Nom : MOSAAD
Prénom : Chehab
Classe : 1A STRI

TP N°2 (2023) :

Gestion des postes :

Objectif : Apprendre à gérer un réseau de postes de manière centralisée.

Compétences :
- Concevoir l'organisation de réseaux de postes.
- Exécuter des commandes PowerShell et en faire des scripts
- Concevoir des stratégies de groupes

Sujet :

Sur votre réseau se trouvent de nombreux postes aux profils différents. Ces postes permettent à chacun d'effectuer son travail. Cependant, ils sont également vecteurs de nombreuses attaques. Il est donc important de les gérer au même titre que les serveurs.

1. Conception du schéma de votre réseau :

L'entreprise possède 3 filiales F1, F2, F3. Chacune de ces filiales possède 2 services : PRODUCT, LOGISTIQUE. Sachant que la DRH est opérée en central et que les filiales ne communiquent pas entre elles, présentez un schéma de l'organisation réseau de vos postes de travail. Tous sont reliés à votre Active Directory central, un serveur VPN en central, à un stockage interne en central et ainsi qu'un stockage local pour la filiale F3.

2. Structure de l'Active Directory :

Proposez une organisation des OUs, des groupes et des comptes dans votre Active Directory. Expliquez les raisons, les points forts et les points faibles de vos choix.

3. Gestion des sites :

Mettez en place la notion de sites AD.
Expliquez l'intérêt, que manque-t-il dans cette architecture.

4. Un peu de PowerShell pour automatiser :

Proposez une nomenclature pour les postes et pour les serveurs faisant apparaitre la filiale d'appartenance.

Ecrire un script PowerShell qui déplace les serveurs dans l'OU serveur et les postes dans l'OU Postes en fonction de leur nom et mettez en place l'exécution de ce script par tâche planifiée.

5. Déploiement de logiciels :

Créez une Stratégie de groupe qui déploie le logiciel 7-Zip au démarrage de l'ordinateur et une autre le publiant dans "obtenir des programmes". Expliquez dans quel cadre chacun peut servir.

6. Déploiement de paramètres :

Créez une GPO qui déploie un raccourci sur le bureau de tous les utilisateurs vers le site de l'université.

Sommaire :

Introduction :

Ce travail a pour objectif d'apprendre à gérer un réseau de postes de manière centralisée, en utilisant les outils et les concepts de l'Active Directory, de la stratégie de groupe et du PowerShell. Il s'agit d'un exercice pratique qui consiste à concevoir et à mettre en œuvre une architecture réseau adaptée aux besoins et aux contraintes d'une entreprise fictive, qui possède trois filiales et deux services par filiale. Le travail se compose de six questions, qui portent sur les aspects suivants :

- La conception du schéma du réseau, en tenant compte des filiales, des services, du serveur VPN, du stockage interne et local, et du serveur Active Directory.
- La structure de l'Active Directory, en proposant une organisation des unités d'organisation (OU), des groupes et des comptes, et en expliquant les raisons, les points forts et les points faibles des choix effectués.
- La gestion des sites AD, en mettant en place la notion de sites, en expliquant son intérêt, et en identifiant ce qui manque dans l'architecture proposée.
- Un peu de PowerShell pour automatiser, en proposant une nomenclature pour les postes et les serveurs, et en écrivant un script PowerShell qui déplace les objets AD dans les OUs correspondantes, et qui s'exécute par tâche planifiée.
- Le déploiement de logiciels, en créant une GPO qui déploie le logiciel 7-Zip en mode attribué au démarrage de l'ordinateur, et une autre qui le publie dans "Obtenir des programmes", et en expliquant dans quel cadre chacune peut servir.
- Le déploiement de paramètres, en créant une GPO qui déploie un raccourci sur le bureau de tous les utilisateurs vers le site de l'université.

Réponse à la question 1 :

