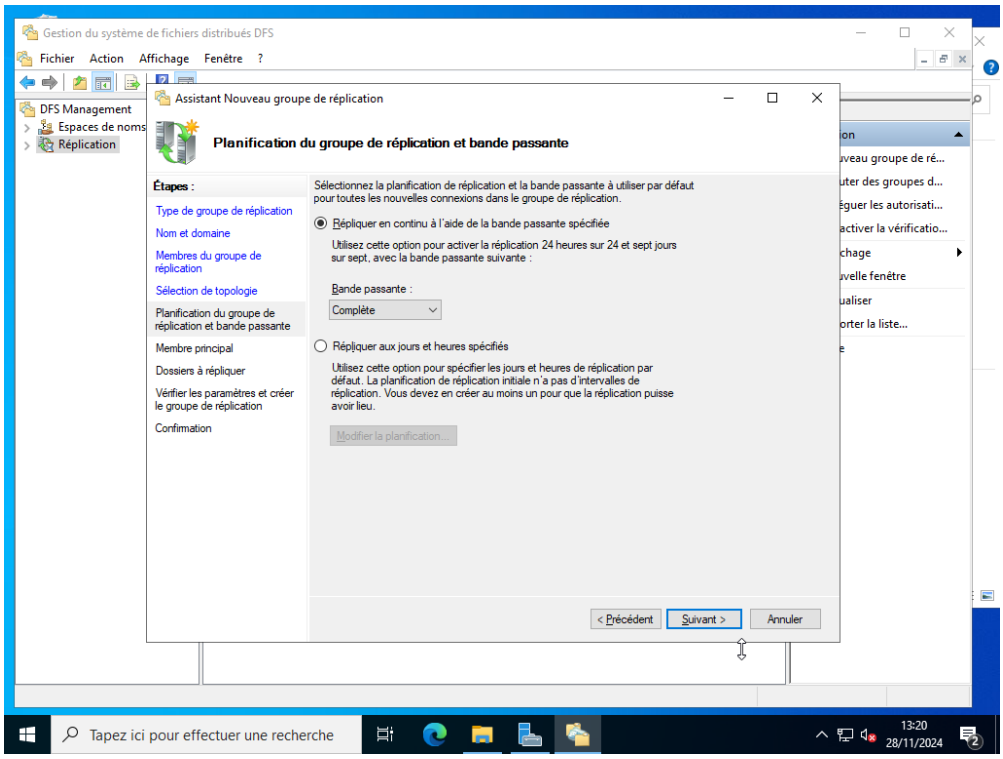
- Ajouter tous les serveurs comme membre du groupe de réplication



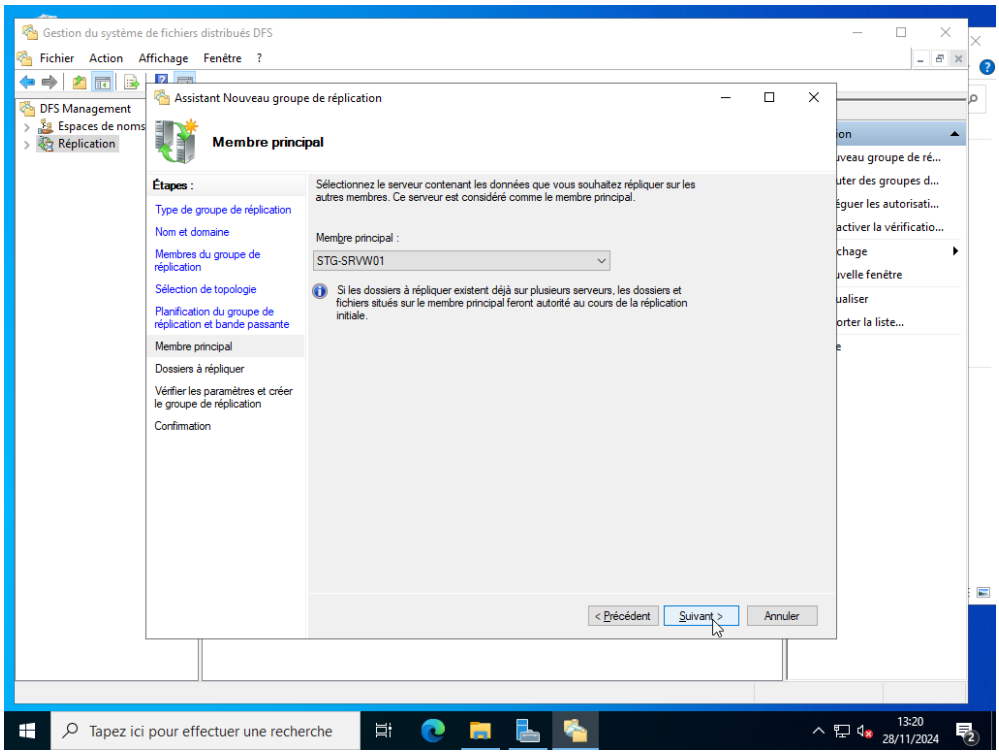
- Sélectionner **maille pleine** en typologie



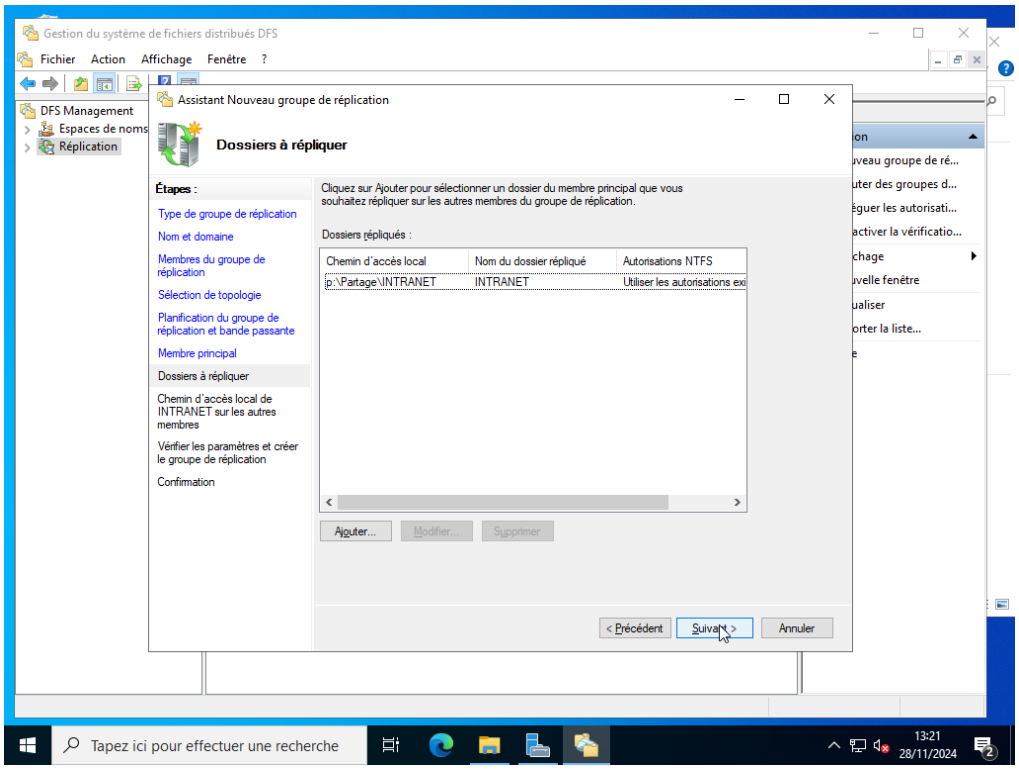
- Répliquer le contenu avec une bande passante complète



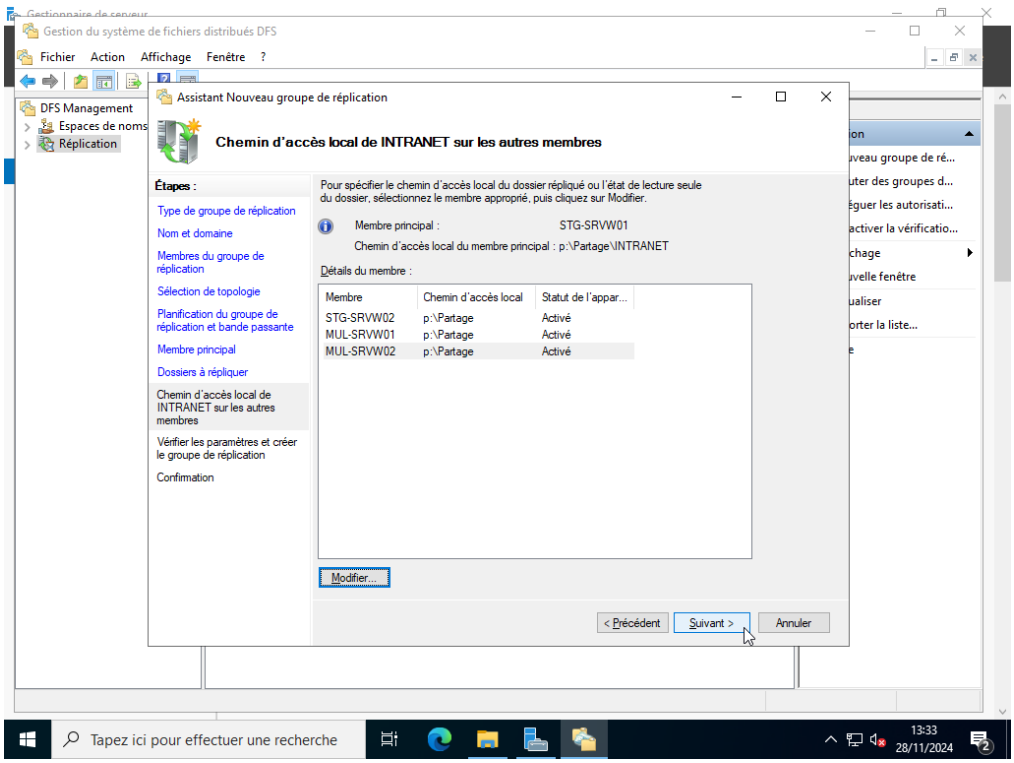
- Sélectionner le serveur principal



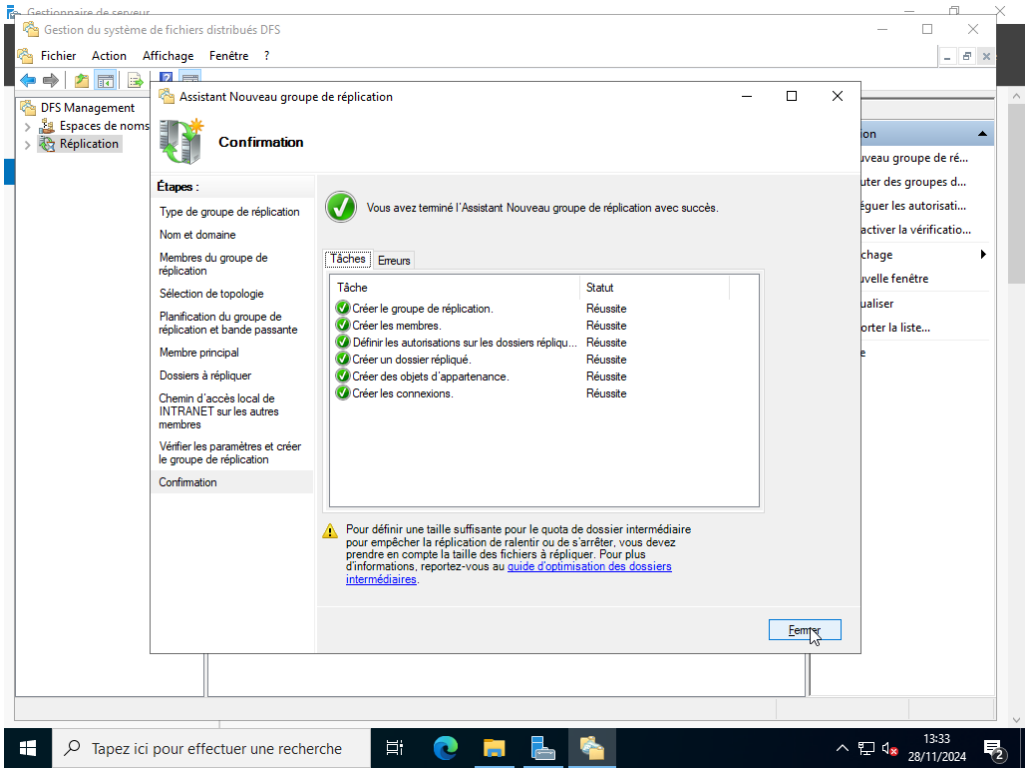
- Sélectionner le dossier **INTRANET** à répliquer



- Ajouter le chemin d'accès des autres serveurs



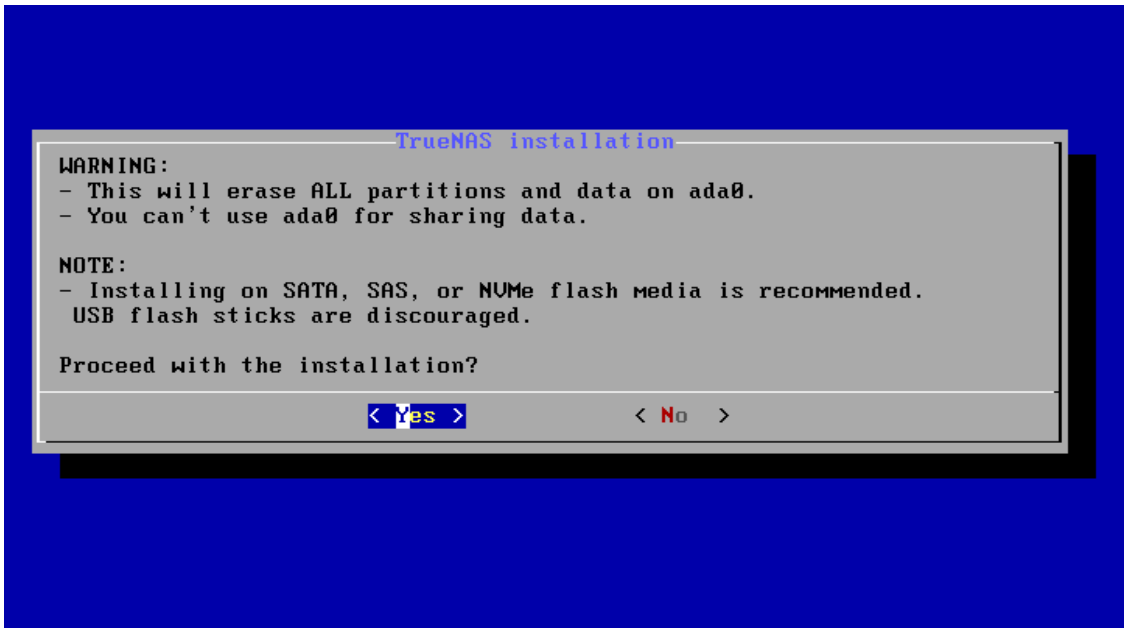
- La réplication est maintenant effective



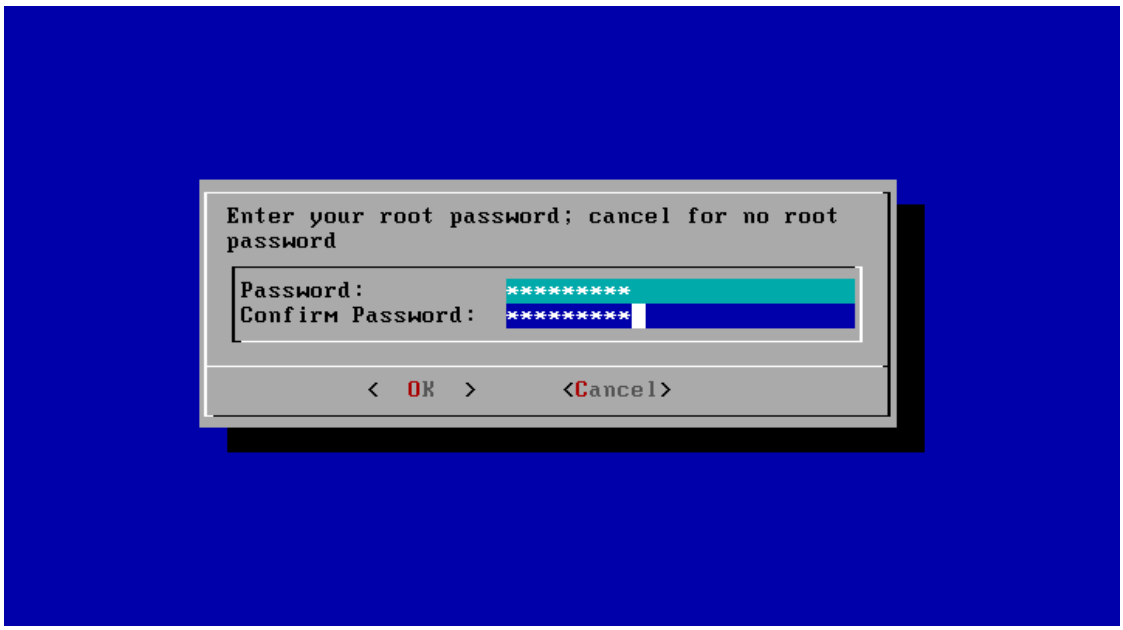
Mise en place de TrueNas

Installation

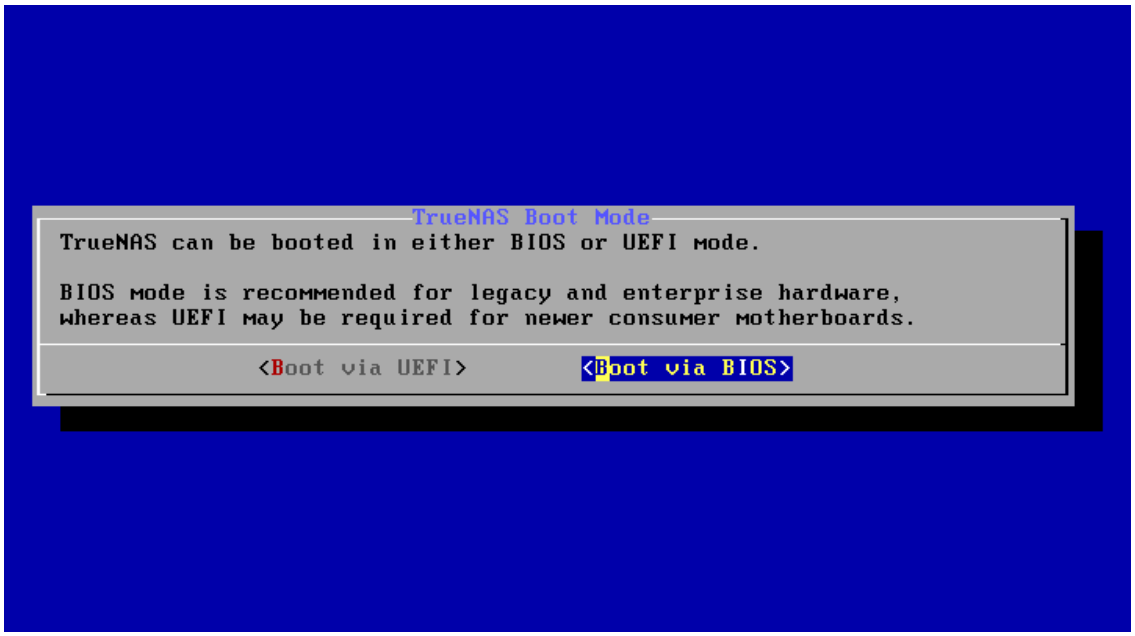
- Au début de l'installation cliquer sur **yes**



