

SOMMAIRE

I/ Contexte du projet

Descriptif du projet	1
Présentation de l'infrastructure	1

II/ Configuration de la logique administrative

Changement du nom de machine	2
Mise en place d'une IP statique	2

III/ Configuration de l'infrastructure

Mise en place et configuration de l'AD DS et DNS	3
Ajout des collaborateurs au domaine	6
Création des utilisateurs	10
Mise en place du rôle DFS	13
Mise en place des règles GPO	14
Règle "Deploy 7-Zip"	14
Règle "Suggest Notepad++"	15
Règle "Disable control panel"	16
Règle "Disable command prompt"	17
Règle "IT password"	18
Règle "User password"	19
Règle "Mapping"	20
Règle "Wallpaper"	21
Règle "Homescreen Internet Explorer"	22
Mise en place du IIS	23
Configuration de la relation de confiance "Trust"	24

I/ CONTEXTE DU PROJET

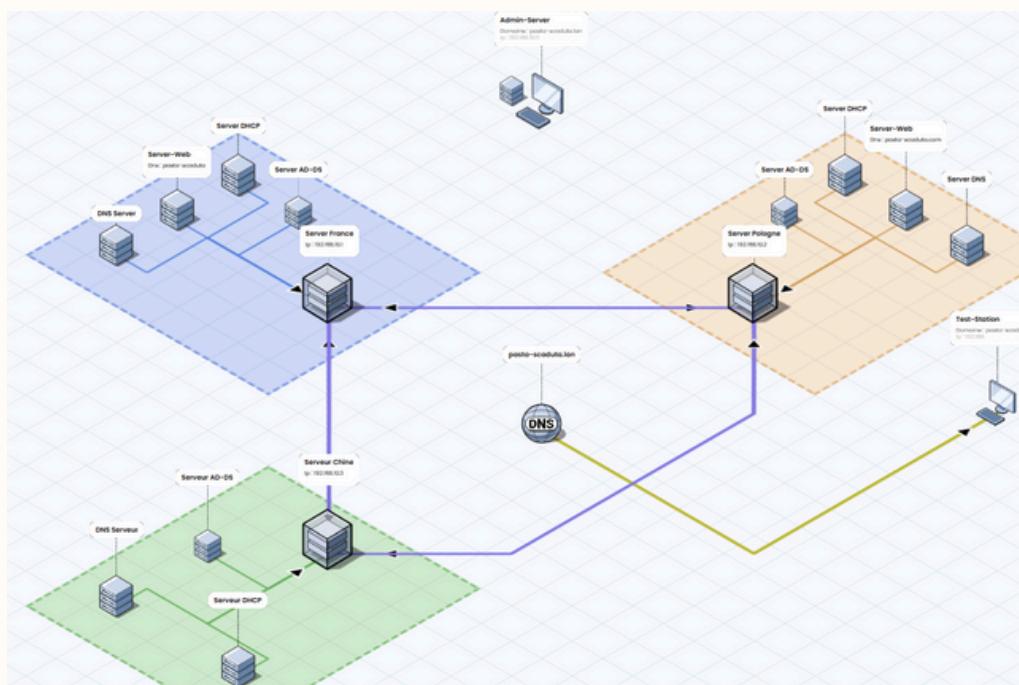


Descriptif du projet

Ce projet, à réaliser en binôme sur deux semaines, vise à concevoir une infrastructure informatique complète pour l'entreprise Pasta Scaduta, en s'appuyant sur les compétences acquises durant le cours tout en intégrant des recherches complémentaires selon les besoins.

Présentation de l'infrastructure :

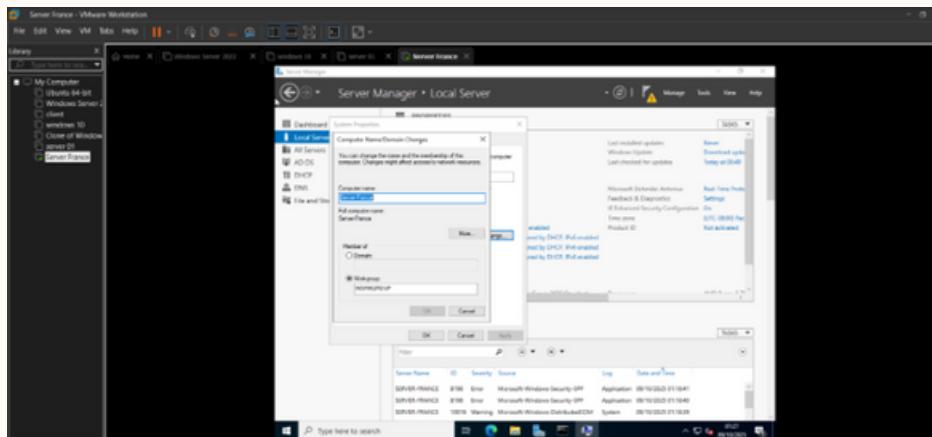
Dans le cadre de son expansion internationale, l'entreprise Pasta Scaduta nous confie la mise en place d'une infrastructure informatique multisite, répartie entre la France, la Pologne et la Chine. Ce projet, vise à répondre aux nouveaux besoins techniques de l'entreprise, jusque-là peu informatisée, en assurant une organisation robuste, sécurisée et adaptée à ses ambitions industrielles mondiales.



II / CONFIGURATION DE LA LOGIQUE ADMINISTRATIVE

CHANGEMENT DU NOM DE MACHINE

Accessible depuis : Server Manager → Local Server → Computer Name → Change → on entre un nouveau nom → OK → on redémarre le serveur



MISE EN PLACE D'UNE IP STATIQUE

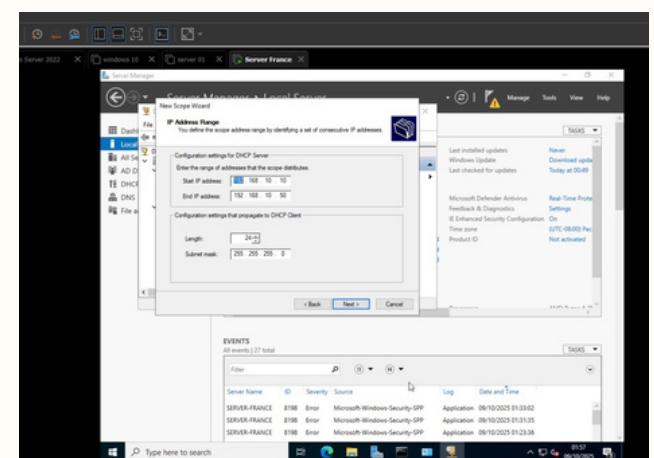
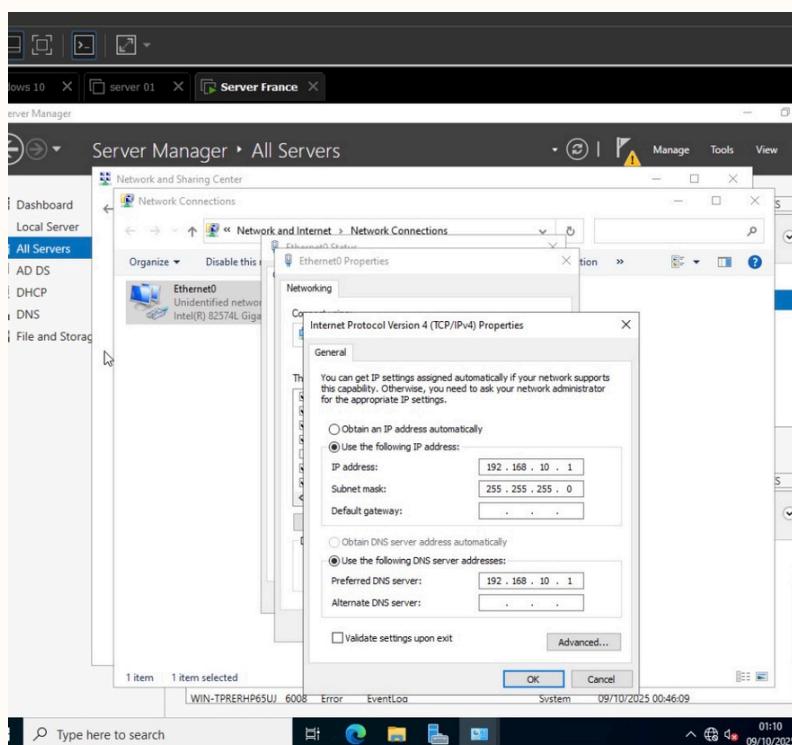
Mise en place de l'infrastructure réseau, configuration de la carte réseau du Server-France, désigné comme serveur principal du domaine. Dans le panneau Network Connections, accessible depuis Control Panel → Network and Sharing Center → Change adapter settings, l'adresse IPv4 a été définie manuellement. Le serveur a reçu l'adresse 192.168.10.1, conformément au plan d'adressage du réseau local 192.168.10.0/24, avec un masque de sous-réseau 255.255.255.0.

Le serveur DNS préféré a également été défini sur 192.168.10.1, car le Server-France assure le rôle de serveur DNS principal pour l'ensemble de l'infrastructure.

Configuration DHCP :

Depuis la console DHCP accessible dans le menu Tools. Un nouveau scope nommé Scope_Pasta a été créé afin de définir la plage d'adresses IP attribuables aux clients du réseau.

La plage configurée s'étend de 192.168.10.10 à 192.168.10.50, avec un masque de sous-réseau 255.255.255.0, conformément à l'architecture du LAN définie pour le projet.

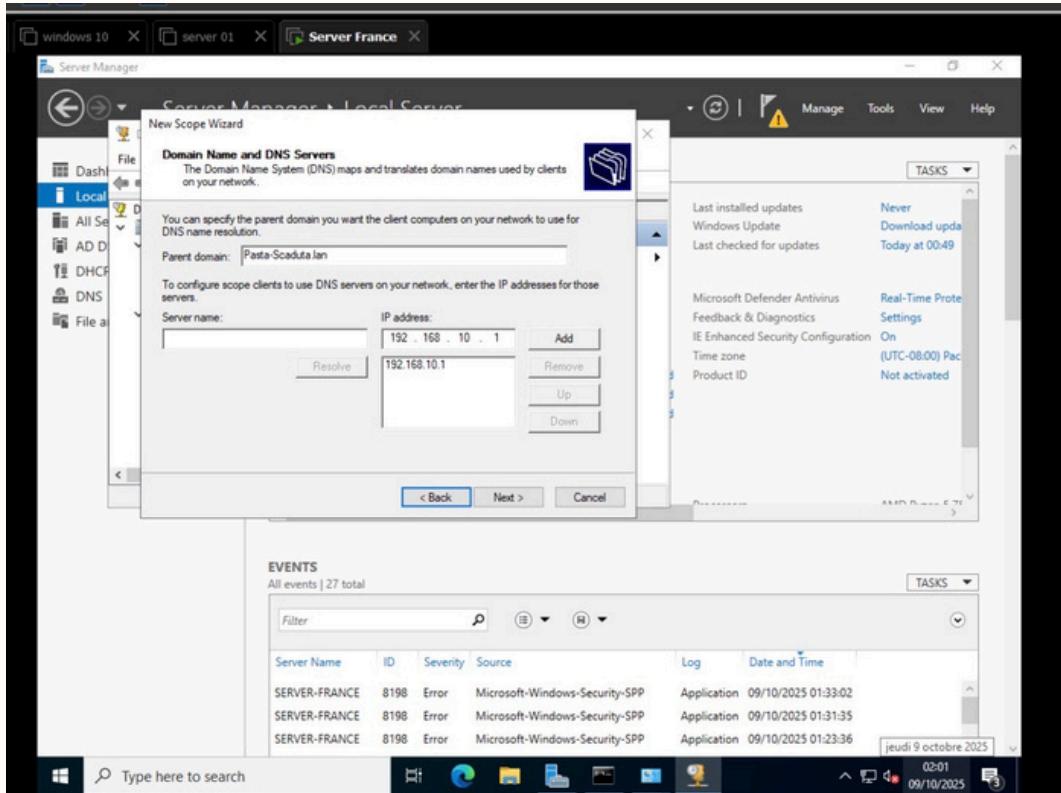


La passerelle par défaut a été fixée à 192.168.10.1, correspondant à l'adresse du serveur principal.