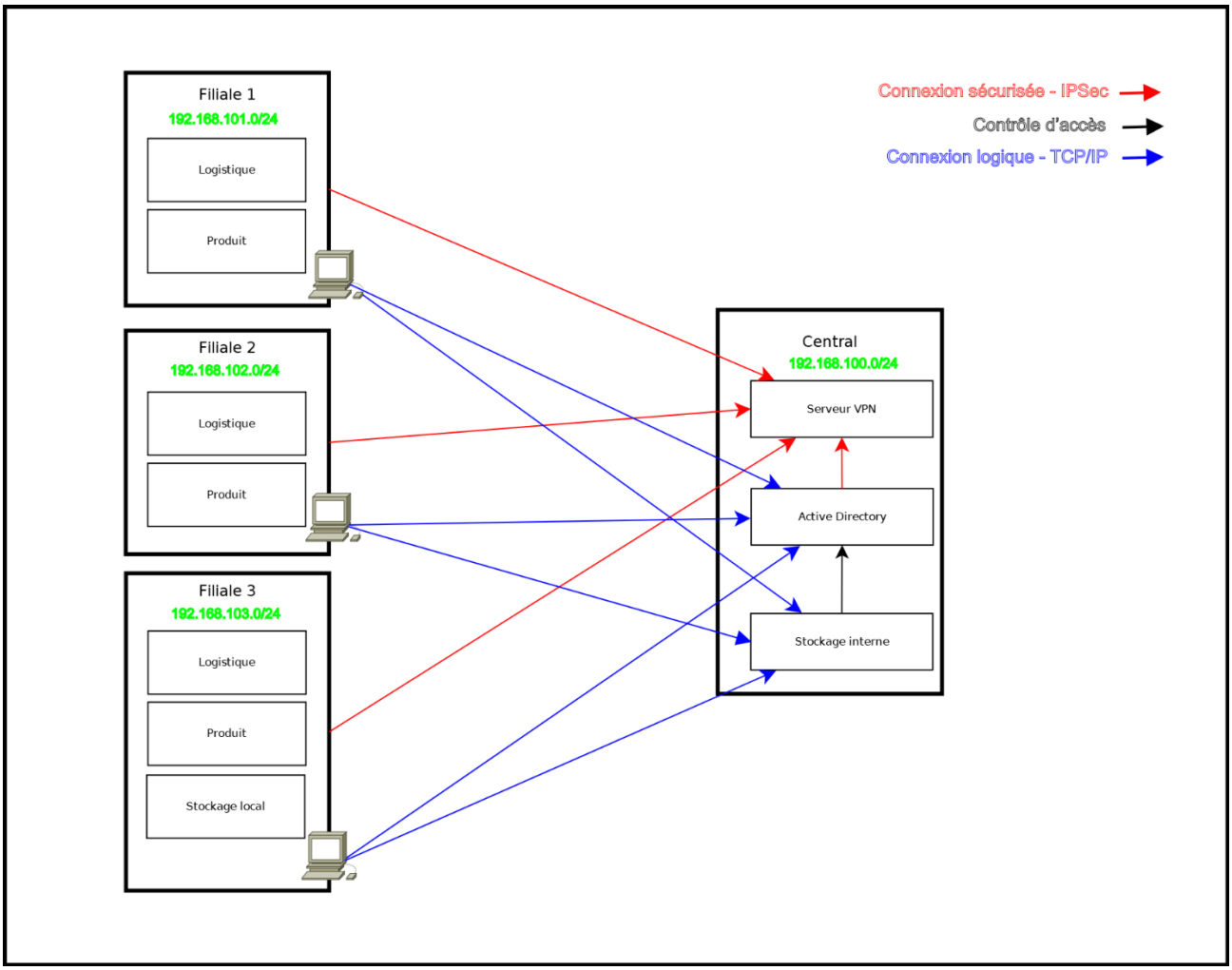

Figure 1 : Schéma du réseau.

Ce schéma montre que :

- Chaque filiale possède un réseau local (LAN) qui regroupe les postes de travail des deux services : PRODUCT et LOGISTIQUE. Ces postes sont configurés avec des stratégies de groupe adaptées à leur fonction et à leur niveau de sécurité.
- Les filiales sont reliées entre elles par un réseau étendu (WAN) sécurisé, qui permet la communication avec le siège central. Ce réseau utilise un protocole VPN (Virtual Private Network) pour chiffrer les données échangées et éviter les interceptions ou les intrusions. Le serveur VPN permet d'établir une connexion sécurisée entre les filiales et le siège central.
- Le siège central héberge le serveur Active Directory, qui gère l'authentification, l'autorisation et la configuration des utilisateurs et des postes de travail sur le réseau. Ce serveur est également responsable de la distribution des mises à jour et des correctifs aux postes de travail.
- Le siège central dispose également d'un stockage interne, qui permet de sauvegarder les données importantes de l'entreprise, comme les fichiers RH ou les documents financiers. Ce stockage est accessible uniquement aux utilisateurs autorisés et protégé par des mesures de sécurité renforcées.
- La filiale F3 possède un stockage local en plus du stockage interne, car elle a des besoins spécifiques en termes de volume ou de rapidité d'accès aux données. Ce stockage local est synchronisé avec le stockage interne pour assurer la cohérence et la fiabilité des données.

Réponse à la question 2 :

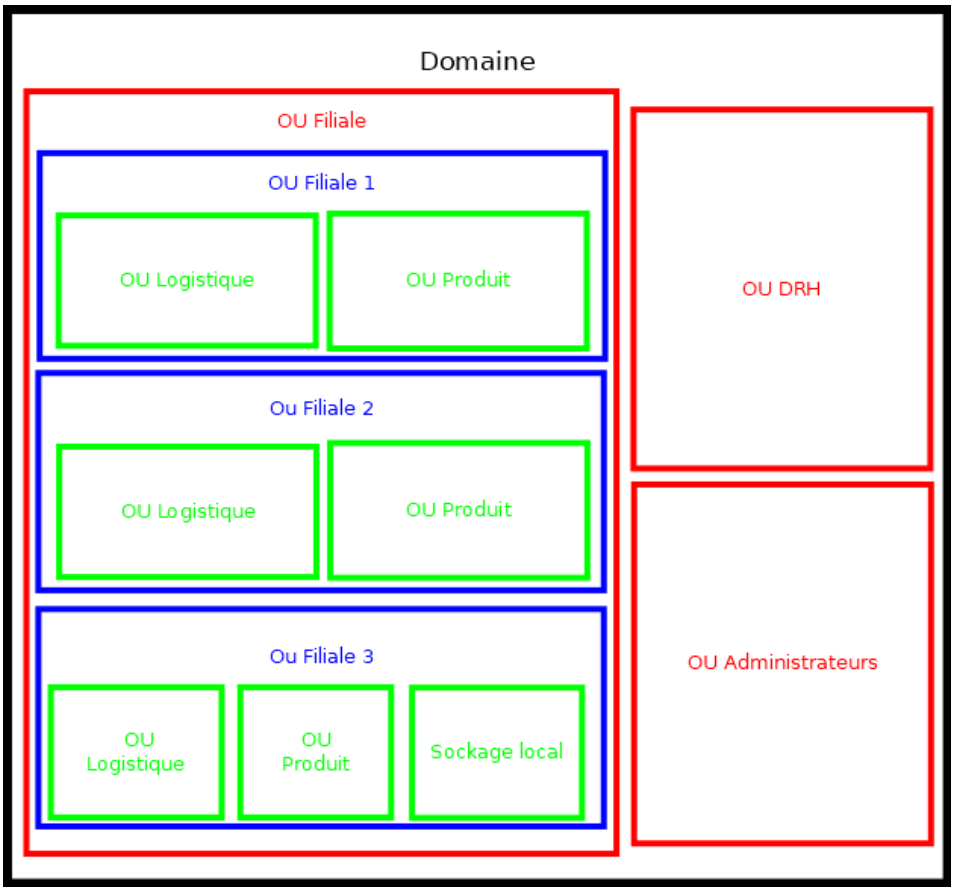

Figure 2 : Schéma décrivant la structure de l'Active Directory.