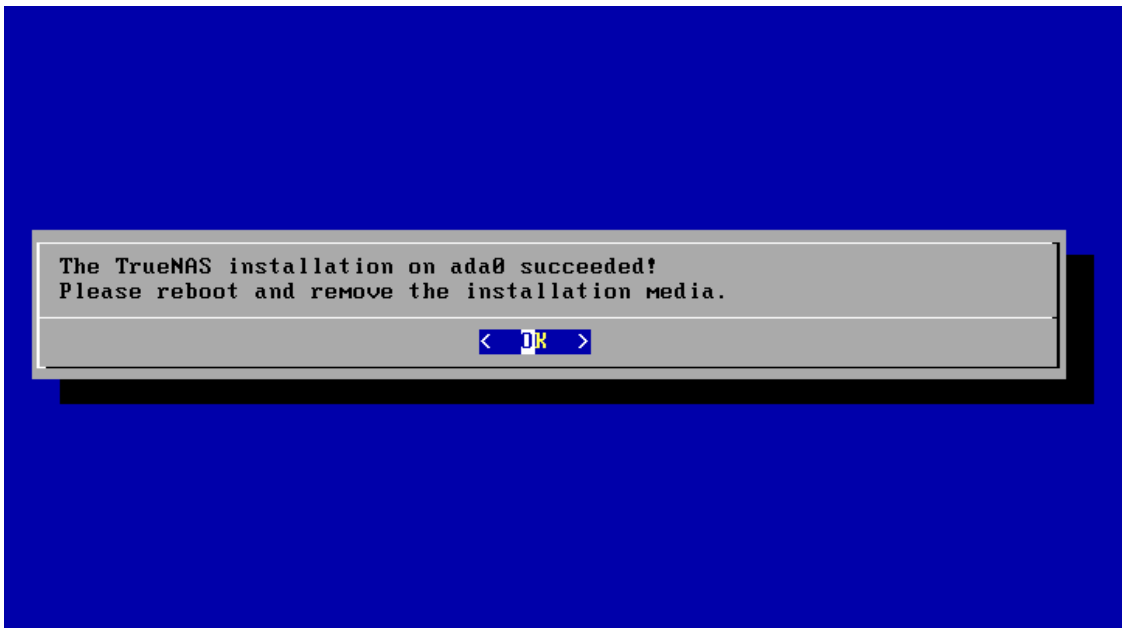
- Choisissez un mot de passe



- Sélectionner **boot via BIOS**

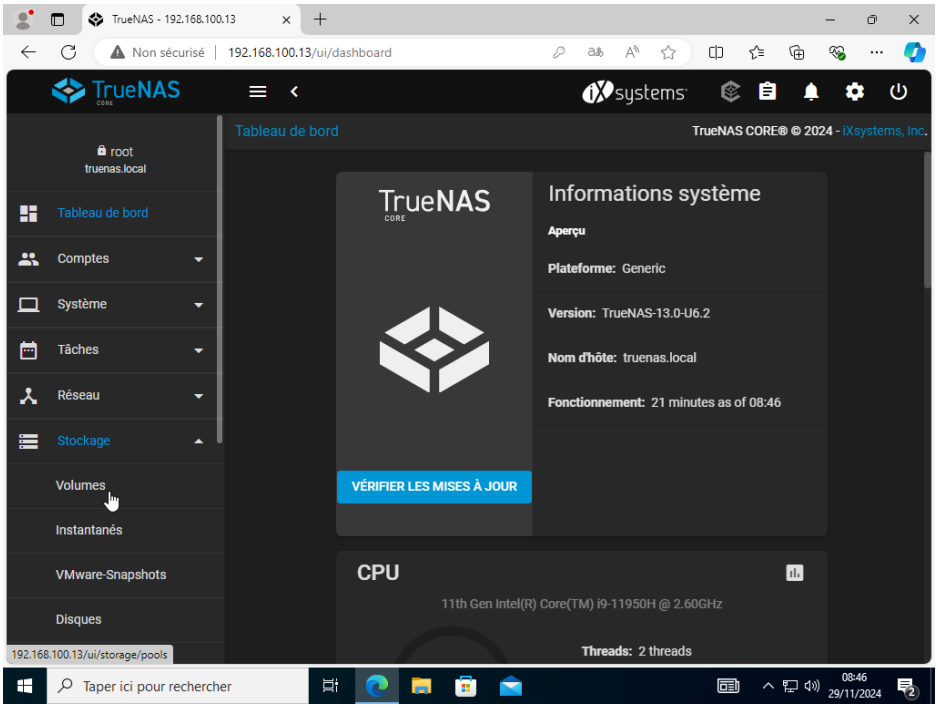


- Redémarrer le système

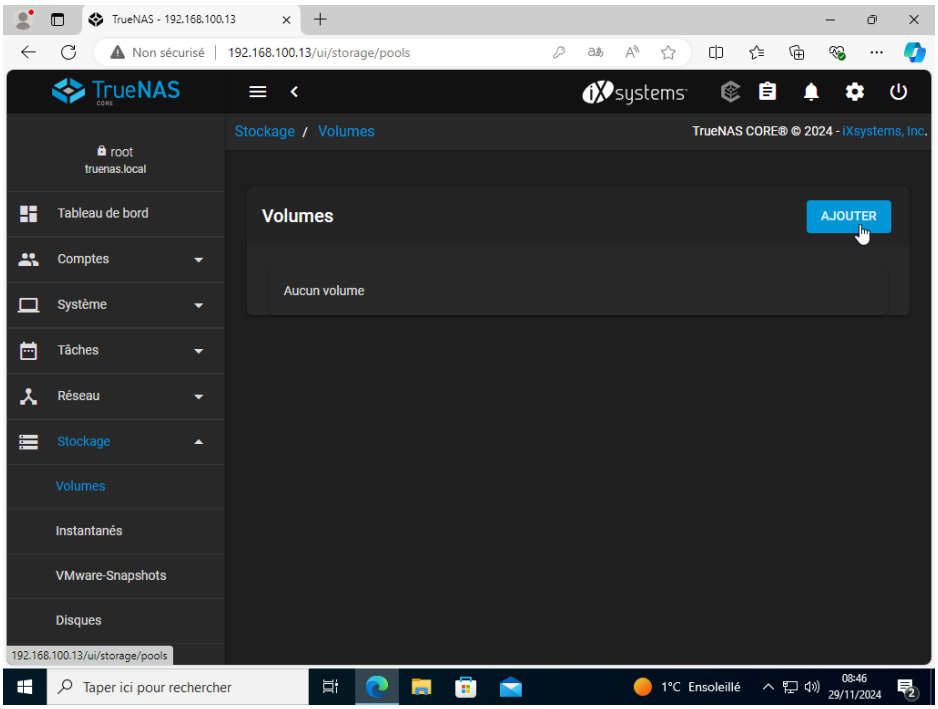


Création du volume

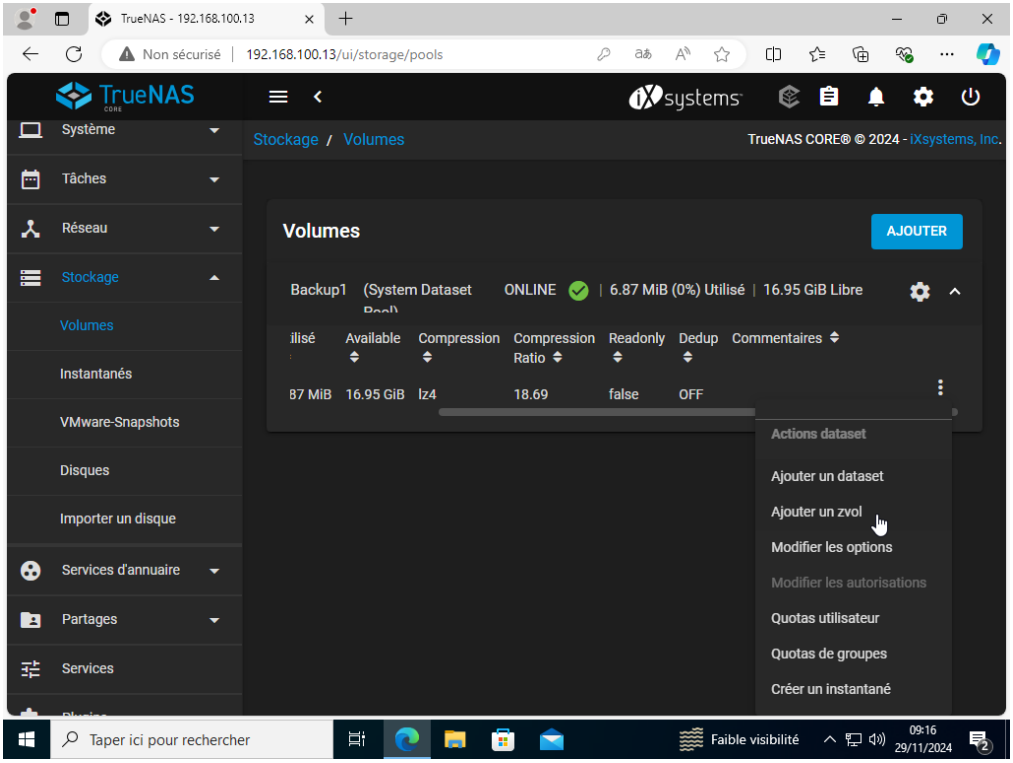
- Une fois redémarré on accède au tableau de bord, puis se rendre dans l'onglet **stockage -> volumes**



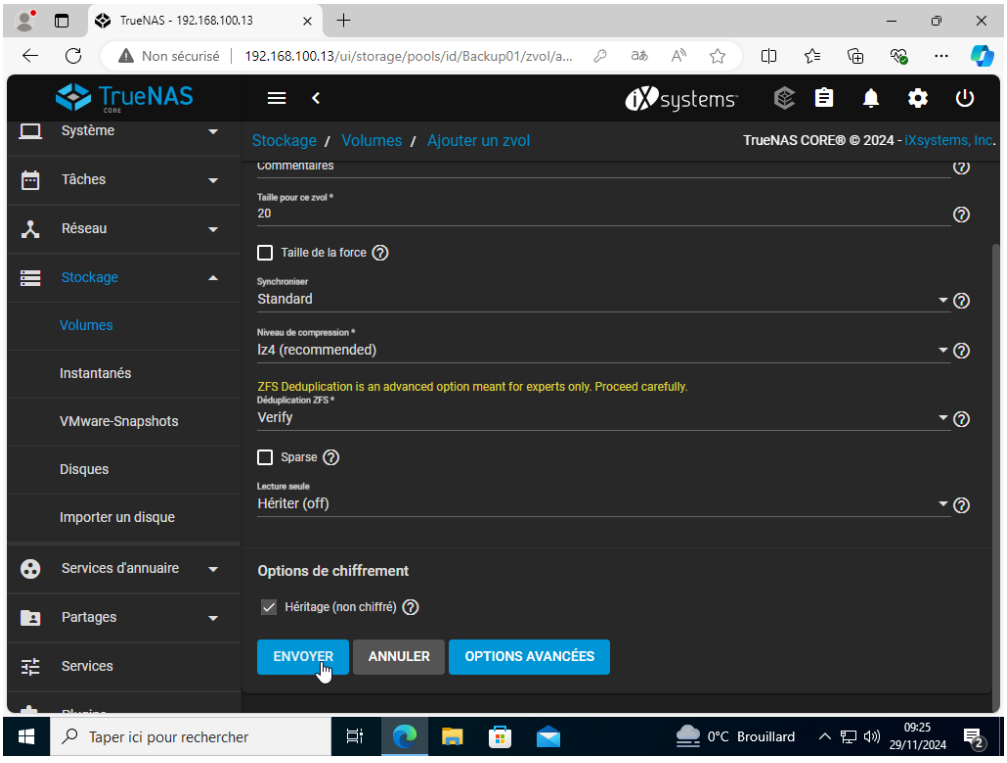
- Ajouter un nouveau volume



- Une fois le volume créer, ajouter un zvol

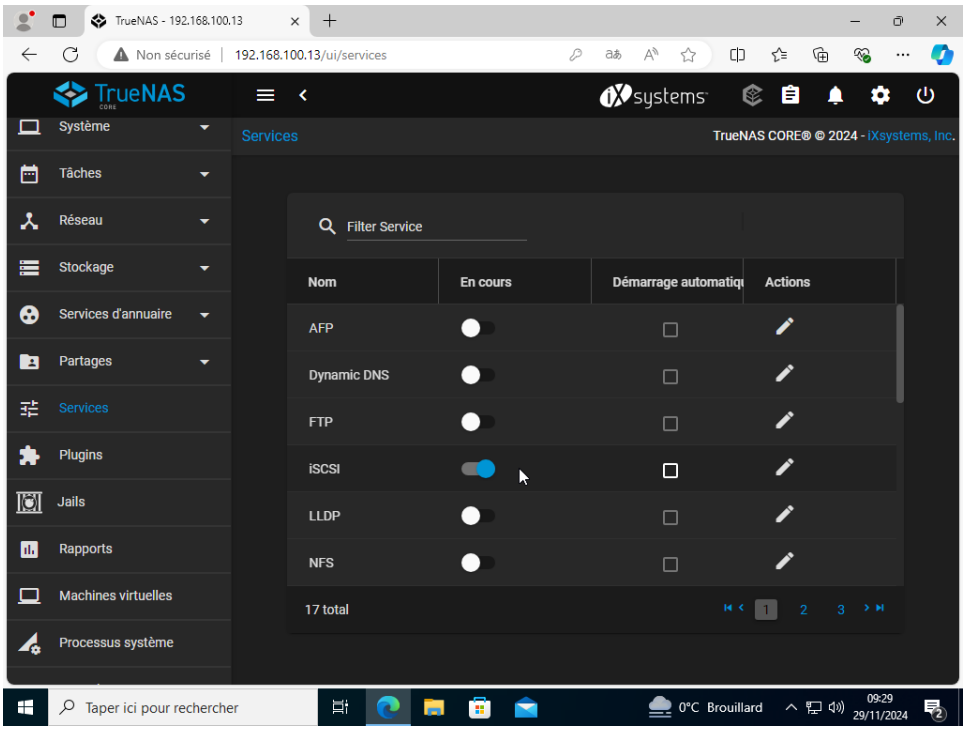


- Confirmer la création du zvol

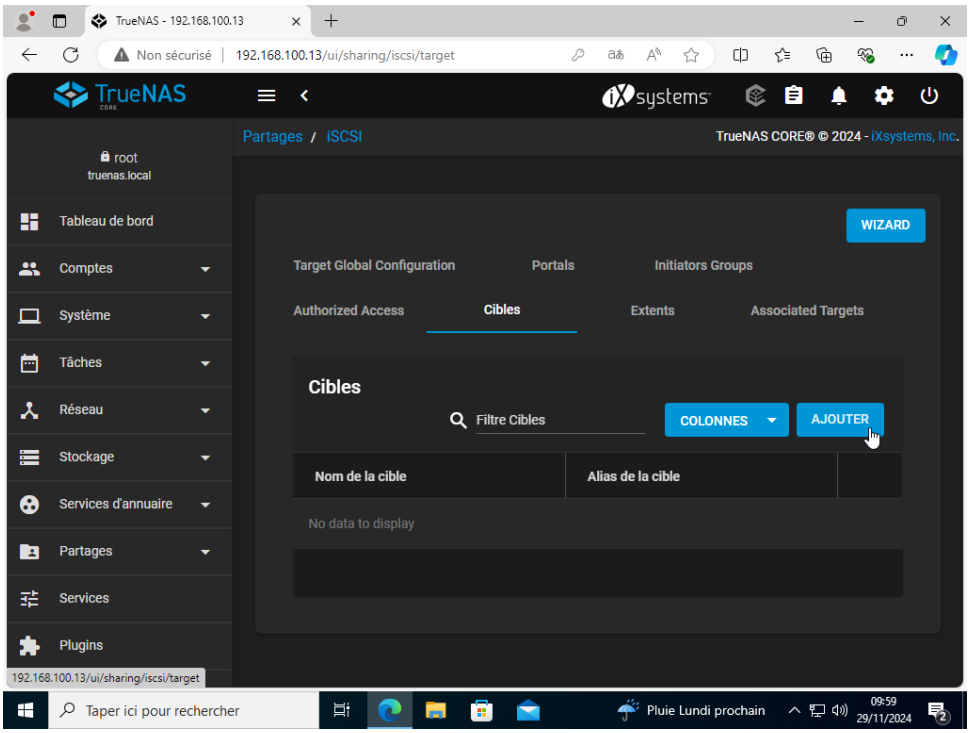


Configuration du partage ISCSI

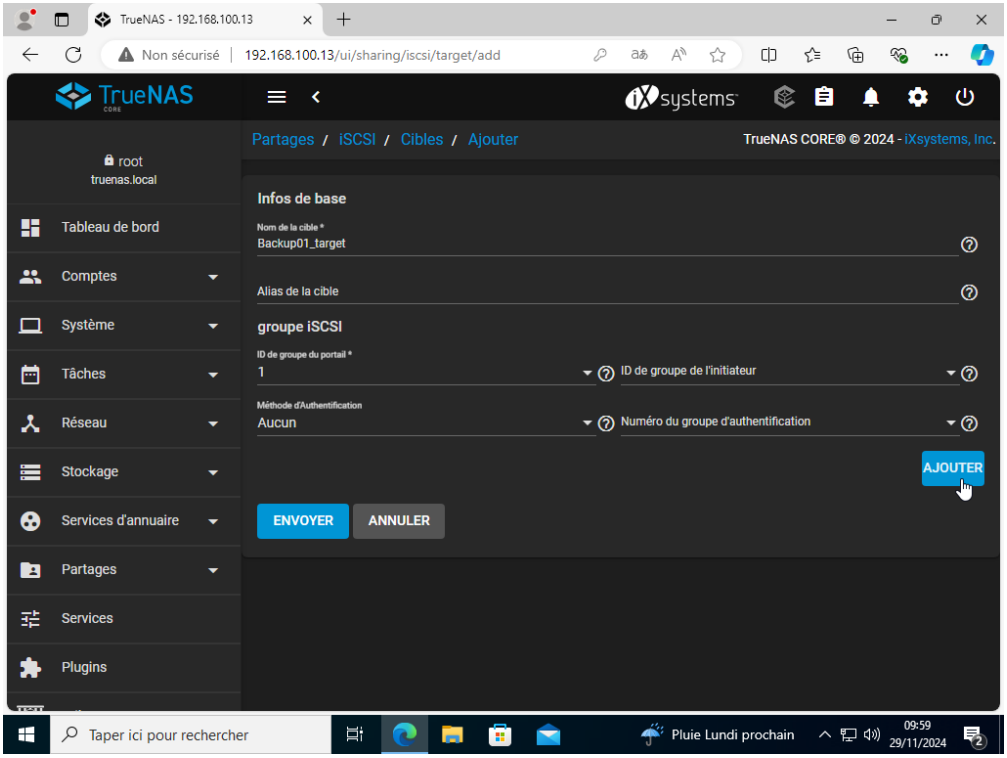
- Dans l'onglet **services**, activé le service **ISCSI**



