Présentation du projet

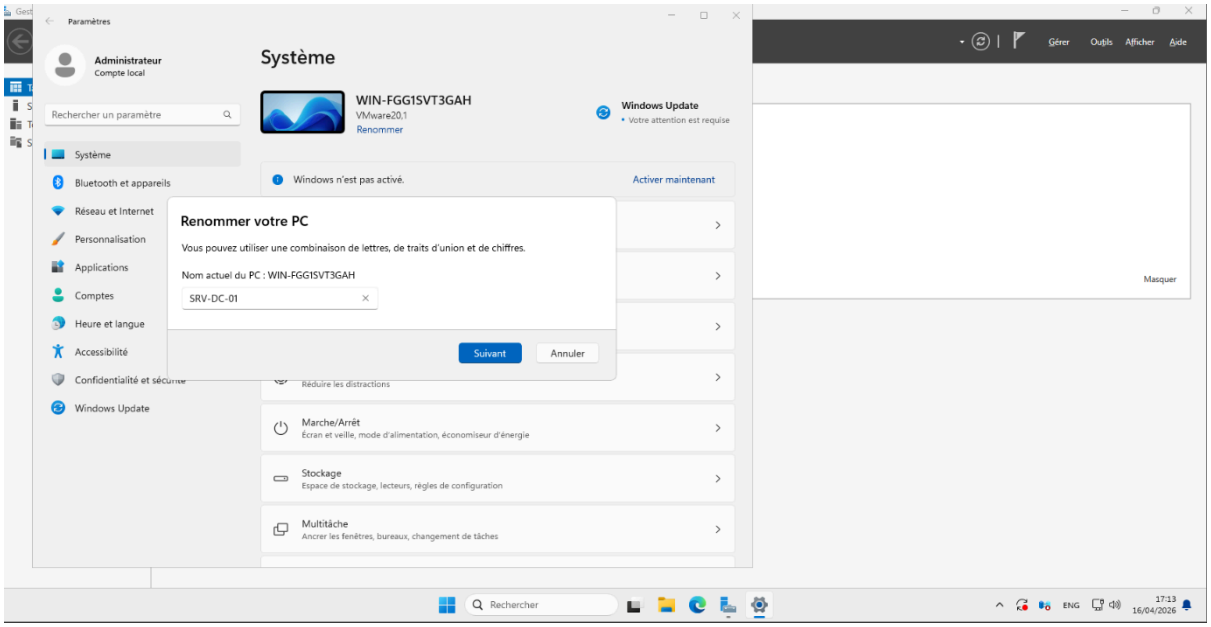
Ce projet consiste à concevoir et à déployer une infrastructure réseau complète et sécurisée pour l'entreprise SeZoRo, basée sur l'écosystème Windows Server 2025. L'objectif principal est de centraliser la gestion des ressources, d'assurer la haute disponibilité des services critiques et d'offrir une flexibilité de travail aux collaborateurs.

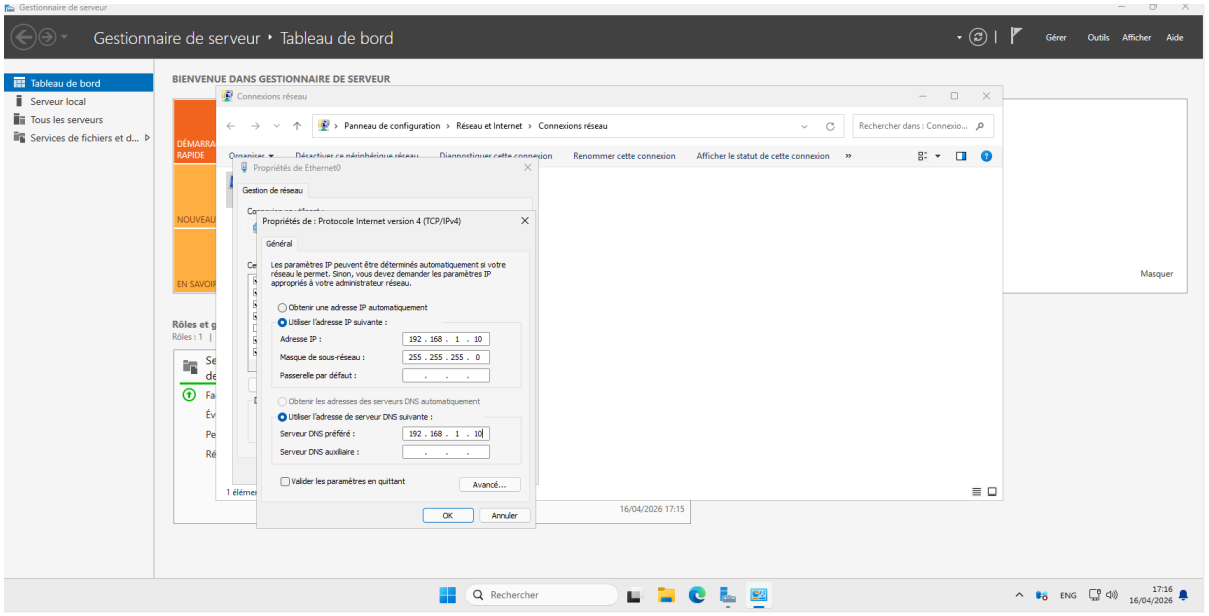
Réalisations Techniques

L'infrastructure repose sur les piliers technologiques suivants :

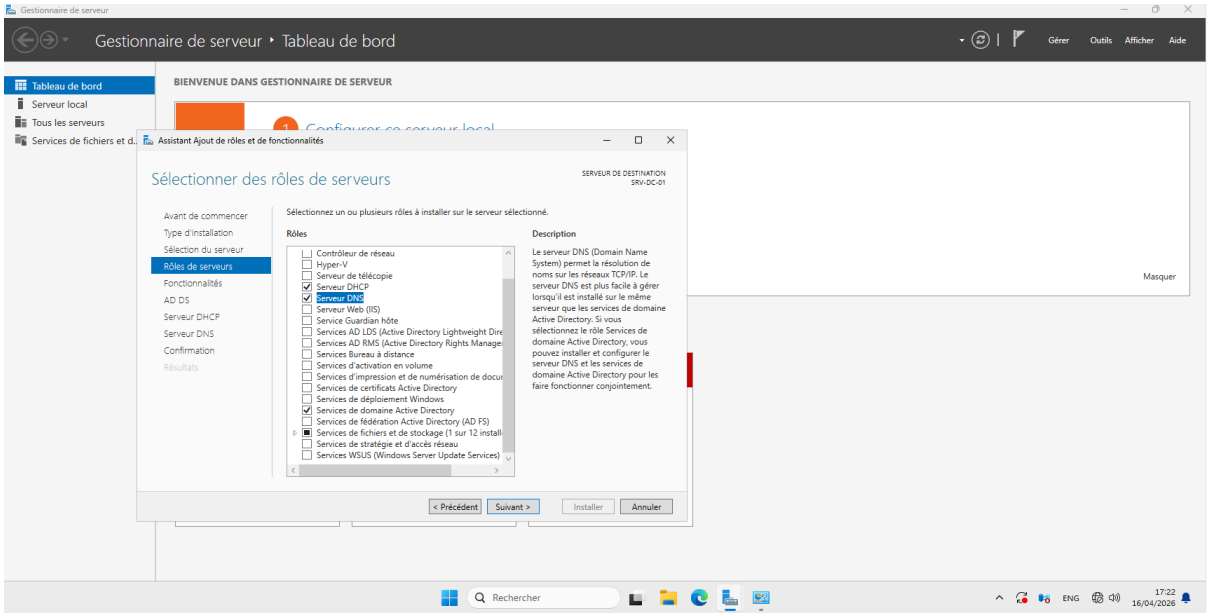
- **Gestion Centralisée (AD DS & DNS) :** Mise en place du domaine **sezoro.local** pour centraliser l'annuaire des utilisateurs et la gestion des machines.
- **Automatisation Réseau (DHCP) :** Distribution dynamique des adresses IP pour simplifier la connectivité des postes clients.
- **Continuité de Service (Haute Disponibilité Web) :** Déploiement de deux serveurs Web (**IIS-1 & IIS-2**) avec un mécanisme de **DNS Round Robin** pour garantir que l'Intranet reste accessible en cas de défaillance d'un serveur.
- **Sécurité et Conformité (GPO) :** Application de politiques de groupe strictes (blocage USB, CMD, Panneau de configuration) et personnalisation de l'environnement de travail (Wallpaper, Mappage lecteur réseau H:).
- **Mobilité et Virtualisation (RDS) :** Mise en œuvre des services de bureau à distance pour permettre un accès sécurisé aux outils de travail depuis n'importe quel emplacement.

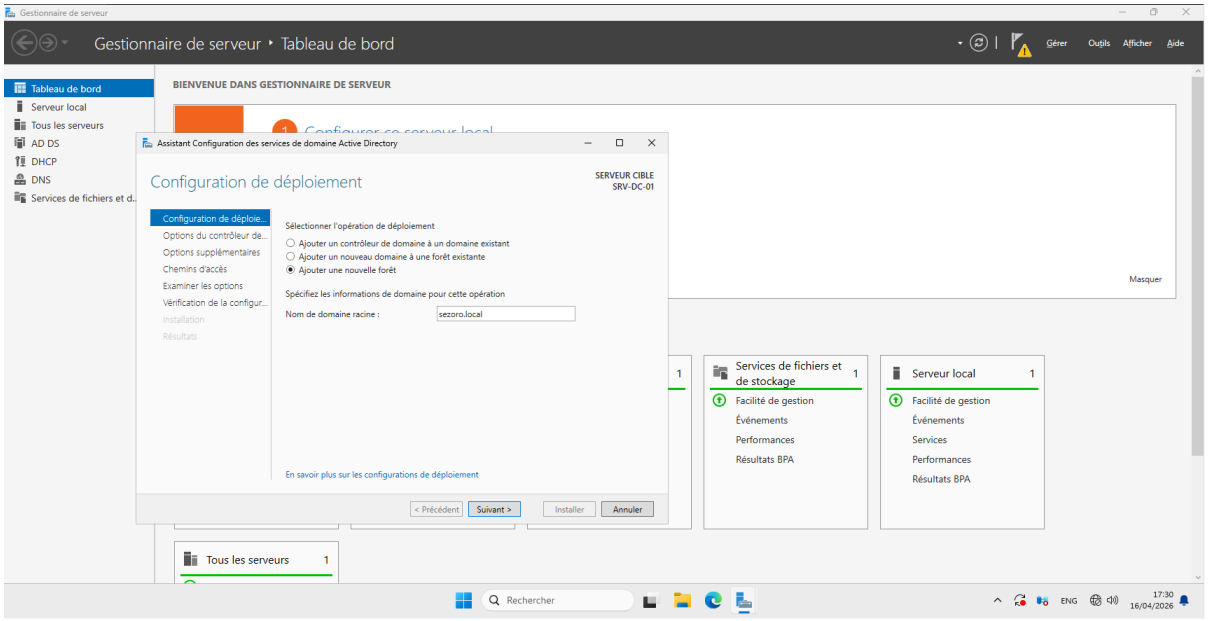
<u>Préparation du système et nommage du serveur</u> : Avant d'installer les rôles, nous commençons par renommer le serveur en **SRV-DC-01** et configurer une adresse IP statique pour assurer la stabilité des services réseau.

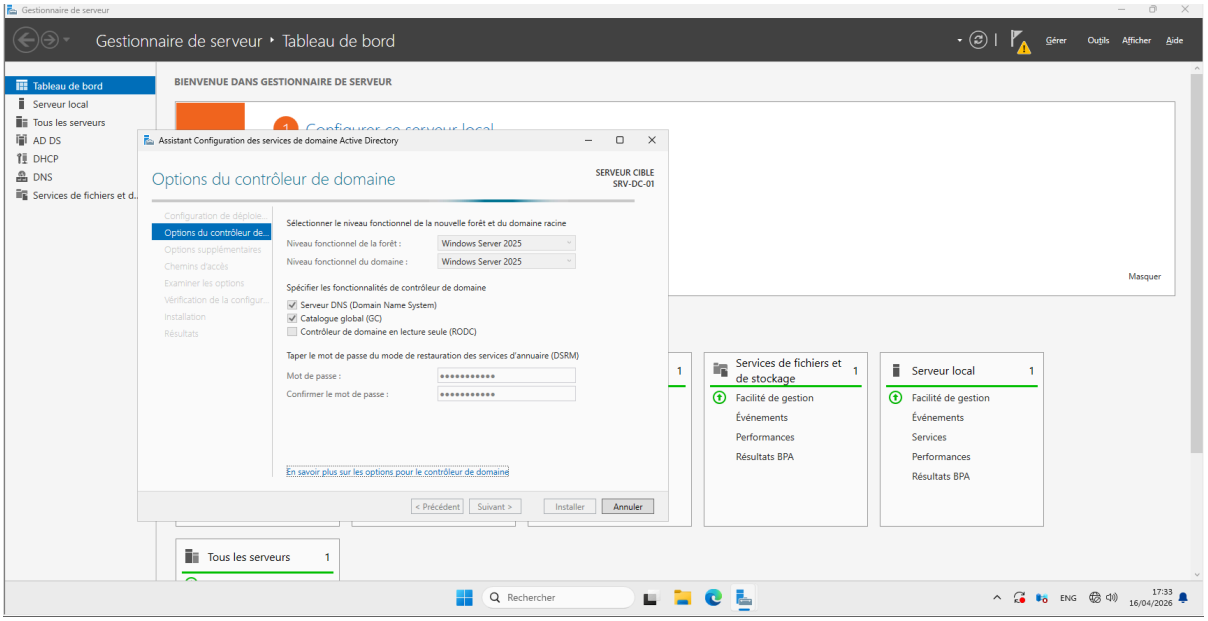




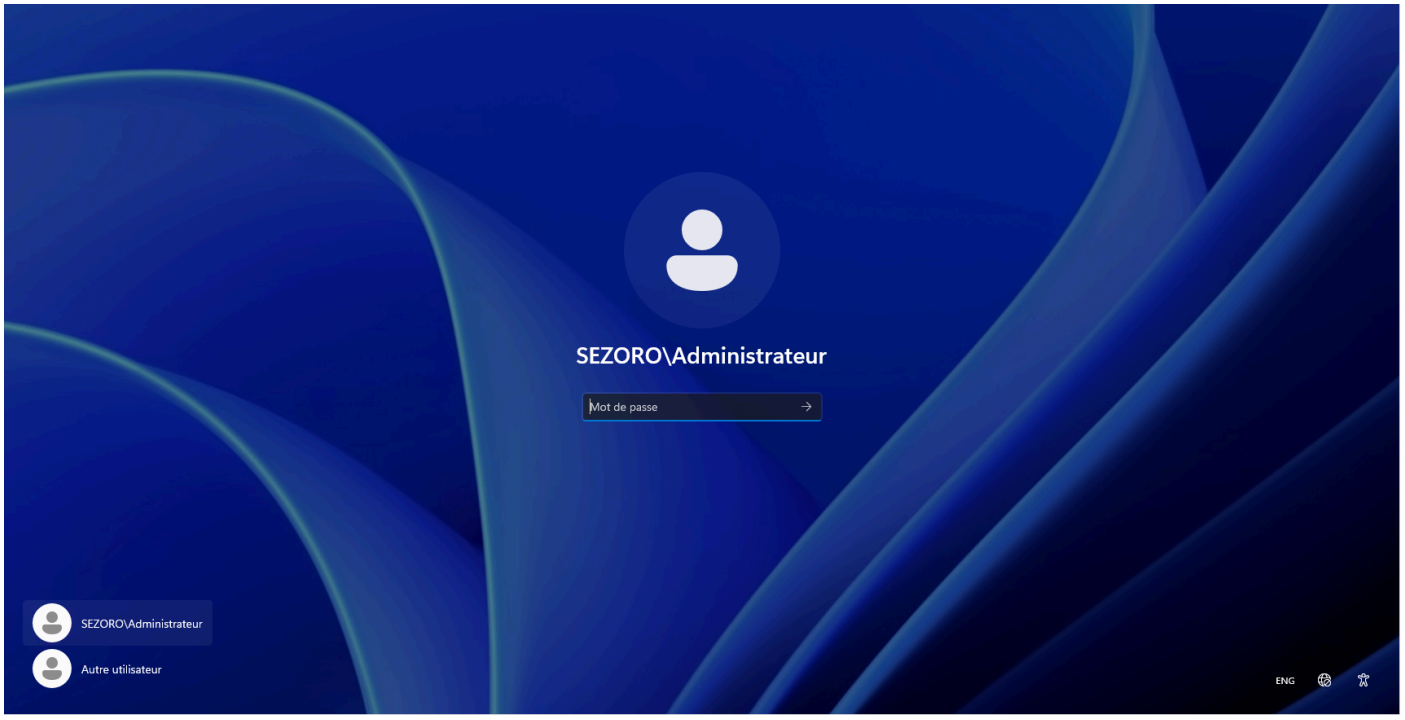
<u>Installation des services AD DS, DNS et DHCP</u> : Nous procédons à l'installation du rôle **Active Directory Domain Services** pour créer notre domaine **sezoro.local** et le rôle DHCP pour la distribution automatique des paramètres ip. Le service **DNS** est installé simultanément pour la résolution de noms.



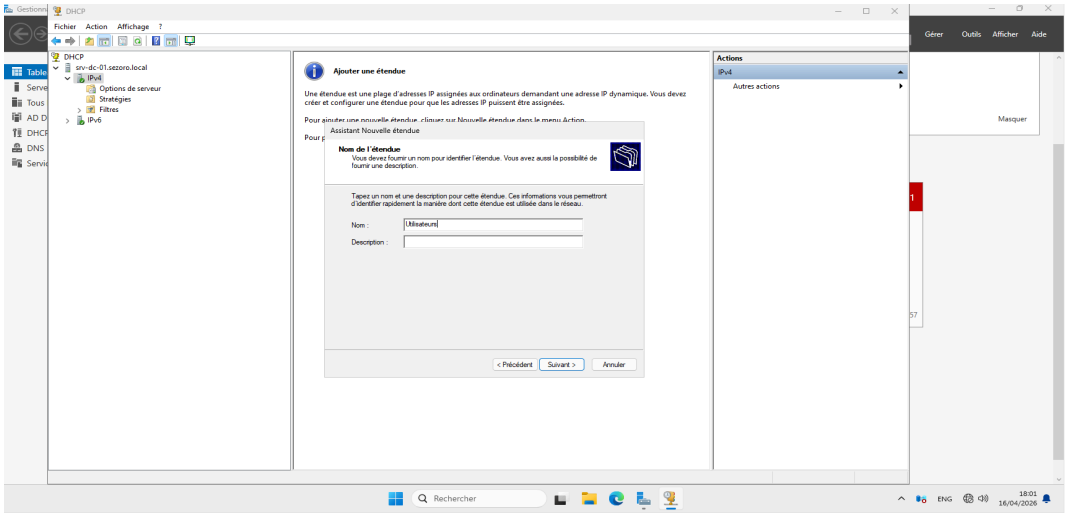


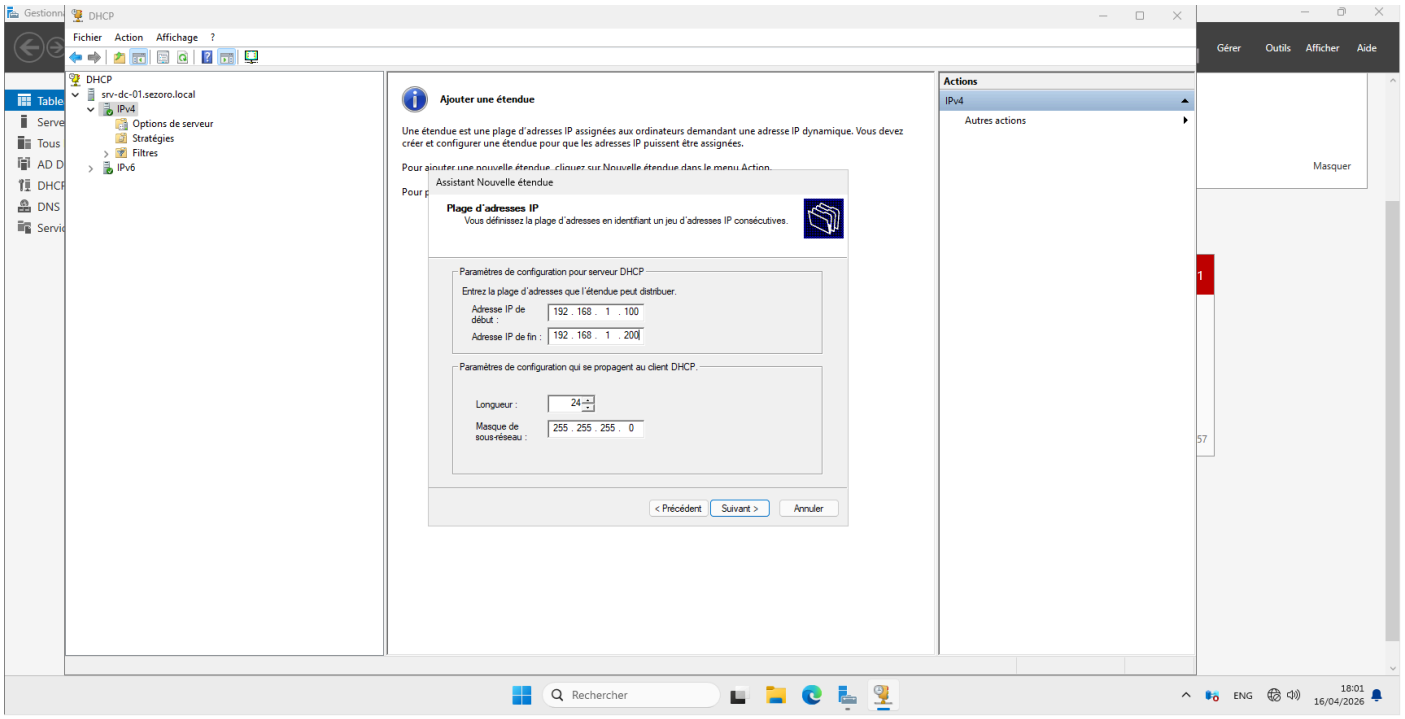


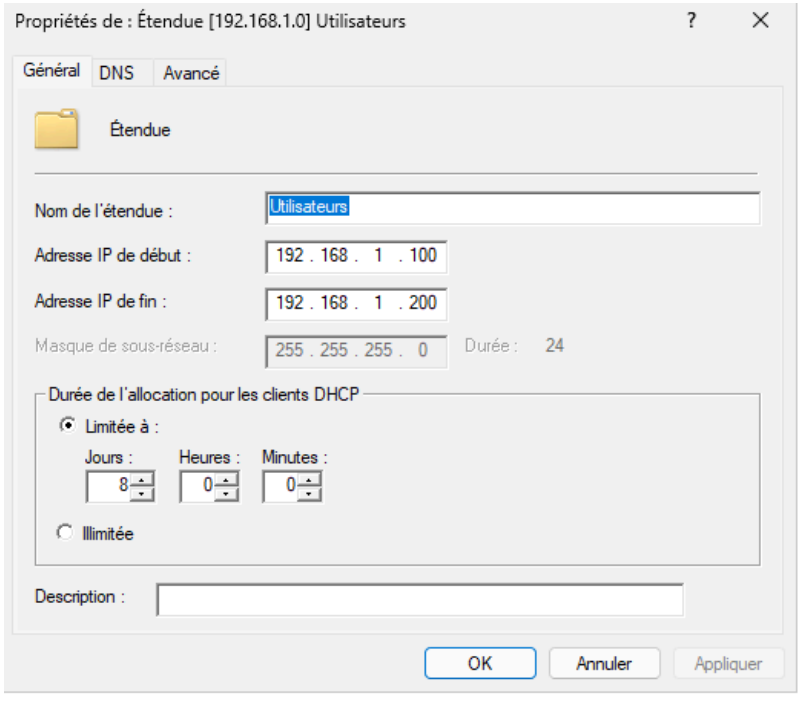
Mot de pass : Windows2025



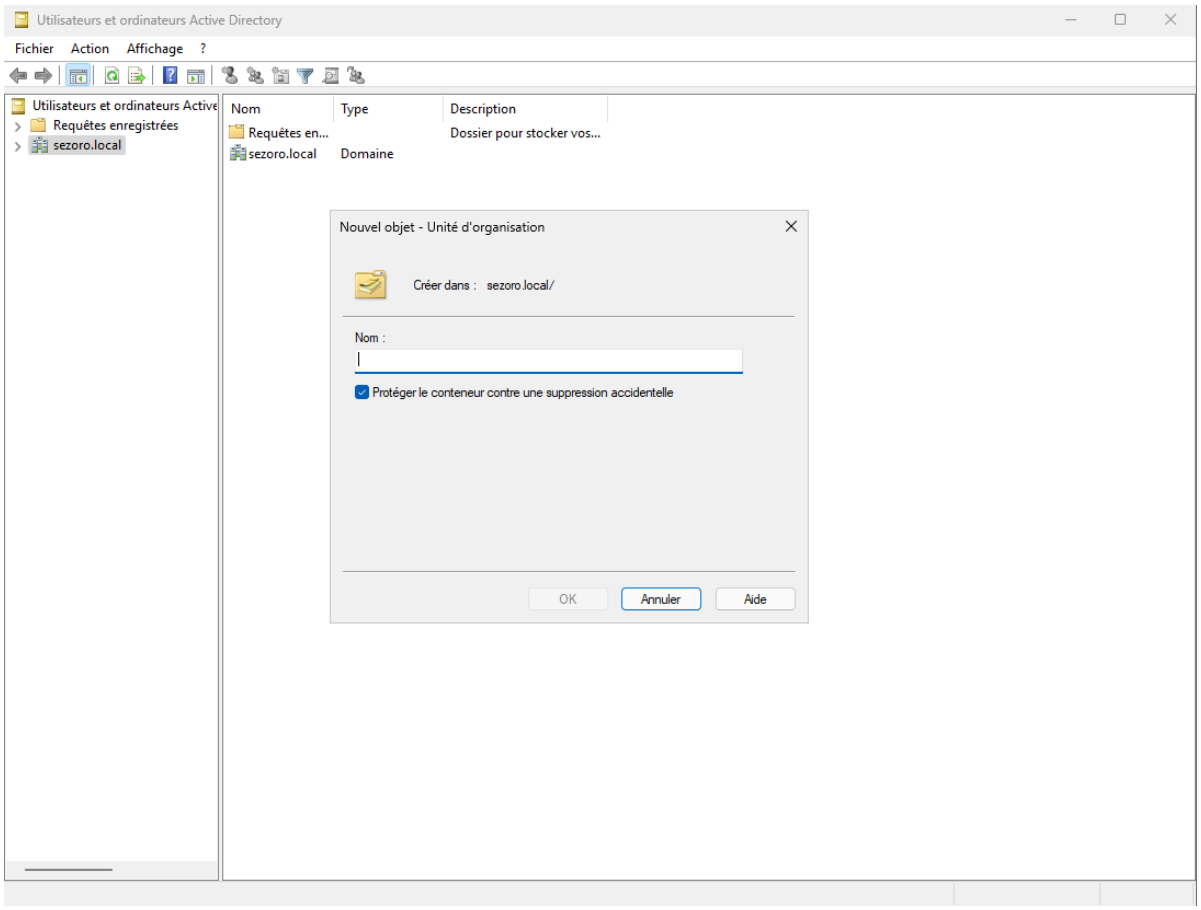
Configuration du serveur DHCP : Pour automatiser l'attribution des adresses IP aux clients, nous créons une étendue avec une plage allant de **192.168.1.100** à **192.168.1.200**.

