Maxime LE BRAS - Sami BOUKRAB - Kervin BERNARD - Daniel SELVAM
SIO2
Bloc 2 - SISR

Le 18/09/2024

TP2 - Société ALSET

Sommaire

Lot 1 - Mise en place d'un serveur Windows

Schéma réseau de départ (Plan d'adressage du lycée) :

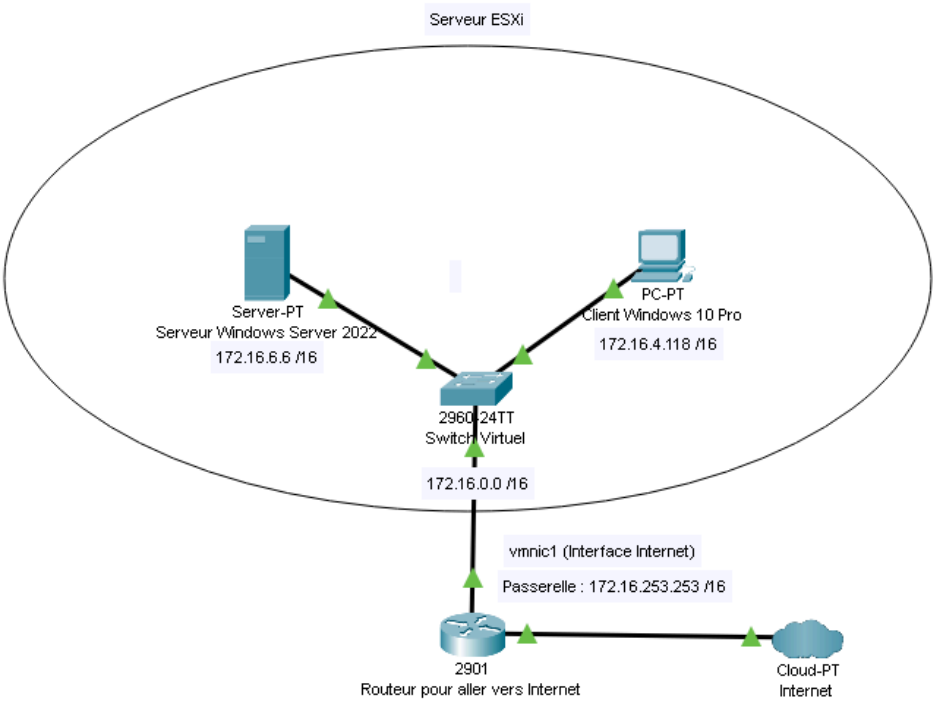
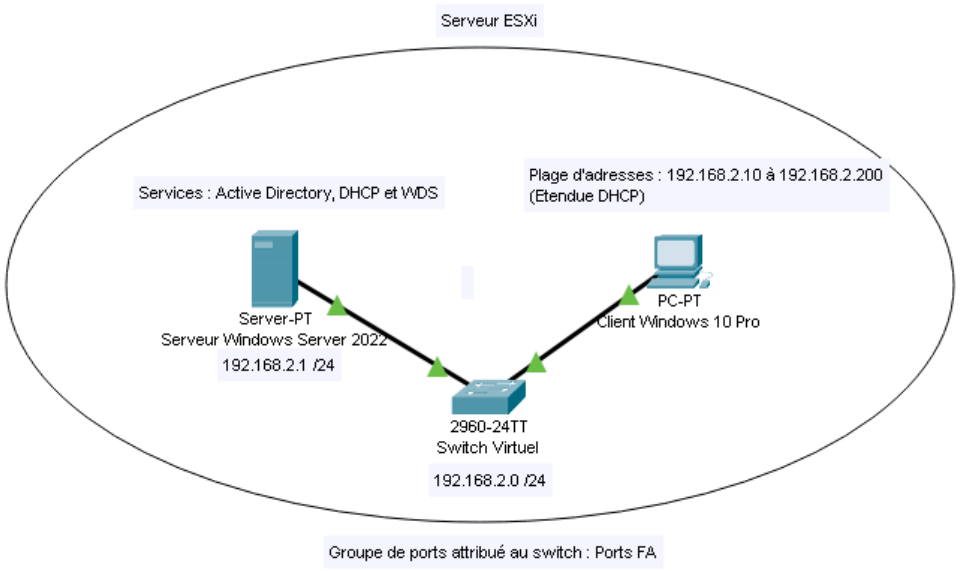


Schéma réseau final (Mise en place du nouveau plan d'adressage réalisé par le groupe) :



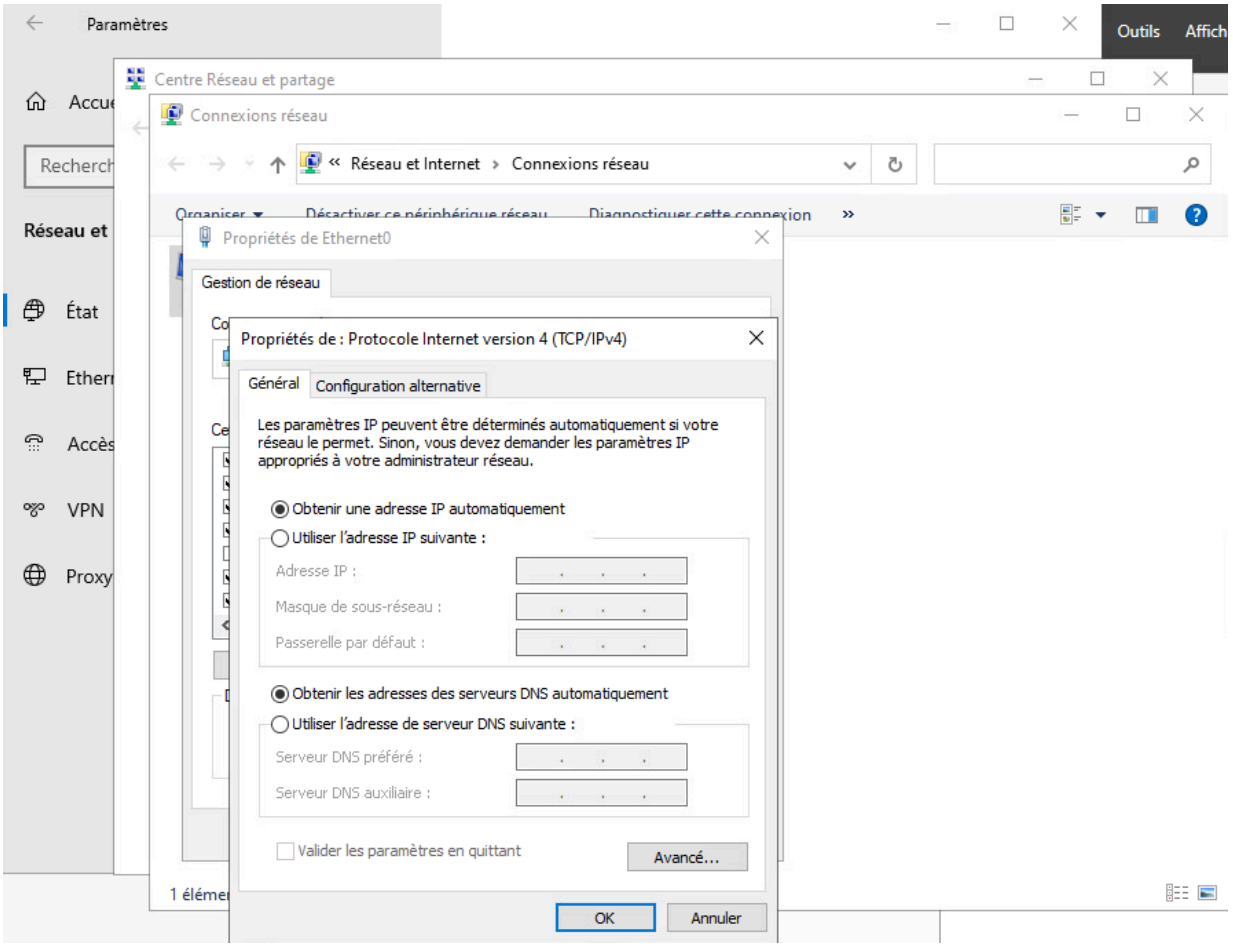
Création de machines virtuelles :

Tout d'abord, nous avons créé des machines virtuelles sur le serveur ESXi. La démarche est la suivante :

1) "Créer / Enregistrer une machine virtuelle".
2) Sélectionner un nom de machine - famille de l'OS - l'OS exact.
3) Sélectionner le dossier "datastore" qui contient les images iso de Debian 9, Debian 12 et Windows 10.
4) Configurer la mémoire RAM, le stockage du SSD, l'adaptateur réseau et sélectionner l'image iso en allant dans le dossier "datastore" puis "iso".
5) Terminer l'installation de la machine.

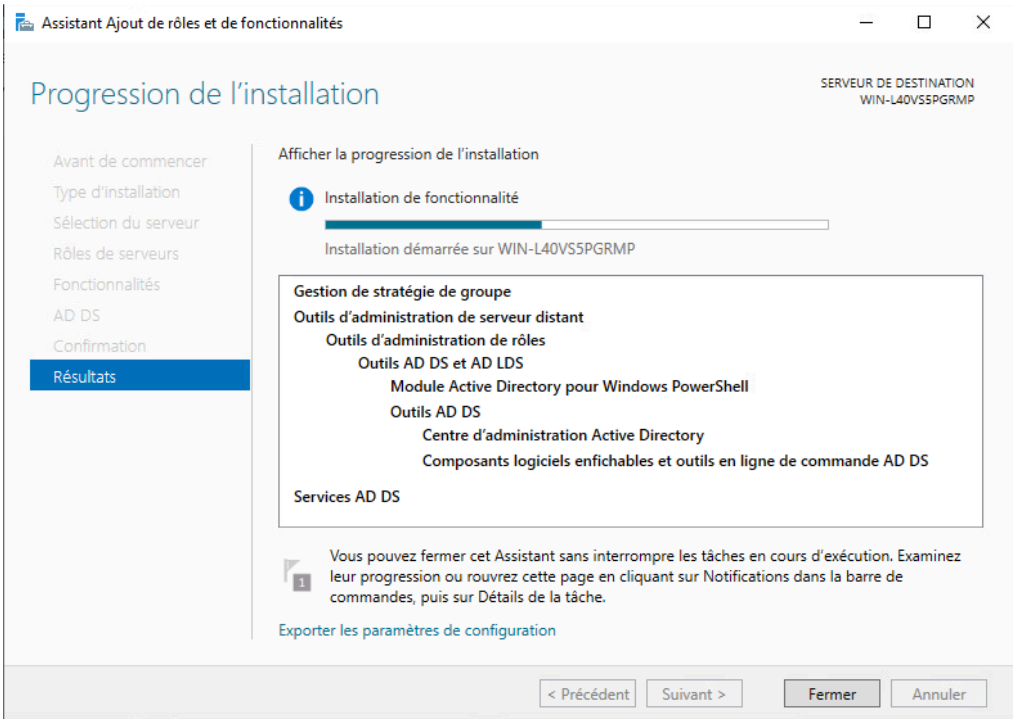
Installation du service Active Directory :

Avant d'installer ce service, il faut mettre en place la configuration IP du serveur Windows Server 2022 :

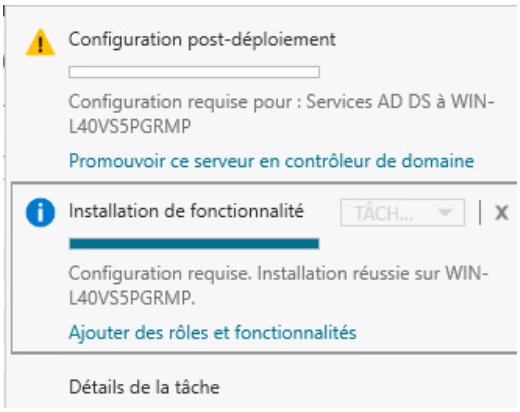


Ici, on a mis l'adresse IP correspondant au schéma réseau qui est 192.168.2.1 /24.

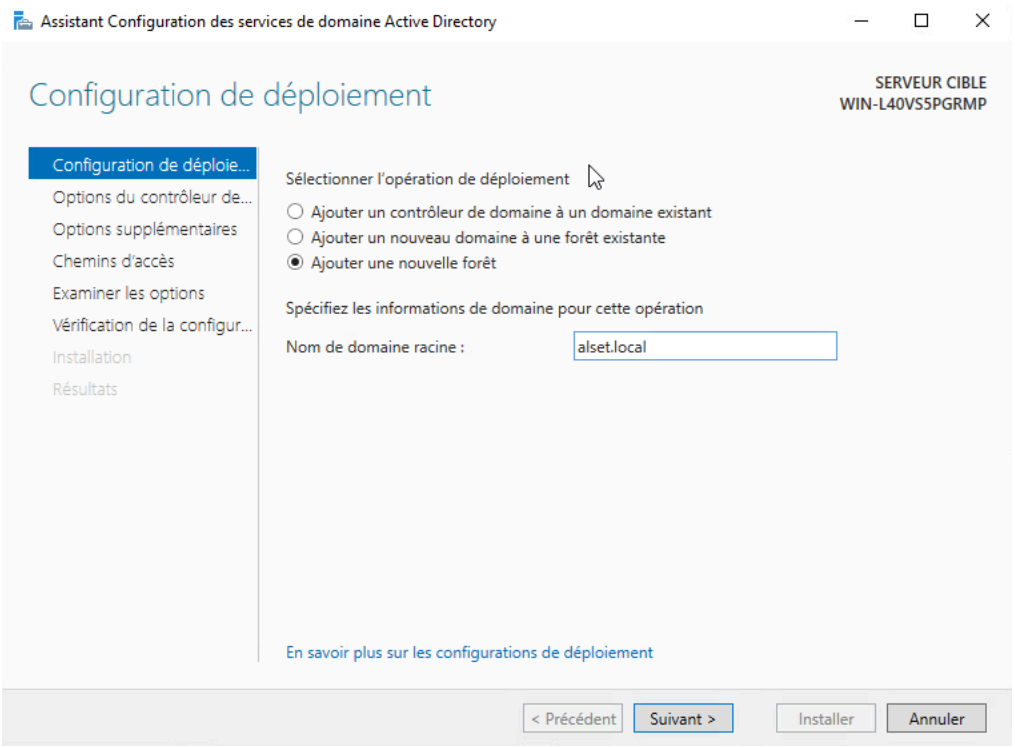
Pour pouvoir installer ce service, il faut aller dans le gestionnaire de serveur, ensuite faire les actions suivantes : “Gérer” > “Ajouter des rôles et fonctionnalités” > “Rôles de serveurs” > “Services AD DS” > “Installer”.