Le DNS utilisé est également 192.168.10.1, afin d'assurer la résolution interne du domaine Active Directory. Le domaine DNS associé au scope a été défini comme pasta-scaduta.lan

III / CONFIGURATION DE L'INFRASTRUCTURE

CONFIGURATION DNS

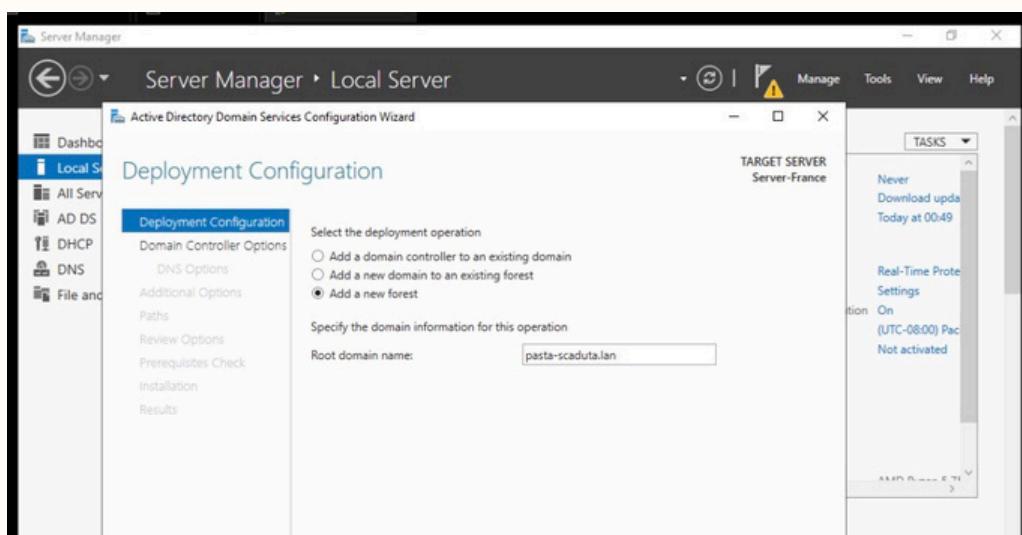


- Installation du rôle DNS Server : cette étape permet à la machine virtuelle de devenir un serveur capable de traduire les noms de domaine (ex. serveur.local) en adresses IP.
- Création d'une zone de recherche directe et/ou inversée : cela sert à enregistrer les correspondances entre les noms d'hôtes et les adresses IP, afin de faciliter la communication entre les ordinateurs du réseau sans avoir à mémoriser les adresses IP.

MISE EN PLACE ET CONFIGURATION DE L'AD DS ET DNS

Configuration AD DS :

Le serveur a été promu en contrôleur de domaine en créant une nouvelle forêt avec le nom de domaine pasta-scaduta.lan.

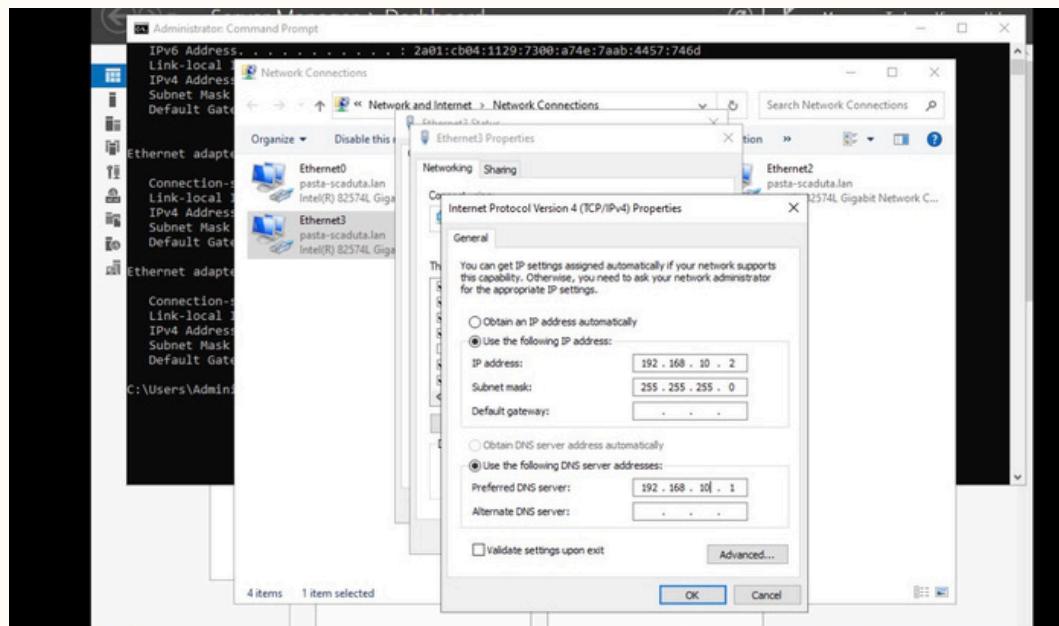


III / CONFIGURATION DE L'INFRASTRUCTURE

AJOUT DES COLLABORATEURS AU DOMAINE - POLOGNE

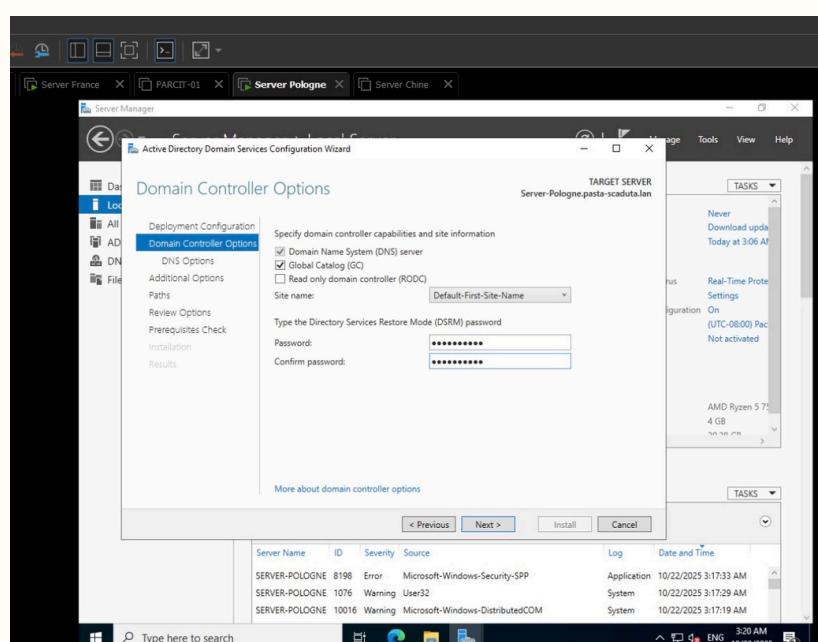
L'adresse IP : 192.168.10.2 a été attribué au serveur Pologne.

Après la configuration réseau et le renommage de la machine, le serveur Pologne a été intégré au domaine existant pasta-scaduta.lan et promu en tant que global catalogue via le rôle AD DS.

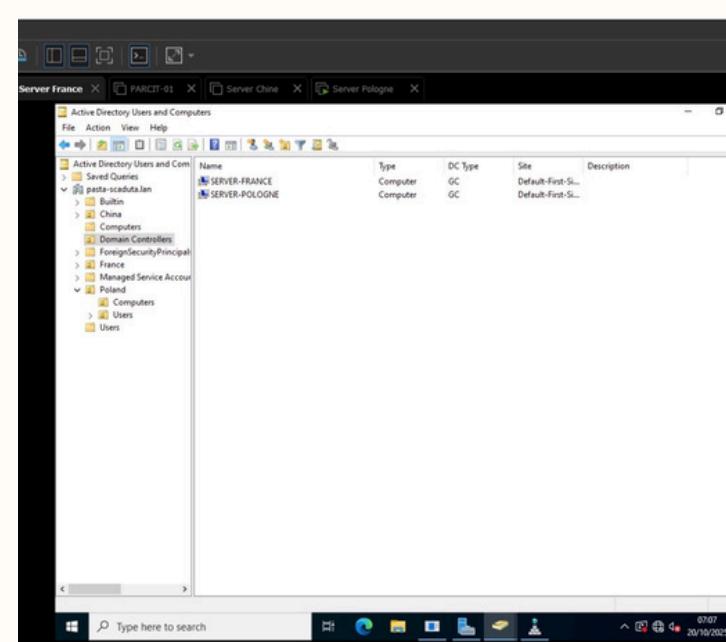


CONFIGURATION GC

Configuration du serveur en Global Catalog (GC) pour qu'il contienne une copie partielle de tous les objets du domaine. Il permet aux utilisateurs de trouver rapidement des informations sur n'importe quel objet de l'Active Directory, même dans d'autres sites ou sous-domaines. Le serveur Pologne a été configuré en GC pour faciliter la recherche et l'authentification des utilisateurs sur les deux principaux sites:



Configuration Global Catalog



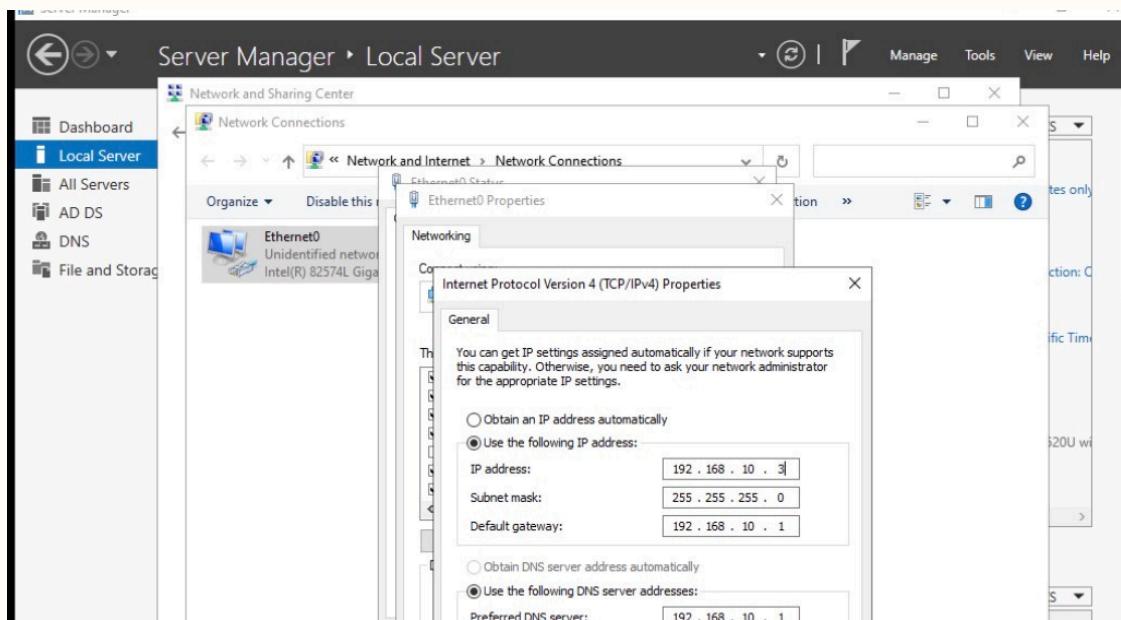
Le serveur Pologne apparaît bien dans le Domain Controllers

III / CONFIGURATION DE L'INFRASTRUCTURE

AJOUT DES COLLABORATEURS AU DOMAINE - CHINE

L'adresse IP 192.168.10.3 a été attribuée au serveur Chine.

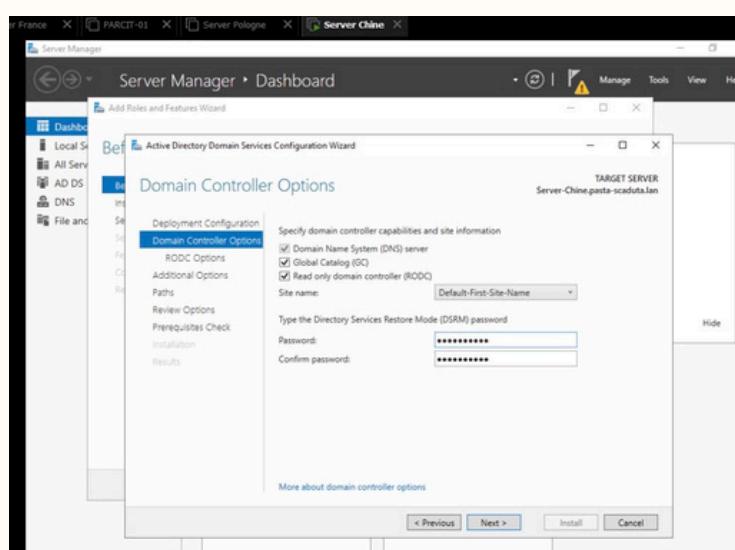
Après la configuration du réseau et le renommage de la machine, le serveur Chine a été rejoint au domaine existant pasta-scaduta.lan et configuré en tant que contrôleur de domaine en lecture seule (RODC) via le rôle AD DS.



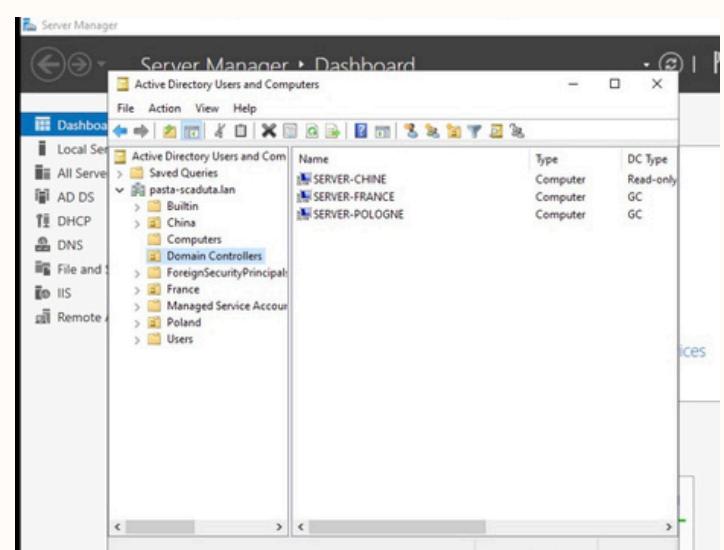
CONFIGURATION RODC

Configuration du serveur chine en RODC : (contrôleur de domaine en lecture seule.) Il contient une copie de l'Active Directory, mais ne peut pas effectuer de modifications. Il permet aux utilisateurs du site distant de s'authentifier localement tout en sécurisant les données les mots de passe et données sensibles restent protégés.

