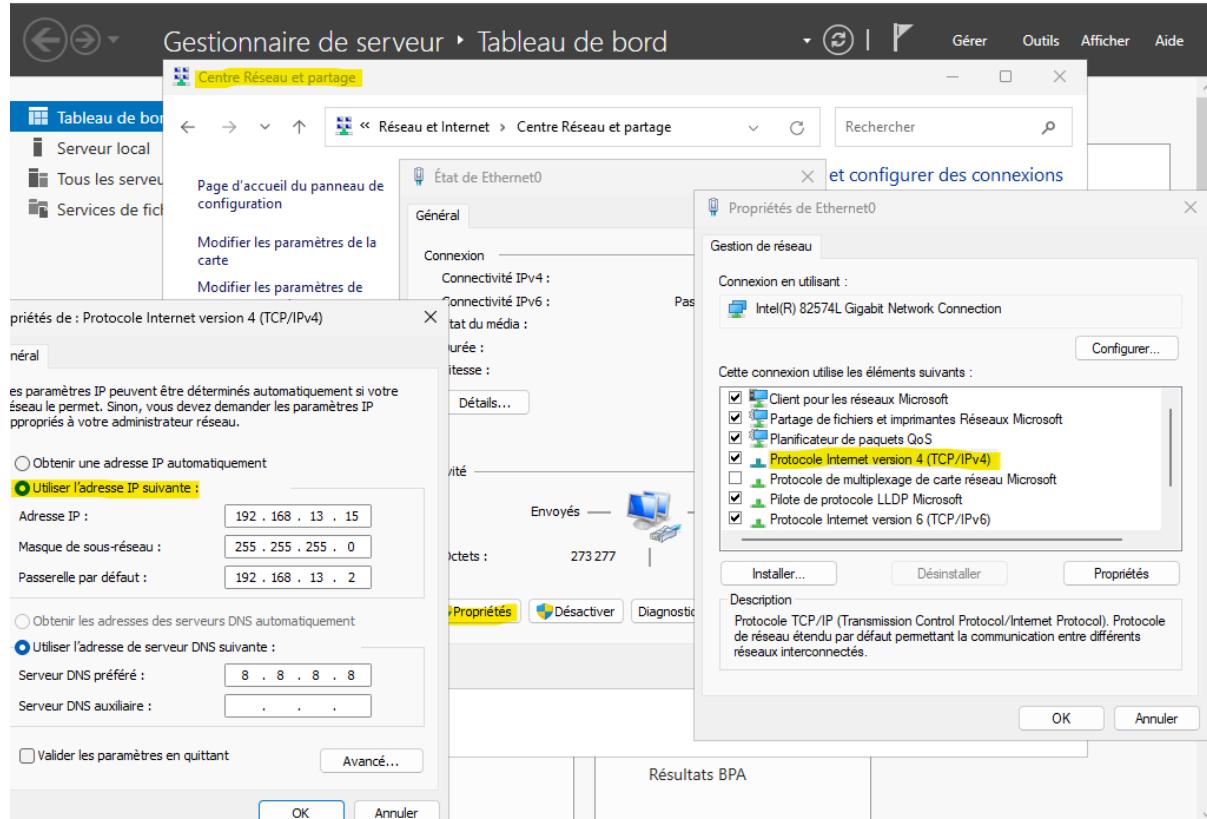


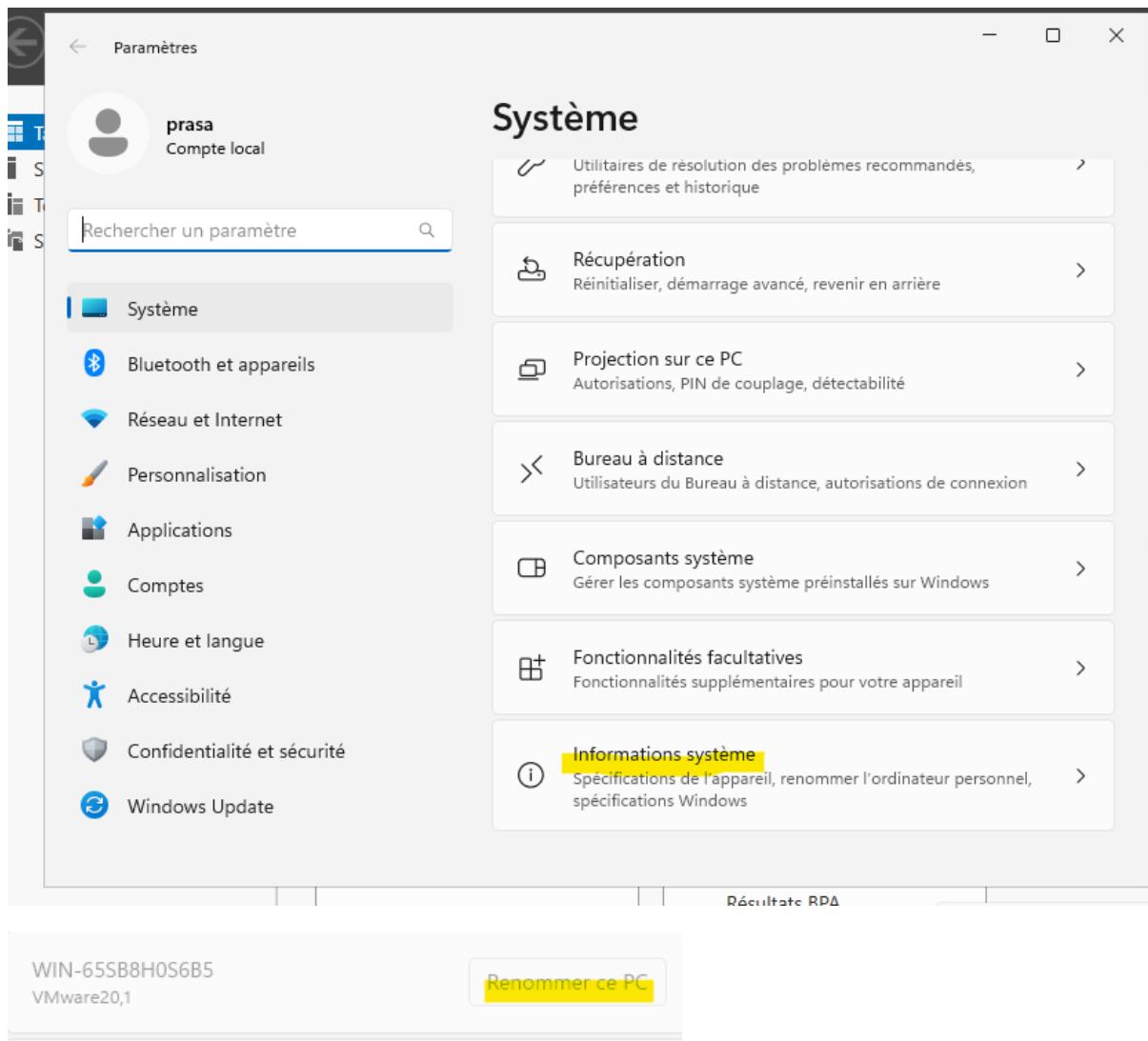
1- Création du site AD

Pour réaliser ce projet, il a fallu commencer par créer un site Active Directory :

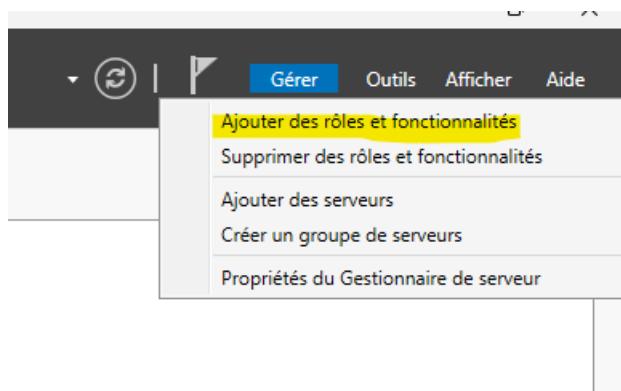
1- Je créer 3 machine virtuelle (pour les 3 sites),

Je renomme le pc et donne un IP statique sur les 3 machines.