Lorsque l’installation du service est terminée, on doit faire ceci :

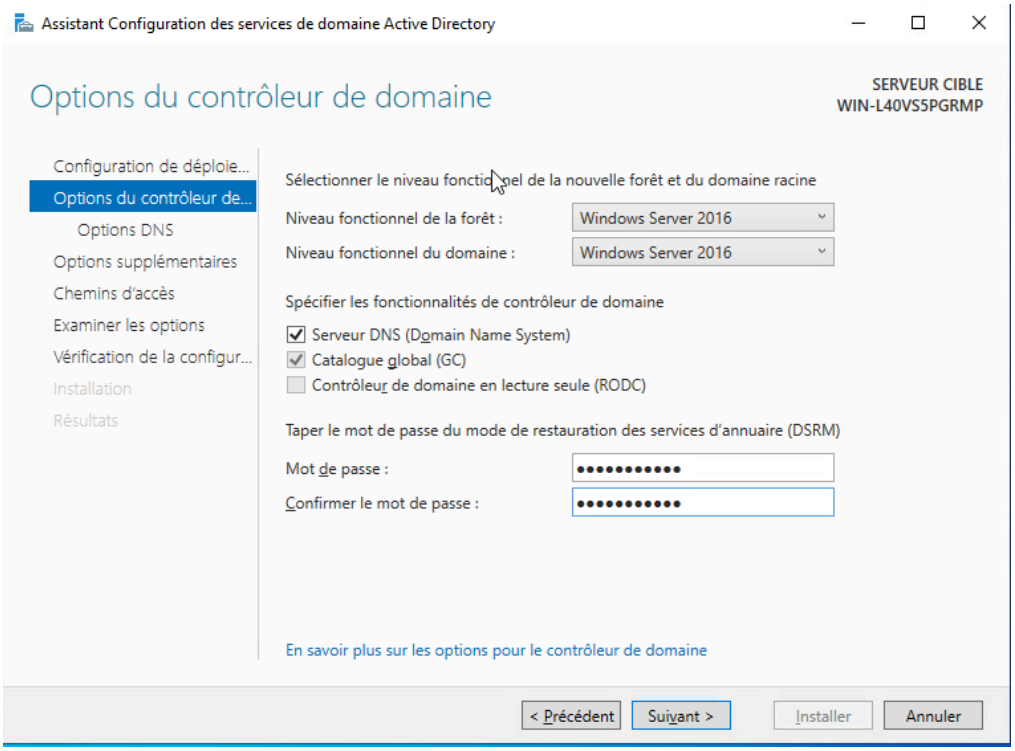


Il faut cliquer sur “Promouvoir ce serveur en contrôleur de domaine” ce qui permettra de créer une nouvelle forêt (domaine).

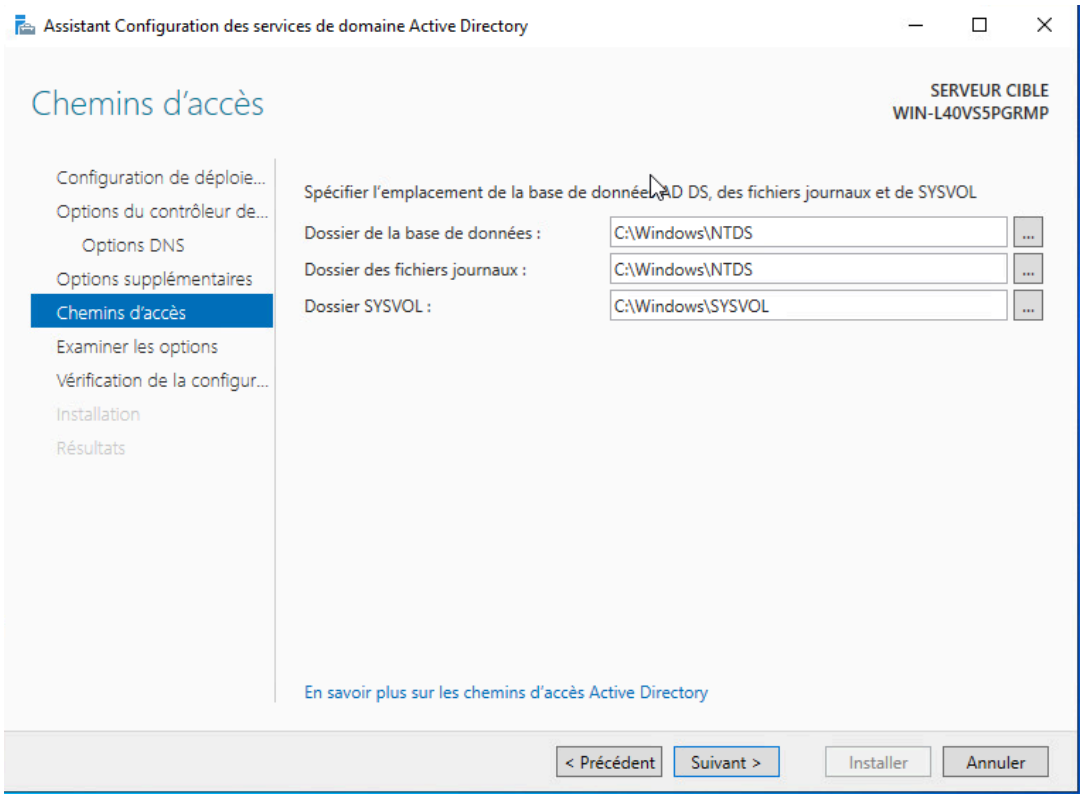


Ici, on fait “Ajouter une nouvelle forêt” et on nomme le nouveau nom de domaine racine à cette forêt. Dans notre cas, on va se fier au contexte de l’entreprise ALSET, donc on l’a appelé “alset.local”.

Une forêt dans un serveur Active Directory est un regroupement de plusieurs arborescences de domaines (arbres).



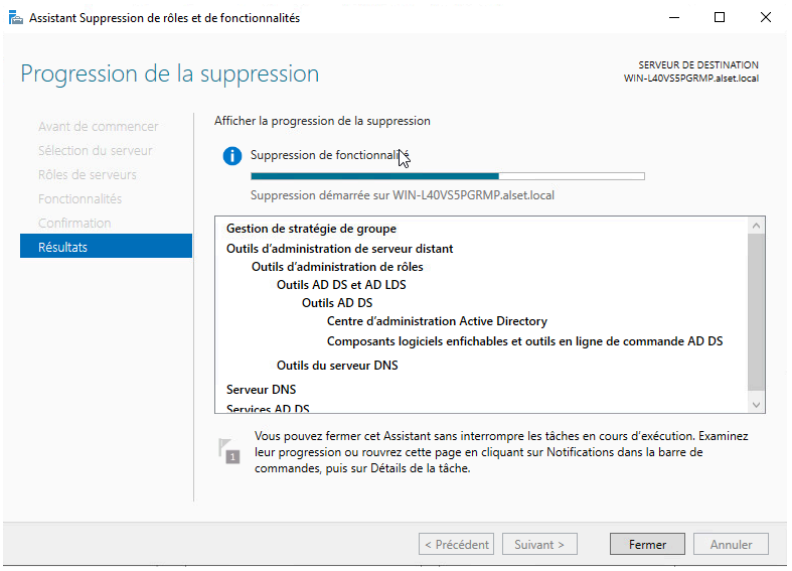
Ici, on sélectionne que le serveur Active Directory intègre aussi un serveur DNS ce qui permettra de faire la résolution entre le nom de domaine de l'Active Directory intégré au serveur Windows et l'adresse IP de la machine serveur (alset.local => 192.168.2.1 /24). Puis, on met un mot de passe pour le DSRM (recherche à faire) afin de protéger le serveur Active Directory.



Ici, ce sont les chemins d'accès par rapport à la base de données, des logs et du répertoire SYSVOL. Le volume système (SYSVOL) est un répertoire spécial propre à chaque contrôleur de domaine. Il stocke les GPOs (Objet de Stratégie de groupe en français) et les scripts de connexion, c'est-à-dire l'authentification aux machines clientes du contrôleur de domaine. Enfin, on a fini l'installation du service Active Directory sur le serveur Windows Server 2022.

Cependant, l'oubli que nous avons réalisé était qu'on a installé le service Active Directory avant de configurer l'adresse IP et le masque du serveur, ce qui a fait qu'on a dû supprimer le service et après faire la configuration IP de la machine serveur.

La procédure est la suivante :



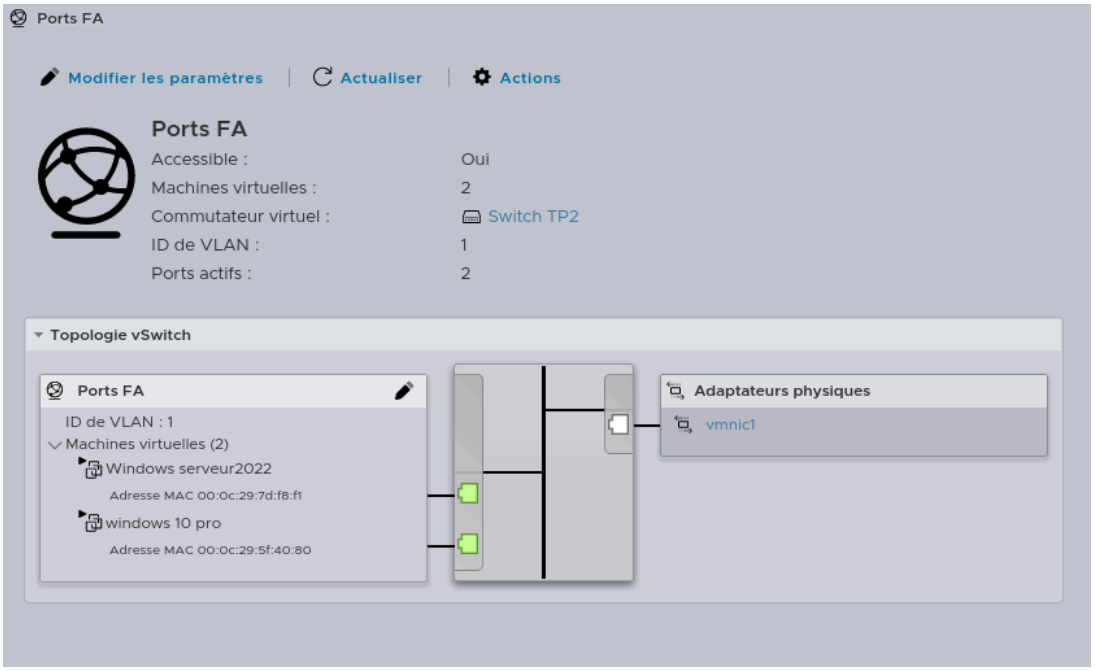
Il faut aller dans le gestionnaire de serveur, sélectionner l'onglet "Gérer", ensuite aller dans "Supprimer des rôles et fonctionnalités" puis choisir le service qu'on veut supprimer (Services AD DS) mais il faudra rétrograder le contrôleur de domaine avant de supprimer sinon cela ne marchera pas.

Création d'un switch virtuel :

L'intérêt de créer un switch virtuel sur le serveur ESXi est de ne pas utiliser le réseau local du lycée et surtout de ne pas utiliser un switch physique, donc on gagne du temps et en efficacité.

Ensuite, on crée un groupe de ports avec la machine serveur et celle qui est cliente qu'on va affecter au switch virtuel créé précédemment afin qu'elles communiquent ensemble :

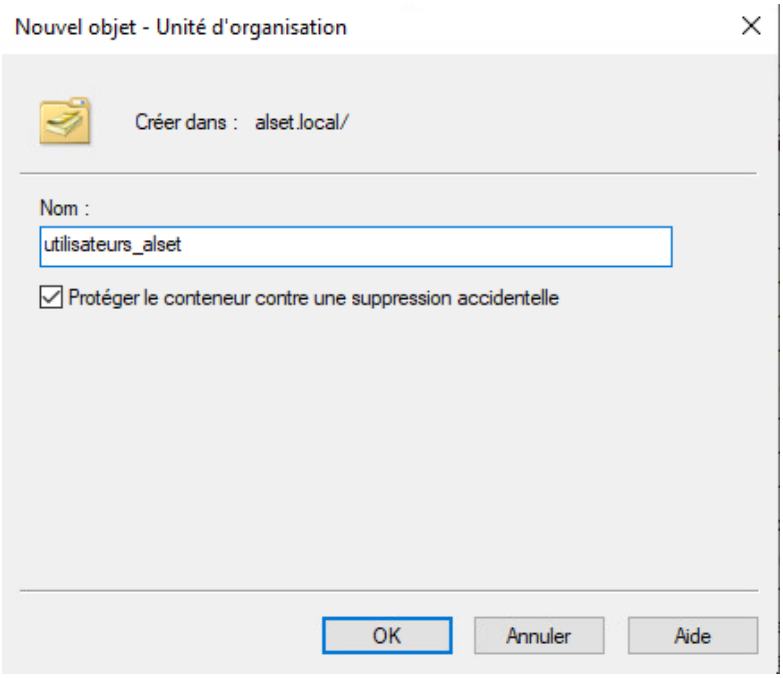
Ici, on affecte le groupe de ports “Ports FA” au switch virtuel “Switch TP2” :

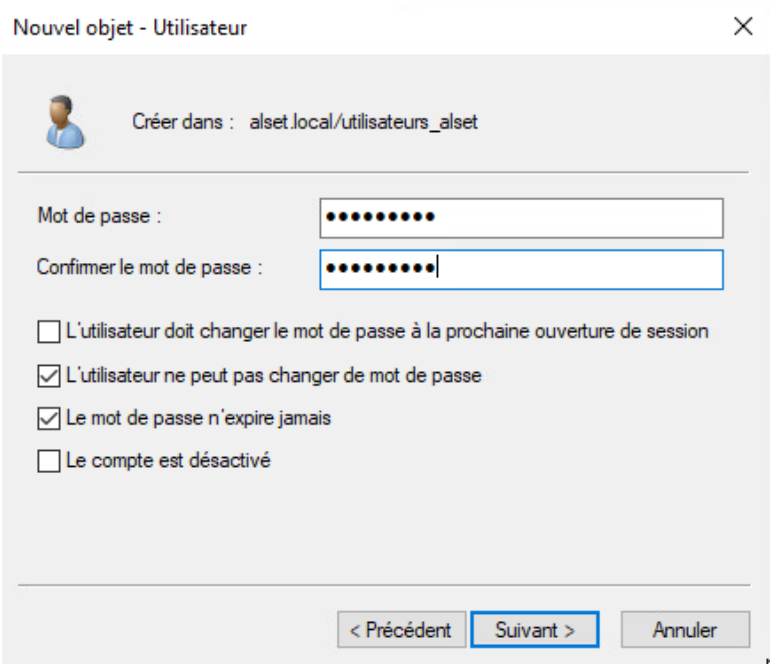


Les adaptateurs physiques vmnic (vmnic0 et vmnic1) permettent de faire la liaison entre le serveur ESXi et Internet. Maintenant, les deux machines communiquent entre elles.

Création d’un utilisateur dans un serveur Active Directory :

Tout d’abord, on a créé une unité d’organisation “utilisateurs_alset” afin de mettre l’utilisateur dans celle-ci :

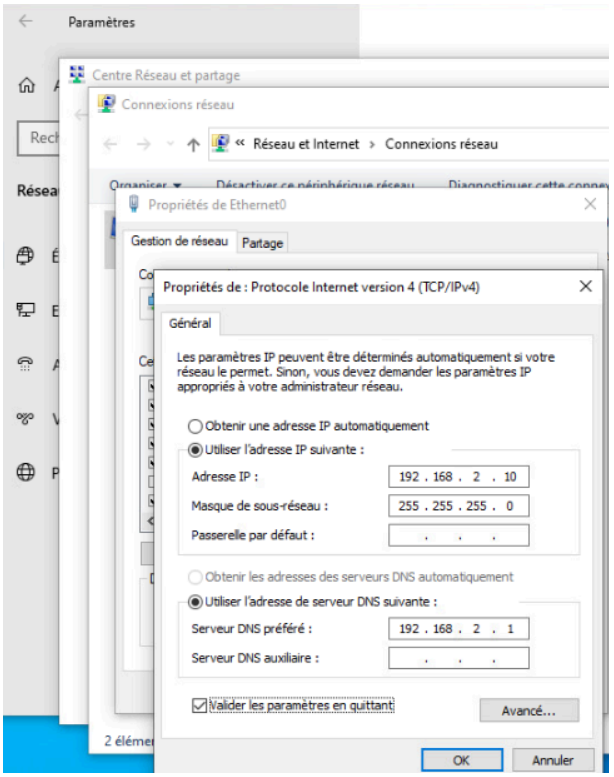




Ici, on protège l'unité d'organisation d'une suppression accidentelle pour une question d'intégrité. Puis, on a mis un mot de passe sécurisé avec 9 caractères (majuscules, minuscules, chiffres, caractères spéciaux).