Le serveur Chine est un RODC pour limiter les risques sur le site éloigné.



Configuration RODC

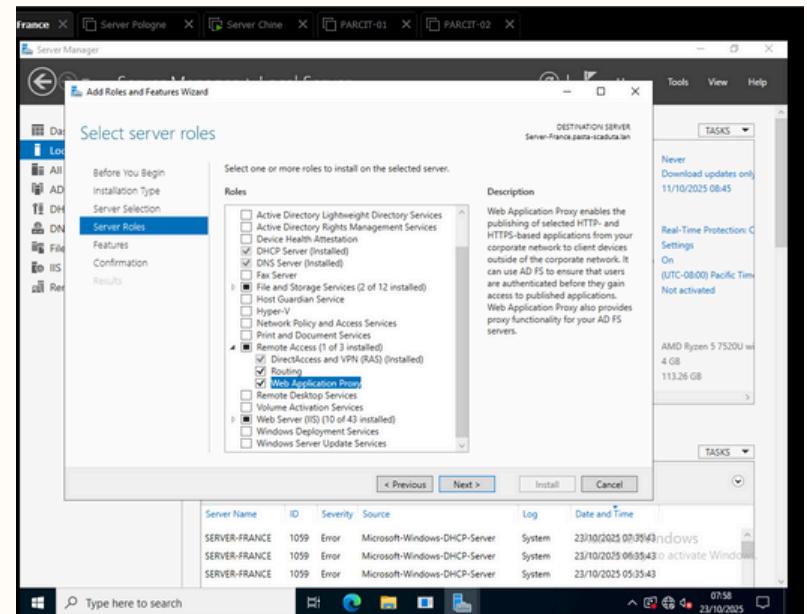


Le serveur Chine apparaît bien dans le Domain Controllers en Read-only

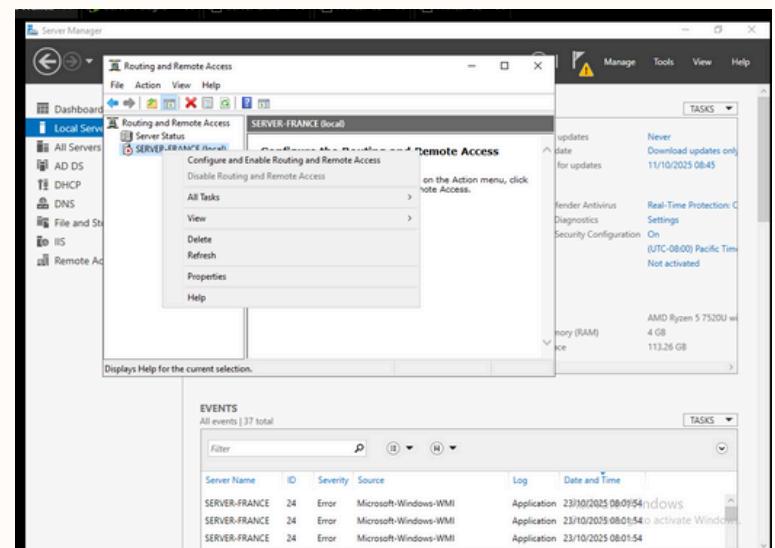
III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE VPN

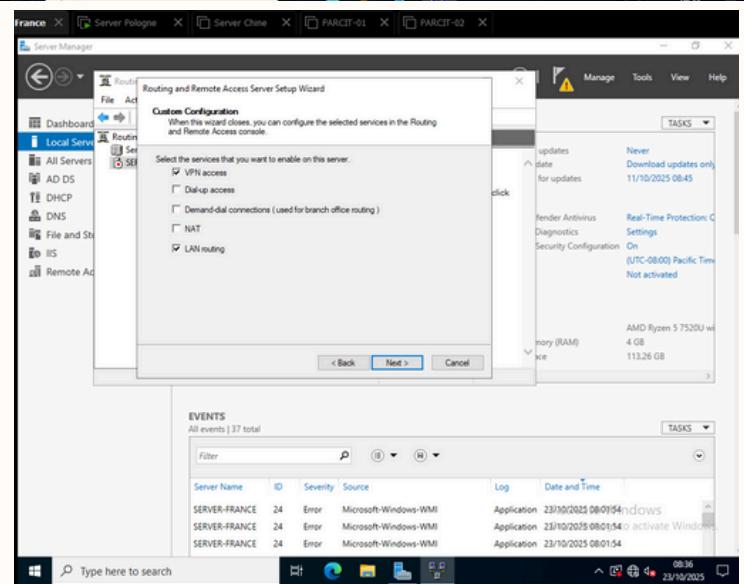
Ajout du role remote Access



Ouverture de routing et remote access



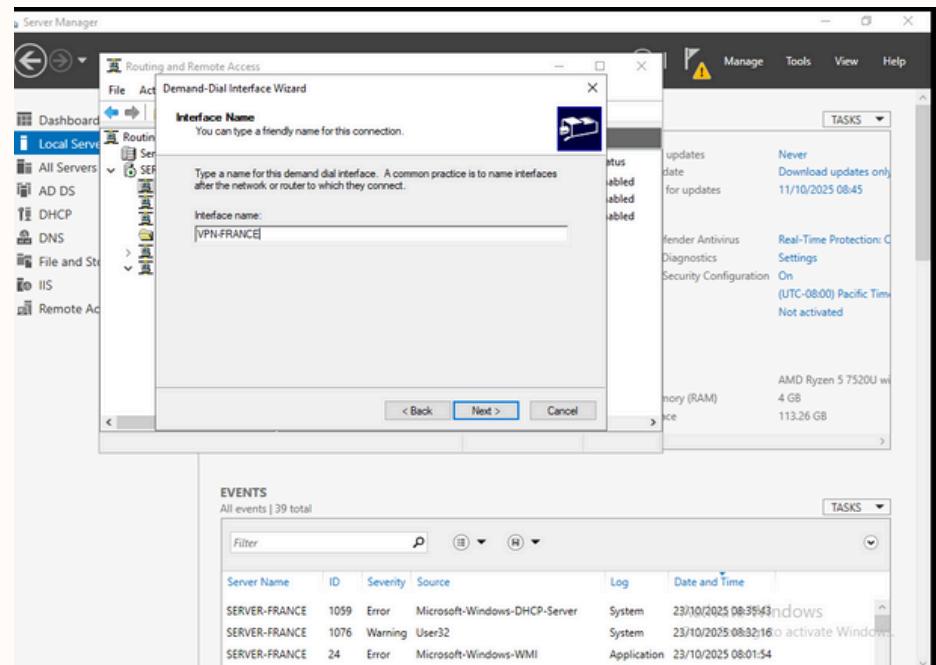
Configuration du VPN



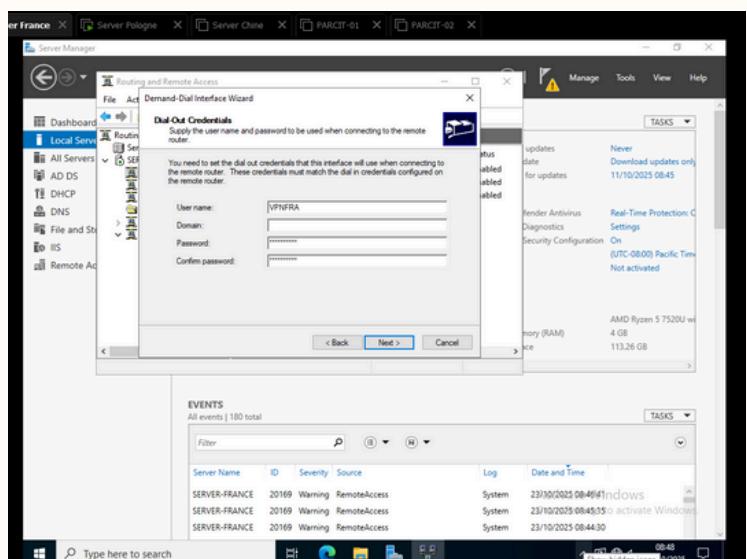
III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE VPN

Configuration du VPN (le nom VPN-FRANCE a été attribué)



Configuration du VPN (définition d'un Username et d'un mot de passe)



Les mêmes étapes ont été effectuées sur le serveur Pologne et Chine.

Le VPN site-to-site a été configuré entre les trois sites (France, Pologne, Chine) à l'aide du rôle RRAS.

Ce VPN permet la communication sécurisée entre les serveurs, la réplication Active Directory et le partage de ressources DFS.

Afin de limiter la consommation de bande passante, la réplication entre les contrôleurs de domaine a été planifiée de 20h à 6h, avec un coût de lien fixé à 400.

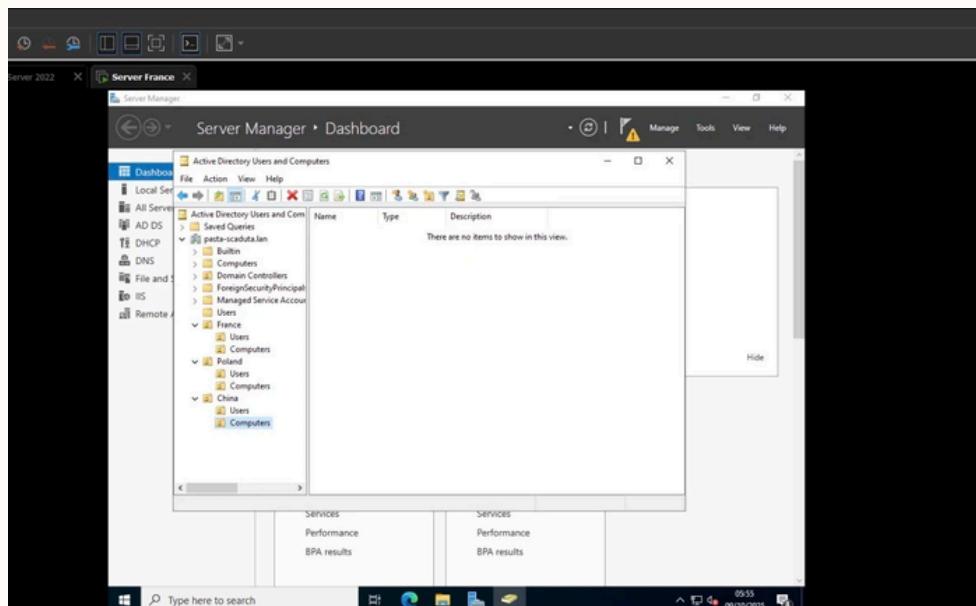
Le site chinois, disposant d'un RODC, utilise également une réplication de mot de passe pour garantir un fonctionnement local autonome en cas de déconnexion du VPN.

III / CONFIGURATION DE L'INFRASTRUCTURE

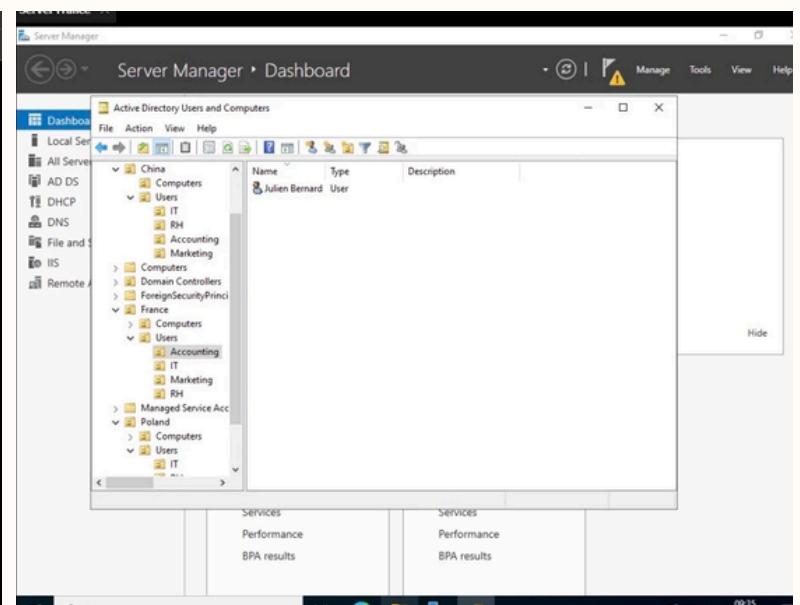
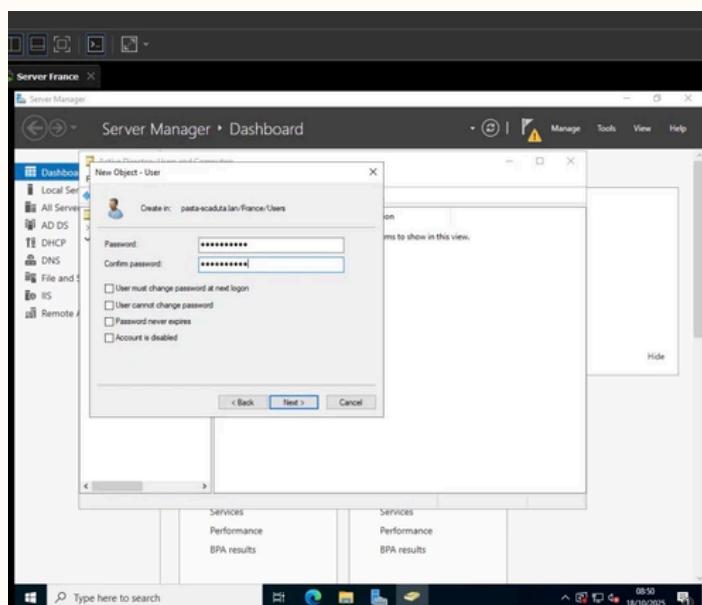
CRÉATION DES UTILISATEURS

Après la mise en place de la structure Active Directory, des Unités d'Organisation (OU) ont été créées afin de structurer les utilisateurs et ordinateurs par site et par service.