Ce schéma montre que :

- Nous avons créé une OU Filiale dans laquelle il se trouve une OU pour chaque filiale (F1, F2, F3), une OU pour la DRH et une OU pour les administrateurs, qui est opérée en central. Ces OUs sont directement sous le domaine et permettent de déléguer l'administration aux responsables de chaque filiale et de la DRH.
- Nous avons créé une OU pour chaque service (PRODUCT, LOGISTIQUE) sous l'OU de la filiale correspondante. Ces OUs permettent de regrouper les comptes d'utilisateurs, de groupes et d'ordinateurs selon leur fonction et leur niveau de sécurité. Elles permettent également de lier des stratégies de groupe spécifiques à chaque service.

Les points forts de cette organisation sont :

- La modularité : nous pouvons facilement ajouter ou supprimer des filiales, des services, des groupes ou des comptes sans affecter le reste du réseau. Également, elle respecte la structure hiérarchique de l'entreprise et facilite la gestion des droits et des autorisations.
- La sécurité : nous pouvons contrôler l'accès aux ressources du réseau en fonction du rôle et du service des employés. Également, elle permet d'appliquer le principe du moindre privilège et de limiter les risques d'attaques ou d'erreurs.
- La performance : nous pouvons optimiser la configuration des postes de travail en fonction des besoins spécifiques de chaque service.
- Elle offre une bonne lisibilité et une bonne cohérence du schéma AD.

Les points faibles de cette organisation sont :

- La complexité : il faut gérer un grand nombre d'OUs, de groupes et de comptes, ce qui peut nécessiter des outils d'administration efficaces et une bonne documentation.
- La redondance : il peut y avoir des doublons ou des conflits entre les stratégies de groupe, les droits d'accès ou les scripts PowerShell appliqués aux différents niveaux du réseau.
- La flexibilité : il peut être difficile de modifier l'organisation du réseau en cas de changement de structure ou de stratégie de l'entreprise.

Réponse à la question 3 :

L'intérêt de la notion de sites Active Directory est :

- Optimiser le trafic réseau en limitant les échanges entre les sites et en favorisant les accès locaux.
- Améliorer la disponibilité et la fiabilité des services AD en assurant une répartition de la charge et une tolérance aux pannes.
- Faciliter l'administration et la supervision du réseau en simplifiant la gestion des stratégies de groupe et des objets AD.

Nous avons utilisé PowerShell pour gérer les sites d'Active Directory, en suivant les étapes suivantes :

1. Nous avons créé quatres nouveaux sites, nommés Central, F1, F2 et F3 en utilisant la commande New-ADReplicationSite. Puis nous avons affiché la liste des sites existants en utilisant la commande Get-ADReplicationSite.
2. Nous avons ajouté un sous-réseau à chaque site, en utilisant la commande New-ADReplicationSubnet. Nous avons associé le sous-réseau 192.168.100.0/24 au site Central, le sous-réseau 192.168.101.0/24 au site F1, le sous-réseau 192.168.102.0/24 au site F2 et le sous-réseau 192.168.103.0/24 au site F3. Puis, nous avons affiché les associations entre les sous-réseaux et les sites en utilisant la commande Get-ADReplicationSubnet.
3. Nous avons déplacé le contrôleur de domaine ChehabDomain vers le site Central, en utilisant la commande Move-ADDirectoryServer. Puis, nous avons affiché les contrôleurs de domaine et le site auquel ils sont associés en utilisant la commande Get-ADReplicationSiteLink.
4. Nous avons créé un lien de réplication entre chaque site et le site Central, en utilisant la commande New-ADReplicationSiteLink. Nous avons nommé les liens Central-F1, Central-F2 et Central-F3, et nous avons spécifié la fréquence et le coût de la réplication.
5. Nous avons exécuté la commande nslookup -type=all _ldap._tcp.dc._msdcs.DOM1.local, pour vérifier la résolution des noms des contrôleurs de domaine.
6. Nous avons vérifié à quel site un PC est associé, en utilisant la commande nltest /dsgetsite. Puis, nous avons affiché l'état de la réplication, en utilisant la commande repadmin /showrepl.

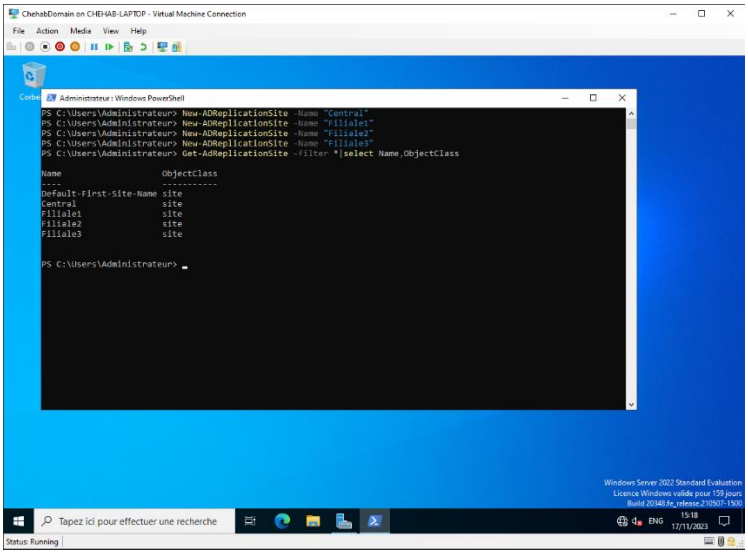

Figure 3 : La création des nouveaux sites et l'affichage de la liste des sites.

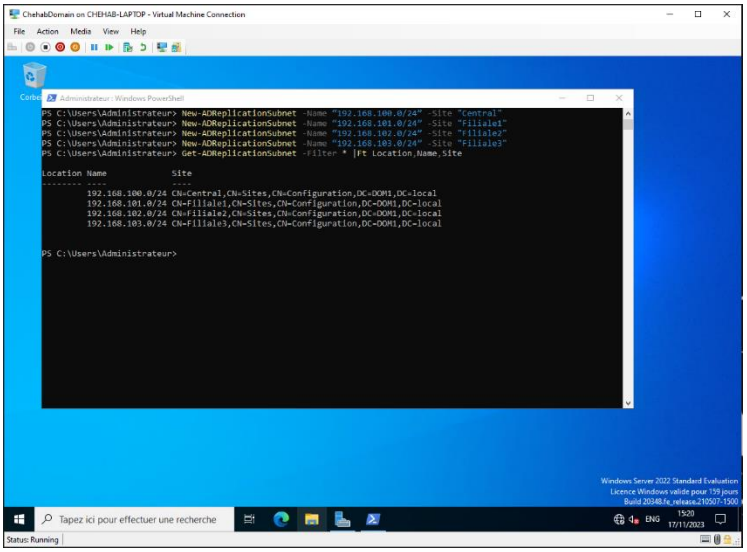

Figure 4 : L'ajout d'un sous-réseau à chaque site et l'affichage des associations sous-réseau et sites.