Intégration de la machine cliente dans le domaine :

D'abord, il faut configurer la machine cliente (192.168.2.10 /24) et vérifier la connectivité entre celle-ci et le serveur Windows (192.168.2.1 /24) :

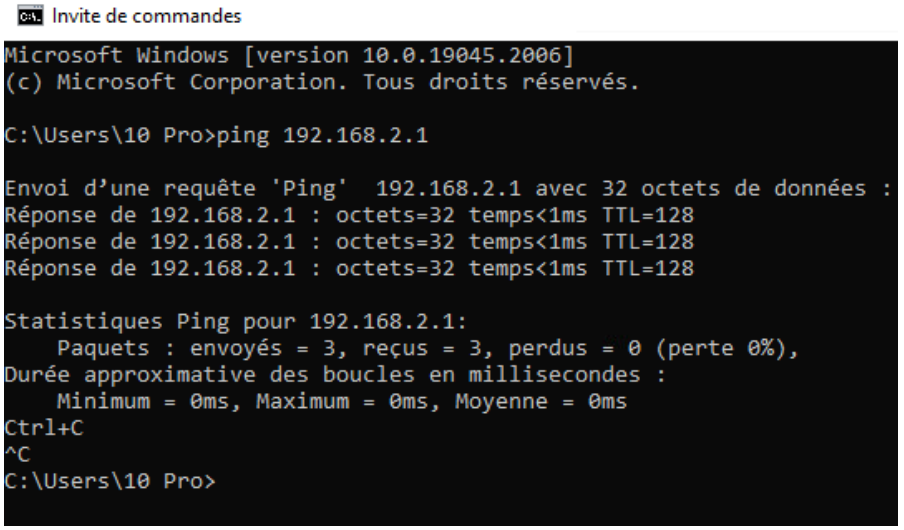


Configuration IP Machine Windows 10 Pro :

- 192.168.2.10 /24 (Adresse IP et masque de sous-réseau)
- 192.168.2.1 (Serveur DNS préféré => Serveur AD/DS)

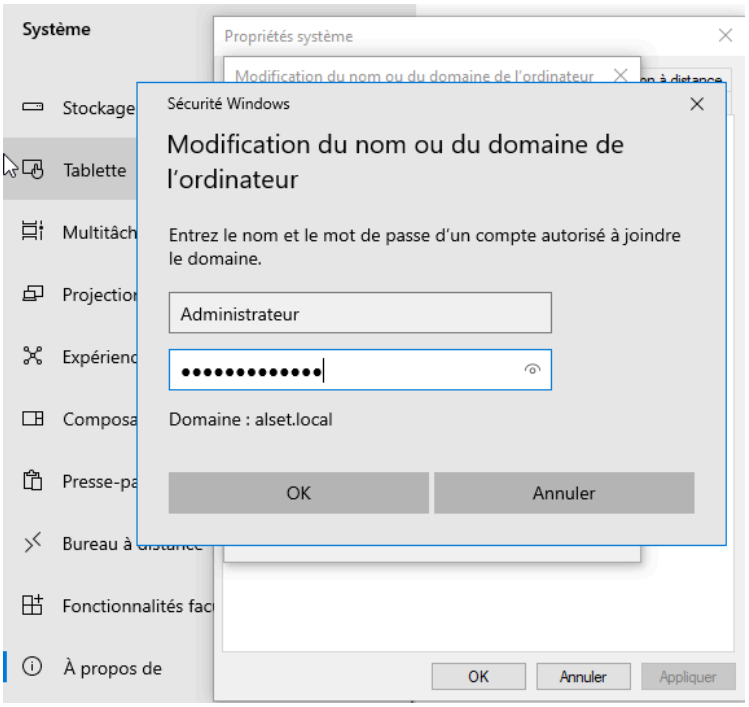
On a configuré comme ceci afin que la machine cliente puisse intégrer le domaine “alset.local”.

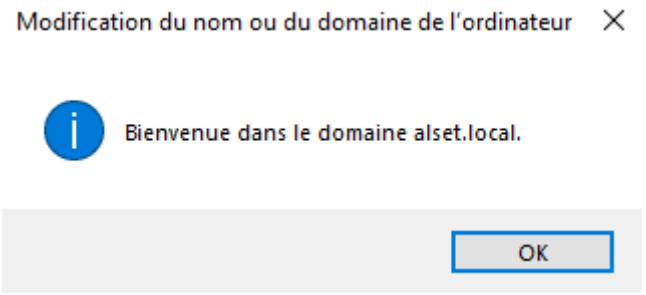
Puis, on vérifie la connectivité entre la machine cliente et le serveur Active Directory :



Le ping est fonctionnel, donc on peut tester de faire l’intégration du client au domaine.

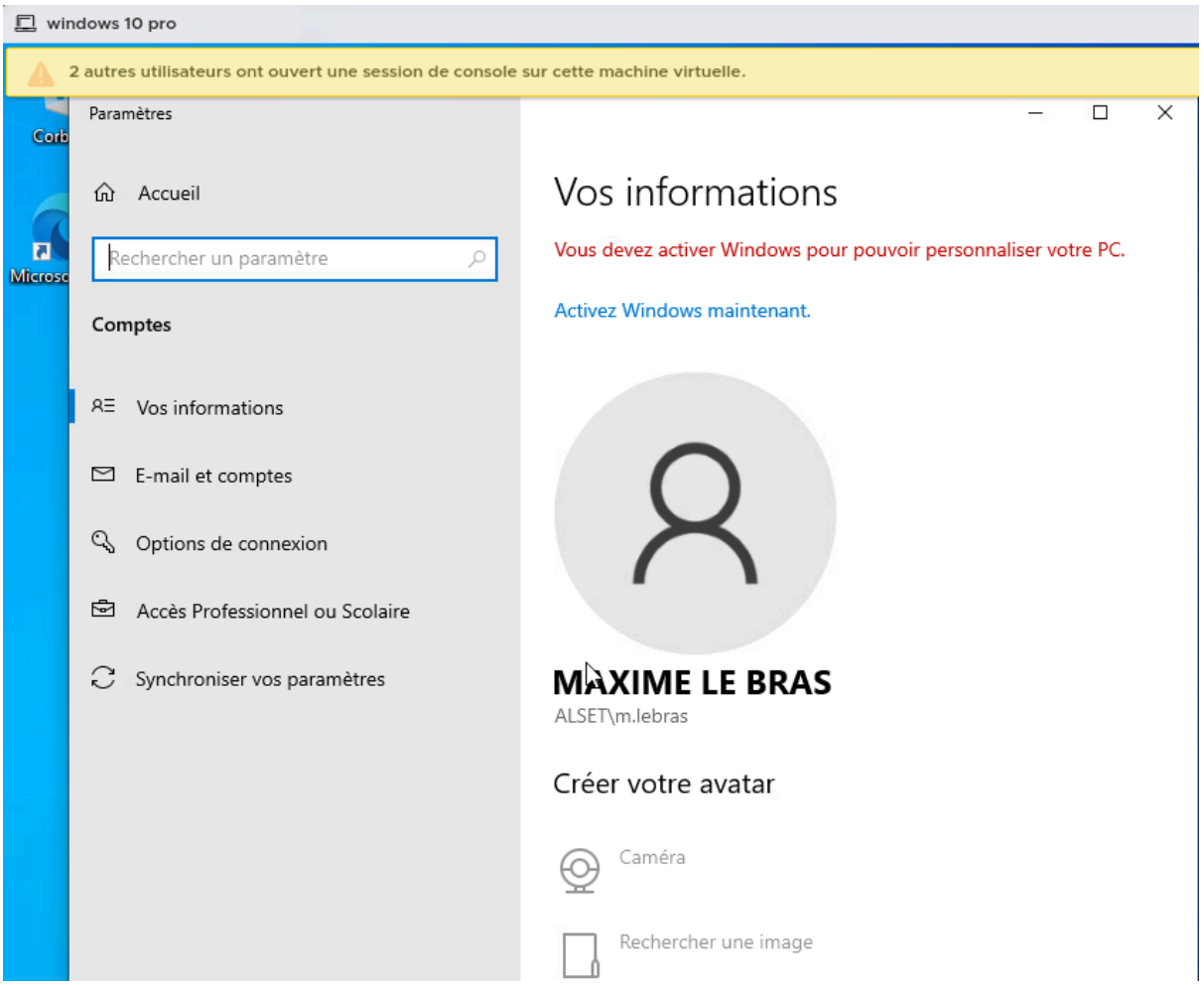
Pour intégrer un poste au domaine, il faut réaliser la démarche suivante : “Paramètres” > “Système” > “A propos de” > “Paramètres système avancés” > “Nom de l’ordinateur” > “Modifier”.





Le poste client a bien été intégré au domaine “alset.local”.

<u>Test d’accès à l’utilisateur créé :</u>

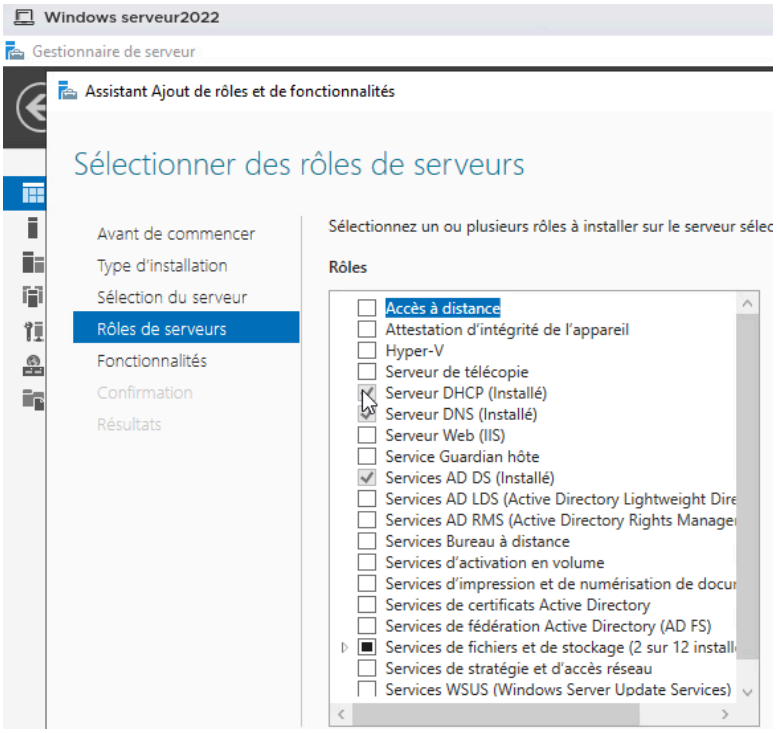


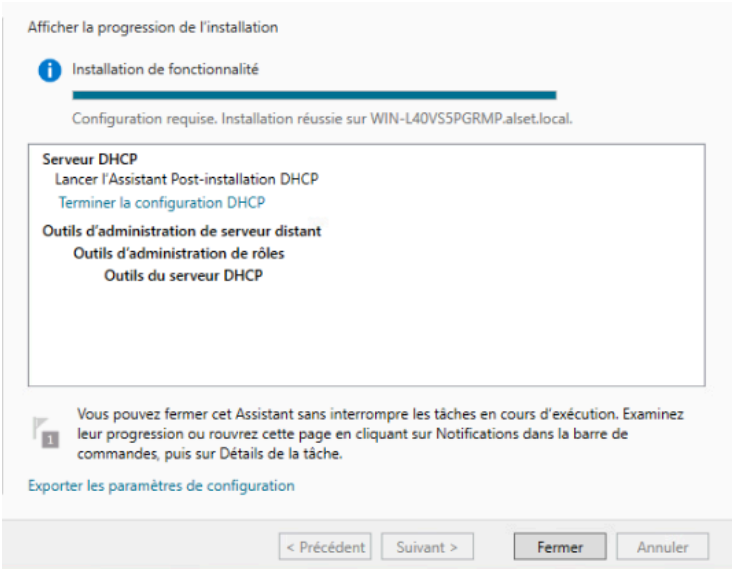
J’ai réussi à s’authentifier avec le compte créé précédemment (voir partie “Création d’un utilisateur dans un serveur Active Directory”) sur la machine cliente Windows 10 Pro.

Lot 2 - Intégration de services

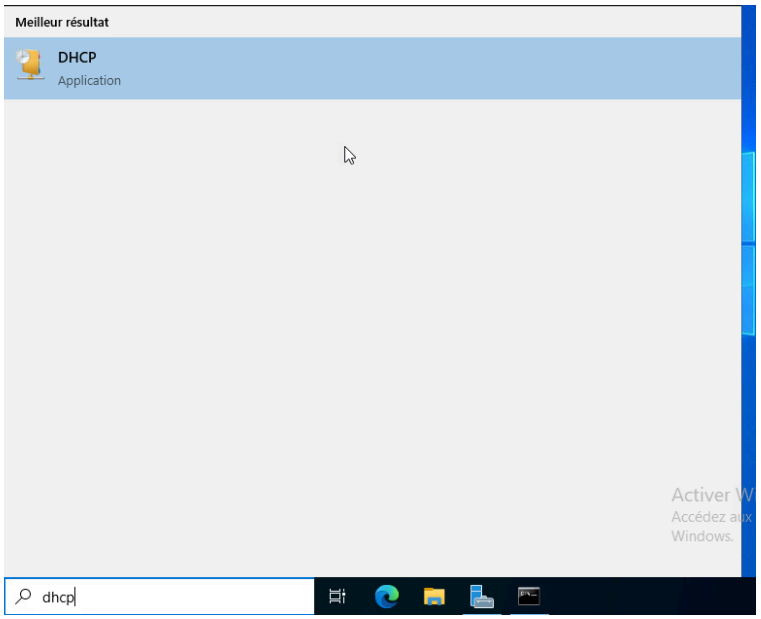
Installation et configuration du service DHCP dans le serveur Windows :

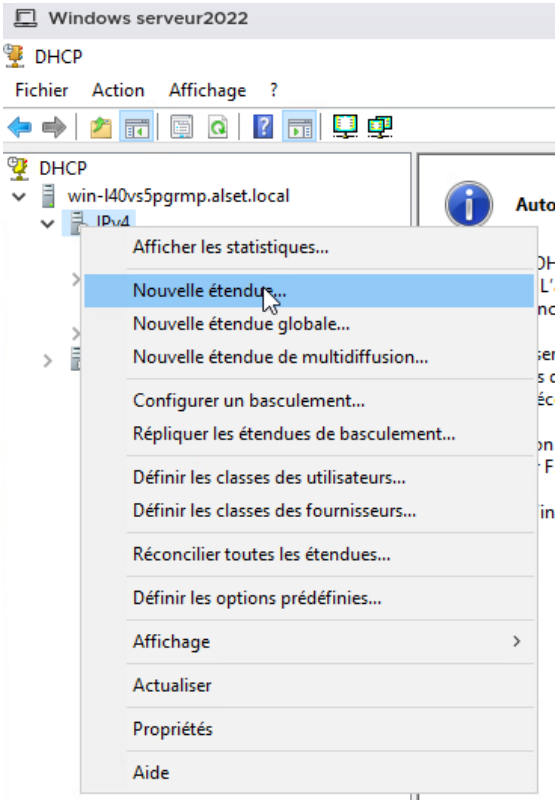
Pour installer le service DHCP, il faut aller dans le gestionnaire de serveur, ensuite faire “Gérer” > “Ajouter des rôles et fonctionnalités” > “Rôles de serveurs” > “Services AD DS” > “Installer”.