Les OU France, Pologne et Chine ont été subdivisées en deux catégories : Users et Computers, chacune contenant les sous-dossiers correspondant aux départements IT, Marketing, Sales, Accounting et RH.



À l'intérieur des différentes unités d'organisations, plusieurs comptes utilisateurs ont été créés pour représenter les employés de chaque service (exemple : Antoine Dupont → antoine.dupont). Chaque utilisateur a été configuré avec un mot de passe conforme aux politiques de sécurité



Un mot de passe est attribué à chaque utilisateur

Exemple de la création d'un utilisateur du département Accounting du serveur France

III / CONFIGURATION DE L'INFRASTRUCTURE

CRÉATION DES UTILISATEURS

Une fois la structure des unités d'organisation et les utilisateurs créés, des groupes de sécurité ont été mis en place afin de faciliter la gestion des permissions et des accès dans le domaine pasta-scaduta.lan.

Depuis la console Active Directory Users and Computers, la création s'effectue en sélectionnant l'OU concernée (par exemple France/Users/IT), puis en choisissant New → Group.

Chaque groupe a reçu un nom explicite correspondant à sa fonction, comme Global_IT_Admins, afin d'assurer une compréhension claire de leur rôle.

Les groupes ont été créés avec le scope Global, ce qui permet d'attribuer des permissions à des ressources situées dans d'autres domaines au sein de la même forêt.

Enfin, les utilisateurs correspondants ont été ajoutés à leurs groupes respectifs via l'onglet Members, garantissant une administration centralisée et une meilleure cohérence des droits d'accès sur l'ensemble de l'infrastructure.

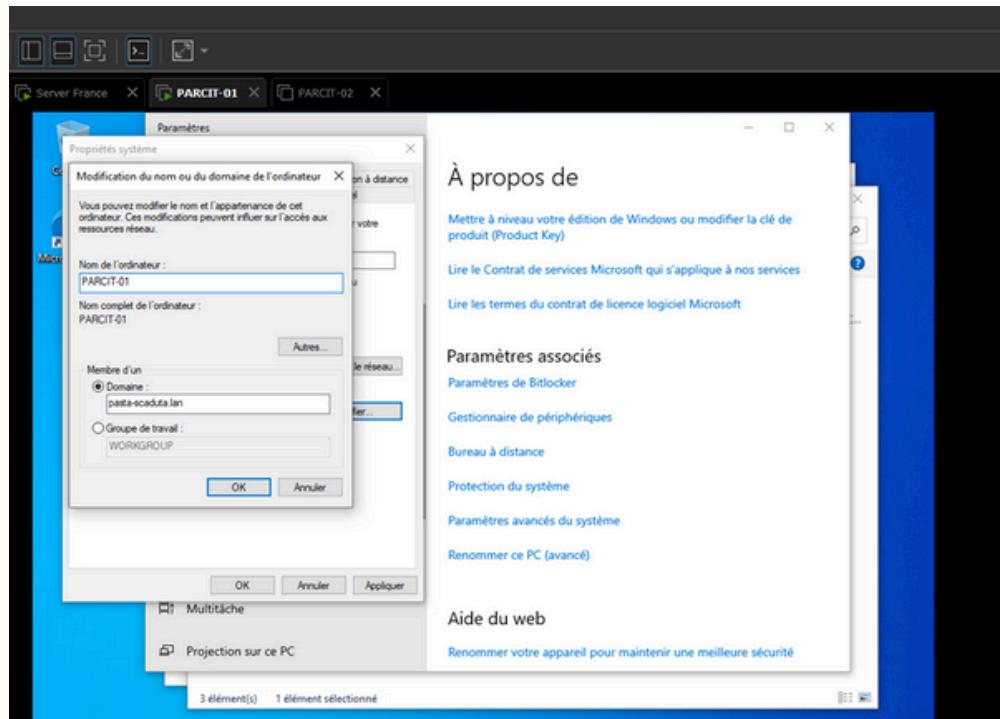
The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane displays the organizational structure under 'Active Directory Users and Computers'. It includes 'Saved Queries', 'pastascaduta.lan' (with 'Builtin' and 'Chine' containers), 'COMPUTER' (with Accounting, HR, IT, Marketing, Sales), 'USER' (with Accounting, Groupe, HR, IT, Marketing, Sales), 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'France', 'Group', 'Keys', and 'LostAndFound'. On the right, a table lists three security groups: 'Global.IT.Ad...', 'Group', and 'Securite', all categorized as 'Security Group ...'. The 'Groupe' group is currently selected in the tree view.

Name	Type
Global.IT.Ad...	Security Group ...
Group	Security Group ...
Securite	Security Group ...

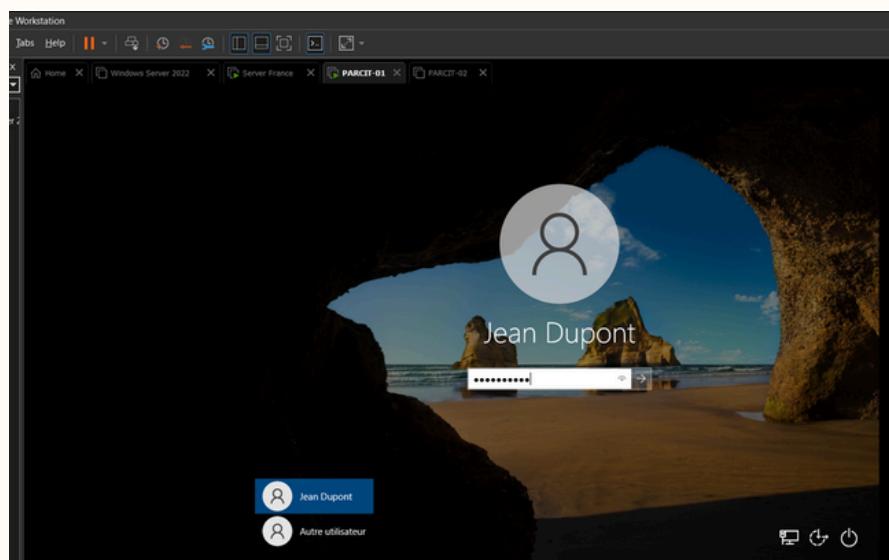
III / CONFIGURATION DE L'INFRASTRUCTURE

CRÉATION D'UN PC CLIENT

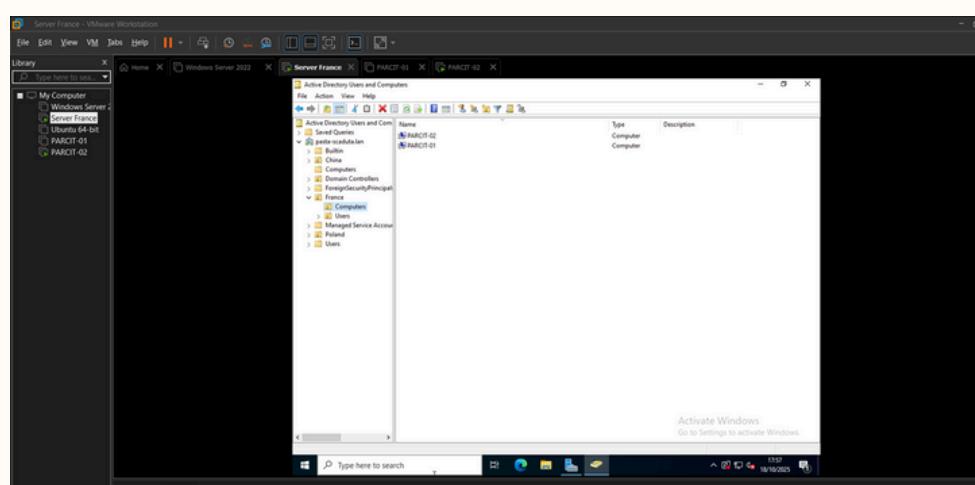
Ajout du Pc client 1 au domaine pastascudeta (clique droit sur windows → système → renommer ce PC):



Test de connexion via un des comptes créés :



Le PC client apparait bien dans l'AD DS dans l'onglet computers



III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DU ROLE DFS

- Après l'installation du rôle DFS, il faut créer un espace de noms (Namespace) via le Gestionnaire DFS. Celui-ci regroupe plusieurs partages de fichiers provenant de serveurs différents sous un chemin d'accès unique, ce qui simplifie la navigation et la gestion des données.
- Utilité : Le Namespace DFS offre une vue unifiée et logique des partages réseau, améliore la résilience grâce à la réPLICATION des données, et optimise la disponibilité des fichiers pour les utilisateurs.
- Pour établir le lien entre DFS et iSCSI, il faut d'abord configurer une cible iSCSI sur le serveur de stockage, puis connecter cette cible depuis le serveur principal à l'aide de l'outil iSCSI Initiator. Une fois le volume iSCSI monté et formaté, celui-ci est utilisé comme emplacement de stockage pour les partages DFS, assurant ainsi une gestion logique des données via DFS et un stockage centralisé via iSCSI.

The screenshot shows the 'SERVICES' section of the Windows Server 2012 Control Panel. The left sidebar is titled 'Servers' and includes links for Volumes, Disks, Storage Pools, Shares, iSCSI, and Work Folders. The main pane displays a table of services with the following data:

Server Name	Display Name	Service Name	Status	Start Type
SERVEUR-FRANCE	DFS Namespace	Dfs	Running	Automatic
SERVEUR-FRANCE	DFS Replication	DFSR	Running	Automatic
SERVEUR-FRANCE	Microsoft iSCSI Target Server	WinTarget	Running	Automatic
SERVEUR-FRANCE	Server	LanmanServer	Running	Automatic (Triggered)

EXTENSION D'UN VOLUME RAID 5

On ajoute 3 disques à une configuration RAID 5 existante :

- On augmente la capacité totale disponible (tout en gardant l'équivalent d'un disque réservé à la parité).
- On améliore la tolérance aux pannes : toujours une seule panne tolérée, mais sur un plus grand volume.
- On optimise les performances en lecture, car les données sont lues en parallèle sur plusieurs disques

The screenshot shows the 'Disk Management' tool in the Windows Server 2012 Control Panel. The left sidebar lists 'Computer Tools' (Task Scheduler, Event Viewer, Shared Folders, Performance, Device Manager), 'Storage' (Windows Server Backup, Local Backup, Disk Management), and 'Services and Applications'. The main pane shows a table of volumes and a graphical representation of disk drives:

Volume	Layout	Type	File System	Status
(C)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Basic Data Part)
(Disk 4 partition 1)	Simple	Basic		Healthy (EFI System Partition)
New Volume (M:)	RAID-5	Dynamic	NTFS	Healthy

The graphical interface shows two disks: 'Disk 0' (Unknown, 60.00 GB, Offline) and 'Disk 1' (Dynamic, 9.98 GB, NTFS, Online). A new volume 'New Volume (M:)' is being created, utilizing the available space on both disks. The status bar at the bottom indicates: 'Unallocated' (black), 'Primary partition' (dark blue), and 'RAID-5 volume' (light blue).

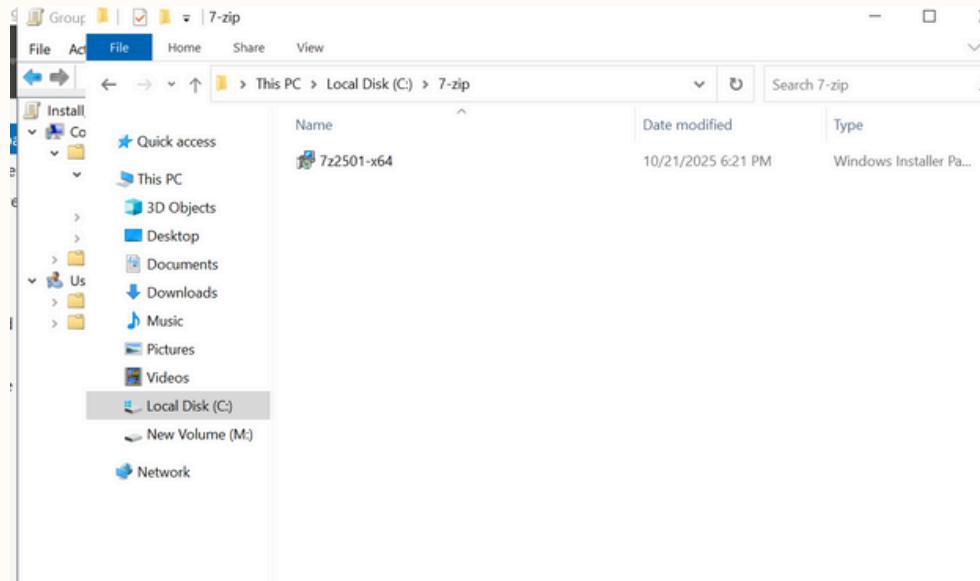
L'extension du volume RAID 5 permet à PastaScaduta d'augmenter sa capacité de stockage globale tout en maintenant la sécurité des données grâce à la parité. Cette configuration assure une meilleure performance en lecture et une continuité d'activité en cas de défaillance d'un disque, garantissant ainsi la disponibilité et la fiabilité des données critiques de l'entreprise (comptabilité, production, fichiers partagés entre les filiales de Chine et de Pologne).