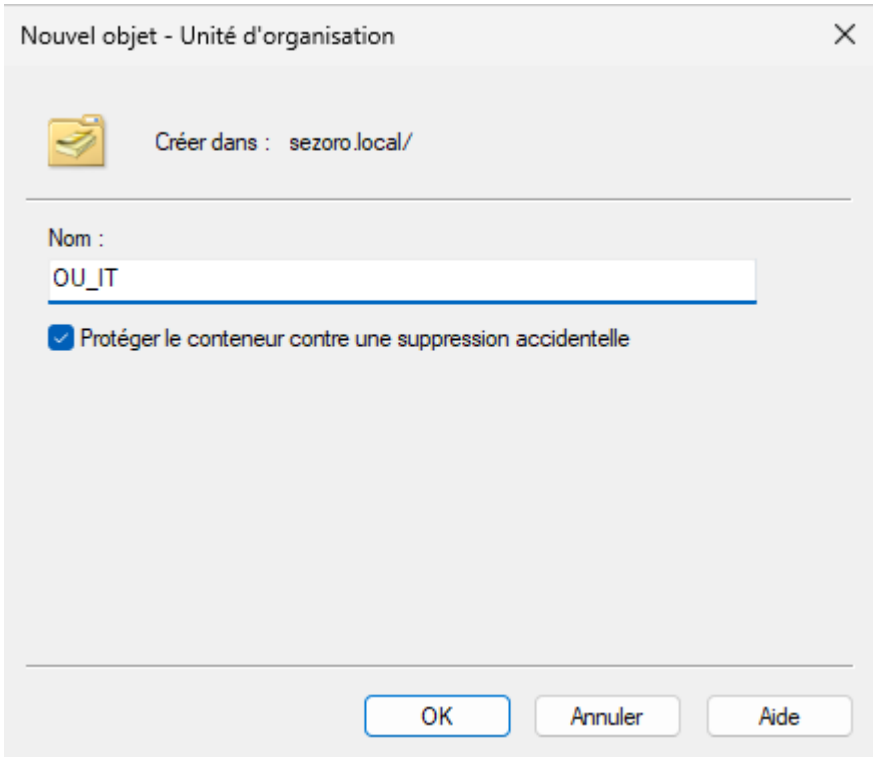

DHCP
Fichier Action Affichage ?
srv-dc-01.sezoro.local
IPv4
Options de serveur
Stratégies
Filtres
IPv6
Ajouter une étendue
Une étendue est une plage d'adresses IP assignées aux ordinateurs demandant une adresse IP dynamique. Vous devez créer et configurer une étendue pour que les adresses IP puissent être assignées.
Assistant Nouvelle étendue
Nom de l'étendue
Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.
Nom :
Utilisateurs
Description :
< Précédent
Suivant >
Annuler
Actions
IPv4
Autres actions
Gérer Outils Afficher Aide
Masquer

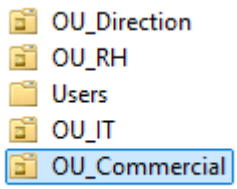

DHCP
Fichier Action Affichage ?
srv-dc-01.sezoro.local
IPv4
Options de serveur
Stratégies
Filtres
IPv6
Ajouter une étendue
Une étendue est une plage d'adresses IP assignées aux ordinateurs demandant une adresse IP dynamique. Vous devez créer et configurer une étendue pour que les adresses IP puissent être assignées.
Assistant Nouvelle étendue
Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.
Paramètres de configuration pour serveur DHCP
Entrez la plage d'adresses que l'étendue peut distribuer.
Adresse IP de début : 192 . 168 . 1 . 100
Adresse IP de fin : 192 . 168 . 1 . 200
Paramètres de configuration qui se propagent au client DHCP.
Longueur : 24
Masque de sous-réseau : 255 . 255 . 255 . 0
< Précédent
Suivant >
Annuler
Actions
IPv4
Autres actions
Gérer Outils Afficher Aide
Masquer
Rechercher
ENG
18:01
16/04/2026

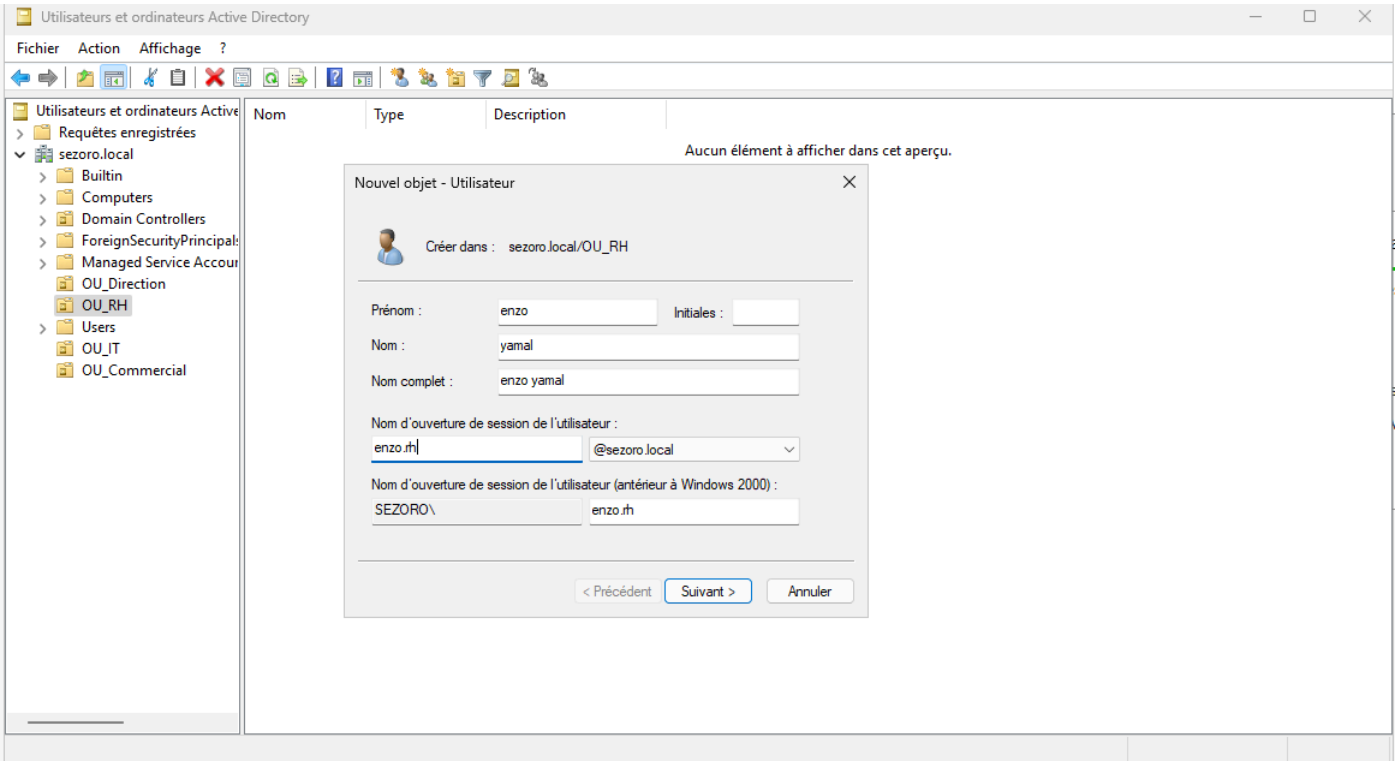

Propriétés de : Étendue [192.168.1.0] Utilisateurs
Général
DNS
Avancé
Étendue
Nom de l'étendue : Utilisateurs
Adresse IP de début : 192 . 168 . 1 . 100
Adresse IP de fin : 192 . 168 . 1 . 200
Masque de sous-réseau : 255 . 255 . 255 . 0
Durée : 24
Durée de l'allocation pour les clients DHCP
Limitée à :
Jours : 8
Heures : 0
Minutes : 0
Illimitée
Description :
OK
Annuler
Appliquer

<u>Création des Unités d'Organisation (OU) et des Utilisateurs</u> : Nous organisons l'annuaire en créant des **OU** (RH, IT, Direction,Commercial) et nous ajoutons les comptes utilisateurs, comme l'utilisateur **enzo.rh**, pour tester les accès.

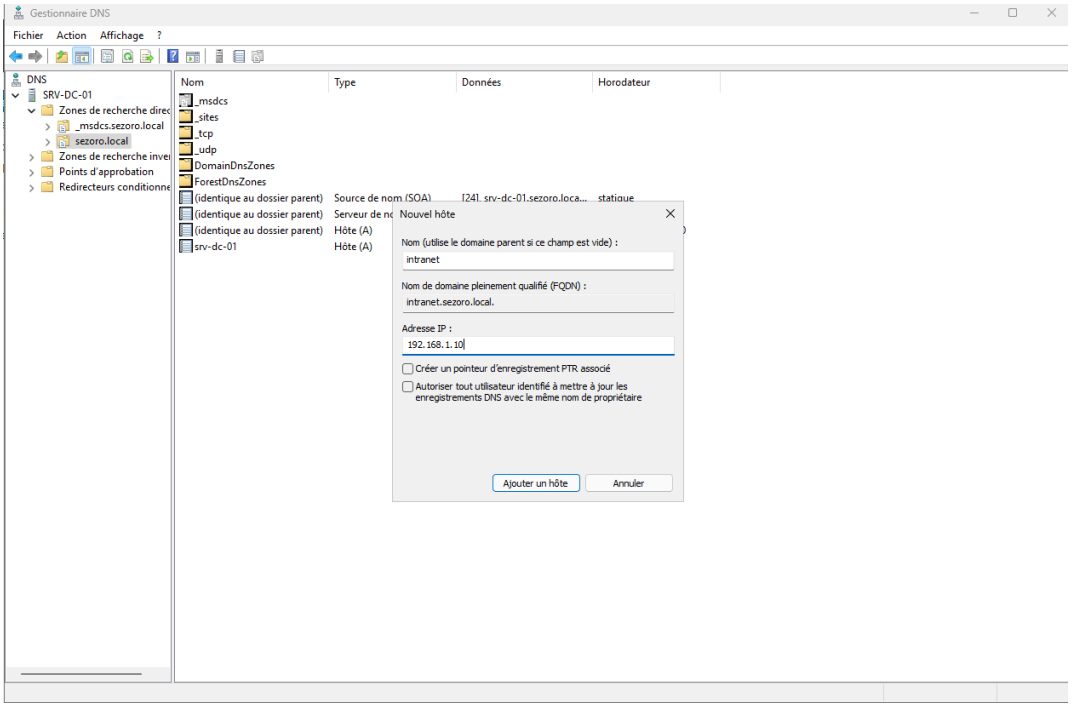




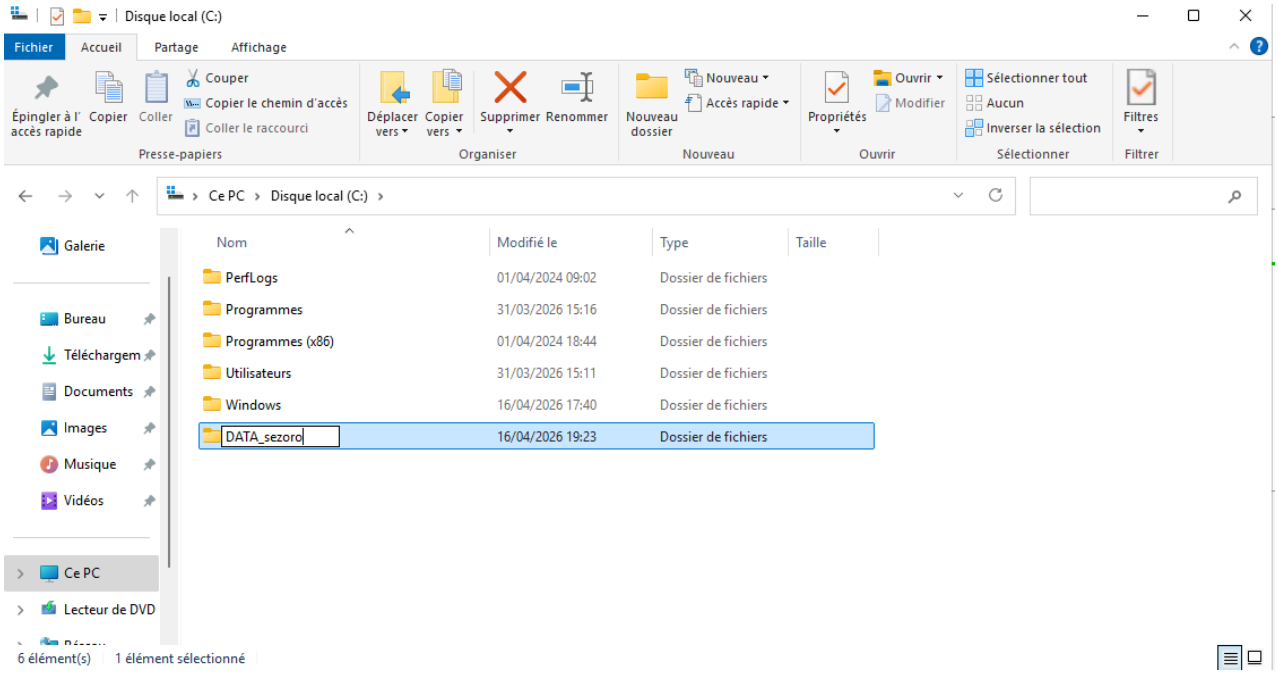


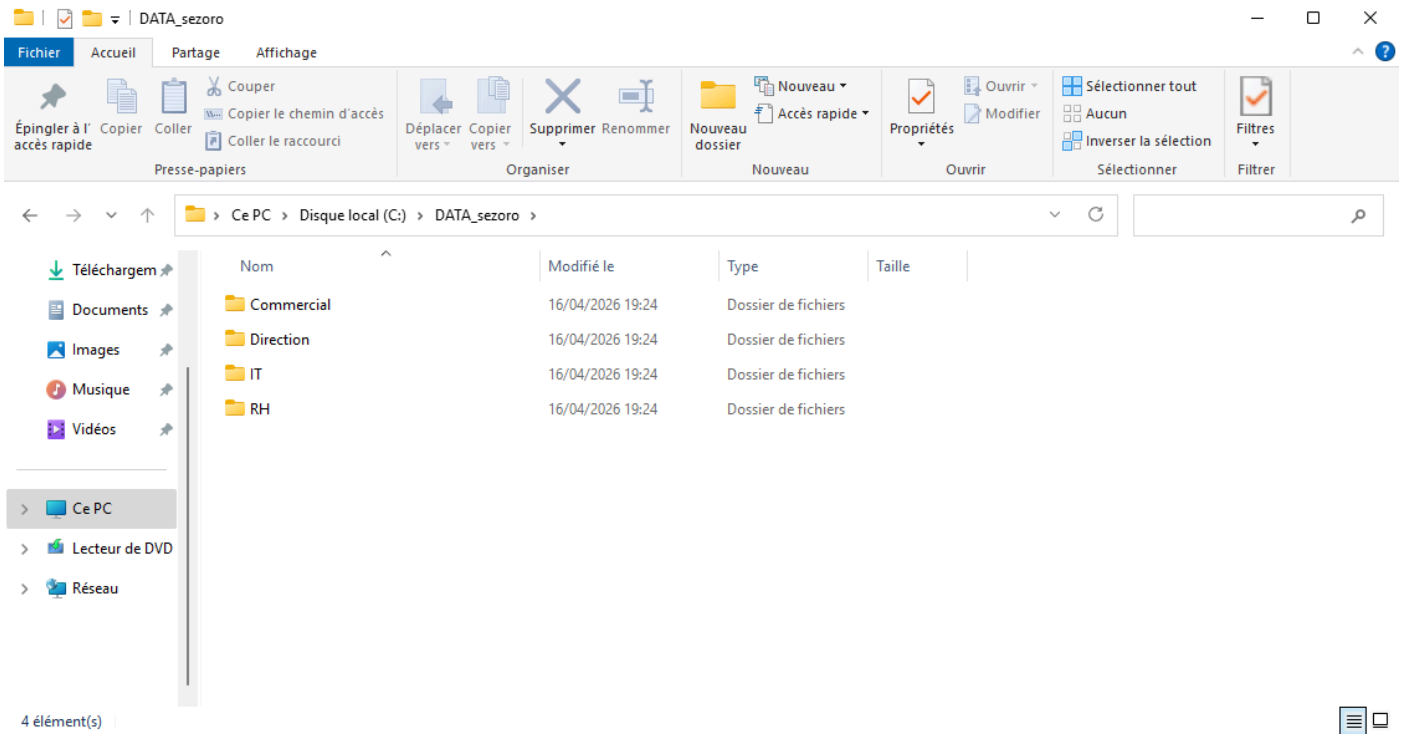


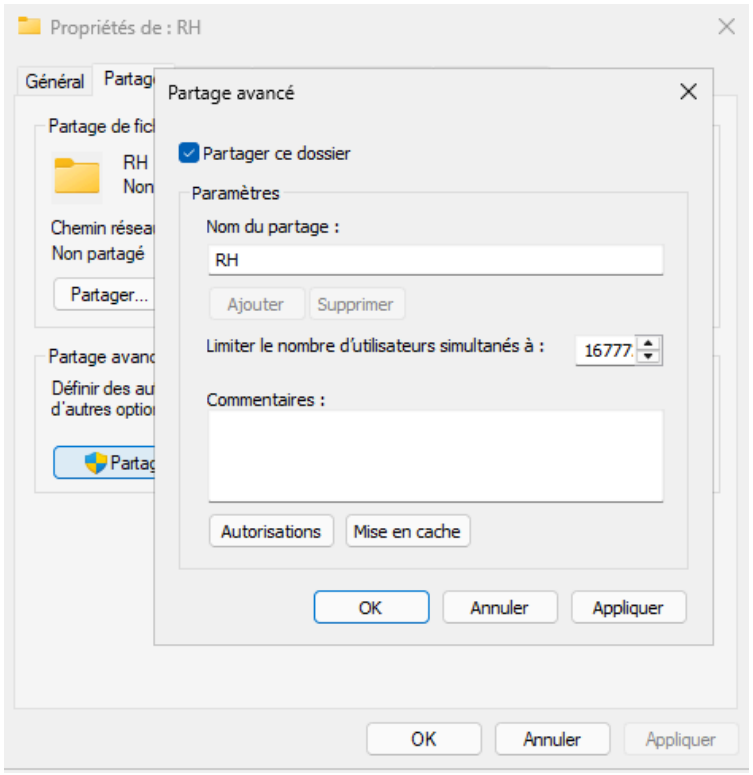
Pour que l'Intranet soit accessible via un nom convivial au lieu de l'adresse IP, nous créons un enregistrement de type **A** dans notre zone de recherche directe DNS, pointant **intranet.sezoro.local** vers l'adresse **192.168.1.10**.

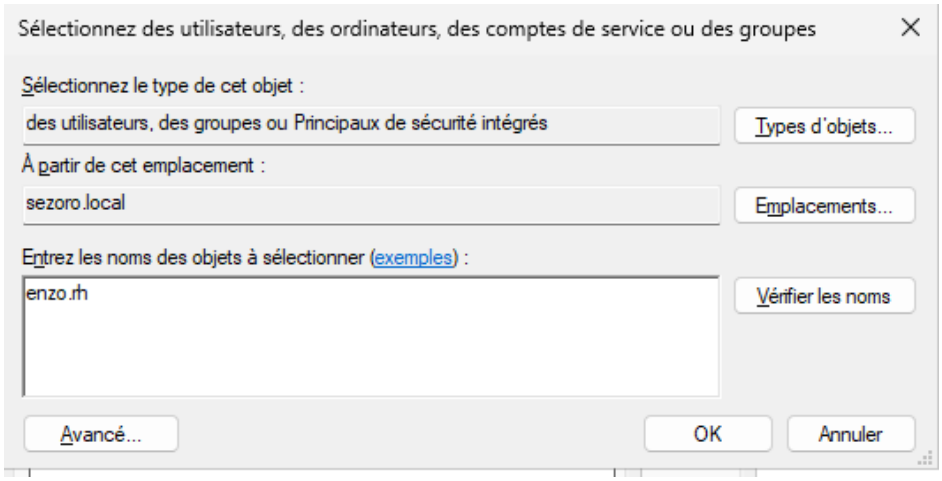


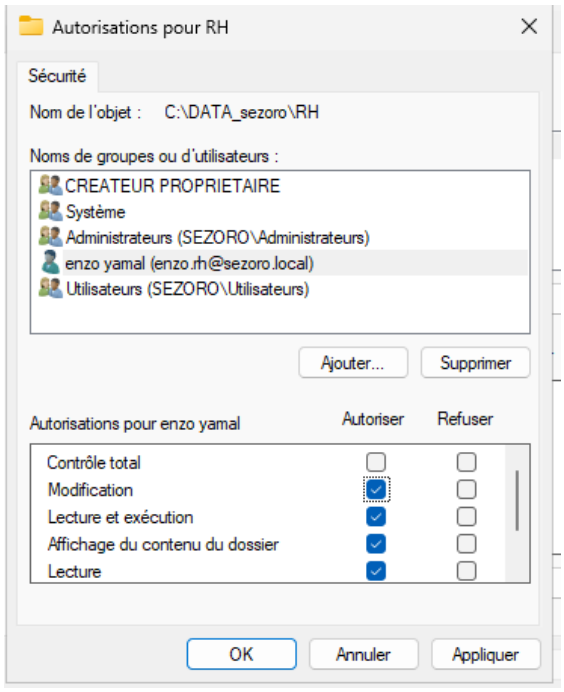
Création et partage des dossiers de données : Nous créons une structure de dossiers sur le disque **C:** (DATA_sezoro) et nous configurons les partages réseau avec les permissions **NTFS** appropriées pour chaque département.





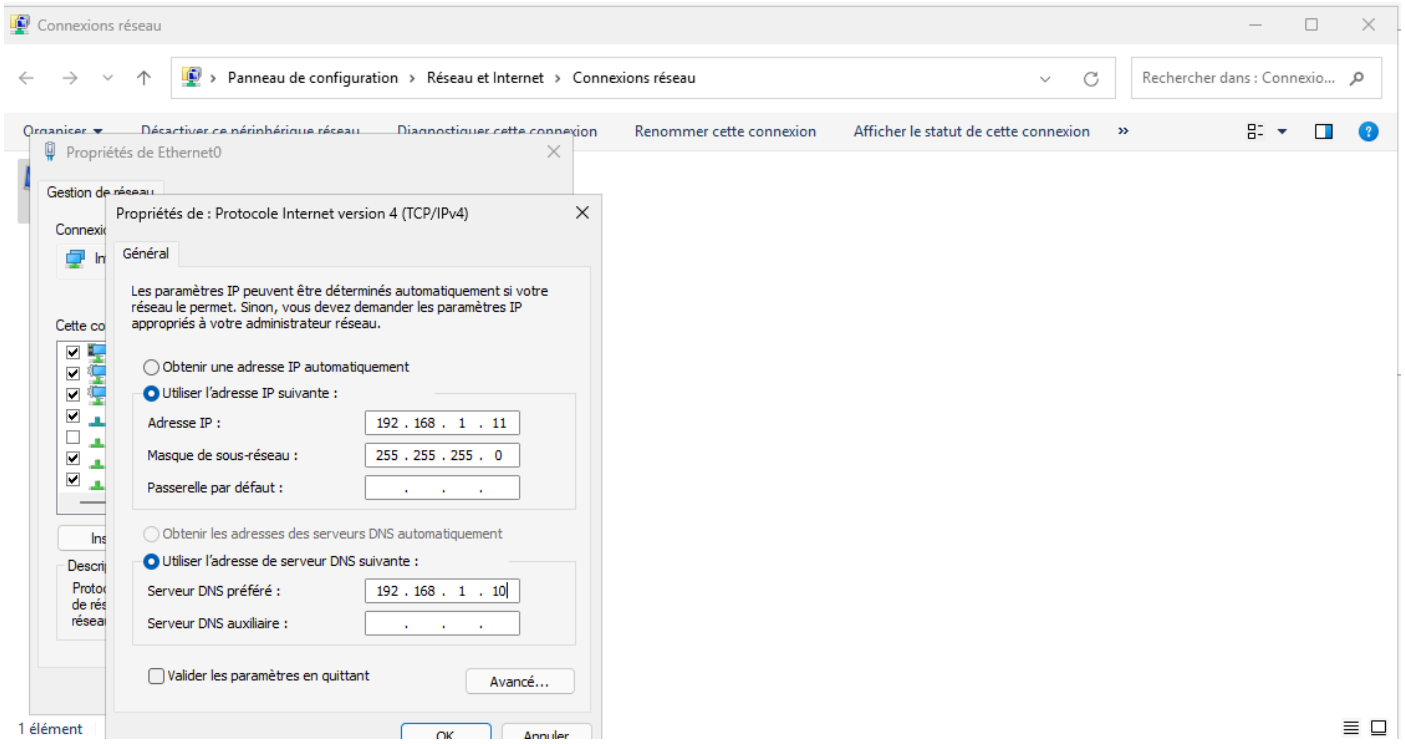

Propriétés de : RH
Général
Partage avancé
Partager ce dossier
Paramètres
Nom du partage :
RH
Ajouter
Supprimer
Limiter le nombre d'utilisateurs simultanés à :
16777
Commentaires :
Autorisations
Mise en cache
OK
Annuler
Appliquer
Partager...
Chemin réseau
Non partagé
OK
Annuler
Appliquer


Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes
Sélectionnez le type de cet objet :
des utilisateurs, des groupes ou Principaux de sécurité intégrés
Types d'objets...
À partir de cet emplacement :
sezoro.local
Emplacements...
Entrez les noms des objets à sélectionner (exemples) :
enzo.rh
Vérifier les noms
Avancé...
OK
Annuler


Autorisations pour RH
Sécurité
Nom de l'objet : C:\DATA_sezoro\RH
Noms de groupes ou d'utilisateurs :
CREATEUR PROPRIETAIRE
Système
Administrateurs (SEZORO\Administrateurs)
enzo yamal (enzo.rh@sezoro.local)
Utilisateurs (SEZORO\Utilisateurs)
Ajouter...
Supprimer
Autorisations pour enzo yamal
Autoriser
Refuser
Contrôle total
Modification
Lecture et exécution
Affichage du contenu du dossier
Lecture
OK
Annuler
Appliquer

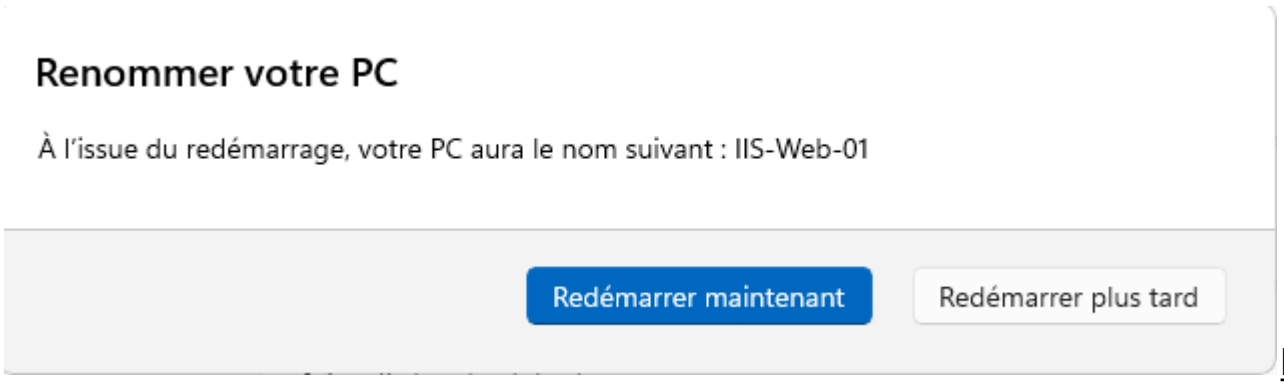
Mise en place de la Haute Disponibilité Web (IIS-1 & IIS-2)

Après avoir configuré l'Intranet de base sur le contrôleur de domaine, nous passons à une architecture plus robuste. L'objectif est de déployer deux serveurs Web dédiés (**IIS-1** et **IIS-2**) pour garantir que le site de l'entreprise reste accessible même si l'un des serveurs tombe en panne.