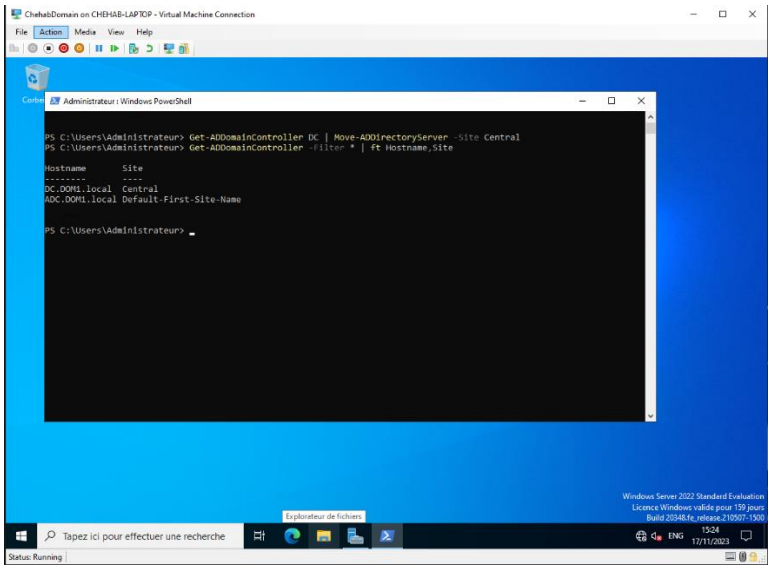

Figure 5 : La déplacement du contrôleur de domaine sur un autre site et l'affichage des contrôleurs de domaine et le site auquel ils sont associés.

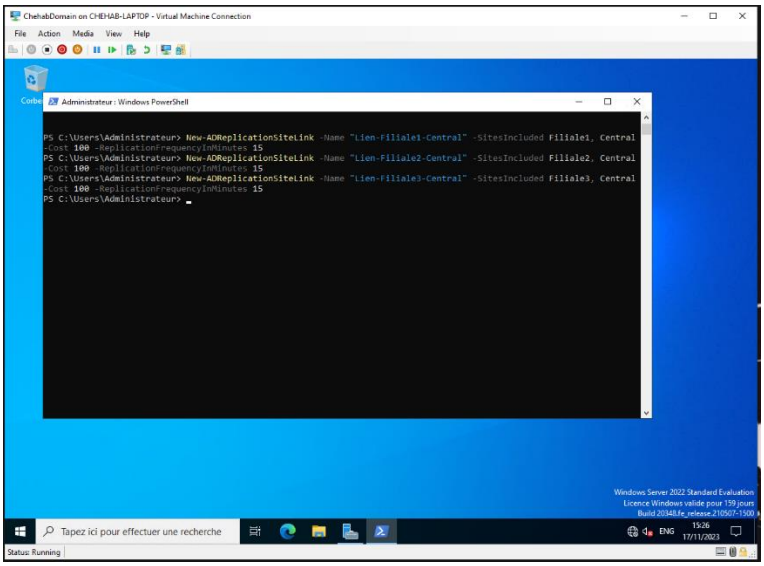

Figure 6 : La création un lien de réplication entre chaque site et le central.

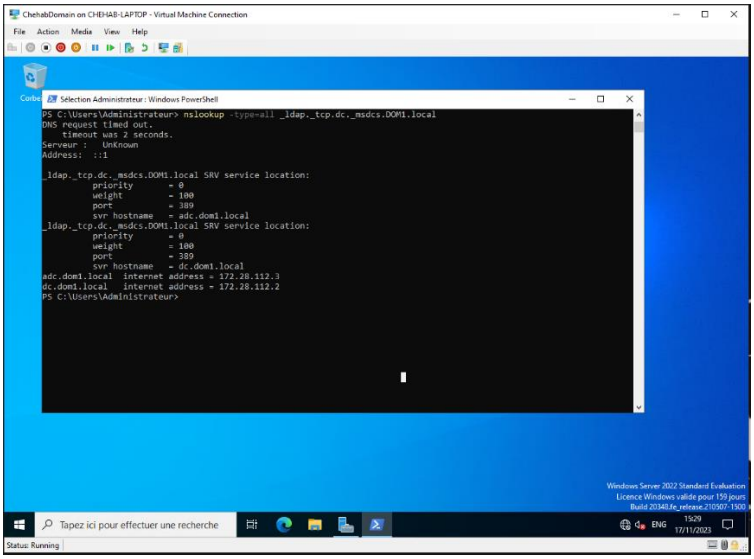

Figure 7 : L'exécution de la commande « nslookup -type=all _ldap._tcp.dc._msdcs.[Domain_Name] ».

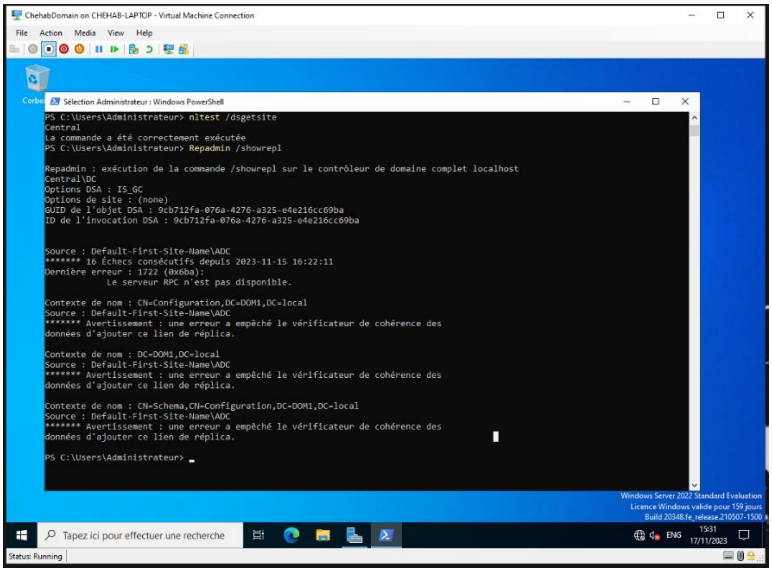

Figure 8 : La vérification à quel site un PC est associé et l'affichage de l'état de réplication avec échec.