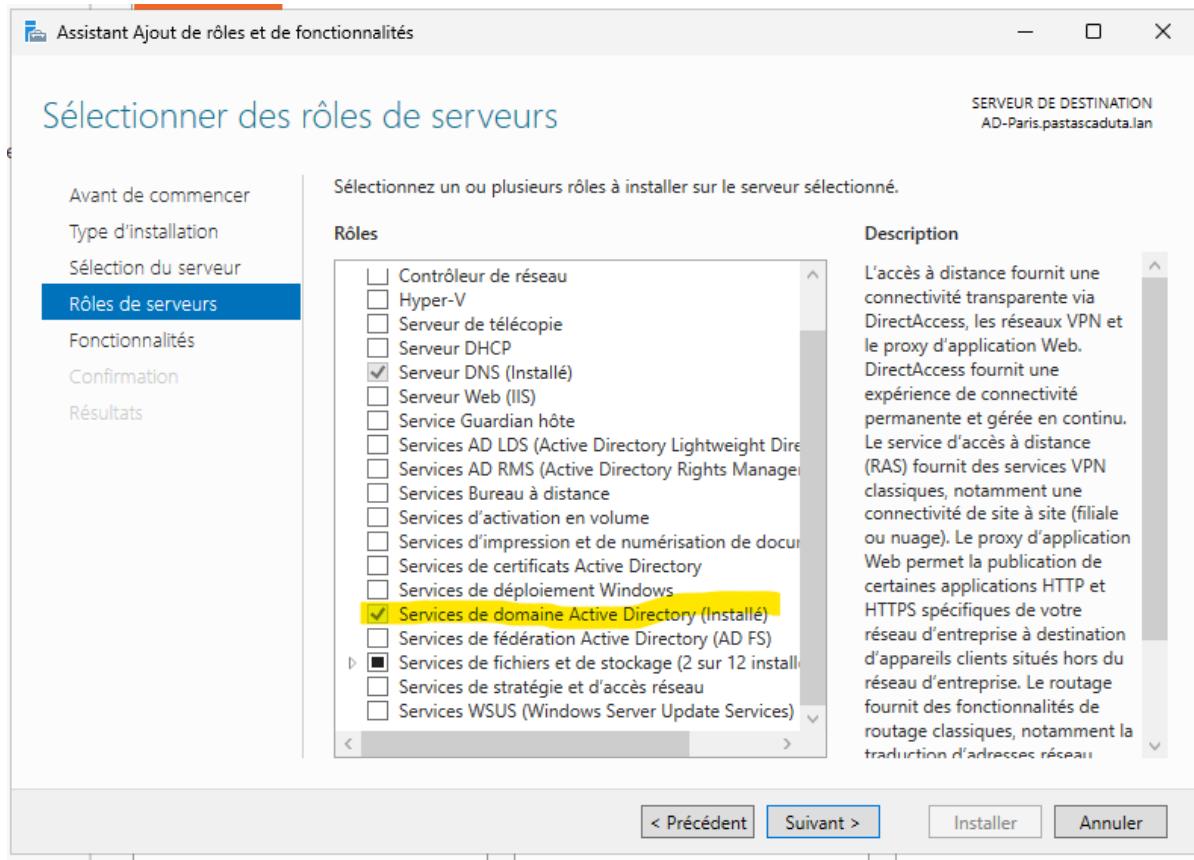




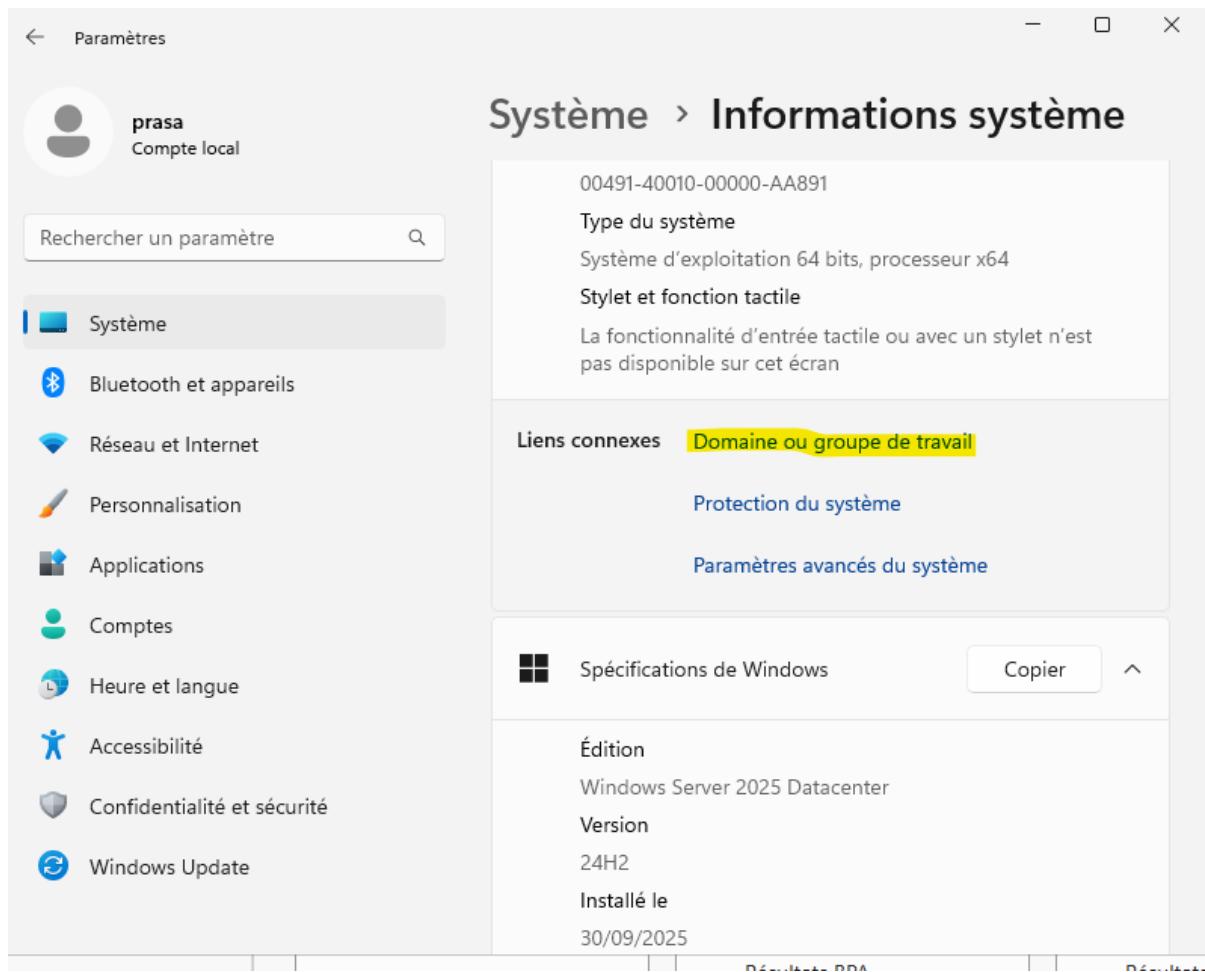
Puis j'installe le AD sur la machine France :



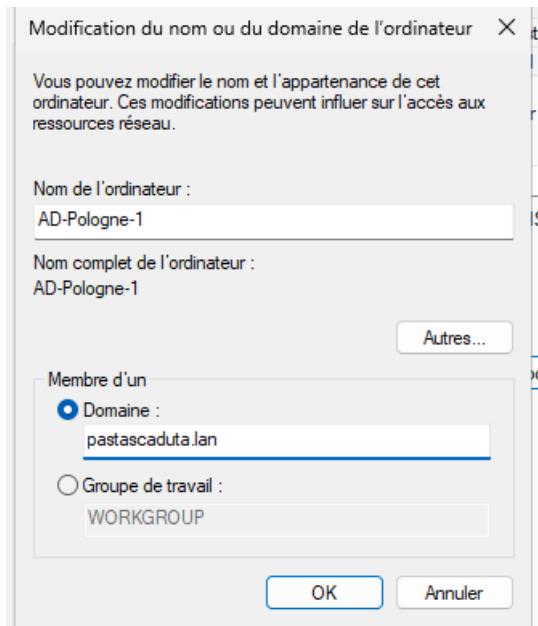
Puis je sélectionne : ‘service Active Directory’



Puis j'ouvre la configuration, ou je coche sur ‘nouvelle foret’, j'entre le nom du domaine : ‘pastascaduta.lan’ puis je le créer. Une fois ceci fait, je fais rejoindre les 2 autres machines sur le domaine.