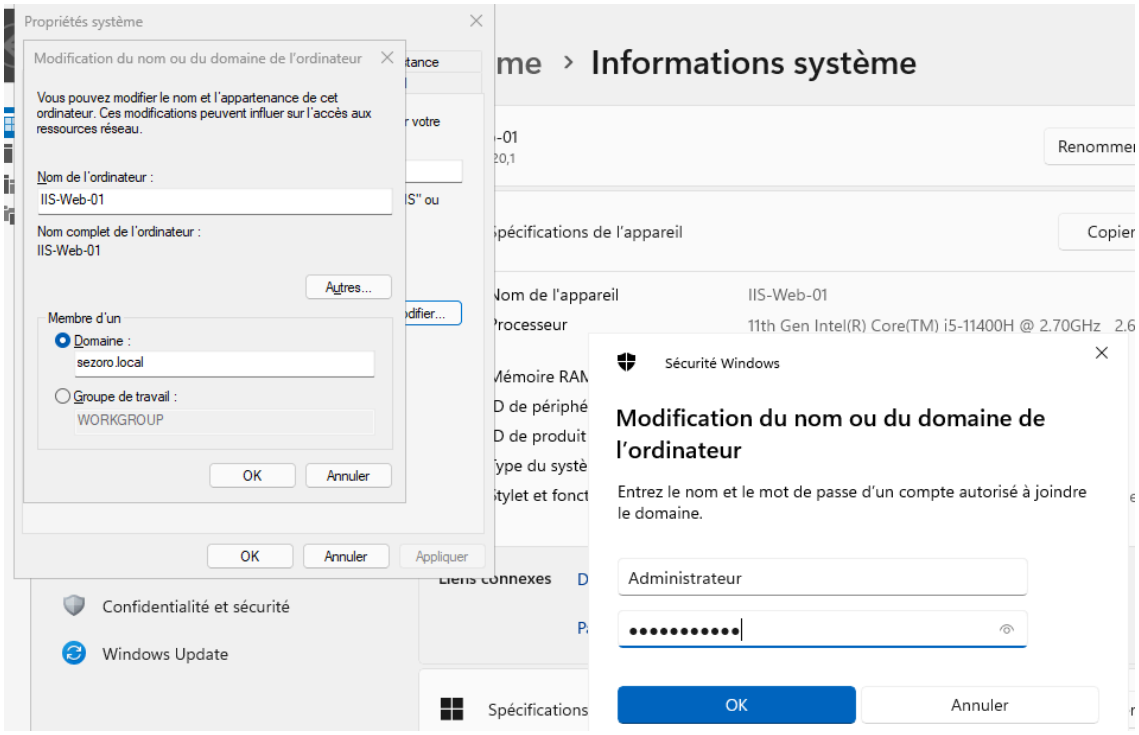


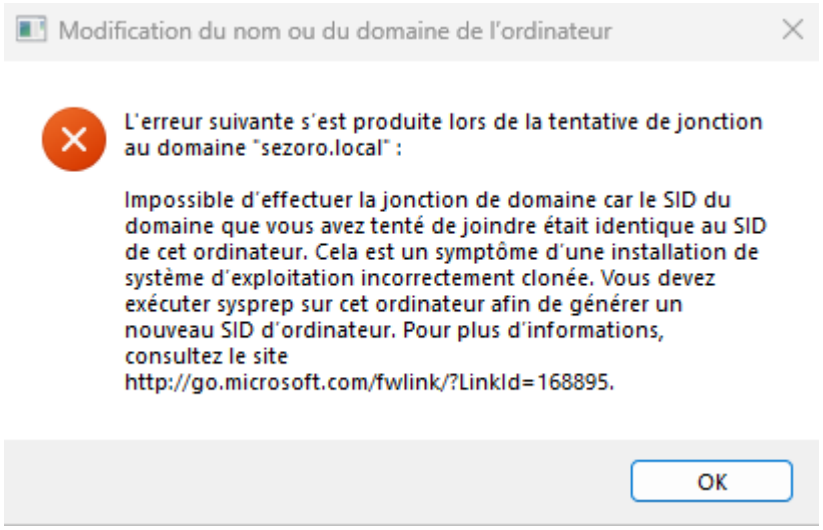
Intégration au Domaine et DNS

Nous joignons les deux serveurs au domaine sezoro.local. Ensuite, nous créons les enregistrements DNS nécessaires pour que les requêtes des clients soient dirigées vers l'infrastructure Web.



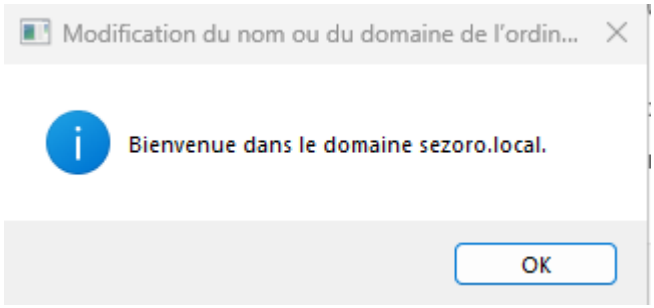
DNS



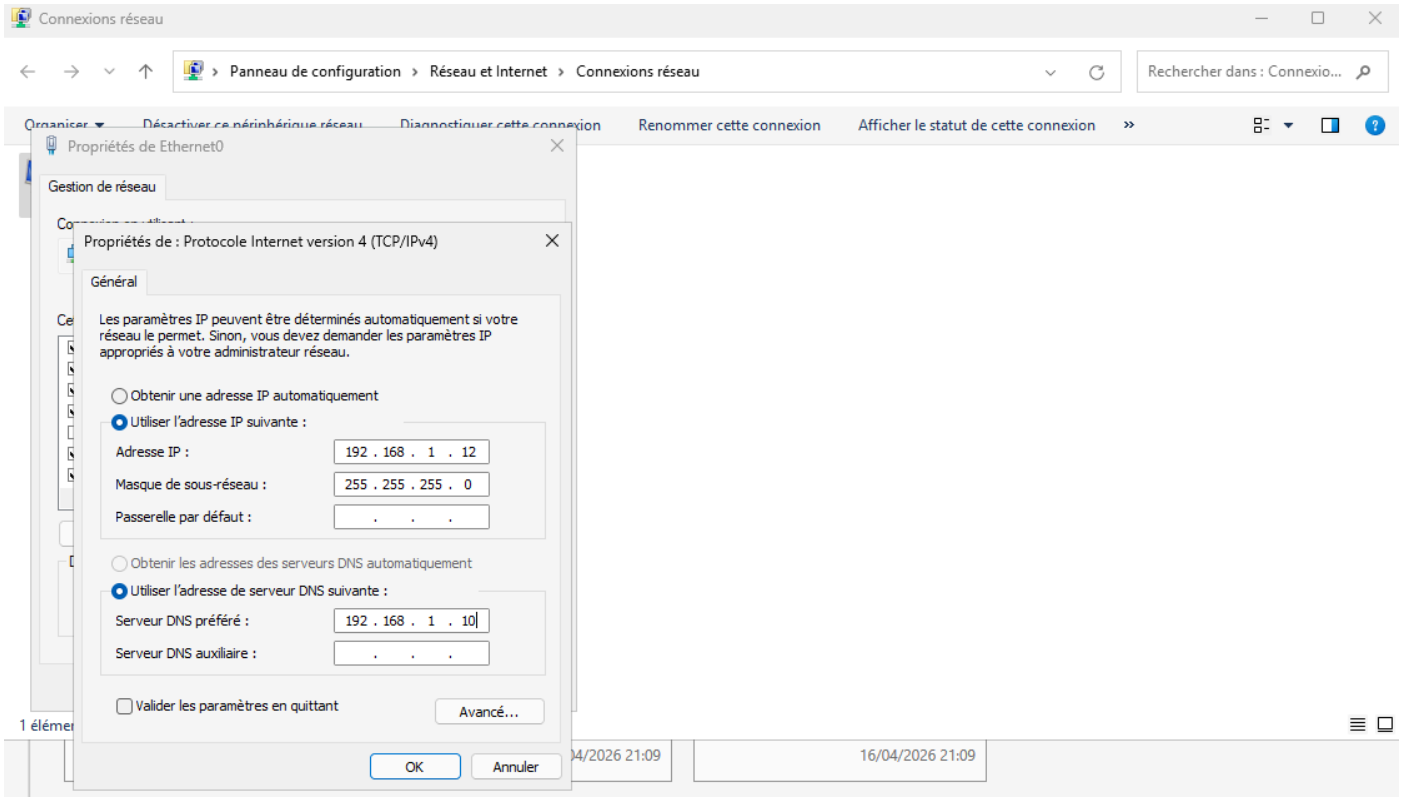


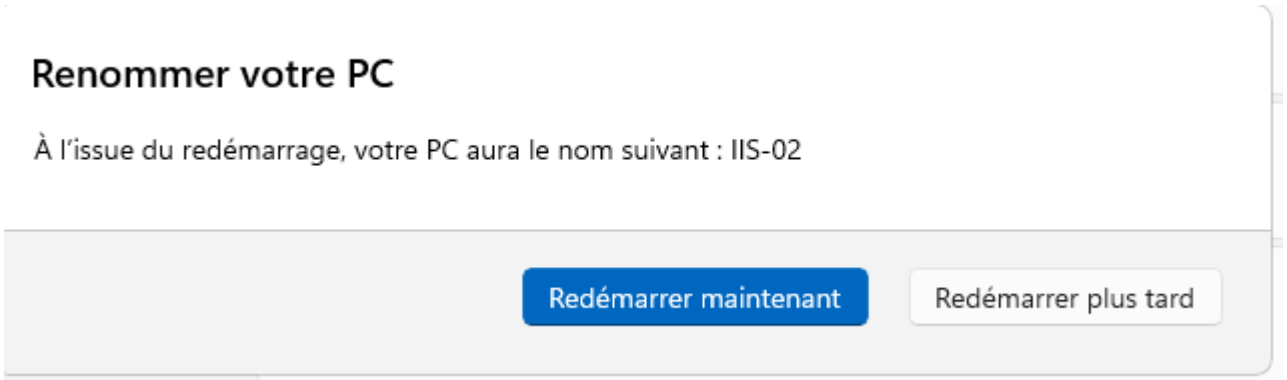
⚠️ Problème de Clonage et Solution

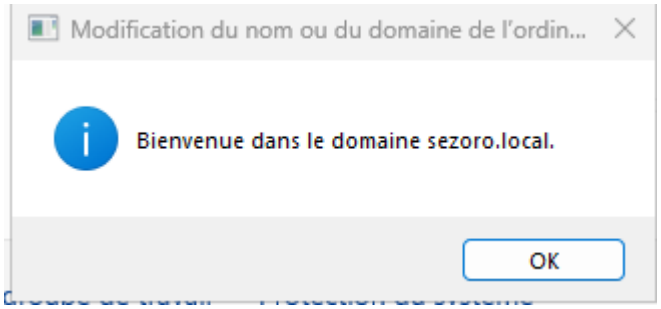
- **Le Problème : Conflit de SID** Échec de la jonction au domaine des serveurs clonés (**IIS-01/02**). Le domaine refuse l'accès car les serveurs possèdent le même identifiant de sécurité (**SID**) que la machine source.
- **La Solution : Utilisation de SYSPREP** Exécution de l'outil sysprep.exe avec l'option **"Généraliser"**.
    - **Action :** Réinitialisation de l'identifiant de sécurité unique de Windows.
    - **Résultat :** Attribution d'un **SID unique** à chaque serveur, permettant une intégration réussie au domaine sezoro.local.


Modification du nom ou du domaine de l'ordin...
Bienvenue dans le domaine sezoro.local.
OK

Sur IIS-2 :

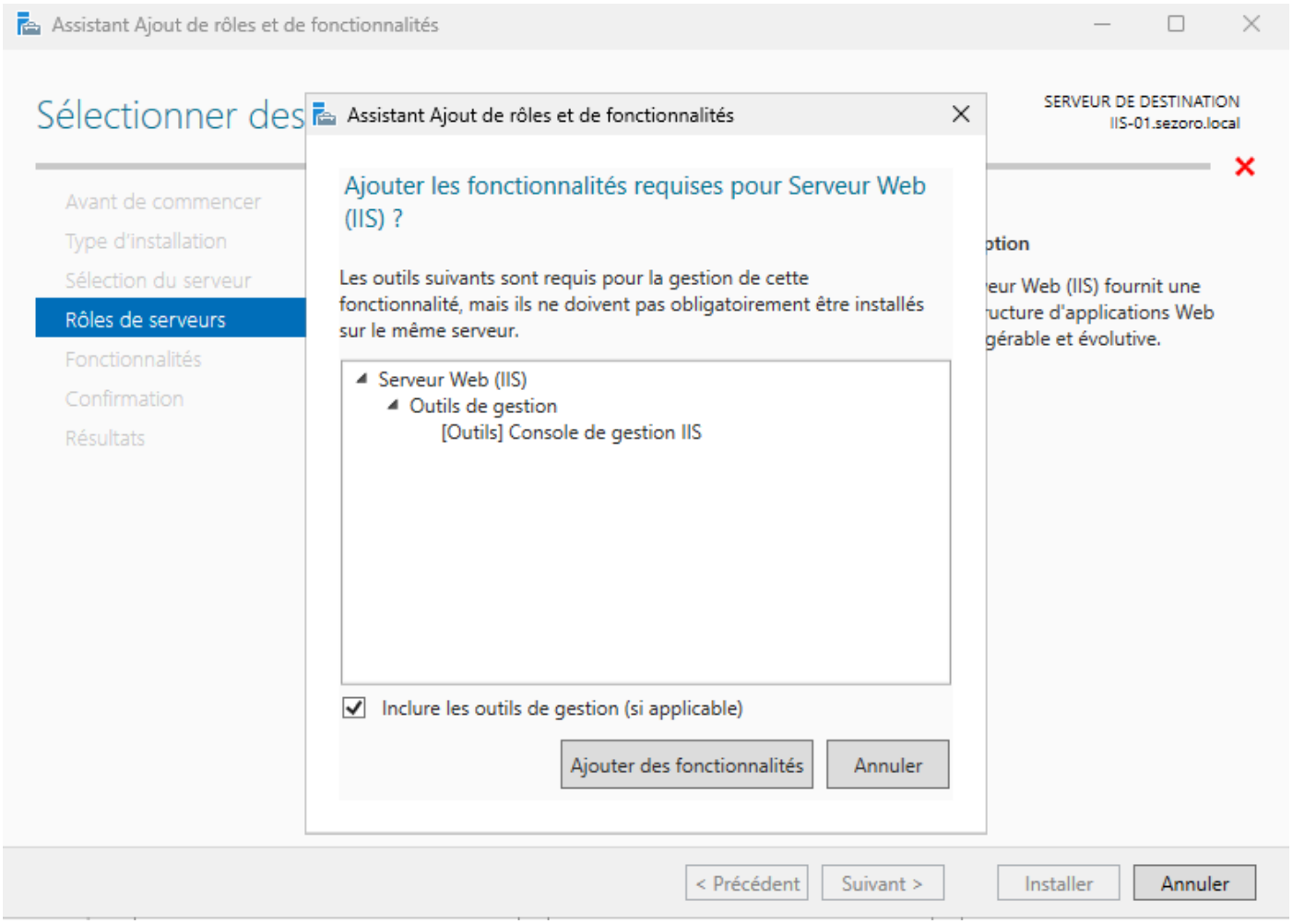

Connexions réseau
Panneau de configuration › Réseau et Internet › Connexions réseau
Rechercher dans : Connexio...
Organiser
Désactiver ce périphérique réseau
Diagnostiquer cette connexion
Renommer cette connexion
Afficher le statut de cette connexion
Propriétés de Ethernet0
Gestion de réseau
Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 1 . 12
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut :
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 192 . 168 . 1 . 10
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler
16/04/2026 21:09


Renommer votre PC
À l'issue du redémarrage, votre PC aura le nom suivant : IIS-02
Redémarrer maintenant
Redémarrer plus tard


Modification du nom ou du domaine de l'ordin...
Bienvenue dans le domaine sezoro.local.
OK

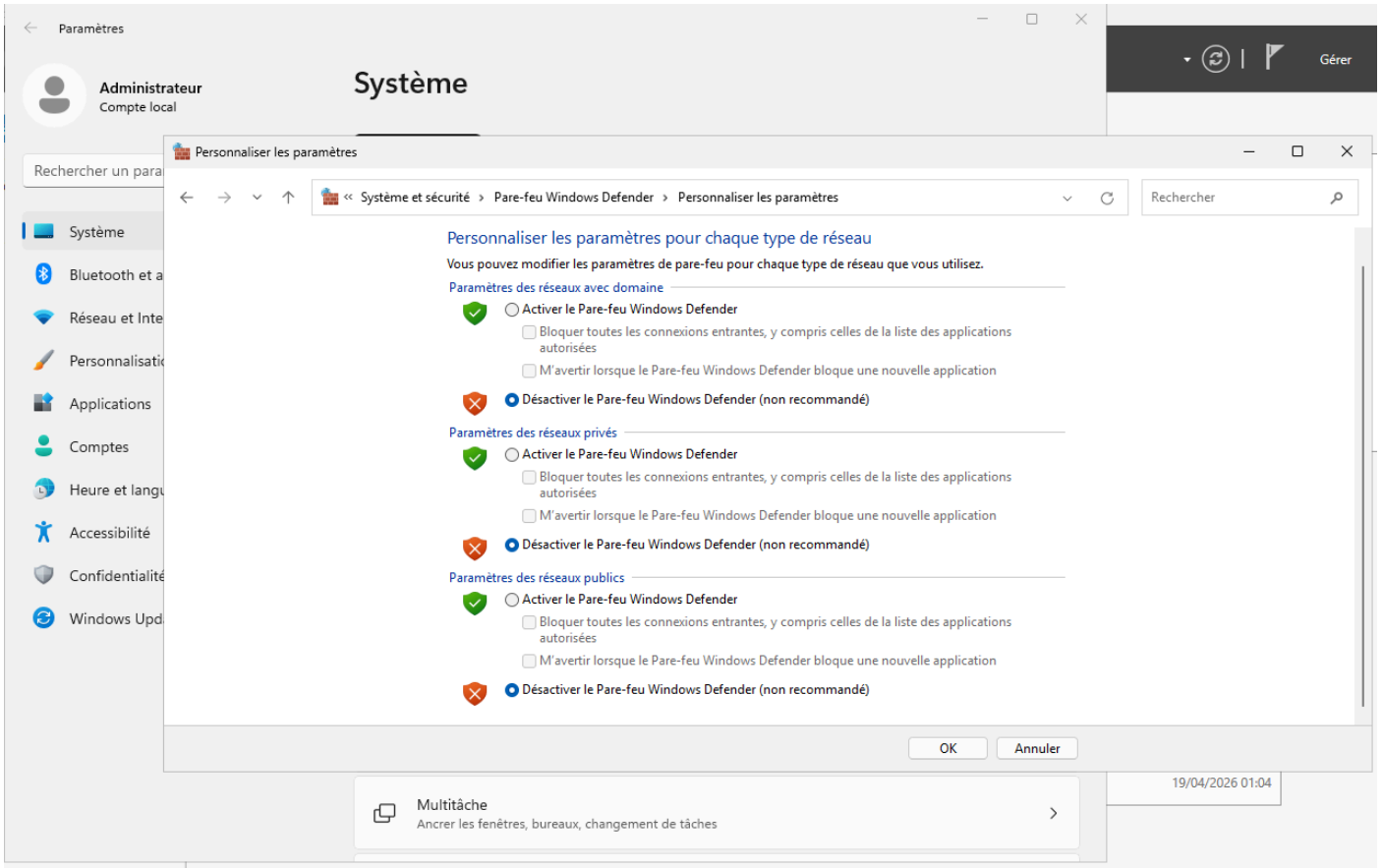
Installation du rôle Web (IIS) sur les deux machines :

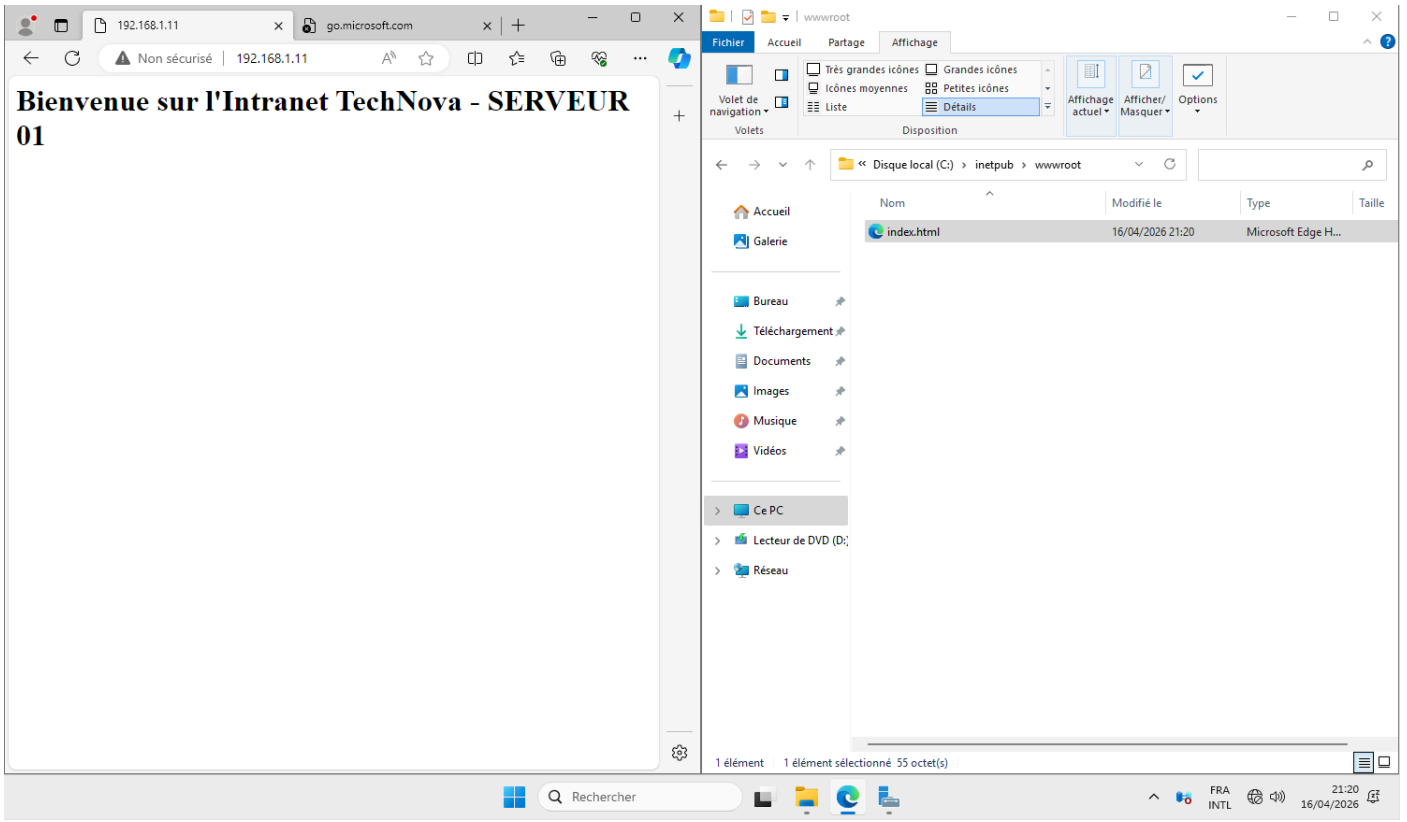
Sur chaque serveur (IIS-1 : 192.168.1.11 و IIS-2 : 192.168.1.12)، nous installons le rôle Web Server (IIS). Nous configurons ensuite des pages d'accueil légèrement différentes (ex: 'Welcome to IIS-1') pour pouvoir tester et identifier quel serveur répond lors de la phase de Load Balancing

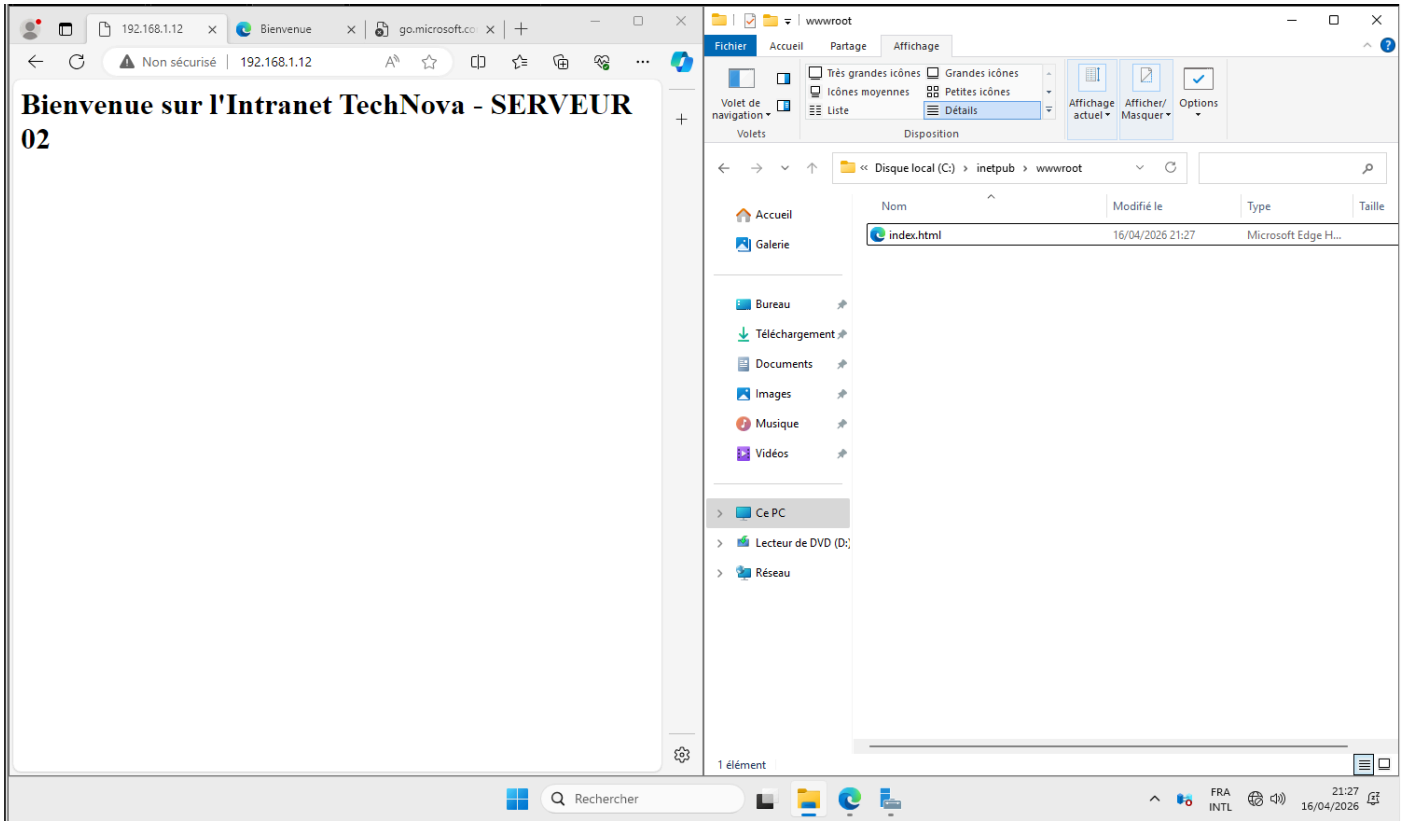


On désactive le firewall sur IIS1 et IIS2 :

Cette action permet d'éliminer tout blocage potentiel des flux HTTP (port 80) et des requêtes ICMP (Ping) durant la phase de test et de mise en place de la haute disponibilité

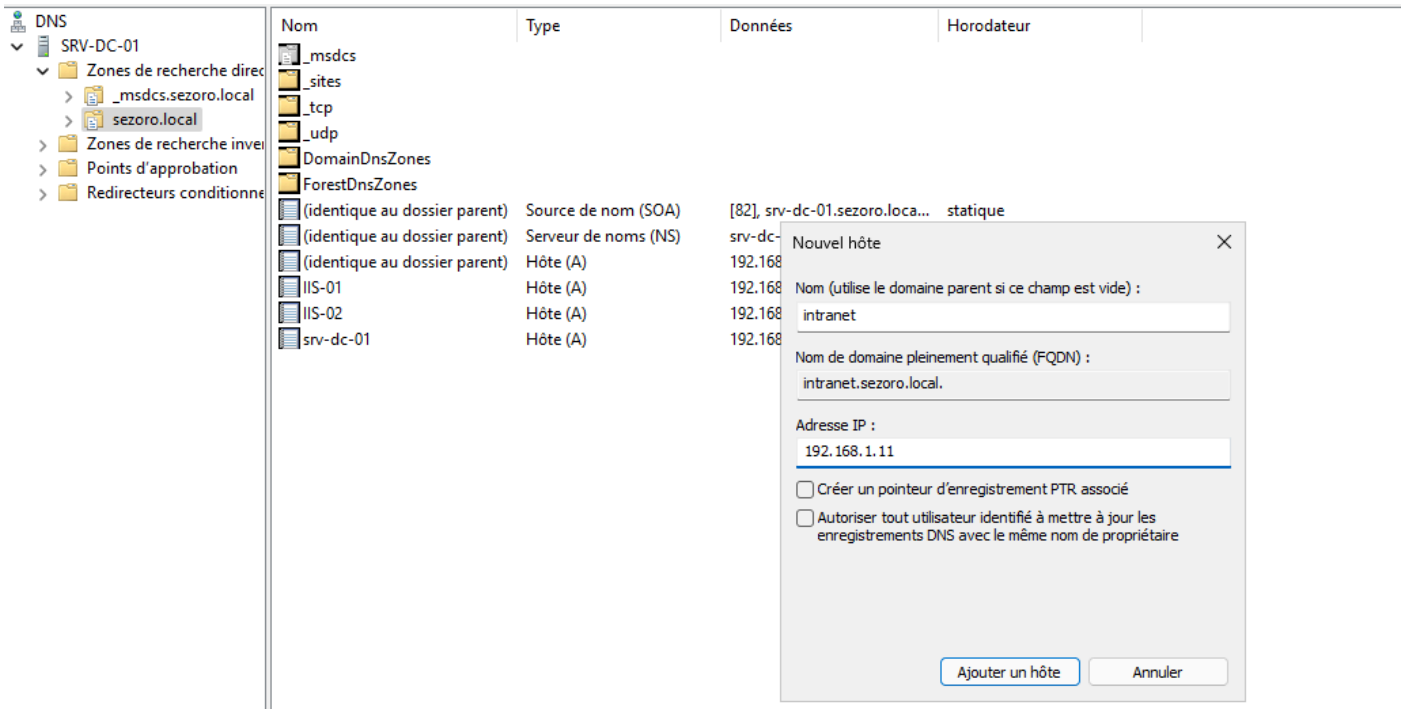

Paramètres
Administrateur
Compte local
Système
Gérer
Personnaliser les paramètres
« Système et sécurité › Pare-feu Windows Defender › Personnaliser les paramètres
Rechercher
Personnaliser les paramètres pour chaque type de réseau
Vous pouvez modifier les paramètres de pare-feu pour chaque type de réseau que vous utilisez.
Paramètres des réseaux avec domaine
Activer le Pare-feu Windows Defender
Bloquer toutes les connexions entrantes, y compris celles de la liste des applications autorisées
M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application
Désactiver le Pare-feu Windows Defender (non recommandé)
Paramètres des réseaux privés
Activer le Pare-feu Windows Defender
Bloquer toutes les connexions entrantes, y compris celles de la liste des applications autorisées
M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application
Désactiver le Pare-feu Windows Defender (non recommandé)
Paramètres des réseaux publics
Activer le Pare-feu Windows Defender
Bloquer toutes les connexions entrantes, y compris celles de la liste des applications autorisées
M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application
Désactiver le Pare-feu Windows Defender (non recommandé)
OK
Annuler
Système
Bluetooth et a
Réseau et Inte
Personnalisati
Applications
Comptes
Heure et langu
Accessibilité
Confidentialité
Windows Upd
Multitâche
Ancrer les fenêtres, bureaux, changement de tâches
19/04/2026 01:04