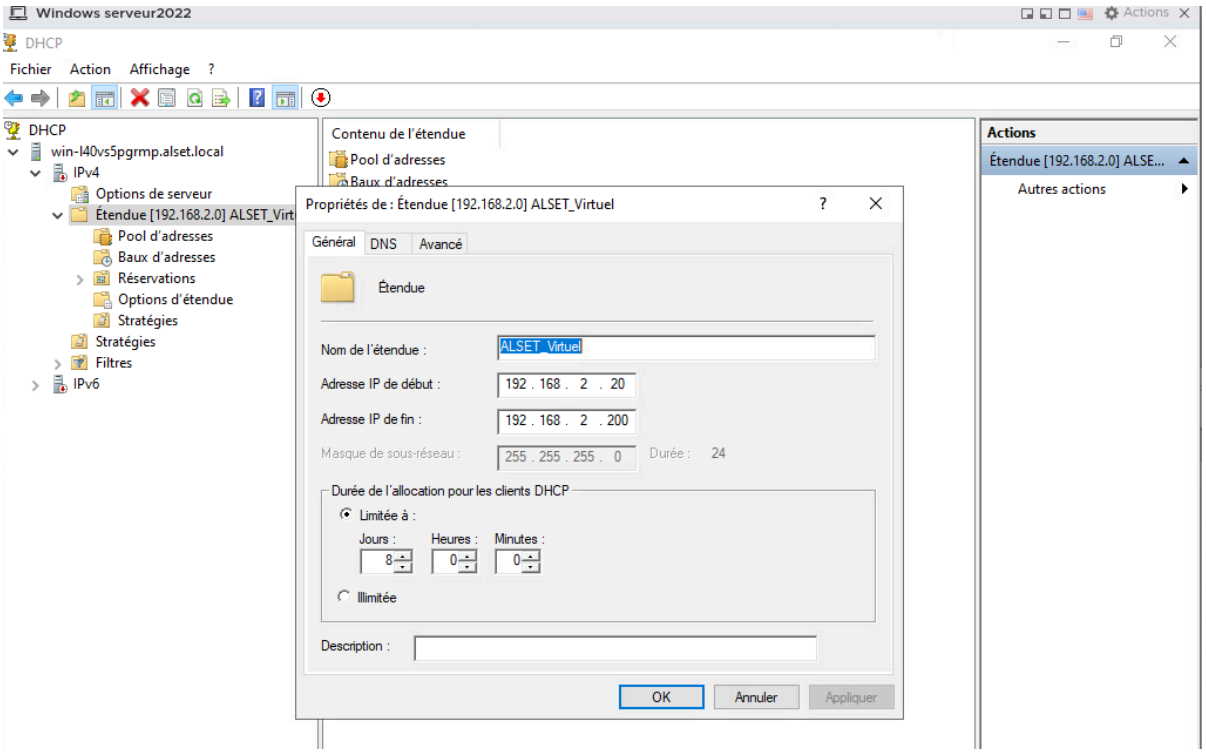




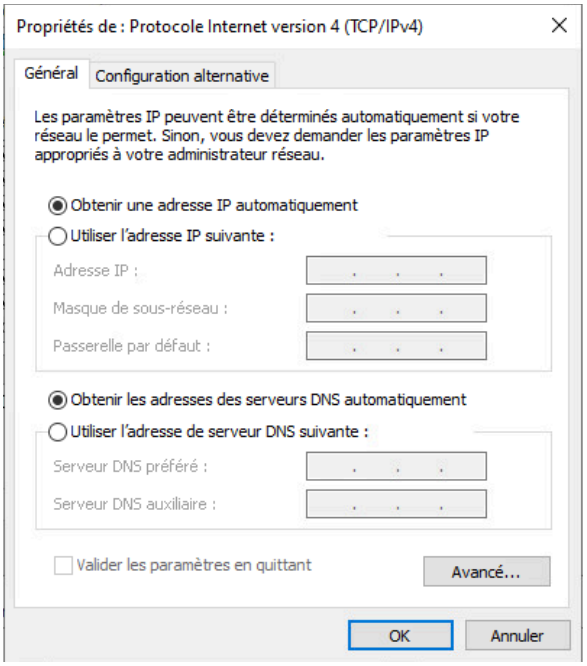
Pour configurer le serveur DHCP et mettre en place l'étendue correspondant au schéma réseau (192.168.2.20 à 192.168.2.200), il faut faire ceci :



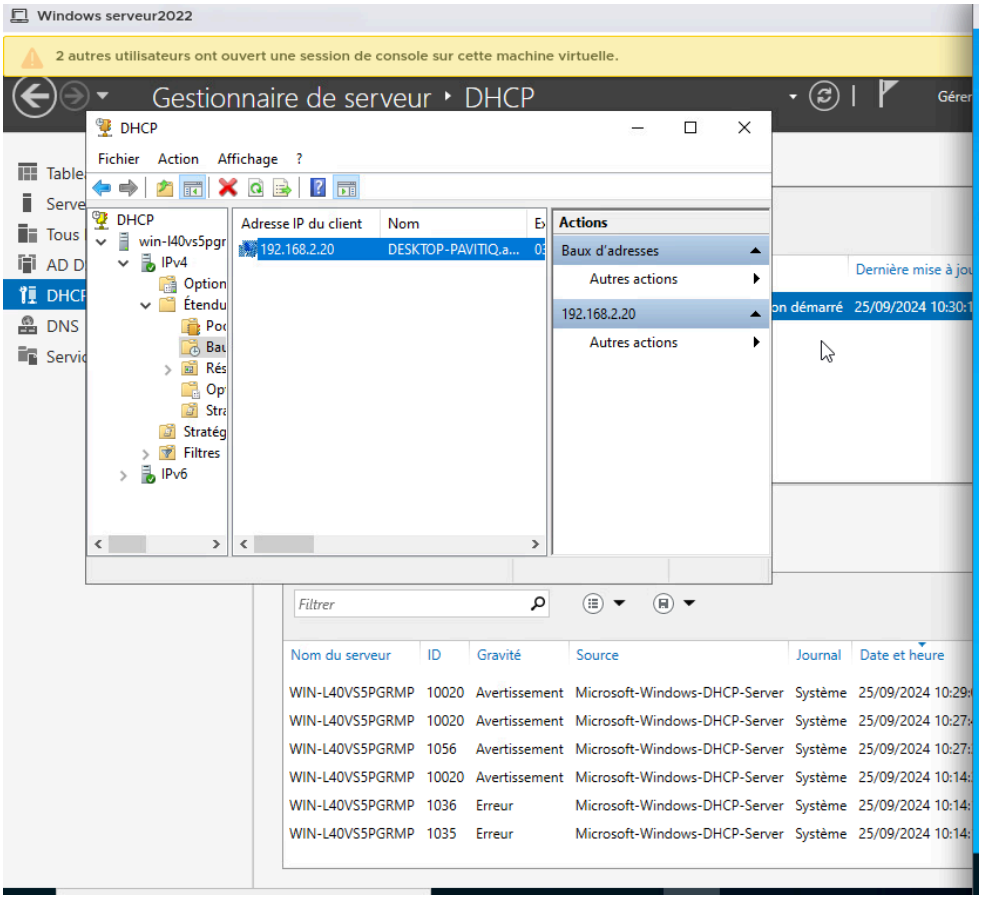


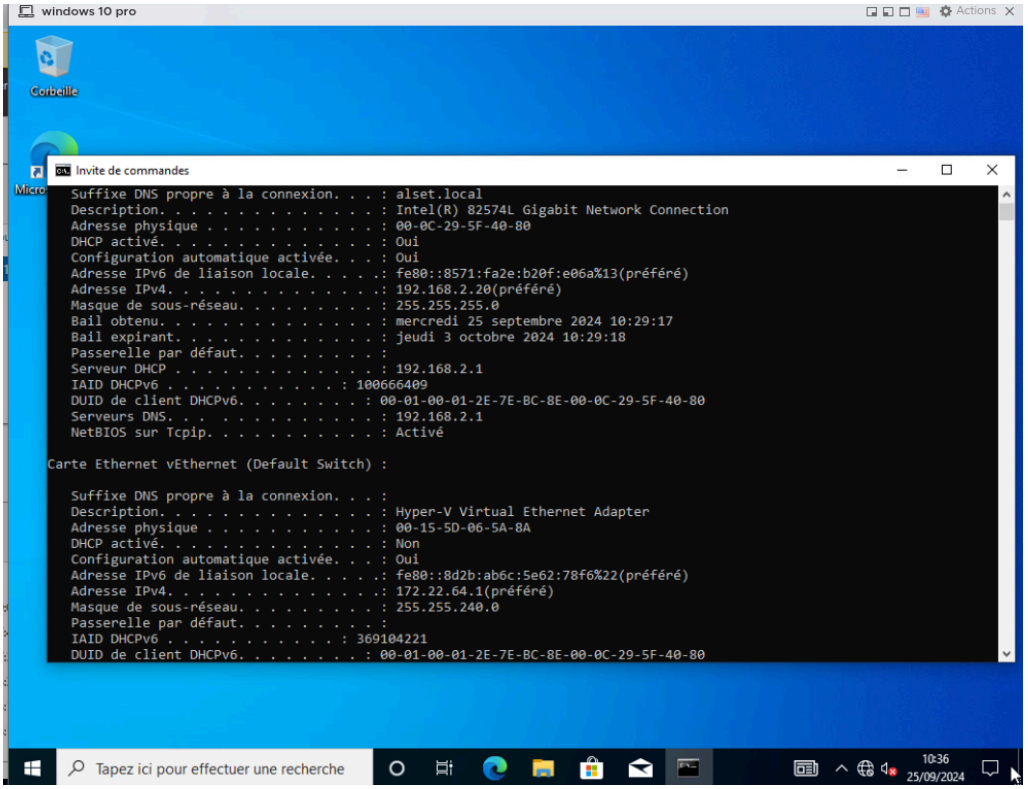


Le rôle du serveur DHCP (Dynamic Host Configuration Protocol) est d'attribuer de manière automatique des adresses dynamiques, c'est-à-dire qu'elles sont changées au bout d'un certain temps (24 heures principalement). L'intérêt de mettre en place ce service est de protéger les machines, car si on a des machines qui sont en adresses IP statiques, elles seront plus vulnérables alors que si on met en place des adresses IP dynamiques, la vulnérabilité des machines sera réduite.



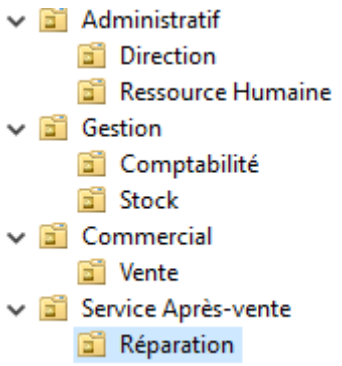
Ici, on remet une configuration IP automatique pour la machine cliente afin de tester le fonctionnement du serveur DHCP au sein du réseau local.





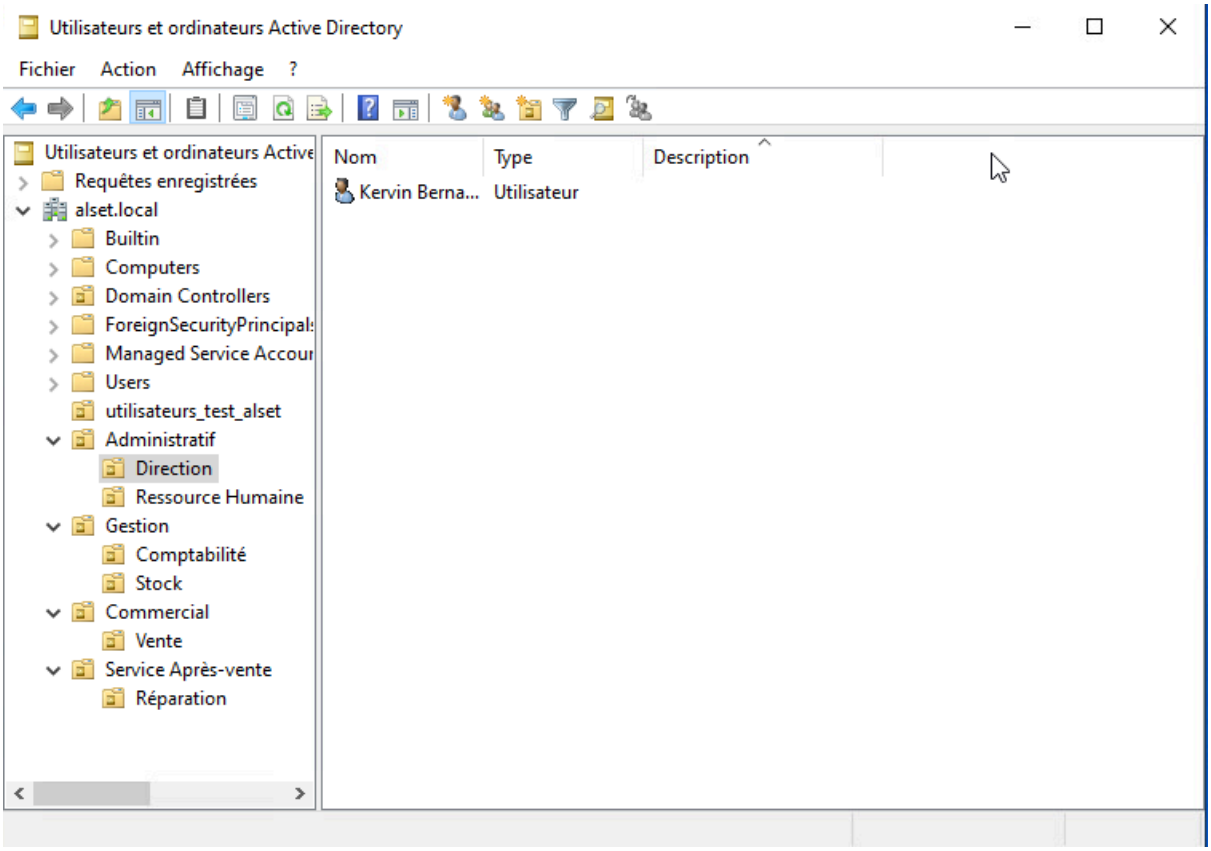
Ici, on voit que le test de fonctionnement du serveur DHCP a été concluant puisqu'il a fourni une adresse IP dynamique à la machine cliente.