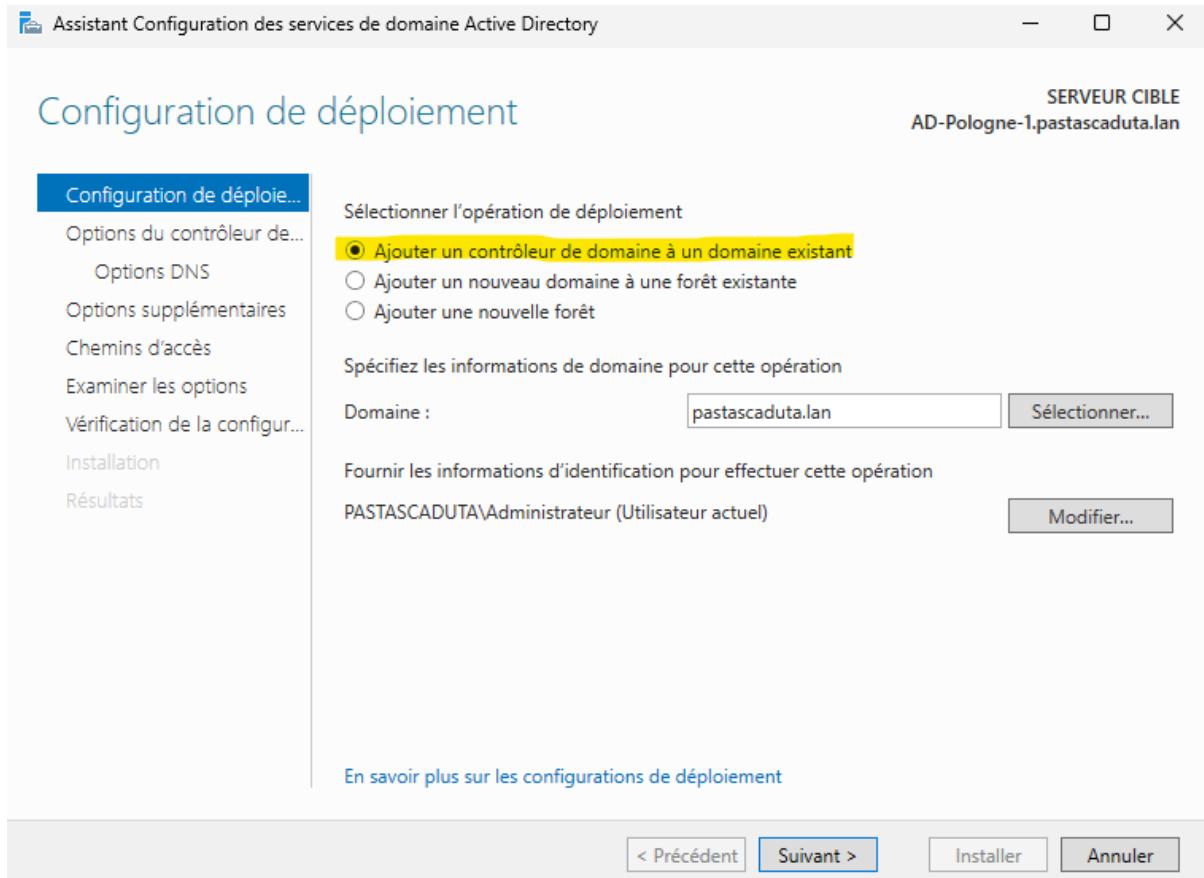
Puis j'entre le nom du domaine.



Les 2 machines ont rejoint le domaine.

Je veux promouvoir le site Pologne en tant que contrôleur de domaine et le site Chine contrôleur RODC.

On installe l'AD sur site Pologne :



Puis, j'installe. Et on observe bien qu'il est contrôleur de domaine :

The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' management console. The left navigation pane shows 'Utilisateurs et ordinateurs Active Directory', 'Requêtes enregistrées', 'pastascaduta.lan' (with 'Computers' and 'Domain Controllers' expanded), and 'ForeignSecurityPrincipal', 'Managed Service Account', and 'Users'. The right pane displays a table of domain controllers:

Nom	Type	Type de contrô... lleur	Site	Description
AD-PARIS	Ordinateur	GC	Default-First-Si...	
AD-POLOGNE-1	Ordinateur	GC	Default-First-Si...	

On veut maintenant que le site Chine soit RODC (pas de droit de modification, seulement lecture).

Comme pour la Pologne on coche sur la case 'ajouter un contrôleur', puis ensuite on coche aussi 'RODC'. Le site Chine est maintenant RODC.

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Nom Type Type de contrô... Site Description

AD-PARIS	Ordinateur	GC	Default-First-S...	
AD-POLOG...	Ordinateur	GC	Default-First-S...	
RODC-CHINE	Ordinateur	Lecture seule, ...	Default-First-S...	

Utilisateurs et ordinateurs Active... > Requêtes enregistrées > pastascaduta.lan > Builtin > Computers > Domain Controllers > ForeignSecurityPrincipal! > Managed Service Accou...

On veut qu'il y ait une réplication des mots de passe sur le rodC :

Propriétés de : Administrateurs

Général Membres Membre de Géré par

Administrateurs

Nom de groupe (antérieur à Windows 2000) : Administrateurs

Description : Les membres du group

Adresse de messagerie :

Étendue du groupe

Local intégré (radio button selected)

group IT

Remarques :

Propriétés de : RODC-CHINE

Général Système d'exploitation Membre de Délégation

Stratégie de réplication de mot de passe LAPS Emplacement Géré par Appel entrant

Ceci est un contrôleur de domaine en lecture seule (RODC). Un contrôleur de domaine en lecture seule stocke les mots de passe des utilisateurs et des ordinateurs selon la stratégie suivante : seuls les mots de passe des comptes figurant dans les groupes d'autorisation, et non dans les groupes de refus, peuvent être répliqués sur le contrôleur de domaine en lecture seule.

Groupes, utilisateurs et ordinateurs :

Nom	Dossier Services de d...	Paramètre
Administrateurs	pastascaduta.lan/Builtin	Refuser
group IT	pastascaduta.lan/use...	Autoriser
Groupe de réplication ...	pastascaduta.lan/Users	Autoriser
Groupe de réplication ...	pastascaduta.lan/Users	Refuser
Opérateurs de compte	pastascaduta.lan/Builtin	Refuser
Opérateurs de sauveg...	pastascaduta.lan/Builtin	Refuser
Opérateurs de serveur	pastascaduta.lan/Builtin	Refuser
user_test	pastascaduta.lan/use...	Autoriser

Avancé... Ajouter... Supprimer OK Annuler Appliquer Aide

Dans le 'site de réplication de mot de passe'. Maintenant on a une réplication des mots de passe sur le serveur Chine.

On va maintenant faire en sorte que les 3 machines soient dans des sites différents :

Sites et services Active Directory

Fichier Action Affichage ?

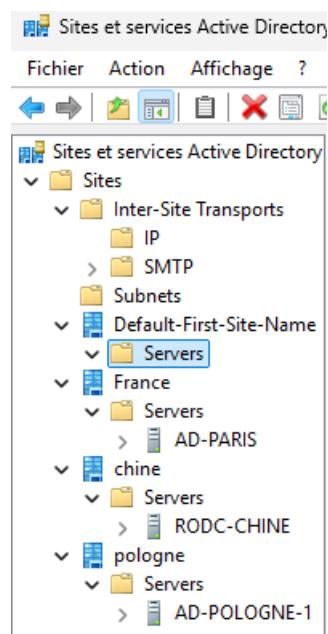
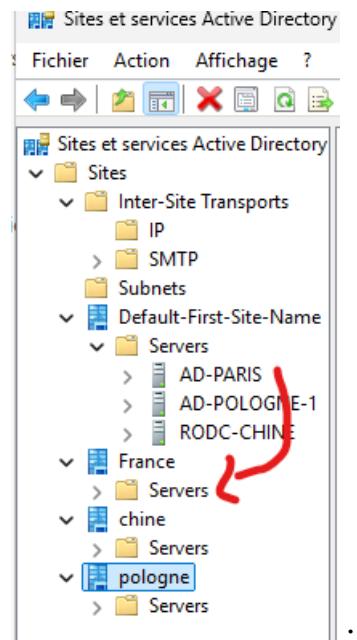
Nom Empl...

Délégation de contrôle...
Nouveau site...
Rechercher...