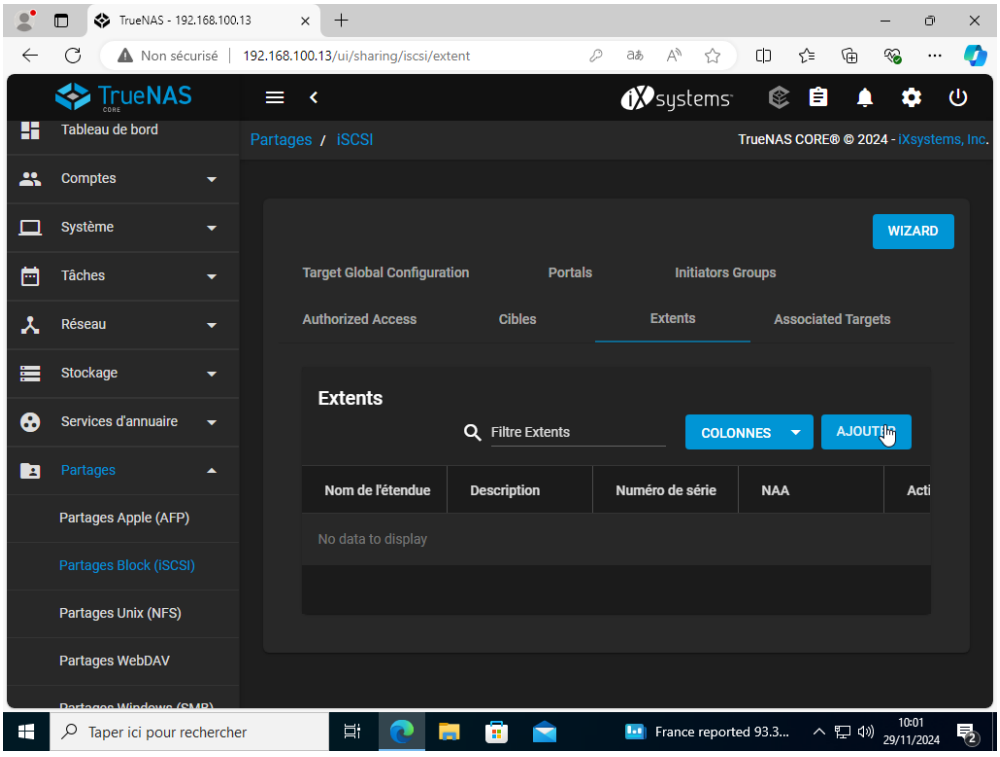
- Dans **partage -> ISCSI** ajouter une nouvelle cible



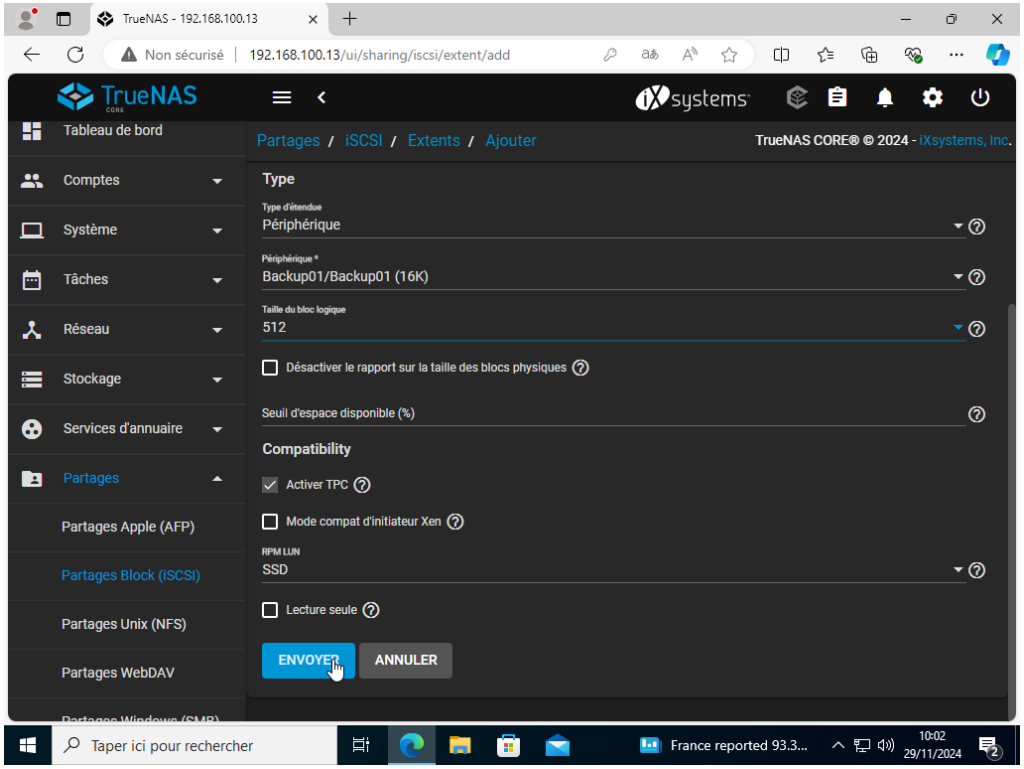
- Choisissez un nom et un id pour la cible



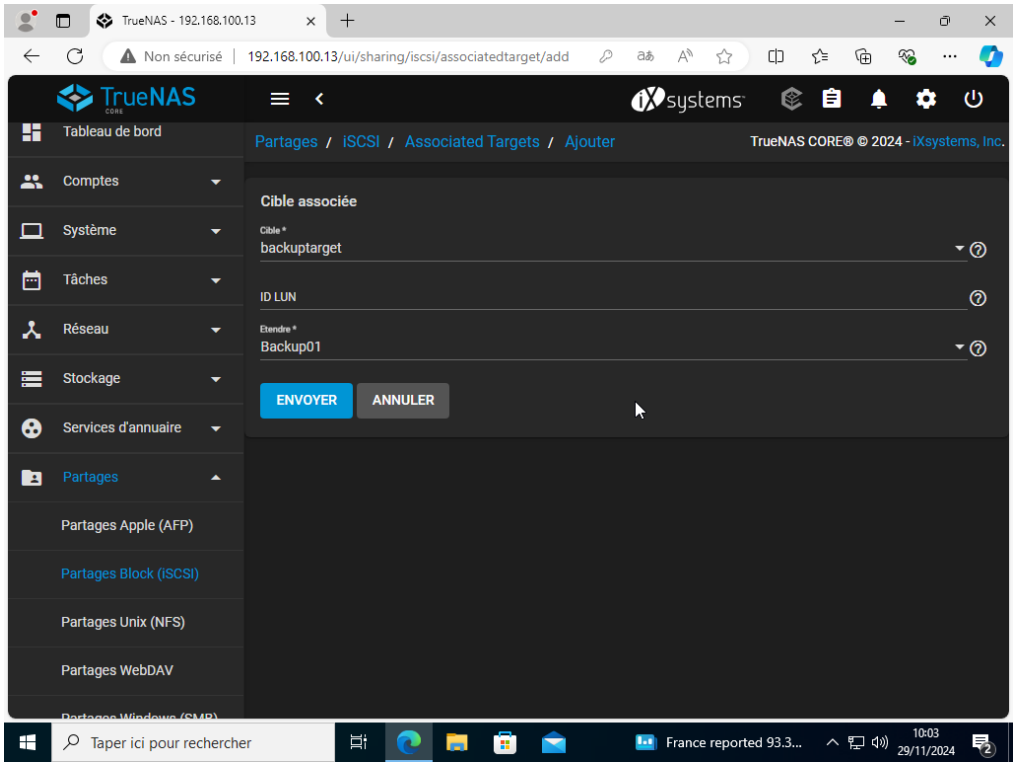
- Ajouter un extents



- Sélectionner le disque ISCSI

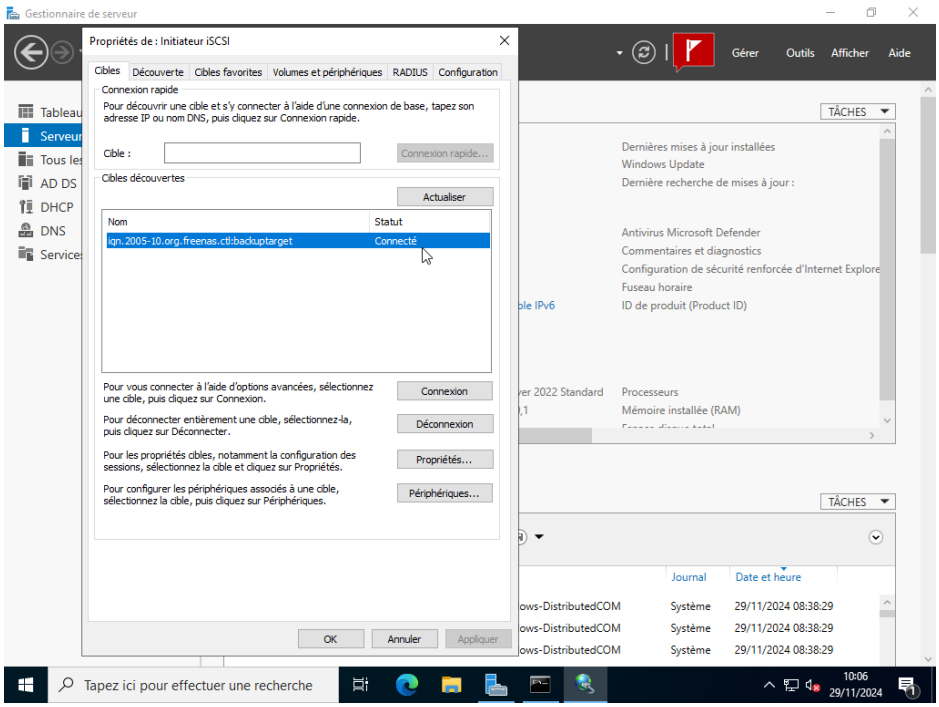


- Configurer l'association de cible

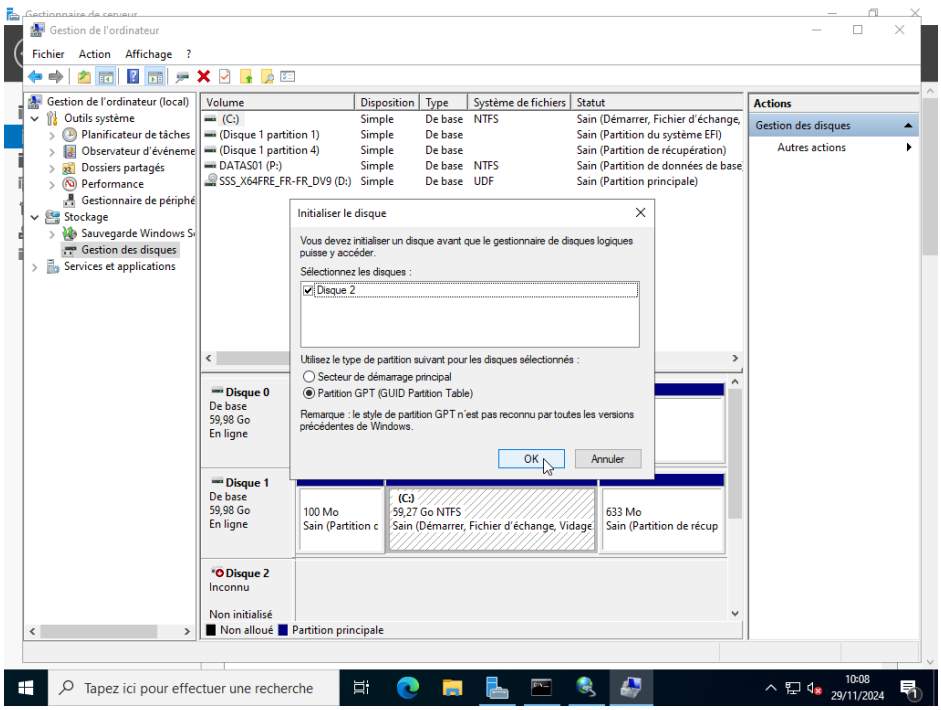


Ajout du disque sur le serveur

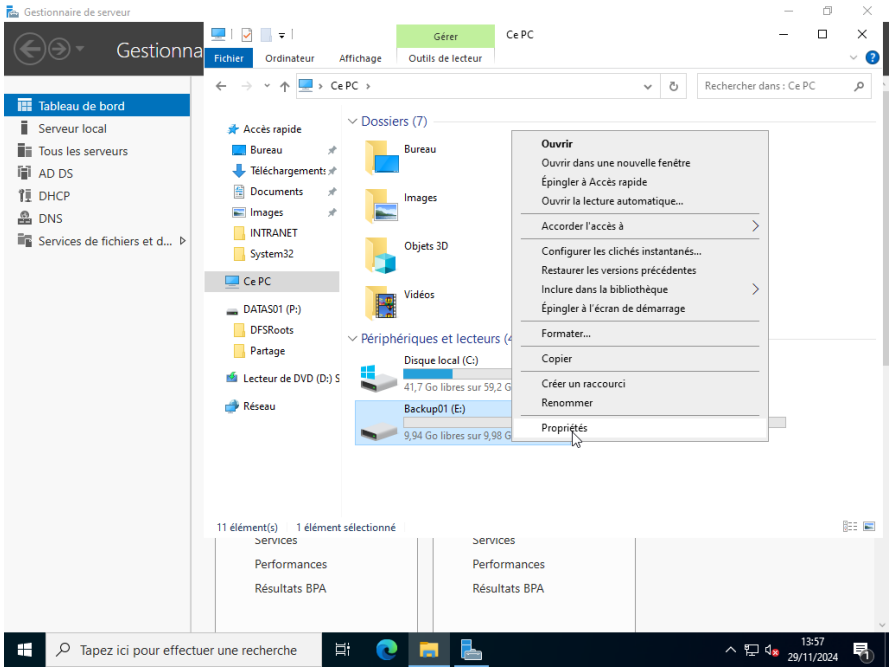
- Ouvrir **l'initiateur ISCSI** et dans le champ cible entrer l'adresse IP de TrueNas