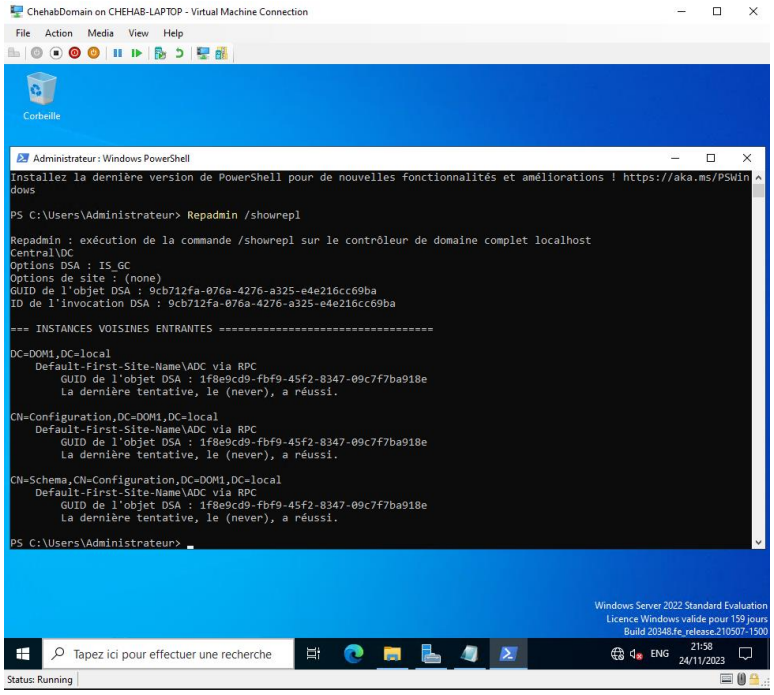

Figure 9 : L'affichage de l'état de réplication avec succès.

Nous avons constaté que la réplication échouait avec le contrôleur de domaine, car la machine virtuelle de redondance n'était pas allumée. Donc nous avons allumé la machine virtuelle de redondance et nous avons répété la commande repadmin /showrepl. Ensuite, nous avons affiché l'état de la réplication avec succès, et nous avons vérifié que les données étaient synchronisées entre les contrôleurs de domaine.

Ce qui manque dans cette architecture est :

- La définition des rôles FSMO (Flexible Single Master Operations) pour chaque site, afin de déterminer quels contrôleurs de domaine sont responsables de certaines opérations critiques sur le domaine ou la forêt.
- La stratégie de maintenance et de mise à jour des contrôleurs de domaine.
- La stratégie de sécurité et de surveillance des accès AD.

Réponse à la question 4 :

Pour la nomenclature des postes et des serveurs, nous proposons d'utiliser le format suivant : [Type]-[Filiale]-[Nom], où [Type] est soit PC pour les postes, soit SRV pour les serveurs, [Filiale] est le nom ou l'abréviation de la filiale d'appartenance, et [Nom] est le nom unique du poste ou du serveur. Par exemple, PC-F1-Compta01 désigne le poste de la comptabilité de la filiale F1, et SRV-Central-DNS01 désigne le serveur DNS du siège central.

Nous avons écrit le script PowerShell en utilisant les commandes du module Active Directory, qui permettent de gérer les objets AD à partir de la console PowerShell. Nous avons suivi les étapes suivantes :

1. Nous avons importé le module Active Directory avec la commande Import-Module ActiveDirectory.
2. Nous avons obtenu la liste des ordinateurs du domaine avec la commande Get-ADComputer -Filter *.
3. Nous avons parcouru la liste des ordinateurs avec une boucle foreach.
4. Pour chaque ordinateur, nous avons extrait le nom de l'ordinateur avec la propriété $Computer.Name.
5. Nous avons testé si l'ordinateur est un serveur ou un poste et selon le résultat du test, nous avons déplacé l'ordinateur dans l'OU correspondante.

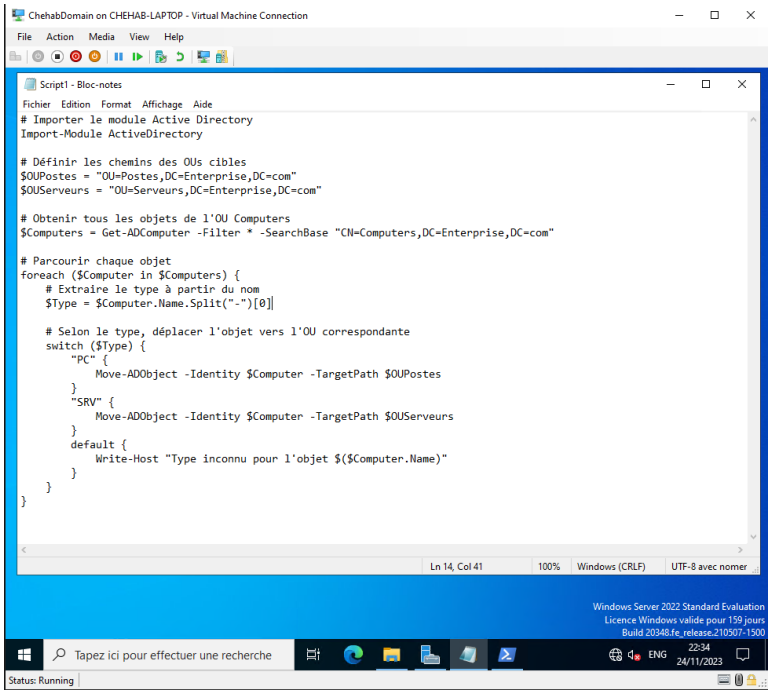

Figure 10 : Le script PowerShell de déplacement.

