

BRETON Théo

Projet N°5 : PROJET SMARTHOME

Active Directory • DHCP • DNS • RADIUS Cisco • IIS Web Server • FortiGate Security • BGInfo



Contexte :

La société SMARTHOME, acteur majeur de la vente d'objets connectés et de solutions domotiques, souhaite moderniser son infrastructure technique. Actuellement dépourvue de gestion centralisée, l'entreprise doit sécuriser son site web marchand tout en structurant son réseau interne pour accompagner sa croissance.

Votre mission sera de mettre en place le contrôleur de domaine de l'entreprise en installant le rôle ADDS sur un serveur Windows Server 2022. De plus, il faudra gérer la partie DHCP pour l'adressage dynamique du parc informatique de l'entreprise. Il faudra créer des utilisateurs pour les services de Direction et du Bureau Administrateur Réseau, mais également assurer la gestion des GPOs pour le mappage des lecteurs réseau, les dossiers communs aux services et les dossiers personnels des utilisateurs. De plus, il faudra mettre en place BGINFO afin d'afficher sur le bureau des utilisateurs les informations de la machine.

Vous mettrez en place sur le serveur ADDS le protocole RADIUS via le rôle NPS (Network Policy Server) afin de gérer les authentifications SSH sur les équipements Cisco du réseau local de SMARTHOME. Vous configurerez également le protocole 802.1X sur les ports non utilisés des commutateurs afin qu'aucun attaquant externe ne puisse obtenir une adresse IP du serveur DHCP de l'entreprise.

Pour mettre en lumière l'image de l'entreprise, vous mettrez en place un serveur hébergeant le rôle IIS pour l'hébergement du site web marchand de l'entreprise, placé en DMZ. Le site web devra être accessible depuis internet. Pour protéger le réseau local et la DMZ, vous mettrez en œuvre les règles de filtrage sur le pare-feu Fortinet afin de contrôler les flux entrants et sortants entre les différentes zones du réseau.

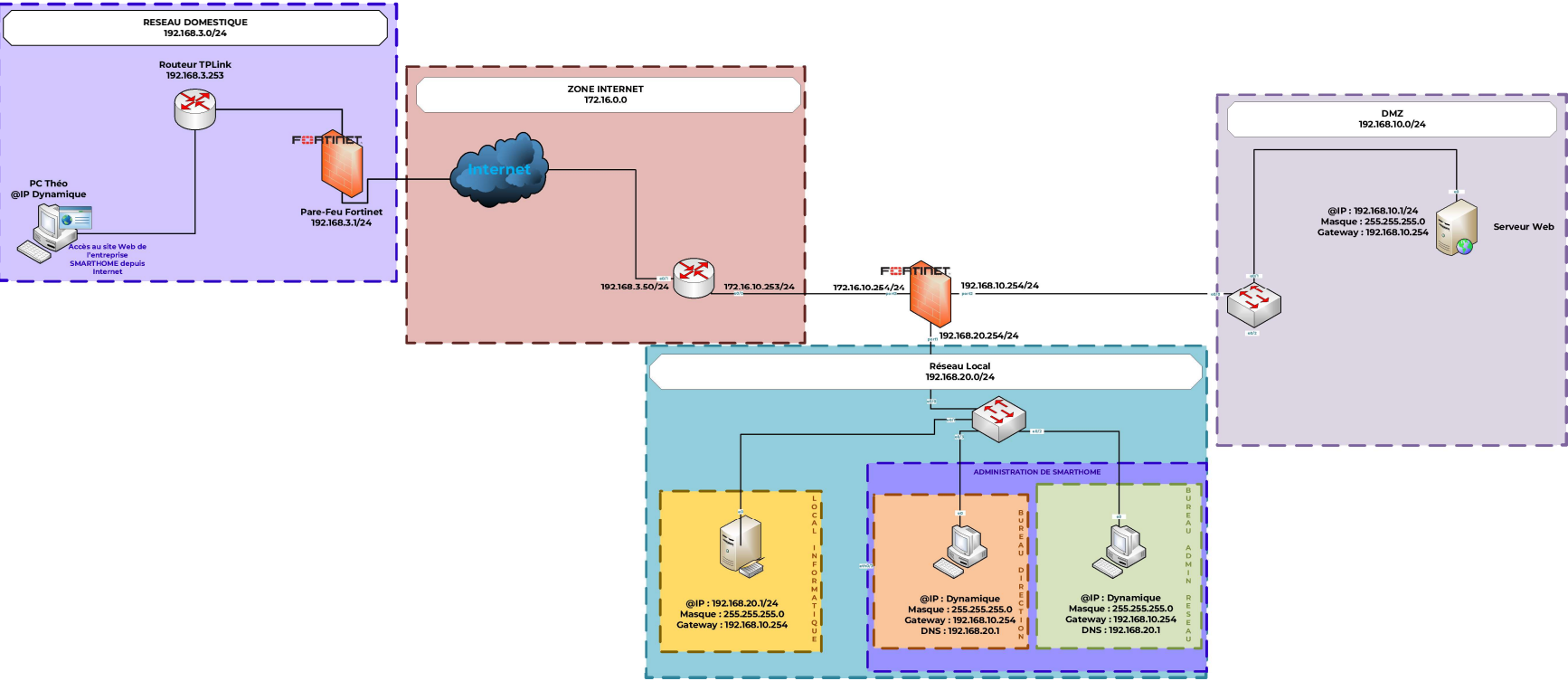
Schéma réseau :



PROJET N°5 – BRETON THEO – SIO1 – EVE_NG



La société SMARTHOME, acteur majeur de la vente d'objets connectés et de solutions domotiques, souhaite moderniser son infrastructure technique. Actuellement dépourvue de gestion centralisée, l'entreprise doit sécuriser son site web marchand tout en structurant son réseau interne pour accompagner sa croissance.



Lettre de mission – Entreprise SMARTHOME

La société SMARTHOME, acteur majeur de la vente d'objets connectés et de solutions domotiques, souhaite moderniser son infrastructure technique. Actuellement dépourvue de gestion centralisée, l'entreprise doit sécuriser son site web marchand tout en structurant son réseau interne pour accompagner sa croissance.

Votre mission sera de mettre en place le contrôleur de domaine de l'entreprise en installant le rôle ADDS sur un serveur Windows Server 2022. De plus, il faudra gérer la partie DHCP pour l'adressage dynamique du parc informatique de l'entreprise. Il faudra créer des utilisateurs pour les services de Direction et du Bureau Administrateur Réseau, mais également assurer la gestion des GPOs pour le mappage des lecteurs réseau, les dossiers communs aux services et les dossiers personnels des utilisateurs. De plus, il faudra mettre en place BGINFO afin d'afficher sur le bureau des utilisateurs les informations de la machine.

Vous mettrez en place sur le serveur ADDS le protocole RADIUS via le rôle NPS (Network Policy Server) afin de gérer les authentifications SSH sur les équipements Cisco du réseau local de SMARTHOME. Vous configurerez également le protocole 802.1X sur les ports non utilisés des commutateurs afin qu'aucun attaquant externe ne puisse obtenir une adresse IP du serveur DHCP de l'entreprise.

Pour mettre en lumière l'image de l'entreprise, vous mettrez en place un serveur hébergeant le rôle IIS pour l'hébergement du site web marchand de l'entreprise, placé en DMZ. Le site web devra être accessible depuis internet.

Pour protéger le réseau local et la DMZ, vous mettrez en œuvre les règles de filtrage sur le pare-feu Fortinet afin de contrôler les flux entrants et sortants entre les différentes zones du réseau.

Alexandre Martin
A. Martin

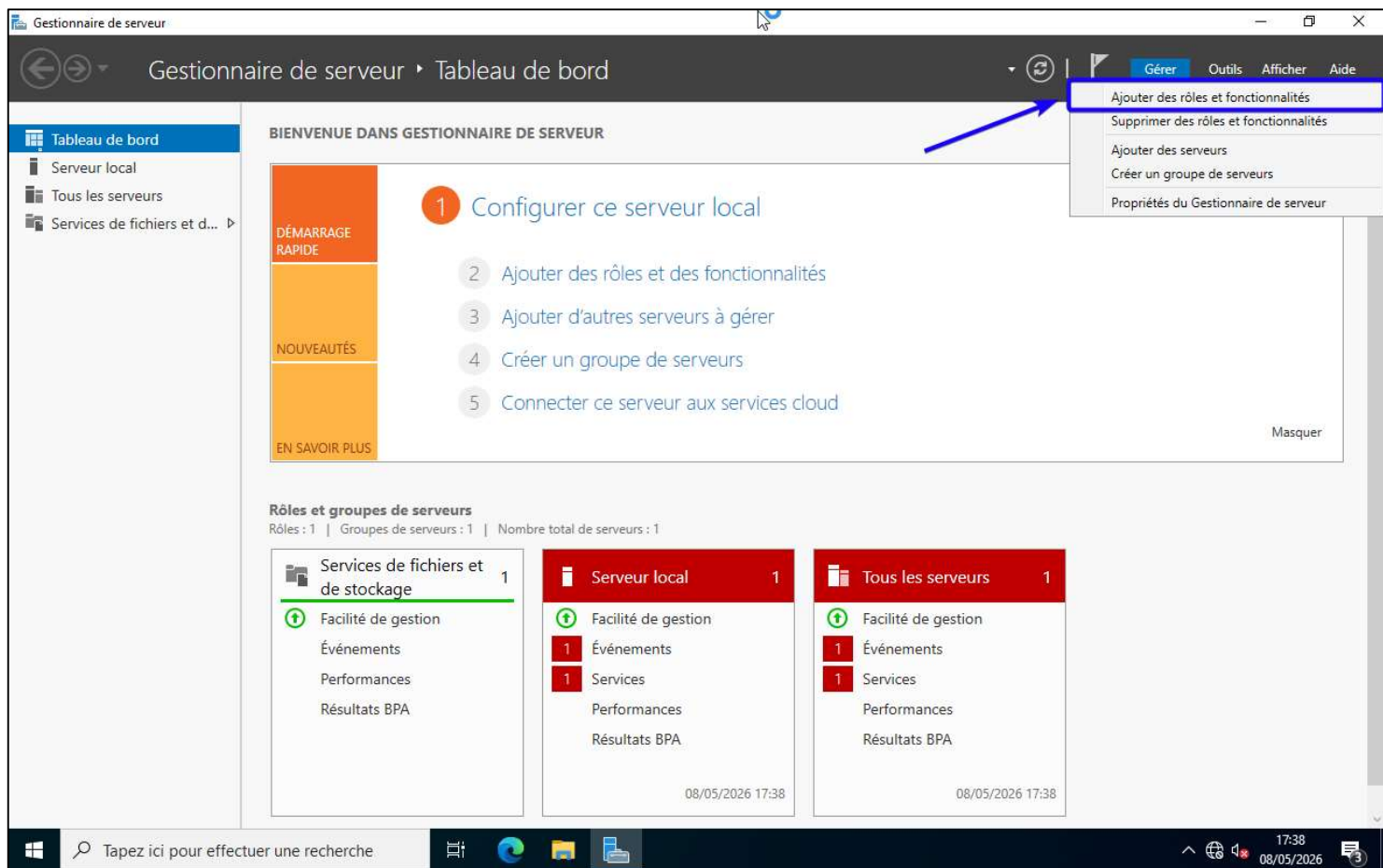
PARTIE 1 : Mise en place de l'environnement de l'entreprise :

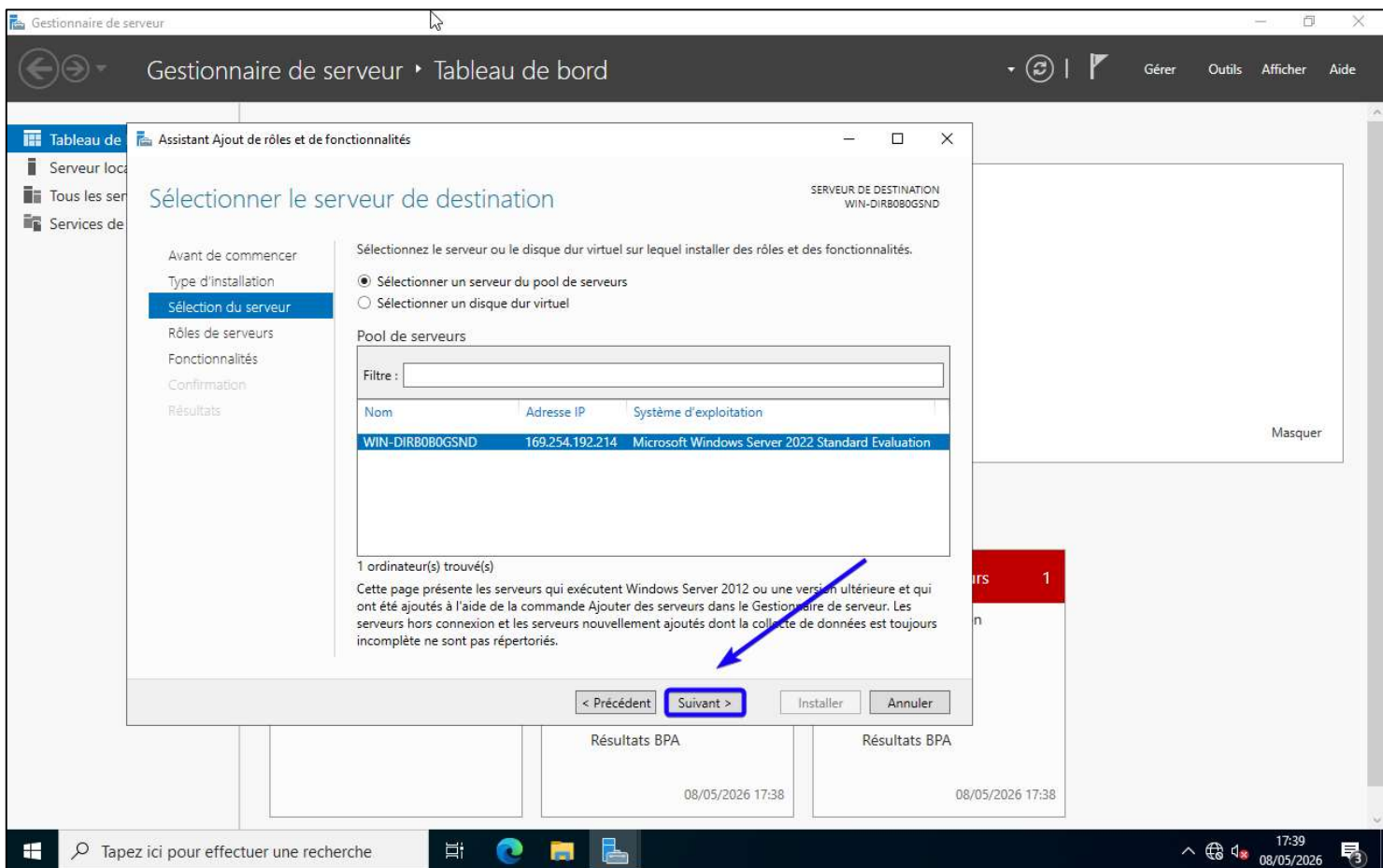
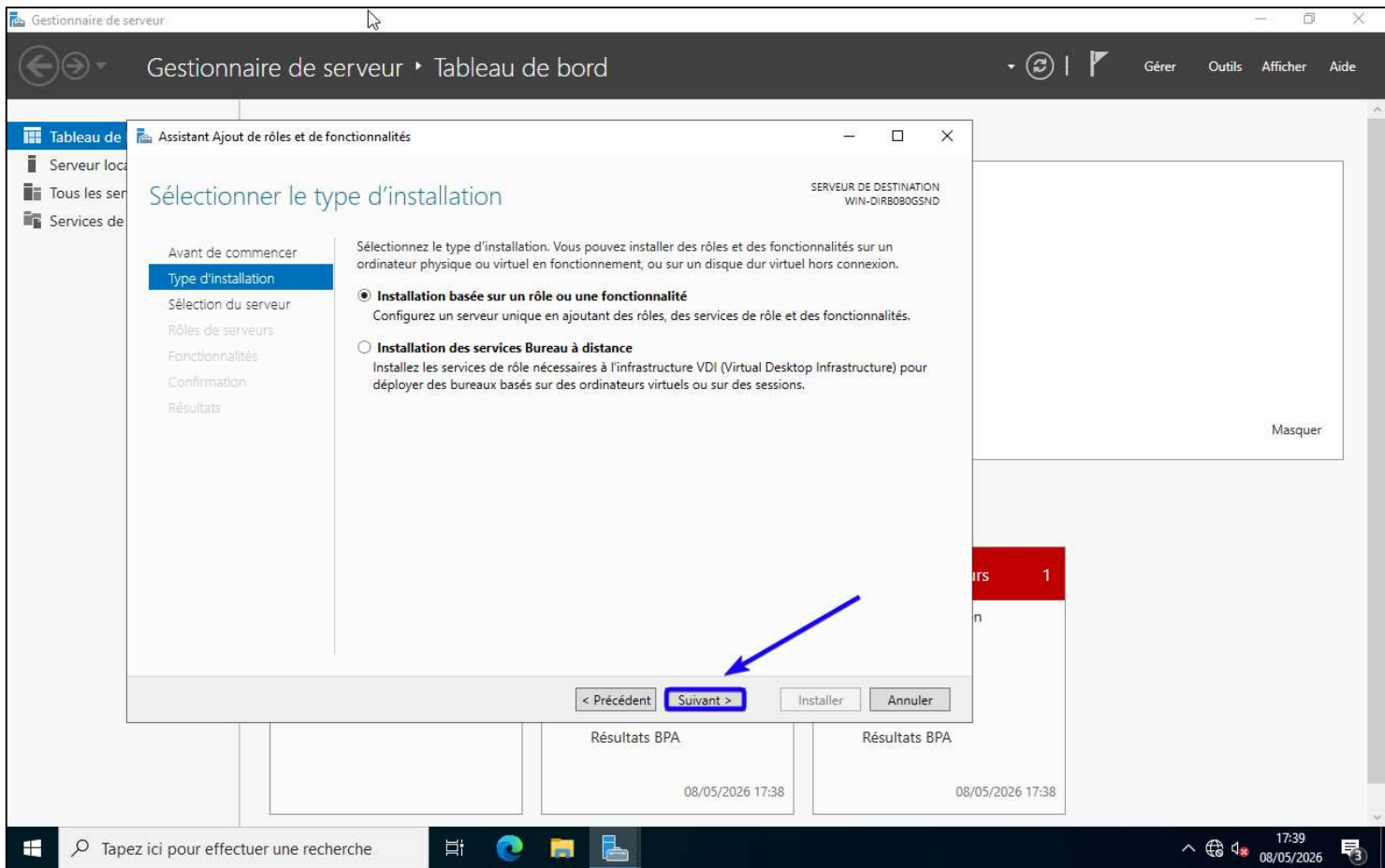
Etape 1 : Installation des machines virtuelle :

Installation du serveurs ADDS :

Rôles à installer :

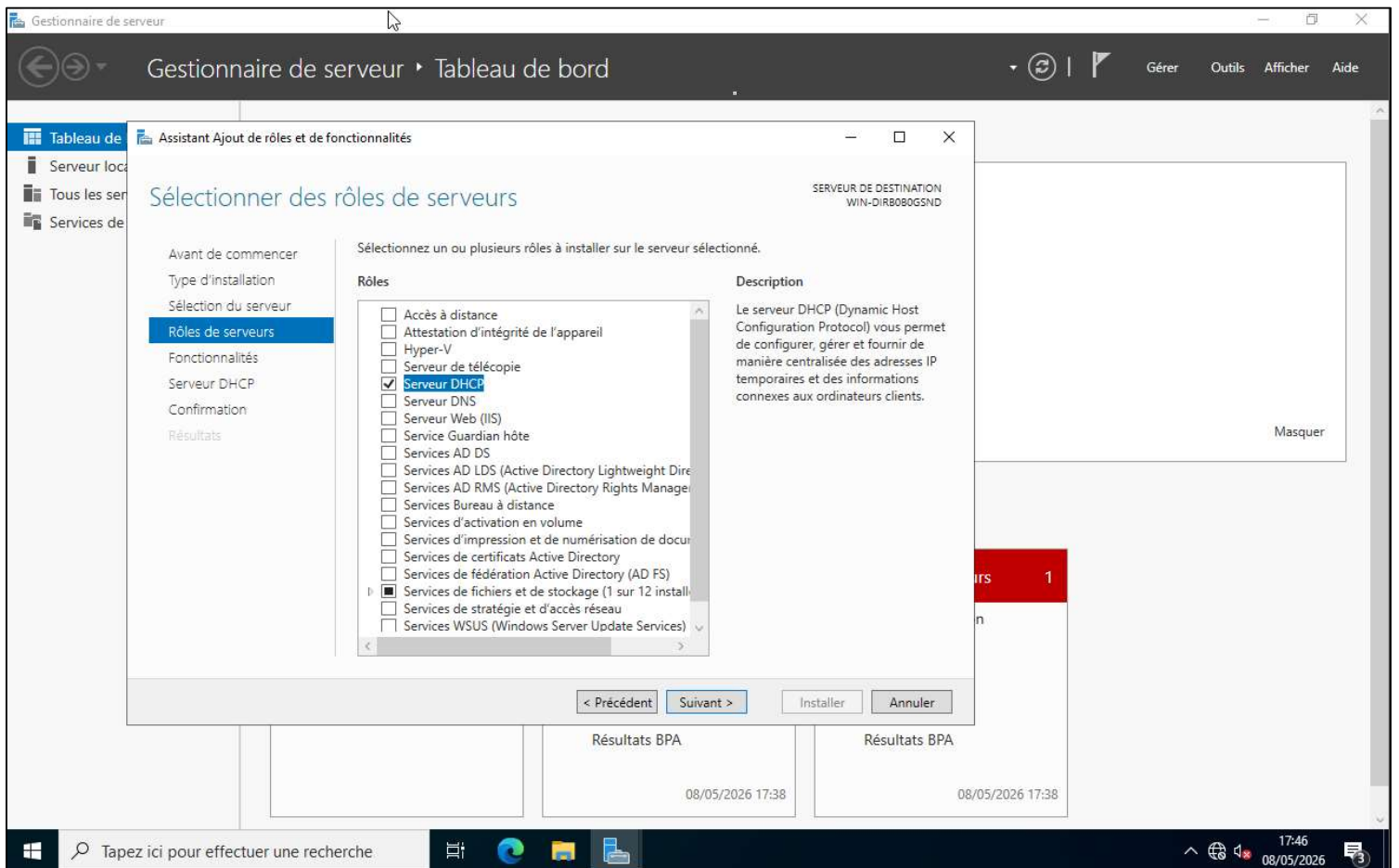
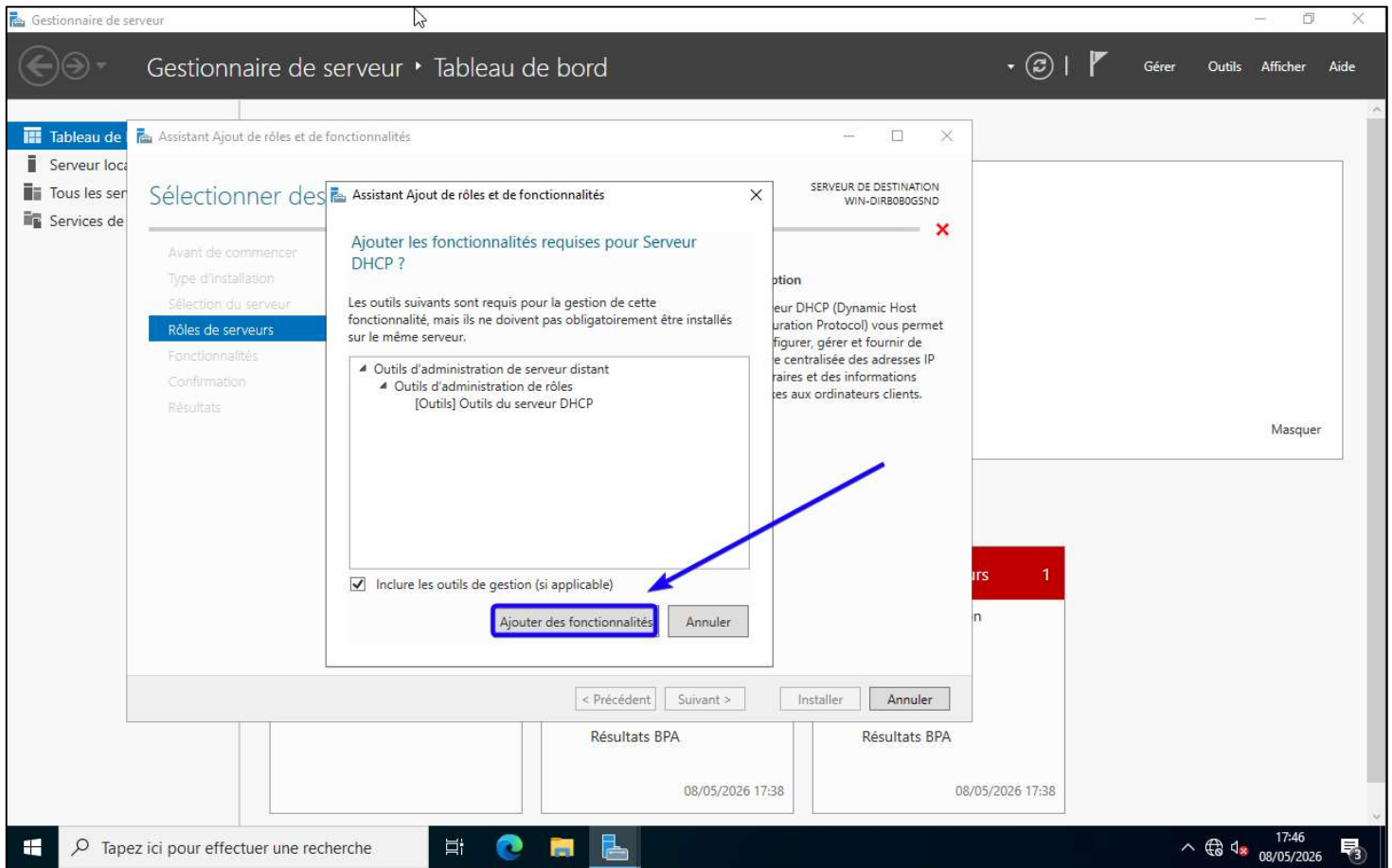
- Rôle ADDS
- Rôle DHCP
- Rôle DNS
- Rôle « Serveur de stratégie et d'accès réseau »







Rôle DHCP :





Rôle DNS :

Gestionnaire de serveur - Tableau de bord

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

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

Ajouter les fonctionnalités requises pour Serveur DNS ?

Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.

- ☑ Outils d'administration de serveur distant
 - ☑ Outils d'administration de rôles
 - [Outils] Outils du serveur DNS

☒ Inclure les outils de gestion (si applicable)

Ajouter des fonctionnalités Annuler

< Précédent Suivant > Installer Annuler

Résultats BPA 08/05/2026 17:47

Gestionnaire de serveur - Tableau de bord

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

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

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles	Description
☐ Accès à distance	Le serveur DNS (Domain Name System) permet la résolution de noms sur les réseaux TCP/IP. Le serveur DNS est plus facile à gérer lorsqu'il est installé sur le même serveur que les services de domaine Active Directory. Si vous sélectionnez le rôle Services de domaine Active Directory, vous pouvez installer et configurer le serveur DNS et les services de domaine Active Directory pour les faire fonctionner conjointement.
☐ Attestation d'intégrité de l'appareil	
☐ Hyper-V	
☐ Serveur de télécopie	
☒ Serveur DHCP	
☒ Serveur DNS	
☐ Serveur Web (IIS)	
☐ Service Guardian hôte	
☐ Services AD DS	
☐ Services AD LDS (Active Directory Lightweight Directory Services)	
☐ Services AD RMS (Active Directory Rights Management Services)	
☐ Services Bureau à distance	
☐ Services d'activation en volume	
☐ Services d'impression et de numérisation de documents	
☐ Services de certificats Active Directory	
☐ Services de fédération Active Directory (AD FS)	
☒ Services de fichiers et de stockage (1 sur 12 installés)	
☐ Services de stratégie et d'accès réseau	
☐ Services WSUS (Windows Server Update Services)	

< Précédent Suivant > Installer Annuler

Résultats BPA 08/05/2026 17:47



Rôle ADDS :

Gestionnaire de serveur - Tableau de bord

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles et de fonctionnalités

Ajouter les fonctionnalités requises pour Services AD DS ?

Vous ne pouvez pas installer Services AD DS sauf si les services de rôle ou les fonctionnalités suivants sont également installés.

- [Outils] Gestion de stratégie de groupe
- ▲ Outils d'administration de serveur distant
 - ▲ Outils d'administration de rôles
 - ▲ Outils AD DS et AD LDS
 - Module Active Directory pour Windows PowerShell
 - ▲ Outils AD DS
 - [Outils] Centre d'administration Active Directory
 - [Outils] Composants logiciels enfichables et outils de gestion

☒ Inclure les outils de gestion (si applicable)

Ajouter des fonctionnalités Annuler

< Précédent Suivant > Installer Annuler

Résultats BPA 08/05/2026 17:47

Gestionnaire de serveur - Tableau de bord

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

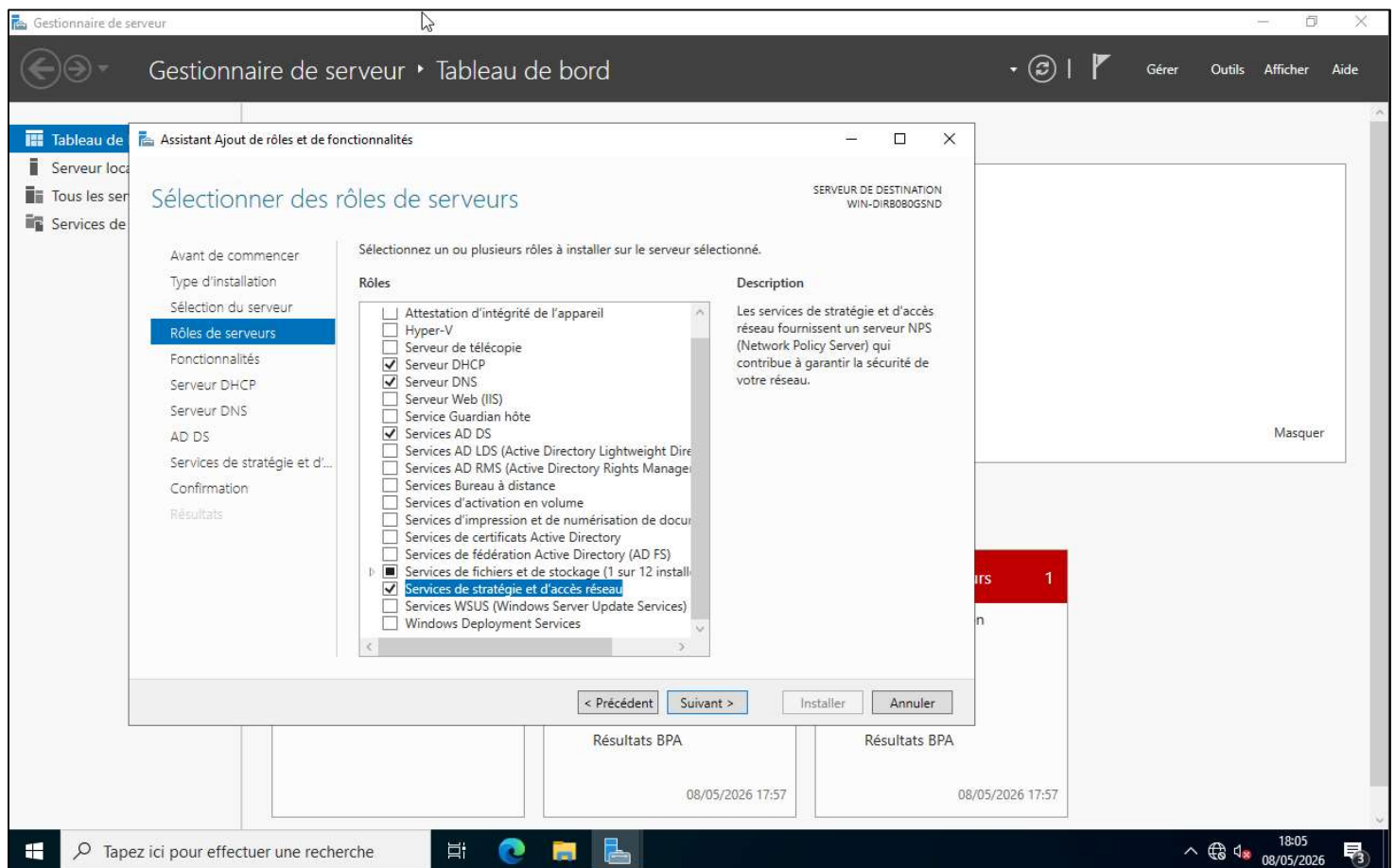
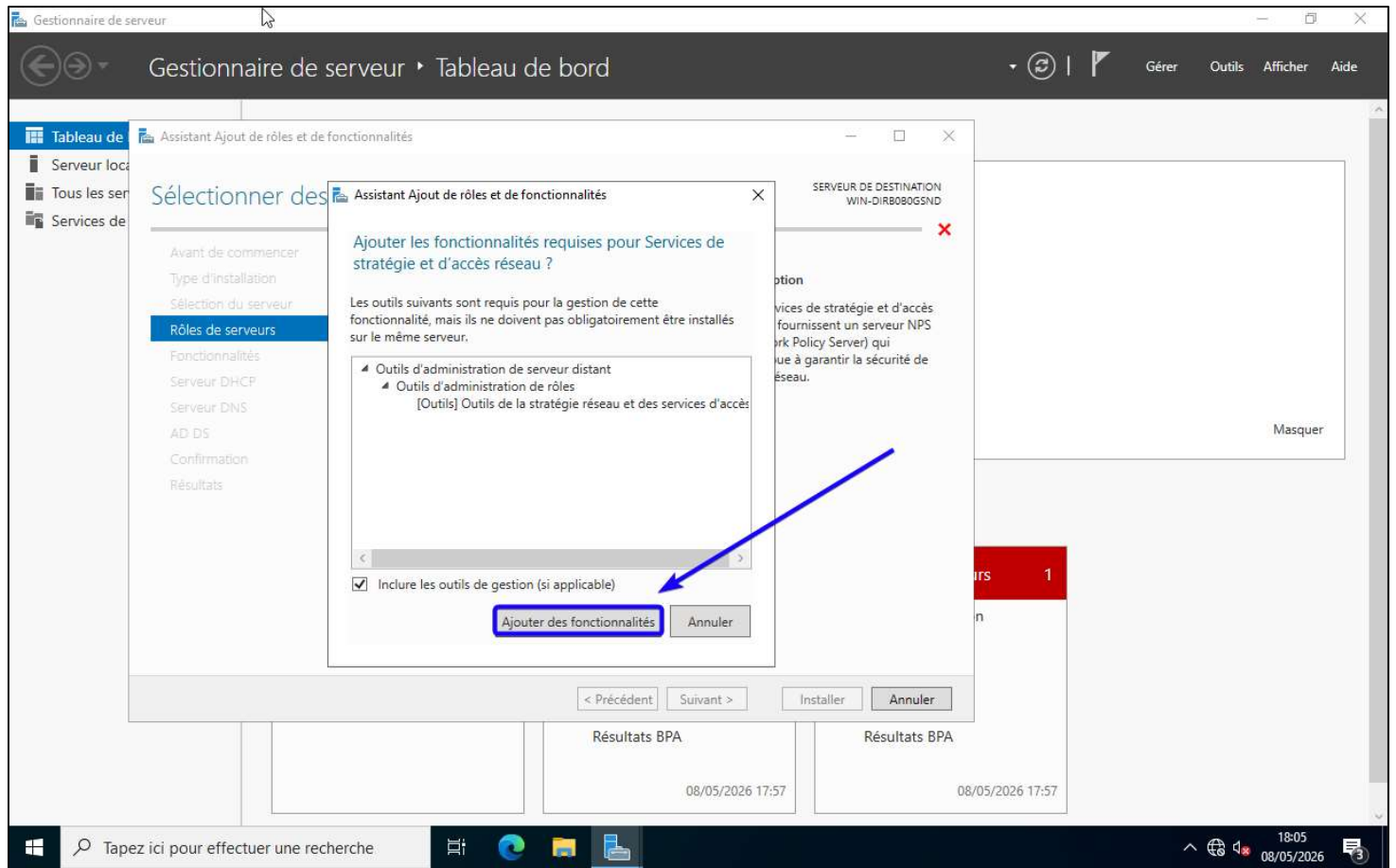
Rôles	Description
☐ Accès à distance	Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.
☐ Attestation d'intégrité de l'appareil	
☐ Hyper-V	
☐ Serveur de télécopie	
☒ Serveur DHCP	
☒ Serveur DNS	
☐ Serveur Web (IIS)	
☐ Service Guardian hôte	
☒ Services AD DS	
☐ Services AD LDS (Active Directory Lightweight Directory Services)	
☐ Services AD RMS (Active Directory Rights Management Services)	
☐ Services Bureau à distance	
☐ Services d'activation en volume	
☐ Services d'impression et de numérisation de documents	
☐ Services de certificats Active Directory	
☐ Services de fédération Active Directory (AD FS)	
☒ Services de fichiers et de stockage (1 sur 12 installés)	
☐ Services de stratégie et d'accès réseau	
☐ Services WSUS (Windows Server Update Services)	

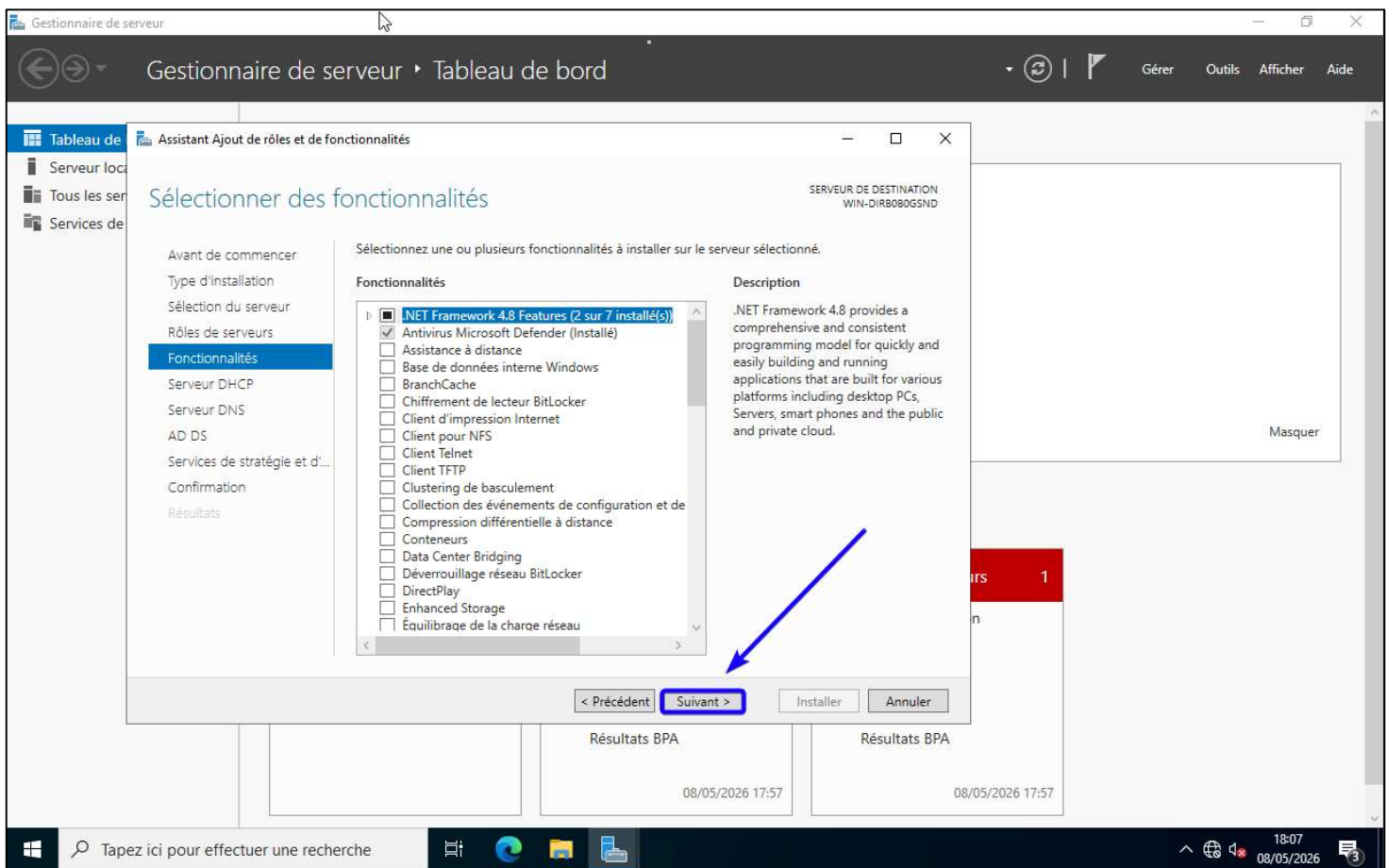
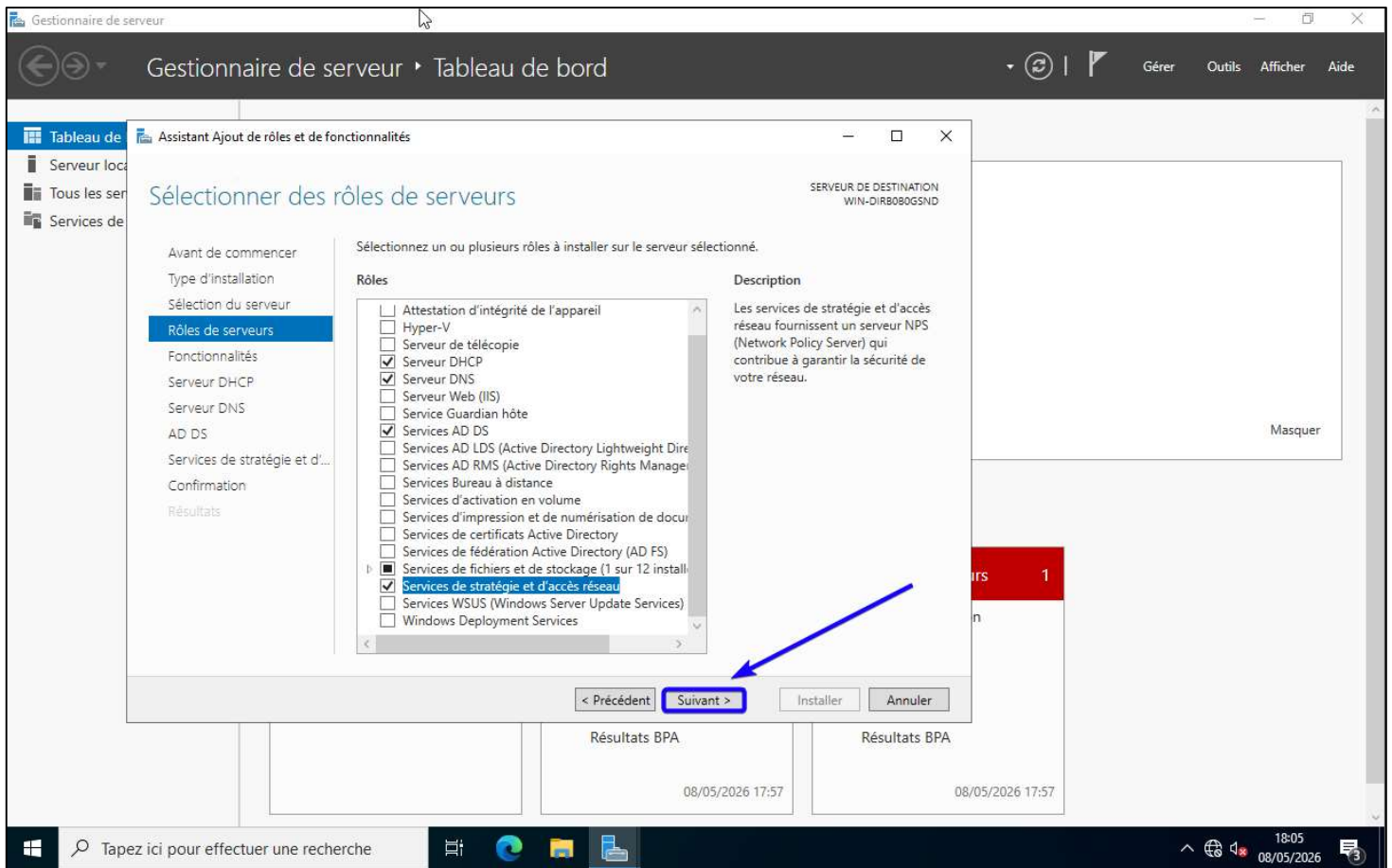
< Précédent Suivant > Installer Annuler

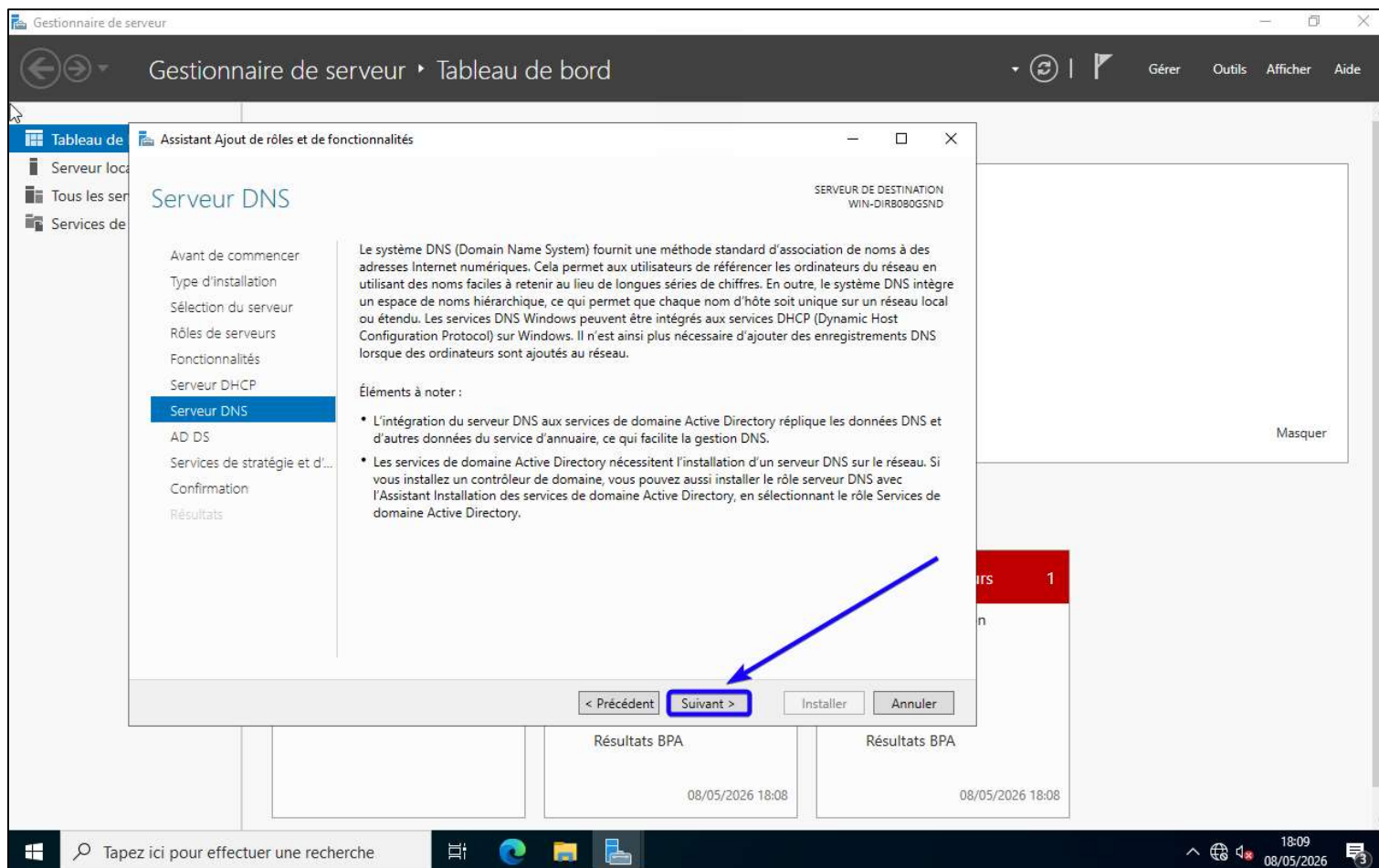
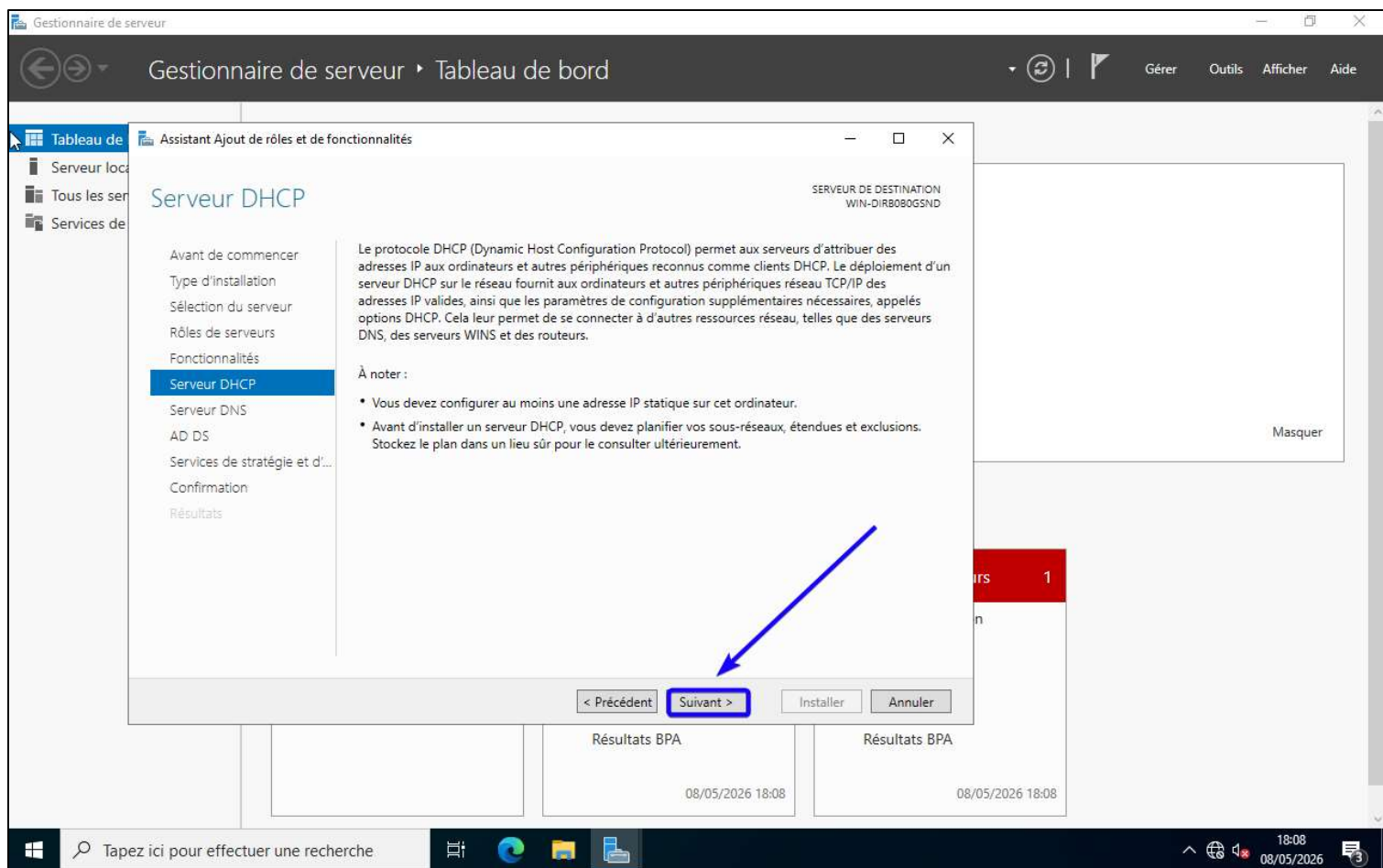
Résultats BPA 08/05/2026 17:47

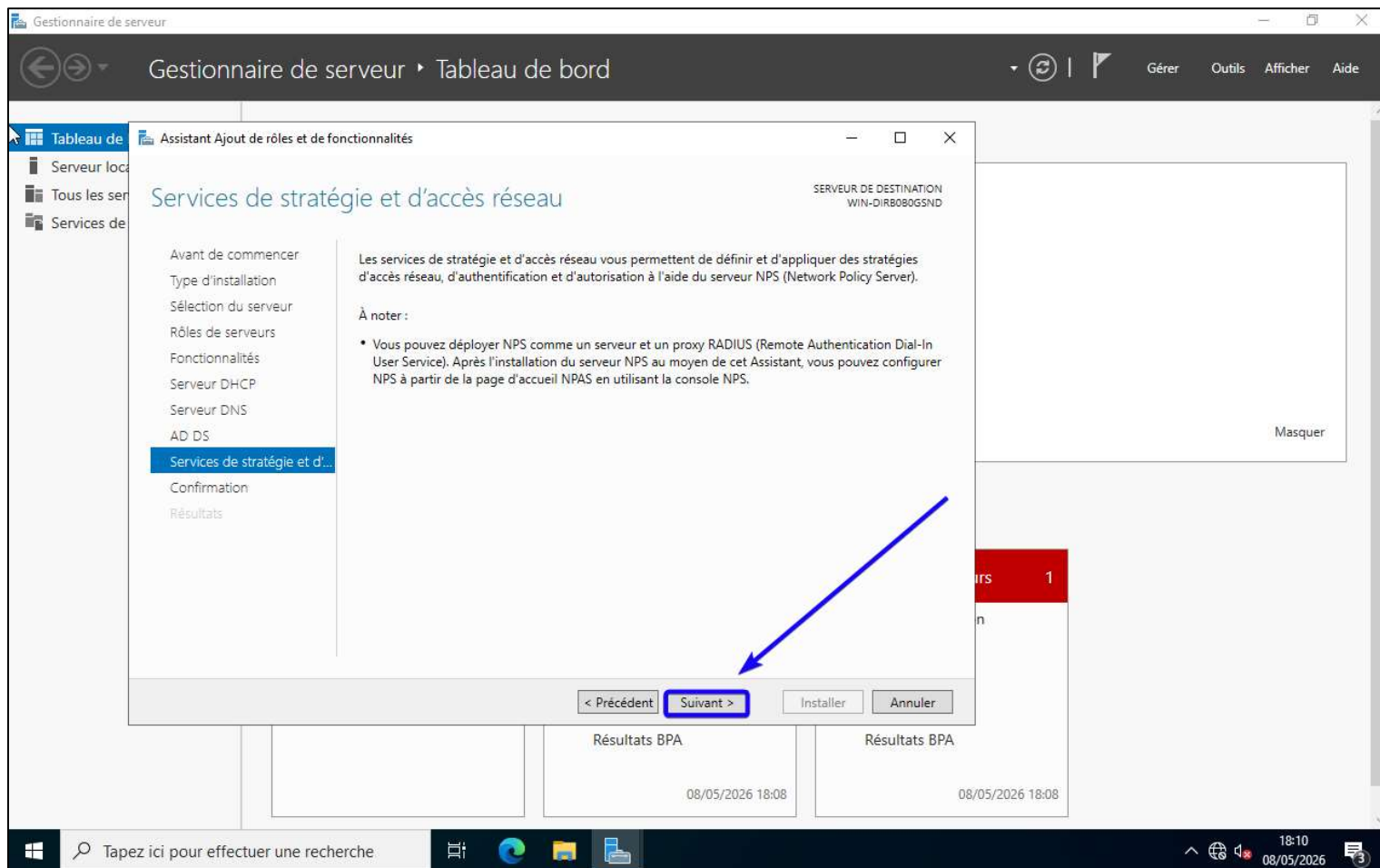
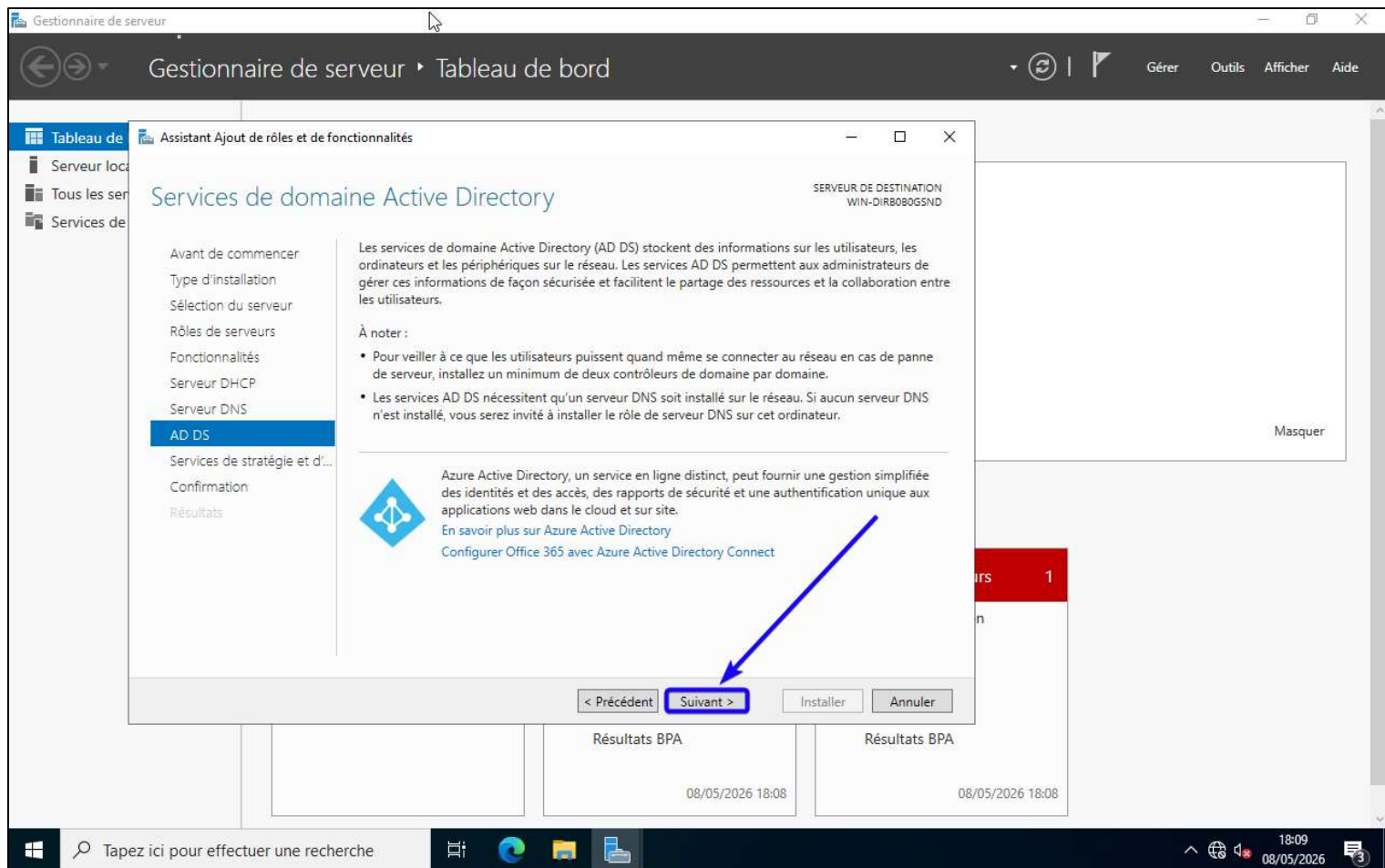


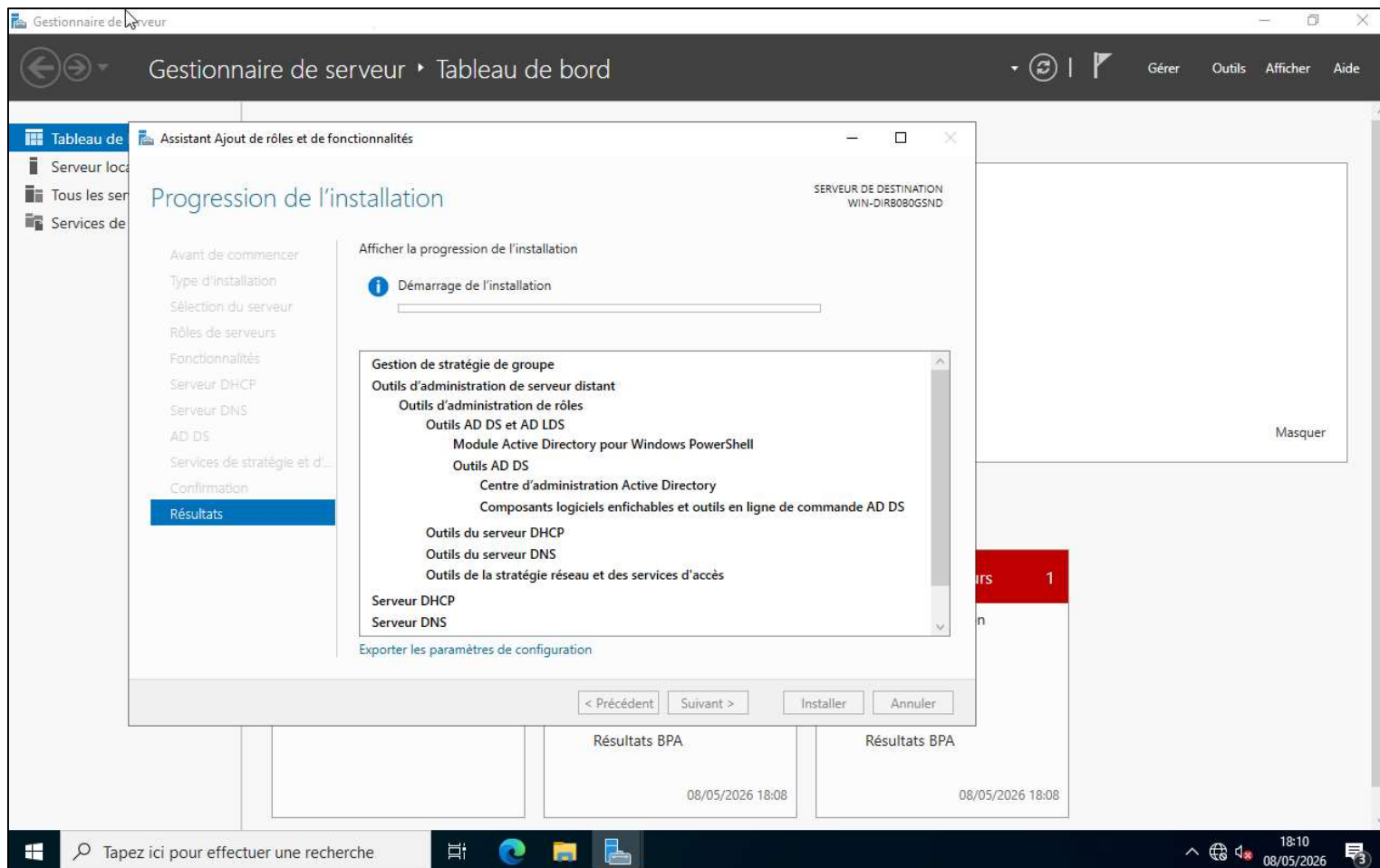
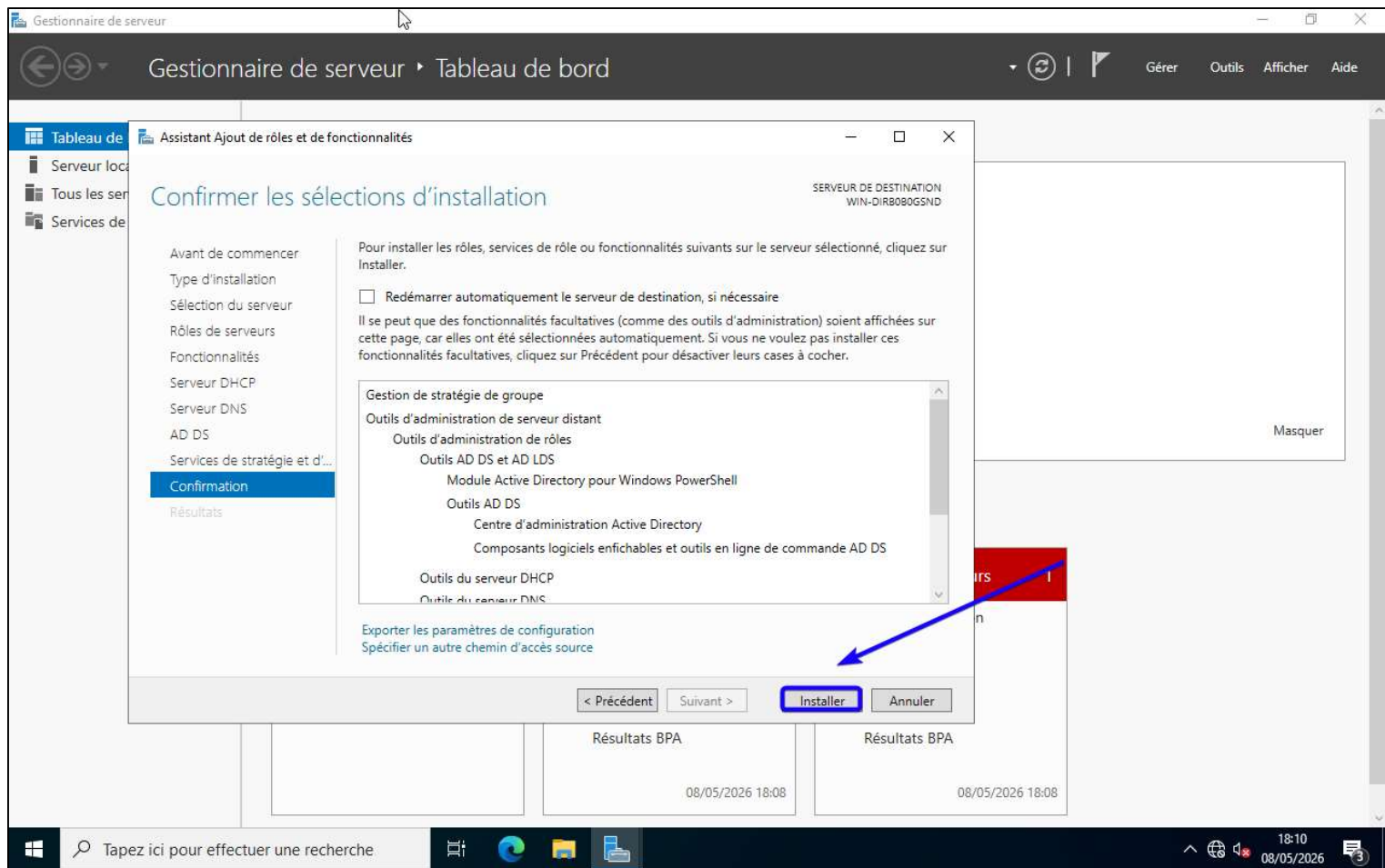
Rôle : « Serveur de stratégie et d'accès réseau » NPS











Gestionnaire de serveur

Gestionnaire de serveur ▶ Tableau de bord

Gérer Outils Afficher Aide

Tableau de bord

Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SERVER DE DESTINATION
WIN-DIRB080GSND

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DHCP
Serveur DNS
AD DS
Services de stratégie et d...
Confirmation
Résultats

Afficher la progression de l'installation

Installation de fonctionnalité

Configuration requise. Installation réussie sur WIN-DIRB080GSND.

Promouvoir ce serveur en contrôleur de domaine

Gestion de stratégie de groupe

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils AD DS et AD LDS

Module Active Directory pour Windows PowerShell

Outils AD DS

Centre d'administration Active Directory

Composants logiciels enfichables et outils en ligne de commande AD DS

Outils du serveur DHCP

Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

< Précédent Suivant > Fermer Annuler

Résultats BPA

Résultats BPA

Résultats BPA

Tapez ici pour effectuer une recherche

18:23
08/05/2026

Installation Rôle Serveur Web :

Rôle à installer :

- Rôle IIS

The screenshot shows the Windows Server Management console. The title bar reads 'Gestionnaire de serveur'. The breadcrumb navigation shows 'Gestionnaire de serveur > Tableau de bord'. The left sidebar has a 'Tableau de bord' section with links to 'Serveur local', 'Tous les serveurs', and 'Services de fichiers et d...'. The main area is titled 'BIENVENUE DANS GESTIONNAIRE DE SERVEUR' and contains a 'DÉMARRAGE RAPIDE' section with a numbered list of tasks: 1. Configurer ce serveur local, 2. Ajouter des rôles et des fonctionnalités, 3. Ajouter d'autres serveurs à gérer, 4. Créer un groupe de serveurs, and 5. Connecter ce serveur aux services cloud. A blue arrow points to the 'Ajouter des rôles et fonctionnalités' option in the 'Gérer' dropdown menu. Below this, the 'Rôles et groupes de serveurs' section shows a list of roles and groups, including 'Services de fichiers et de stockage', 'Serveur local', and 'Tous les serveurs', each with a count of 1. The bottom of the screen shows the Windows taskbar with the search bar and system clock.

Gestionnaire de serveur

Gestionnaire de serveur > Tableau de bord

Tableau de bord

- Serveur local
- Tous les serveurs
- Services de fichiers et d...

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

1 Configurer ce serveur local

2 Ajouter des rôles et des fonctionnalités

3 Ajouter d'autres serveurs à gérer

4 Créer un groupe de serveurs

5 Connecter ce serveur aux services cloud

Ajouter des rôles et fonctionnalités

Supprimer des rôles et fonctionnalités

Ajouter des serveurs

Créer un groupe de serveurs

Propriétés du Gestionnaire de serveur

Rôles et groupes de serveurs

Rôles : 1 | Groupes de serveurs : 1 | Nombre total de serveurs : 1

Services de fichiers et de stockage 1

- Facilité de gestion
- Événements
- Performances
- Résultats BPA

Serveur local 1

- Facilité de gestion
- Événements 1
- Services 1
- Performances
- Résultats BPA

Tous les serveurs 1

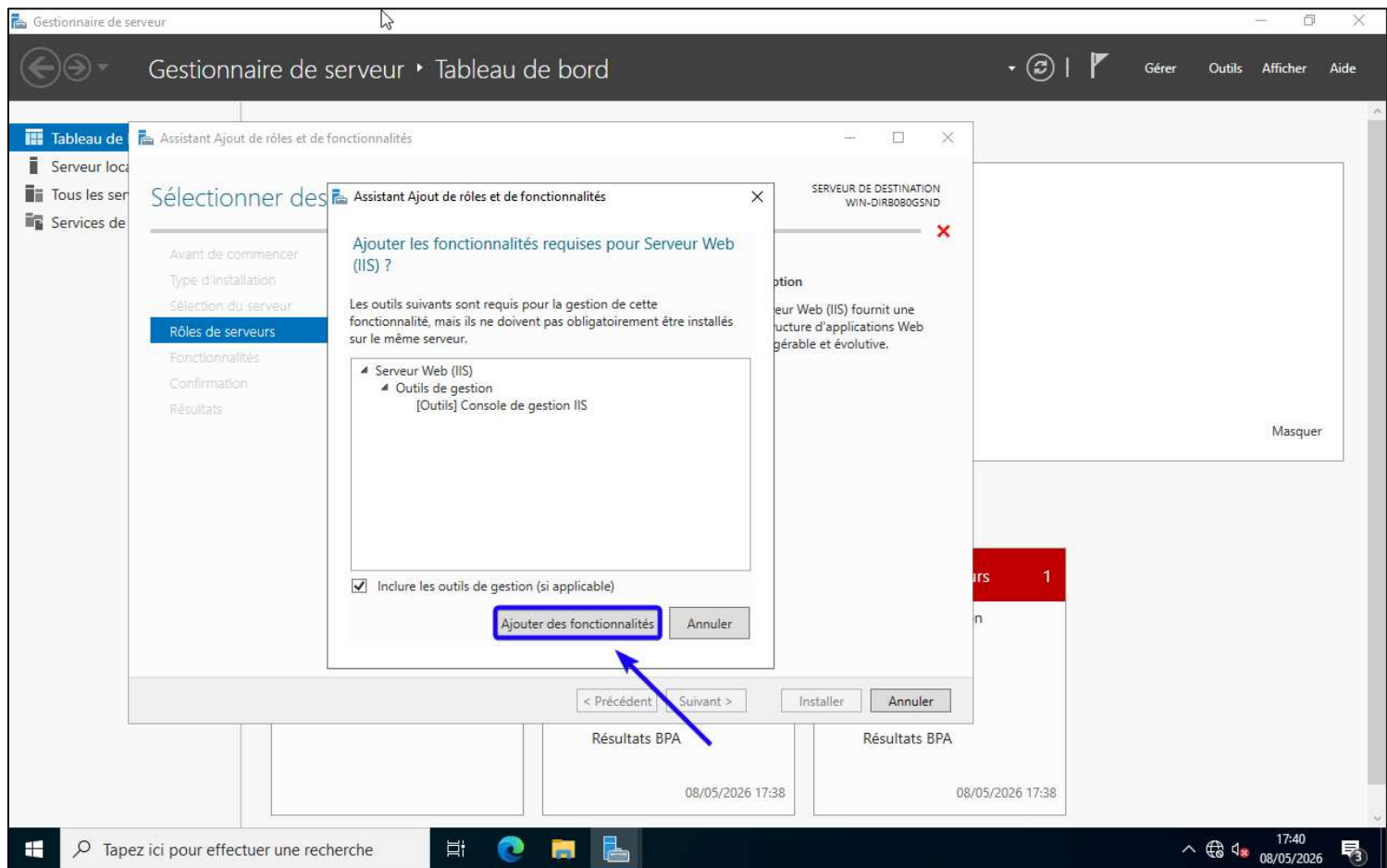
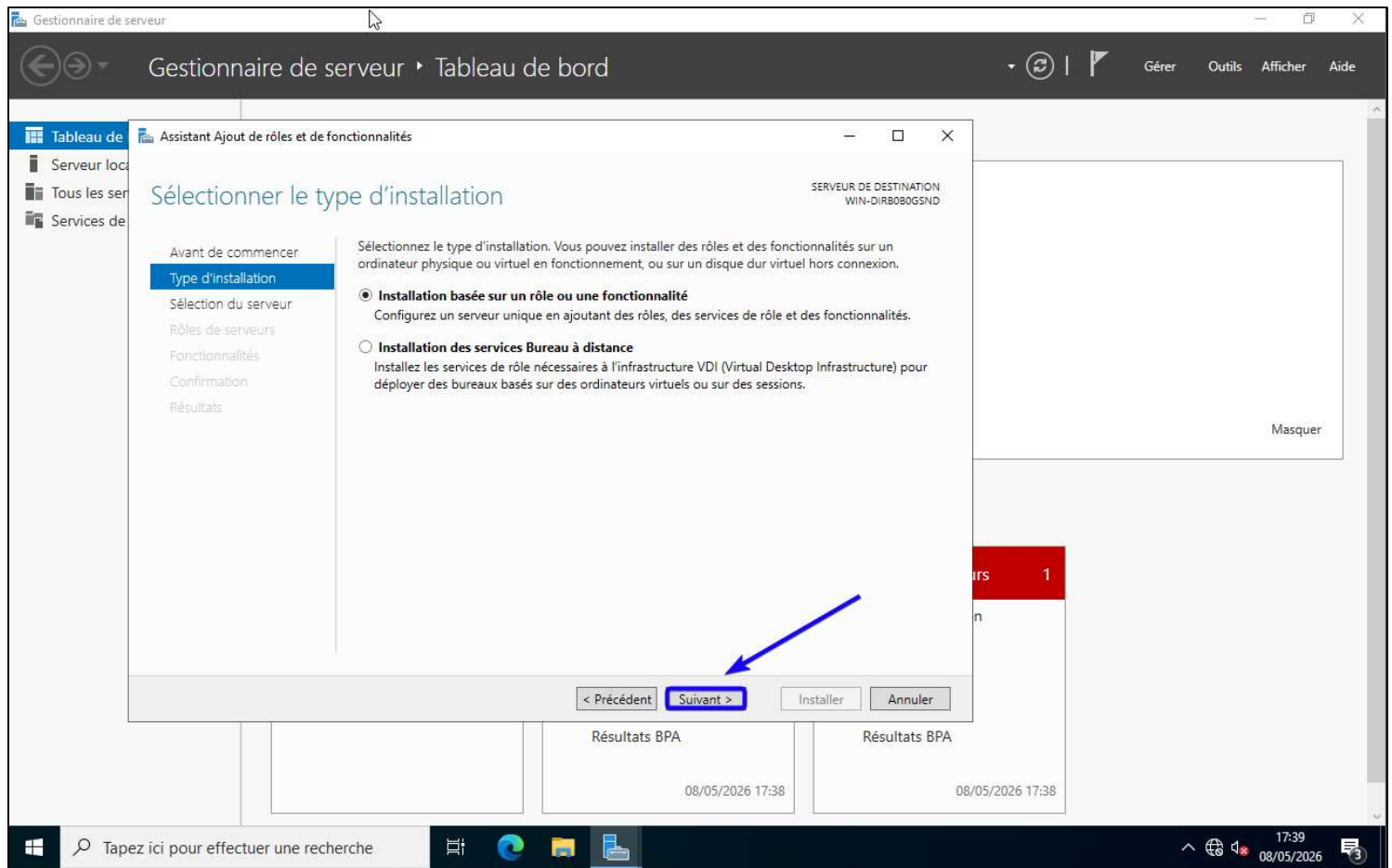
- Facilité de gestion
- Événements 1
- Services 1
- Performances
- Résultats BPA

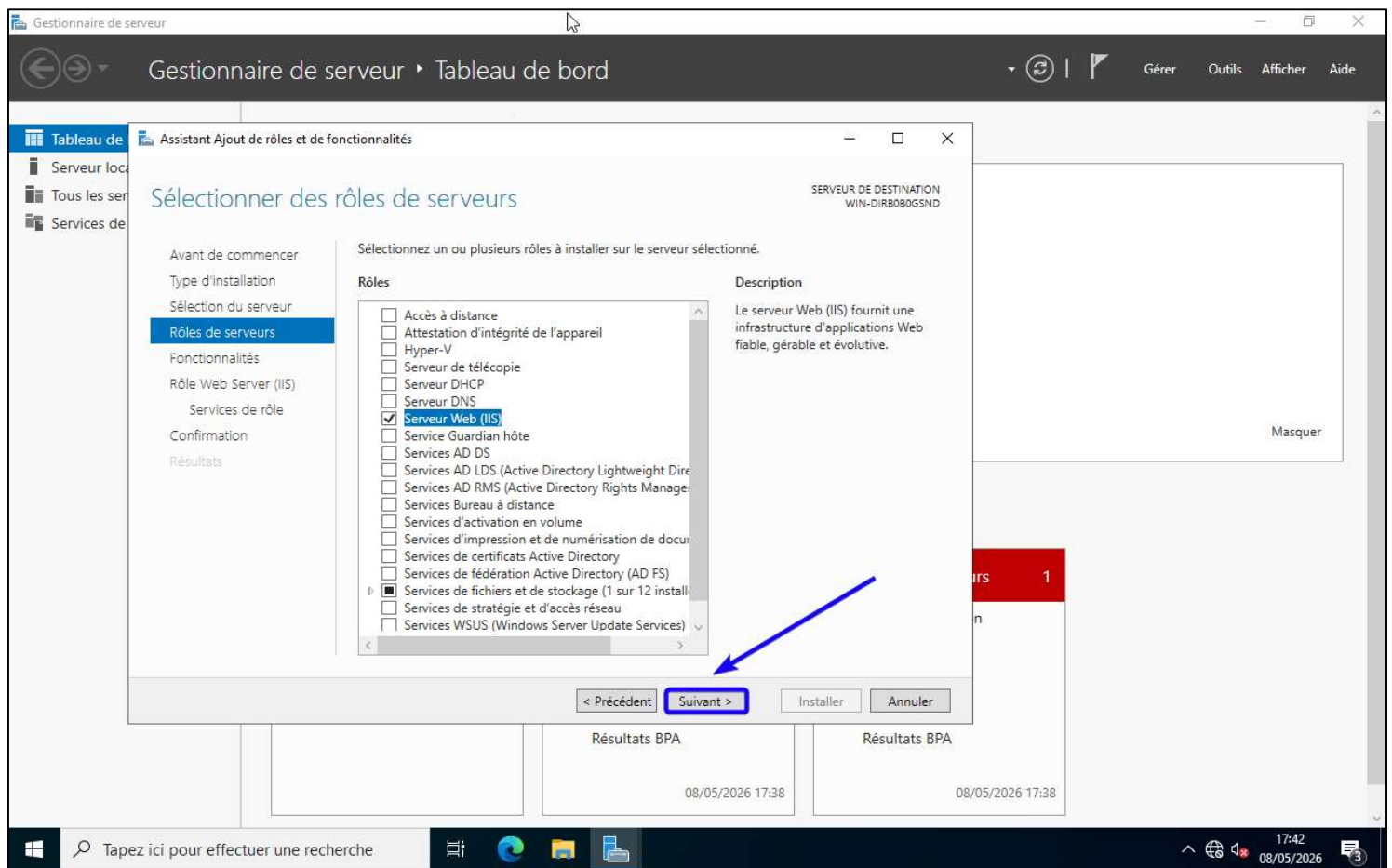
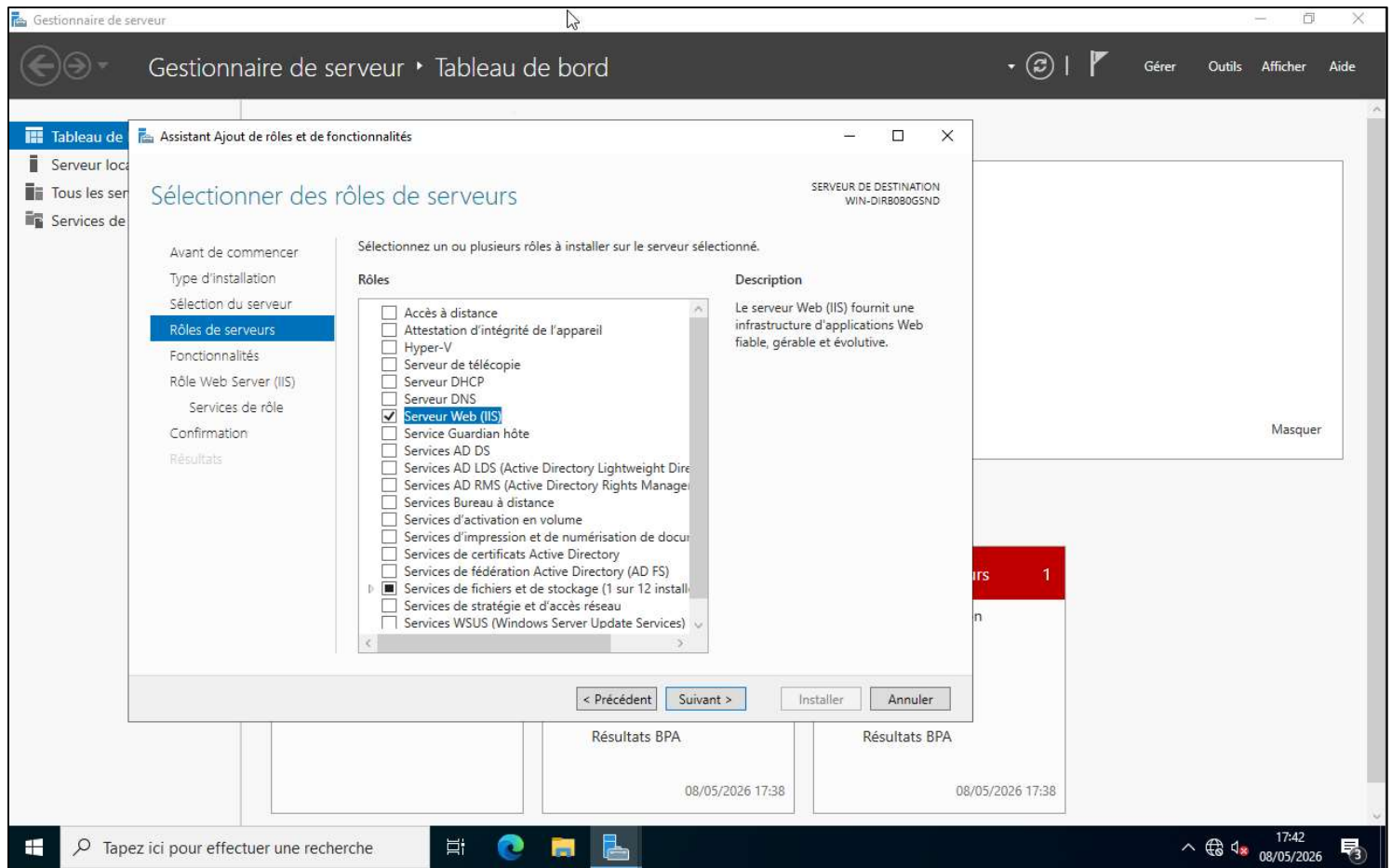
08/05/2026 17:38

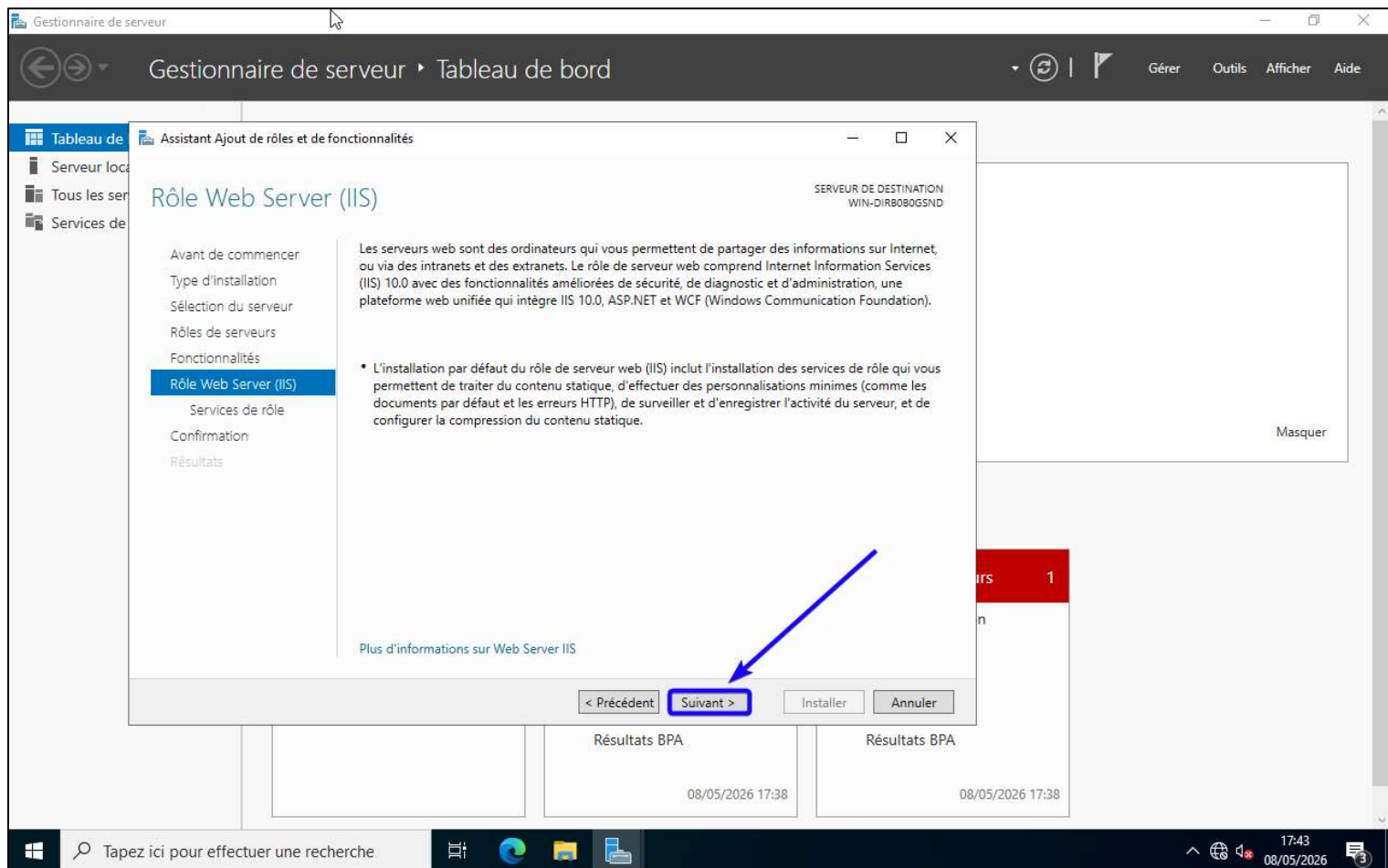
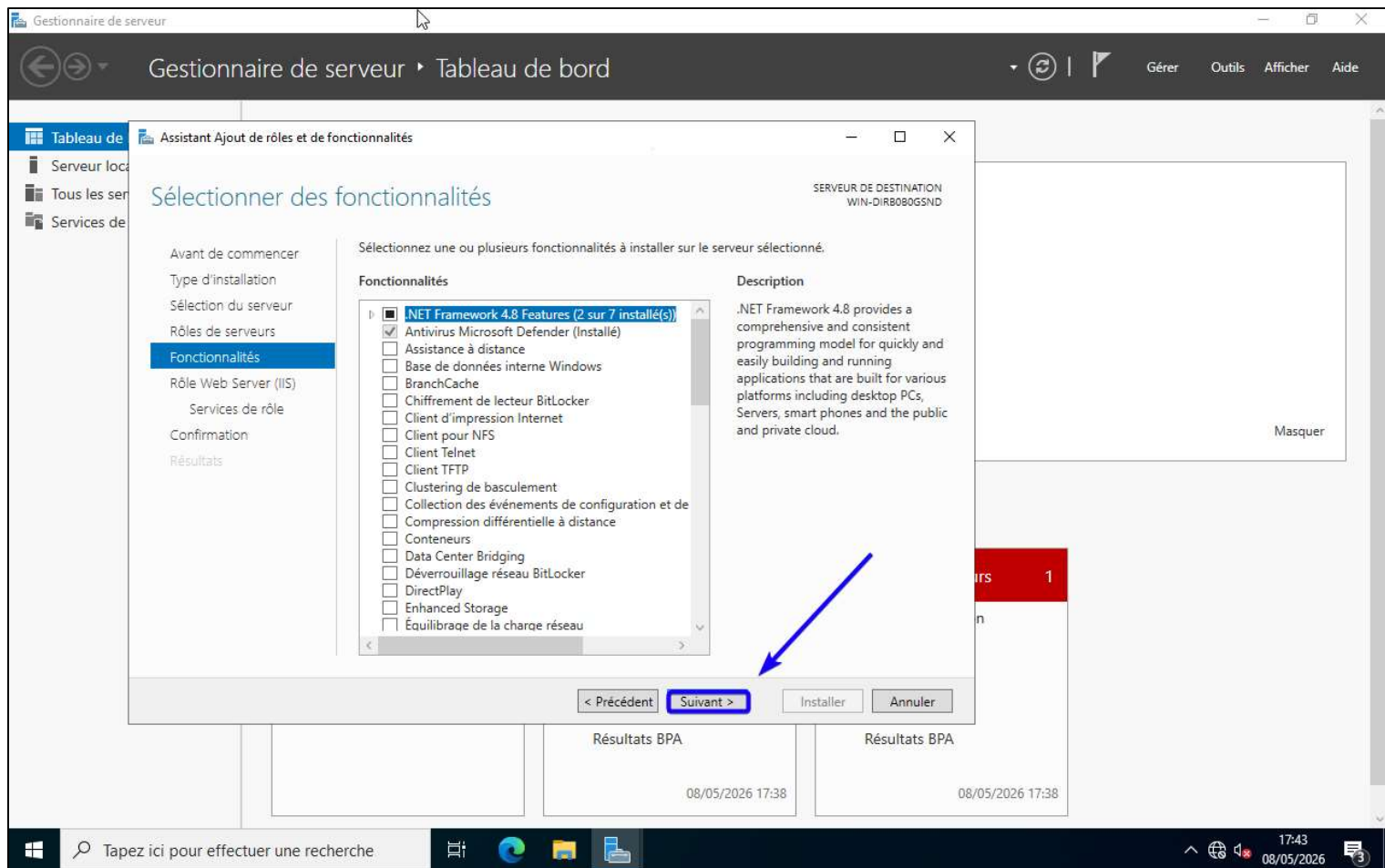
08/05/2026 17:38

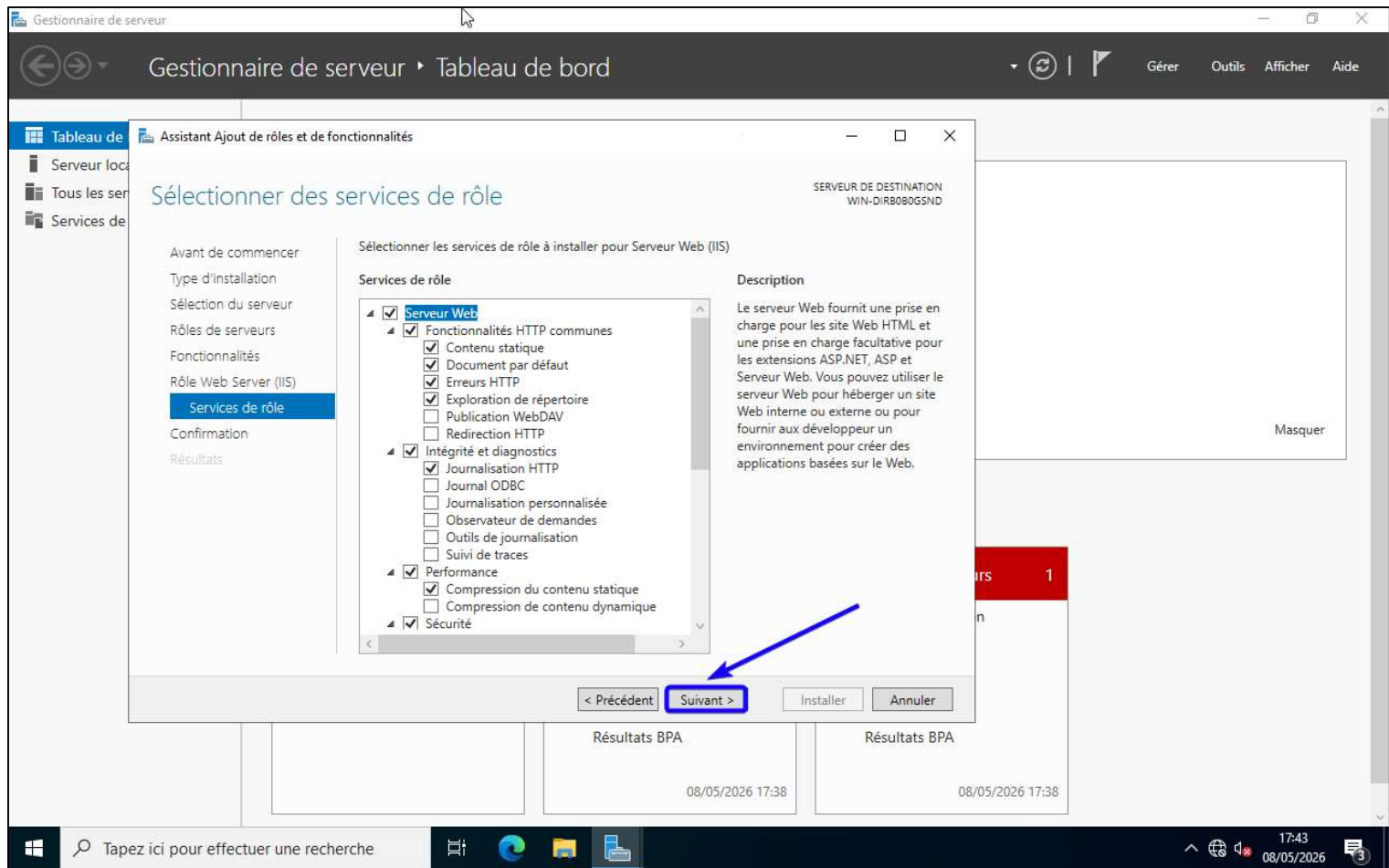
Tapez ici pour effectuer une recherche

17:38 08/05/2026

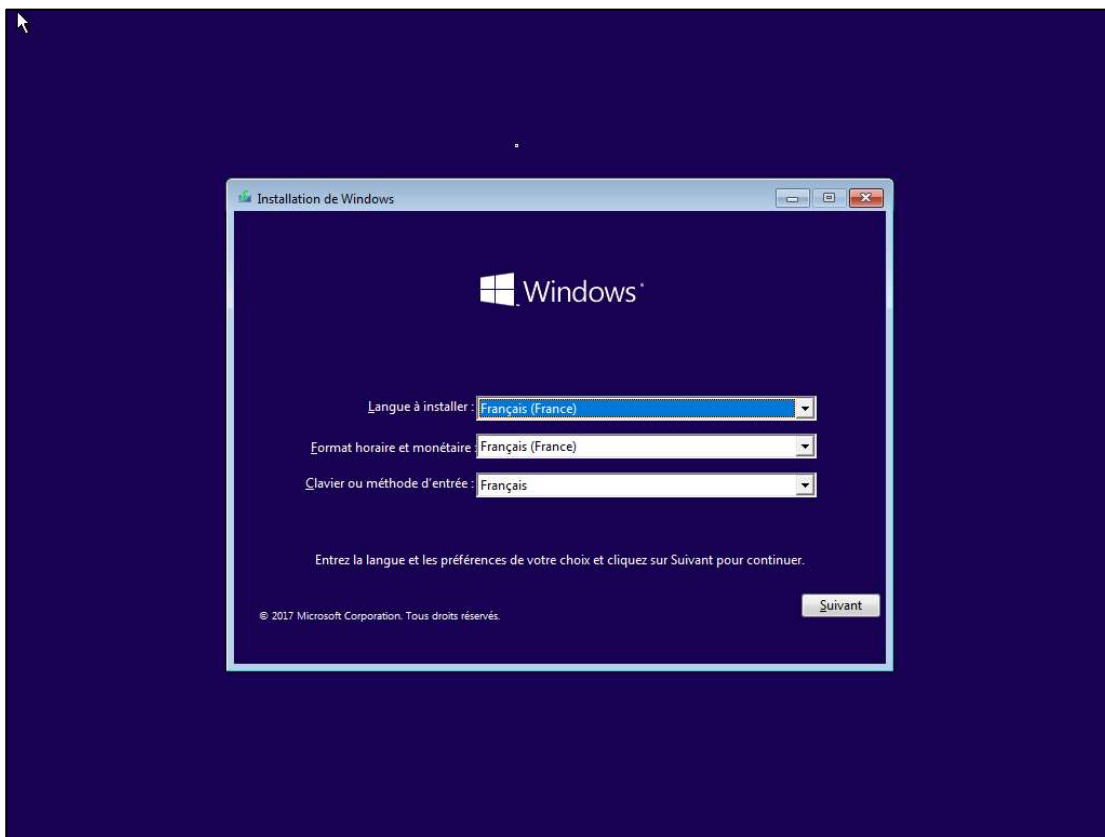


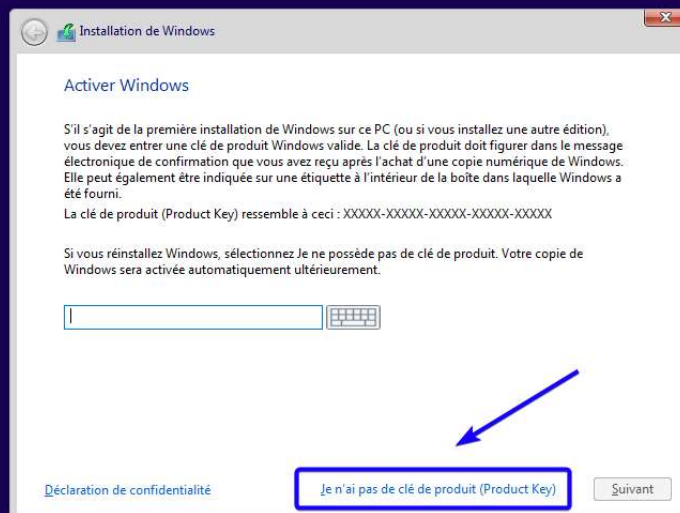




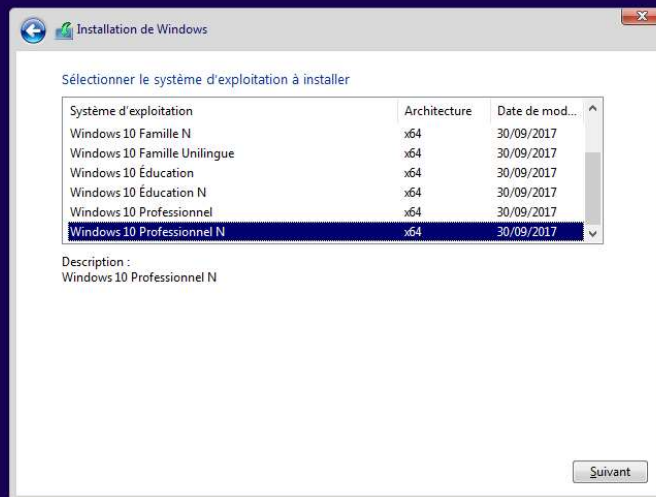


Installation de Windows 1709 – Professionnel :

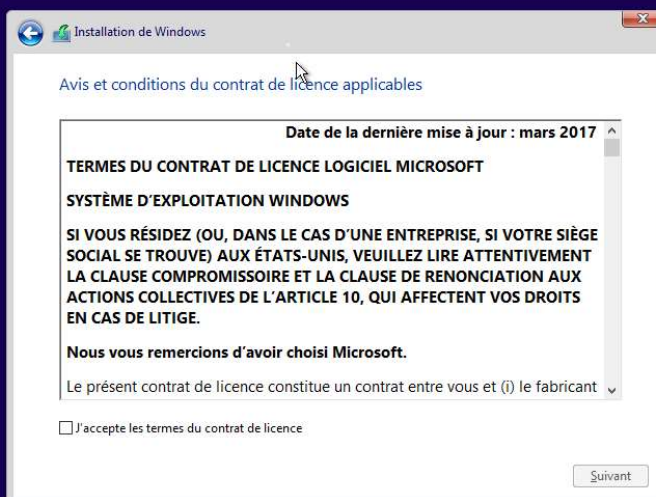




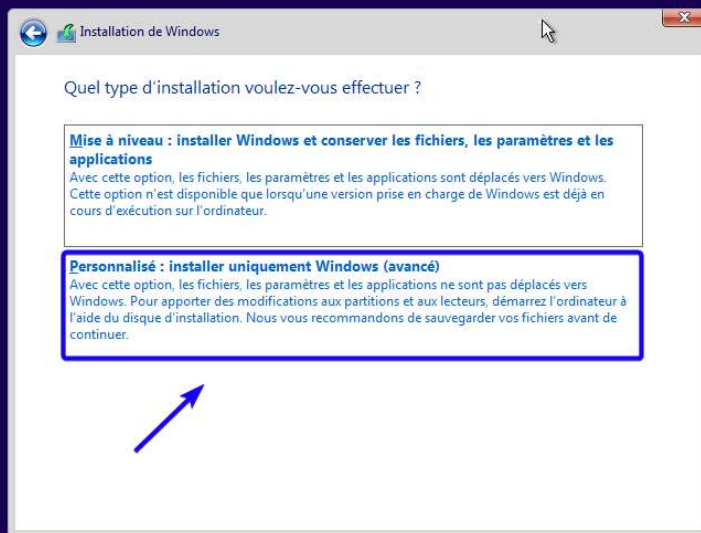
1 Collecte des informations 2 Installation de Windows



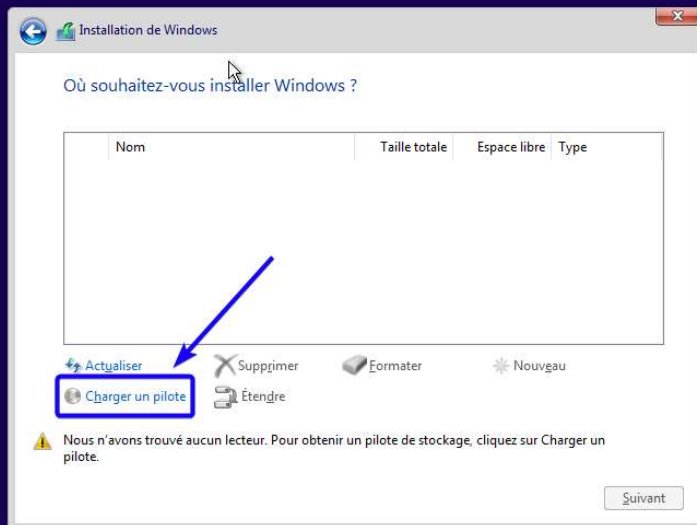
1 Collecte des informations 2 Installation de Windows



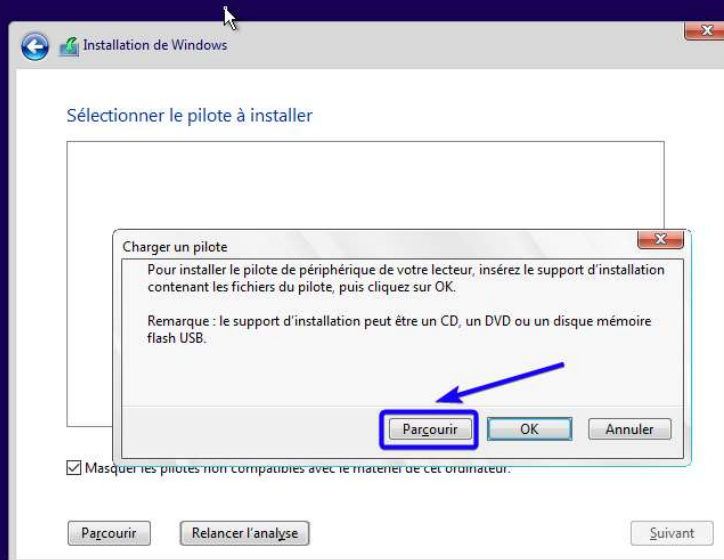
1 Collecte des informations 2 Installation de Windows



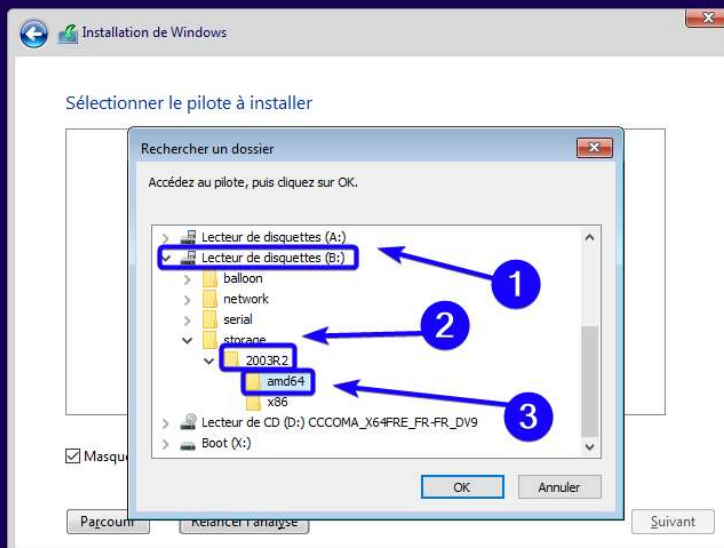
1 Collecte des informations 2 Installation de Windows



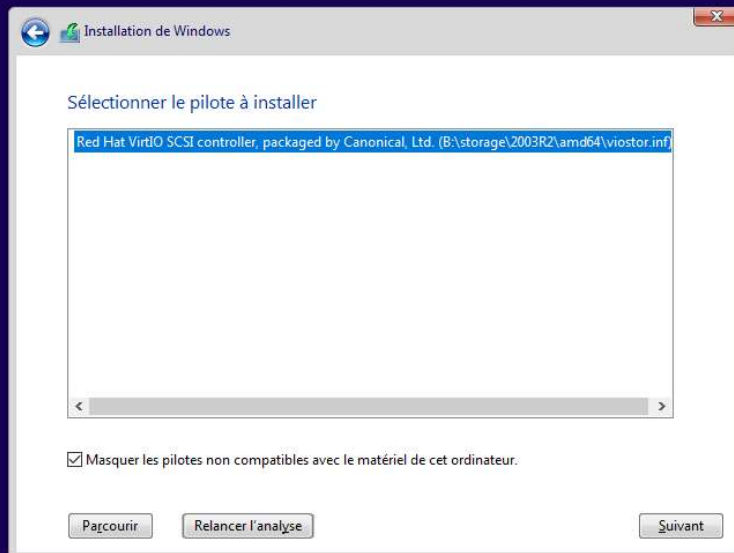
1 Collecte des informations 2 Installation de Windows



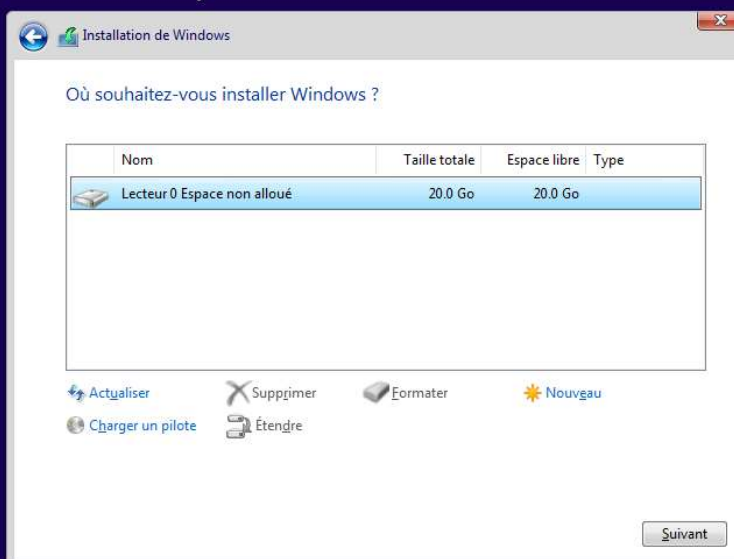
1 Collecte des informations 2 Installation de Windows



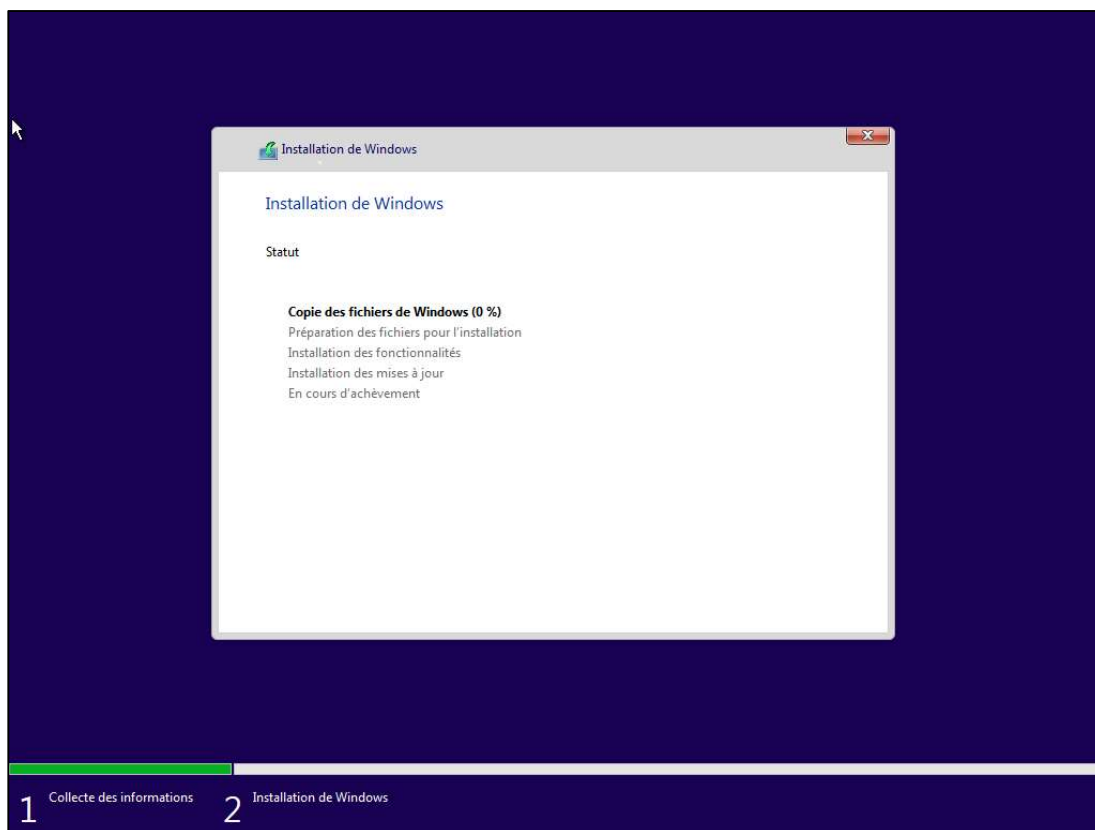
1 Collecte des informations 2 Installation de Windows



1 Collecte des informations 2 Installation de Windows



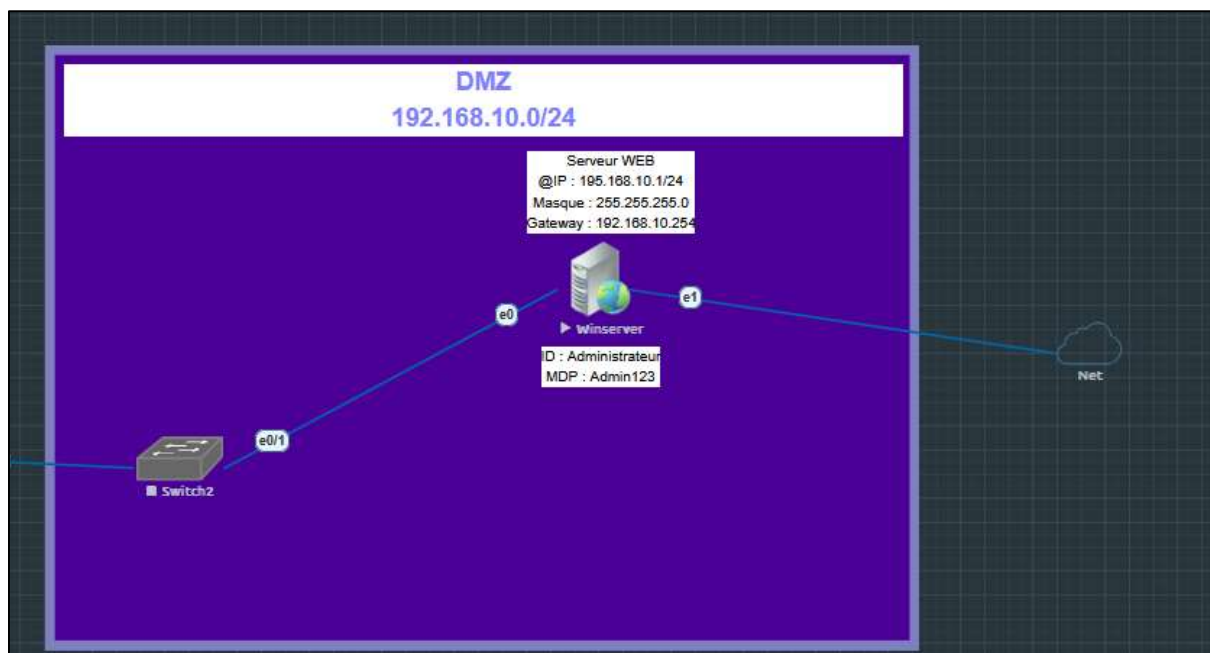
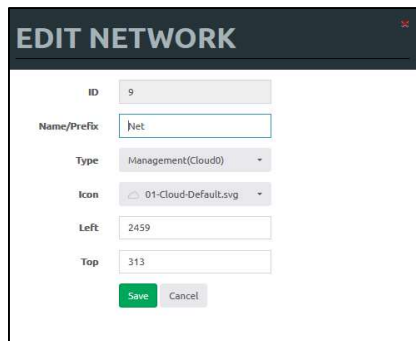
1 Collecte des informations 2 Installation de Windows



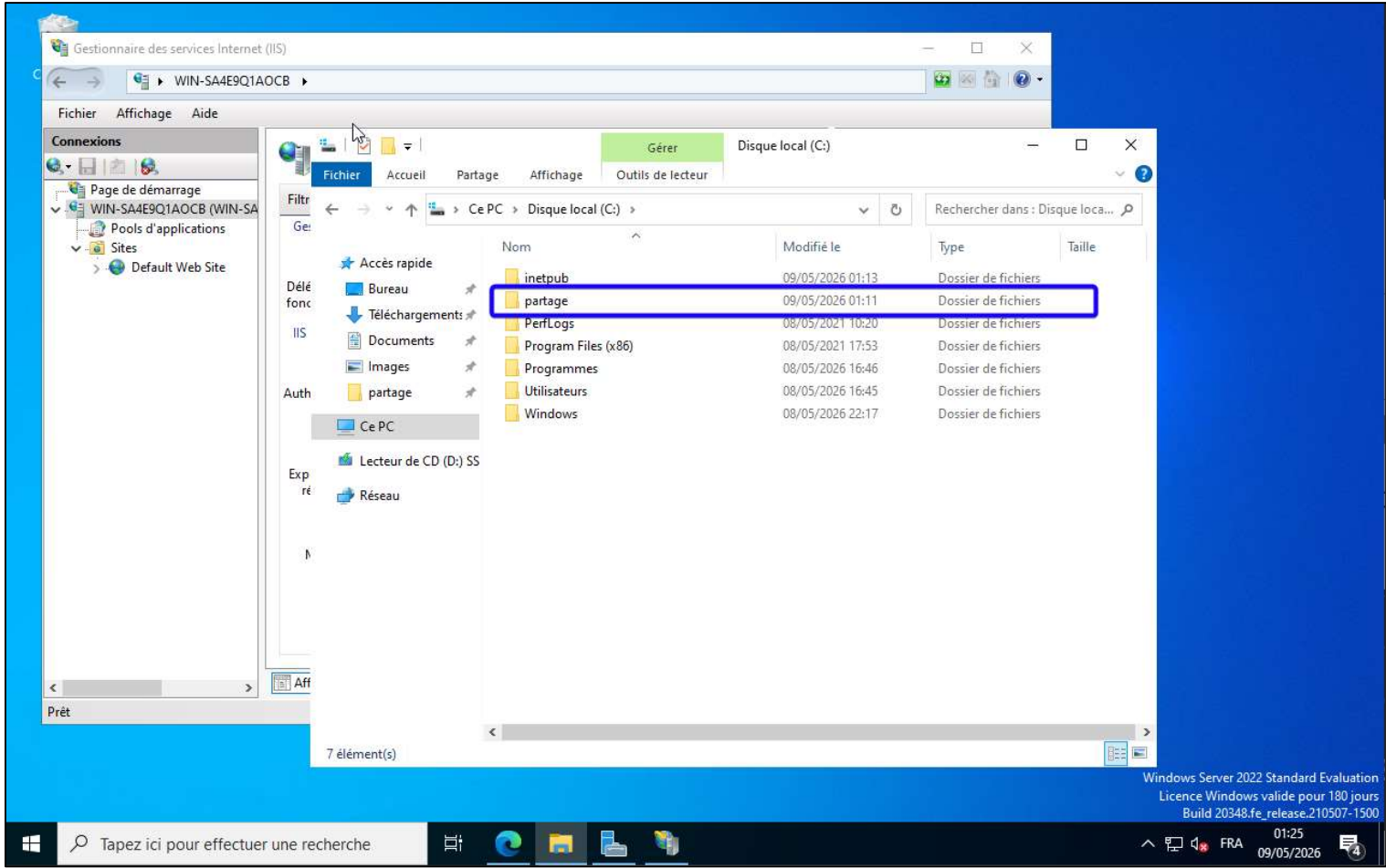
Intégration du site de l'entreprise dans le serveur Web :

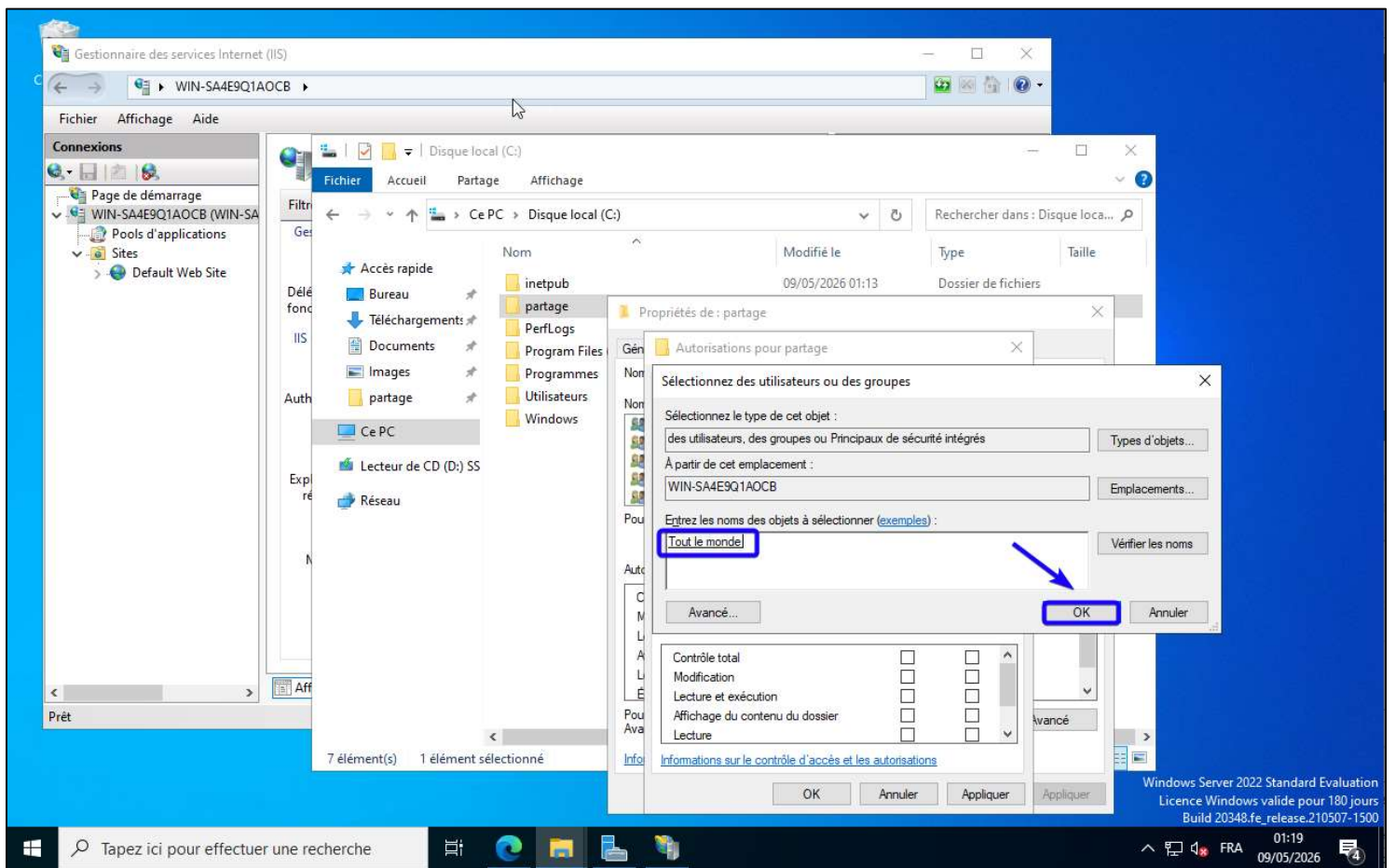
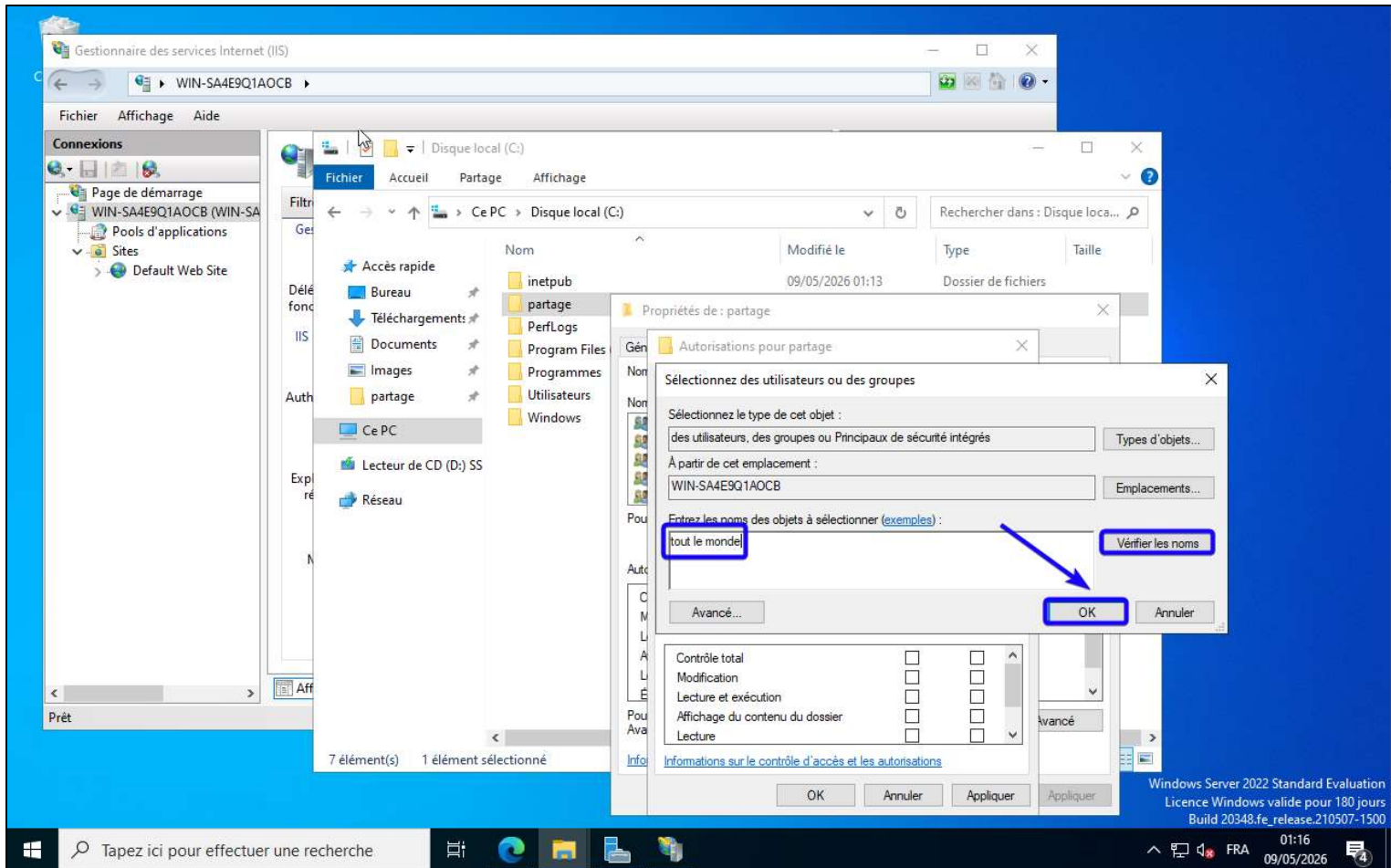
On va créer un dossier partagé sur notre serveur accessible sur réseau domestique :

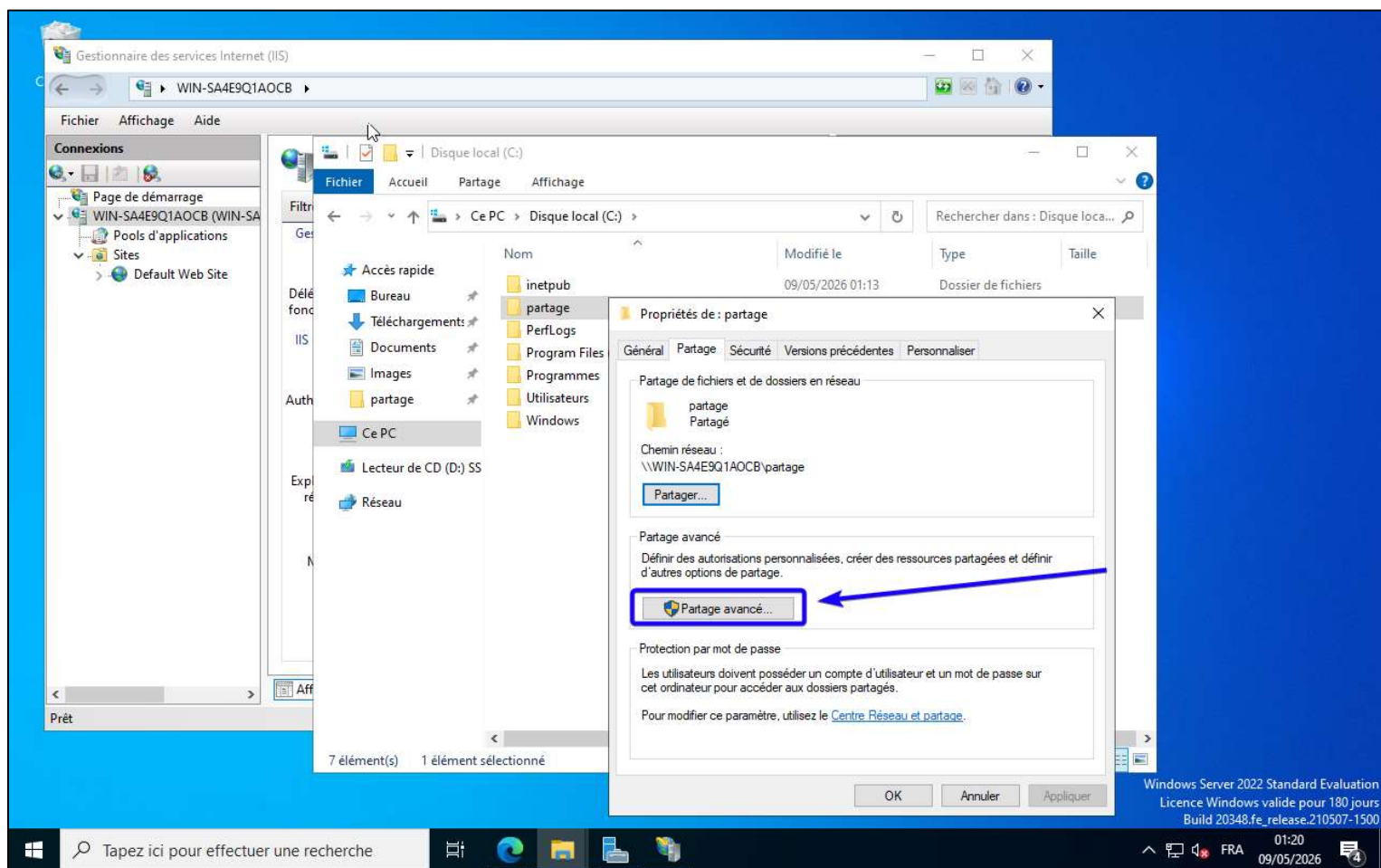
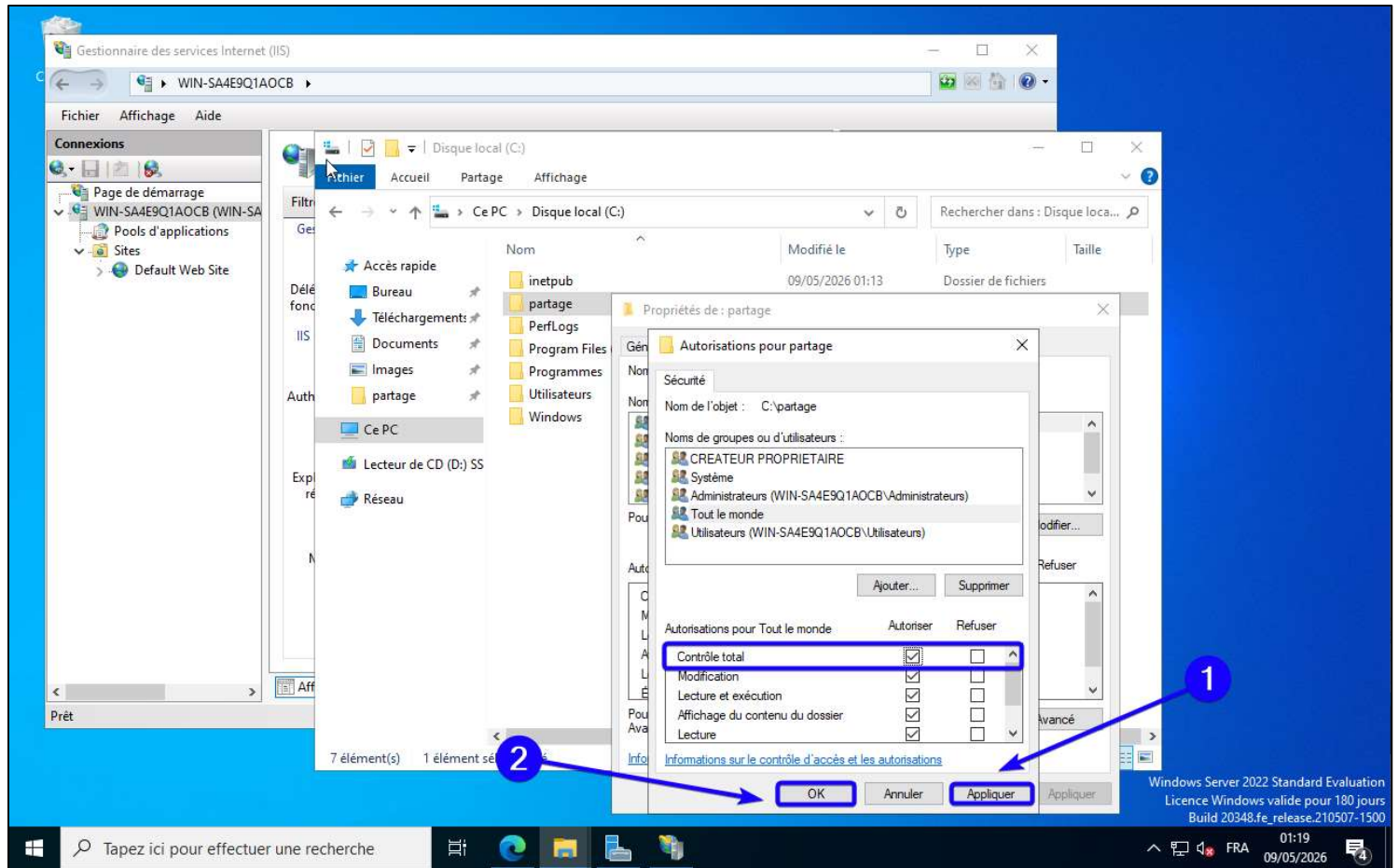
J'ai raccordé mon serveur Web à un Net Management Cloud0 pour qu'il soit accessible sur mon réseau.