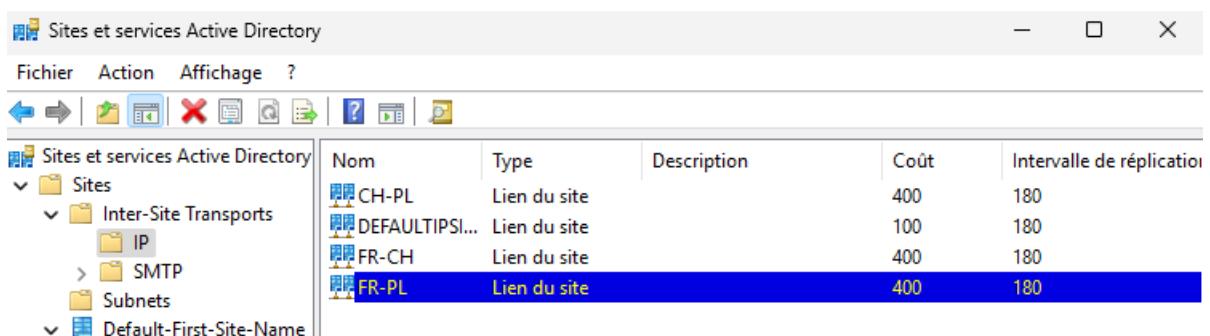
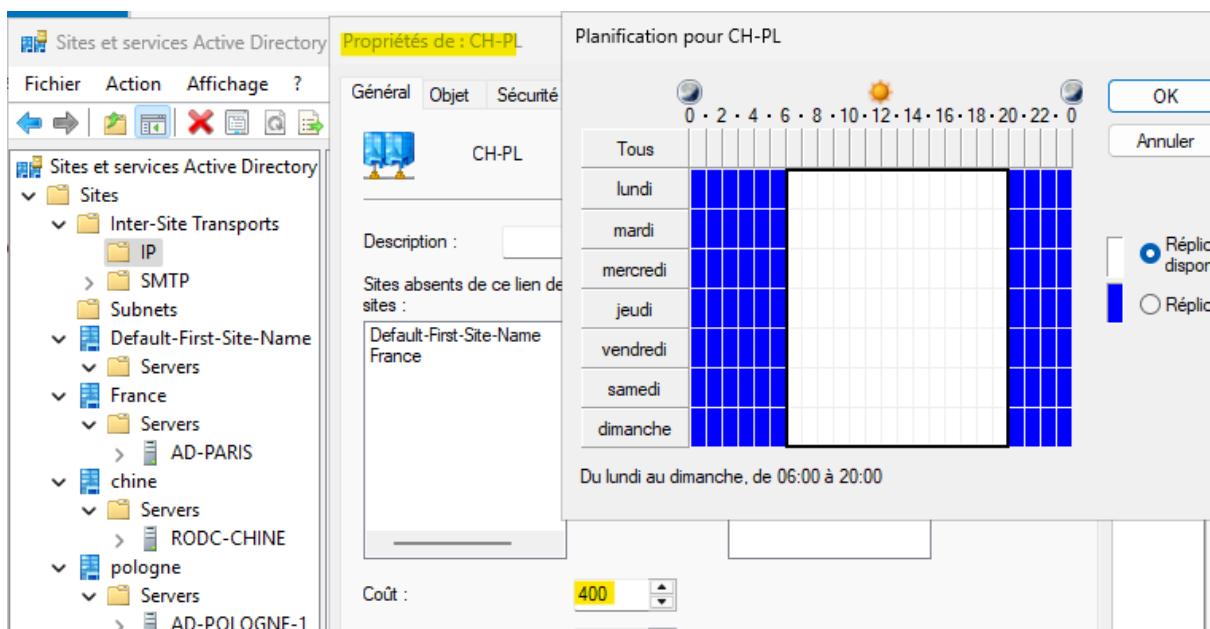
Sites > Nouveau

Un pour la France, un pour la Pologne et l'autre pour la Chine

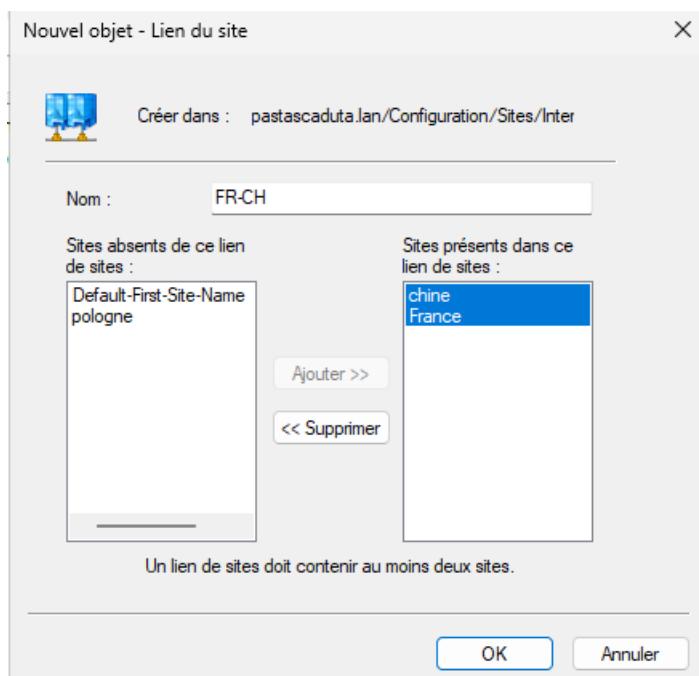
Puis on déplace les sites



On veut maintenant que l'AD tourne de 20h à 6h et qu'il a un cout de 400 :



On va créer des liens entre les sites : Fr-Po, Fr-Ch, Po-Ch



Sites et services Active Directory

Fichier Action Affichage ?

Back Forward Refresh Stop Help

Sites et services Active Directory

- Sites
 - Inter-Site Transports
 - IP
 - SMTP
 - Subnets
 - Default-First-Site-Name
 - Servers
 - France
 - Servers
 - AD-PARIS
 - chine
 - Servers
 - RODC-CHINE
 - pologne
 - Servers
 - AD-POLOGNE-1

Nom	Type	Description	Coût	Intervalle de réplication
CH-PL	Lien du site		100	180
DEFAULTPSI...	Lien du site		100	180
FR-CH	Lien du site		100	180
FR-PL	Lien du site		100	180

Leur cout sont mis à 400 dans le screen d'avant.

On doit appliquer des GPO (Groupe Policies Object) :

On va dans ‘Gestionnaire des stratégies des groupes’ et on peut modifier les GPO. On clique droit sur le domaine ‘pastascaduta.lan’ et ‘créer une nouvelle GPO et la lier’, on leur donnera des noms représentatifs.

J'ai créé 2 dossiers pour différencier les utilisateurs et les utilisateur IT

1er GPO : sur les mots de passe

The screenshot shows the Group Policy Management (GPM) console. On the left, the navigation pane lists various policy categories under 'Stratégies de sécurité'. The 'Stratégie de mot de passe' node is selected. On the right, the main pane displays the 'Stratégie' tab for this policy. It shows several parameters and their current values:

Paramètre de stratégie	Valeur
Assouplir les limites de longueur minimale du mot de passe	Non défini
Audit de la longueur minimale du mot de passe	Non défini
Conserver l'historique des mots de passe	5 mots de passe mémorisés
Durée de vie maximale du mot de passe	30 jours
Durée de vie minimale du mot de passe	0 jours
Enregistrer les mots de passe en utilisant un chiffrement rév...	Non défini
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	8 caractère(s)

Below this, a specific setting for 'Le mot de passe doit respecter des exigences de complexité' is highlighted in yellow. A properties dialog box is open for this setting, showing the value 'Activé' (Enabled) is selected:

Propriétés de : Le mot de passe doit respecter des exigenc...

Paramètre de stratégie de sécurité Expliquer

Le mot de passe doit respecter des exigences de complexité

Définir ce paramètre de stratégie :

Activé

Désactivé

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Stratégie Default Domain Controllers Policy [AD-PARIS.PASTACADUTA.LAN]

- Configuration ordinateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Stratégie de résolution de noms
 - Scripts (démarrage/arrêt)
 - Paramètres de sécurité
 - Stratégies de comptes
 - Stratégie de mot de passe
 - Stratégie de verrouillage du compte
 - Stratégie Kerberos
 - Stratégies locales
 - Journal des événements
 - Groupes restreints
 - Services système
 - Registre
 - Système de fichiers

Stratégie

Stratégie	Paramètre
Assouplir les limites de longueur minimale du mot de passe	Non défini
Audit de la longueur minimale du mot de passe	Non défini
Conserver l'historique des mots de passe	Non défini
Durée de vie maximale du mot de passe	Non défini
Durée de vie minimale du mot de passe	Non défini
Enregistrer les mots de passe	
Le mot de passe doit respecter les règles	
Longueur minimale du mot de passe	Propriétés de : Longueur minimale du mot de passe

Paramètre de stratégie de sécurité Expliquer

Longueur minimale du mot de passe

Définir ce paramètre de stratégie

Le mot de passe doit faire au minimum : 8 caractère(s)

On change adéquatement pour les utilisateurs IT.