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

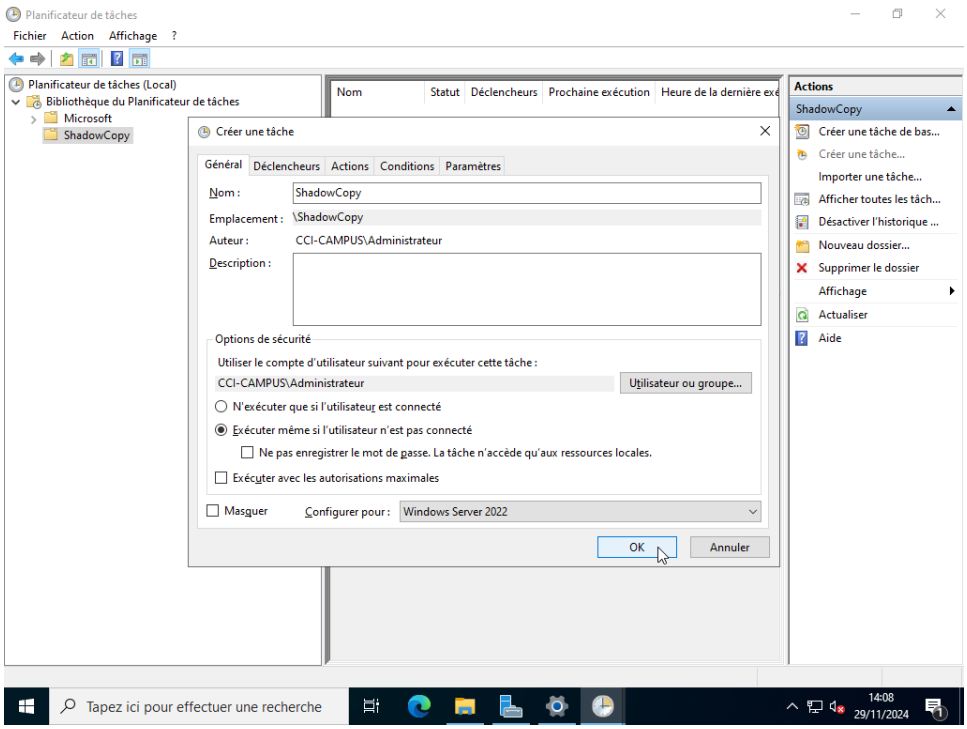


- Le disque est maintenant créé et disponible dans l'explorateur de fichier



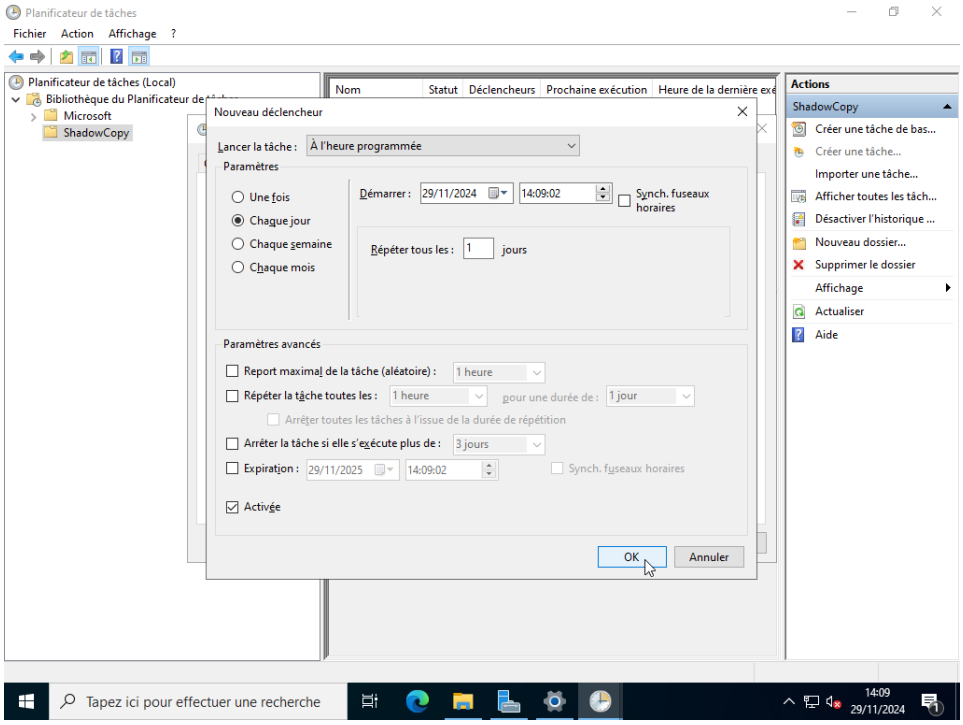
Mise en place de ShadowCopy

- Créer une tache

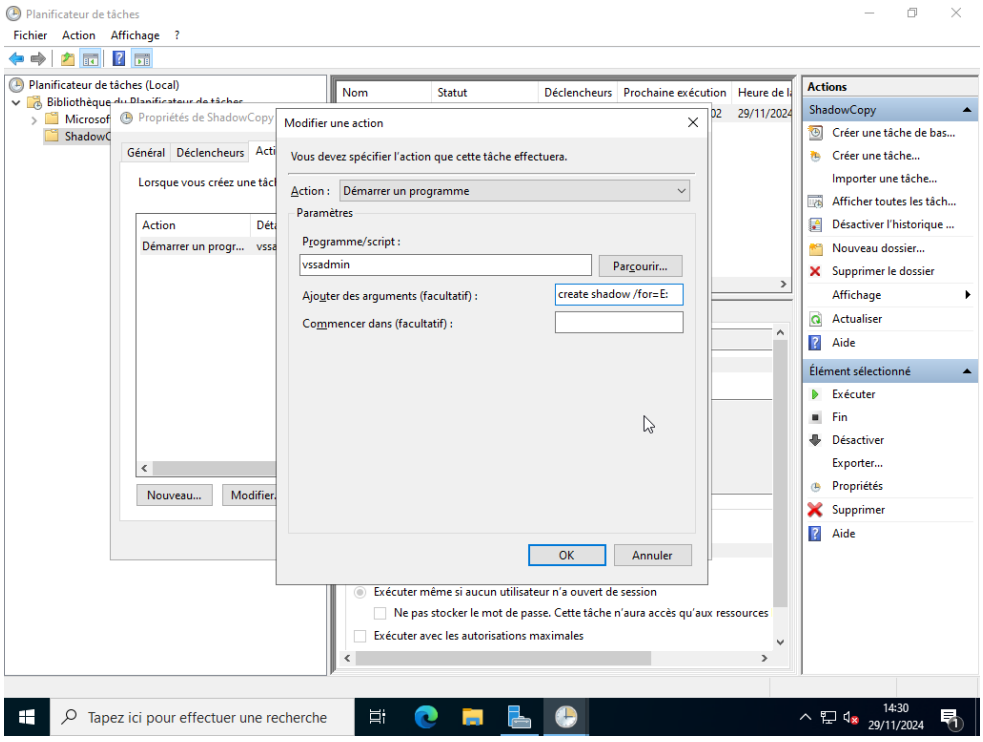


- Activé la

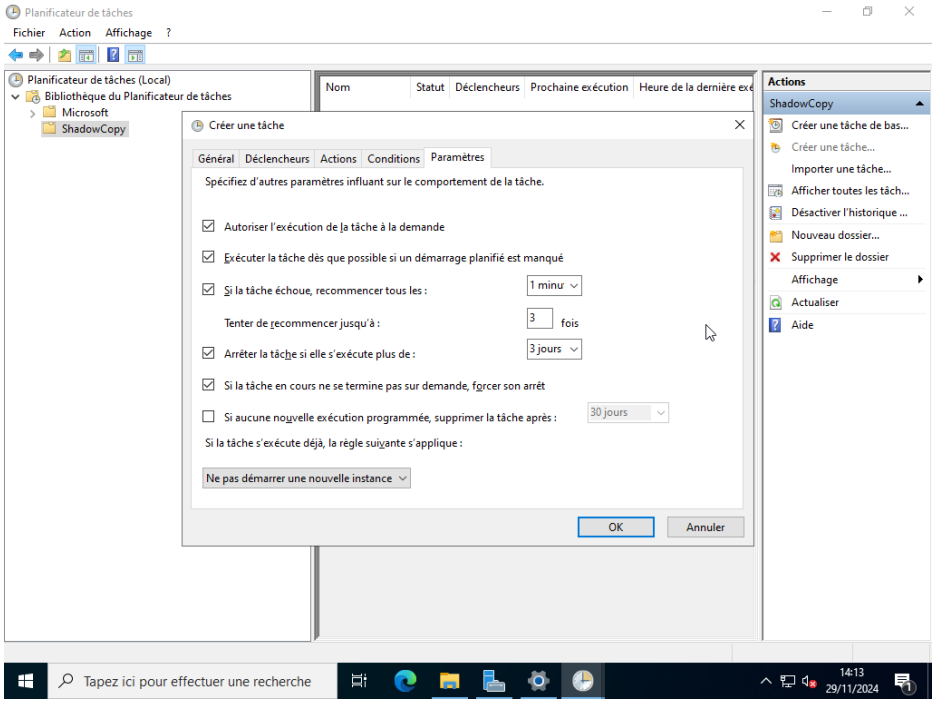
tâche tous les jours à une certaine heure



- Définir l'action de la tâche



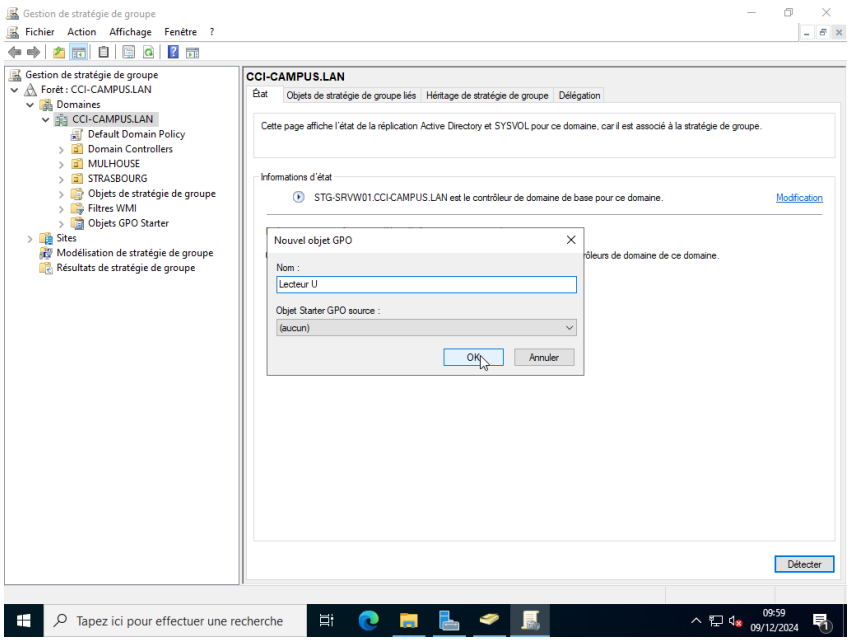
- Cocher les mêmes paramètres ci-dessous



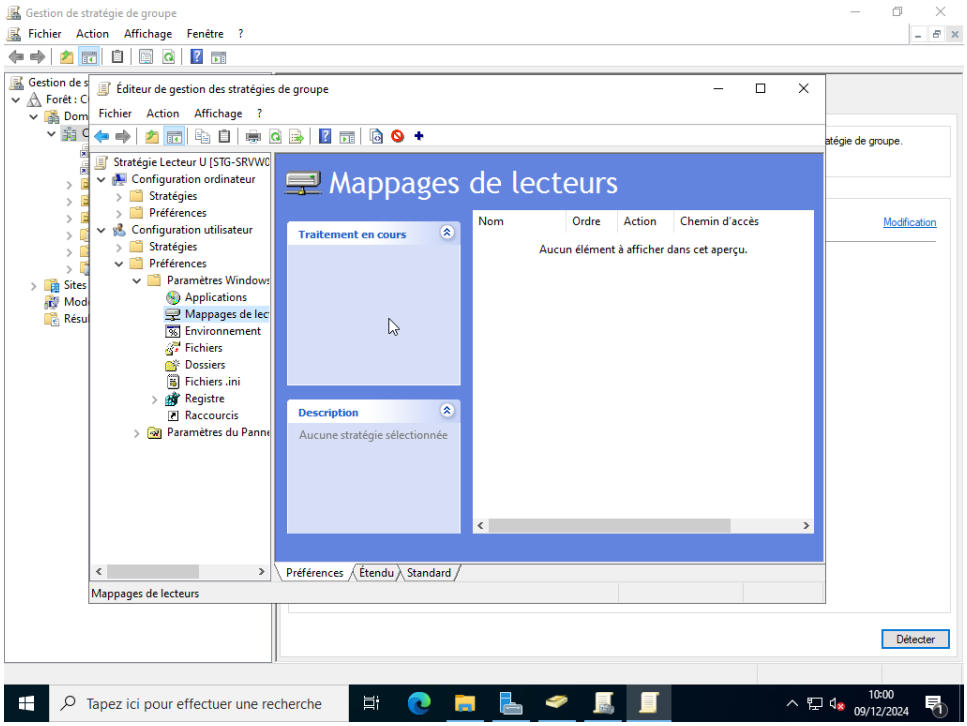
Mise en place des GPO

Mappage des lecteurs

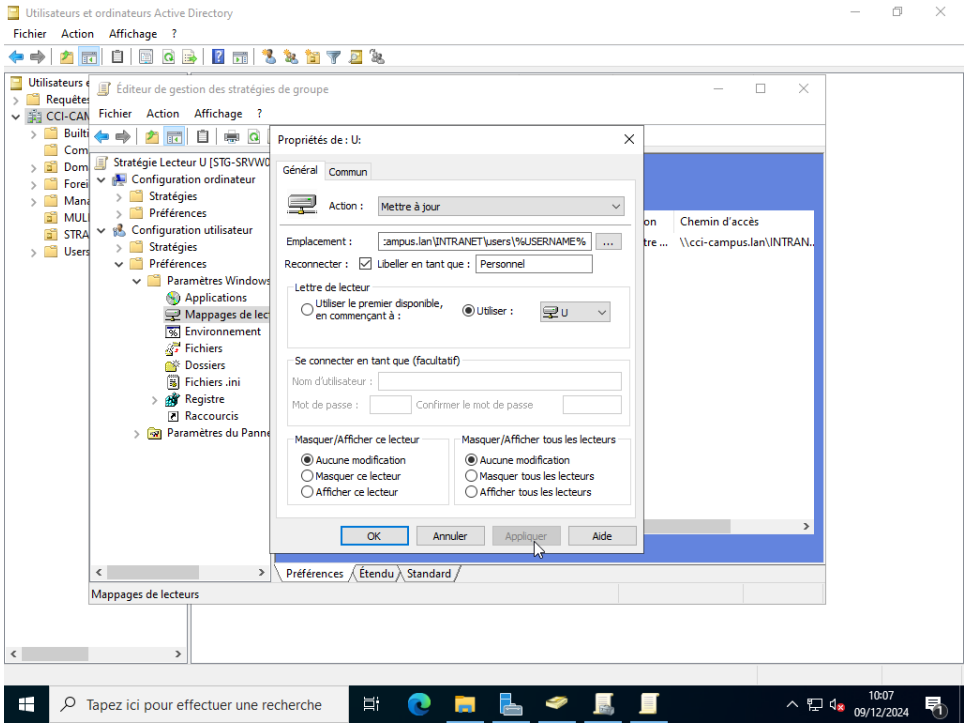
- Dans le gestionnaire de stratégie de groupe créer une nouvelle GPO



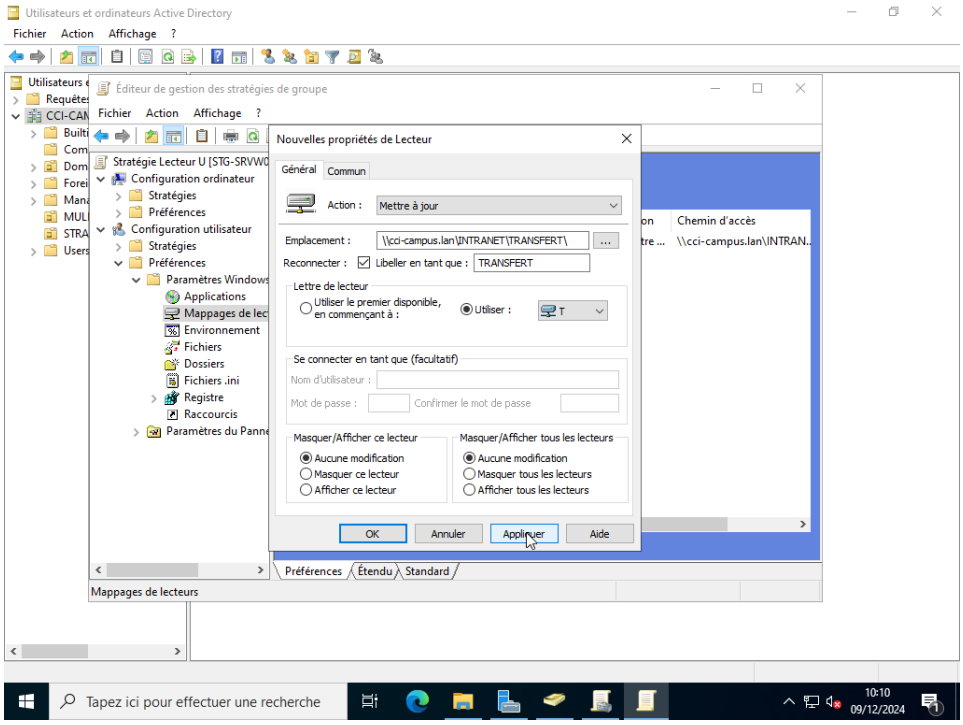
- Faire un clique droit -> **modifier** sur la GPO puis se rendre dans **Configuration utilisateur -> Préférences -> Paramètres Windows -> Mappages de lecteurs**