III / CONFIGURATION DE L'INFRASTRUCTURE

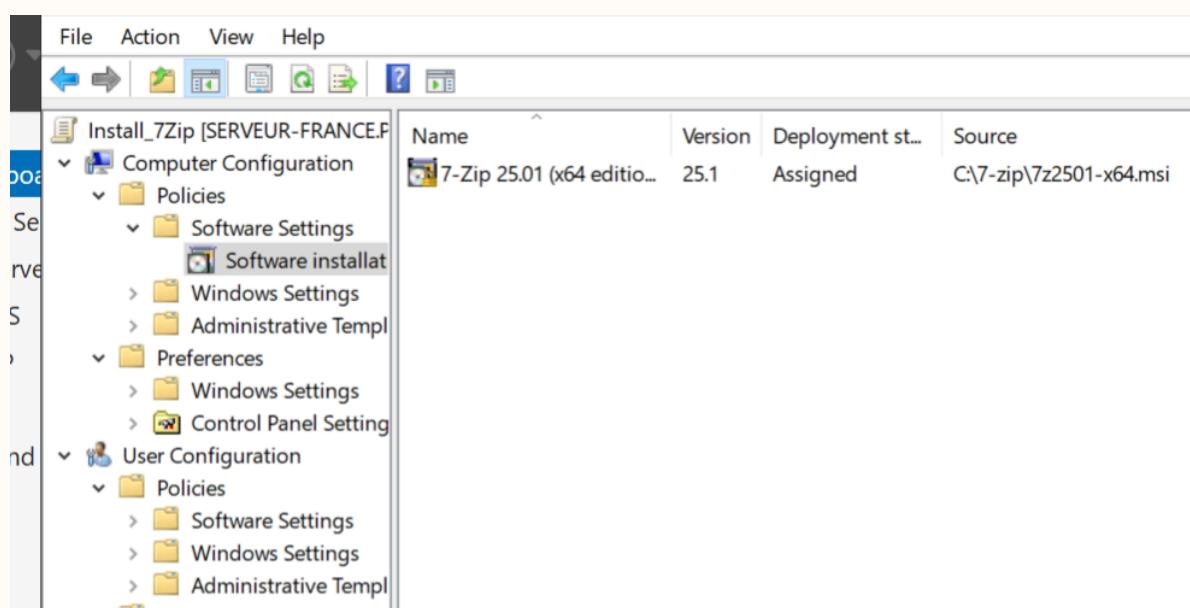
MISE EN PLACE DES REGLES GPO

RÈGLE "DEPLOY 7-ZIP"

Téléchargement de la version 7-zip en msi, puis créer un dossier dans (:C)



Cette étape consiste à créer une stratégie de groupe (GPO) permettant d'installer automatiquement le logiciel 7-Zip sur les ordinateurs du domaine. Pour cela, le fichier d'installation au format MSI est placé dans un dossier partagé accessible au réseau, puis ajouté dans la GPO via *Computer Configuration* → *Policies* → *Software Settings* → *Software Installation*, afin qu'il soit déployé sur les machines de l'unité d'organisation ciblée au redémarrage.

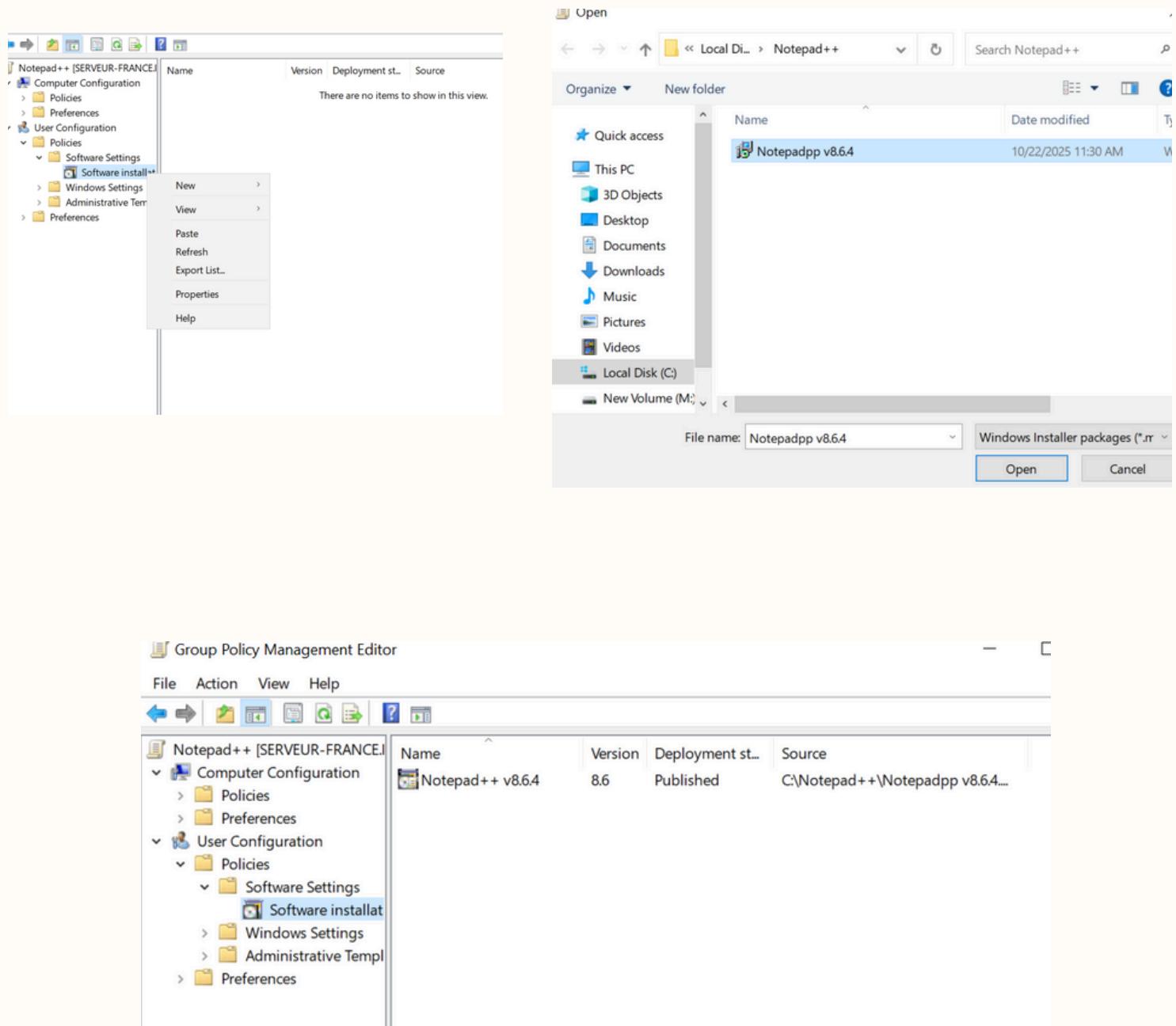


III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DES REGLES GPO

RÈGLE “SUGGEST NOTEPAD++”

Cette étape consiste à proposer ou installer Notepad++ sur les ordinateurs du domaine en utilisant un script d’installation placé dans un dossier réseau partagé. Le script exécute silencieusement le fichier d’installation EXE au démarrage des ordinateurs ciblés par la GPO, permettant ainsi l’installation centralisée et automatique du logiciel sur toutes les machines de l’unité d’organisation choisie.



Aller dans User Configuration → Policies → Software Setting

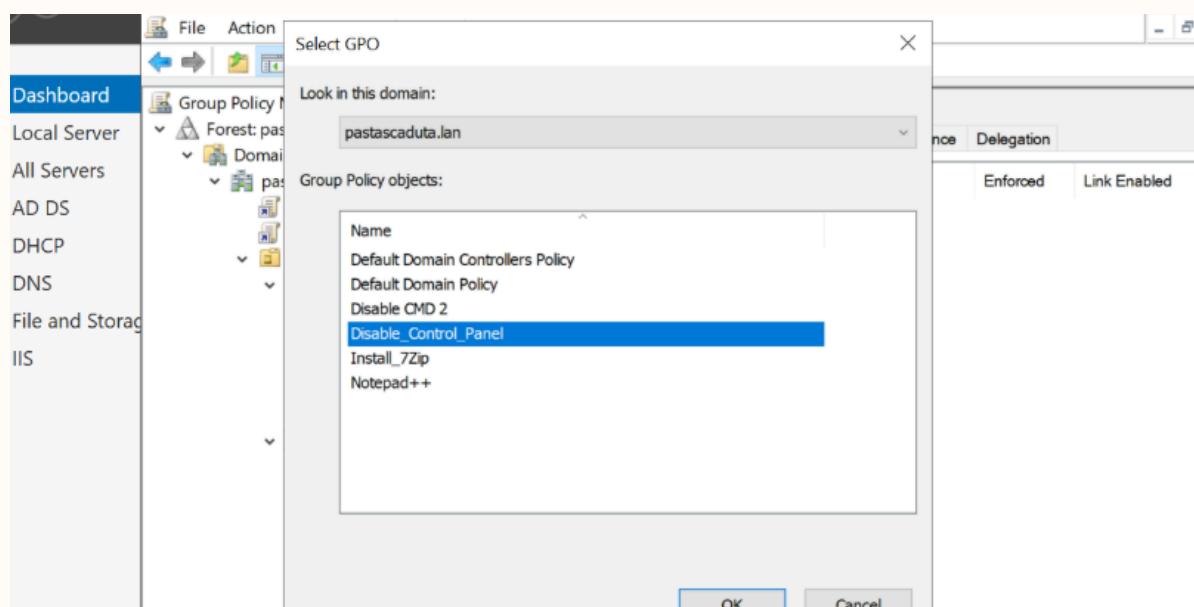
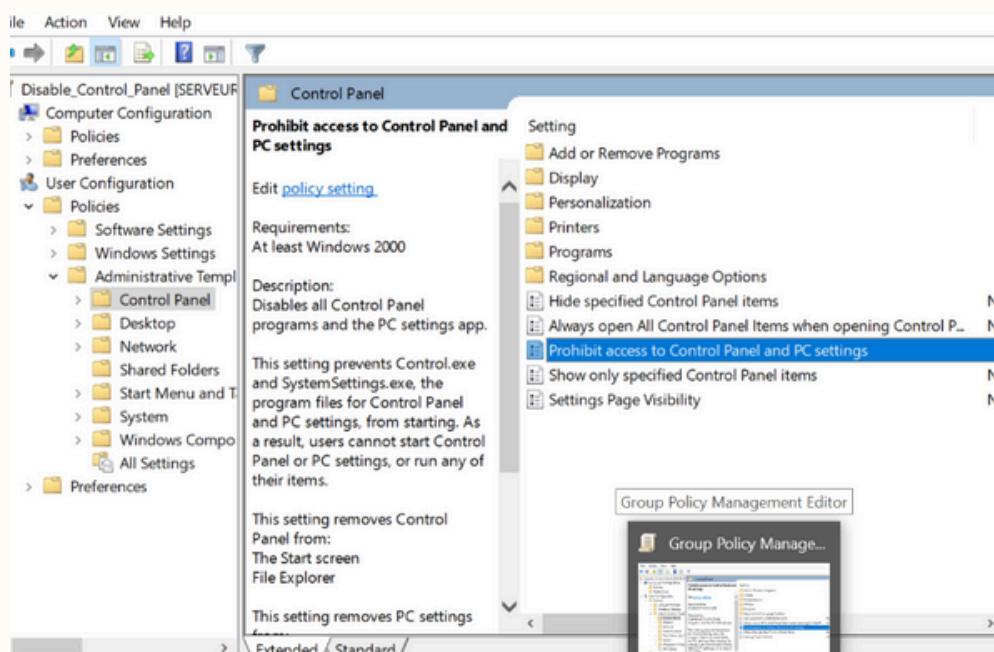
Créer un “New Package” et sélectionner le logiciel en msi installé et cliquer sur “Publish”.

III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DES REGLES GPO

RÈGLE "DISABLE CONTROL PANEL"

Création d'une nouvelle GPO sur le contrôleur de domaine en cliquant droit sur Group Policy Objects → New, puis en la nommant Disable_Control_Panel et en validant par OK. Ensuite, on édite cette GPO en cliquant droit sur Disable_Control_Panel → Edit et on navigue dans User Configuration → Policies → Administrative Templates → Control Panel pour configurer les paramètres qui interdisent l'accès au Panneau de configuration aux utilisateurs ciblés.



Lien de la GPO à l'OU cible.