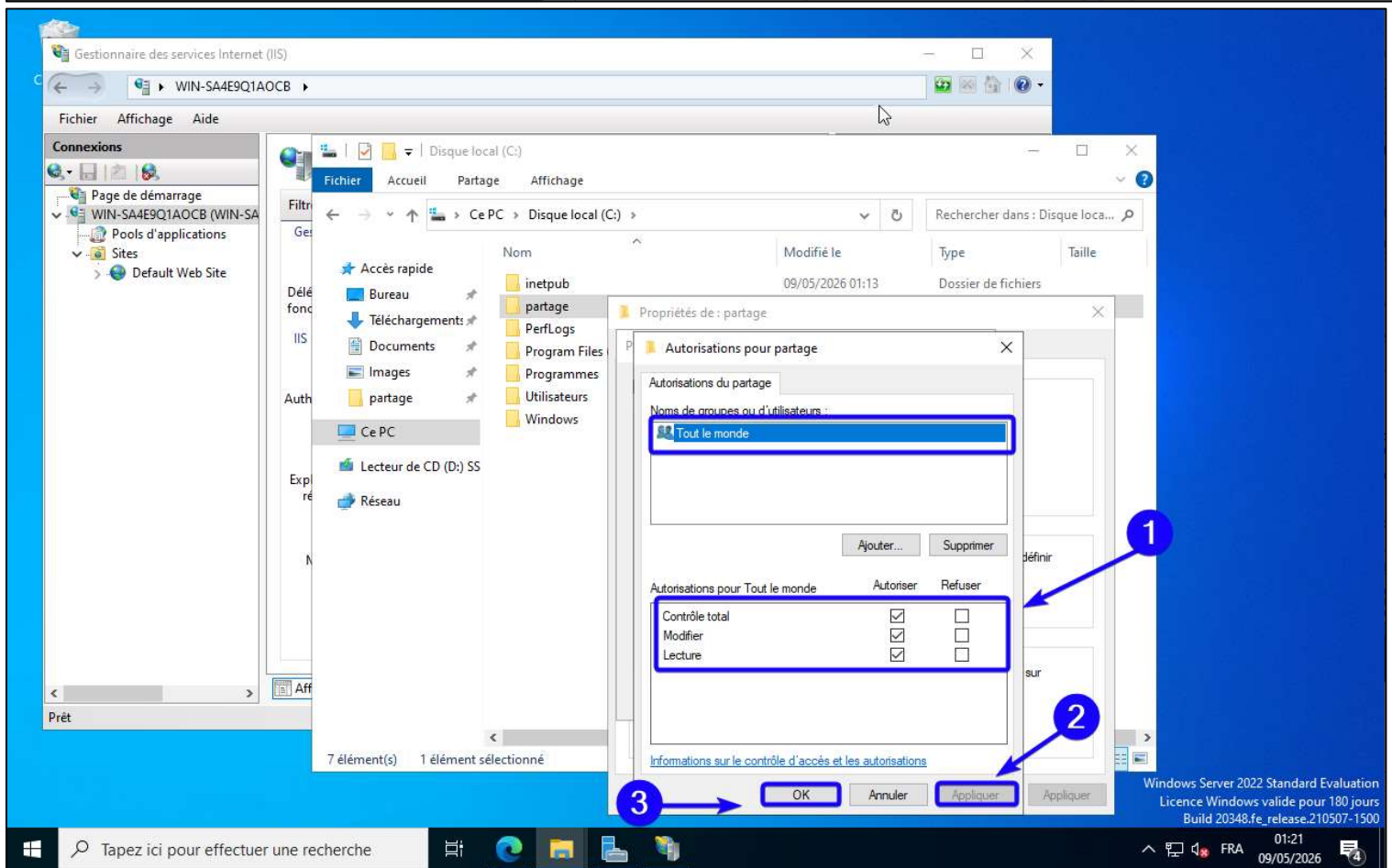
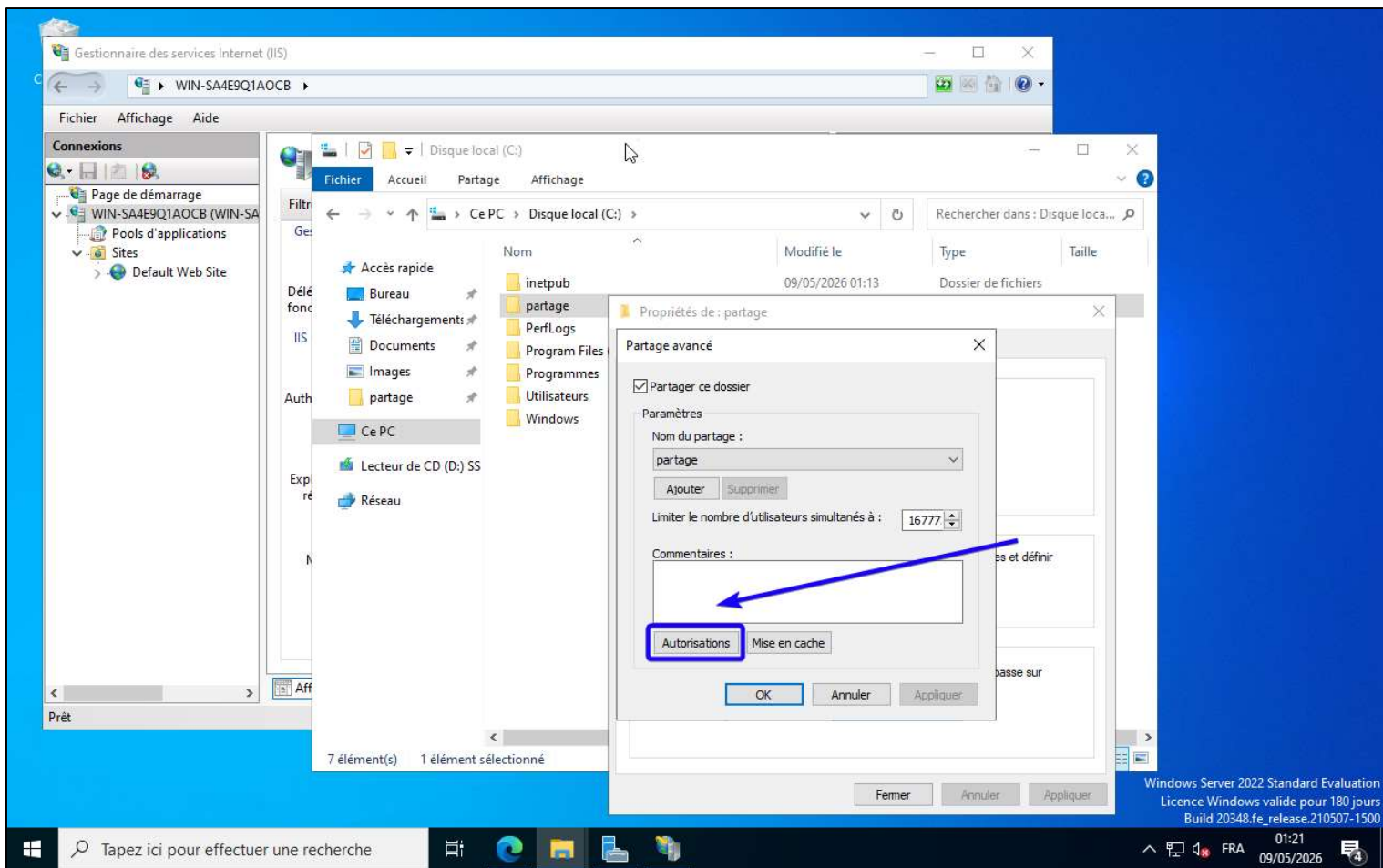


Je créer mon dossier partage :



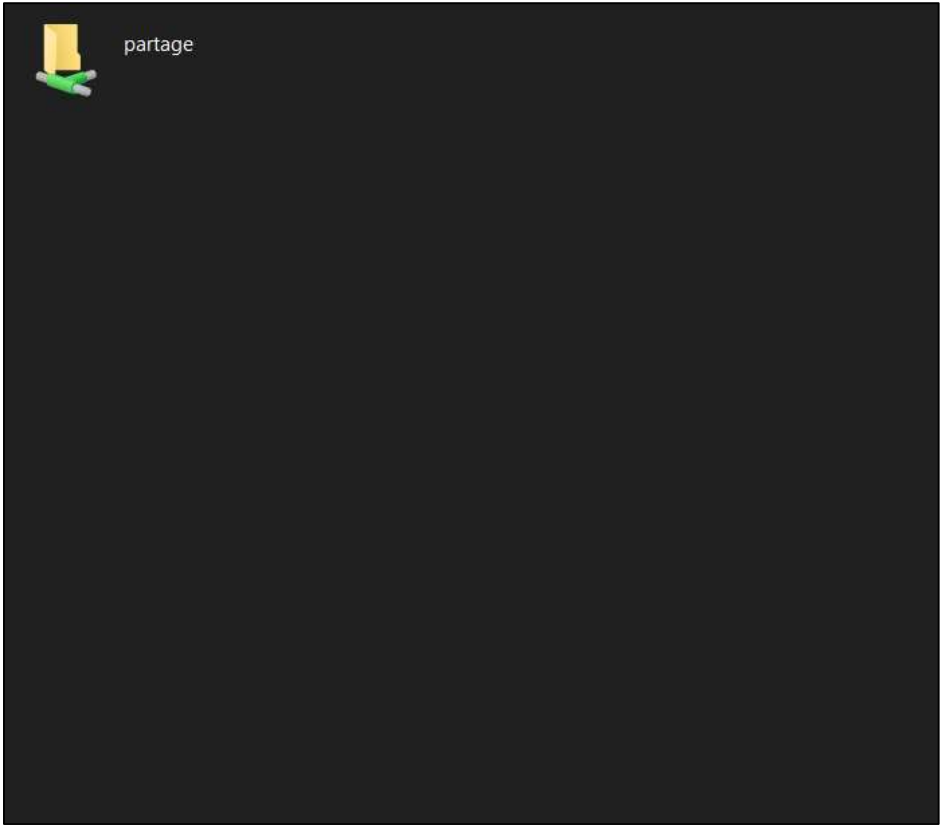




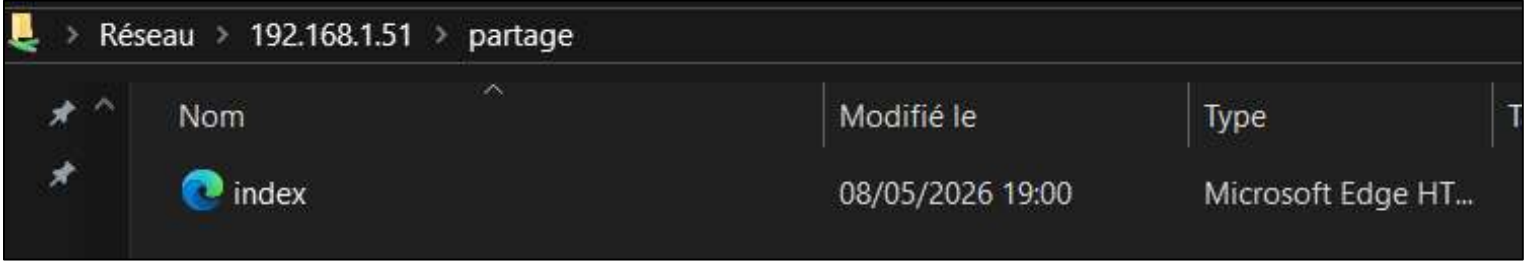


En tapant [\\@ServeurWeb](#) dans l'onglet Réseau de l'explorer :

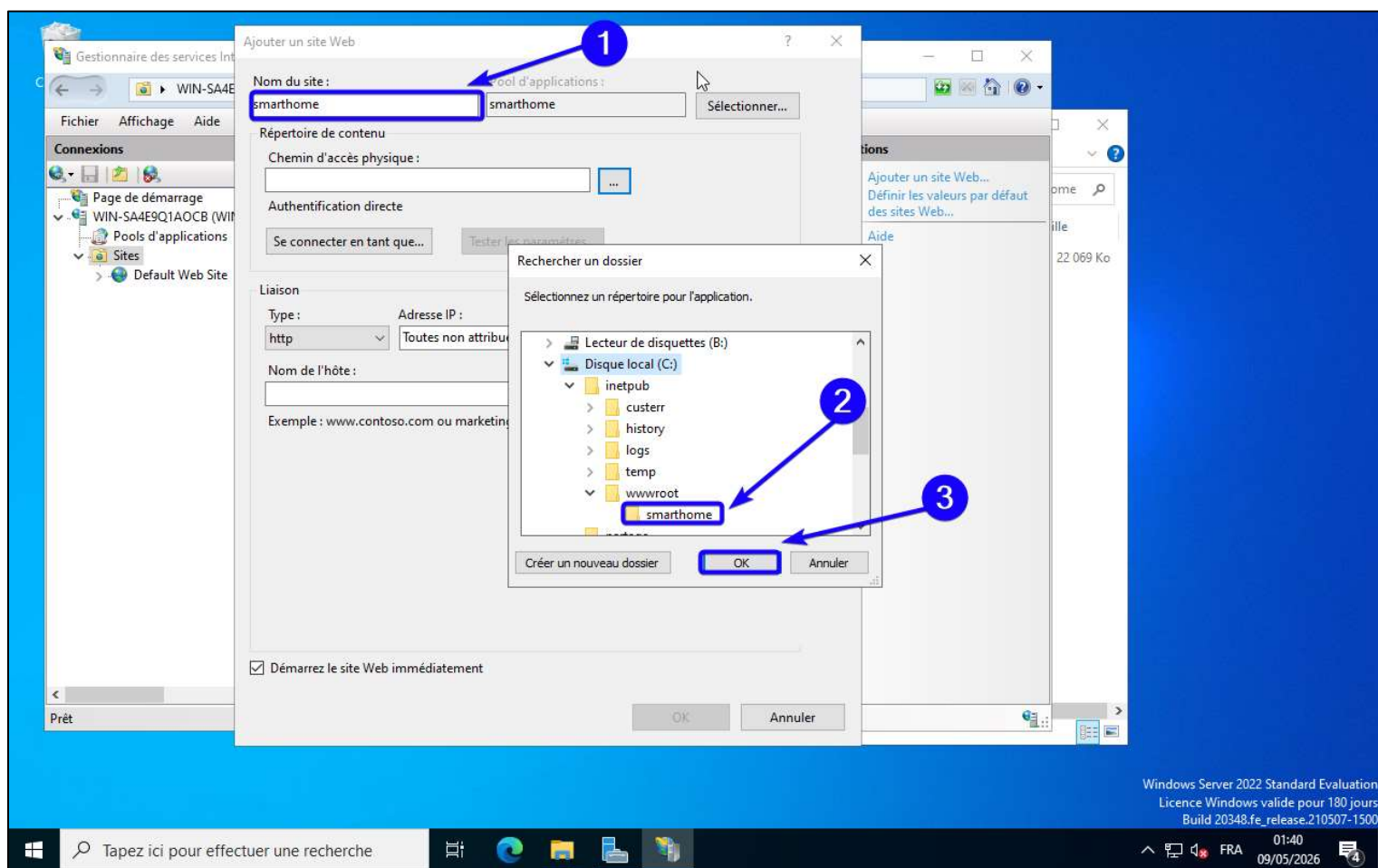
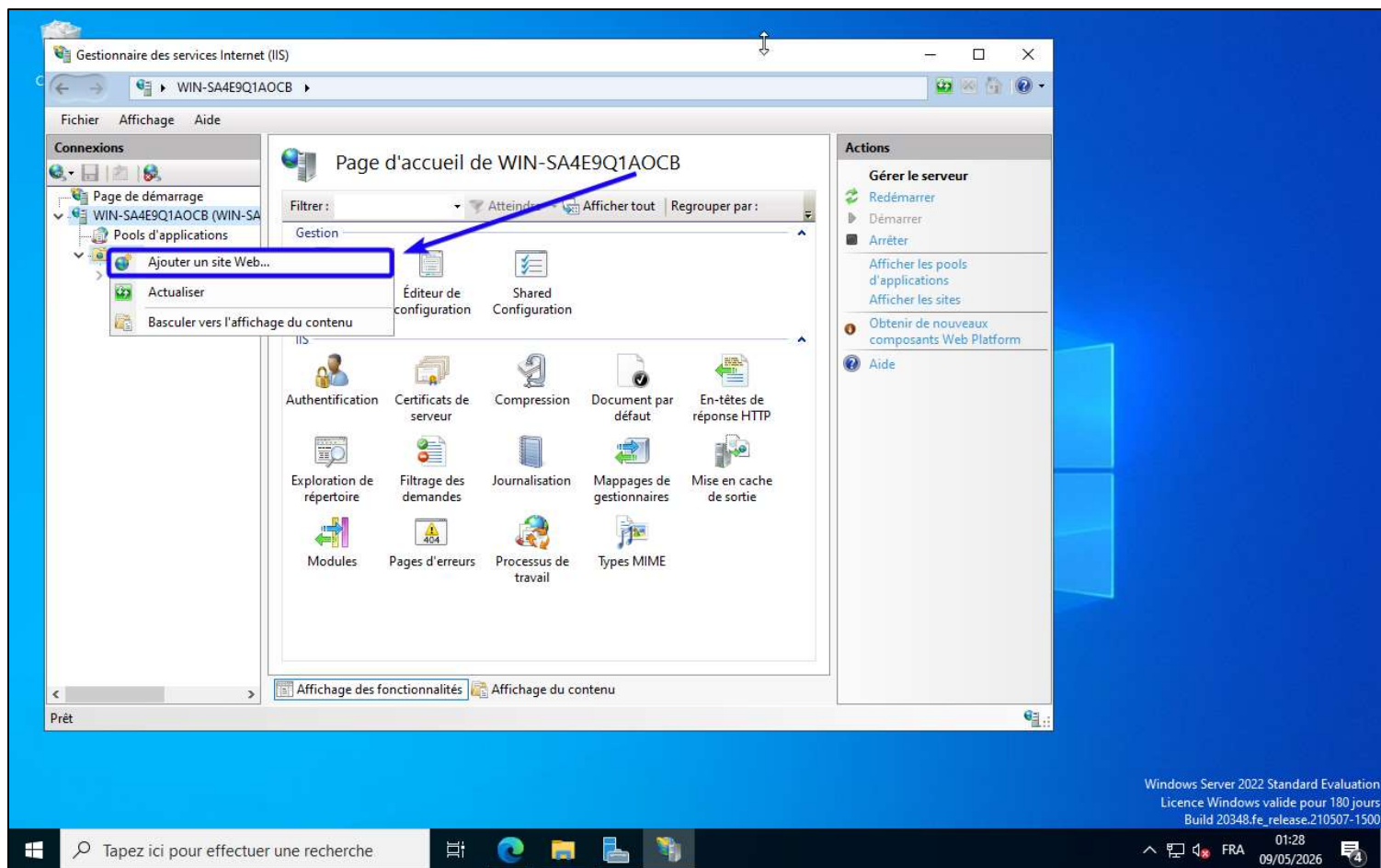
On se connecté avec les identifiants de l'admin du serveur on obtient :

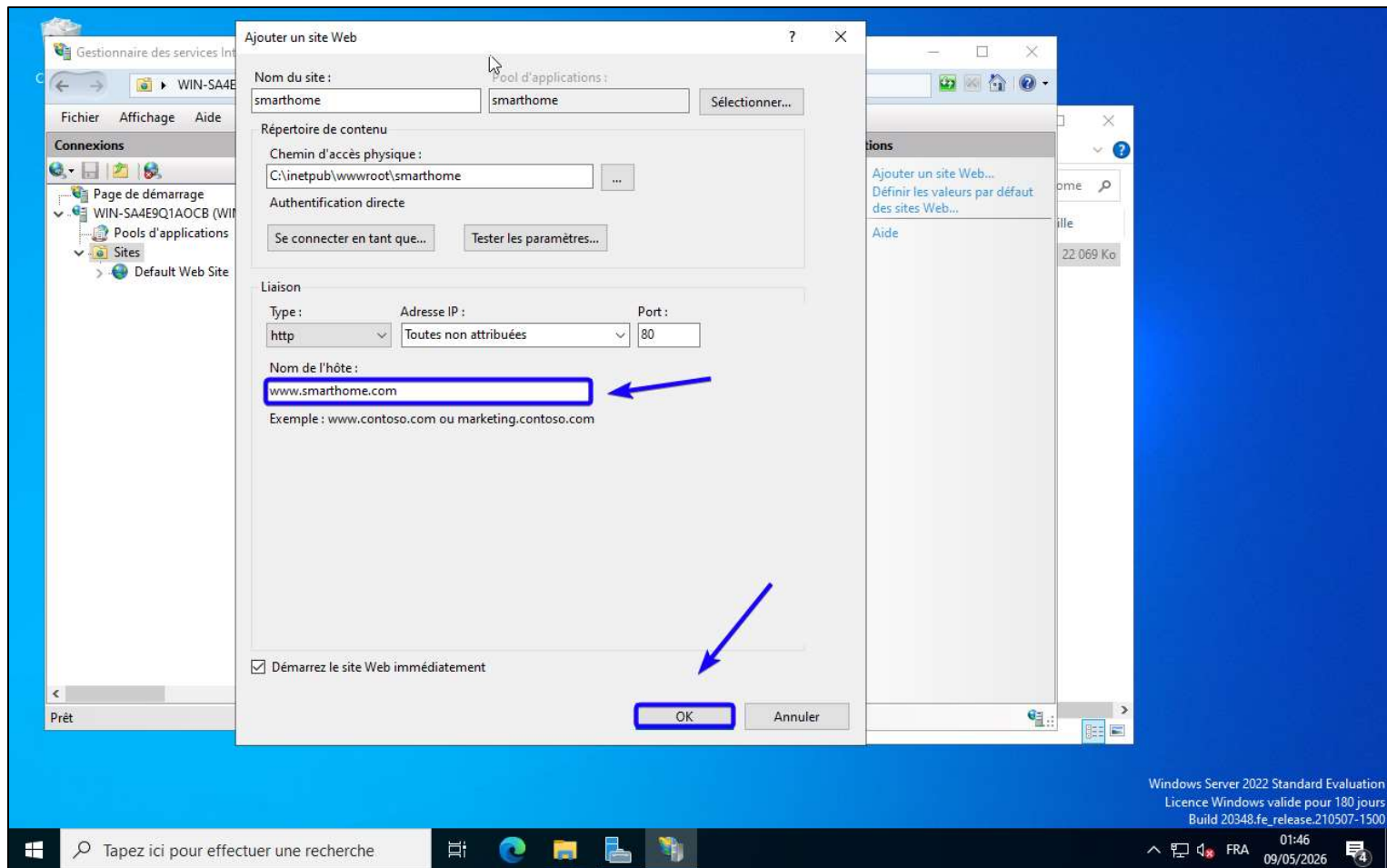


Ayant les droits de lecture & écriture on insérer et modifier le contenu du dossier « partage ».



Maintenant on va intégrer héberger le site sur votre serveur Web.



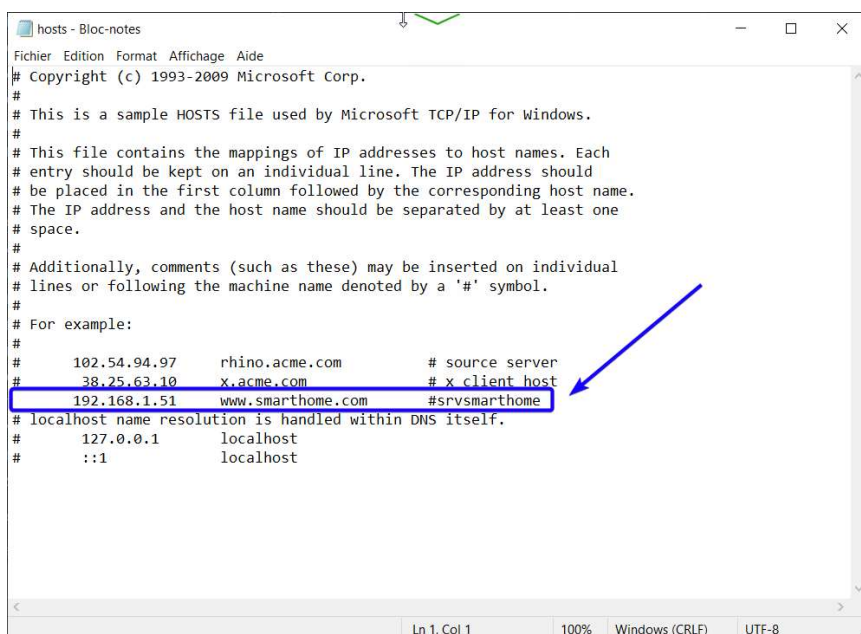


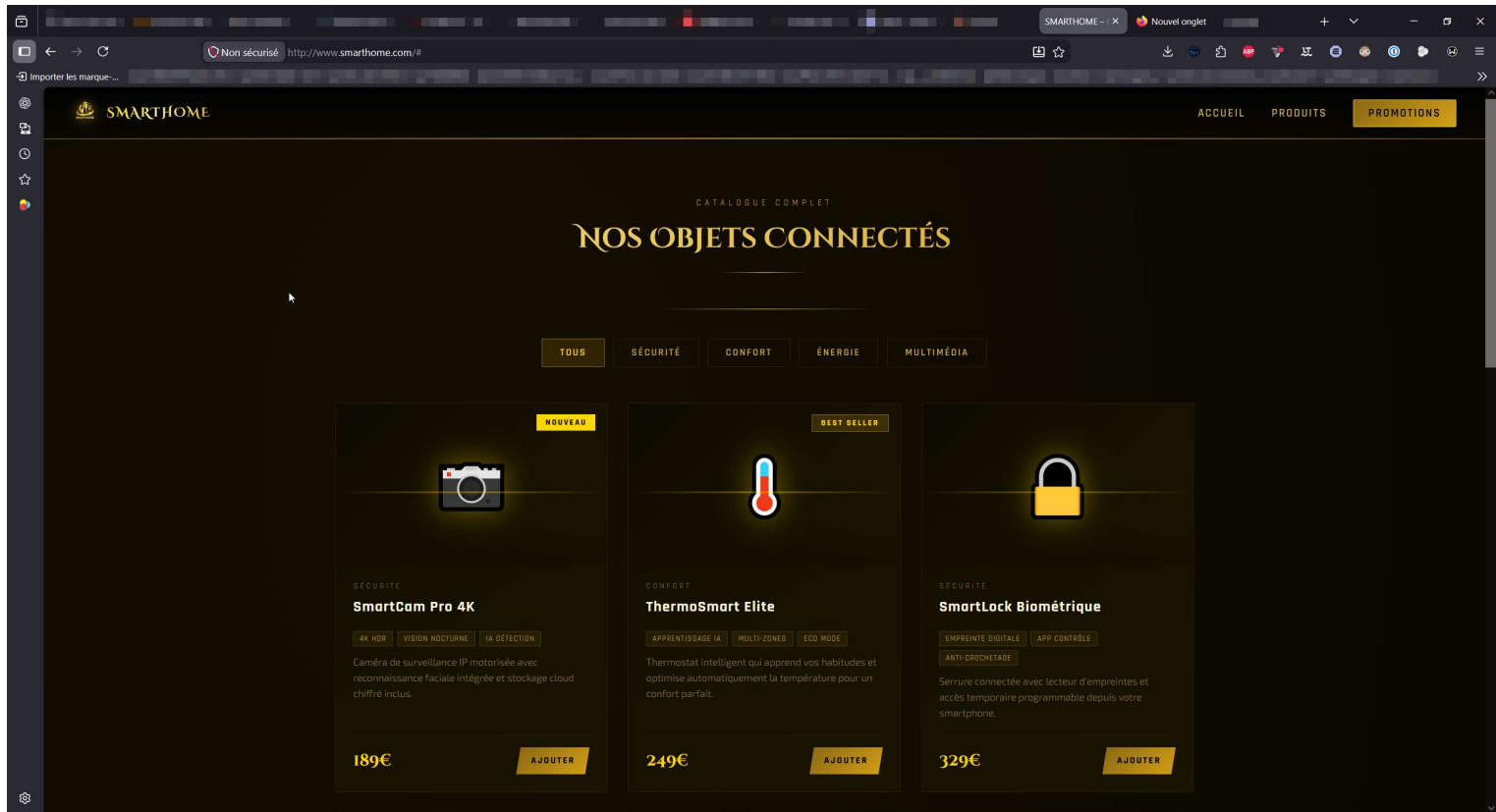
Test de Validation :

Tester le site web sur votre navigateur :

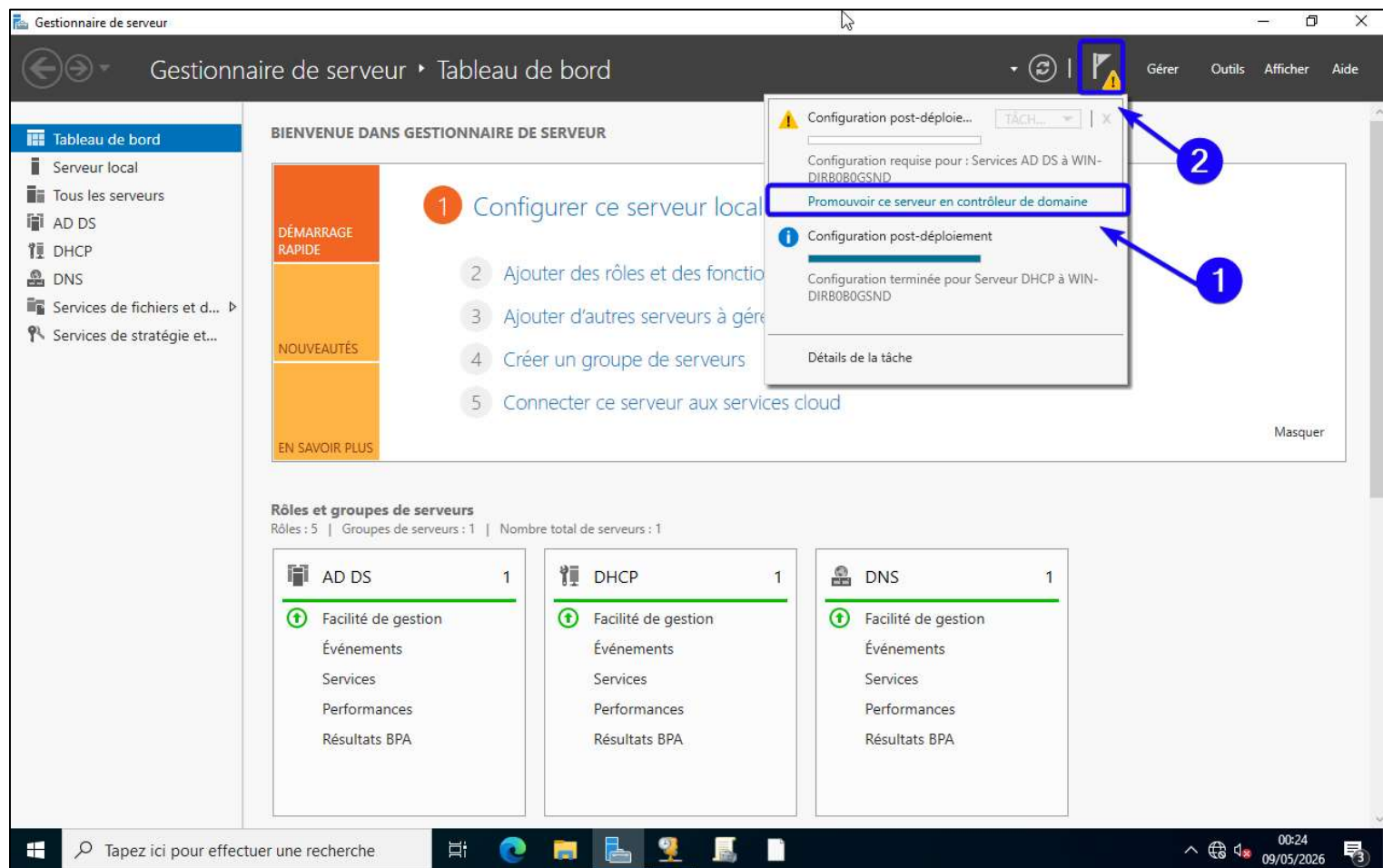
C:\Windows\System32\drivers\etc\hosts

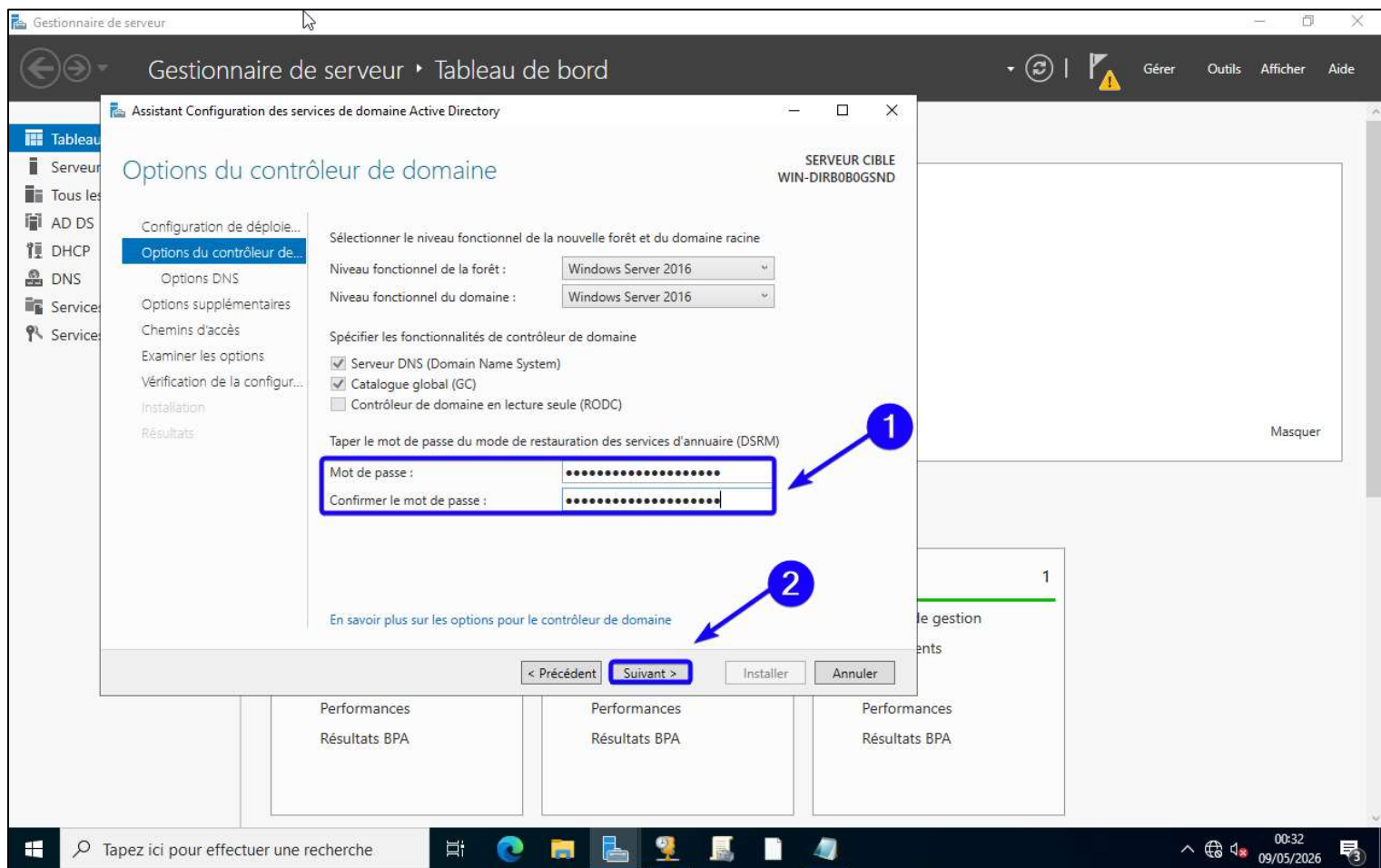
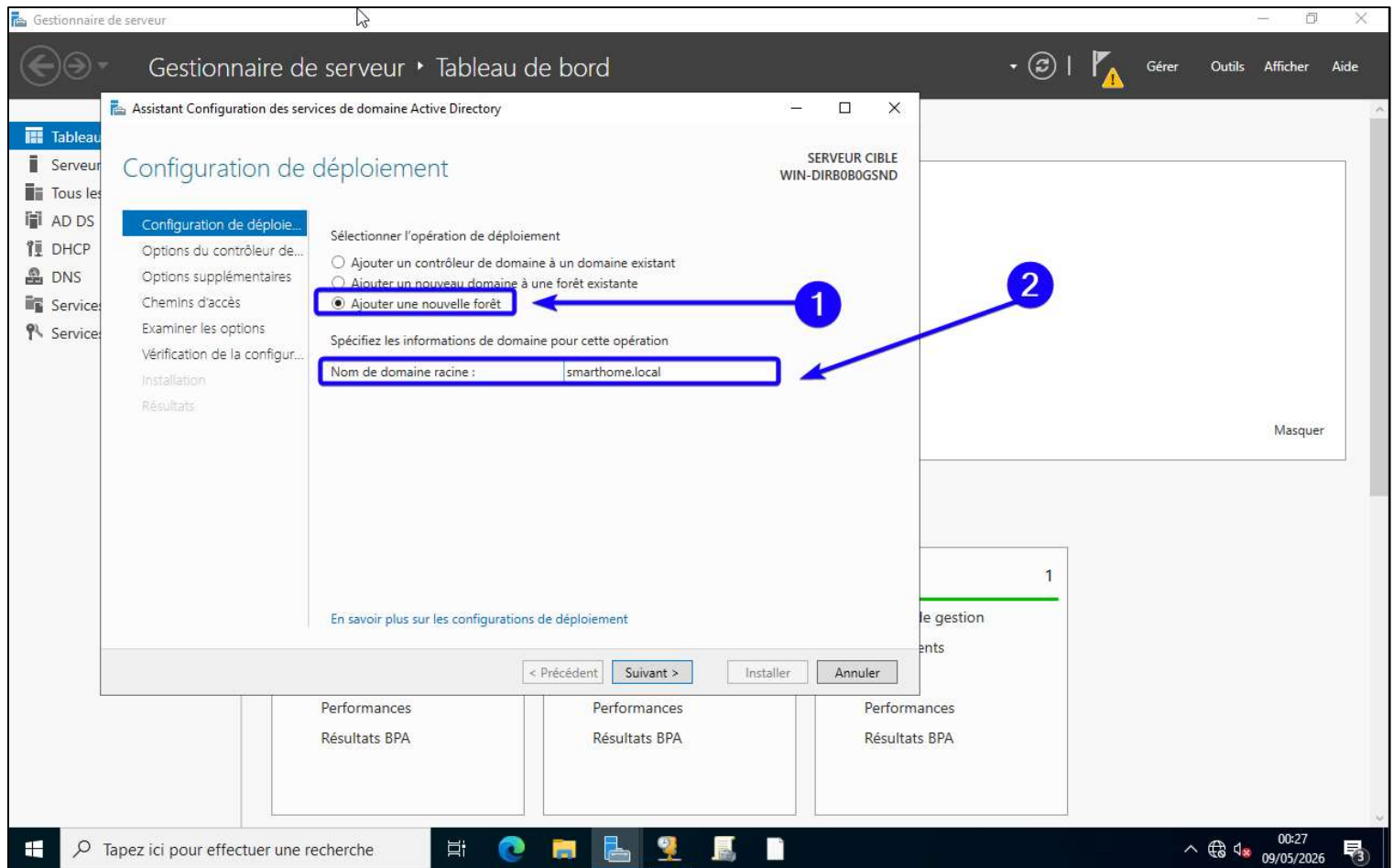
Modifier votre fichiers hosts comme nous n'avons pas de **redirection DNS**.

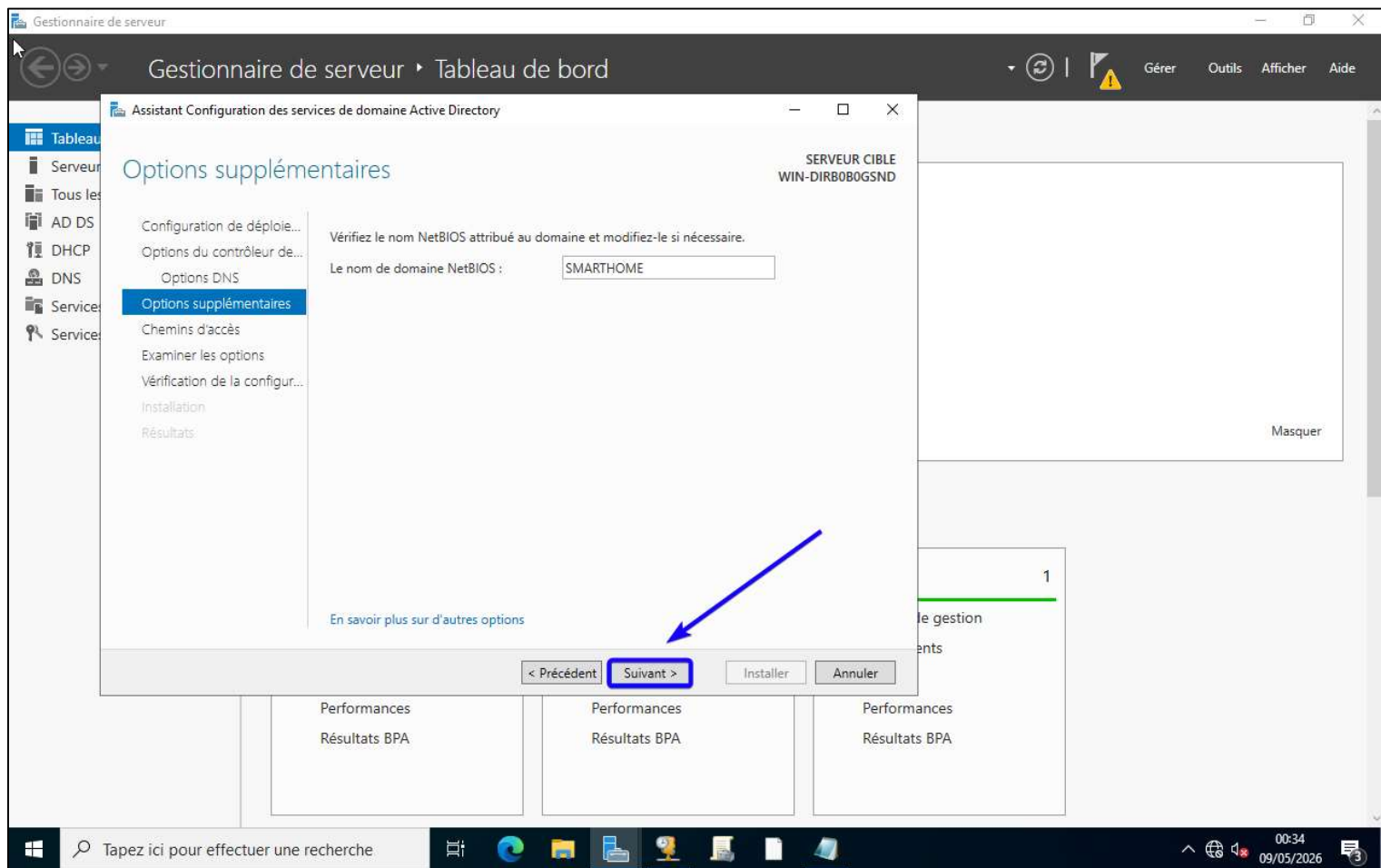
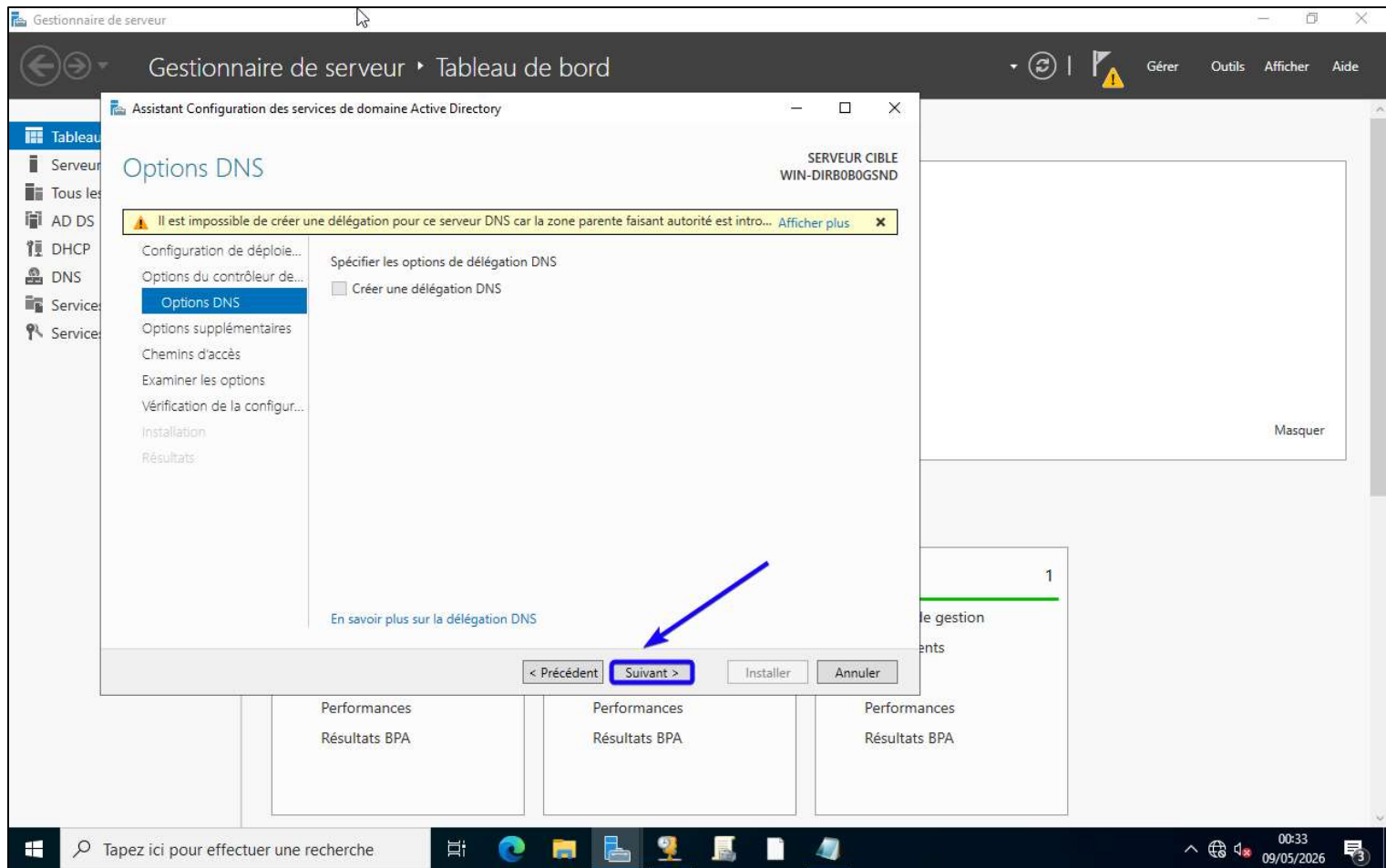


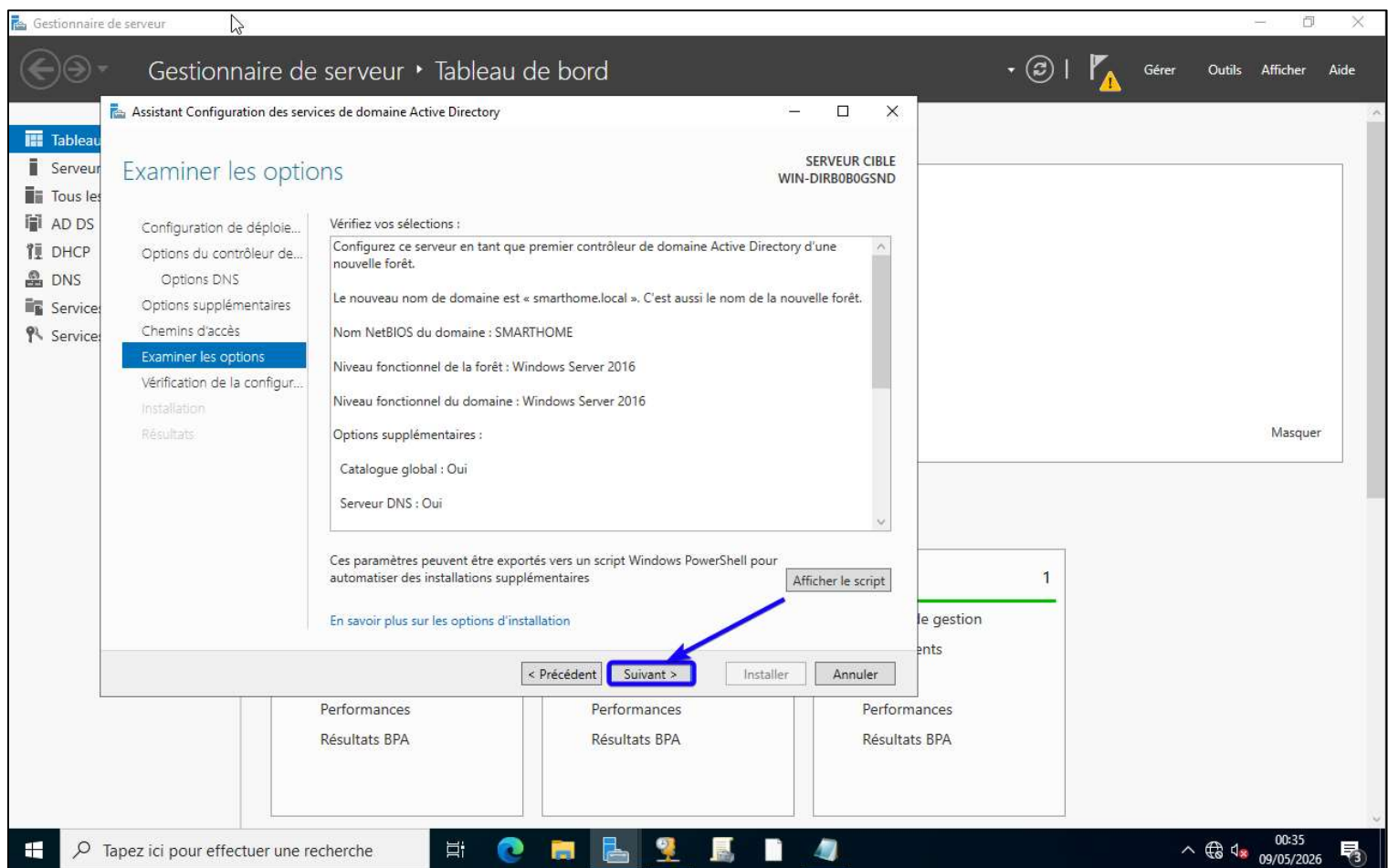
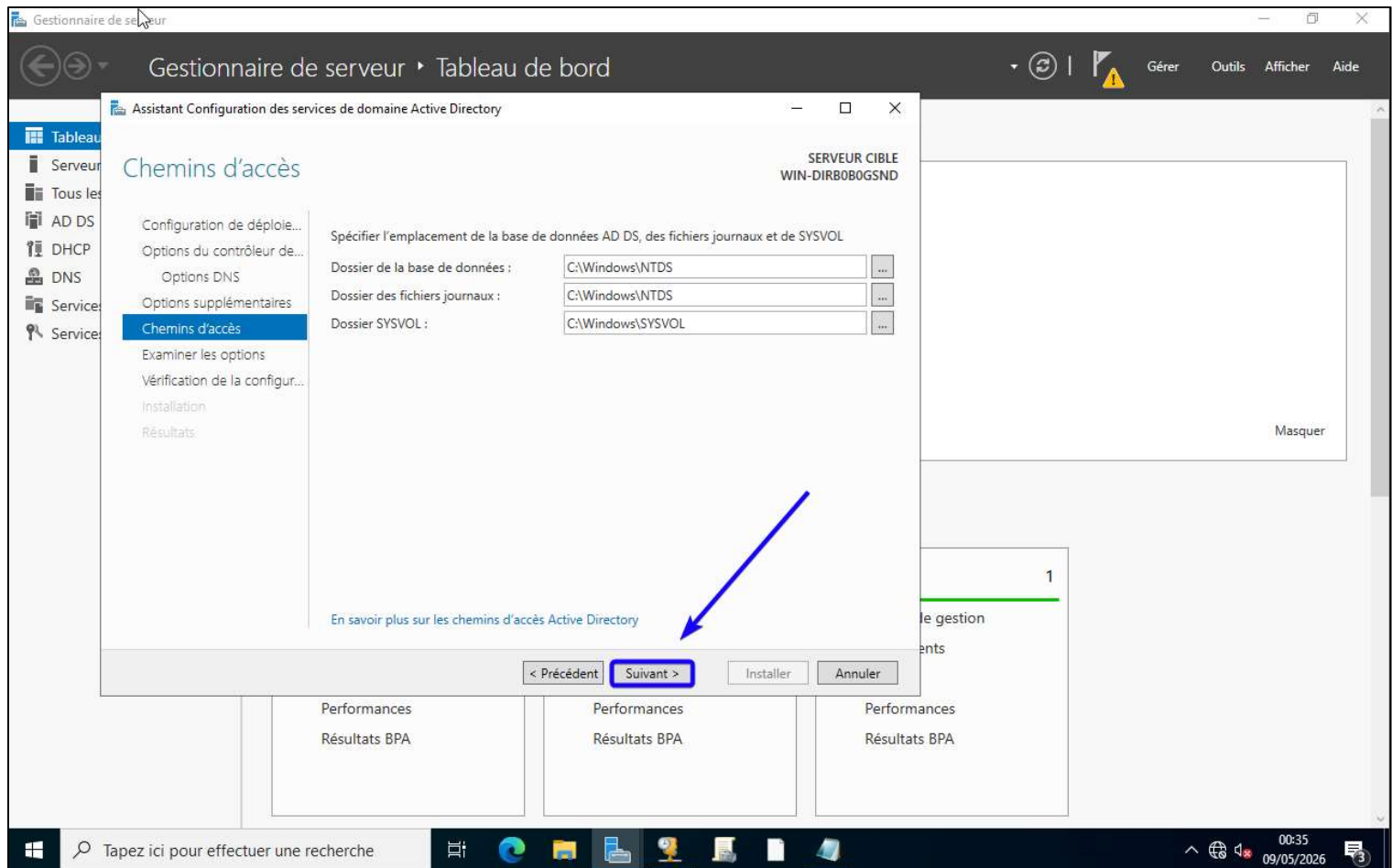


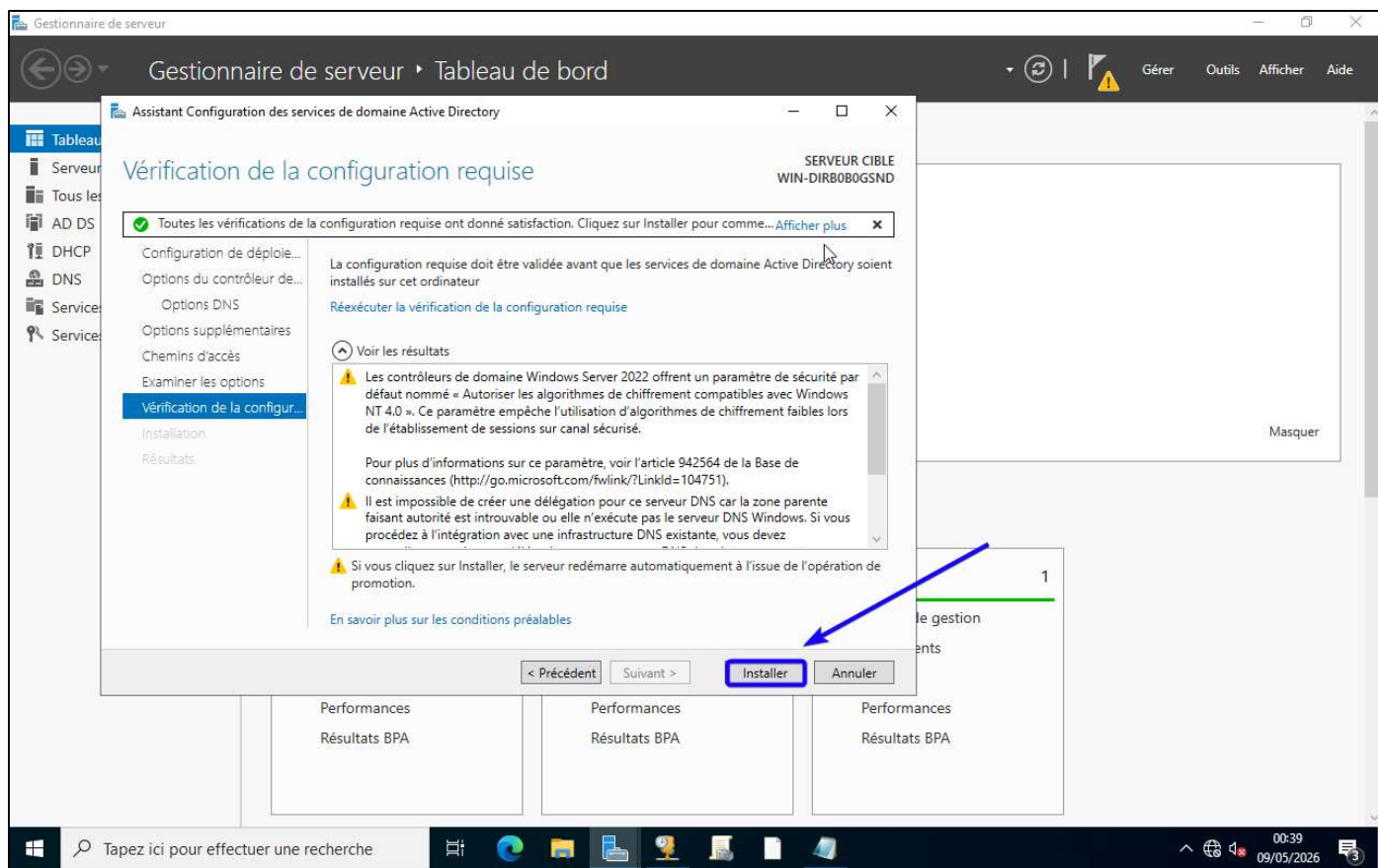
Créer le contrôleur de domaine de SmartHome :



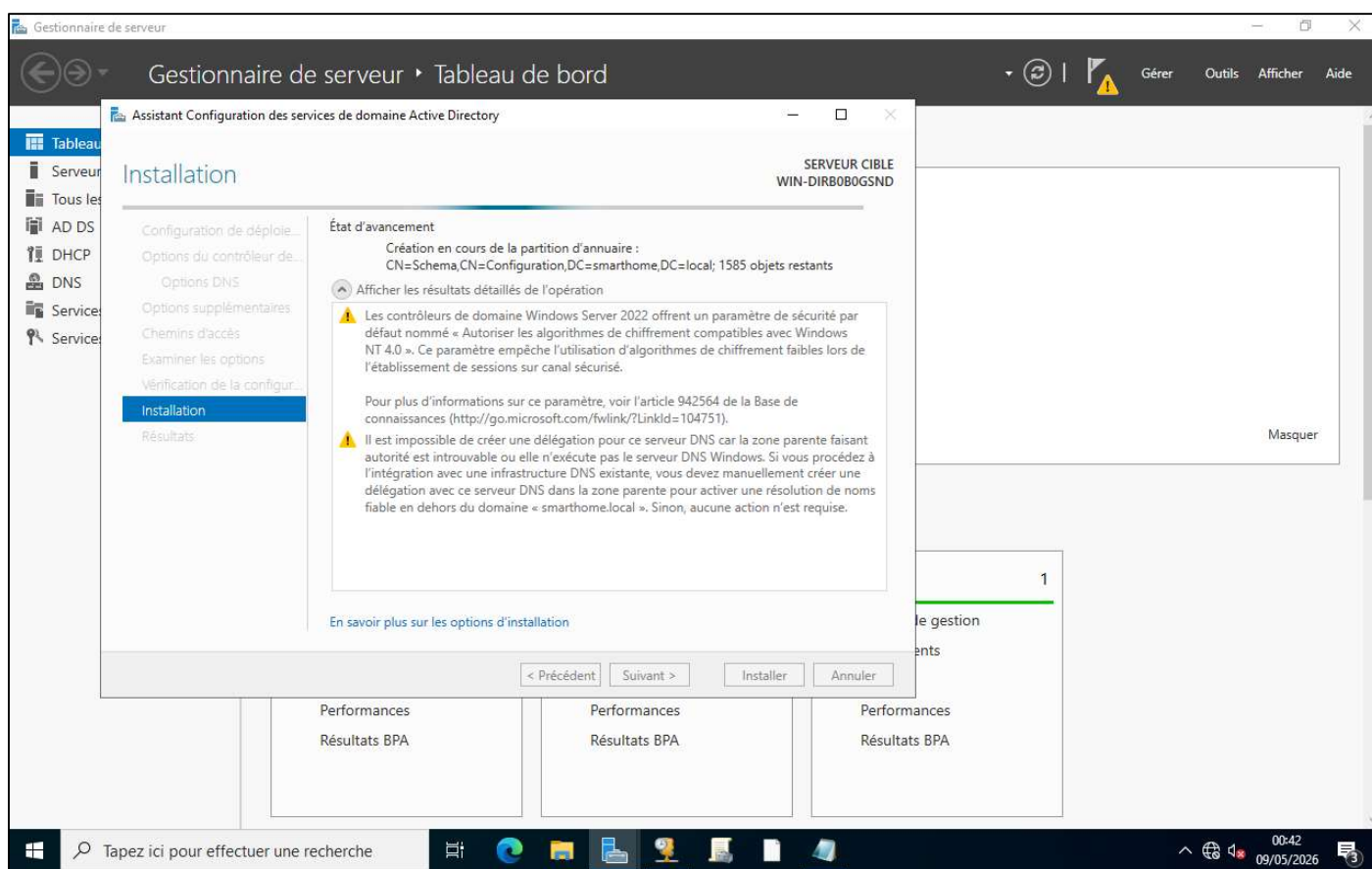








 Patienter....

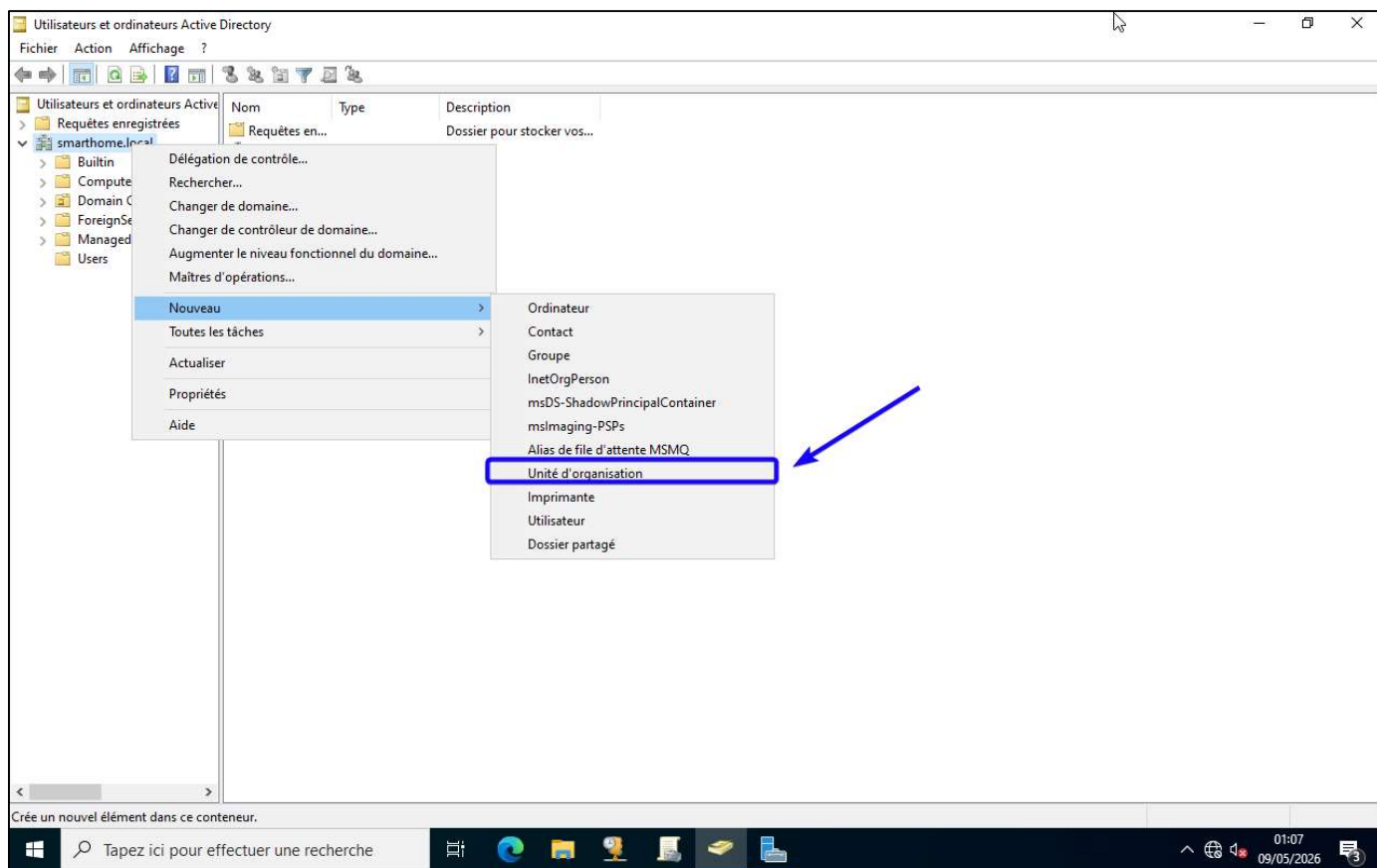


La machine virtuelle va redémarrer...

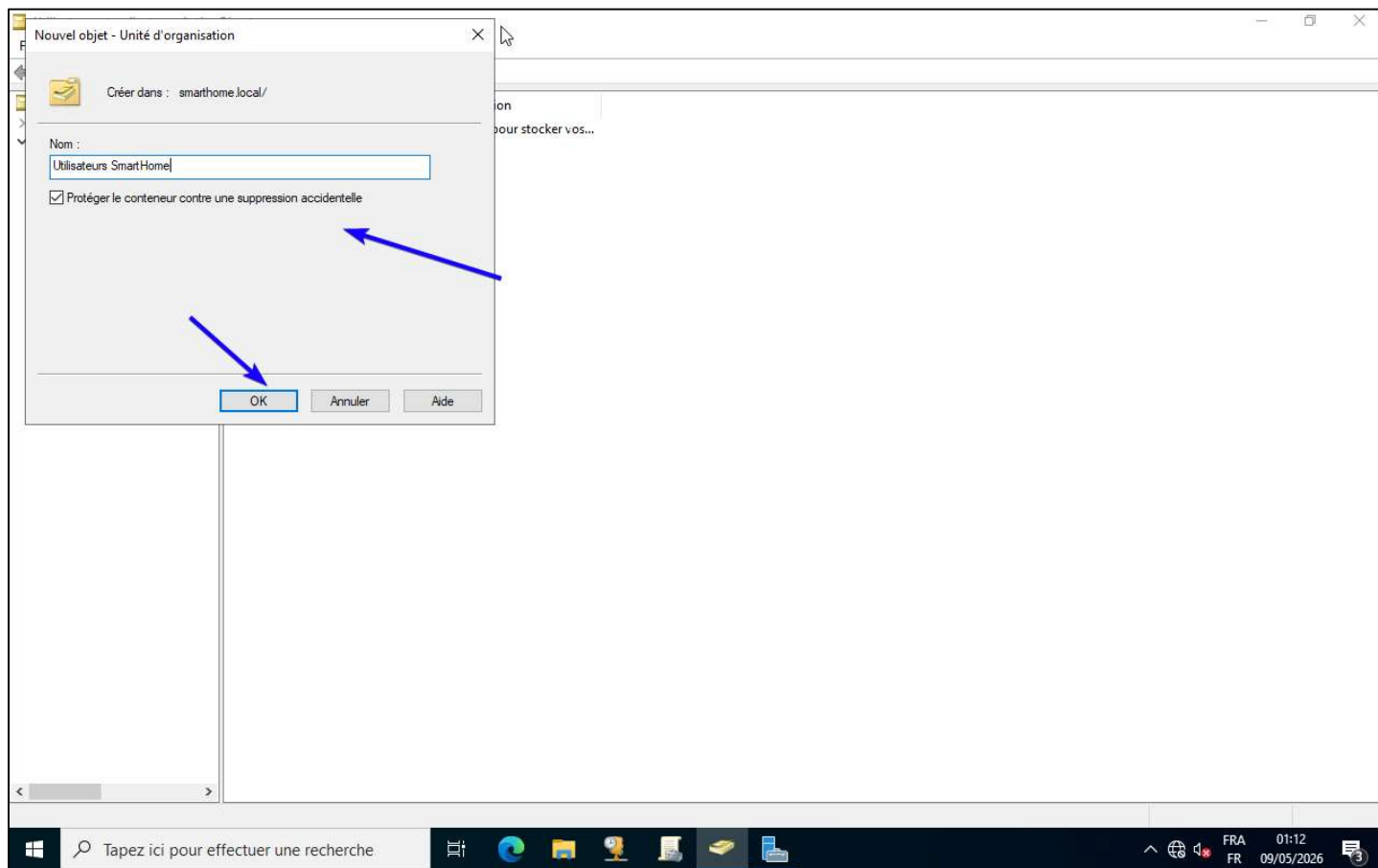


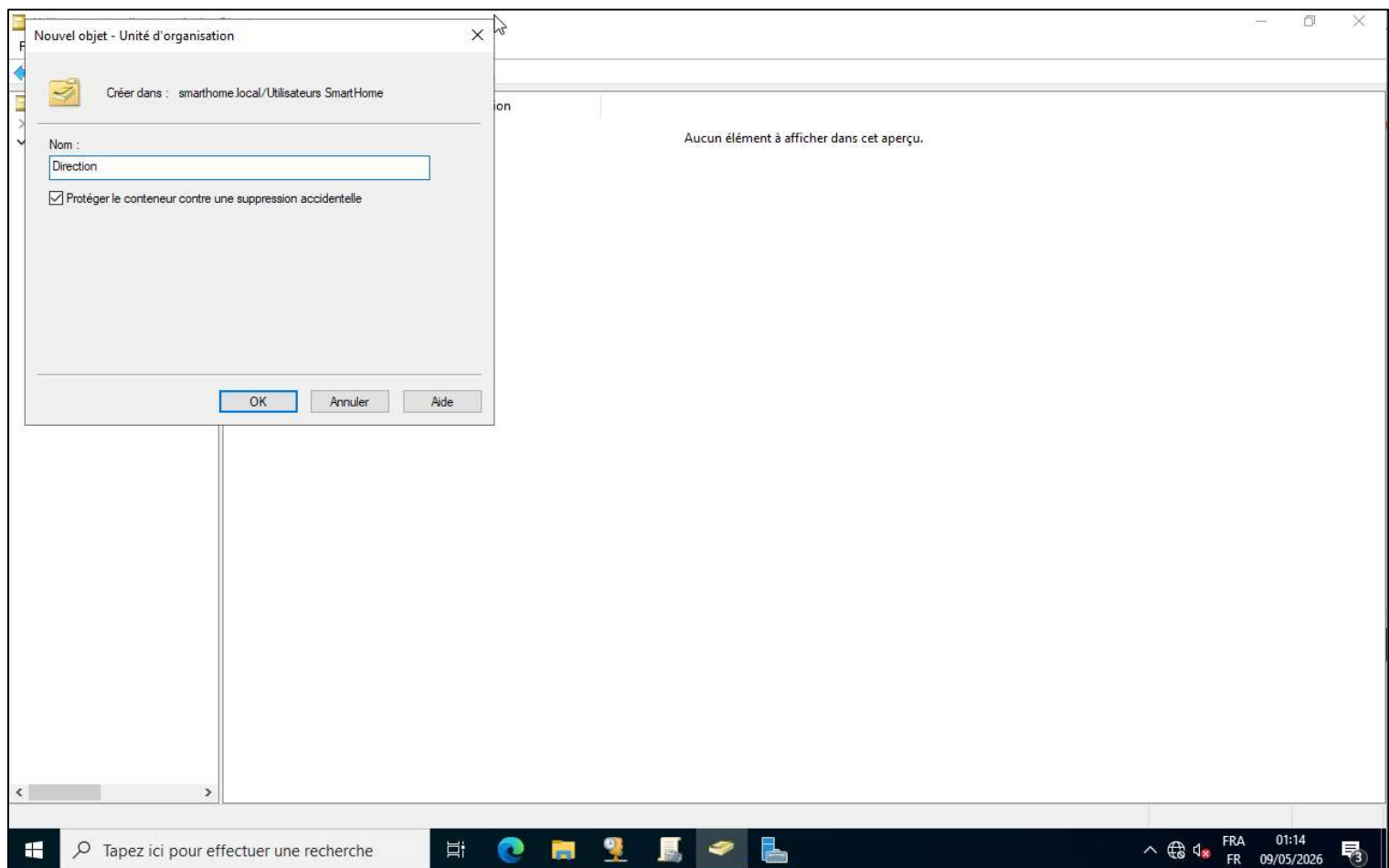
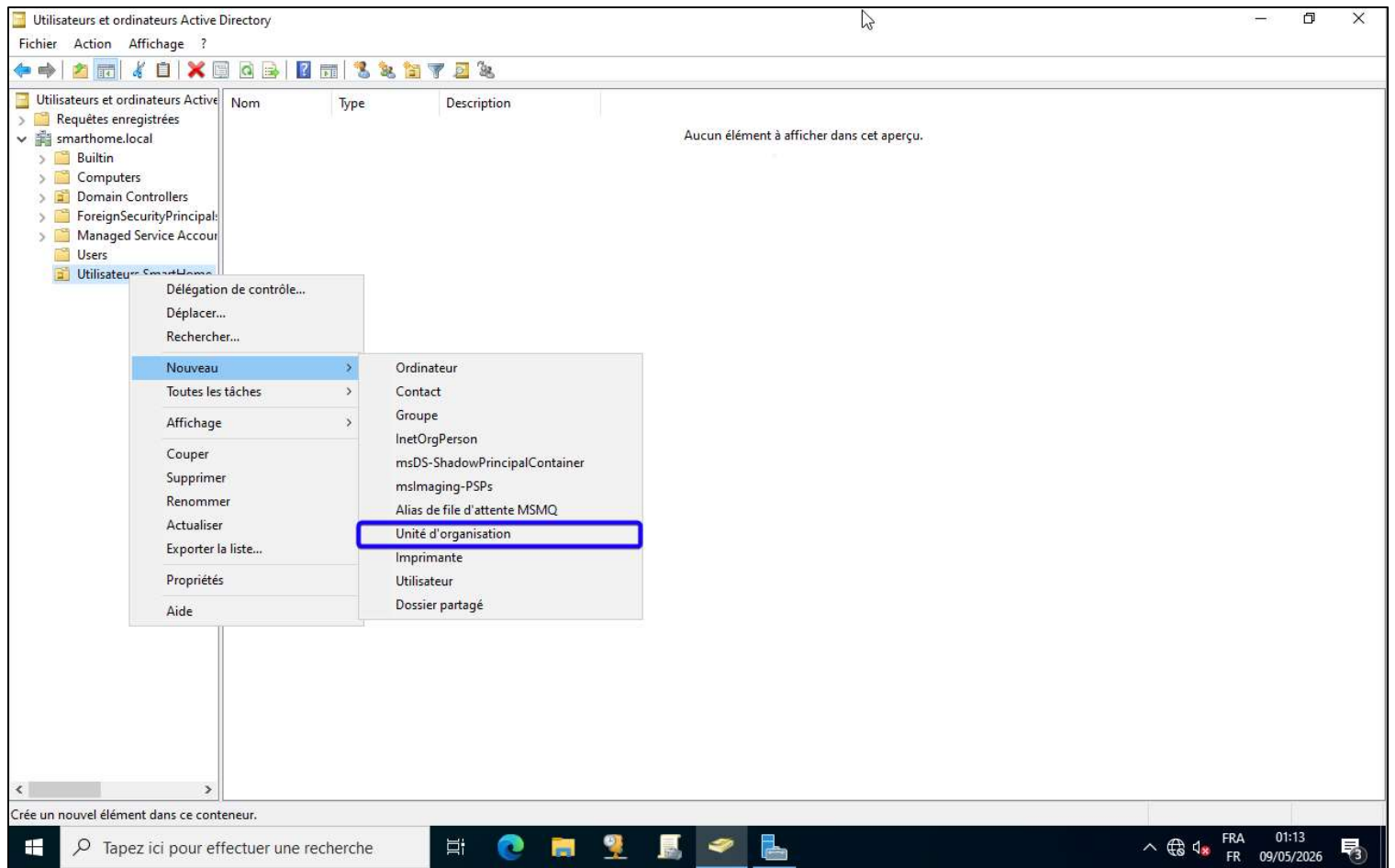
Application des paramètres de l'ordinateur

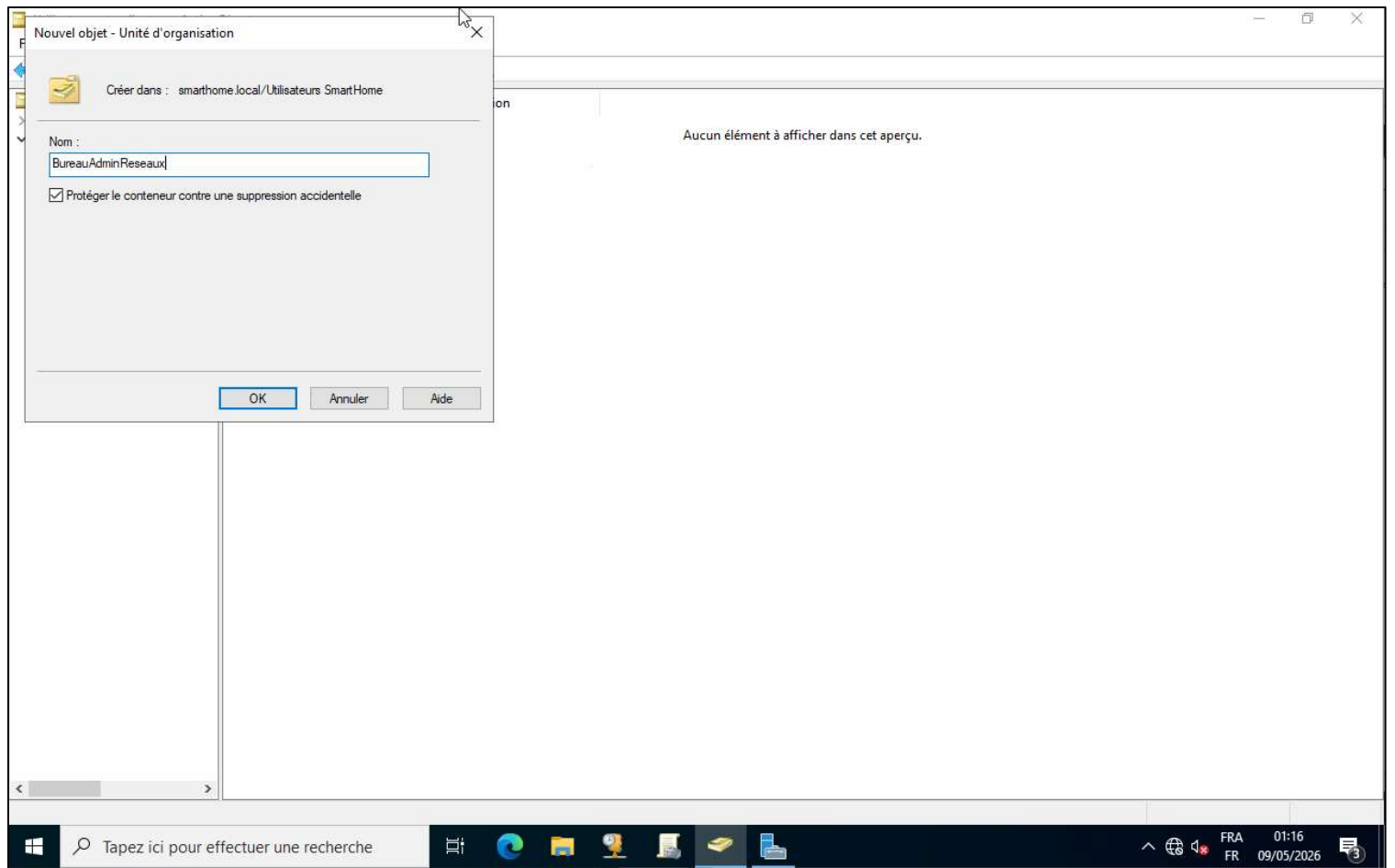
Le domaine de l'entreprise et maintenant créer on va pouvoir créer nos Unités d'organisation avec nos utilisateurs.



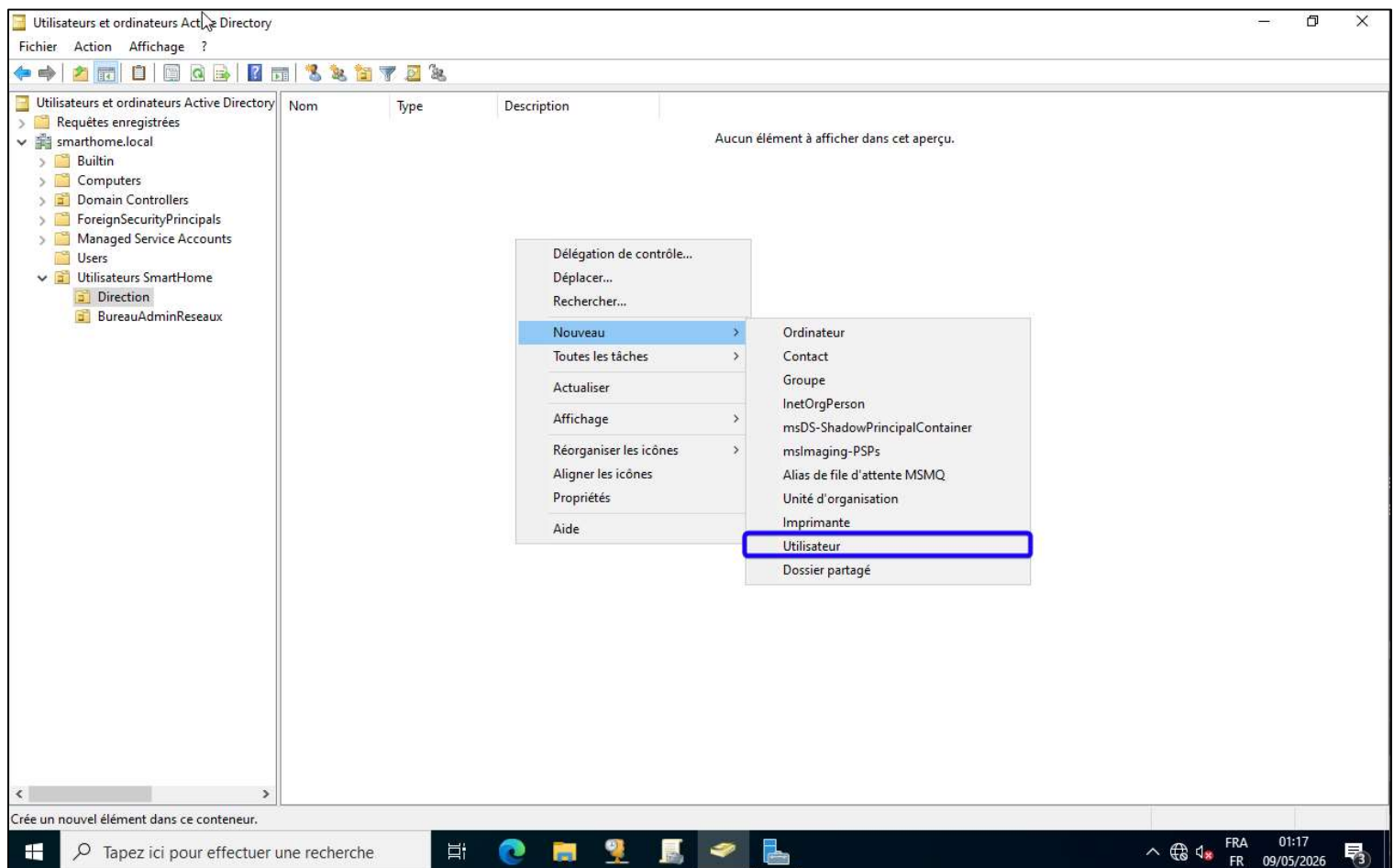
UO globale pour tous nos services :



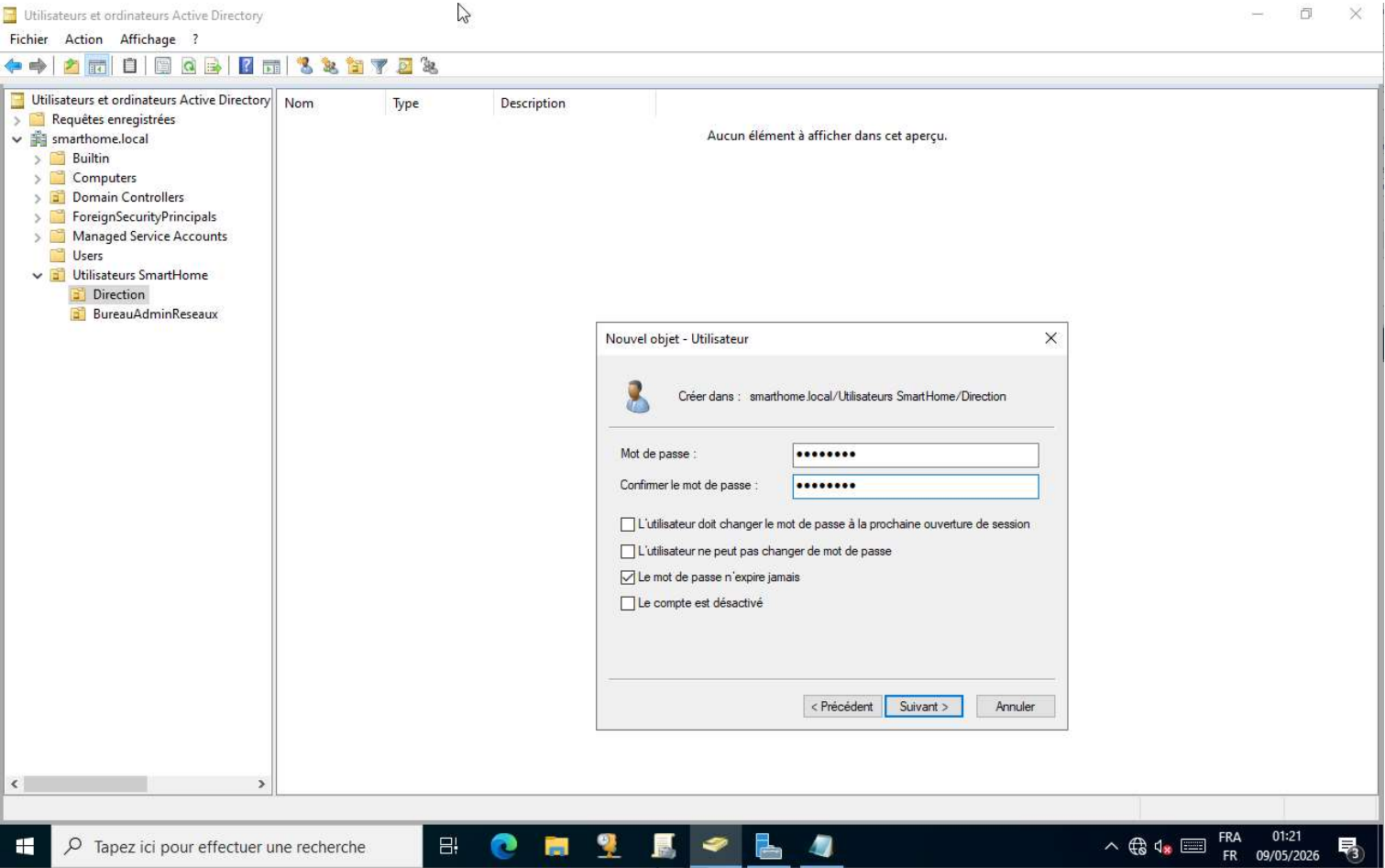
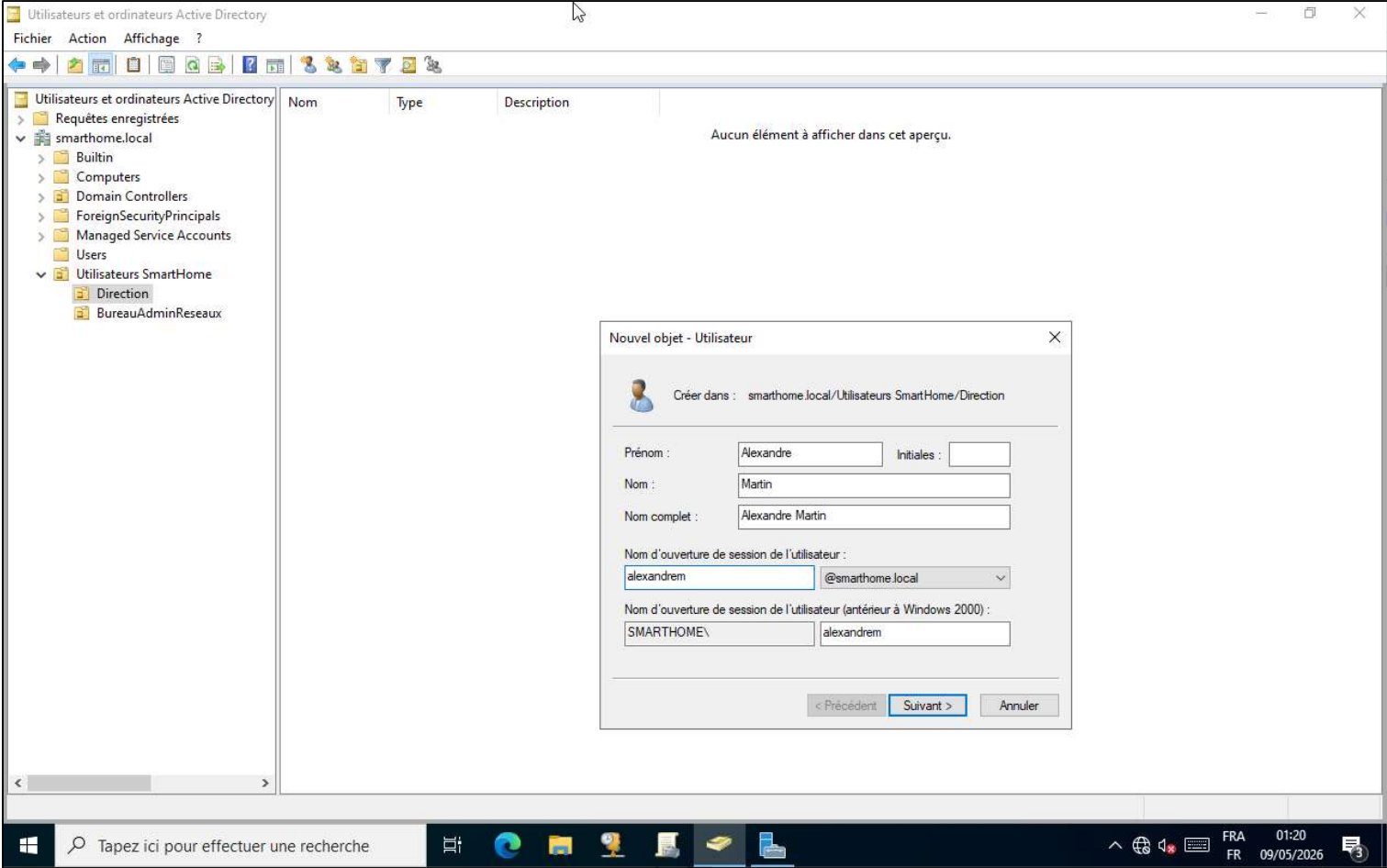


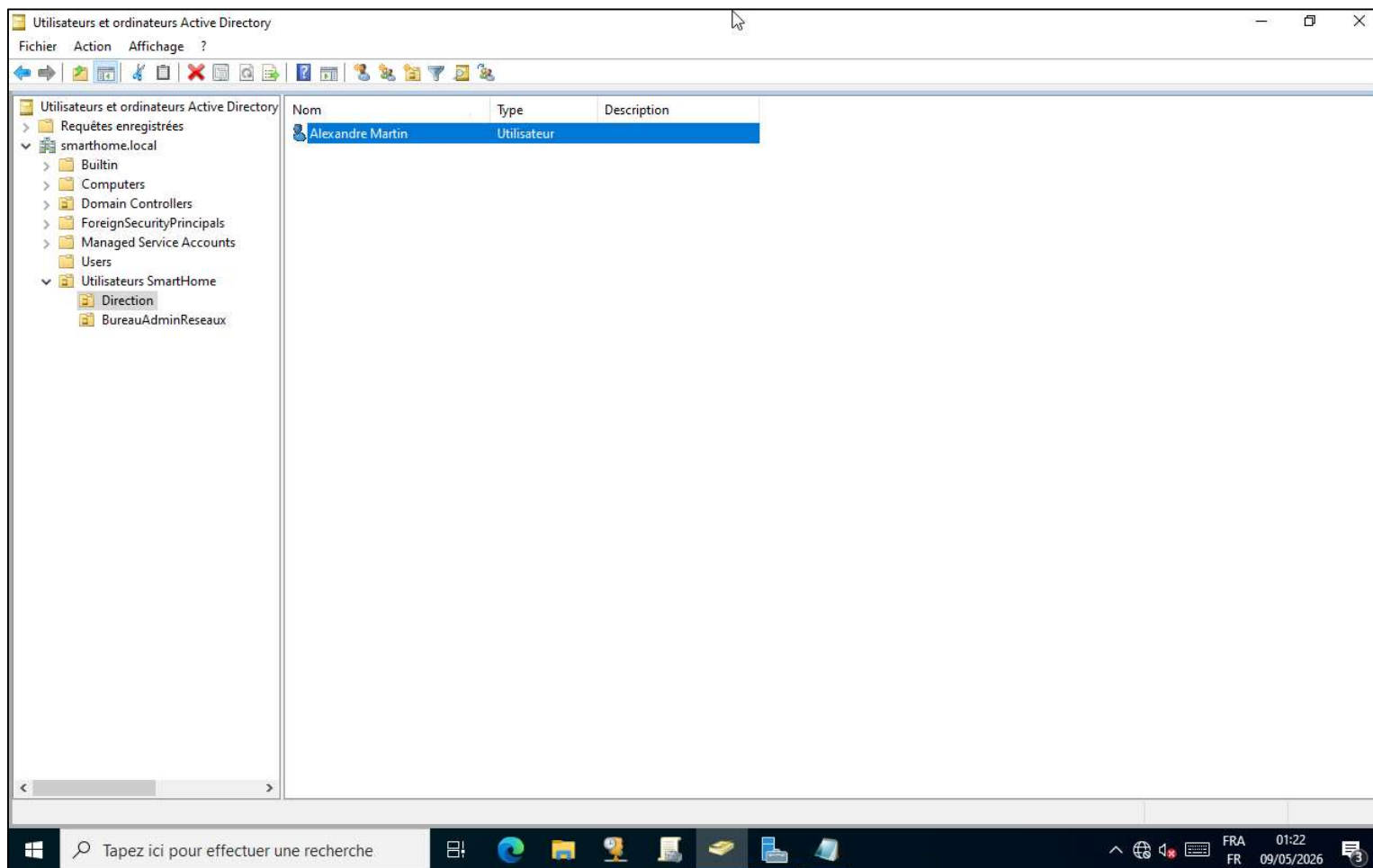
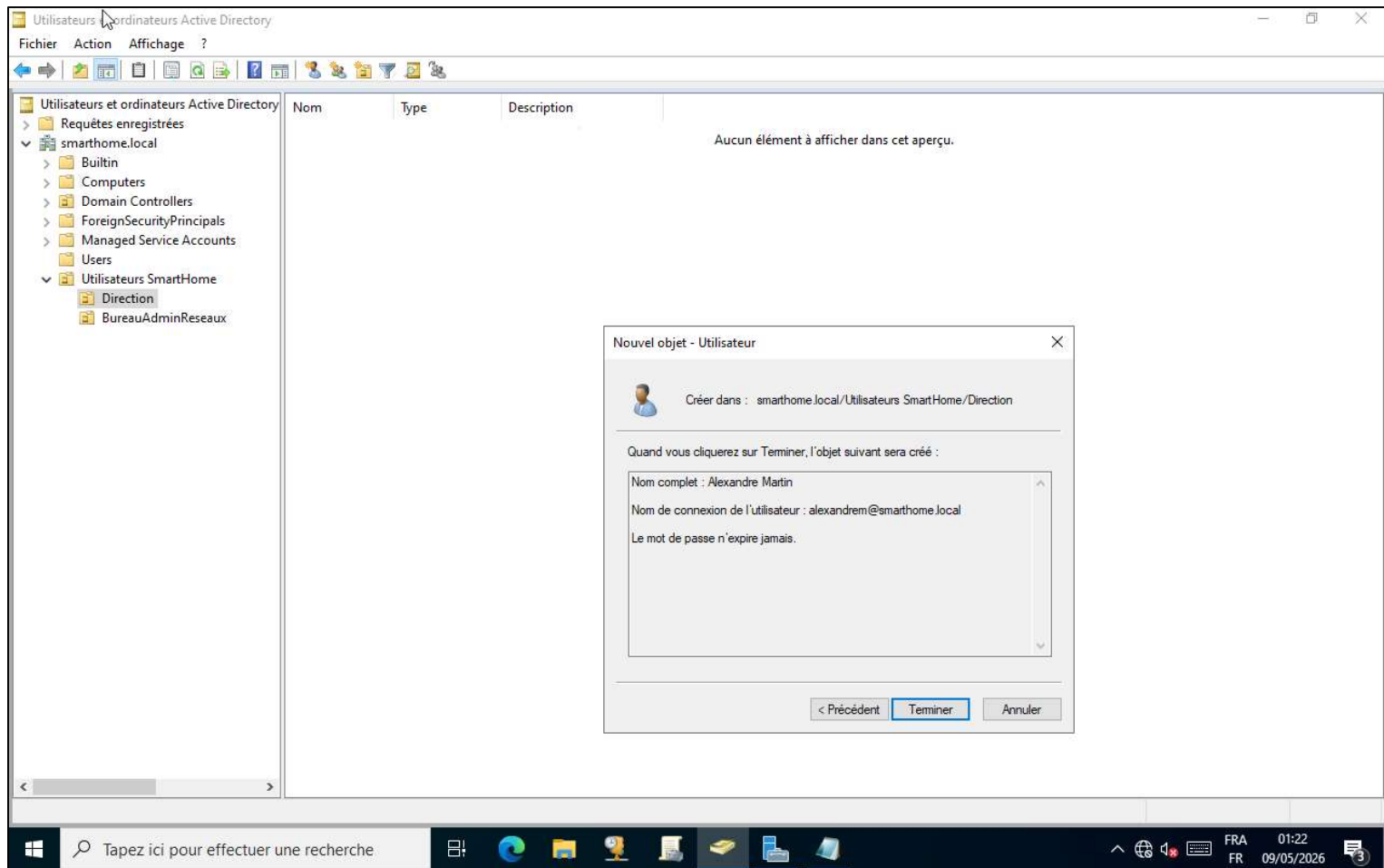


Dans chaque UO on peut ajouter nos Utilisateurs



D'abord le directeur Martin Alexandre, le dirigeant de SmartHome.





Créer votre utilisateur « vous êtes l'admin réseaux » de **SMARTHOME** :

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Nouvel objet - Utilisateur

Créer dans : rthome.local/Utilisateurs SmartHome/BureauAdminRezeaux

Prénom : Theo Initiales :

Nom : Breton

Nom complet : Theo Breton

Nom d'ouverture de session de l'utilisateur : theob @smarthome.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : SMARTHOME\ theob

< Précédent Suivant > Annuler

Aucun élément à afficher dans cet aperçu.

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Nouvel objet - Utilisateur

Créer dans : smarthome.local/Utilisateurs SmartHome/BureauAdminRv

Mot de passe :

Confirmer le mot de passe :

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

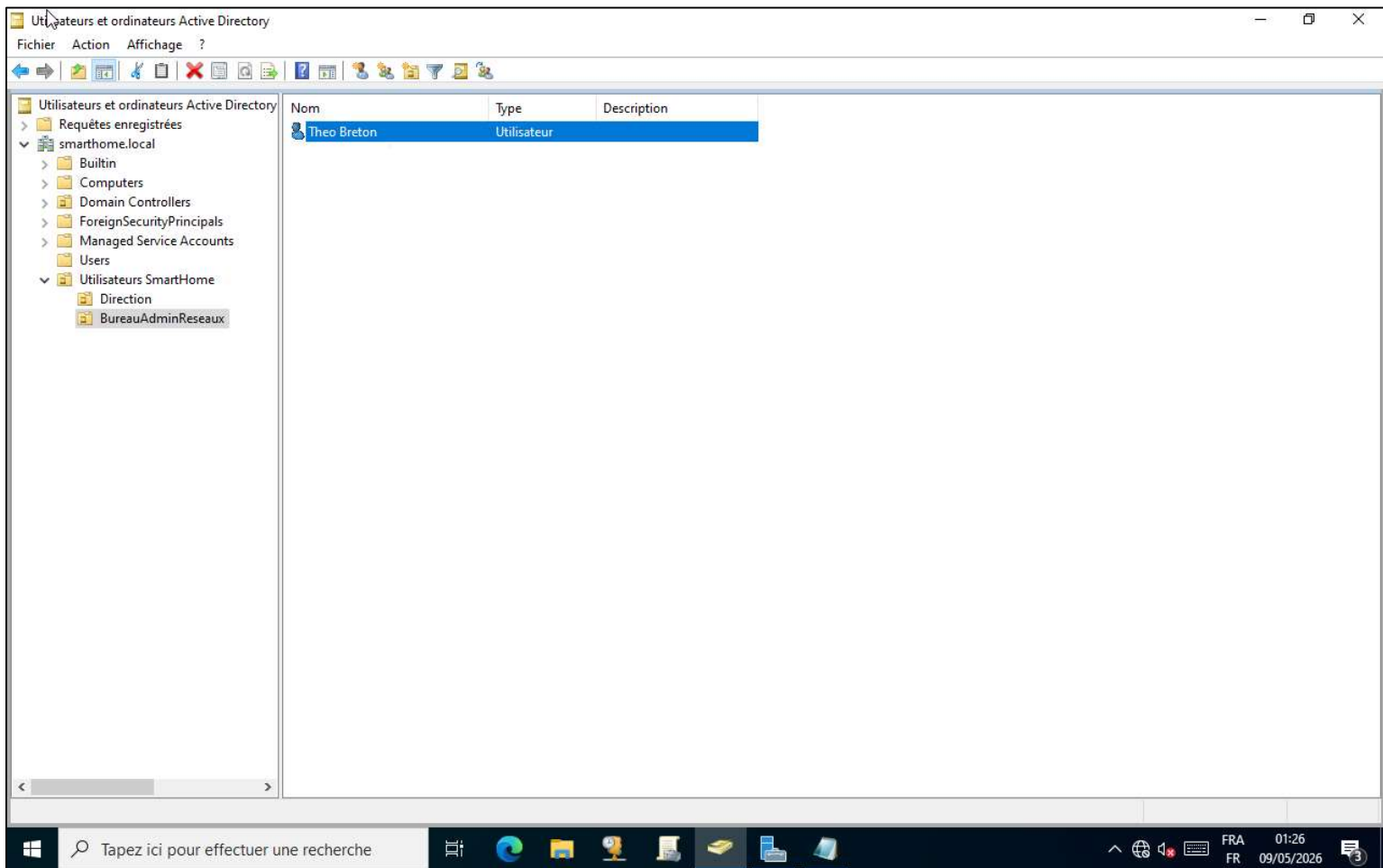
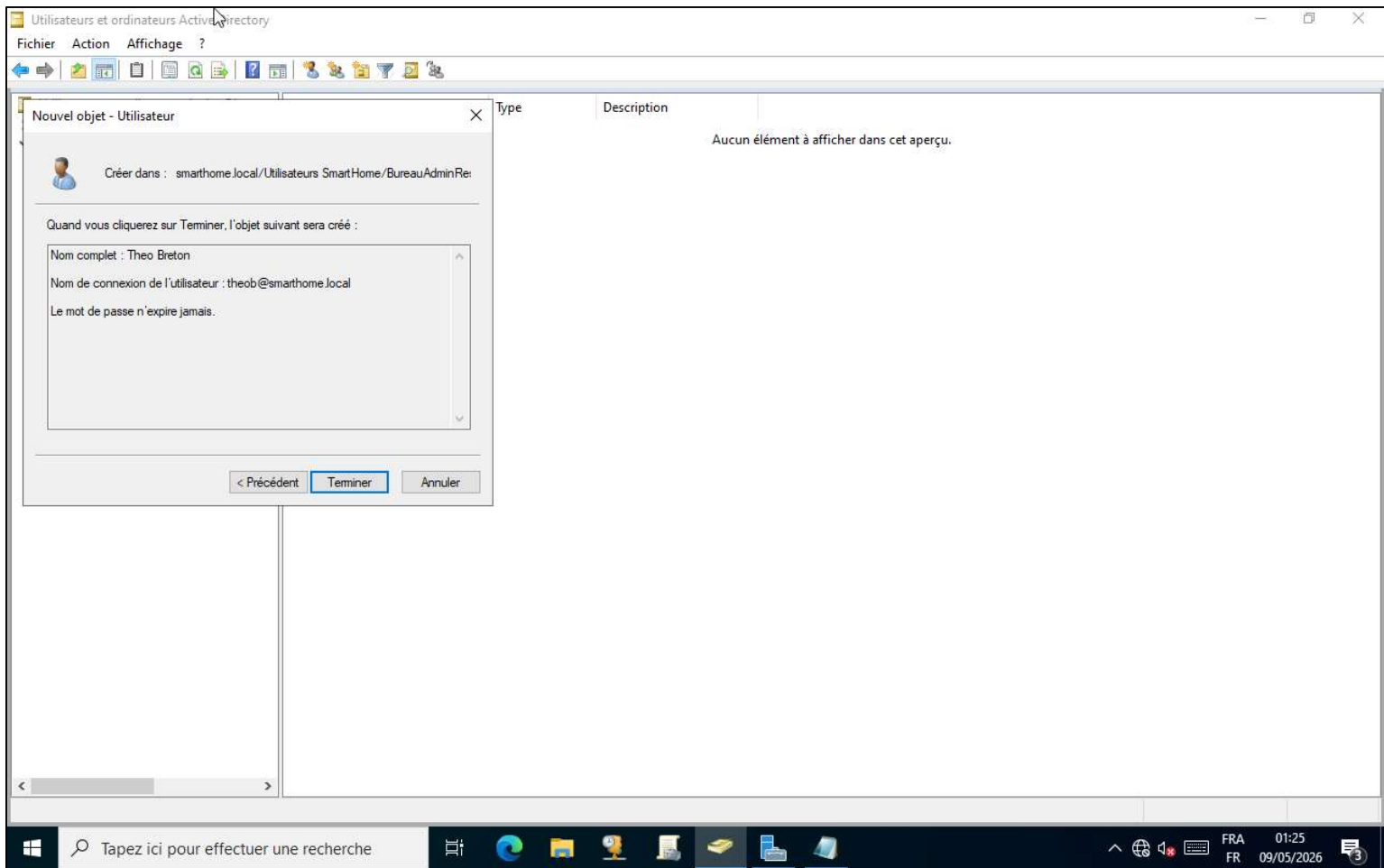
☐ L'utilisateur ne peut pas changer de mot de passe

☒ Le mot de passe n'expire jamais

☐ Le compte est désactivé

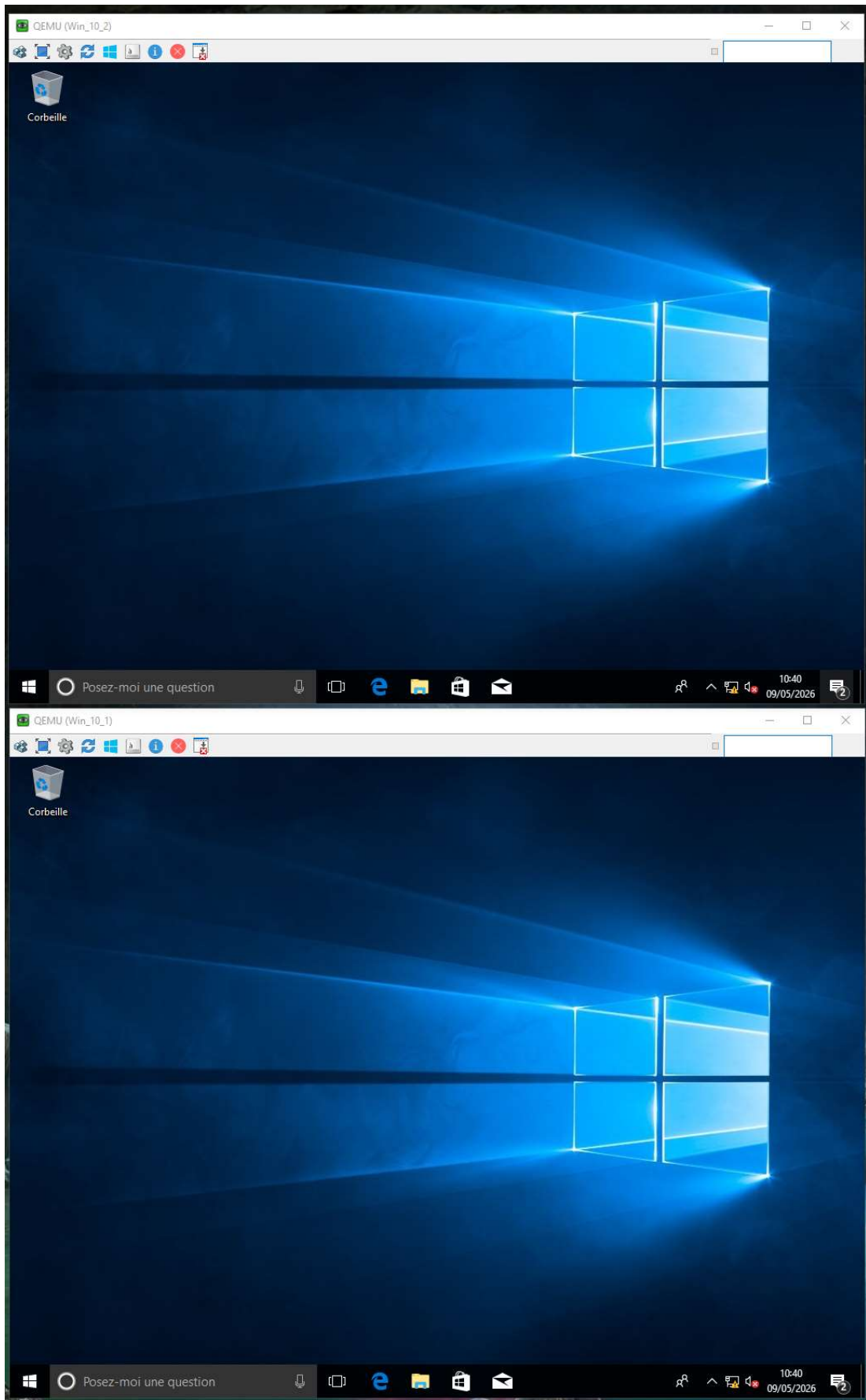
< Précédent Suivant > Annuler

Aucun élément à afficher dans cet aperçu.

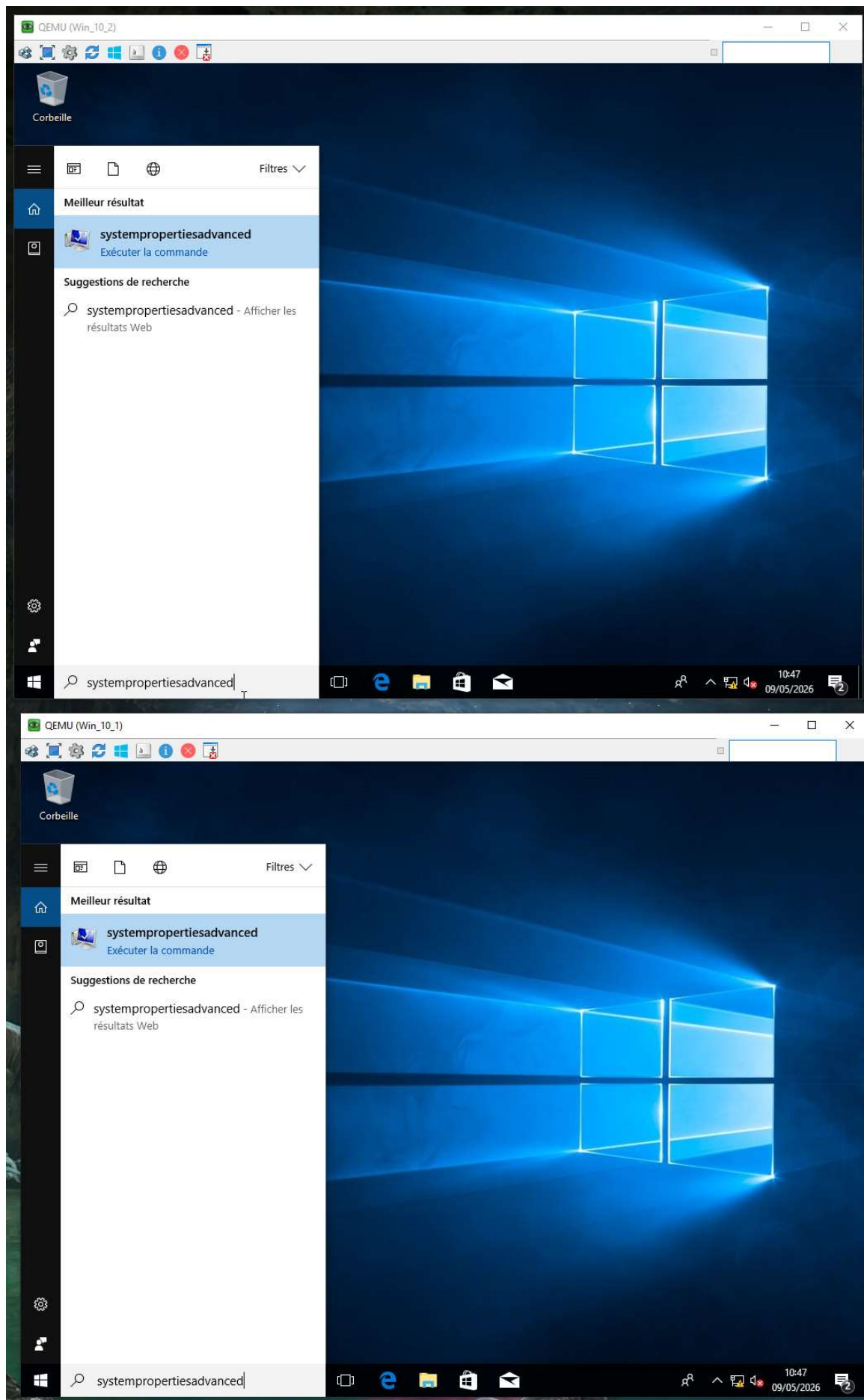


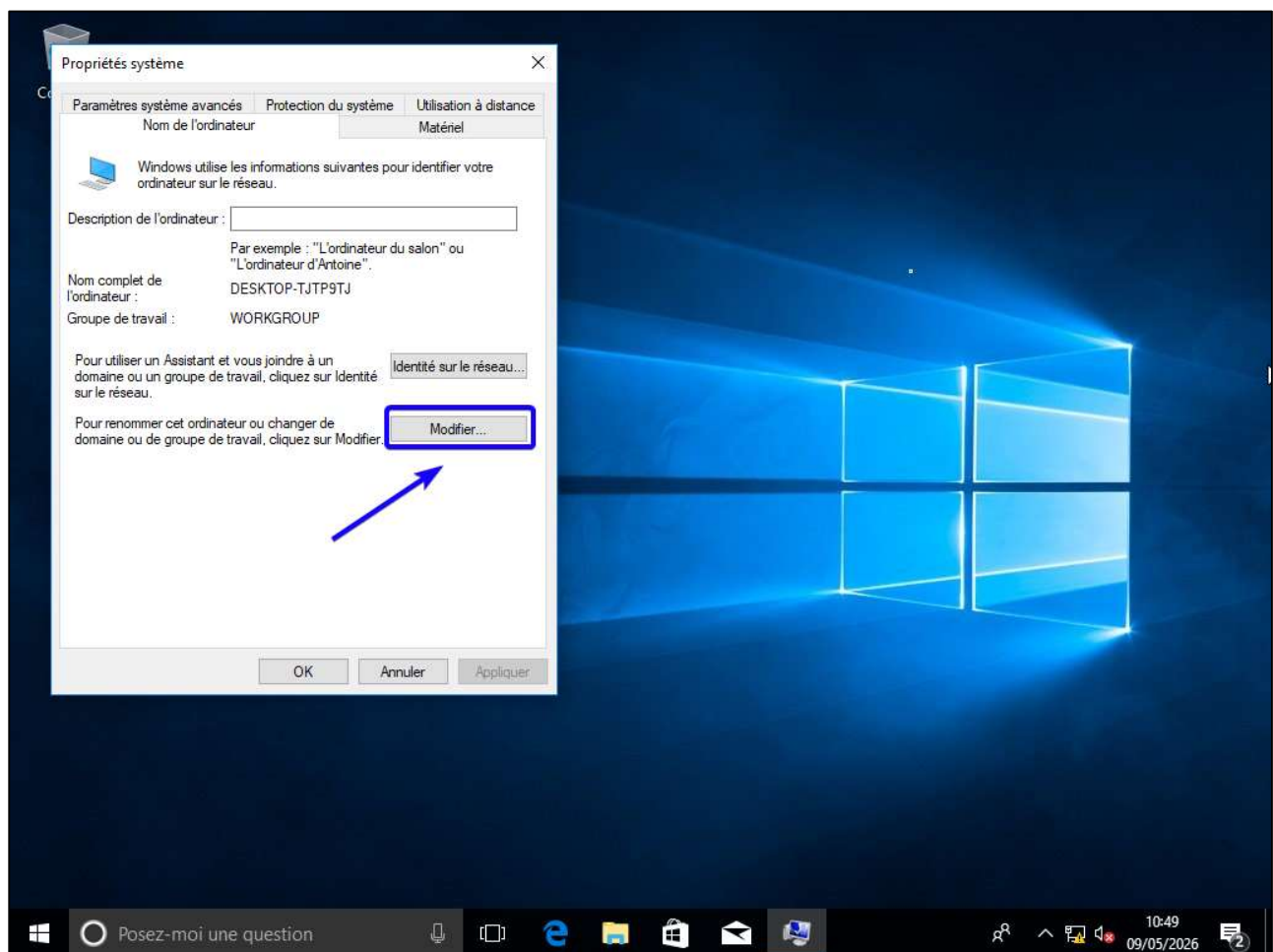
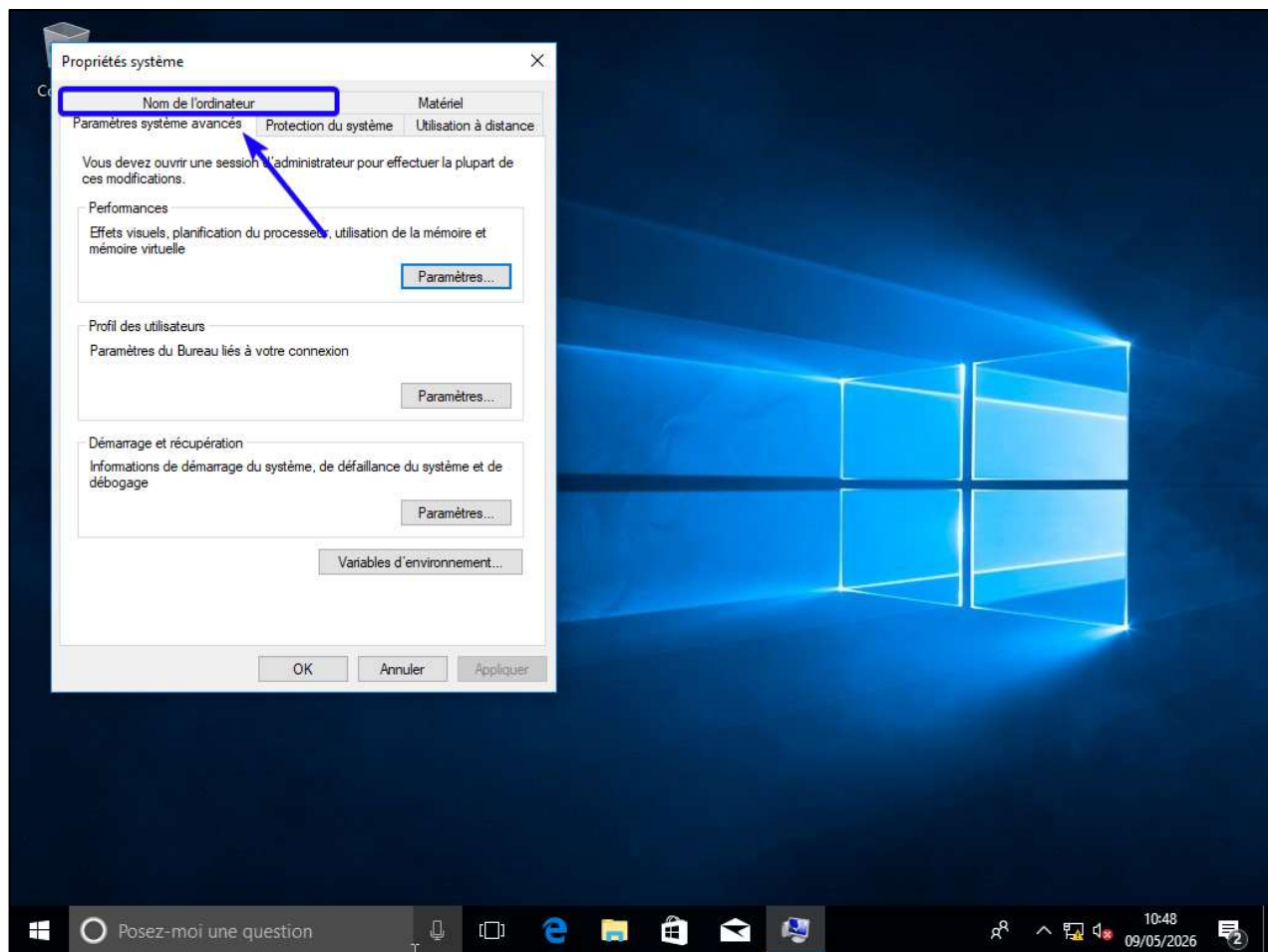
Maintenant que nos deux utilisateurs sont créés dans leur UO respective on va pouvoir liés les machines virtuelle cliente au domaine Active Directory de l'entreprise.