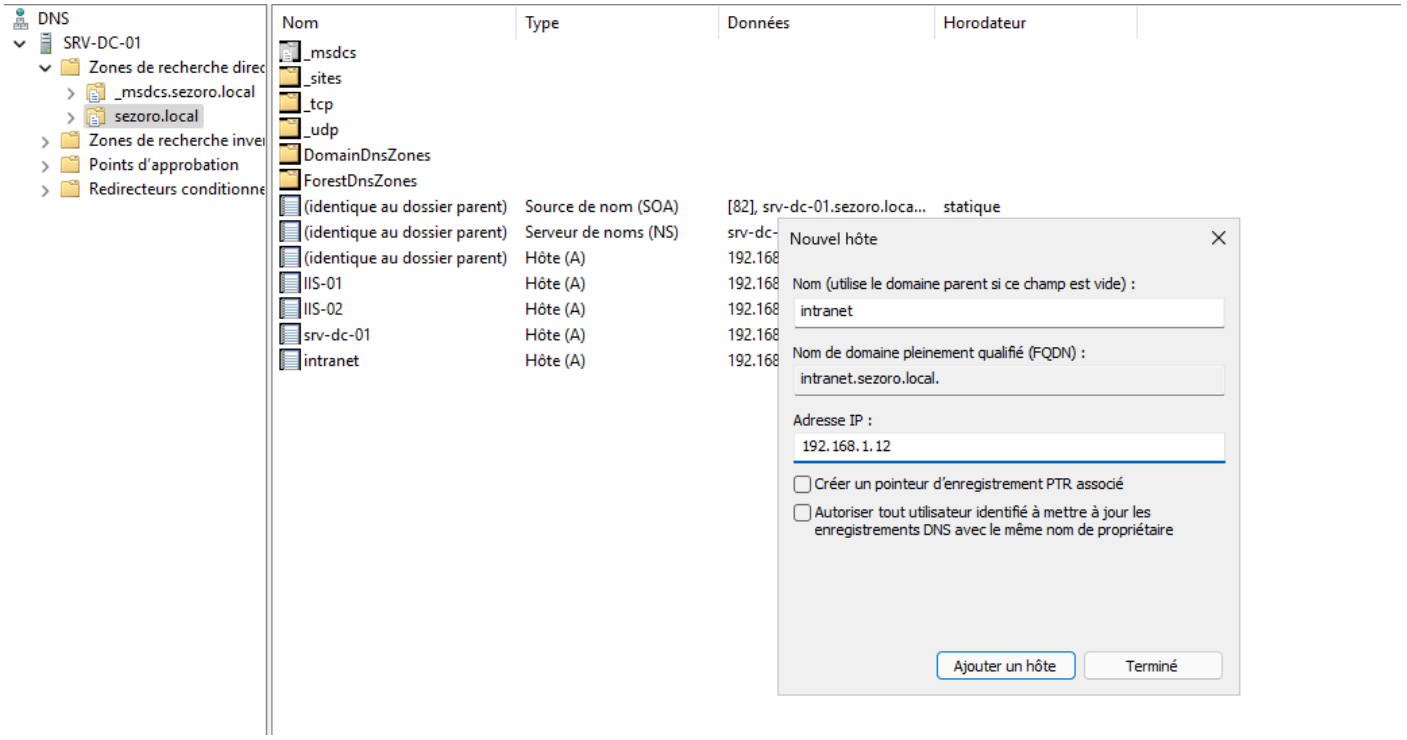

192.168.1.11
go.microsoft.com
Non sécurisé
192.168.1.11
Bienvenue sur l'Intranet TechNova - SERVEUR 01
wwwroot
Fichier
Accueil
Partage
Affichage
Volet de navigation
Très grandes icônes
Grandes icônes
Icônes moyennes
Petites icônes
Liste
Détails
Affichage actuel
Afficher/ Masquer
Options
Volets
Disposition
« Disque local (C:) › inetpub › wwwroot
Accueil
Galerie
Bureau
Téléchargement
Documents
Images
Musique
Vidéos
Ce PC
Lecteur de DVD (D:)
Réseau
Nom
Modifié le
Type
Taille
index.html
16/04/2026 21:20
Microsoft Edge H...
1 élément
1 élément sélectionné 55 octet(s)
Rechercher
FRA
INTL
21:20
16/04/2026



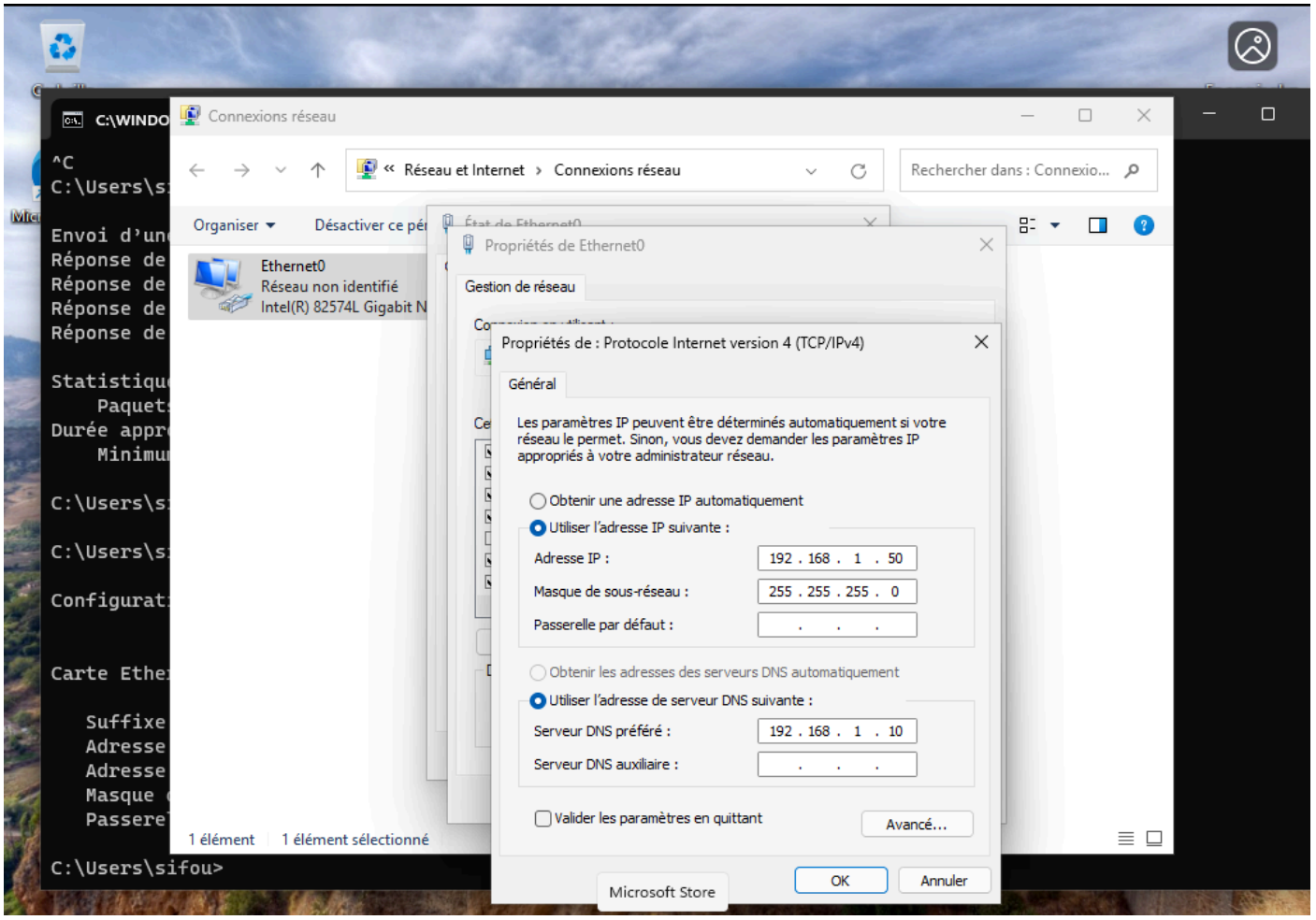
Redondance DNS pour le service Intranet

Pour assurer la haute disponibilité de notre Intranet, nous créons deux enregistrements de type A dans le DNS pour le même nom d'hôte 'intranet'. En pointant 'intranet.sezoro.local' vers les deux adresses IP (192.168.1.11 et 192.168.1.12), nous activons la technique du DNS Round Robin. Cela permet de répartir les requêtes des utilisateurs entre IIS-1 et IIS-2، garantissant ainsi la continuité du service en cas de panne de l'un des deux serveurs.

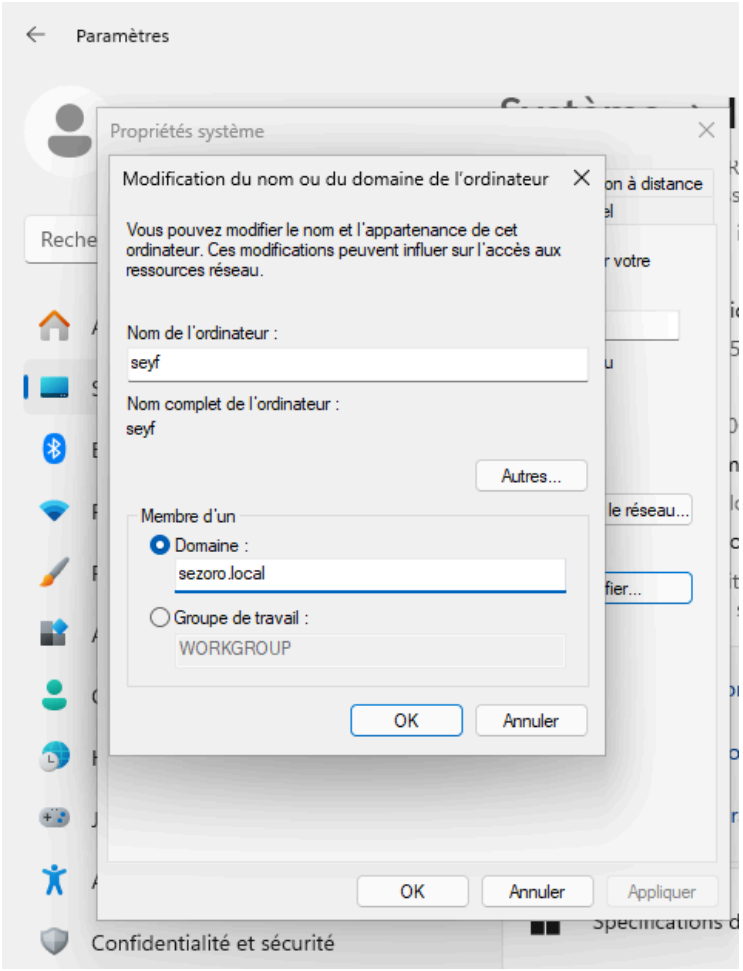


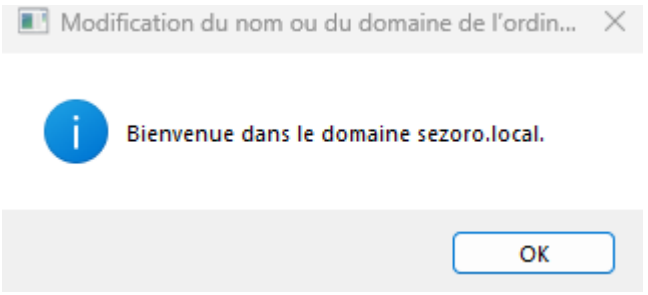


Pour tester les serveur web, sur un pc client :

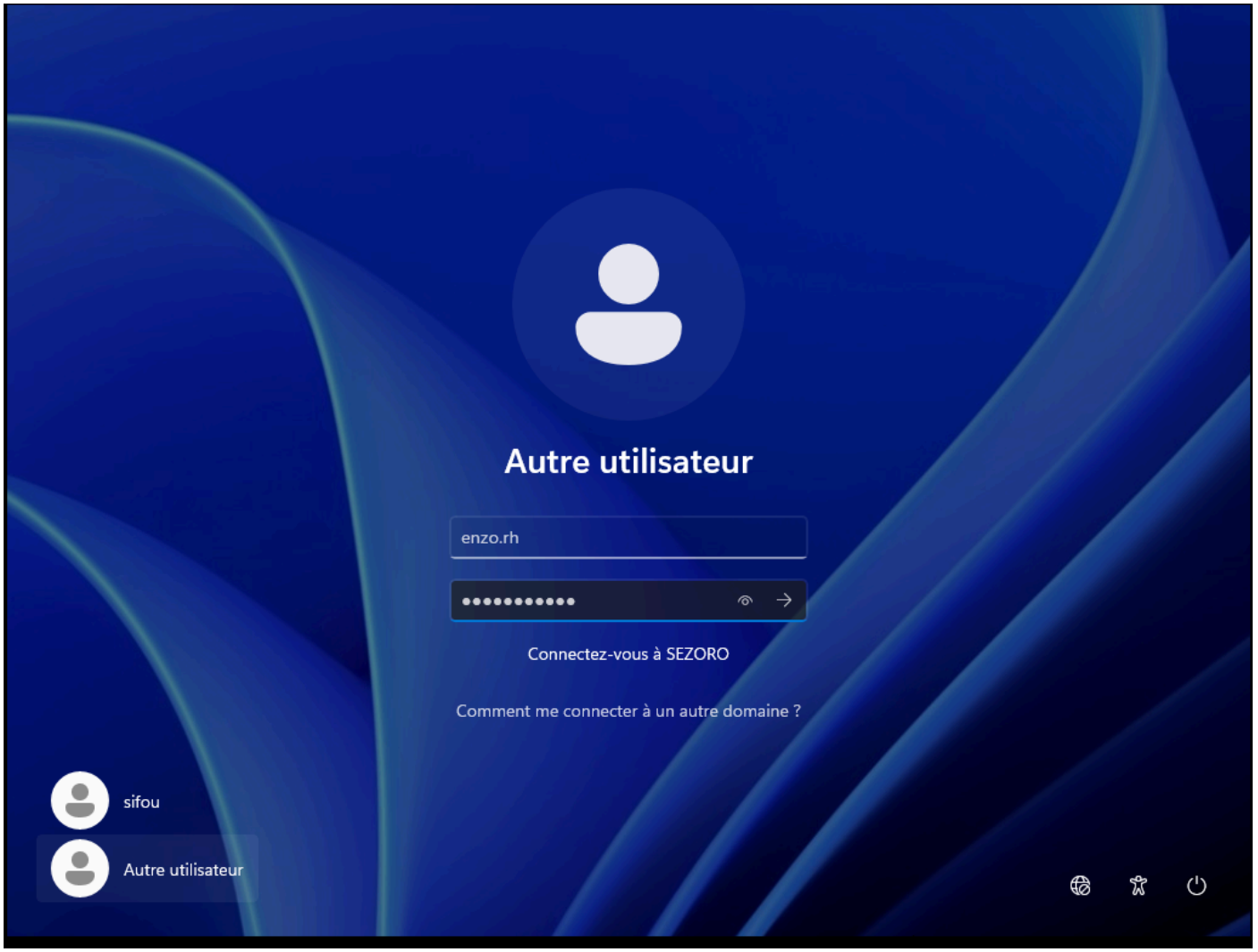


Regoindre le domain :



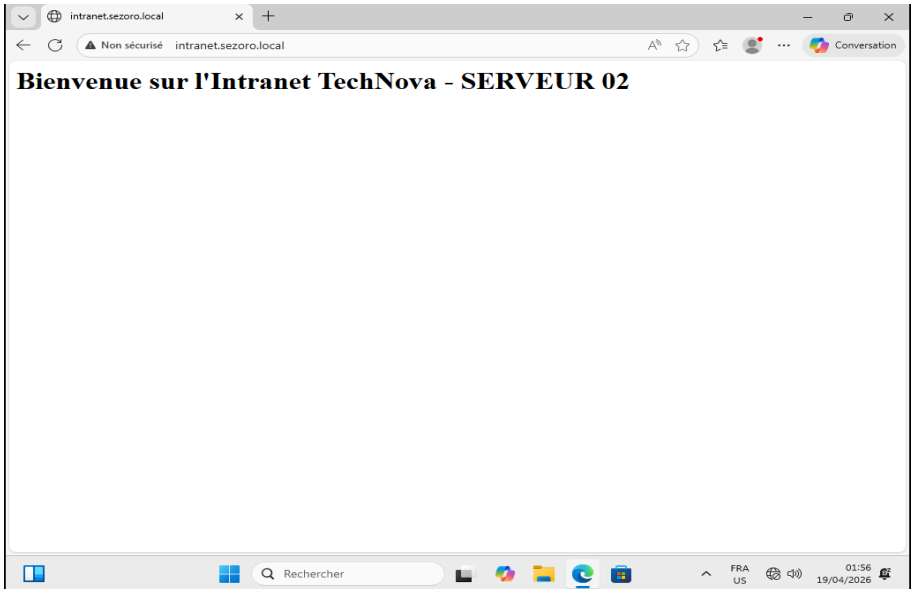


Entre avec l'utlisateur qu'on a crée sur AD DS

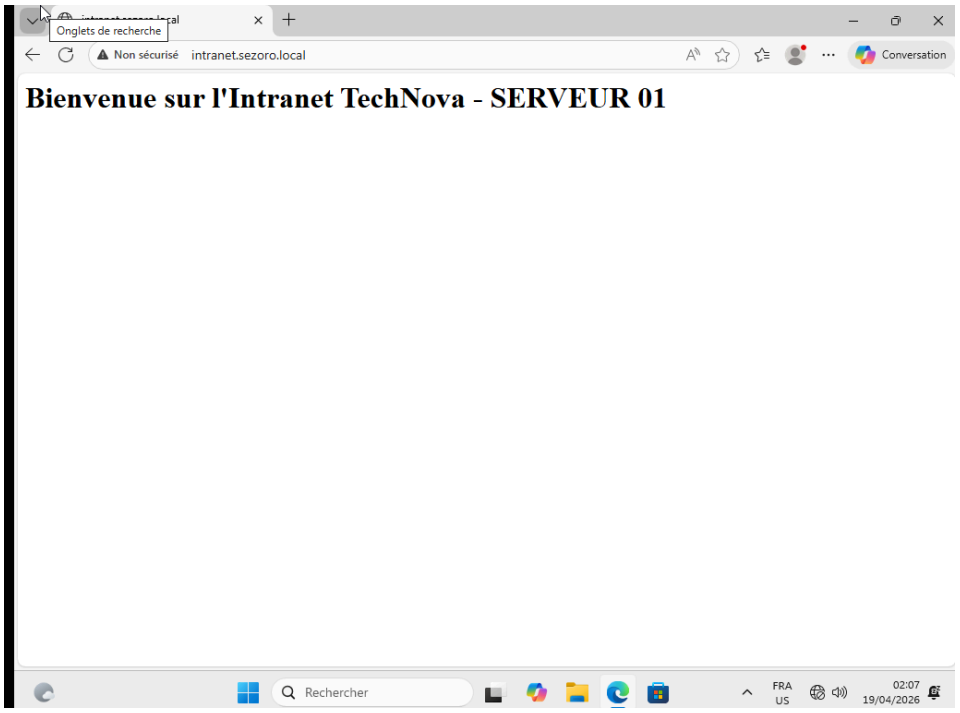


Depuis le navigateur du PC Client, nous accédons à l'adresse http://intranet.sezoro.local. Grâce à la configuration DNS Round Robin réalisée précédemment :

- **Résultat attendu :** Le client affiche la page d'accueil de l'un des deux serveurs.
- **Validation :** En rafraîchissant la page ou en simulant une panne sur l'un des serveurs (ex: éteindre IIS-2), le client bascule automatiquement vers le second serveur, garantissant ainsi un accès ininterrompu à l'Intranet.



éteindre IIS-2 :



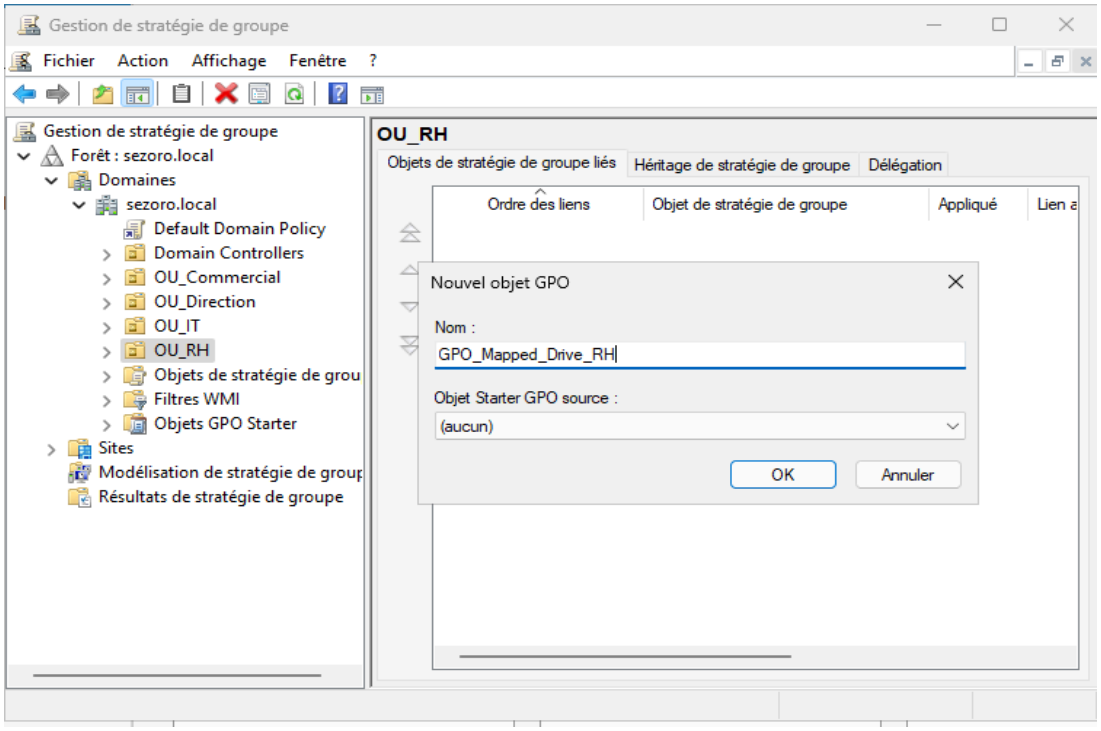
Pour le GPO :

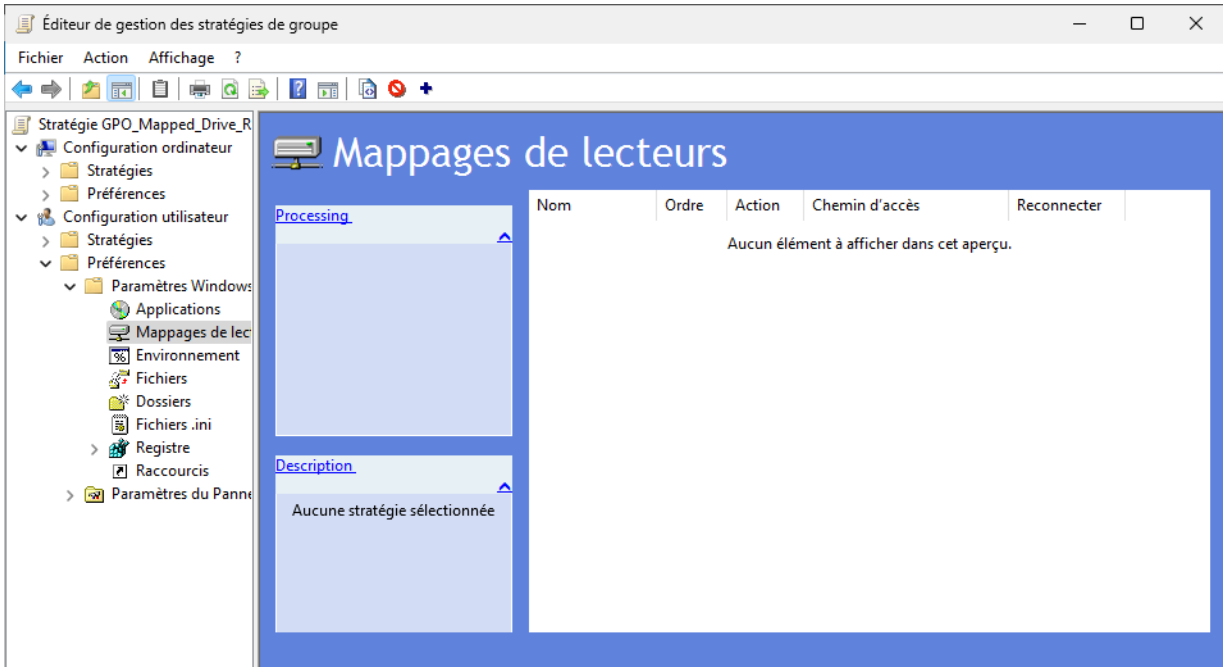
Afin de sécuriser et d'uniformiser l'environnement de travail des utilisateurs du domaine sezoro.local,On a configuré une GPO incluant :

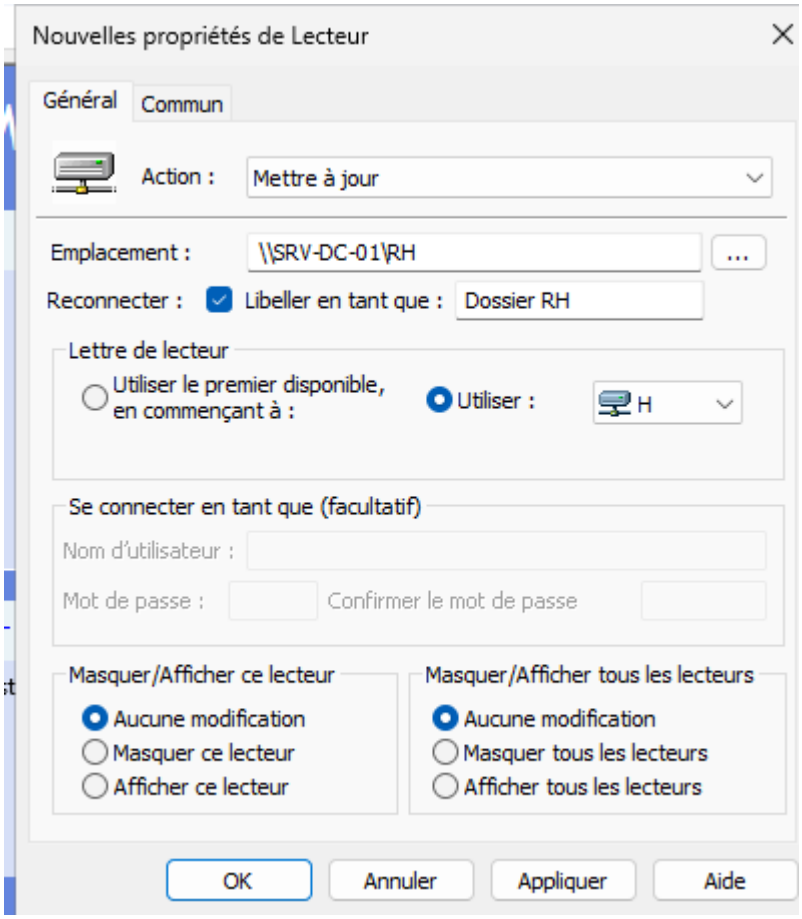
- **Mappage de Lecteur Réseau :** Connexion automatique du dossier partagé \\SRV-DC-01\RH sur la lettre H: pour le service RH.
- **Restrictions de Sécurité :** Désactivation de l'accès au Panneau de configuration et à l'Invite de commande (CMD) pour limiter les risques de modifications système.
- **Personnalisation (Wallpaper) :** Application forcée d'un fond d'écran corporatif via les modèles d'administration du Bureau.