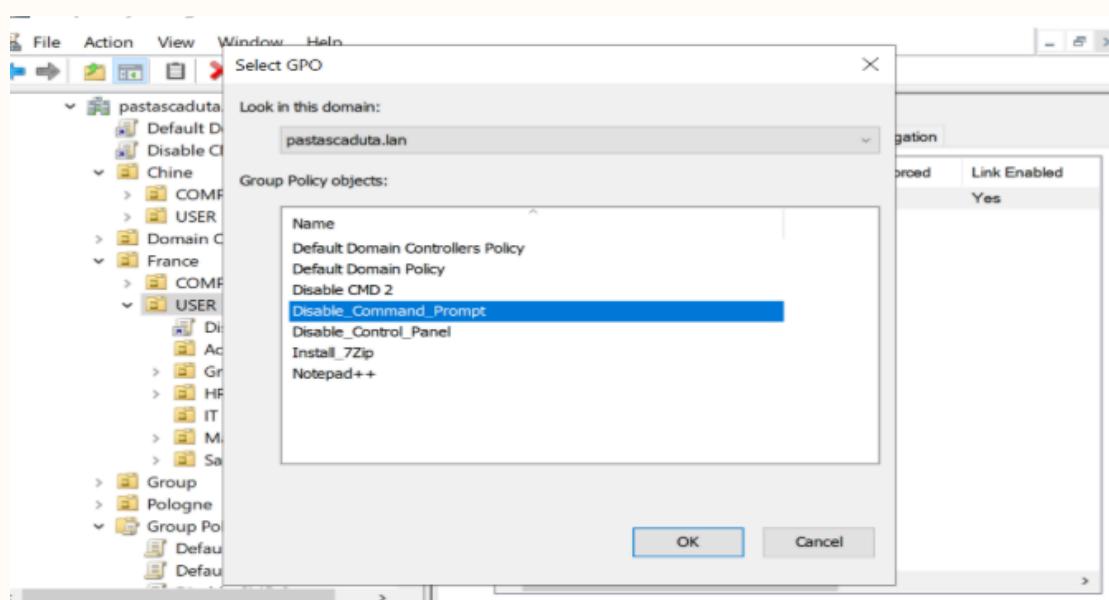
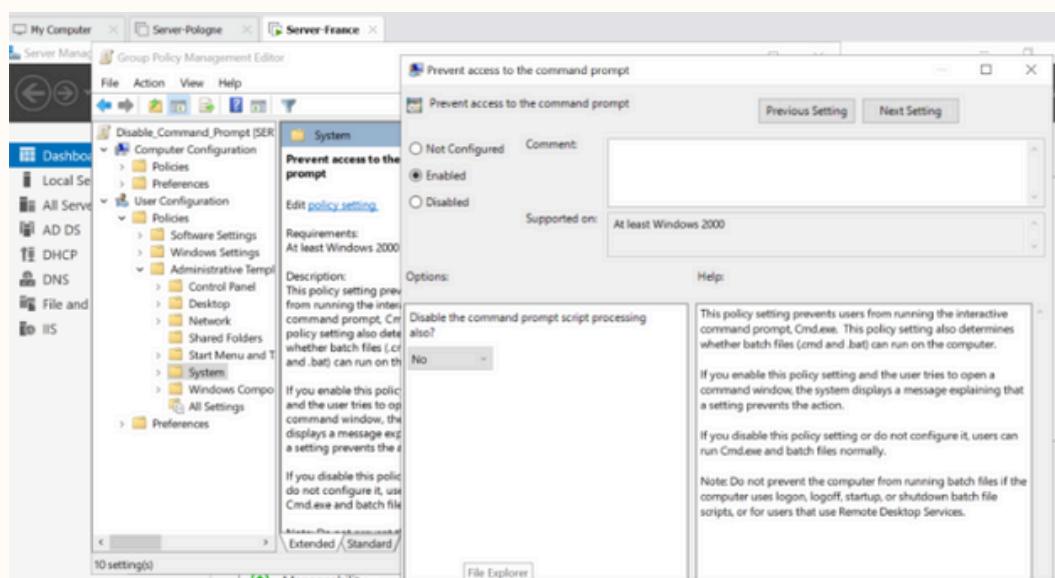
III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DES REGLES GPO

RÈGLE "DISABLE COMMAND PROMPT"

La GPO "Disable Command Prompt" est créée dans GPMC sur le contrôleur de domaine en cliquant droit sur Group Policy Objects → New et en la nommant Disable_Command_Prompt. Elle permet d'empêcher les utilisateurs ciblés d'ouvrir l'invite de commandes (cmd) et, si configuré, d'exécuter des scripts batch, garantissant ainsi la sécurité et le contrôle des actions sur les postes du domaine.

Clic droit sur la GPO → Edit → Aller dans User Configuration → Policies → Administrative Templates → System → Ouvrir Prevent access to the command prompt, sélectionner Enabled → (Optionnel) cocher Disable the command prompt script processing pour bloquer les scripts batch



Pour appliquer la GPO, il faut la lier à l'OU contenant les utilisateurs concernés. Dans GPMC, clic droit sur l'OU → Link an Existing GPO... → sélectionne Disable_Command_Prompt → OK. Les paramètres de la GPO seront alors appliqués à tous les comptes utilisateurs de cette OU.

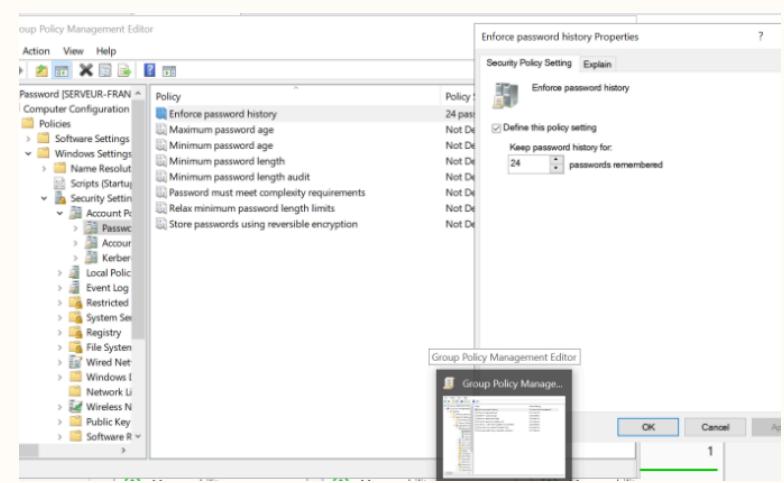
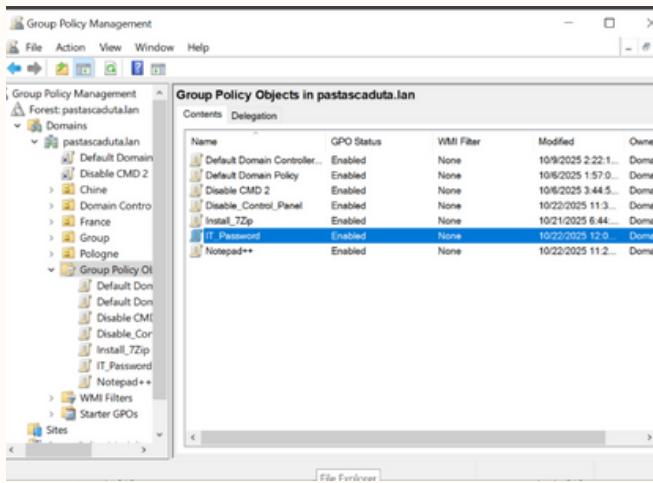
III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DES REGLES GPO

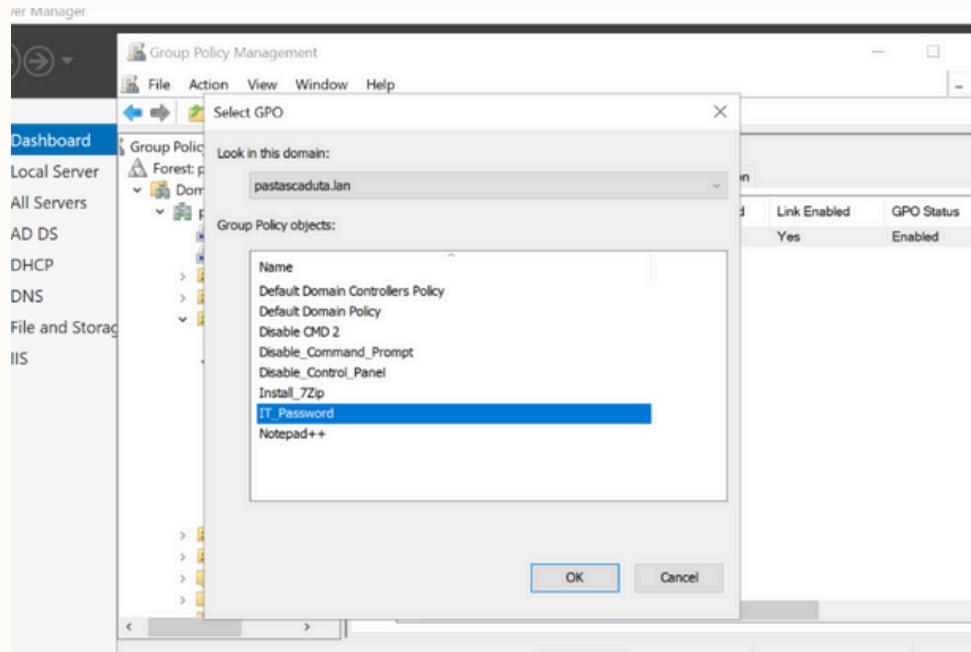
RÈGLE "IT PASSWORD"

La GPO "IT Password" est créée dans la **GPMC** et permet de définir des règles de sécurité pour les mots de passe des utilisateurs du domaine.

Clic droit sur Group Policy Objects → New, nommer la GPO IT_Password → Clic droit sur la GPO → Edit → Aller dans Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy → Configurer les paramètres souhaités (longueur minimale, complexité, durée maximale, historique) → Lier la GPO à l'unité d'organisation contenant les utilisateurs ciblés.



- Longueur minimale : 20
- Complexité : activée
- Durée de vie maximale : 15 jours
- Mémorisez 10 mots de passe



Toutes les règles définies dans IT_Password (ex. longueur minimale du mot de passe, complexité...) seront appliquées aux utilisateurs du domaine ou de l'OU choisie.

Important : la GPO doit être liée à l'IT concerné, c'est-à-dire à l'OU ou au domaine où se trouvent les comptes utilisateurs qui doivent suivre ces règles. Sinon, la GPO existera mais ne sera pas appliquée à ces comptes.

- Dans GPMC, clic droit sur le domaine ou sur une OU contenant les utilisateurs → Link an Existing GPO... → sélectionner IT_Password → OK
- Les règles de mot de passe seront alors appliquées aux comptes utilisateurs ciblés.

III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DES REGLES GPO

RÈGLE "USER_PASSWORD"

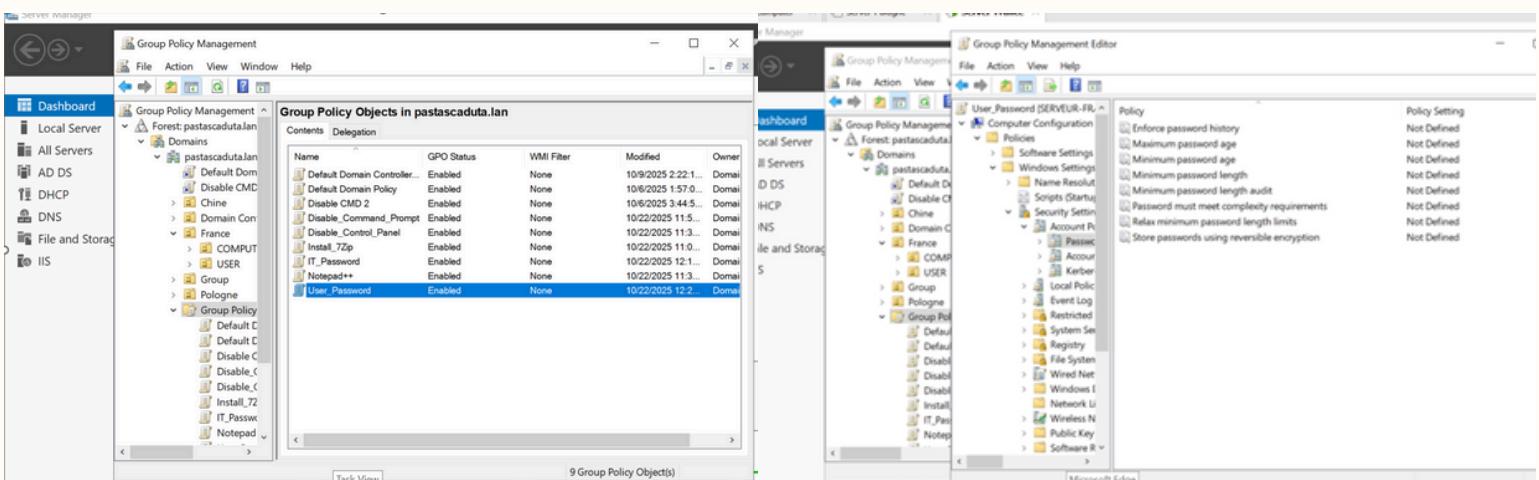
La GPO "**User_Password**" a été créée dans la GPMC afin de définir les règles de sécurité appliquées aux mots de passe des utilisateurs du domaine.

Pour cela, un nouveau GPO a été ajouté via Group Policy Objects → New, puis nommé User_Password.

La GPO a ensuite été modifiée en accédant à Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy.