On a nos deux machine virtuelle cliente opérationnelle avec une connexion au moyen d'un utilisateur à la base SAM.

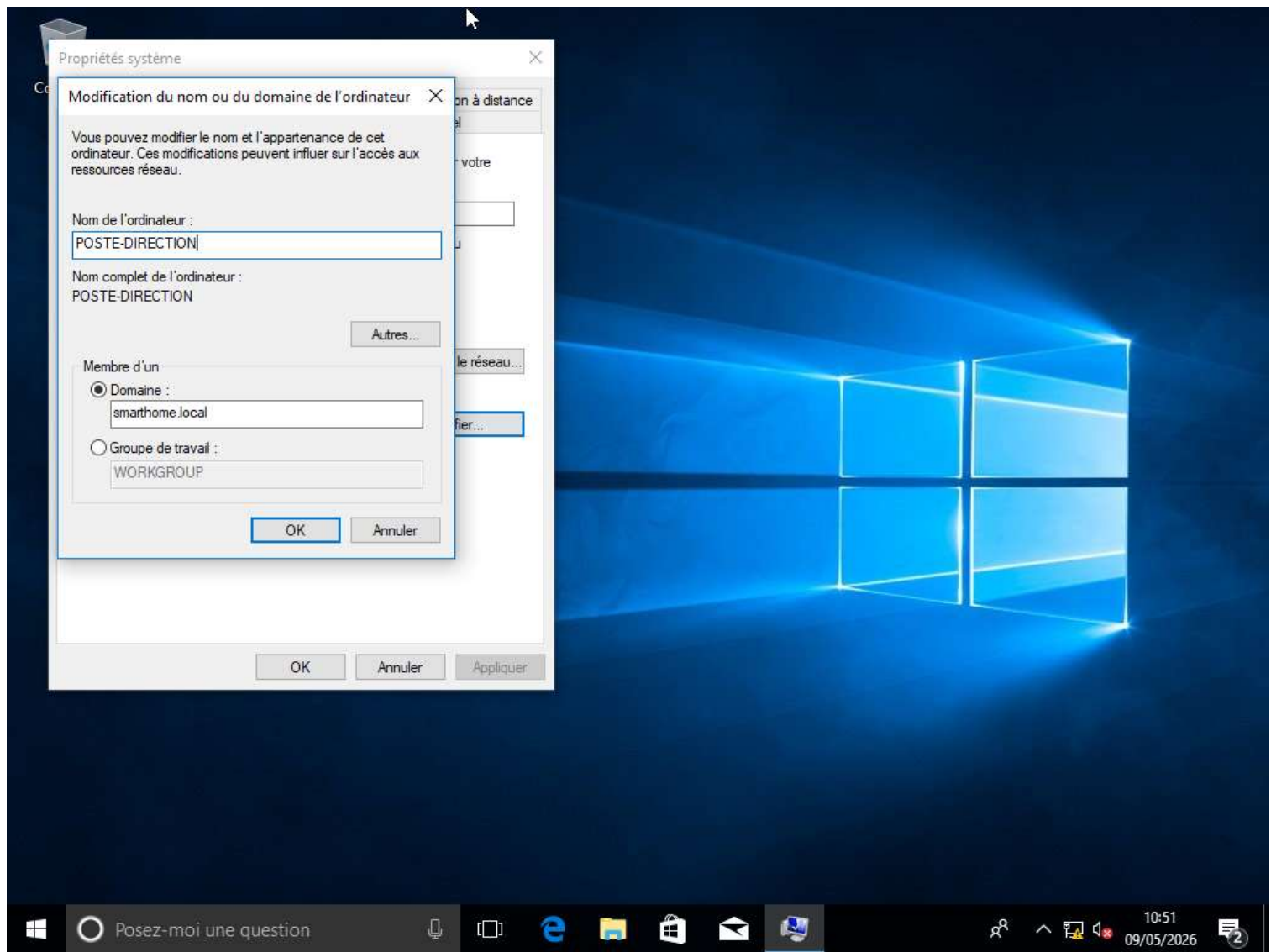


Pour aller dans les propriétés système avancé de nos deux VMs on a taper dans zone recherche : systempropertiesadvanced



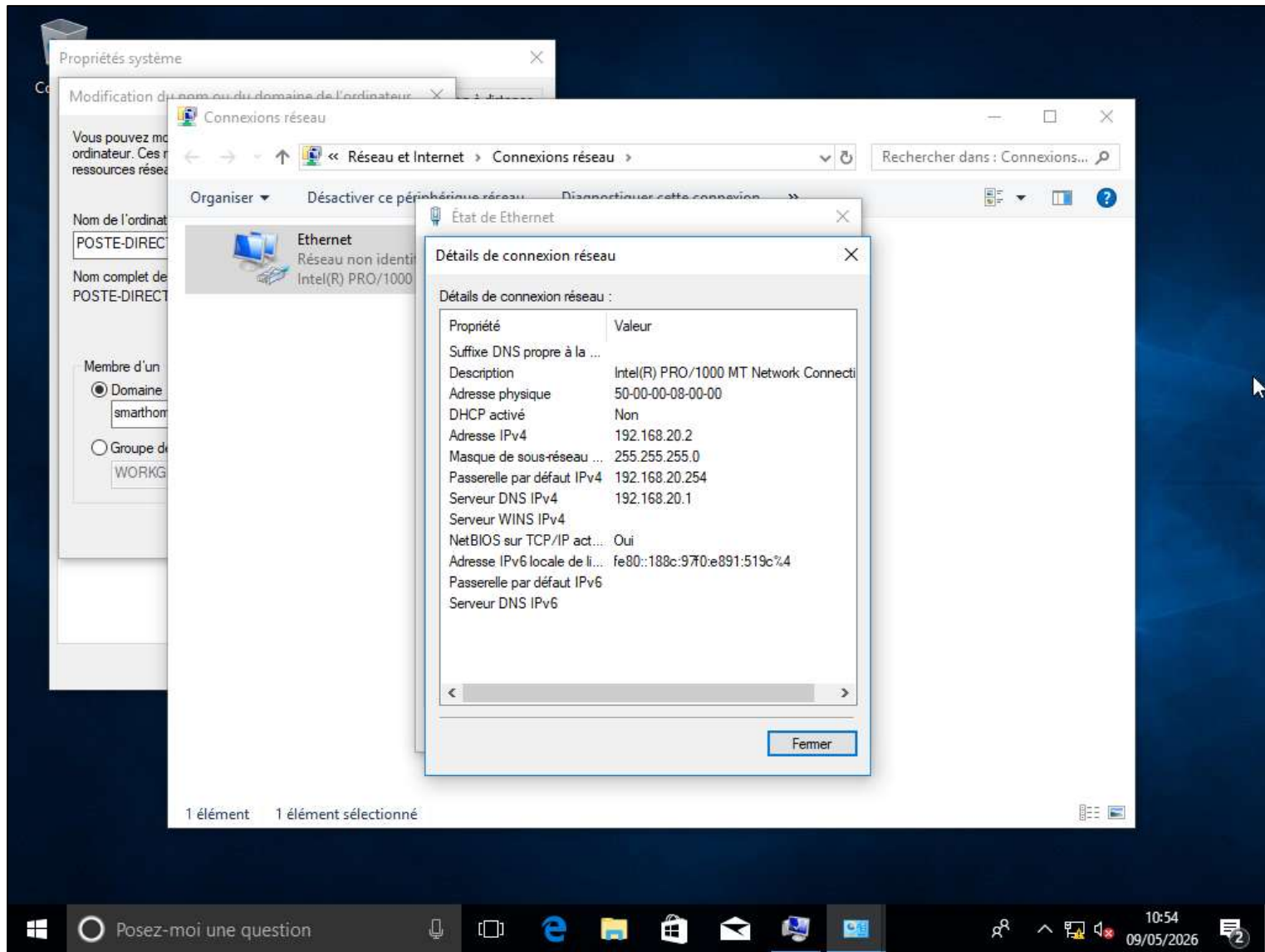


Poste Win_10_2 → Poste de DIRECTION :

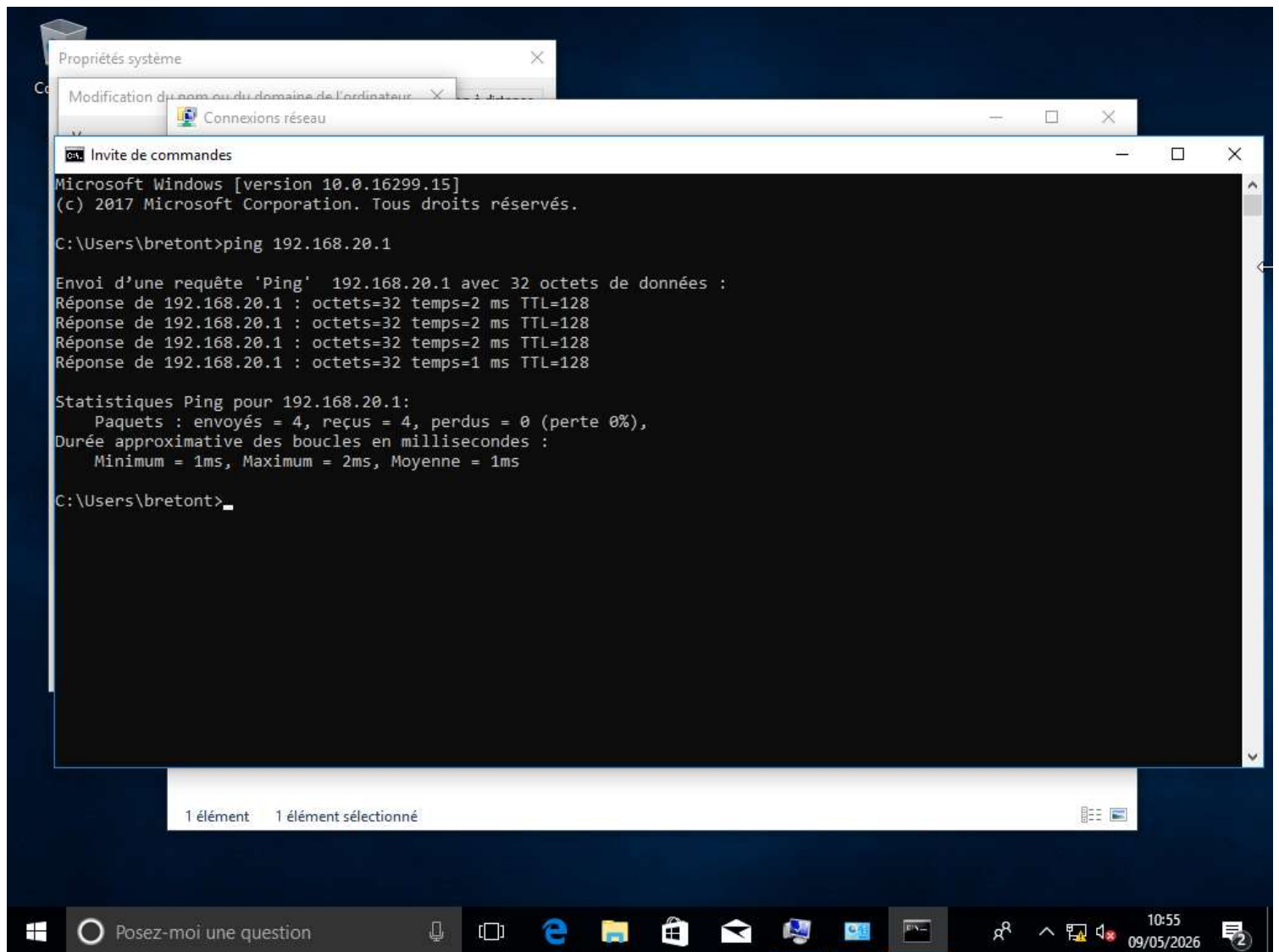


Avant de la valider on va mettre à notre machine virtuelle une configuration IP dans sa carte réseau comme il n'y a pas encore de DHCP.

On vérifie que la configuration est bien prise en compte :



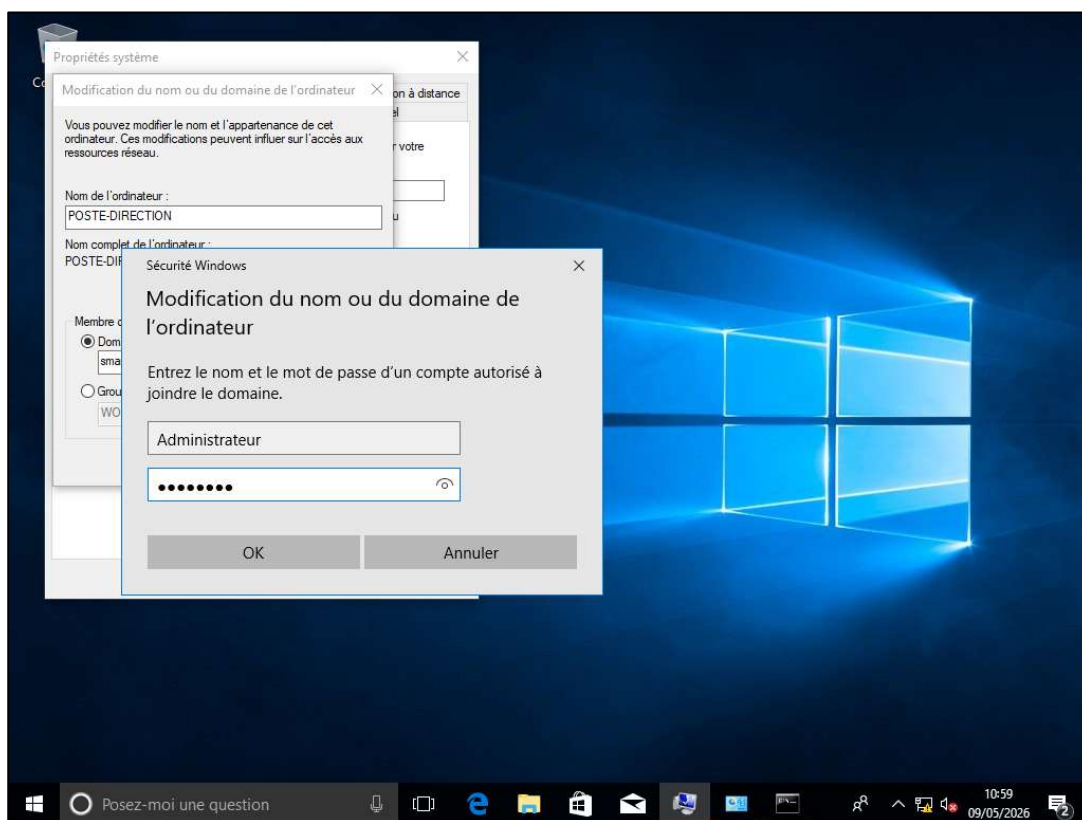
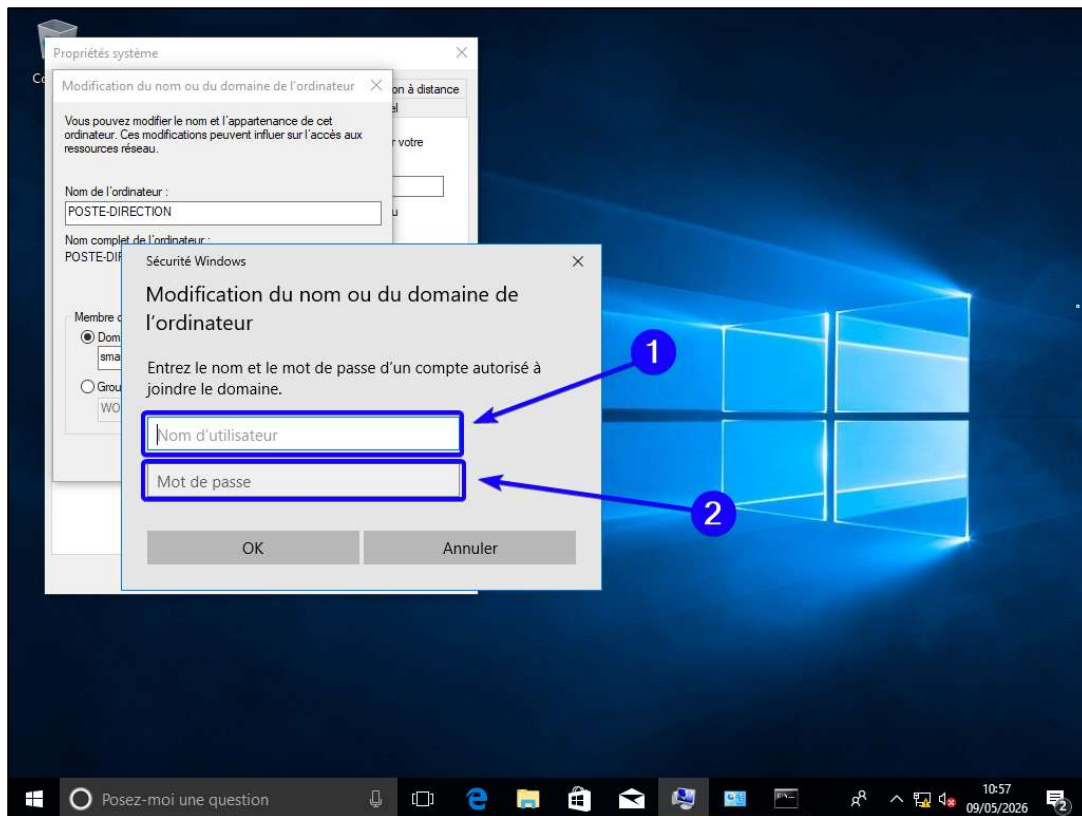
On essaye de communiquer avec notre serveur AD au moyen de son @IP en 192.168.20.1/24



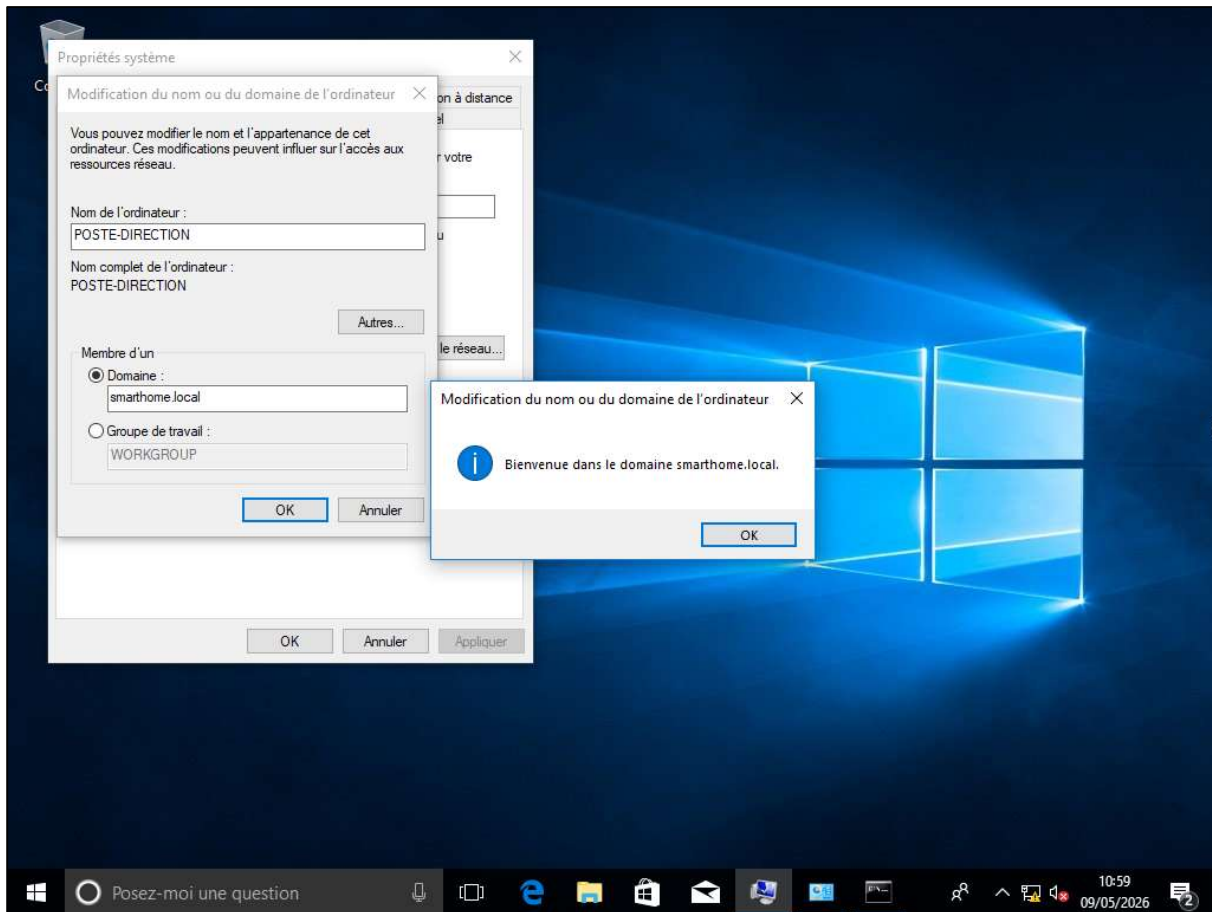
On peut voir qu'il communique parfaitement, donc on peut maintenant valider nos paramètres pour **la lier au domaine**.

Une page d'authentification va apparaître :

On va se connecter avec nos identifiants de connexion au serveur AD en tant que Administrateurs.

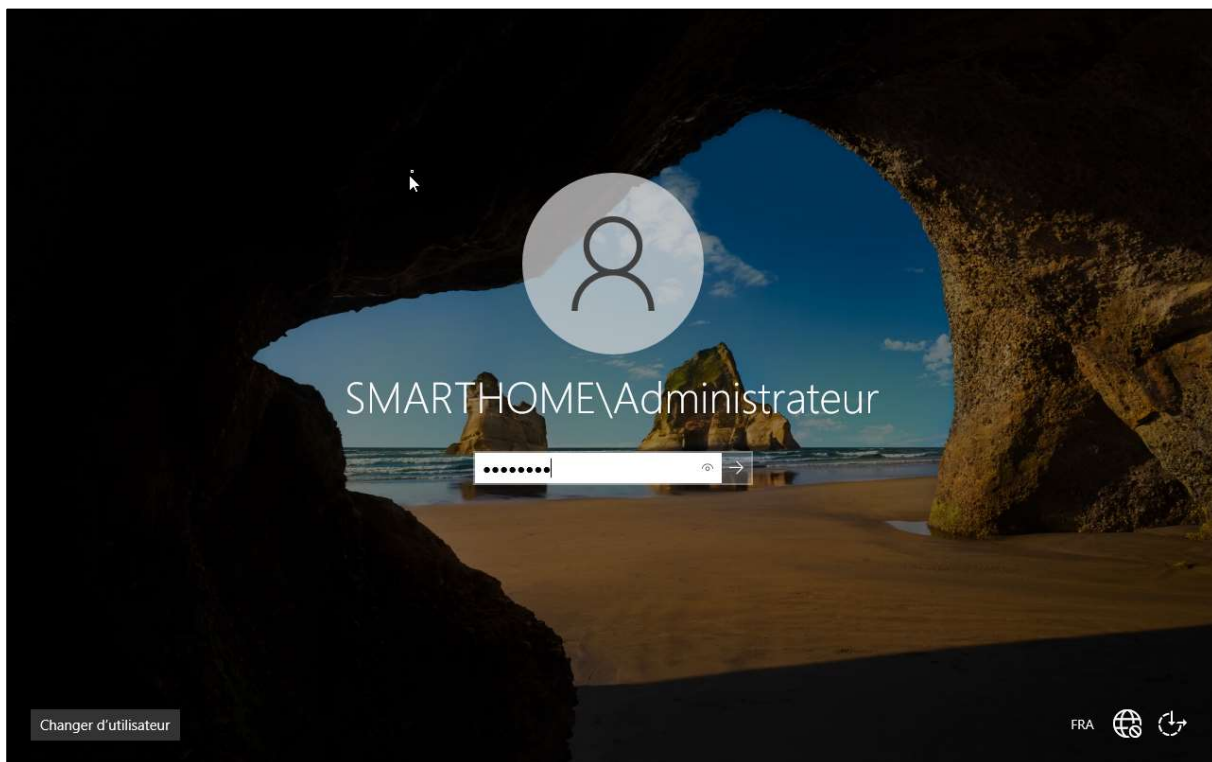


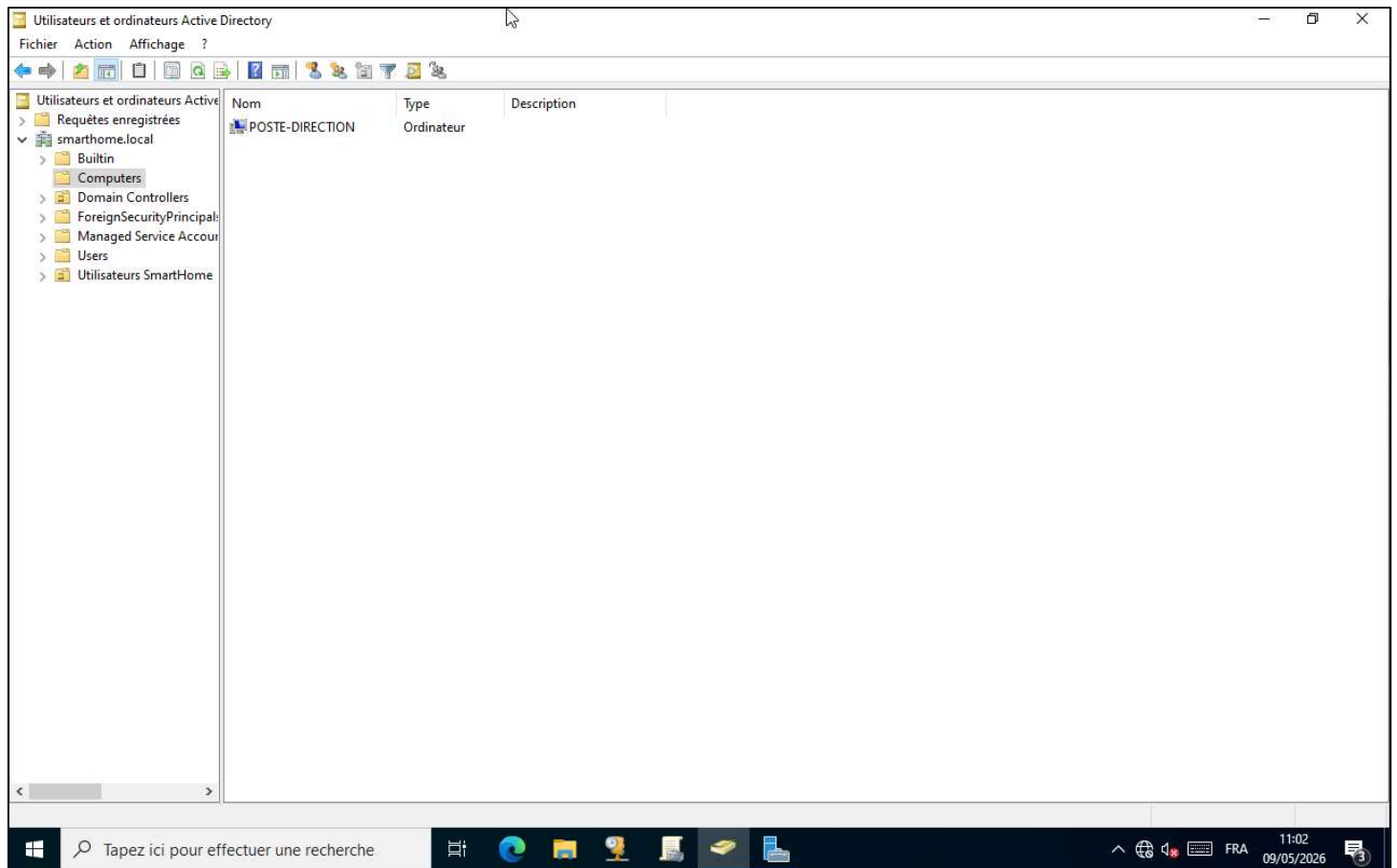
Notre machine virtuelle et maintenant lié au domaine **smarthome.local**



On peut la voir apparaitre dans **l'annuaire LDAP**.

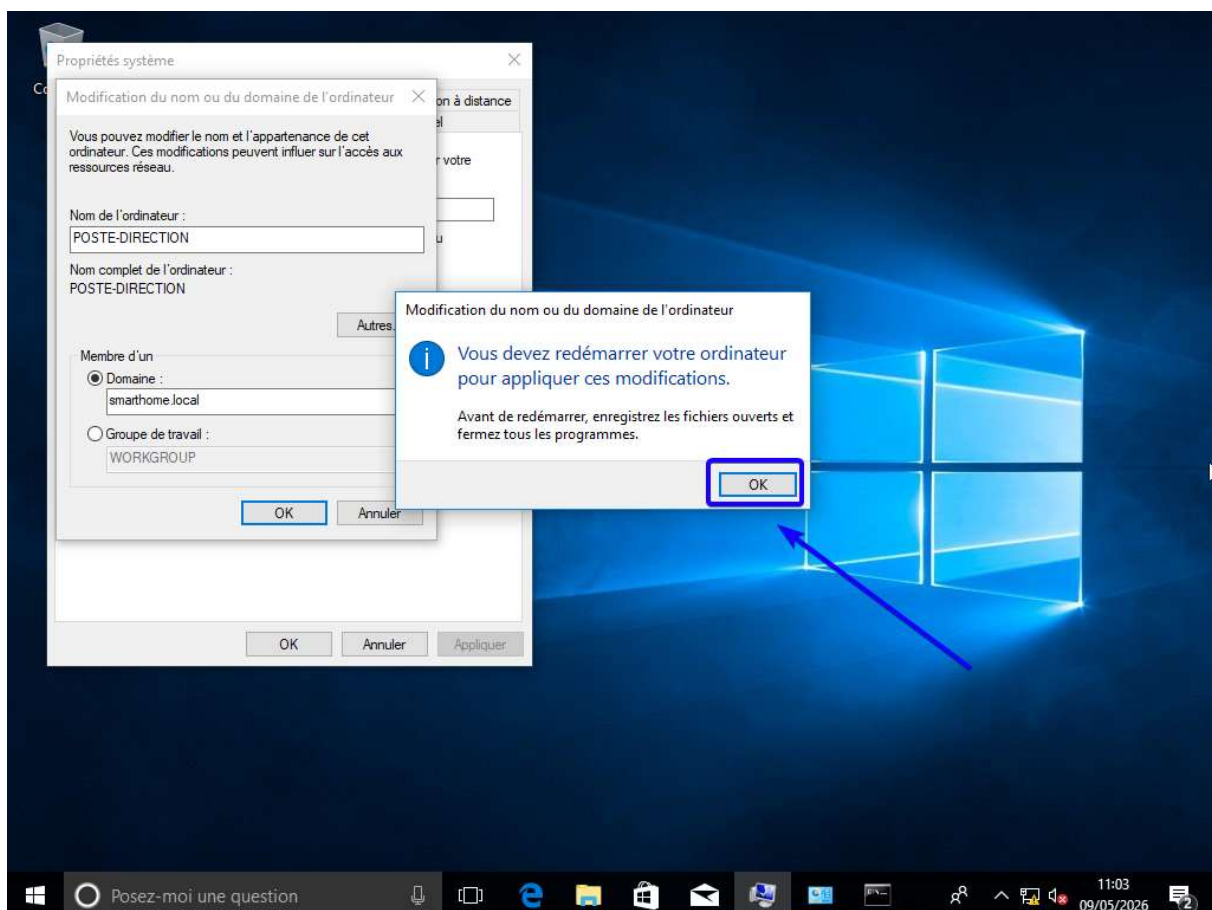
On se connecte sur le serveur AD

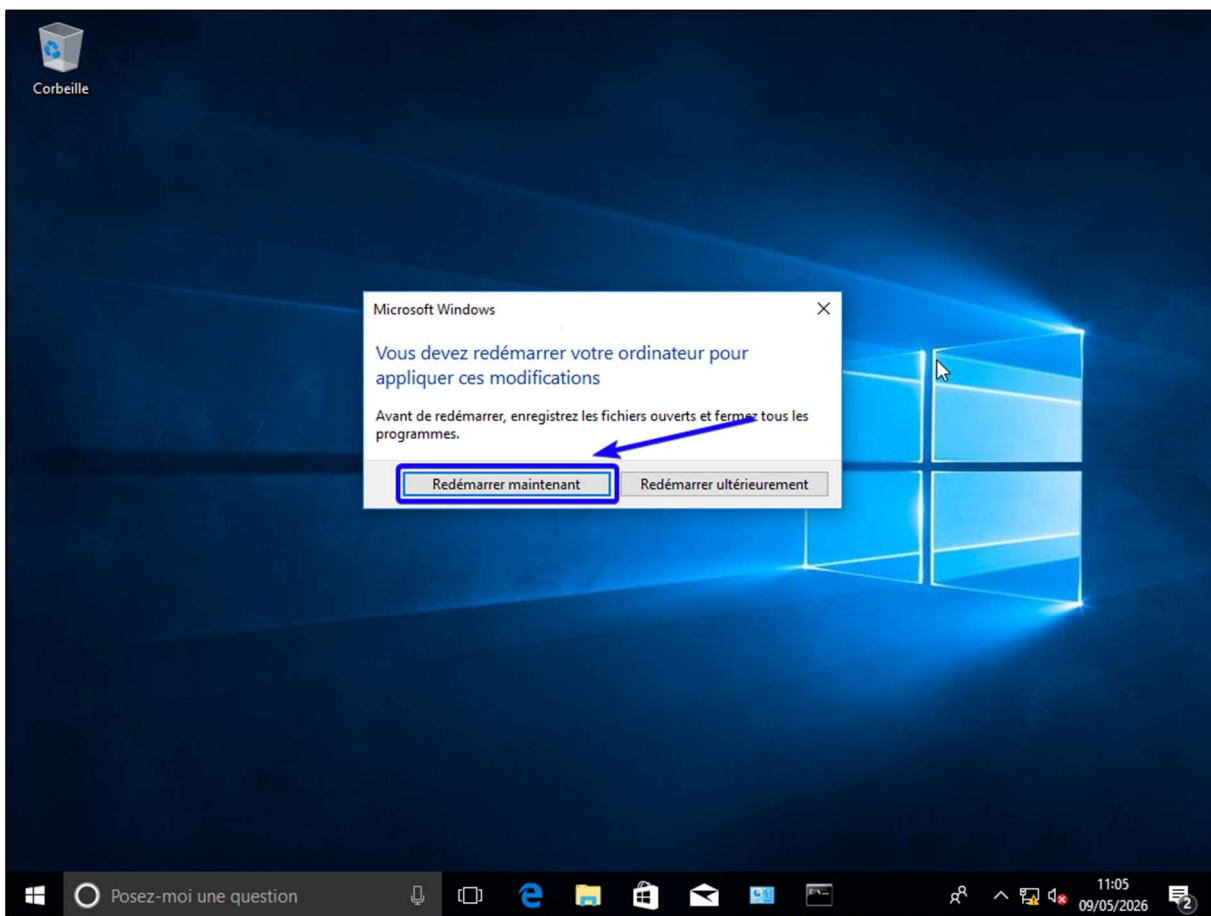
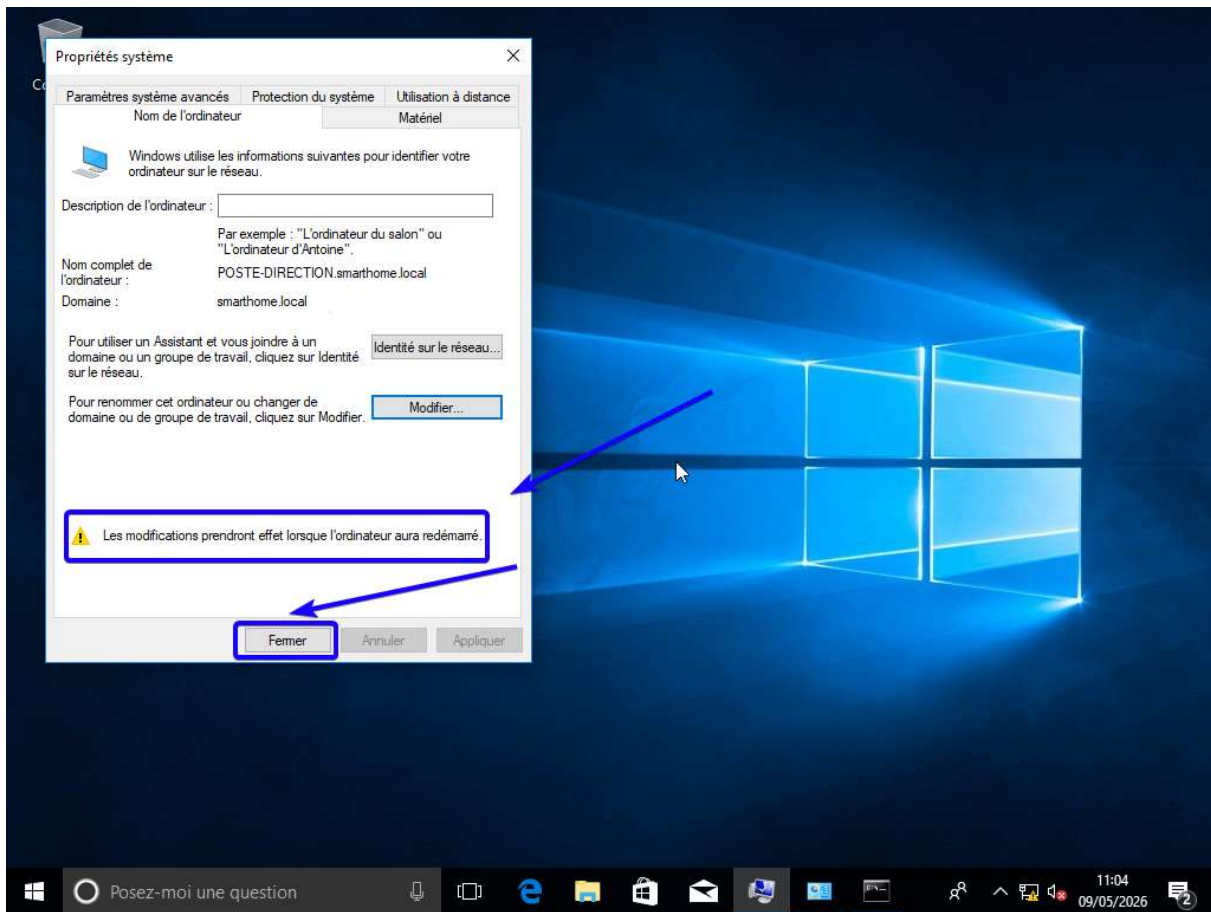




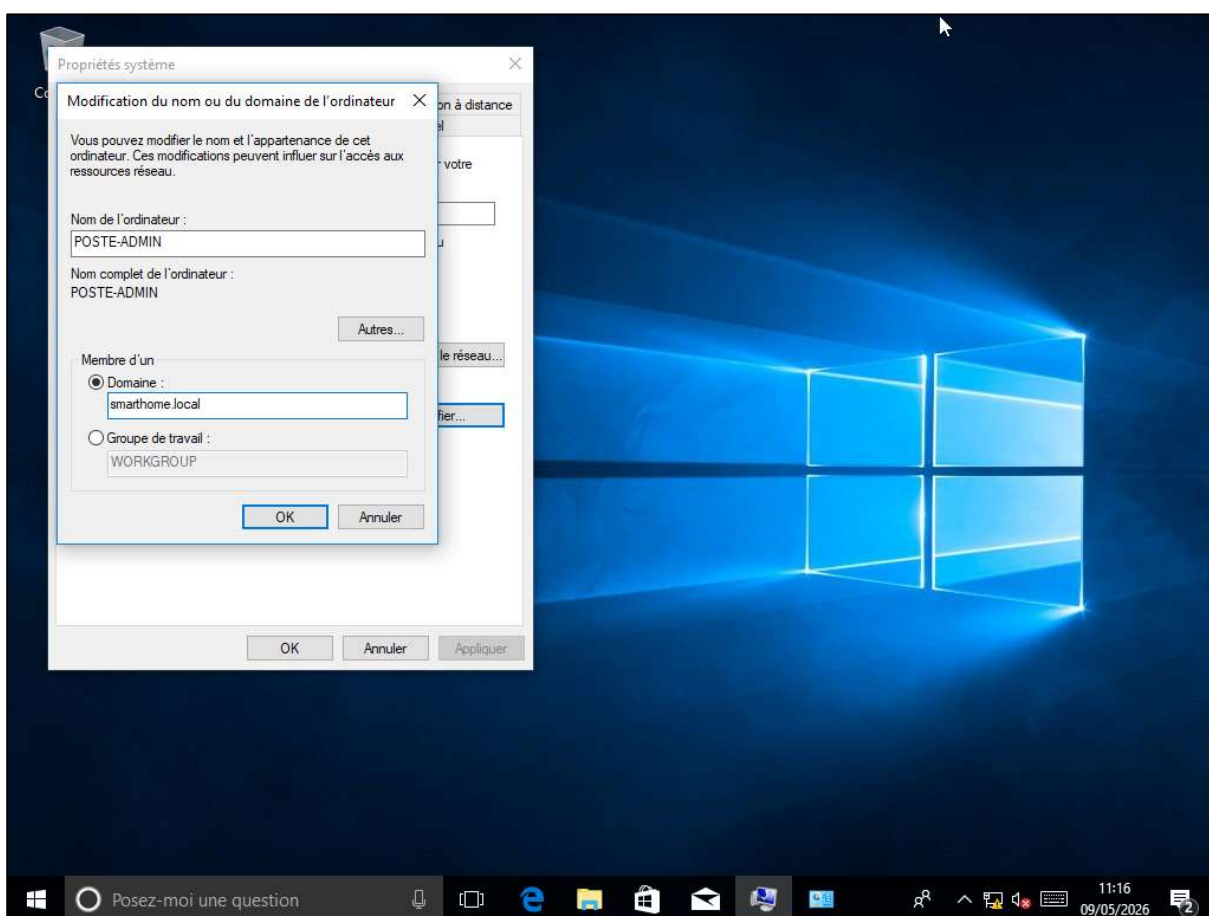
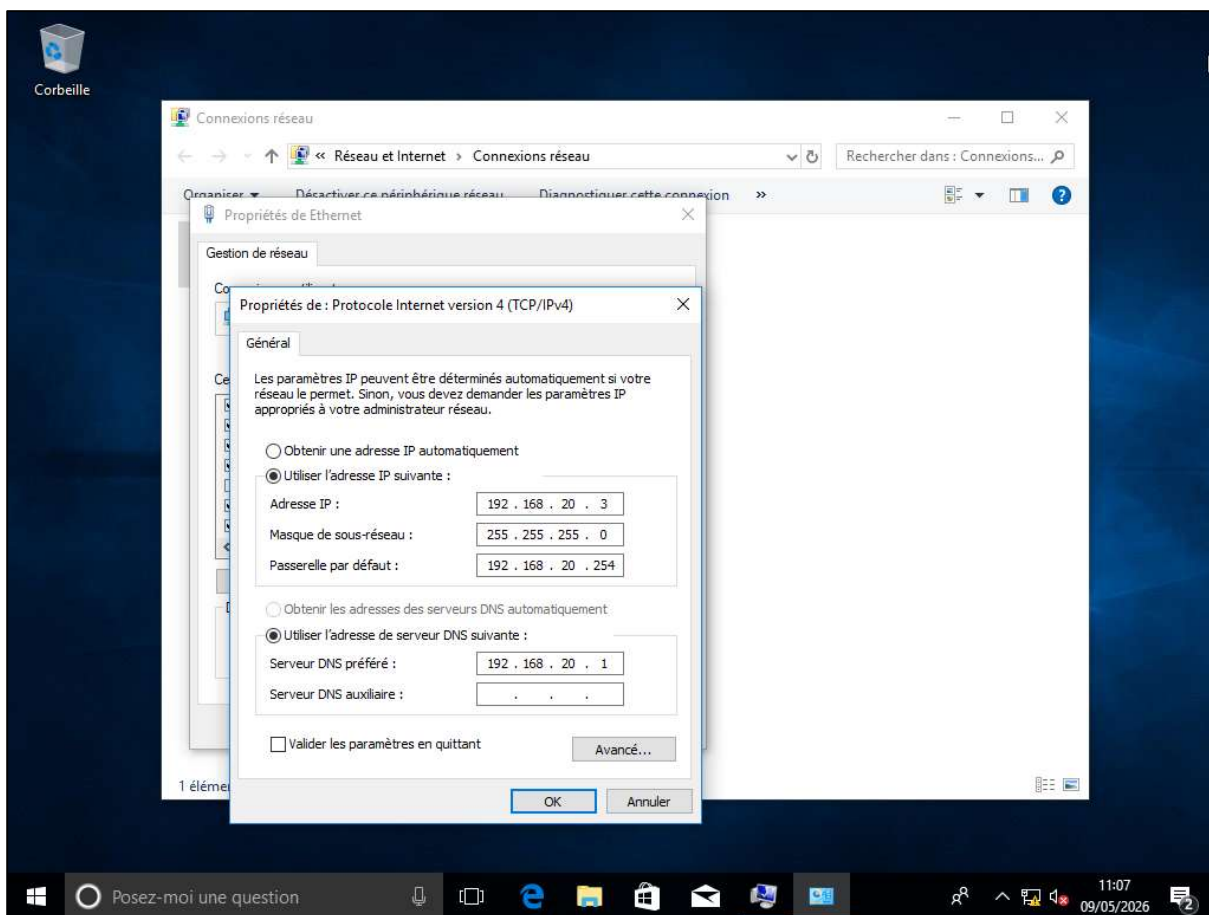
Elle est bien présente dans **notre annuaire LDAP**.

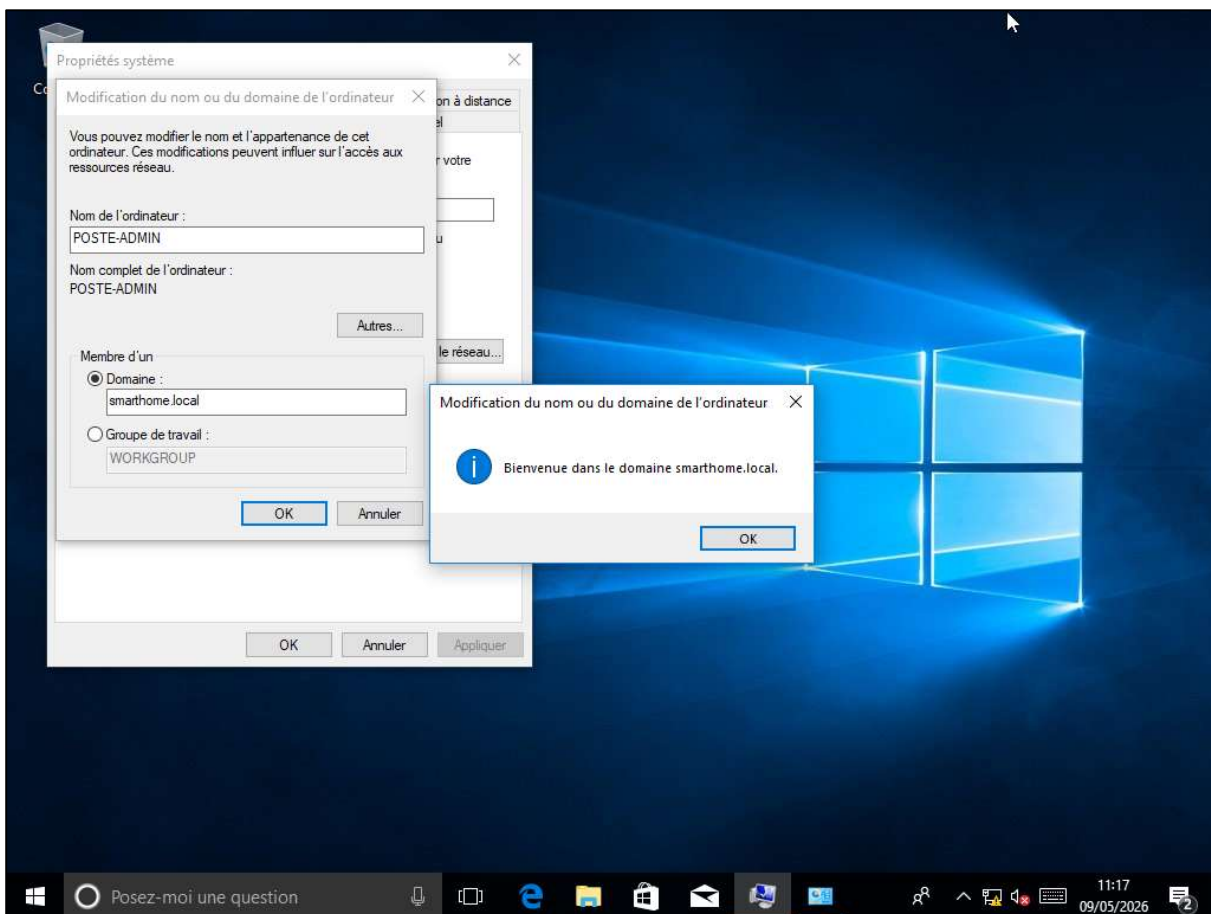
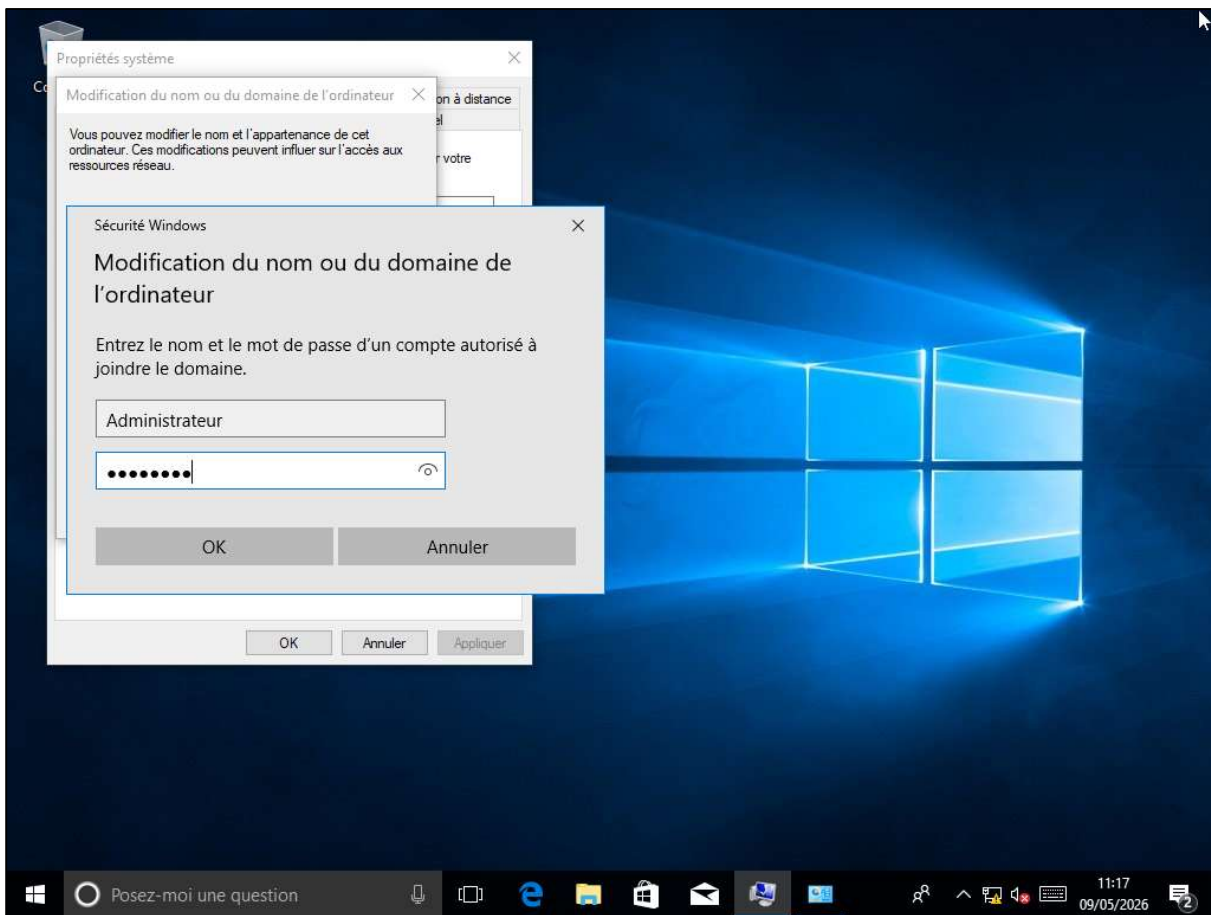
Pour que tous les paramètres soit pris en compte il faut redémarrer la VM.



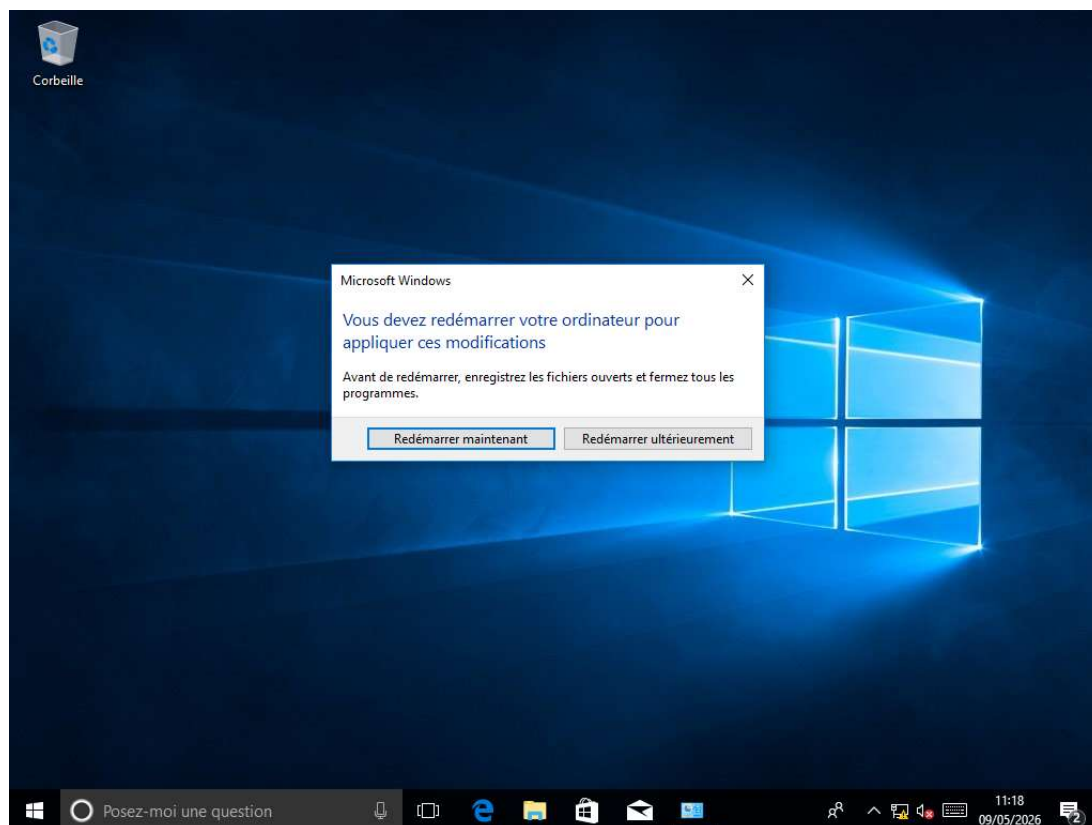


Pendant que notre VM Win_10_2 redémarre on va lier au domaine la Win_10_1 au domaine :

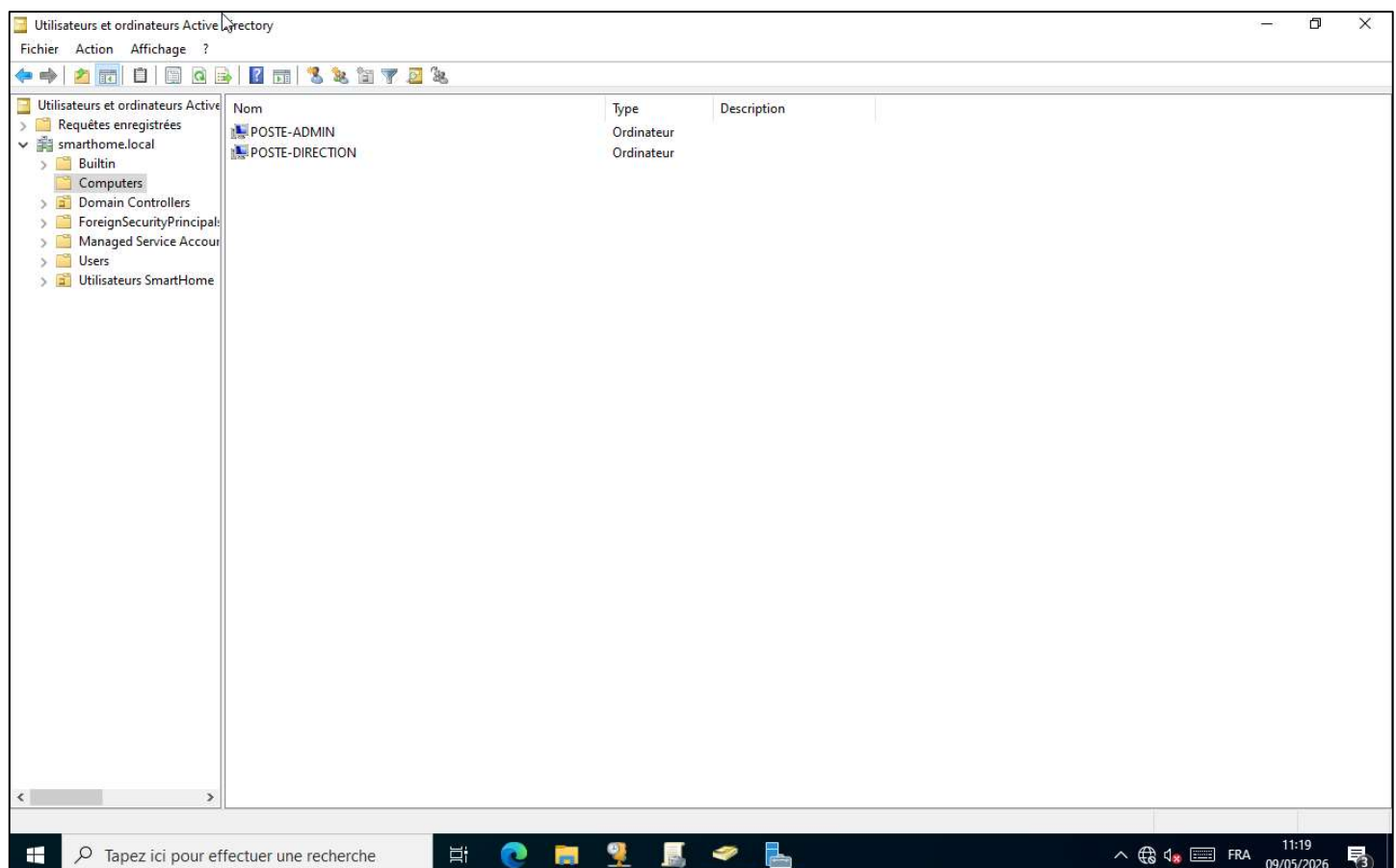




Même chose on redémarre maintenant pour appliquer les paramètres :



Nos deux machines sont maintenant liées au domaine :

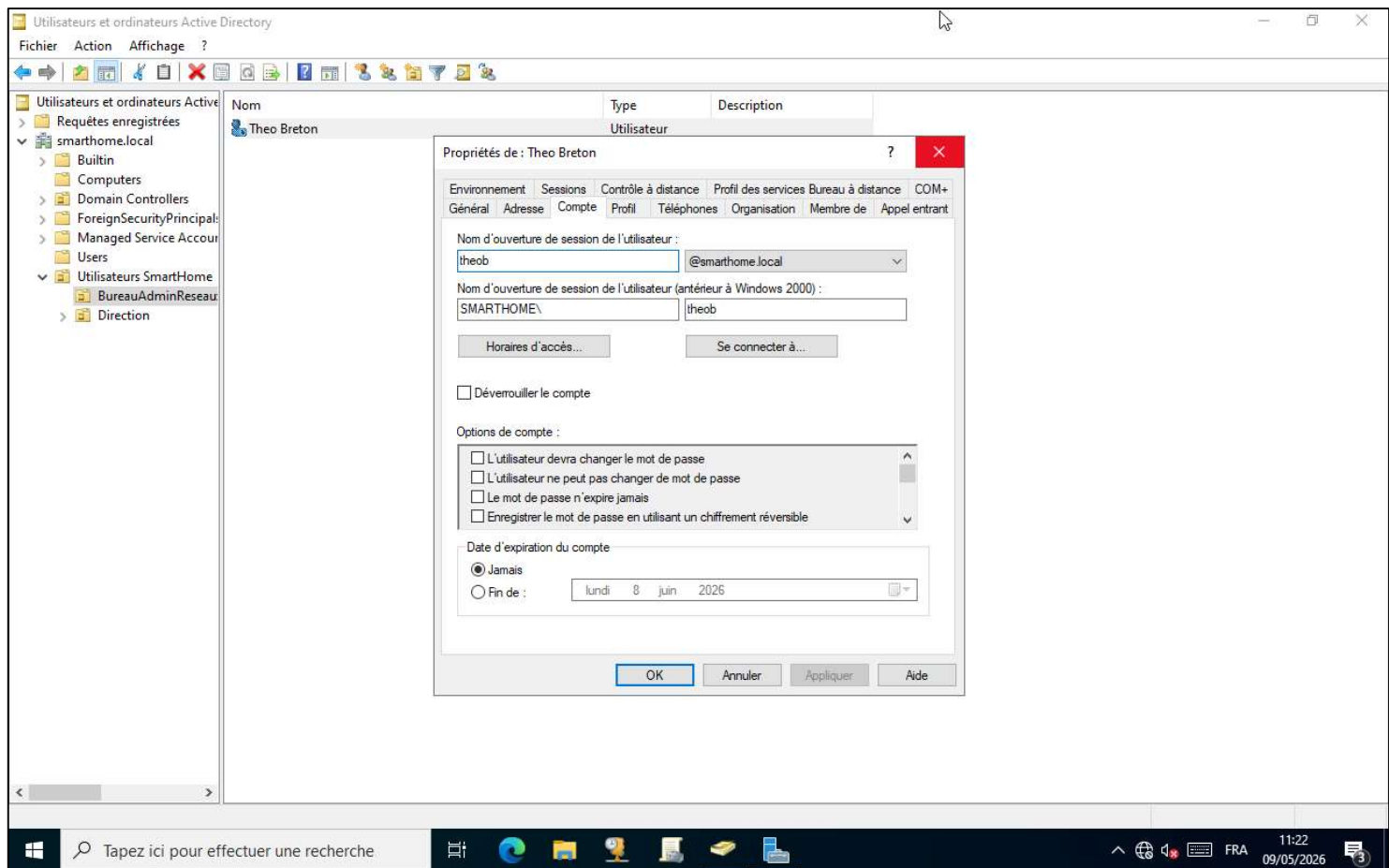


Maintenant le teste va être simple « se connecter à avec un utilisateur du service concerné.

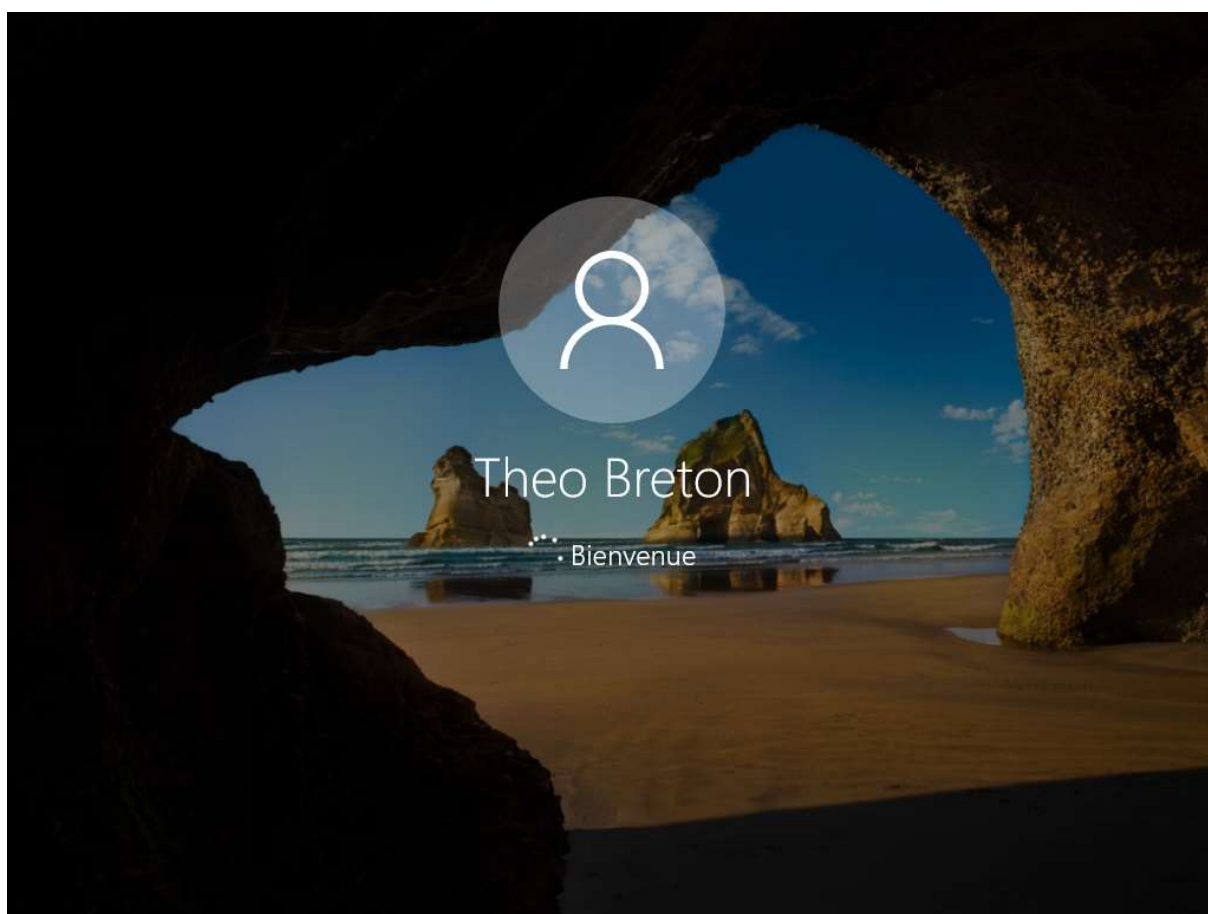
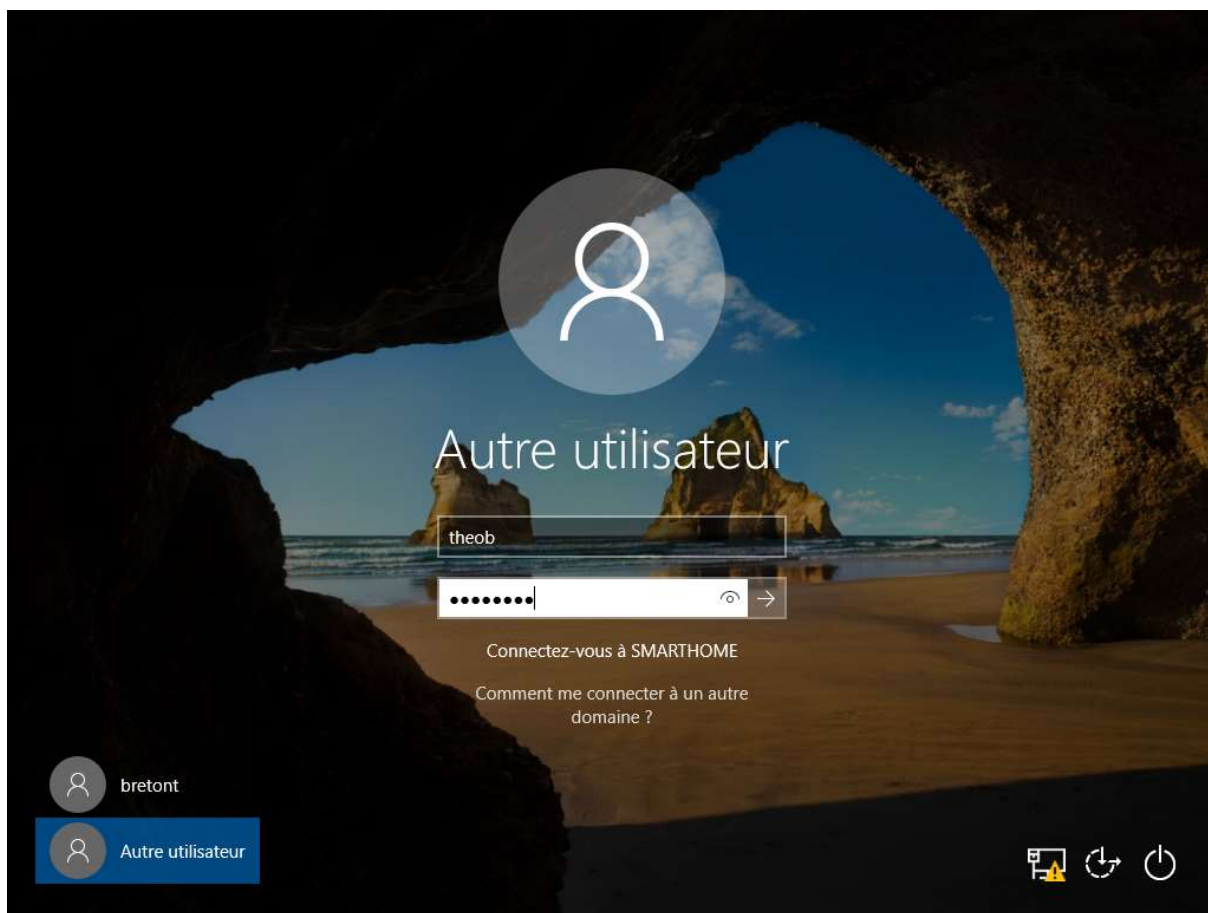
Win_10_1 → Poste de l'administrateur réseau donc l'utilisateur se Théo Breton.

Win_10_2 → Poste de la direction donc l'utilisateur se Alexandre Martin.

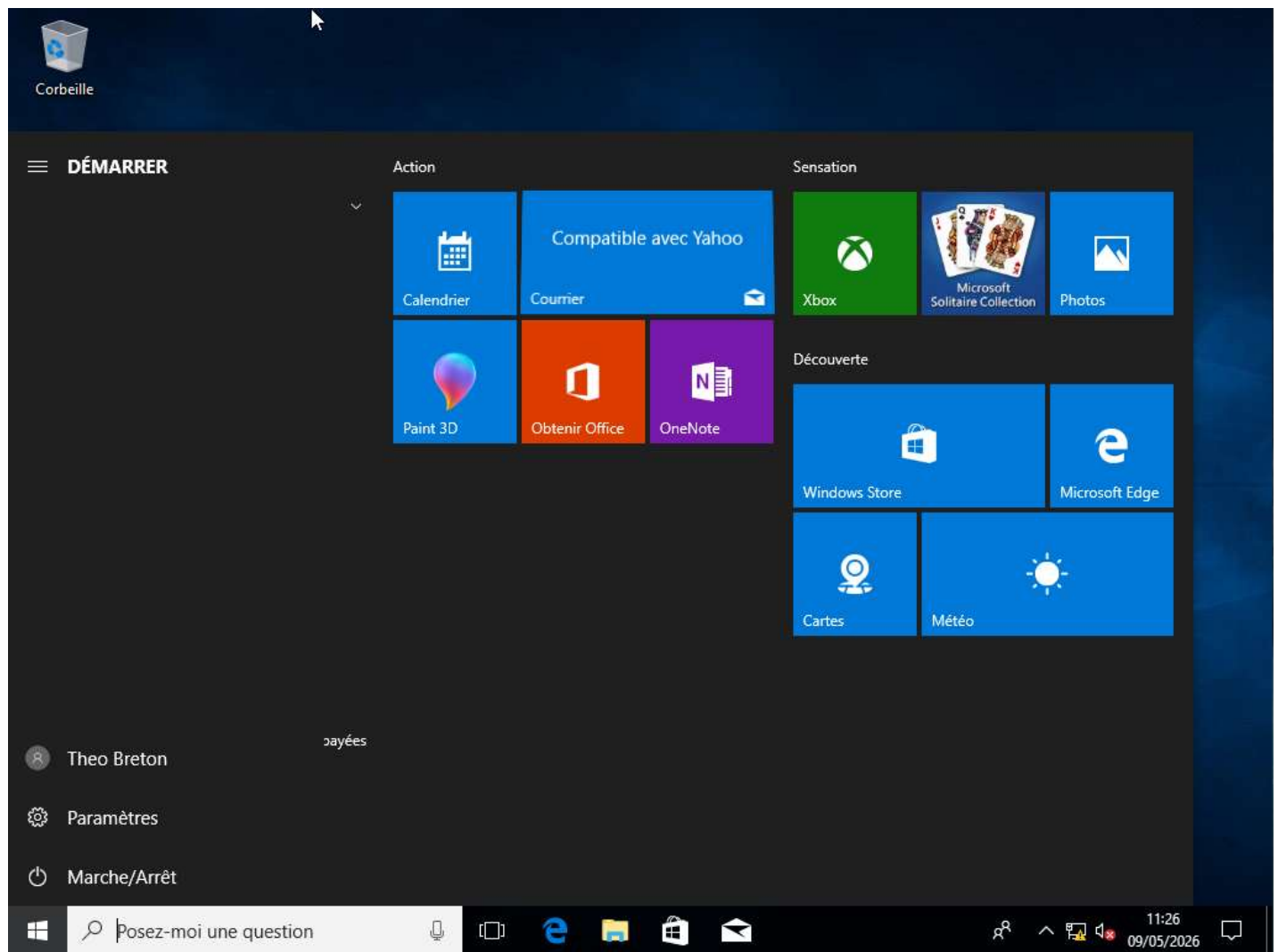
Donc notre identifiant et theob + mdp :

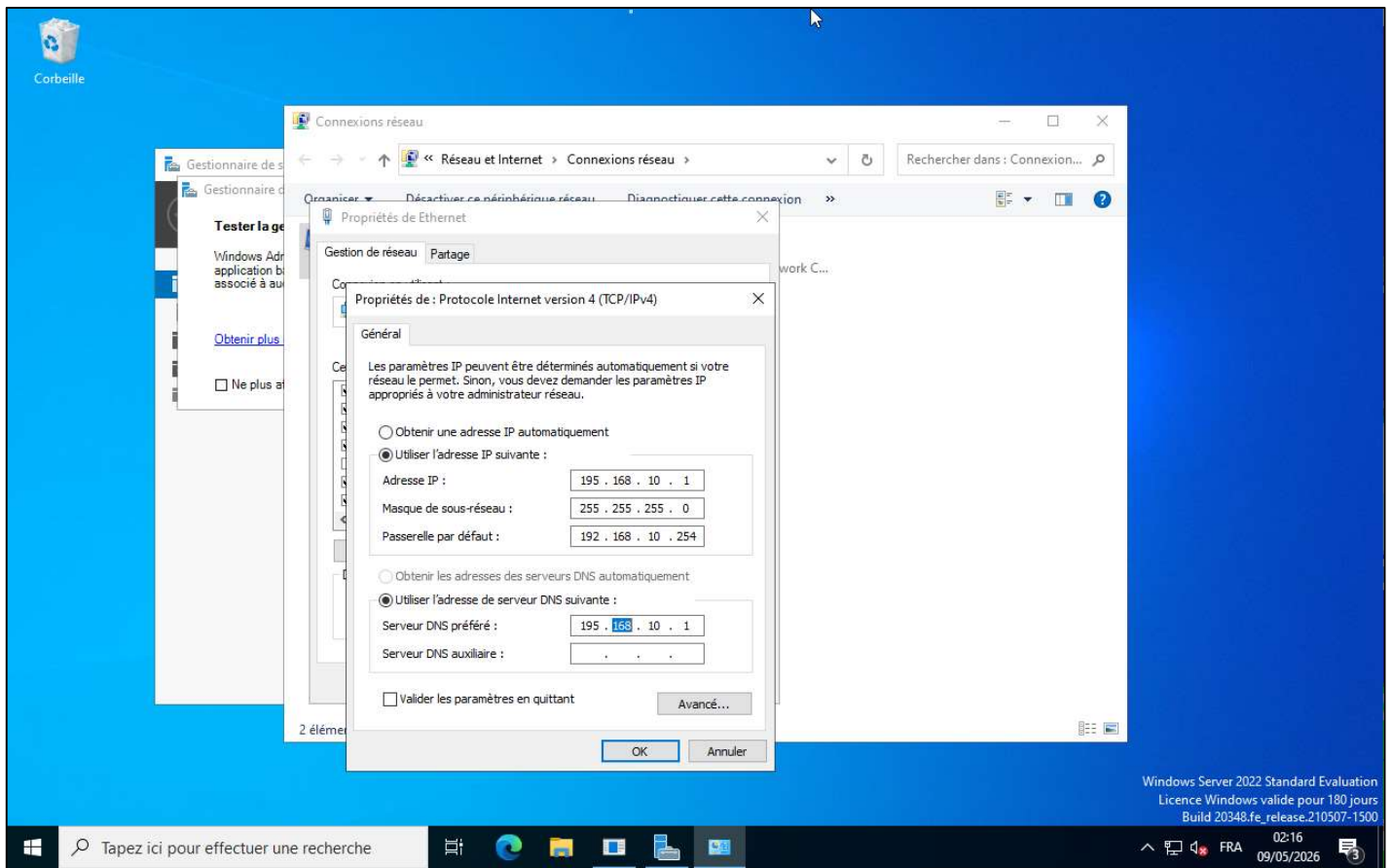


Donc depuis Win_10_1 on se connecte :

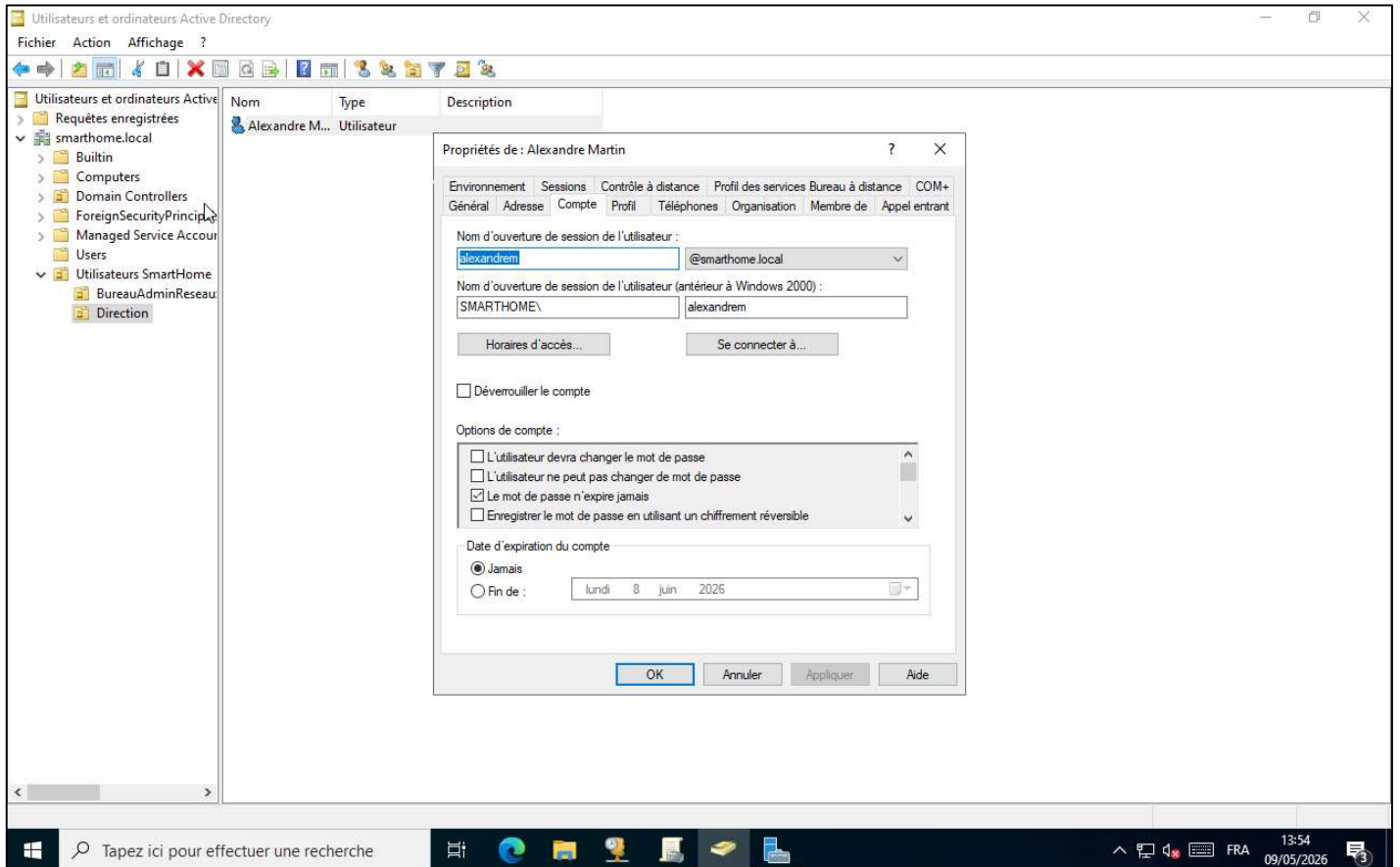


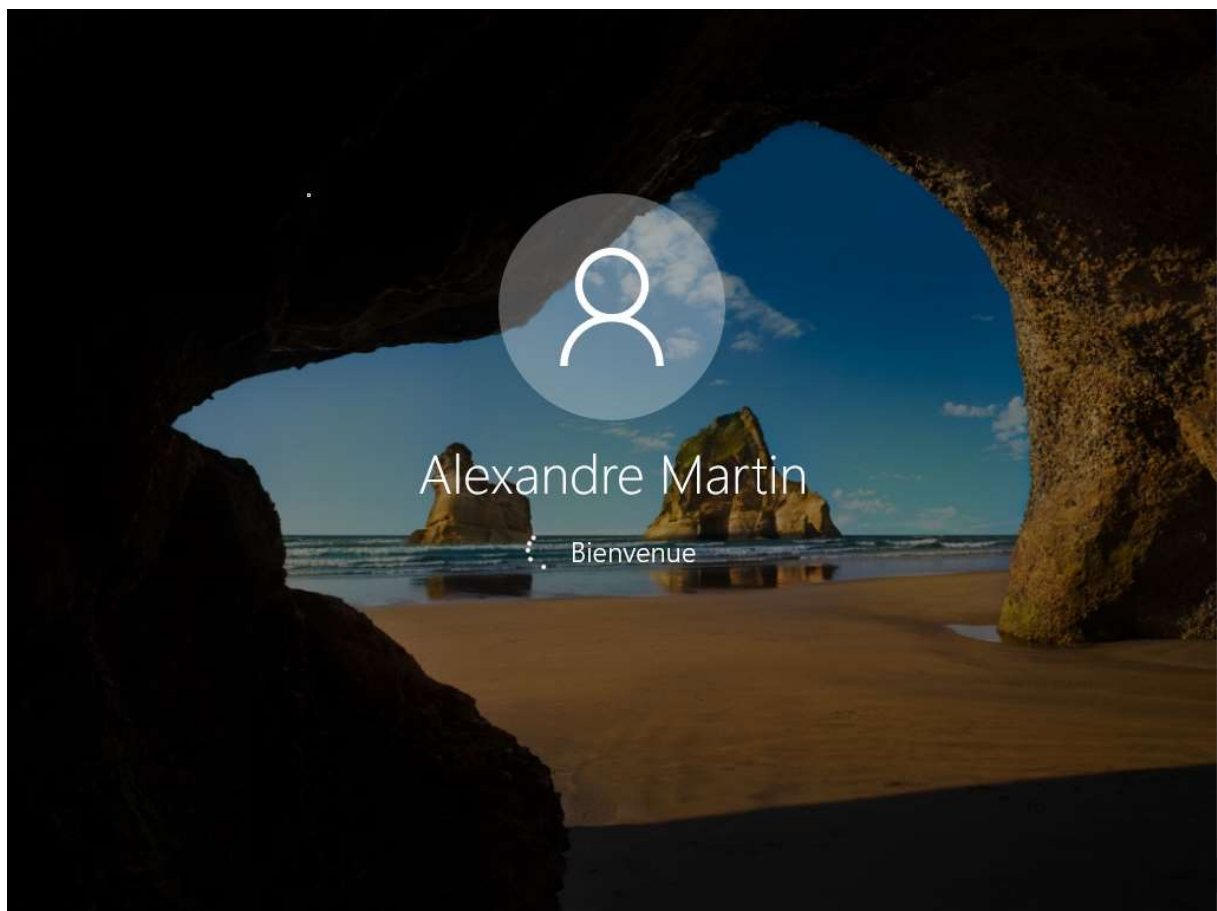
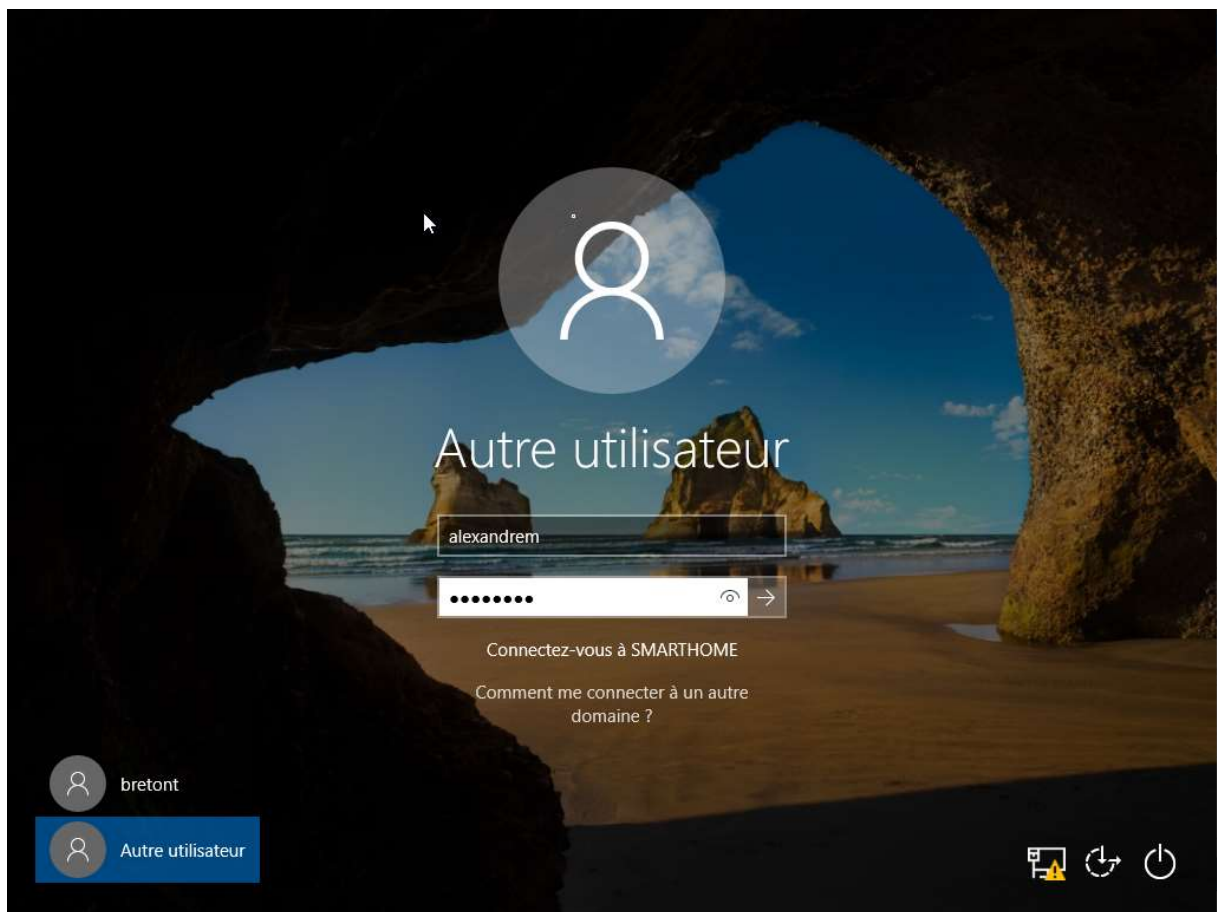
Notre Utilisateur fonctionne :

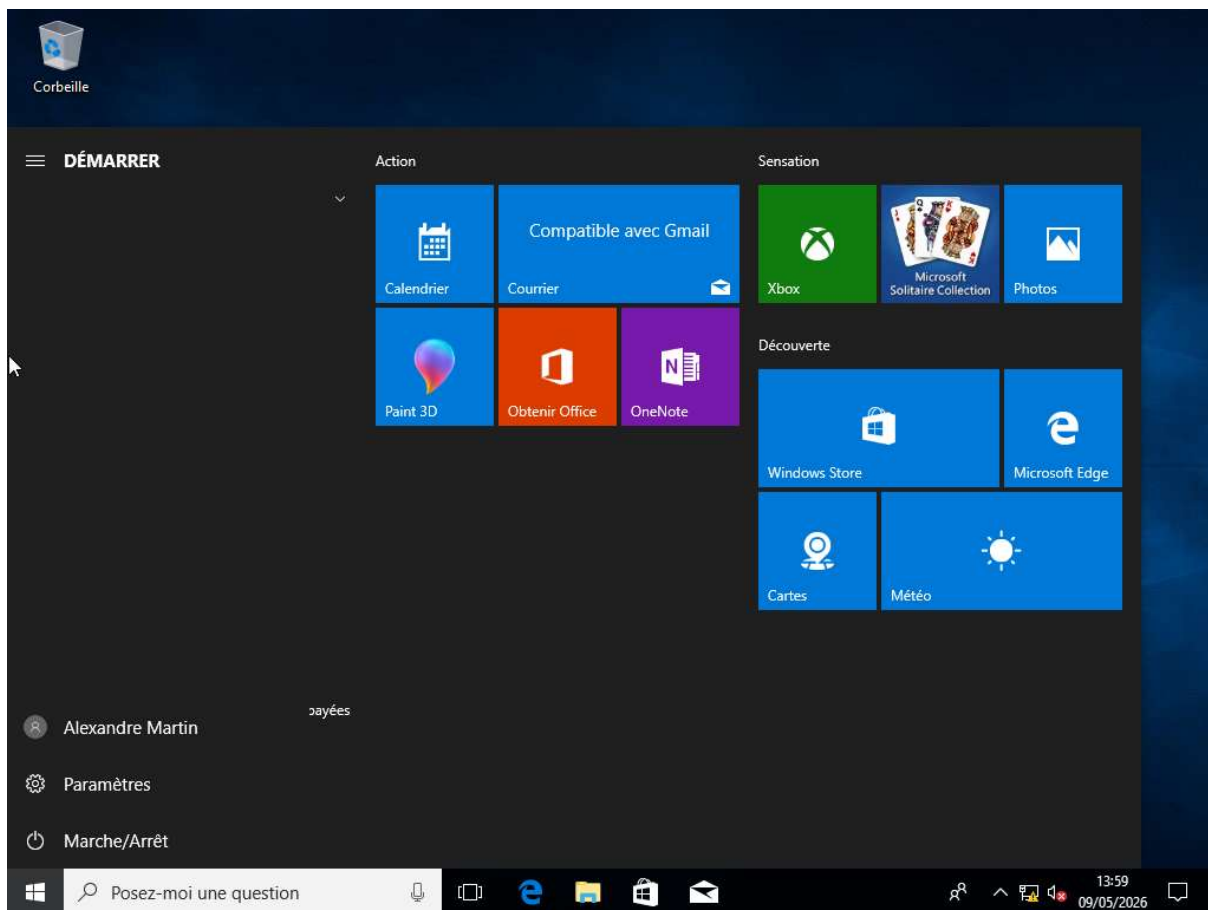




Nous allons maintenant vous connecté avec le compte du dirigeant sur la machine virtuelle Win_10_1 :







PARTIE 2 : Mise en place de l'environnement des utilisateurs sur leurs sessions :

❶ Fond d'écran & BGInfo :

Pour déployer BGInfo il va falloir mettre en place une GPO qui va consister à exécuter un script batch qui va exécuter la Template de BGInfo mais également le fond écran désigné.



ATTENTION !!! La GPO "Fond écran" de base a un paramètre "**Papier peint du Bureau**" activé avec le chemin de l'image, ce qui s'appliquera après BGInfo et écrasera son résultat, empêchant ainsi l'affichage des informations sur le bureau.



BGInfo est un logiciel permettant d'afficher des informations concernant le serveur sur le quel il est installé directement sur le fond d'écran. BGInfo peut être téléchargé sur ce lien.



Télécharger le logiciel depuis : <https://learn.microsoft.com/fr-fr/sysinternals/downloads/bginfo>

Learn Documentation Formation et Labs Q&A Rubriques

Sysinternals Téléchargements Communauté Ressources

Certains parties de cette rubrique peuvent être traduites par une machine ou par l'IA.

Rechercher par titre

Domicile

Téléchargements

Utilitaires de fichiers et de disques

Utilitaires de mise en réseau

Utilitaires de processus

Utilitaires de sécurité

Informations système

Miscellaneous

Miscellaneous

Bginfo

Économiseur d'écran BlueScreen

CpuStress

Ctrl2Cap

DebugView

Desktops

Hex2dec

NotMyFault

De Debut

Télécharger le PDF

Learn > Sysinternals >

BgInfo v4.33

Par Mark Russinovich

Publication : 13 février 2025

Télécharger BgInfo (2,2 Mo)

Exécutez maintenant à partir de Sysinternals Live.

Introduction

Combien de fois avez-vous parcouru un système dans votre bureau et avez-vous eu besoin de cliquer sur plusieurs fenêtres de diagnostic pour vous rappeler des aspects importants de sa configuration, tels que son nom, son adresse IP ou la version de son système d'exploitation ? Si vous gérez plusieurs ordinateurs, vous avez probablement besoin de *Bginfo*. Il affiche automatiquement des informations pertinentes sur un ordinateur Windows sur l'arrière-plan du bureau, telles que le nom de l'ordinateur, l'adresse IP, la version du Service Pack, etc. Vous pouvez modifier n'importe quel champ, ainsi que la police et les couleurs d'arrière-plan, et le placer dans votre dossier de démarrage afin qu'il exécute chaque démarrage, ou même le configurer pour qu'il s'affiche en arrière-plan de l'écran de connexion.

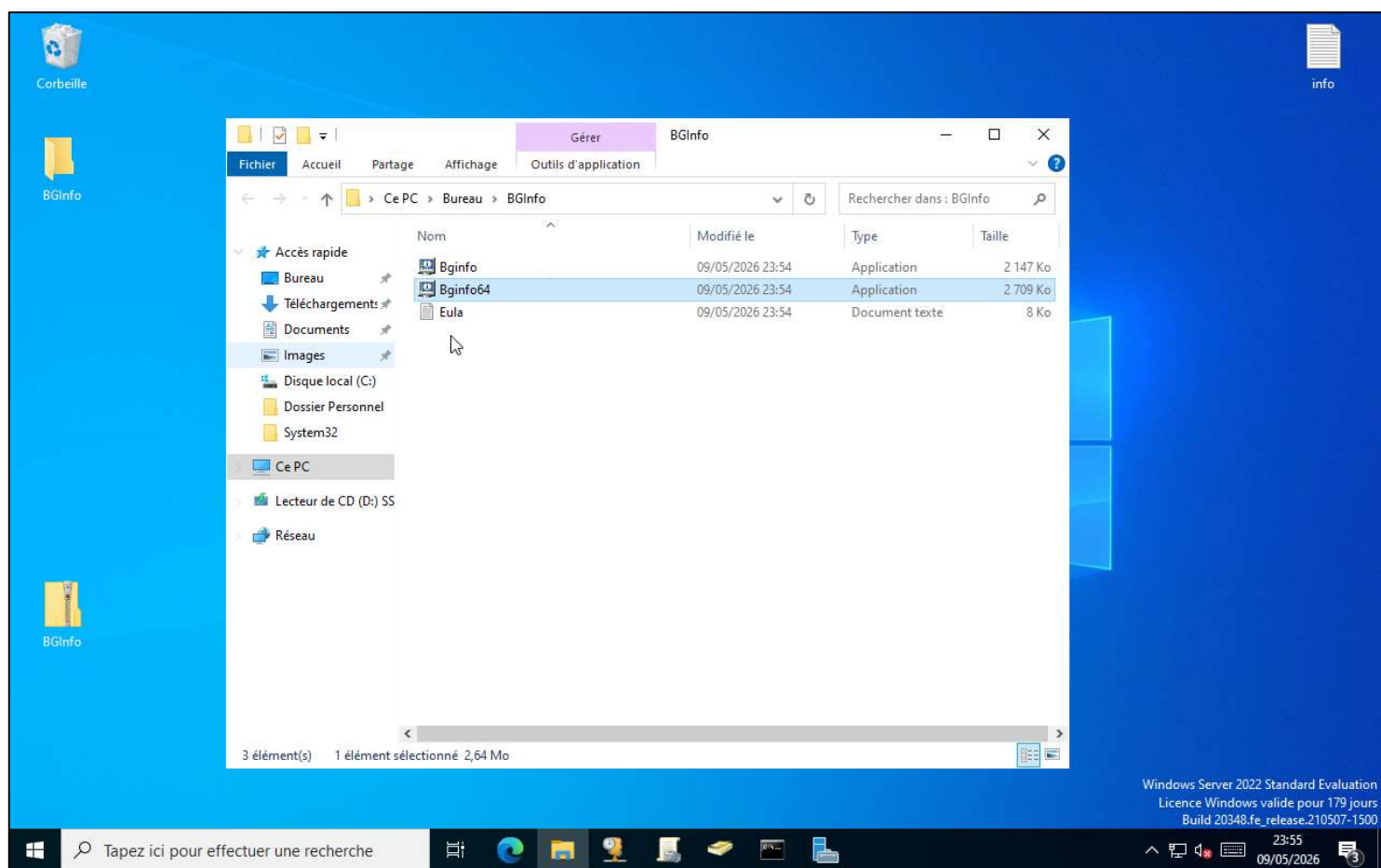
Étant donné que *Bginfo* écrit simplement une nouvelle image bitmap de bureau et quitte, vous n'avez pas à vous soucier de la consommation de ressources système ni de l'interférence avec d'autres applications.

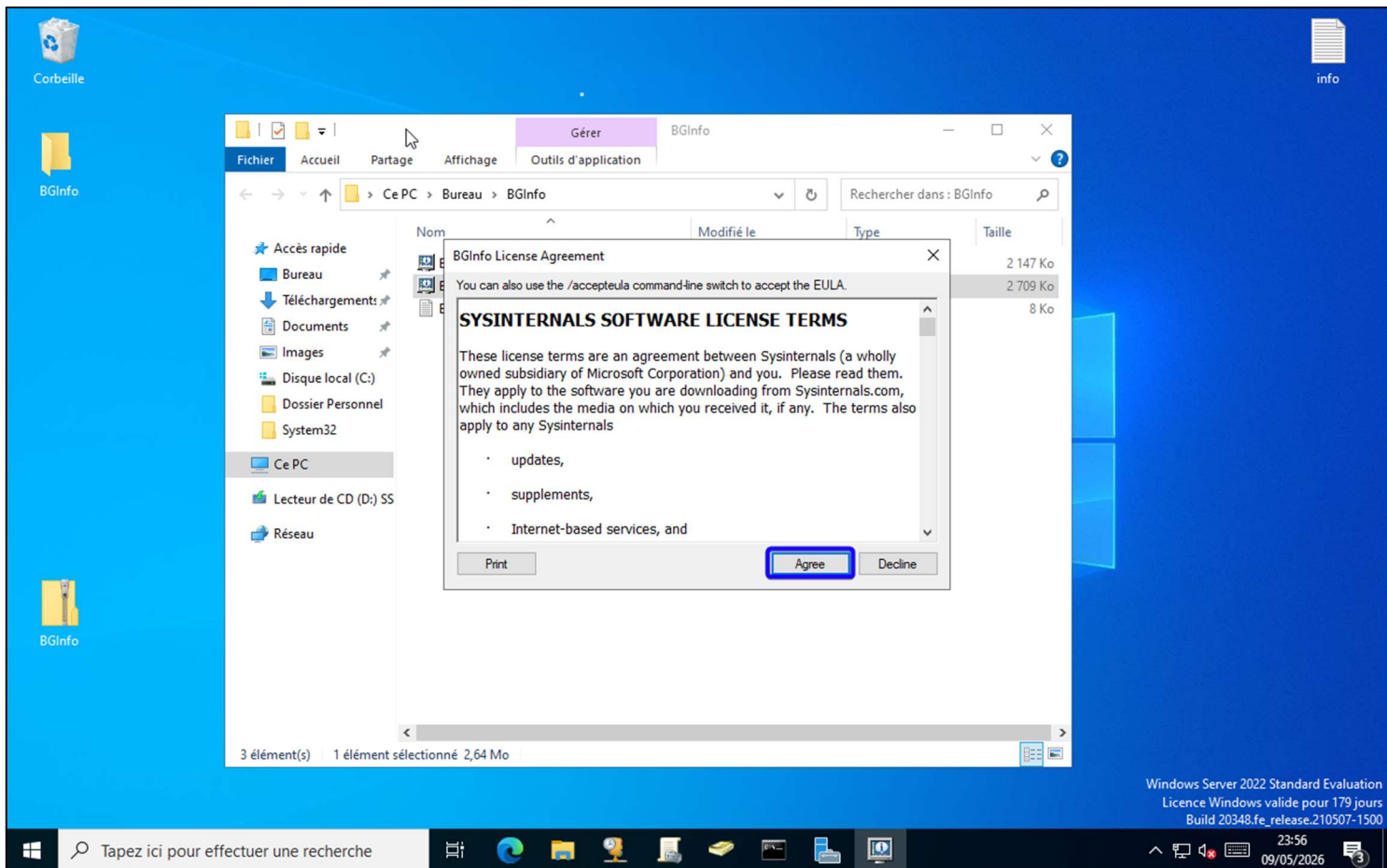
Sysinternals BgInfo

Dans cet article

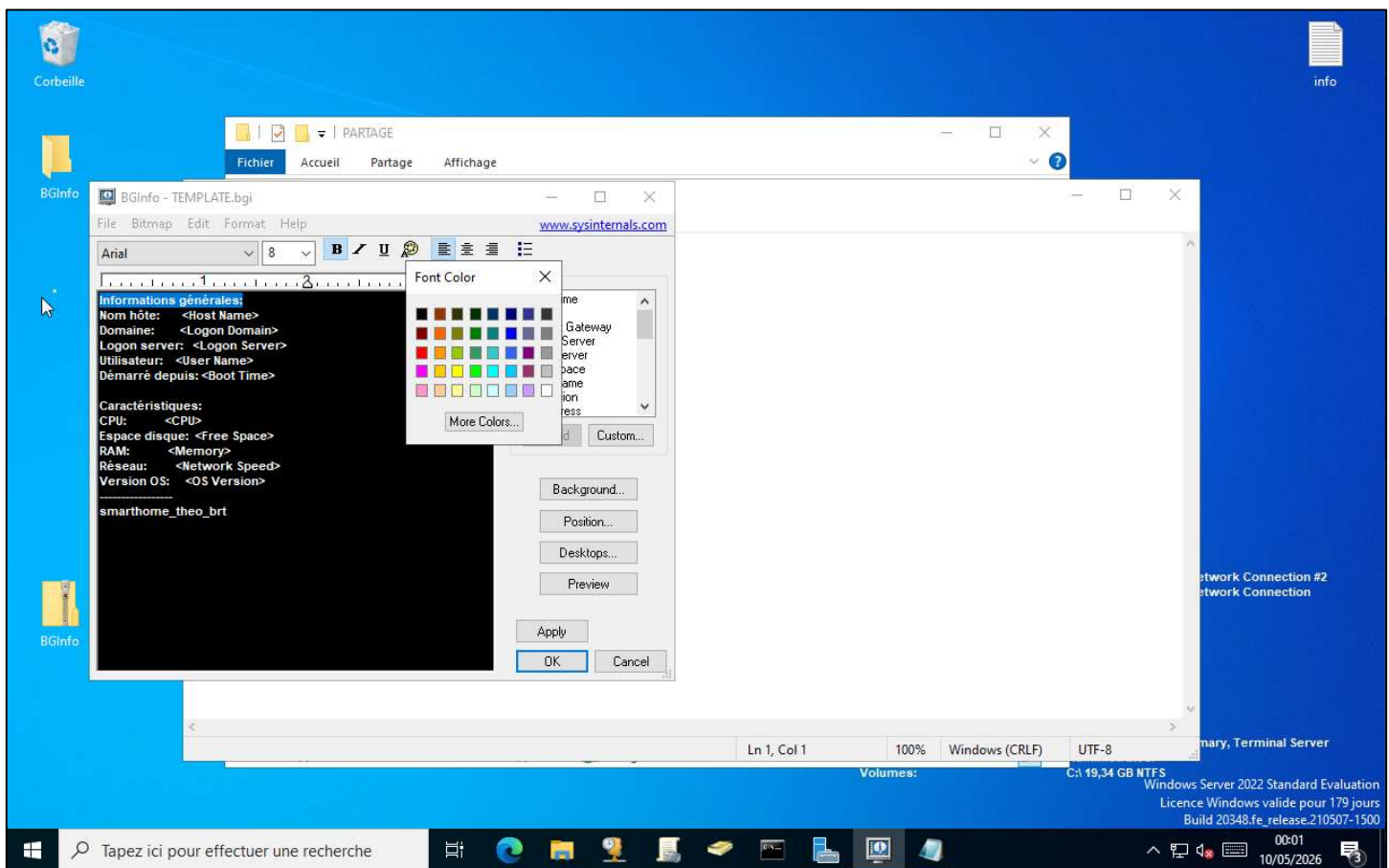
- Introduction
- Installation et utilisation
- Utilisation de BgInfo
- Boutons d'apparence
- Éléments du menu Configuration
- Options de la ligne de commande

Lancer BGInfo :

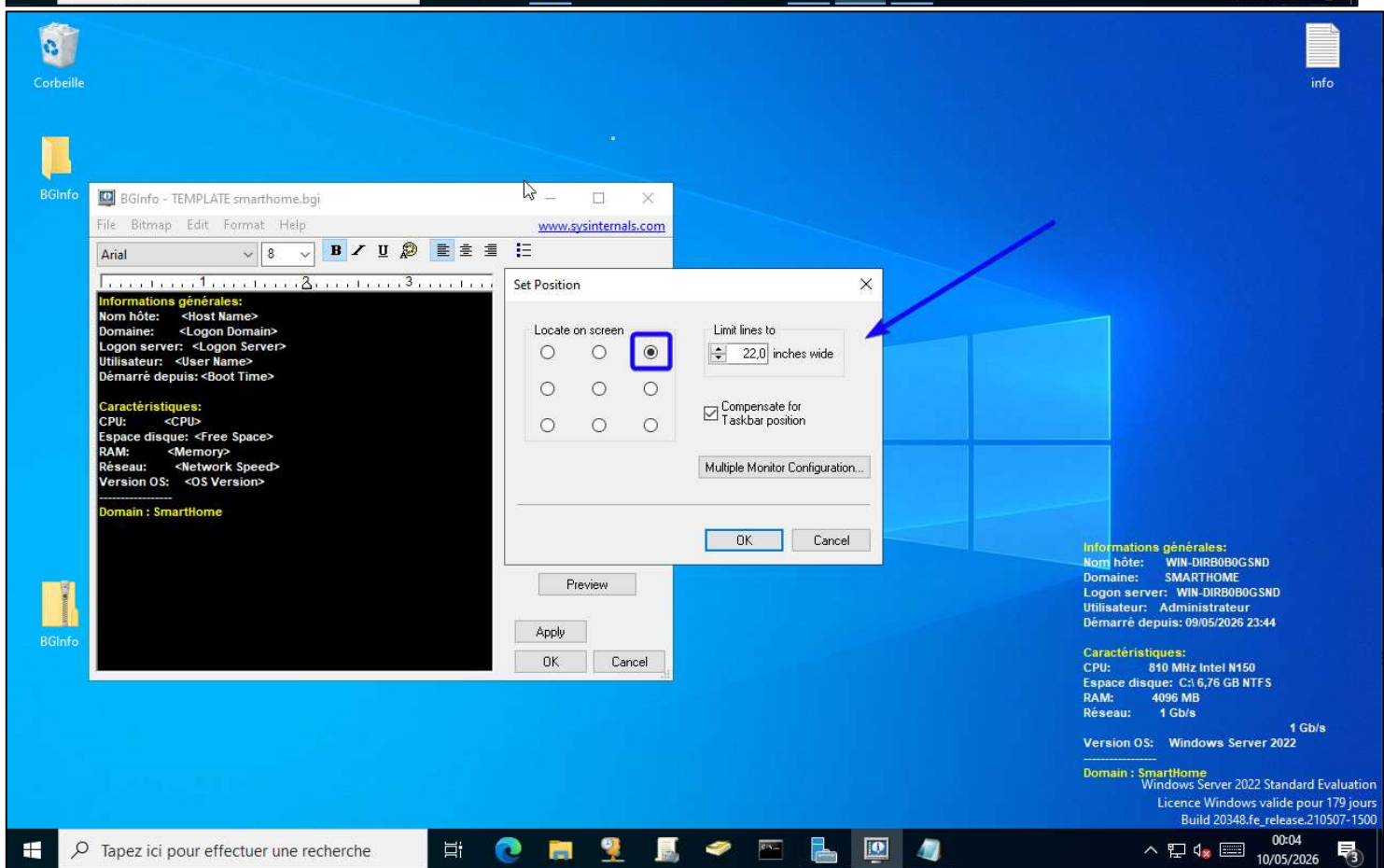
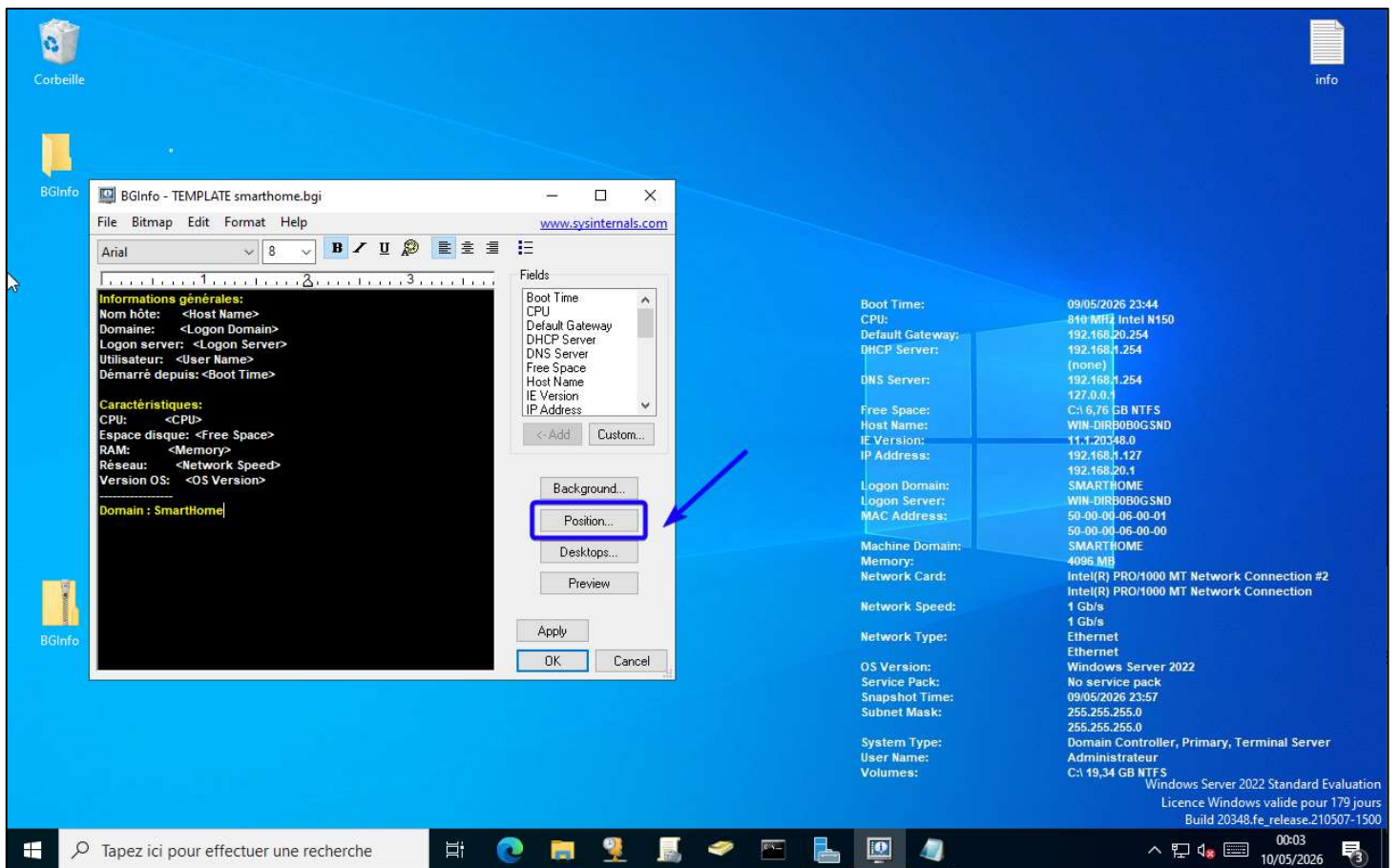


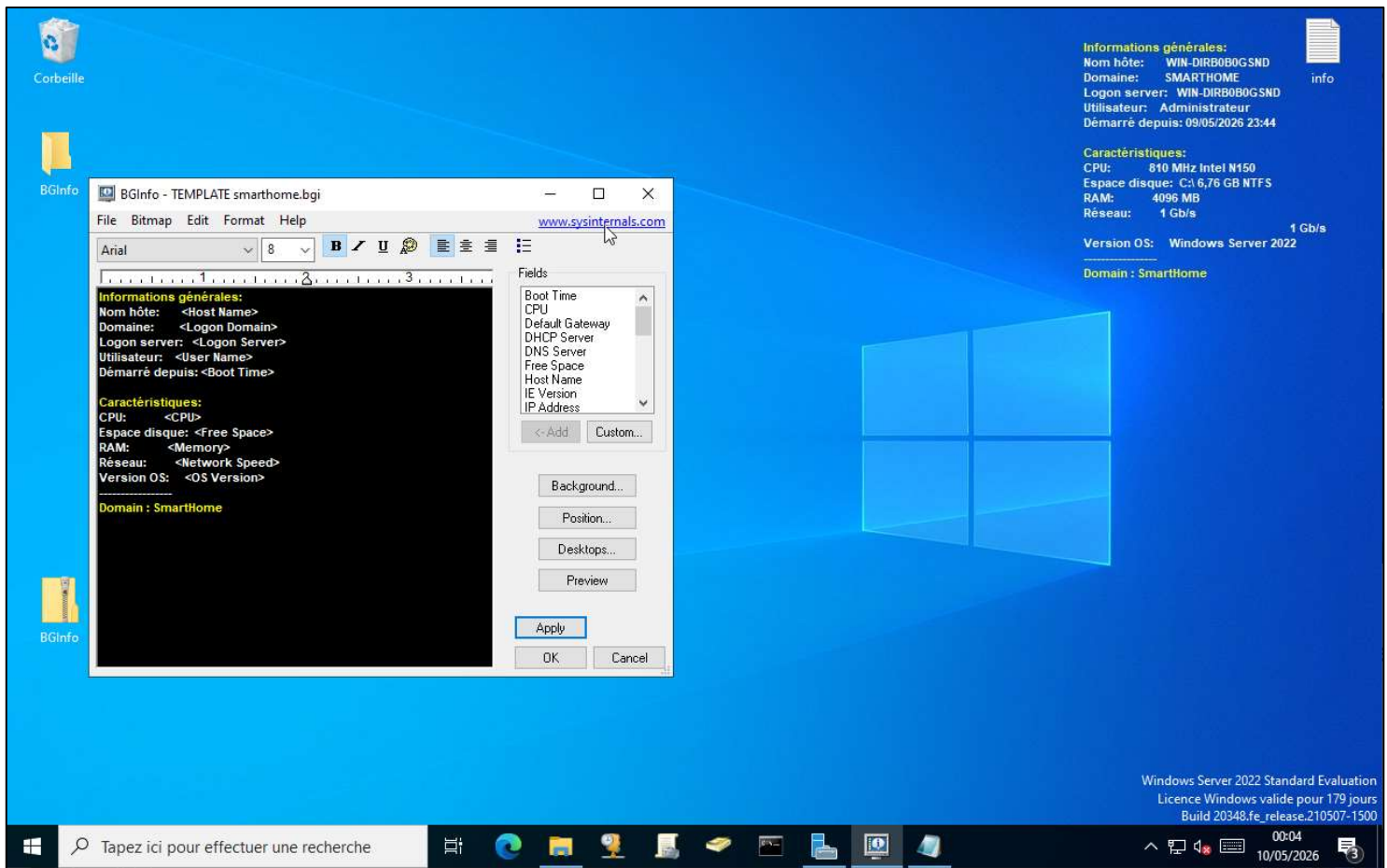


On peut le personnaliser avec des couleurs :



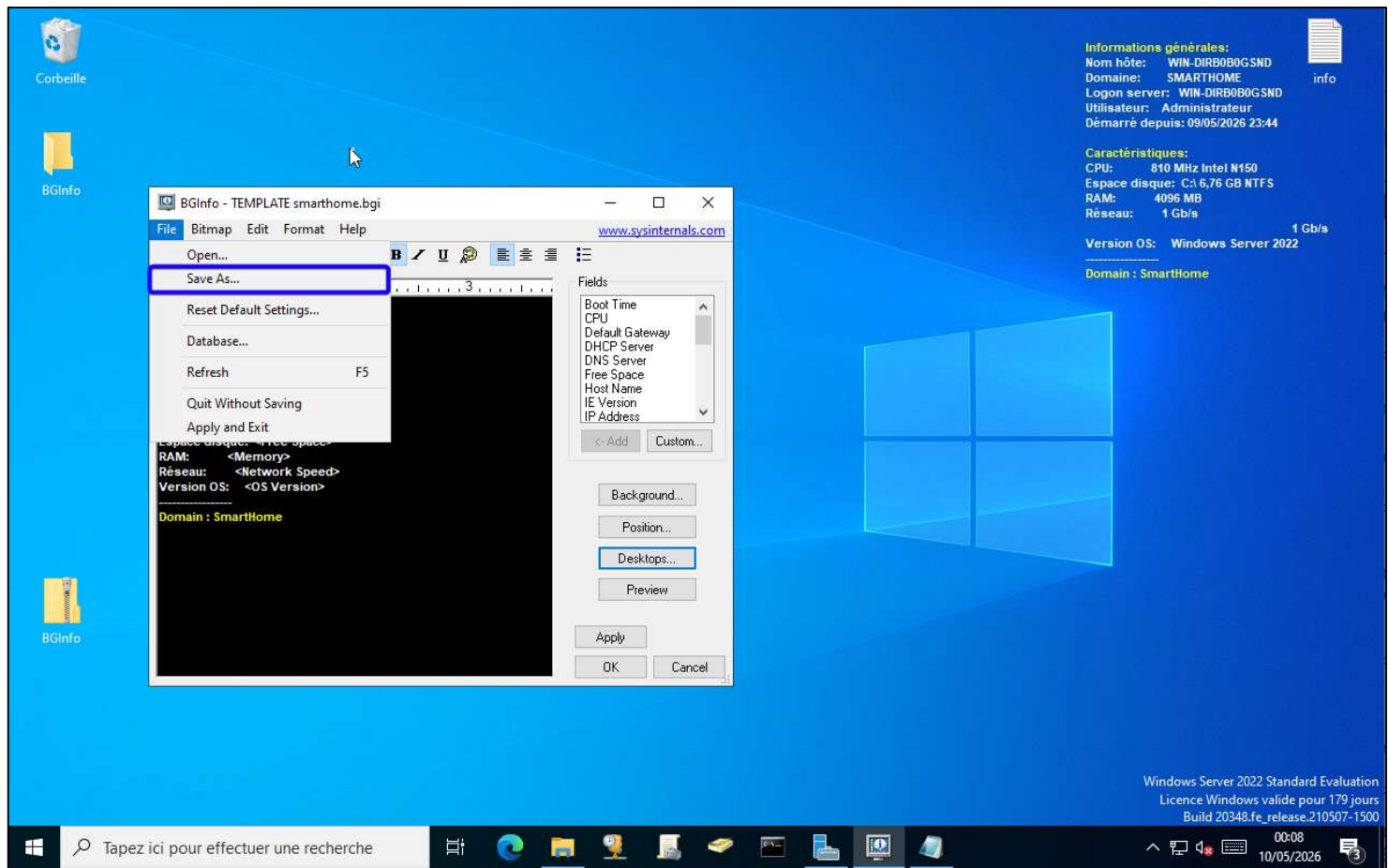
Choisir la position du texte dans le bureau :



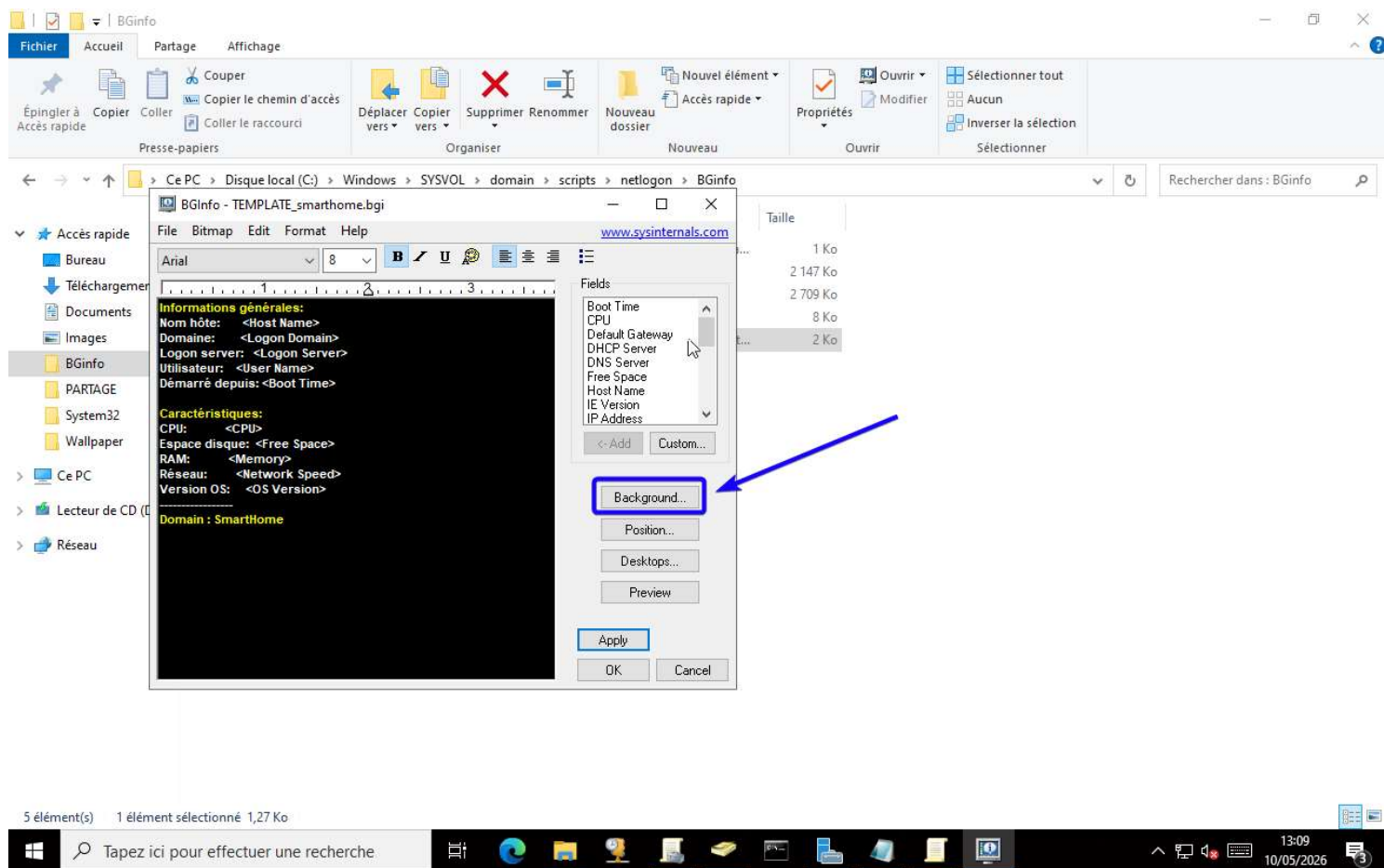


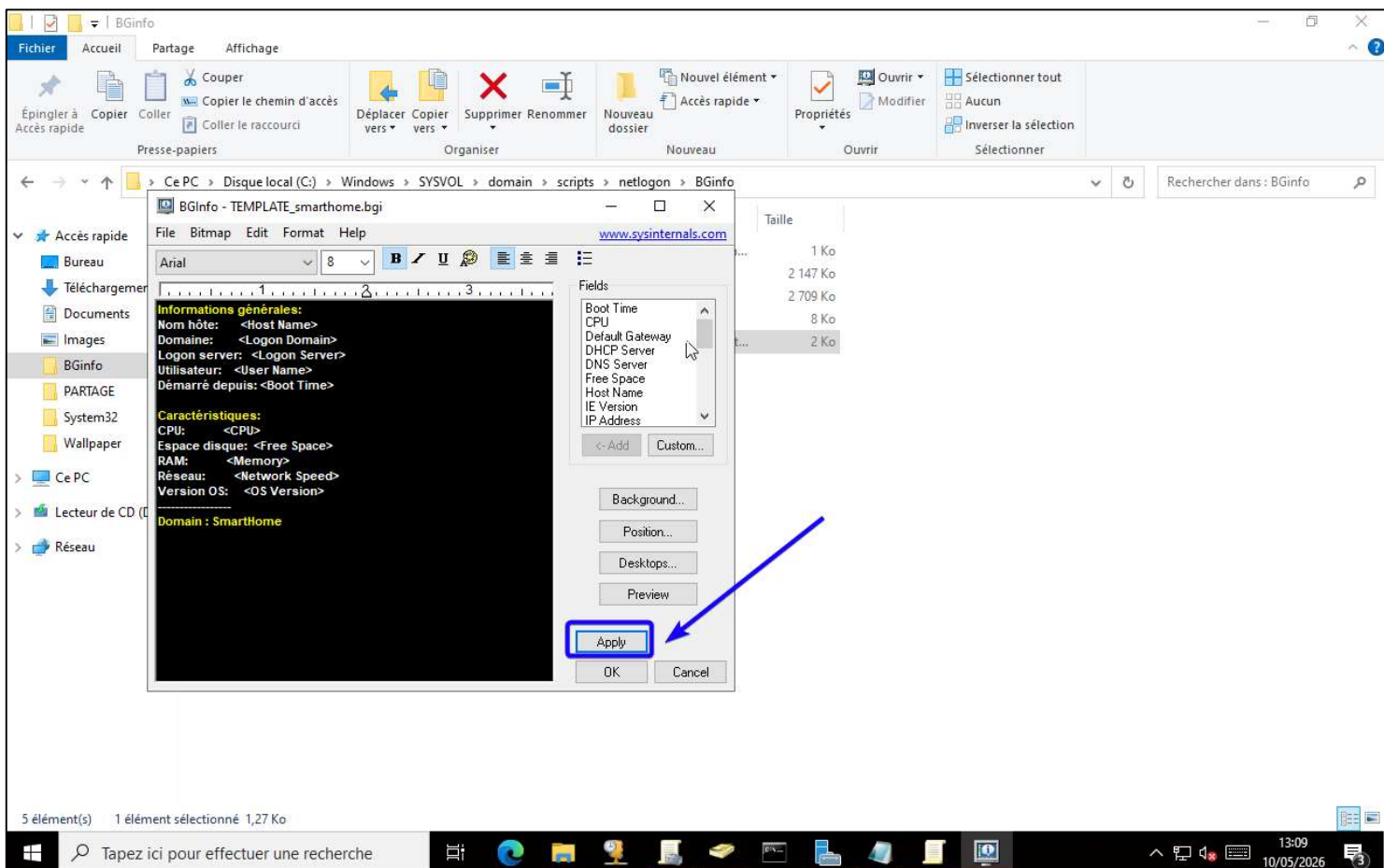
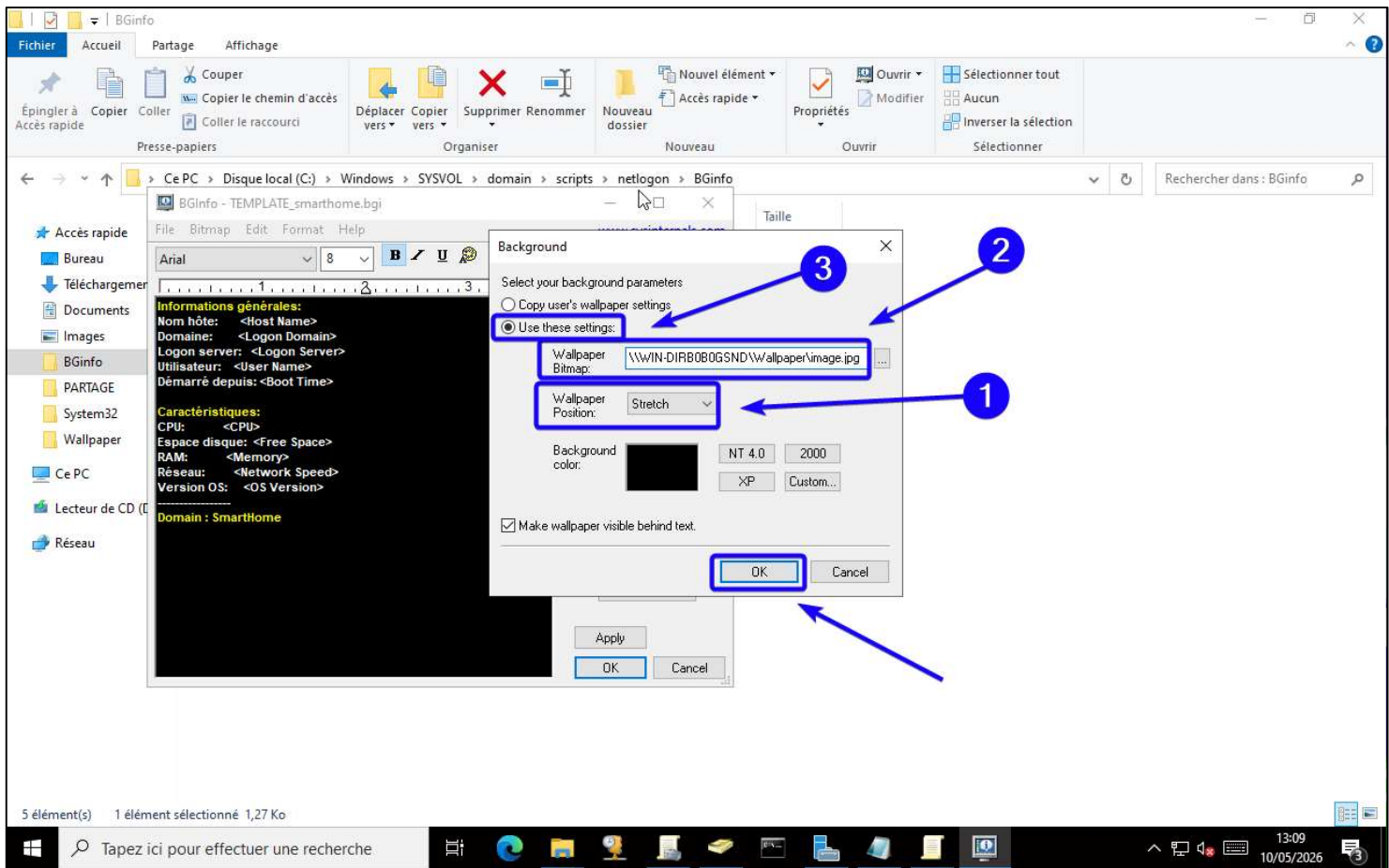
Une fois que tout est bien réglé, on clique sur « **Apply** »

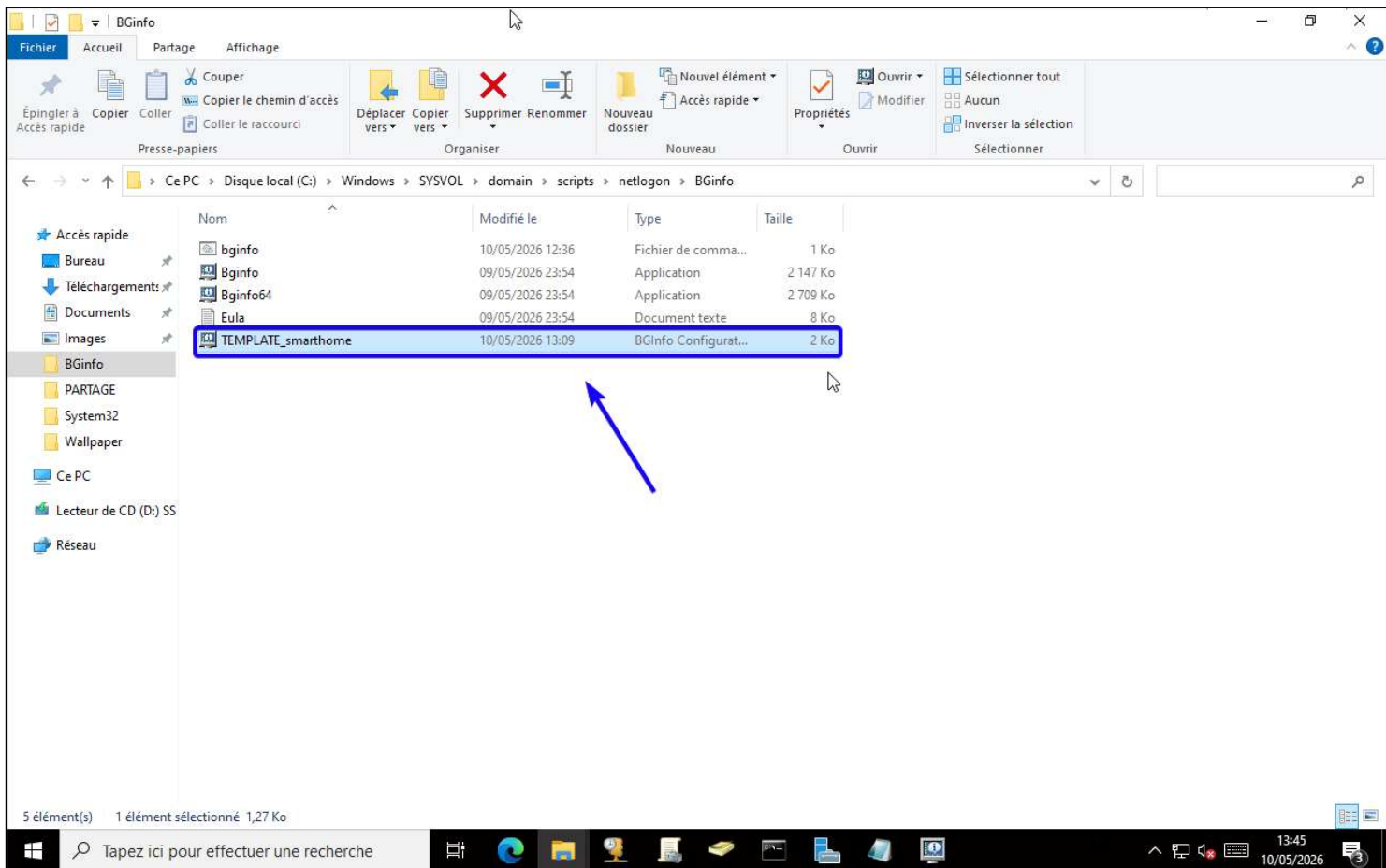
Une fois que notre Template est prêt, on peut l'enregistrer, en un fichier en .bgi



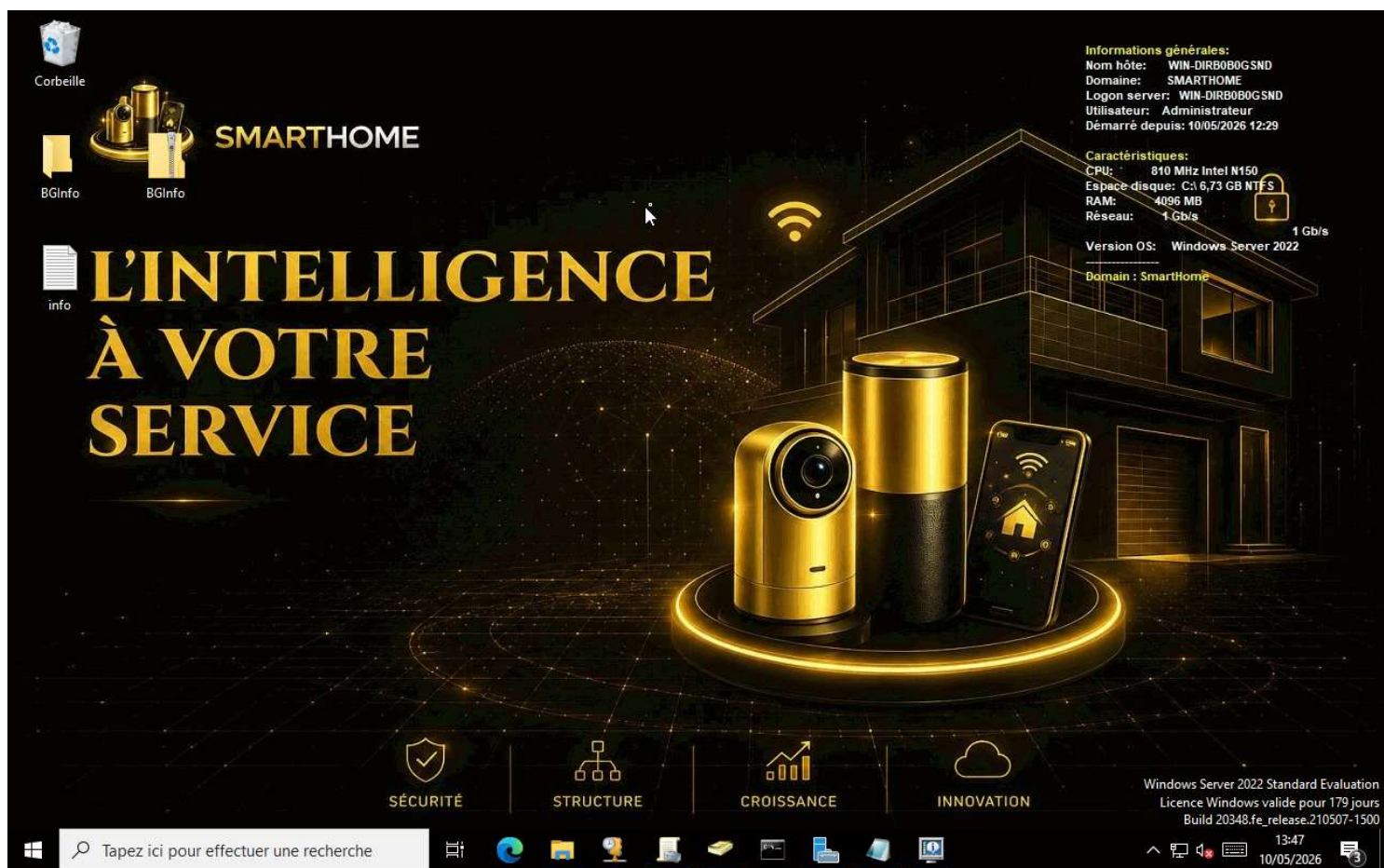
Mettre le fond d'écran avec le bon chemin dans le template :







Résultat en directe sur le serveur :



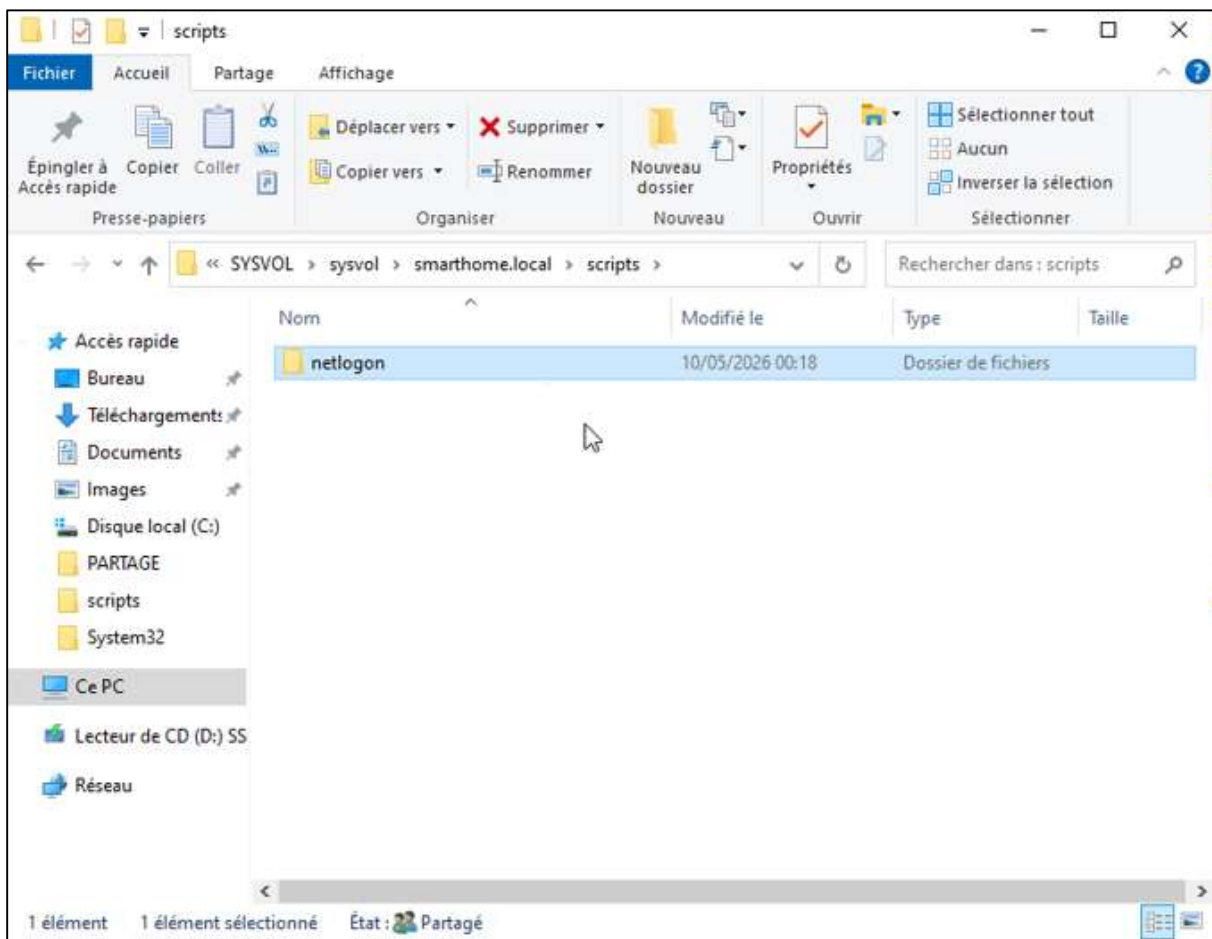
On va maintenant créer une GPO pour déployer BGInfo sur nos poste client.