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

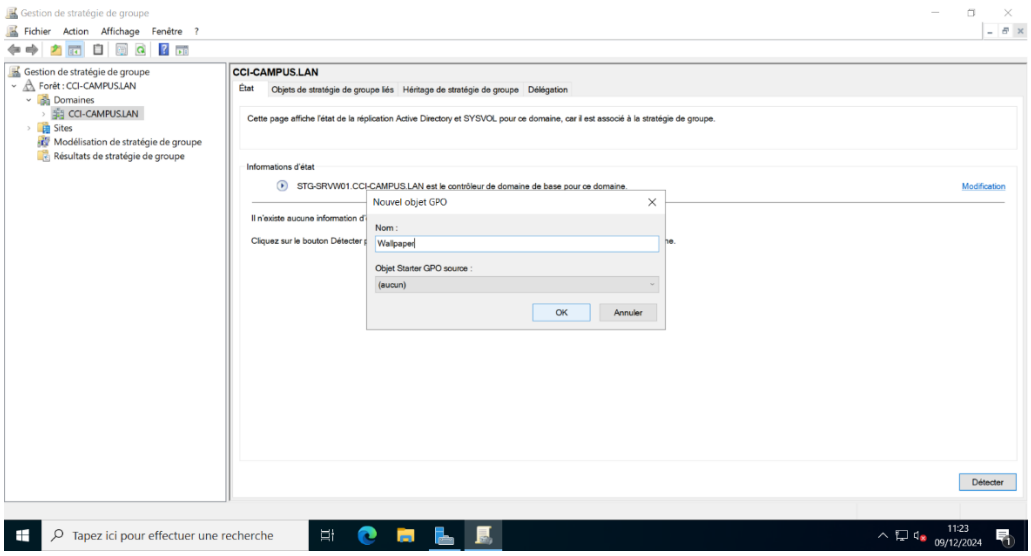


- Faire de même pour le lecteur TRANSFERT

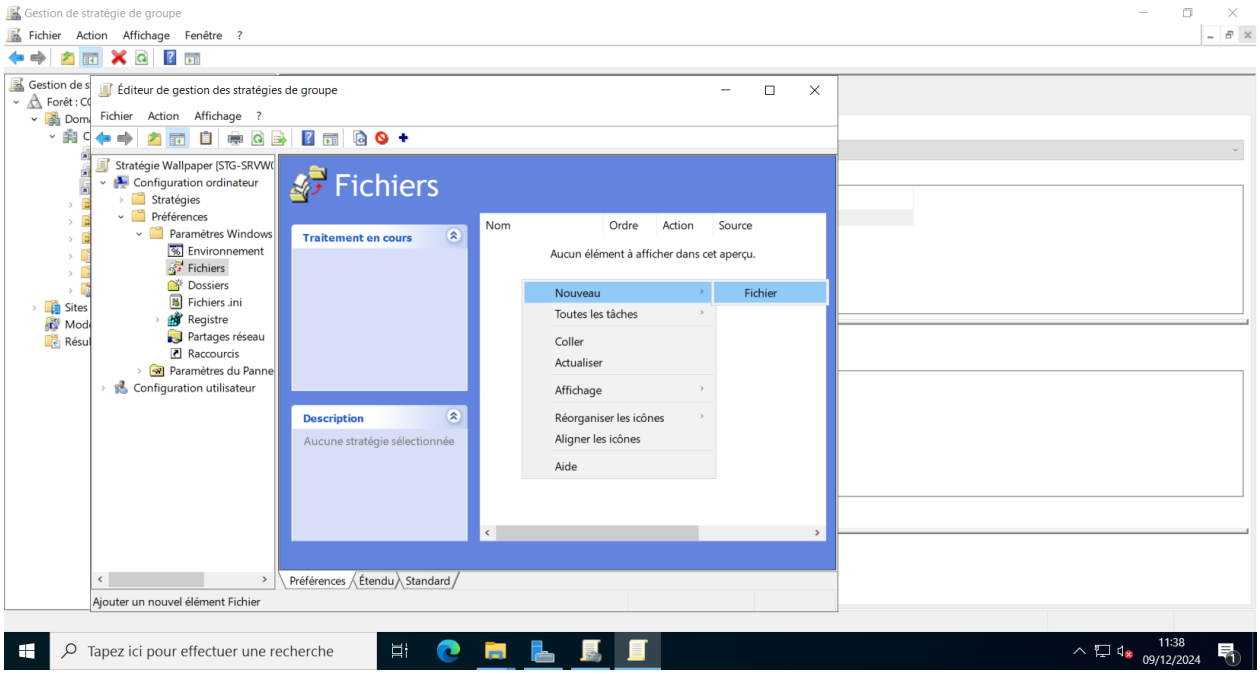


Papier peint du bureau

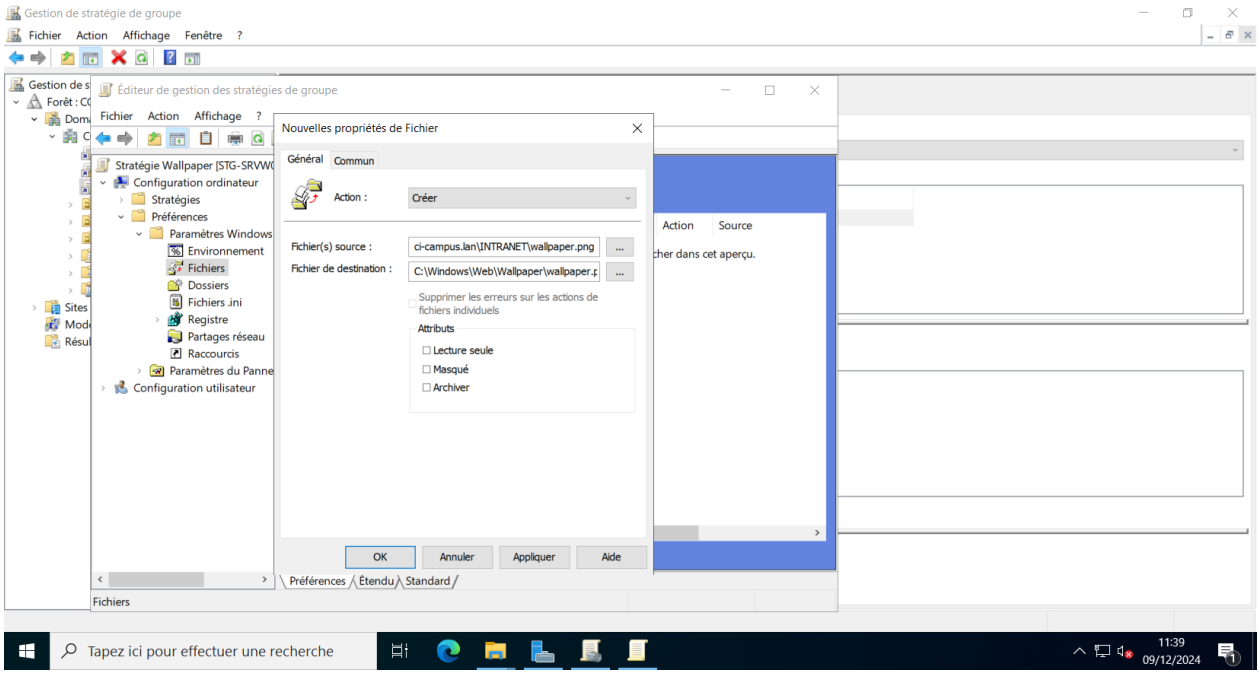
- Créer une GPO à la racine du domaine



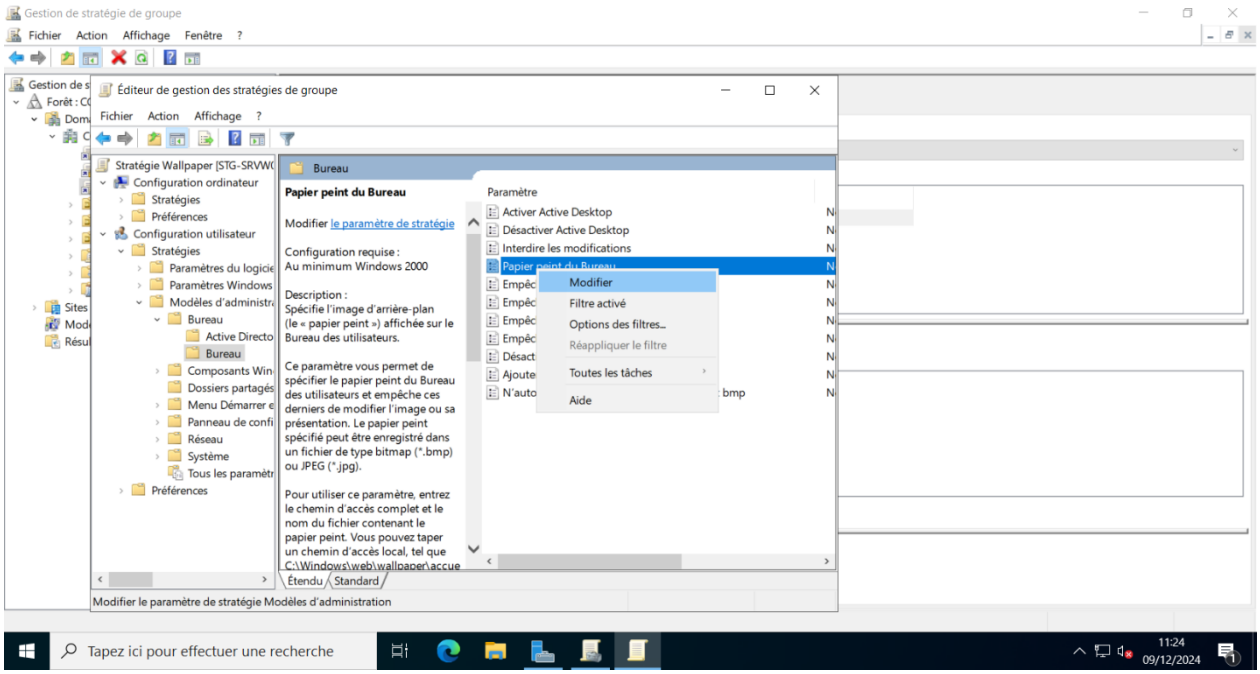
- Se rendre dans **Configuration ordinateur -> Préférences -> Paramètres Windows -> Fichiers**. Ajouter un nouveau fichier



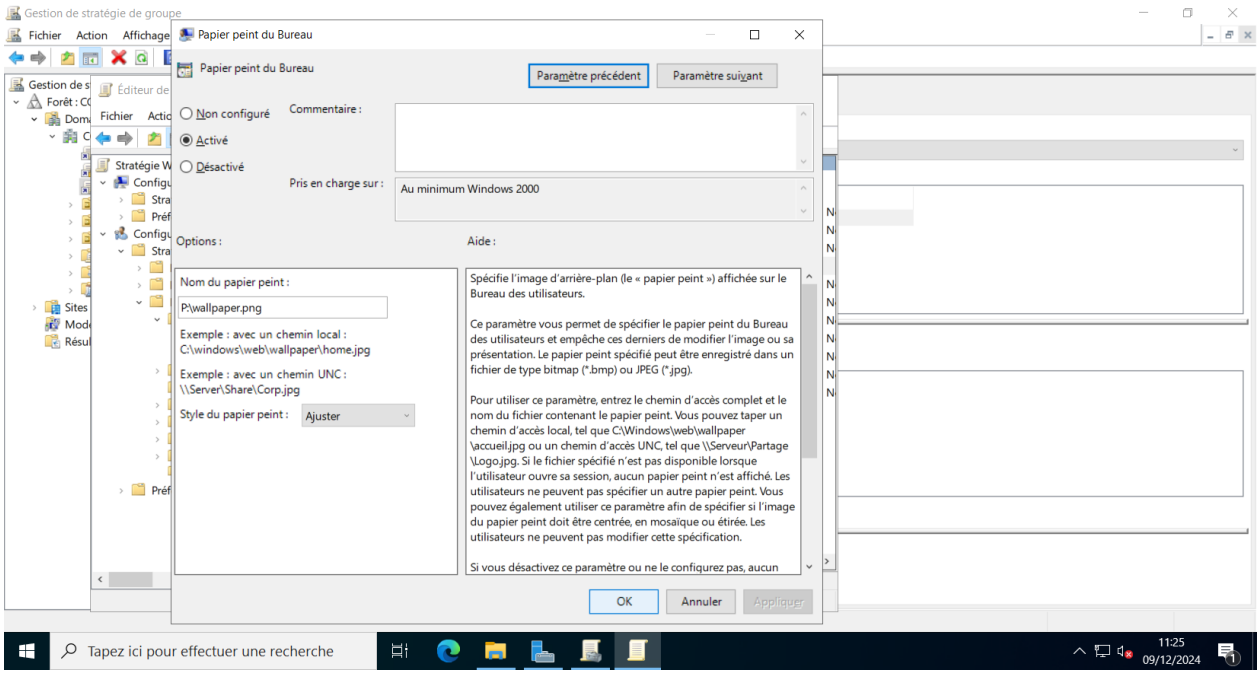
- Sélectionner le fichier source, c'est-à-dire la où se trouve le fichier sur le réseau et un fichier de destination la où sera copier le fichier sur le client afin de pouvoir y accéder.



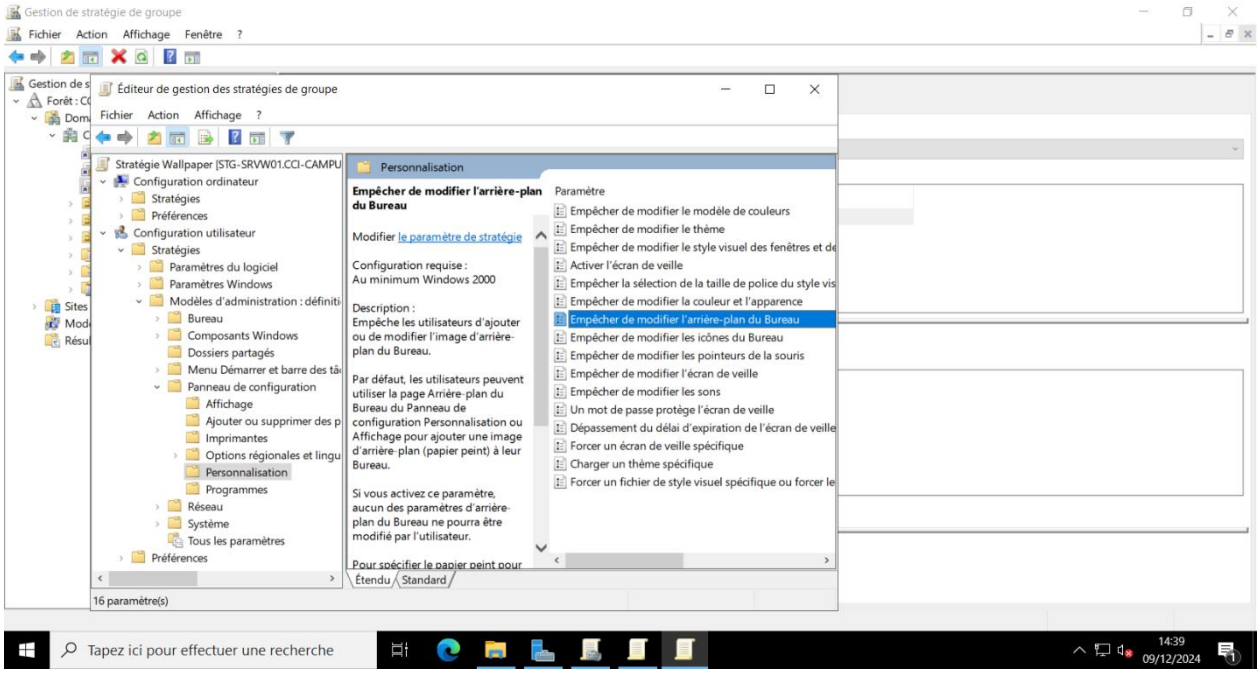
- Ensuite se rendre dans **Configuration utilisateur -> Stratégies -> Modèles d'administration -> Bureau -> Bureau**.



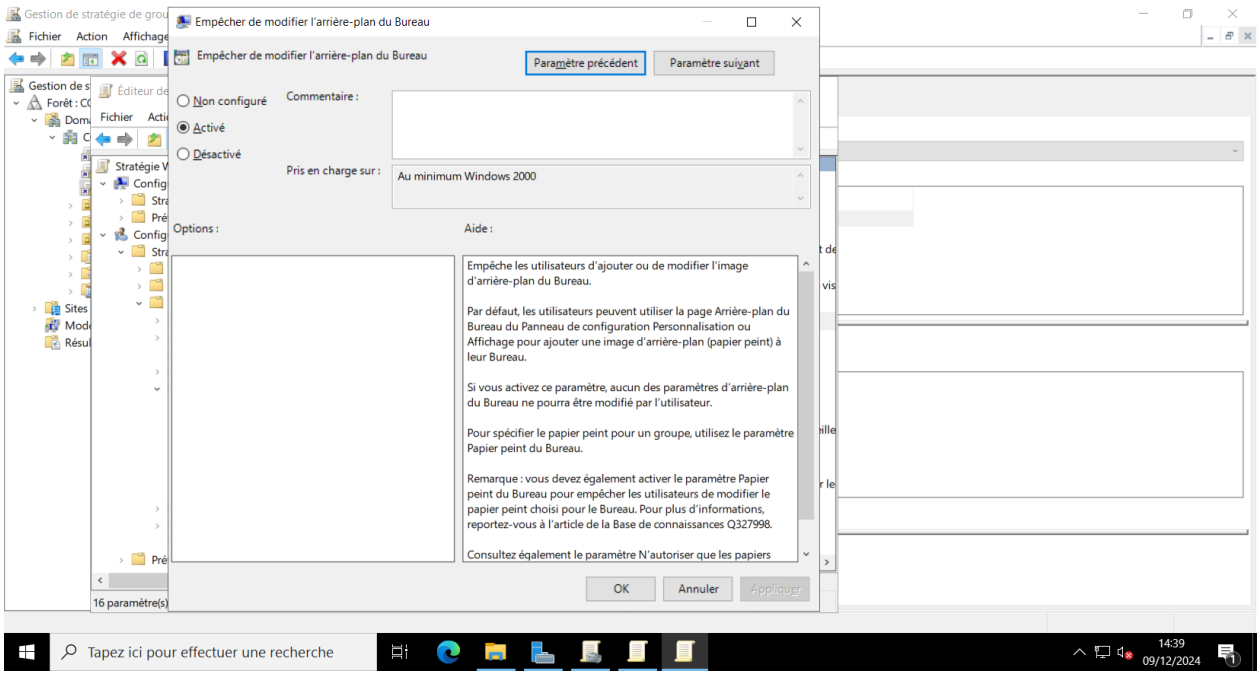
- Ajouter le chemin du fichier du font d'écran