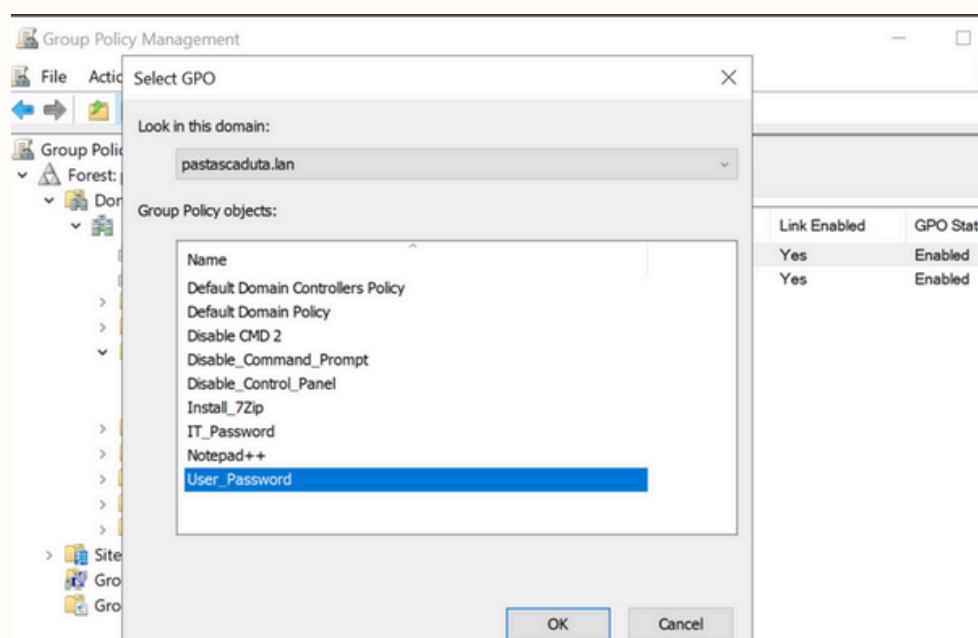
Les paramètres ont été configurés conformément aux exigences de sécurité

Enfin, la GPO a été liée à l'unité d'organisation contenant les utilisateurs standards, afin d'assurer l'application automatique de ces règles à l'ensemble des comptes concernés.



- Longueur minimale : 8
- Complexité : activée

- Durée de vie maximale : 30 jours
- Mémorisez 5 mots de passe



Toutes les règles définies dans la GPO User_Password (par exemple : longueur minimale, complexité, durée maximale, historique des mots de passe) sont appliquées aux utilisateurs du domaine ou de l'OU ciblée.

Il est important de lier la GPO à l'OU ou au domaine où se trouvent les comptes utilisateurs concernés, sinon la stratégie existera dans GPMC mais ne sera pas appliquée.

Pour effectuer cette liaison :

1. Dans GPMC, clic droit sur le domaine ou sur l'OU contenant les utilisateurs → Link an Existing GPO...

2. Sélectionner la GPO User_Password → OK

Après cette opération, toutes les règles définies seront automatiquement appliquées aux comptes utilisateurs ciblés.

III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DES REGLES GPO

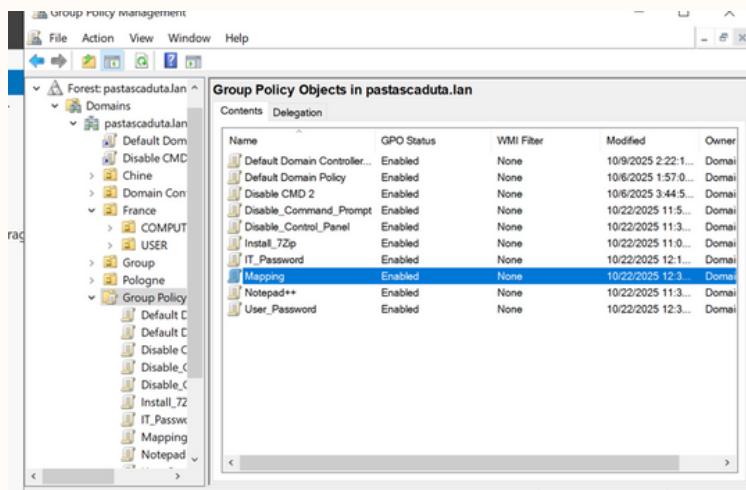
RÈGLE "MAPPING"

La GPO "Mapping" est créée dans Group Policy Management (GPMC) et permet de connecter automatiquement des lecteurs réseau aux utilisateurs ou ordinateurs ciblés, facilitant l'accès centralisé aux dossiers partagés et garantissant que chaque poste dispose des ressources réseau nécessaires.

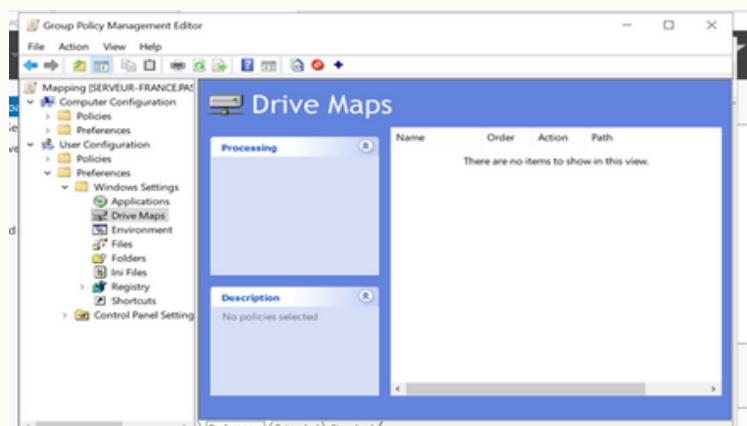
Pour configurer le mappage il faut ouvrir la console GPMC, puis créer une nouvelle GPO via Group Policy Objects → New et la nommer, Mapping.

Ensuite, faire un clic droit sur la GPO et sélectionner Edit. Dans l'éditeur de stratégie de groupe, naviguer vers User Configuration → Preferences → Windows Settings → Drive Maps.

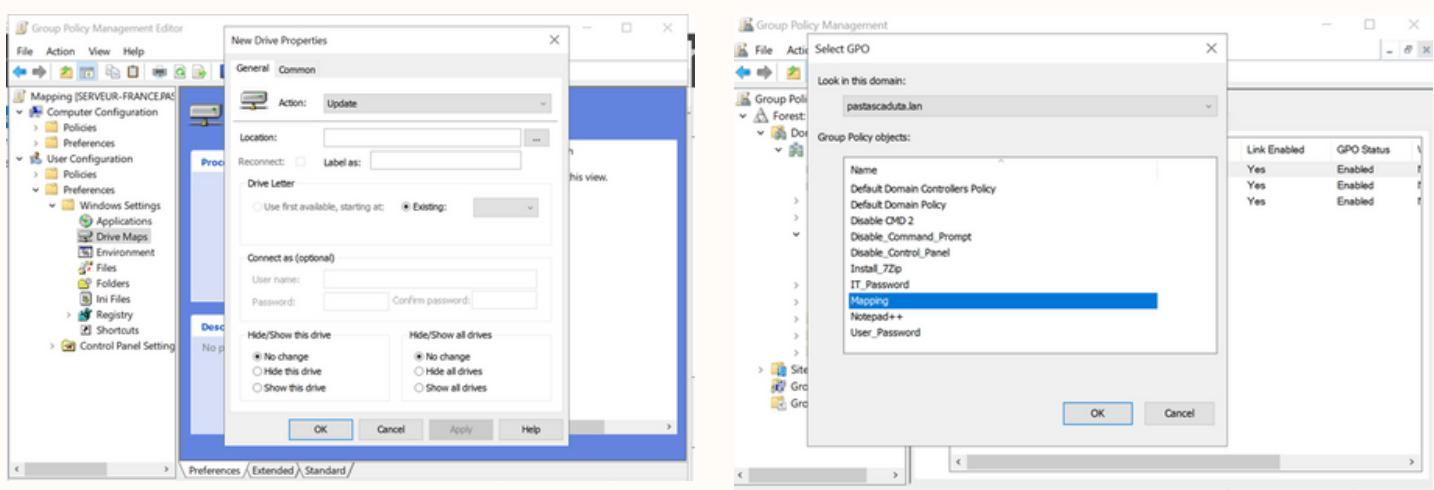
Cliquer sur New → Mapped Drive, puis définir la lettre du lecteur et le chemin UNC du partage correspondant au département ou groupe d'utilisateurs



Pour un mapping utilisateur :



Pour un mapping machine :



Enfin, il faut lier la GPO à l'OU contenant les utilisateurs ciblés via clic droit sur l'OU → Link an Existing GPO... → sélectionner Mapping → OK.

Une fois cette opération effectuée, les lecteurs réseau seront automatiquement mappés sur les postes des utilisateurs lors de leur prochaine connexion.

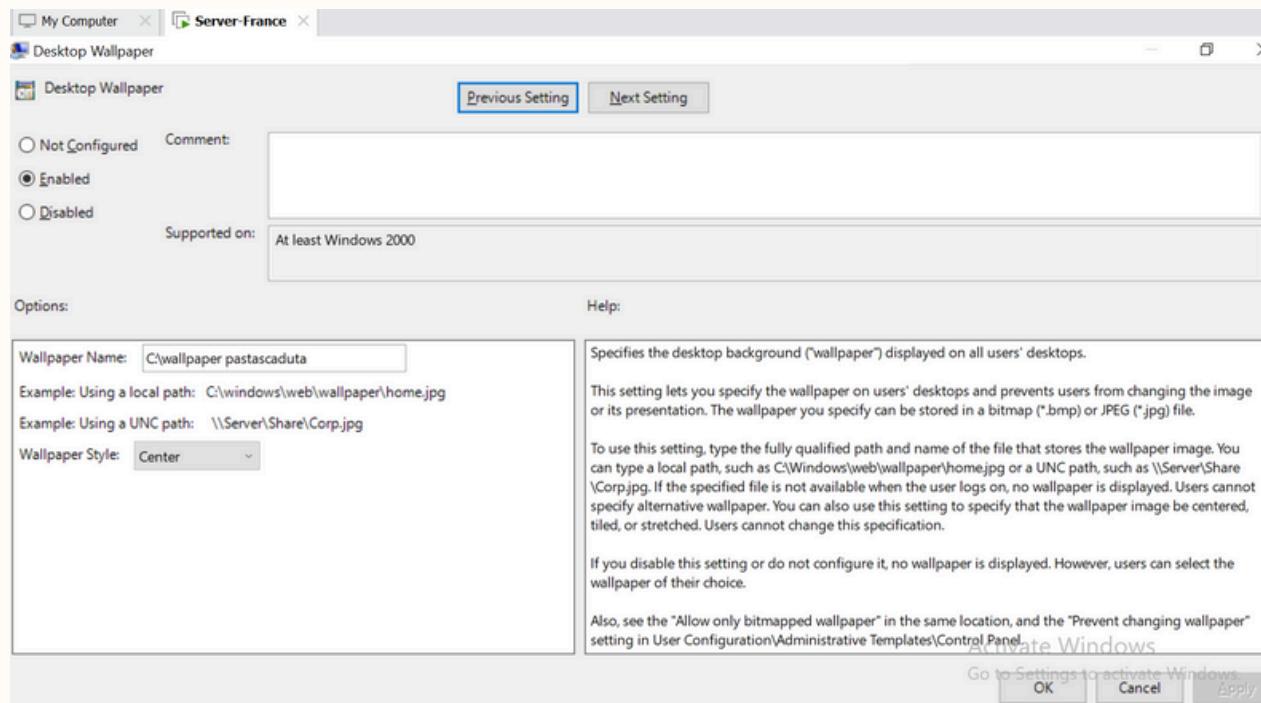
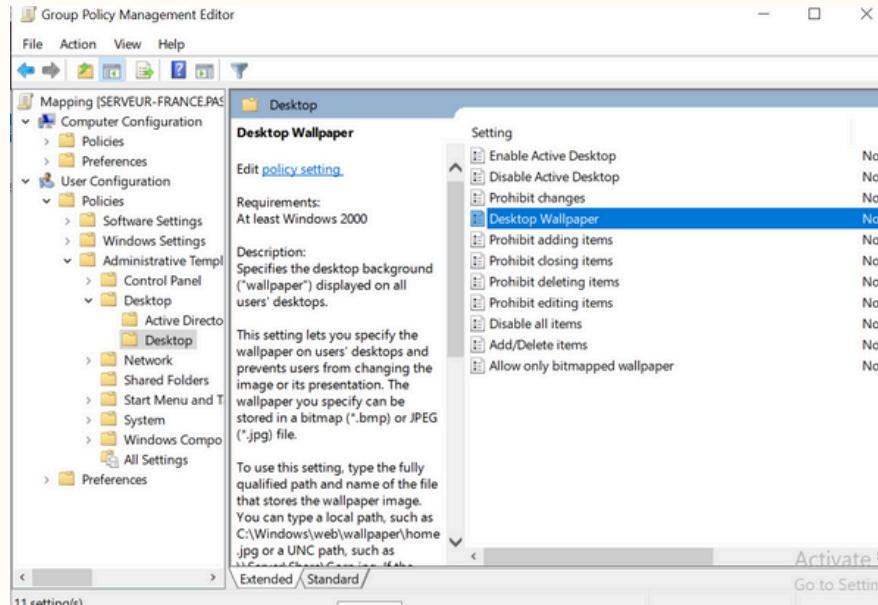
III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DES REGLES GPO

RÈGLE "WALLPAPER"

Pour renforcer l'identité visuelle de l'entreprise, un fond d'écran commun est déployé sur tous les postes utilisateurs.