Résultat : Les politiques sont appliquées instantanément à chaque ouverture de session, garantissant un contrôle total sur les postes clients\

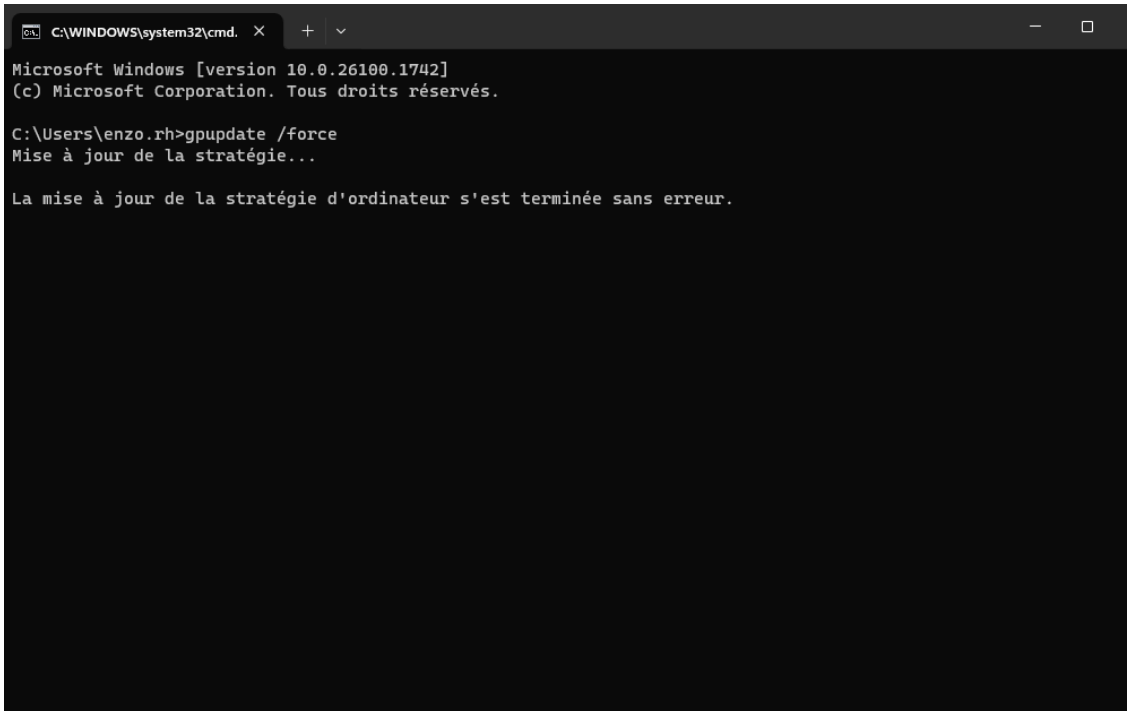
- **Gestion du Mappage de Lecteur Réseau:**

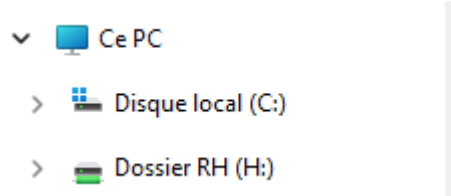



Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie GPO_Mapped_Drive_R
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Préférences
Paramètres Windows
Applications
Mappages de lec
Environnement
Fichiers
Dossiers
Fichiers .ini
Registre
Raccourcis
Paramètres du Panne
Mappages de lecteurs
Processing
Description
Aucune stratégie sélectionnée
Nom
Ordre
Action
Chemin d'accès
Reconnecter
Aucun élément à afficher dans cet aperçu.


Nouvelles propriétés de Lecteur
Général
Commun
Action :
Mettre à jour
Emplacement :
\\SRV-DC-01\RH
...
Reconnecter :
Libeller en tant que :
Dossier RH
Lettre de lecteur
Utiliser le premier disponible, en commençant à :
Utiliser :
H
Se connecter en tant que (facultatif)
Nom d'utilisateur :
Mot de passe :
Confirmer le mot de passe
Masquer/Afficher ce lecteur
Aucune modification
Masquer ce lecteur
Afficher ce lecteur
Masquer/Afficher tous les lecteurs
Aucune modification
Masquer tous les lecteurs
Afficher tous les lecteurs
OK
Annuler
Appliquer
Aide

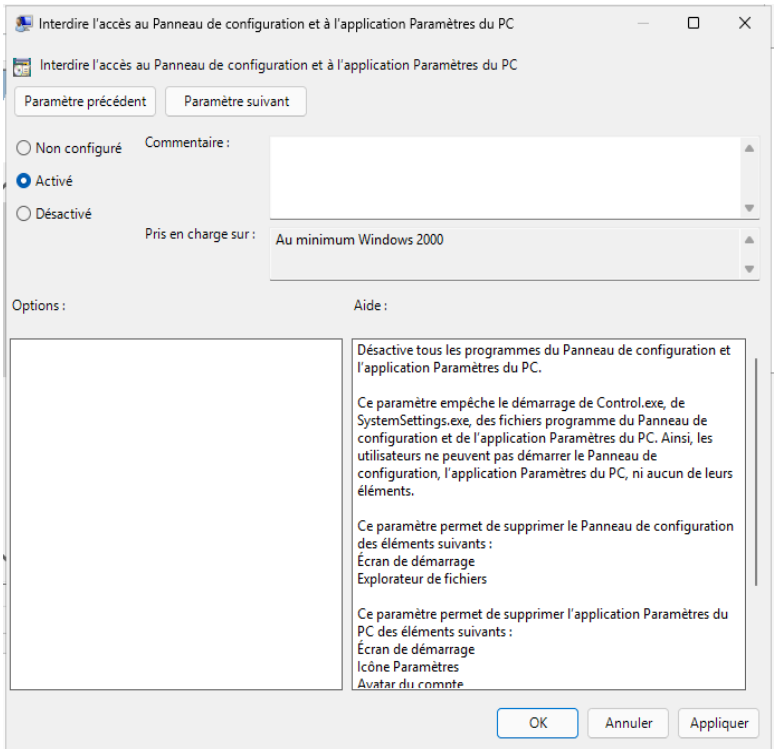
Tester sur le pc client (enzo.rh):



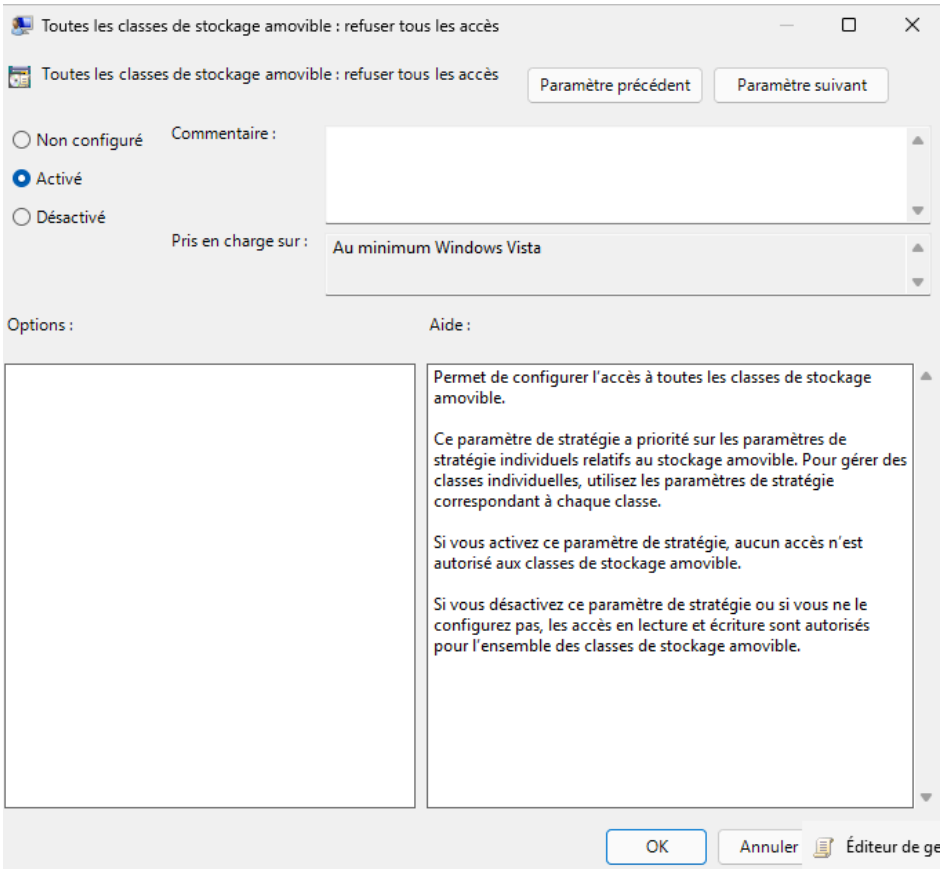


Restrictions :

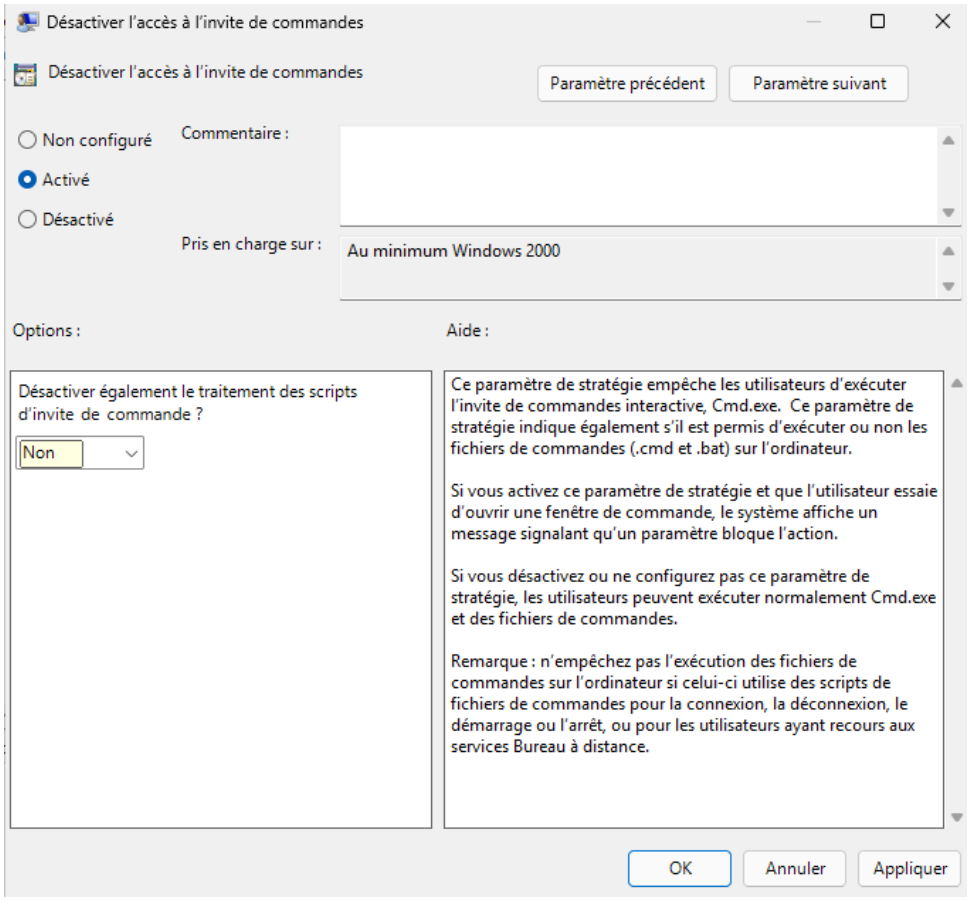
Interdire l'accès au Panneau de configuration et aux paramètres du PC



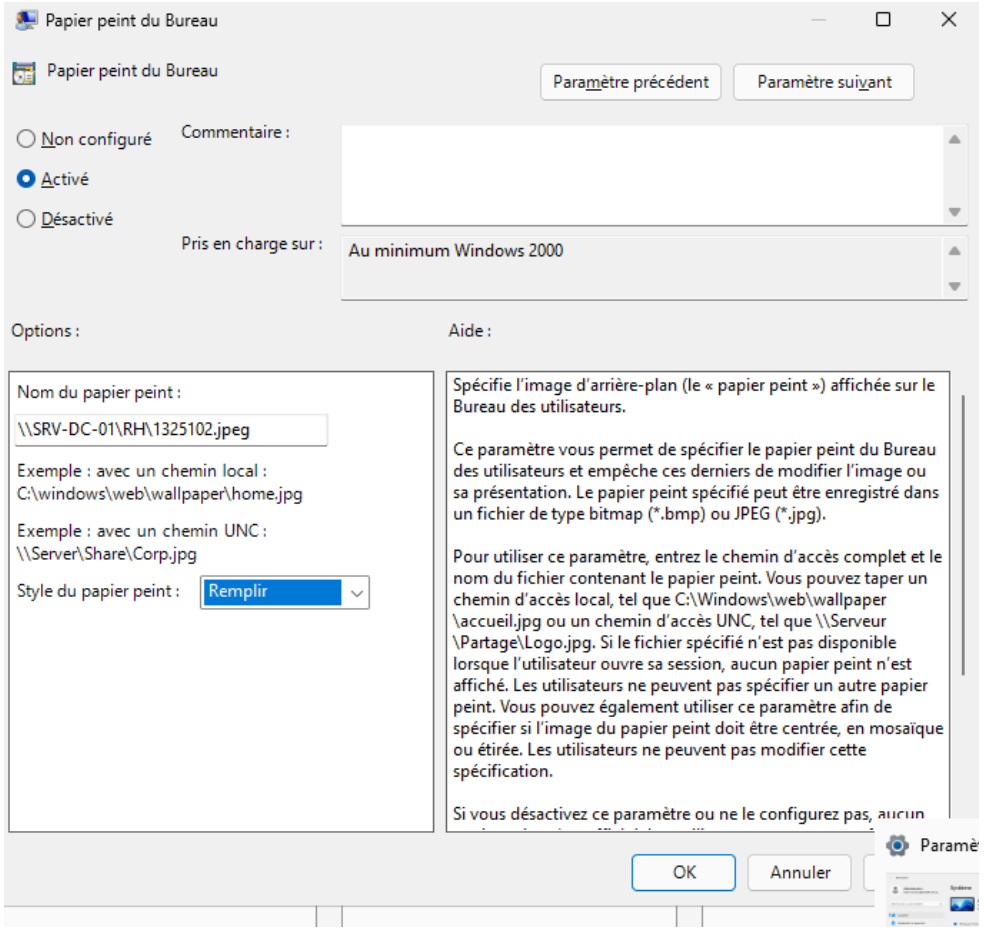
USB (Restrictions Stockage) :



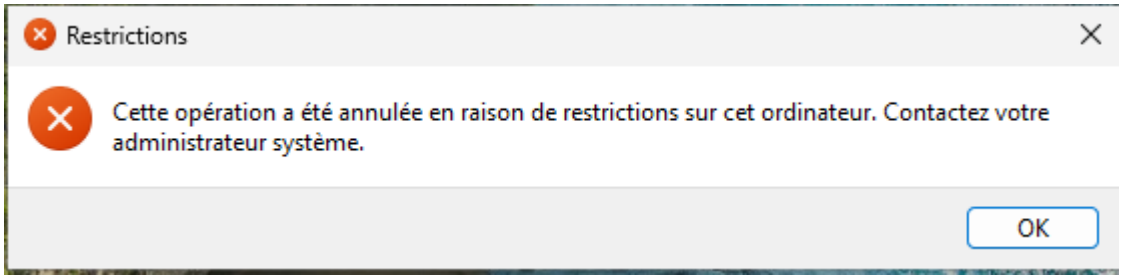
Désactiver le cmd

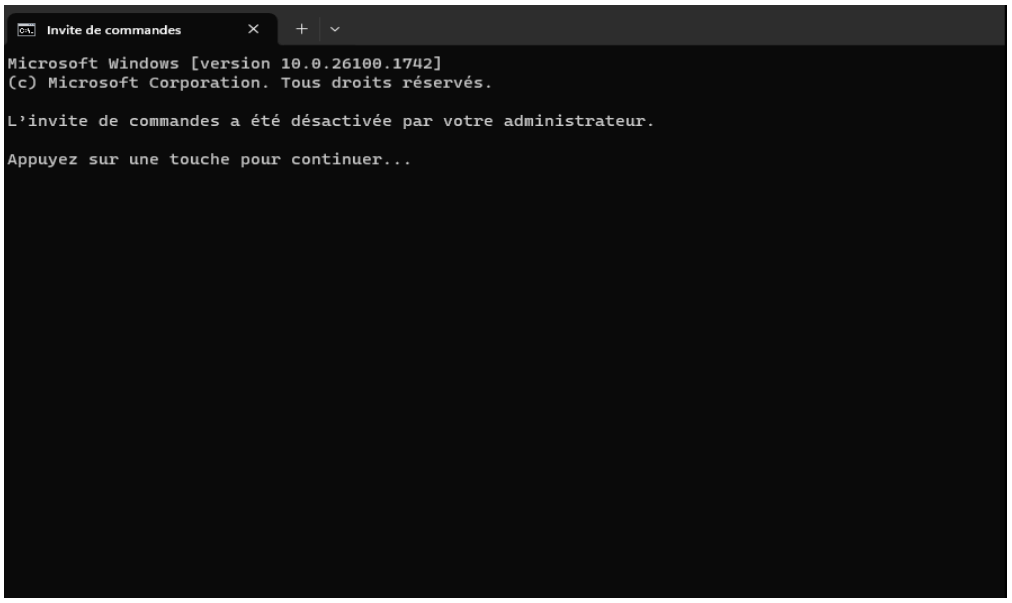


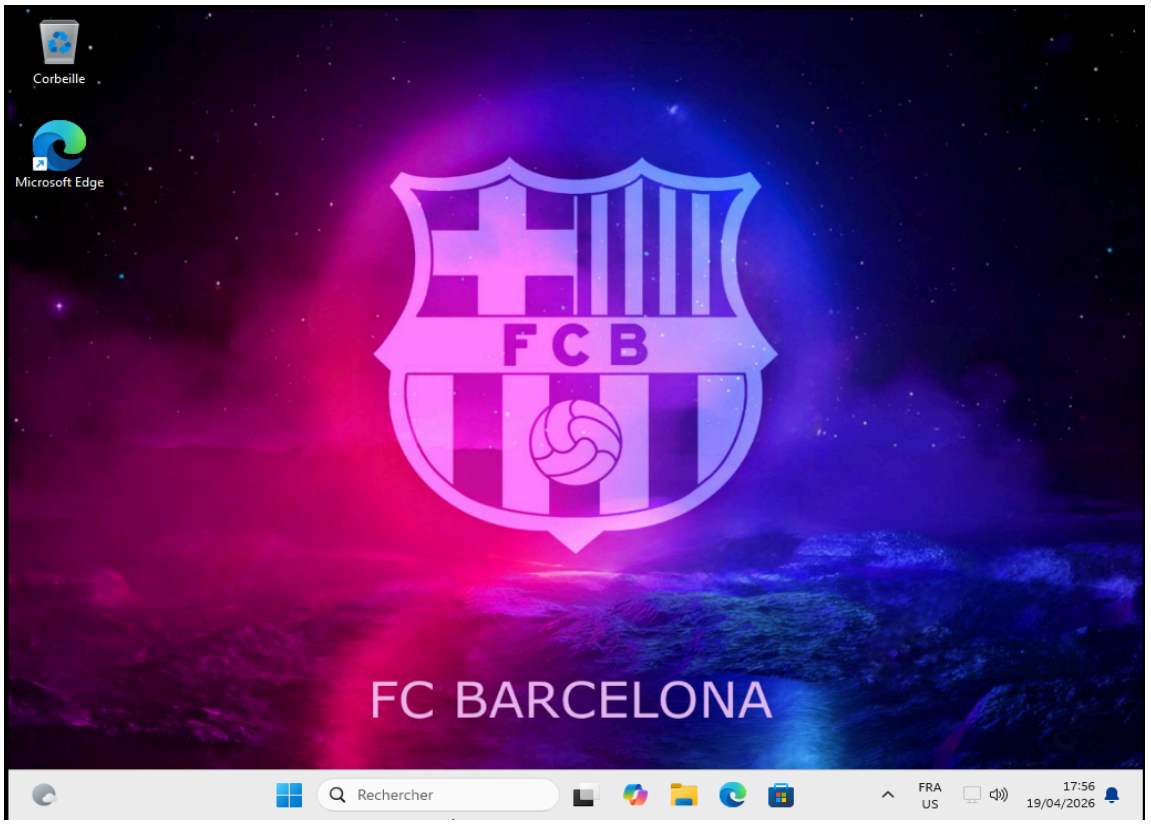
Ajuster Wallpaper :



Tester sur le pc client :


Restrictions
Cette opération a été annulée en raison de restrictions sur cet ordinateur. Contactez votre administrateur système.
OK


Invite de commandes
Microsoft Windows [version 10.0.26100.1742]
(c) Microsoft Corporation. Tous droits réservés.
L'invite de commandes a été désactivée par votre administrateur.
Appuyez sur une touche pour continuer...


Corbeille
Microsoft Edge
FCB
FC BARCELONA
Rechercher
FRA
US
17:56
19/04/2026

Domaine	*sezoro.local*
Serveur	*SRV-DC-01	192.168.84.10*
Client	*w11-client	192.168.84.50 (DHCP)*
Groupe RDS	*RDS_Users (Rober RH + Enzo IT)*
Objectif	*Permettre l'accès à un bureau distant sécurisé pour le télétravail*

Membre 3 – RDS : Bureau à distance

Objectif : Mettre en place une solution de télétravail permettant aux utilisateurs d'accéder à un environnement de bureau complet et sécurisé, hébergé sur le serveur de l'entreprise.

. Architecture technique :

- Serveur de Session (srv-dc-01) : Installation du rôle Hôte de session Bureau à distance (RD Session Host). C'est la machine qui héberge les sessions des utilisateurs.
- Authentification (AD DS) : Le serveur RDS utilise le contrôleur de domaine pour vérifier l'identité des utilisateurs (Annuaire centralisé).

. Étapes de mise en œuvre :

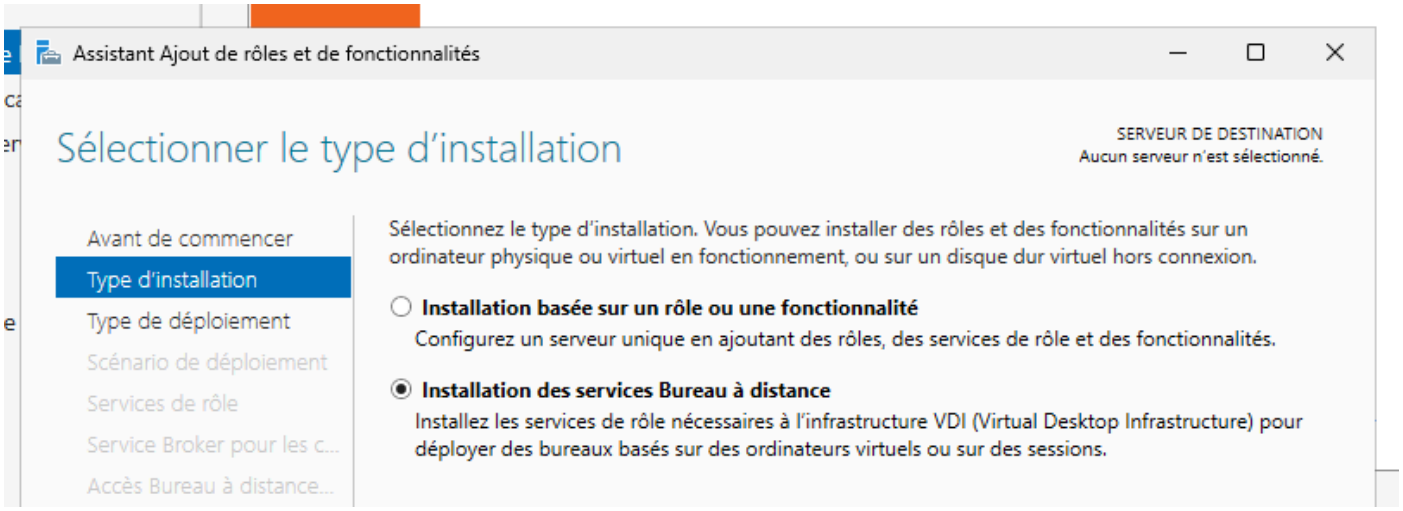
1. Côté AD DS : Création d'un groupe de sécurité global nommé RDS_Users et ajout des utilisateurs autorisés comme membres.
2. Côté RDS : Ajout du groupe RDS Users dans la liste des utilisateurs autorisés à se connecter à distance (Paramètres système).
3. Côté Client : Utilisation du client RDP (MSTSC) sur Windows 11 pour se connecter à l'adresse IP du serveur (192.168.84.10).

1. Installation du rôle RDS

1 — Sélection du type d'installation

📷 1

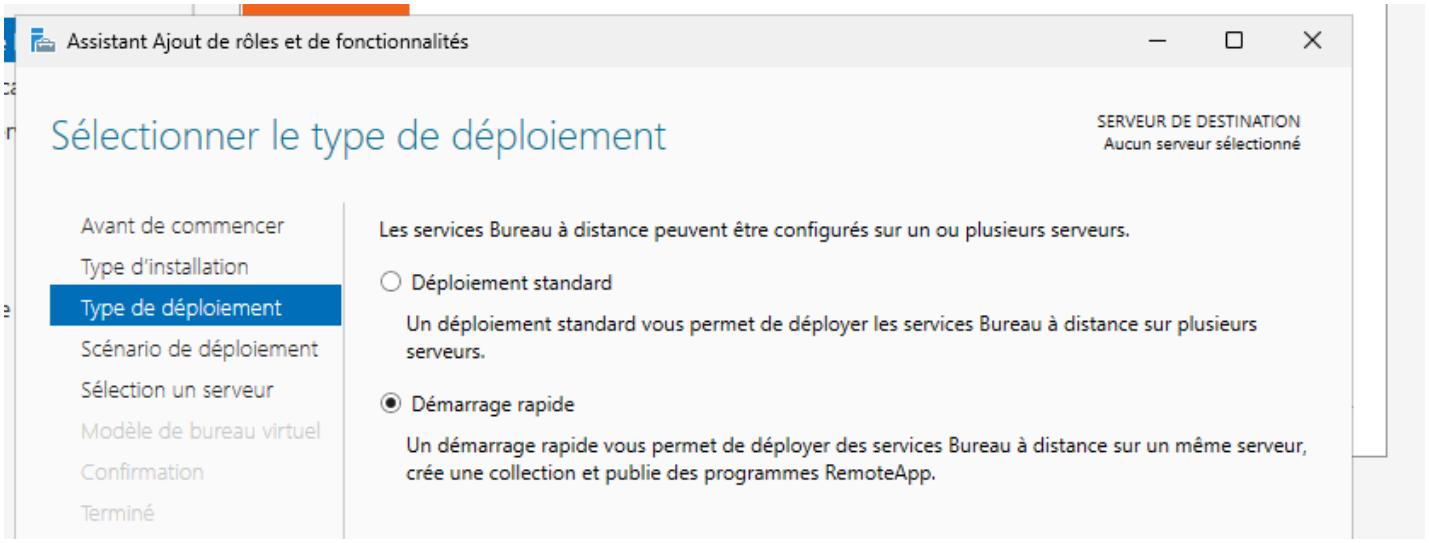
installe automatiquement l'ensemble des services RDS nécessaires : Service Broker, Accès Web et Hôte de session.