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

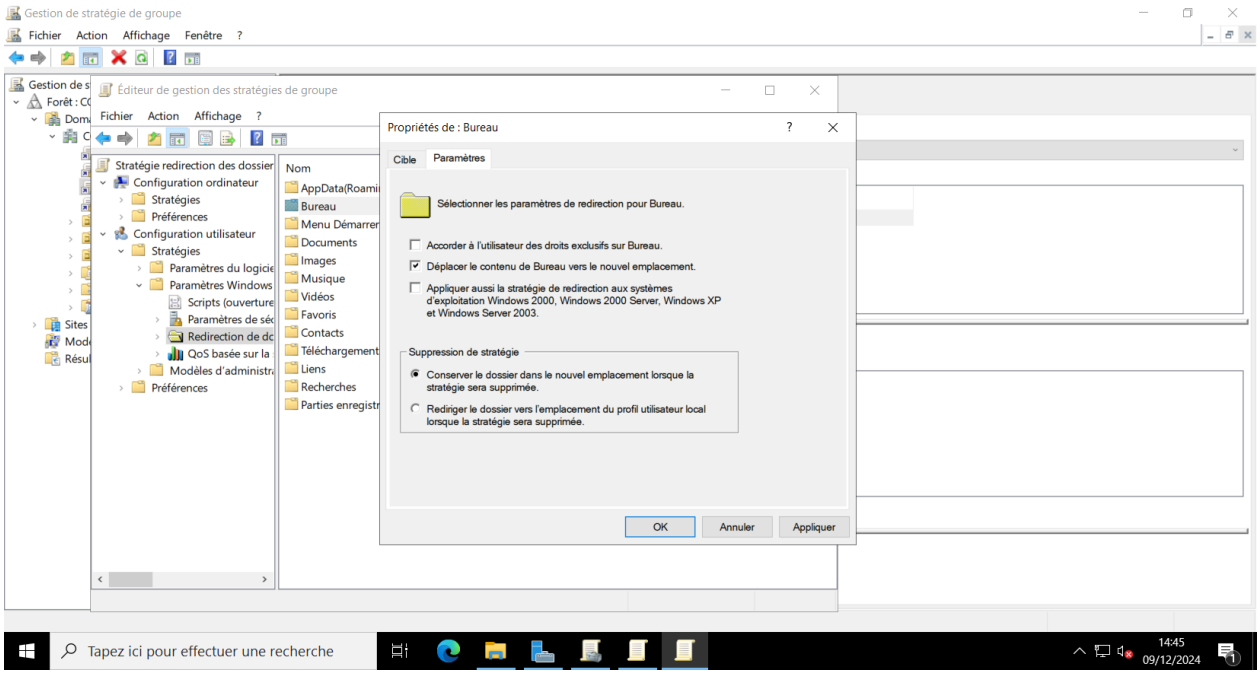


- Activer la GPO

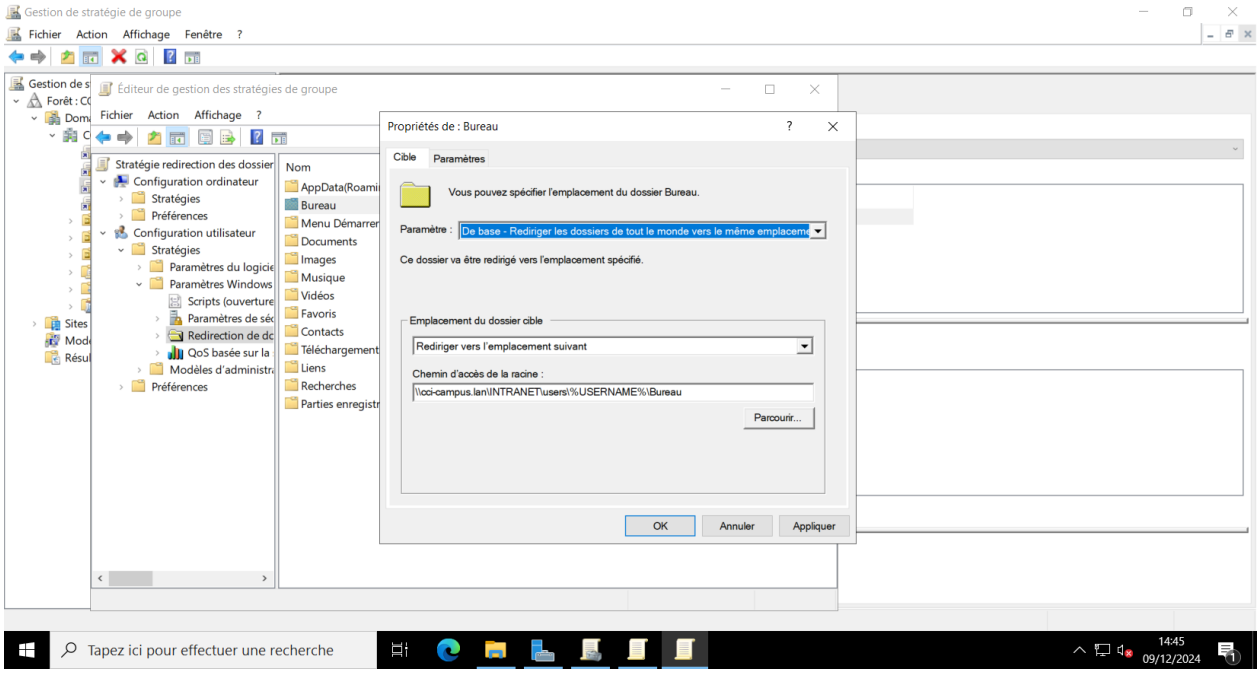


Redirection des dossiers personnels

- 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**

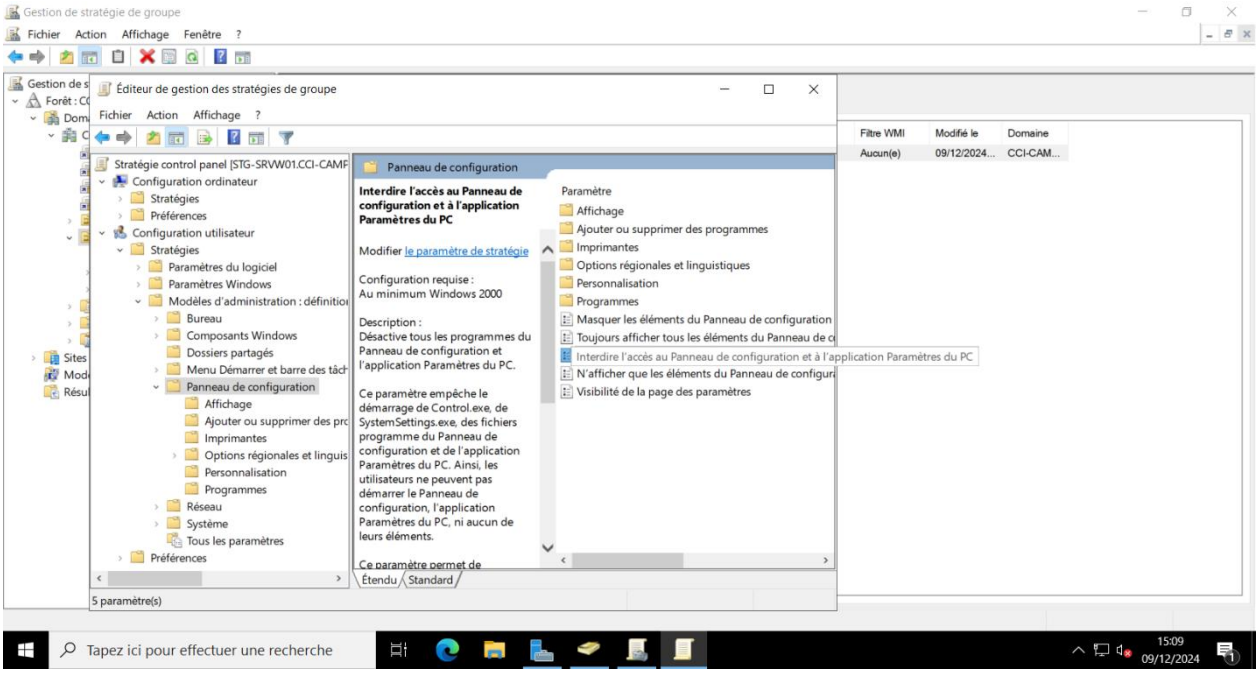


- Choisir l'emplacement vers lequel sera redirigé le dossier

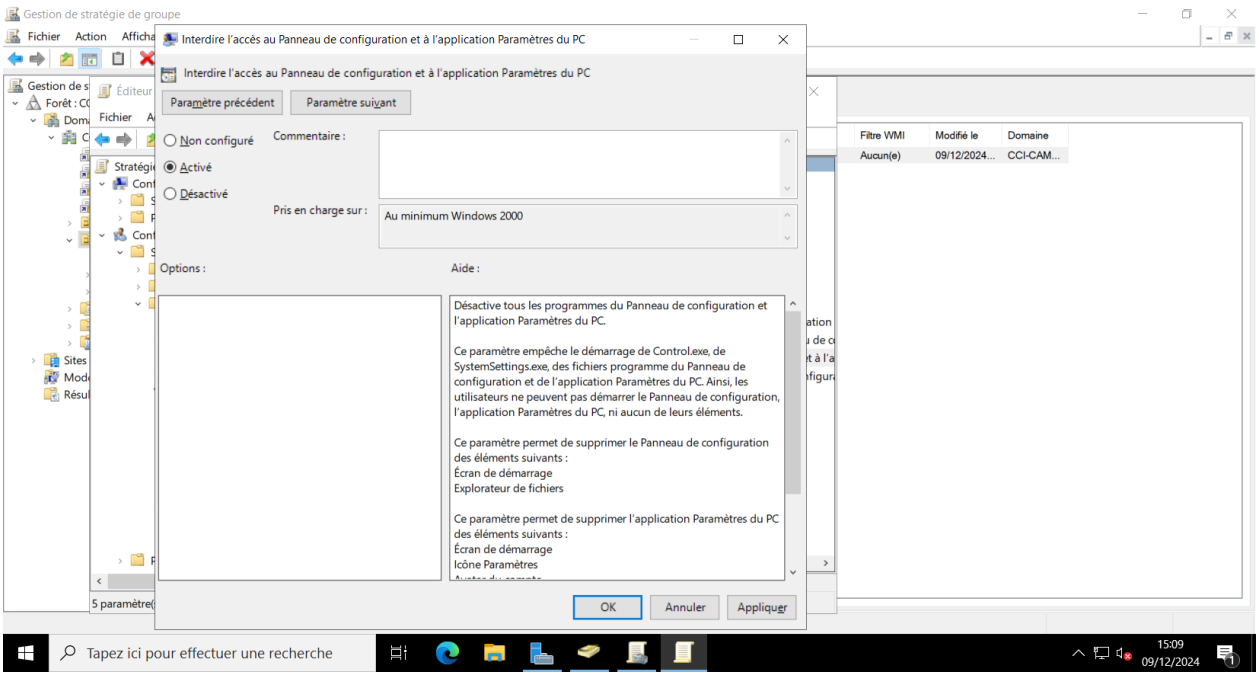


Interdire l'accès aux paramètres

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

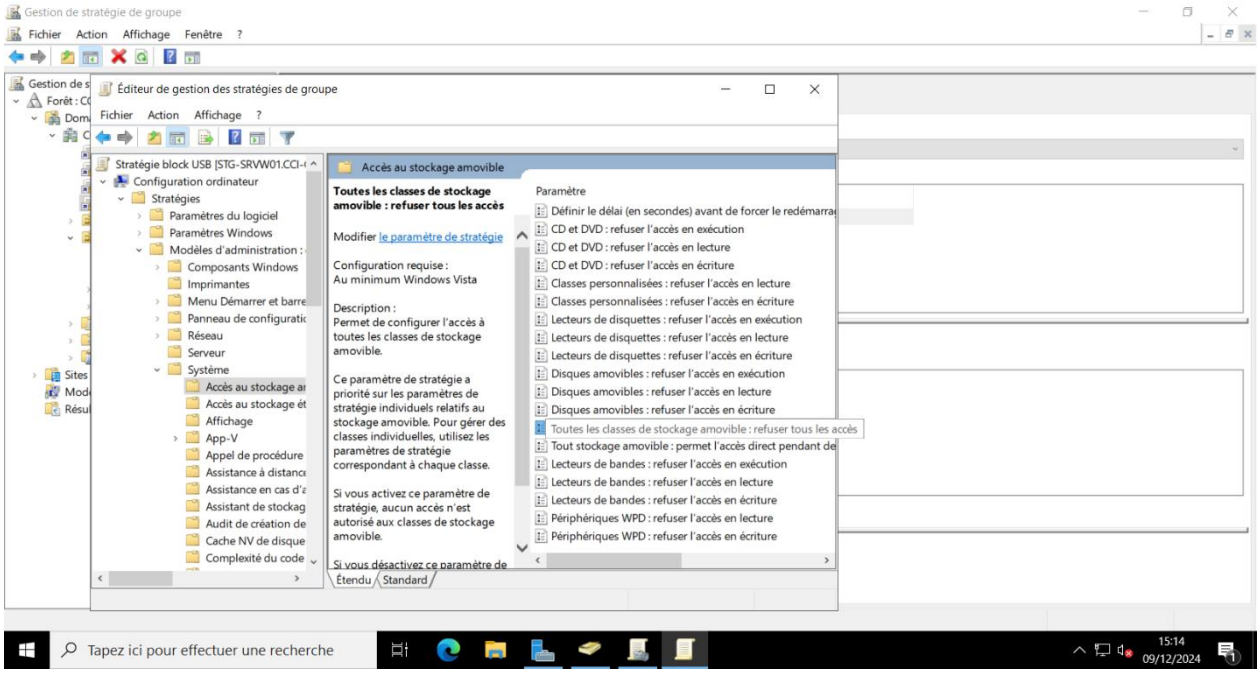


- Activer la GPO

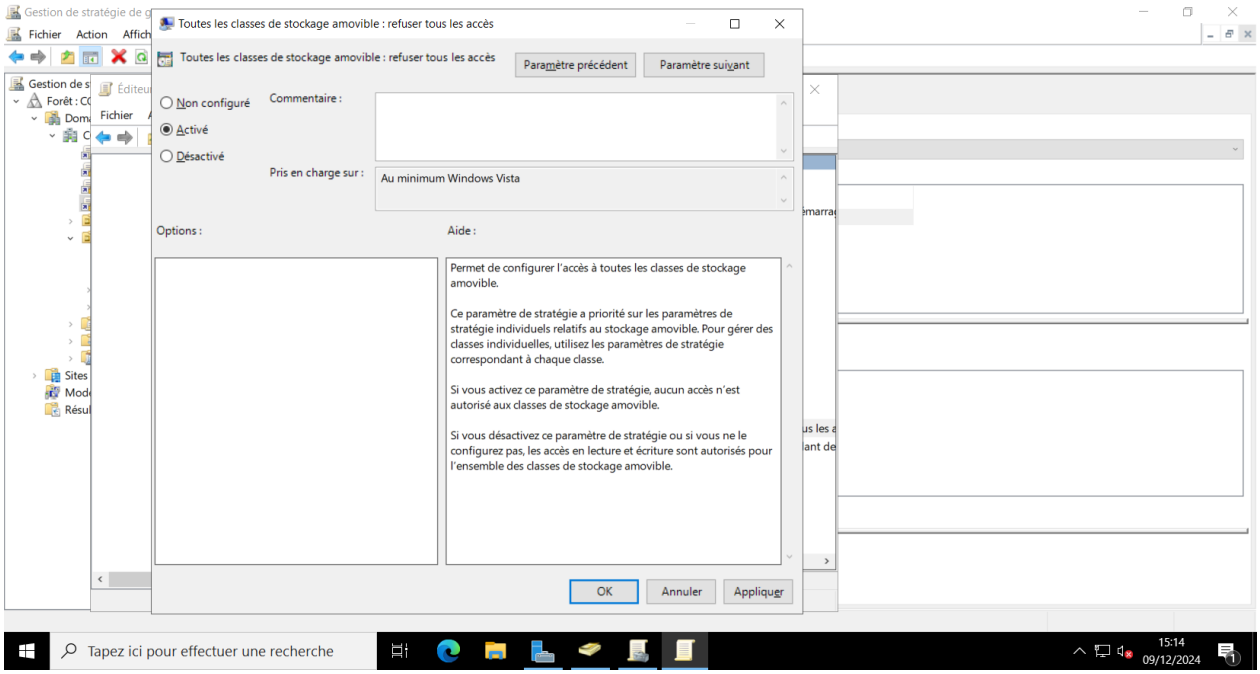


Bloquer les ports USB

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