Puis, pour mettre en place l'exécution de ce script par tâche planifiée, nous avons suivi les étapes suivantes :

1. Nous avons enregistré le script dans un fichier .ps1.
2. Nous avons ouvert le Planificateur de tâches et créé une nouvelle tâche.
3. Nous avons donné un nom et une description à la tâche, et choisi un compte d'utilisateur qui dispose des droits nécessaires pour gérer les objets AD.
4. Dans l'onglet Déclencheurs, nous avons choisi la fréquence et l'heure d'exécution de la tâche.
5. Dans l'onglet Actions, nous avons choisi Démarrer un programme comme action, et spécifié les paramètres suivants :
    1. Programme/script : powershell.exe
    2. Ajouter des arguments : -ExecutionPolicy Bypass -File Script1.ps1]
    3. Démarrer dans : [Téléchargement]
    4. Nous avons validé la création de la tâche.

Réponse à la question 5 :

Pour déployer le logiciel 7-Zip à l'aide de la stratégie de groupe, nous pouvons utiliser deux méthodes : l'attribution ou la publication.

- L'attribution consiste à installer le logiciel automatiquement sur les ordinateurs ou les utilisateurs ciblés par la GPO. Le logiciel est installé au démarrage de l'ordinateur ou à l'ouverture de session de l'utilisateur. Cette méthode est utile si nous voulons que le logiciel soit disponible pour tous les utilisateurs d'un ordinateur ou d'un groupe d'ordinateurs, sans qu'ils aient à intervenir.
  L'intérêt de l'attribution est de :
    - Installer automatiquement le logiciel sur tous les ordinateurs ciblés
    - Garantir la conformité et l'uniformité des versions du logiciel
    - Faciliter la maintenance et la mise à jour du logiciel
- La publication consiste à rendre le logiciel disponible dans le panneau de configuration "Obtenir des programmes". L'utilisateur peut alors choisir d'installer le logiciel s'il le souhaite. Cette méthode est

utile si nous voulons offrir aux utilisateurs la possibilité d'installer le logiciel selon leurs besoins, sans leur imposer. Donc l'intérêt de la publication est de :

- Laisser le choix aux utilisateurs d'installer ou non le logiciel
- Réduire la consommation de ressources et de bande passante
- Adapter le logiciel aux besoins spécifiques de chaque utilisateur

Pour déployer le logiciel 7-Zip à l'aide de la stratégie de groupe, nous avons effectué les opérations suivantes :

1. Nous avons téléchargé le fichier d'installation de 7-Zip au format MSI sur le site officiel du logiciel.
2. Nous avons copié le fichier MSI dans un dossier partagé sur le serveur, auquel tous les ordinateurs du domaine ont accès.
3. Nous avons créé une nouvelle GPO nommée "7zip" et nous l'avons liée à l'unité d'organisation (OU) Postes, qui contient les comptes des ordinateurs cibles.
4. Nous avons modifié la GPO et nous sommes rendus dans la section Configuration ordinateur / Stratégies / Paramètres du logiciel / Installation de logiciel.
5. Nous avons fait un clic droit dans l'espace vide et nous avons choisi Nouveau / Package.
6. Nous avons parcouru le dossier partagé et nous avons sélectionné le fichier MSI de 7-Zip. Nous avons cliqué sur Ouvrir.
7. Nous avons choisi le type de déploiement Affecté, qui permet d'installer le logiciel automatiquement sur les ordinateurs au démarrage.

Ainsi, nous avons configuré la GPO pour déployer le logiciel 7-Zip sur les postes de travail de l'OU Postes.

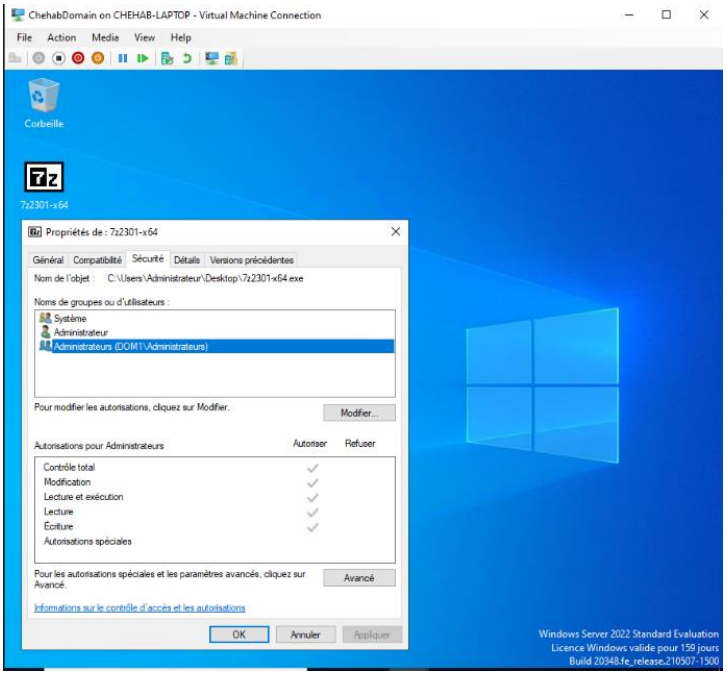

Figure 11 : L'attribution des permissions de partage.

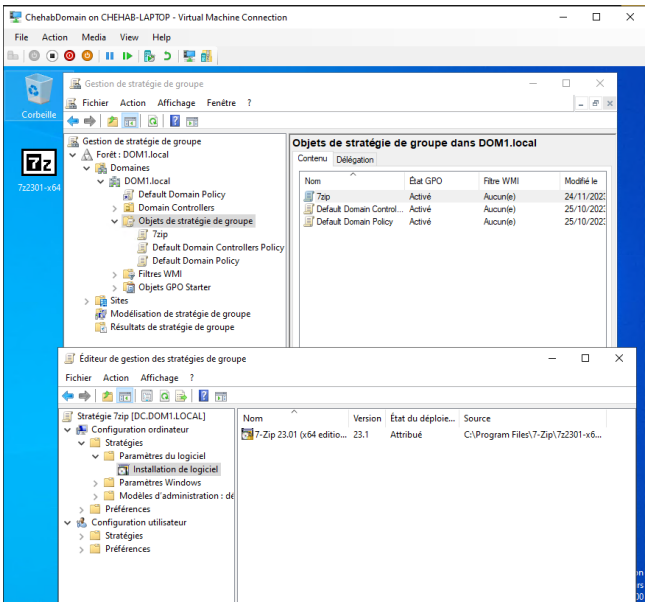

Figure 12 : La mise en place d'une nouvelle GPO et la configurer.