On va aller mettre les fichiers suivants dans le chemin suivants :

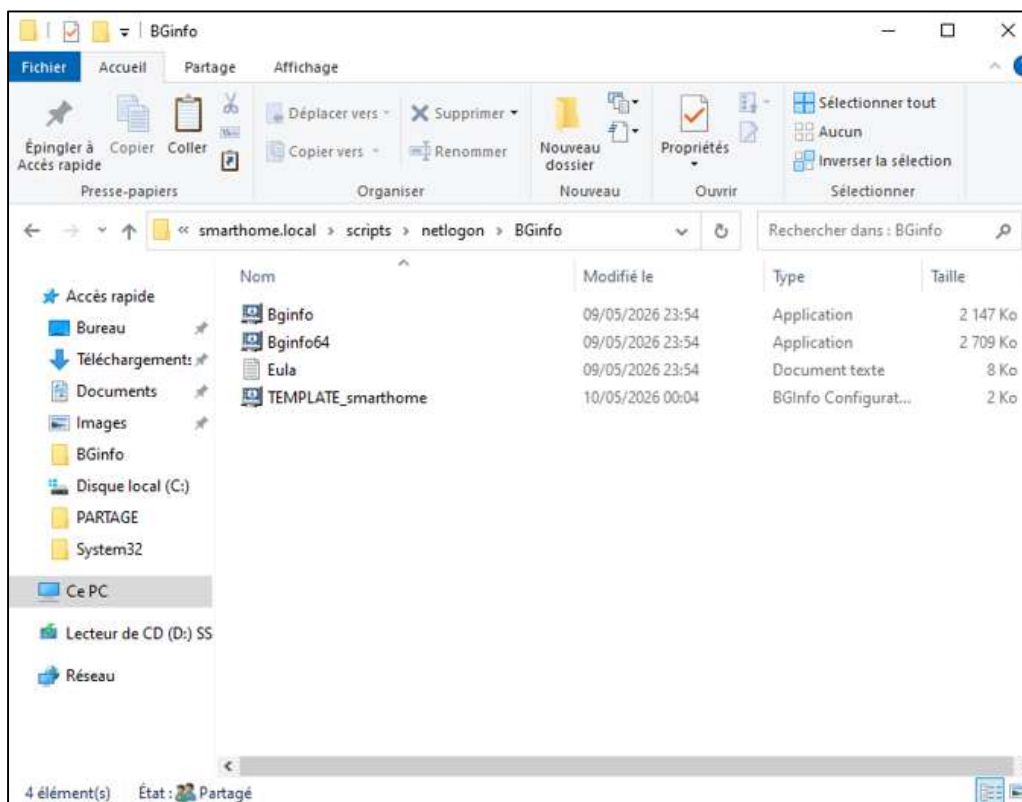
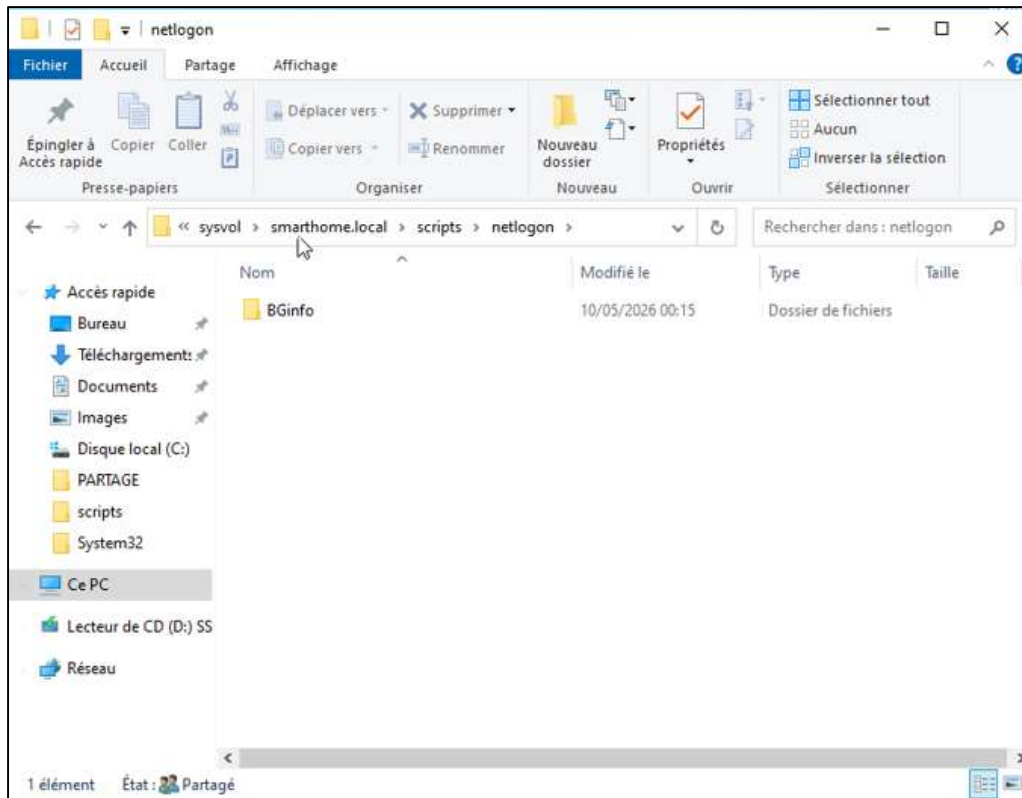
C:\Windows\SYSVOL\sysvol\smarthome.local\scripts

Pour cela, nous allons créer un dossier "**BgInfo**" au sein du partage "Netlogon" de notre contrôleur de domaine. Dans ce dossier, déposez "Bginfo.exe" et le modèle "Template_Bginfo.bgi".

Créer le dossier « **netlogon** » dans scripts



Créer le dossier « **BGinfo** » dans netlogon



Créer le script batch pour la GPO.

*shshhshs - Bloc-notes

Fichier Edition Format Affichage Aide

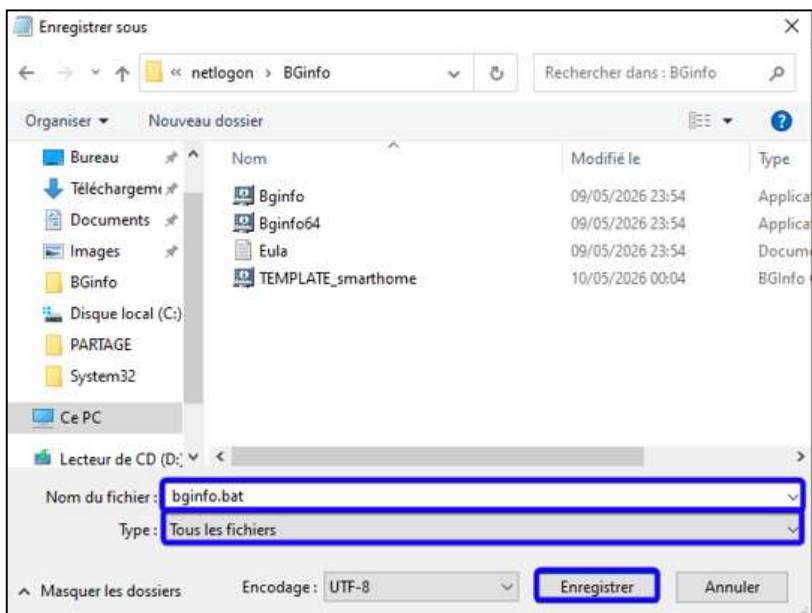
```
@echo off
\\smarthome.local\NETLOGON\netlogon\BGinfo\Bginfo.exe \\smarthome.local\NETLOGON\netlogon\BGinfo\TEMPLATE_smarthome.bgi /accepteula /silent /timer 0
Exit
```

Admin123

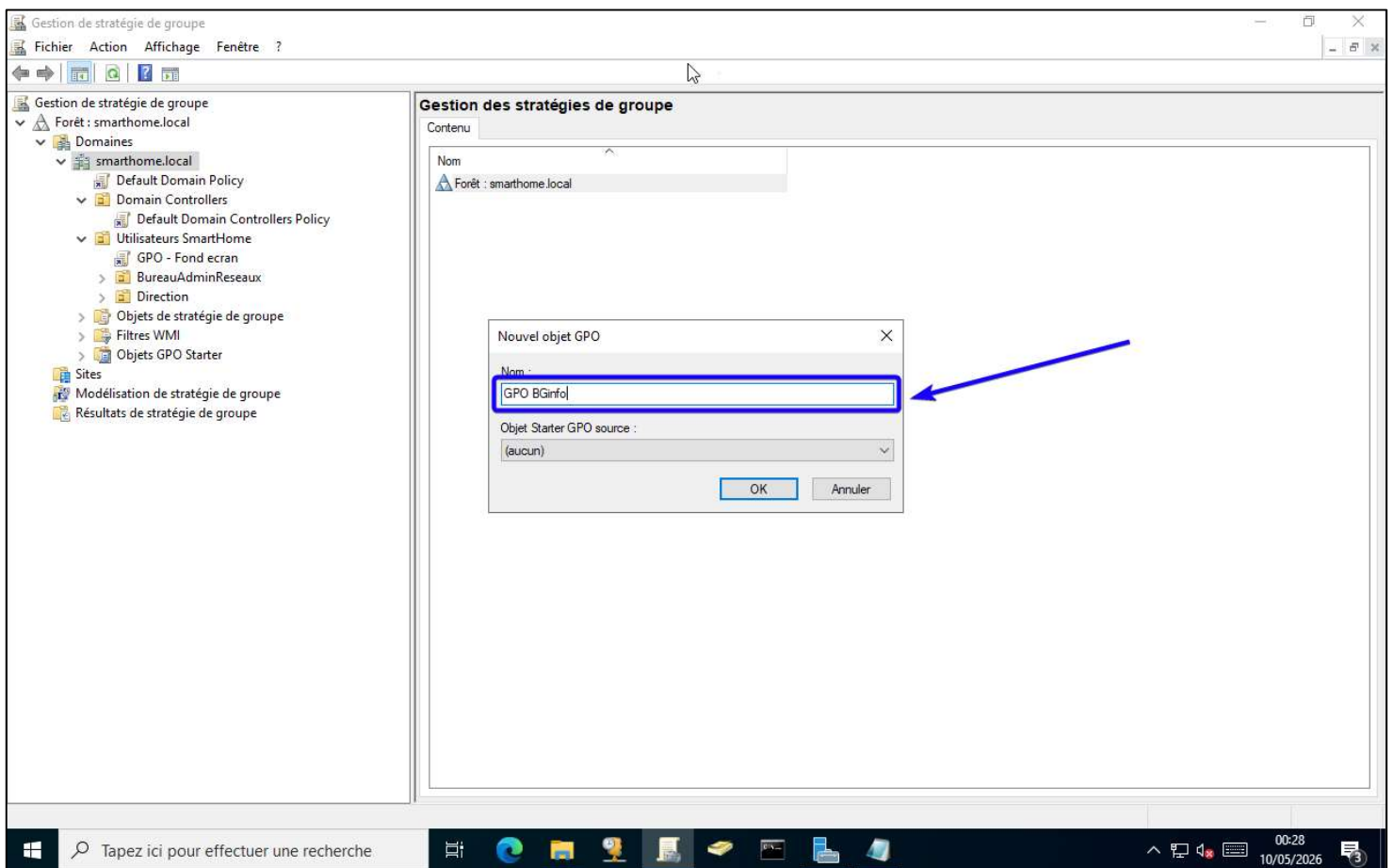
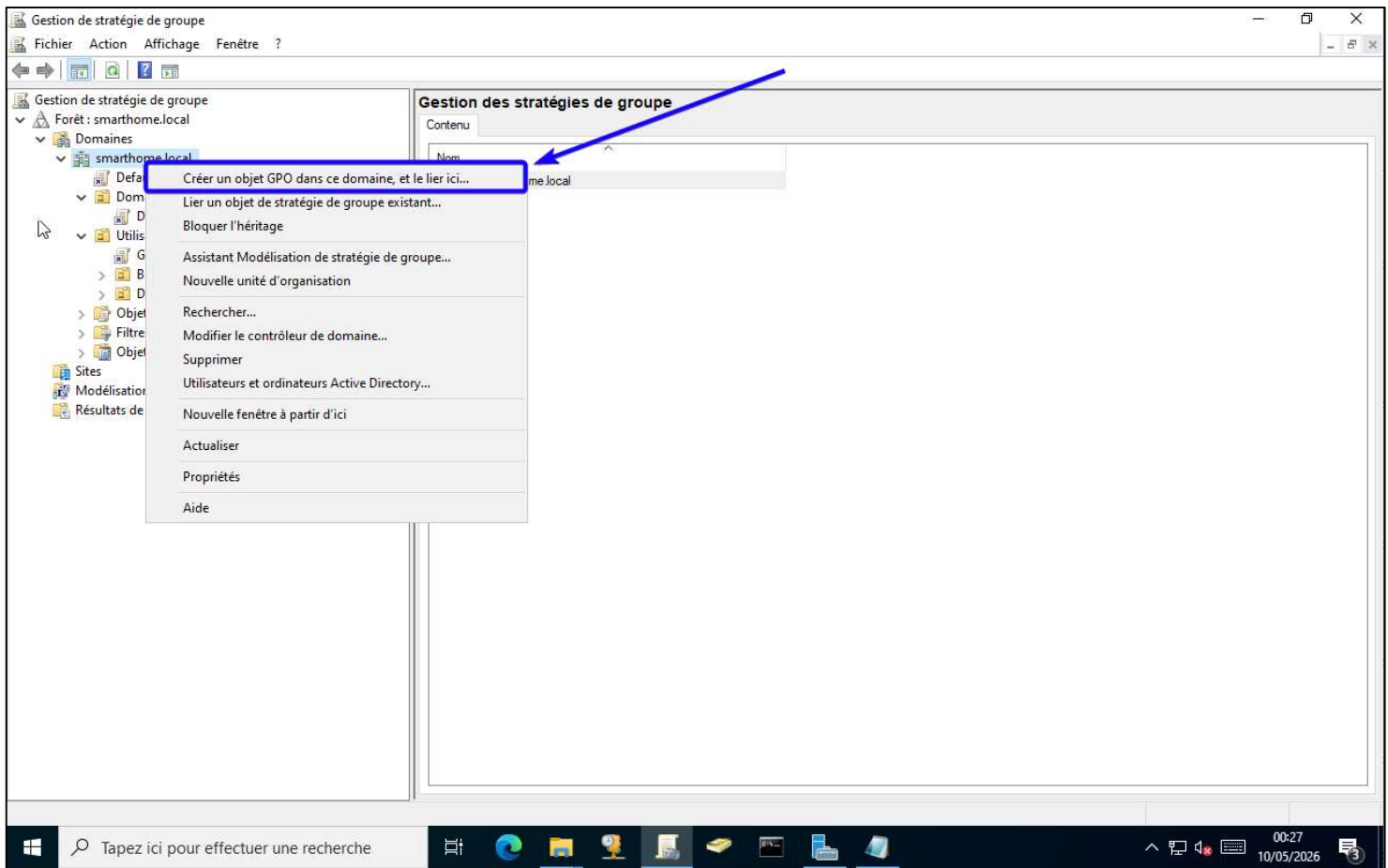
Ln 6, Col 9 100% Windows (CRLF) UTF-8

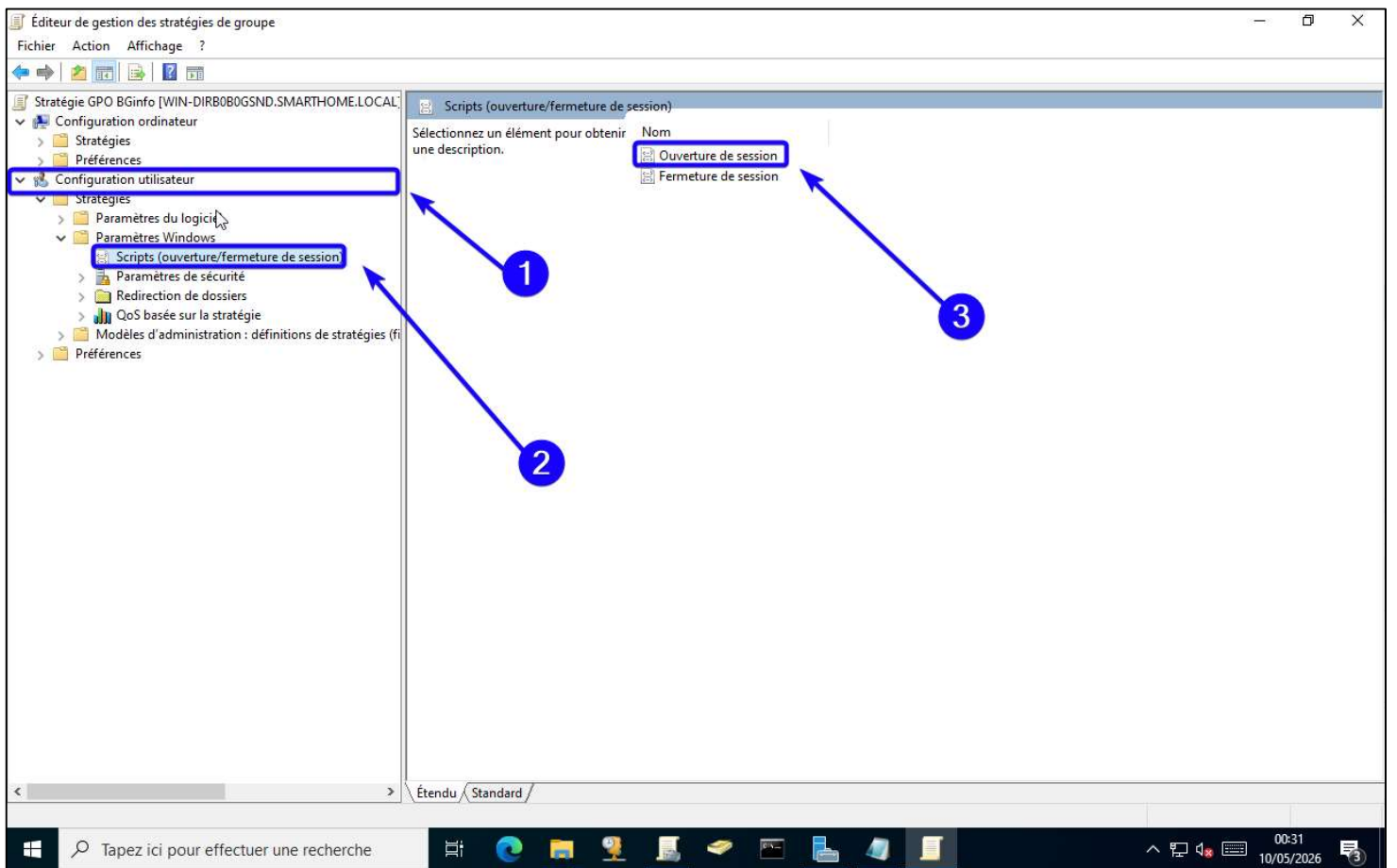
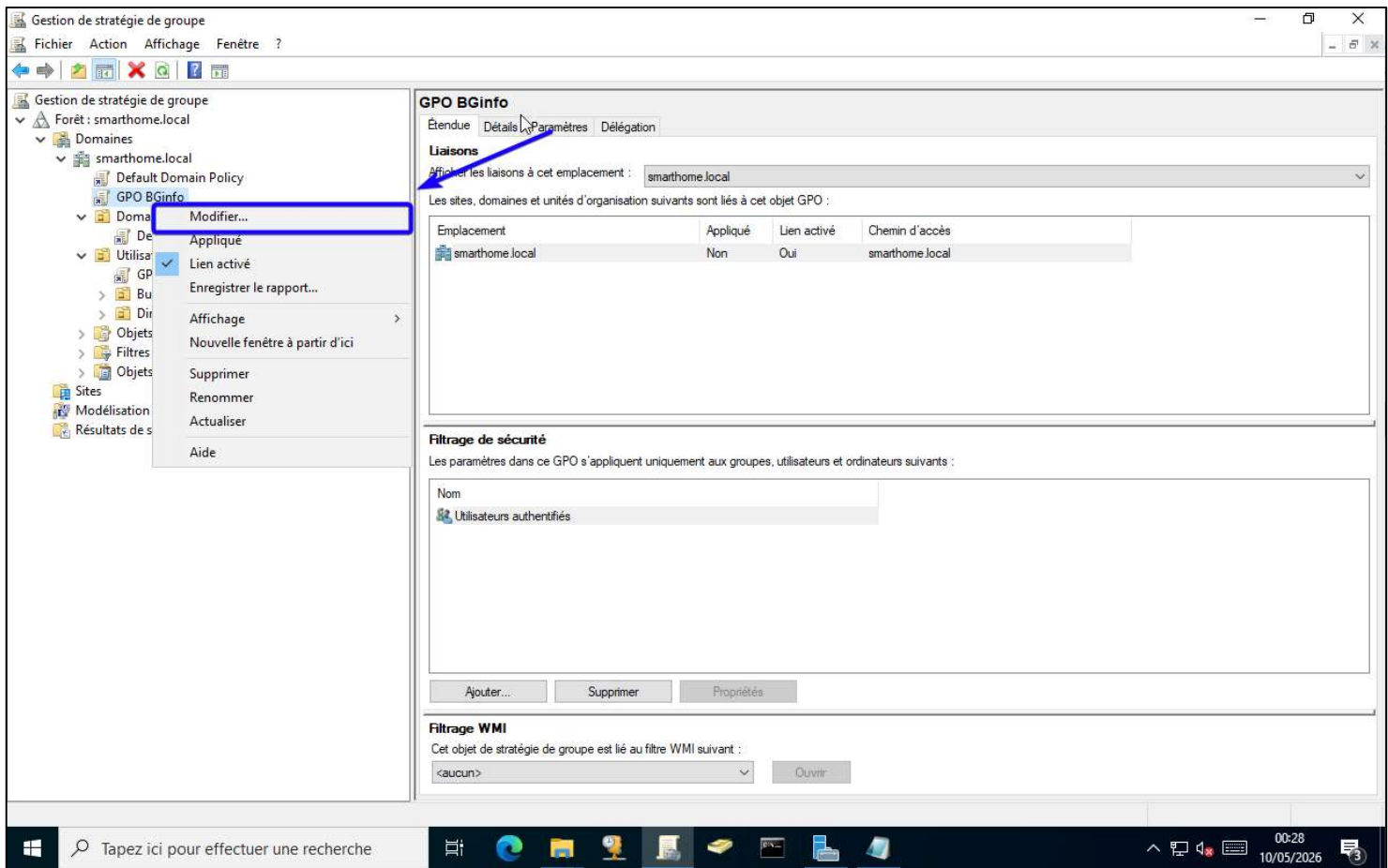
Tapez ici pour effectuer une recherche

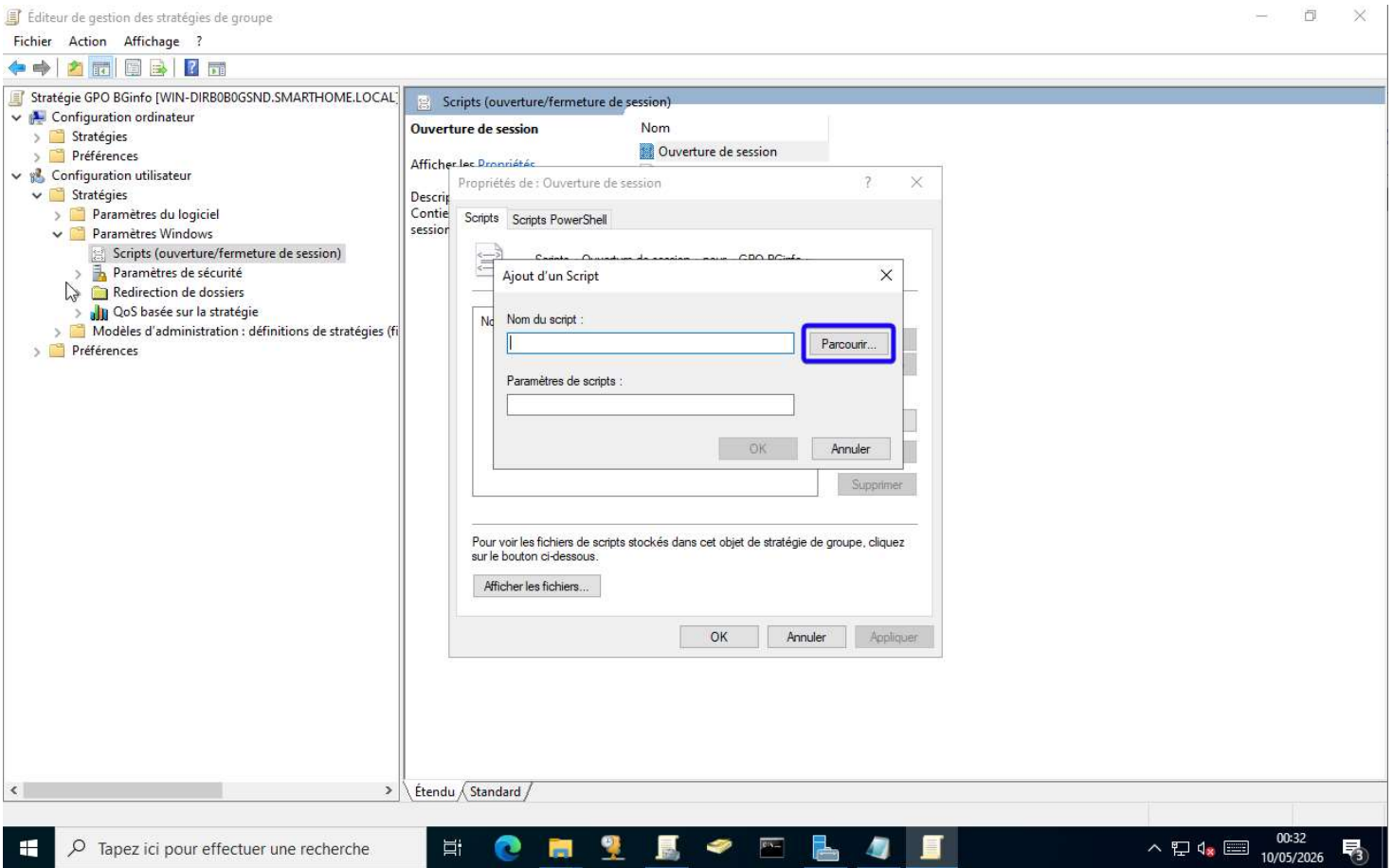
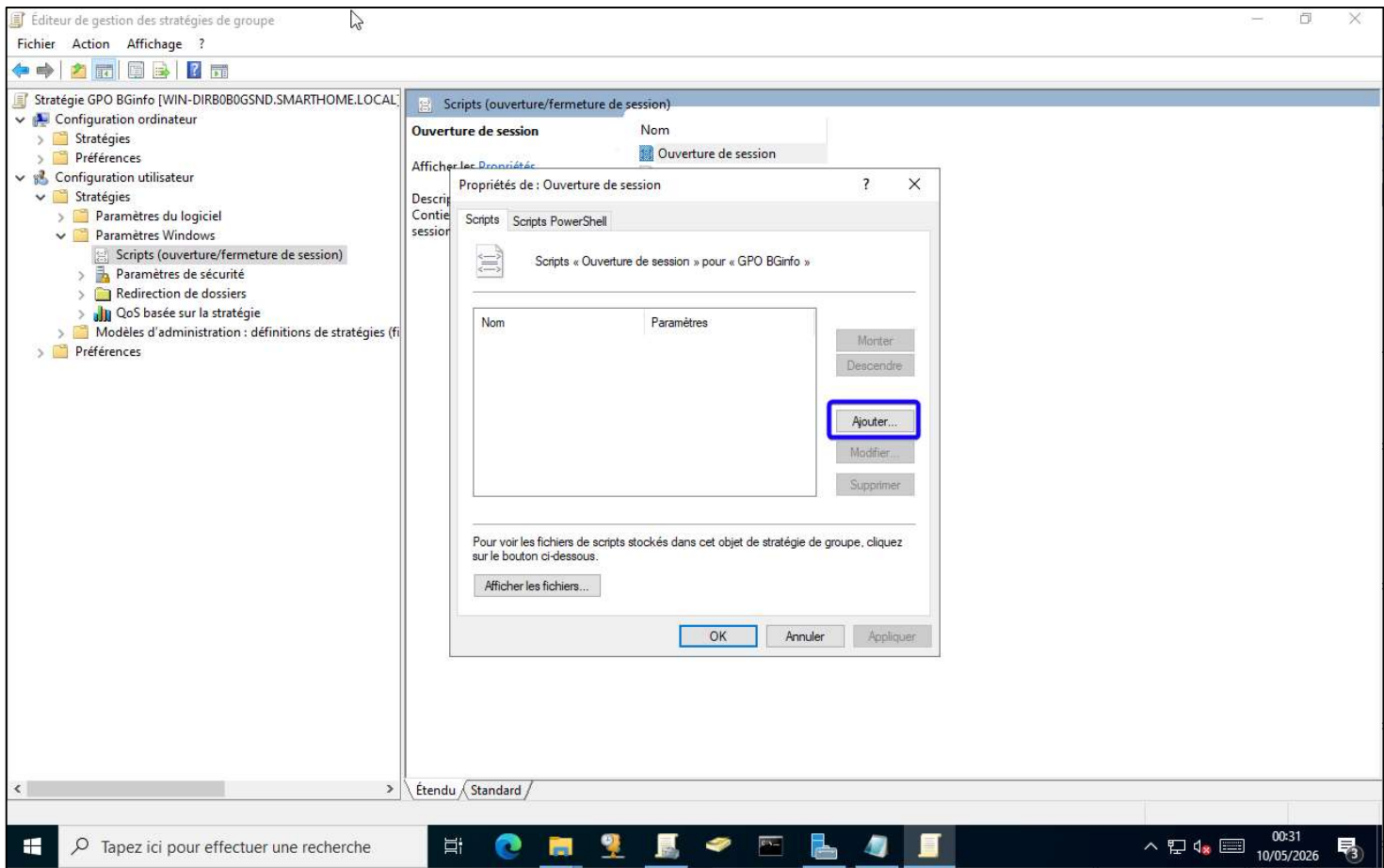
13:49 10/05/2026

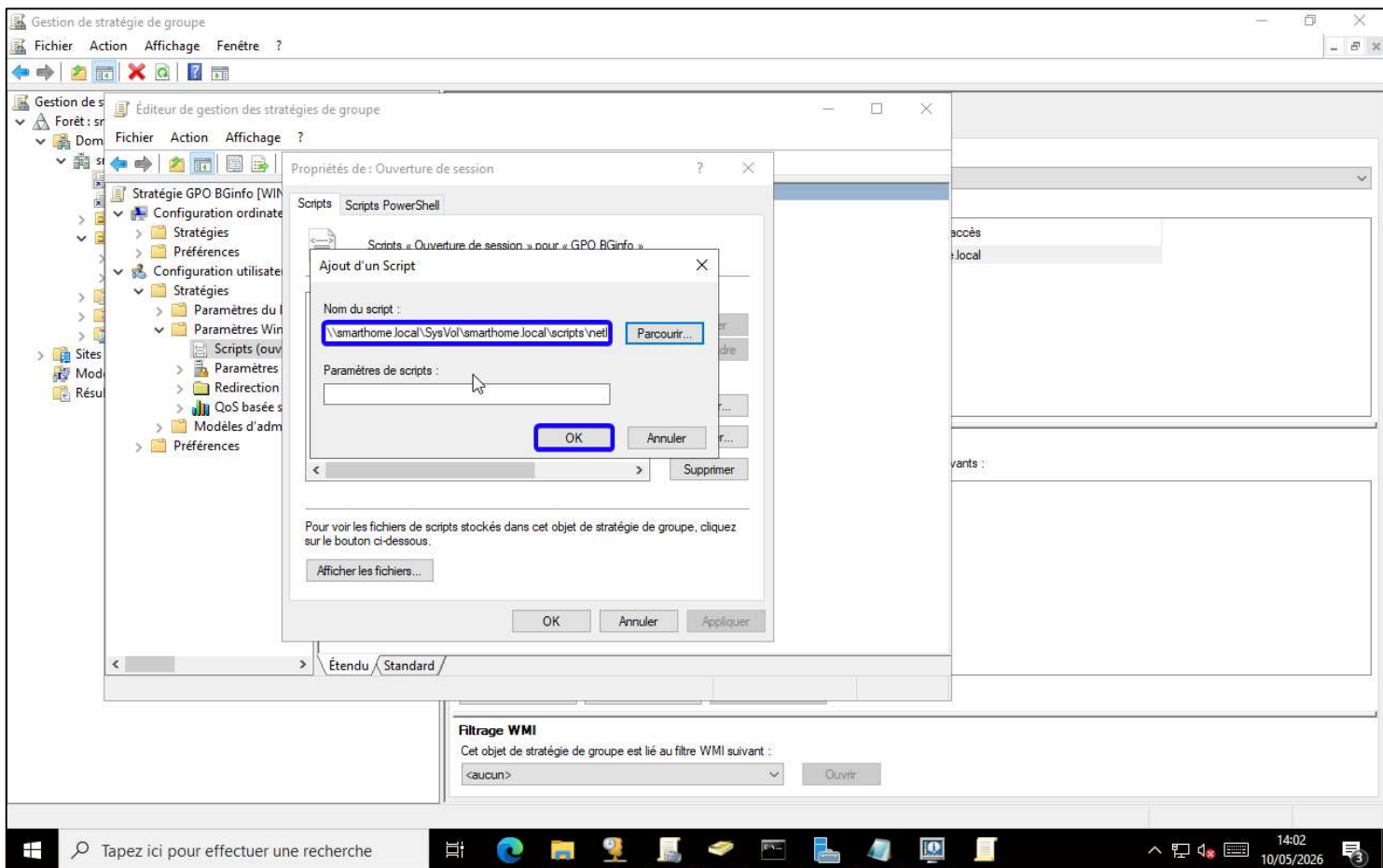
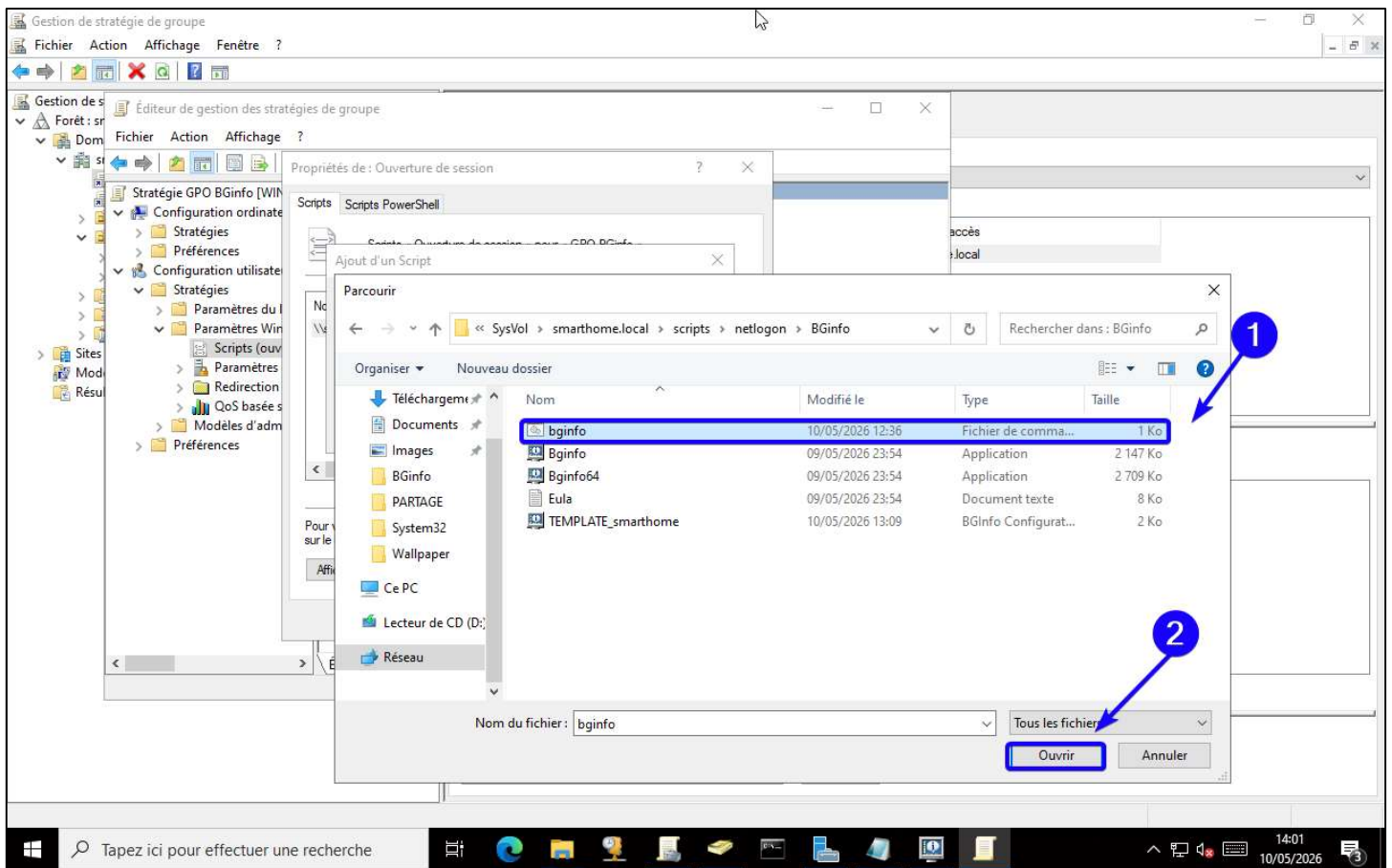


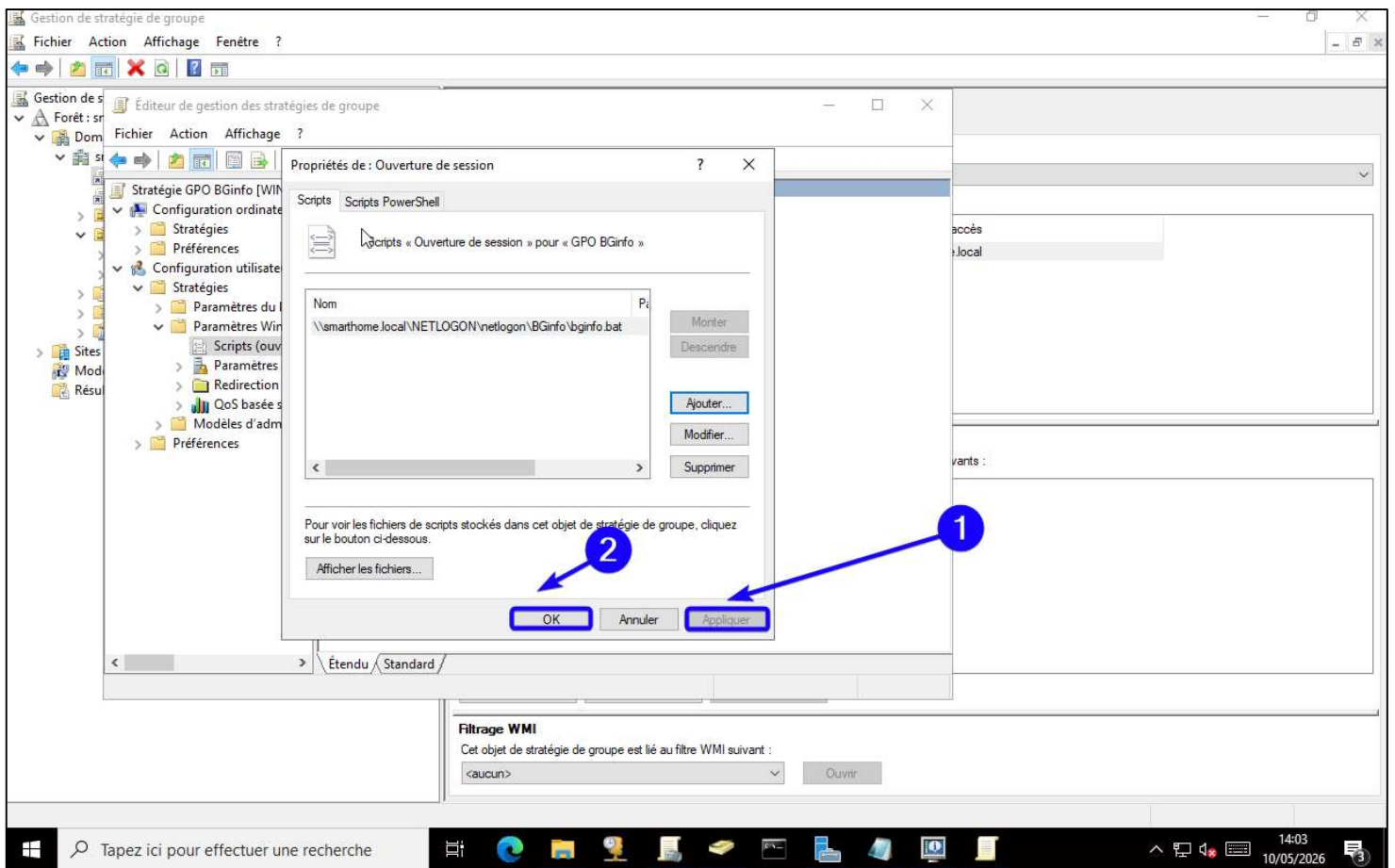
Créer la **GPO BGInfo** :





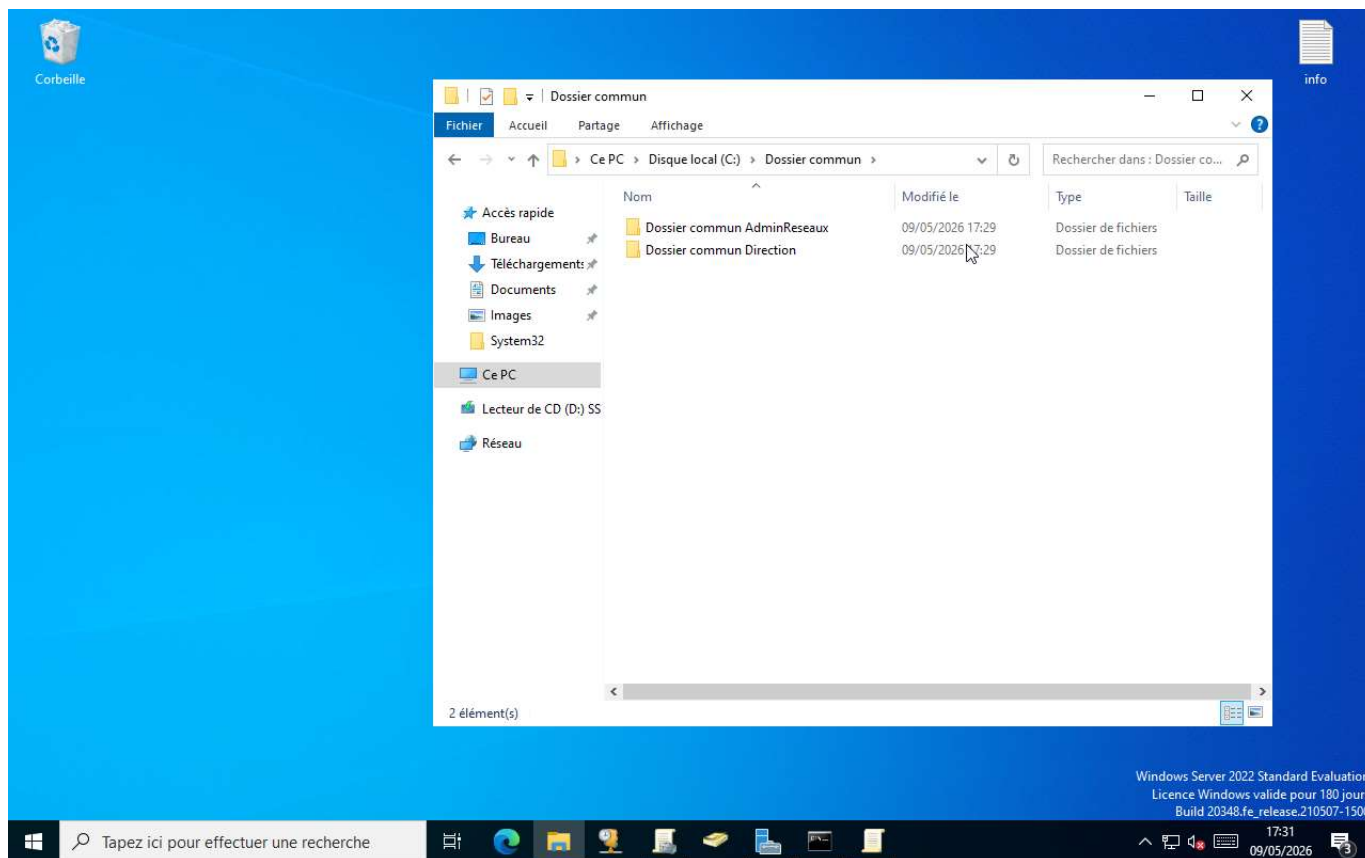






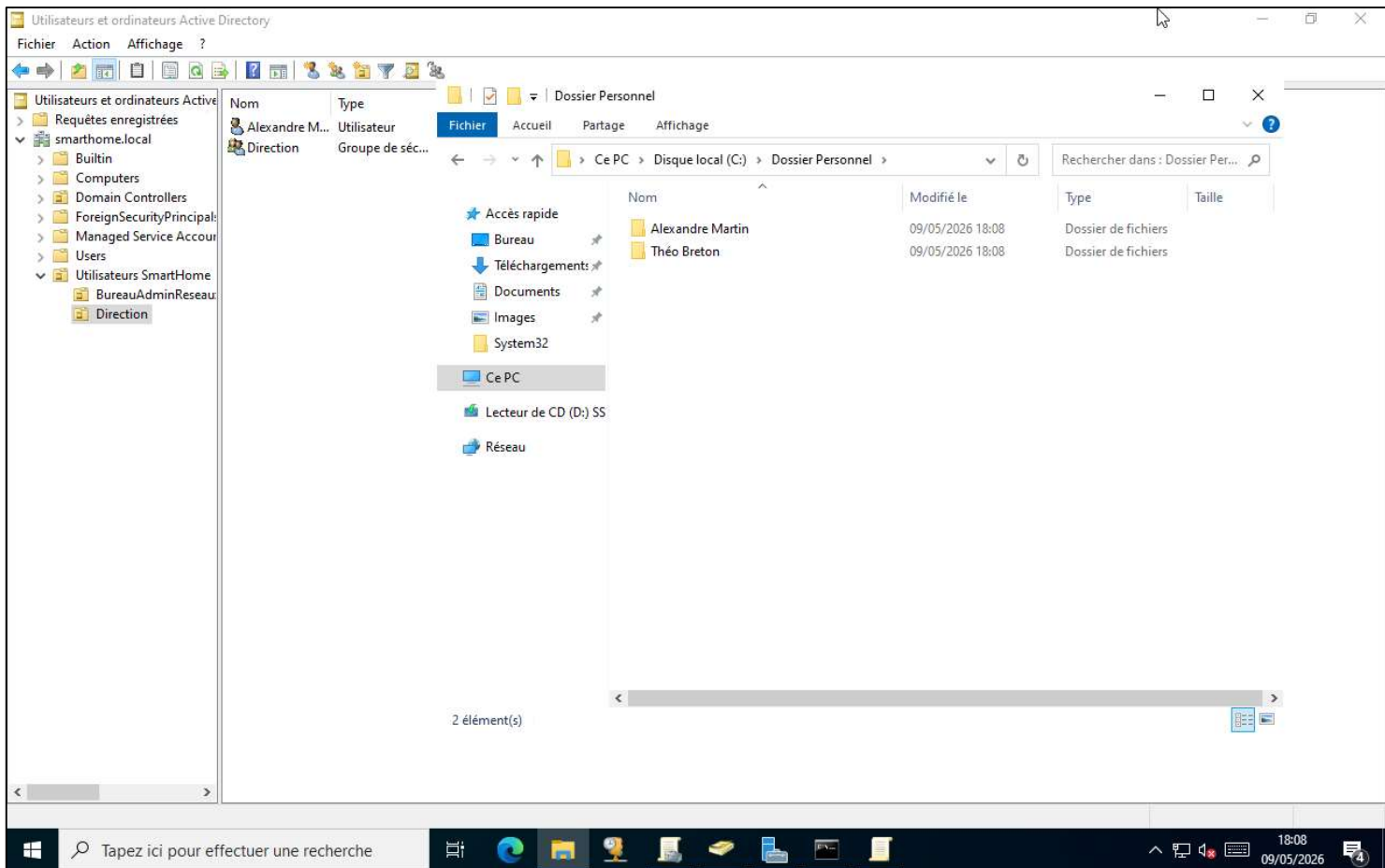
② Dossier Personnels et Dossiers Communs :

Création des dossiers parents pour les dossiers personnel et commun.

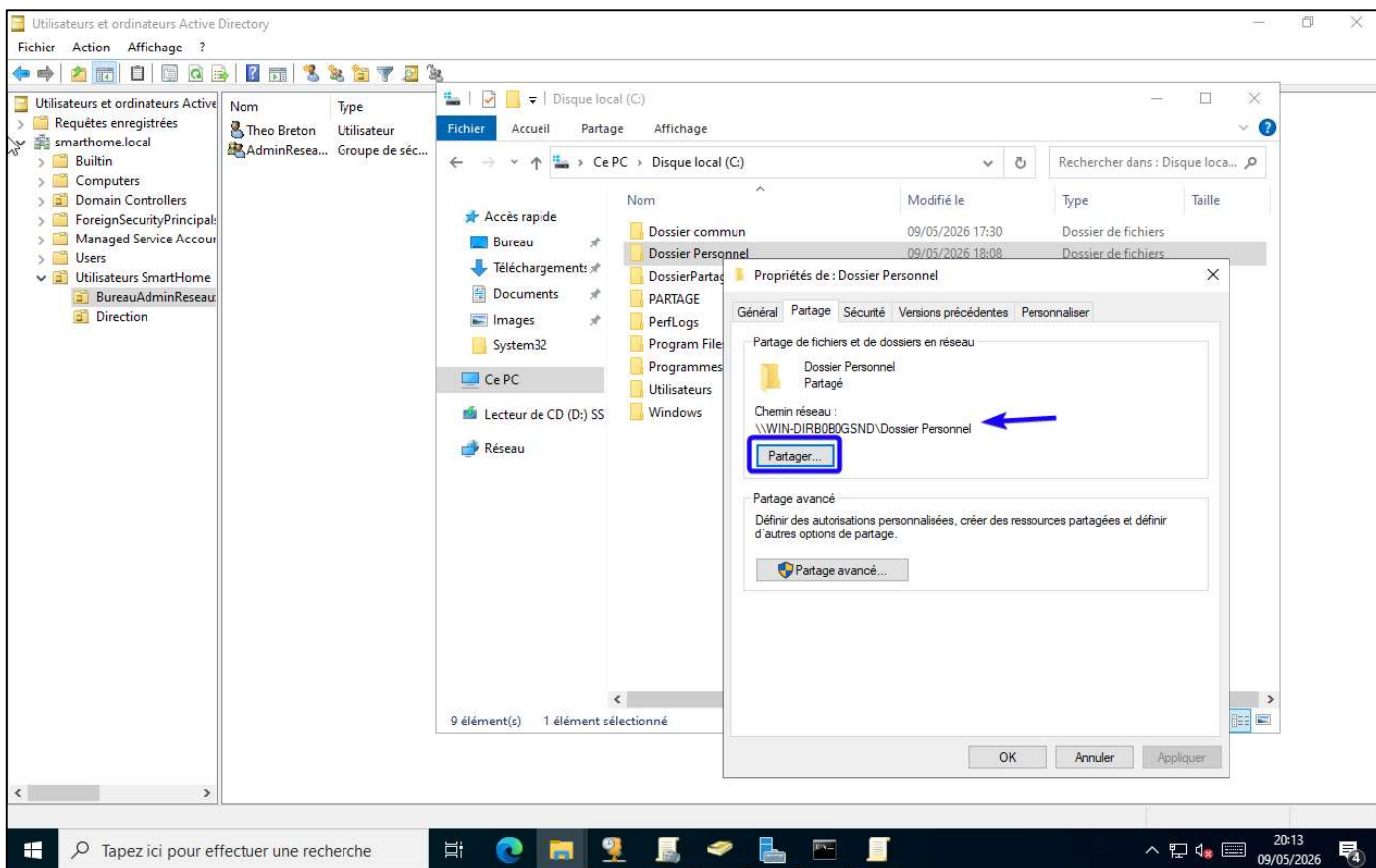


On va créer des groupes dans nos UO.

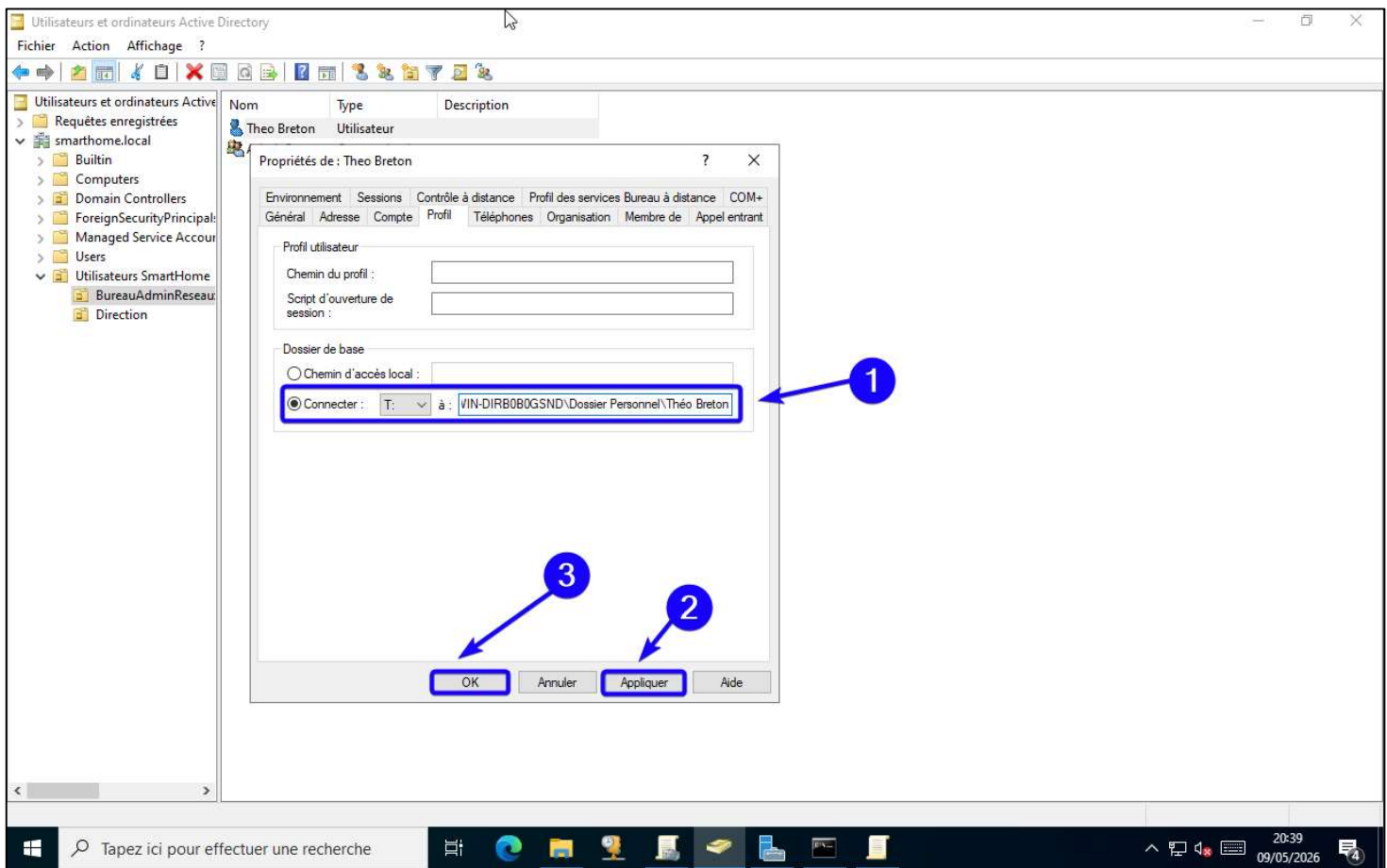
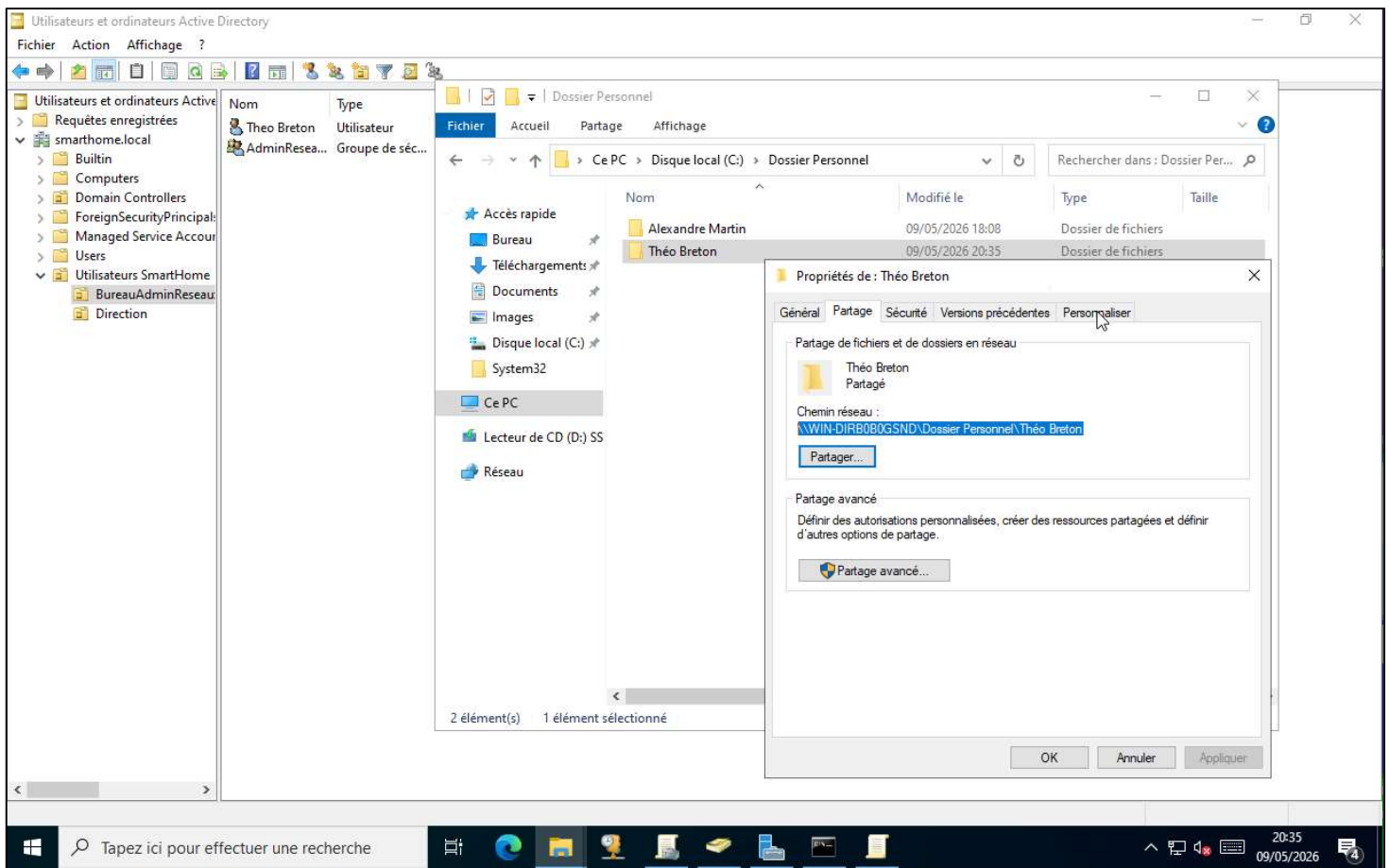
Création des dossiers personnels :

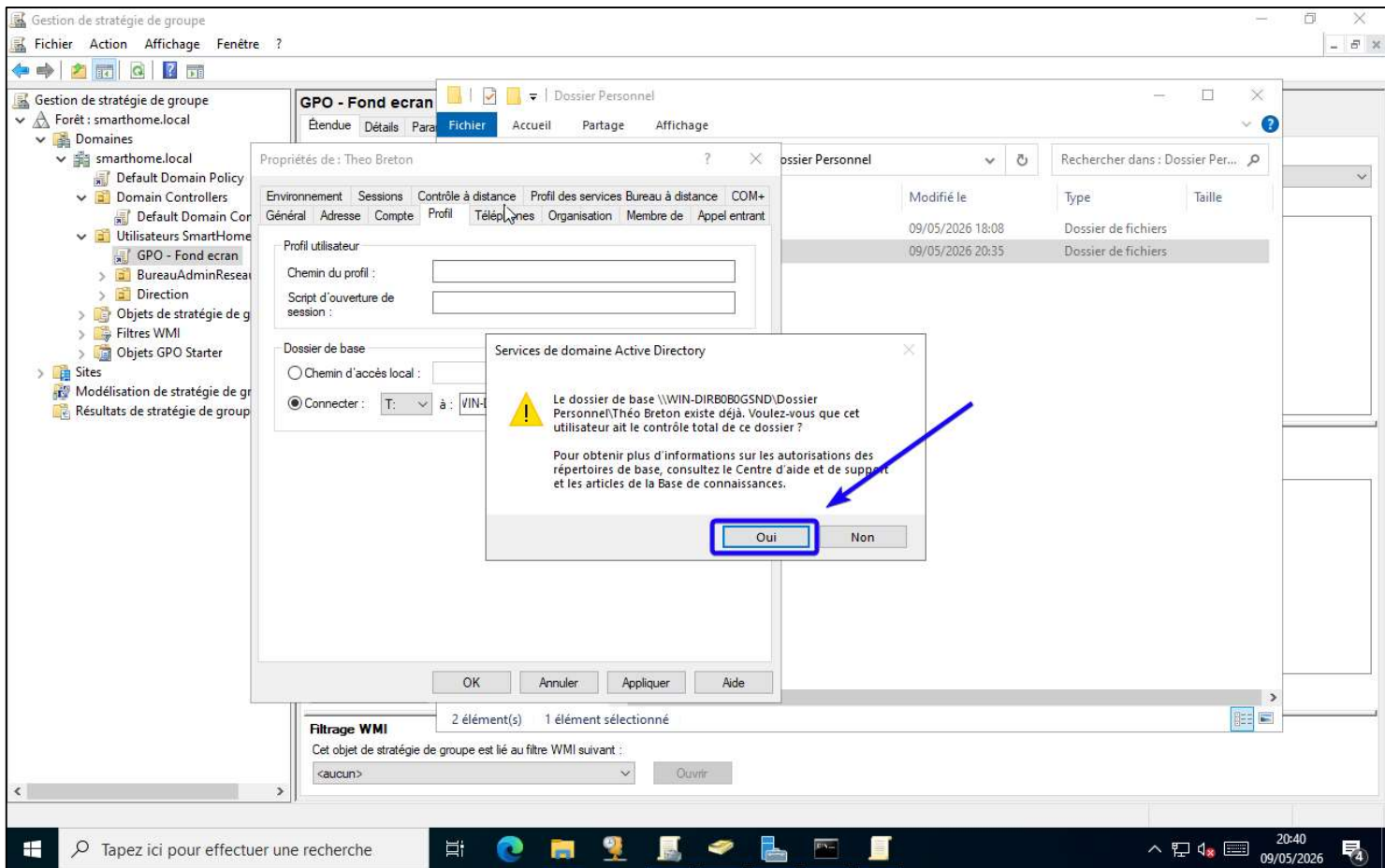


Partager le dossier parent « **Dossier Personnel** »

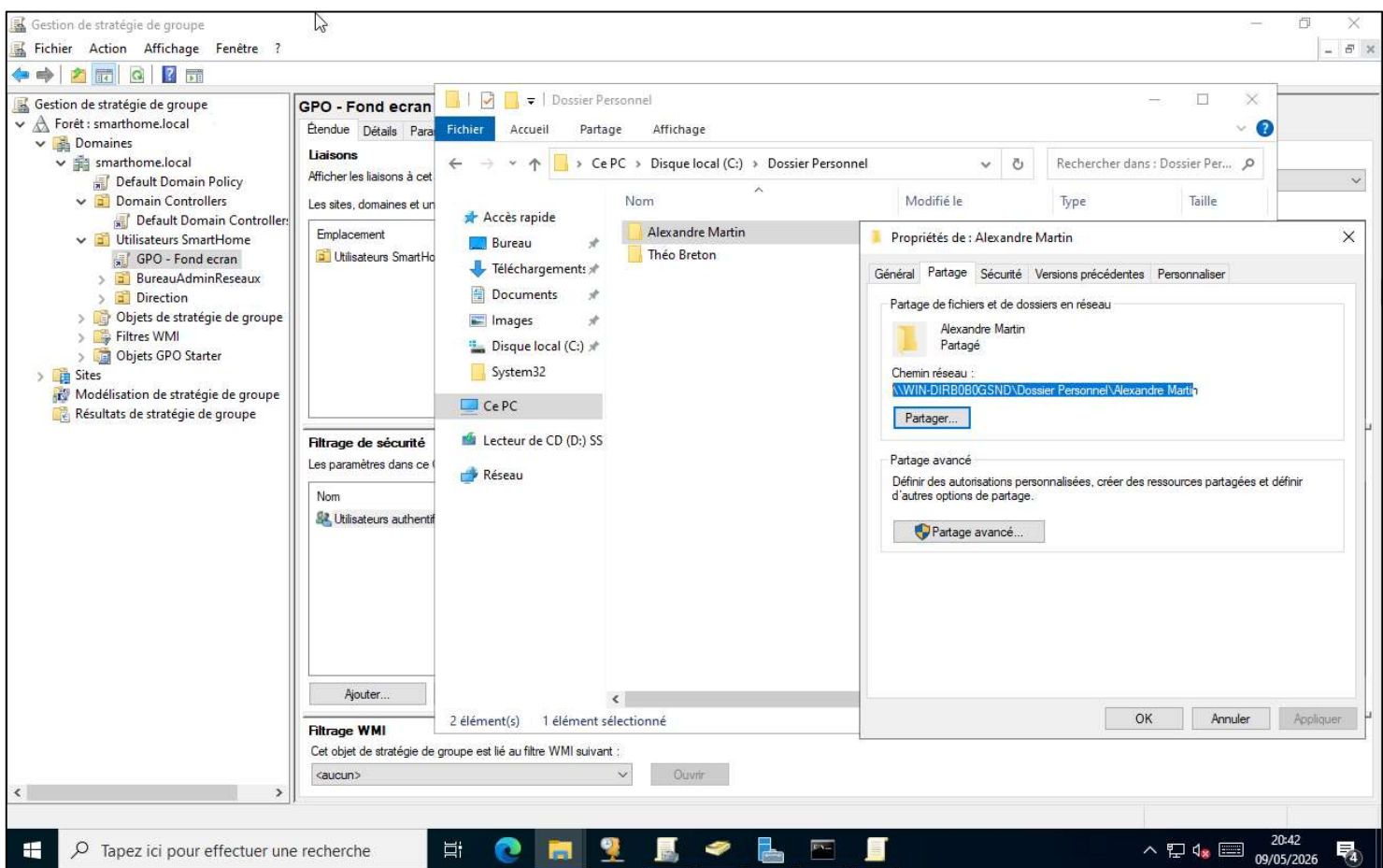


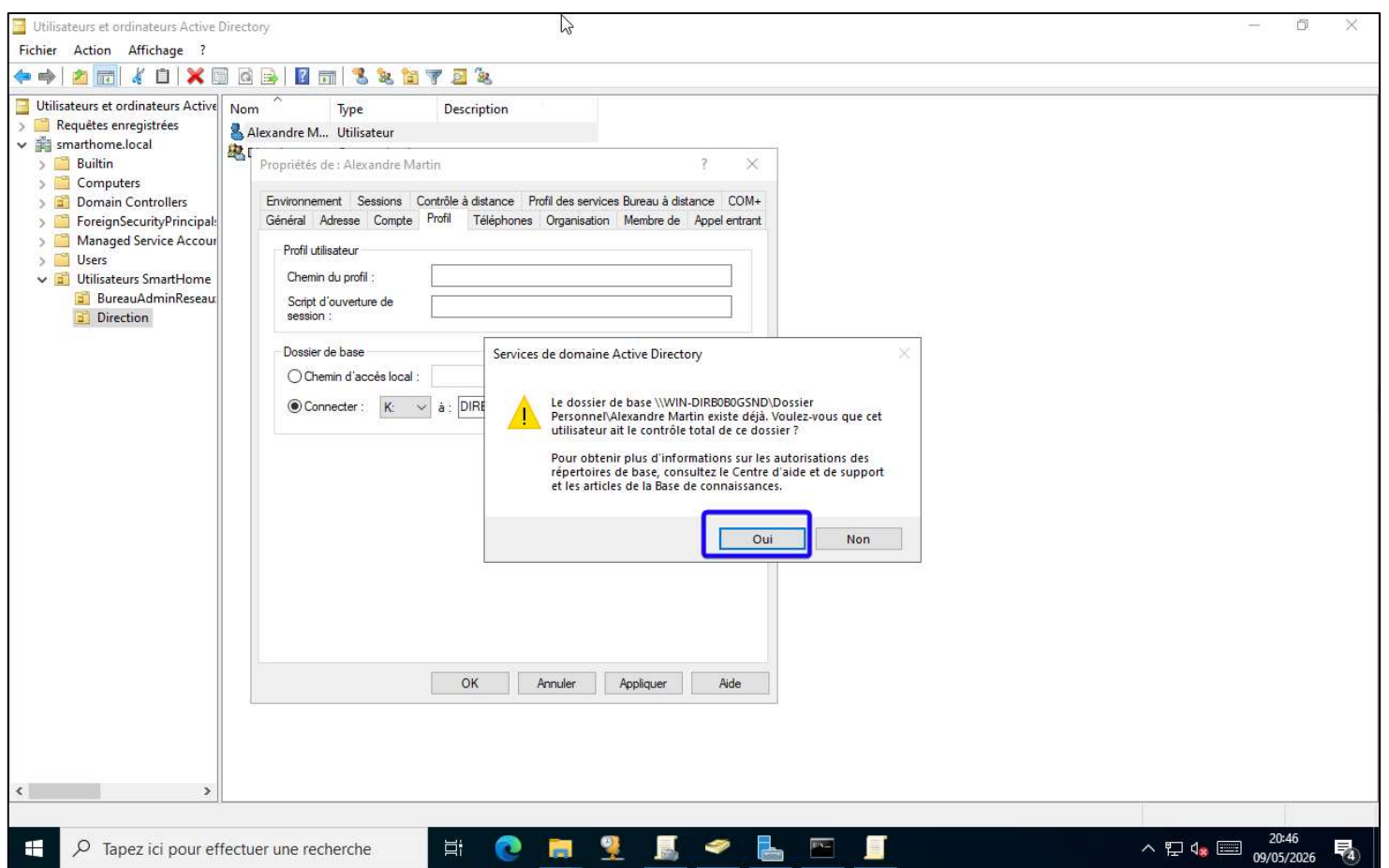
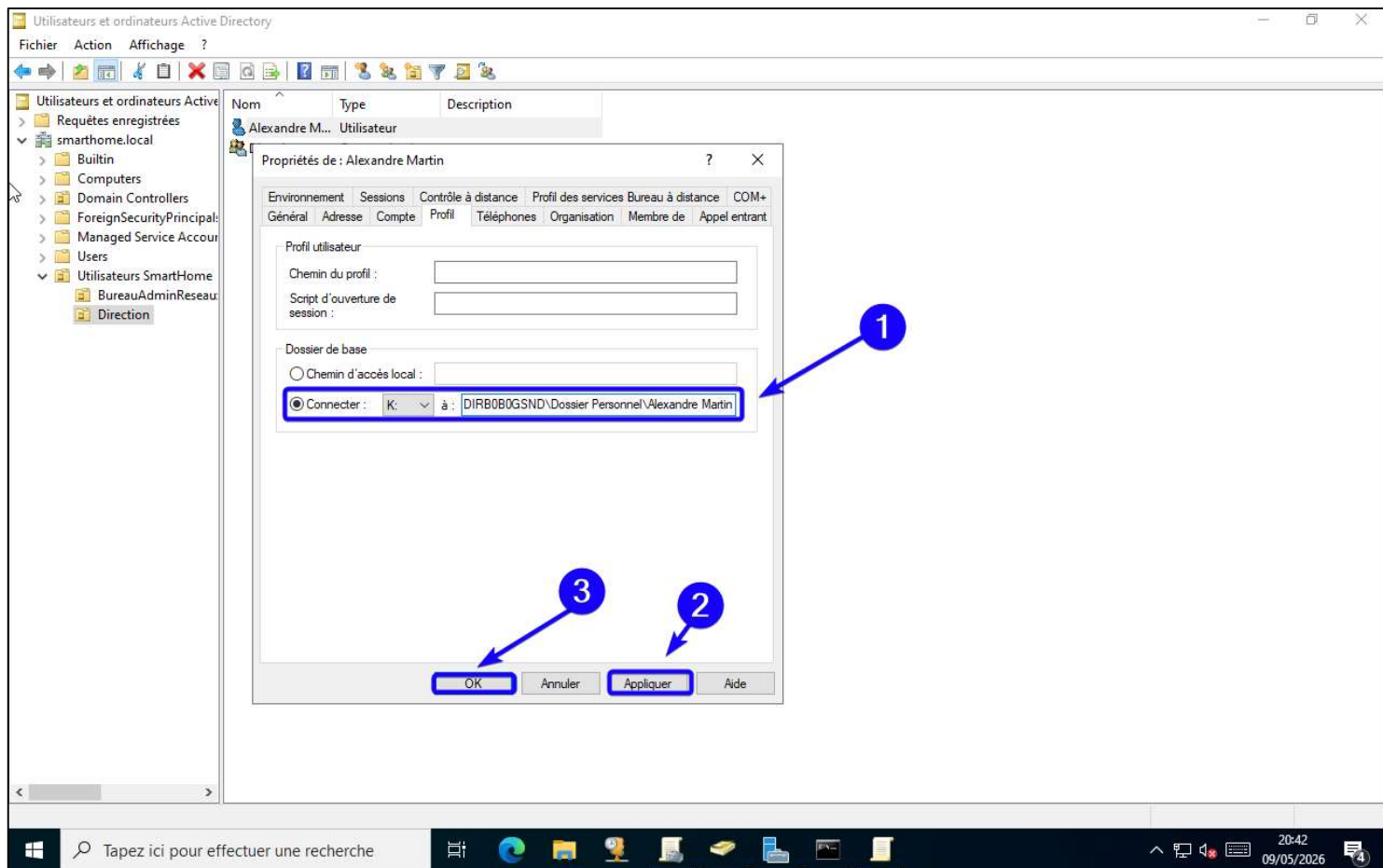
Copier le chemin réseau du dossier perso et l'affecter à l'utilisateur concerné :



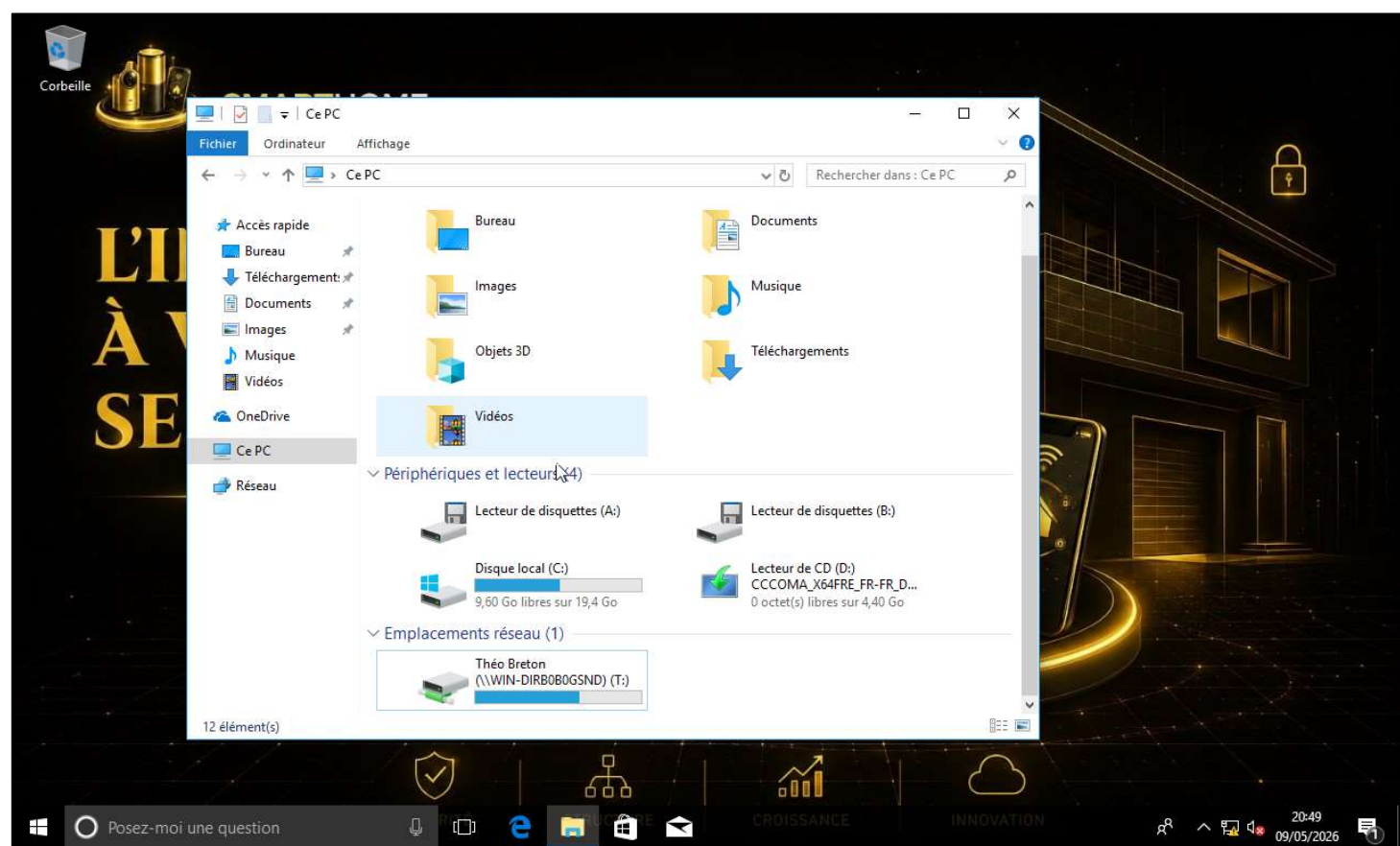
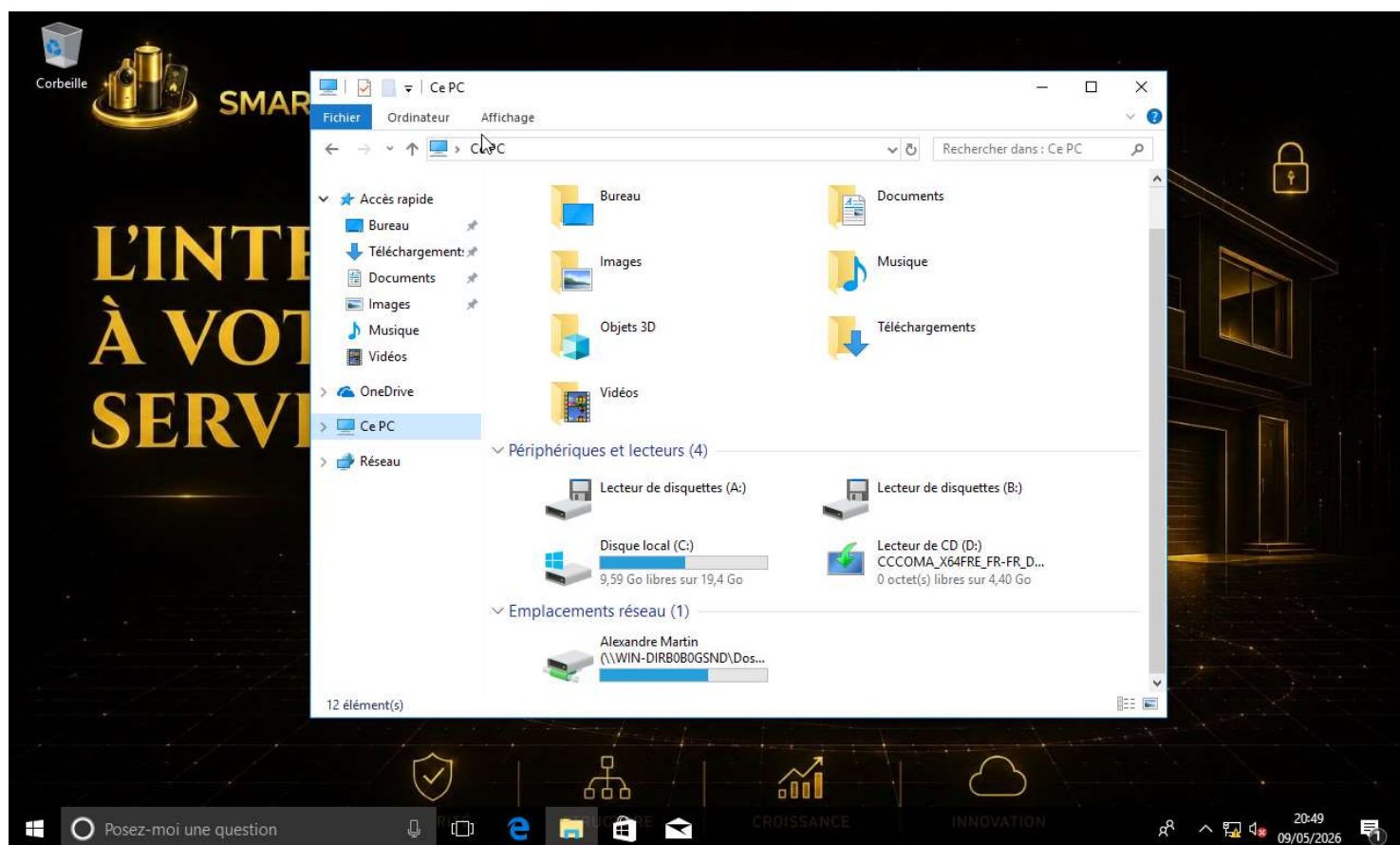


Pour l'utilisateur Alexandre Martin :

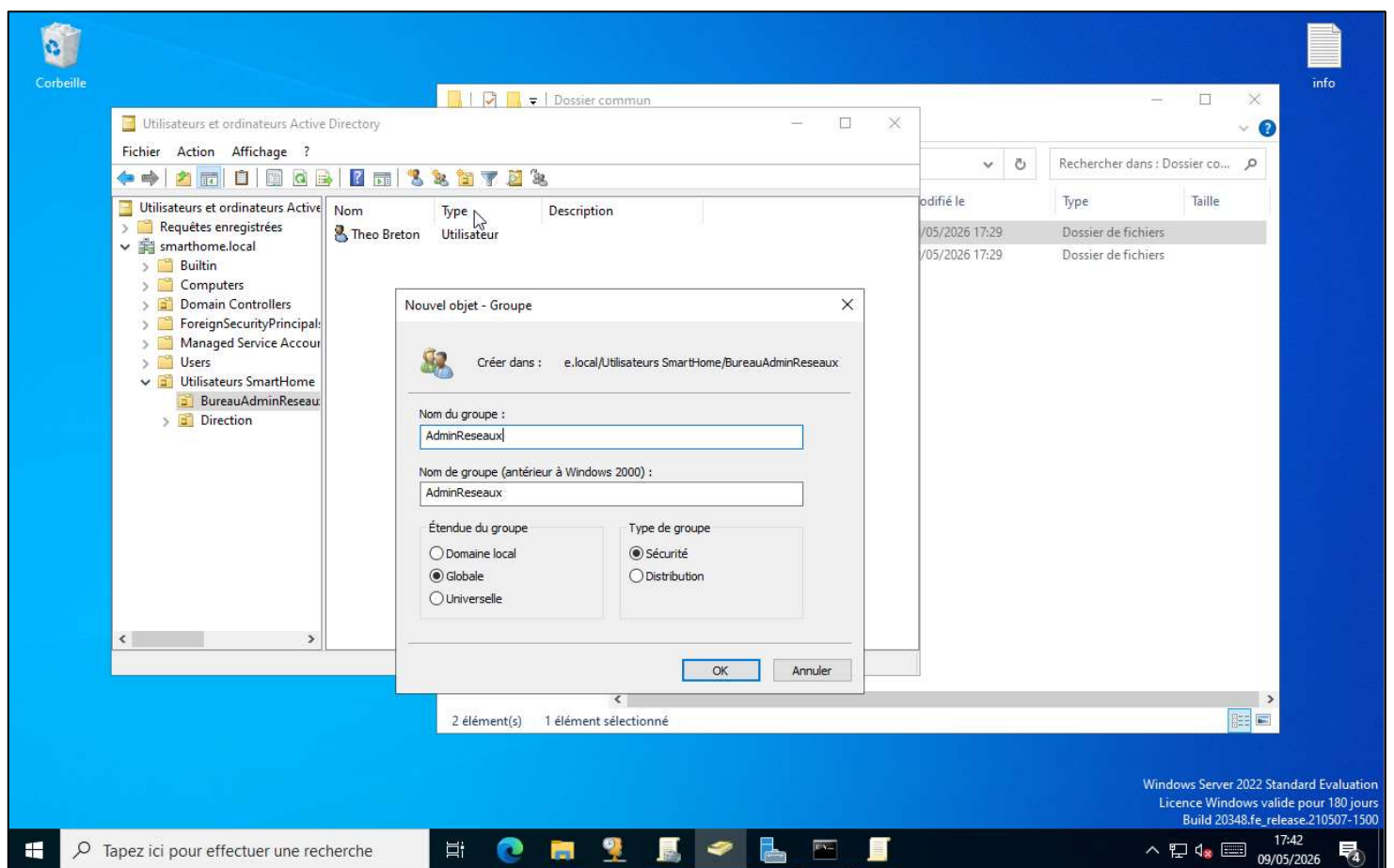
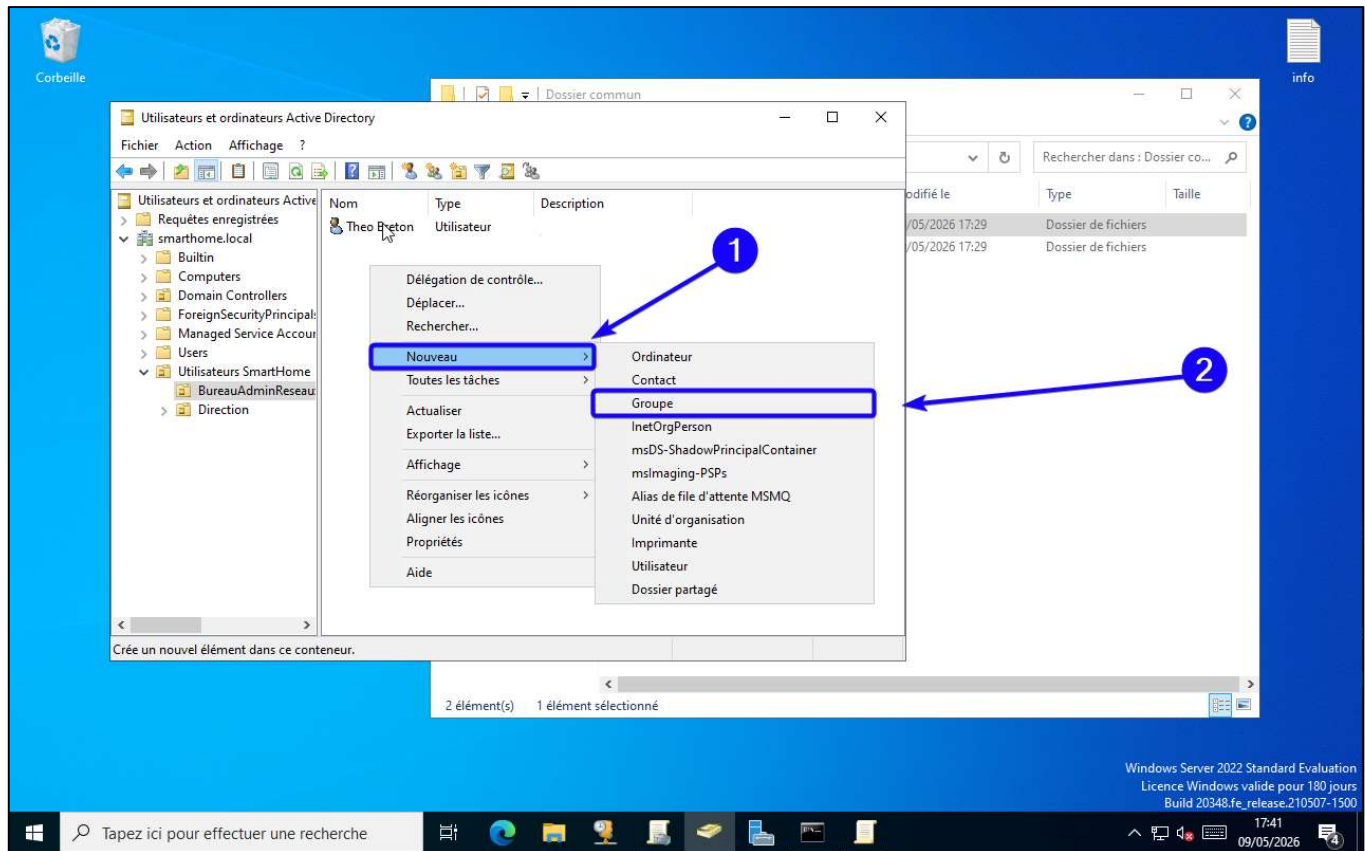




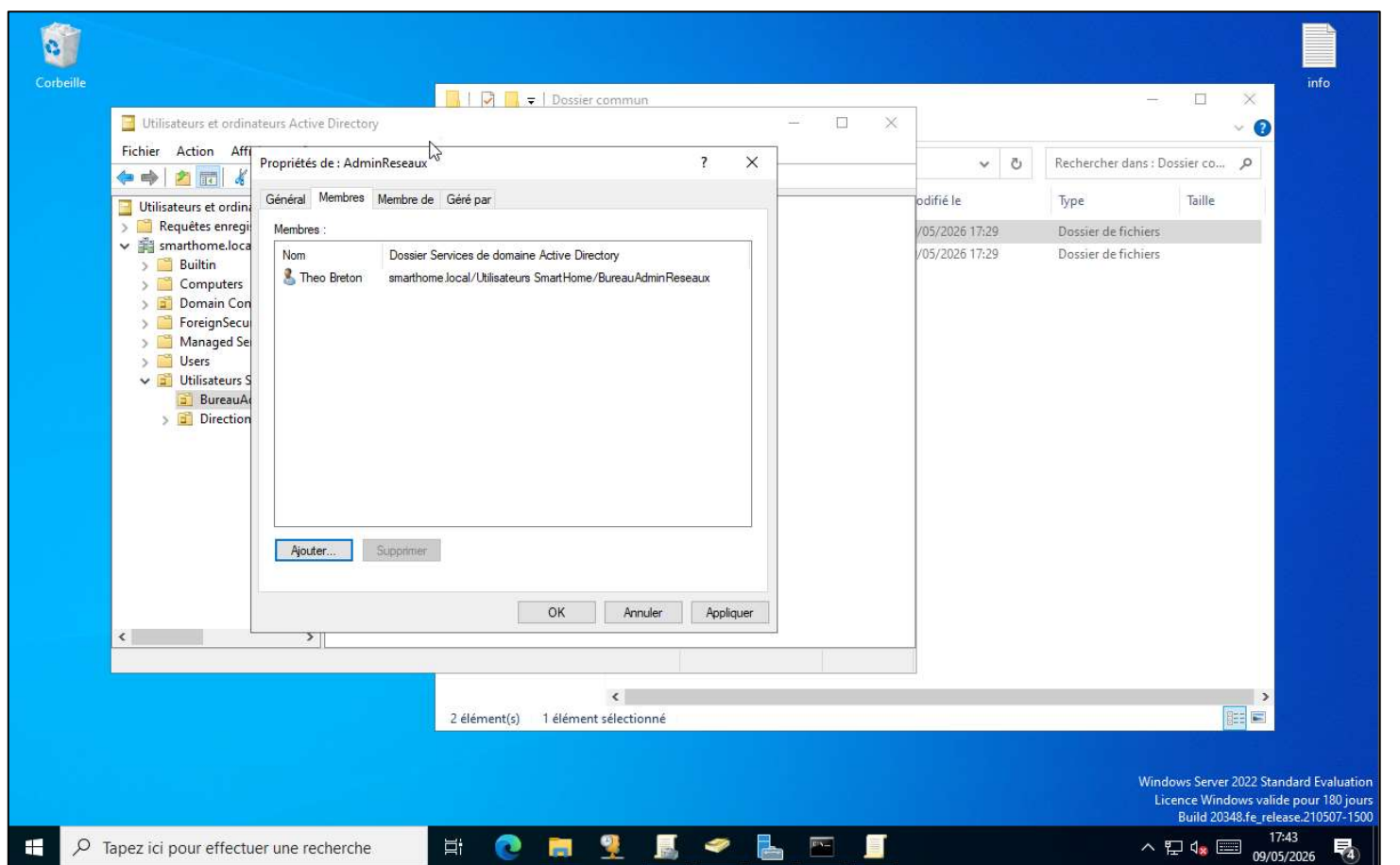
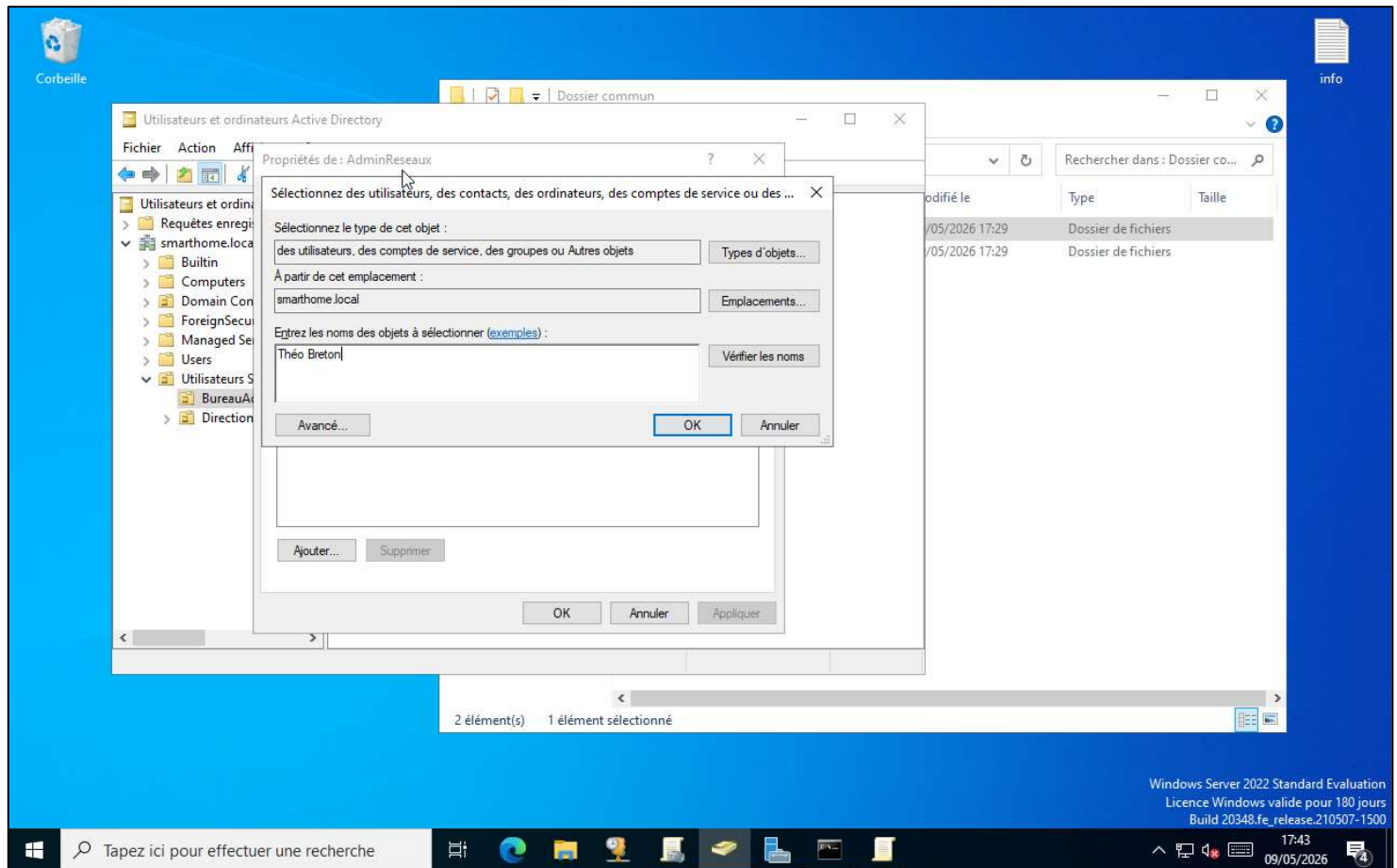
Mes **deux utilisateurs** ont maintenant leurs **dossiers personnels** :

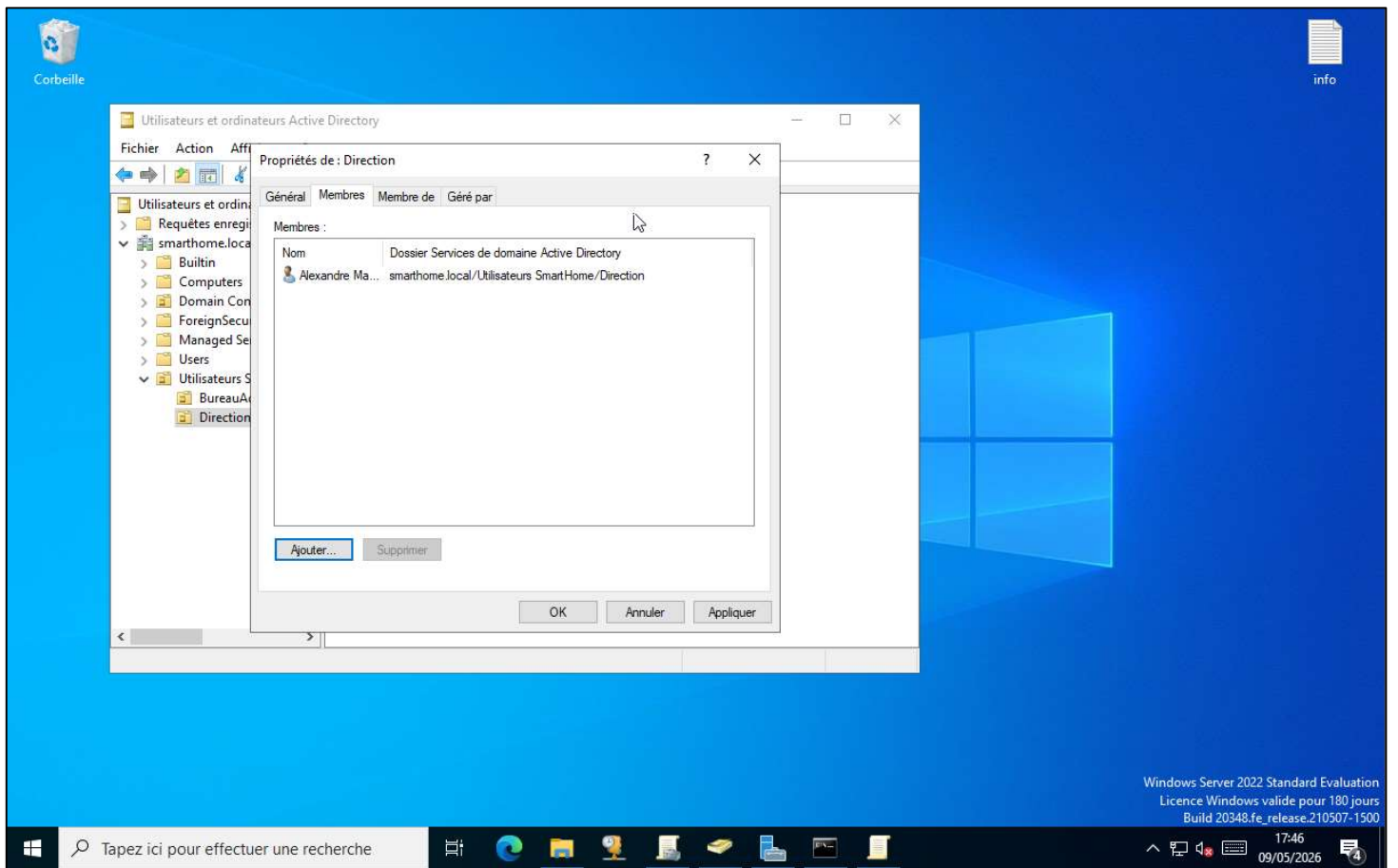
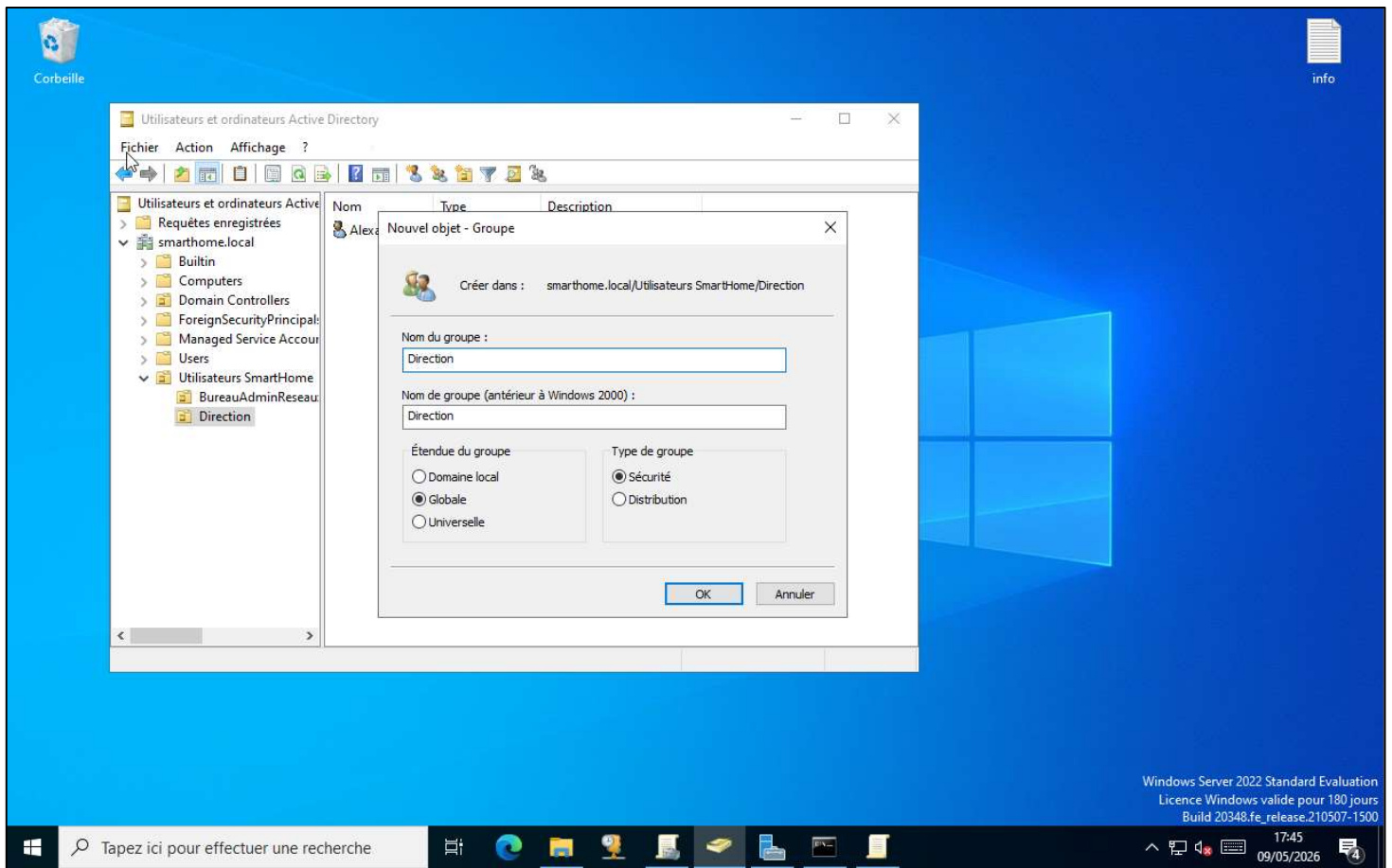


Mappage des lecteurs pour les dossiers communs pour les deux services :

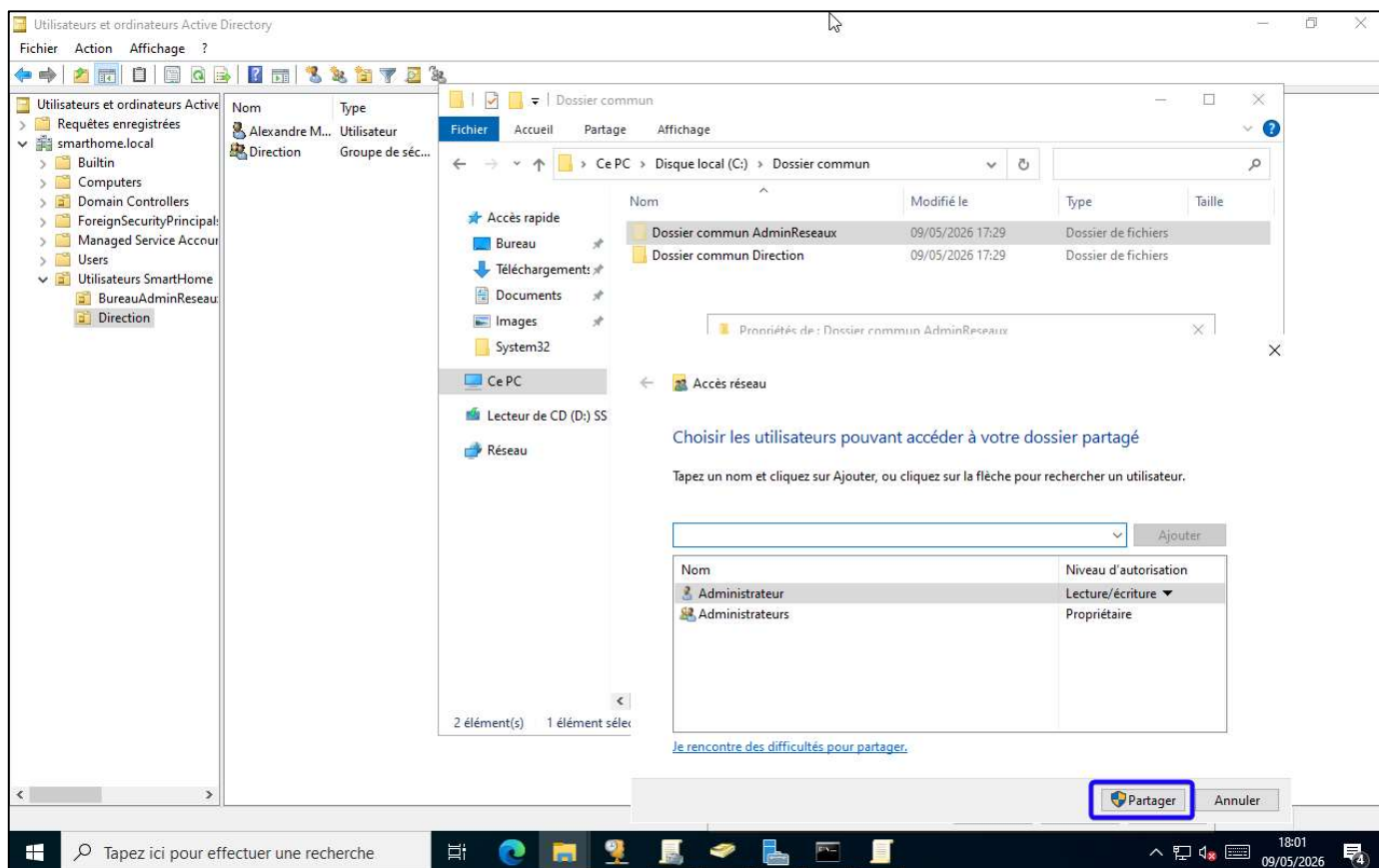
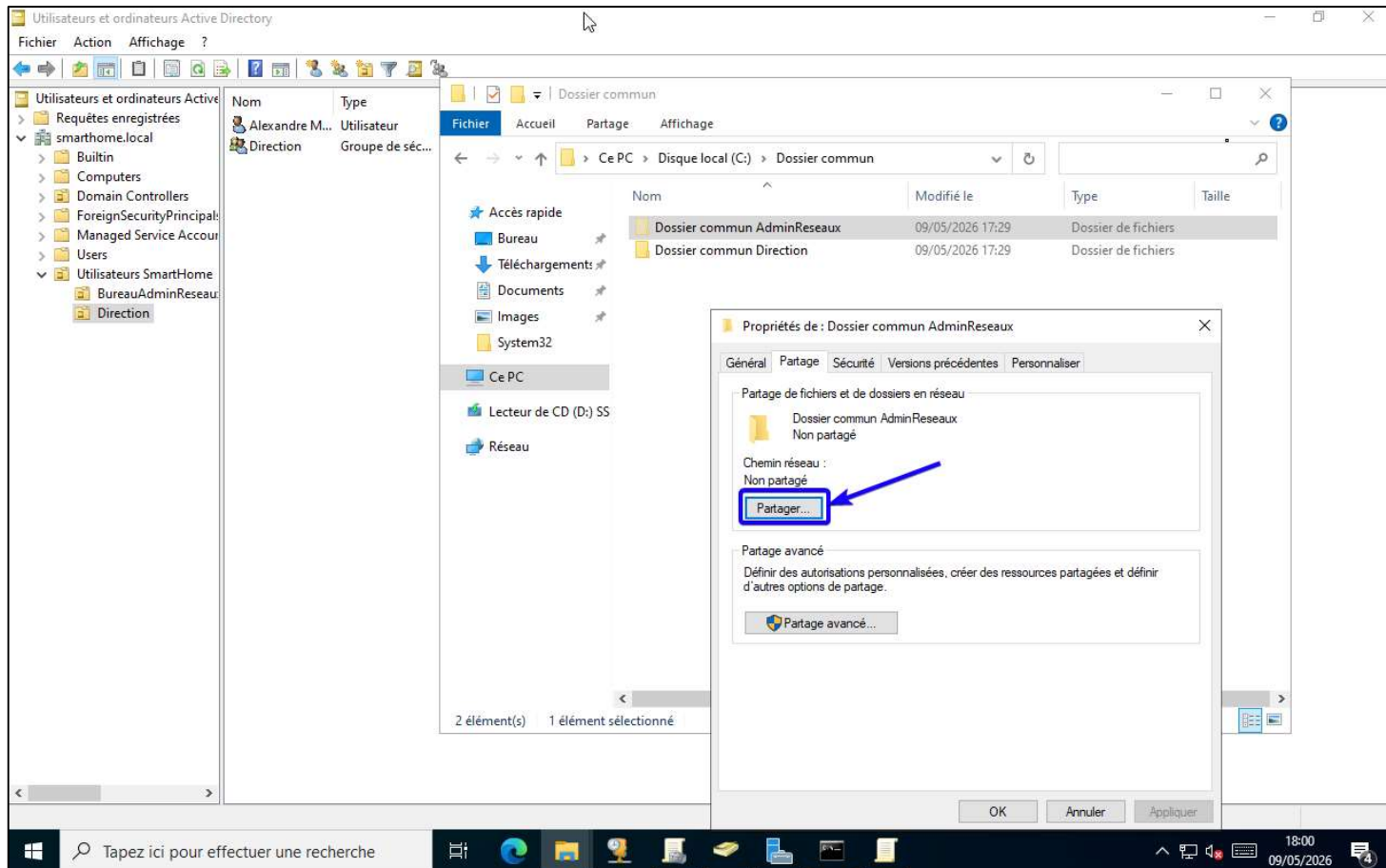