2 — Type de déploiement : Démarrage rapide

📷 2

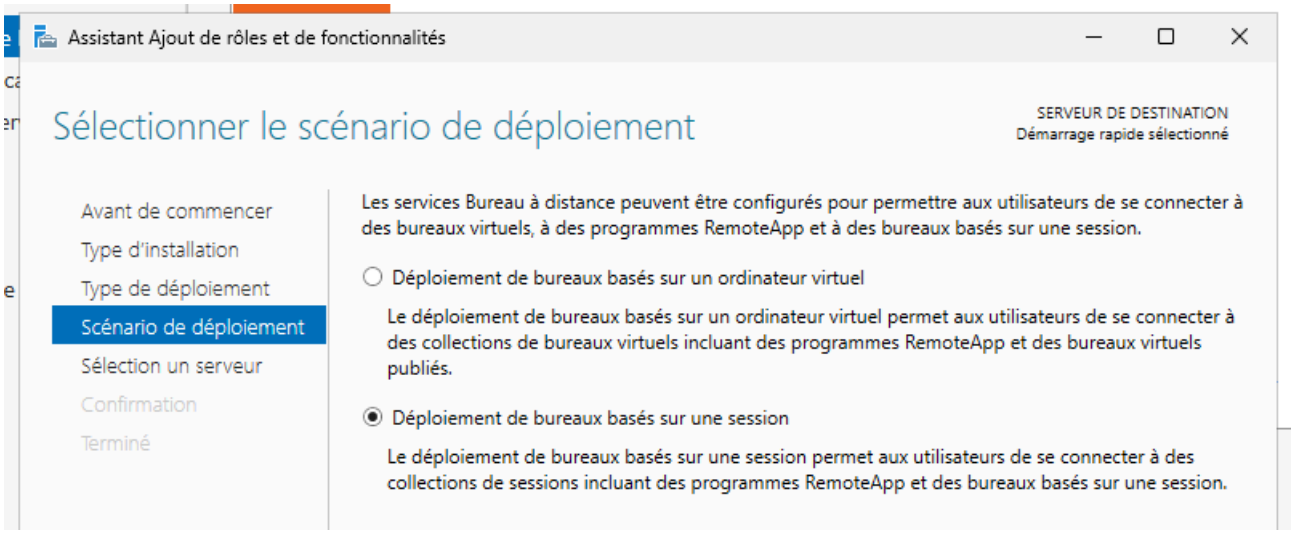
Configure automatiquement tous les composants RDS sur un seul serveur et crée une collection de sessions par défaut, ce qui est adapté à notre infrastructure monoserveur.



3 — Scénario de déploiement et sélection du serveur

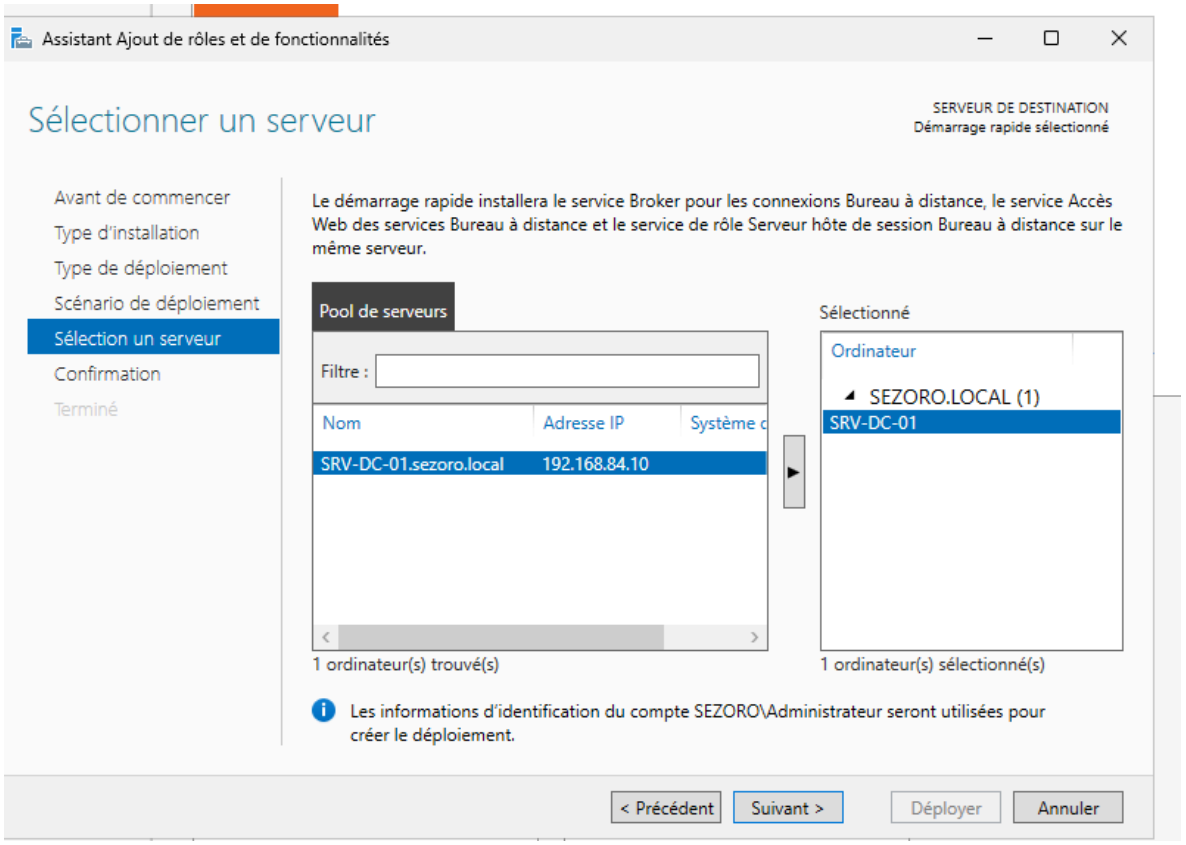
📷 3 — Bureaux basés sur une session

(Session-Based Desktop Deployment). Ce mode permet aux utilisateurs de se connecter à des sessions Windows hébergées sur le serveur, ce qui est la configuration standard pour le télétravail.



📷 3 — Sélection du serveur SRV-DC-01

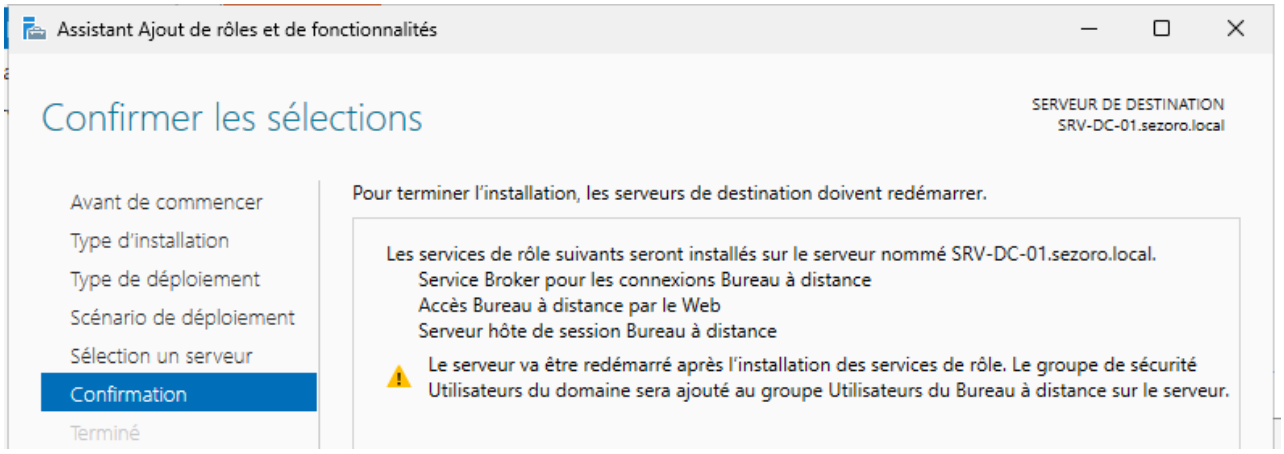
On sélectionne SRV-DC-01.sezoro.local (192.168.84.10) comme serveur de destination. Le système précise que les trois services RDS (Broker, Accès Web, Hôte de session) seront installés sur ce même serveur. On clique Suivant pour passer à la confirmation.

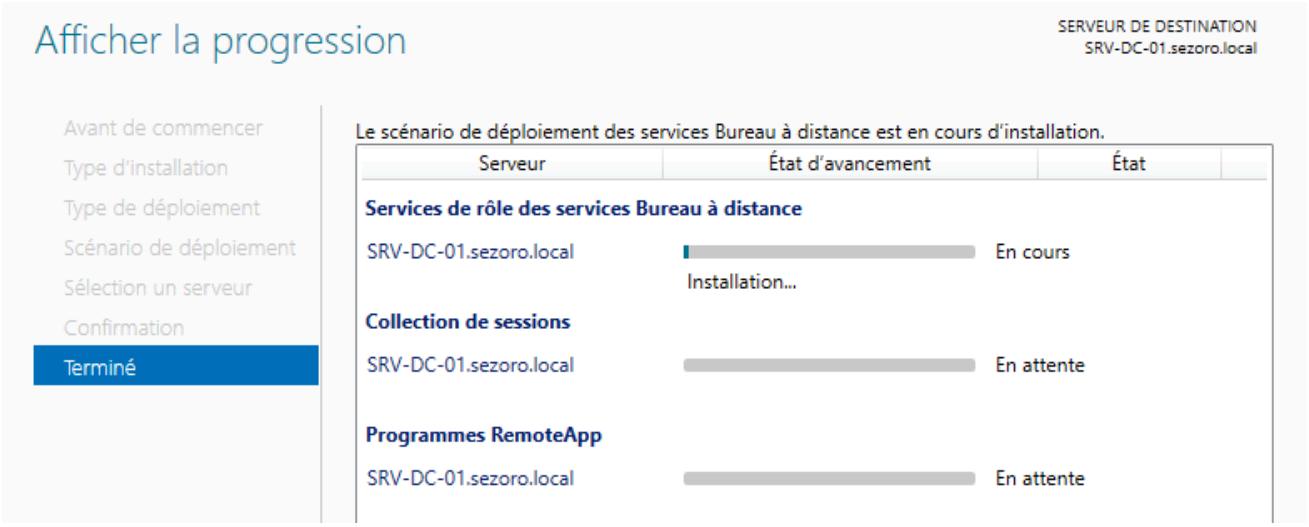


4 — Confirmation et progression de l'installation

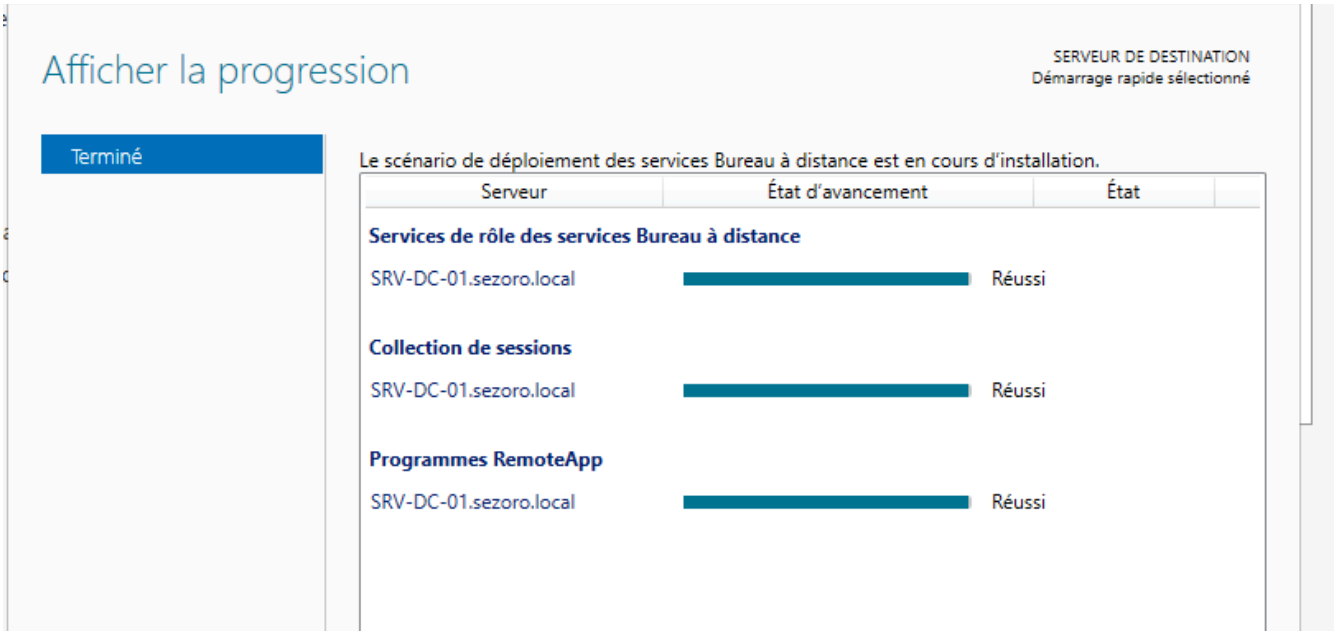
4

Les trois rôles qui seront installés : Service Broker pour les connexions, Accès Bureau à distance par le Web, et Serveur hôte de session. On coche "Redémarrer automatiquement le serveur si nécessaire" puis on clique Déployer.





Installation réussie

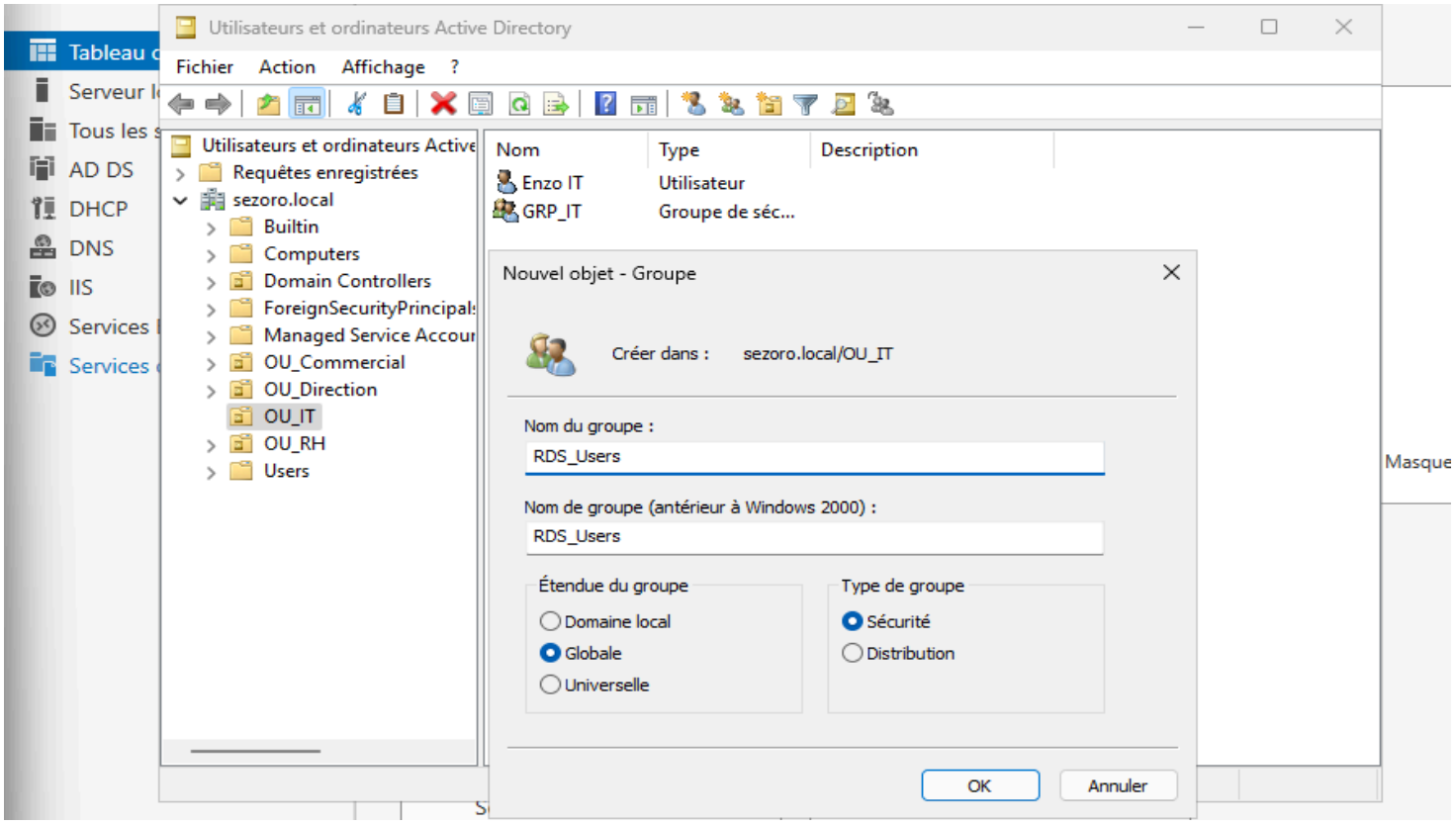


2. Vérification et création du groupe RDS_Users

5. Création du groupe RDS_Users.

Après le redémarrage du serveur, on vérifie que l'installation est réussie, puis on crée dans Active Directory le groupe de sécurité RDS_Users qui contrôlera les autorisations d'accès au bureau distant.

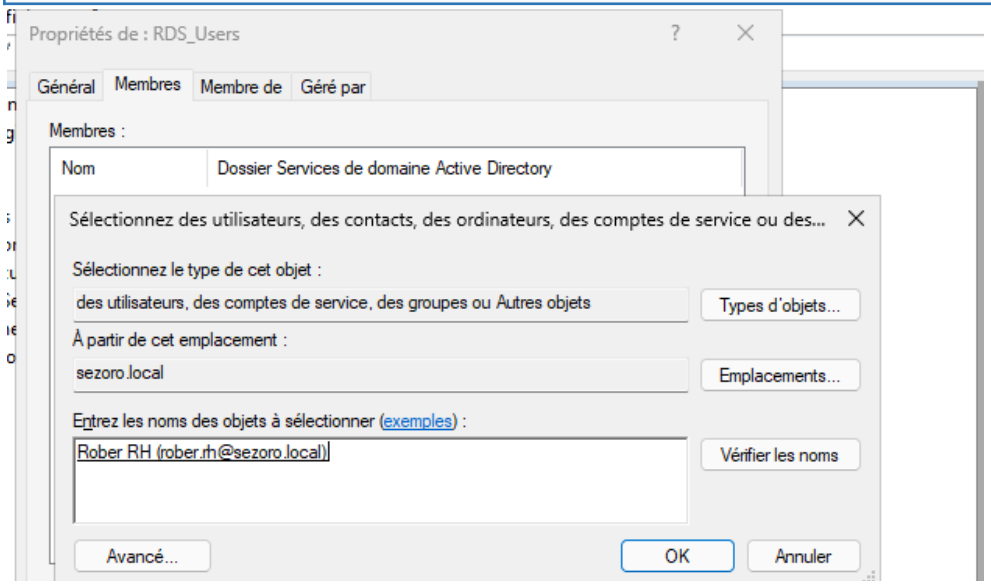
📷 5	Création du groupe RDS_Users dans OU_IT
Utilisateurs et ordinateurs Active Directory: on navigue vers sezoro.local > OU_IT. On crée un nouveau groupe nommé RDS_Users, de type Sécurité et d'étendue Globale. Ce groupe servira à contrôler précisément qui peut se connecter en RDS.	



6 — Ajout des membres dans RDS_Users

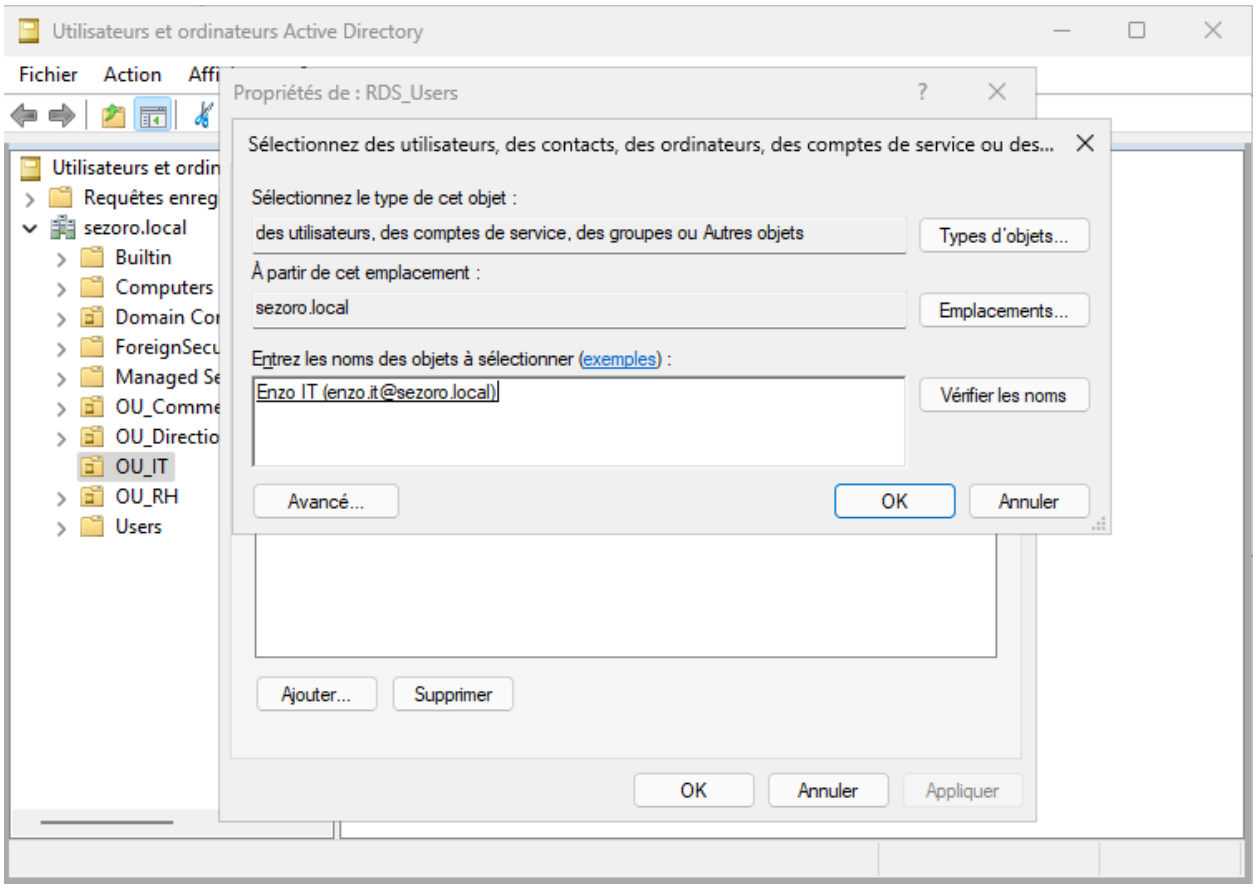
6 Ajout de Rober RH dans RDS_Users

Propriétés du groupe RDS_Users -> onglet Membres, on clique Ajouter et on recherche l'utilisateur Rober RH (rober.rh@sezoro.local). Cet utilisateur du service RH est autorisé à utiliser le bureau distant, ce qui lui permettra de télétravailler.



📷 6 Ajout de Enzo IT dans RDS_Users

On ajoute également Enzo IT (enzo.it@sezoro.local) dans le groupe RDS_Users. Le groupe contient maintenant deux membres autorisés : un utilisateur RH et un utilisateur IT, démontrant que la fonctionnalité est accessible à plusieurs services.



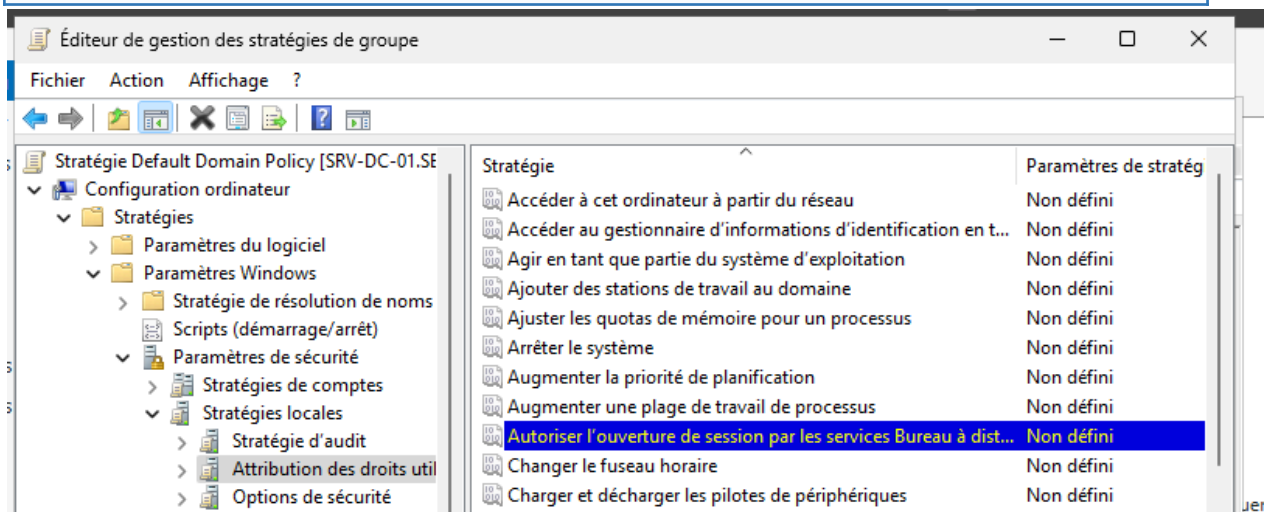
3. Configuration des autorisations RDS via GPO

L'autorisation de connexion RDS ne suffit pas seule. Il faut également configurer via la stratégie de groupe (GPO) le droit d'ouverture de session RDS, puis appliquer immédiatement la stratégie avec gpupdate.

7 — Configuration GPO : autoriser RDS_Users

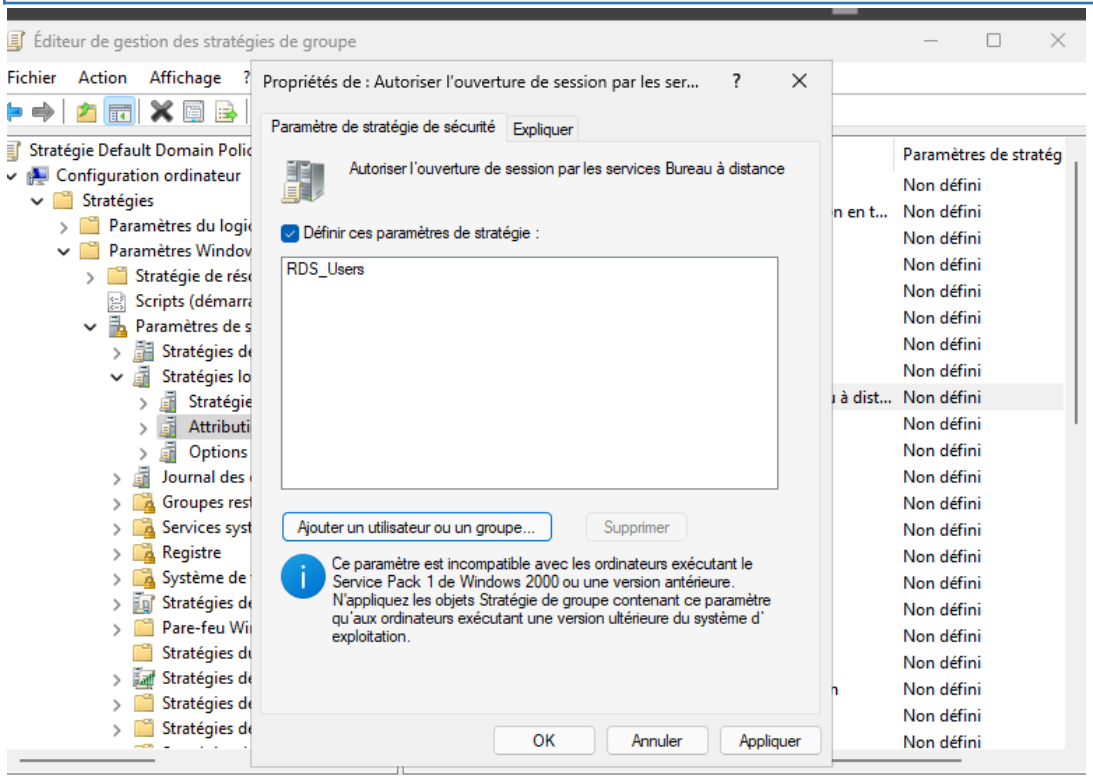
📷 7 Localisation du paramètre GPO dans l'éditeur

On ouvre l'Éditeur de gestion des stratégies de groupe sur la stratégie Default Domain Policy. On navigue vers : Configuration ordinateur >...