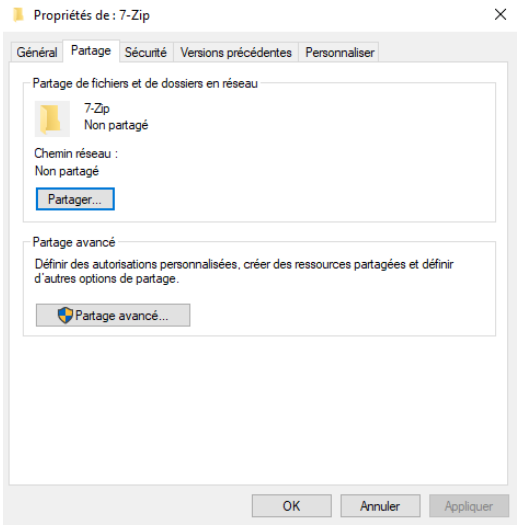

Figure 13 : Le saisie du chemin réseau qui s'affiche l'onglet de partage

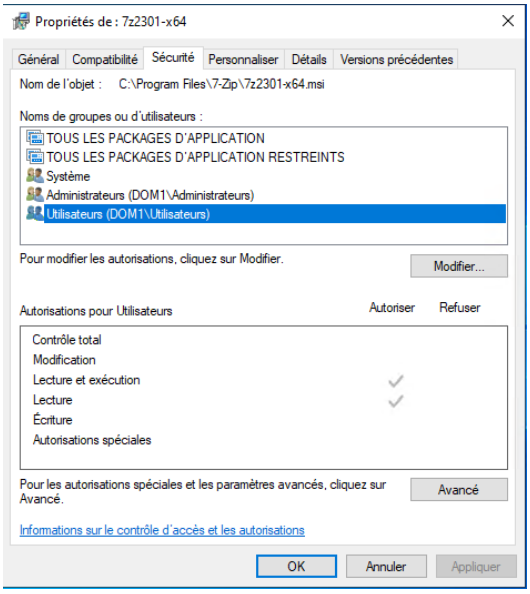

Figure 14 : La mesure d'ajuster les droits d'accès.

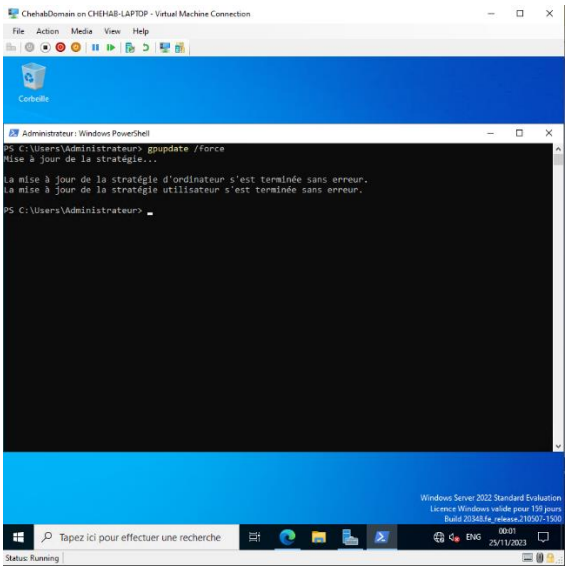

Figure 15 : Nous devons actualiser la stratégie.

Réponse à la question 6 :

Cette stratégie de groupe pour déployer un raccourci sur le bureau de tous les utilisateurs vers le site de l'université peut être utile pour faciliter l'accès à des ressources pédagogiques ou administratives, ou pour renforcer le sentiment d'appartenance à l'établissement. Alors, pour la créer, nous avons suivi les étapes suivantes :

1. Nous avons créé une nouvelle GPO nommée "Déploiement raccourci université" et nous l'avons liée au domaine ou à l'OU qui contient les utilisateurs cibles.
2. Nous avons ouvert la fenêtre de l'éditeur de gestion de stratégie de groupe et nous avons choisi Raccourcis dans l'onglet Paramètres Windows de l'onglet Préférences.
3. Nous avons sélectionné le nom "UPSSITECH" et nous avons inséré l'URL "https://www.upssitech.eu/" pour le raccourci. Nous avons également choisi le type URL, l'emplacement Bureau, et l'icône du site de l'université que nous avons téléchargée sur [ce site] et copiée dans un dossier partagé.
4. Nous avons validé le raccourci et nous avons fermé la fenêtre de l'éditeur.
5. Nous avons exécuté la commande "gpupdate /force" pour mettre à jour la stratégie sur les ordinateurs du domaine ou de l'OU.

Ainsi, nous avons configuré la GPO pour déployer le raccourci vers le site de l'université sur le bureau de tous les utilisateurs.

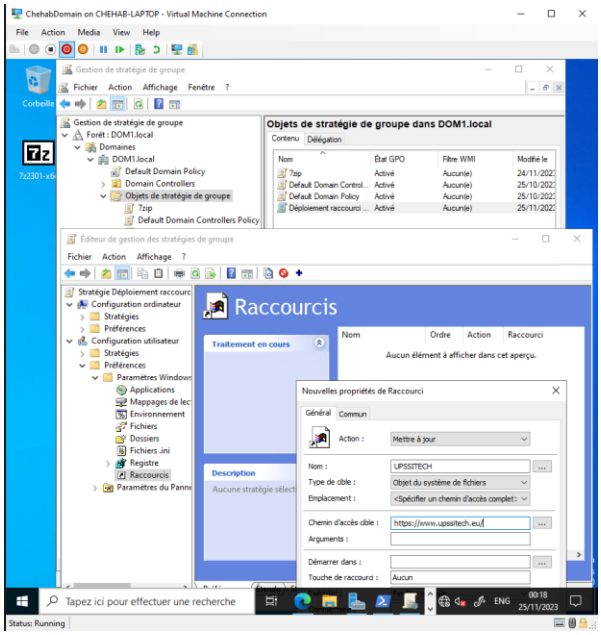

Figure 16 : La mise en place d'une nouvelle GPO raccourcie nommée " Déploiement raccourci université " puis la sélection du nom et l'insertion d'url pour le raccourci.