Création des UO et GROUP pour les différents services parents et enfants :

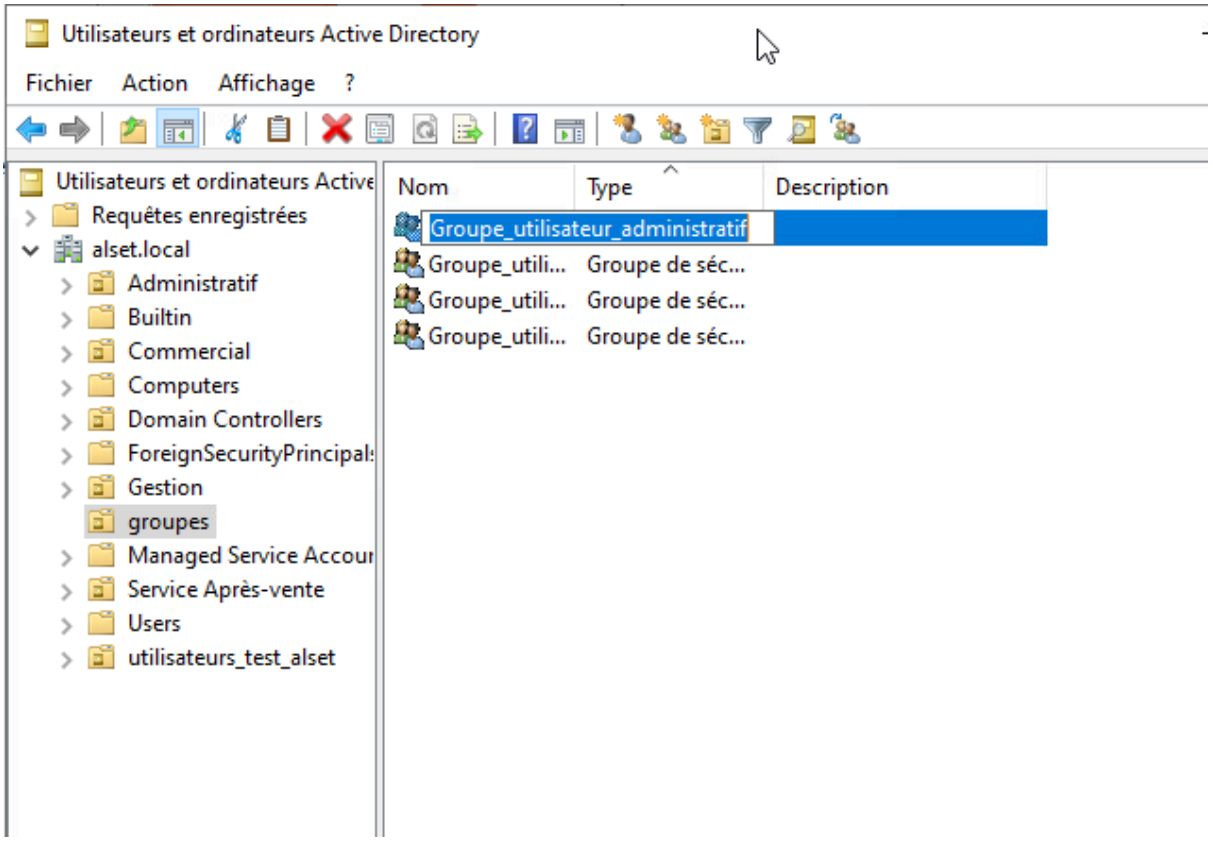


Voici l'arborescence de l'Active Directory de la société ALSET avec quatre services principaux : Administratif, Gestion, Commercial et Service Après-Vente avec ses différents sous-services ainsi que les salariés affectés dans leurs services et sous-services.

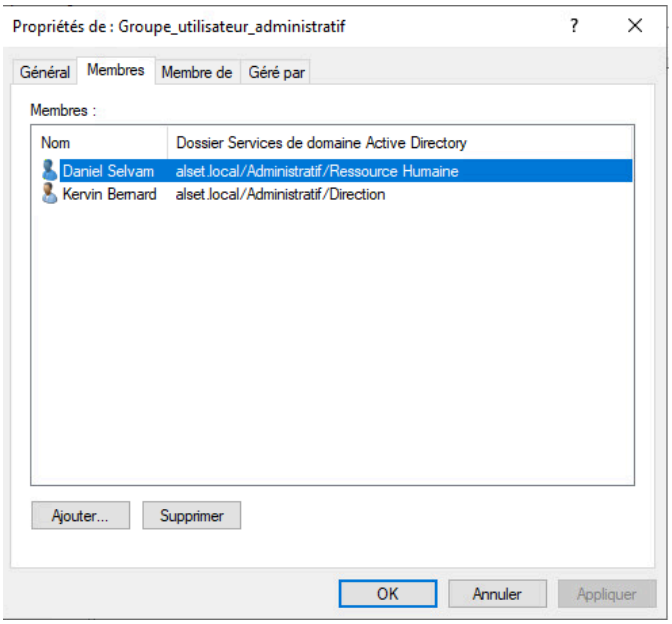
Exemple :



Création de dossier partagé par service parent accessible aux services enfants :

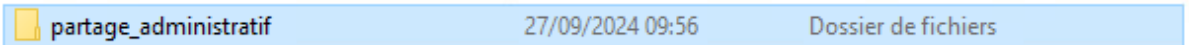


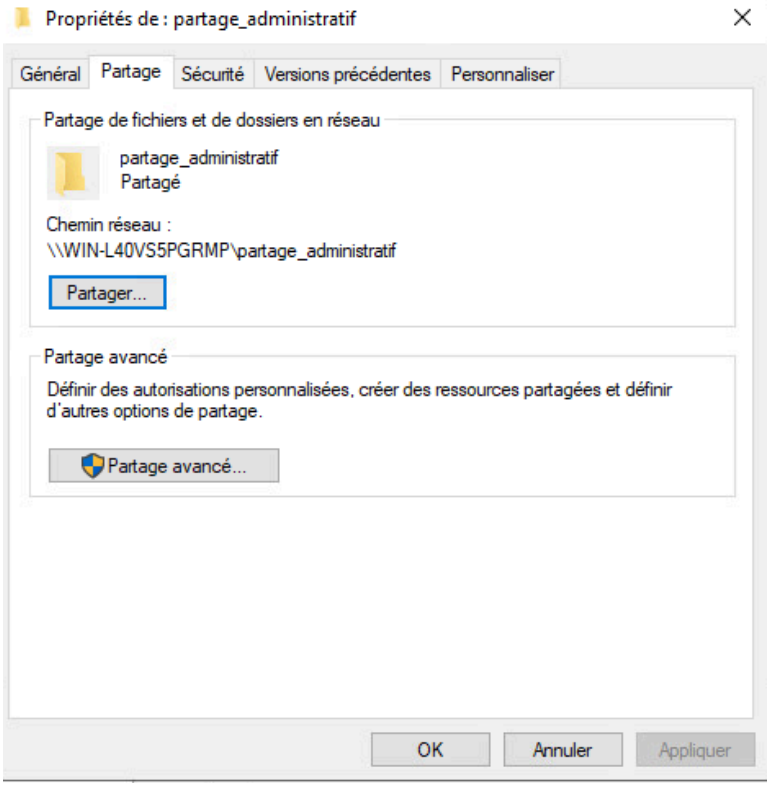
Ici, j'ai créé des groupes de sécurité (groupes d'utilisateurs) liés aux différents services parents afin que les utilisateurs puissent au dossier partagé propre au service.

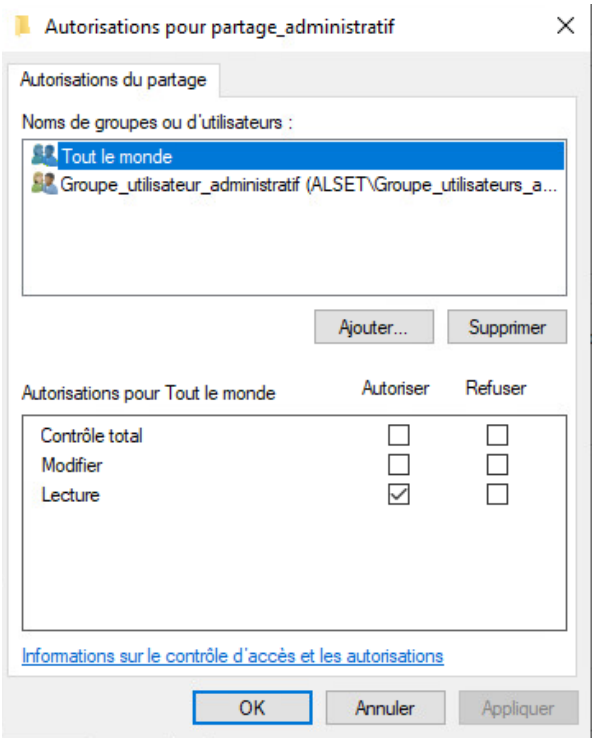


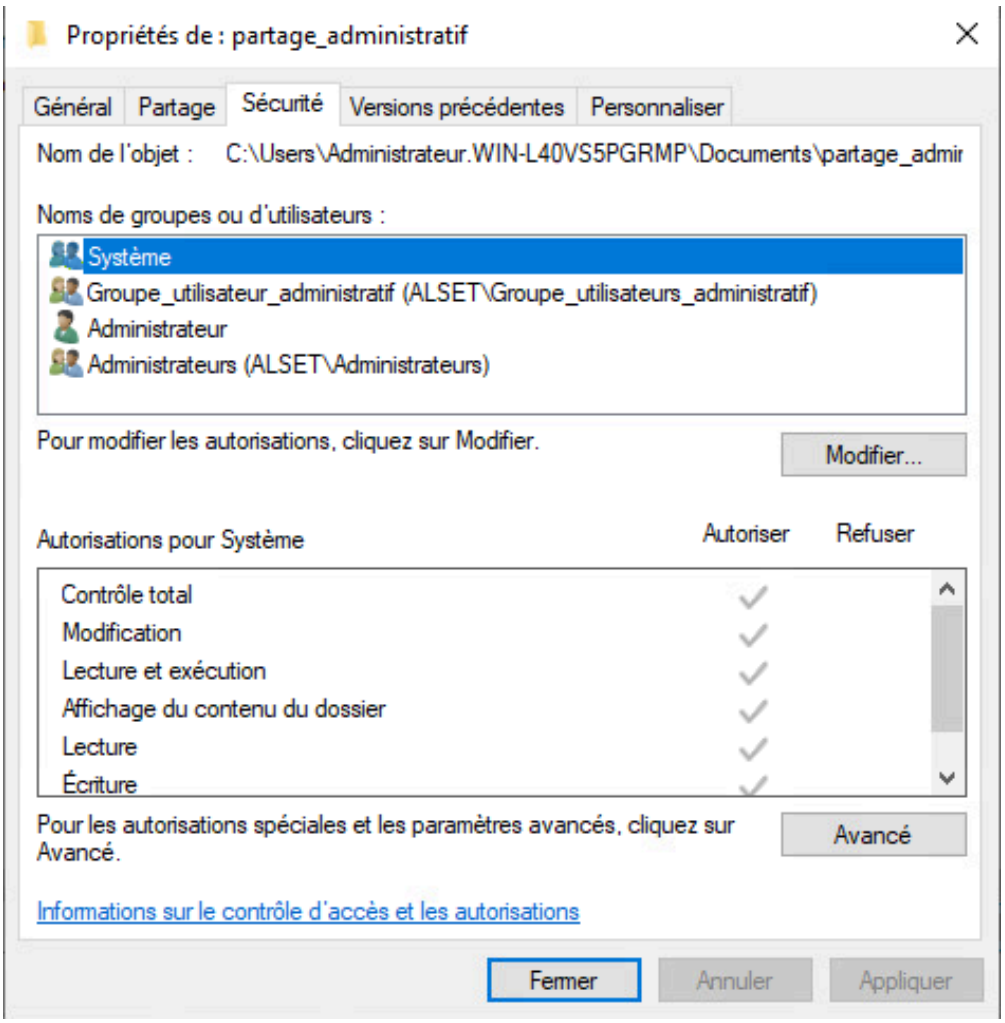
Par exemple, on a attribué les salariés du service Administratif dans le groupe de sécurité "Groupe_utilisateur_administratif".

Ensuite, on a créé les différents dossiers partagés (ex : partage_administratif) pour les différents services de l'entreprise :

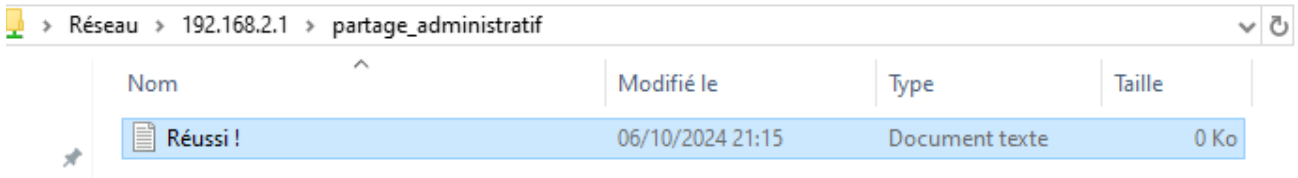








Nous avons fini de mettre en place les dossiers partagés, donc il faut vérifier si ça fonctionne bien sur les utilisateurs concernés.



Daniel Selvam et Kervin Bernard ont bien accès au dossier partagé “partage_administratif”.

Création d'un lecteur réseau et connexion du lecteur réseau avec le client :

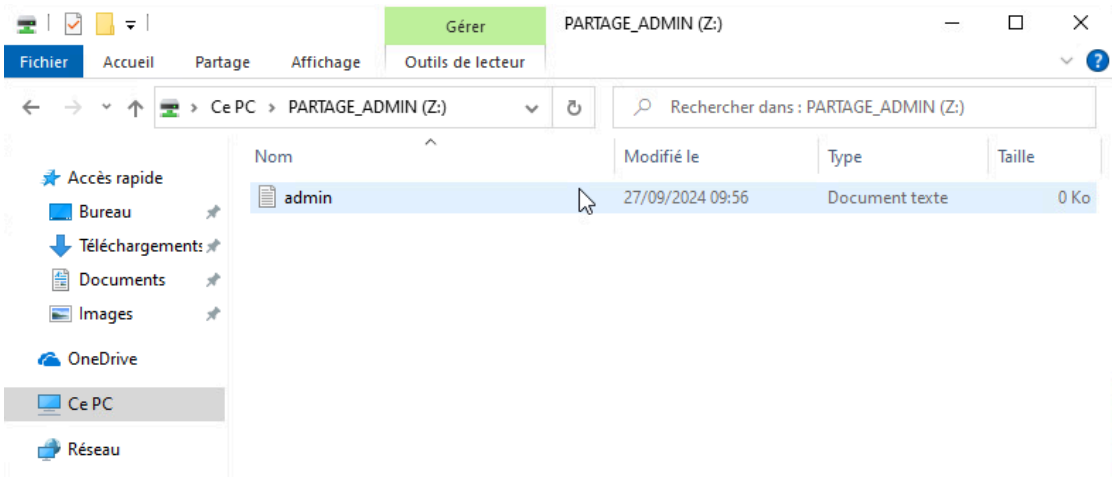
Voici la démarche pour réaliser la GPO Lecteur Réseau :

- Création de dossier partagé (autorisations - sécurité)
- il faut aller dans le fichier de gestion de stratégies de groupe (gpedit.msc)
- ensuite faire un clic droit sur l'UO
- "Créer un objet GPO dans ce domaine, et le lier ici…"
- faire un clic droit sur la GPO
- "Modifier"
- Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs
- faire "Appliqué"
- Créer le lecteur réseau
- Action : Mettre a jour
- Emplacement : indiquer le chemin réseau obtenu précédemment : \\nomhote\partage
- Cocher Reconnecter
- Libeller selon le contexte
- Lettre de lecteur : Z (Commencer par la dernière lettre disponible)
- Afficher ce lecteur
- Cibler un groupe de sécurité (ex : groupe_utilisateurs_administratif) : Aller dans les priorités du lecteur réseau, ensuite allez dans l'onglet "Commun", après cocher "Ciblage au niveau de l'élément", appuyez sur "Ciblage..."
- "Nouvel élément" - "Groupe de sécurité" - "..." - Sélectionner le groupe de sécurité en question

Vérification de l'application des GPOs sur le client :

- Appliquer la GPO
- cmd
- gpupdate /force
- gpresult /h result.html
- result.html

Après, il faut aller vérifier si le lecteur réseau est bien mis en place.