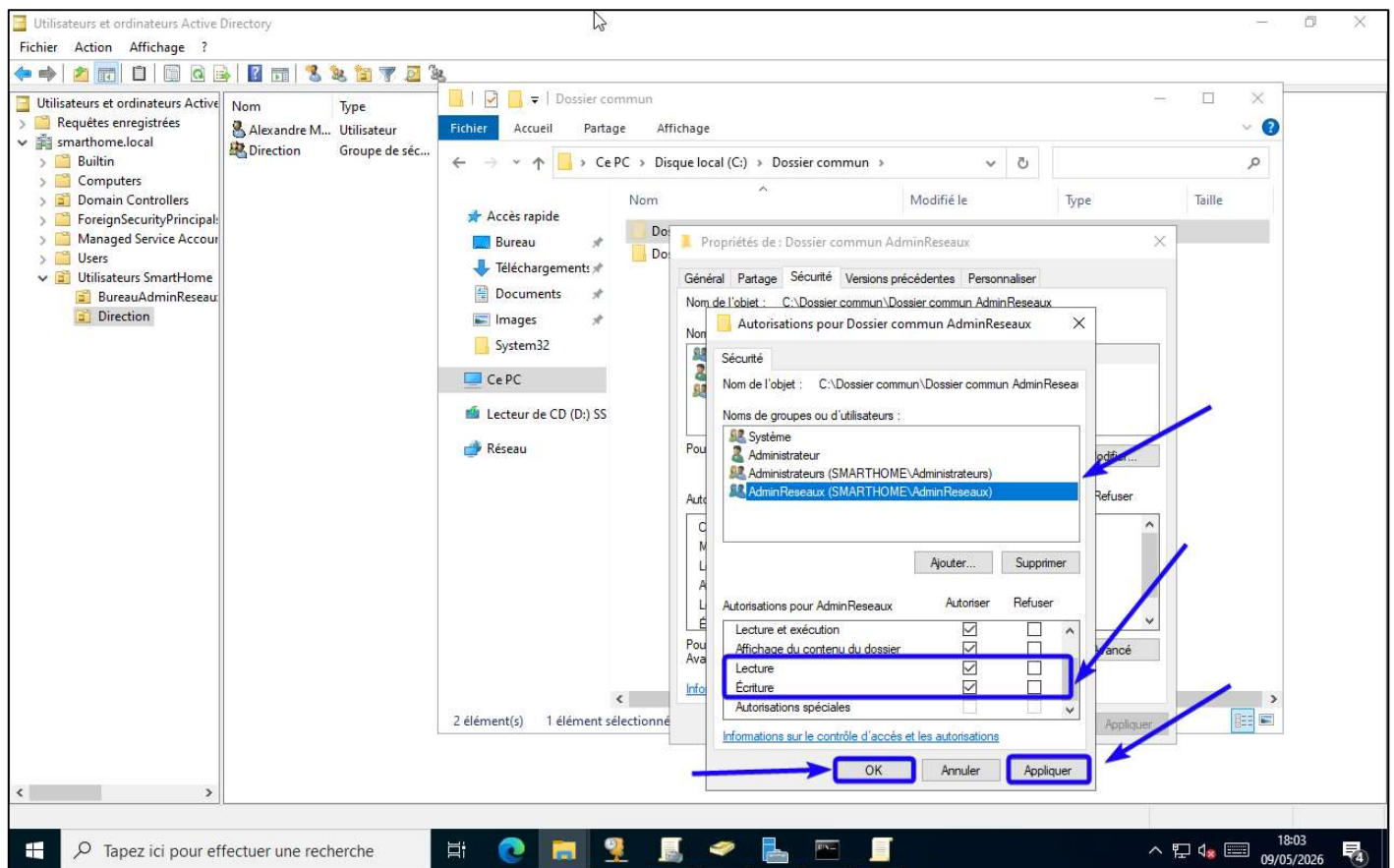
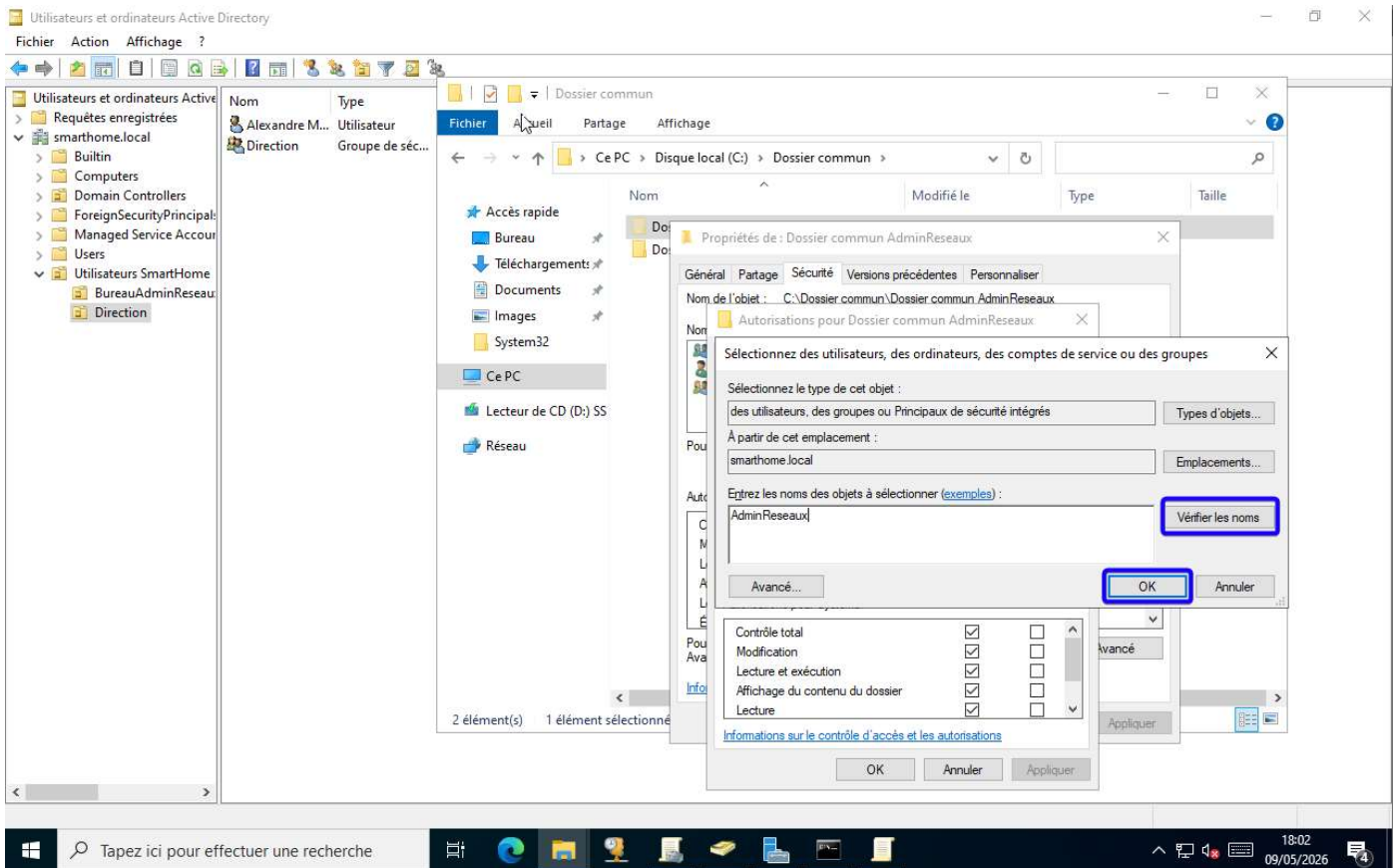
Ajouté l'utilisateur au groupe :

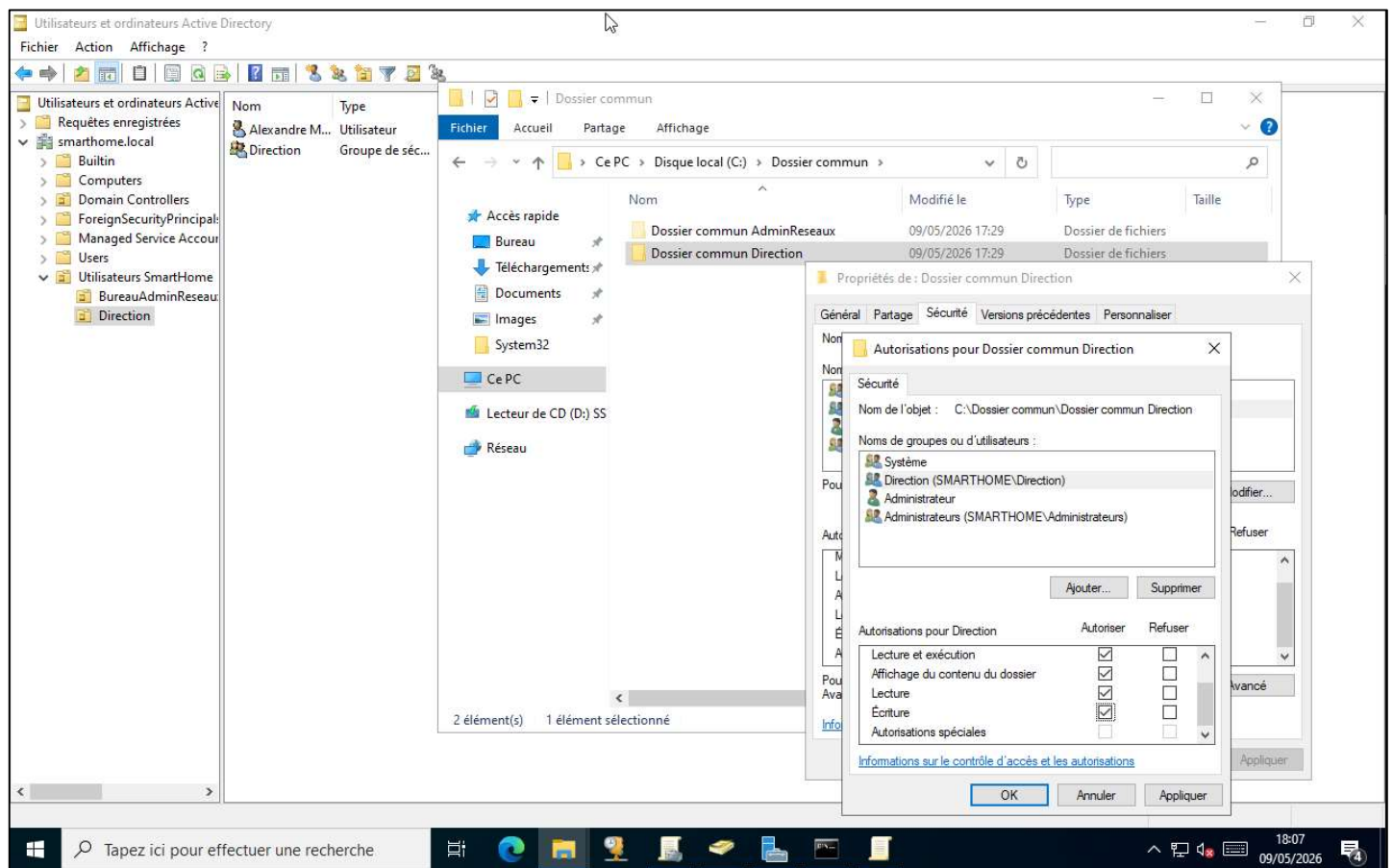




Effectuer le partage des dossier communs :







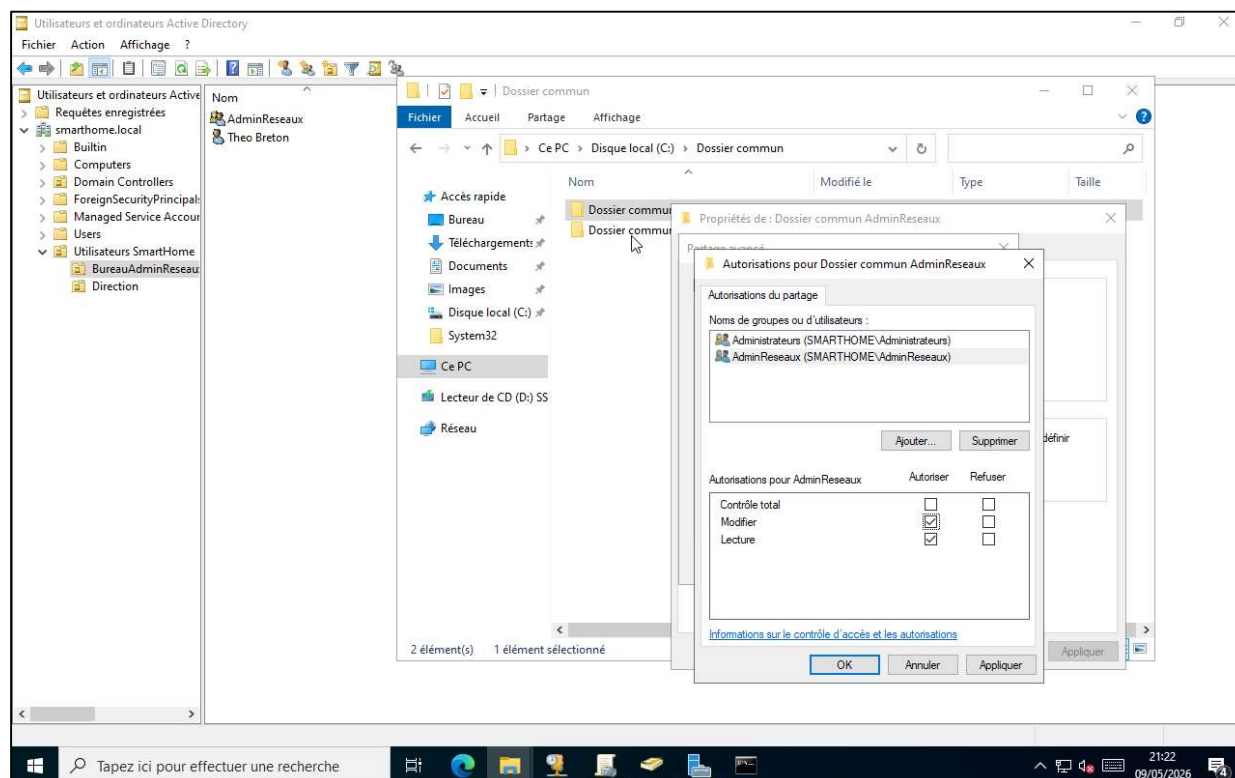
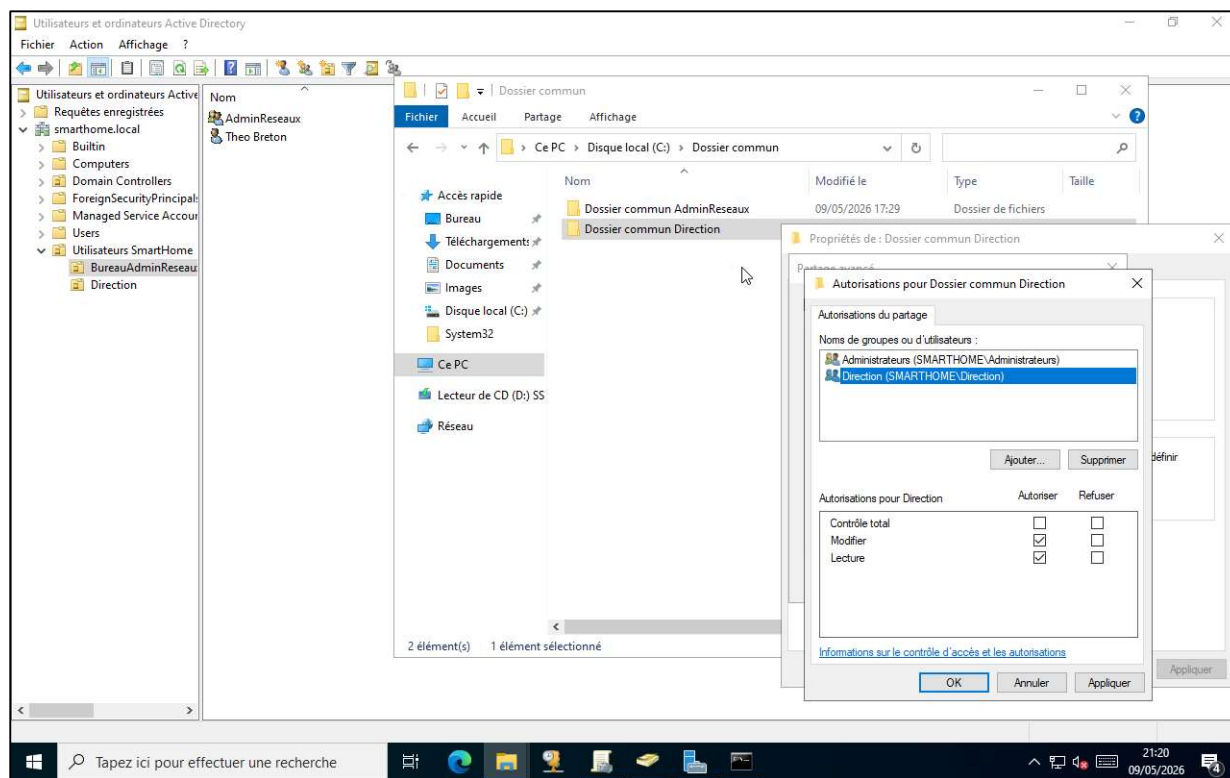
Les droits NTFS sur Partage Avancée :

Supprimer le groupe « Tout le monde »

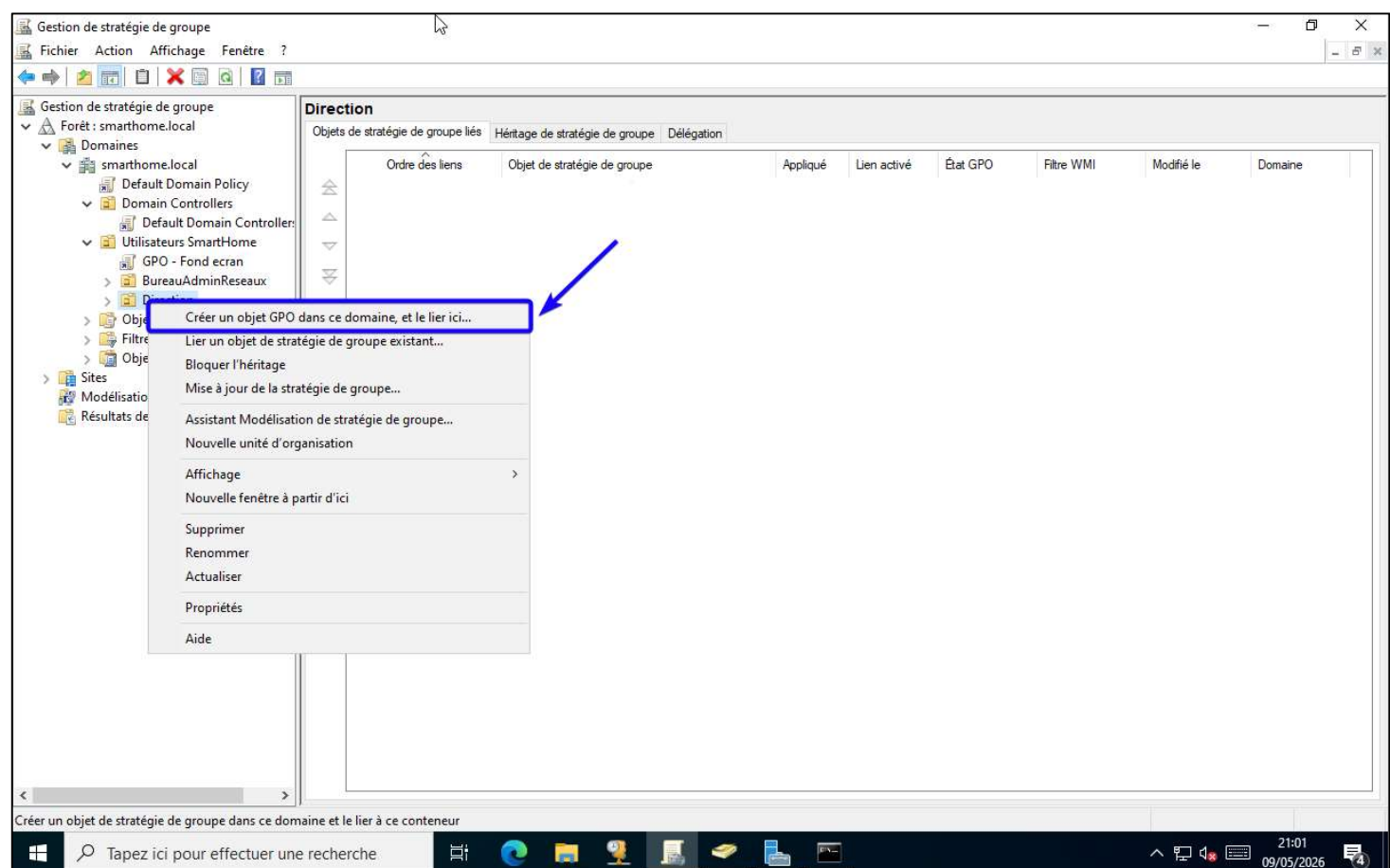
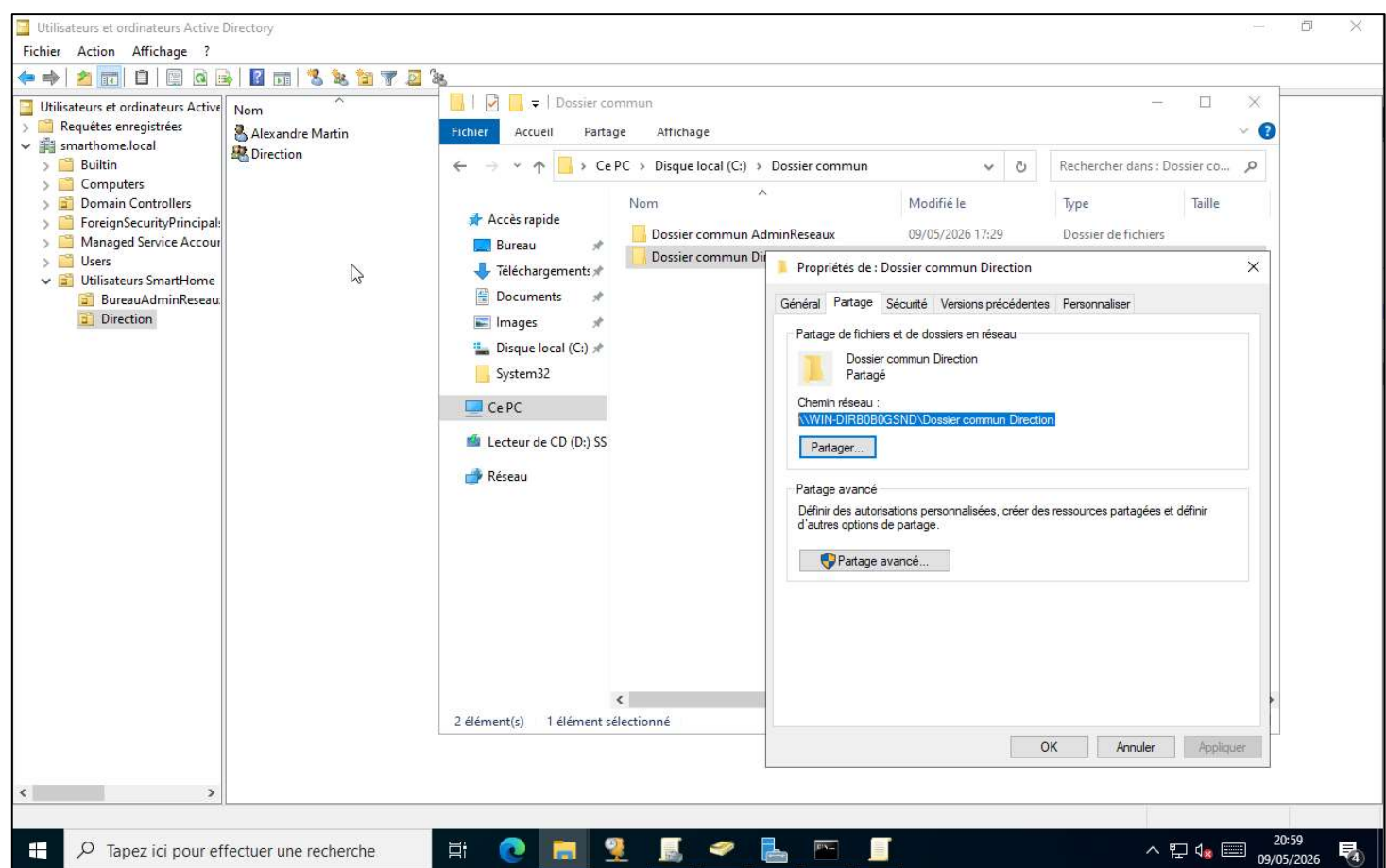
Partage avancé

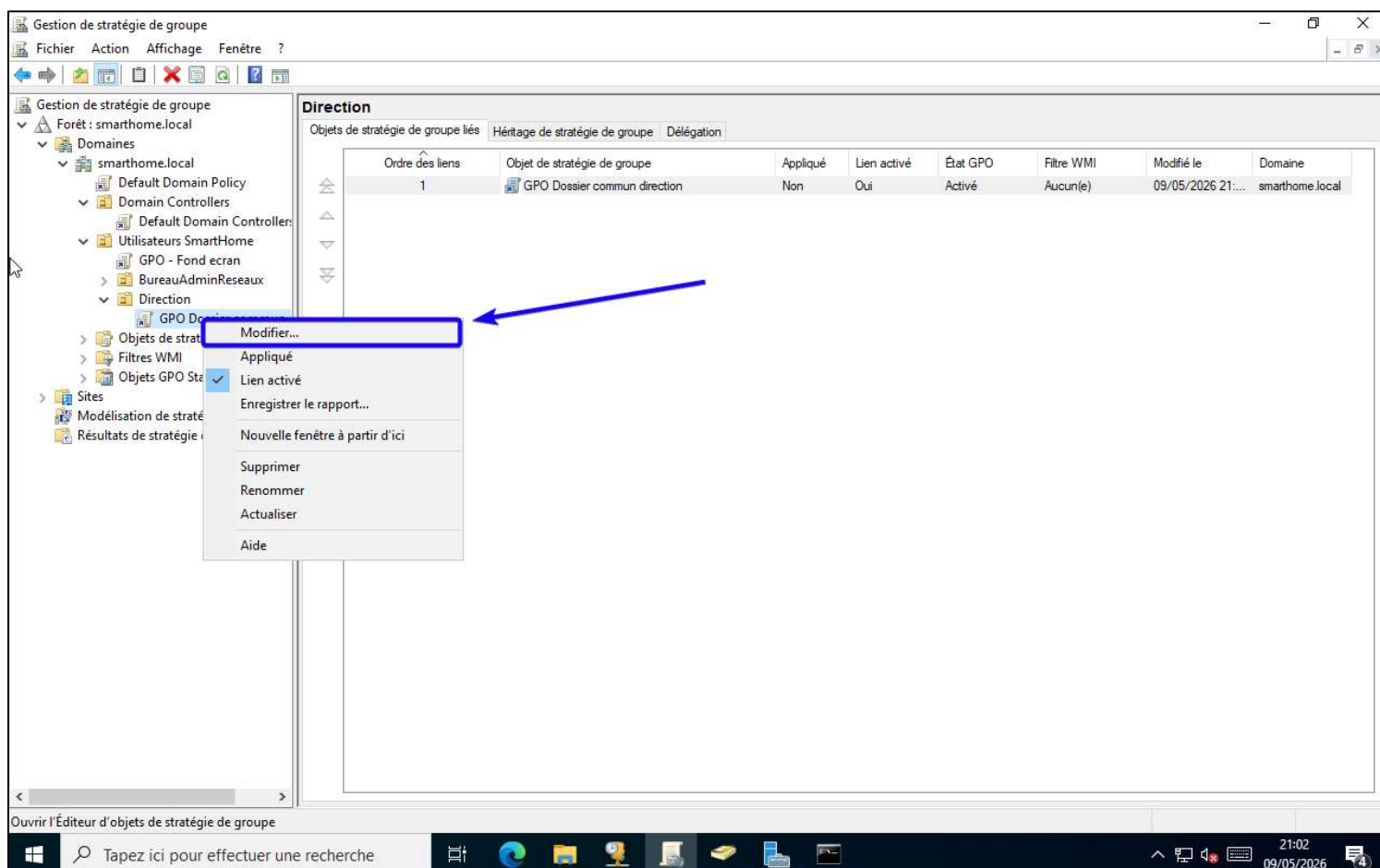
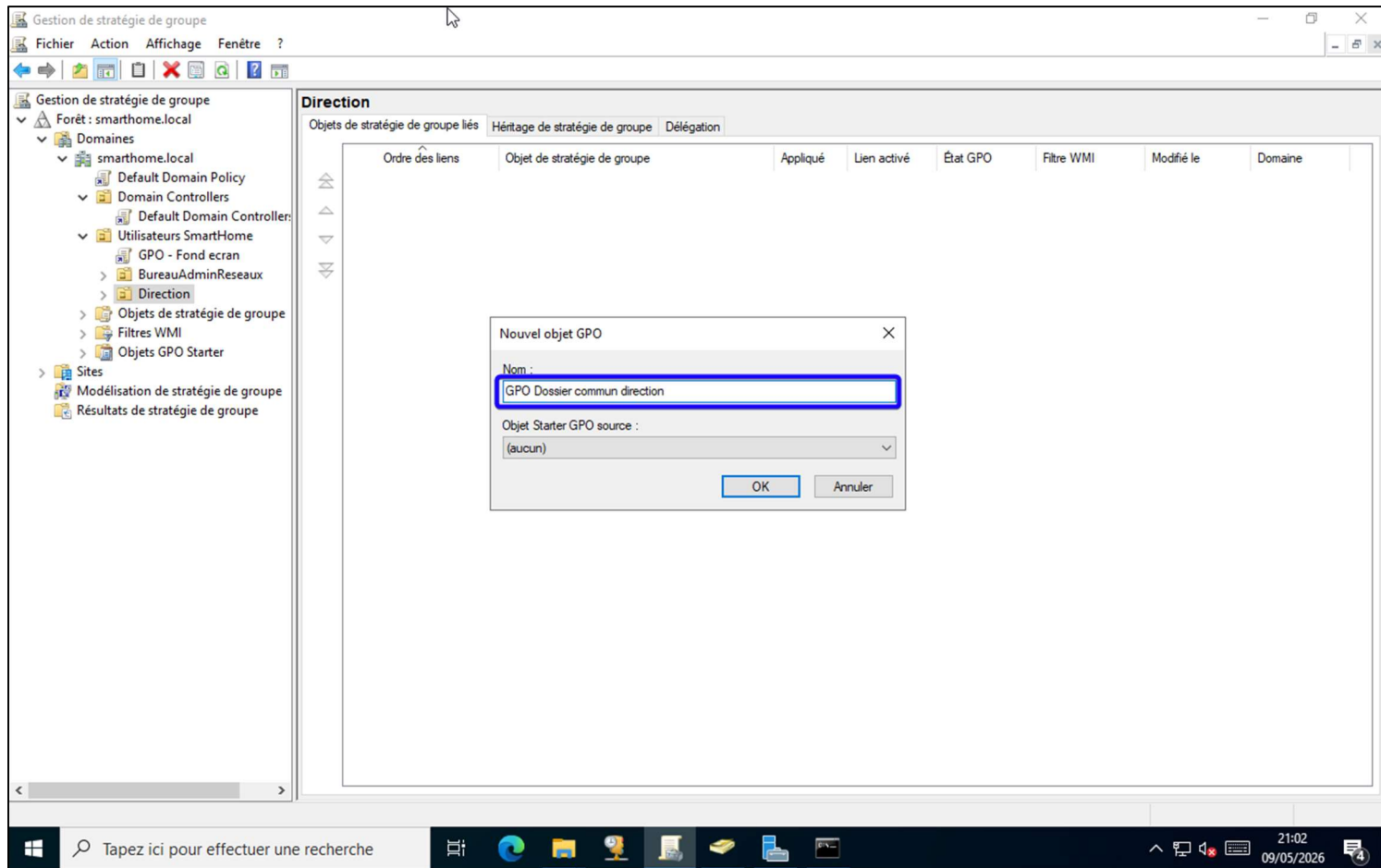
Définir des autorisations personnalisées, créer des ressources partagées et définir d'autres options de partage.

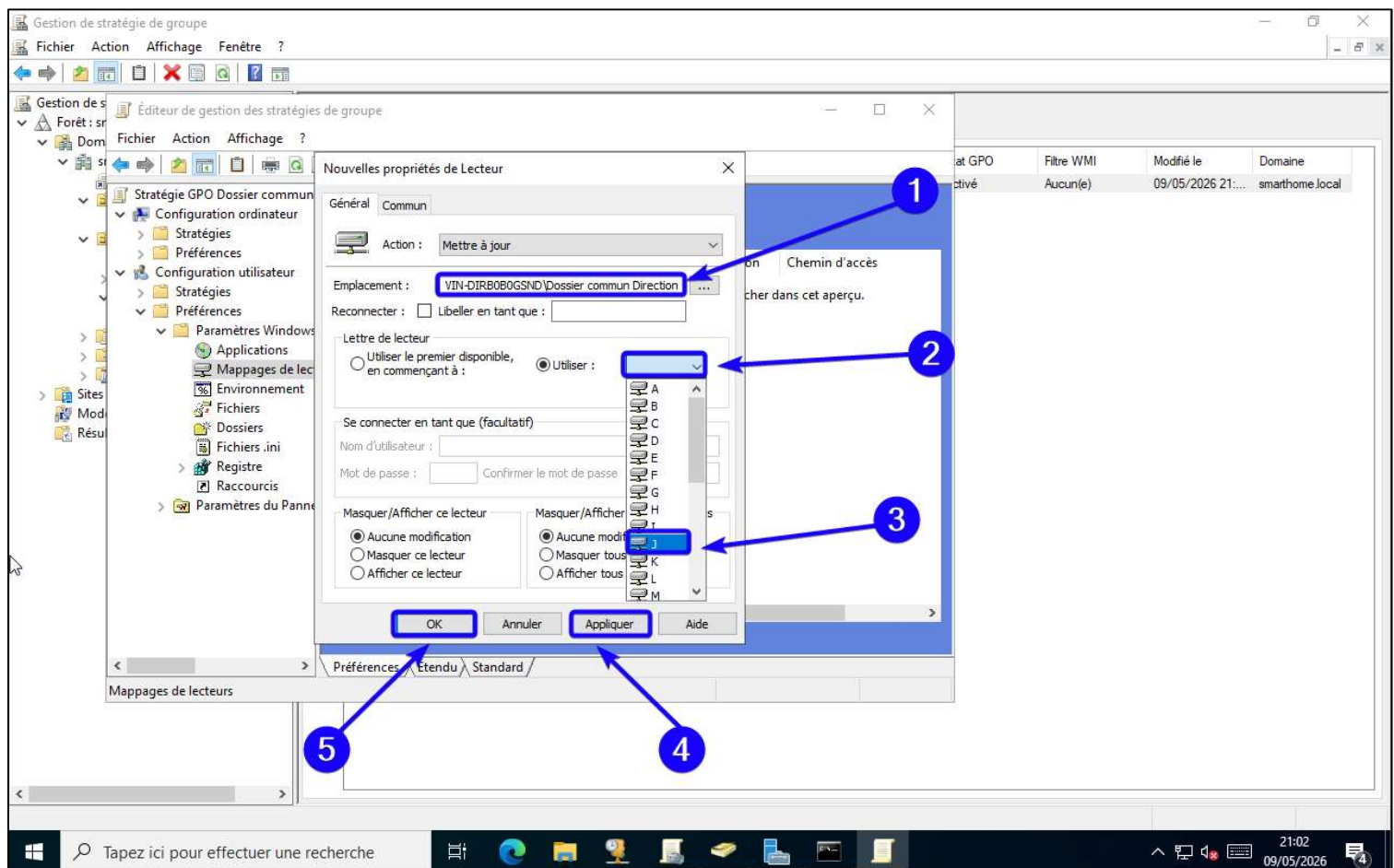
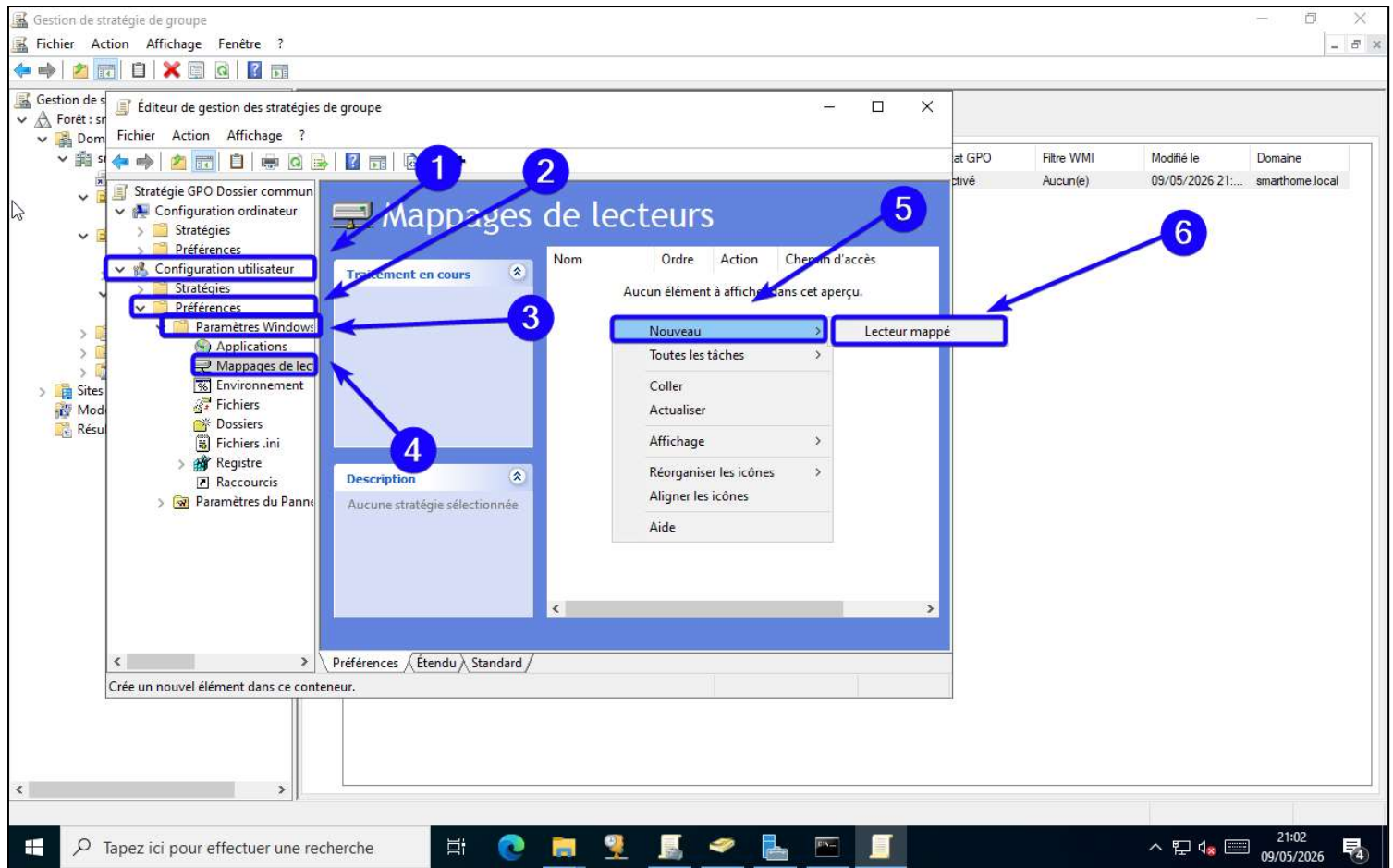
 Partage avancé...

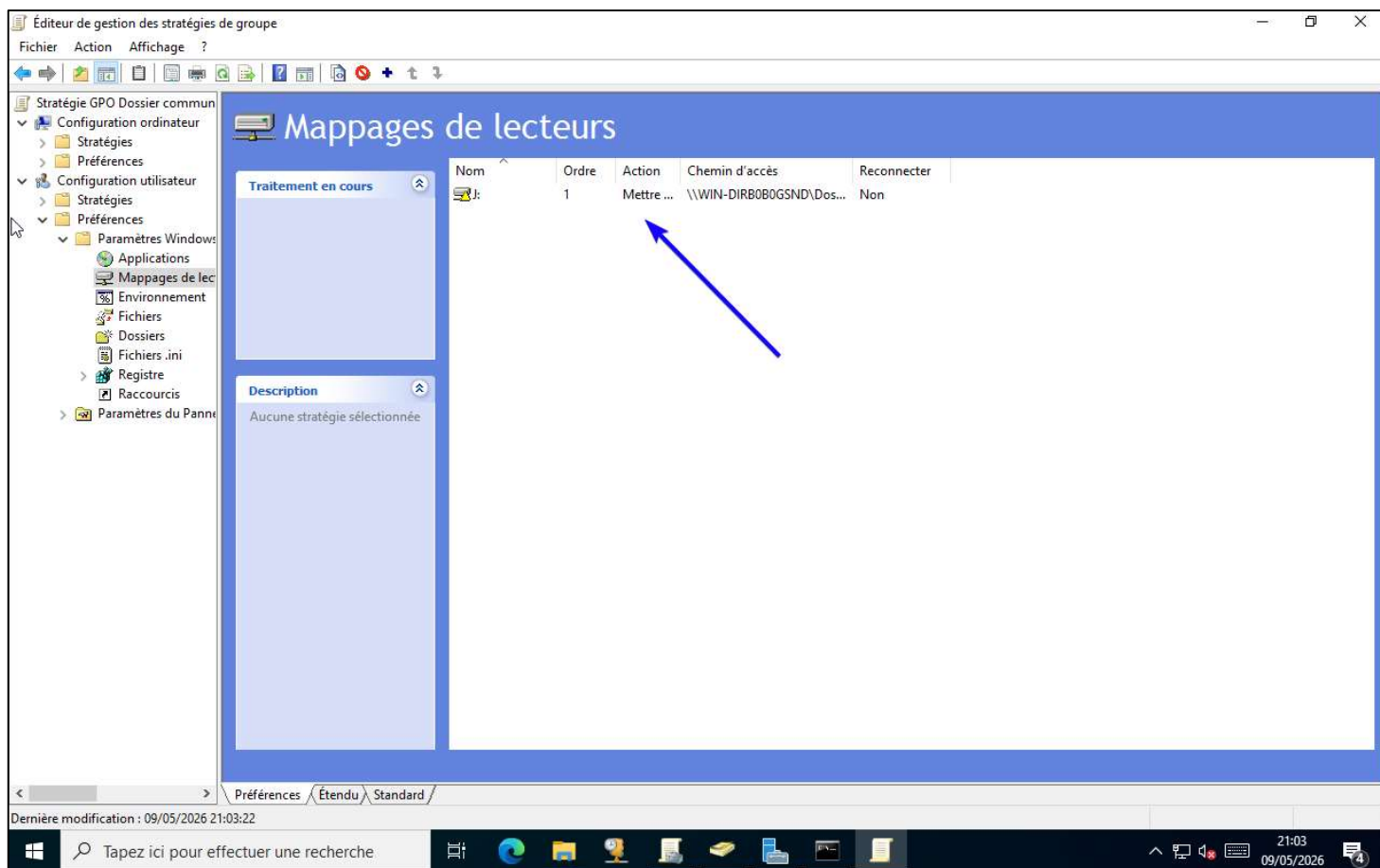


Pour le mappage des lecteurs il faut copier le chemin réseau du dossier concerné :

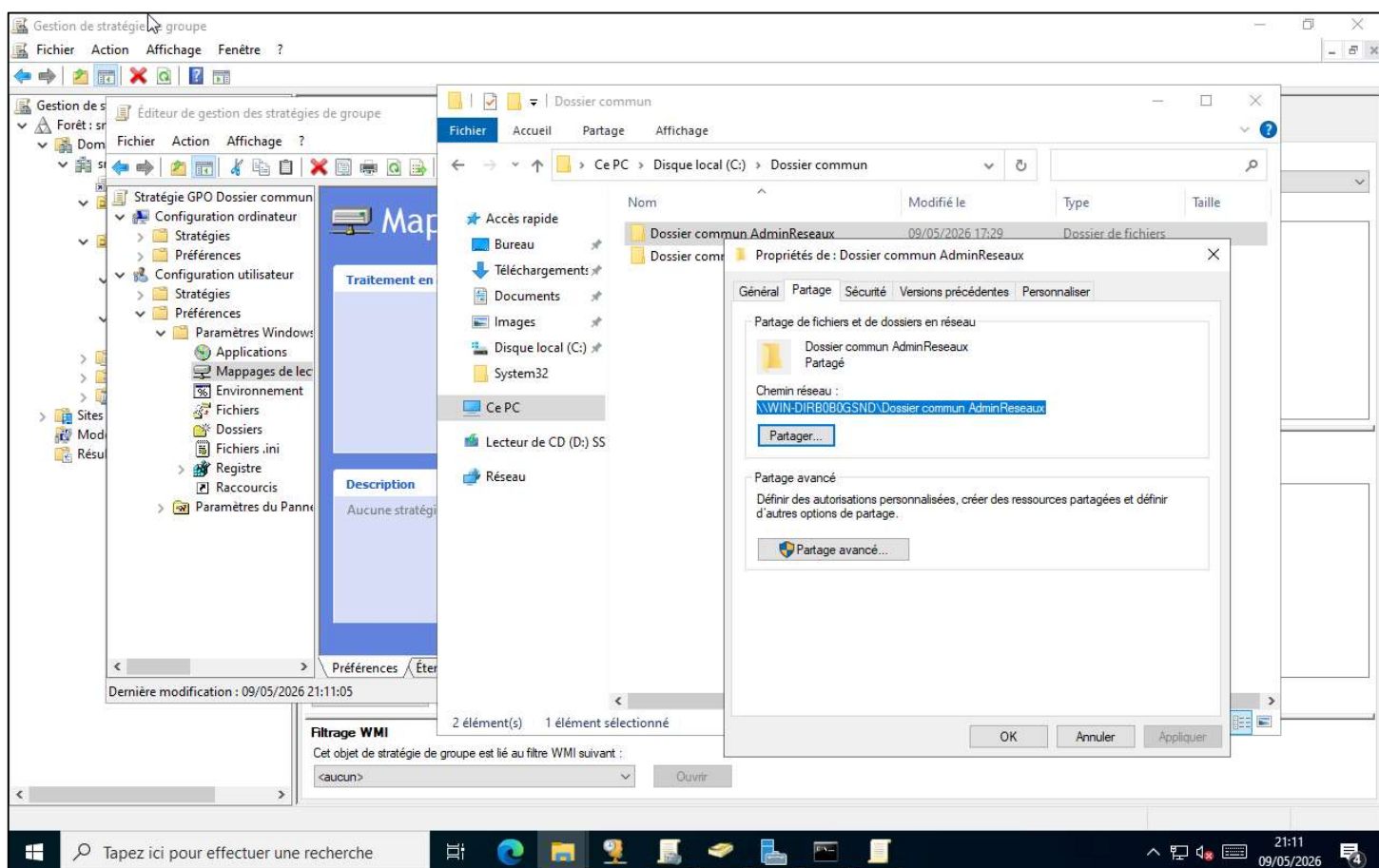


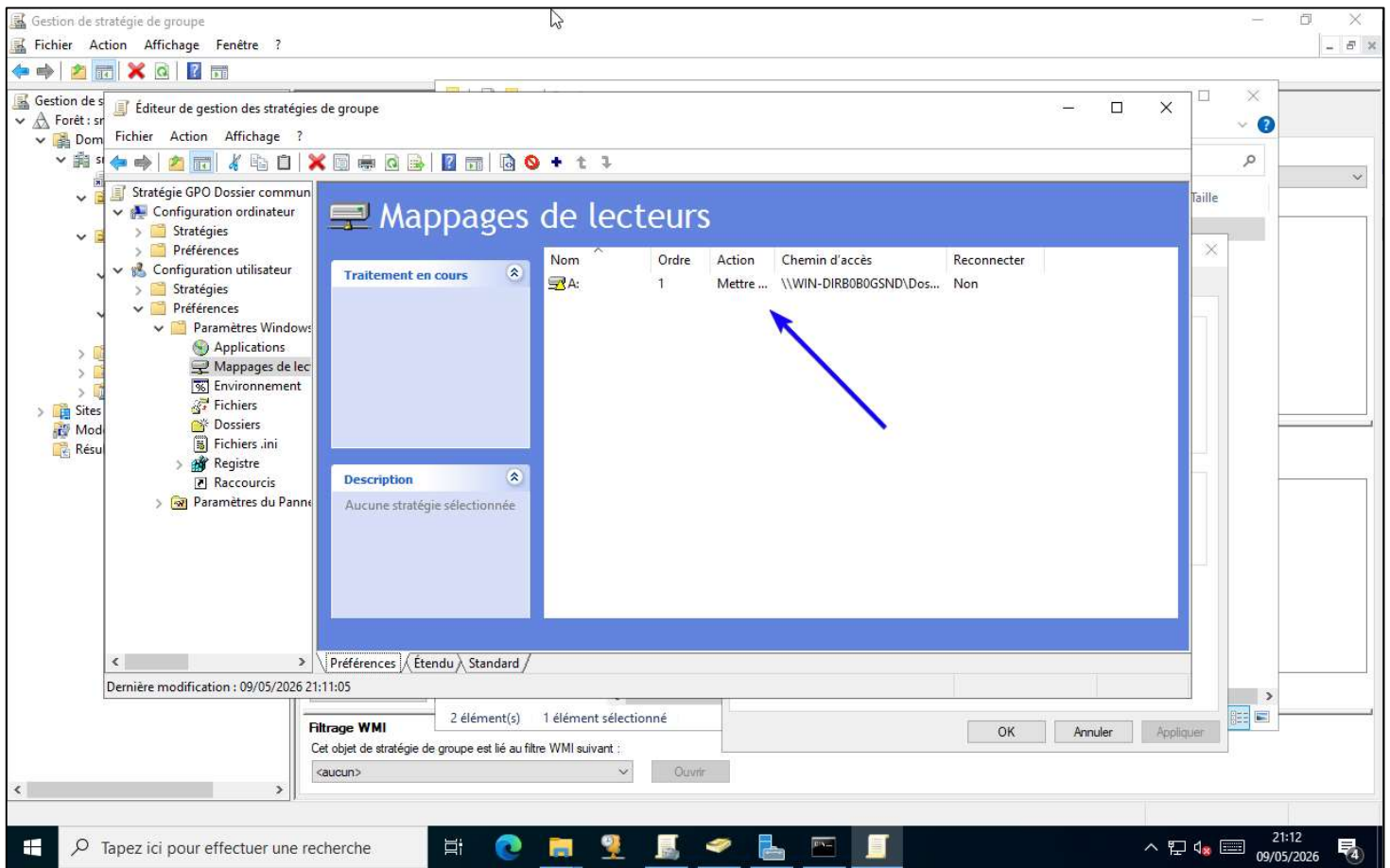
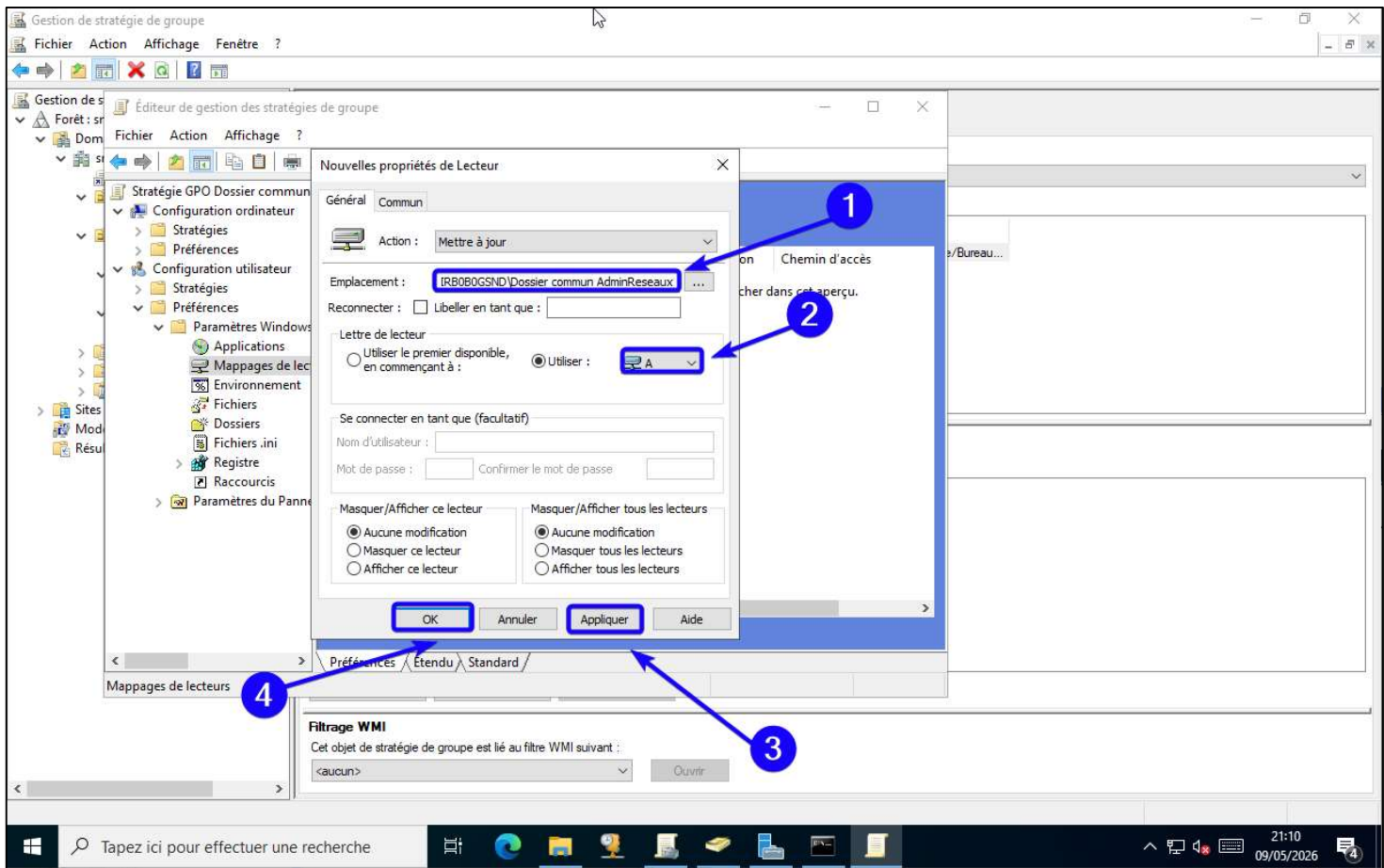




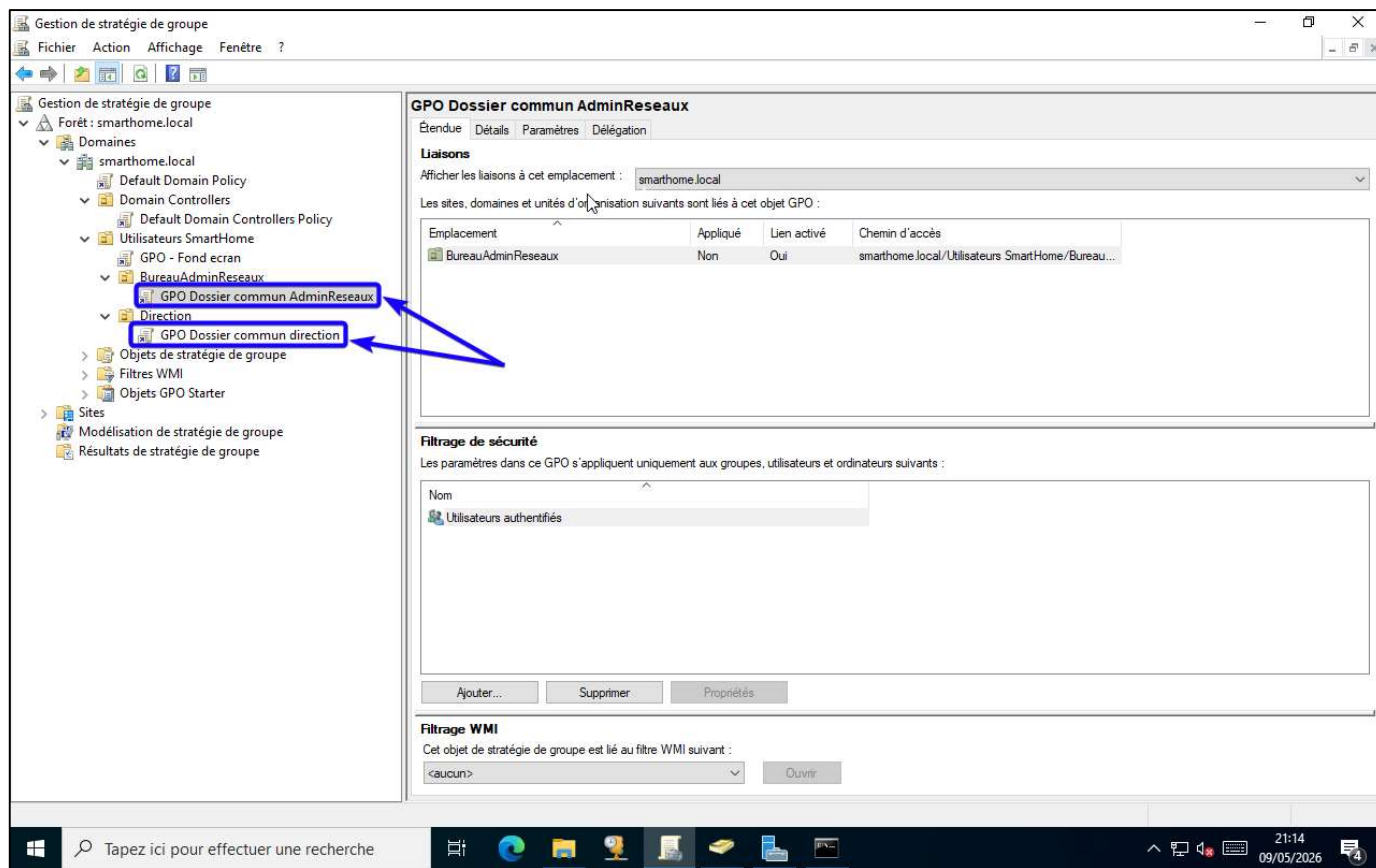


Même manipulation pour le dossier commun du services **AdminRéseaux**.





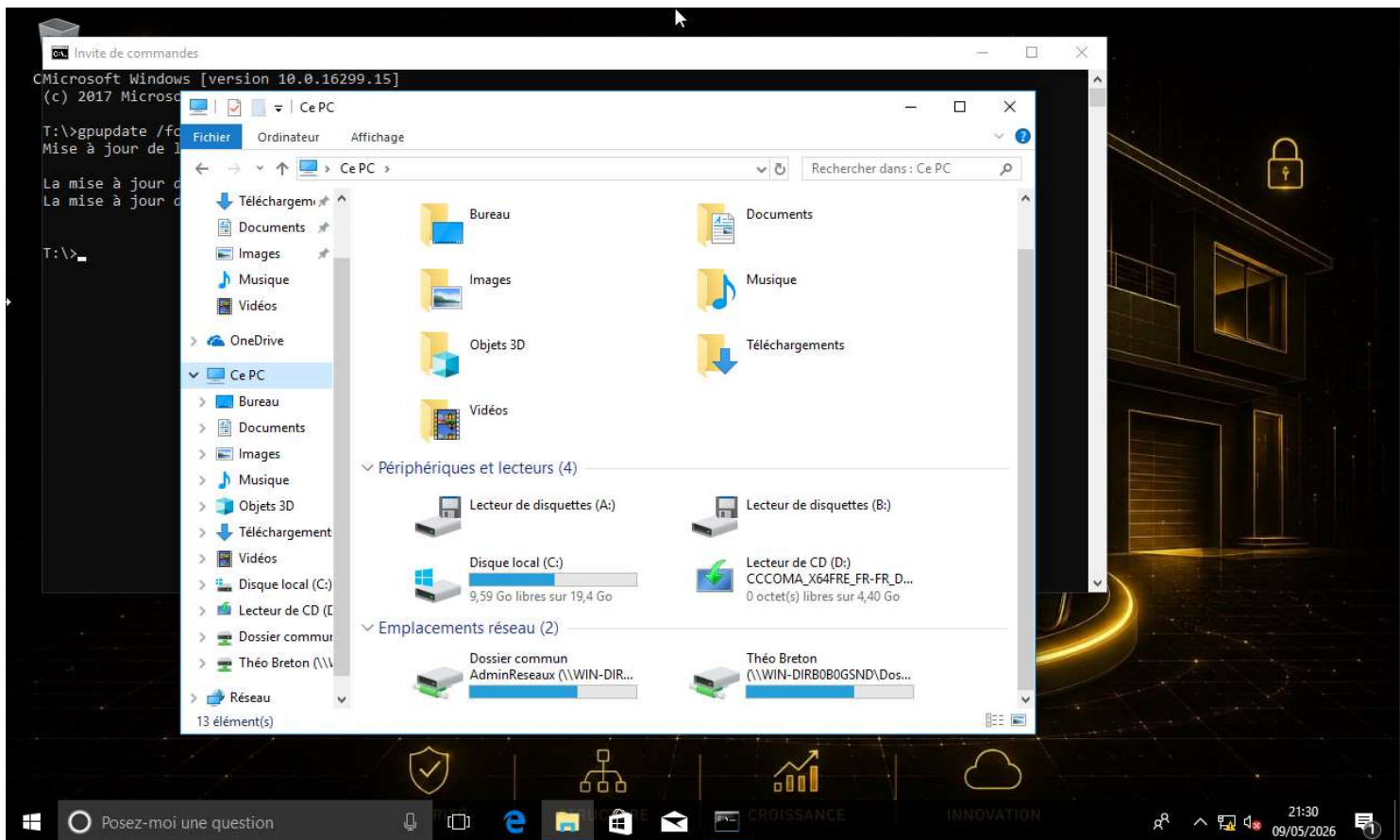
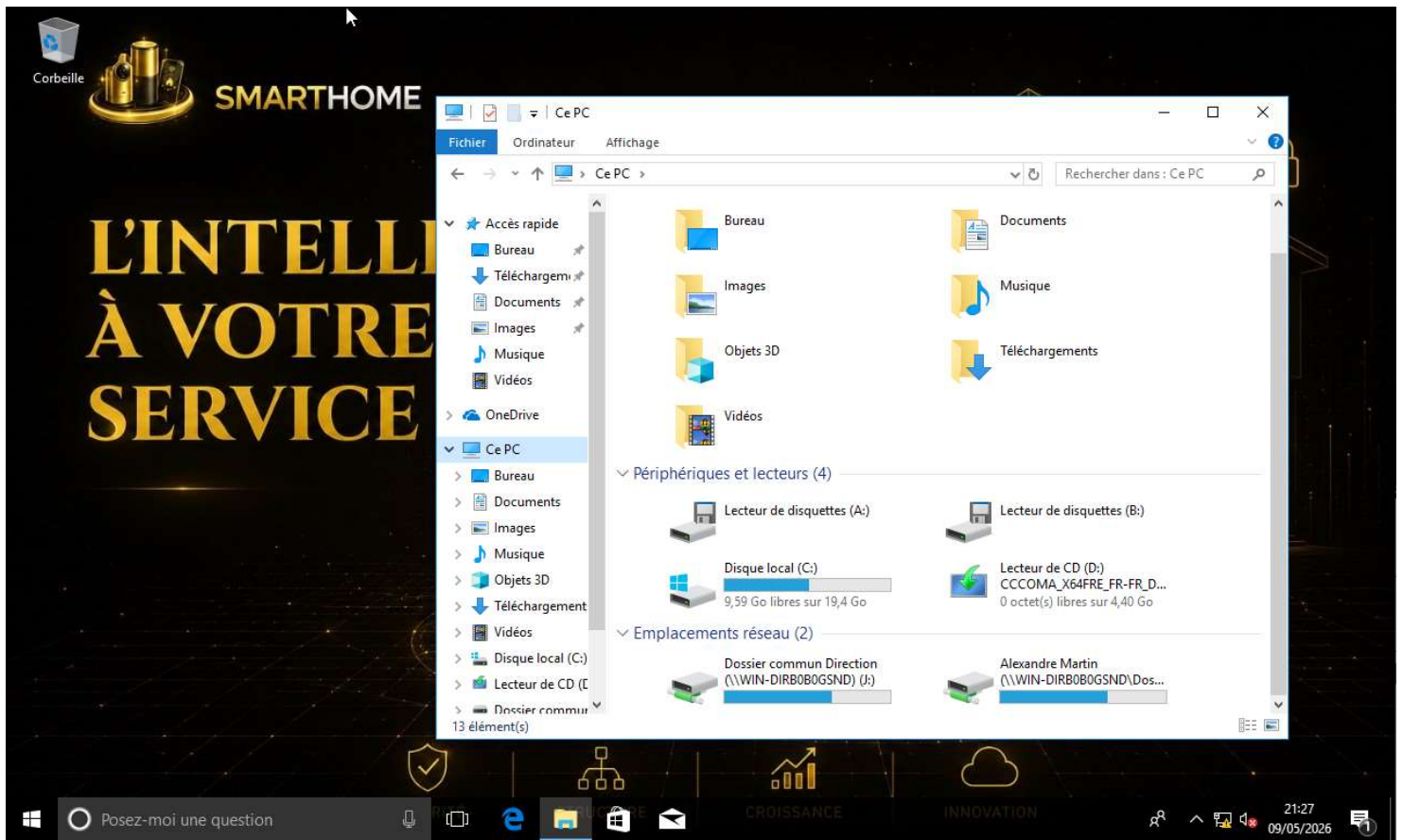
Nos deux GPOs sont maintenant opérationnel :



Test Validation:

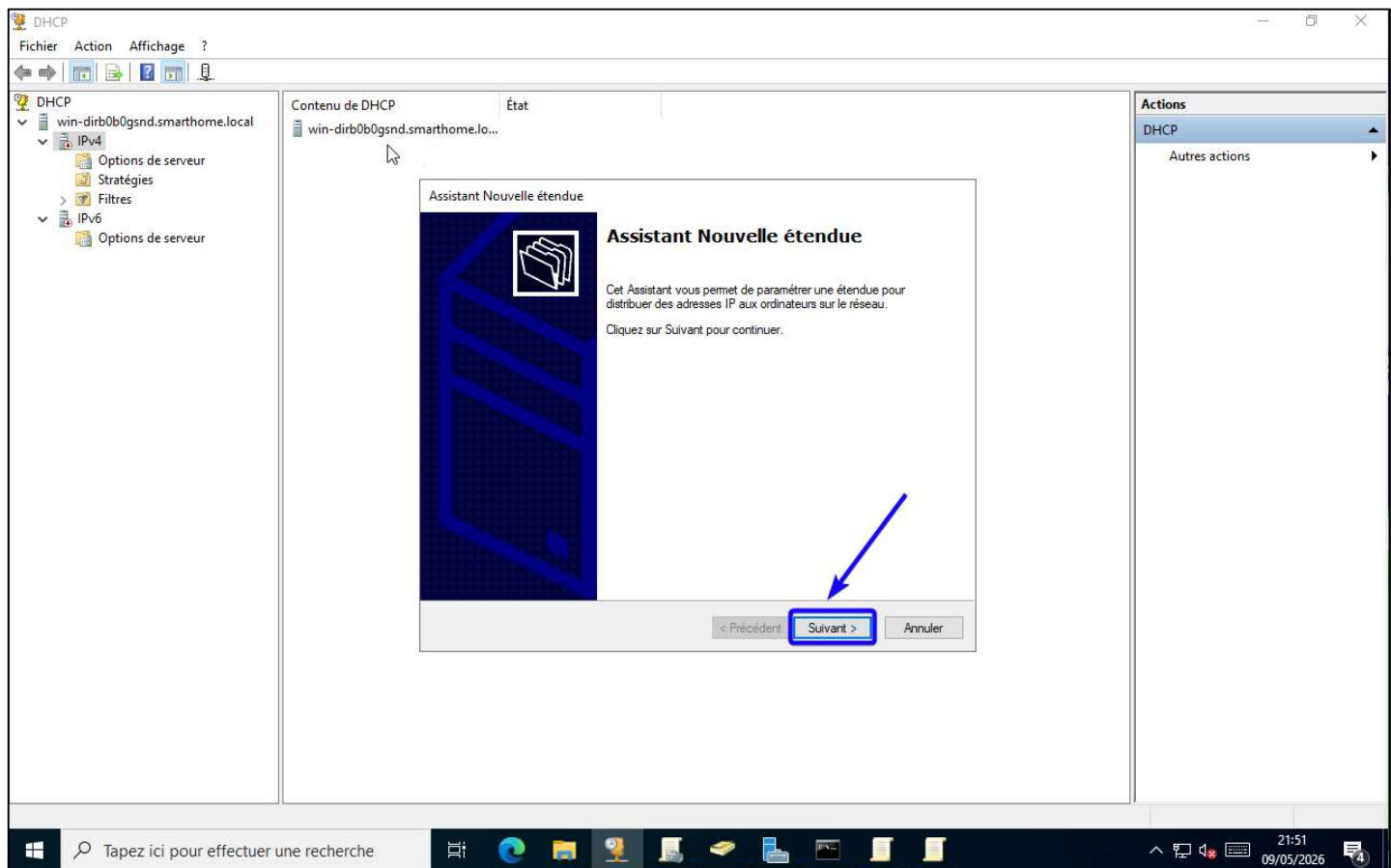
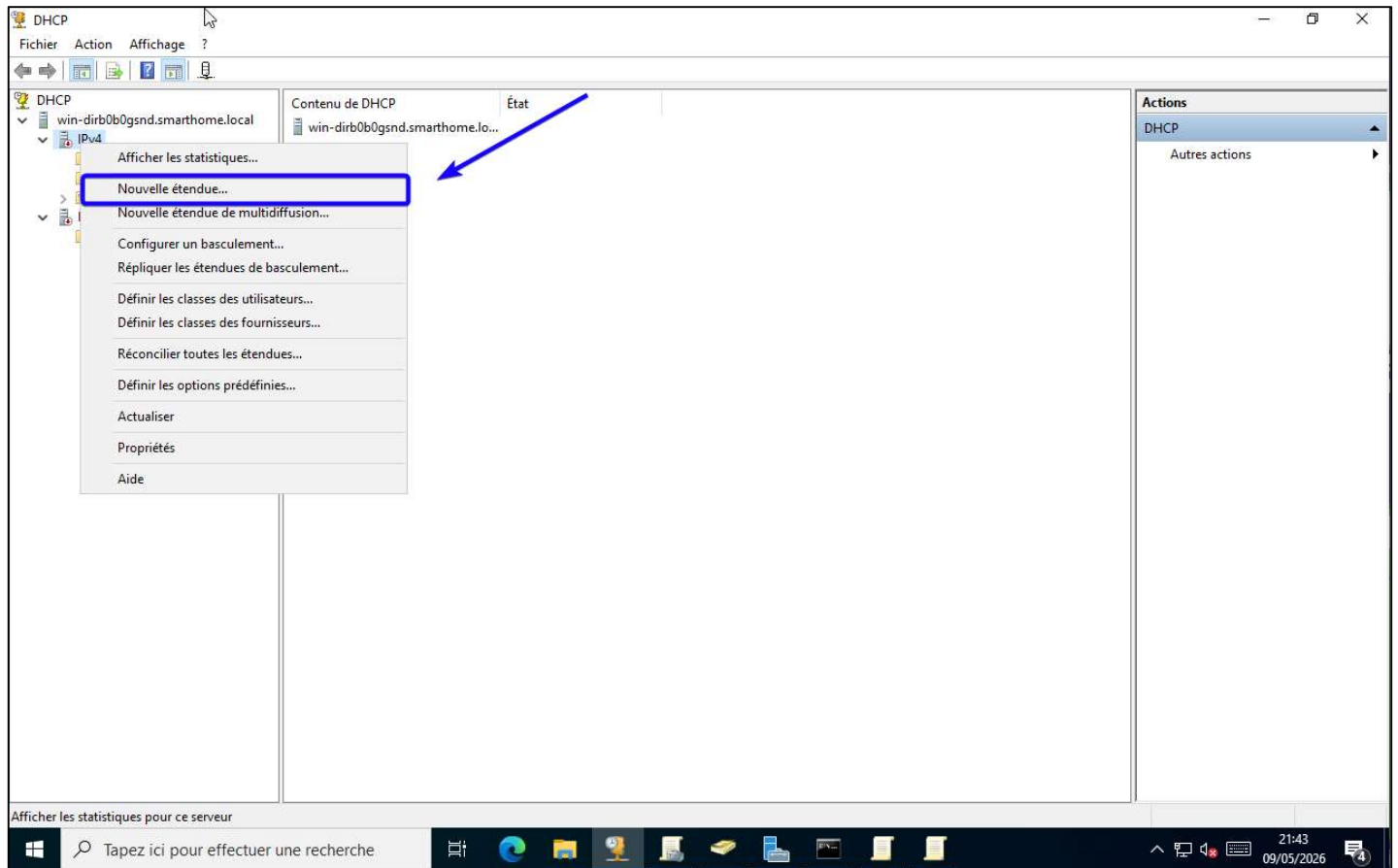
Vérification sur la session utilisateur :

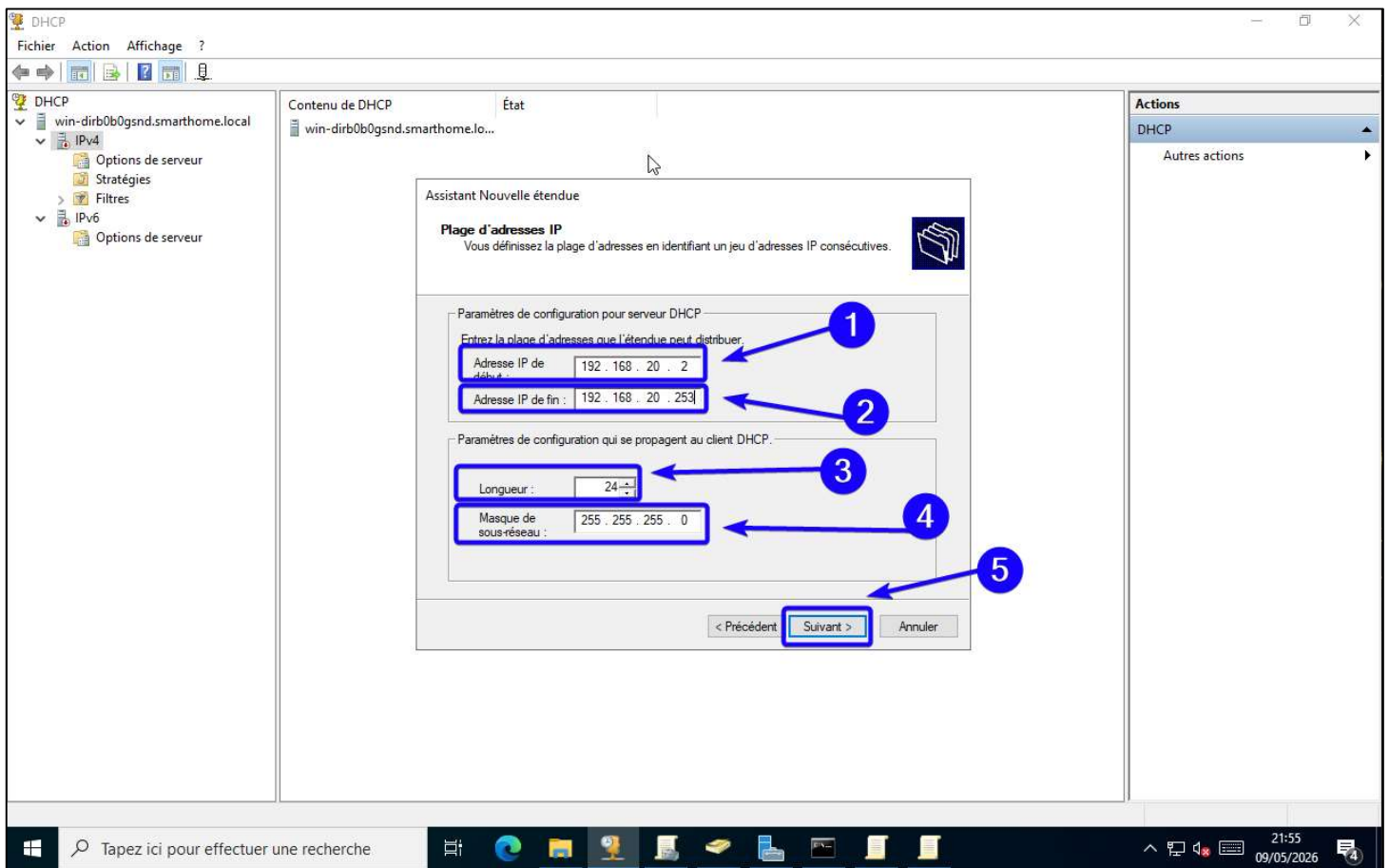
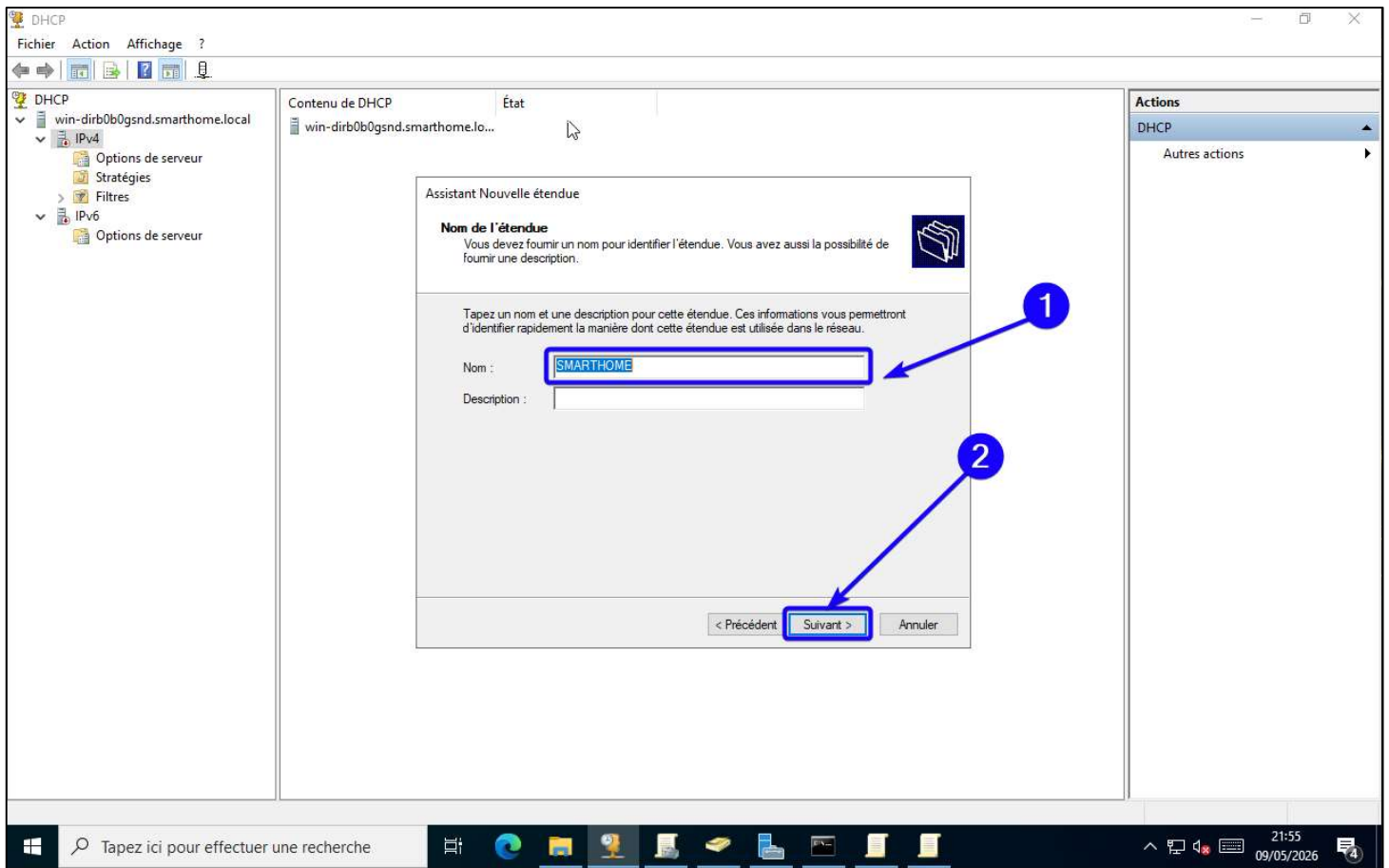
Pour mettre les stratégies de groupe : **gpupdate /force**

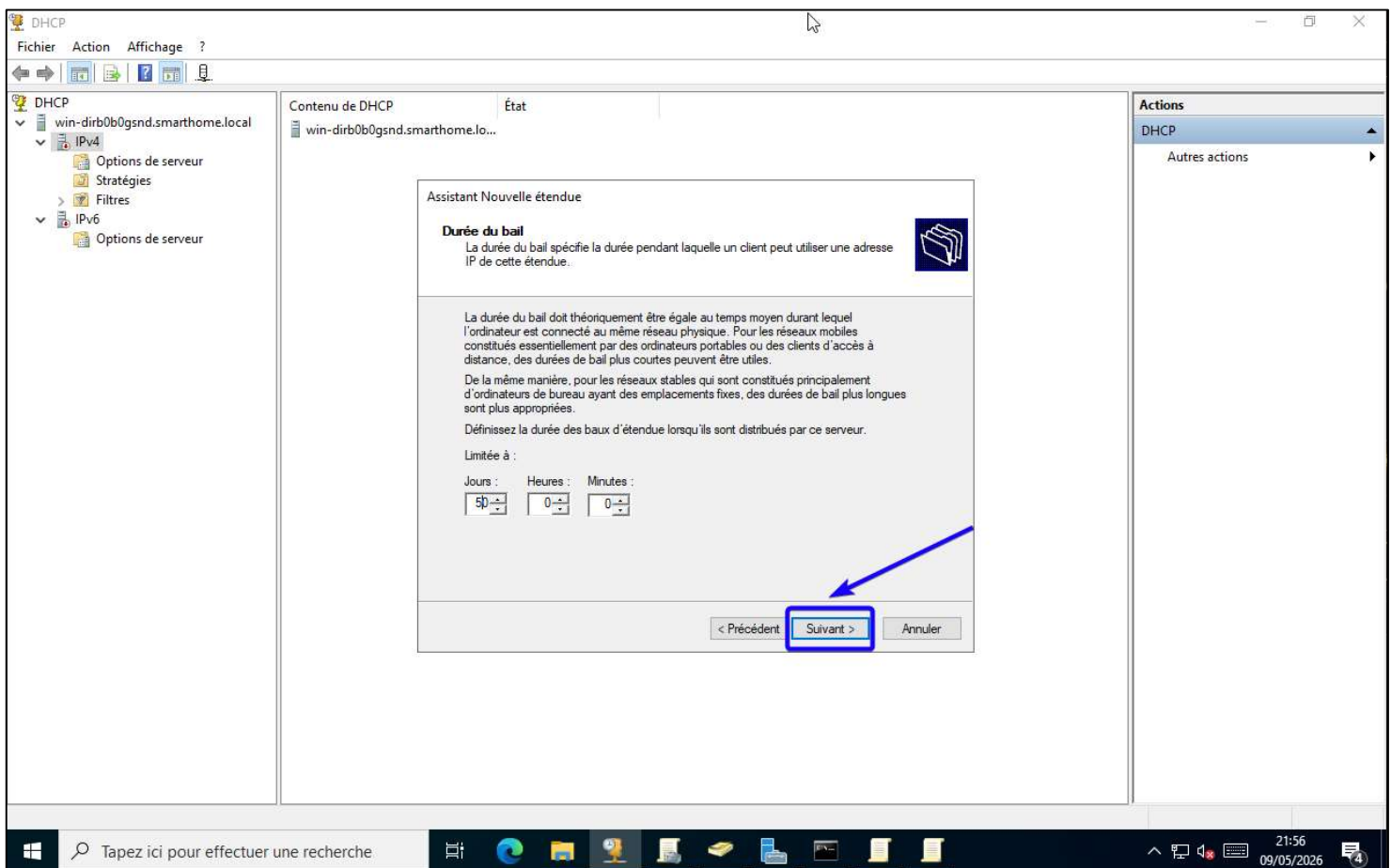
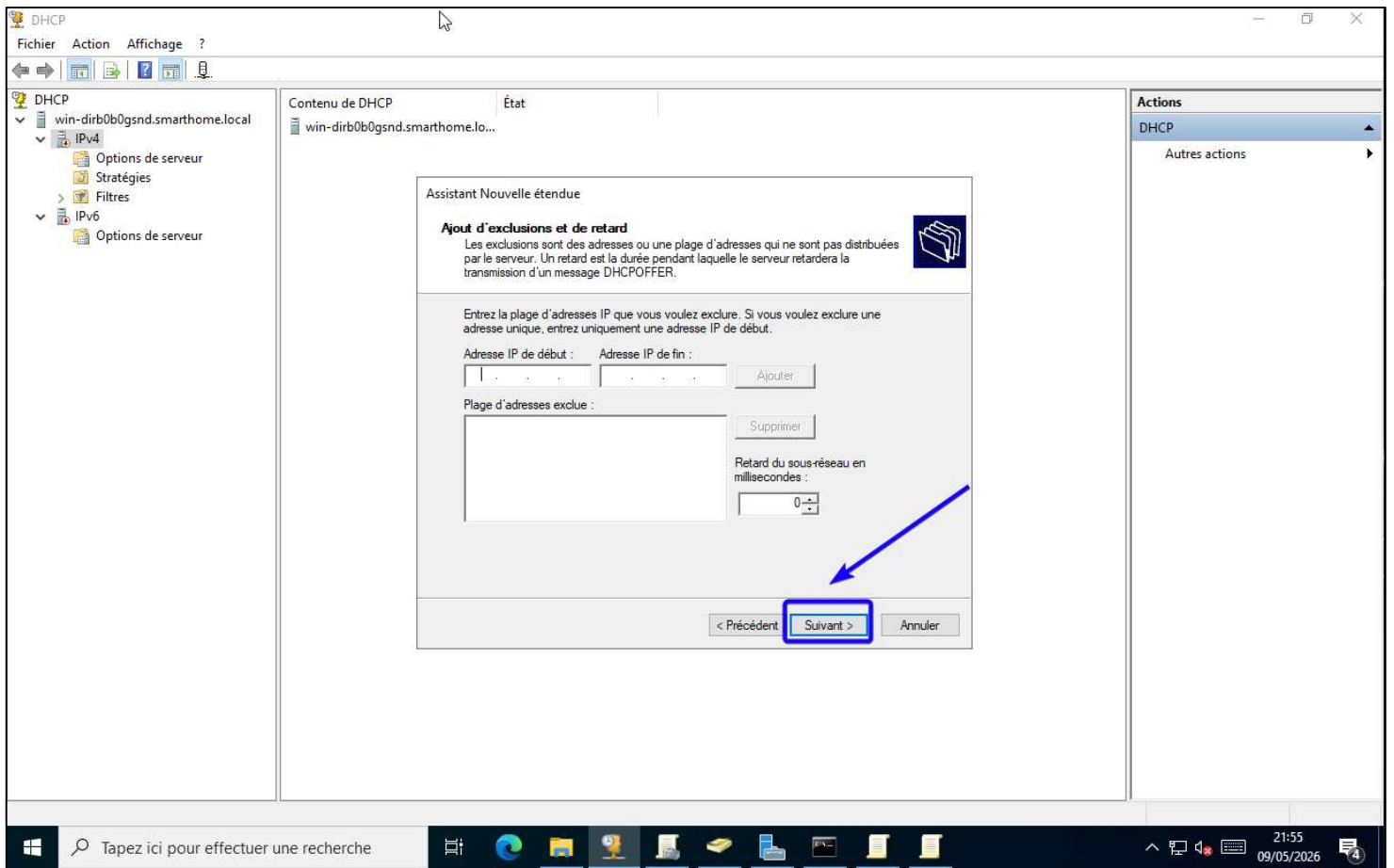


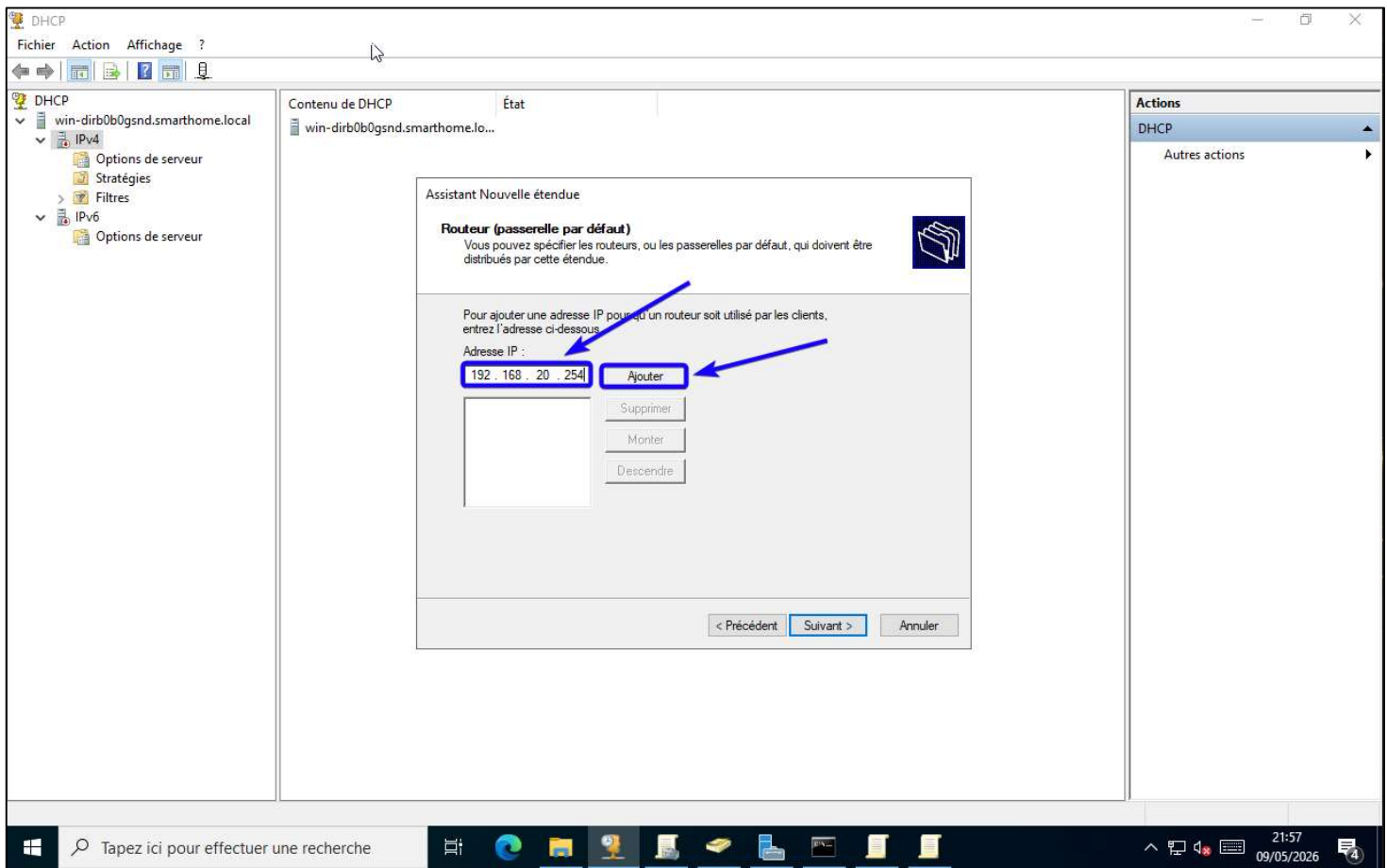
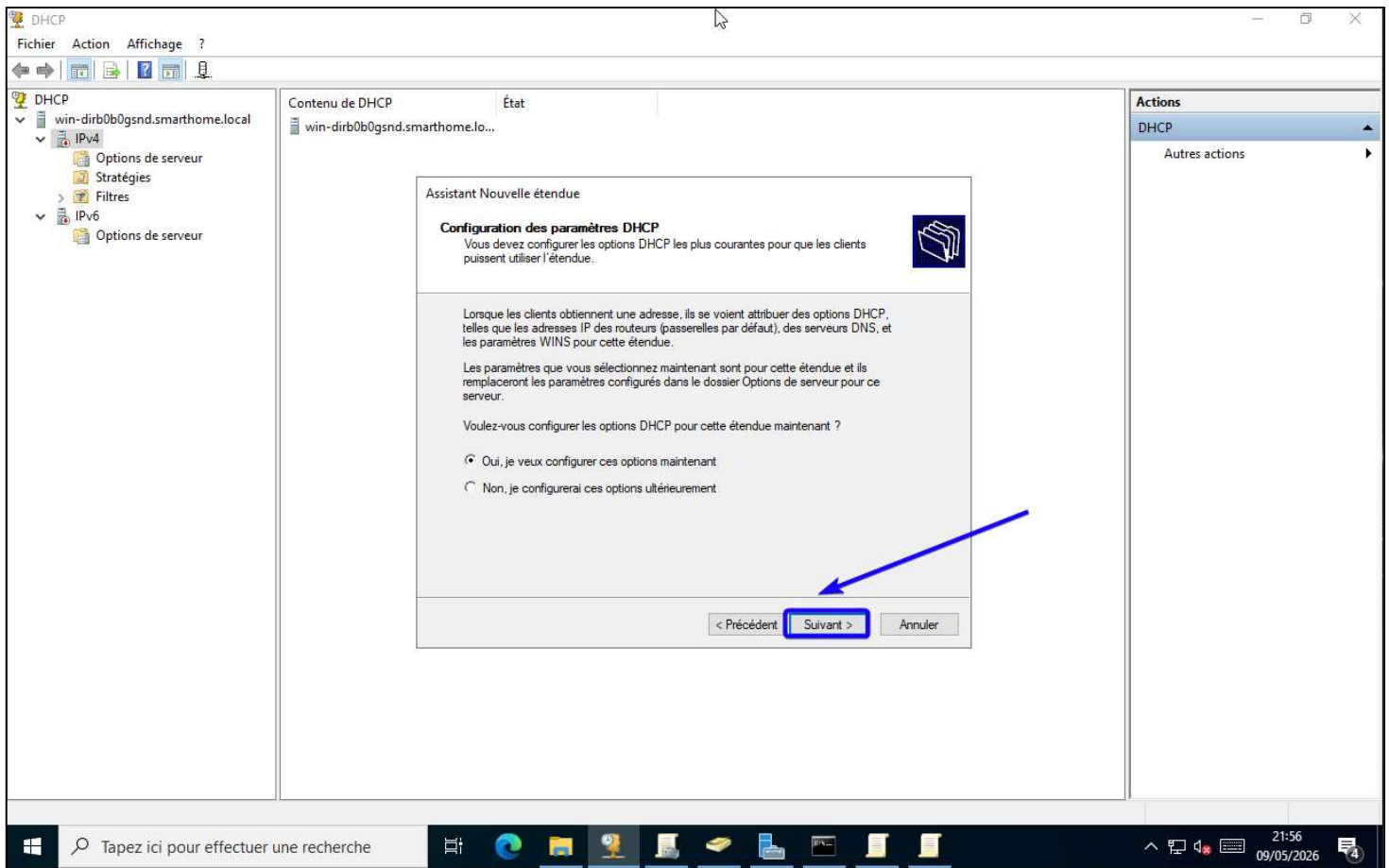
PARTIE 3 : Mise en place de l'adressage dynamique sur le réseau local de l'entreprise :

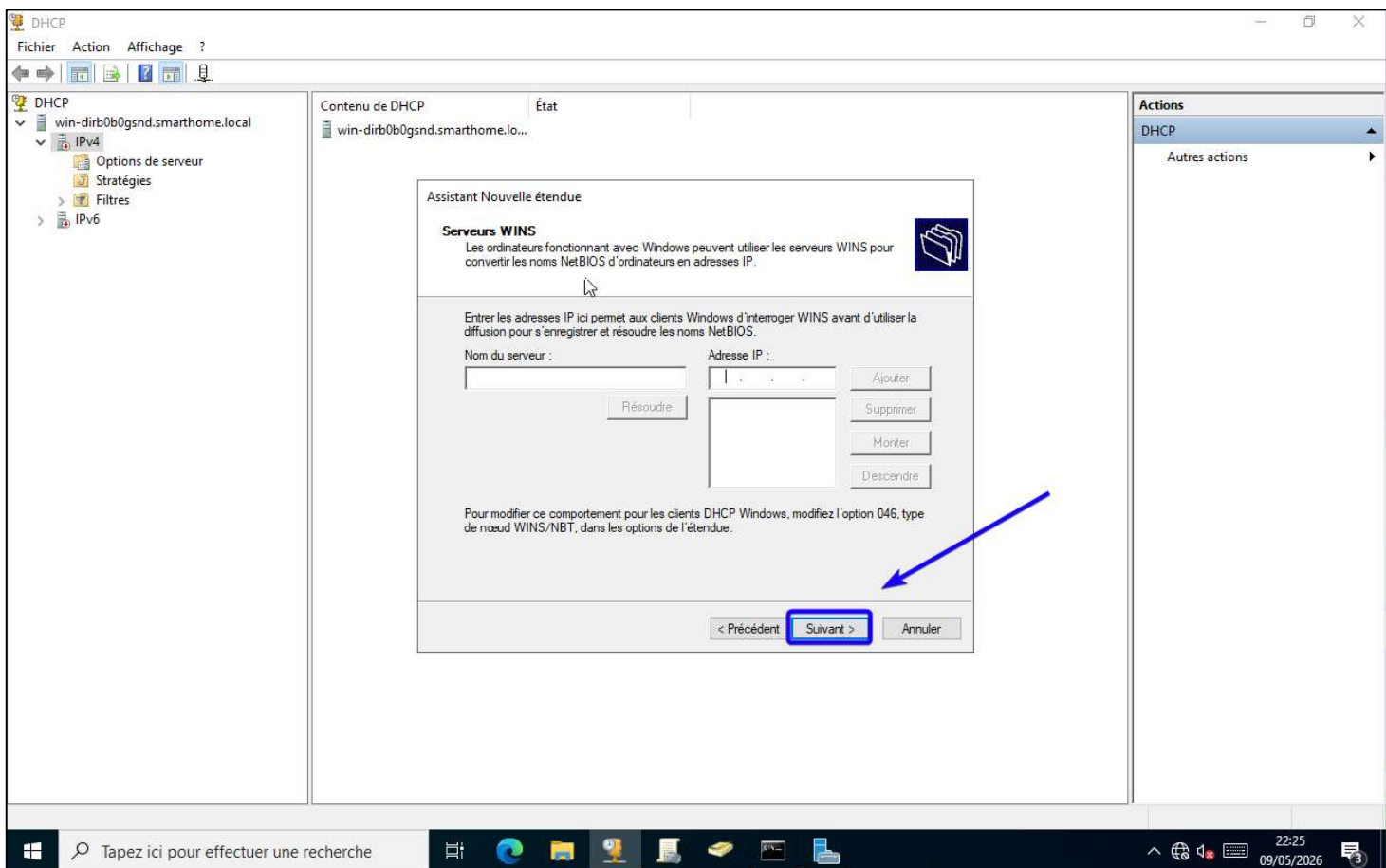
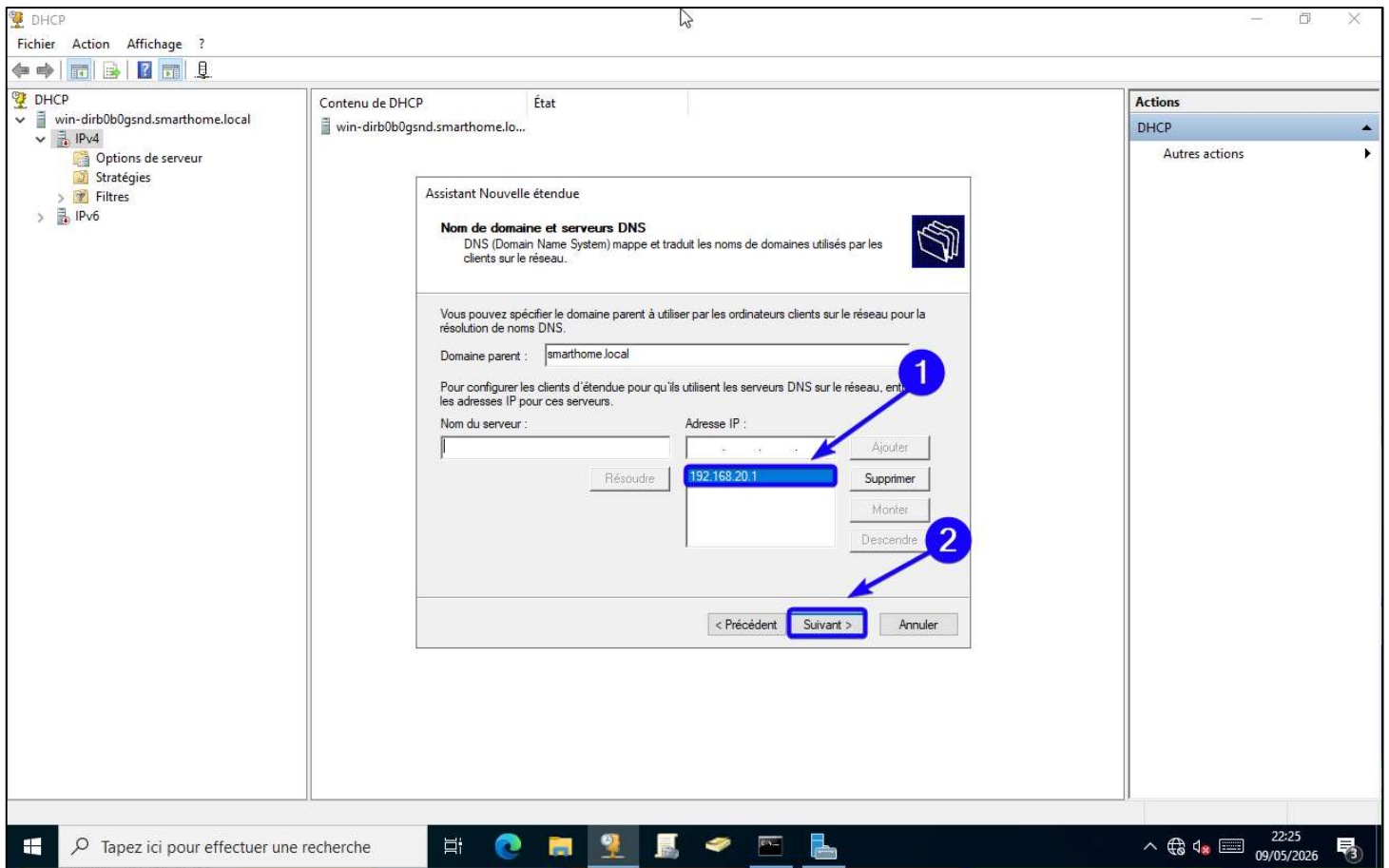
❶ Configuration DHCP

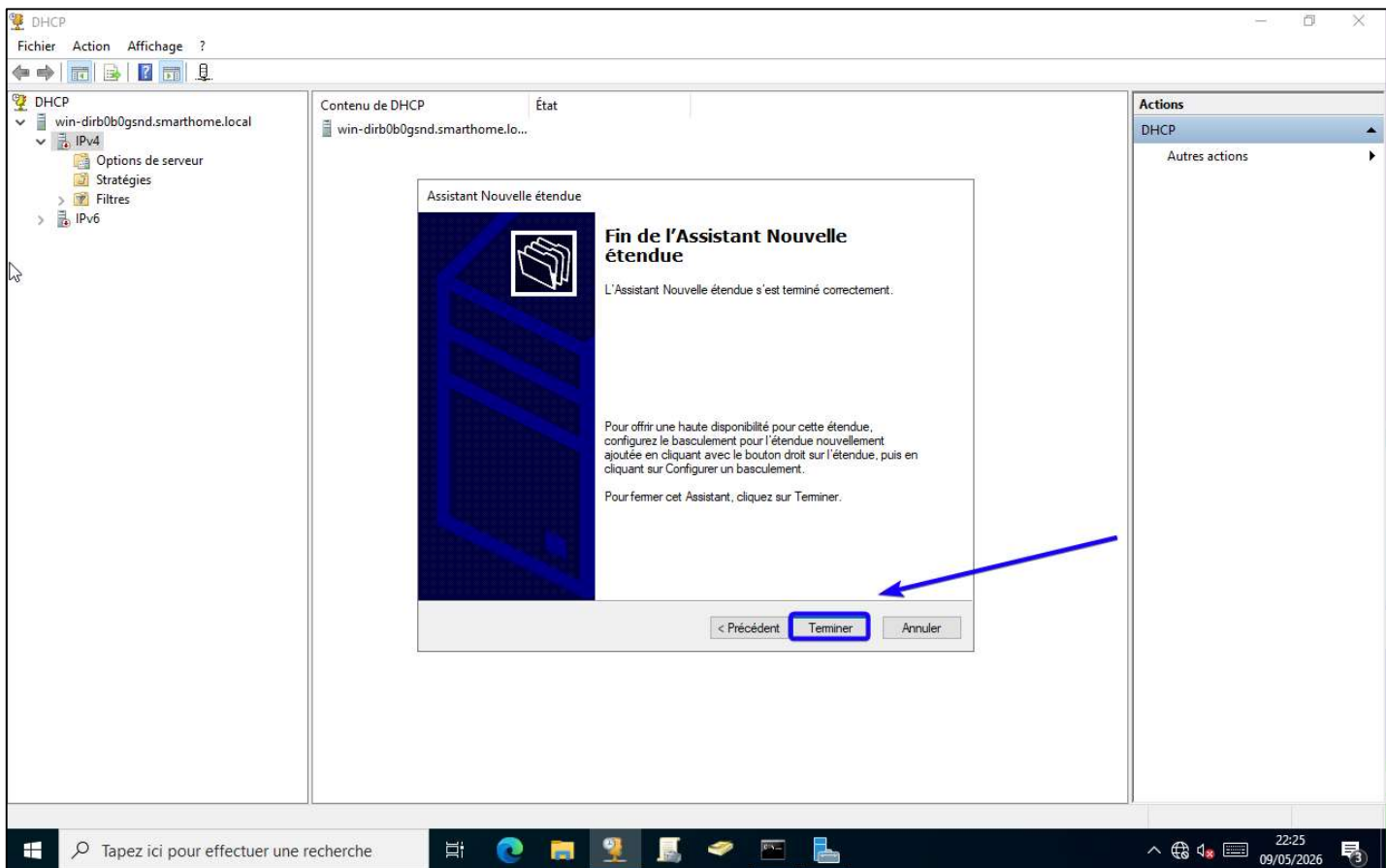
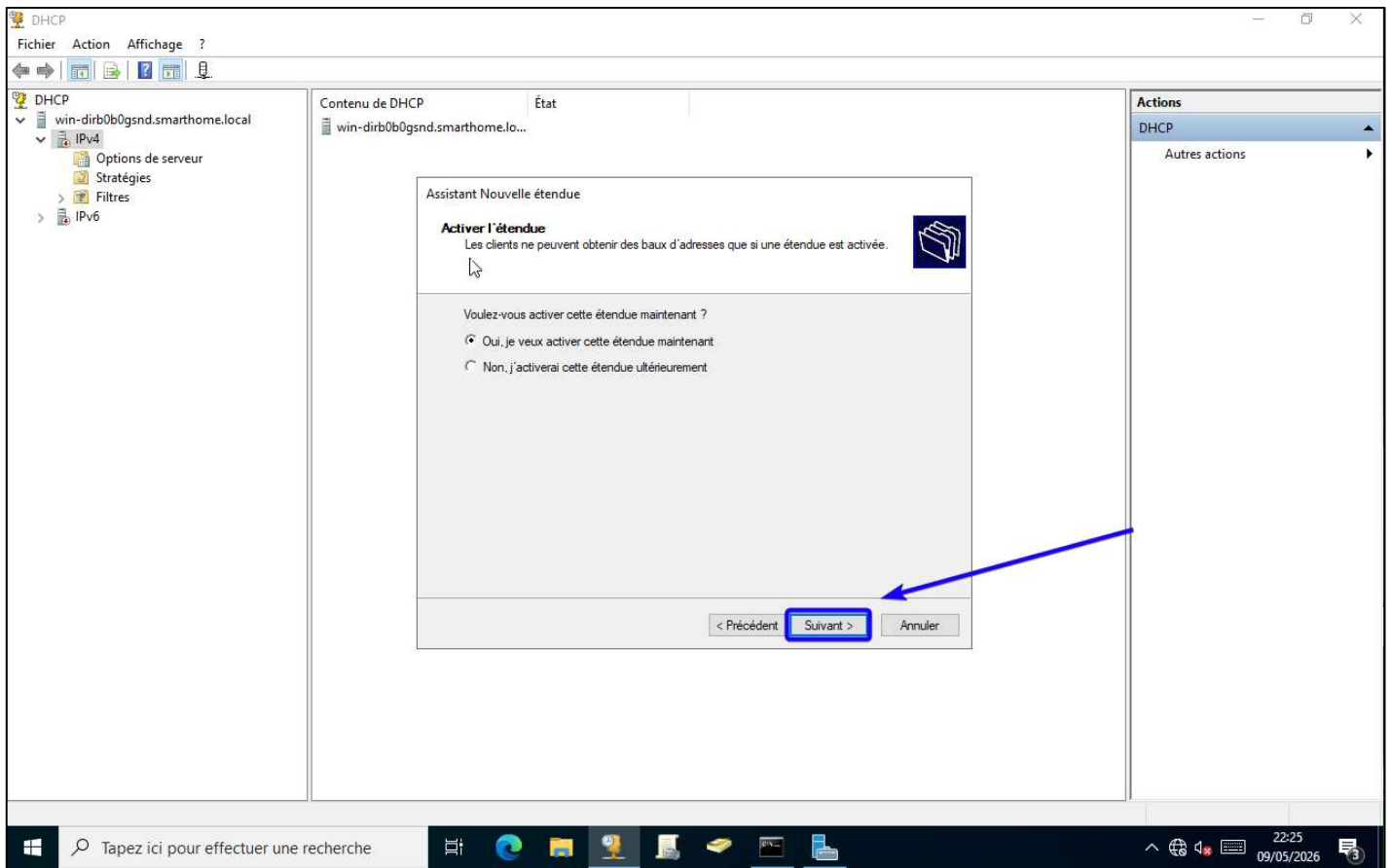




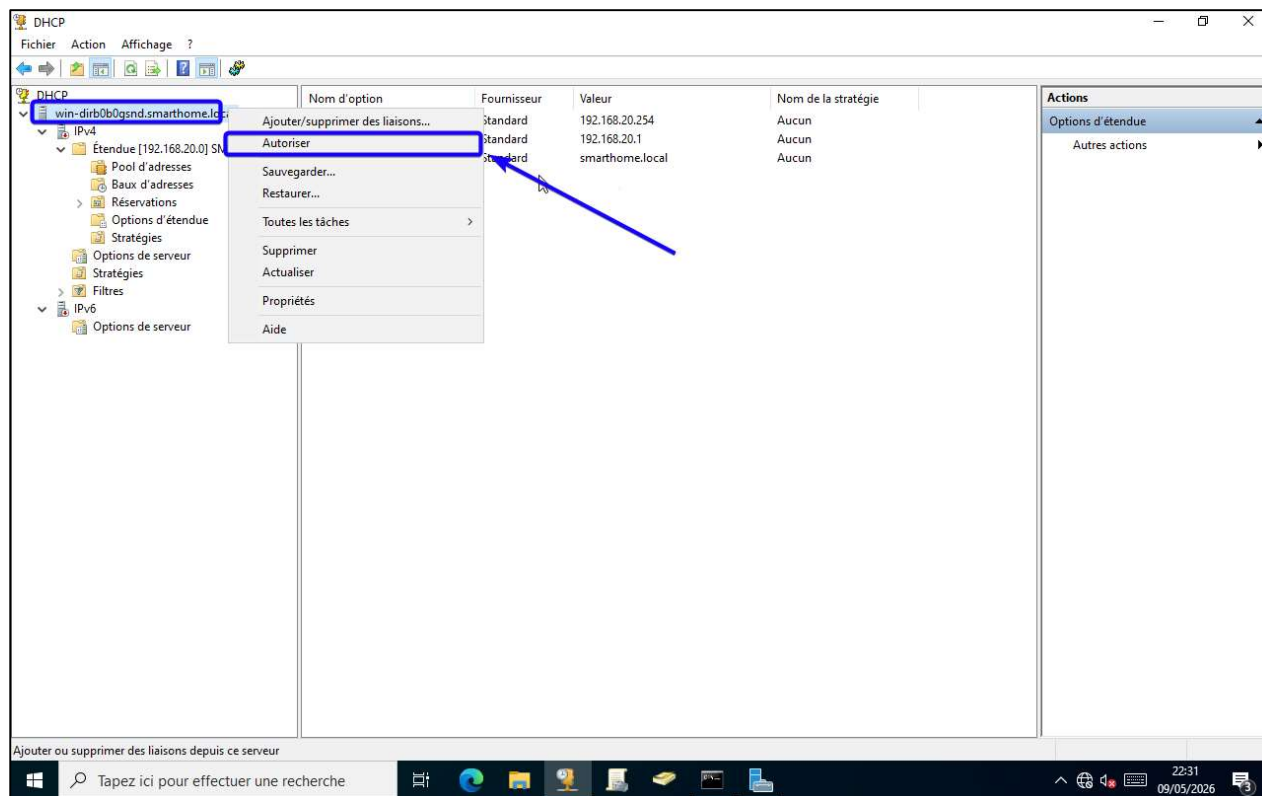
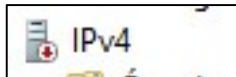




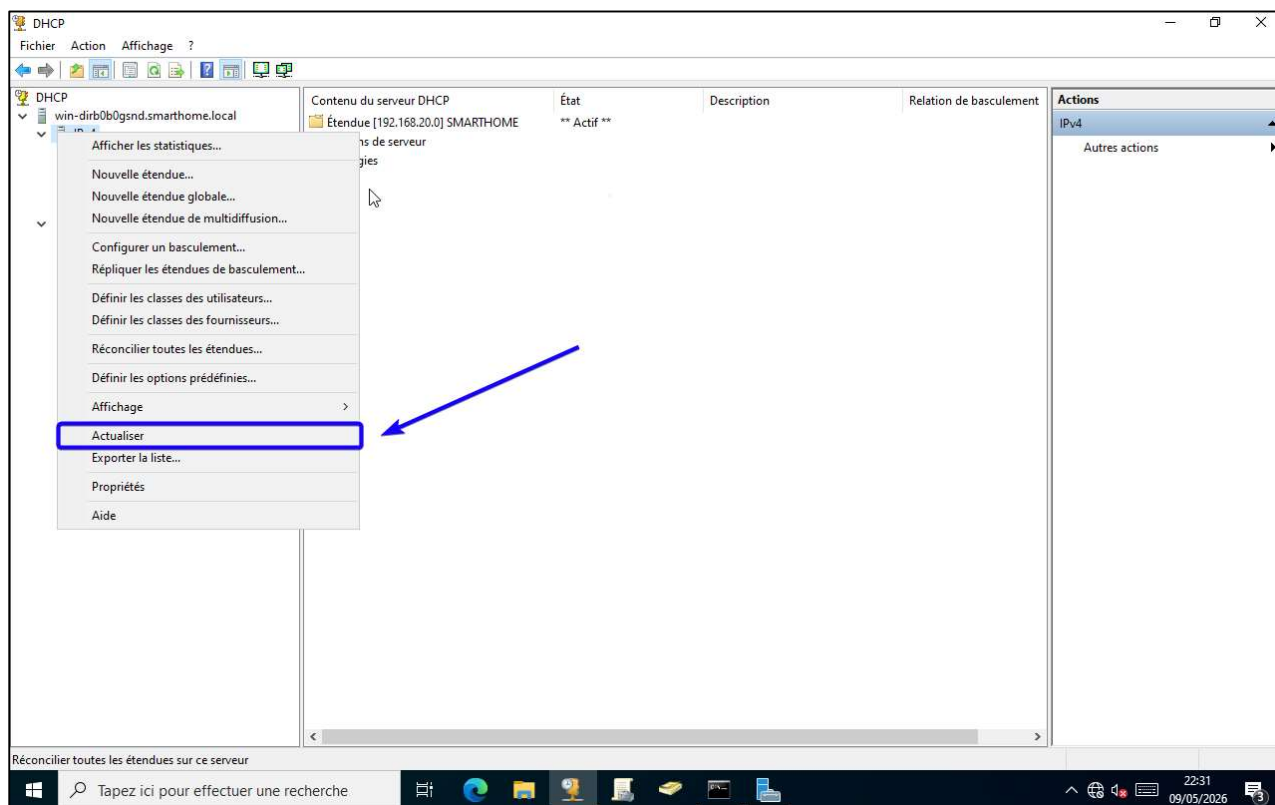




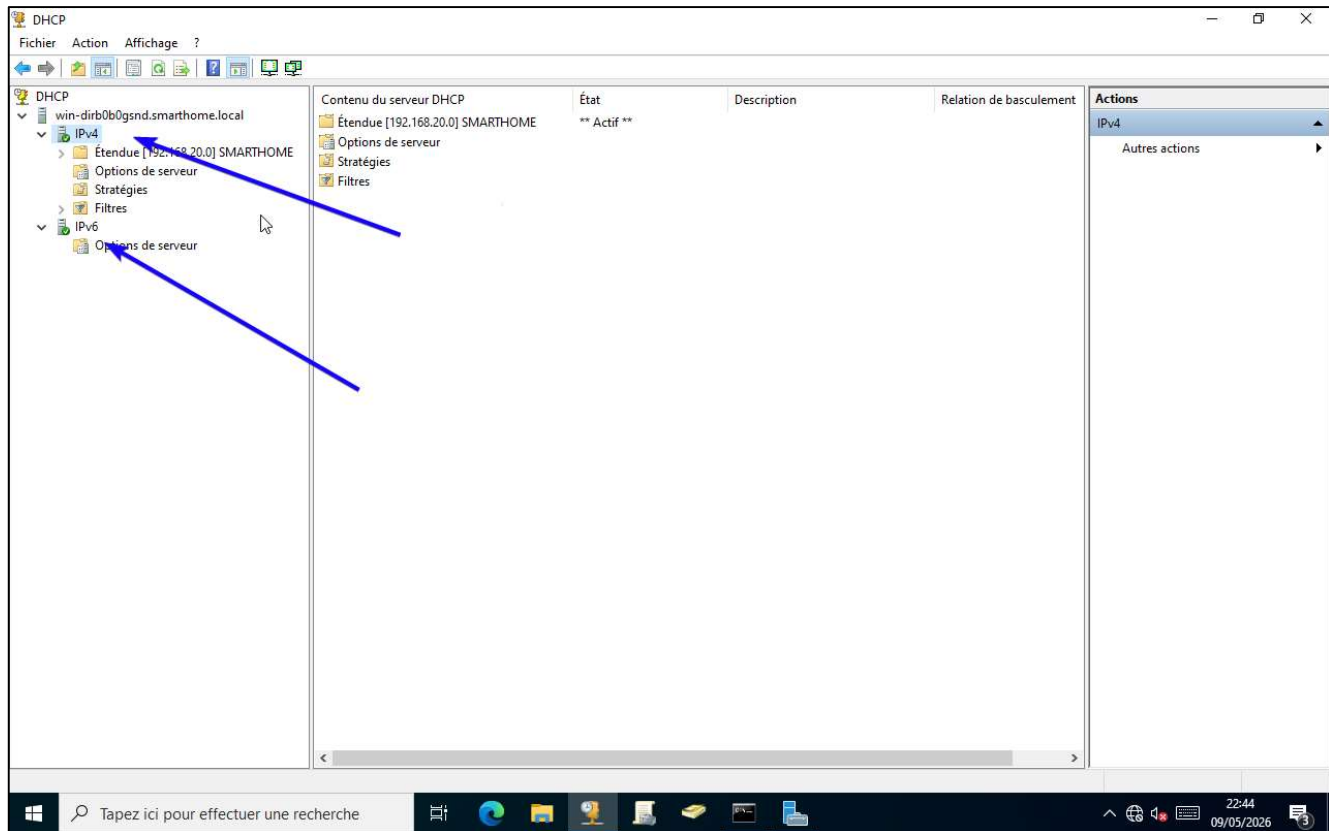
Pour activer votre service DHCP :



Puis clique droit sur IPv4 et IPv6 → Actualiser :

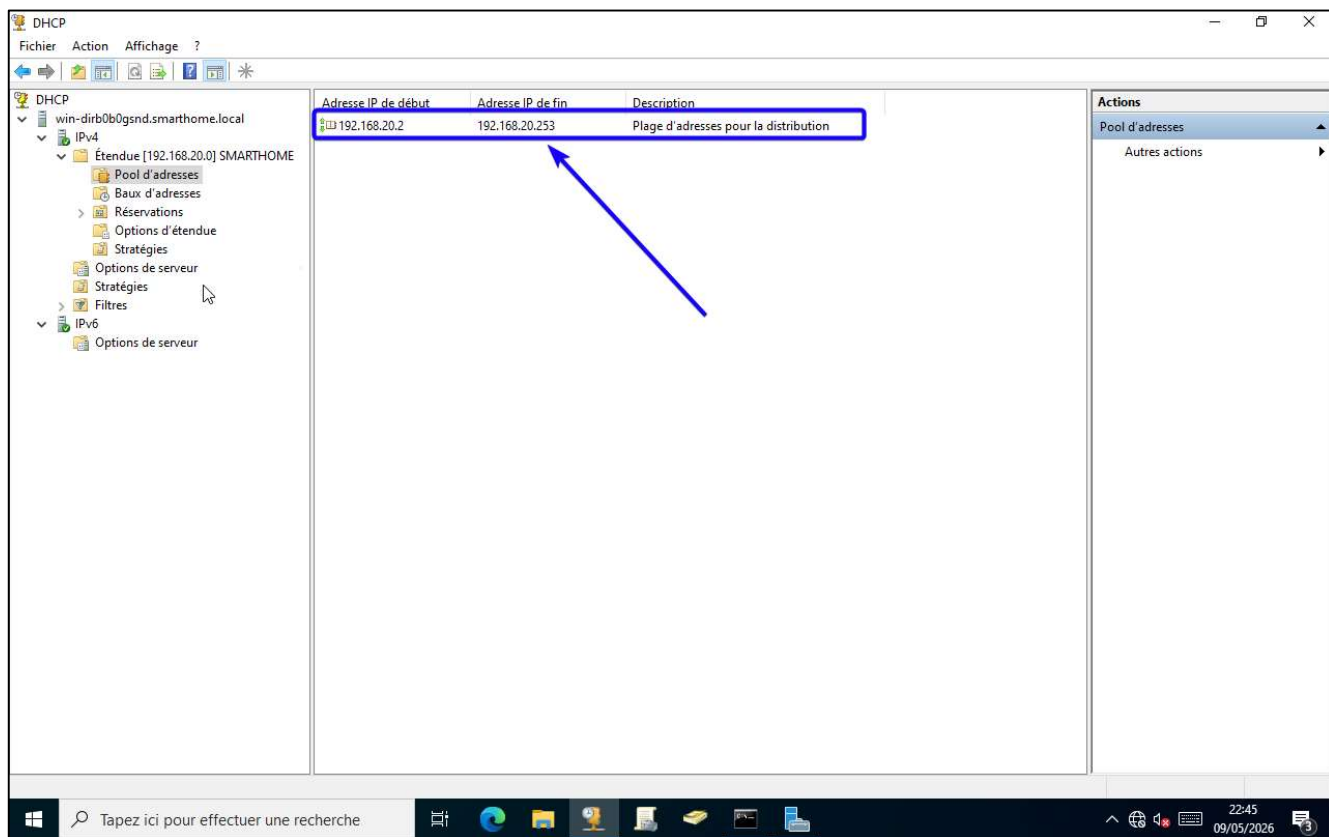


Notre service DHCP et maintenant **opérationnel** :



Vérification que nos paramétrages sont appliqués :

Notre « pool » :



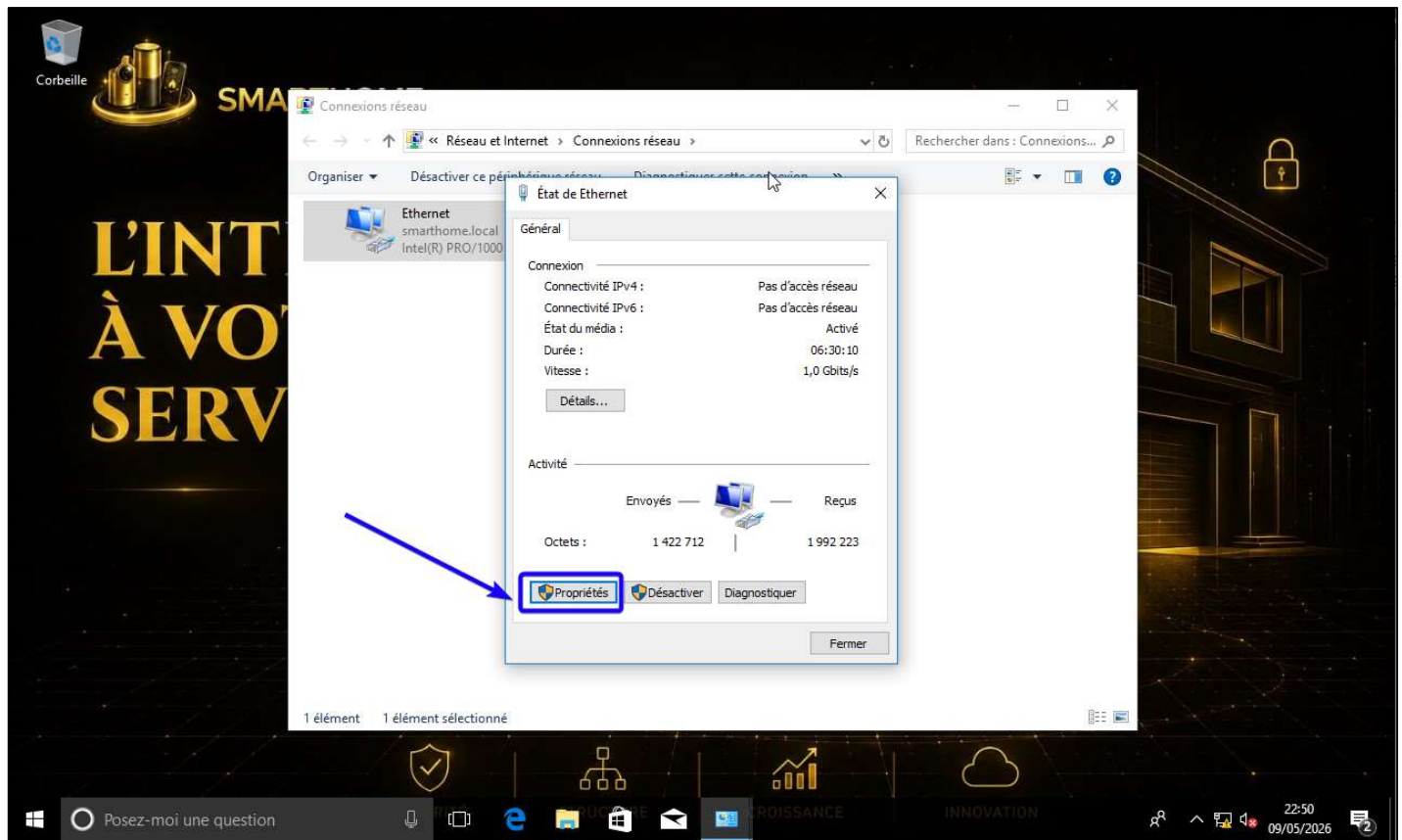
Notre Passerelle, notre DNS, notre nom de domaine :

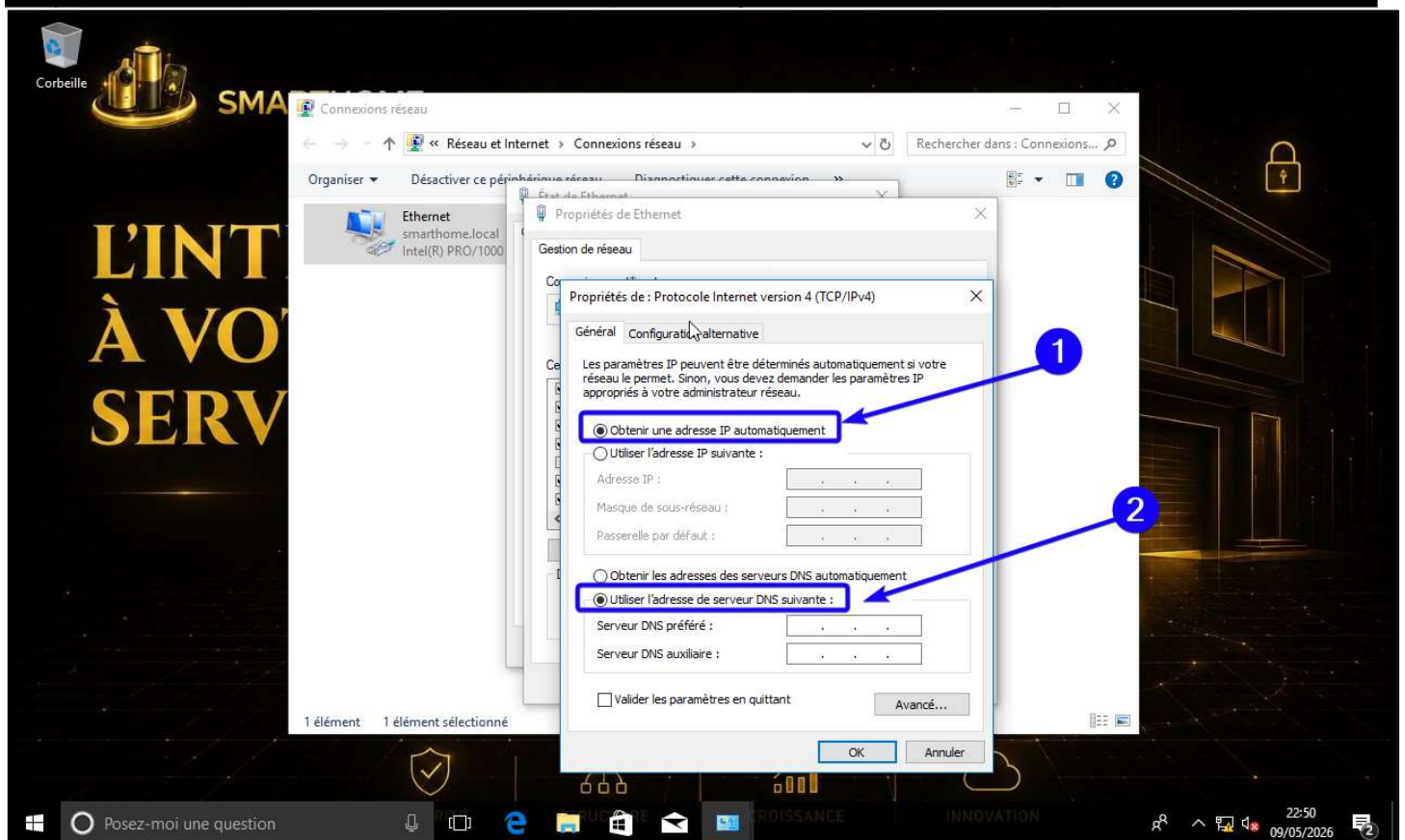
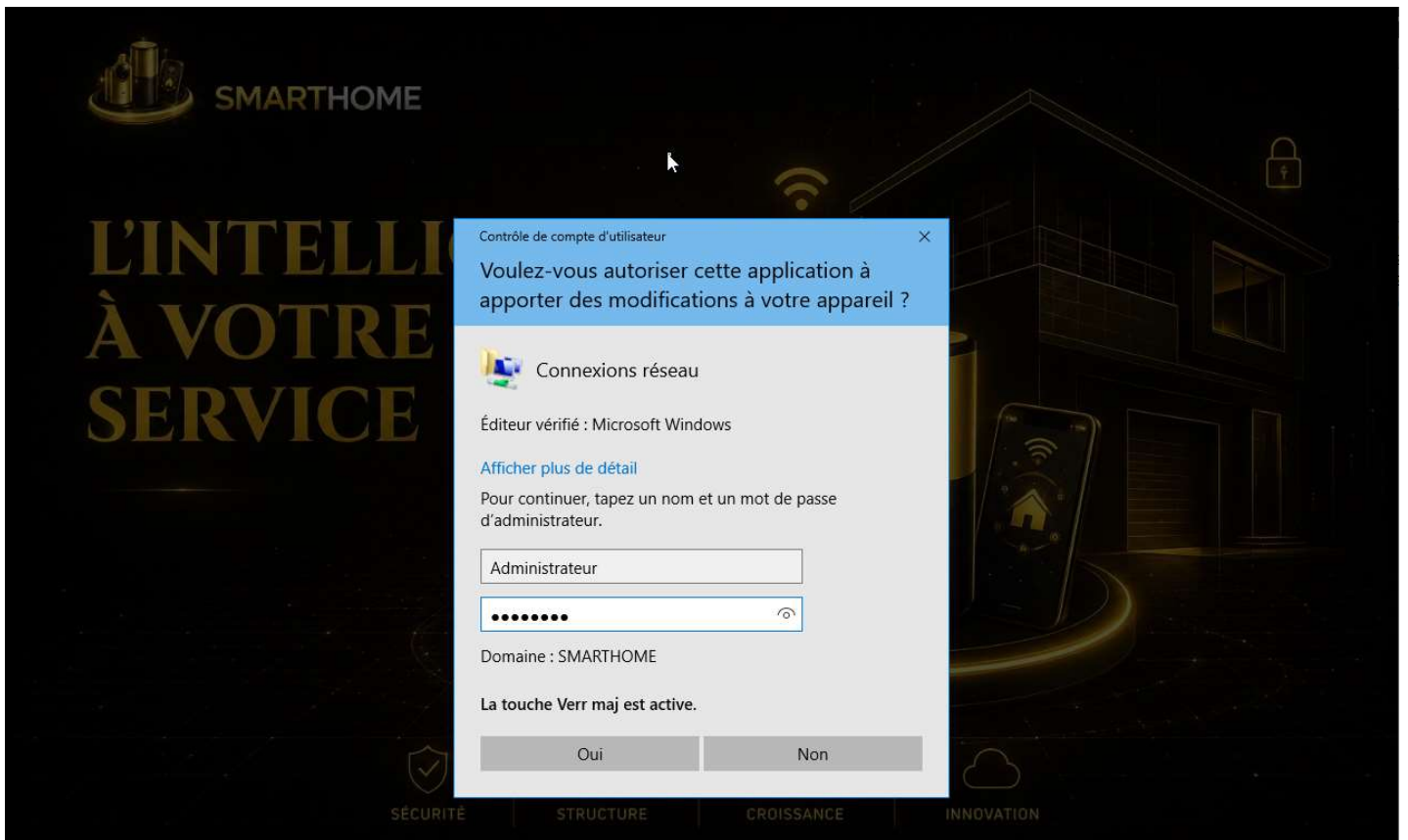
Nom d'option	Fournisseur	Valeur	Nom de la stratégie
003 Routeur	Standard	192.168.20.254	Aucun
006 Serveurs DNS	Standard	192.168.20.1	Aucun
015 Nom de domaine DNS	Standard	smarthome.local	Aucun

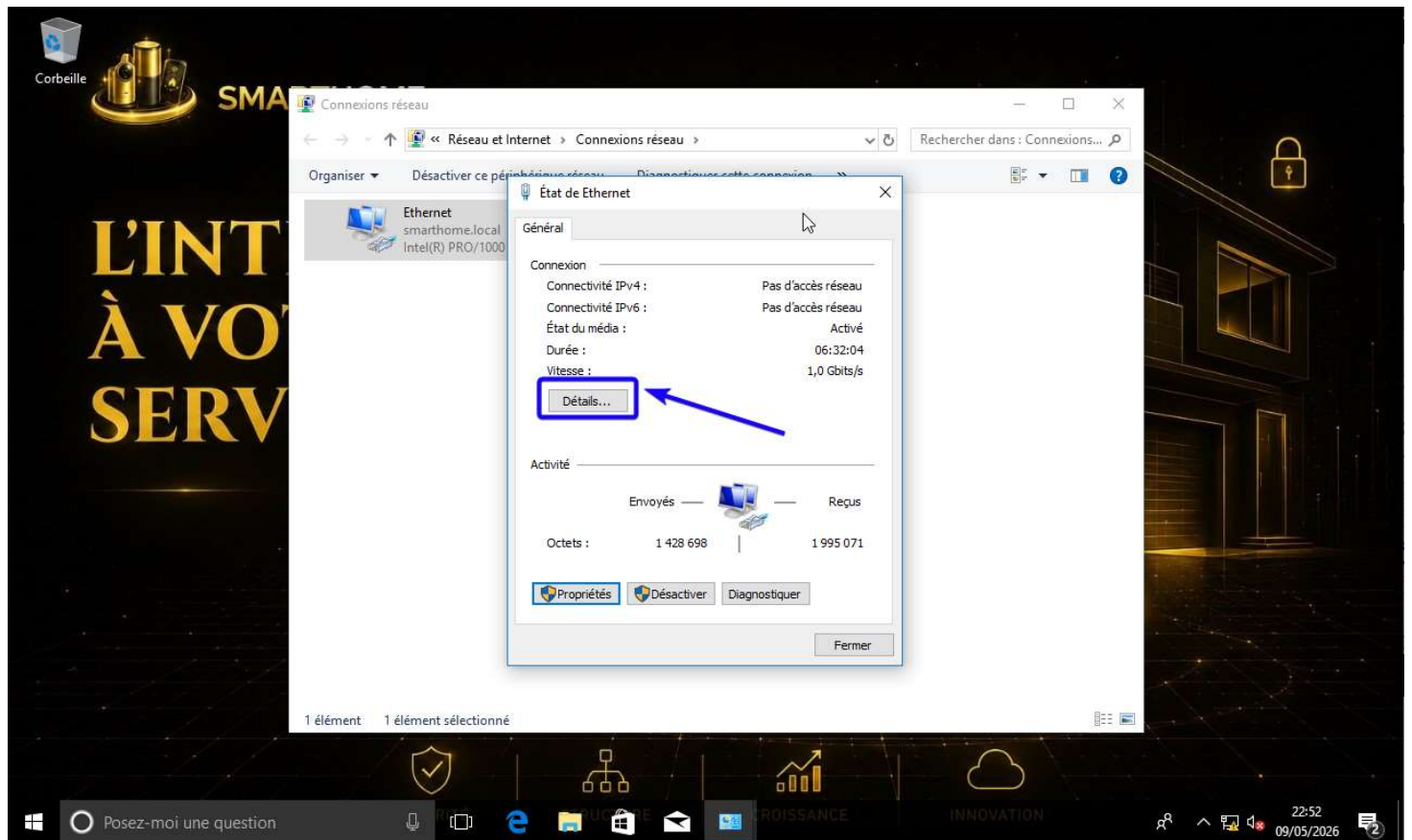
Test Validation :

Passer les machine virtuelle clientes en adressage dynamique :

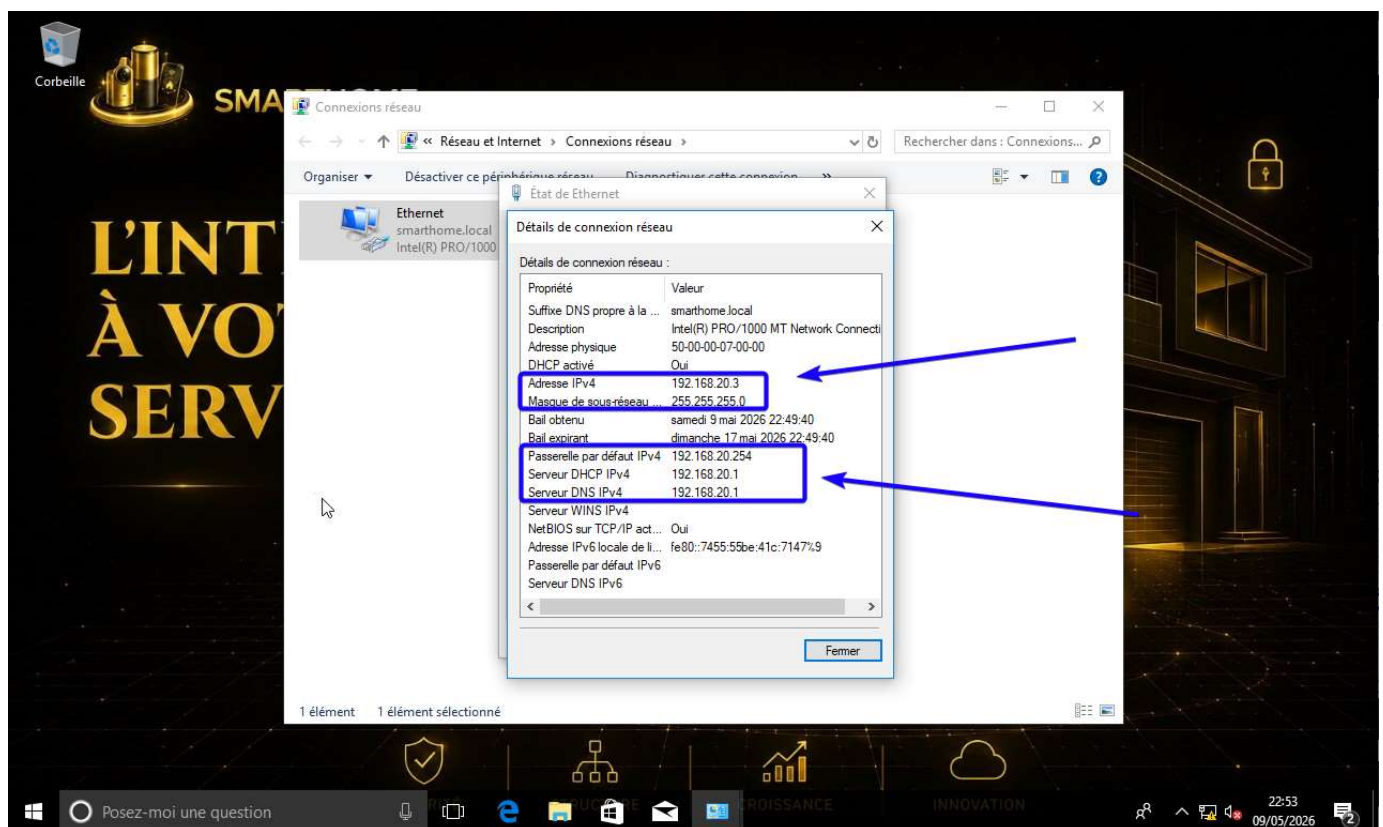
Win + R → ncpa.cpl





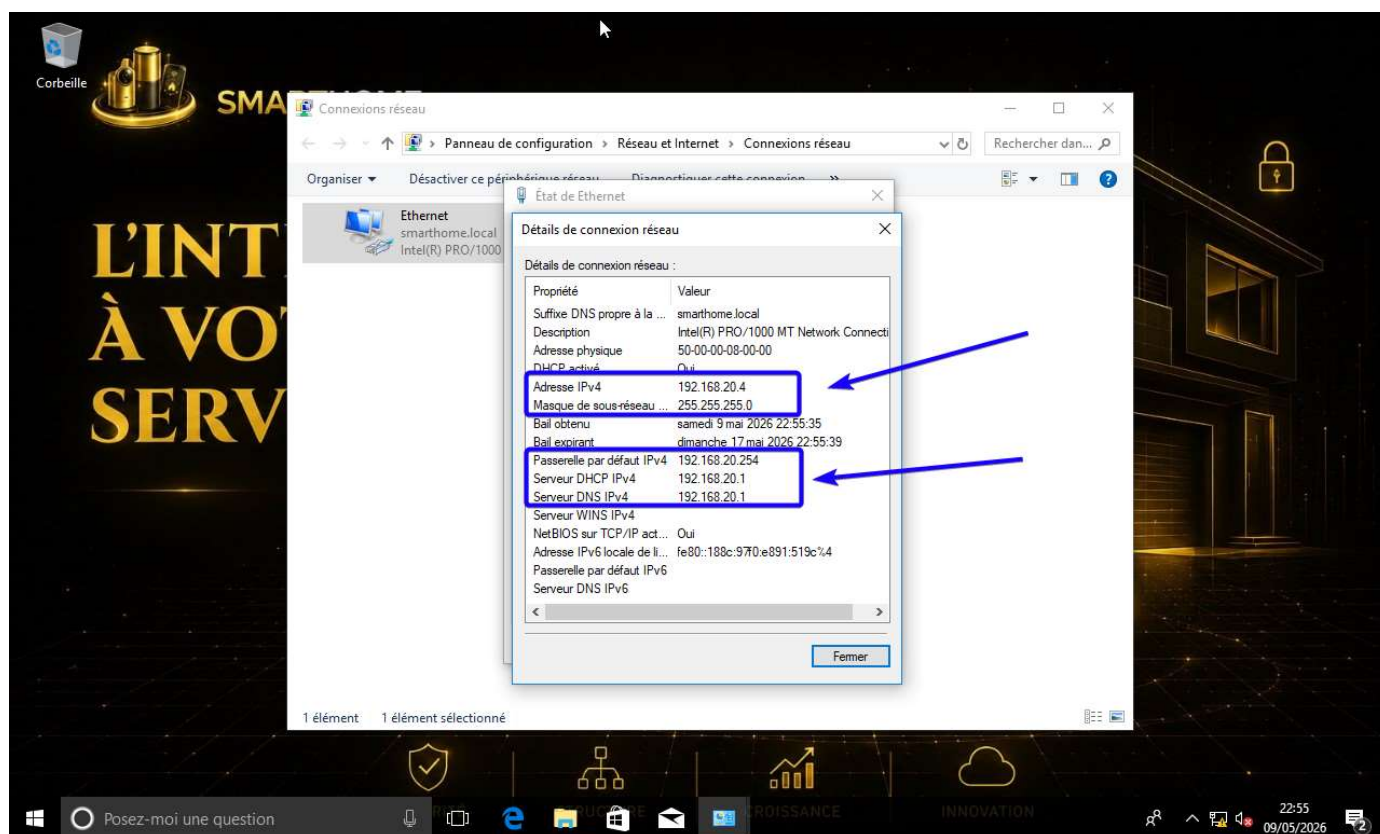


Le poste client de l'Administrateur à bien reçu une adresse IP.