2eme GPO : Application : on doit installer l'application '7-zip' et suggérer l'installation de 'notepad++'. Je n'ai pas réussi à trouver de fichier '.msi' pour 'Notepad++'.

Gestion de stratégie de groupe

Fichier Action Affichage Fenêtre ?

Gestion de stratégie de groupe

Forêt : pastacaduta.lan

- Domaines
 - pastacaduta.lan
 - Default Domain Policy
 - installer_7_zip_notepad**
- Domain Controllers

Éditeur de gestion des stratégies de groupe

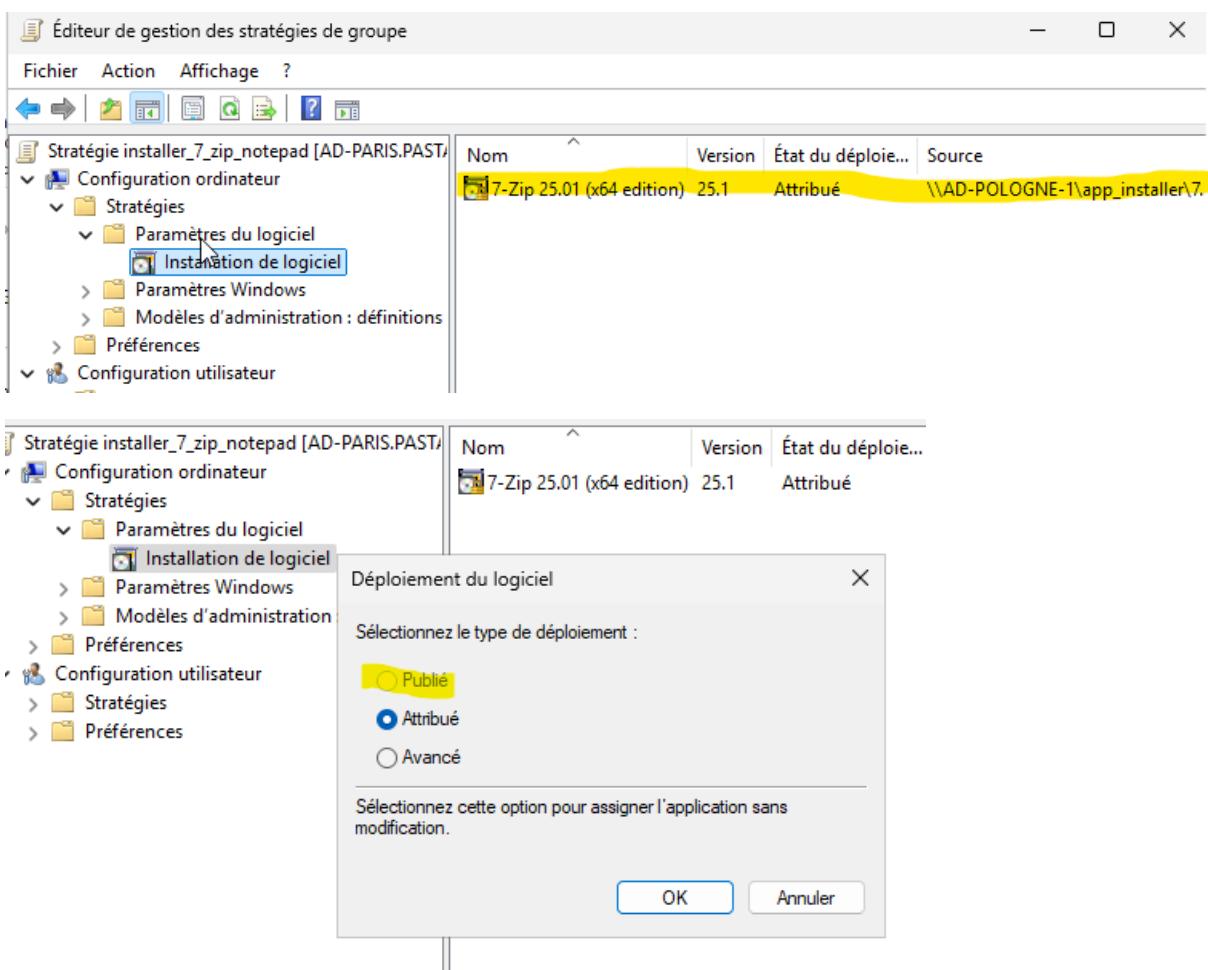
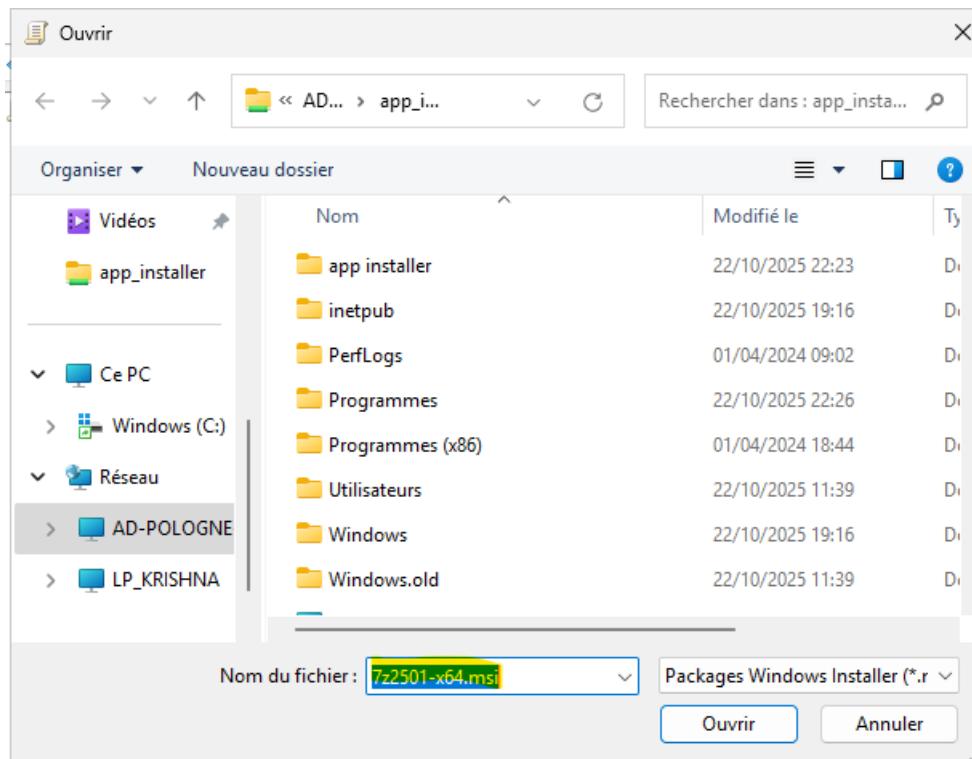
Fichier Action Affichage ?

Stratégie installer_7_zip_notepad [AD-PARIS.PASTACADUTA.LAN]

- Configuration ordinateur
 - Stratégies
 - Paramètres du logiciel
 - Nouveau > Package...