On voit ici que la GPO d'installation d'un lecteur réseau sur un des services d'ALSET, a bien été mise en place.

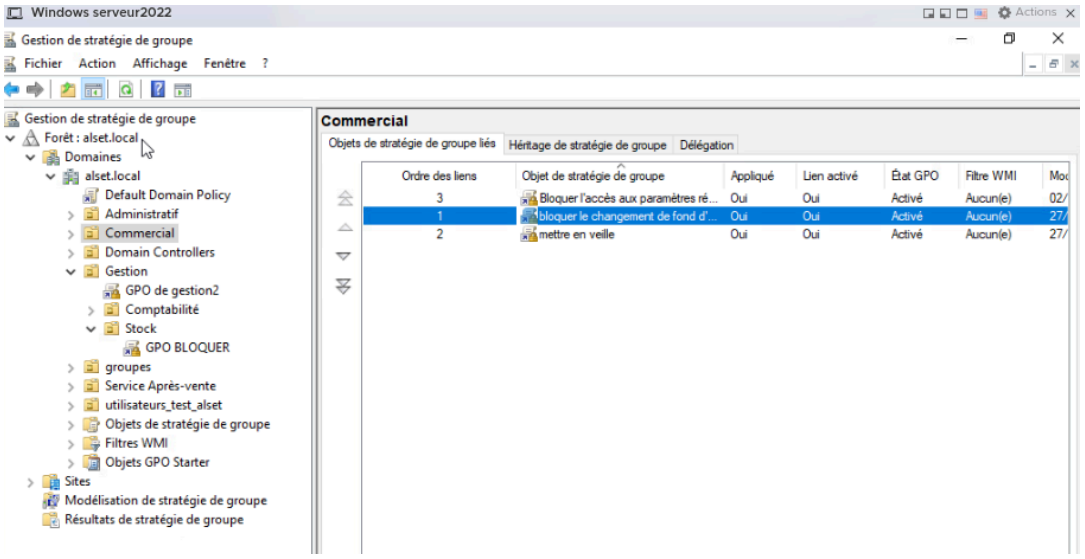
Lot 3 - Stratégie de groupe "GPO"

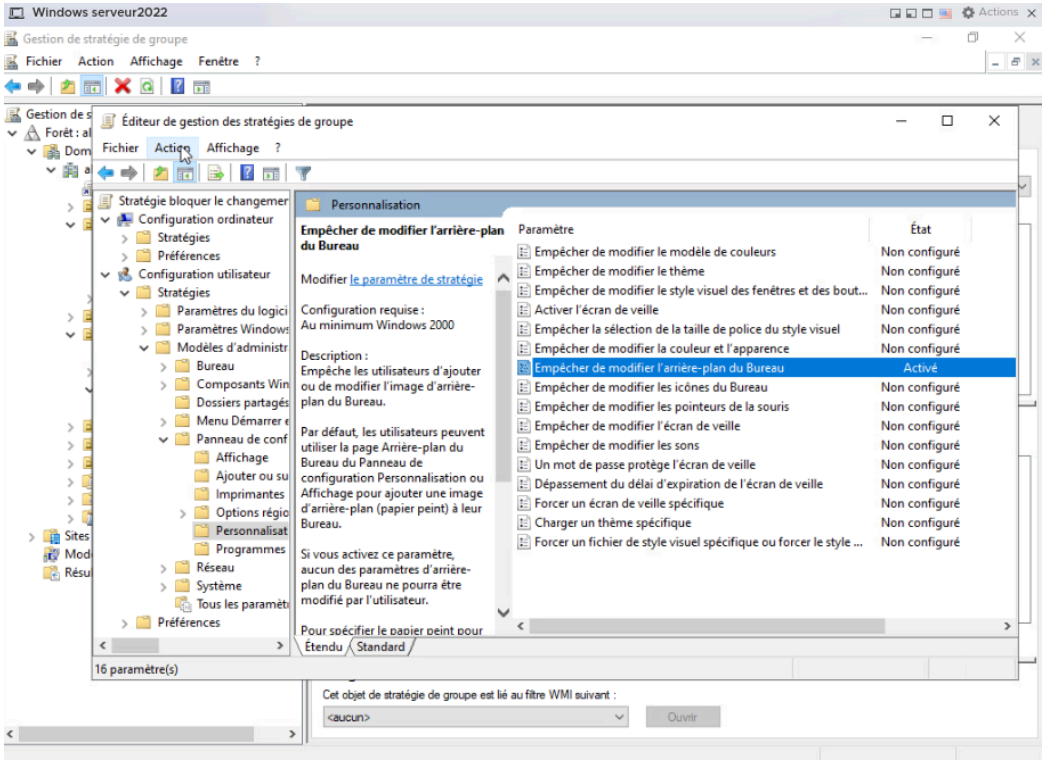
Pour commencer, un objet de stratégie de groupe (dit GPO (Group Policy Object en anglais) est un ensemble de paramètres qui définissent à quoi va ressembler un système et comment il va se comporter pour un groupe défini d'utilisateurs. Chaque GPO contient deux parties, ou nœuds : une configuration utilisateur et une configuration ordinateur.

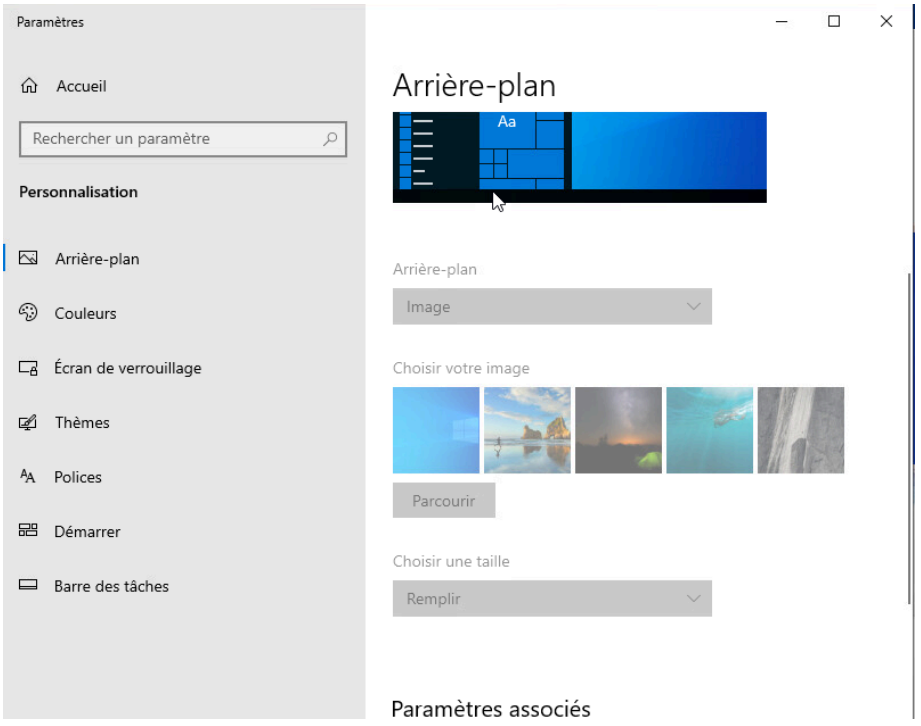
Pour pouvoir mettre en place une GPO correctement sur des utilisateurs, il faut réaliser les commandes suivantes dans le cmd de l'utilisateur Windows et appliquer celle-ci :

- gpupdate /force
- gpresult /h result.html
- result.html

Tout d'abord, pour les services Commercial, Service Après-Vente et Comptabilité, on devait réaliser une GPO qui bloque le changement du fond d'écran pour les utilisateurs. Pour réaliser cette stratégie de groupe, il faut faire ça :







On a réalisé le test sur un des utilisateurs d'un des services de l'organisation ALSET et cela a bien fonctionné.

Ensuite, pour les services Commercial, Service Après-Vente, Administratif et Stock, on devait réaliser deux GPOs : la première qui permettait de bloquer les accès aux paramètres réseaux sans désactiver l'accès au panneau de configuration et la deuxième qui permettait de ne pas afficher le bouton Mise en veille. Pour réaliser ces stratégies de groupe, il faut faire ça :

Stratégies masquer

Modèles d'administration masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Panneau de configuration masquer

Stratégie	Paramètre	OSG gagnant
Masquer les éléments du Panneau de configuration spécifiés	Activé	GPO Bloquage accès paramètres réseau

Liste des éléments du Panneau de configuration non autorisés
Centre Réseau et Partage

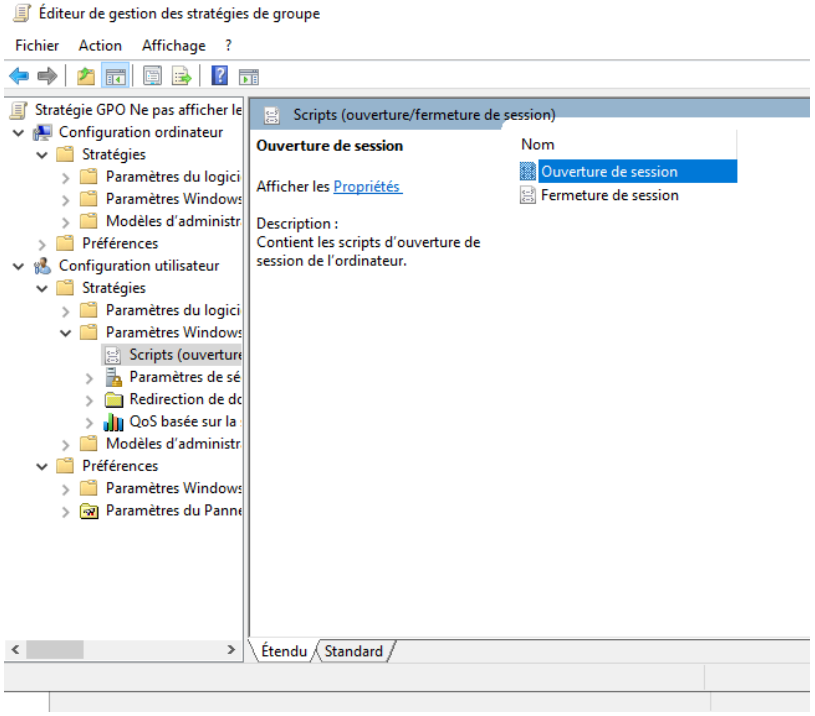
Stratégie	Paramètre	OSG gagnant
Visibilité de la page des paramètres	Activé	GPO Bloquage accès paramètres réseau

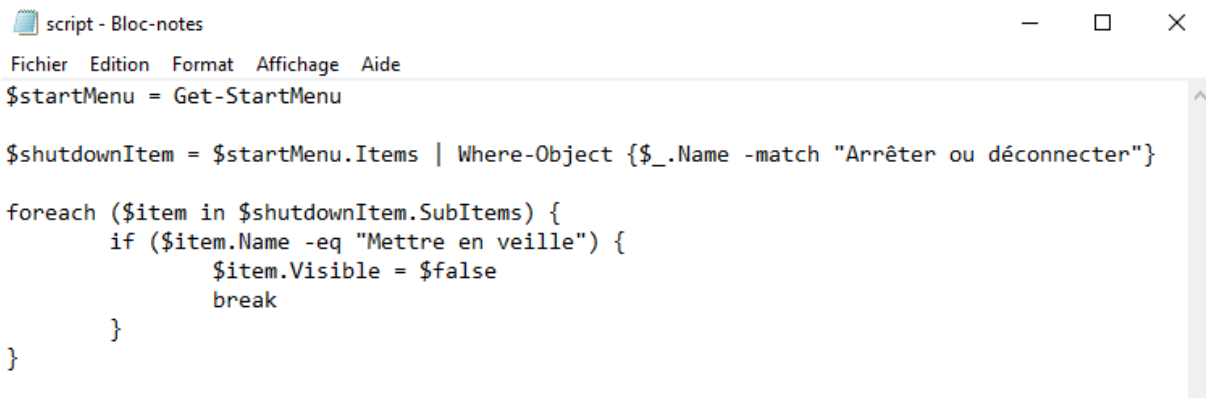
Visibilité de la page des paramètres :	hide:network-status;network-ethernet;network-wifi;network-vpn;network-proxy;network-mobilehotspot;network-dialup

Réseau/Connexions réseau masquer

Stratégie	Paramètre	OSG gagnant
Interdire l'accès aux propriétés d'une connexion au réseau local	Activé	GPO Bloquage accès paramètres réseau

Cela va permettre de masquer l'élément "Centre Réseau et Partage" du panneau de configuration ainsi que les paramètres réseaux dans les paramètres générales de l'ordinateur et enfin d'interdire l'accès aux propriétés de la carte réseau.

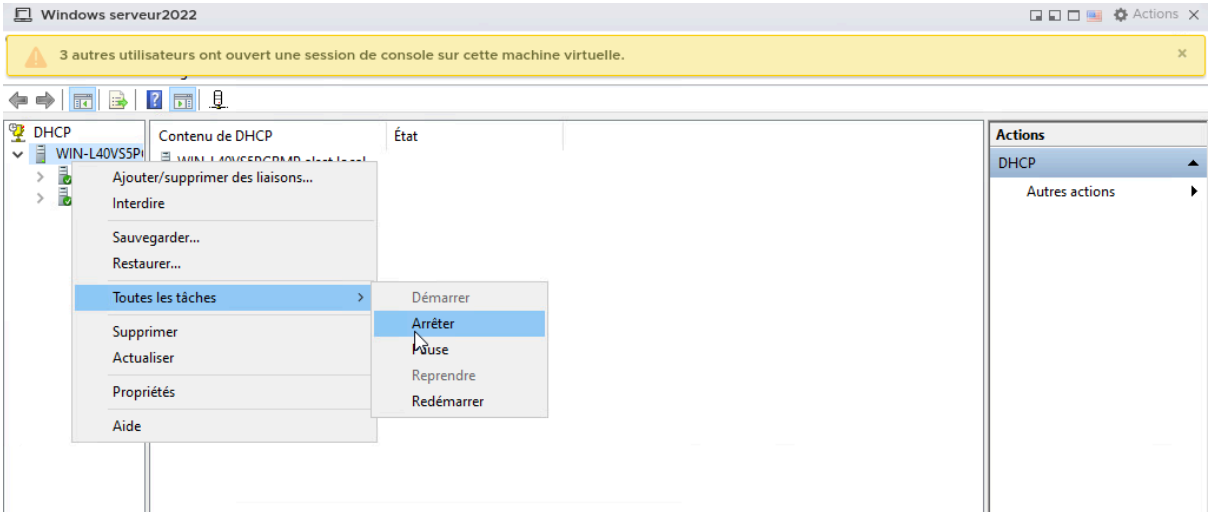




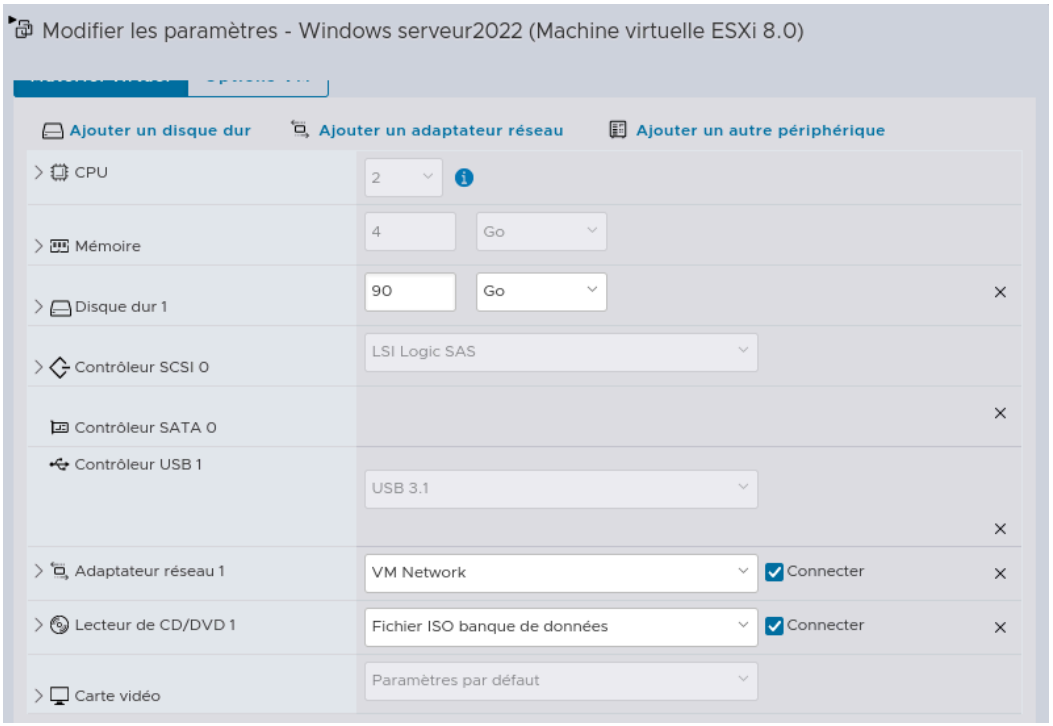
Ici, on va intégrer ce script en extension .ps1 (Windows Powershell) à l'ouverture de session des utilisateurs concernés. Ce script Powershell va permettre de masquer le bouton Mise en veille pour les utilisateurs.