Même procédure pour le poste client du directeur de SMARTHOME :

Le poste client de l'Administrateur a bien reçu une adresse IP.

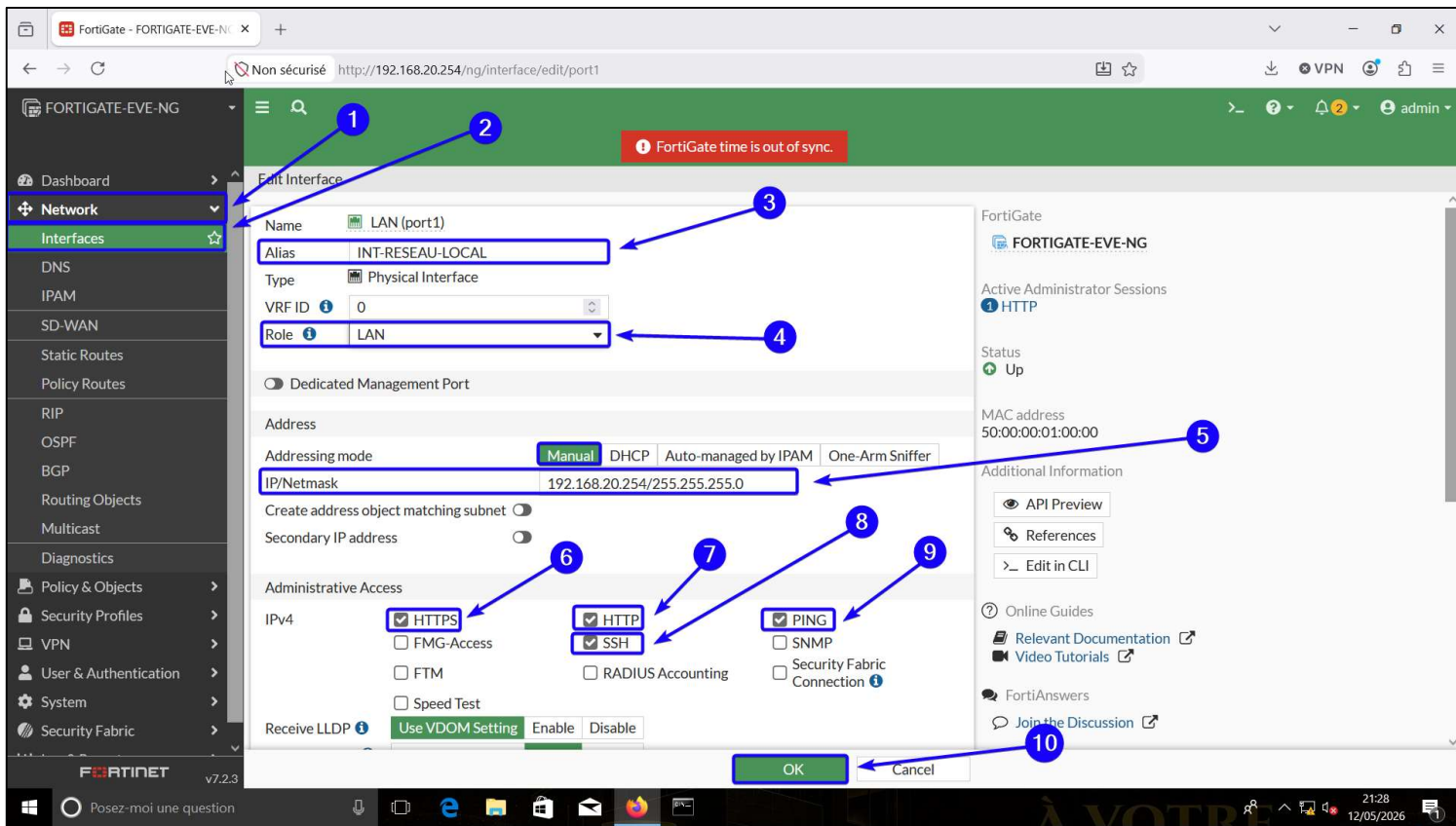


PARTIE 3 : Configuration du pare feu Fortinet et Routage :

❶ Configuration des interfaces du pare feu.

Pour configurer les interfaces du pare Fortinet on va s'appuyer du schéma réseau transmit par l'entreprise.

Configuration de l'interface du réseau locale 192.168.20.0

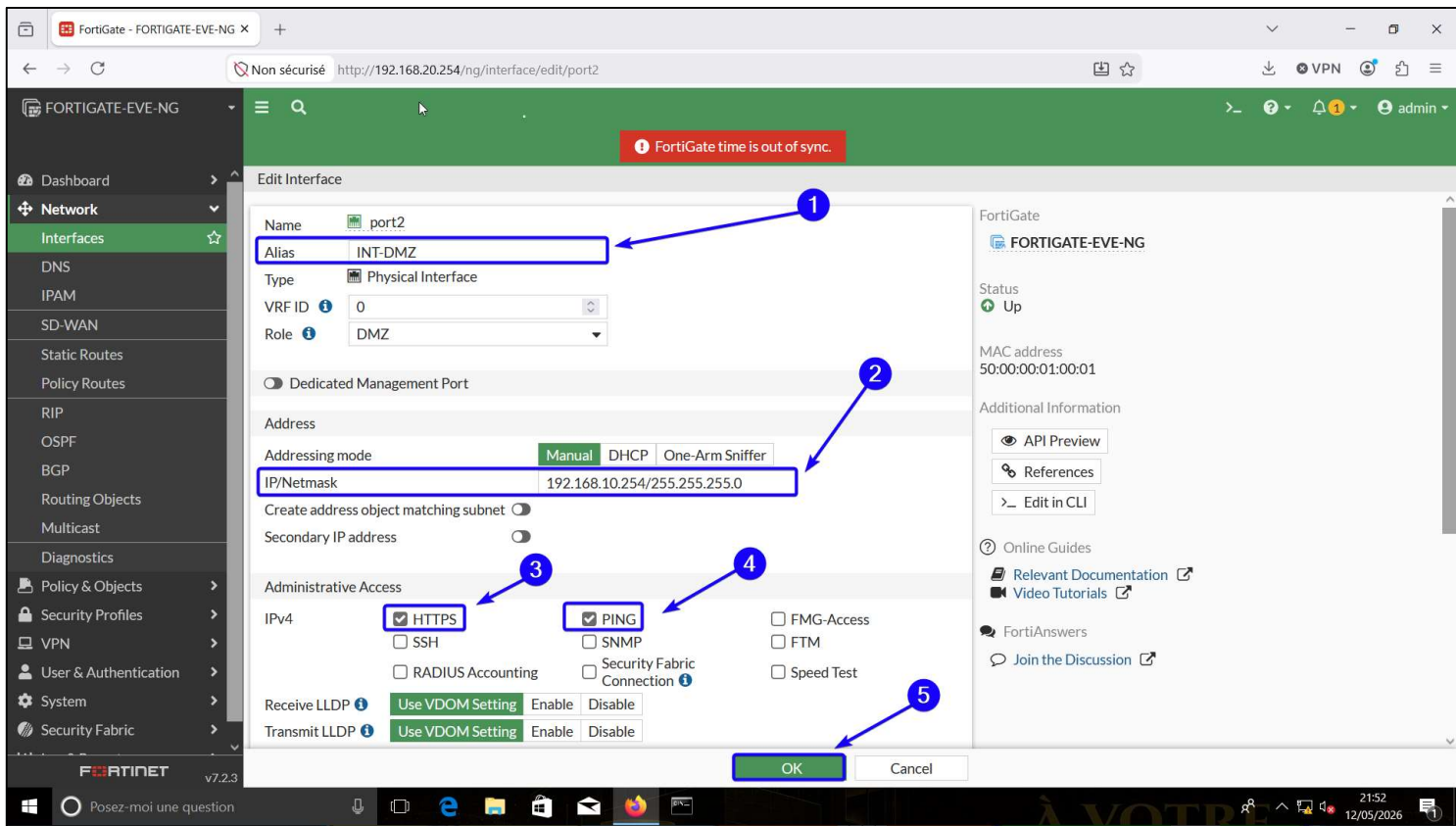


Alternative en ligne de commande :

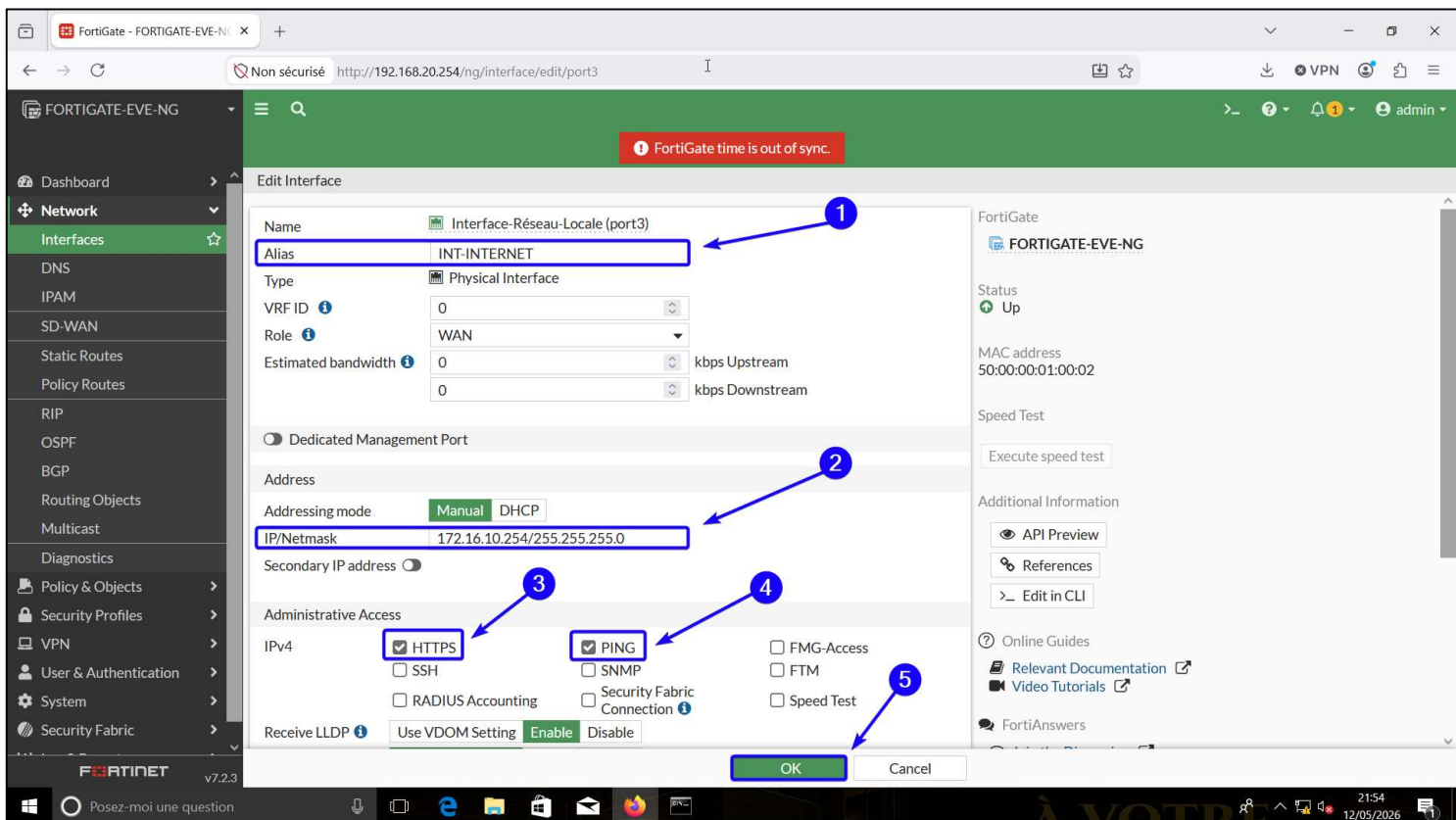
```

CLI Console (1)
FORTIGATE-EVE-NG # config system interface
FORTIGATE-EVE-NG (interface) # edit "port1"
FORTIGATE-EVE-NG (port1) # show
config system interface
  edit "port1"
    set vdom "root"
    set ip 192.168.20.254 255.255.255.0
    set allowaccess ping https ssh http
    set type physical
    set alias "INT-RESEAU-LOCAL"
    set device-identification enable
    set lldp-transmission enable
    set role lan
    set snmp-index 1
  next
end
FORTIGATE-EVE-NG (port1) #
  
```

Configuration de l'interface du réseau de la DMZ 192.168.10.0/24



Configuration de l'interface du réseau de la DMZ 172.16.10.254/24



Nos interfaces sont maintenant configurées.

FortiGate - FORTIGATE-EVE-NG x

Non sécurisé http://192.168.20.254/ng/interface

FORTIGATE-EVE-NG

Dashboard

Network

Interfaces

DNS

IPAM

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Diagnostics

Policy & Objects

Security Profiles

VPN

User & Authentication

System

Security Fabric

FortiGate VM64-KVM

FortiGate time is out of sync.

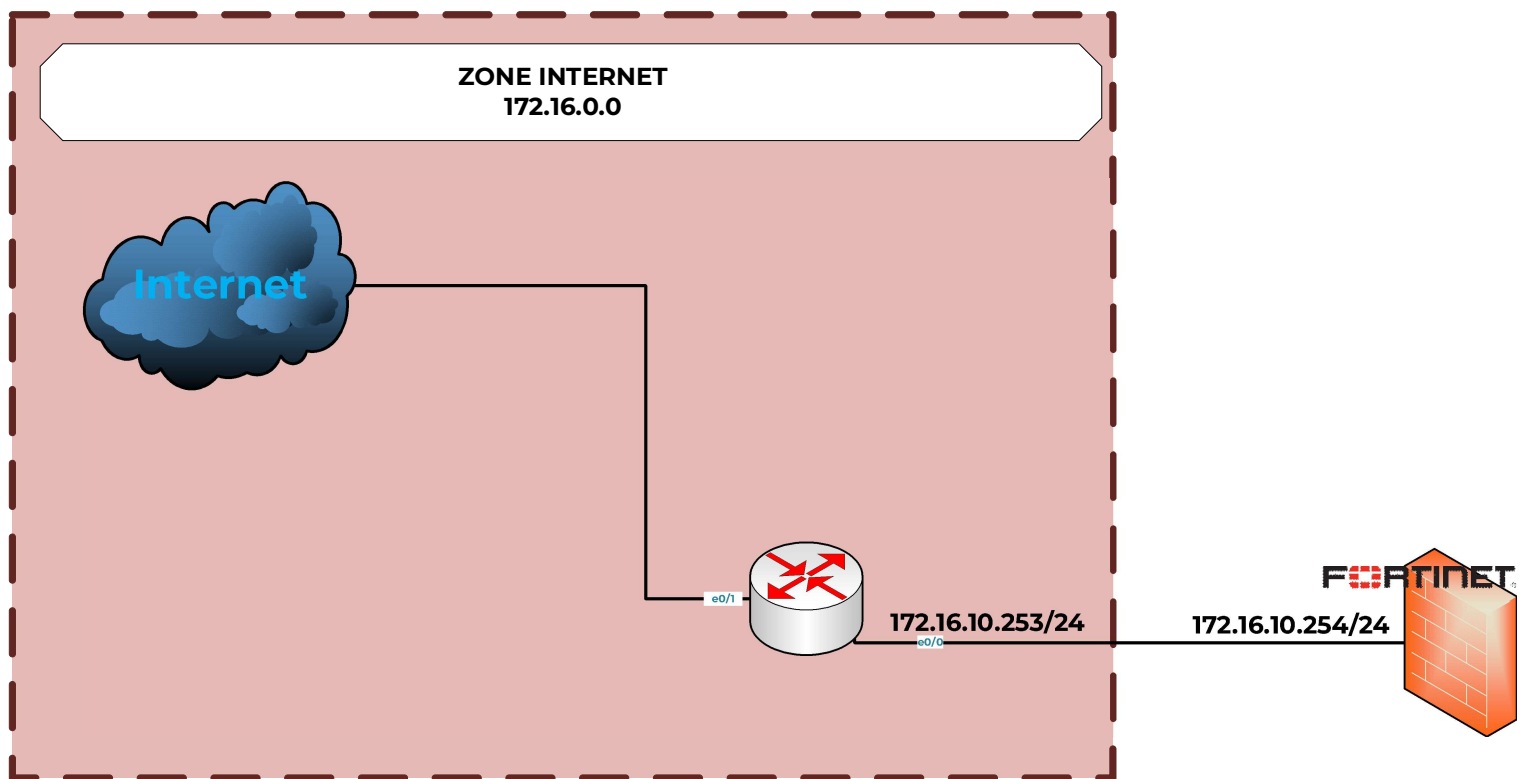
Create New Edit Delete Integrate Interface Search Group By Type

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges
802.3ad Aggregate 1						
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254
Physical Interface 3						
INT-DMZ (port2)	Physical Interface		192.168.10.254/255.255.255.0	PING HTTPS		
INT-INTERNET (port3)	Physical Interface		172.16.10.254/255.255.255.0	PING HTTPS		
INT-RESEAU-LOCAL (port1)	Physical Interface		192.168.20.254/255.255.255.0	PING HTTPS SSH HTTP		
Tunnel Interface 1						
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0			

0 Security Rating Issues

Updated: 12:56:58

2 Configuration du Routage



Configuration de la route par défaut :



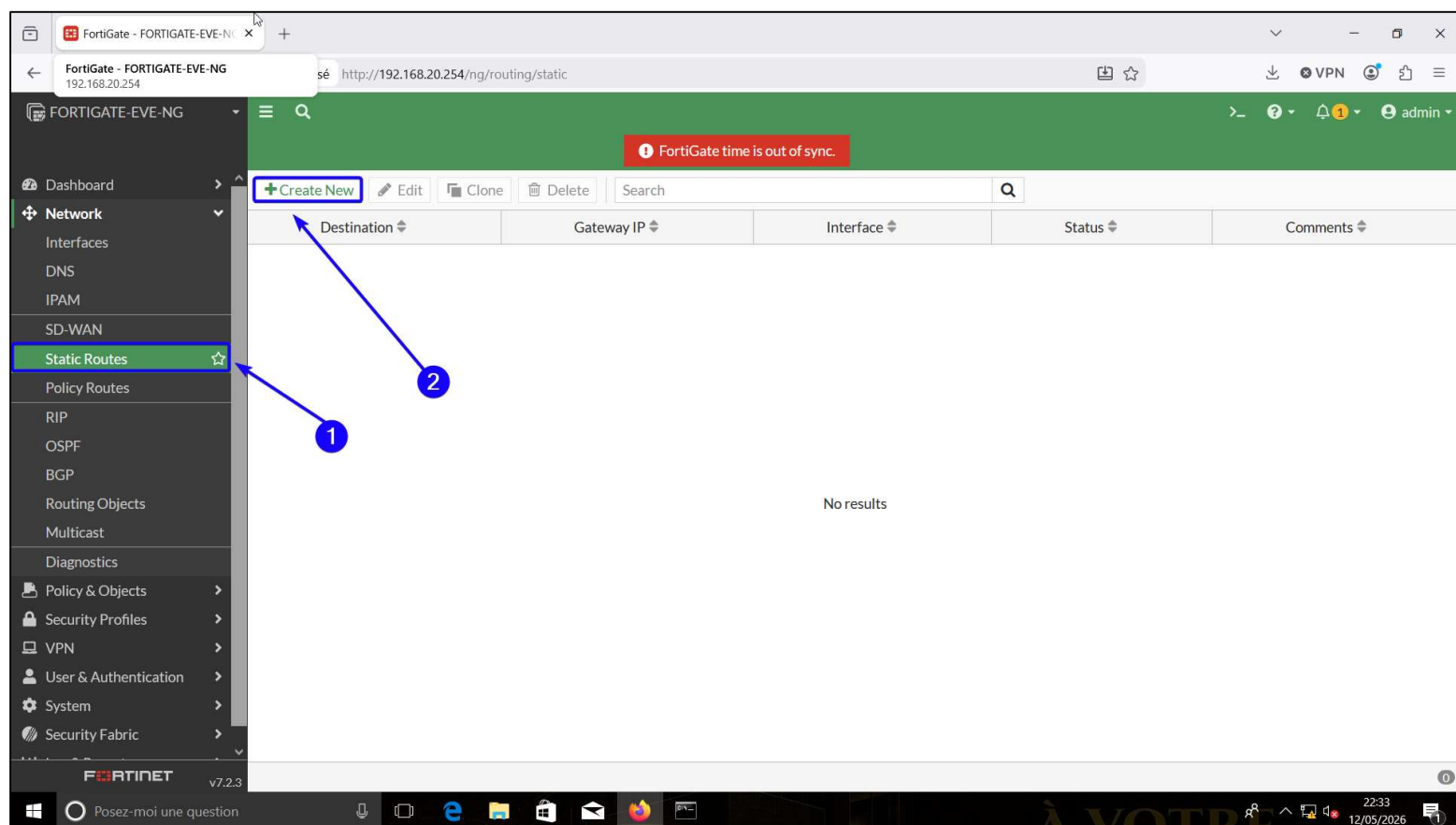
```
ip route 0.0.0.0 0.0.0.0 192.168.3.1
ip route 192.168.10.0 255.255.255.0 172.16.10.254
```

Configuration des interfaces

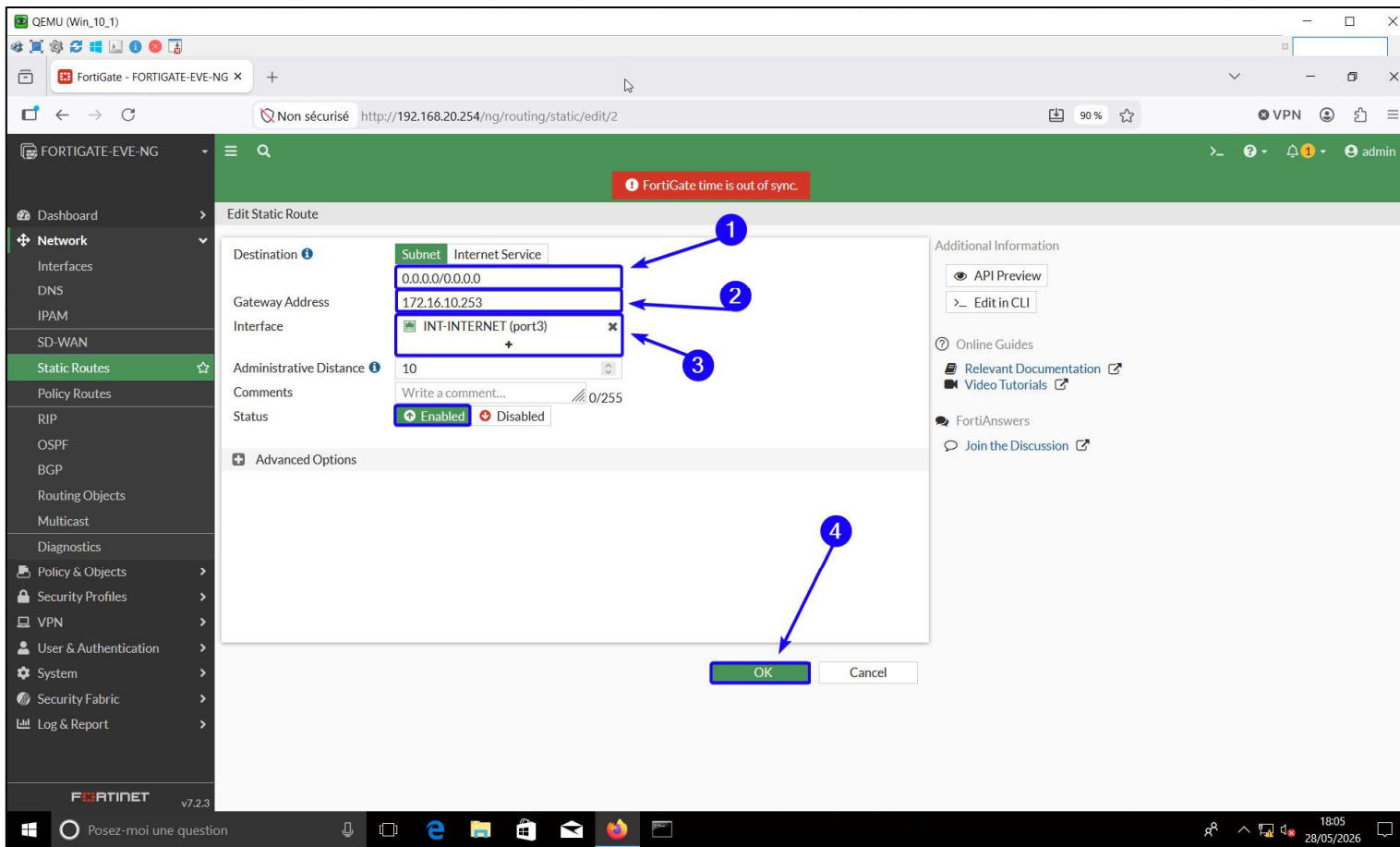
```
int eth0/0
ip address 172.16.10.253 255.255.255.0
```

```
int eth0/2
ip address 192.168.3.50 255.255.255.0
```

➊ Ajouter la passerelle du routeur TPLINK sur le Pare-Feu Fortigate.



Ajout de la route par défaut sur le pare-feu Fortigate.



Test de Validation :

Test n°1 – Routeur → Fortigate_Domicile :

```
Router#ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6 ms
```

Le routeur communique avec le **Fortigate** du réseau domestique.

Test n°2 – Routeur → PC_Gamer :

```
Router#ping 192.168.3.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/19/38 ms
```


③ Configuré le NAT Dynamique :

1. Définir les interfaces de NAT :

```
interface Ethernet0/0  
ip nat inside  
interface Ethernet0/1  
ip nat outside
```

2. Créer une liste d'accès pour autoriser le flux :

```
access-list 1 permit 192.168.10.0 0.0.0.255
```

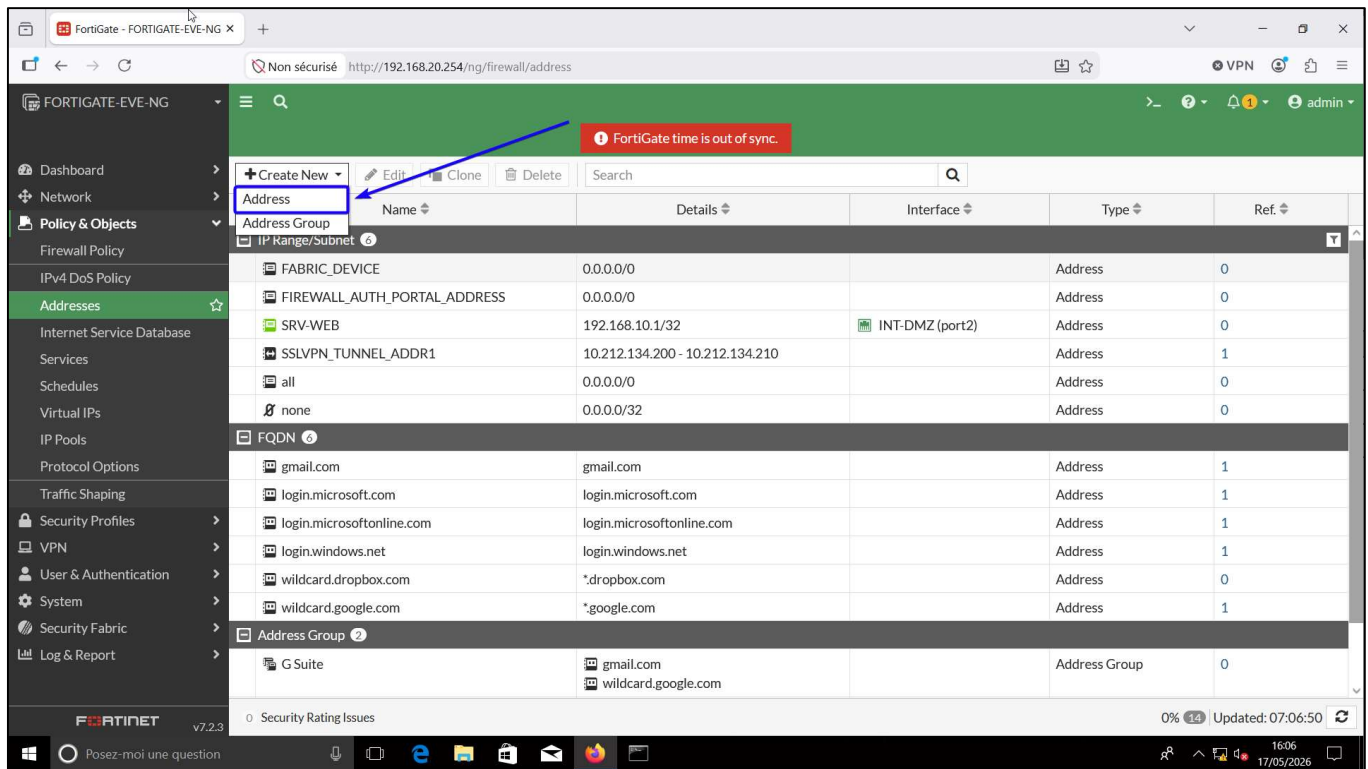
3. Activer la règle de traduction :

```
ip nat inside source list 1 interface Ethernet0/1 overload
```

4. Route Statique retour vers 192.168.10.0

```
ip route 192.168.10.0 255.255.255.0 172.16.10.254
```


④ Ajout des @IP des appareils et des différents réseaux présents dans l'entreprise :

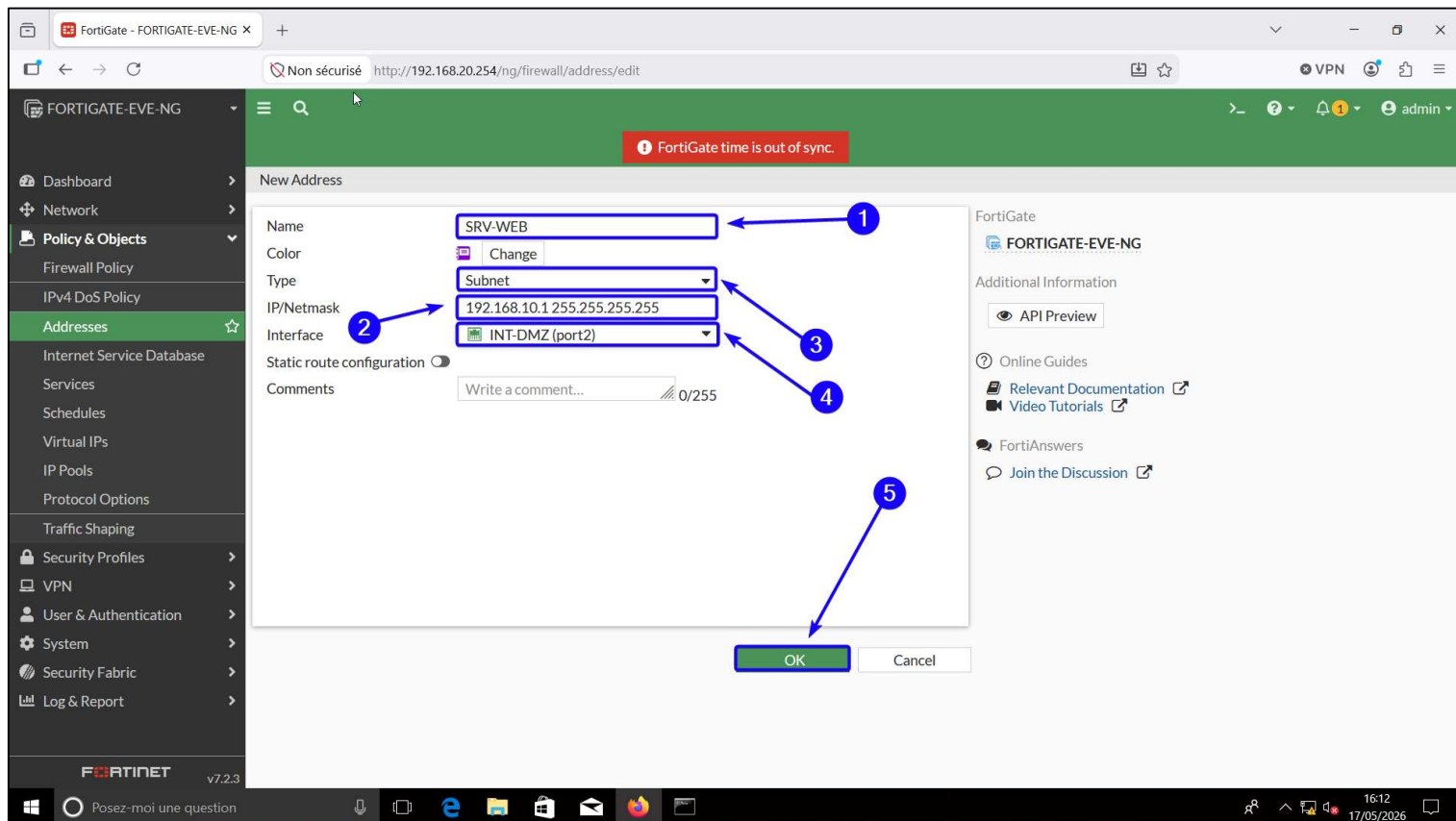


Appareils : SRV-WEB

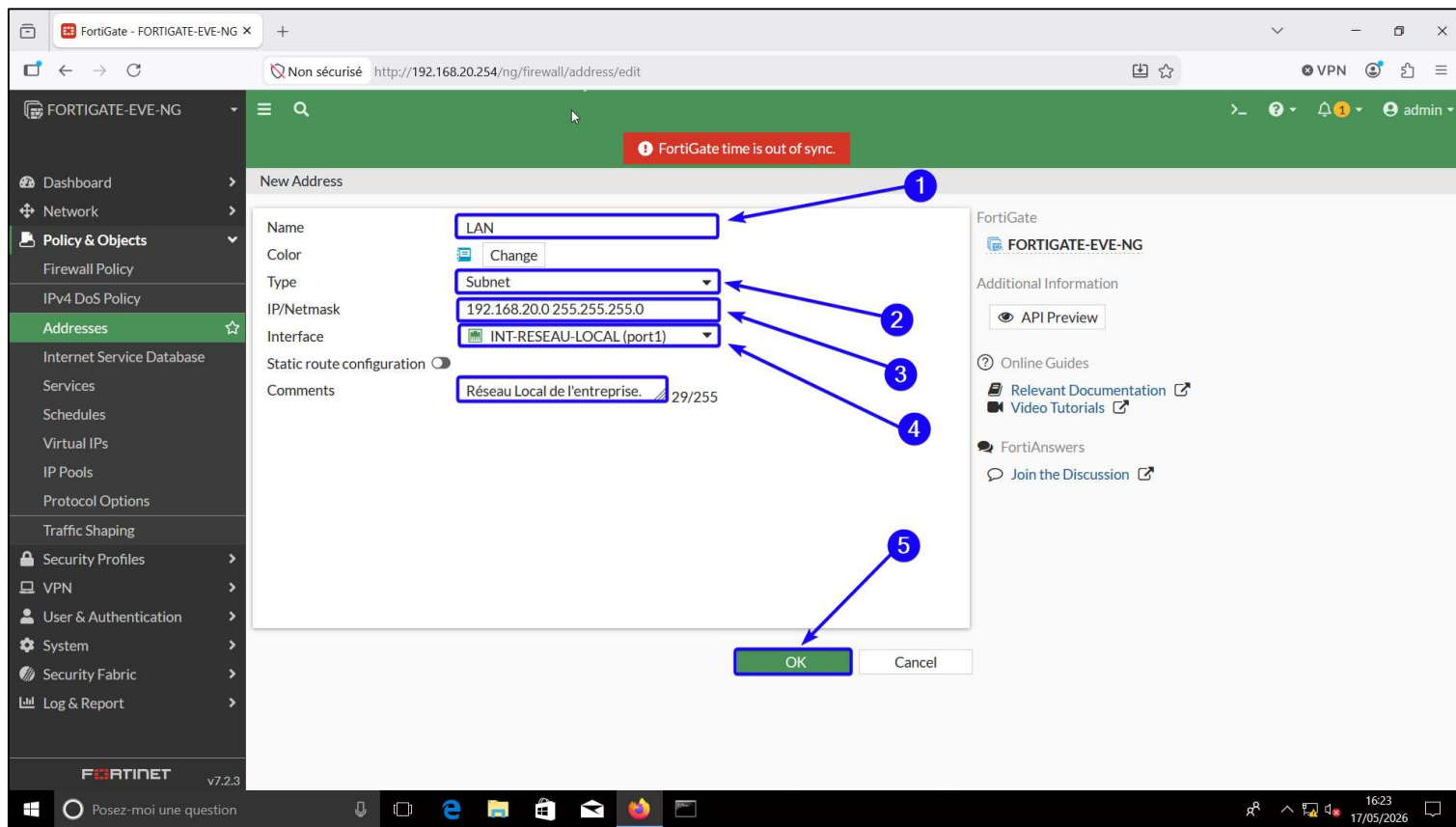
@IP : 192.168.10.1

Masque : 255.255.255.255 - /32 (Désigne une seule et unique machine)

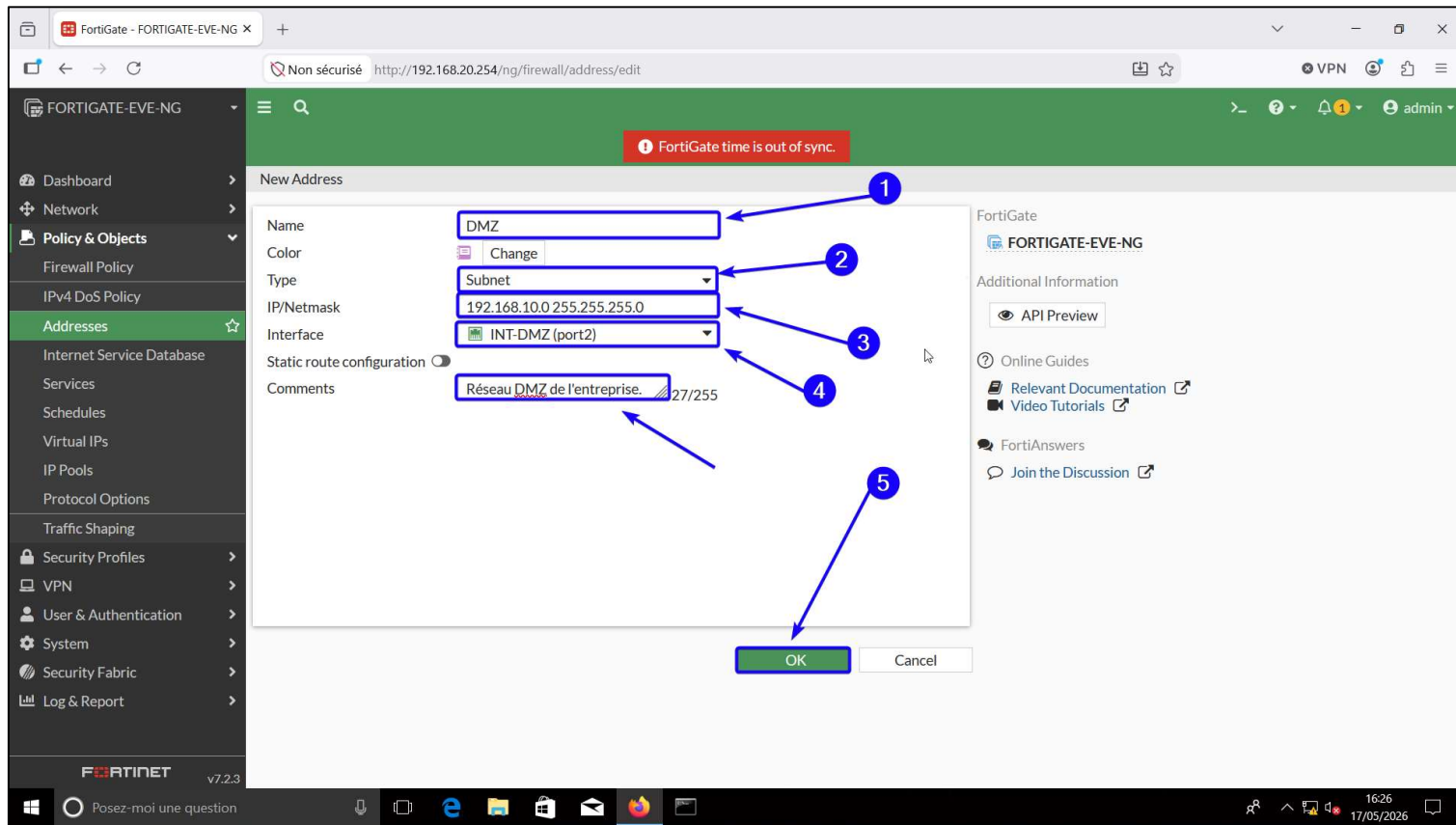
Interface : PORT2 – INT-DMZ



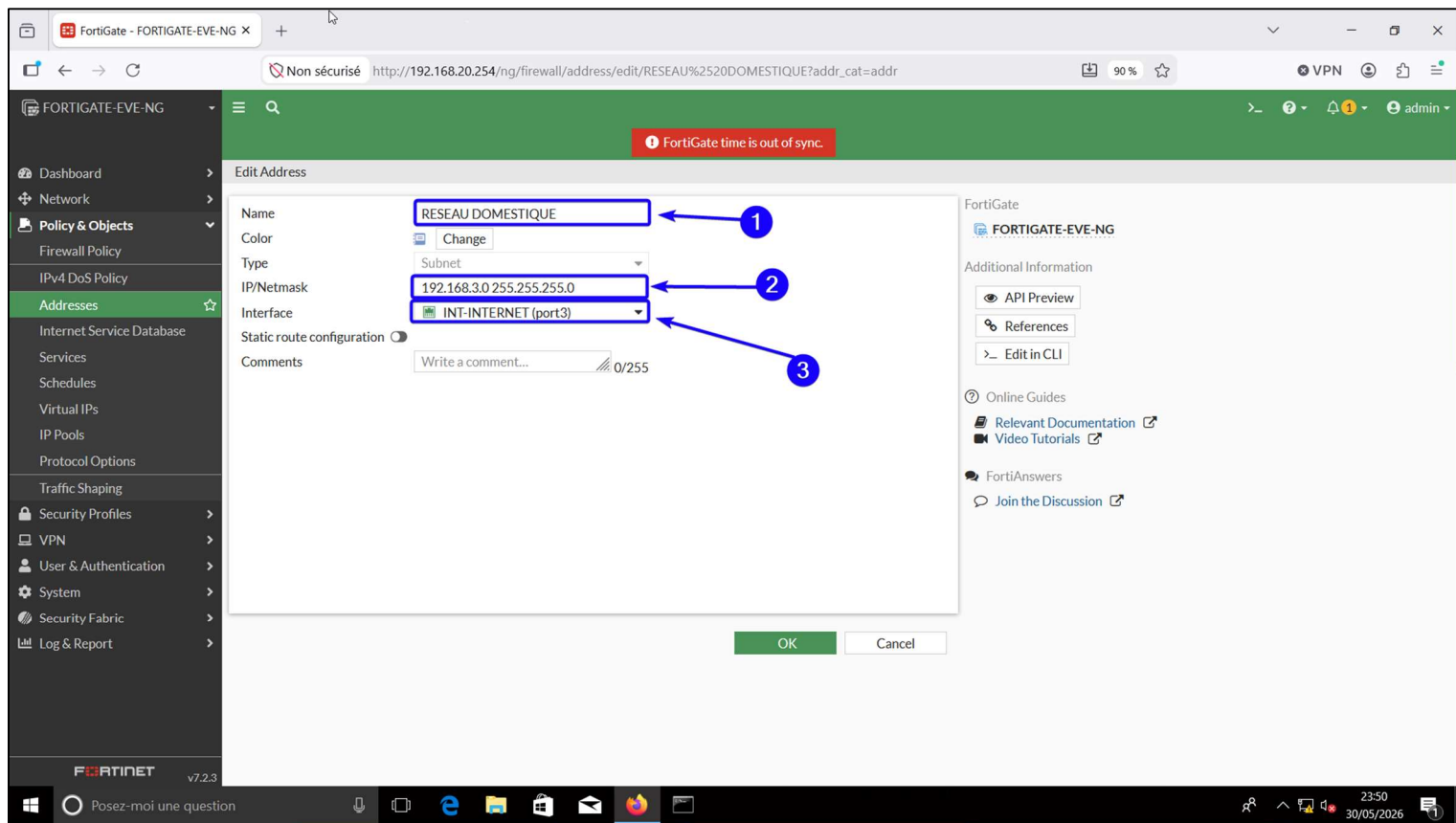
Réseau : LAN
@IP : 192.168.20.0
Masque : 255.255.255.0 - /24
Interface : PORT1 – INT-RESEAU-LOCAL



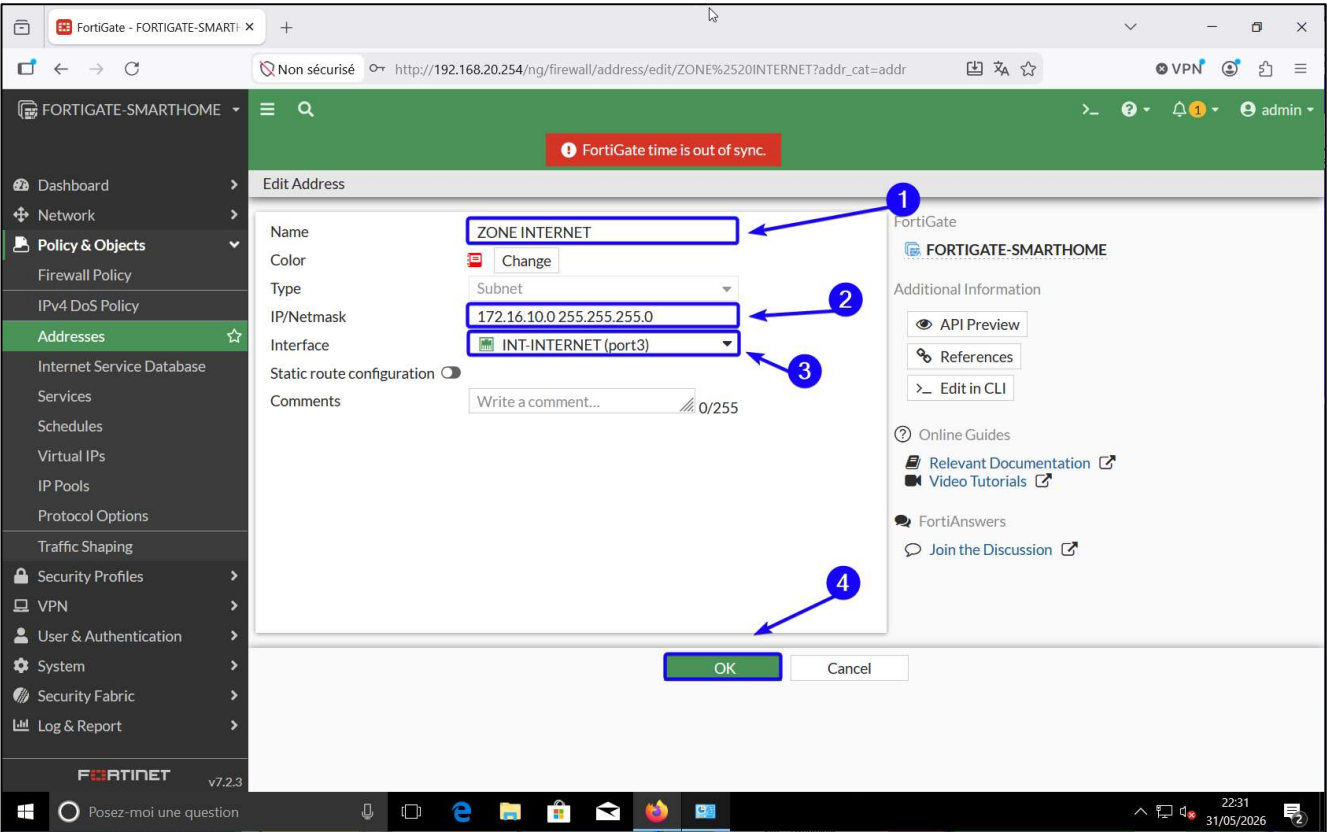
Réseau : DMZ
@IP : 192.168.10.0
Masque : 255.255.255.0 - /24
Interface : PORT2 – INT-DMZ



Réseau : DOMESTIQUE
@IP : 192.168.3.0
Masque : 255.255.255.0 - /24
Interface : PORT3 – INT-INTERNET



Réseau : ZONE INTERNET
@IP : 172.16.10.0
Masque : 255.255.255.0 - /24
Interface : PORT3 – INT-INTERNET



Vue d'ensemble :

FortiGate - FORTIGATE-SMARTHOME

Non sécurisé http://192.168.20.254/ng/firewall/address

FortiGate time is out of sync.

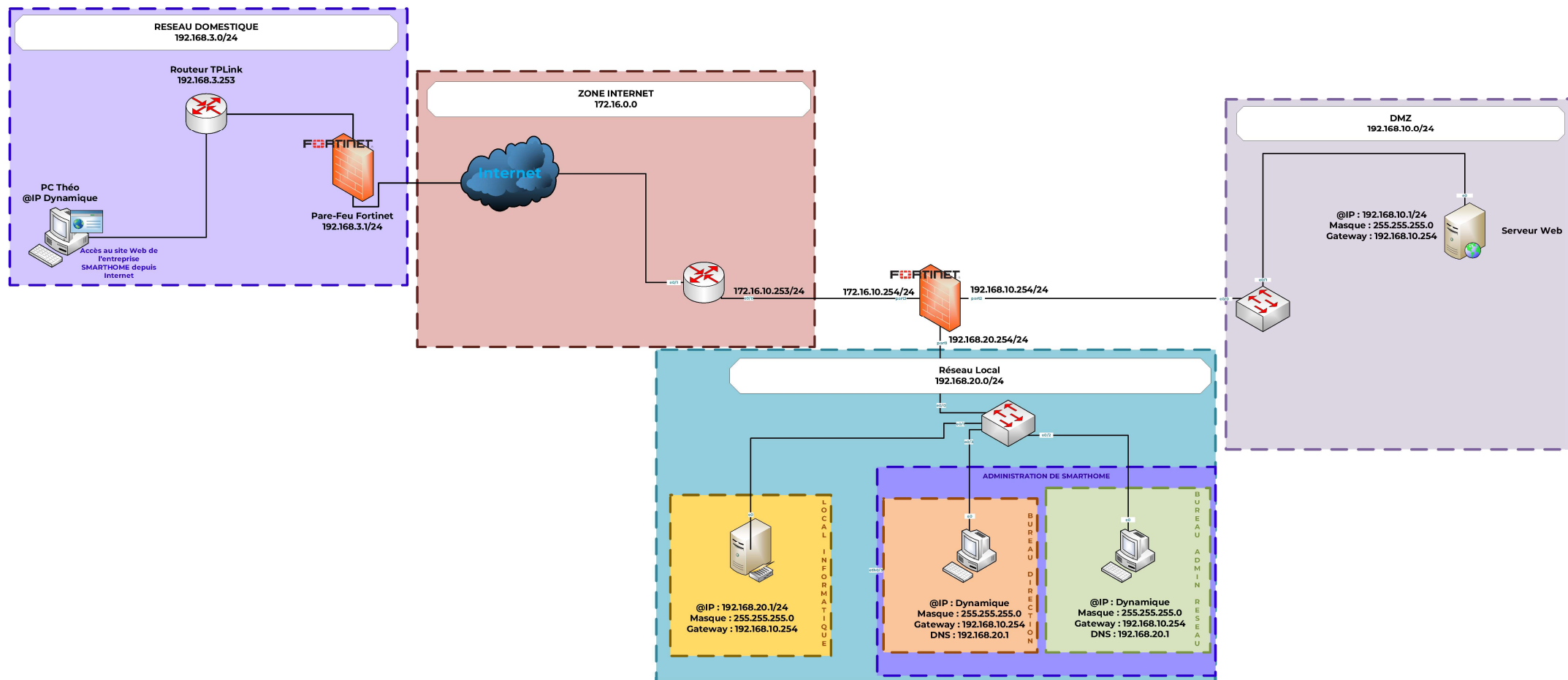
Create New Edit Clone Delete Search

Name	Details	Interface	Type	Ref.
IP Range/Subnet 10				
DMZ	192.168.10.0/24	INT-DMZ (port2)	Address	1
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
LAN	192.168.20.0/24	INT-RESEAU-LOCAL (port1)	Address	1
RESEAU DOMESTIQUE	192.168.3.0/24	INT-INTERNET (port3)	Address	3
SRV-WEB	192.168.10.1/32	INT-DMZ (port2)	Address	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	1
ZONE INTERNET	172.16.10.0/24	INT-INTERNET (port3)	Address	0
all	0.0.0.0/0		Address	1
none	0.0.0.0/32		Address	0
FQDN 6				
gmail.com	gmail.com		Address	1
login.microsoft.com	login.microsoft.com		Address	1
login.microsoftonline.com	login.microsoftonline.com		Address	1
login.windows.net	login.windows.net		Address	1

Security Rating Issues 0% 18 Updated: 08:27:00



Schéma Réseau – Bilan de l'avancée de la maquette :



PROJET PERSONNEL – Théo BRETON

PROJET – RESEAUX/SYSTEME : PROJET N°5 : RADIUS DANS UN ENVIRONNEMENT PROFESSIONNEL

5 Configuration des règles de filtrage :

N° de règle	Nom	Adresse Source	Interface d'entrée	Interface de sortie	Adresse destination	Service	NAT	Action
1	WAN à DMZ	192.168.3.0/24	Port3 (WAN)	Port2 (DMZ)	192.168.10.0/24	HTTP ; HTTPS ; ALL_ICMP	Désactiver	ACCEPT
2	DMZ à ZONE INTERNET	192.168.10.0/24	Port 2 (DMZ)	Port3 (WAN)	172.16.10.0/24	ALL_ICMP ; HTTP ; HTTPS	Désactiver	ACCEPT
3	Bloquer WAN à LAN	192.168.3.0/24	Port3 (WAN)	Port1 (LAN)	192.168.20.0/24	ALL	Désactiver	DENY



Résumé :

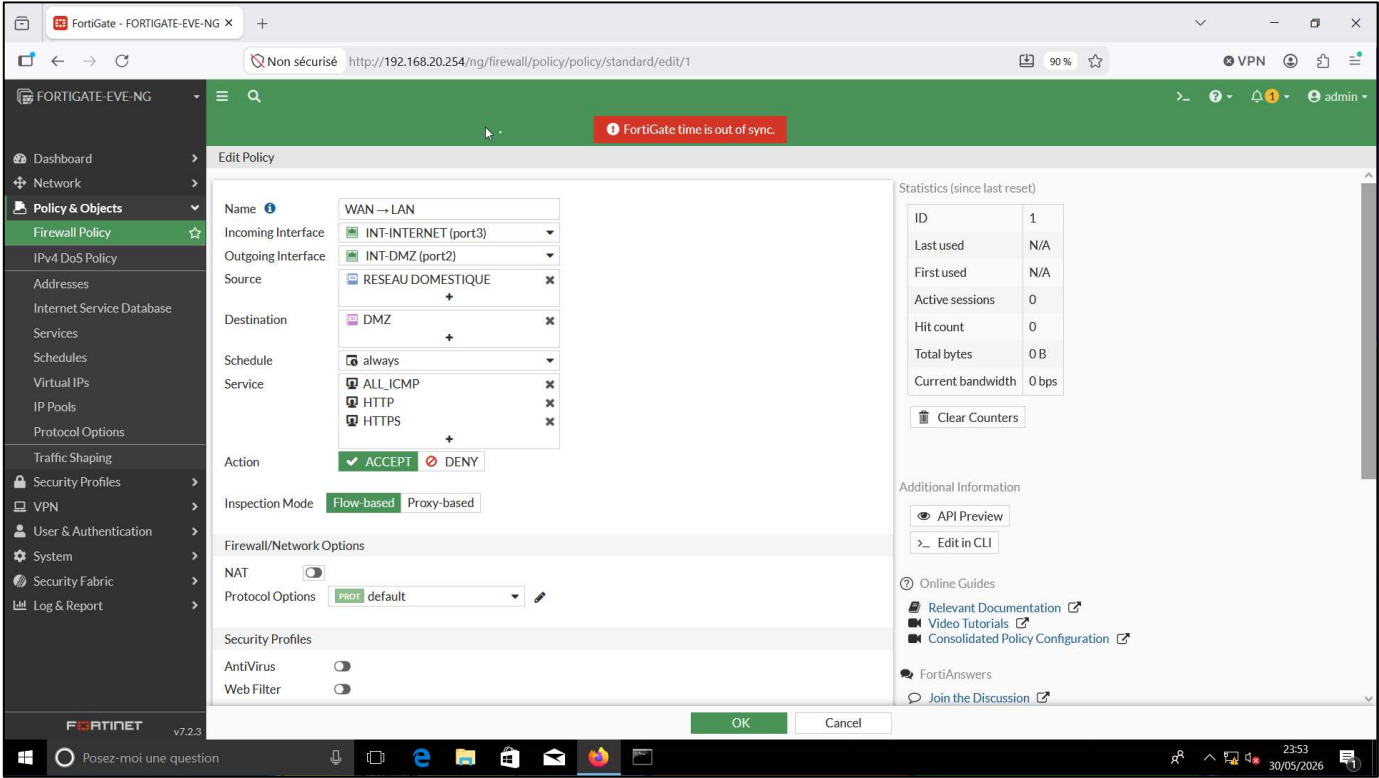
Ajout des règles de filtrage sur le pare feu :

1ère règle de Filtrage :

Rôle de la règle de filtrage :

Cette a pour but d'autoriser le trafic venant du WAN d'accéder à la DMZ

N° de règle	1
Nom	WAN à DMZ
Adresse Source	192.168.3.0/24
Interface d'entrée	Port3 (WAN)
Interface de sortie	Port2 (DMZ)
Adresse destination	192.168.10.0/24
Service	HTTP ; HTTPS ; ALL_ICMP
NAT	Désactiver
Action	ACCEPT

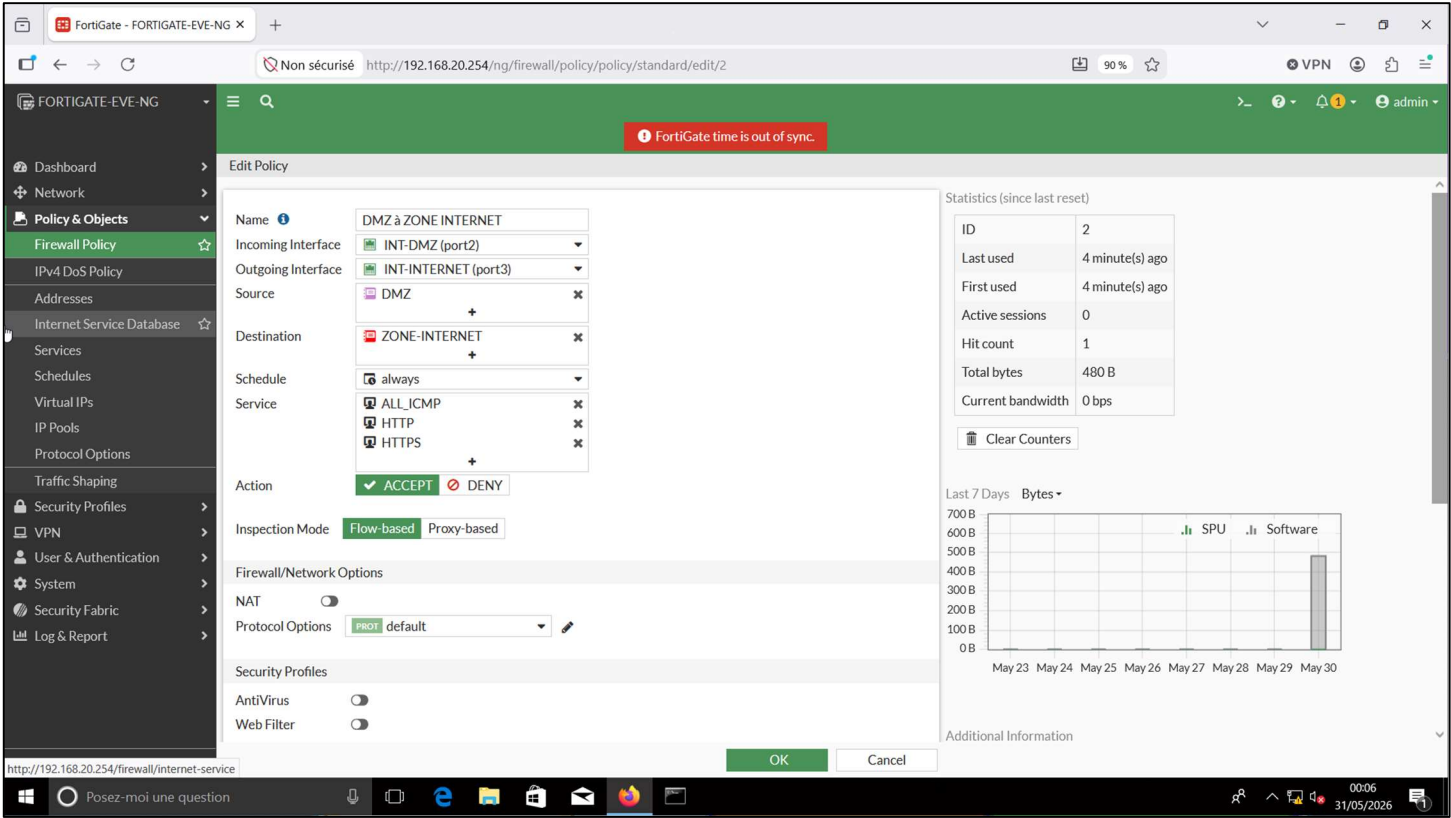


2ème règle de Filtrage :

Rôle de la règle de filtrage :

Isoler le réseau local de l'entreprise de la DMZ pour le protéger du trafic venant du WAN.

N° de règle	2
Nom	DMZ à ZONE INTERNET
Adresse Source	192.168.10.0/24
Interface d'entrée	Port 2 (DMZ)
Interface de sortie	Port3 (WAN)
Adresse destination	172.16.10.0/24
Service	ALL_ICMP ; HTTP ; HTTPS
NAT	Désactiver
Action	ACCEPT

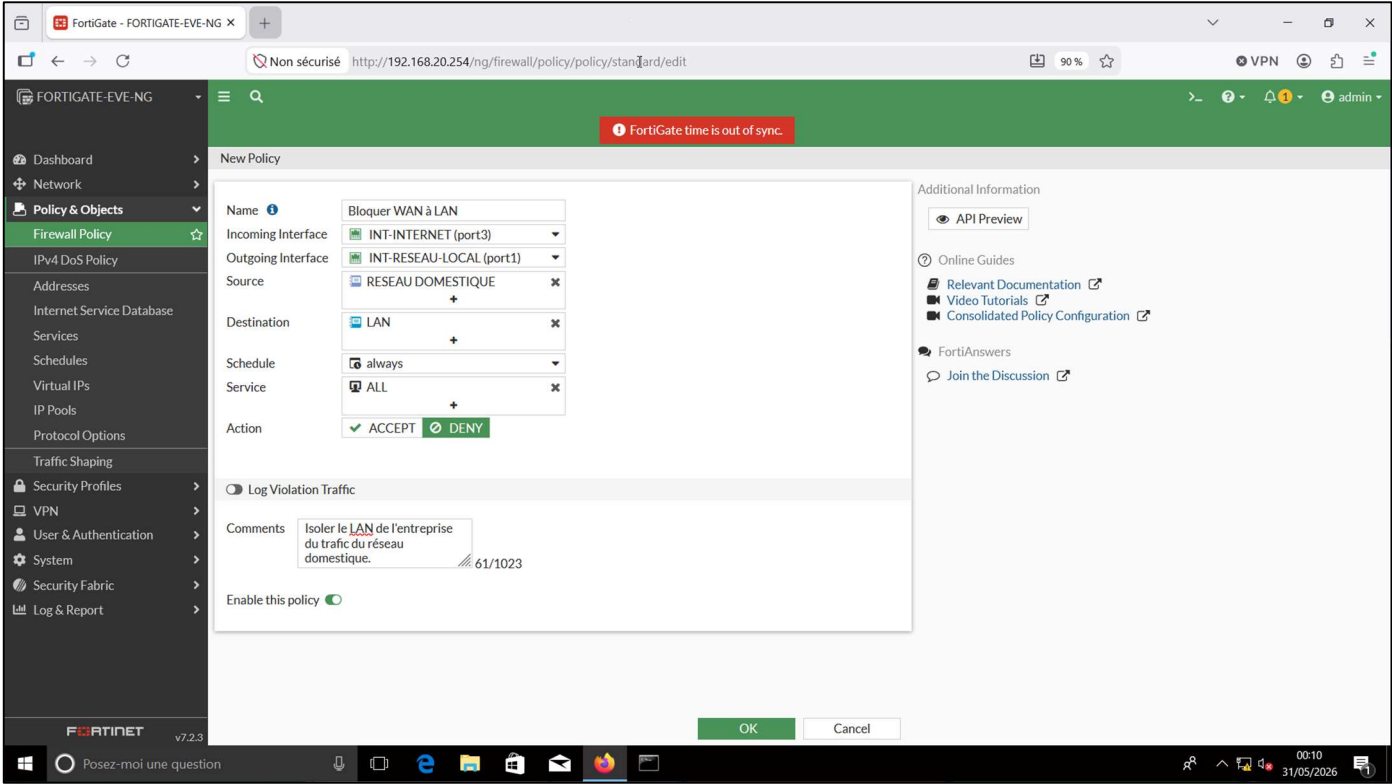


3ème règle de Filtrage :

Rôle de la règle de filtrage :

Isoler le réseau local de l'entreprise de la DMZ pour le protéger du trafic venant du WAN.

N° de règle	3
Nom	Bloquer WAN à LAN
Adresse Source	192.168.3.0/24
Interface d'entrée	Port3 (WAN)
Interface de sortie	Port1 (LAN)
Adresse destination	192.168.20.0/24
Service	ALL
NAT	Désactiver
Action	DENY



Vue d'ensemble :

FortiGate - FORTIGATE-SMARTHOME

Non sécurisé

http://192.168.20.254/ng/firewall/policy/policy/standard?showInList={"q_origin_key":3}

VPN

admin

FORTIGATE-SMARTHOME

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

FortiGate time is out of sync.

Create New

Edit

Delete

Policy Lookup

Search

Export

Interface Pair View

By Sequence

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
INT-DMZ (port2) → INT-INTERNET (port3)							
DMZ à ZONE INTERNET	DMZ	ZONE INTERNET	always	ALL_ICMP HTTP HTTPS	ACCEPT	Disabled	SSL no-inspection
INT-INTERNET (port3) → INT-DMZ (port2)							
WAN → LAN	RESEAU DOMESTIQUE	DMZ	always	ALL_ICMP HTTP HTTPS	ACCEPT	Disabled	SSL no-inspection
INT-INTERNET (port3) → INT-RESEAU-LOCAL (port1)							
Bloquer WAN à LAN	RESEAU DOMESTIQUE	LAN	always	ALL	DENY		
Implicit							
Implicit Deny	all	all	always	ALL	DENY		

0 Security Rating Issues

Updated: 13:37:09

Test de Validation :

Test n°1 – ServerWeb → Fortigate_Domicile :

```
C:\Users\Administrateur>ping 192.168.3.1

Envoi d'une requête 'Ping' 192.168.3.1 avec 32 octets de données :
Réponse de 192.168.3.1 : octets=32 temps=19 ms TTL=253
Réponse de 192.168.3.1 : octets=32 temps=5 ms TTL=253
Réponse de 192.168.3.1 : octets=32 temps=6 ms TTL=253
Réponse de 192.168.3.1 : octets=32 temps=15 ms TTL=253

Statistiques Ping pour 192.168.3.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 5ms, Maximum = 19ms, Moyenne = 11ms
```

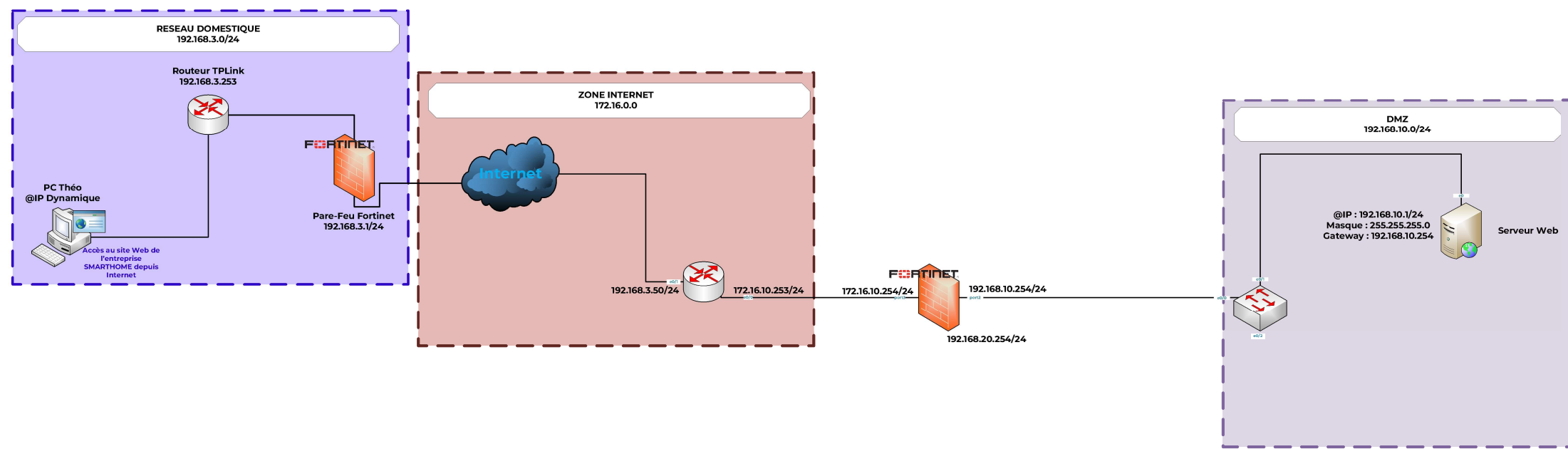
Test n°1 – ServerWeb→ Routeur_TPLink_Domicile :

```
C:\Users\Administrateur>ping 192.168.3.253

Envoi d'une requête 'Ping' 192.168.3.253 avec 32 octets de données :
Réponse de 192.168.3.253 : octets=32 temps=7 ms TTL=62
Réponse de 192.168.3.253 : octets=32 temps=5 ms TTL=62
Réponse de 192.168.3.253 : octets=32 temps=7 ms TTL=62
Réponse de 192.168.3.253 : octets=32 temps=12 ms TTL=62

Statistiques Ping pour 192.168.3.253:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 5ms, Maximum = 12ms, Moyenne = 7ms
```


⑥ Etablir la communication entre le PCThéo et ServeurWeb de SMARTHOME



Etablissement des routes sur les différents équipements de niveau 3, du RESEAU DOMESTIQUE :

Comme on n'a pas de redirection DNS on va modifier le fichier Host de la machine physique pour faire nos tests et accéder au site depuis l'internet du réseau domestique.

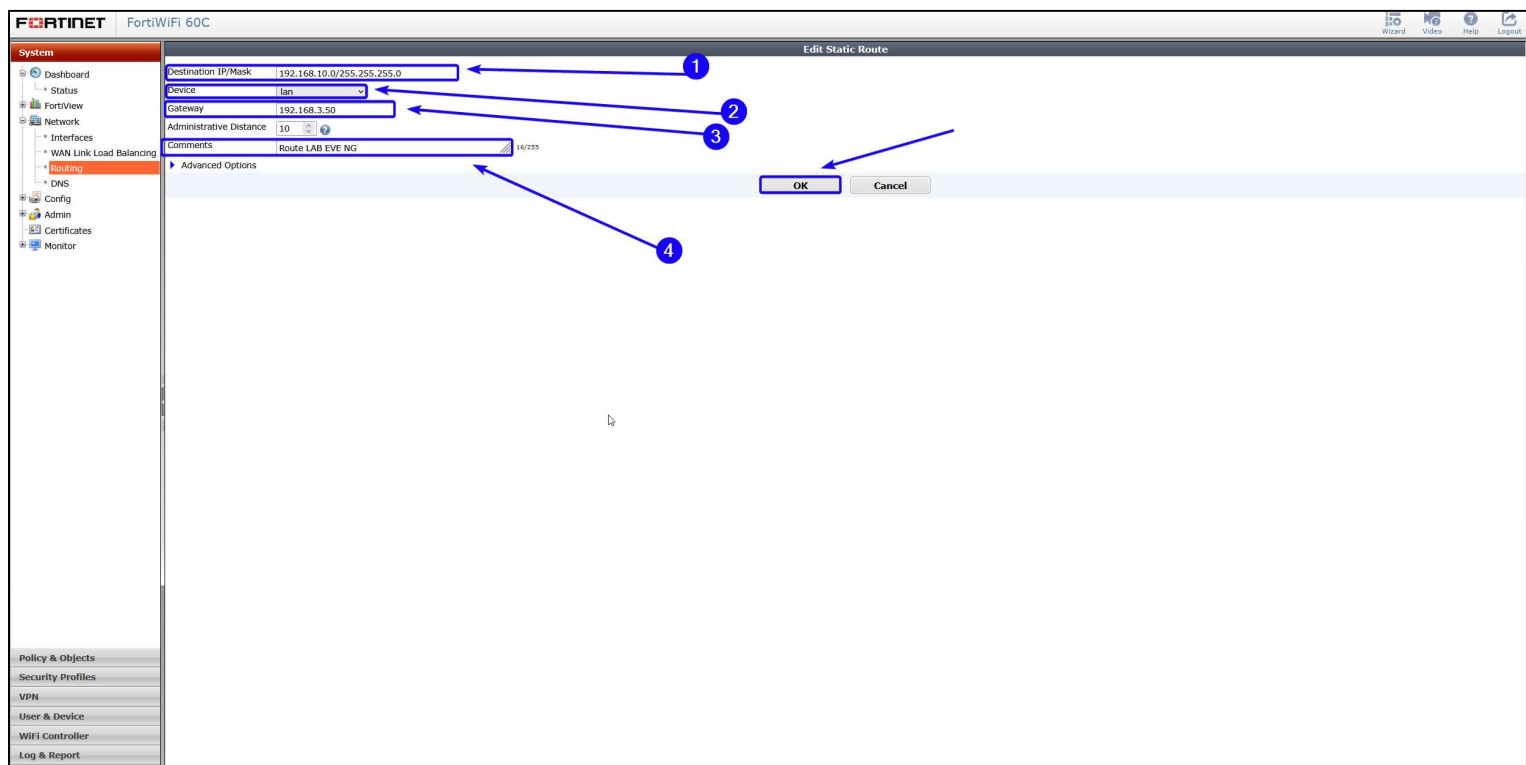
Dans : C:|Windows|System32|drivers|etc

```
hosts - Bloc-notes
Fichier Edition Format Affichage Aide
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com      # source server
#       38.25.63.10     x.acme.com         # x client host
192.168.10.1    www.smarthome.com    #srvsmarthome
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
```

PARE-FEU FORTINET SALON :



Cette route statique oriente le paquet vers l'interface du routeur virtuel Cisco du lab EVE_NG.



Règle de Pare-Feu :

SystemFortiWiFi 60C

Policy & Objects

Policy

Proxy Options

SSL Inspection

Objects

Monitor

1

2

3

4

5

6

Incoming Interface

lan

Source Address

PC GAMER THEO

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

lan

Destination Address

DMZ

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

NAT

Security Profiles

Antivirus

Web Filter

Application Control

SSL Inspection

certificate-inspection

Traffic Shaping

Shared Shaper

guarantee-100kpbs

Reverse Shaper

guarantee-100kpbs

Per-IP Shaper

Click to set...

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Comments

0/1023

Enable this policy

OK

Cancel

Security Profiles

VPN

User & Device

WiFi Controller

Log & Report

SystemFortiWiFi 60C

Create New

Edit

Delete

Policy & Objects

Policy

Proxy Options

SSL Inspection

Objects

Monitor

Seq.#	From	To	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control	SSL Inspection	Log	Count
1	lan	lan	PC GAMER THEO	DMZ	always	ALL	ACCEPT	Disable	None	None	None	None	UTH	0 Packets / 0 B
2	lan	any	all	all	always	ALL	ACCEPT	Enable					UTH	22,047,093 Packets / 19.44 GB
3	ssl.root (SSL VPN interface)	lan	SSLVPN_TUNNEL_ADDR1	LAN_192.168.3.0	always	ALL	ACCEPT	Enable					UTH	43,261 Packets / 32.48 MB
4	any	any	all	all	always	ALL	DENY						Disable	

Security Profiles

VPN

User & Device

WiFi Controller

Log & Report

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

ROUTEUR TP-LINK SALON :



tp-link

BE6500 Dual-Band Wi-Fi 7 Router

Français

Chercher

Identifiant TP-Link

Se déconnecter

Cartographie du réseau

Internet

Wi-Fi

Soins à domicile

Avancé

Configuration rapide

Réseau

Etat

Internet

LAN

IPTV / VLAN

Serveur DHCP

DNS Dynamique

Routage

Identifiant TP-Link

Wi-Fi

USB

Transferts NAT

Soins à domicile

Sécurité

Fusion VPN

Serveur VPN

Routage statique

Prédéterminez un itinéraire fixe pour que les paquets réseau atteignent un hôte ou un réseau spécifique.

Ajouter

Réseau de destination	Passerelle par défaut	Interface	Description	Etat	Modifier
192.168.10.0/24	192.168.3.1	LAN	Route réseau WEB EVE NG	☒	

Table de routage

Affichez toutes les entrées de routage valides actuellement utilisées.

Actualiser

Numéro d'itinéraire actif: 6

Réseau de destination	Passerelle	Interface

SUPPORT

ACCESSIBILITÉ

RETOUR AU SOMMET

Gérez votre réseau à distance via Tether

Configuration plus rapide du réseau, gestion à distance plus pratique et davantage de fonctions cloud.

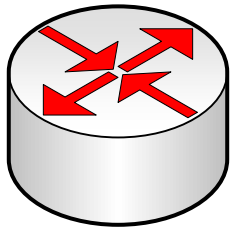
[Apprendre encore plus](#)

App Store

Google Play



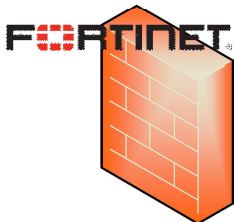
ROUTEUR VIRTUEL SMARTHOME :



Vidage de la mémoire du NAT (Cache) : Cette commande essentielle a permis de forcer le routeur Cisco à oublier les anciennes sessions qui s'étaient emmêlées les pinceaux et créaient la boucle :

```
Router# clear ip nat translation *
```

PARE-FEU FORTIGATE VIRTUEL (EVE-NG)



1^{ère} Manipulation :

Activation du routage asymétrique (Désactivation globale du RPF) : Par défaut, le FortiGate virtuel jetait les paquets du PC car ils arrivaient sur sa patte WAN sans correspondre à son sous-réseau direct. Dans la console CLI du FortiGate virtuel, nous avons tapé :

```
FORTIGATE-SMARTHOME # config system settings
FORTIGATE-SMARTHOME (settings) # set asymroute enable
FORTIGATE-SMARTHOME (settings) # end
```

2^{ème} Manipulation :

Désactivation du contrôle de source strict sur l'interface WAN (port3) :

```
FORTIGATE-SMARTHOME # config system interface
FORTIGATE-SMARTHOME (interface) # edit port3
FORTIGATE-SMARTHOME (port3) # set src-check disable
FORTIGATE-SMARTHOME (port3) # next
FORTIGATE-SMARTHOME (interface) # end
```




Test de Validation :

Vérification du chemin logique que doit le paquet :

```
C:\Users\Theo>tracert 192.168.10.1

Détermination de l'itinéraire vers www.smarthome.com [192.168.10.1]
avec un maximum de 30 sauts :

  1      3 ms      2 ms      2 ms  192.168.3.1
  2     24 ms     9 ms     13 ms  192.168.3.50
  3     24 ms     5 ms     12 ms  172.16.10.254
  4      9 ms     12 ms     13 ms  www.smarthome.com [192.168.10.1]

Itinéraire déterminé.

C:\Users\Theo>
```

PC Gamer → Routeur Cisco :

```
C:\Users\Theo>ping 192.168.3.50

Envoi d'une requête 'Ping' 192.168.3.50 avec 32 octets de données :
Réponse de 192.168.3.50 : octets=32 temps=4 ms TTL=255
Réponse de 192.168.3.50 : octets=32 temps=4 ms TTL=255
Réponse de 192.168.3.50 : octets=32 temps=8 ms TTL=255
Réponse de 192.168.3.50 : octets=32 temps=6 ms TTL=255

Statistiques Ping pour 192.168.3.50:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 8ms, Moyenne = 5ms

C:\Users\Theo>
```

PC Gamer → ServeurWeb :

```
C:\Users\Theo>ping 192.168.10.1

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=29 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=12 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=8 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=12 ms TTL=126

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 8ms, Maximum = 29ms, Moyenne = 15ms

C:\Users\Theo>
```

PC Gamer → www.smarthome.com :

```
C:\Users\Theo>ping www.smarthome.com

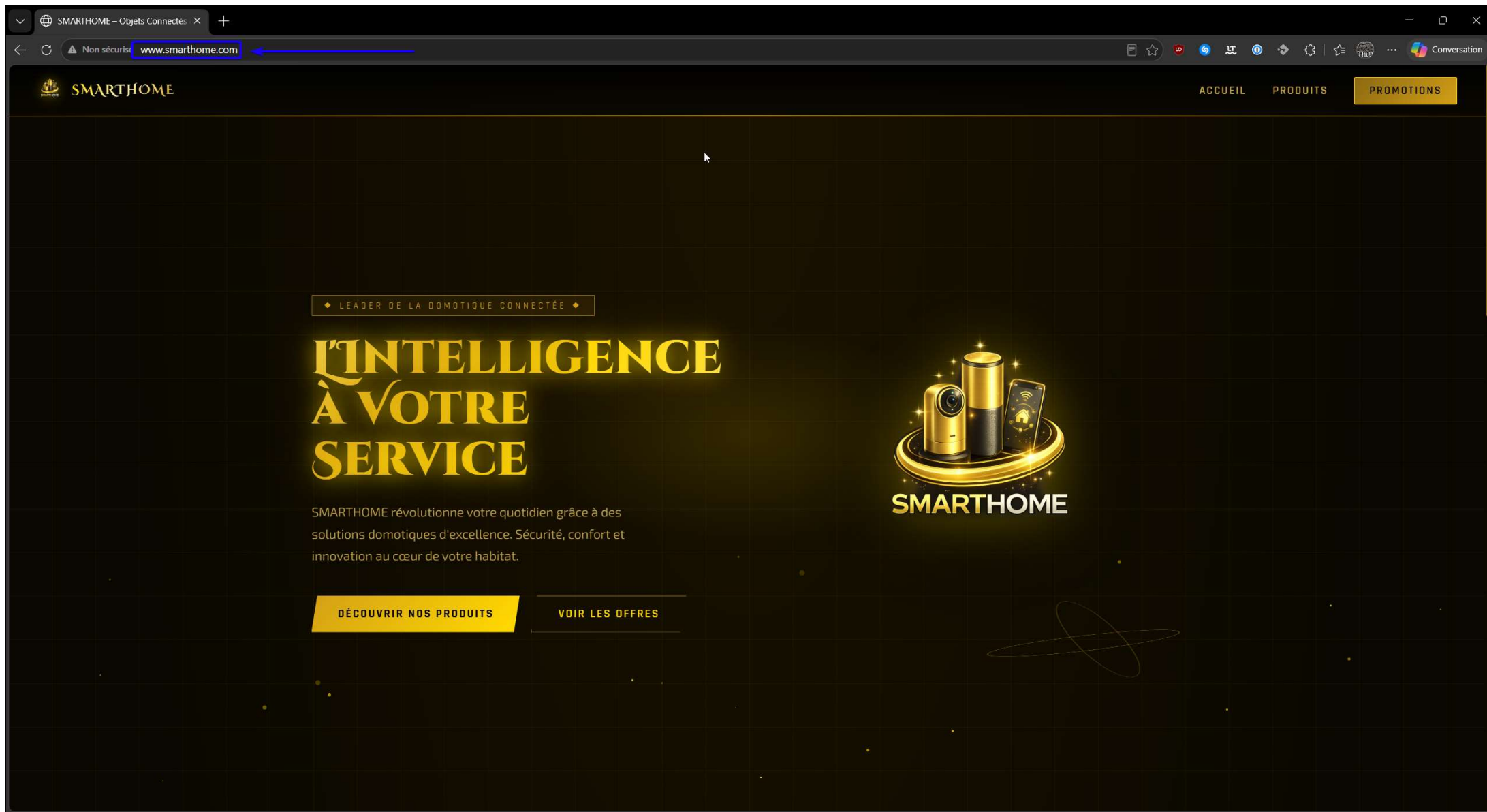
Envoi d'une requête 'ping' sur www.smarthome.com [192.168.10.1] avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=7 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=9 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=8 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=12 ms TTL=126

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 12ms, Moyenne = 9ms

C:\Users\Theo>
```



Maintenant que tous les tests sont validés on peut accéder au site de l'entreprise SMARTHOME.



PROJET PERSONNEL – Théo BRETON

PROJET – RESEAUX/SYSTEME : PROJET N°5 : RADIUS DANS UN ENVIRONNEMENT PROFESSIONNEL

❶ Configuration du SSH

#Configuration du SSH sur tous les équipements

```
Switch(config)#line vty 0 4
Switch(config-line)#transport input ssh
Switch(config-line)#login local
Switch(config-line)#password cisco
Switch(config)#ip domain name smarhome.local
Switch(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: Switch.ssh.key

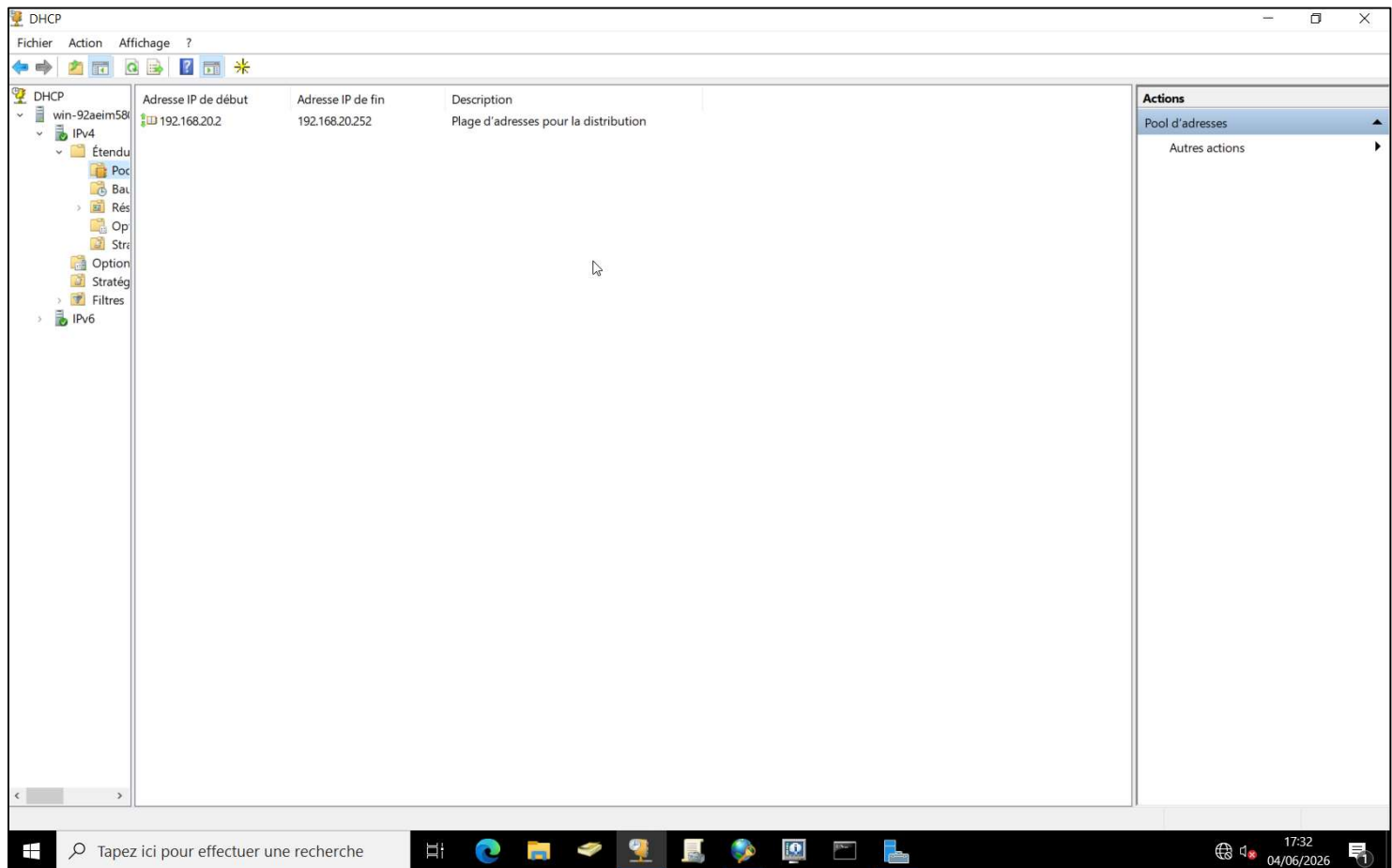
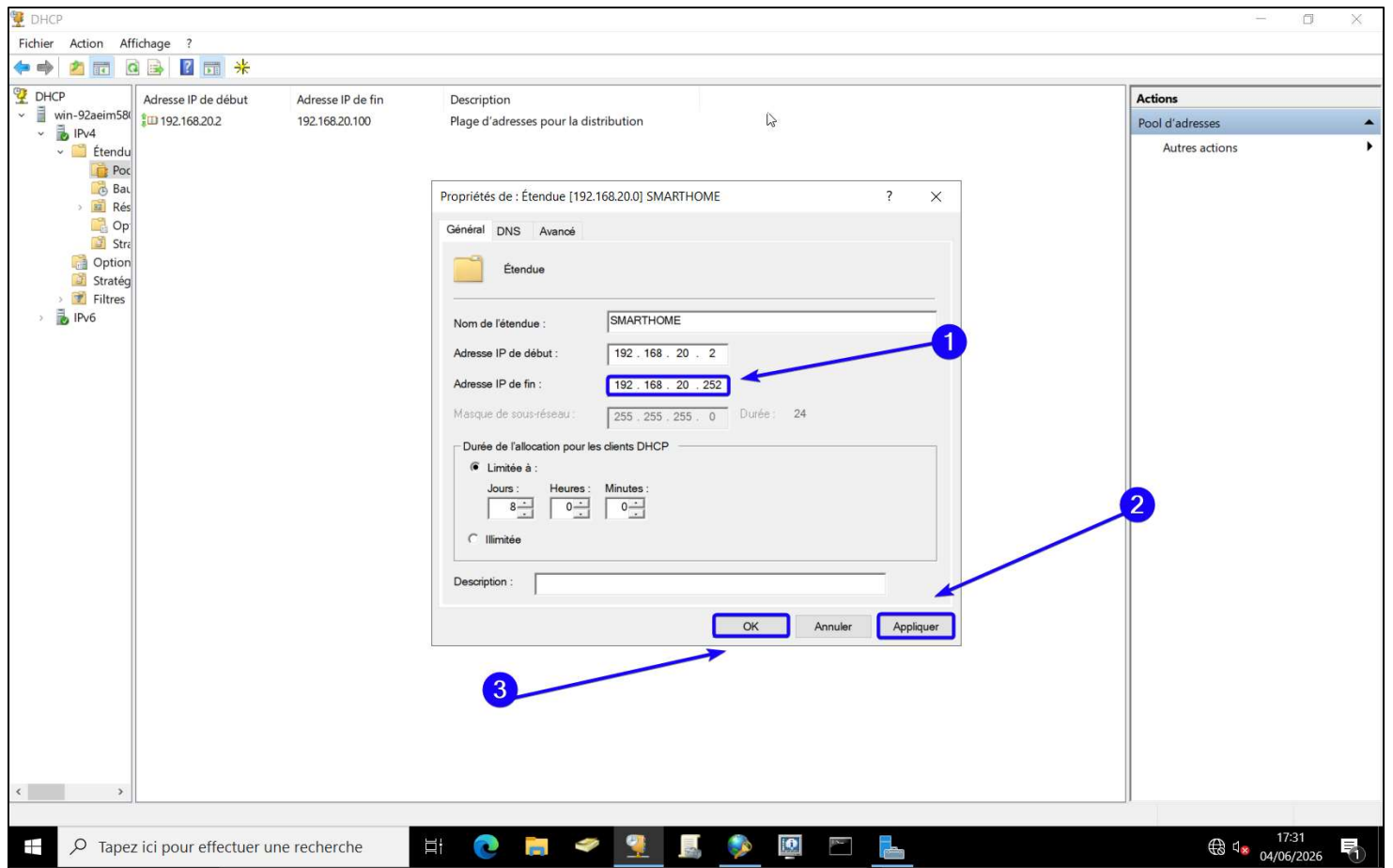
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK]

Switch(config)#username admin password cisco
Switch(config)#exit
```

#Running config

```
line vty 0 4
  password cisco
  login local
```

Pour éviter tout conflit d'attribution d'adresse IP on va modifier l'étendue dans le serveur DHCP.



PARTIE 4 : Mise en place du VLAN Maintenance sur les Switch :

❶ Configuration du VLAN 1 – AdminRéseaux

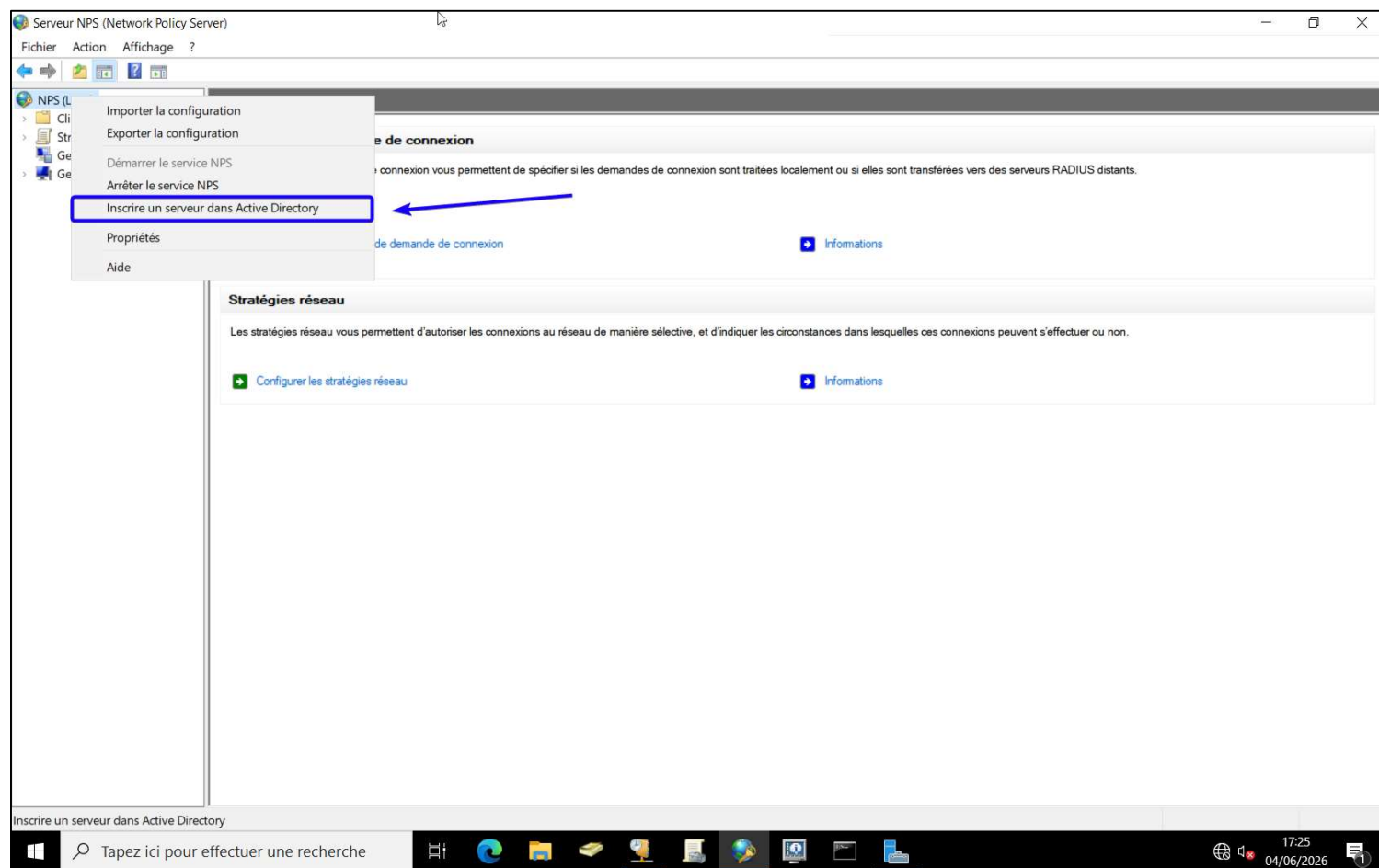
Pour pouvoir tester les deux cas on va mettre les deux postes sur le VLAN Natif.