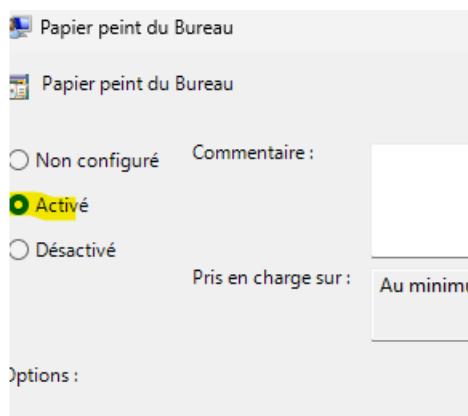
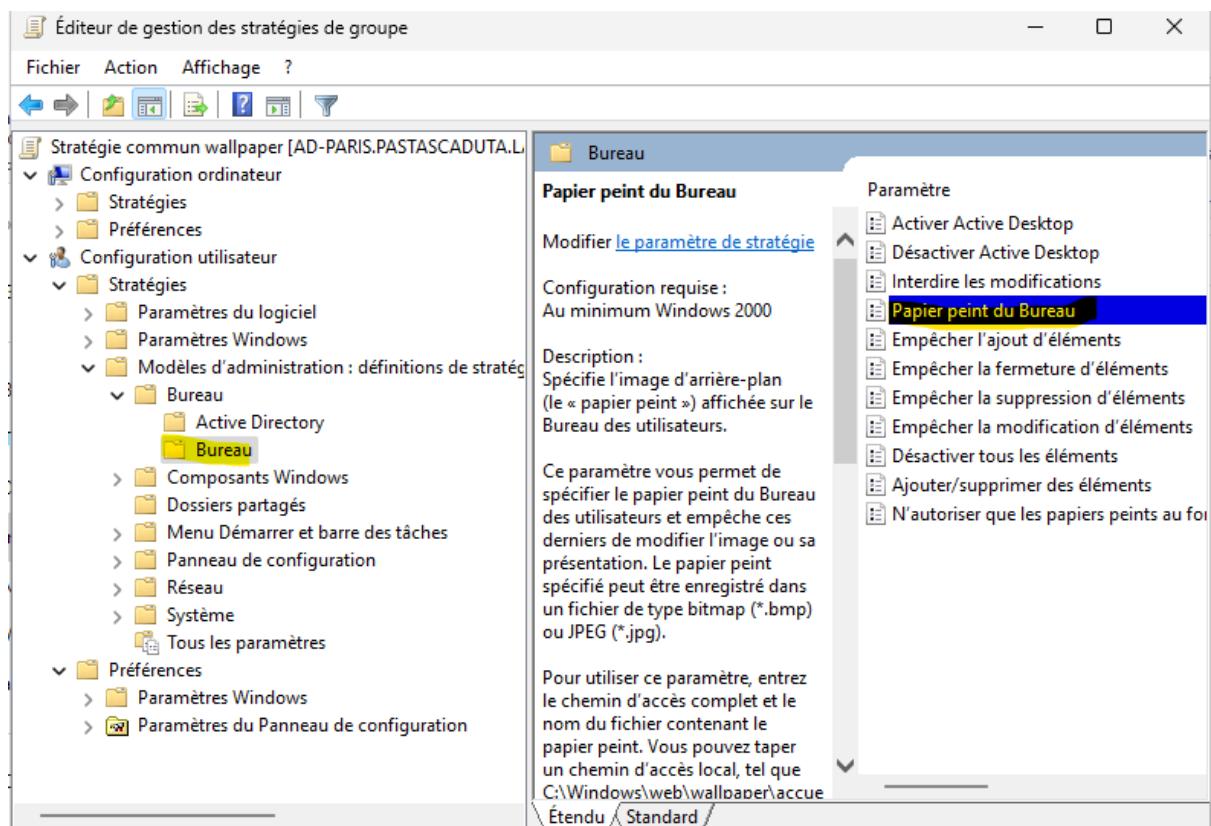
Ouvrir

Organiser Nouveaux filtres Nom



Pour le 'Notepad++' il faudrait cocher le 'Publié'.

Le 3eme GPO qui demande un ‘commun wallpaper’ :



Nom du papier peint :
\\AD-POLOGNE-1\app_installer\wall_pai

Exemple : avec un chemin local :
C:\windows\web\wallpaper\home.jpg

Exemple : avec un chemin UNC :
\\Server\Share\Corp.jpg

Style du papier peint :

La 4eme GPO : qui demande désactiver l'invite de commande sauf pour IT :

The screenshot illustrates the configuration of a Group Policy Object (GPO) named "Stratégie disable command prompt for user". In the left-hand navigation pane, under "Stratégies", the "Système" policy is selected. On the right, the "Système" settings are displayed, showing various options like "Accès au stockage amovible" and "Désactiver l'accès à l'invite de commandes". The latter is highlighted with a yellow box. Below this, the "Gestion de stratégie de groupe" window is open, showing the "Délégation" tab for the "disable command prompt for user" GPO. It lists several security principals, including "group IT (PASTASCADUTA\group IT)", which has the "Appliquer la stratégie de groupe" checkbox checked.

Cela permet de ne pas appliquer ce GPO sur le groupe IT.

5eme GPO : empêcher l'accès à control panel sauf pour it

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Stratégie disable control panel for user [AD]

- Configuration ordinateur
 - Stratégies
 - Préférences
- Configuration utilisateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Modèles d'administration : défin...
 - Bureau
 - Composants Windows
 - Dossiers partagés
 - Menu Démarrer et barre des...
 - Panneau de configuration
 - Réseau
 - Système
 - Tous les paramètres
- Préférences

Panneau de configuration

Sélectionnez un élément pour obtenir une description.

Paramètre	État	Cor
Affichage		
Ajouter ou supprimer des programmes		
Imprimantes		
Options régionales et linguistiques		
Personnalisation		
Programmes		
Masquer les éléments du Panneau de configuration spécifiés	Non configuré	
Toujours afficher tous les éléments du Panneau de config...	Non configuré	
Interdire l'accès au Panneau de configuration et à l'application...	Non configuré	
N'afficher que les éléments du Panneau de configuration sp...	Non configuré	
Visibilité de la page des paramètres	Non configuré	

Gestion de stratégie de groupe

Fichier Action Affichage Fenêtre ?

Forêt : pastascaduta.lan

- Domaines
 - pastascaduta.lan
 - commun wallpaper
 - Default Domain Policy
 - default web home page
 - disable command prompt for user
 - disable control panel for user
 - installer_7_zip_notepad
 - Domain Controllers
 - user_test
 - Objets de stratégie de groupe
 - Filtres WMI
 - Objets GPO Starter
- Sites
- Modélisation de stratégie de groupe
- Résultats de stratégie de groupe

disable control panel for user

Étendue Détails Paramètres Délegation

Ces groupes et utilisateurs ont l'autorisation spécifiée pour cet objet de stratégie de groupe.

Groupes et utilisateurs :

Nom	Autorisations acceptées	Hérité
Administrateurs ...	Modif	Paramètres de sécurité pour disable control panel for user
Admins du dom...	Modif	
ENTERPRISE ...	Lectu	Sécurité
Système	Modif	
Utilisateurs auth...	Lectu	

Noms de groupes ou d'utilisateurs :

- Admins du domaine (PASTASCADUTA\Admins du domaine)
- Administrateurs de l'entreprise (PASTASCADUTA\Administrat...)
- ENTERPRISE DOMAIN CONTROLLERS
- group IT (PASTASCADUTA\group IT)

Ajouter... Supprimer

Autorisations pour group IT

	Autoriser	Refuser
Écrire	<input type="checkbox"/>	<input type="checkbox"/>
Créer tous les objets enfants	<input type="checkbox"/>	<input type="checkbox"/>
Supprimer tous les objets enfants	<input type="checkbox"/>	<input type="checkbox"/>
Appliquer la stratégie de groupe	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autorisations spéciales	<input type="checkbox"/>	<input type="checkbox"/>

Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.