Lot 4 - Le choix du déploiement en groupe avec WDS

Mise en place du service WDS (Windows Deployment Services) non-dépendant de l'Active Directory :



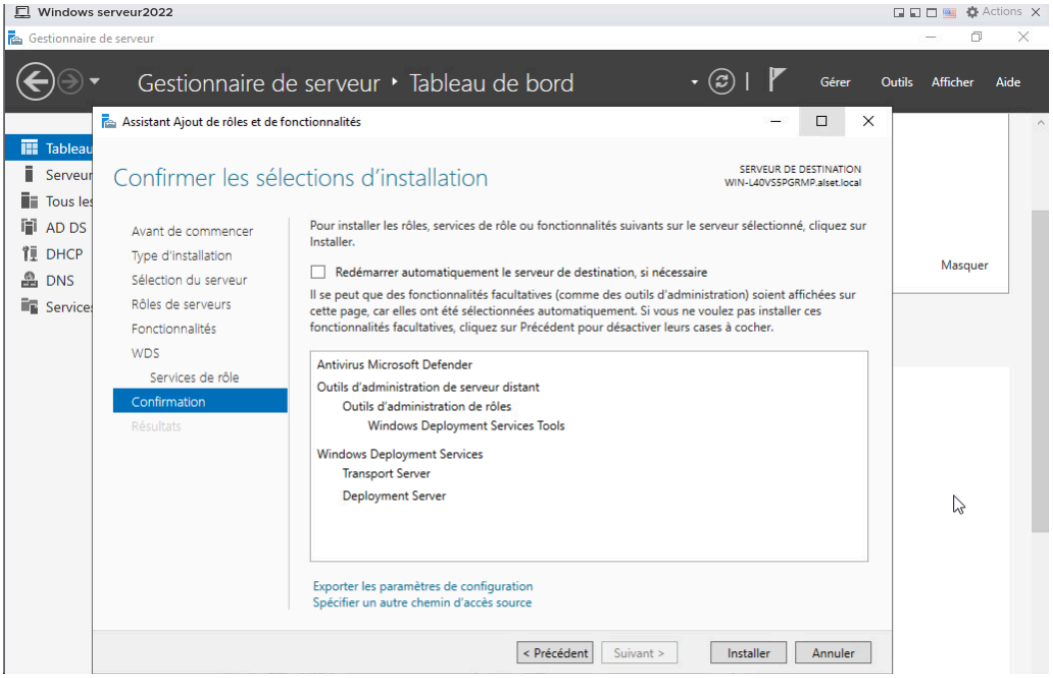
Tout d'abord, on doit enlever le service DHCP afin de ne pas perturber le réseau du lycée.

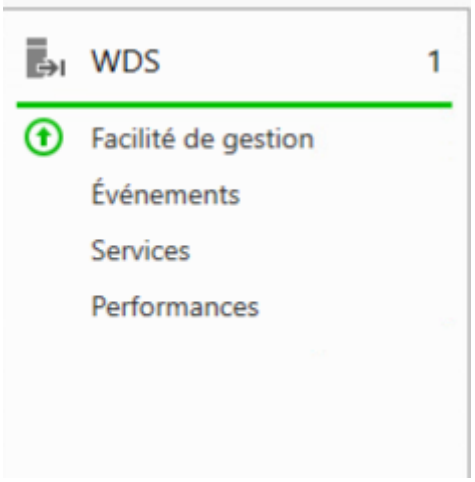


Ensuite, on remet le serveur Windows sur le switch virtuel "VM Network" (switch qui permet d'aller vers Internet comprenant les interfaces vmnic) pour pouvoir mettre en place le service WDS.

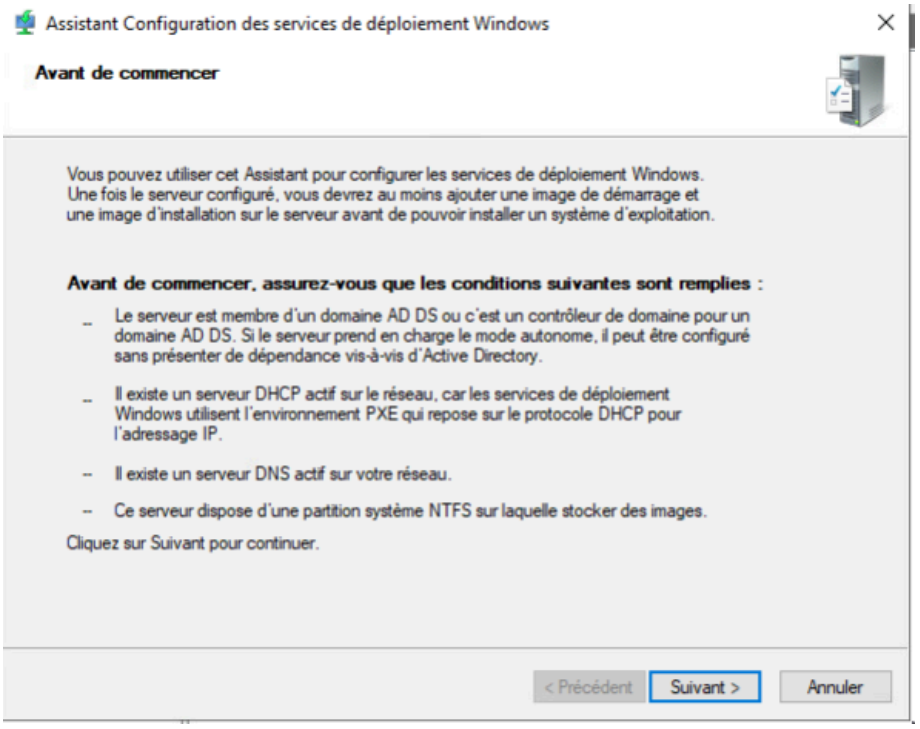
```
Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Adresse physique . . . . . . . . . . . : 00-0C-29-7D-F8-F1
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.6.6(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Bail obtenu. . . . . . . . . . . . . . : mercredi 2 octobre 2024 11:37:32
   Bail expirant. . . . . . . . . . . . . : mercredi 2 octobre 2024 15:37:32
   Passerelle par défaut. . . . . . . . . : 172.16.253.253
   Serveur DHCP . . . . . . . . . . . . . : 172.16.252.150
   Serveurs DNS. . .  . . . . . . . . . . : 80.10.246.2
                                 80.10.246.129
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé

C:\Users\Administrateur.WIN-L40VS5PGRMP>ping www.google.fr

Envoi d'une requête 'ping' sur www.google.fr [142.250.75.227] avec 32 octets de données :
Réponse de 142.250.75.227 : octets=32 temps=4 ms TTL=114
Réponse de 142.250.75.227 : octets=32 temps=5 ms TTL=114

Statistiques Ping pour 142.250.75.227:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 5ms, Moyenne = 4ms
```

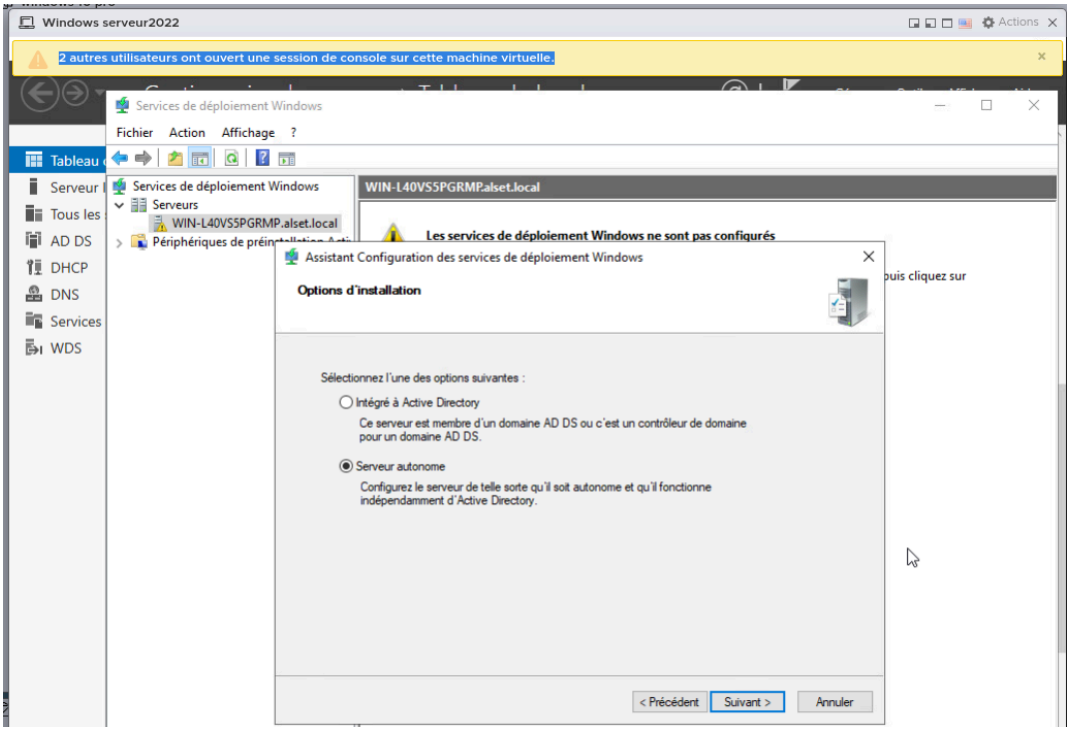
Ici, on remarque qu'on est bien sur le réseau du lycée et que la machine est connectée à Internet et peut accéder à Google.





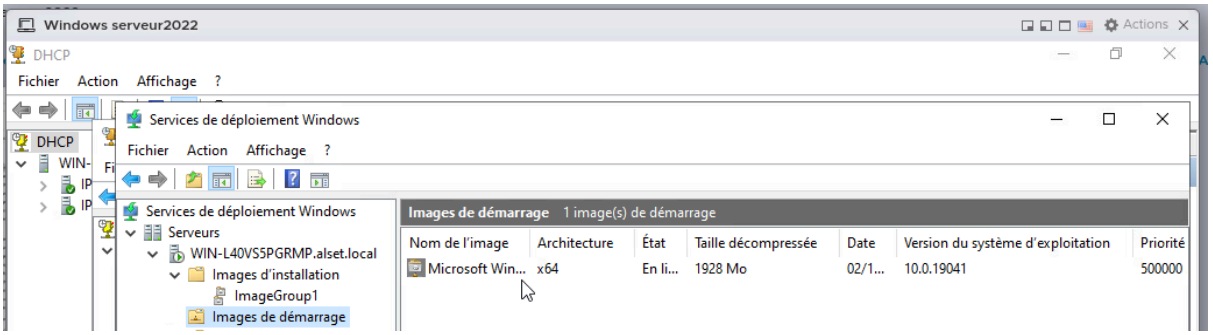
On a réalisé l'installation du service WDS sur le serveur Windows.



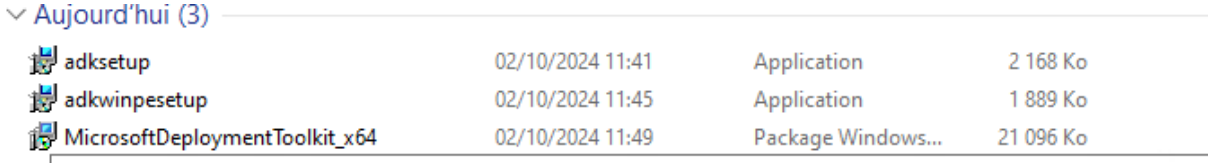


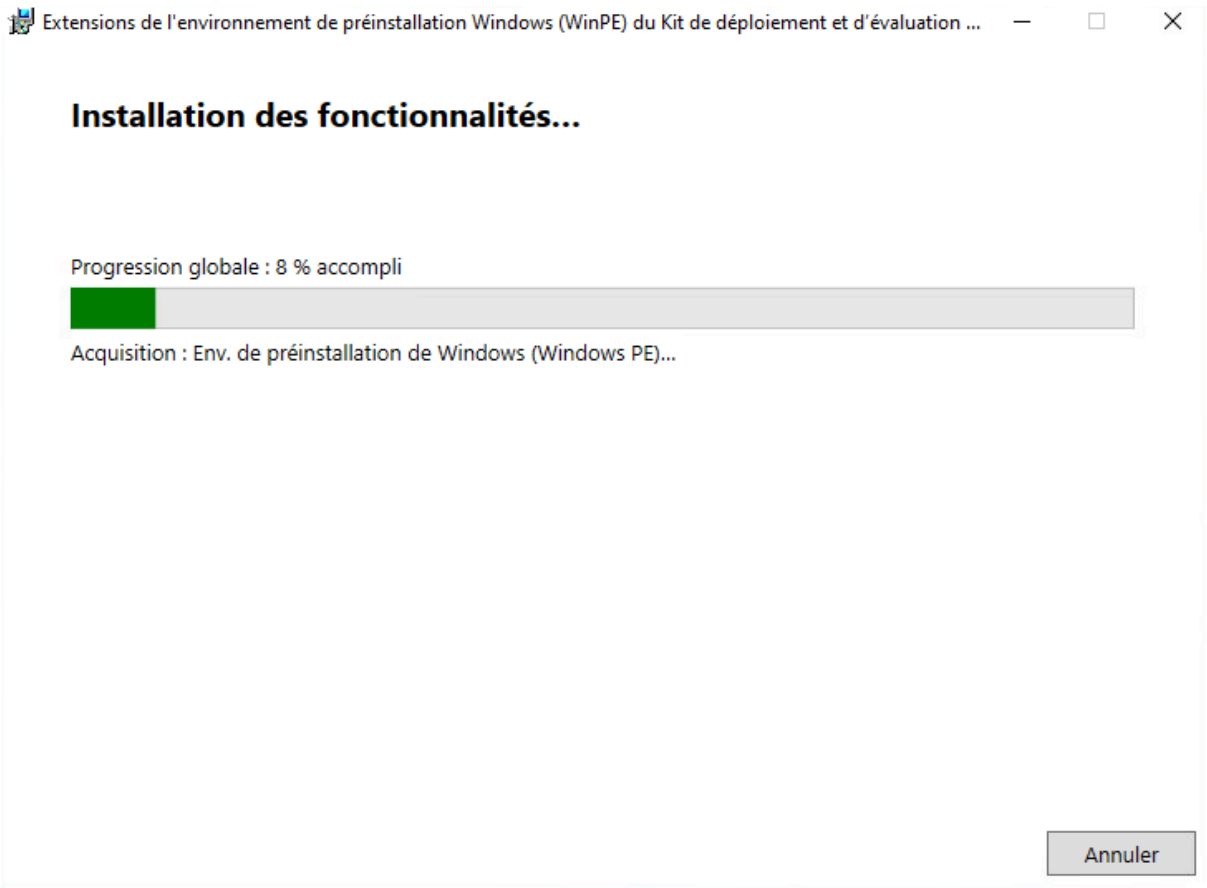
Ici, on sélectionne bien l'option “Serveur autonome” afin qu'il ne soit pas dépendant de l'Active Directory.