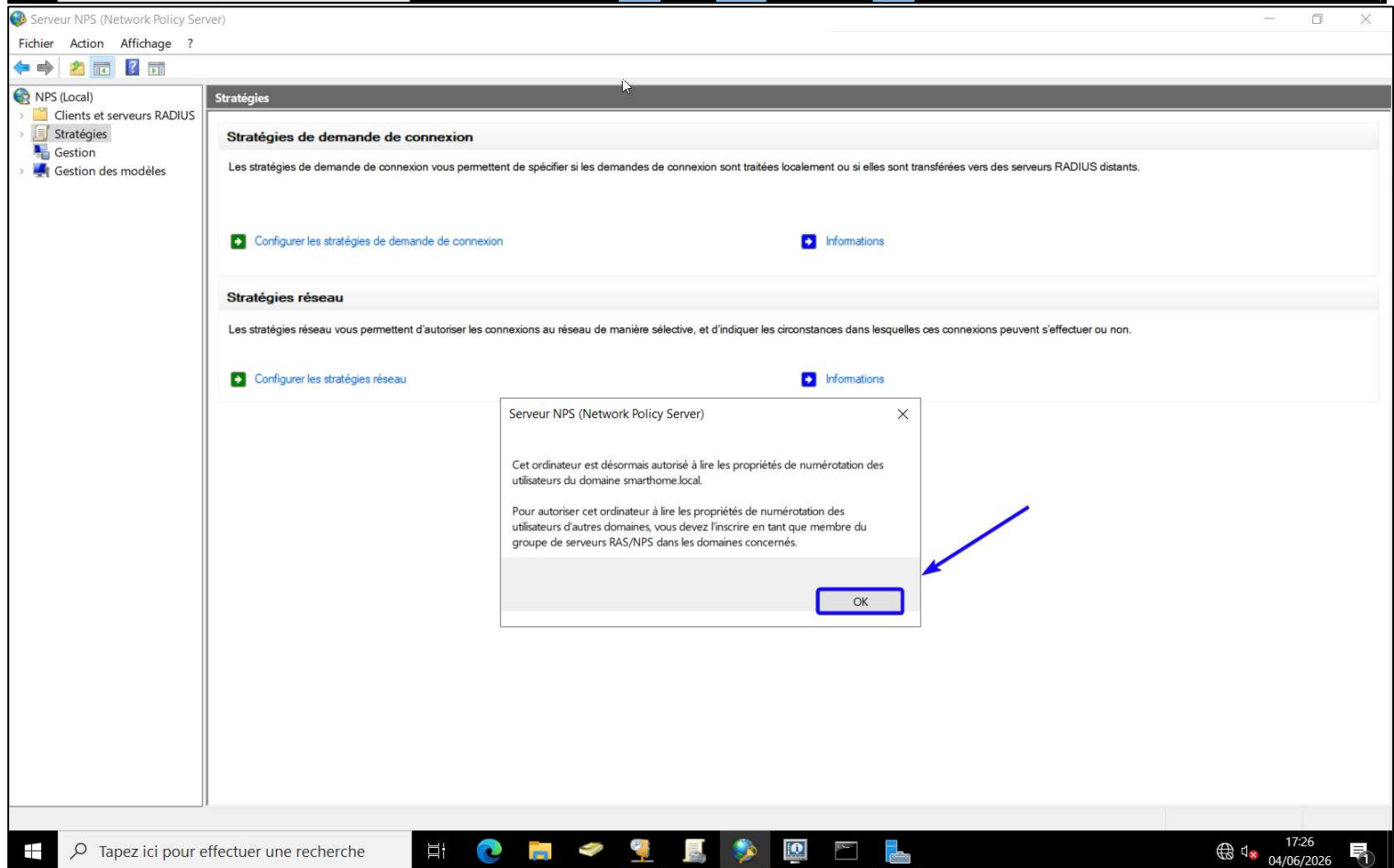
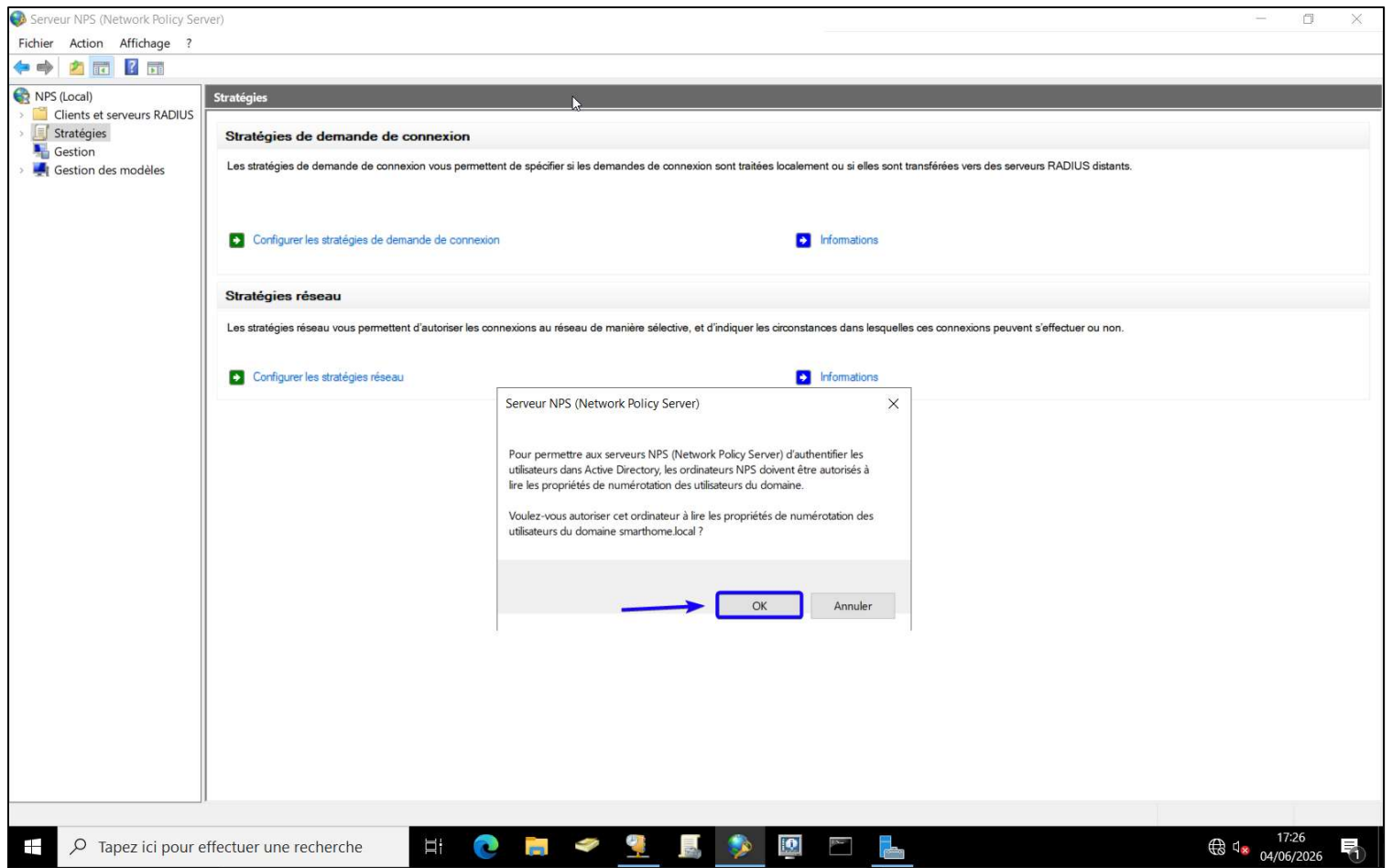
```
SW2(config)#vlan 1
SW2(config-vlan)#name AdminRéseaux
SW2(config-vlan)#exit

SW2(config)#int vlan 1
SW2(config-if)#ip address 192.168.20.253 255.255.255.0
SW2(config-if)#no sh
SW2(config-if)#exit
```

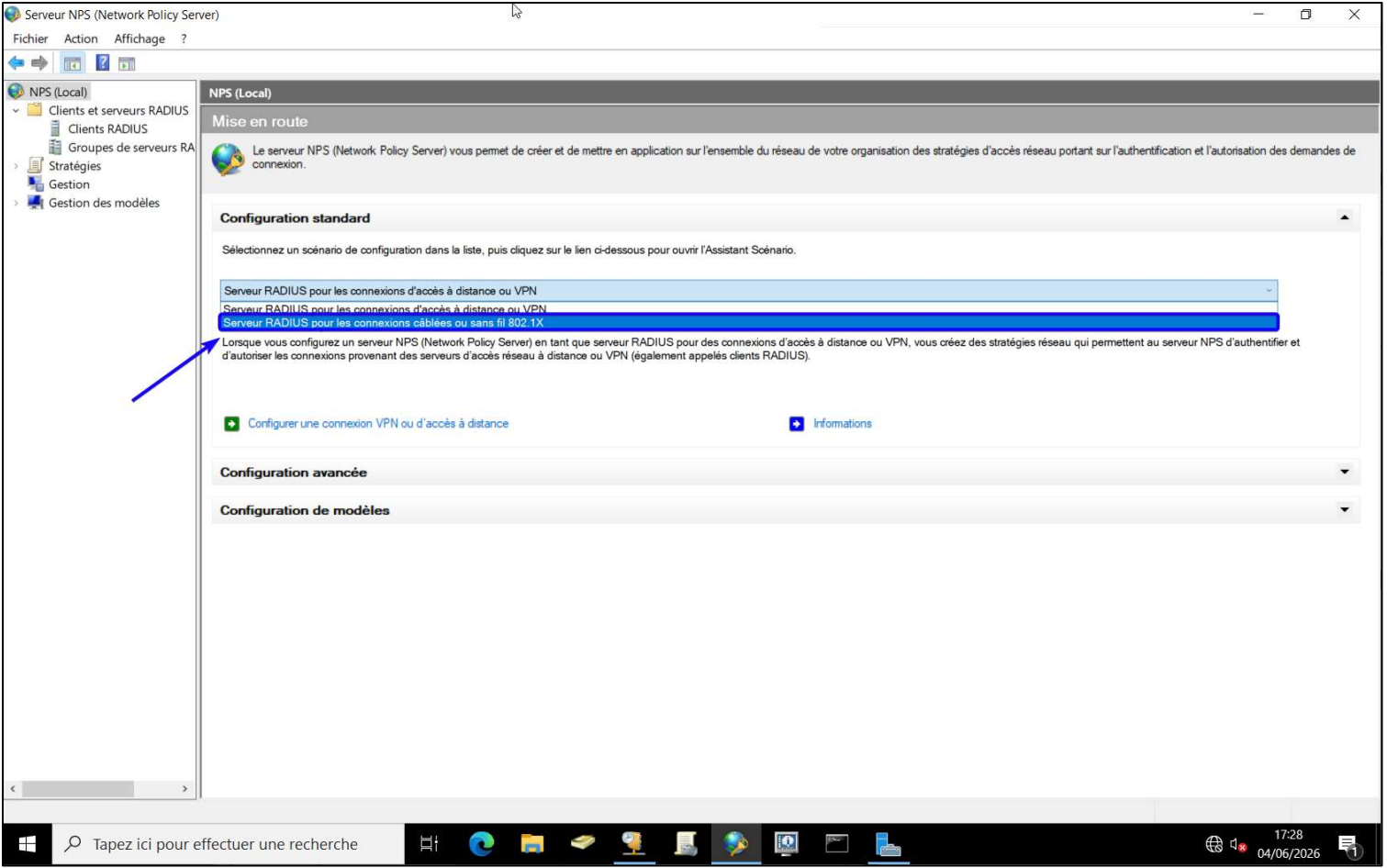
PARTIE 5 : Mise en place de RADIUS sur Serveur AD

❶ Inscription du serveur NPS dans l'Active Directory





On va maintenant créer des clients RADIUS

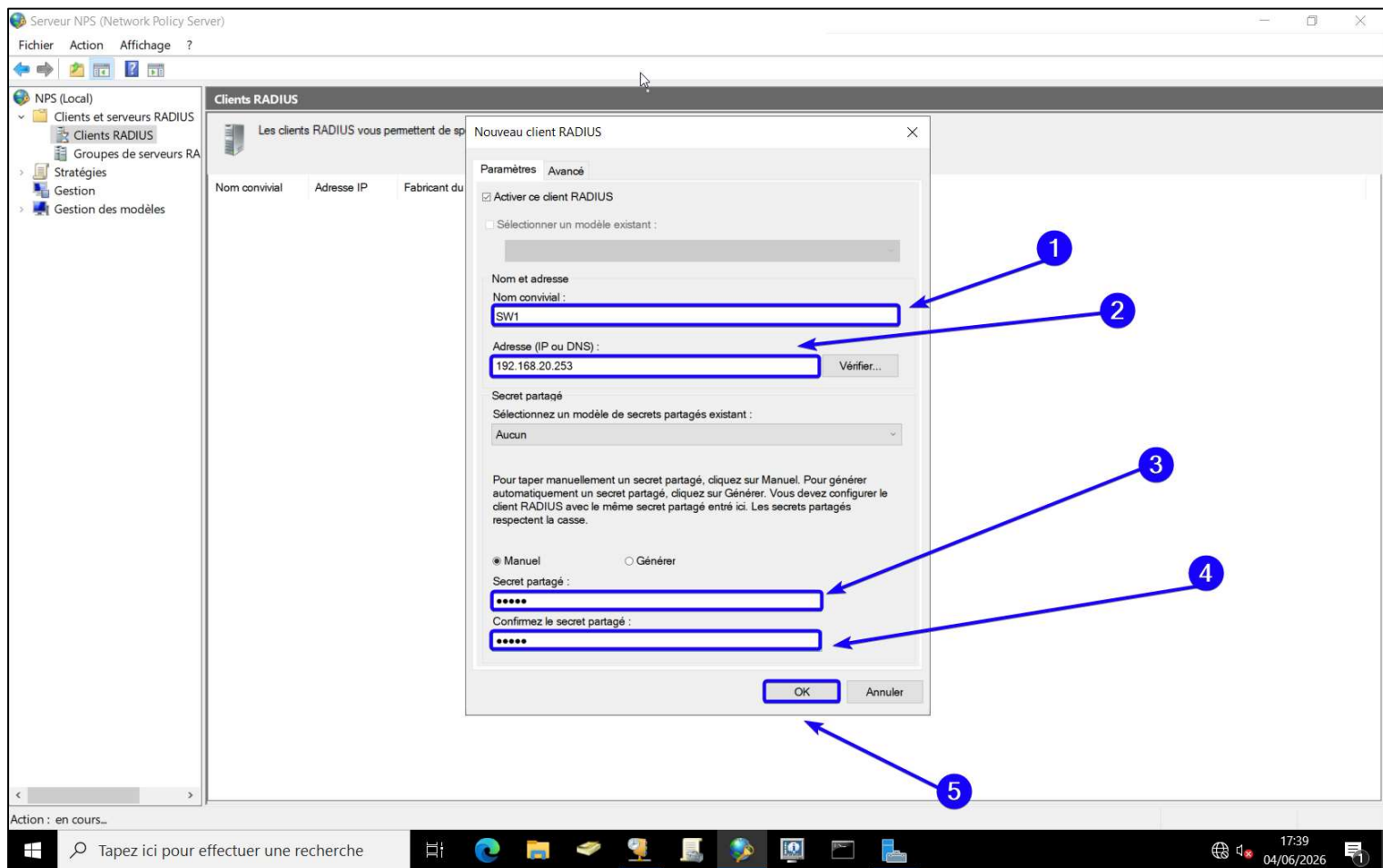
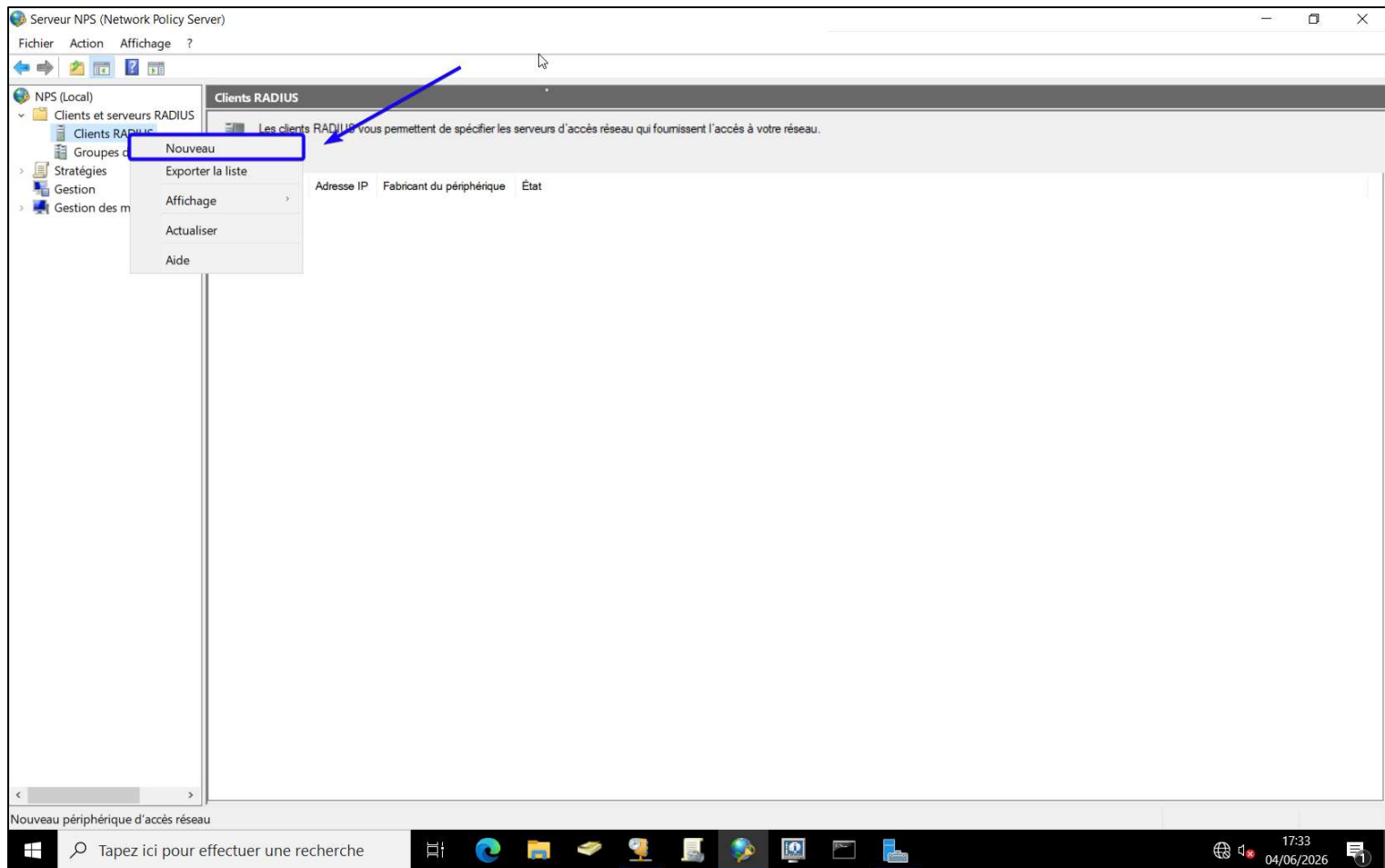


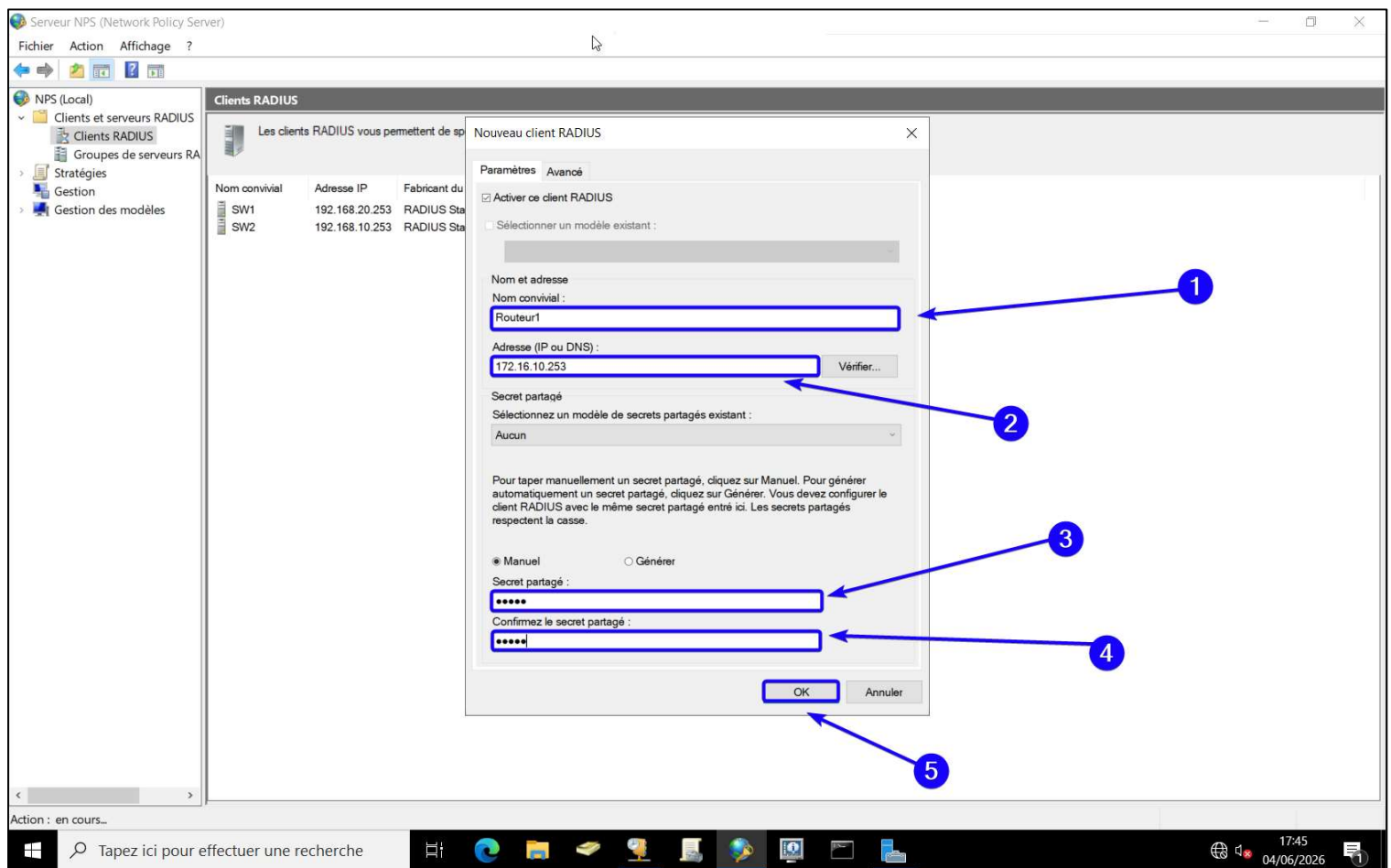
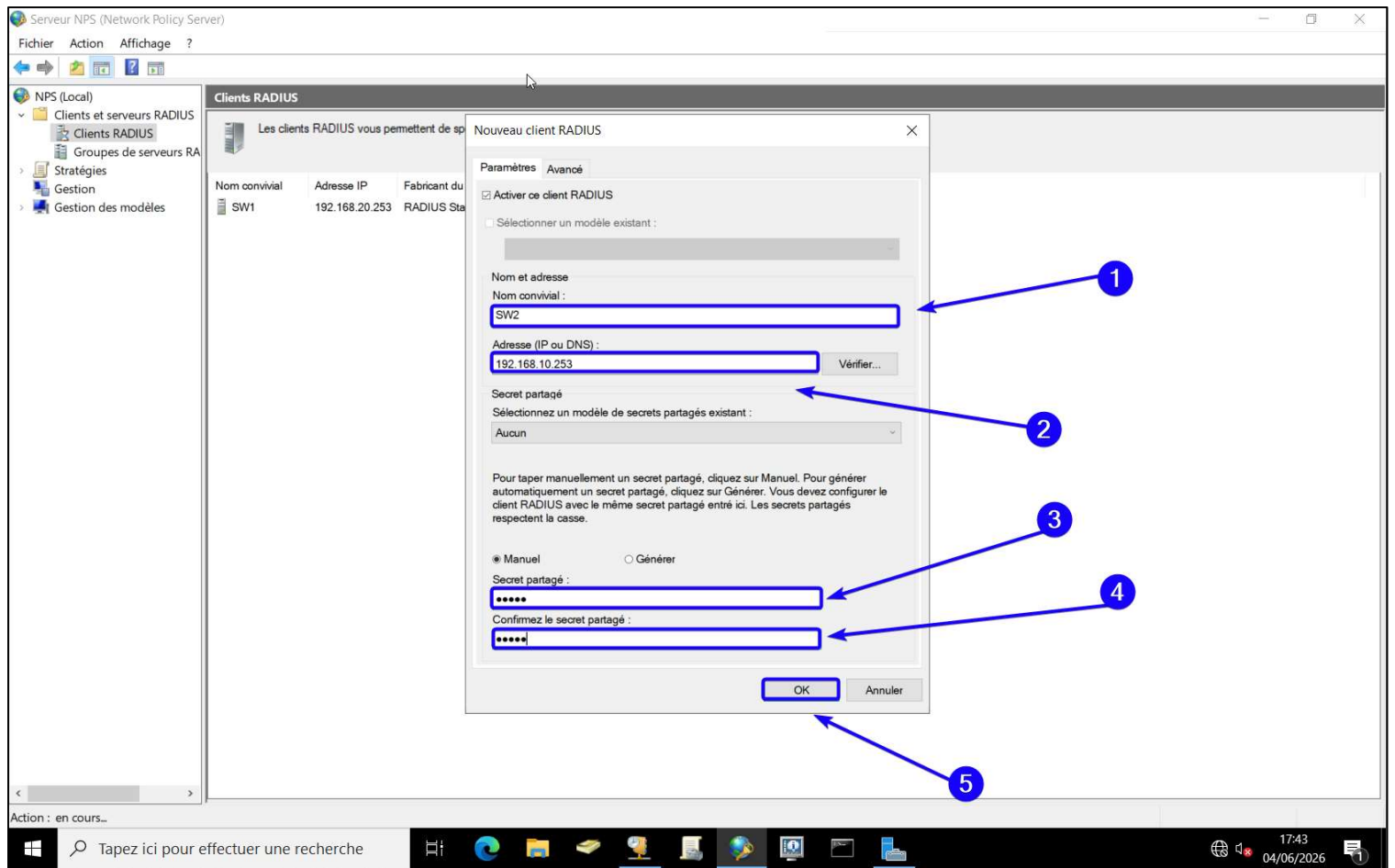
2 Création des clients RADIUS

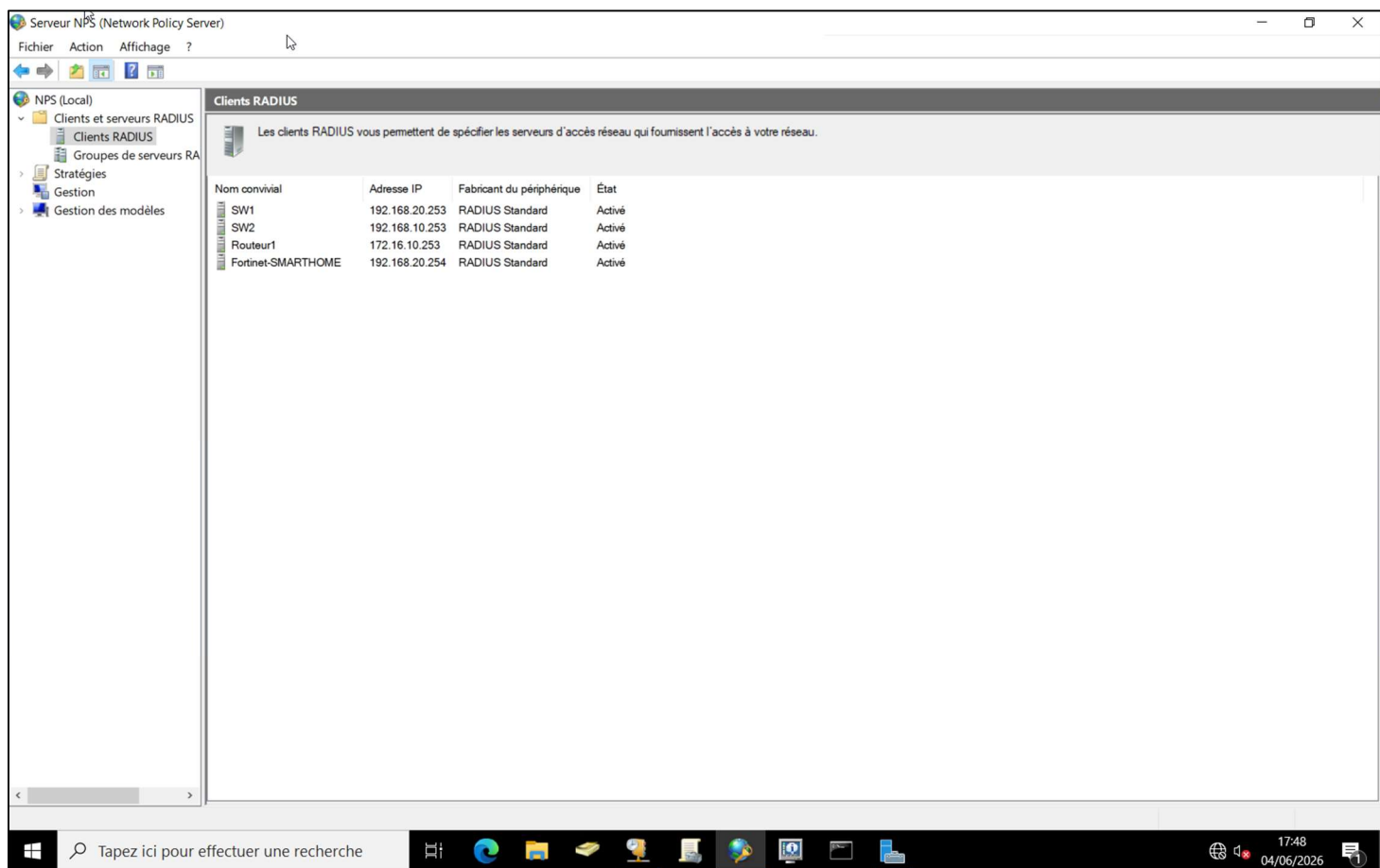
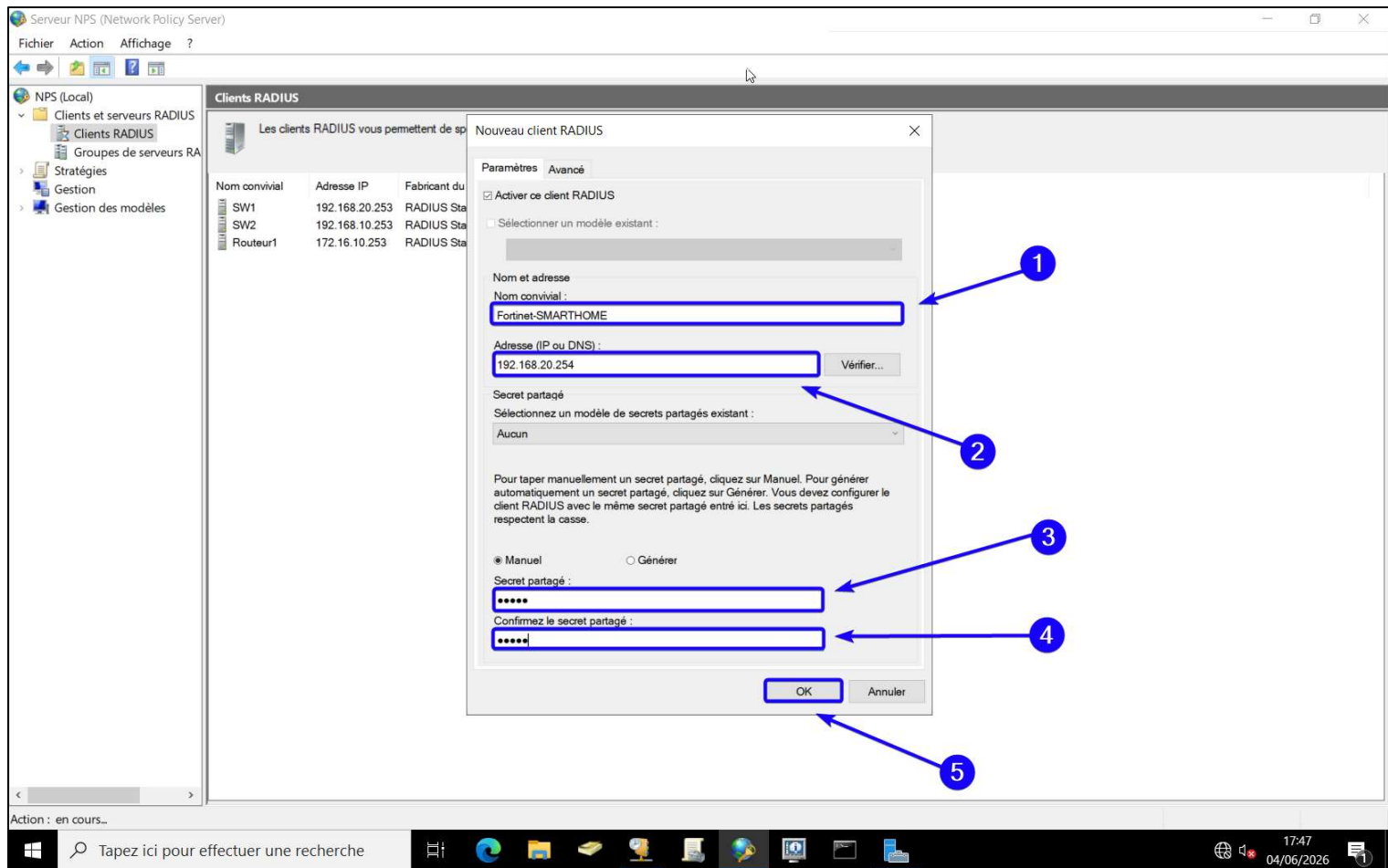


Pour des raisons de restriction au niveau des règles de filtrages au niveau du pare feu, je ferai la supervision de que du switch 1 pour les conditions à suivre.

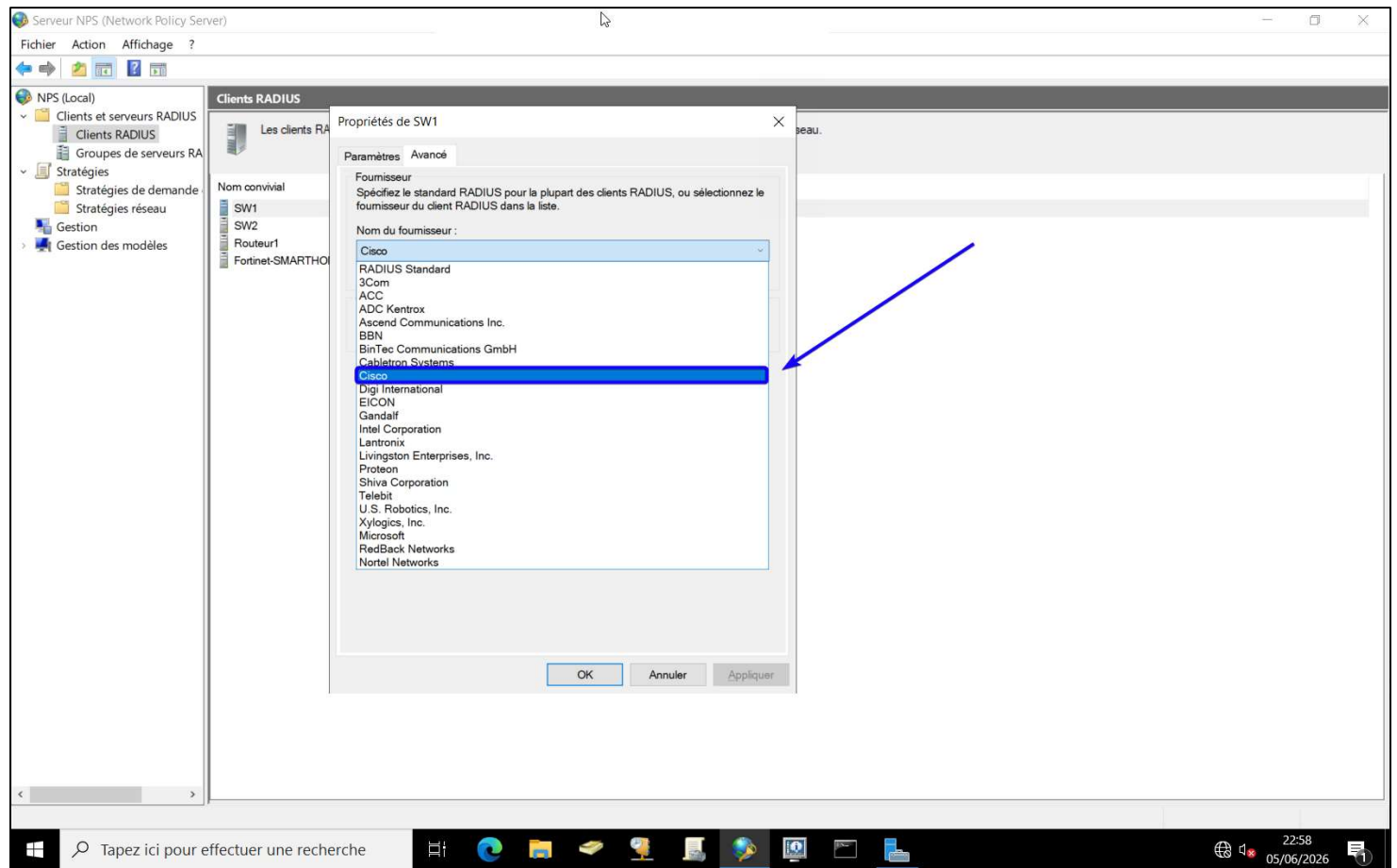
Nom client	Adresse IP	Fabricant	Secret Partagé
SW1	192.168.20.253	Cisco	cisco
SW2	192.168.10.253	Cisco	cisco
Routeur1	172.16.10.253	Cisco	cisco
Fortinet-SMARTHOME	192.168.20.254	RADIUS Standard	cisco







Une fois que j'ai ajouté met client je sélectionne le fournisseur pour les équipements Cisco.



③ Les Conditions à remplir :



Sécurisation des accès physiques au réseau par l'implémentation du protocole 802.1X sur les commutateurs, garantissant que seuls les équipements authentifiés auprès du domaine ADDS puissent obtenir une configuration IP via le serveur DHCP.

Stratégies réseau

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

	État	Ordre de traitement	Type d'accès	Source
Domaine	Activé	1	Accorder l'accès	Non spécifié
du serveur Microsoft de Routage et Accès distants	Activé	2	Refuser l'accès	Non spécifié
d'autres serveurs d'accès	Activé	3	Refuser l'accès	Non spécifié

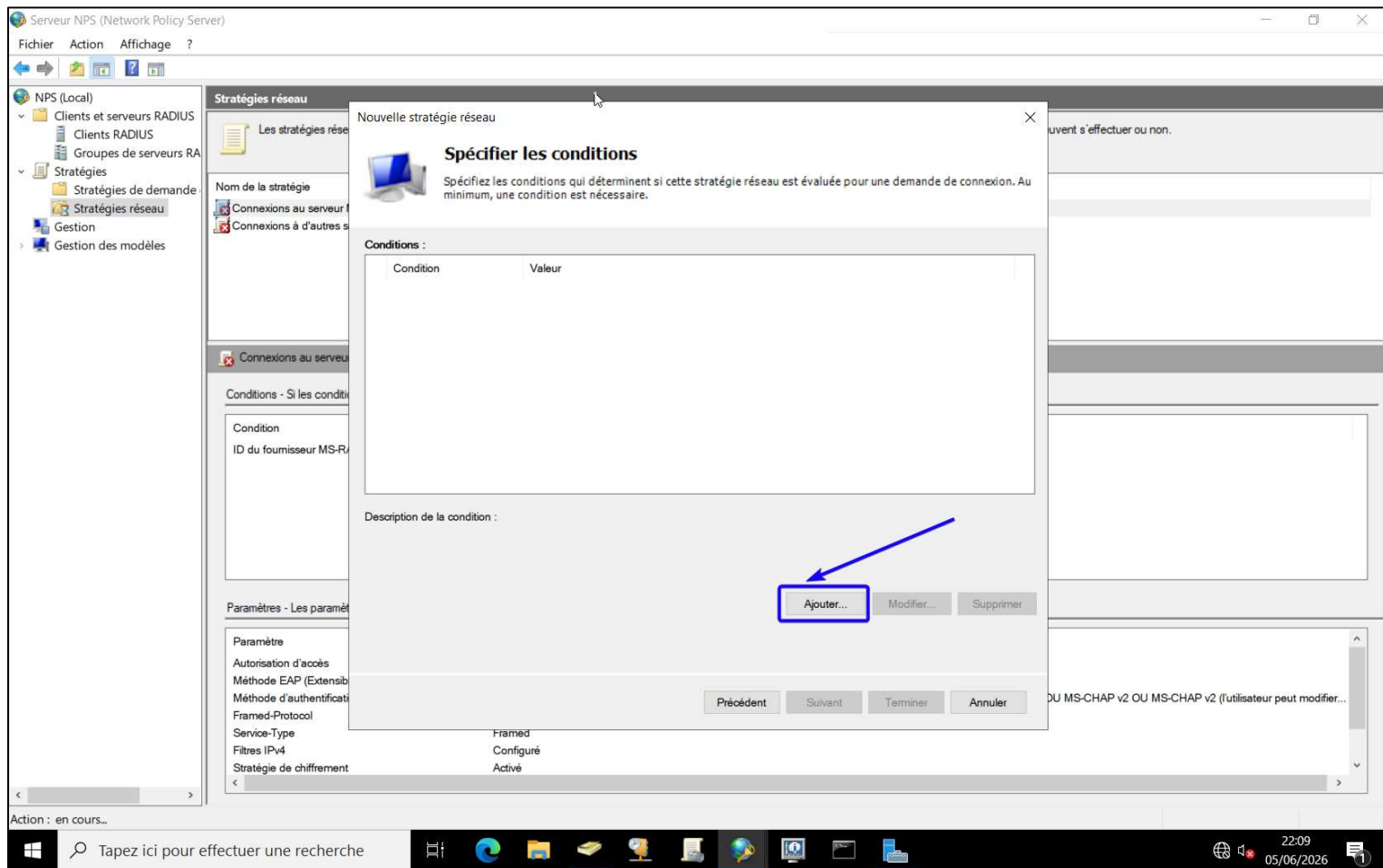
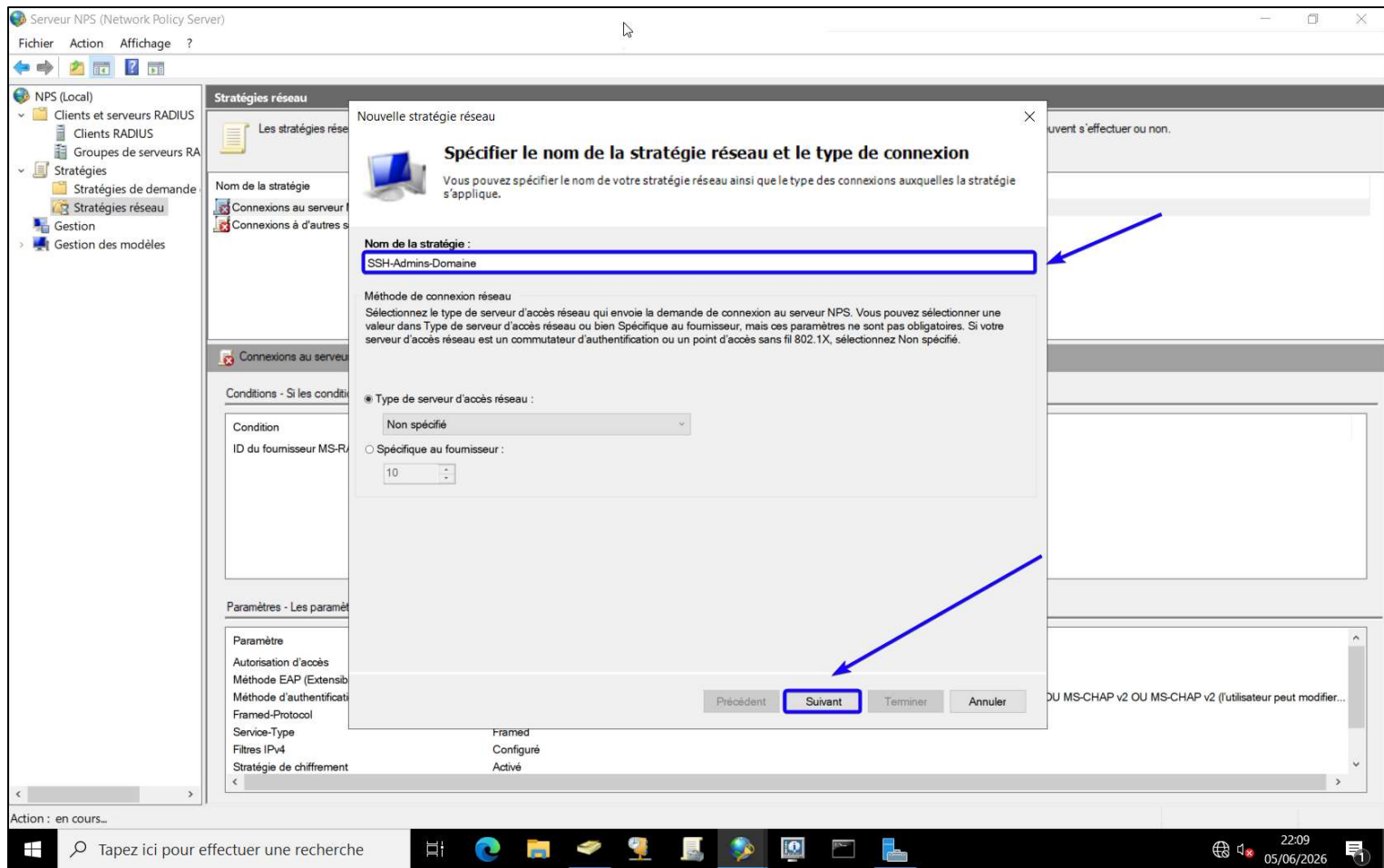
SSH-Admins-Domaine

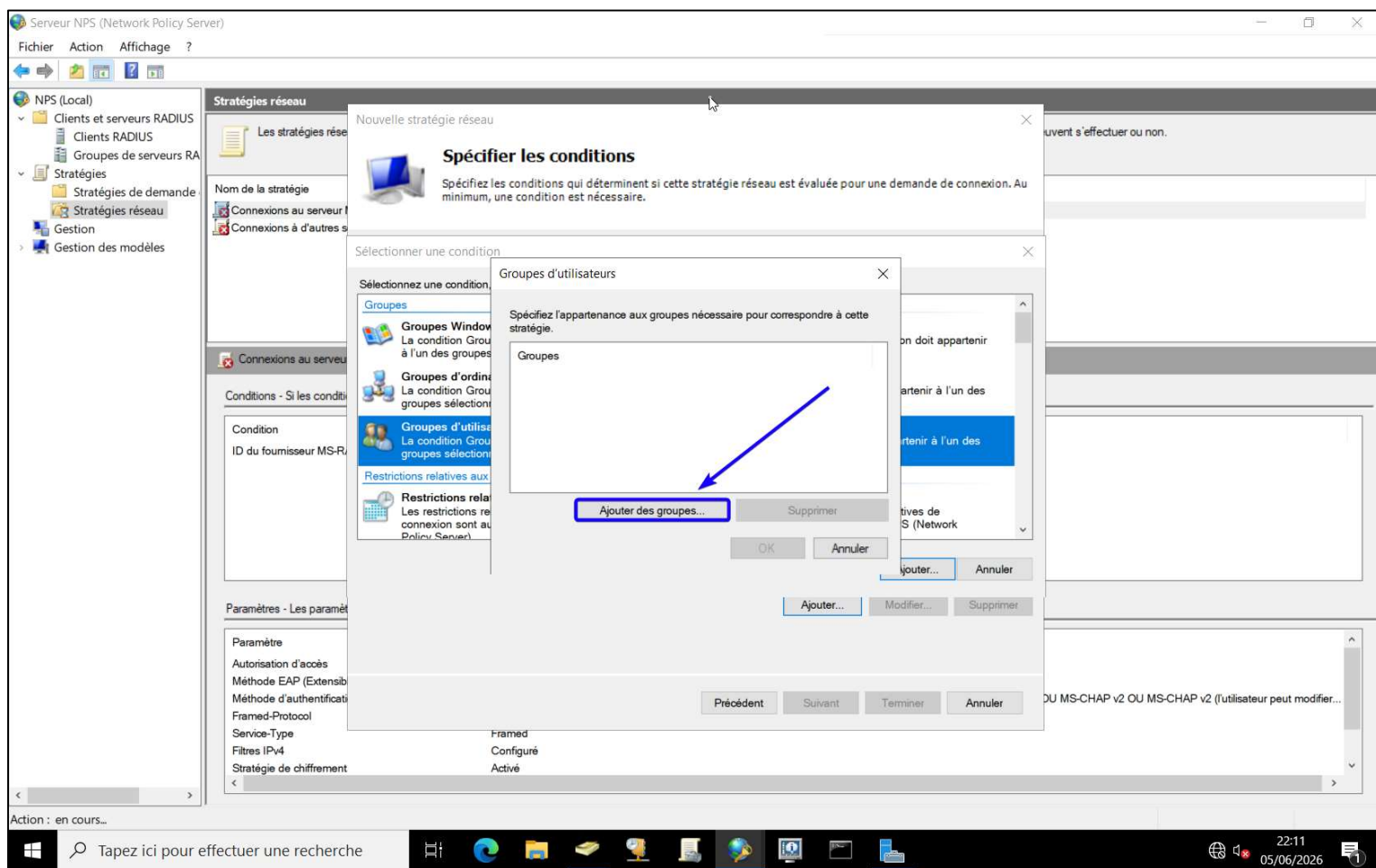
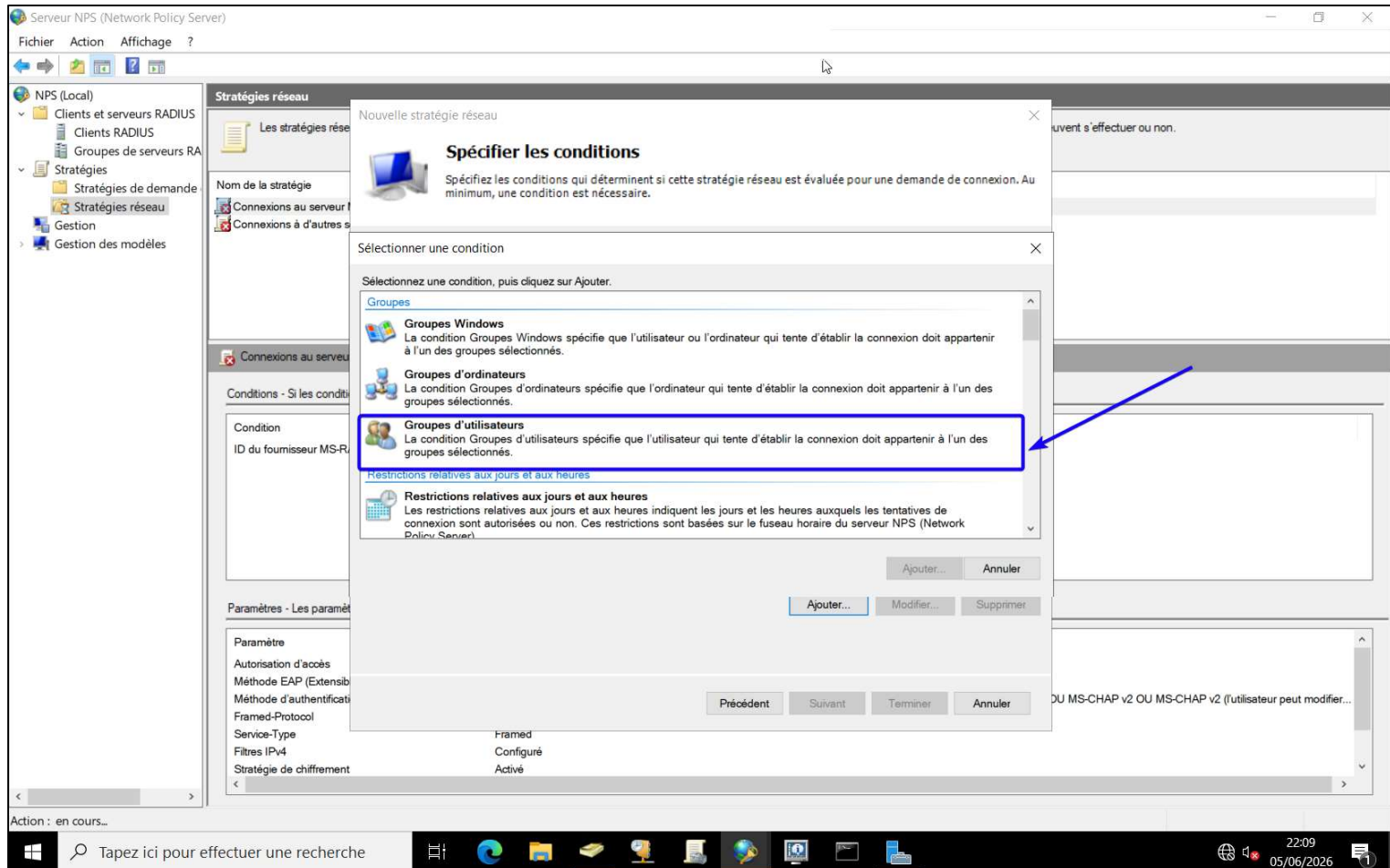
Conditions - Si les conditions suivantes sont réunies :

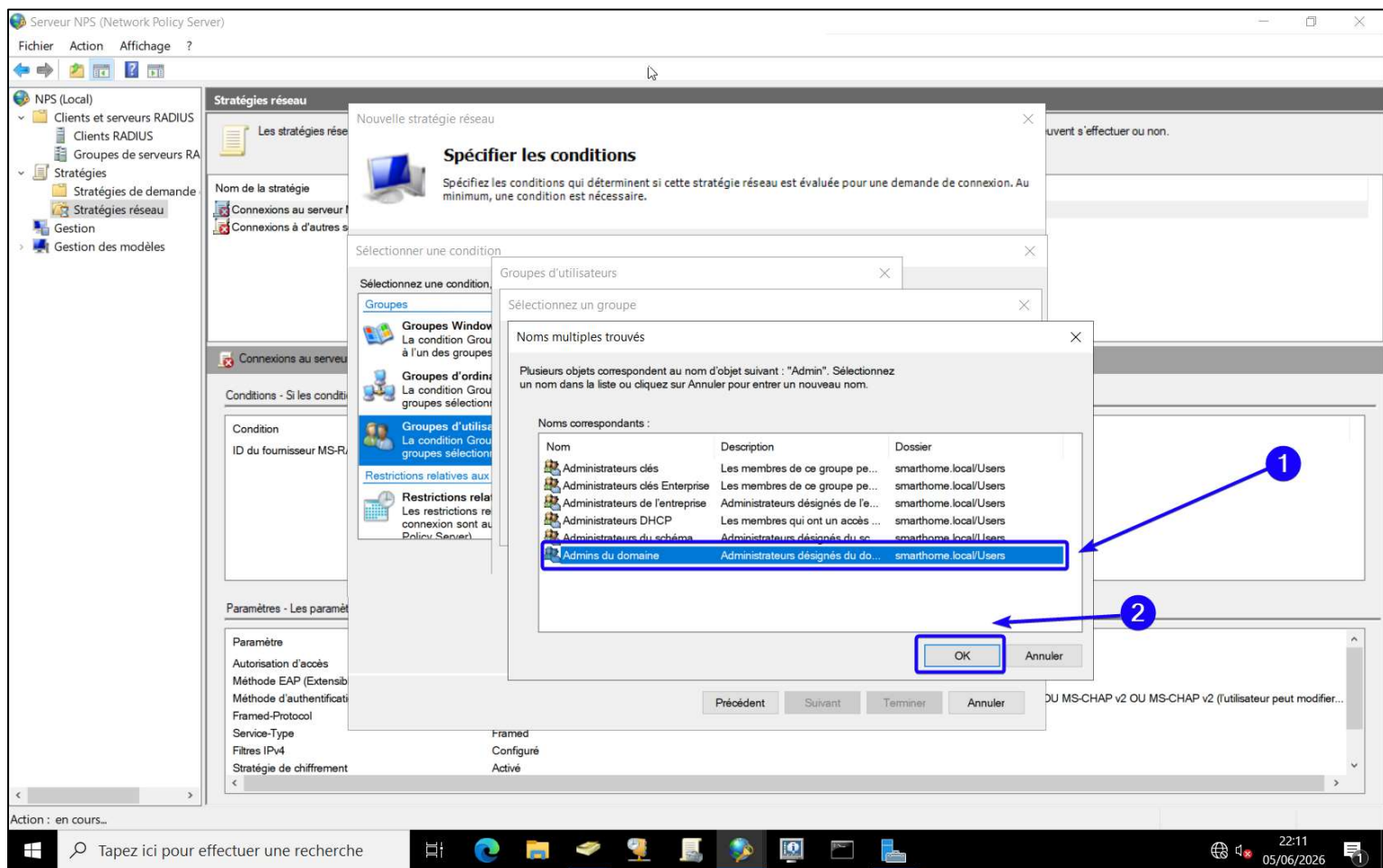
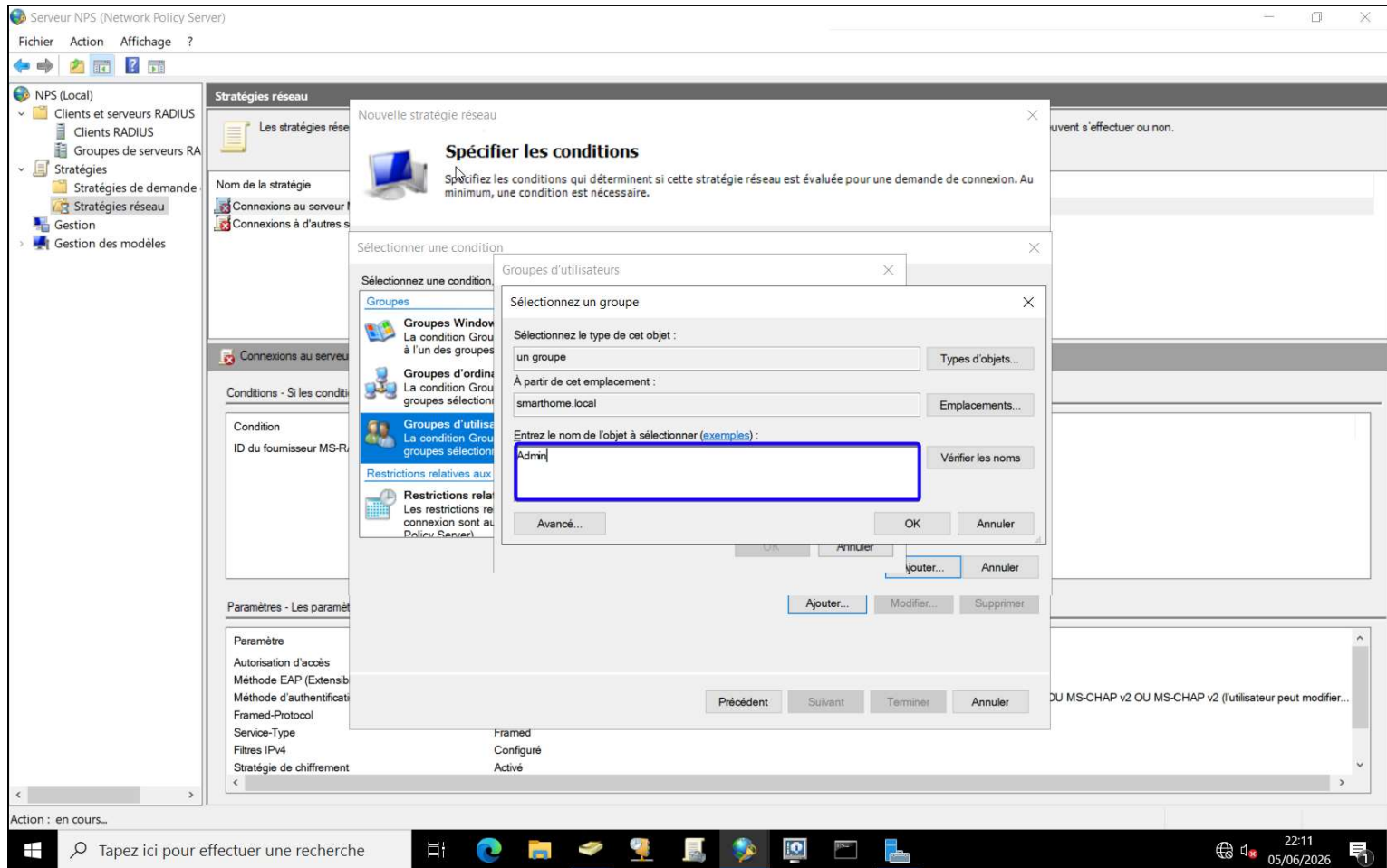
Condition	Valeur
Groupes d'utilisateurs	SMARTHOME\Admins du domaine

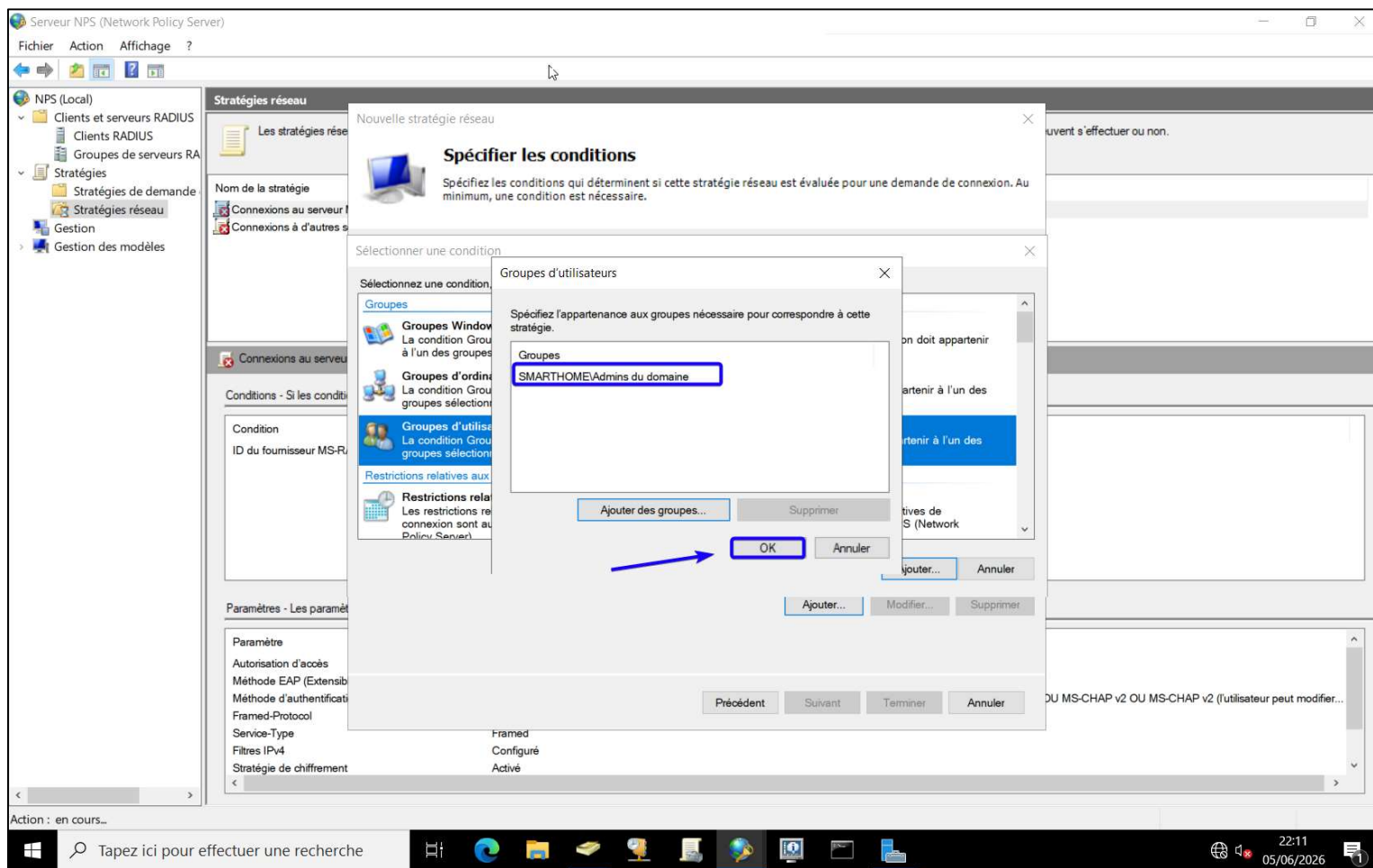
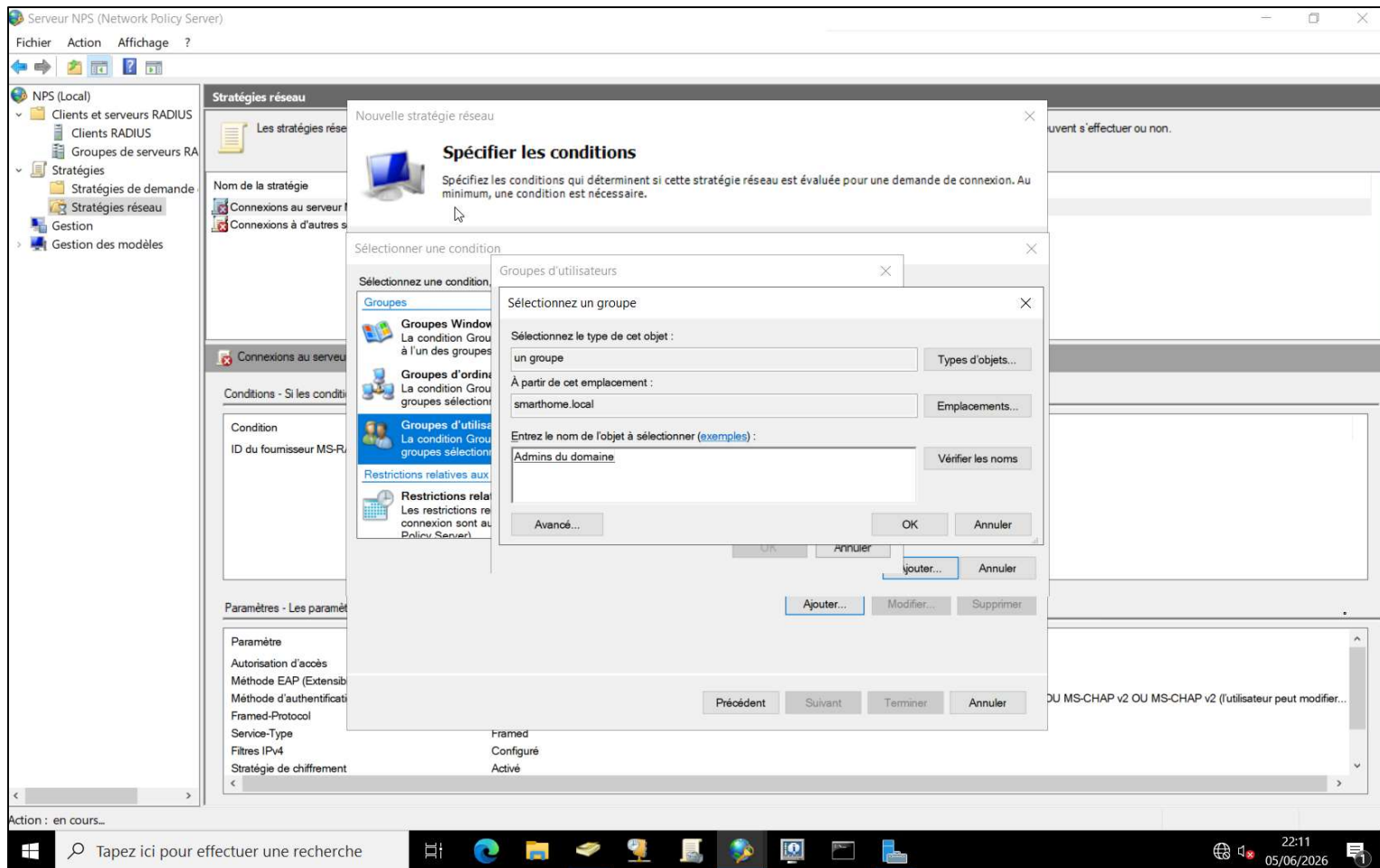
Paramètres - Les paramètres suivants sont appliqués :

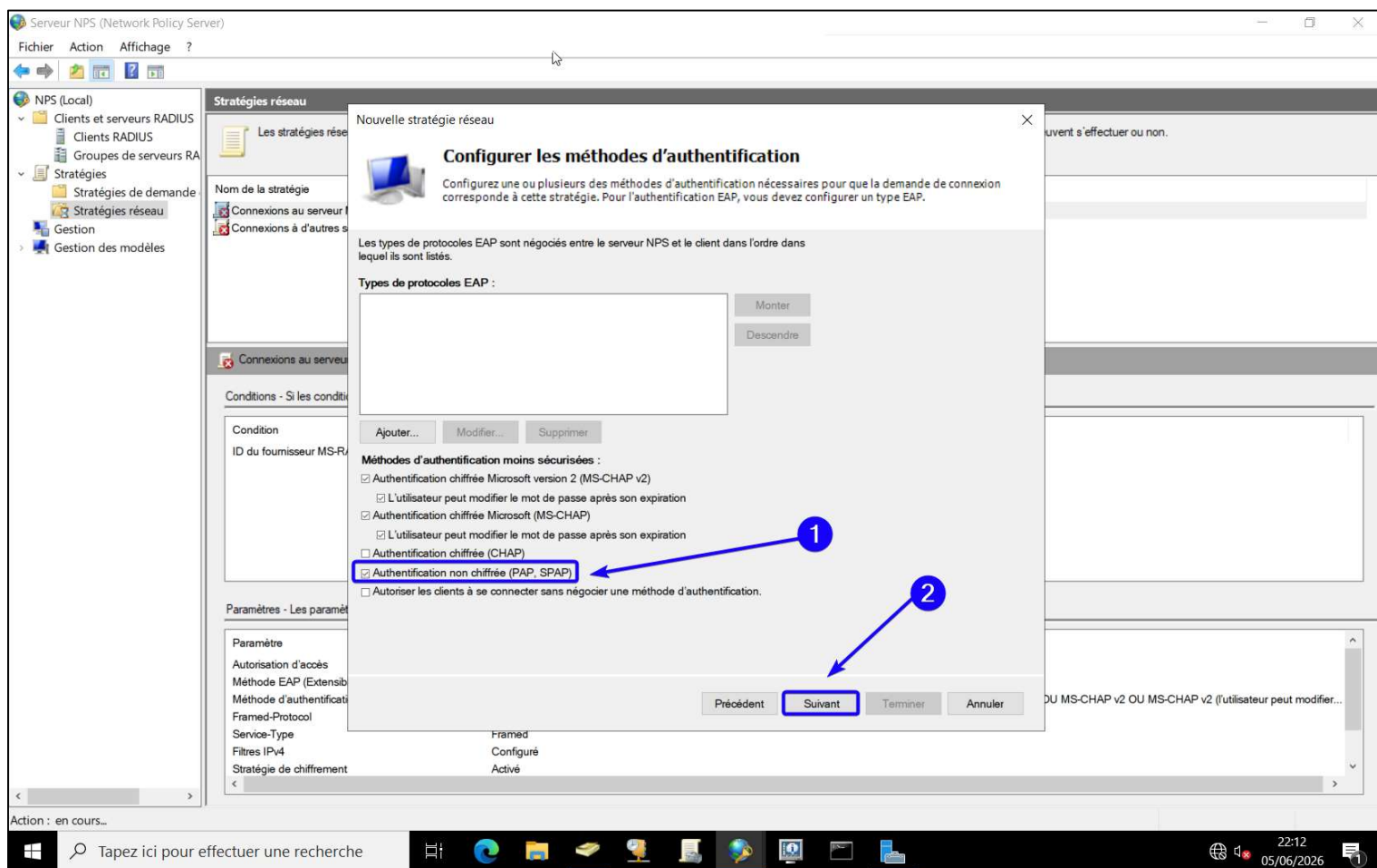
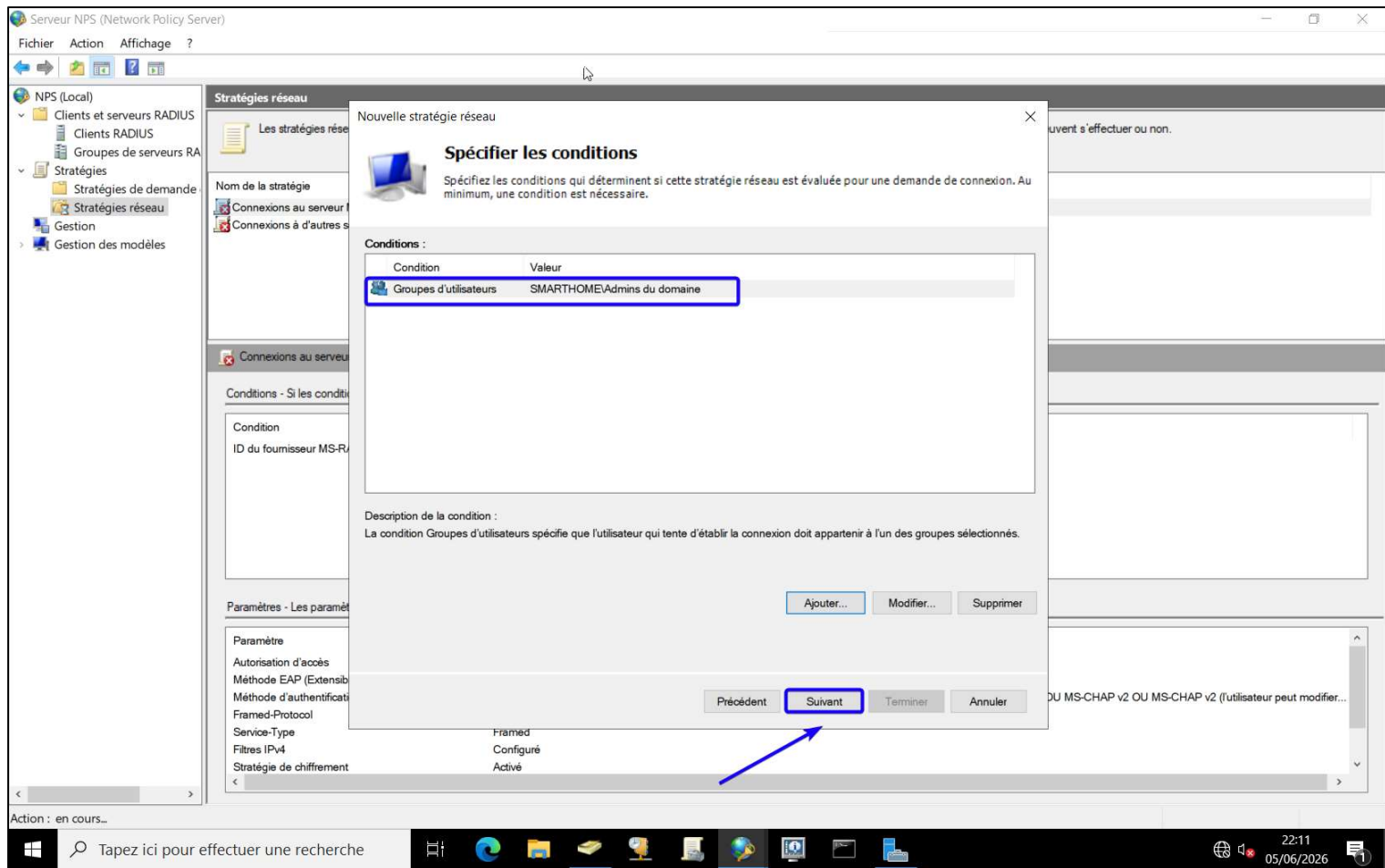
Paramètre	Valeur
Méthode d'authentification	Protocole EAP OU Authentification non chiffrée (PAP, SPAP) OU MS-CHAP v1 OU MS-CHAP v1 (l'utilisateur peut modifier le mot de passe après son expiration) OU MS-CHAP...
Autorisation d'accès	Accorder l'accès
Service-Type	Login
Méthode EAP (Extensible Authentication Protocol)	Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)

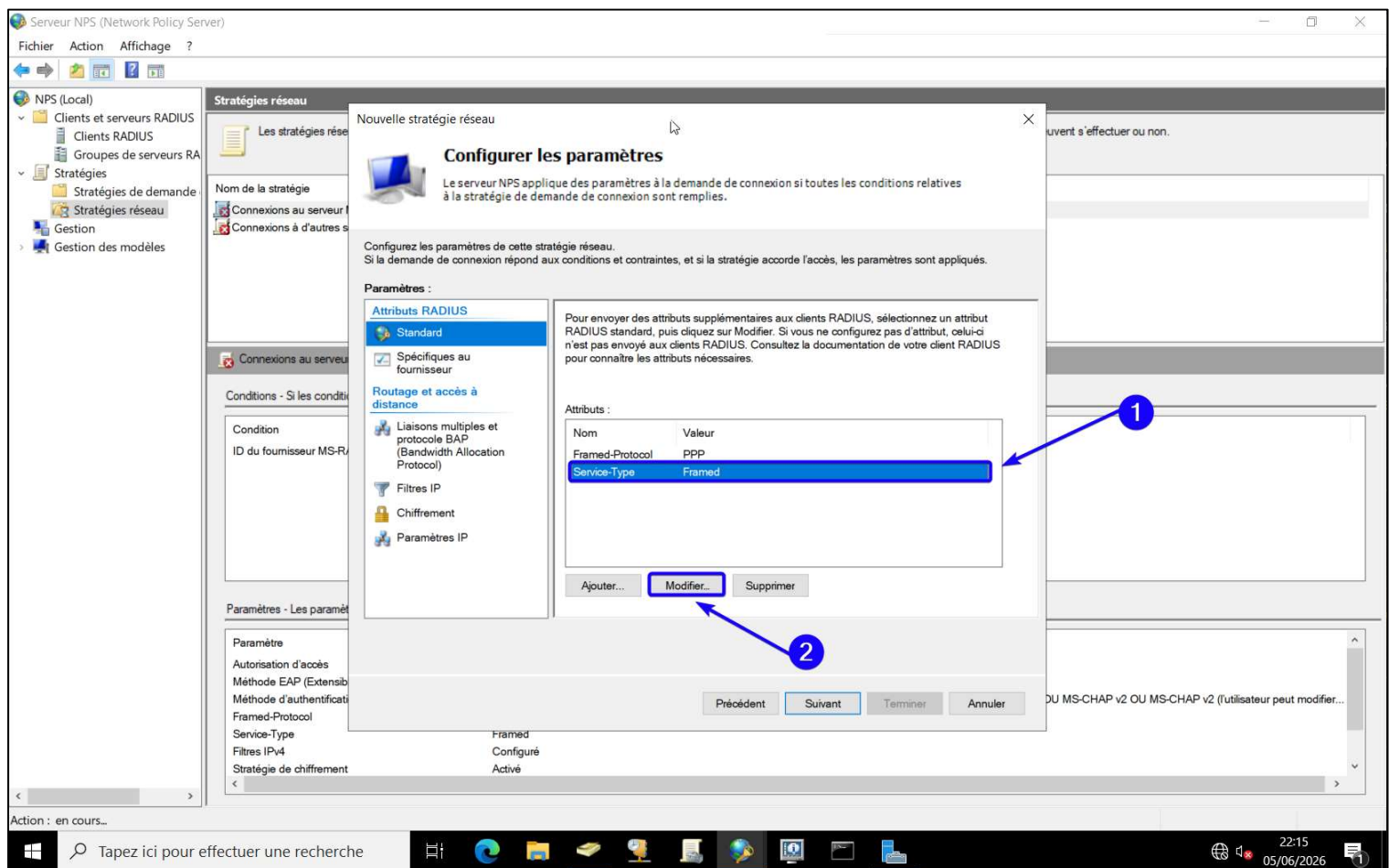
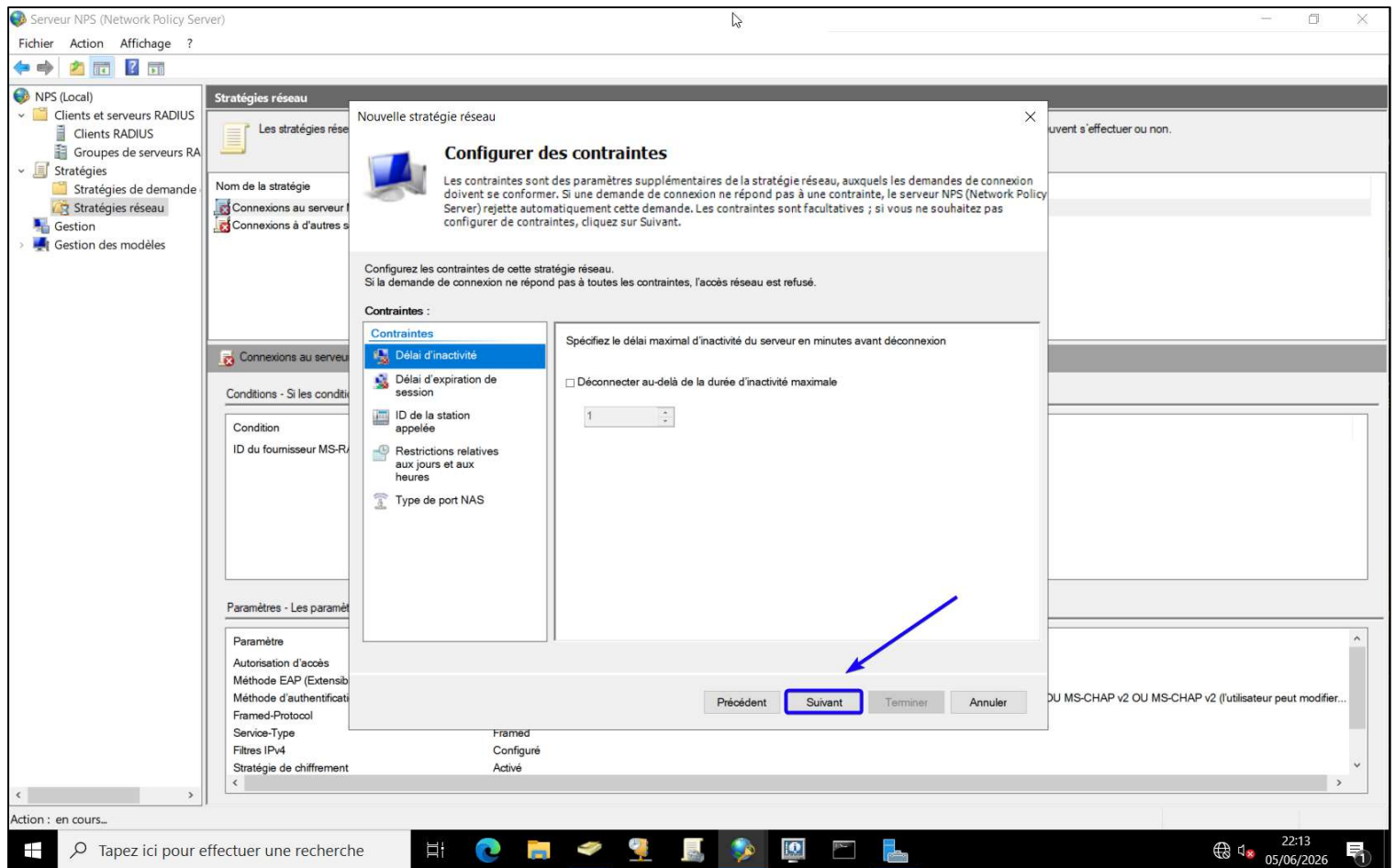


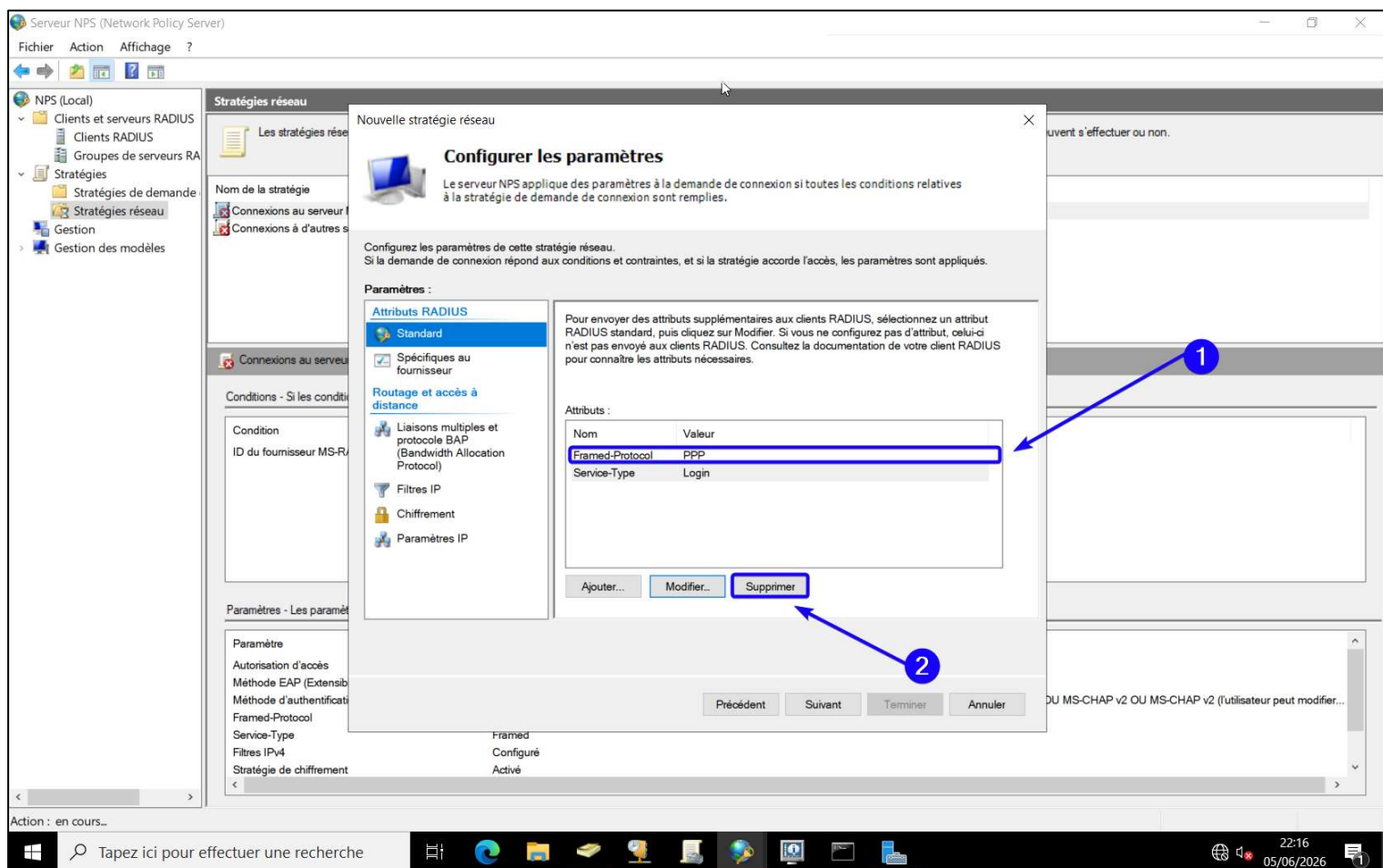
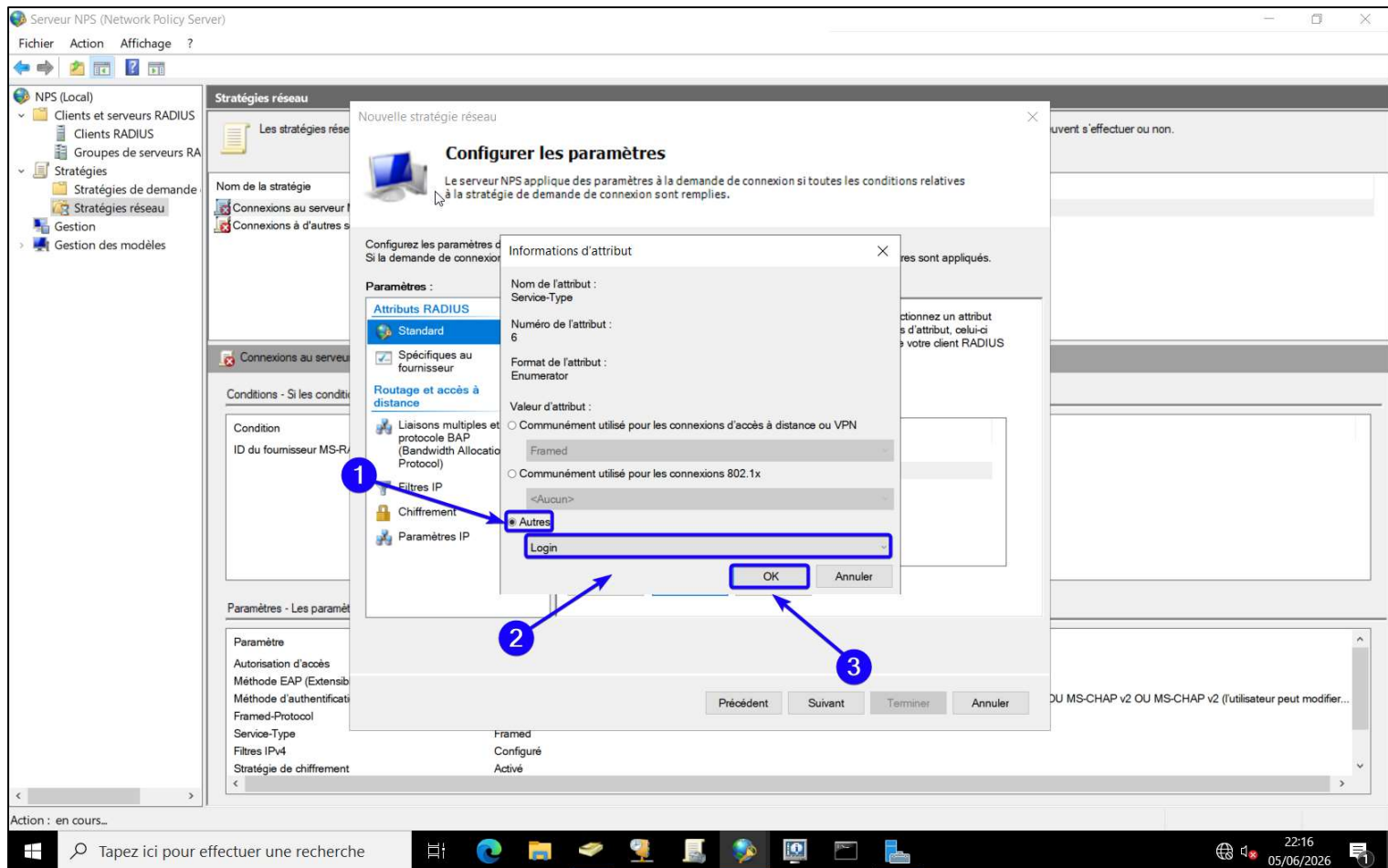


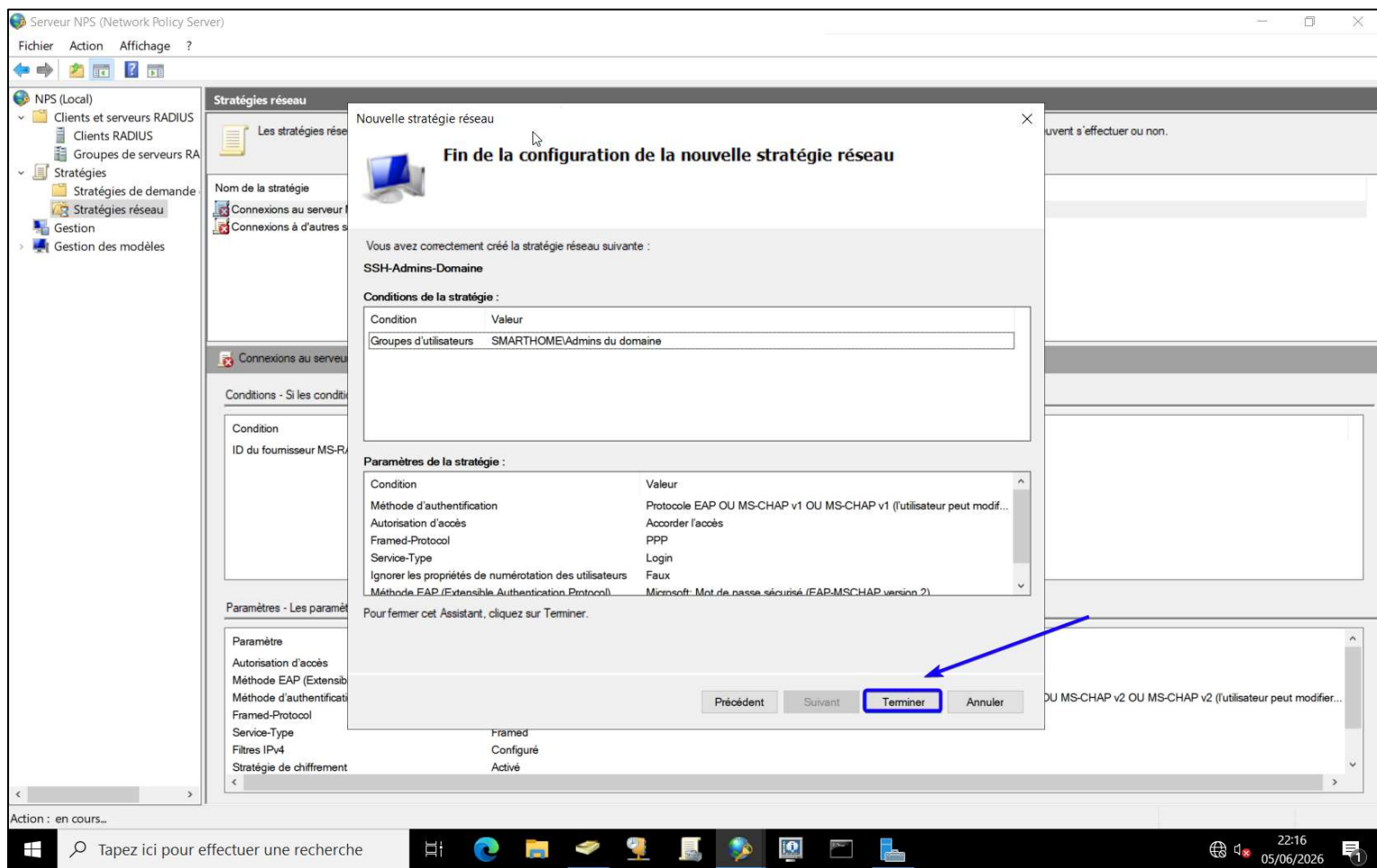
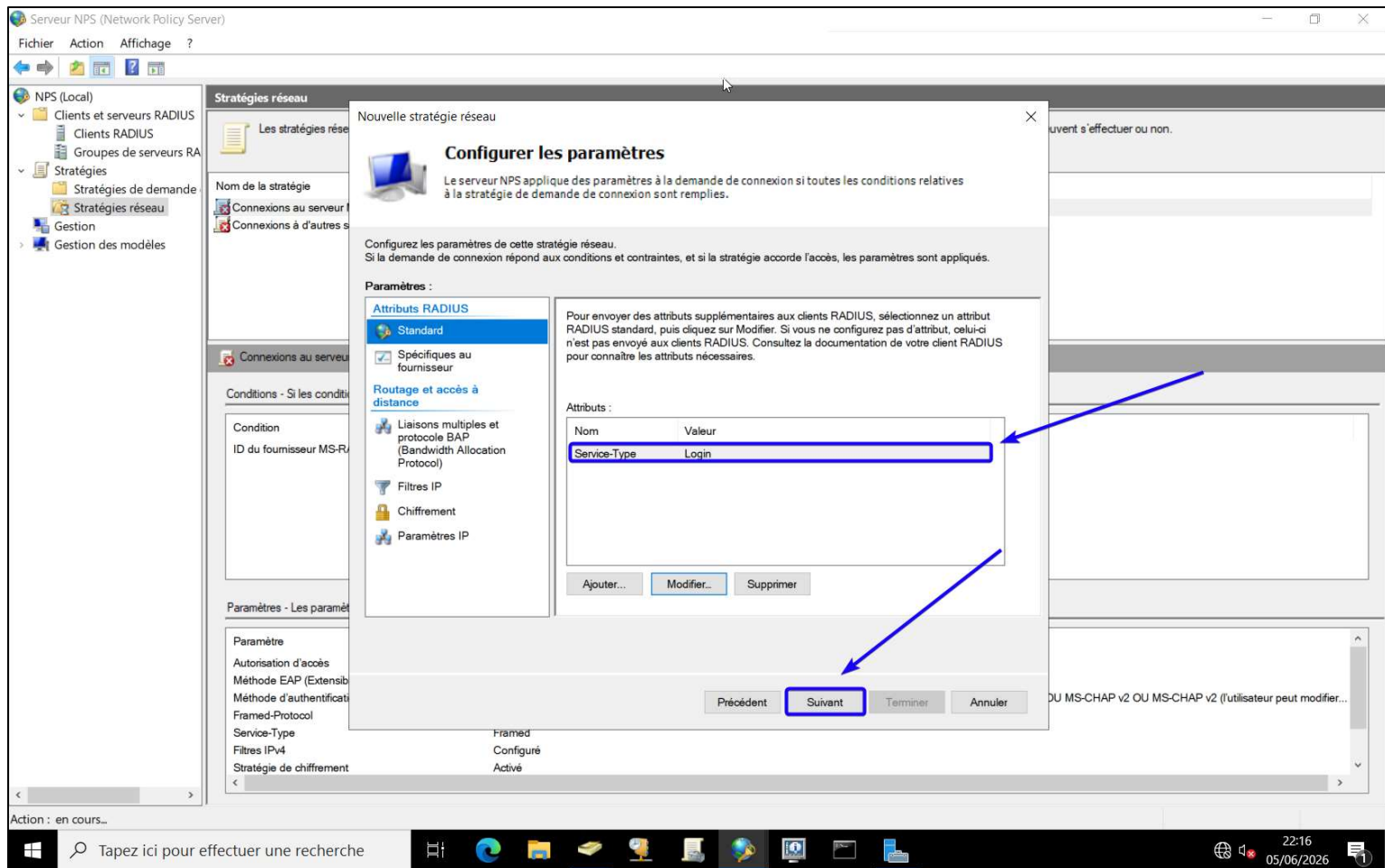












Serveur NPS (Network Policy Server)

FichierActionAffichage?

NPS (Local)

Clients et serveurs RADIUS

Stratégies

Stratégies de demande

Stratégies réseau

Gestion

Gestion des modèles

Stratégies réseau

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

Nom de la stratégie	État	Ordre de traitement	Type d'accès	Source
SSH-Admins-Domaine	Activé	1	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Activé	2	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Activé	3	Refuser l'accès	Non spécifié

SSH-Admins-Domaine

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes d'utilisateurs	SMARTHOME\Admins du domaine

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Méthode d'authentification	Protocole EAP OU Authentification non chiffrée (PAP, SPAP) OU MS-CHAP v1 OU MS-CHAP v1 (l'utilisateur peut modifier le mot de passe après son expiration) OU MS-CHAP...
Autorisation d'accès	Accorder l'accès
Service-Type	Login
Méthode EAP (Extensible Authentication Protocol)	Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)

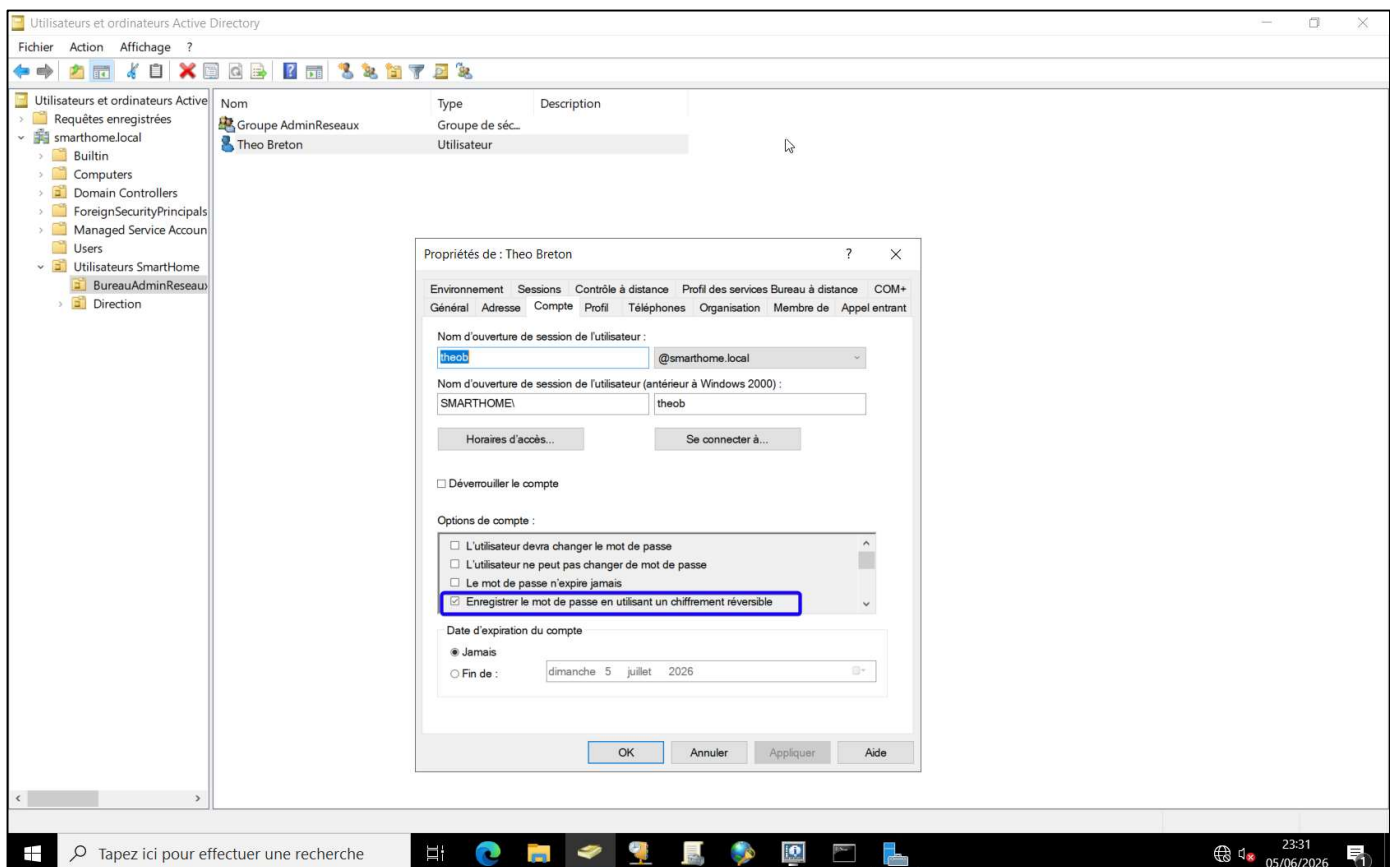
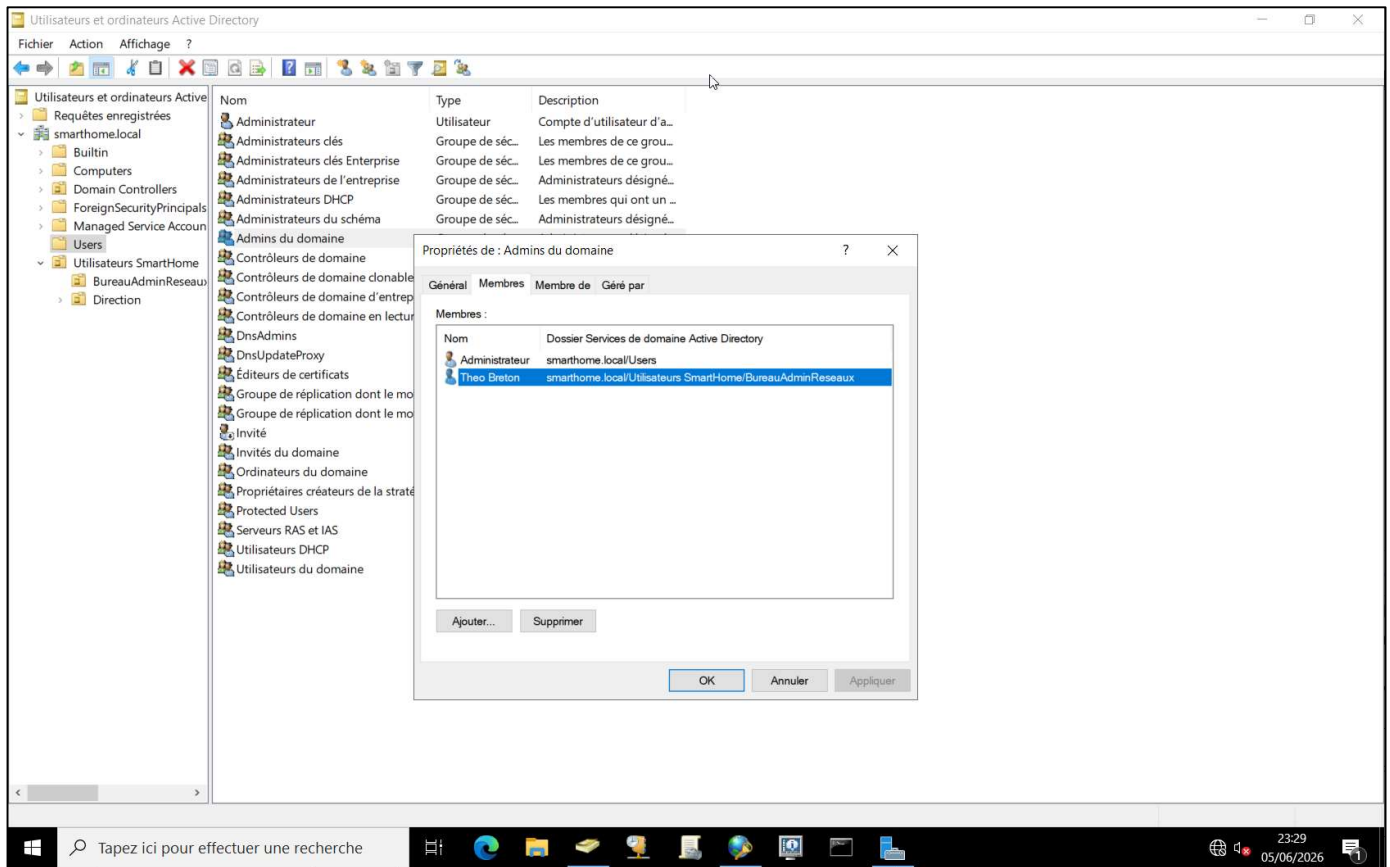
Tapez ici pour effectuer une recherche

23:20

05/06/2026

Configuration de l'utilisateur AdminRéseaux :

- Ajout de l'utilisateur dans le groupe Admin du domaine
- Onglet Compte : cocher "Enregistrer le mot de passe en utilisant un chiffrement réversible"



Étape 1 : Activation du modèle AAA global

Cette commande est obligatoire pour que le switch accepte de créer des règles de sécurité basées sur un serveur distant.

```
SW1# configure terminal
SW1(config)# aaa new-model
```

Protocole AAA

17 langues

Article Discussion Lire Modifier Modifier le code Voir l'historique Outils

Cet article est une **ébauche** concernant la **sécurité informatique**.
Vous pouvez partager vos connaissances en l'améliorant (**comment ?**) selon les recommandations des **projets correspondants**.

Pour les articles homonymes, voir **AAA**.

En **sécurité informatique**, **AAA** correspond à un **protocole** qui réalise trois fonctions : l'**authentification**, l'**autorisation**, et la **traçabilité** (en anglais : *Authentication, Authorization, Accounting/Auditing*).

AAA est un modèle de sécurité implémenté dans certains **routeurs Cisco** mais que l'on peut également utiliser sur toute machine qui peut servir de NAS (*Network Access Server*), ou certains **switches Alcatel**.

AAA est la base des protocoles de télécommunication **RADIUS** et **Diameter** qui sont notamment utilisés dans les réseaux mobiles **UMTS** et **LTE**¹ pour authentifier et autoriser l'accès des terminaux mobiles au réseau.

Liste de protocoles AAA

[modifier | modifier le code]

- RADIUS**
- Diameter**
- TACACS**
- TACACS+**

Source : https://fr.wikipedia.org/wiki/Protocole_AAA

Étape 2 : Configuration de l'authentification et l'autorisation SSH

```
SW1(config)# aaa authentication dot1x default group radius
SW1(config)# aaa authorization exec default group radius local
```

Étape 3 : Déclaration du serveur RADIUS

```
SW1(config)# radius server AD-SMARTHOME
SW1(config-radius-server)# address ipv4 192.168.20.1 auth-port 1812 acct-port 1813
SW1(config-radius-server)# key cisco
SW1(config-radius-server)# exit
```

Étape 4 : Activation de l'attribut Service-Type pour SSH

```
SW1(config)# radius-server attribute 6 on-for-login-auth
```

Étape 5 : Configuration des lignes VTY

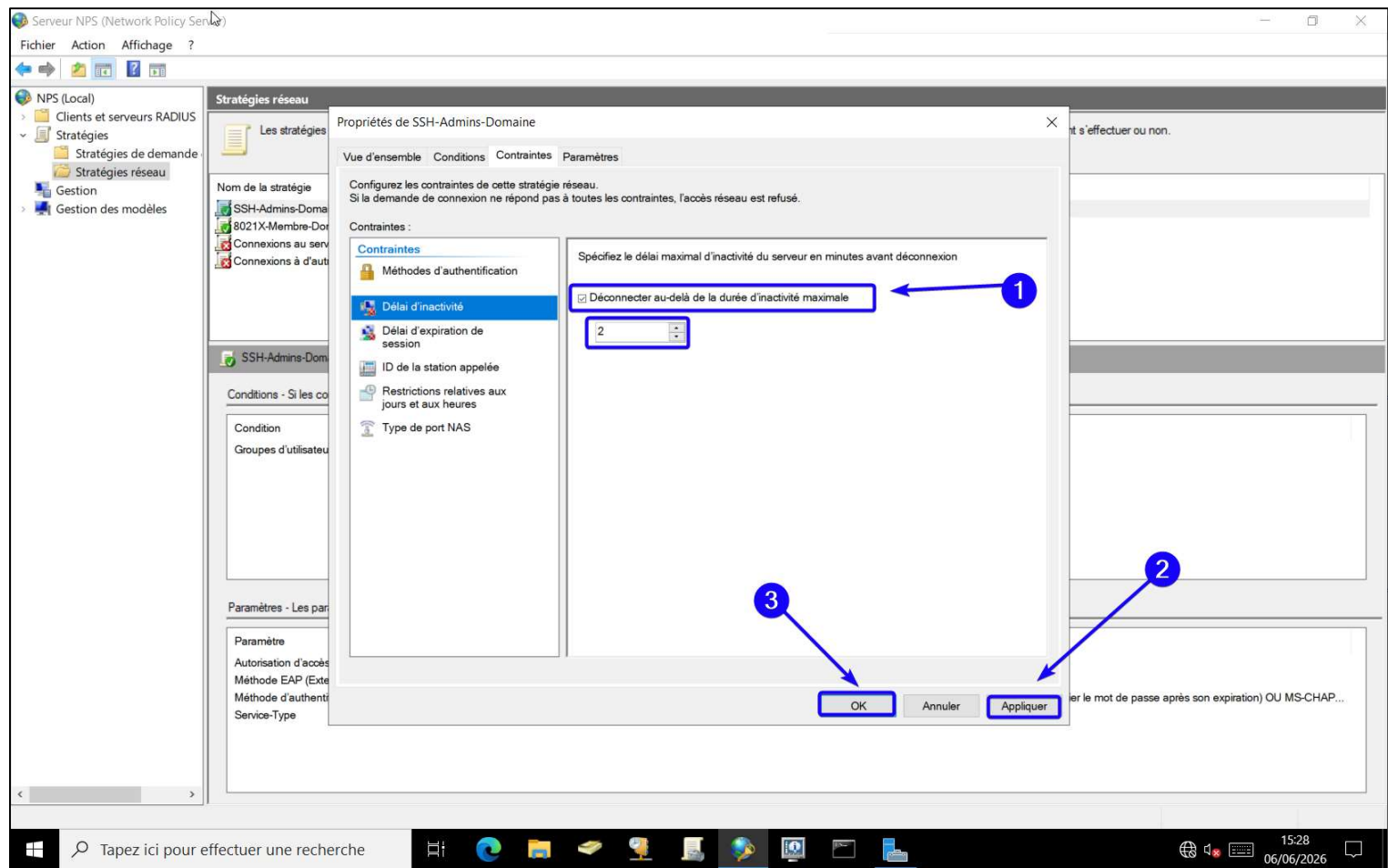
```
SW1(config)# line vty 0 4
SW1(config-line)# login authentication default
SW1(config-line)# authorization exec default
SW1(config-line)# transport input ssh
SW1(config-line)# exit
```

Étape 6 : Sauvegarde de la configuration

Pour éviter de perdre ton travail si le switch redémarre :

```
SW1(config)# exit
SW1# write memory
```

Pour plus de sécurité j'ai ajouté un délai d'inactivité sur les sessions ouverte. Après 2 minutes d'inactivité la personne aura sa session de verrouiller.





Test de Validation :

CAS N°1 : On se connecte avec un utilisateur autorisé, en l'occurrence l'utilisateur Théo Breton qui est l'AdminRéseaux de SMARTHOME.

Logs SW1 :

```
*Jun  5 23:36:54.946: RADIUS/ENCODE(00000016):Orig. component type
= Exec
*Jun  5 23:36:54.946: RADIUS:  AAA Unsupported Attr: interface
[221] 4    3123053124
*Jun  5 23:36:54.946: RADIUS(00000016): Config NAS IP: 0.0.0.0
*Jun  5 23:36:54.946: RADIUS(00000016): Config NAS IPv6: ::
*Jun  5 23:36:54.946: RADIUS/ENCODE(00000016): acct_session_id: 12
*Jun  5 23:36:54.946: RADIUS(00000016): sending
*Jun  5 23:36:54.946: RADIUS/ENCODE: Best Local IP-Address
192.168.20.253 for Radius-Server 192.168.20.1
*Jun  5 23:36:54.946: RADIUS(00000016): Sending a IPv4 Radius
Packet
*Jun  5 23:36:54.946: RADIUS(00000016): Send Access-Request to
192.168.20.1:1812 id 1645/11,len 75
*Jun  5 23:36:54.946: RADIUS:  authenticator CE 39 4A D7 92 49 BF
53 - 5A 08 CC 9D 5C 23 2C E3
*Jun  5 23:36:54.946: RADIUS:  User-Name          [1]    7
"theob"
*Jun  5 23:36:54.946: RADIUS:  User-Password      [2]    18  *
*Jun  5 23:36:54.946: RADIUS:  NAS-Port          [5]     6    2
*Jun  5 23:36:54.946: RADIUS:  NAS-Port-Id       [87]    6    "tty2"
*Jun  5 23:36:54.946: RADIUS:  NAS-Port-Type     [61]    6
Virtual                    [5]
*Jun  5 23:36:54.946: RADIUS:  Service-Type      [6]     6    Login
[1]
*Jun  5 23:36:54.946: RADIUS:  NAS-IP-Address    [4]     6
192.168.20.253
Username:
*Jun  5 23:36:54.946: RADIUS(00000016): Started 5 sec timeout
*Jun  5 23:36:54.985: RADIUS: Received from id 1645/11
192.168.20.1:1812, Access-Accept, len 72
*Jun  5 23:36:54.985: RADIUS:  authenticator CC 49 40 35 E7 A1 E6
58 - CB 85 3D E9 9D 2E 5B 01
*Jun  5 23:36:54.985: RADIUS:  Service-Type      [6]     6    Login
[1]
*Jun  5 23:36:54.985: RADIUS:  Class              [25]    46
*Jun  5 23:36:54.985: RADIUS:  AE 6D 09 27 00 00 01 37 00 01 02 00
C0 A8 14 01 00 00 00 00 3D 45 7C 4D 75 D8 64 E7 01 DC F5 1C 28 06
A2 B0 00 00 00 00 00 00 1D          [ m'7=E|Mud(]
*Jun  5 23:36:54.985: RADIUS(00000016): Received from id 1645/11
Username:
*Jun  5 23:36:57.822: AAA: parse name=tty2 idb type=-1 tty=-1
*Jun  5 23:36:57.822: AAA: name=tty2 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=2 channel=0
```

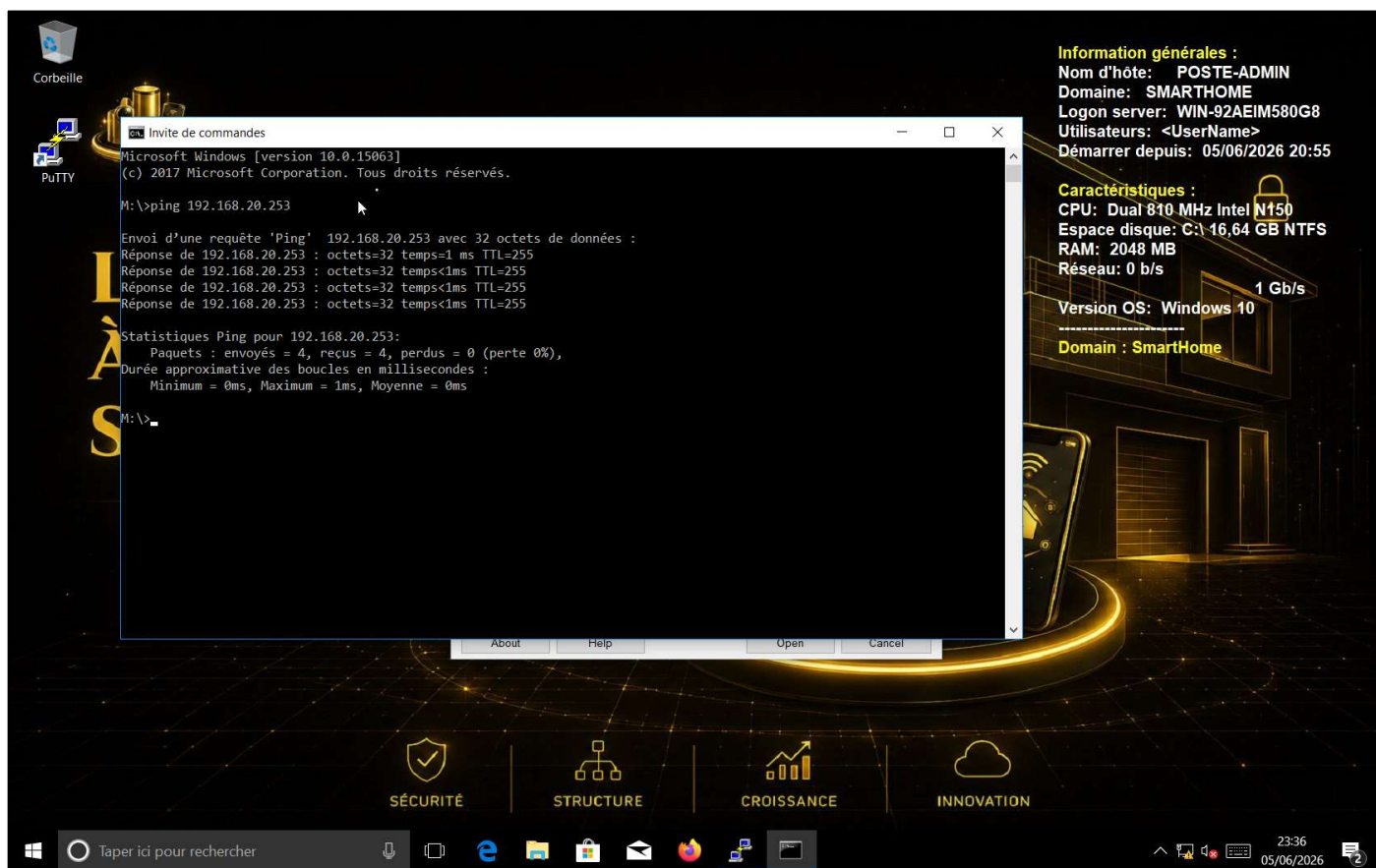


```

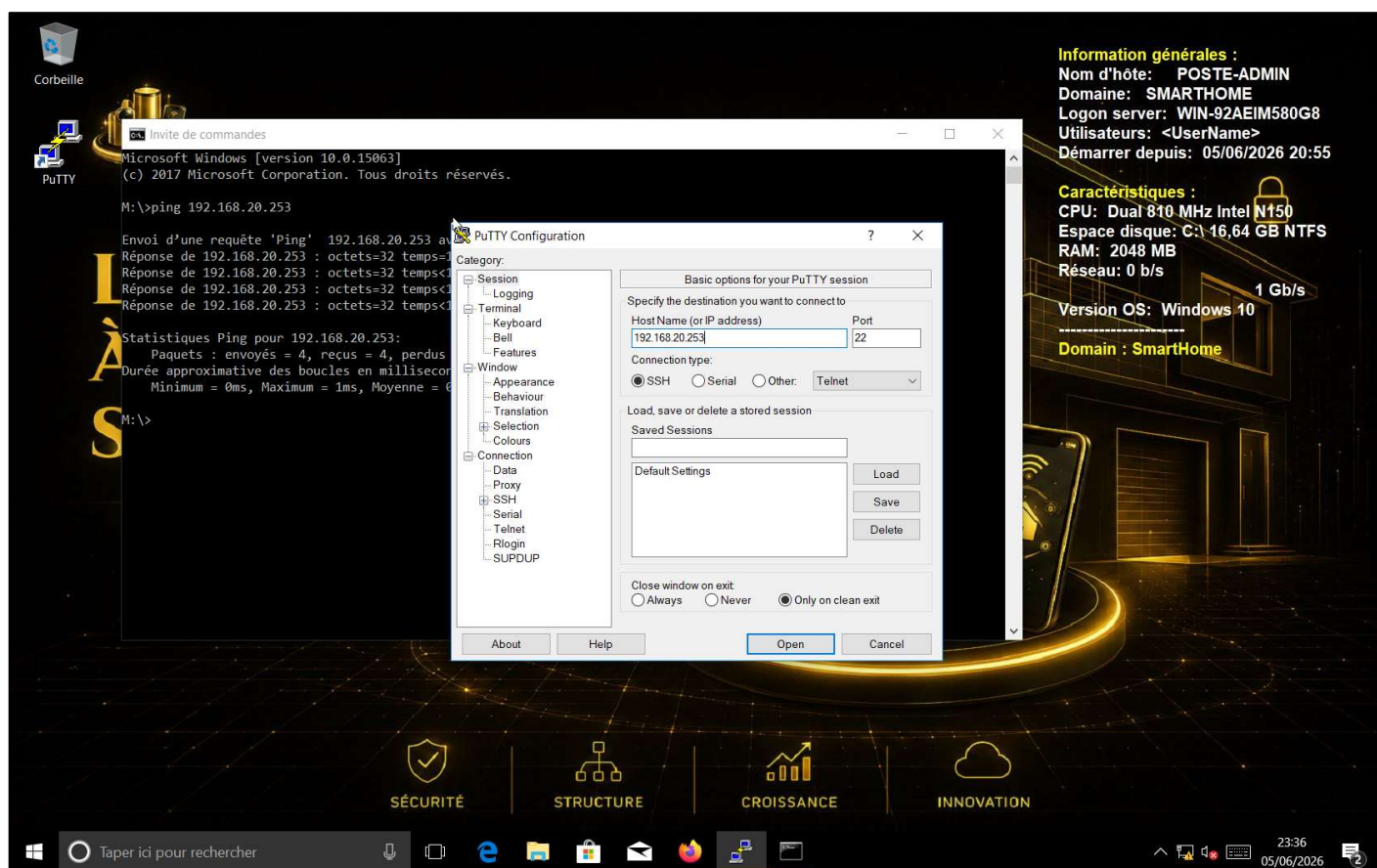
*Jun  5 23:36:57.822: AAA/MEMORY: create_user (0xBB1191D8)
user='theob' ruser='NULL' ds0=0 port='tty2' rem_addr='192.168.20.4'
authen_type=ASCII service=ENABLE priv=15 initial_task_id='0', vrf=
(id=0)
*Jun  5 23:36:57.822: AAA/AUTHEN/START (568529534): port='tty2'
list='' action=LOGIN service=ENABLE
*Jun  5 23:36:57.822: AAA/AUTHEN/START (568529534): console enable
- default to enable password (if any)
*Jun  5 23:36:57.822: AAA/AUTHEN/START (568529534): Method=ENABLE
Username:
*Jun  5 23:36:57.822: AAA/AUTHEN(568529534): can't find any
passwords
*Jun  5 23:36:57.822: AAA/AUTHEN (568529534): status = ERROR
*Jun  5 23:36:57.822: AAA/AUTHEN/START (568529534): Method=NONE
*Jun  5 23:36:57.822: AAA/AUTHEN (568529534): status = PASS
*Jun  5 23:36:57.822: AAA/MEMORY: free_user (0xBB1191D8)
user='theob' ruser='NULL' port='tty2' rem_addr='192.168.20.4'
authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)

```

On vérifie que le poste communique avec l'adresse IP du VLAN.



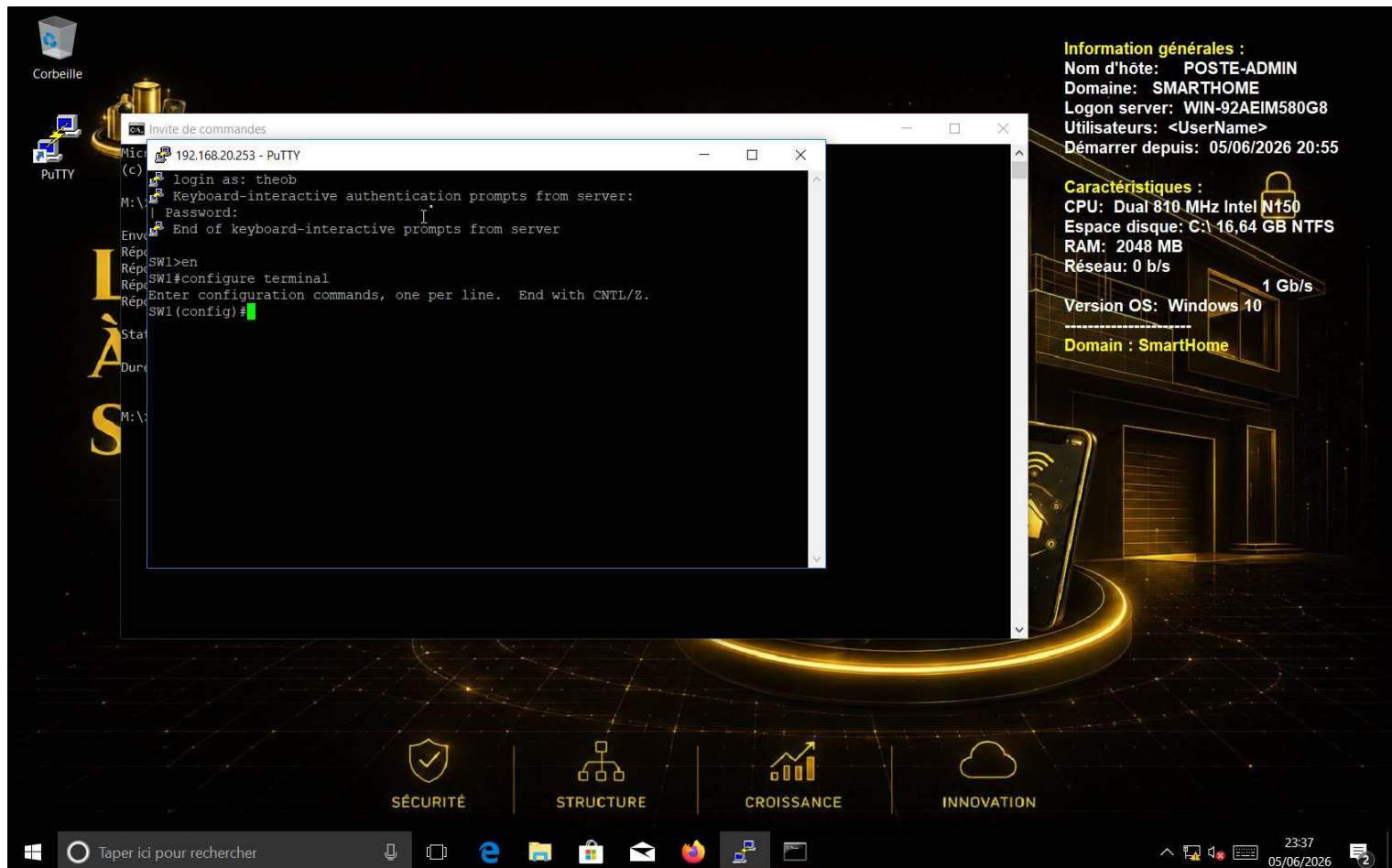
Ensuite une fois que la communication est validée on lance une session SSH.



Puis on se connecte via nos identifiant Active Directory

Pour mon cas :

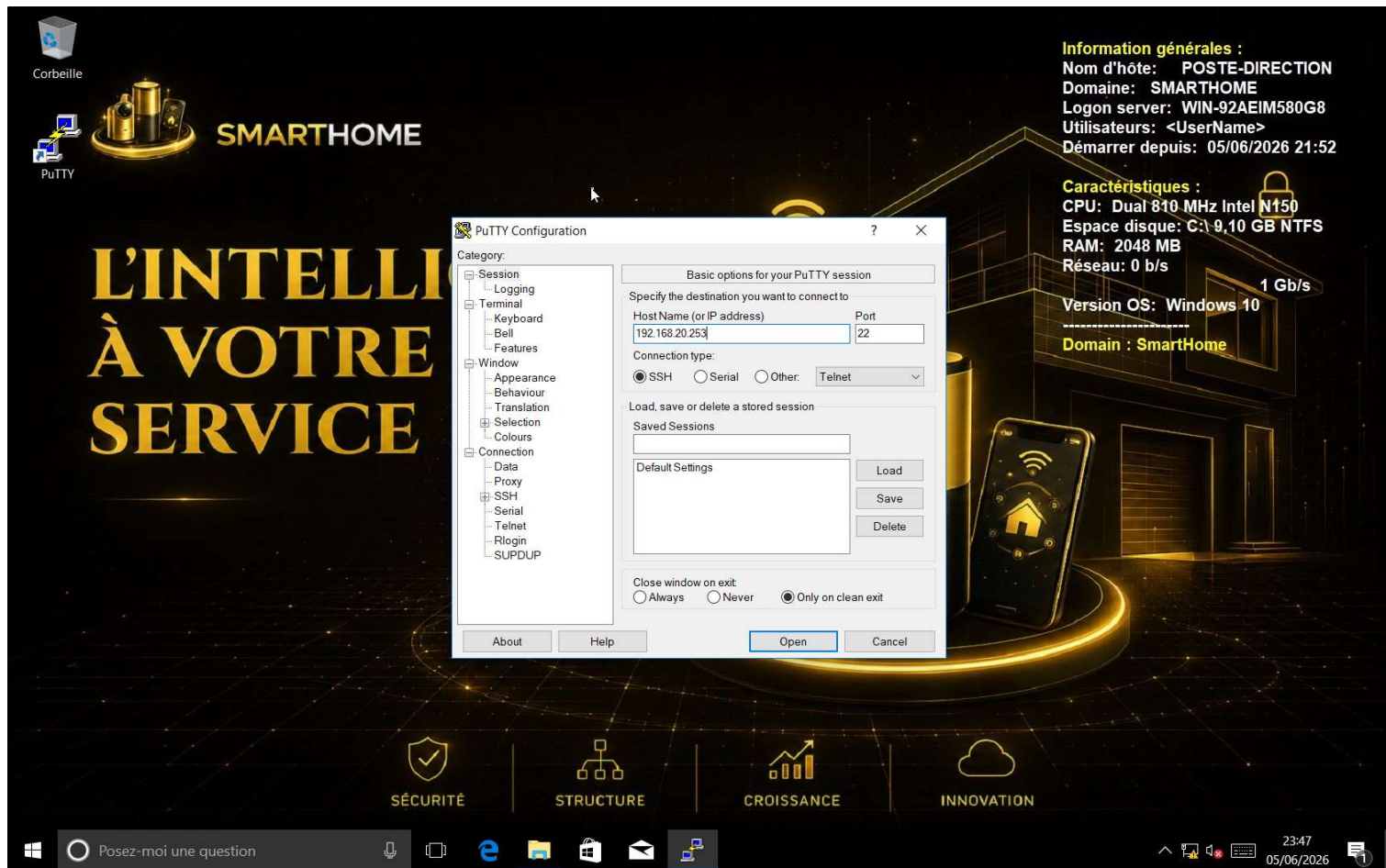
Identifiant : theob
MDP : Admin1234



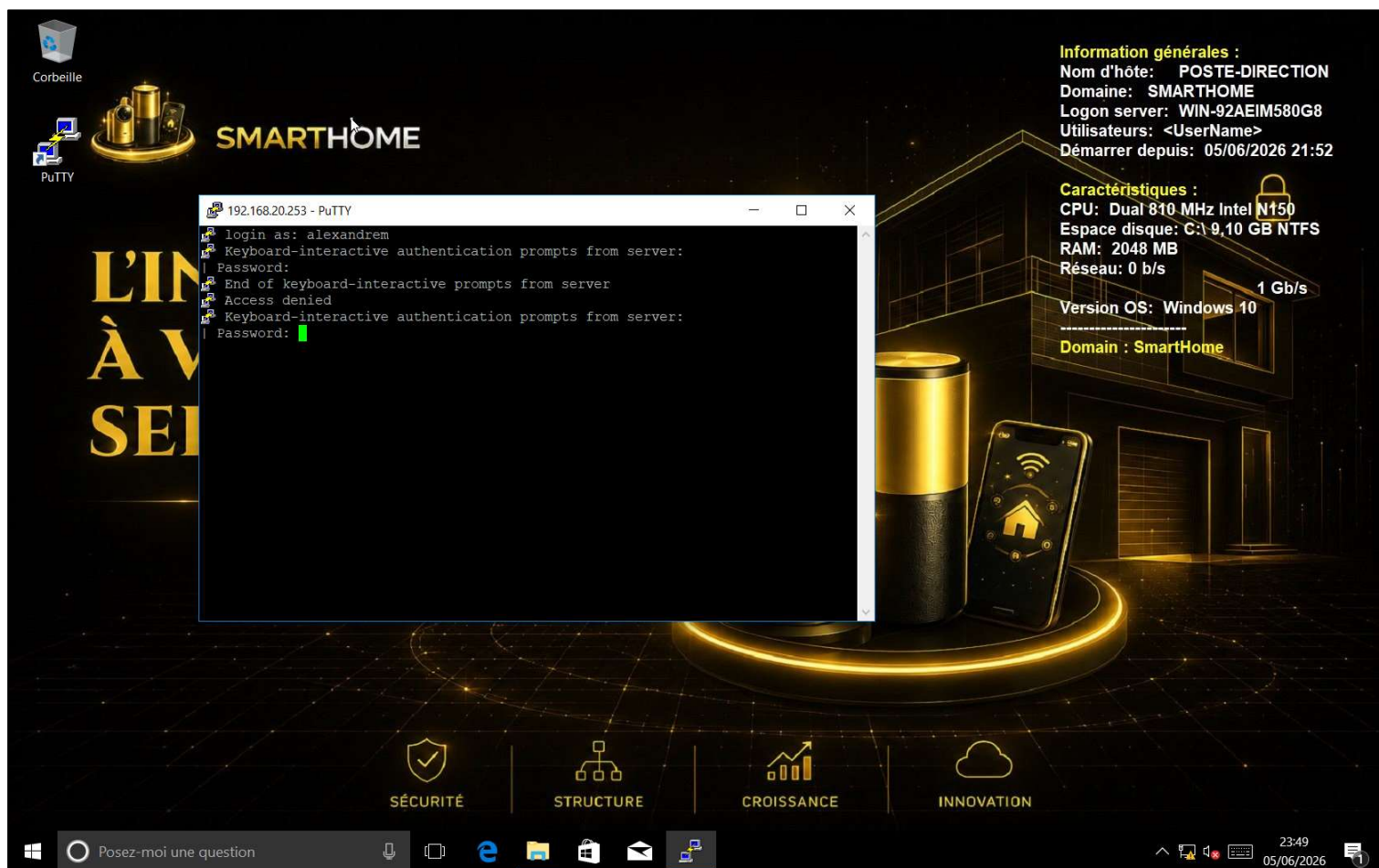
CAS N°2 : On se connecte avec un utilisateur qui n'est pas autorisé, en l'occurrence l'utilisateur Alexandre Marti qui est le directeur de SMARTHOME.

Logs SW1 :

```
*Jun  5 23:47:02.873: %SYS-5-CONFIG_I: Configured from console by
theob on vty0 (192.168.20.4)
*Jun  5 23:47:39.427: AAA/BIND(00000017): Bind i/f
*Jun  5 23:47:39.427: AAA/AUTHEN/LOGIN (00000017): Pick method list
'default'
*Jun  5 23:47:39.427: RADIUS/ENCODE(00000017): ask "Password: "
*Jun  5 23:47:39.427: RADIUS/ENCODE(00000017): send packet;
GET_PASSWORD
*Jun  5 23:47:44.229: RADIUS/ENCODE(00000017):Orig. component type
= Exec
*Jun  5 23:47:44.229: RADIUS:  AAA Unsupported Attr: interface
[221] 4    3123053124
*Jun  5 23:47:44.229: RADIUS(00000017): Config NAS IP: 0.0.0.0
*Jun  5 23:47:44.229: RADIUS(00000017): Config NAS IPv6: ::
*Jun  5 23:47:44.229: RADIUS/ENCODE(00000017): acct_session_id: 13
*Jun  5 23:47:44.229: RADIUS(00000017): sending
*Jun  5 23:47:44.229: RADIUS/ENCODE: Best Local IP-Address
192.168.20.253 for Radius-Server 192.168.20.1
*Jun  5 23:47:44.229: RADIUS(00000017): Sending a IPv4 Radius
Packet
*Jun  5 23:47:44.229: RADIUS(00000017): Send Access-Request to
192.168.20.1:1812 id 1645/12,len 80
*Jun  5 23:47:44.229: RADIUS:  authenticator F3 16 4B D8 0F 50 D6
DB - EB F5 63 9C 55 A7 14 95
*Jun  5 23:47:44.229: RADIUS:  User-Name          [1]    12
"alexandrem"
*Jun  5 23:47:44.229: RADIUS:  User-Password      [2]    18  *
*Jun  5 23:47:44.229: RADIUS:  NAS-Port           [5]     6   2
*Jun  5 23:47:44.229: RADIUS:  NAS-Port-Id        [87]    6  "tty2"
*Jun  5 23:47:44.229: RADIUS:  NAS-Port-Type      [61]    6
Virtual          [5]
*Jun  5 23:47:44.229: RADIUS:  Service-Type       [6]     6  Login
[1]
*Jun  5 23:47:44.229: RADIUS:  NAS-IP-Address     [4]     6
192.168.20.253
*Jun  5 23:47:44.229: RADIUS(00000017): Started 5 sec timeout
*Jun  5 23:47:44.237: RADIUS: Received from id 1645/12
192.168.20.1:1812, Access-Reject, len 20
*Jun  5 23:47:44.237: RADIUS:  authenticator E5 01 67 63 21 7B 5D
52 - 44 D0 1A 23 DB 8B D5 8B
*Jun  5 23:47:44.237: RADIUS(00000017): Received from id 1645/12
*Jun  5 23:47:46.249: AAA/AUTHEN/LOGIN (00000017): Pick method list
'default'
*Jun  5 23:47:46.249: RADIUS/ENCODE(00000017): ask "Password: "
*Jun  5 23:47:46.249: RADIUS/ENCODE(00000017): send packet;
GET_PASSWORD
```

Le directeur étant pas le groupe des admins du domaine, l'accès et refusé !