OK Annuler Appliquer

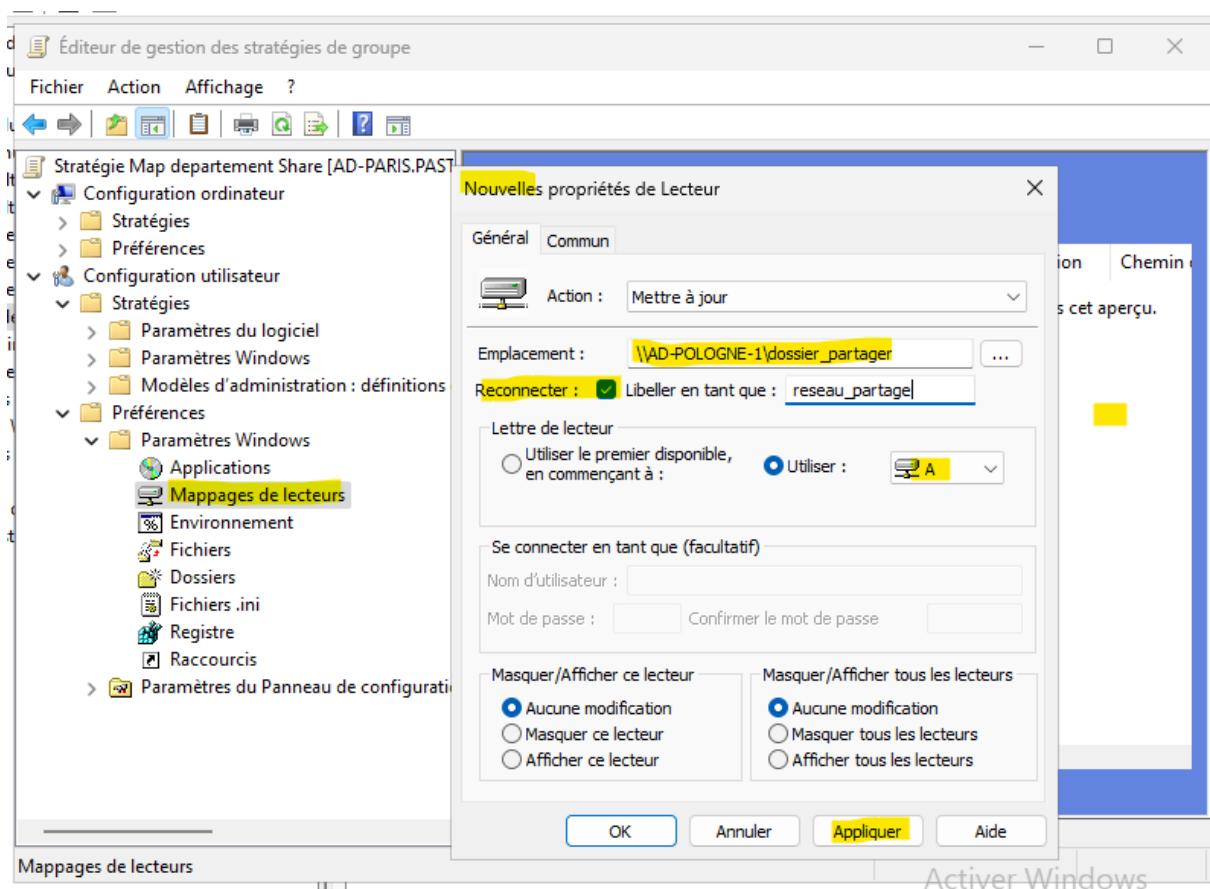
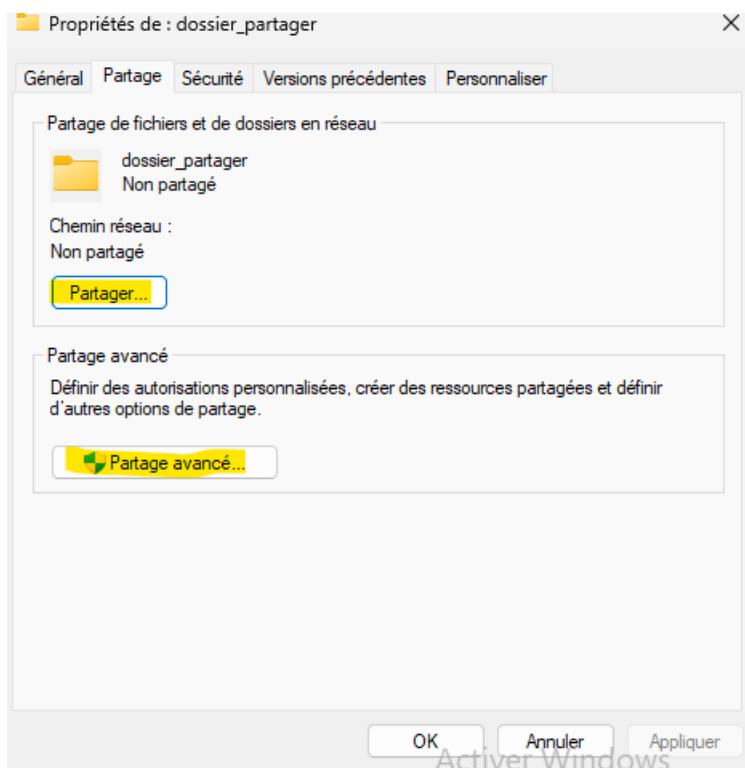
Activer Windows

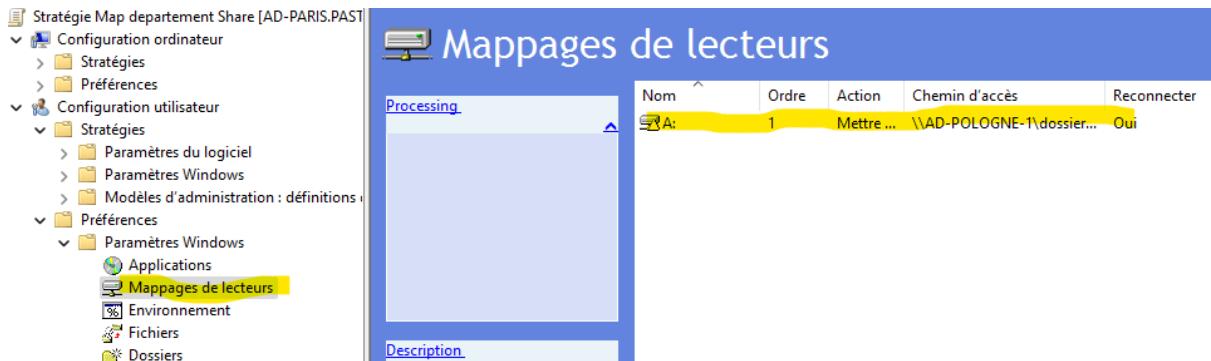
Accédez aux paramètres pour activer Windows.

Haut-parleurs (High Definition Audio Device): 67%

6eme GPO : mappage de réseaux :

Je créer un dossier que je partage





On peut bien voir le mappage de réseaux.

Je vais maintenant présenter les outils que je n'ai pas pu implémenter jusqu'au bout :

1 : Configuration du DNS pour le IIS.

The screenshot shows the 'Gestionnaire DNS' interface. The left pane shows the tree structure with 'DNS' and 'AD-Paris.pastascaduta.lan' selected. The right pane shows a list of objects under 'Nom': Zones de recherche directes, Zones de recherche inversée, Points d'approbation, Rediecteurs conditionnels, Indications de racine, and Rediecteurs. A context menu is open over the 'Rediecteurs' item.

Propriétés de : AD-Paris.pastascaduta.lan

Enregistrement de débogage Enregistrement des événements Analyse Sécurité
Interfaces Redirecteurs Avancé Indications de racine

Sélectionnez les adresses IP qui serviront les requêtes DNS. Le serveur peut écouter les requêtes DNS sur toutes les adresses IP définies pour cet ordinateur, ou vous pouvez le limiter aux adresses IP sélectionnées.

Écouter sur :

Toutes les adresses IP
 Uniquement les adresses IP suivantes :

Adresses IP :

- fe80::3cf2:25f5:c197:a629
- 192.168.13.15
- fe80::27da:98bb:2370:c704
- 192.168.1.15

J'ai 2 cartes réseaux car j'ai essayé de faire la connexion VPN mais échouer.

On ne définit uniquement les ip du site.

Assistant Nouvelle zone

Type de zone

Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

Zone principale
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.

Zone secondaire

Assistant Nouvelle zone

Nom de la zone

Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone : **pastascaduta.lan**

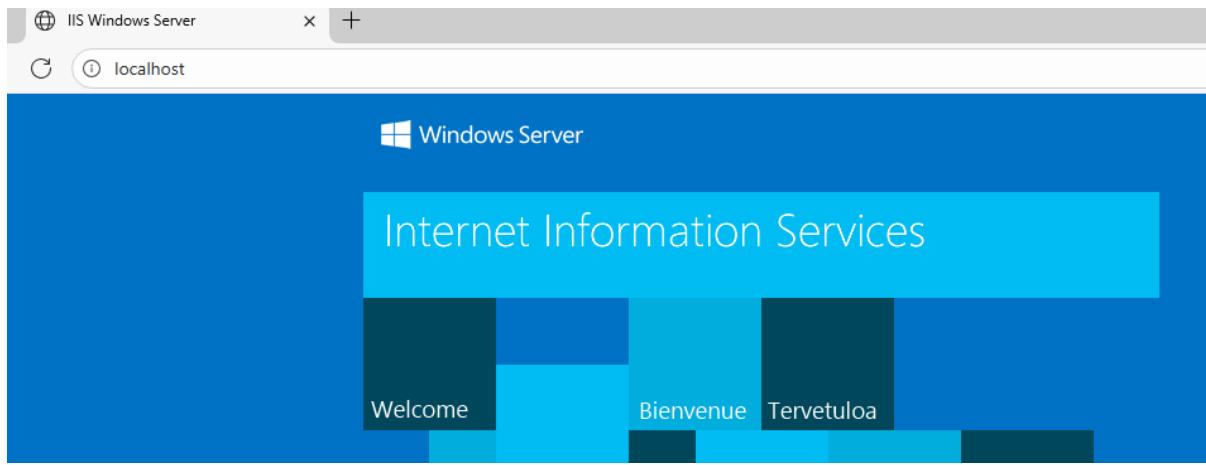
Gestionnaire DNS

Fichier Action Affichage ?

Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[110], ad-paris.pastascadu...	statique
(identique au dossier parent)	Serveur de noms (NS)	ad-paris.pastascadu.lan.	statique
(identique au dossier parent)	Serveur de noms (NS)	ad-pologne-1.pastascadut...	statique
(identique au dossier parent)	Hôte (A)	192.168.1.15	22/10/2025 12:00:00
(identique au dossier parent)	Hôte (A)	192.168.13.15	21/10/2025 23:00:00
(identique au dossier parent)	Hôte (A)	192.168.13.17	22/10/2025 11:00:00
ad-paris	Hôte (A)	192.168.1.15	statique
ad-paris	Hôte (A)	192.168.13.15	statique
AD-Pologne-1	Hôte (A)	192.168.13.17	statique
RODC-Chine	Hôte (A)	192.168.13.19	22/10/2025 12:00:00
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			

Comme on peut le voir on a les 2 hôtes (A) : serveur Paris et serveur Pologne. On retire le 'rodc Chine' du hote A. Comme cela lors d'une demande internet, il sera répondu sur le serveur disponible (serveur Paris ou serveur Chine).

Si on tape 'localhost', on tombe bien sur le site suivant :



Dans le ‘gestion IIS’ il faut changer pour qu'il affiche : ‘pastascaduta.com’.

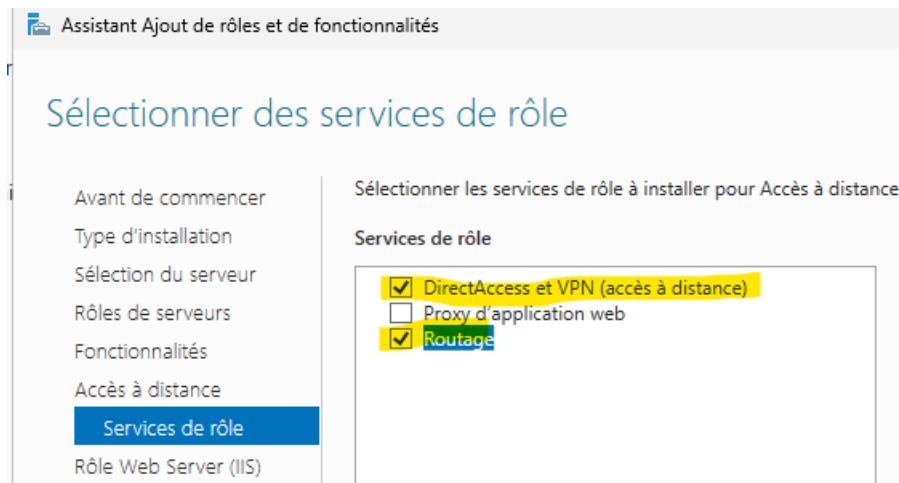
J'ai installer le routeur pour la connexion VPN :

Sélectionner des rôles de serveurs

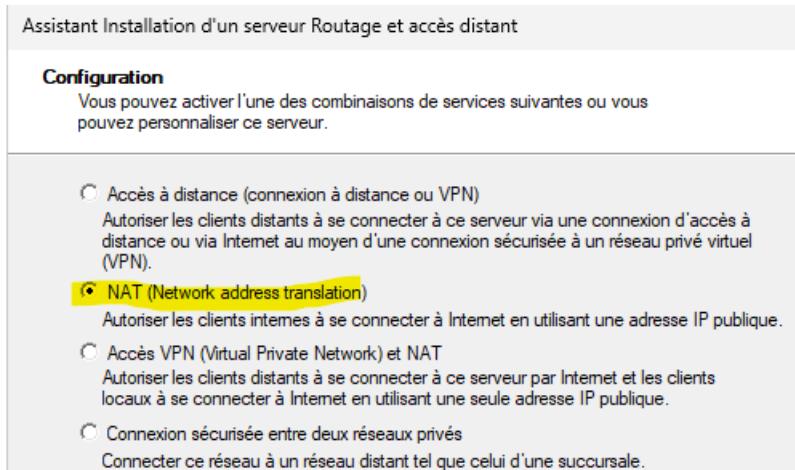
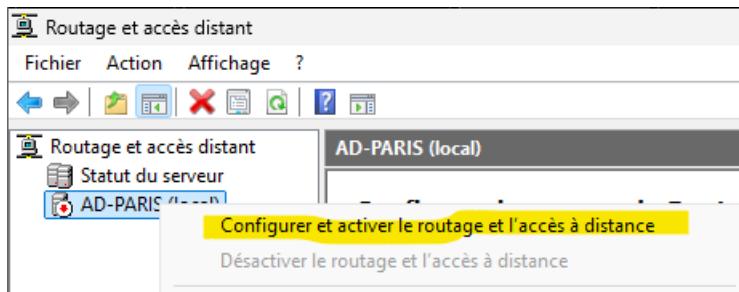
SÉLECTIONNER DES RÔLES DE SERVEURS

SERVEUR DE DESTINATION
AD-Paris.pastascaduta.lan

Rôles	Description
<input checked="" type="checkbox"/> Accès à distance (Installé)	L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la traduction d'adresses réseau.
<input type="checkbox"/> Attestation d'intégrité de l'appareil	
<input type="checkbox"/> Contrôleur de réseau	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Serveur de télécopie	
<input type="checkbox"/> Serveur DHCP	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
<input checked="" type="checkbox"/> Serveur Web (IIS) (10 sur 42 installé(s))	
<input type="checkbox"/> Service Guardian hôte	
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Directory Services)	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Management Services)	
<input type="checkbox"/> Services Bureau à distance	
<input type="checkbox"/> Services d'activation en volume	
<input type="checkbox"/> Services d'impression et de numérisation de document	
<input type="checkbox"/> Services de certificats Active Directory	
<input type="checkbox"/> Services de déploiement Windows	
<input checked="" type="checkbox"/> Services de domaine Active Directory (Installé)	
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (2 sur 12 installé(s))	



Puis j'ai configuré le routage pour mettre en place le VPN :



Cela n'a pas donné le résultat souhaité, j'ai essayé de passer directement par le VPN :

Assistant Installation d'un serveur Routage et accès distant

Configuration

Vous pouvez activer l'une des combinaisons de services suivantes ou vous pouvez personnaliser ce serveur.

Accès à distance (connexion à distance ou VPN)

Autoriser les clients distants à se connecter à ce serveur via une connexion d'accès à distance ou via Internet au moyen d'une connexion sécurisée à un réseau privé virtuel (VPN).

NAT (Network address translation)

Autoriser les clients internes à se connecter à Internet en utilisant une adresse IP publique.

Accès VPN (Virtual Private Network) et NAT

Autoriser les clients distants à se connecter à ce serveur par Internet et les clients locaux à se connecter à Internet en utilisant une seule adresse IP publique.

Connexion sécurisée entre deux réseaux privés

Connecter ce réseau à un réseau distant tel que celui d'une succursale.

Configuration personnalisée

Sélectionner une combinaison de fonctionnalités disponibles dans Routage et accès distant.

Assistant Installation d'un serveur Routage et accès distant

Configuration personnalisée

À la fermeture de l'Assistant, vous pourrez configurer les services sélectionnés dans la console Accès à distance et routage.

Sélectionnez les services que vous voulez activer sur ce serveur.

Accès VPN

Cela a résulté par une erreur. Je n'ai pas pu la résoudre.

J'ai fait le projet tout seul à cause d'un souci avec mon binôme (mon binôme n'a pas donner de nouvelle, j'ai dû le commencer seul). Je n'ai pas eu le temps de pouvoir le finir à temps (beaucoup de charge de travail en plus d'un autre projet qui je devais le faire en binôme mais mon binôme n'a pas donner de nouvelle non plus) je tenais à le préciser.