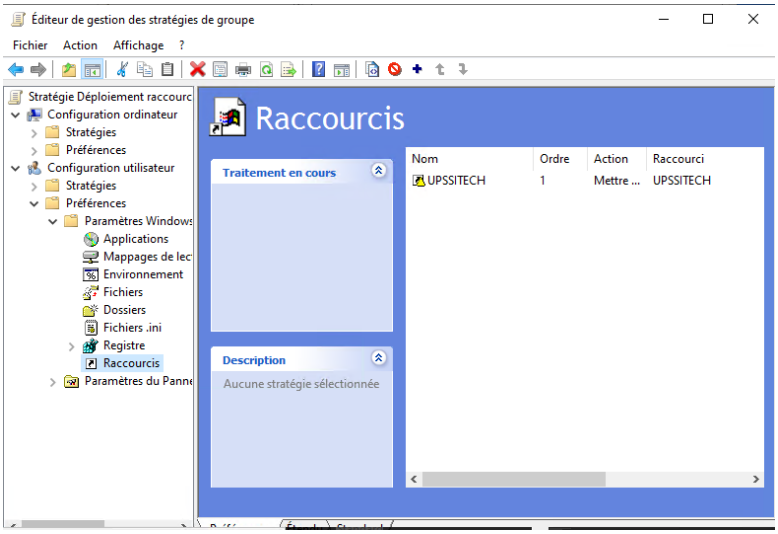

Figure 17 : La nouvelle GPO est correctement mise en place.

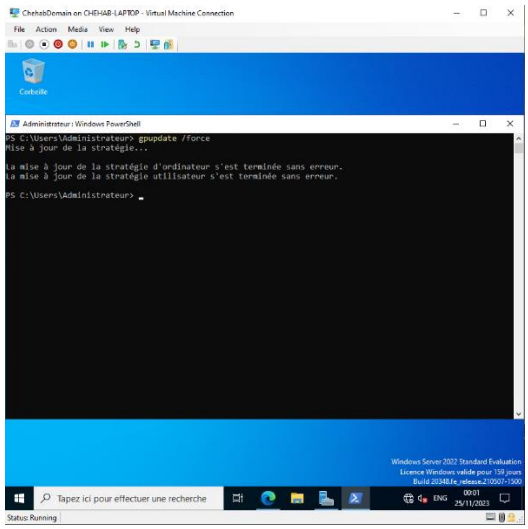

Figure 15 : Nous devons actualiser la stratégie.

Conclusion :

Ce travail nous a permis de réviser et d'approfondir mes connaissances sur la gestion des réseaux de postes, en utilisant les outils et les concepts de l'Active Directory, de la stratégie de groupe et du PowerShell. Nous avons pu appliquer ces notions à un cas concret, en tenant compte des besoins et des contraintes d'une entreprise fictive.

Ce travail nous a également permis de développer notre méthodologie, en suivant les étapes de la conception, de la mise en œuvre, de la vérification et de la documentation de l'architecture réseau. Nous avons appris à utiliser les bonnes pratiques, à respecter les principes de sécurité et de performance, et à justifier mes choix.

Enfin, ce travail nous a permis de faire une auto-critique de notre architecture, en identifiant les points forts et les points faibles, et en proposant des pistes d'amélioration comme : Pour l'architecture réseau, nous pourrions optimiser la répartition des rôles FSMO, la configuration des serveurs DNS, la sécurisation des communications entre les sites, et la gestion des sauvegardes et des restaurations des données.

En conclusion, nous pensons que ce travail a été très enrichissant et intéressant, et que nous pourrions l'utiliser comme base pour d'autres projets similaires ou plus ambitieux.

Bibliographie :

1. Qu’est-ce que la gestion des postes de travail ? : https://www.vmware.com/fr/topics/glossary/content/desktop-management.html
2. Comment gérer les unités d'organisation dans Active Directory : https://serverspace.io/fr/support/help/how-to-manage-ous-in-active-directory/
3. Bonnes pratiques de gestion des groupes Active Directory : https://www.netwrix.fr/active_directory_group_management.html
4. Understanding Active Directory Site Topology : https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-active-directory-site-topology
5. Active Directory sites in a nutshell : https://blogs.manageengine.com/active-directory/2022/07/25/active-directory-sites-in-a-nutshell.html
6. Gérer les OUs et déplacer leurs objets avec PowerShell : https://blog.netwrix.fr/2018/07/25/gerer-les-uos-et-deplacer-leurs-objets-avec-powershell/
7. Exemples de scripts pour l’administration système : https://learn.microsoft.com/fr-fr/powershell/scripting/samples/sample-scripts-for-administration?view=powershell-7.3
8. PowerShell - Lister les objets contenus dans une OU : https://social.technet.microsoft.com/Forums/fr-FR/d95d7b48-63bd-40ba-95c4-41a49a1f9505/powershell-lister-les-objet-contenu-dans-une-ou
9. Saisie de sous-postes : https://help.sap.com/saphelp_me61/helpdata/fr/ea/e9b62c4c7211d189520000e829fbbd/frameset.htm
10. Comment déployer un logiciel au format MSI par GPO ? : https://www.it-connect.fr/comment-deployer-un-logiciel-au-format-msi-par-gpo/
11. GPO - Créer un raccourci sur le bureau de l’utilisateur : https://techexpert.tips/fr/windows-fr/gpo-creer-un-raccourci-sur-le-bureau-de-lutilisateur/
12. GPO : Créer un raccourci sur le bureau pour des utilisateurs de domaine (Préférences) : https://www.youtube.com/watch?v=3nxxZO9_YHY&ab_channel=AbderrahimHILALI