Ouverture de session à 15:34:56 :

192.168.20.253 - PuTTY

login as: theob
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
[SW1]>

Information générales :
Nom d'hôte: POSTE-ADMIN

15:34:56
samedi 6 juin 2026

juin 2026

lu	ma	me	je	ve	sa	di
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Aujourd'hui

Configurez vos calendriers pour voir où vous devez vous trouver

Prise en main

Masquer la configuration de l'agenda

SÉCURITÉ

STRUCTURE

CROISSANCE

INNOVATION

Taper ici pour rechercher

15:34
06/06/2026

2 minutes plus tard – 15:36:57 :

192.168.20.253 - PuTTY

login as: theob
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
[SW1]>

PuTTY Fatal Error

Remote side unexpectedly closed network connection

OK

Information générales :
Nom d'hôte: POSTE-ADMIN

15:36:57
samedi 6 juin 2026

juin 2026

lu	ma	me	je	ve	sa	di
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Aujourd'hui

Configurez vos calendriers pour voir où vous devez vous trouver

Prise en main

Masquer la configuration de l'agenda

SÉCURITÉ

STRUCTURE

CROISSANCE

INNOVATION

Taper ici pour rechercher

15:36
06/06/2026



Faire en sorte que aucune autre personne ne se branche sur le switch puisse obtenir une IP du serveur DHCP à part les utilisateurs du domaine.

Configuration de SW1 :

Les port ethernet 1/0 à 3 sont inutilisé on va donc mettre l'authentification au moyen du 802.1X

IEEE 802.1X

Article Discussion Lire Modifier Modifier le code Voir l'historique Outils

Cet article est une **ébauche** concernant la **sécurité informatique**.

Vous pouvez partager vos connaissances en l'améliorant (**comment ?**) selon les recommandations des **projets correspondants**.

802.1X est un **standard** lié à la sécurité des réseaux informatiques, mis au point en 2001 par l'**IEEE** (famille de la norme **IEEE 802**).

Il permet de contrôler l'accès aux équipements d'infrastructures réseau (et par ce biais, de relayer les informations liées aux dispositifs d'identification).

Principe général de fonctionnement [modifier | modifier le code]

En s'appuyant sur le protocole **EAP** pour le transport des informations d'identification en mode client/serveur, et sur un serveur d'authentification (tel que **RADIUS**, **TACACS**, **CAS**, etc.) le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil.

Si un équipement réseau actif, tel qu'un **commutateur réseau** ou une borne **Wi-Fi** est compatible avec la norme IEEE 802.1X, il est possible de contrôler l'accès à chacun de ses ports (PAE : Port Access Entity).

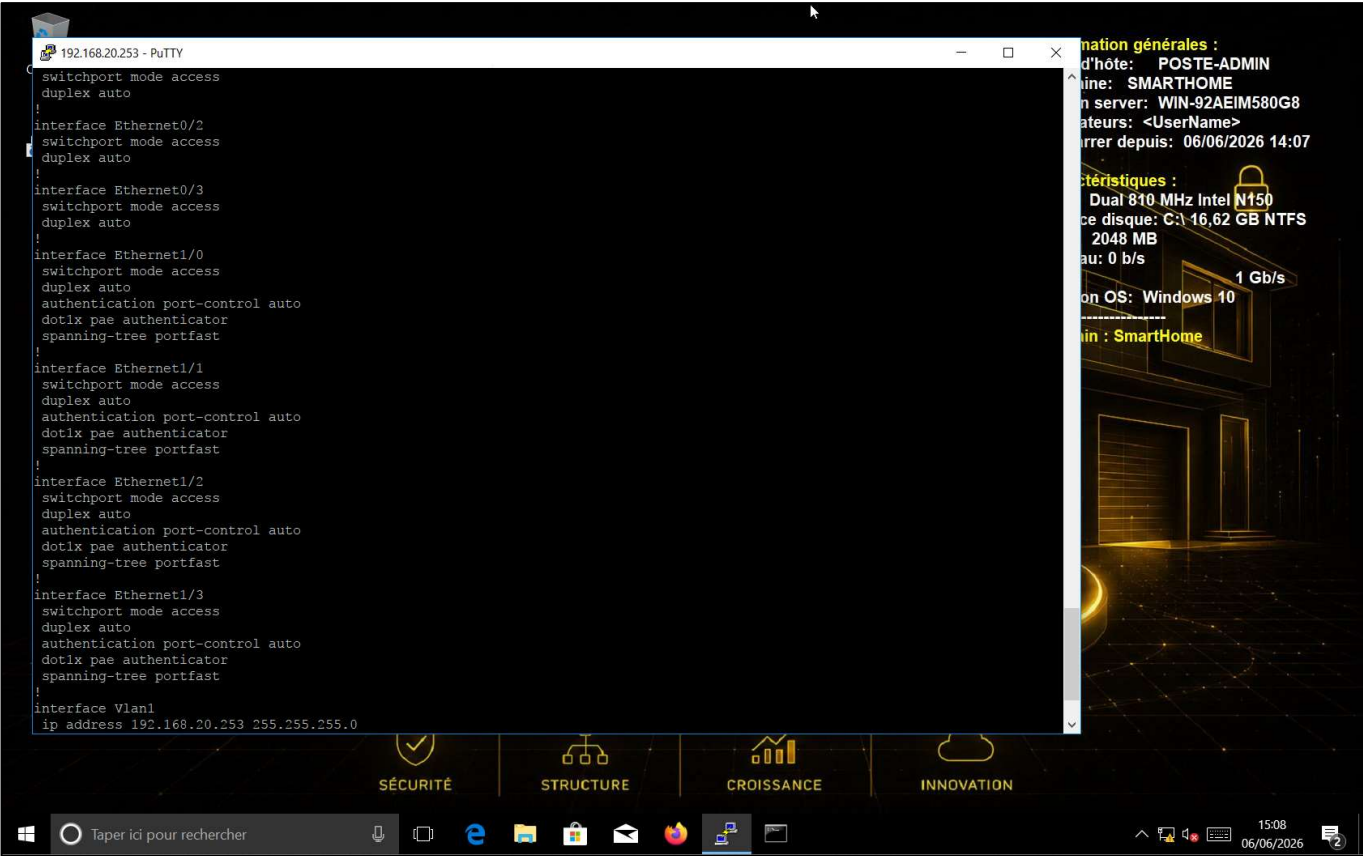
Indépendamment du type de connexion, chaque port se comporte alors comme une bascule à deux états : un état contrôlé en cas de succès d'identification et un état non contrôlé.

Diagramme montrant les protocoles impliqués dans l'authentification filaire 802.1X

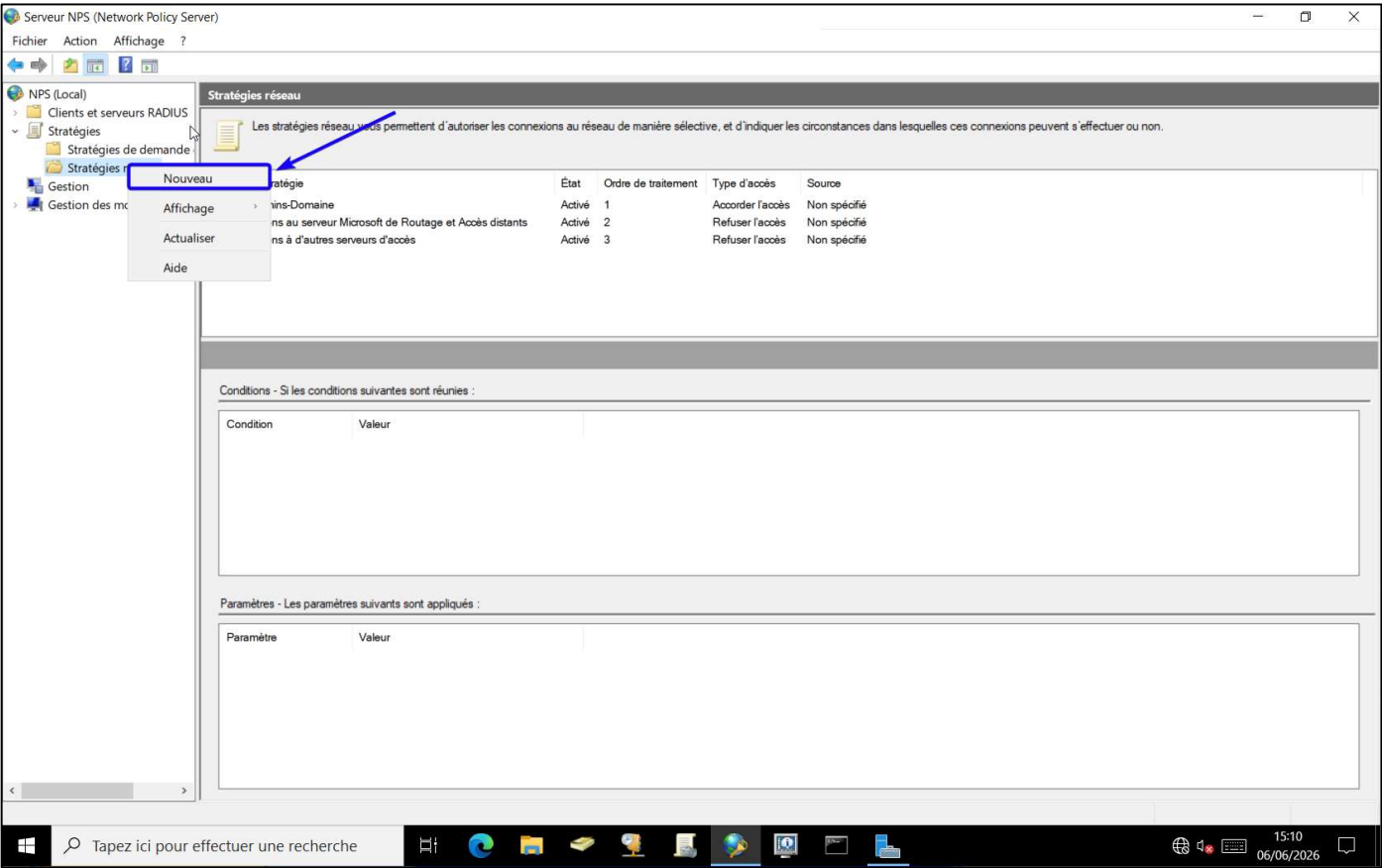
```
SW1(config)# aaa authentication dot1x default group radius
SW1(config)# dot1x system-auth-control
```

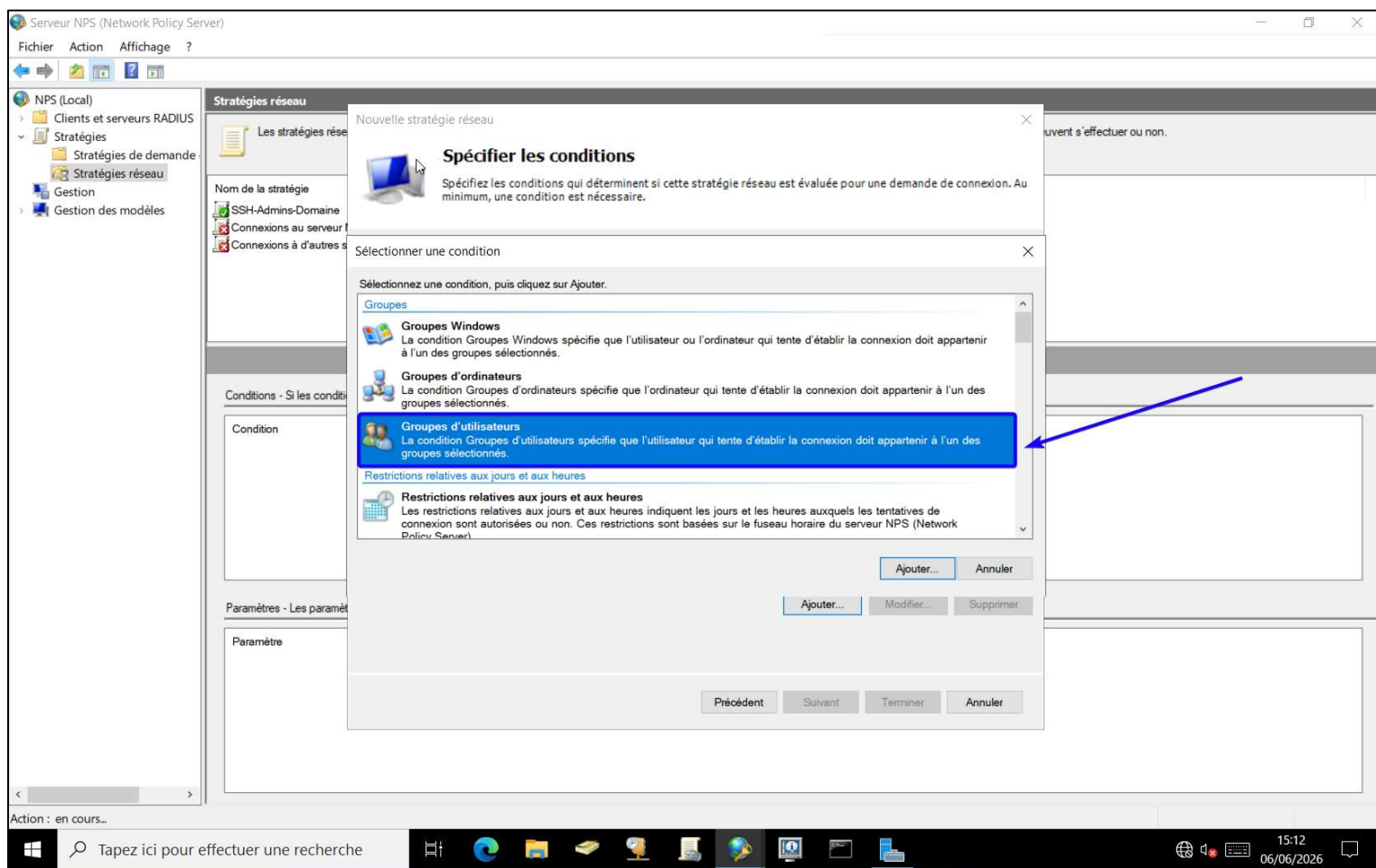
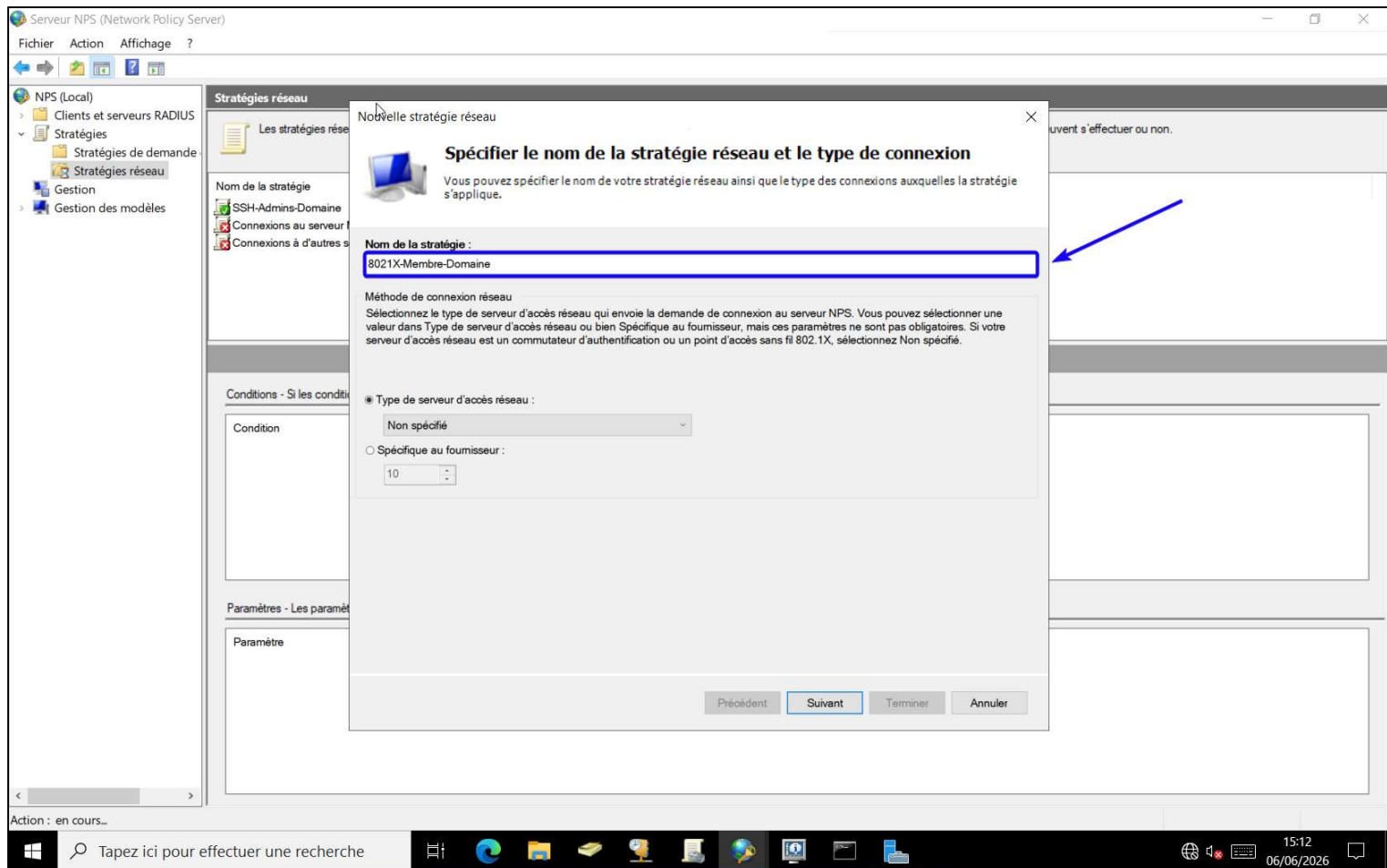
```
SW1(config)# interface range ethernet 1/0-3
SW1(config-if-range)# switchport mode access
SW1(config-if-range)# authentication port-control auto
SW1(config-if-range)# dot1x pae authenticator
SW1(config-if-range)# spanning-tree portfast
SW1(config-if-range)# exit
```

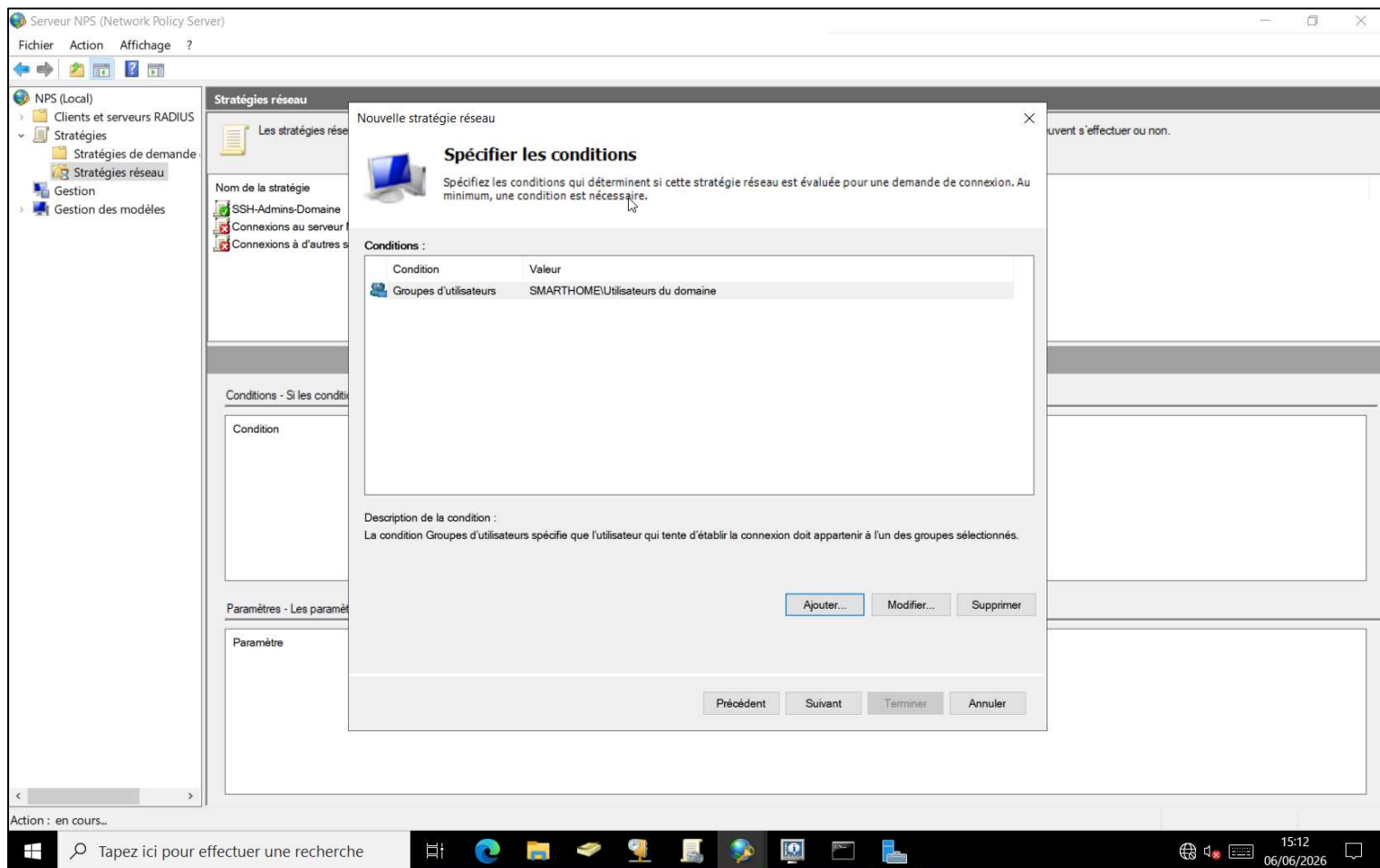
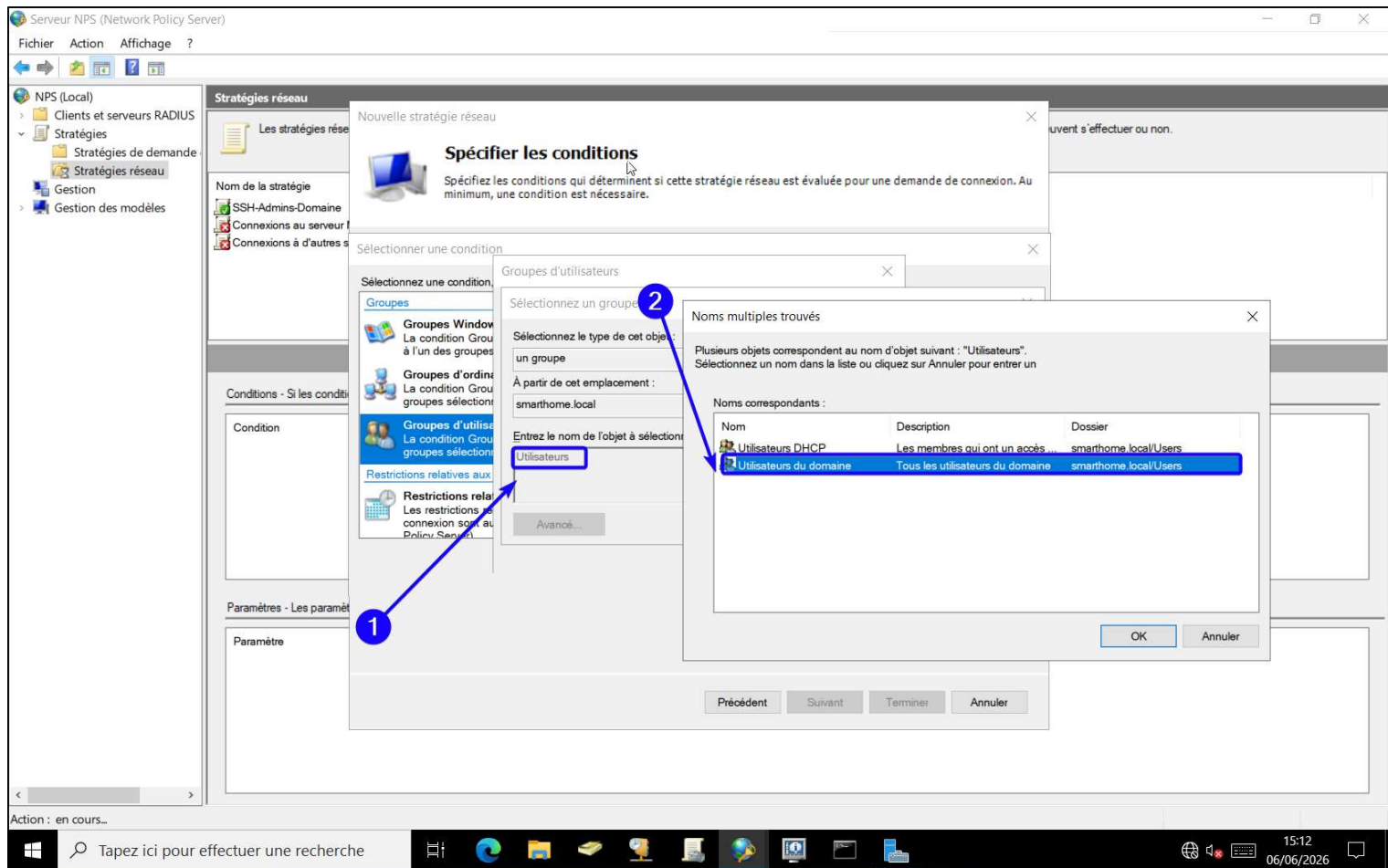
Vue d'ensemble :

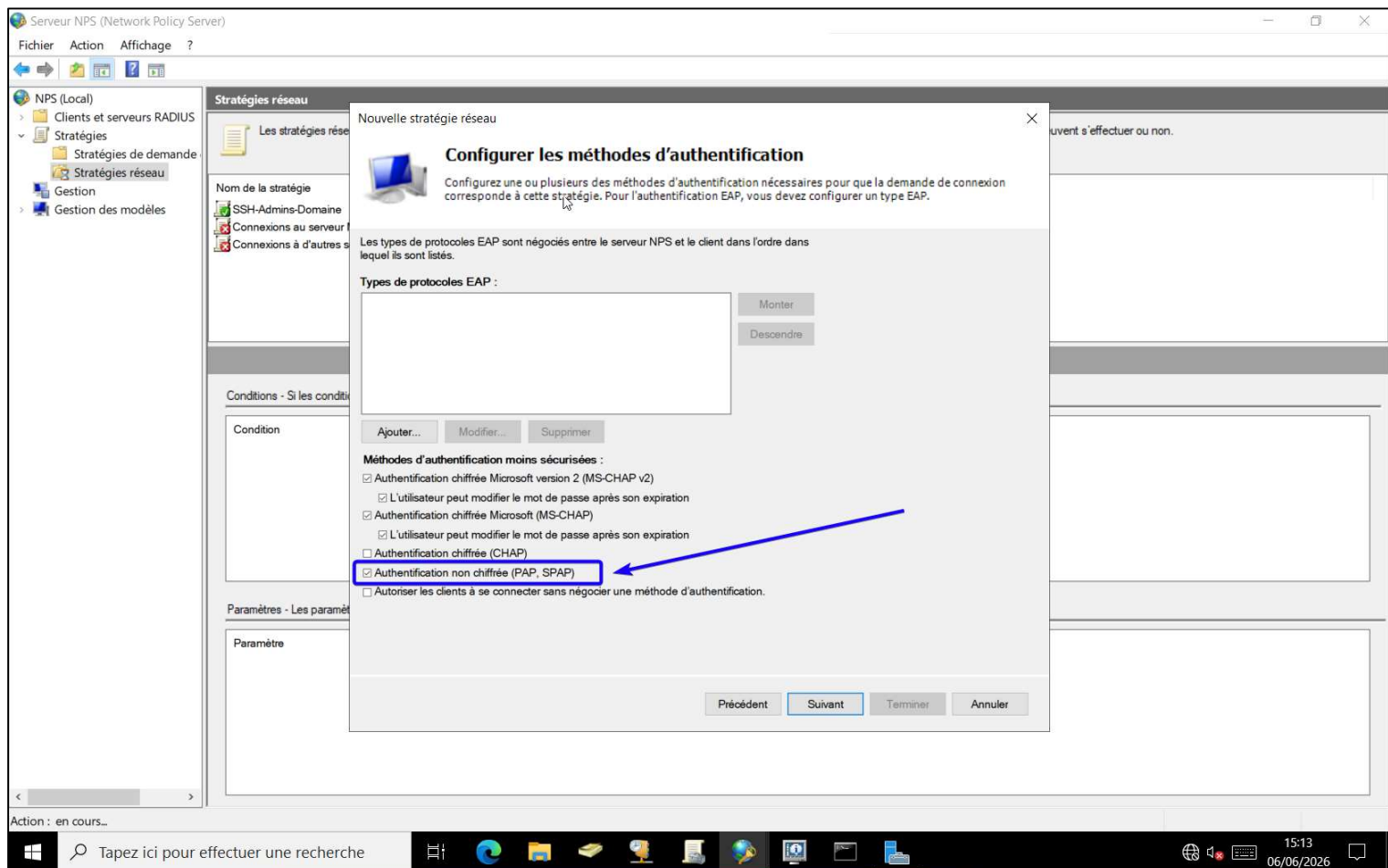
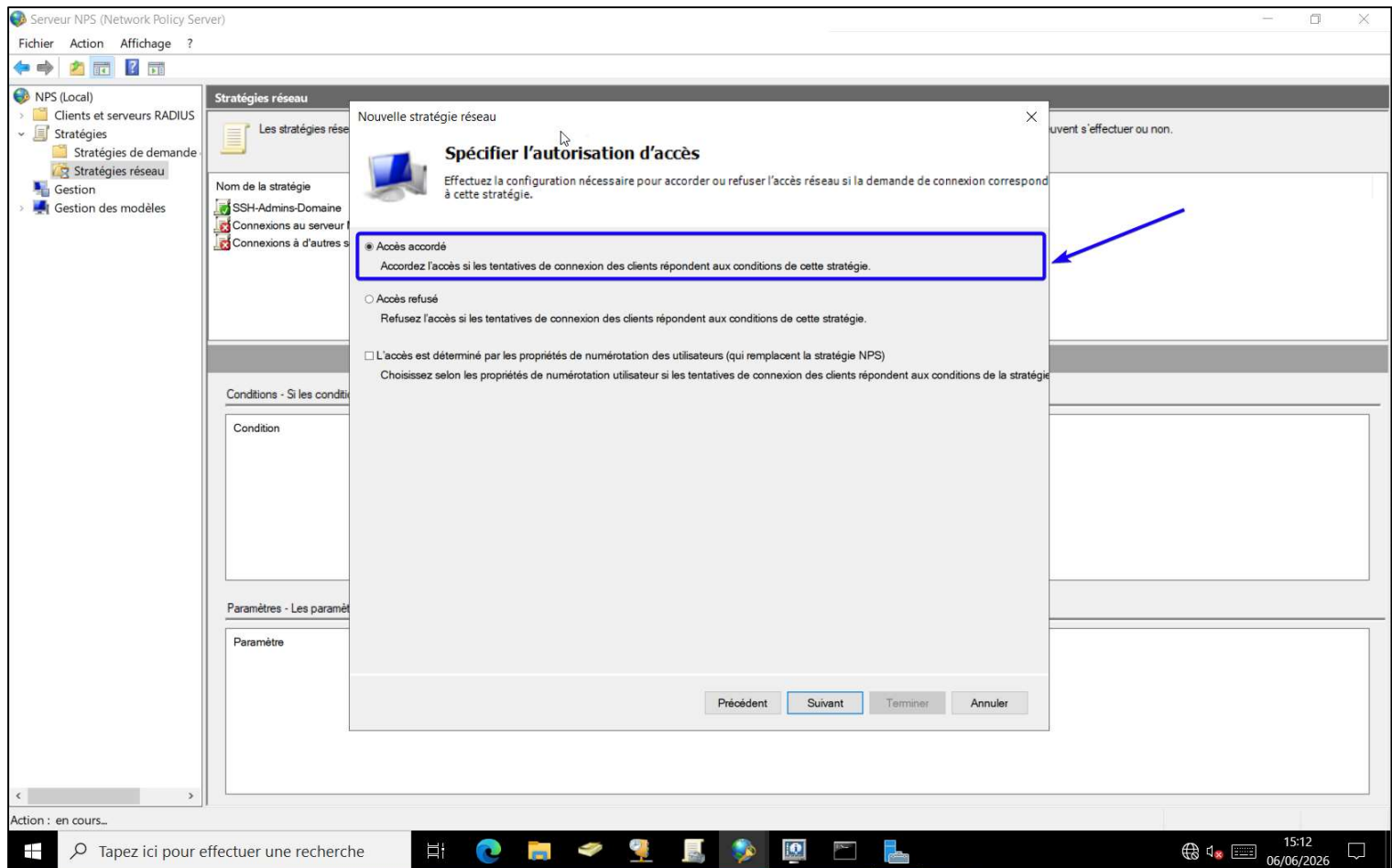


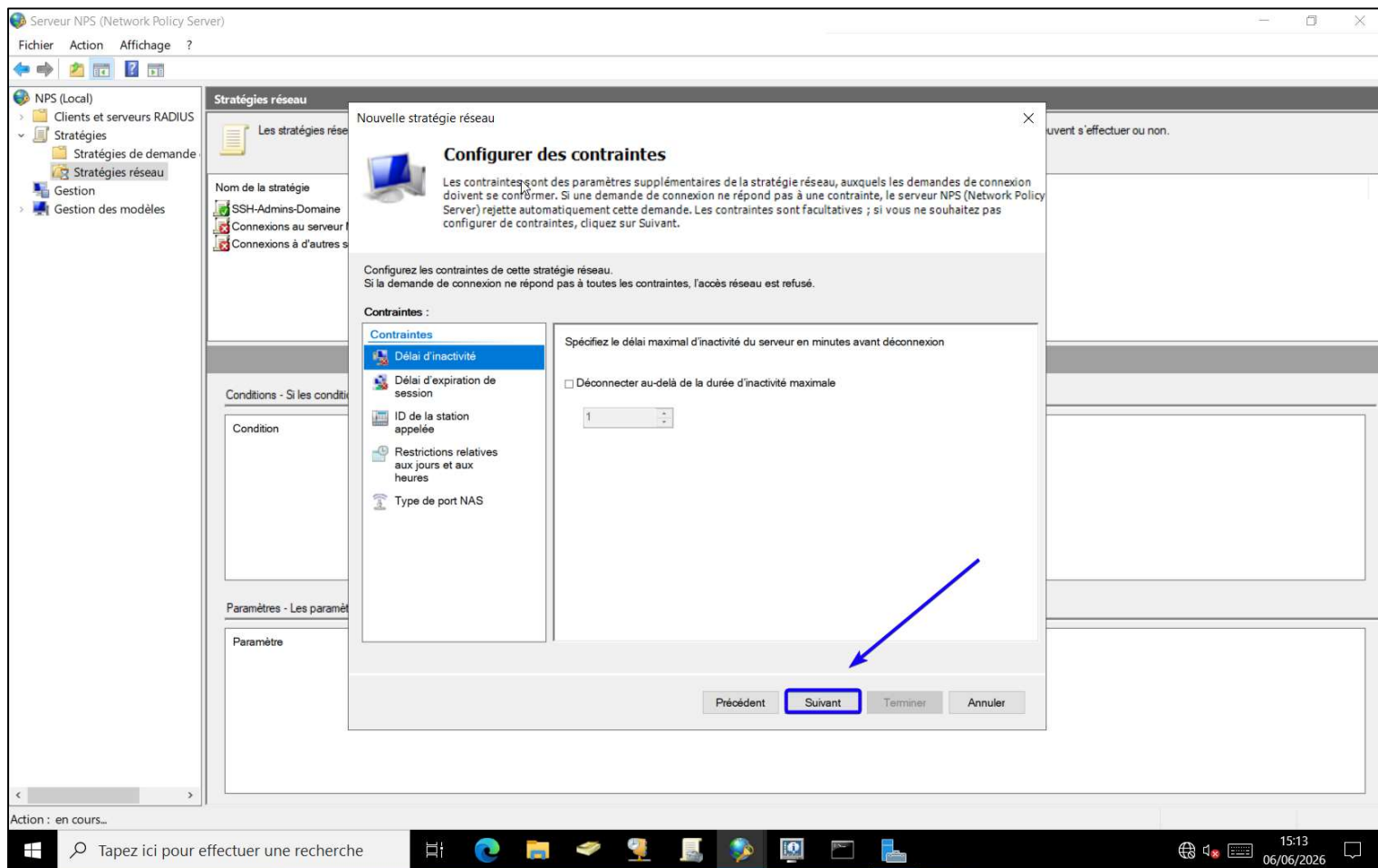
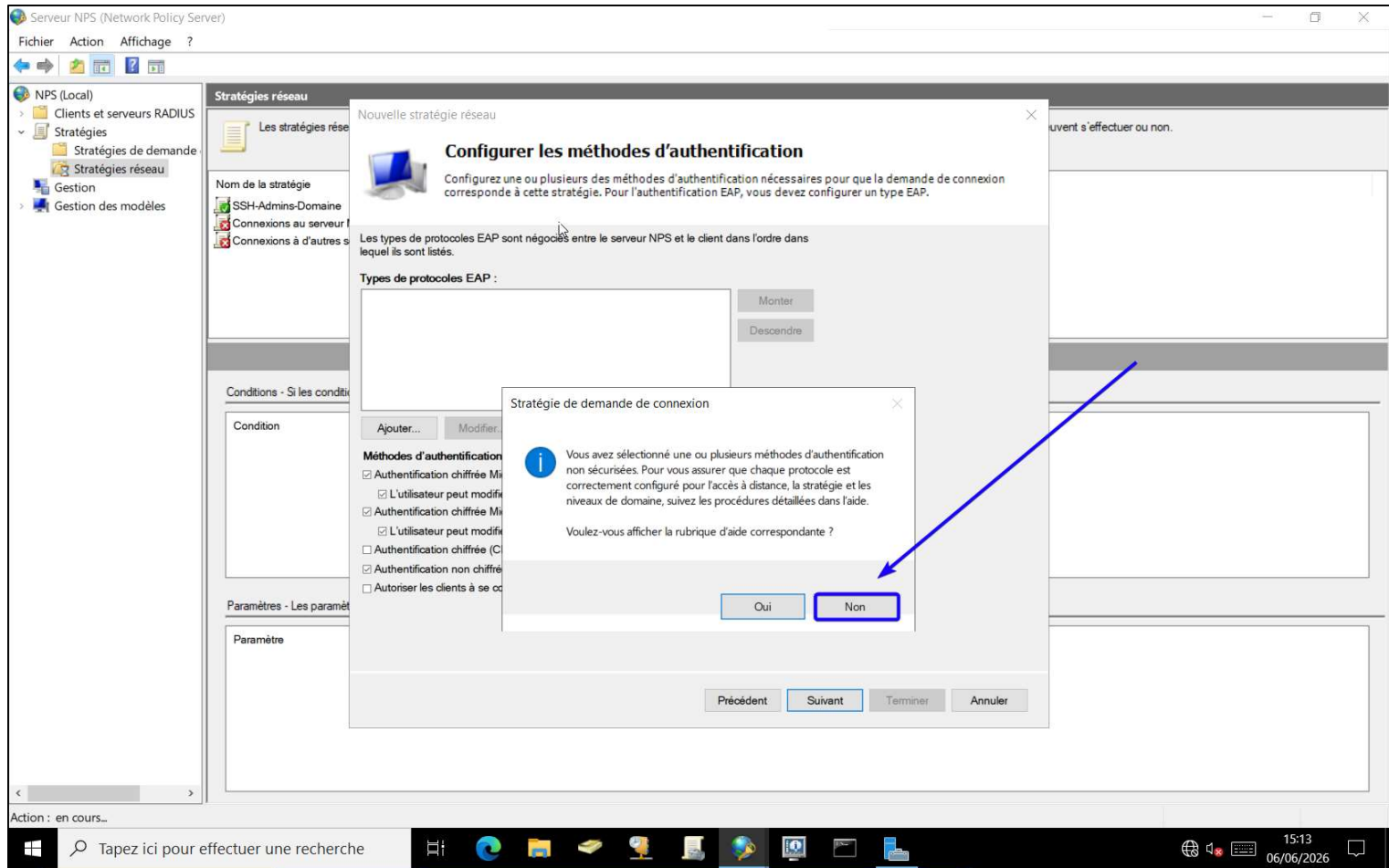
Configuration de la stratégie sur le service NPS :

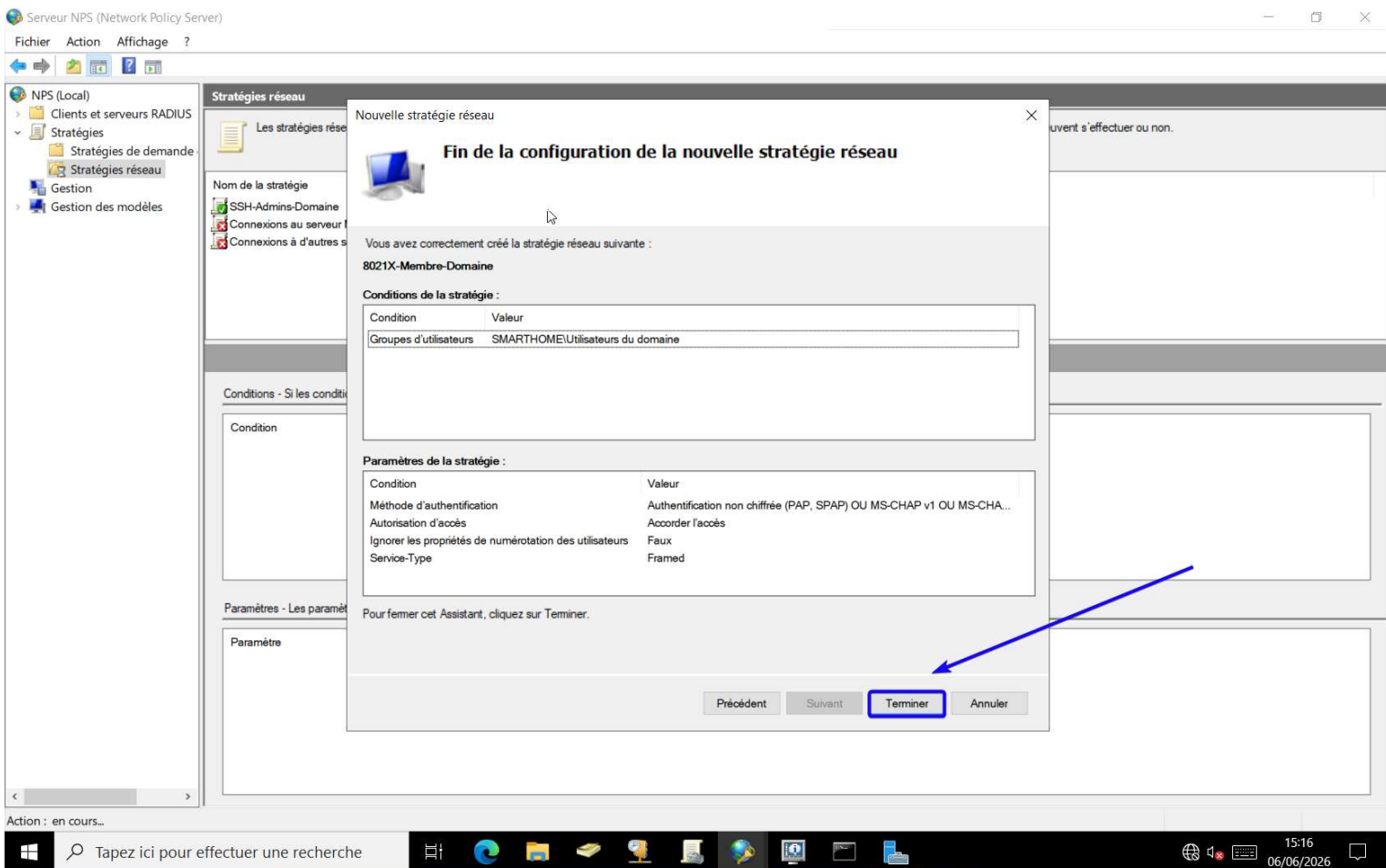
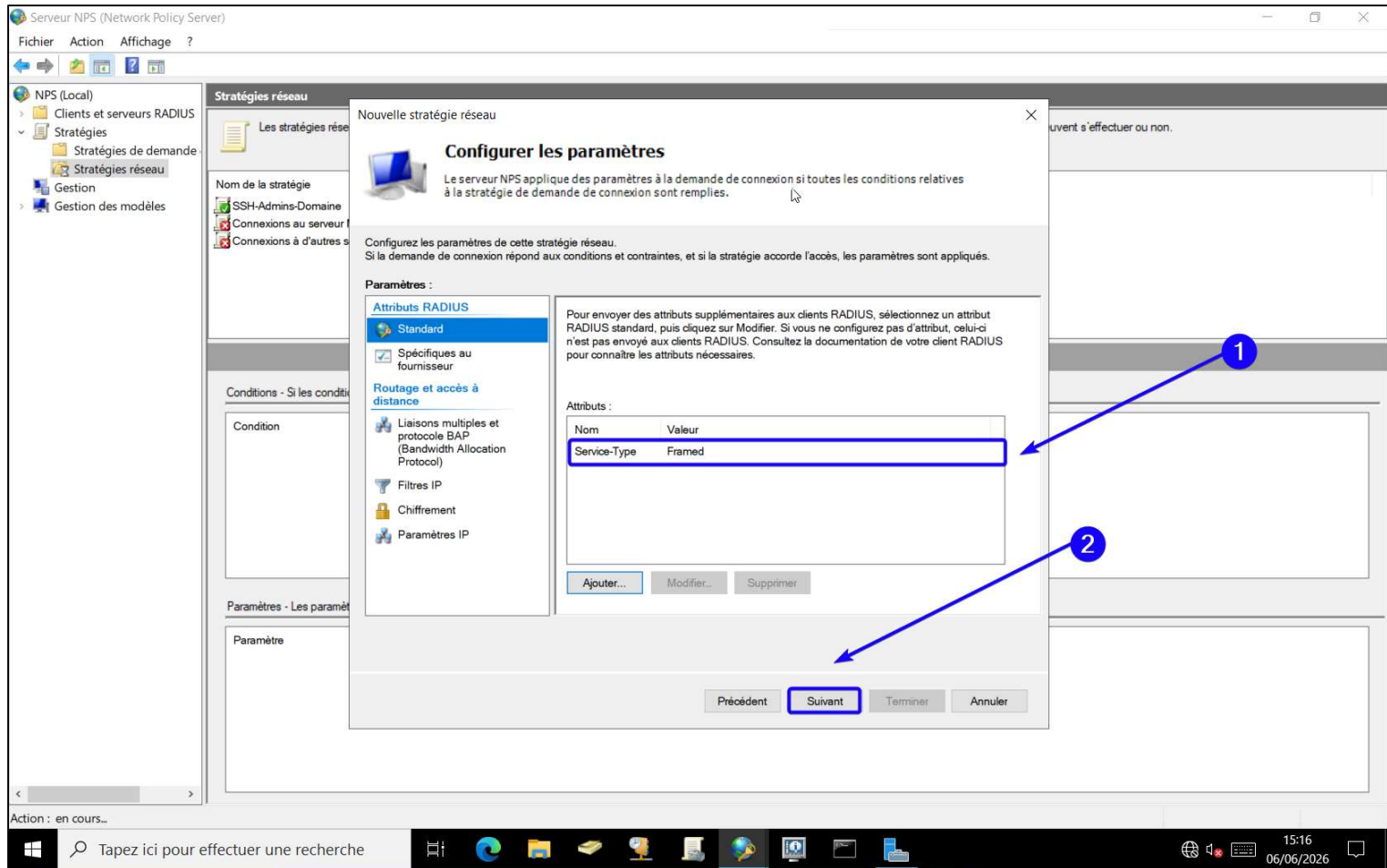










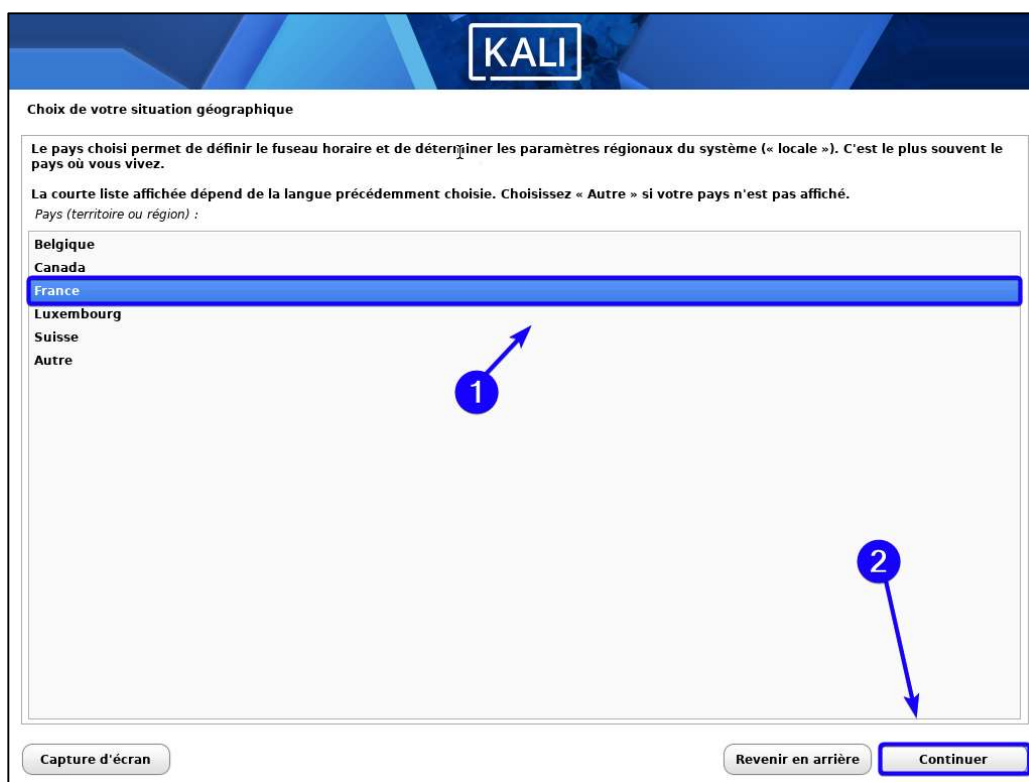
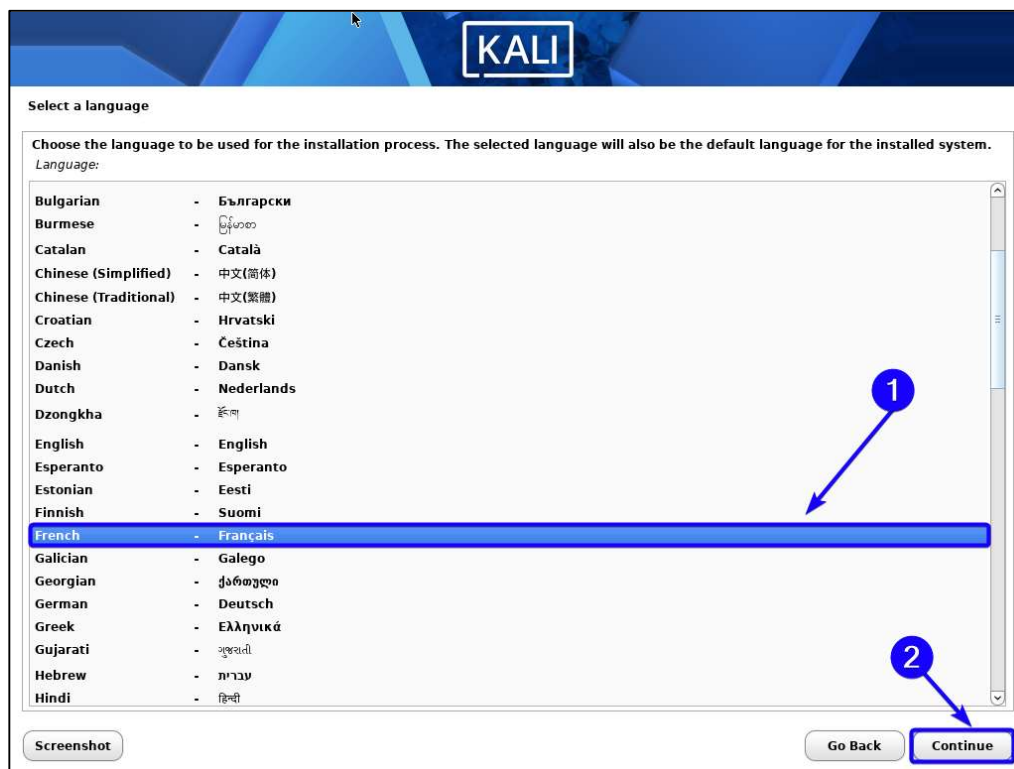


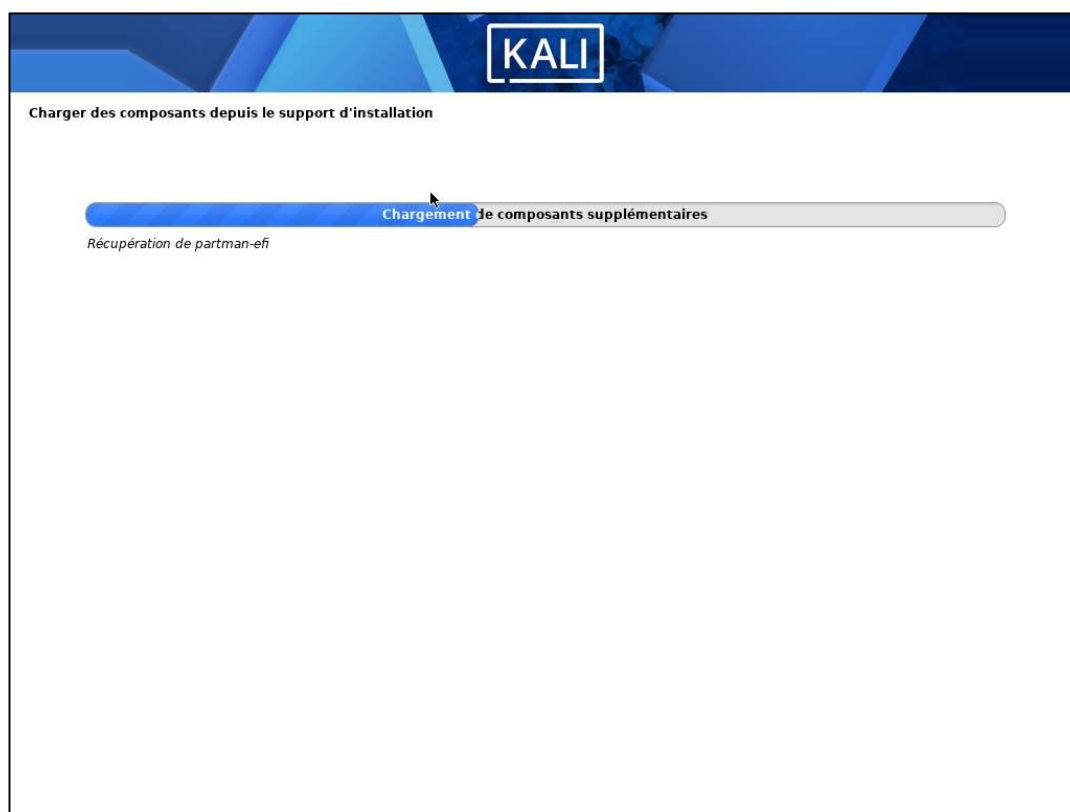
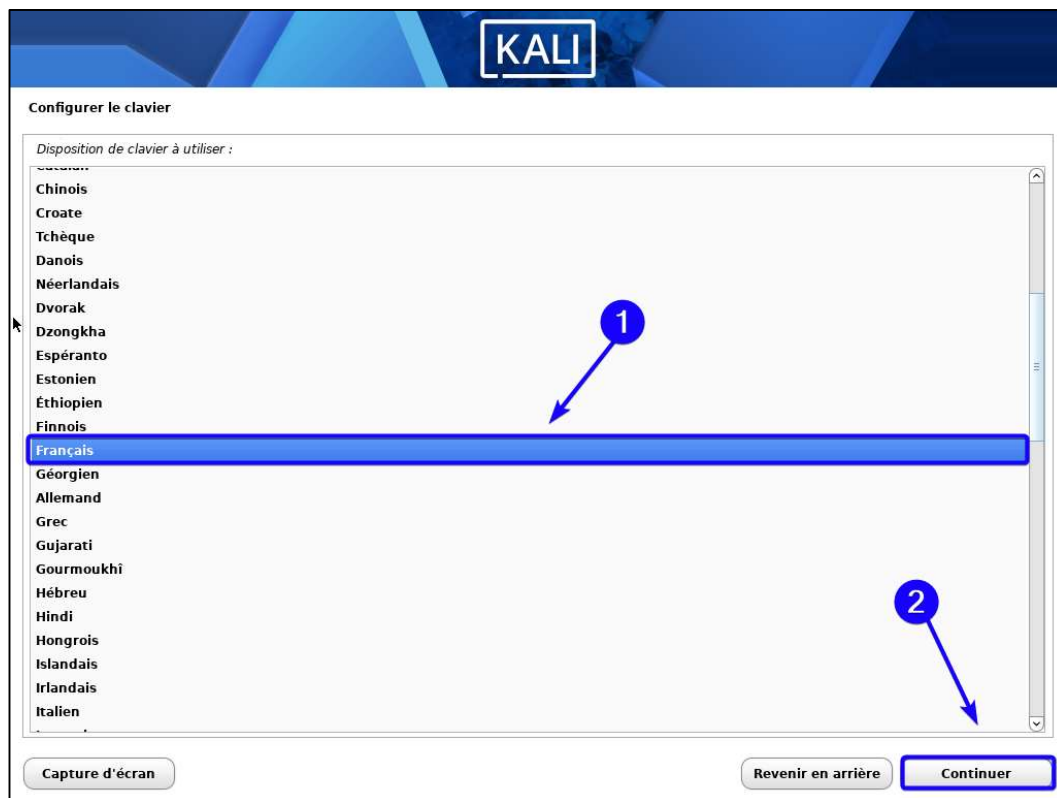


Test de Validation :

Pour tester que les ports ethernet 1/0 à 3 sont bien bloqué par RADIUS et que n'importe quel attaquant voulant se connecter au domaine en obtenant une @IP sera bloqué immédiatement. J'ai créer une machine virtuelle avec KaliLinux.

Installation de la VM de la personne extérieure





KALI

Configurer le réseau

Vous pouvez maintenant réessayer la configuration automatique du réseau, - cela peut réussir si le serveur DHCP met du temps à répondre -, ou bien vous pouvez configurer vous-même le réseau. Certains serveurs DHCP demandent qu'un hôte DHCP soit donné par le client, vous pouvez l'indiquer avant de réessayer la configuration automatique.

Méthode pour la configuration du réseau :

Réessayer la configuration automatique du réseau

Réessayer la configuration automatique avec un nom d'hôte DHCP

Configurer vous-même le réseau

Ne pas configurer le réseau maintenant

Capture d'écran

Revenir en arrière

Continuer

KALI

Configurer le réseau

Please enter the hostname for this system.

The hostname is a label that identifies your system. It may be either a single word giving it a unique name within the local network, or a fully qualified domain name (FQDN) which combines the hostname and domain name in one string, separated by periods.

If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make up the hostname yourself.

Hostname:

kali

Capture d'écran

Revenir en arrière

Continuer

PROJET PERSONNEL – Théo BRETON

PROJET – RESEAUX/SYSTEME : PROJET N°5 : RADIUS DANS UN ENVIRONNEMENT PROFESSIONNEL

179

Créer les utilisateurs et choisir les mots de passe

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

Veillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse d'origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

Nom complet du nouvel utilisateur :

attaquant

1

2

Capture d'écran

Revenir en arrière

Continuer

Créer les utilisateurs et choisir les mots de passe

Veillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.

Identifiant pour le compte utilisateur :

attaquant

1

2

Capture d'écran

Revenir en arrière

Continuer

KALI

Créer les utilisateurs et choisir les mots de passe

Assurez-vous de choisir un mot de passe suffisamment robuste pour qu'il ne puisse pas être deviné.
Mot de passe pour le nouvel utilisateur :

Admin123

☒ Afficher le mot de passe en clair

Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.
Confirmation du mot de passe :

Admin123

☒ Afficher le mot de passe en clair

Capture d'écran

Revenir en arrière

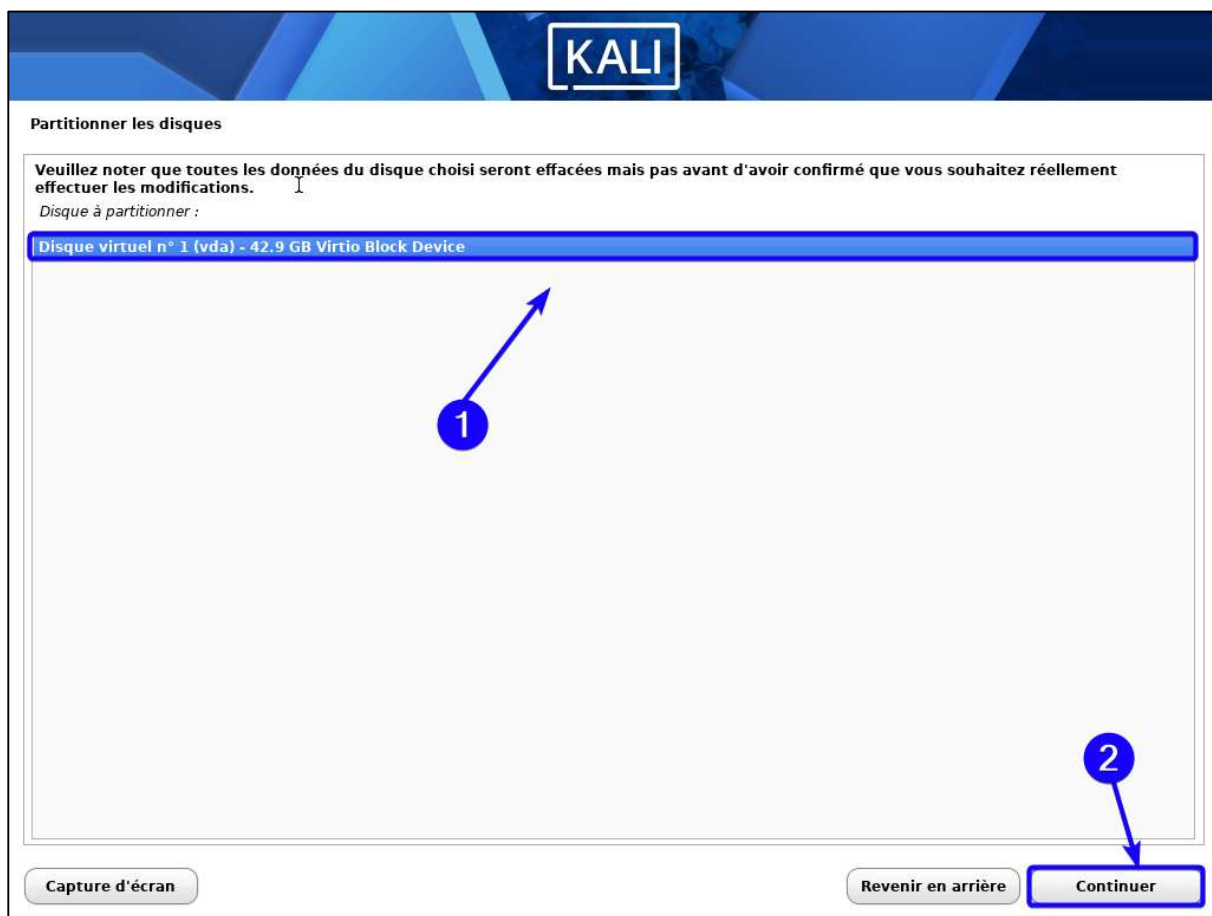
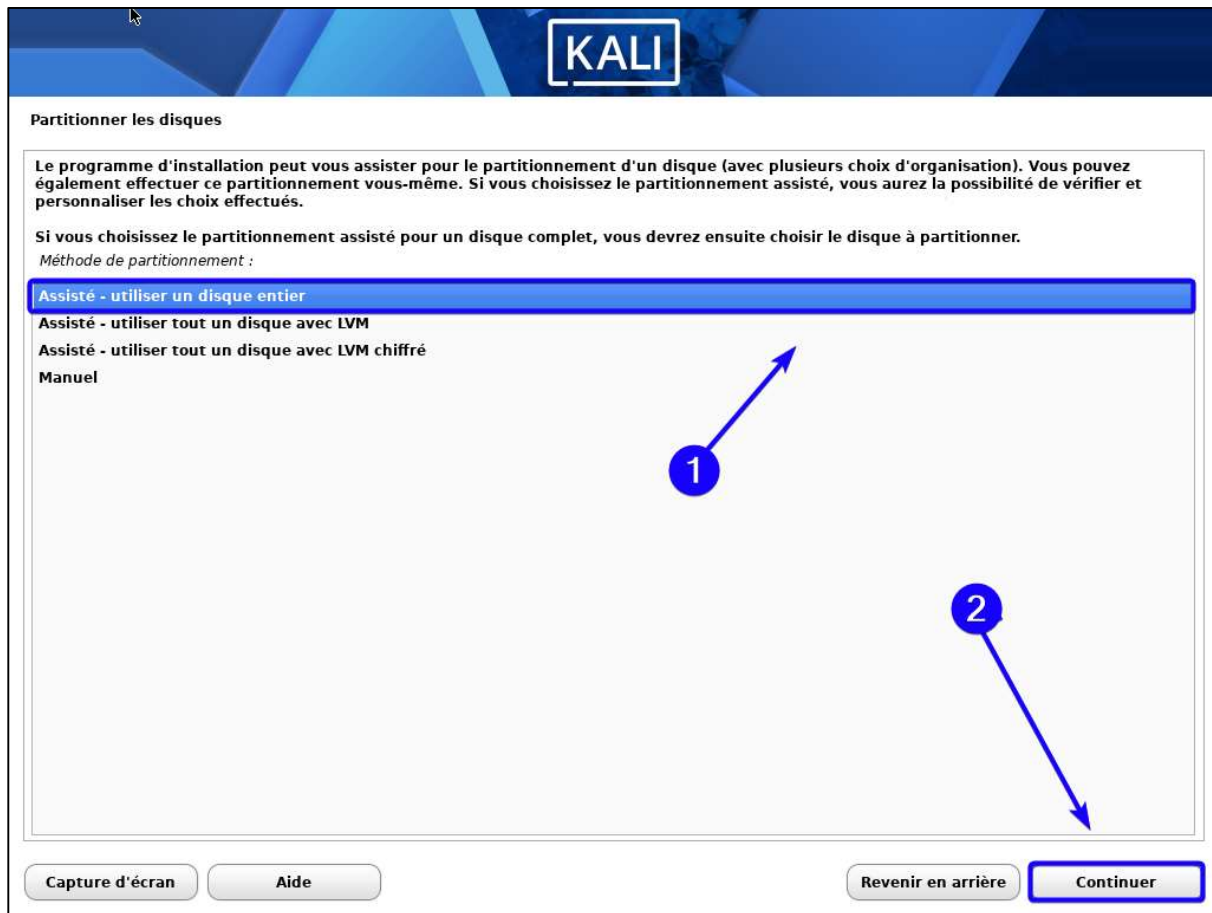
Continuer

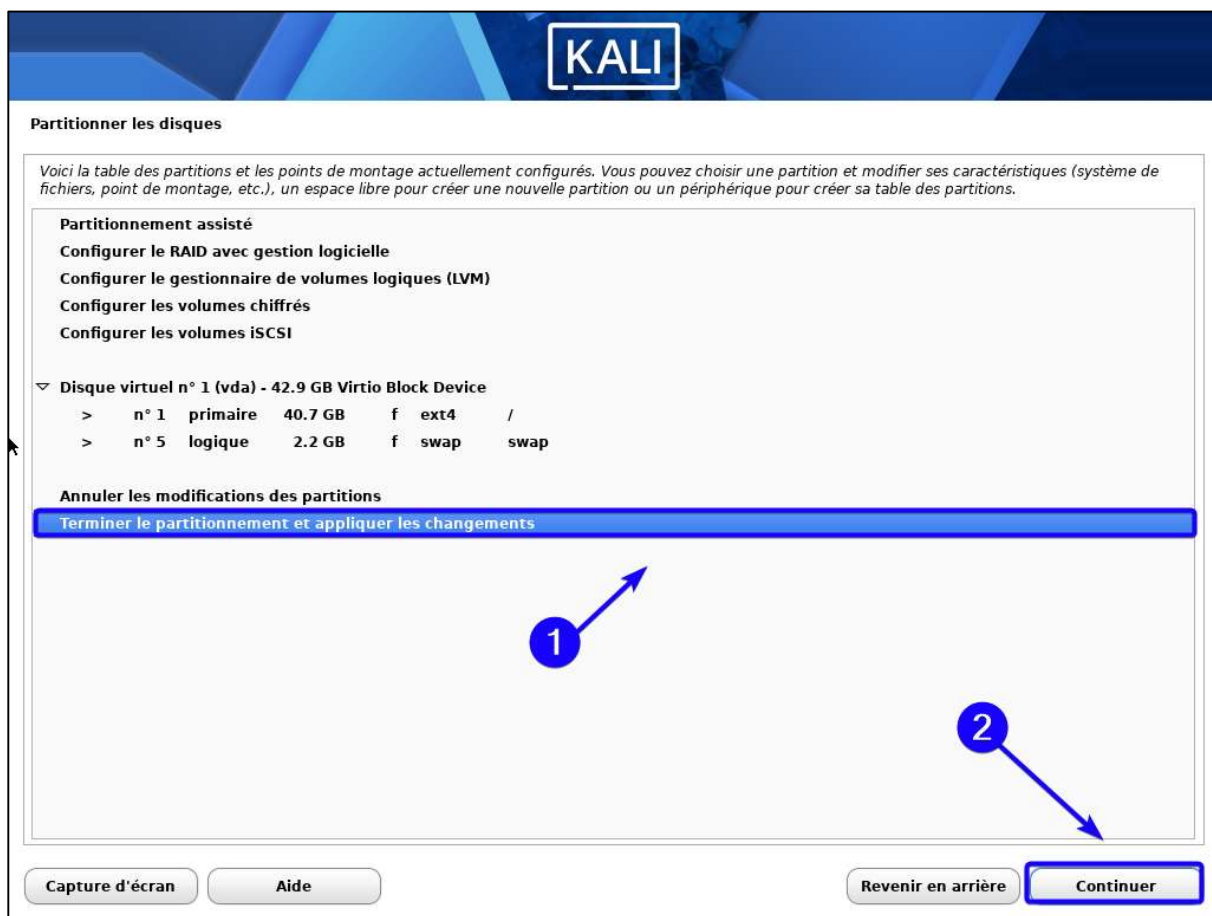
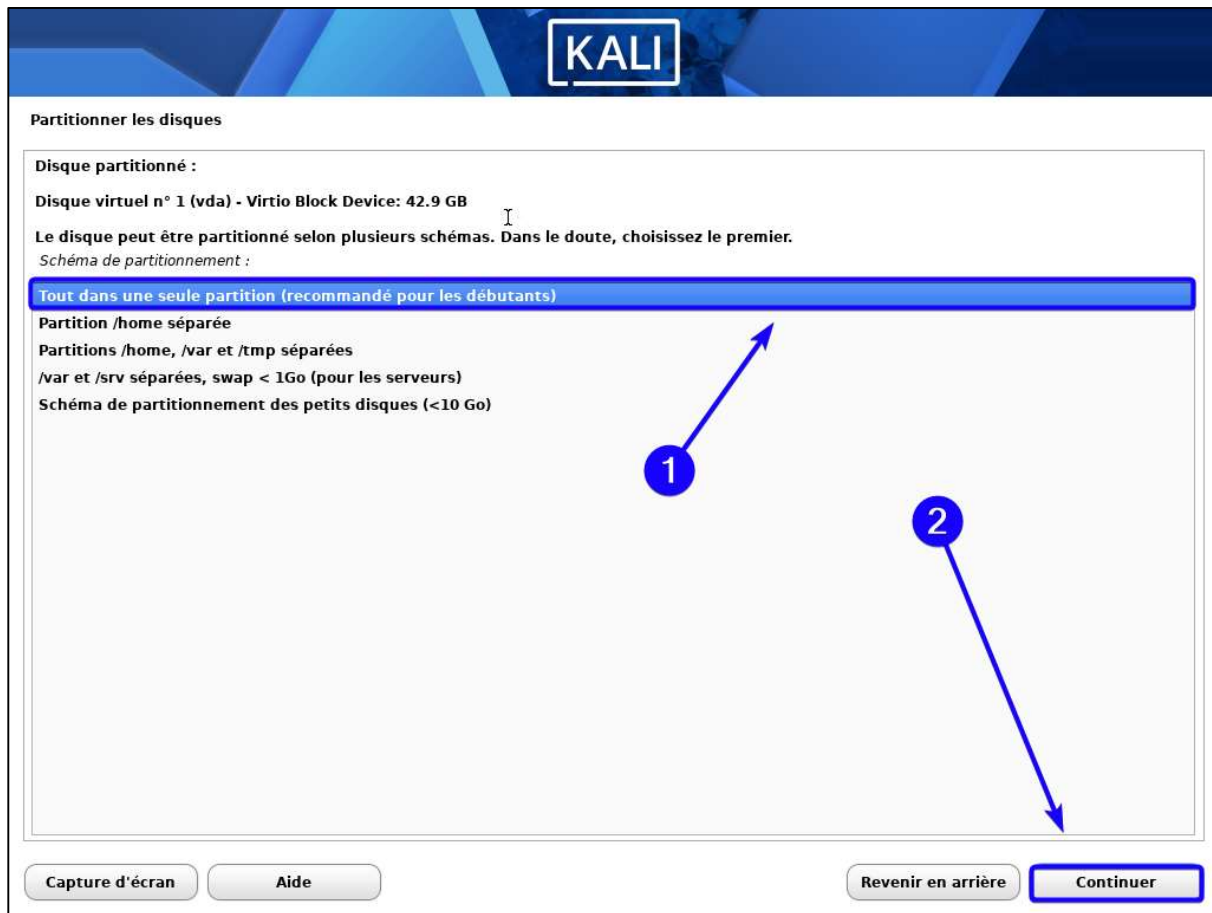
KALI

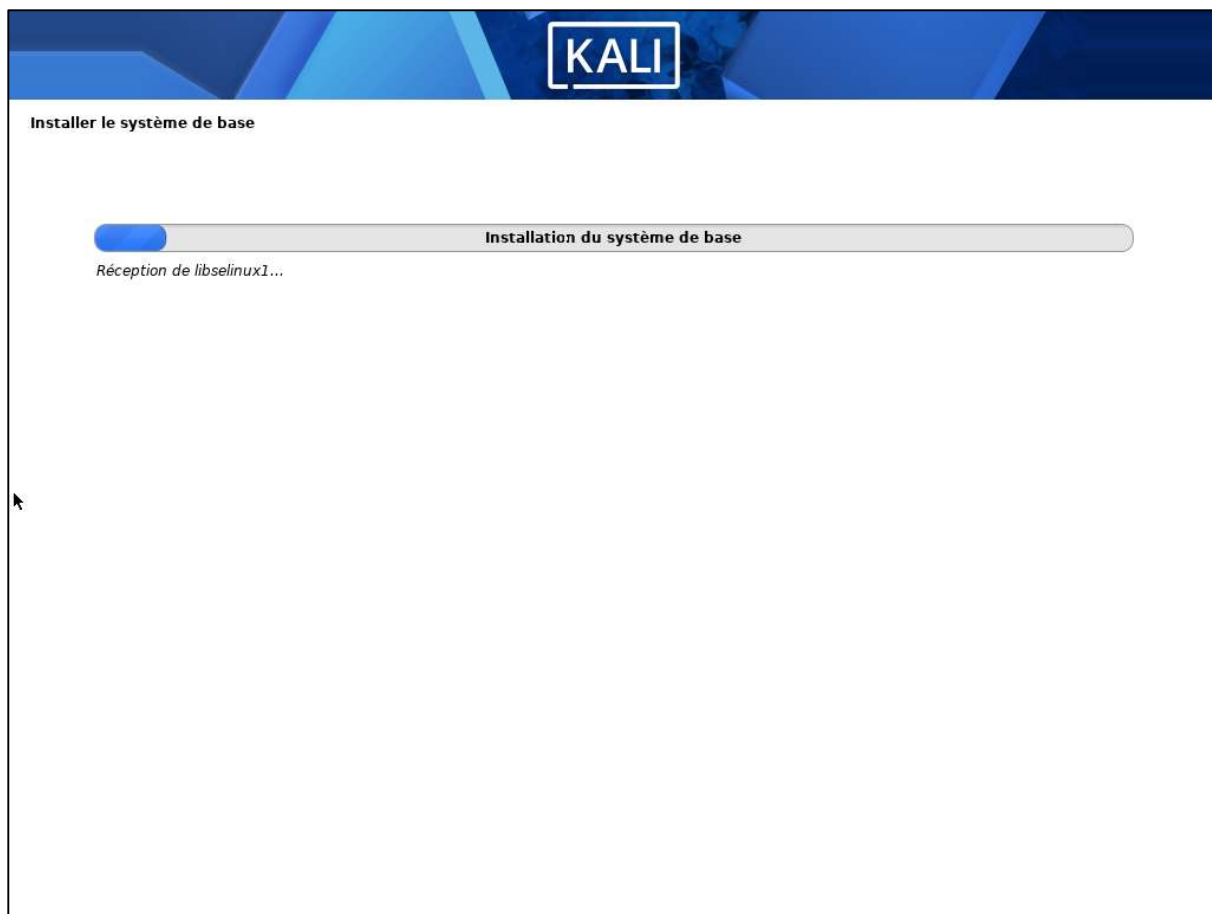
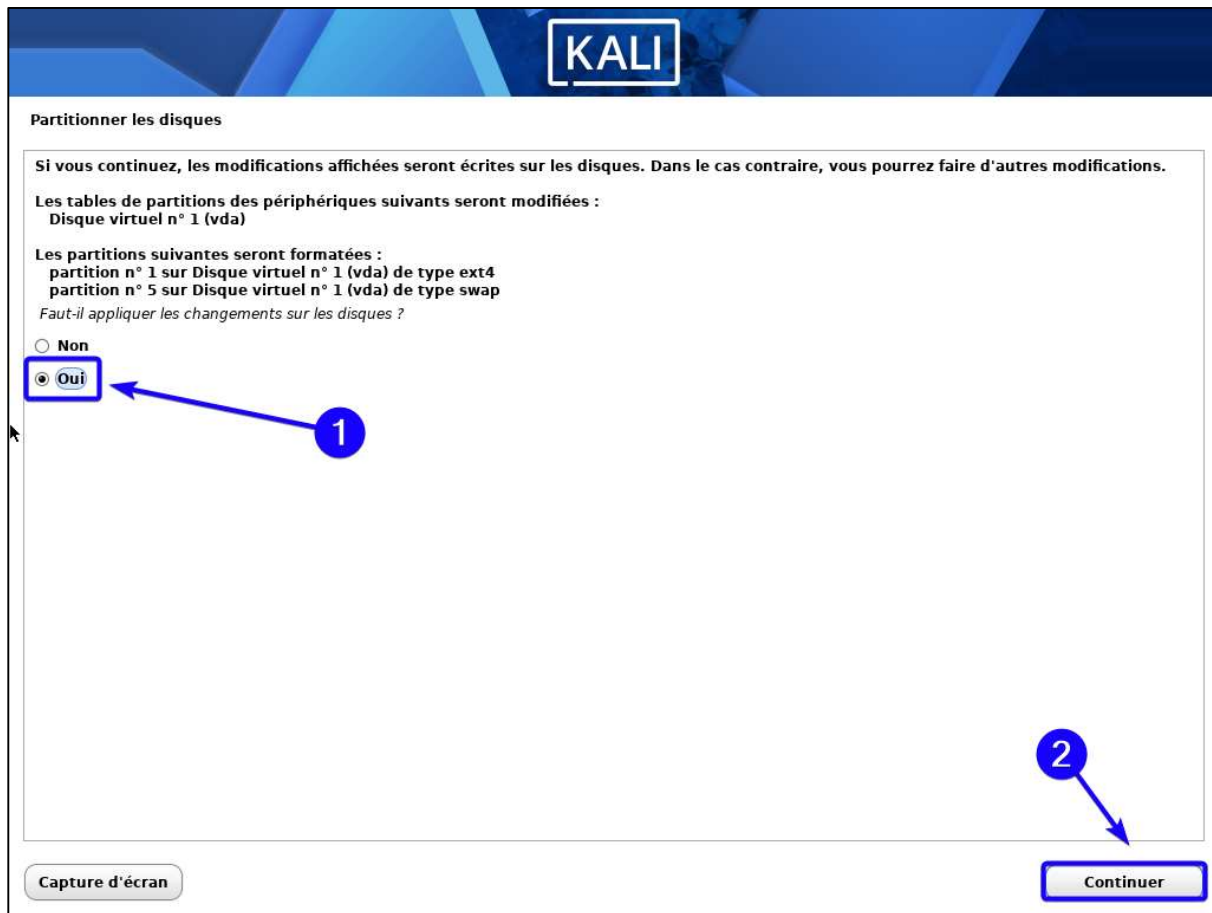
Partitionner les disques

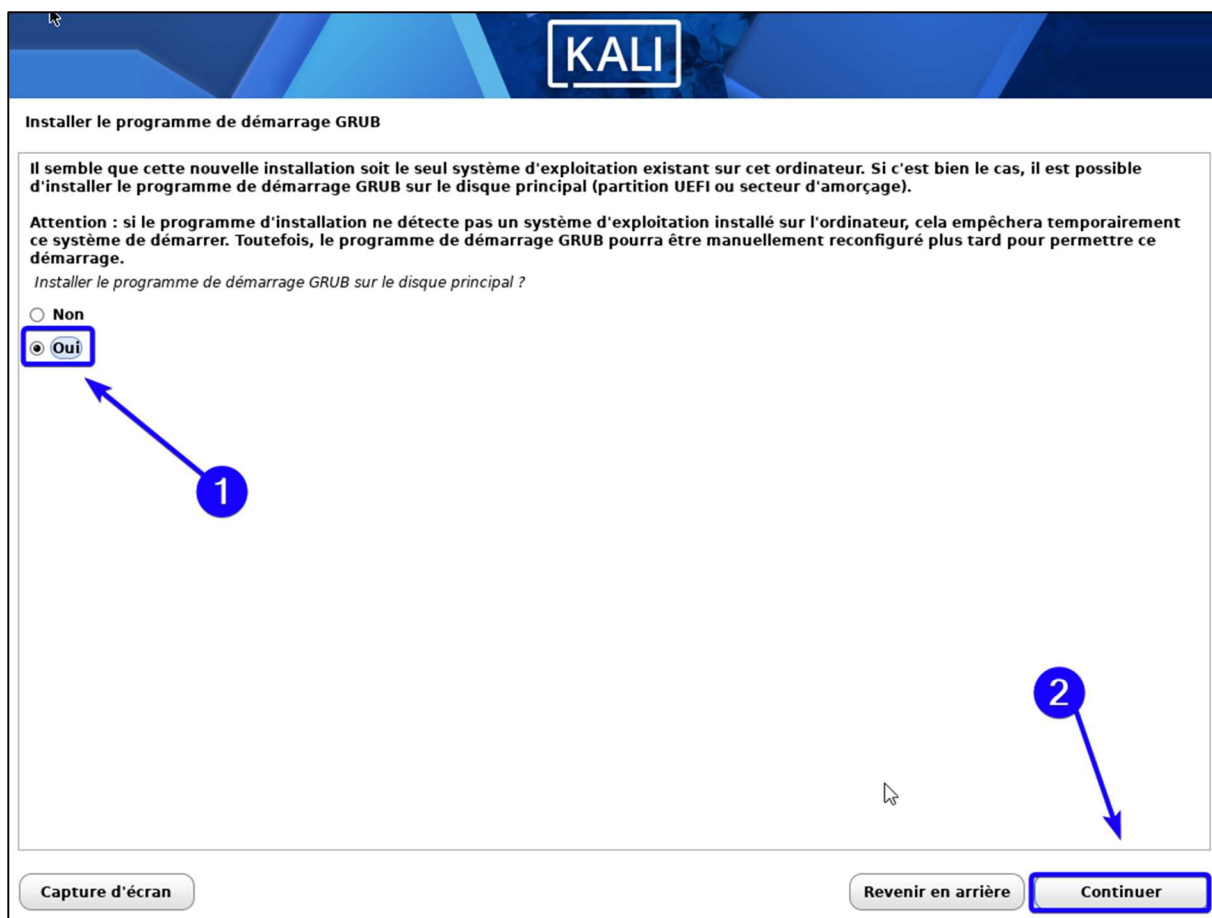
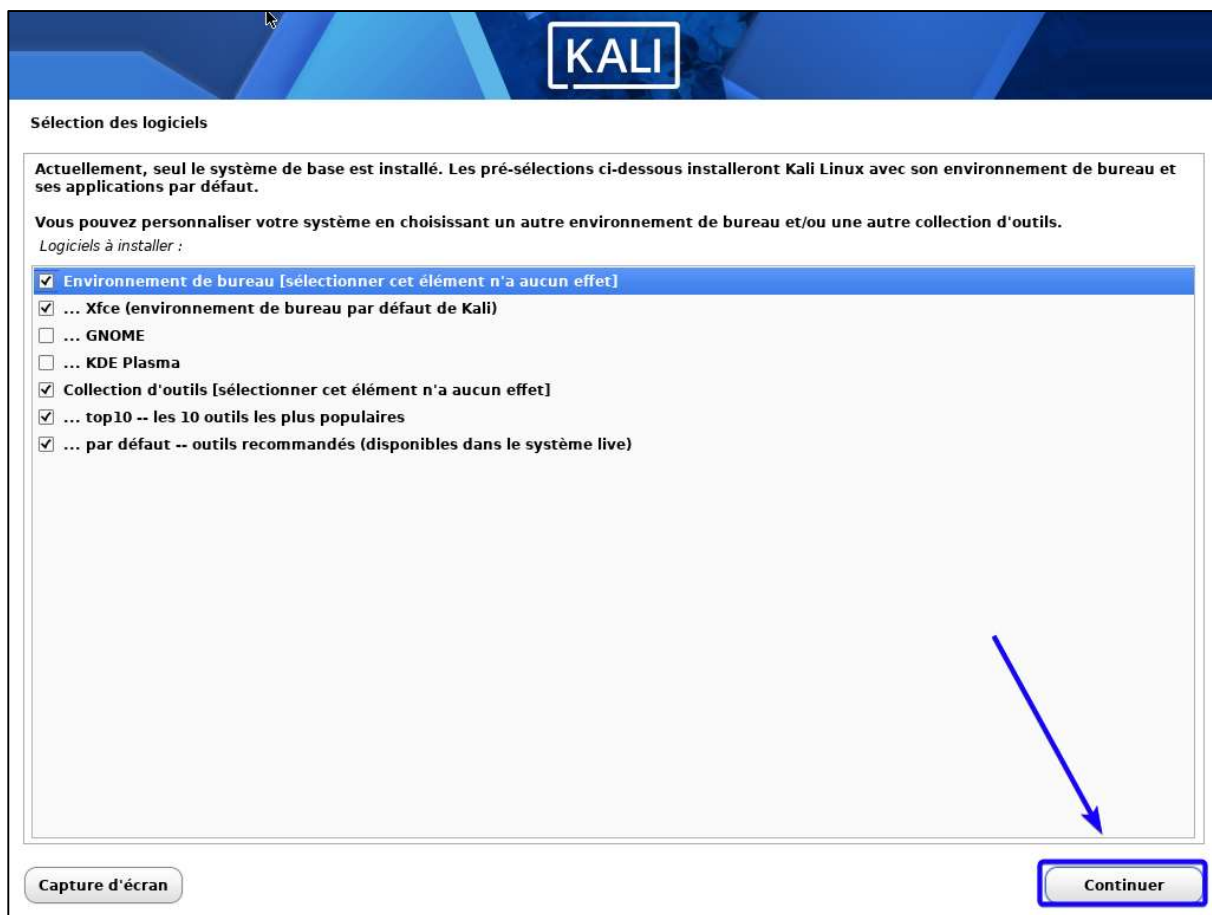
démarrage de l'outil de partitionnement

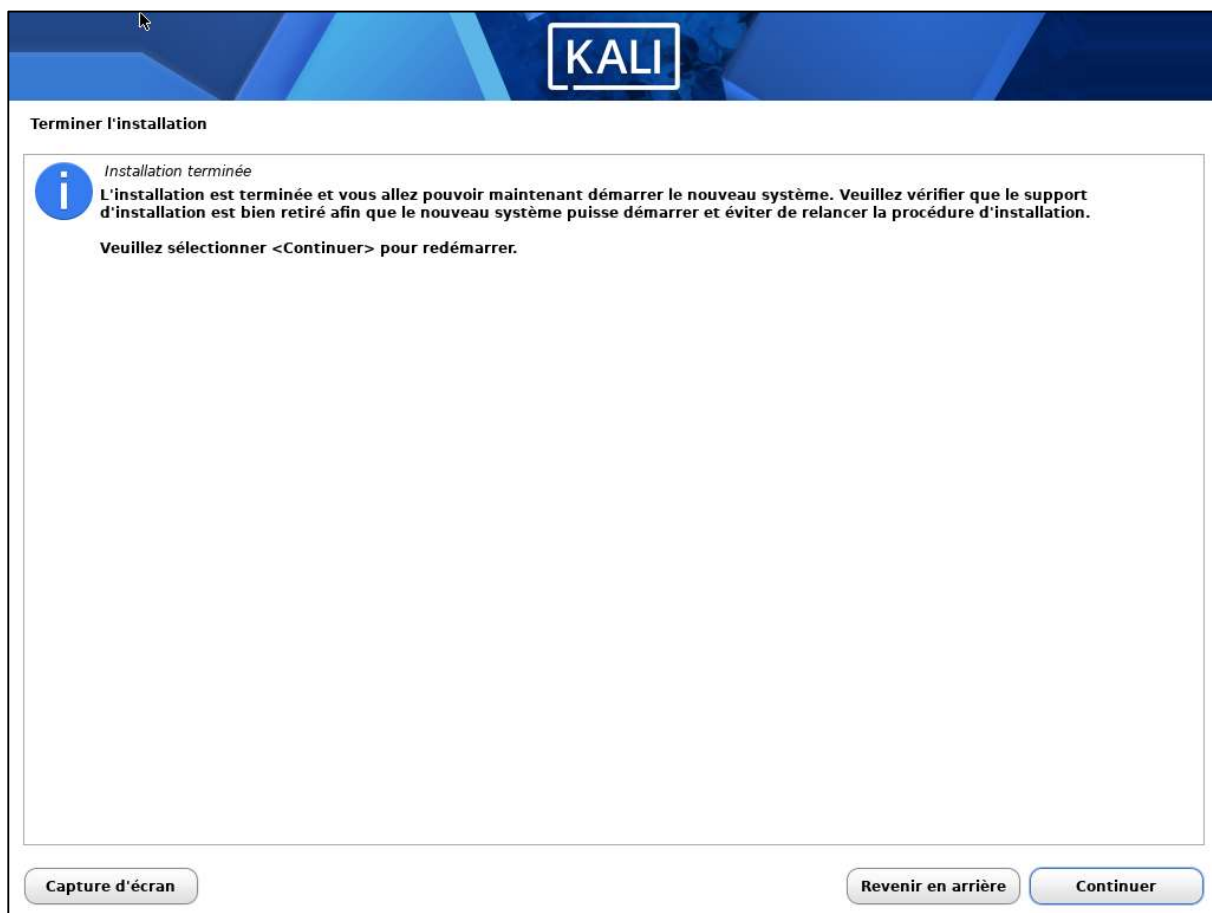
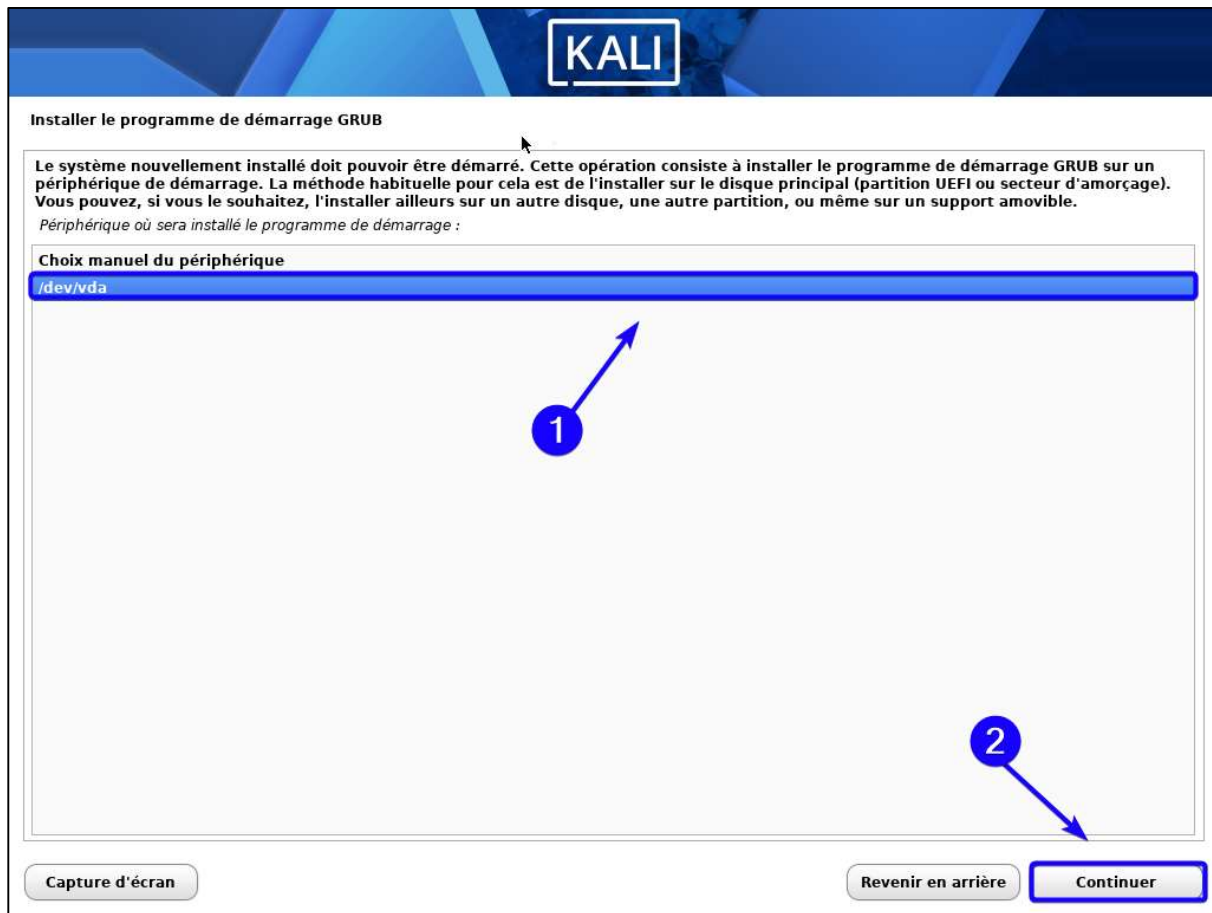
Veuillez patienter...

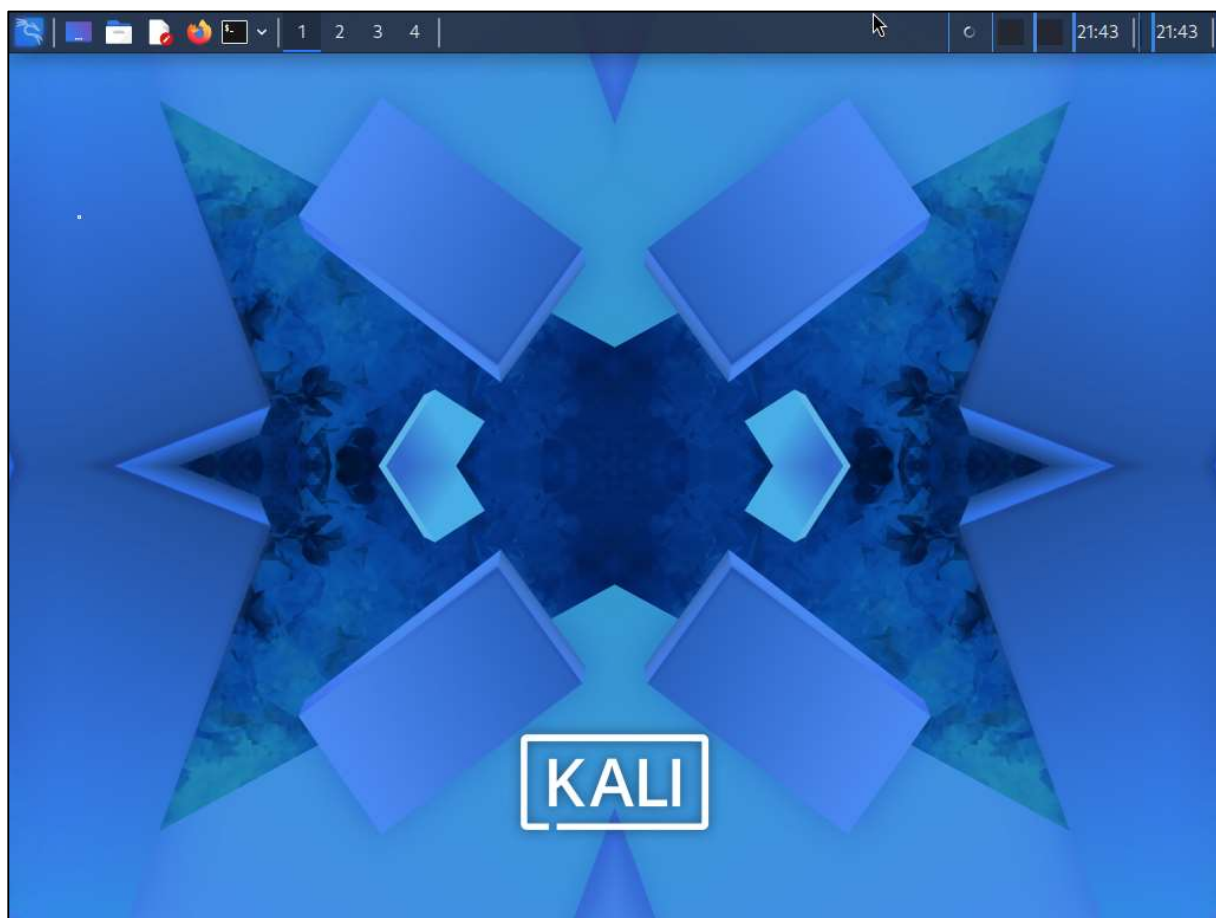
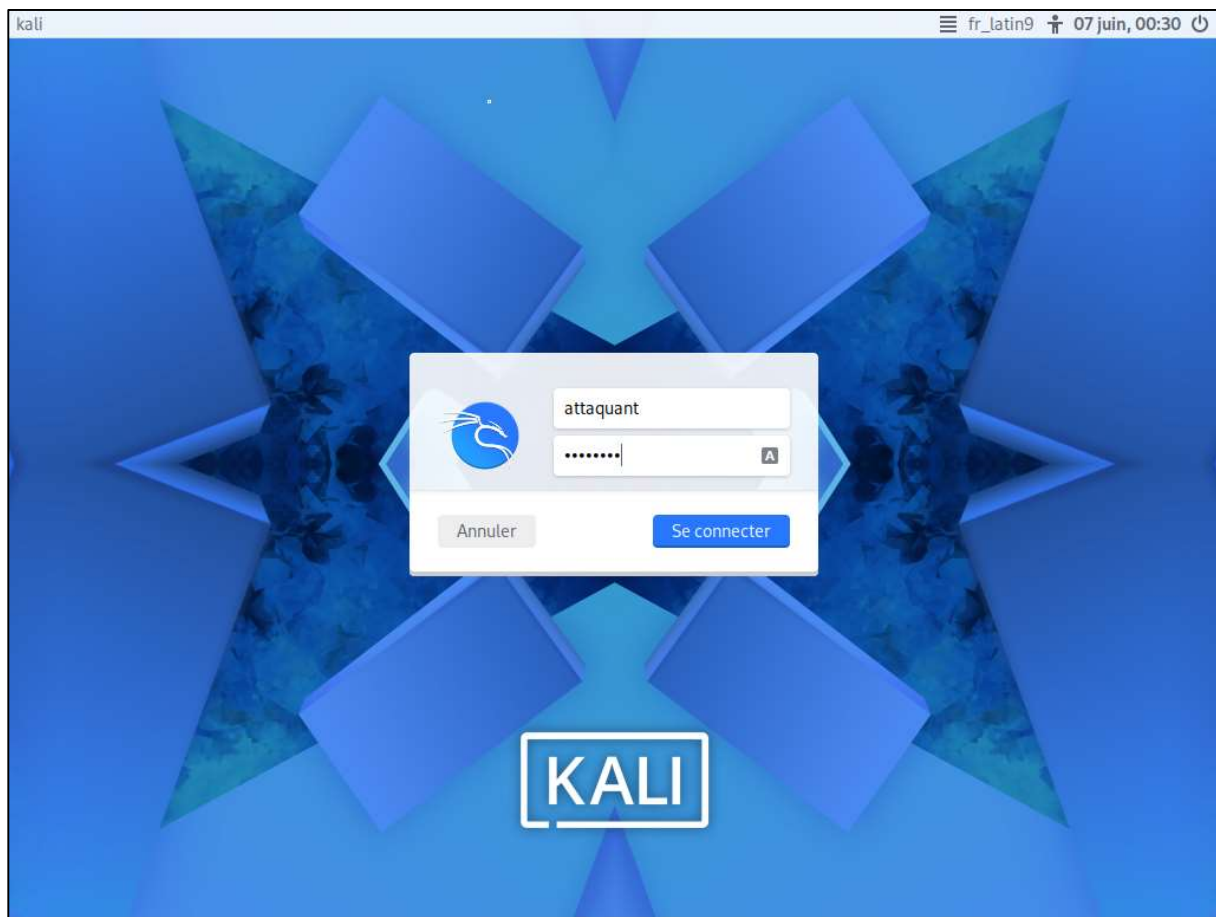








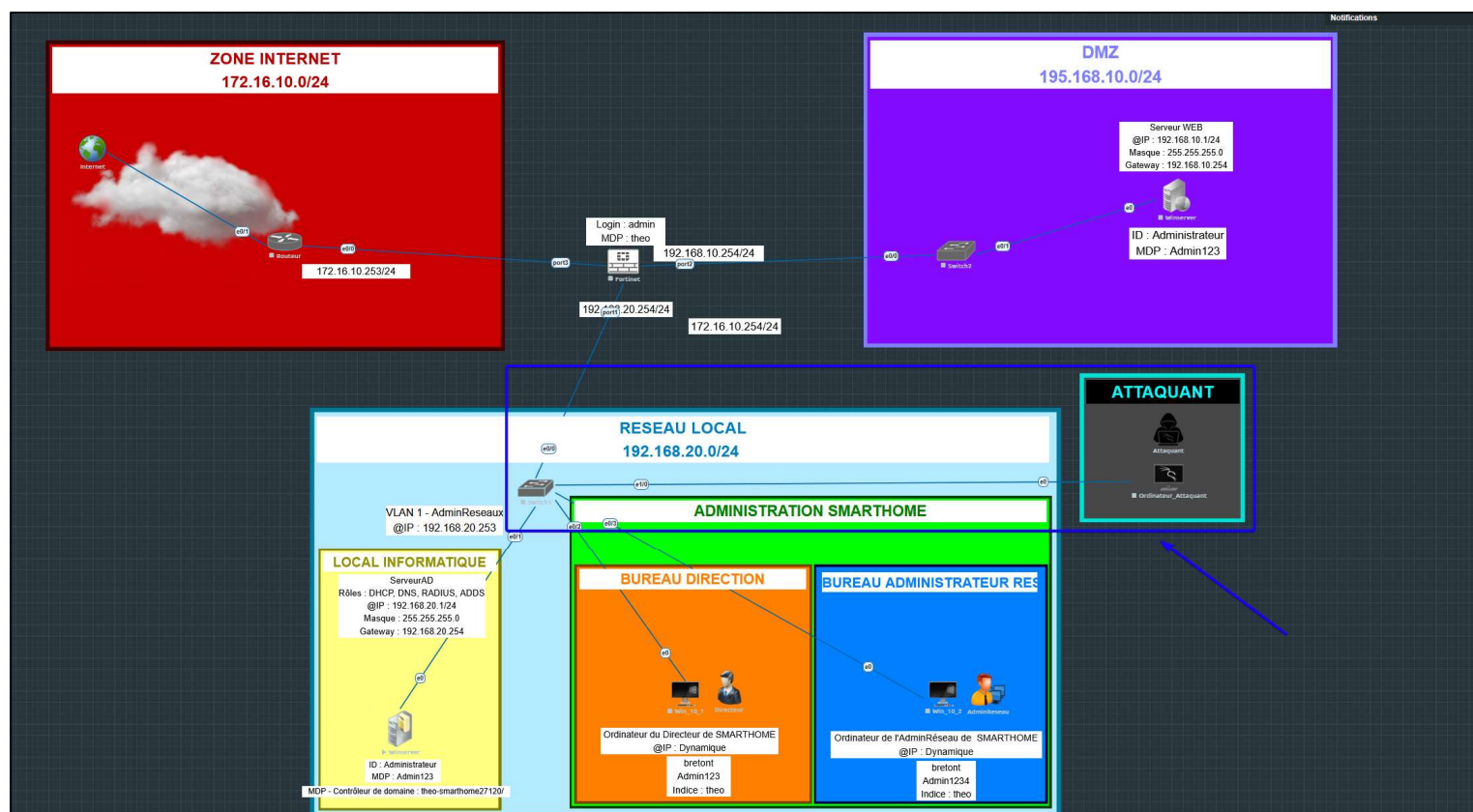




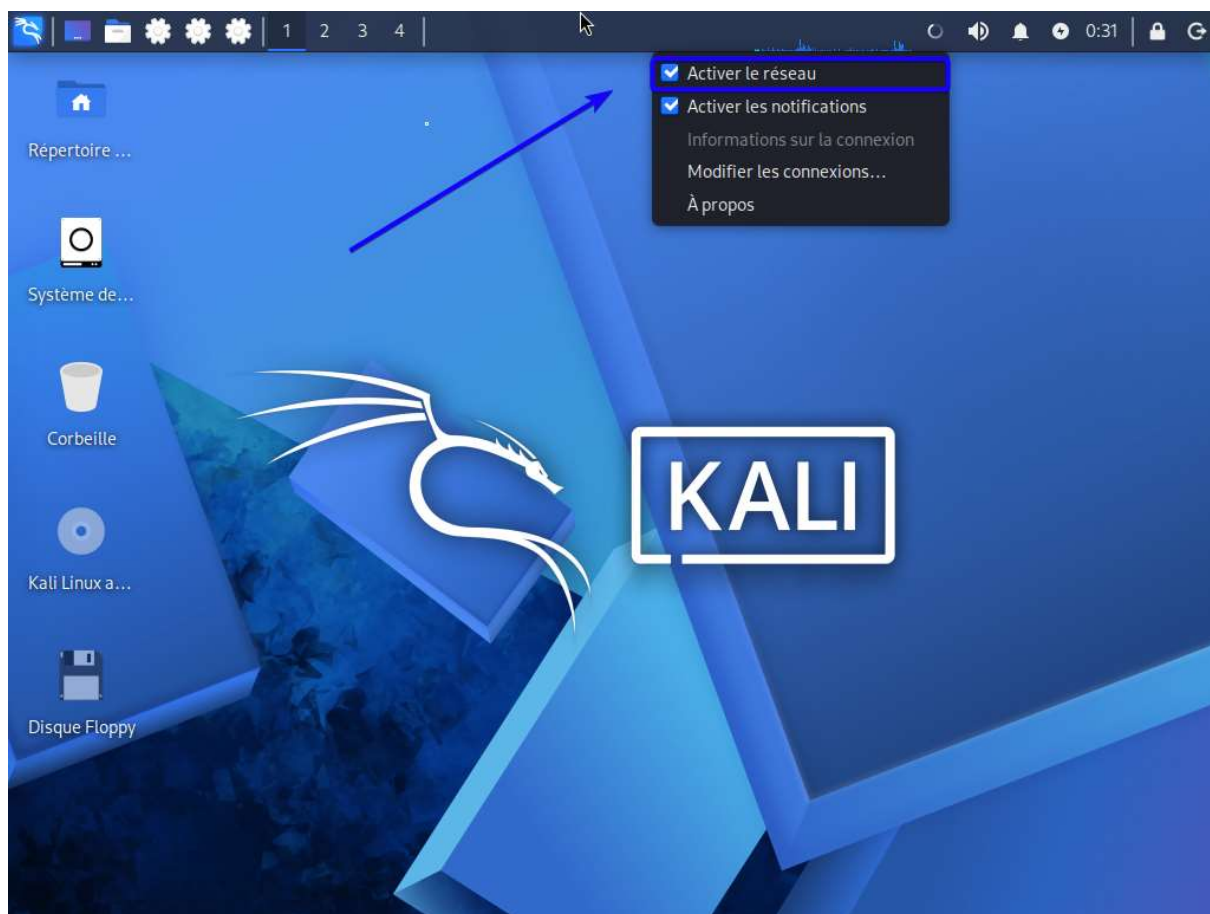
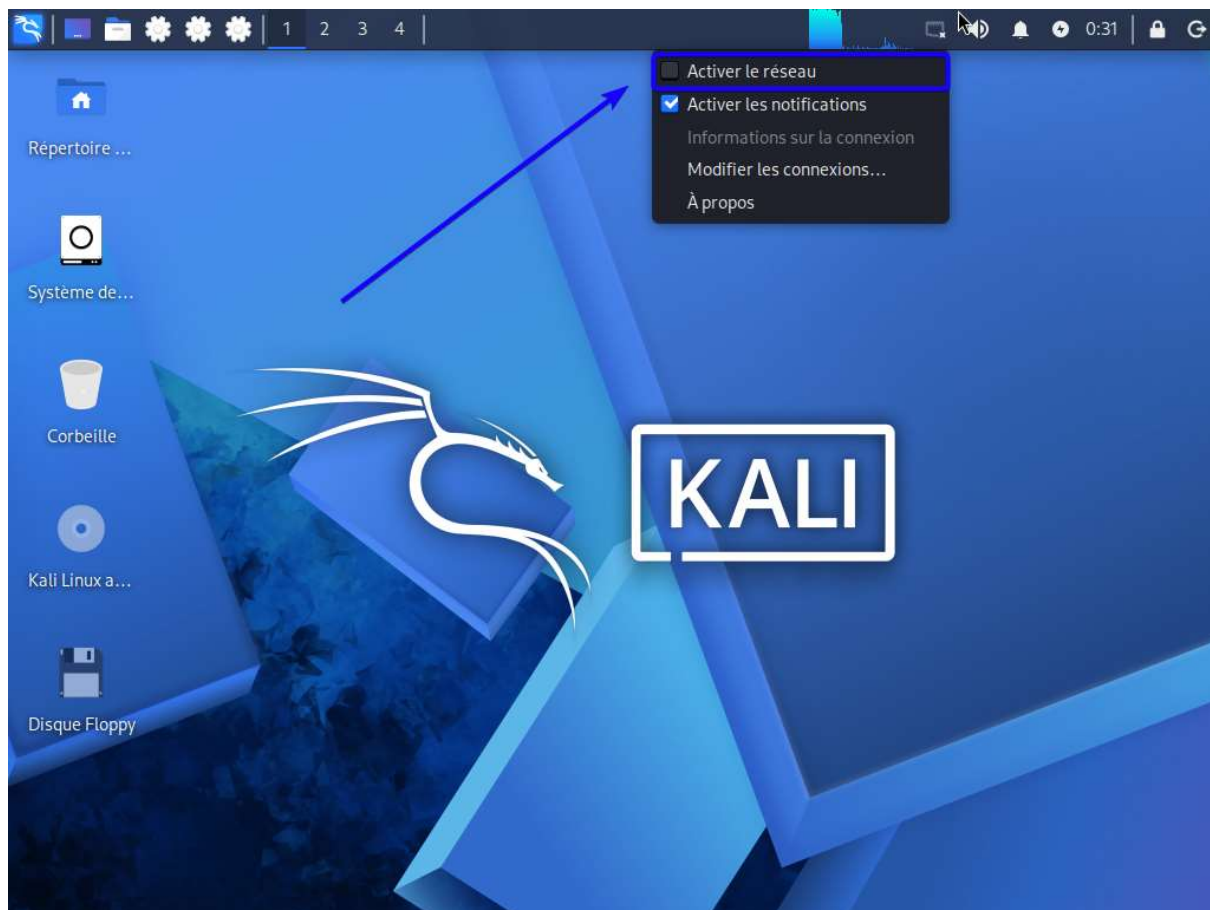


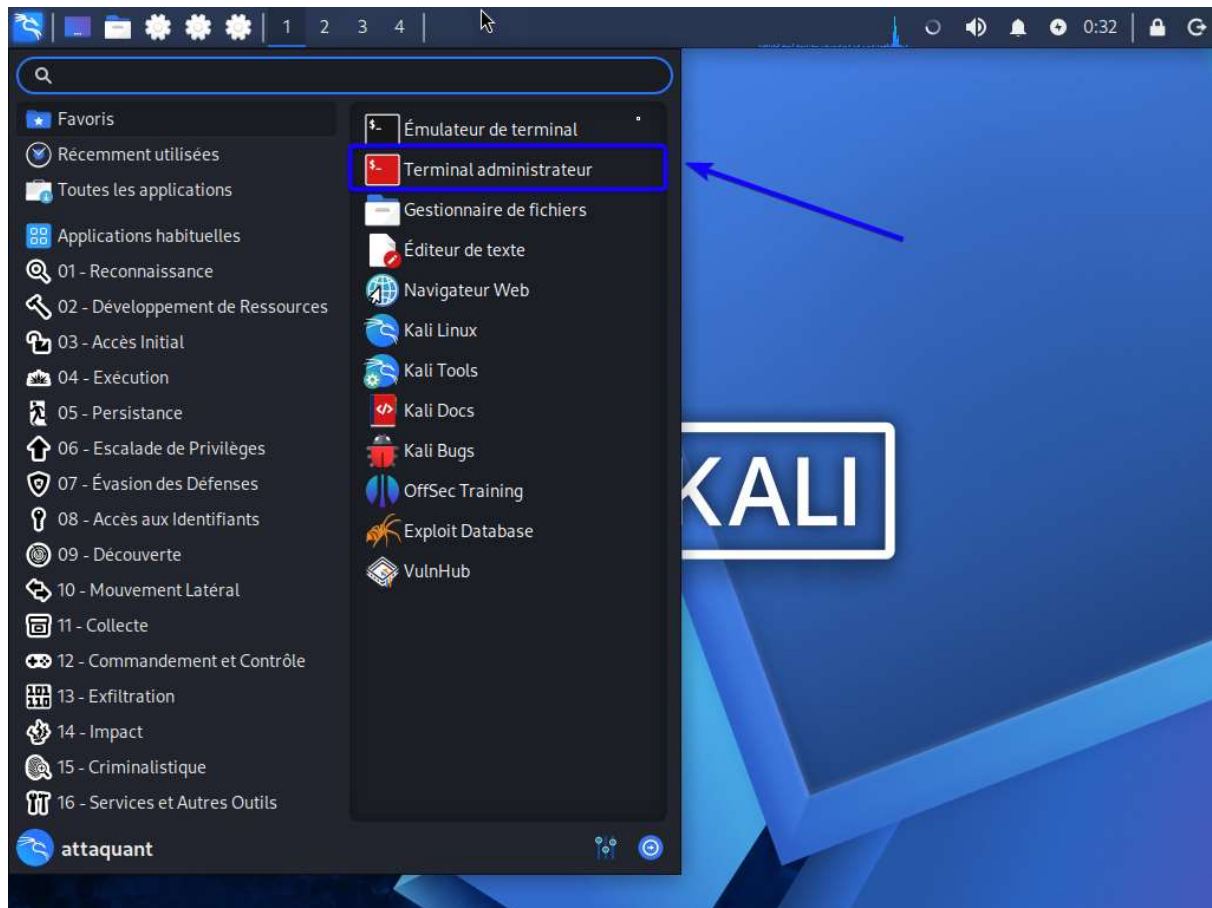
Test de Validation :

Maintenant que le PC de l'attaquant est sur KaliLinux on va le raccorder sur un port bloqué.

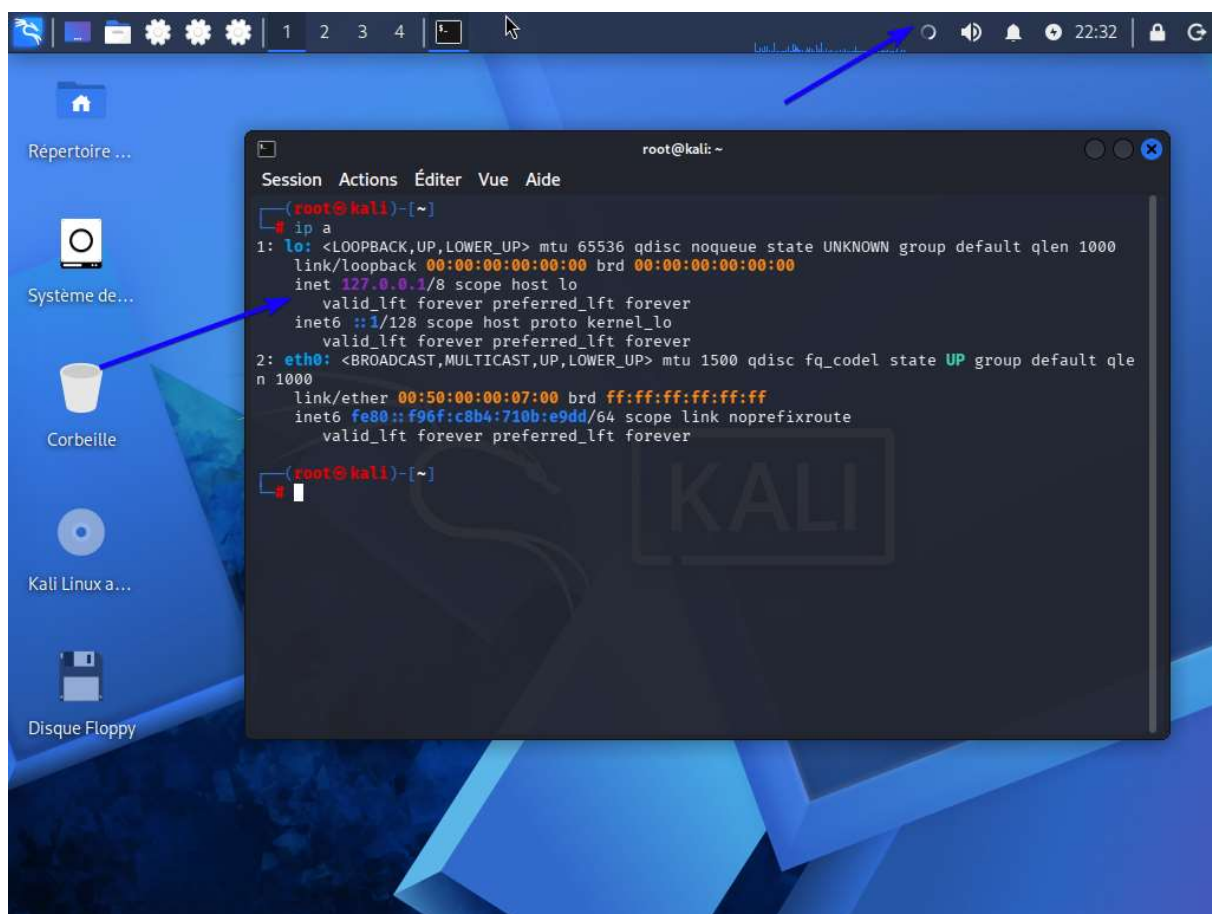


Je désactive la carte réseau manuellement puis je la réactive.





En tapant la commande « ip a » je vois que je ne reçois aucune @IP du serveur DHCP de SMARTHOME.



ANNEXE 1 – INSTALLATION ET CONFIGURATION DU FORTIGATE

Installation du pare feu – Fortigate de chez Fortinate :



Configuration de la VM – Fortinet

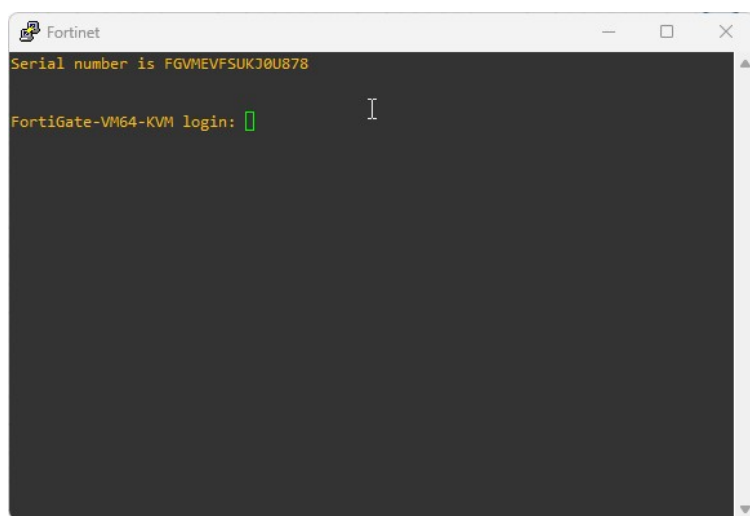
On vous demande le nom d'utilisateur, le nom d'utilisateur et mot de passe par défaut :



login : **admin**



password : **et vide donc entrée directement**

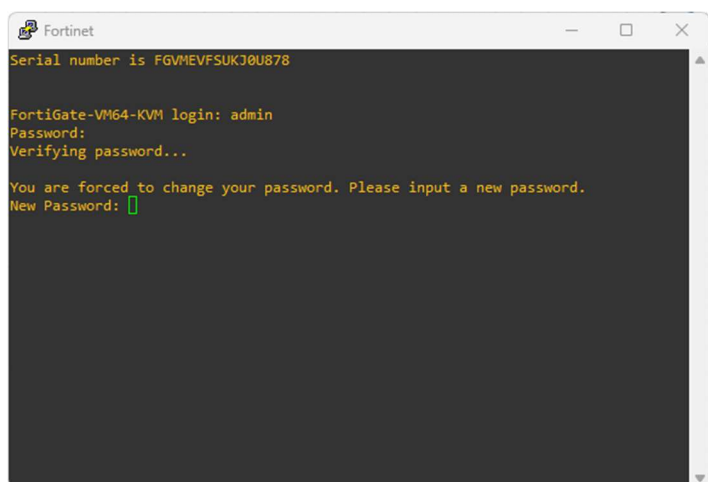


On va vous demander à un nouveau mot de passe
Conseil :



password : **theo**

Comme pour la connexion au serveur EVE_NG.




```
Fortinet
Serial number is FGVMEVFSUKJ0U878

FortiGate-VM64-KVM login: admin
Password:
Verifying password...

You are forced to change your password. Please input a new password.
New Password:

FortiGate-VM64-KVM login: admin
Password:
Verifying password...

You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Verifying password...
Welcome!

FortiGate-VM64-KVM #
```

Vous êtes maintenant dans la page d'accueil.

Tapez ensuite la commande suivante :

show system interface

```
Fortinet
Serial number is FGVMEVFSUKJ0U878

FortiGate-VM64-KVM login: admin
Password:
Verifying password...

You are forced to change your password. Please input a new password.
New Password:

FortiGate-VM64-KVM login: admin
Password:
Verifying password...

You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Verifying password...
Welcome!

FortiGate-VM64-KVM # show system interface
```

Voici le résultat de cette commande :

Indique les **informations des port ou l'adresse IP** de la machine virtuelle


```
Fortinet
FortiGate-VM64-KVM # show system interface
config system interface
  edit "port1"
    set vdom "root"
    set mode dhcp
    set allowaccess ping https ssh http
    set type physical
    set snmp-index 1
  next
  edit "port2"
    set vdom "root"
    set type physical
    set snmp-index 2
  next
  edit "port3"
    set vdom "root"
    set type physical
    set snmp-index 3
  next
  edit "port4"
    set vdom "root"
    set type physical
    set snmp-index 4
  next
  edit "naf.root"
    set vdom "root"
    set type tunnel
    set src-check disable
    set snmp-index 5
  next
  edit "l2t.root"
    set vdom "root"
    set type tunnel
    set snmp-index 6
  next
  edit "ssl.root"
    set vdom "root"
    set type tunnel
    set alias "SSL VPN interface"
    set snmp-index 7
  next
  edit "fortilink"
    set vdom "root"
    set fortilink enable
    set ip 10.255.1.1 255.255.255.0
    set allowaccess ping fabric
    set type aggregate
    set lldp-reception enable
    set lldp-transmission enable
    set snmp-index 8
  next
end
FortiGate-VM64-KVM #
```

Configurer l'interface port1 du FortiGate pour qu'elle obtienne automatiquement une adresse IP via DHCP, afin de permettre l'administration via HTTPS/SSH depuis le réseau auquel elle est connectée.

Ouvrir la console du FortiGate depuis EVE-NG (telnet ou console intégrée).

Entrer en mode configuration :

config system interface

Sélectionner l'interface port1

edit port1

Activer le mode DHCP

set mode dhcp

Autoriser les accès d'administration

set allowaccess ping https ssh http

S'assurer que l'interface est active

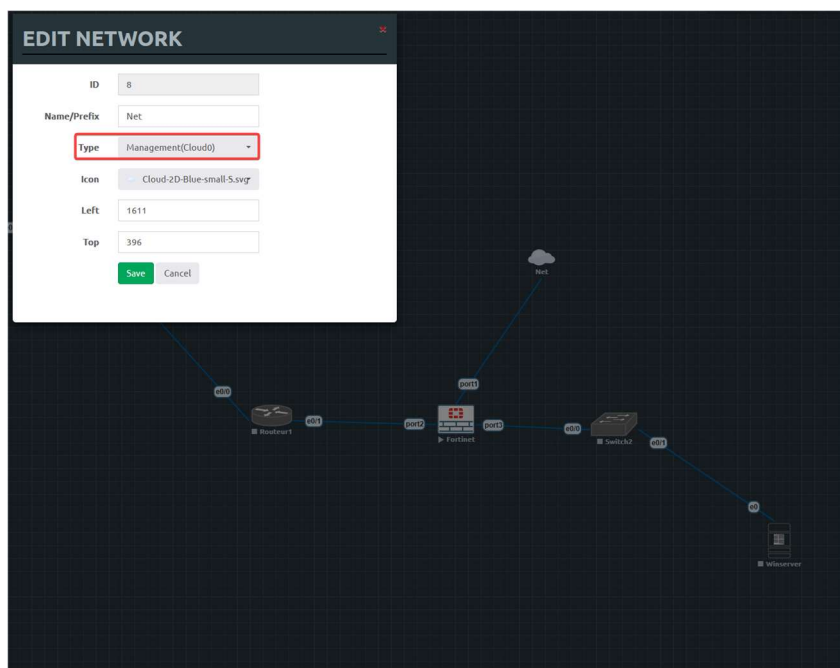
set status up

Valider la configuration

Next

End

Pour que votre pare feu récupère une adresse IP du service DHCP de votre box
verifier qu'il est bien Management (Cloud0)



Management (Cloud0) fonctionne car il relie EVE-NG à la carte réseau physique du PC, alors que Bridge ne crée aucun lien avec le réseau réel.

VS

Le mode Bridge ne relie pas EVE-NG au réseau réel : il crée seulement un lien interne entre VMs, sans accès au DHCP ni à la carte réseau du PC.

Une fois appliqué, tu peux vérifier l'IP obtenue avec

get system interface physical

Aller dans un nouvel onglet

<https://192.168.1.147>

****Pour envoyer une requête au DHCP de ta box :**
execute interface dhcp renew port1

Après vous avez accès à l'interface :