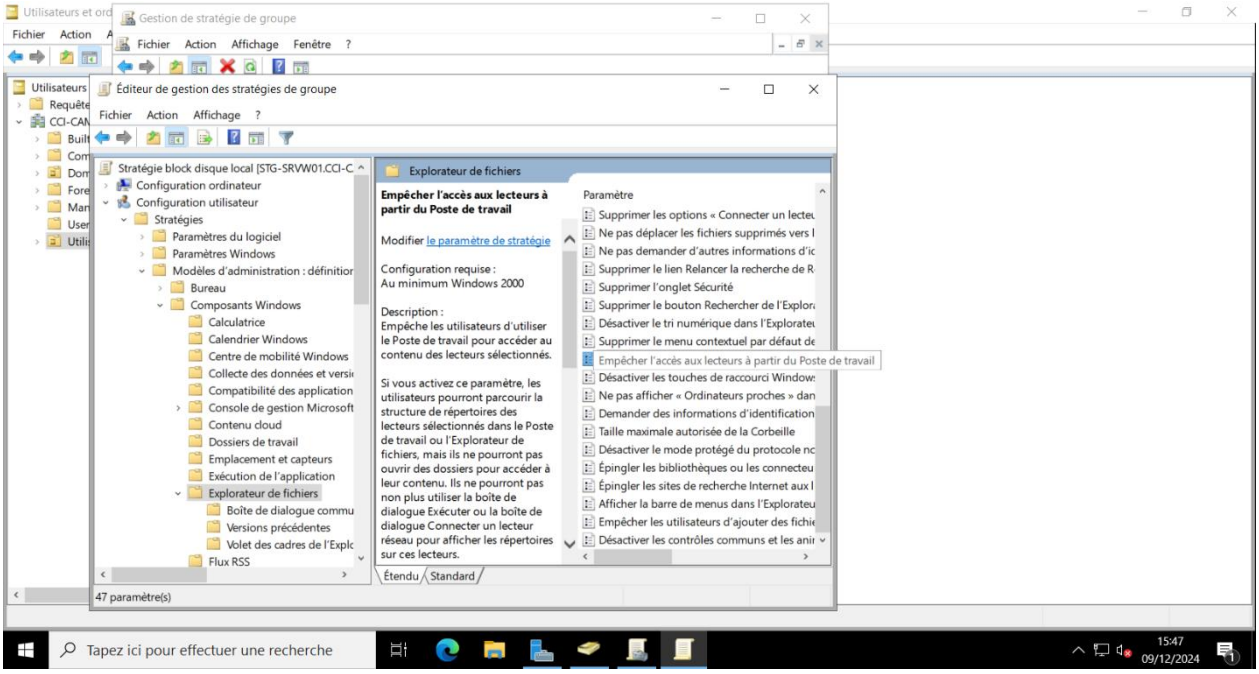


- Activer la GPO

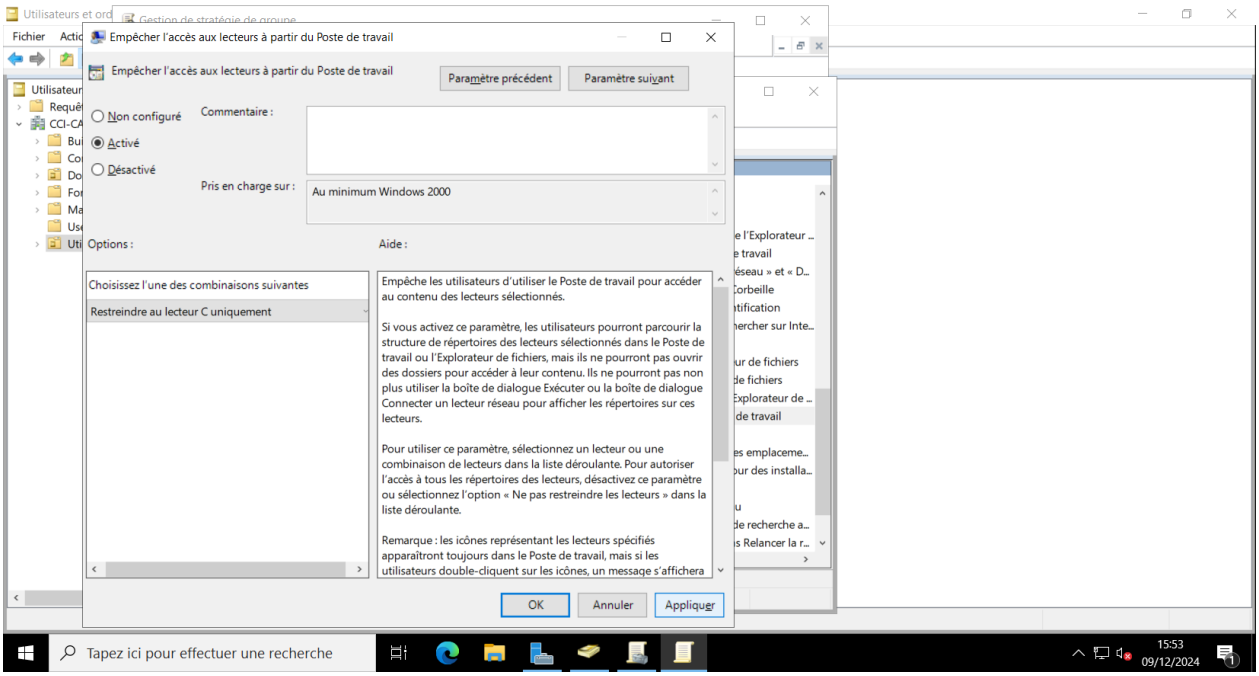


Masquer et bloquer le disque C

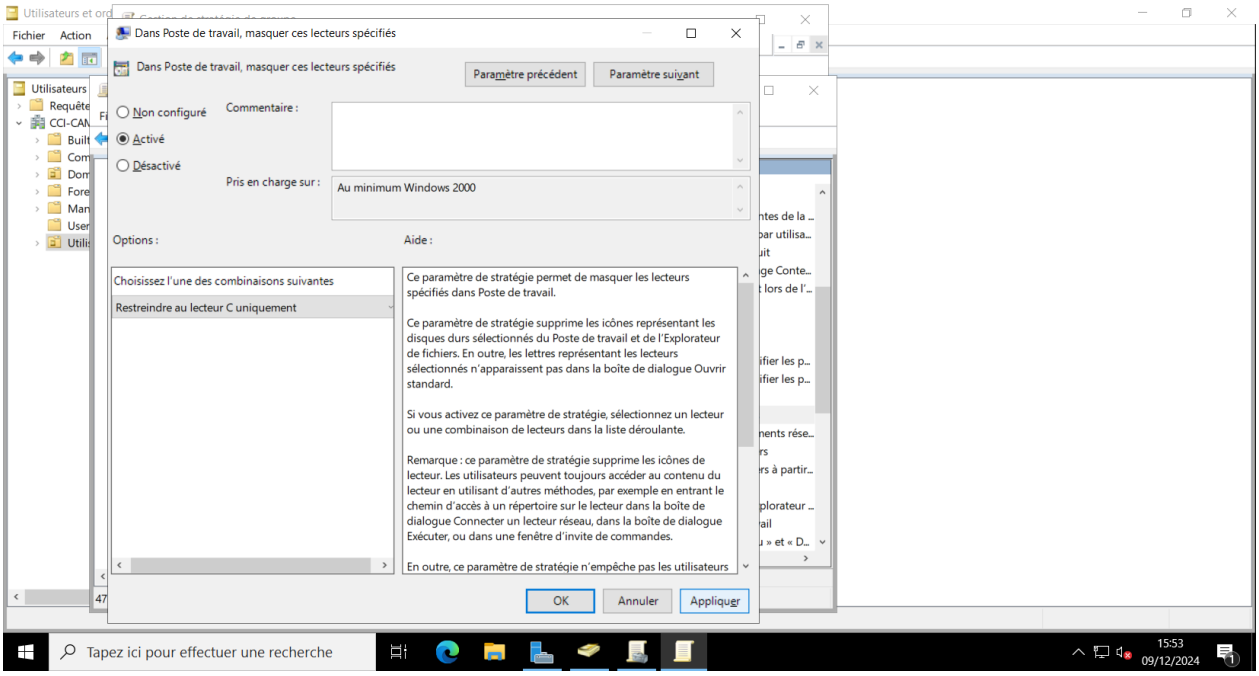
- Pour masquer le disque C, se rendre dans **Configuration utilisateur -> Stratégies -> Modèles d'administration -> Composant Windows -> Explorateur de fichiers**.



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

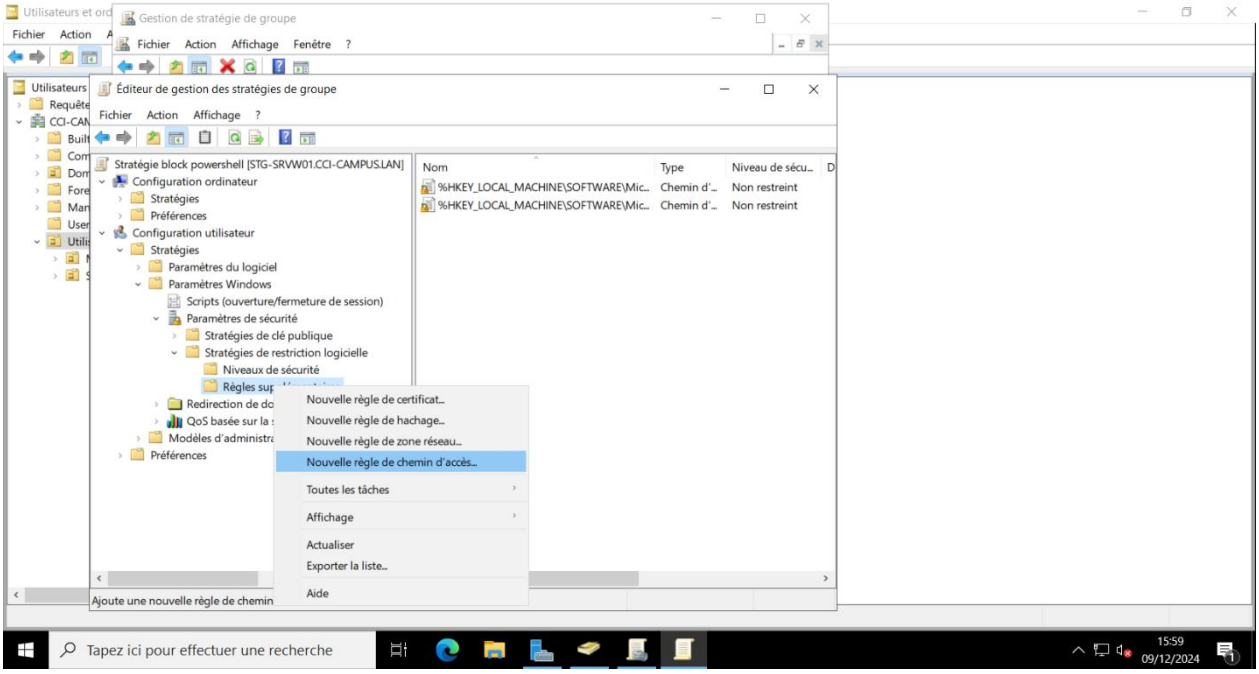


- Faire de même pour masquer le lecteur C

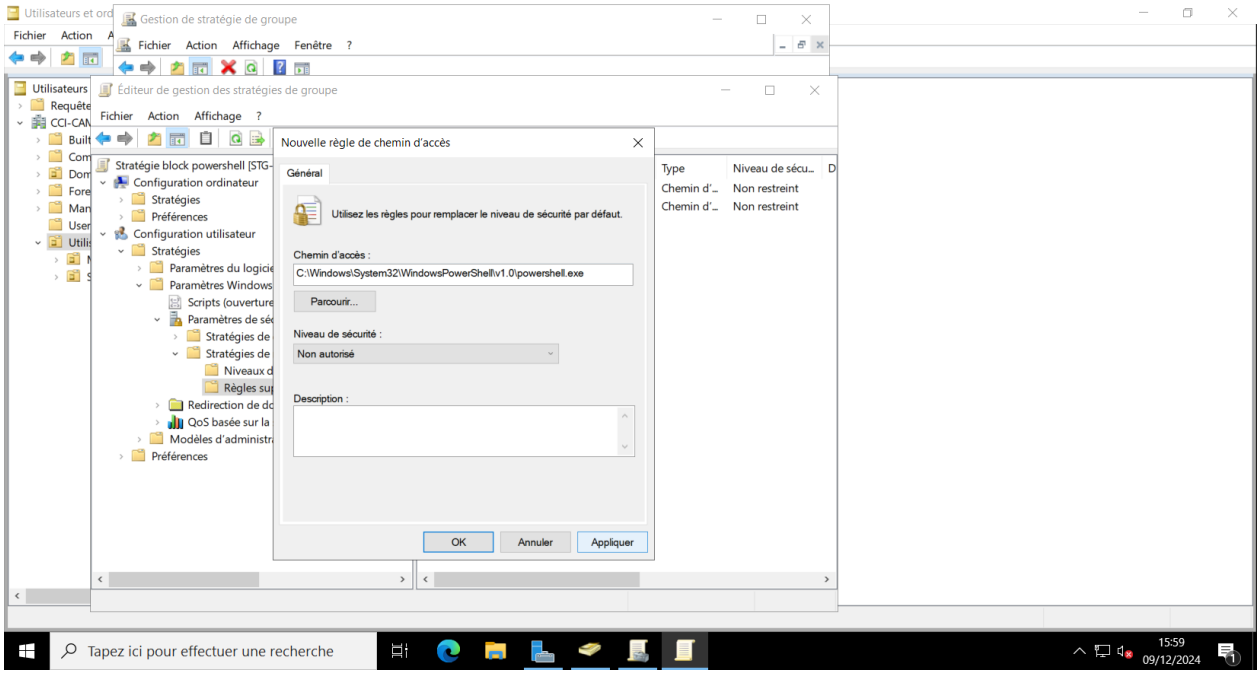


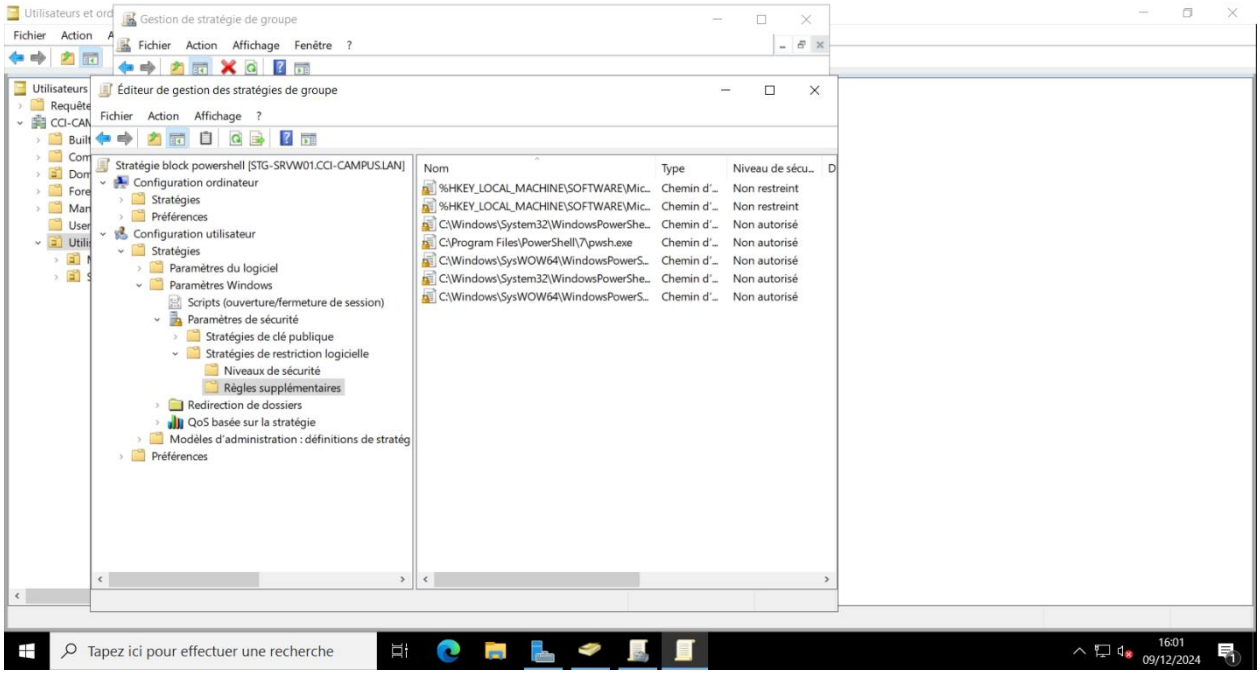
Bloquer l'accès aux consoles Powershell et Invité de commande