→ User Configuration → Administrative Templates → Desktop → Desktop → Desktop Wallpaper



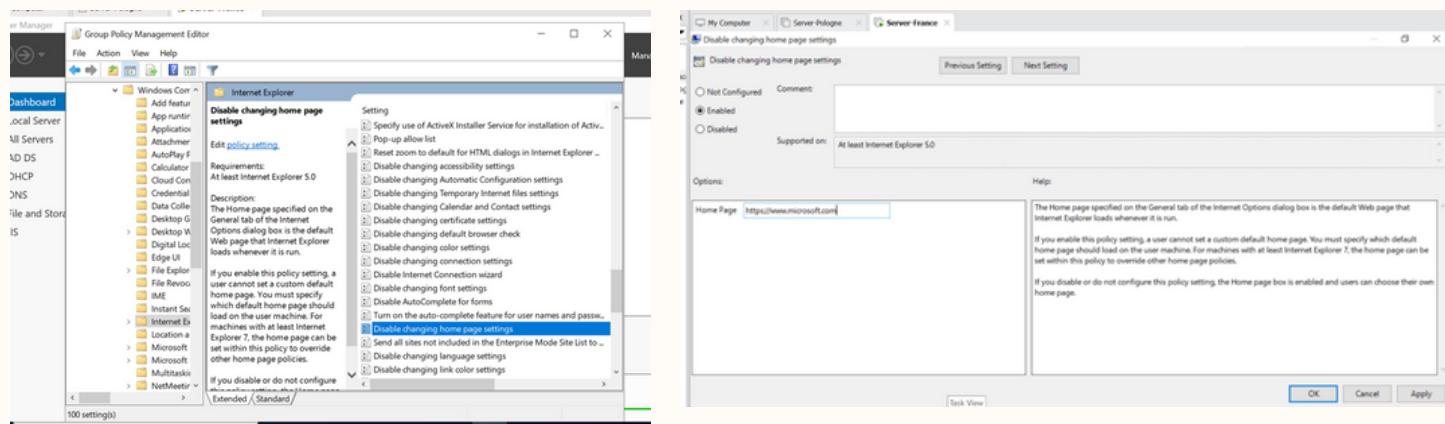
Appuyer sur le bouton "Enabled" → Indiquer l'adresse pour afficher la photo → Apply → Ok

III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DES REGLES GPO

RÈGLE "HOMESCREEN INTERNET EXPLORER"

La GPO "Homescreen Internet Explorer" permet de définir automatiquement la page d'accueil d'Internet Explorer pour les utilisateurs ciblés, assurant un accès uniforme à un site spécifique ou à l'intranet. Elle est créée dans Group Policy Management (GPMC) et configurée dans User Configuration → Policies → Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel → Home Page.



Nom de la GPO : Disable changing home page settings

Emplacement dans GPMC :

User Configuration → Policies → Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel → Disable changing home page settings

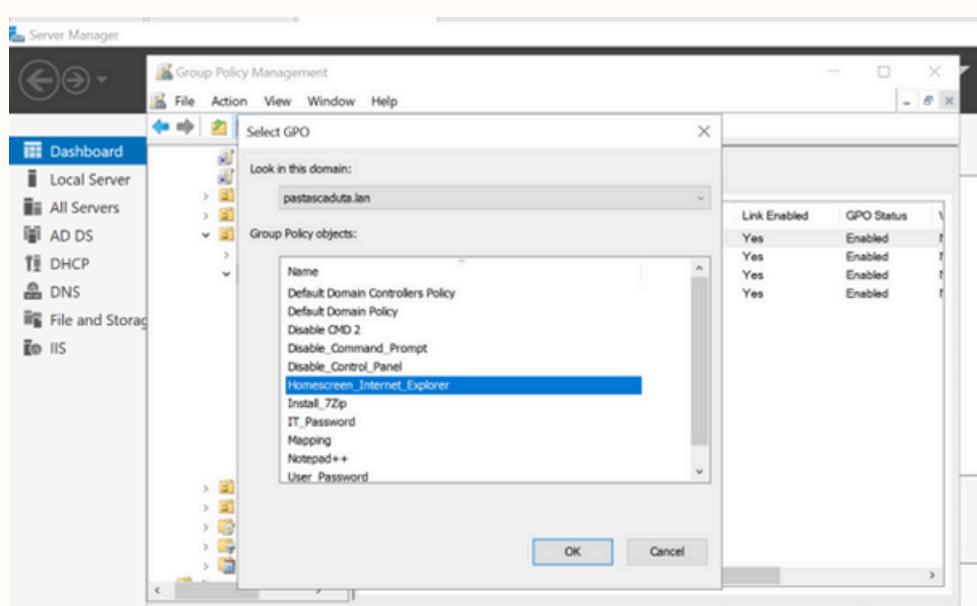
Configuration :

· Paramètre : Enabled

· Effet : La page d'accueil définie par l'administrateur devient verrouillée et les utilisateurs ne peuvent pas la modifier.

OU cible : OU contenant les utilisateurs du domaine devant avoir cette restriction.

Application : Appliquée au prochain logon des utilisateurs ou après gpupdate /force.



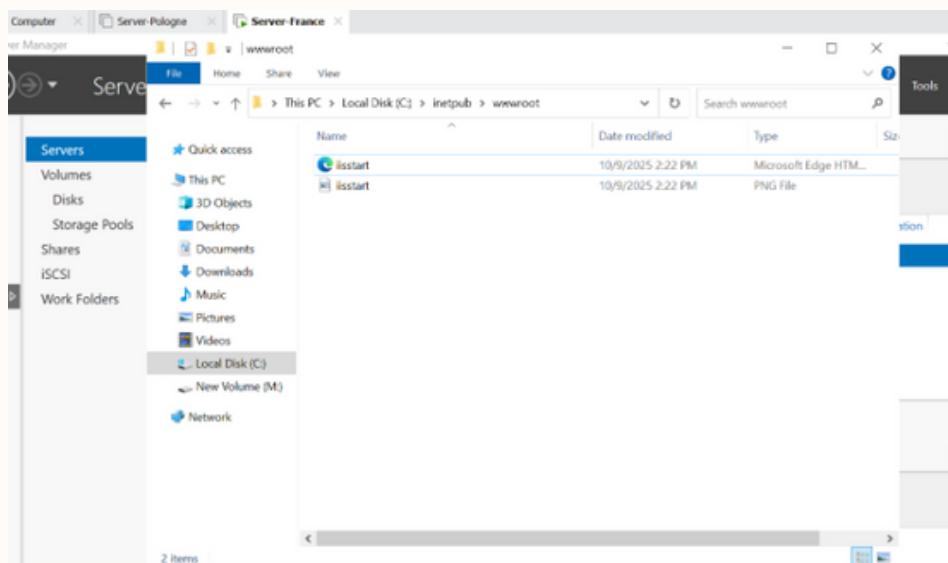
La GPO "Disable changing home page settings" est liée à l'OU contenant les utilisateurs ciblés via Group Policy Management → Link an Existing GPO, ce qui garantit que la restriction sur la page d'accueil d'Internet Explorer est appliquée automatiquement à tous les comptes de cette OU.

III / CONFIGURATION DE L'INFRASTRUCTURE

MISE EN PLACE DU IIS

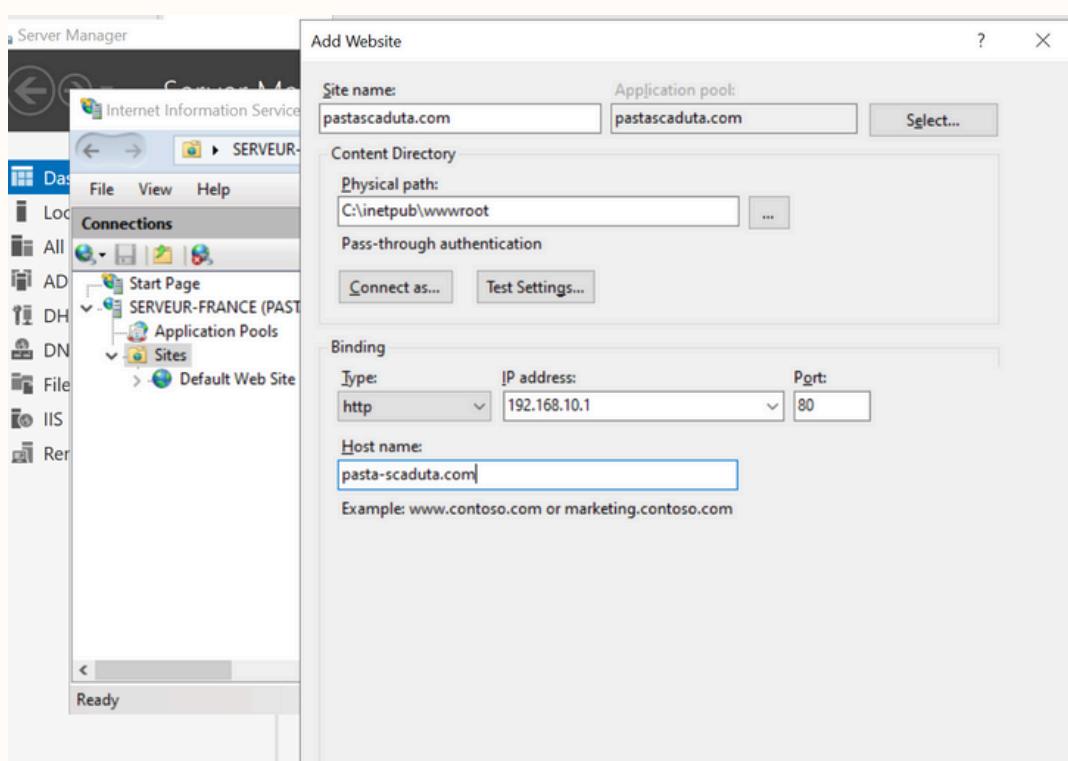
CONFIGURATION DU IIS

Cette étape consiste à créer un site web local en ajoutant un dossier "mysite" dans inetpub (le répertoire par défaut d'IIS), puis à y créer un fichier .html afin de tester l'affichage d'une page web hébergée localement. Gestionnaire de tâches à Local Disk (C :) → inetpub → créer dossier « mysite » à clic droit, new à wwwroot → Text Document → Le renommer en "pasta-scaduta.com" pour afficher le code.



Installer et configurer IIS pour héberger un site web : IIS (Internet Information Services) est le serveur web de Microsoft.

Pour ajouter le rôle : Manage → Add Roles and Features → Web Server IIS à Install

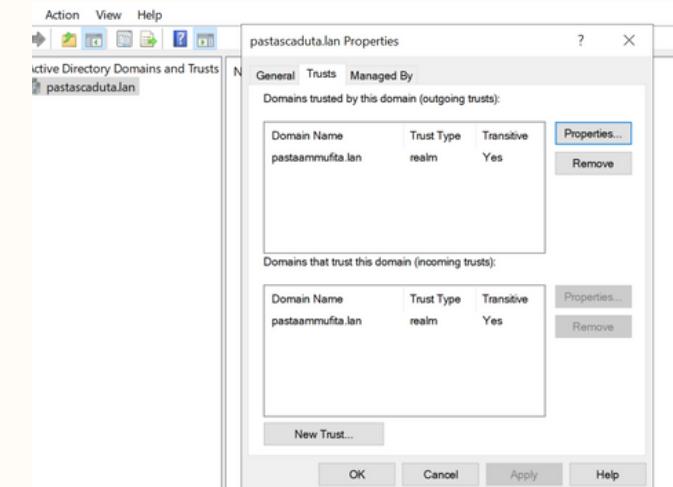
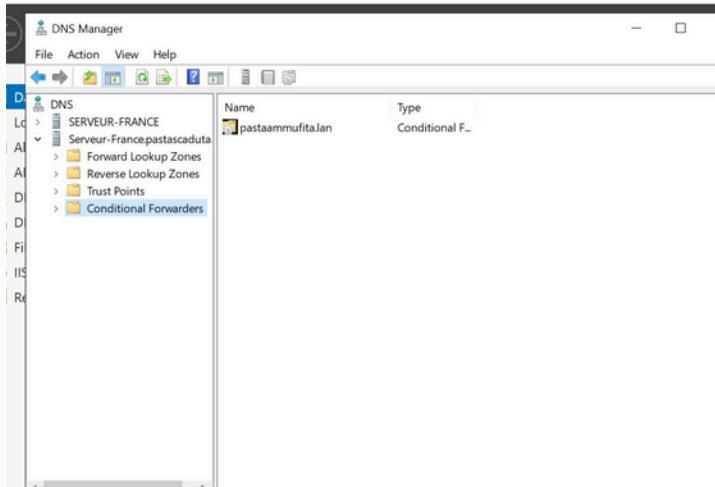


III / CONFIGURATION DE L'INFRASTRUCTURE

CONFIGURATION DE LA RELATION DE CONFIANCE

PARTENARIAT AVEC PASTA AMMUFFITA

Création de la relation de confiance entre deux domaines : pastascaduta et pastammufita
Dans Active Directory Domains and Trusts, créer une relation bidirectionnelle .



→ Clic droit sur le domaine → "Properties" → onglet "Trusts" → "New Trust..."

- Choisir le type de relation → Sélectionner "Forest Trust" → Choisir "Two-way"
- Entrer le nom du domaine distant → L'assistant vérifie la connectivité et la résolution DNS → S'assurer que le domaine distant est joignable.
- Définir les autorisations d'accès → Choisir si tous les utilisateurs du domaine distant peuvent accéder ou seulement certains groupes.
- Une fois la relation créée, tester avec des partages de fichiers, des accès à des ressources ou des authentifications croisées.