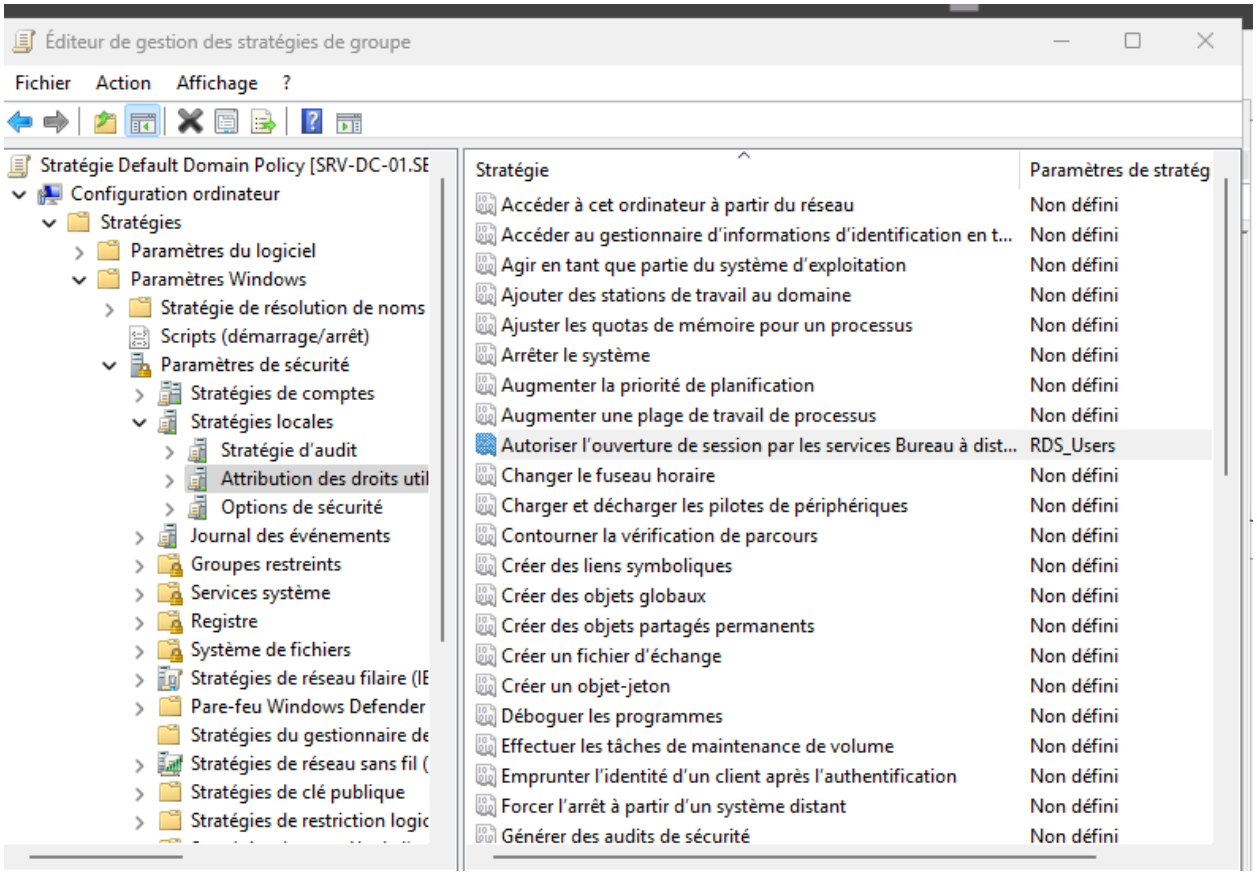


📷 7 Ajout de RDS_Users dans le paramètre GPO

On coche "Définir ces paramètres de stratégie" et on clique "Ajouter un utilisateur ou un groupe". On ajoute le groupe RDS_Users. Ce paramètre garantit que seuls les membres de ce groupe pourront ouvrir une session RDS, indépendamment des droits locaux du serveur.

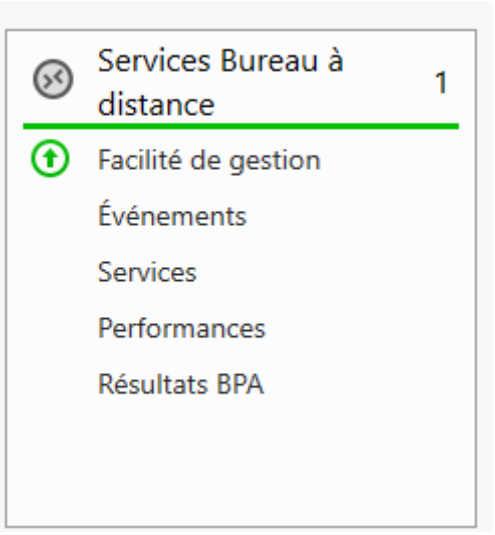


8 — Vérification GPO appliquée et rôle actif



8 Rôle Services Bureau à distance actif dans Server Manager

Cela confirme que le service est correctement installé et en cours d'exécution.

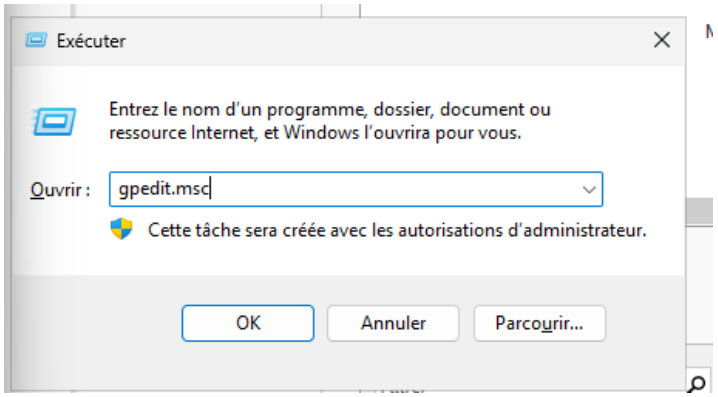


4. Limitation du nombre de connexions simultanées

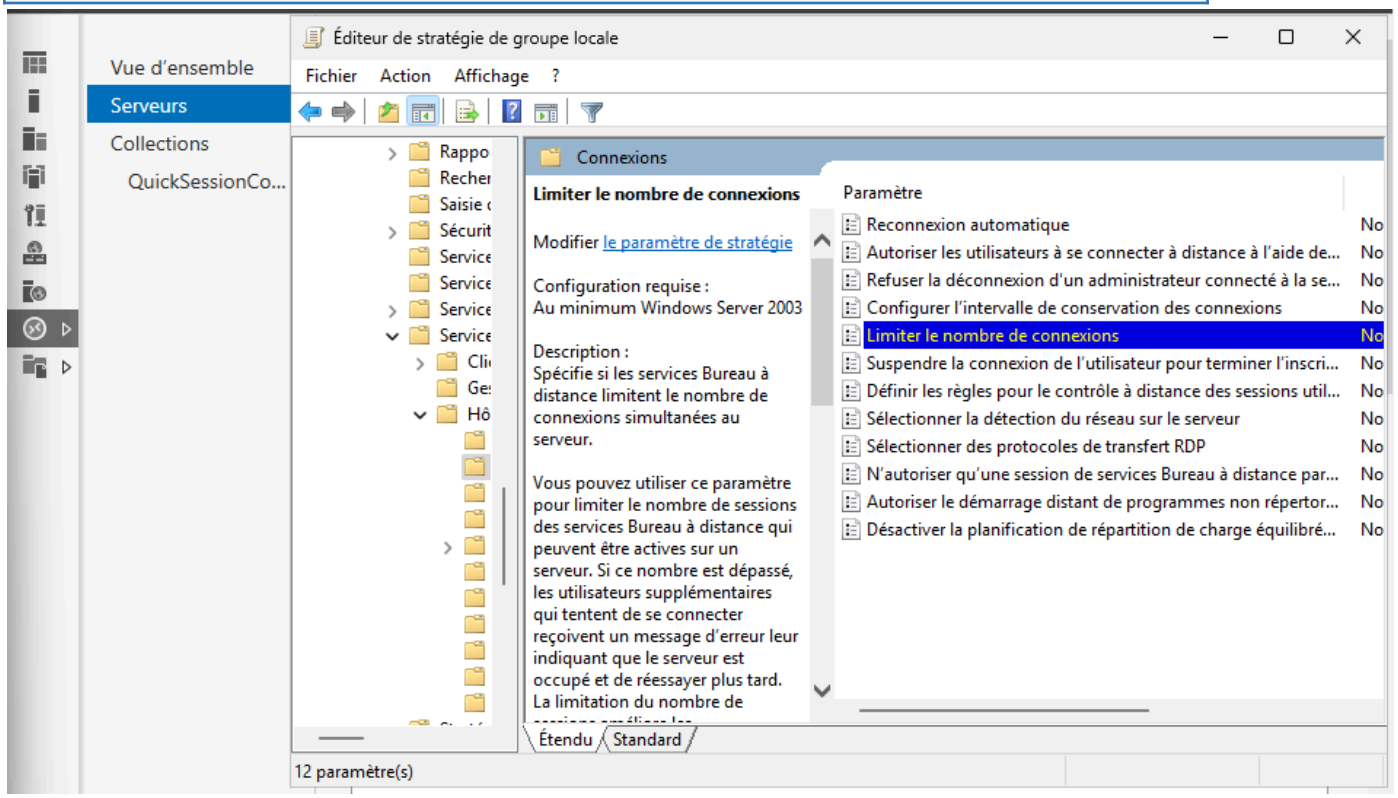
Pour sécuriser et optimiser les ressources du serveur, on configure via la stratégie de groupe locale du serveur RDS une limite maximale de connexions simultanées. Cette configuration se fait directement sur le serveur SRV-DC-01.

9 — Ouverture de gpedit.msc et navigation

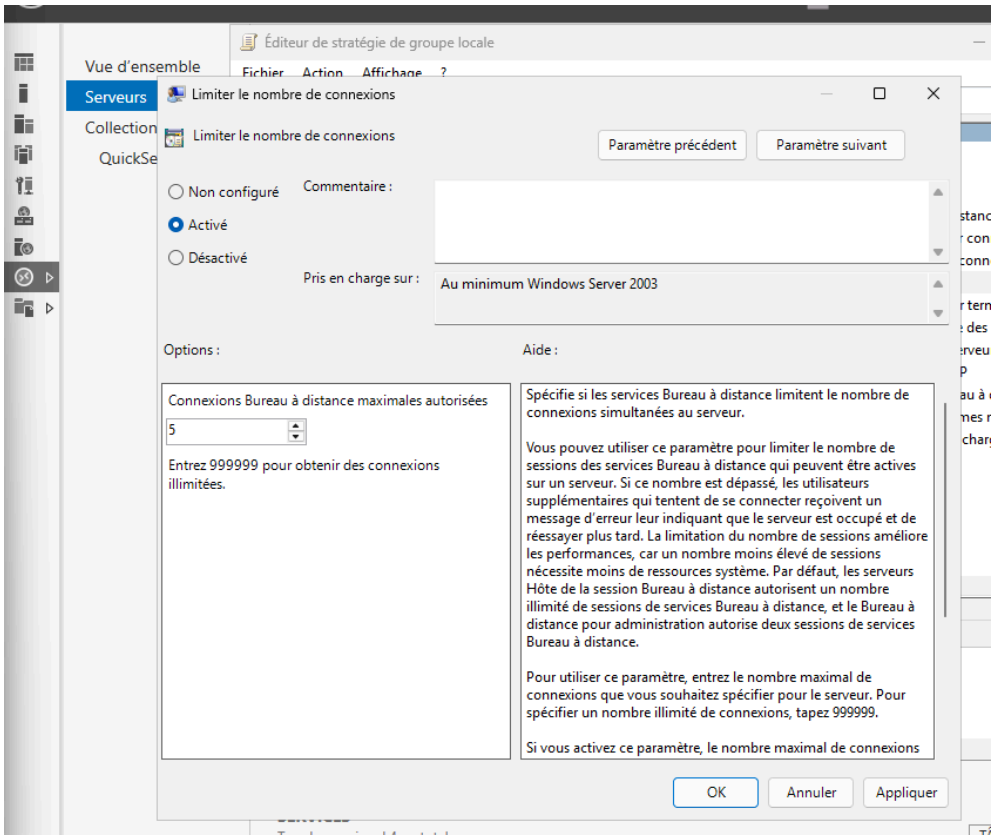
gpedit.msc = Local Group Policy Editor



9 Navigation vers le paramètre Connexions RDS

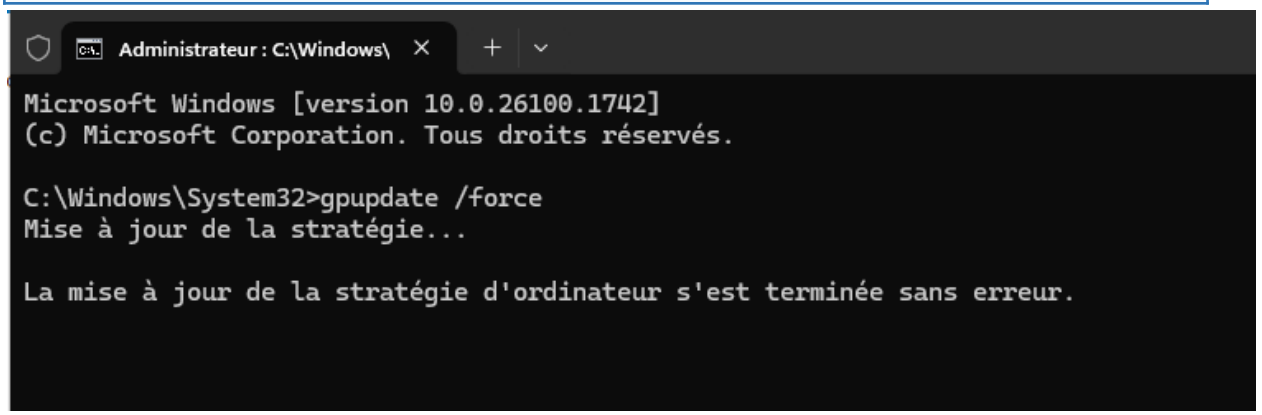


10 — Activation de la limite et gpupdate (5)



📷 10 Forcer l'application des stratégies avec gpupdate /force

Cela garantit que toutes les stratégies GPO sont immédiatement appliquées sans attendre le prochain cycle automatique.



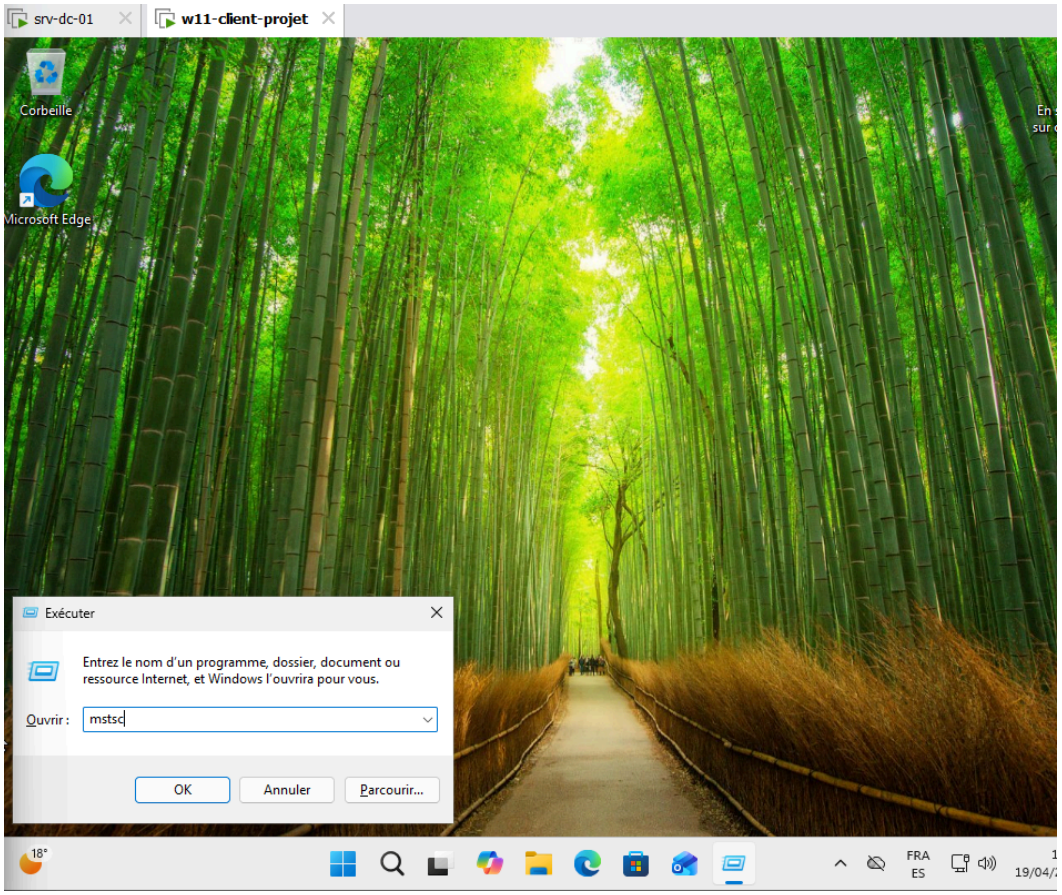
5. Test de connexion RDS — Utilisateur autorisé

On teste maintenant la connexion RDS depuis le poste client w11-client-projet avec l'utilisateur Rober RH, qui est membre du groupe RDS_Users. Ce test valide que la configuration fonctionne correctement pour un utilisateur autorisé.

11 — Lancement de mstsc depuis le client (connecté en tant que Rober RH)

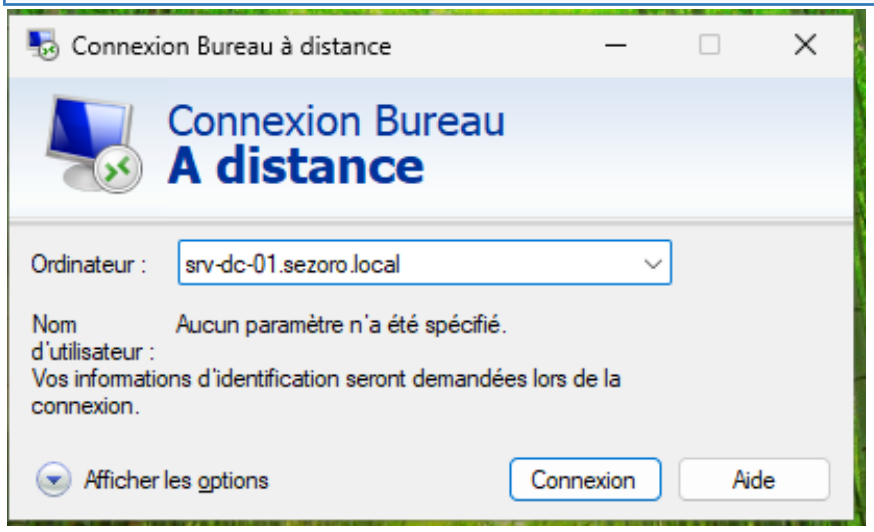
sezoro\rober.rh

mstsc = Microsoft Terminal Services Client



11 — Saisie de l'adresse du serveur

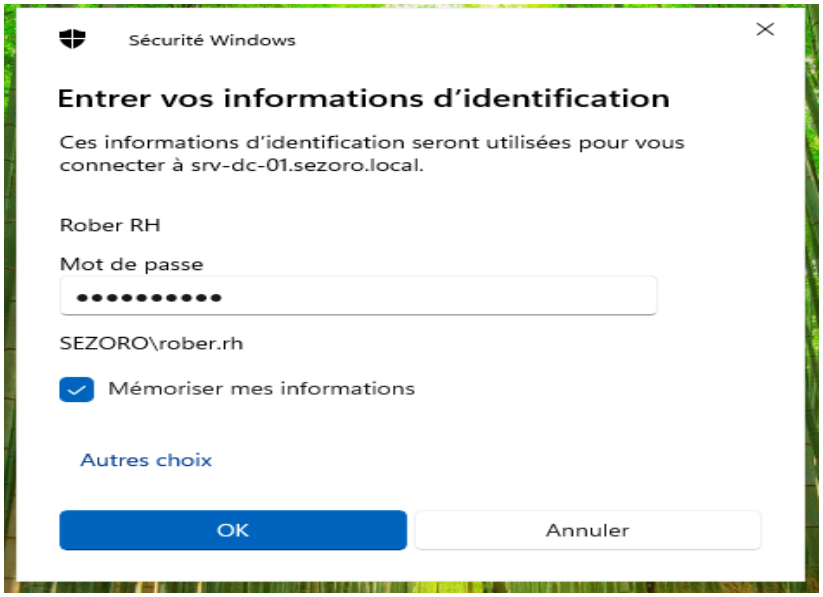
Dans la fenêtre Connexion Bureau à distance, on entre l'adresse srv-dc-01.sezoro.local dans le champ Ordinateur. On aurait aussi pu utiliser l'adresse IP 192.168.84.10. On clique Connexion pour initier la connexion RDS.



12 — Authentification de l'utilisateur Rober RH

📷 12	Fenêtre d'authentification Windows Security

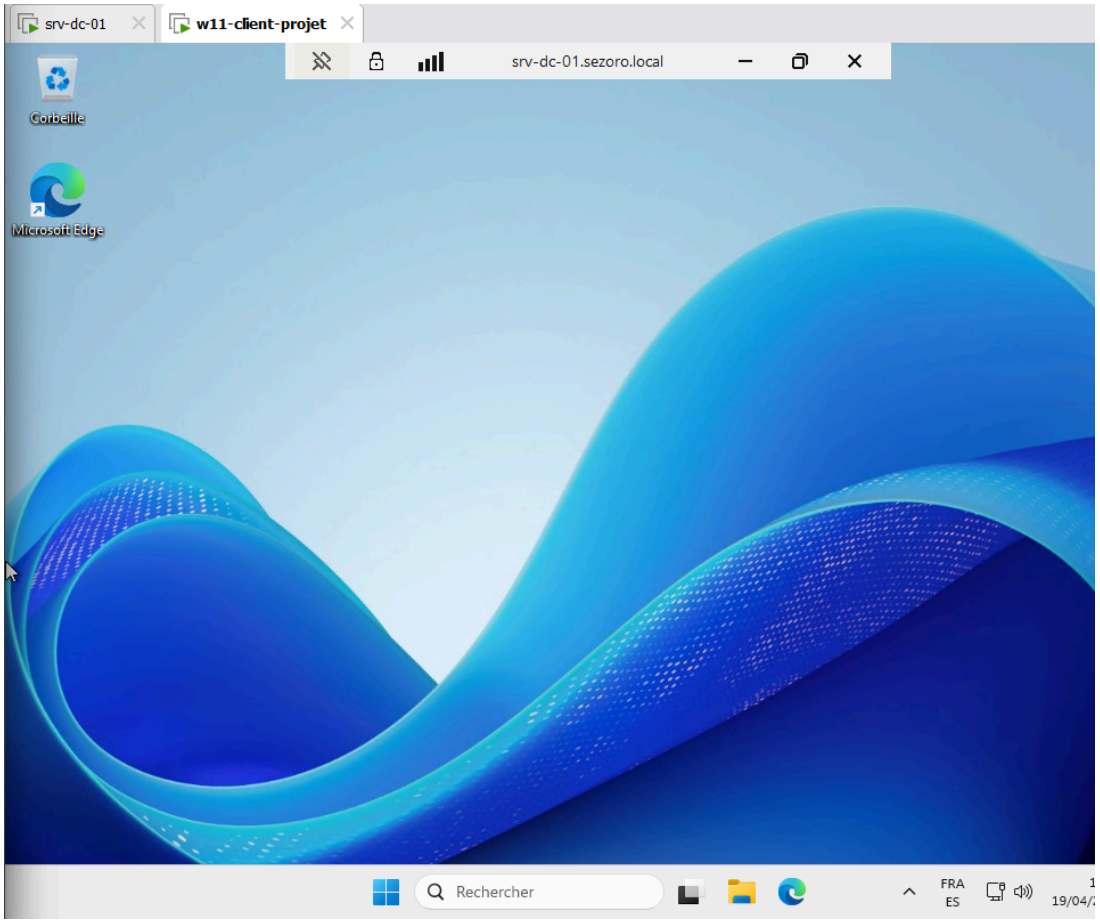
Une fenêtre de sécurité Windows s'ouvre pour demander les identifiants. L'utilisateur Rober RH entre son mot de passe. Le compte affiché est SEZORO\rober.rh, ce qui confirme que l'authentification se fait bien contre le domaine Active Directory sezoro.local.

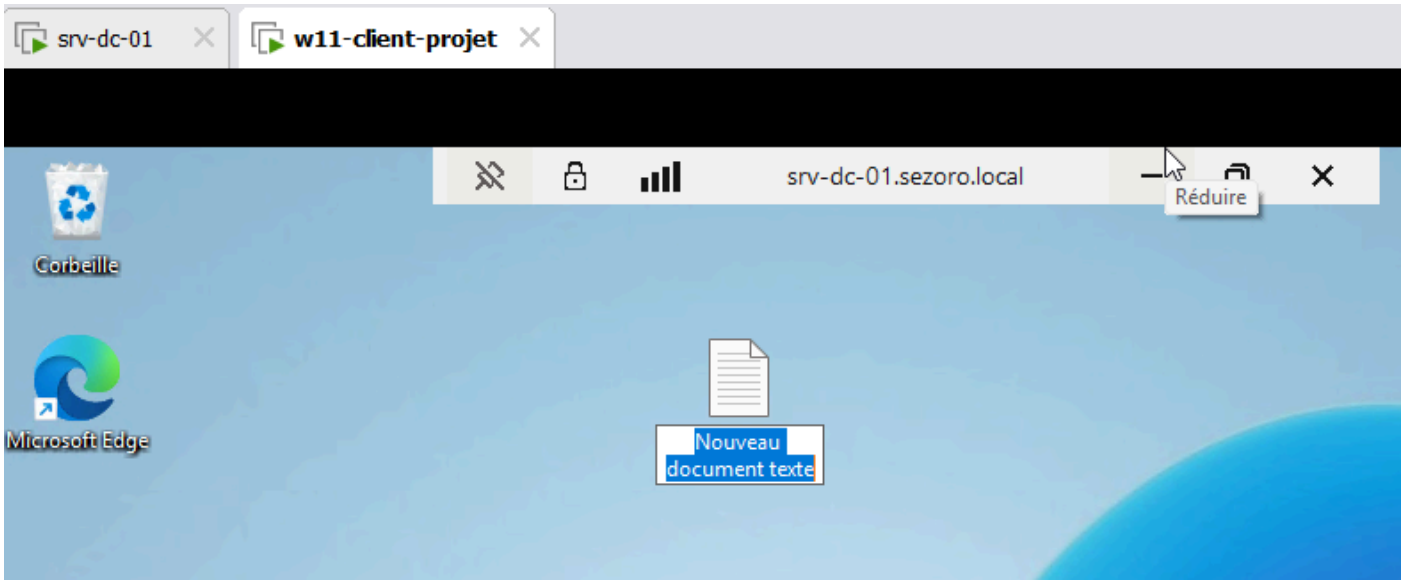


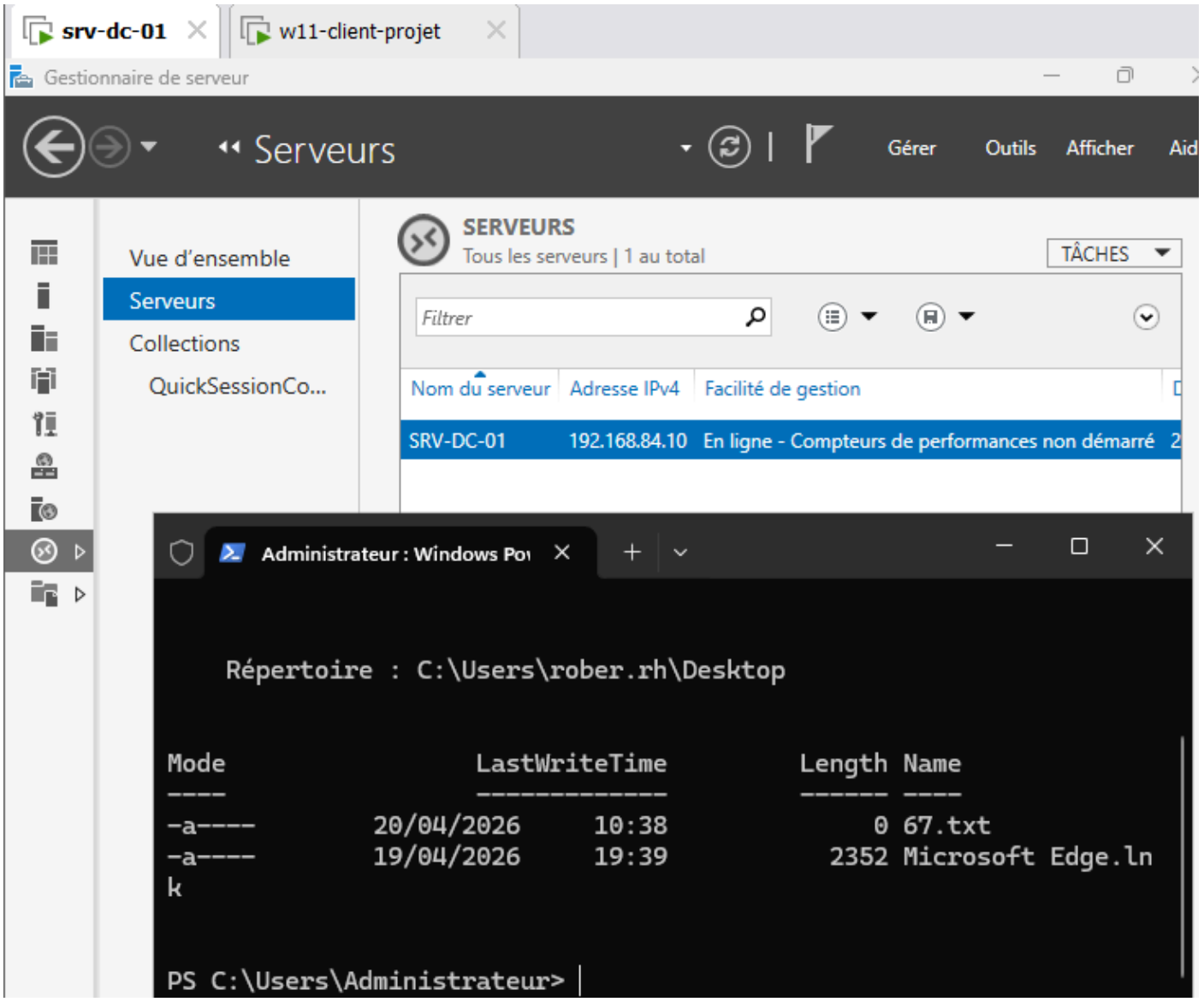
13 — Bureau distant obtenu avec succès

📷 13	Bureau distant de SRV-DC-01 ouvert avec succès

La connexion RDS est établie. On voit le bureau de SRV-DC-01.sezoro.local s'afficher dans une fenêtre distante