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

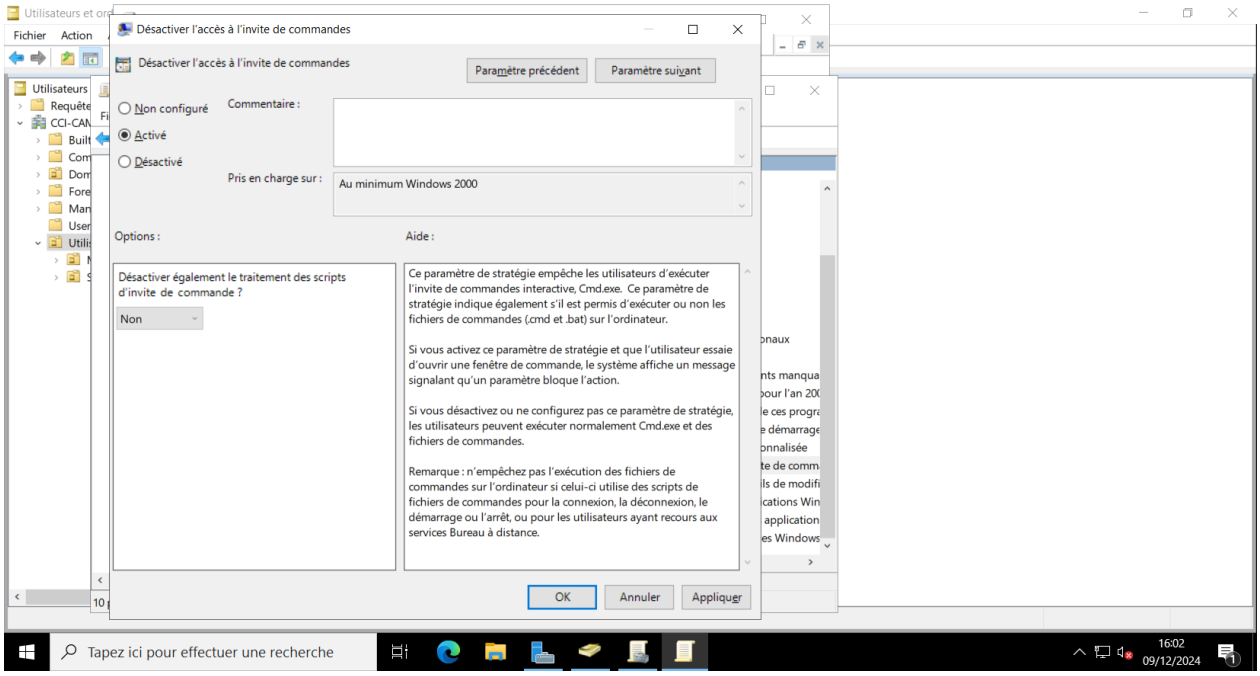


- Créer ensuite une nouvelle règle en bloquant les chemins d'accès de powershell



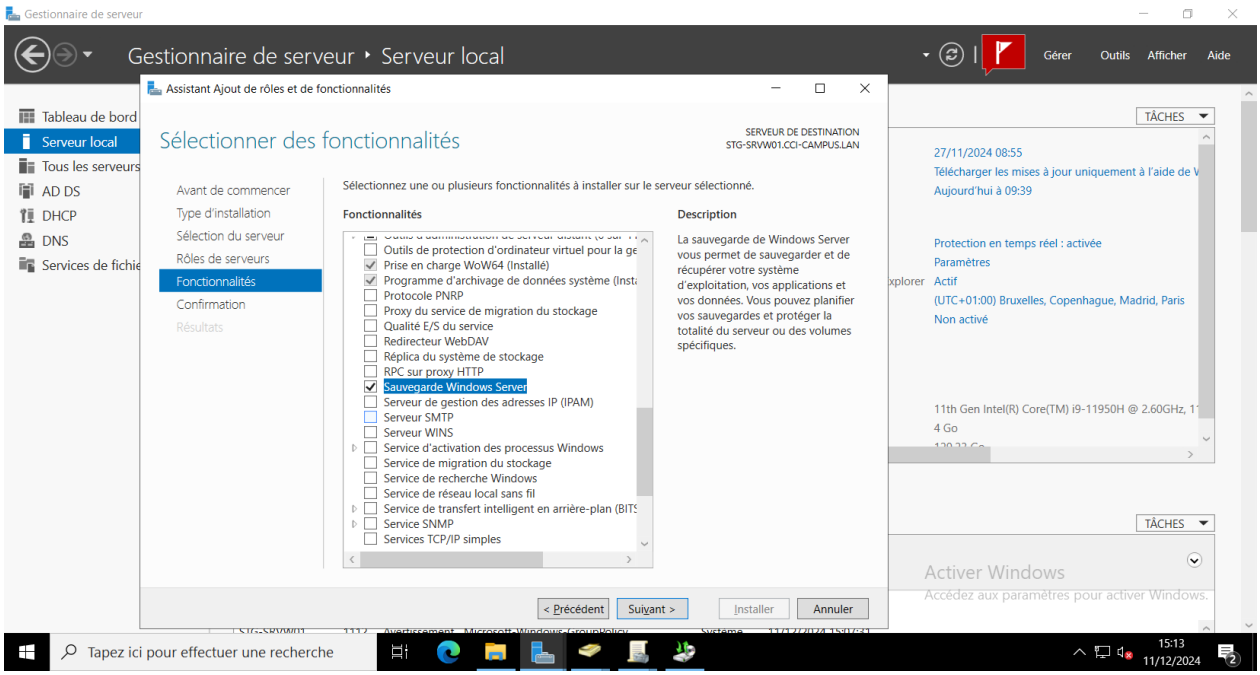


- Activé la GPO bloquant l'accès à l'invite de commande

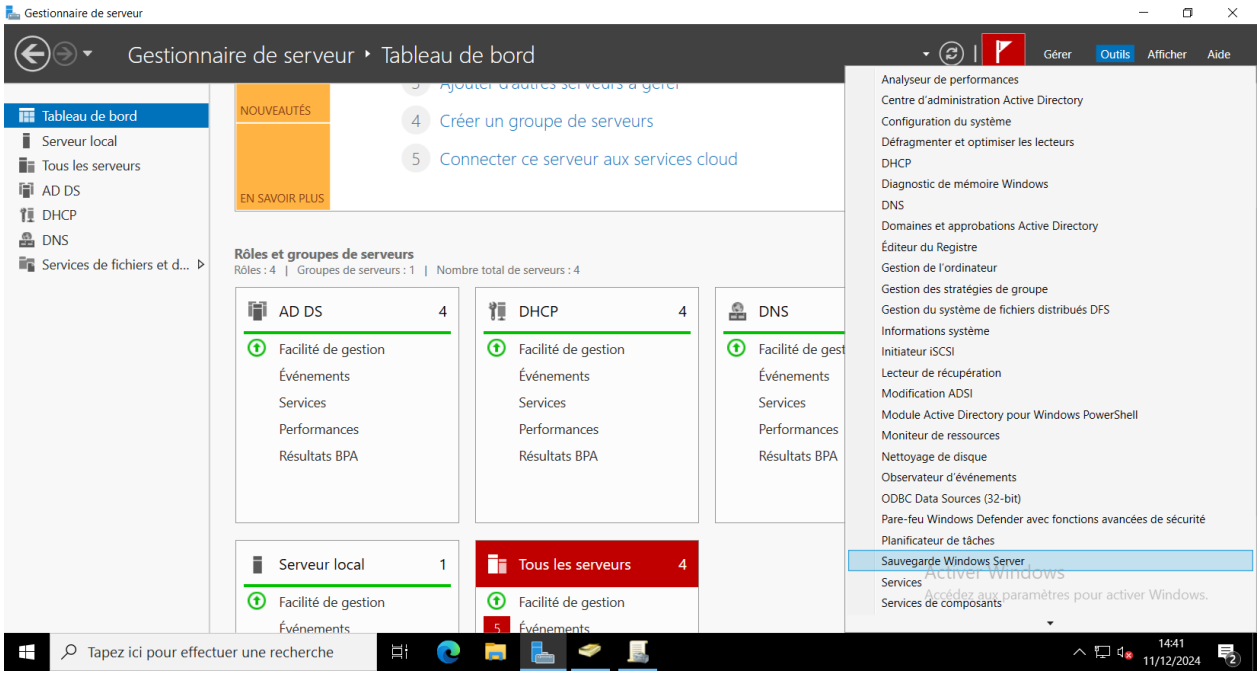


Mise en place de la sauvegarde Windows serveur

- Installer le rôle

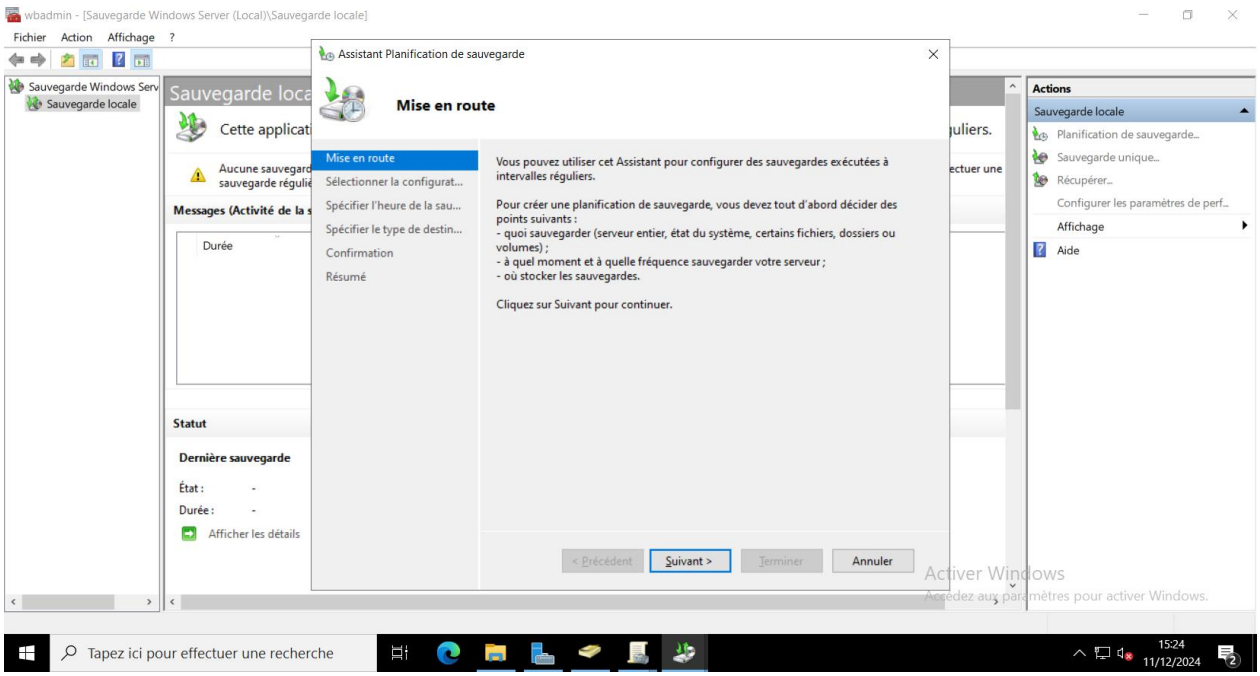


- Ensuite se rendre dans le gestionnaire de sauvegarde

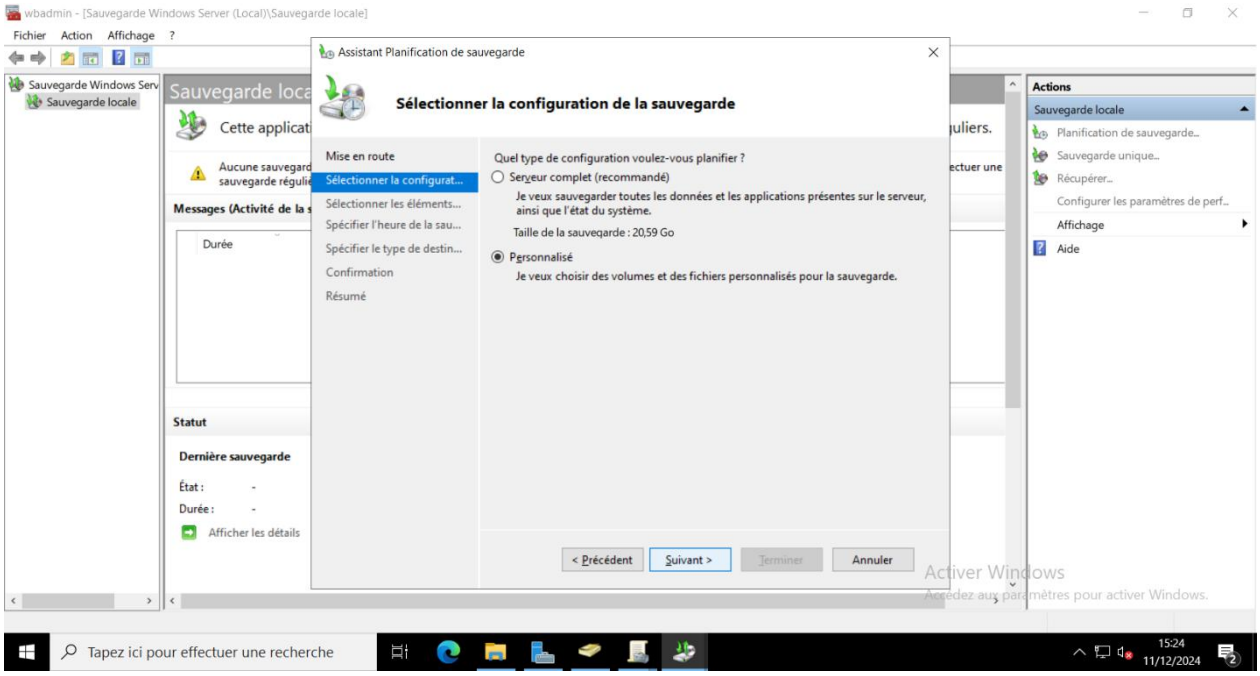


&é

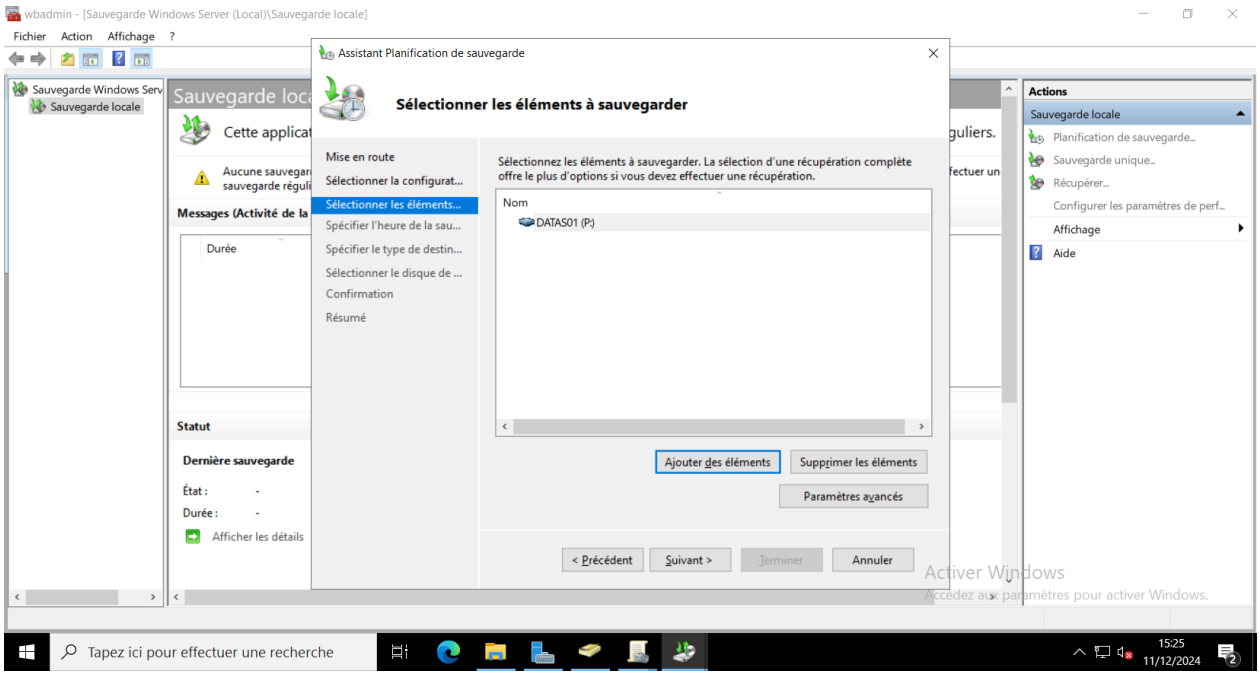
- Créer une nouvelle planification de sauvegarde



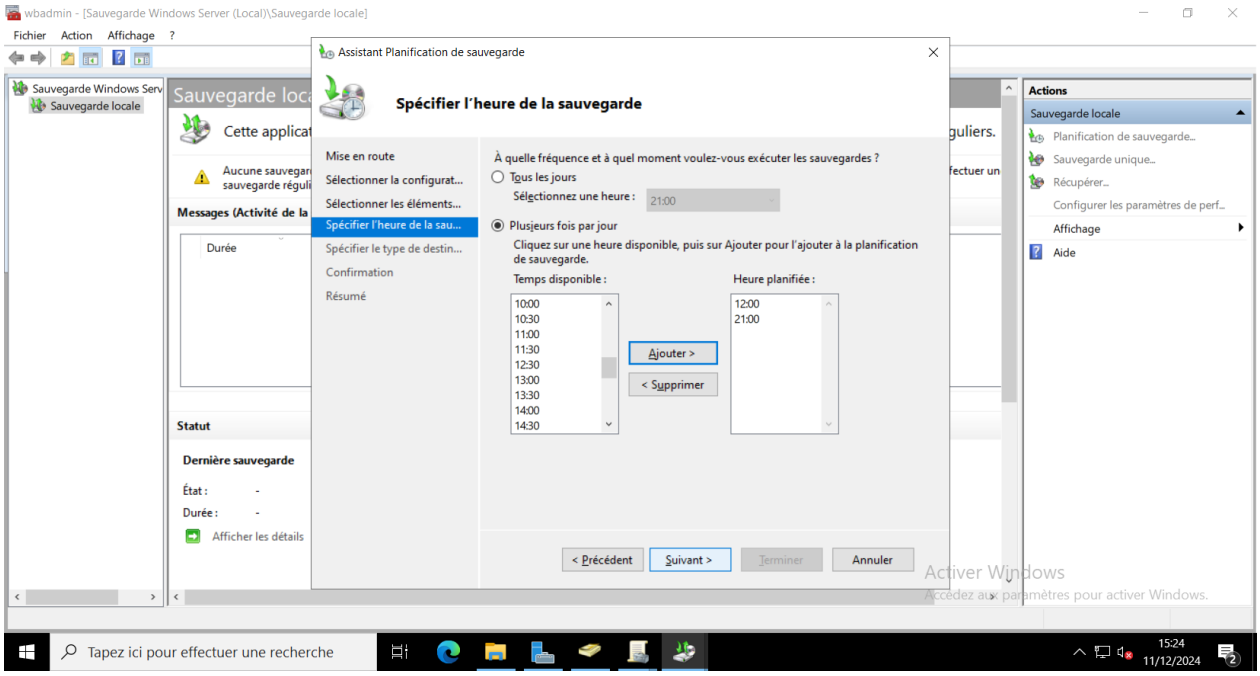
- Sélectionner une configuration personnalisée



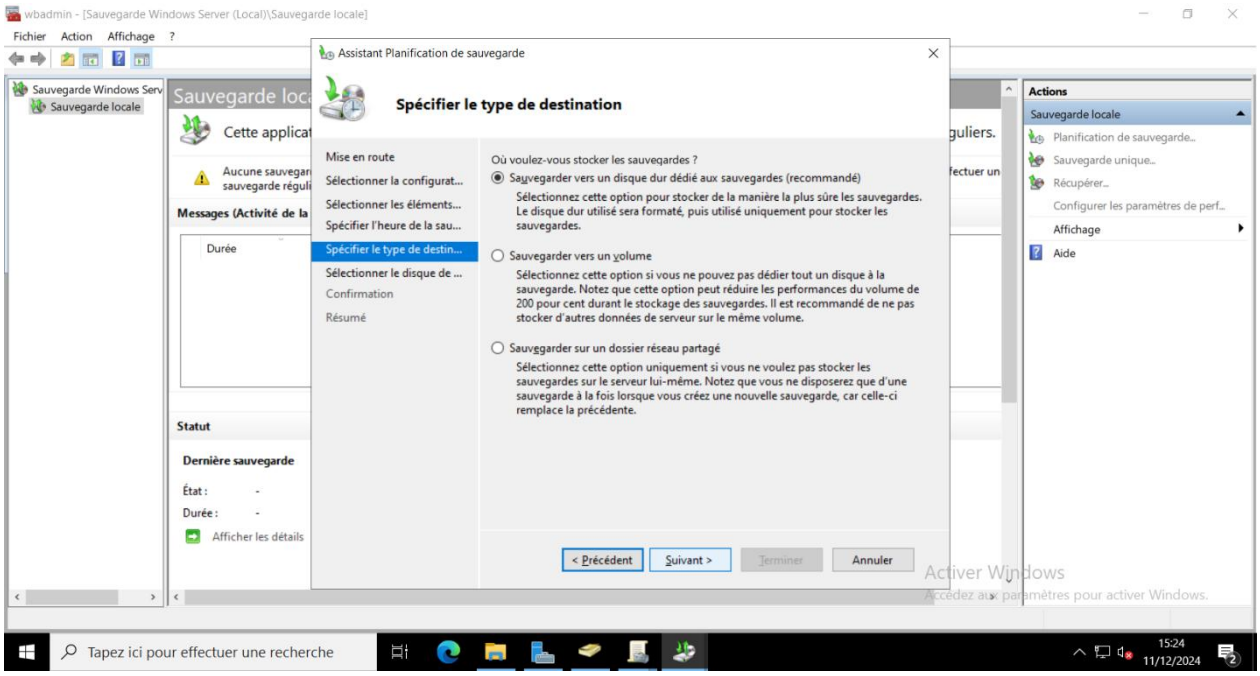
- Sélectionner le disque à sauvegarder



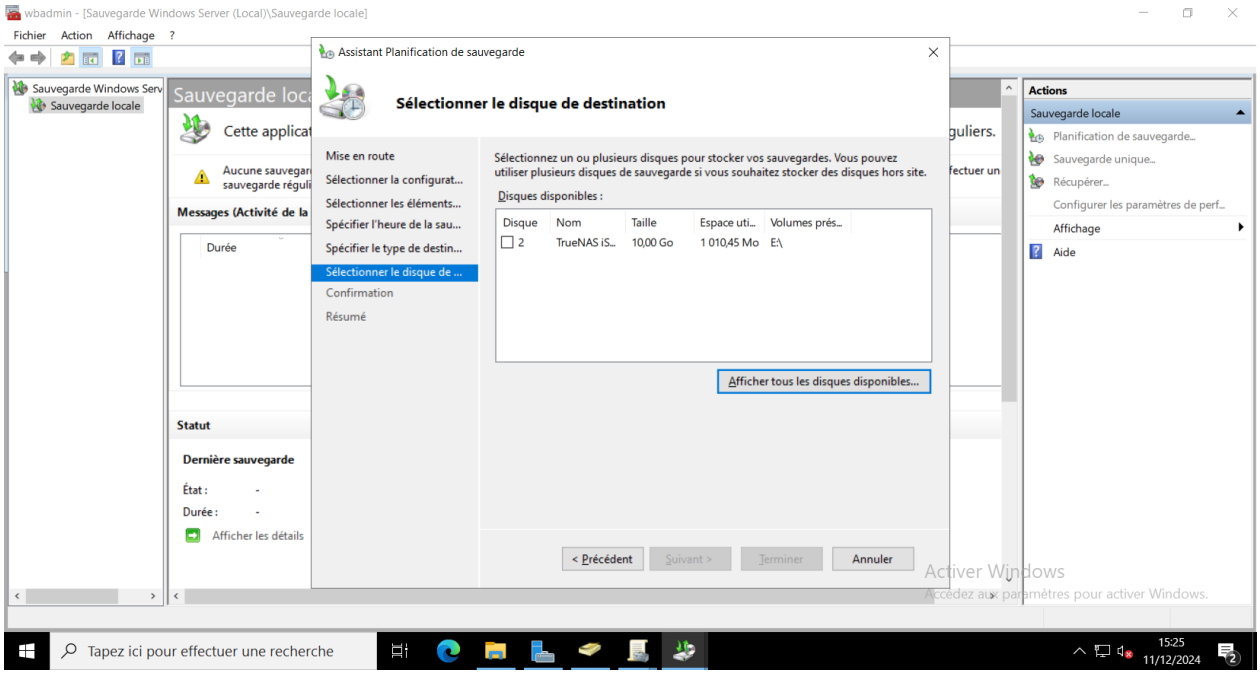
- Ajouter une sauvegarde à une heure régulière



- Sauvegarder vers un disque dur dédier aux sauvegardes



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



- Confirmer le tout et la sauvegarde est maintenant effective