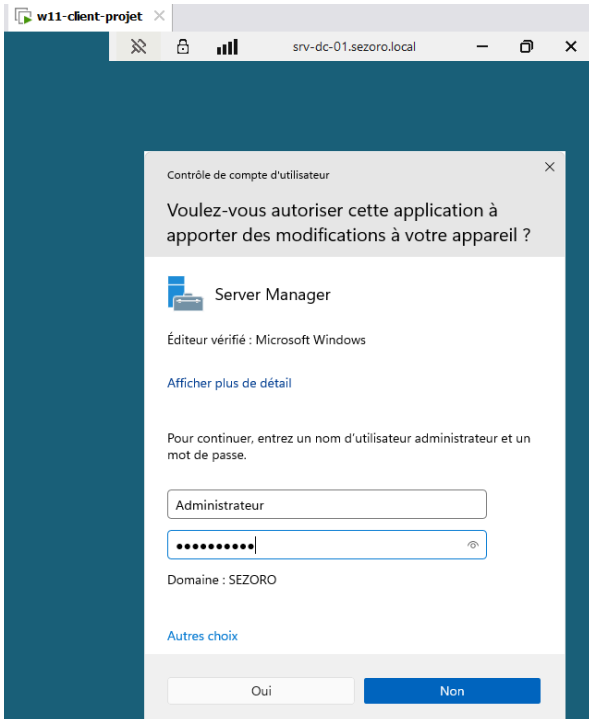

srv-dc-01
w11-client-projet
srv-dc-01.sezoro.local
Réduire
Corbeille
Microsoft Edge
Nouveau
document texte


srv-dc-01
w11-client-projet
Gestionnaire de serveur
Serveurs
Gérer
Outils
Afficher
Vue d'ensemble
Serveurs
Collections
QuickSessionCo...
SERVEURS
Tous les serveurs | 1 au total
TÂCHES
Filtrer
Nom du serveur
Adresse IPv4
Facilité de gestion
SRV-DC-01
192.168.84.10
En ligne - Compteurs de performances non démarré
Administrateur : Windows Po
Répertoire : C:\Users\rober.rh\Desktop
Mode
LastWriteTime
Length
Name
-a----
20/04/2026
10:38
0
67.txt
-a----
19/04/2026
19:39
2352
Microsoft Edge.lnk
PS C:\Users\Administrateur>

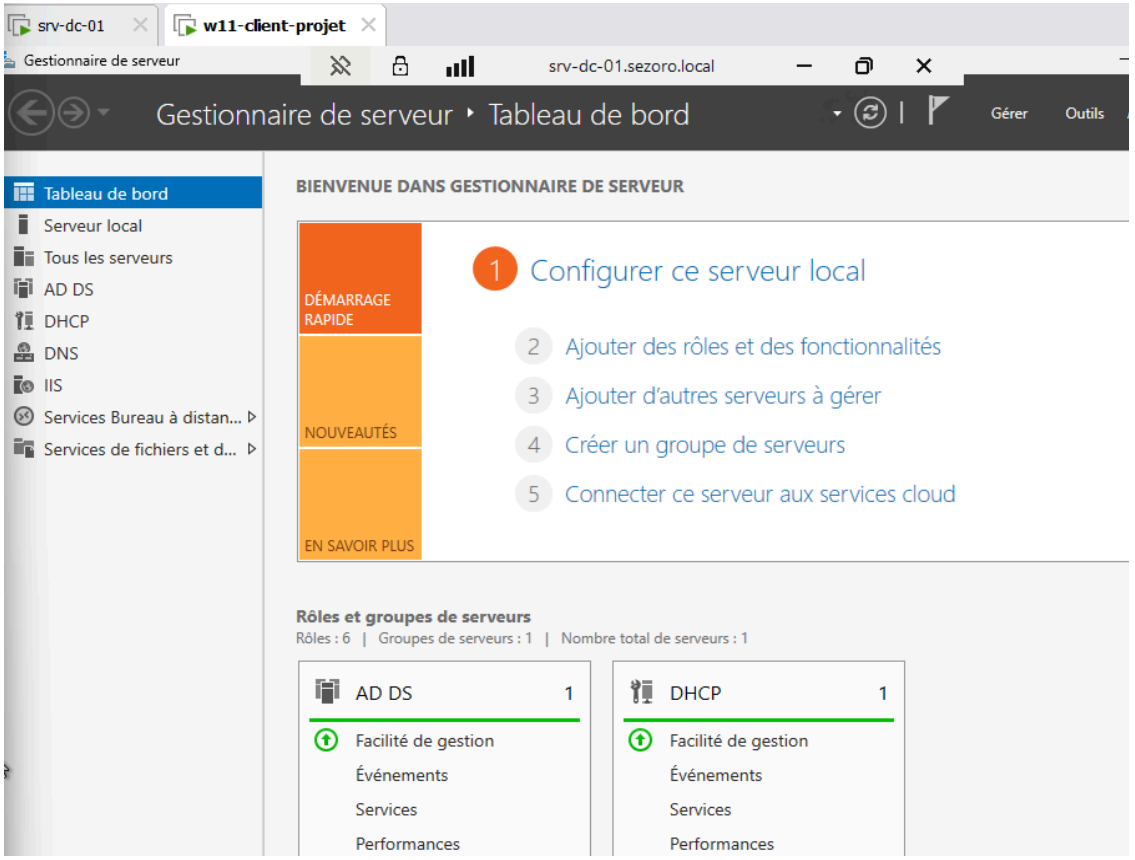
14 — Accès au Server Manager depuis la session RDS

📷 14 — Contrôle UAC lors d'une élévation de privilèges

Le système demande les identifiants d'un administrateur (compte Administrateur du domaine SEZORO) pour autoriser l'action, ce qui confirme que l'utilisateur RH dispose bien de droits limités, même en session distante.



15 - Vue du Gestionnaire de serveur depuis la session RDS autorisée



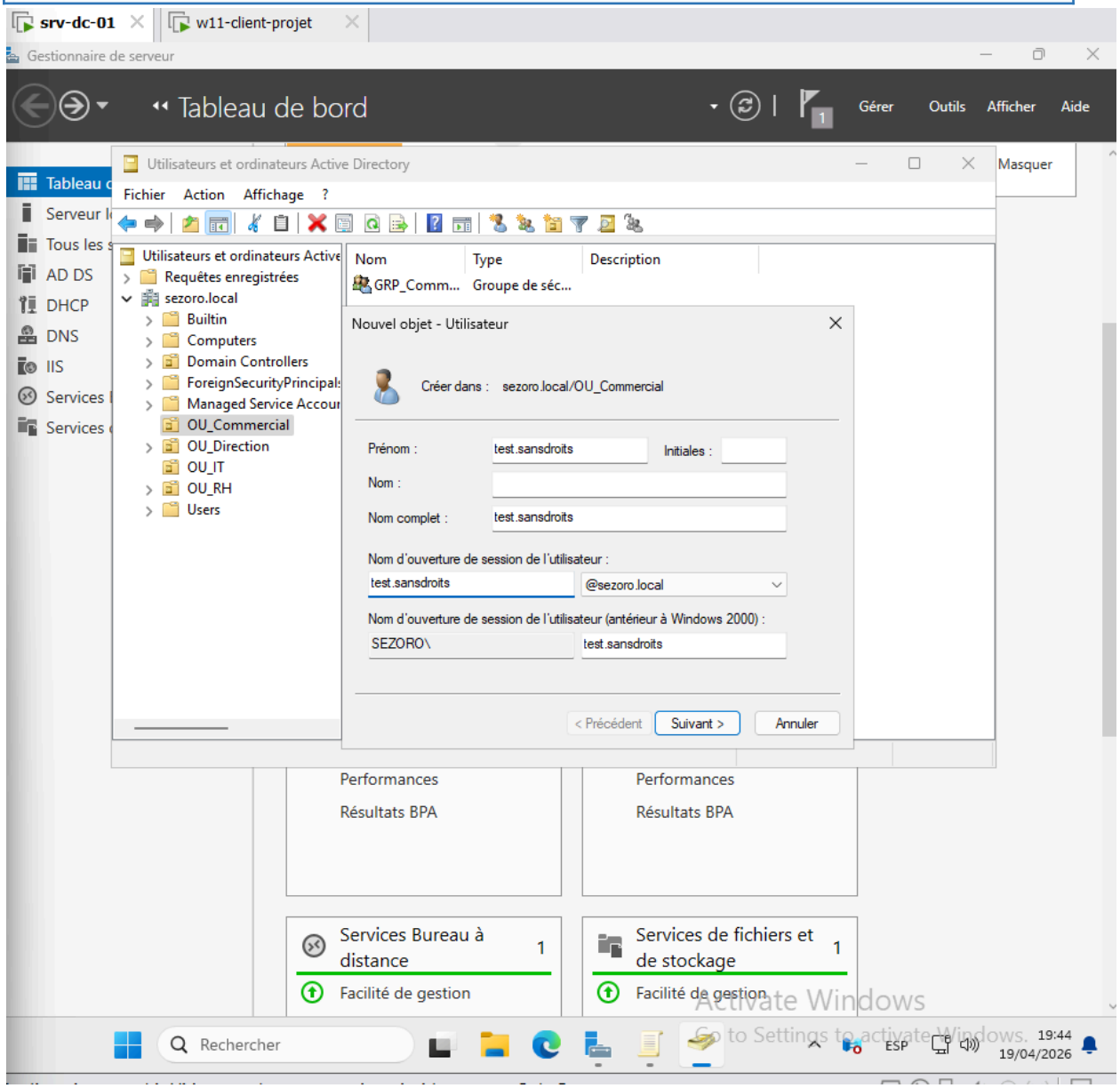
6. Test de refus RDS — Utilisateur non autorisé

Pour valider que la restriction fonctionne, on crée un utilisateur test.sansdroits qui n'est pas membre du groupe RDS_Users, et on tente une connexion RDS avec ce compte. Le serveur doit refuser l'accès.

16 — Création de l'utilisateur test.sansdroits

📷 16 — Création de l'utilisateur test.sansdroits dans OU_Commercial

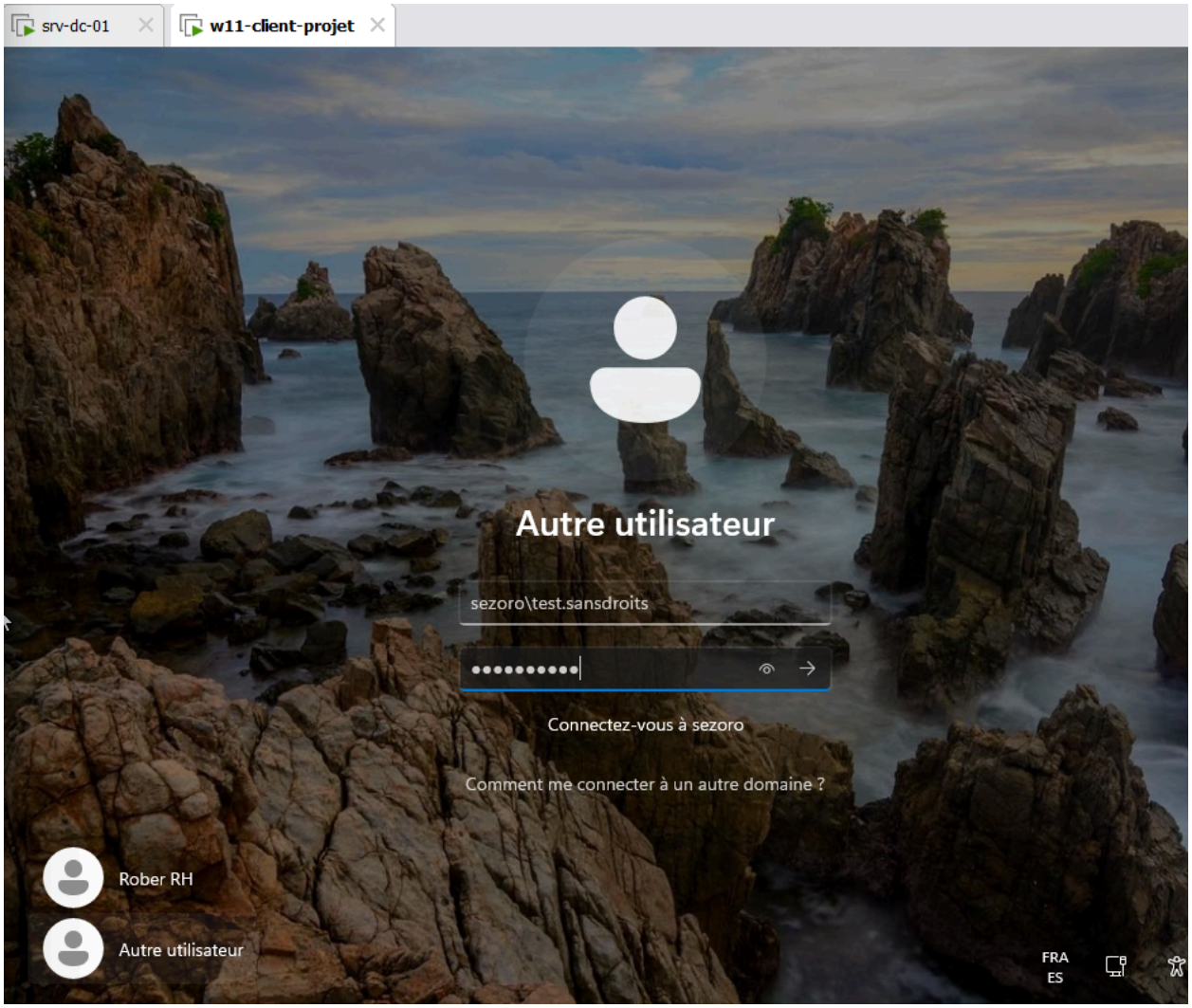
Pour le test de refus, on crée dans Active Directory un nouvel utilisateur nommé test.sansdroits, placé dans l'OU_Commercial. Cet utilisateur n'est ajouté à aucun groupe particulier et surtout pas au groupe RDS_Users, ce qui signifie qu'il ne devrait pas avoir accès au bureau distant.

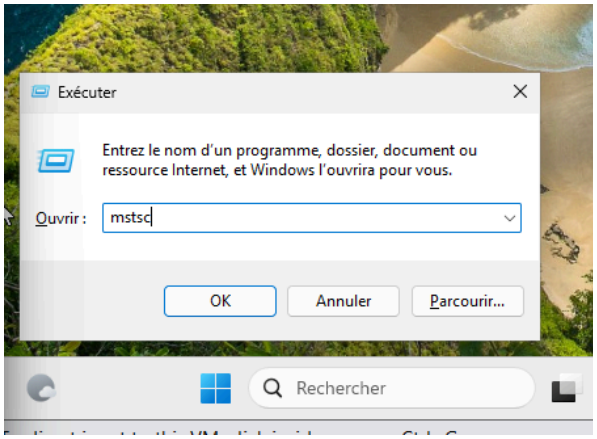


17 — Tentative de connexion de test.sansdroits

📷 17	Connexion sur le poste client avec test.sansdroits

Sur le poste w11-client-projet, on se connecte avec le compte sezoro\test.sansdroits. On voit l'écran de connexion Windows avec Rober RH déjà listé et un autre utilisateur en cours de saisie. Une fois connecté sur le poste, on ouvre mstsc (boîte Exécuter visible en bas à gauche).

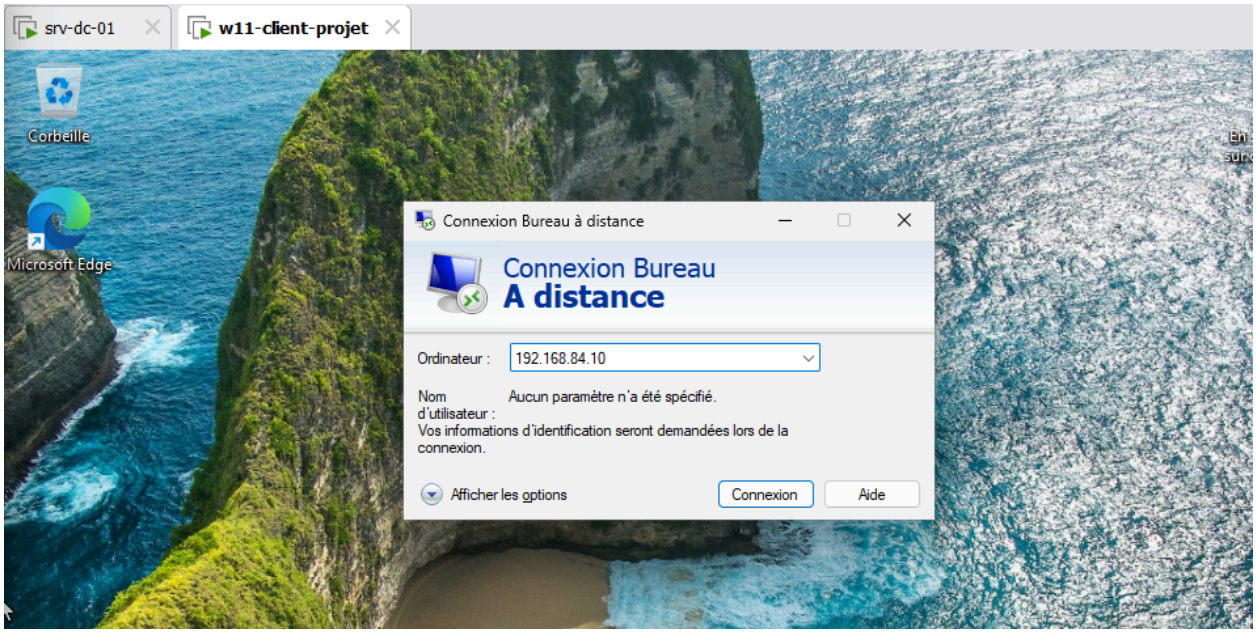




18 — Saisie des identifiants pour la tentative RDS

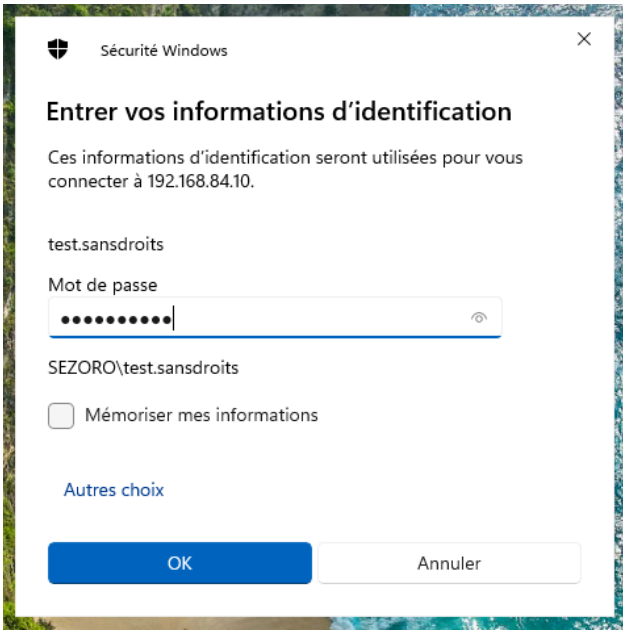
18 Connexion Bureau à distance vers 192.168.84.10

Dans la Connexion Bureau à distance, on entre l'adresse IP du serveur (192.168.84.10). On clique Connexion. La tentative de connexion est initiée avec le compte test.sansdroits.



18 Fenêtre d'identification avec test.sansdroits

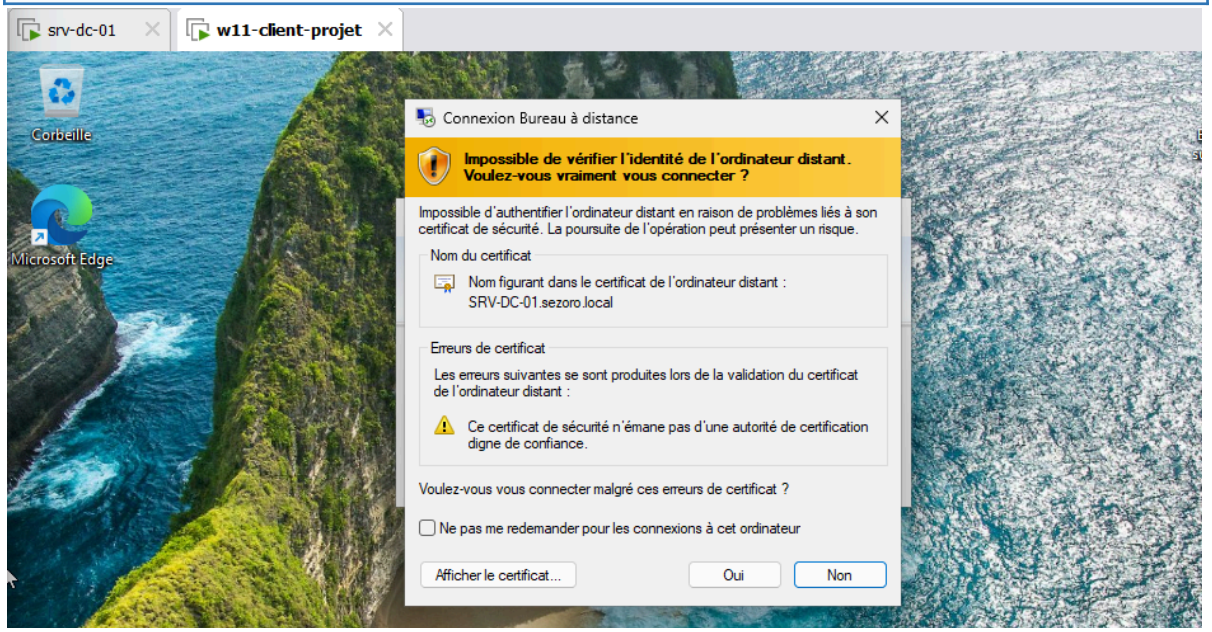
La fenêtre de sécurité Windows s'ouvre et affiche le compte SEZORO\test.sansdroits. L'utilisateur entre son mot de passe et clique OK. La demande de connexion RDS est envoyée au serveur.



19 — Avertissement certificat (normale)

📷 19	Avertissement de certificat non reconnu

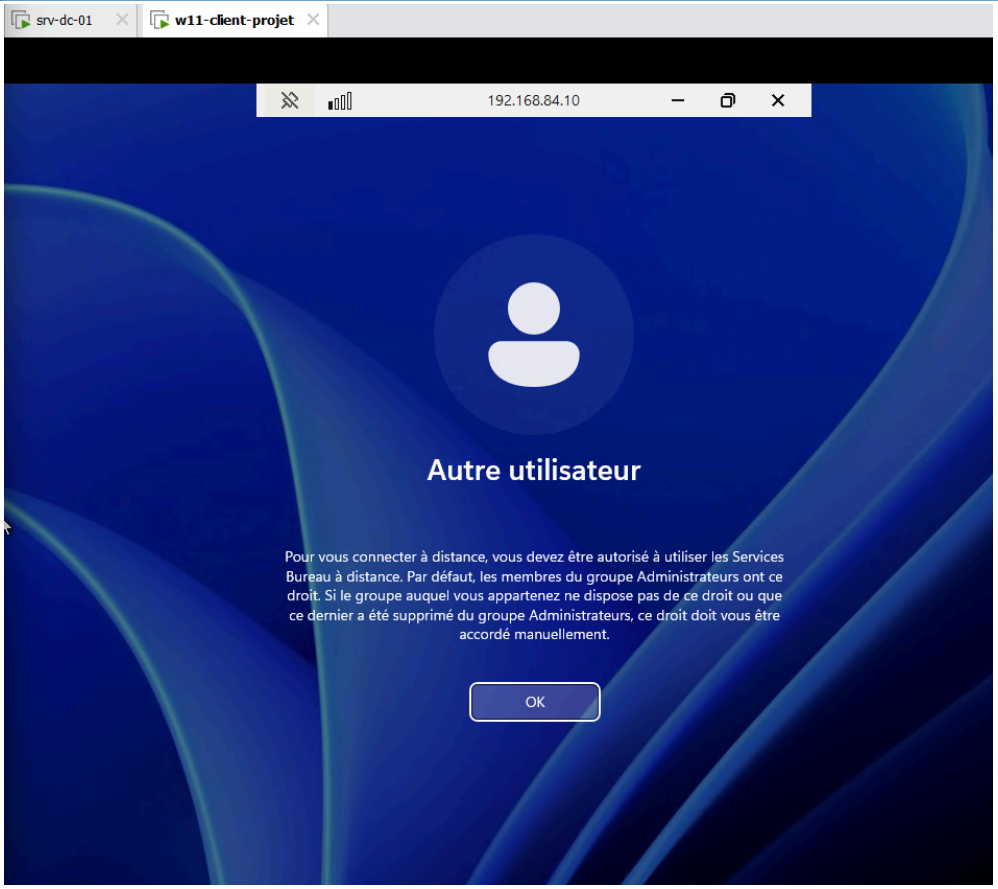
Windows affiche un avertissement indiquant que le certificat de SRV-DC-01.sezoro.local ne peut pas être vérifié. Ceci est normal dans un environnement lab sans autorité de certification d'entreprise



20 — Refus de connexion RDS : test réussi

📷 20	REFUS : l'accès RDS est bien bloqué pour test.sansdroits

Ce message confirme que la restriction GPO fonctionne parfaitement : seuls les membres du groupe RDS_Users (Rober RH et Enzo IT) peuvent se connecter.



Récapitulatif des étapes

#	Étape	Action réalisée	Résultat
1-4	**Installation rôle RDS**	Démarrage rapide, session-based, SRV-DC-01	**Réussi ✓**
5	**Création groupe RDS_Users**	Groupe Sécurité Globale dans OU_IT	**Réussi ✓**
6	**Ajout membres RDS_Users**	Rober RH + Enzo IT ajoutés	**Réussi ✓**
7-8	**GPO autorisation RDS**	Default Domain Policy > Attribution droits	**Réussi ✓**
9-10	**Limite connexions simultanées**	5 connexions max via gpedit.msc + gpupdate	**Réussi ✓**
11-14	**Test utilisateur autorisé**	Rober RH connecté en RDS sur srv-dc-01	**Réussi ✓**
15-20	**Test utilisateur refusé**	test.sansdroits bloqué avec message d'erreur	**Réussi ✓**

- Résultats obtenus :

- Validation : Un utilisateur membre du groupe accède avec succès à son bureau distant.
- Sécurité : Toute tentative de connexion par un utilisateur non membre du groupe est automatiquement rejetée.

- Avantages :

- Réduction des coûts matériels (PC clients légers).
- Sécurisation des données (rien n'est stocké en local sur le PC de l'employé).
- Administration centralisée des applications.

Les difficultés rencontrées

La mise en place de cette infrastructure complexe nous a confrontés à plusieurs défis techniques :

1. **Conflits de SID lors du clonage :** Lors de la création de IIS1 et IIS2 à partir d'une machine virtuelle de base, nous avons rencontré des erreurs d'intégration au domaine. Nous avons dû utiliser l'outil **Sysprep** pour généraliser l'image et générer des identifiants de sécurité uniques pour chaque serveur.
2. **Blocages du Pare-feu (Firewall) :** Initialement, le PC Client ne parvenait pas à afficher les pages Web des serveurs IIS. Après diagnostic, nous avons identifié que le pare-feu Windows bloquait le trafic HTTP. La désactivation du Firewall sur les serveurs de test a résolu le problème.
3. **Application des GPO :** Certaines restrictions ne s'appliquaient pas immédiatement sur le poste client. Nous avons dû forcer la mise à jour via la commande gpupdate /force et effectuer plusieurs redémarrages pour valider les paramètres.