Mise en place des images de démarrage et d'installation :

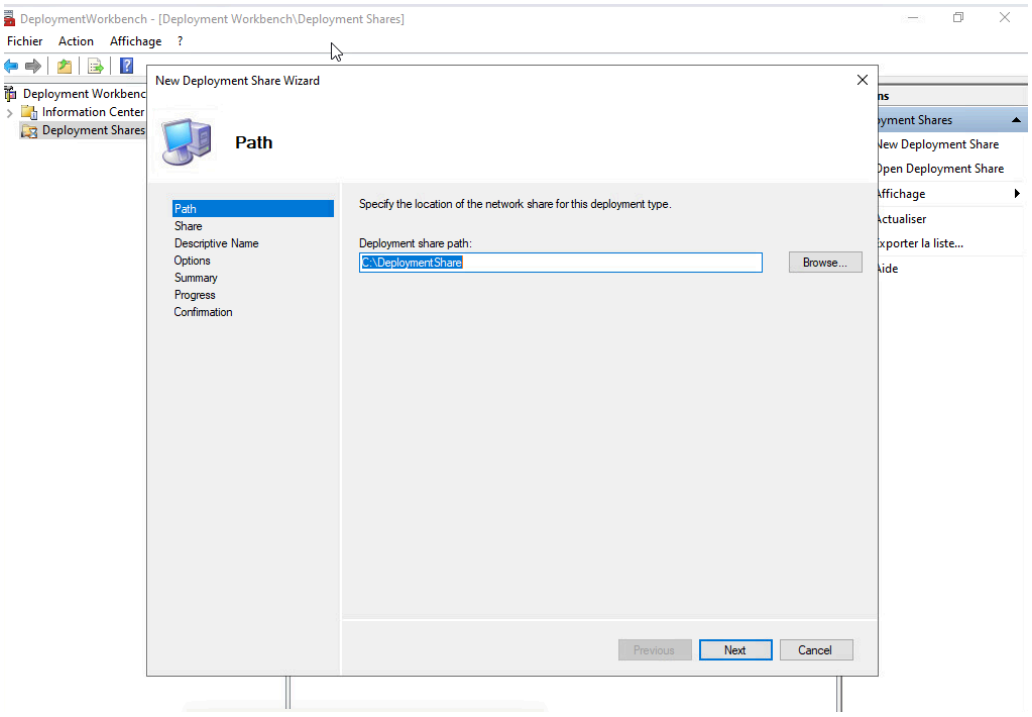


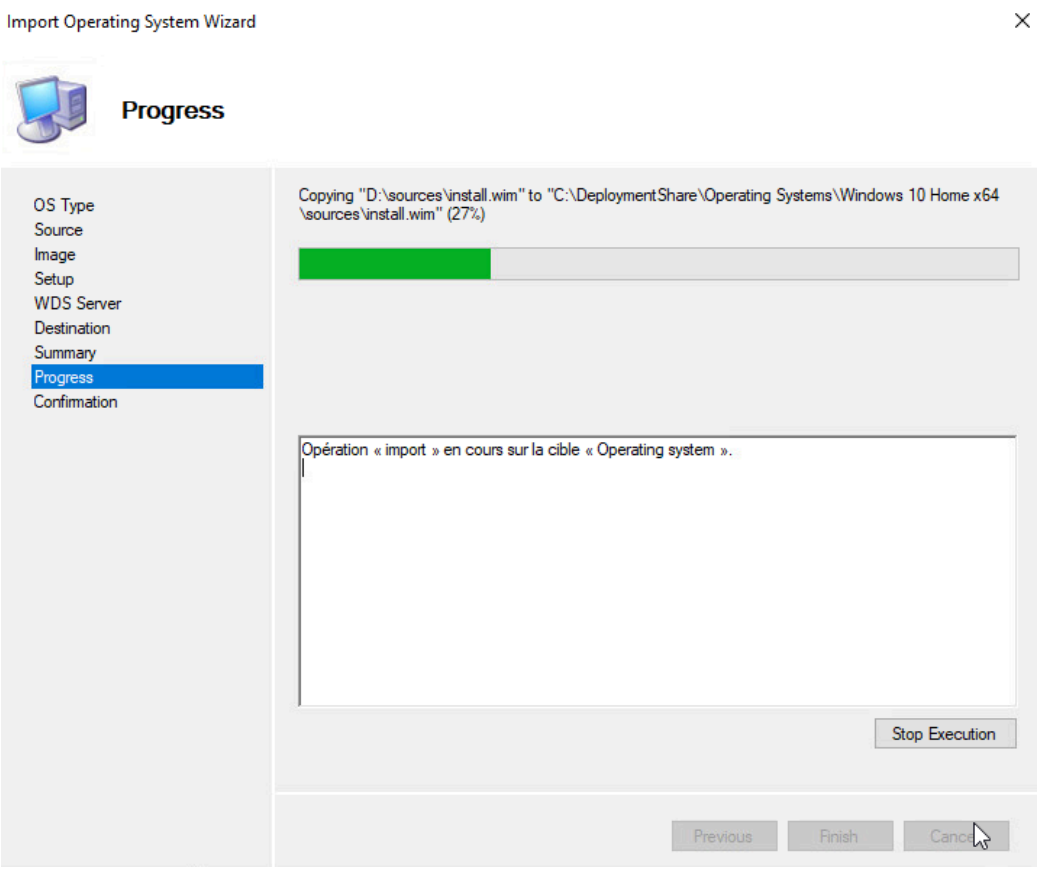
Installation du complément MDT et de ADK pour le déploiement d'un Windows 10 avec l'installation de CCleaner :



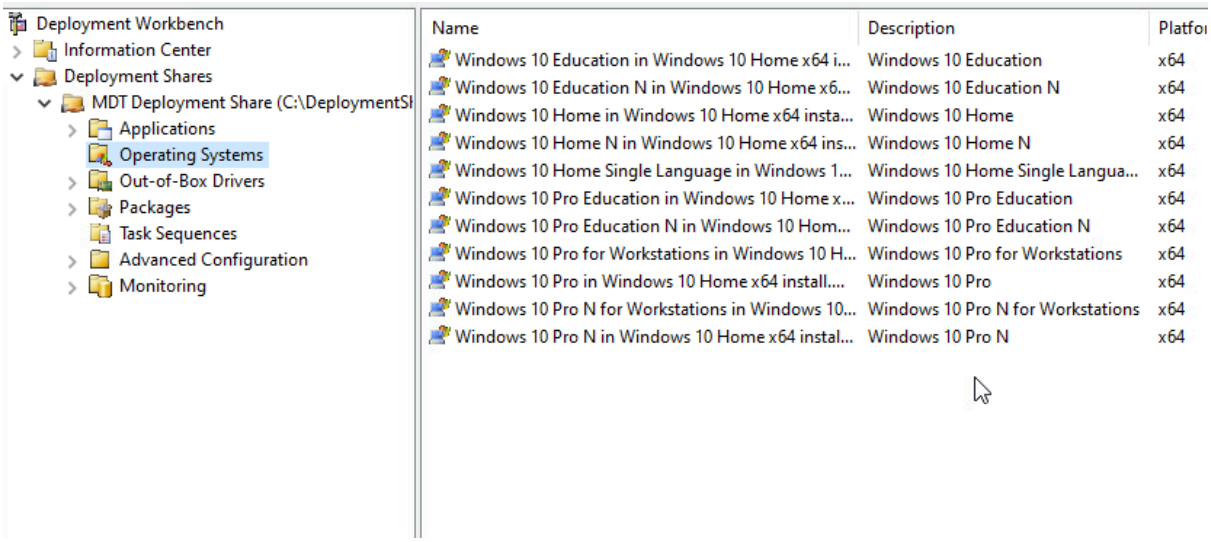


Ici, nous avons fait l'installation du complément MDT (Microsoft Deployment Tool) via le fichier exécutable d'installation de MDT.

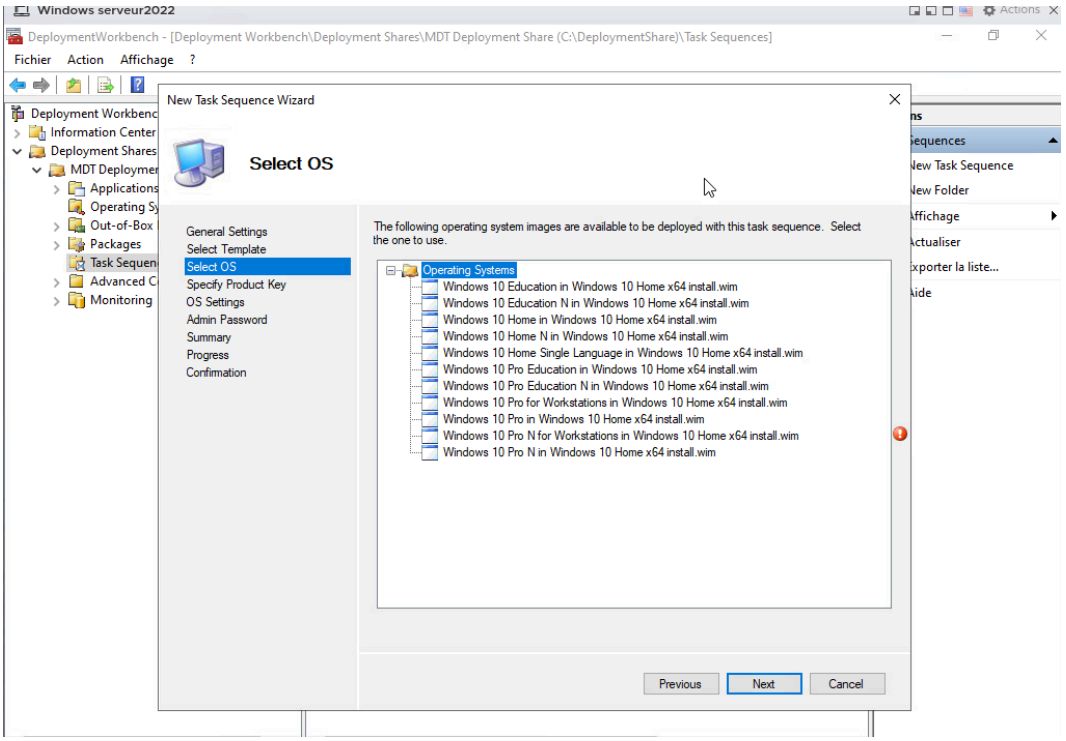




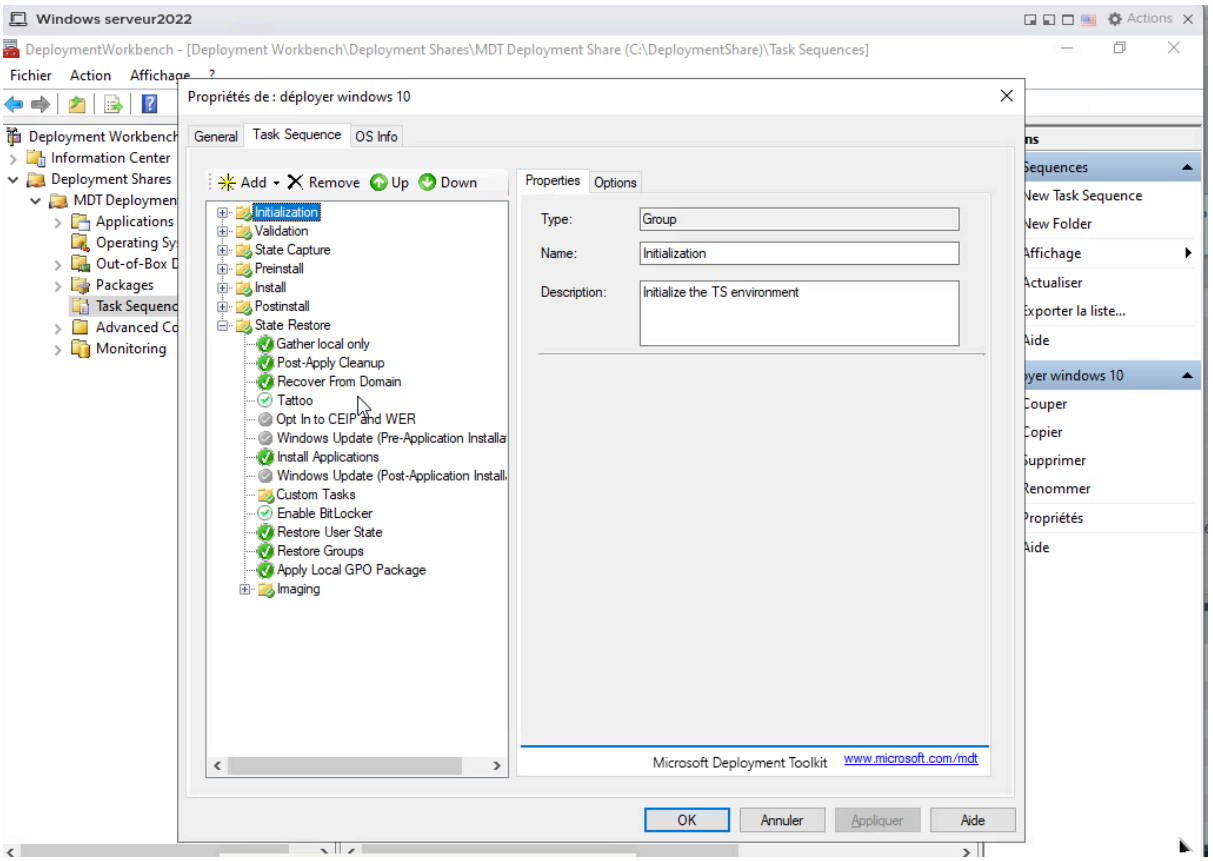
Ici, on va faire l'importation des OS dans le dossier "Operating Systems".



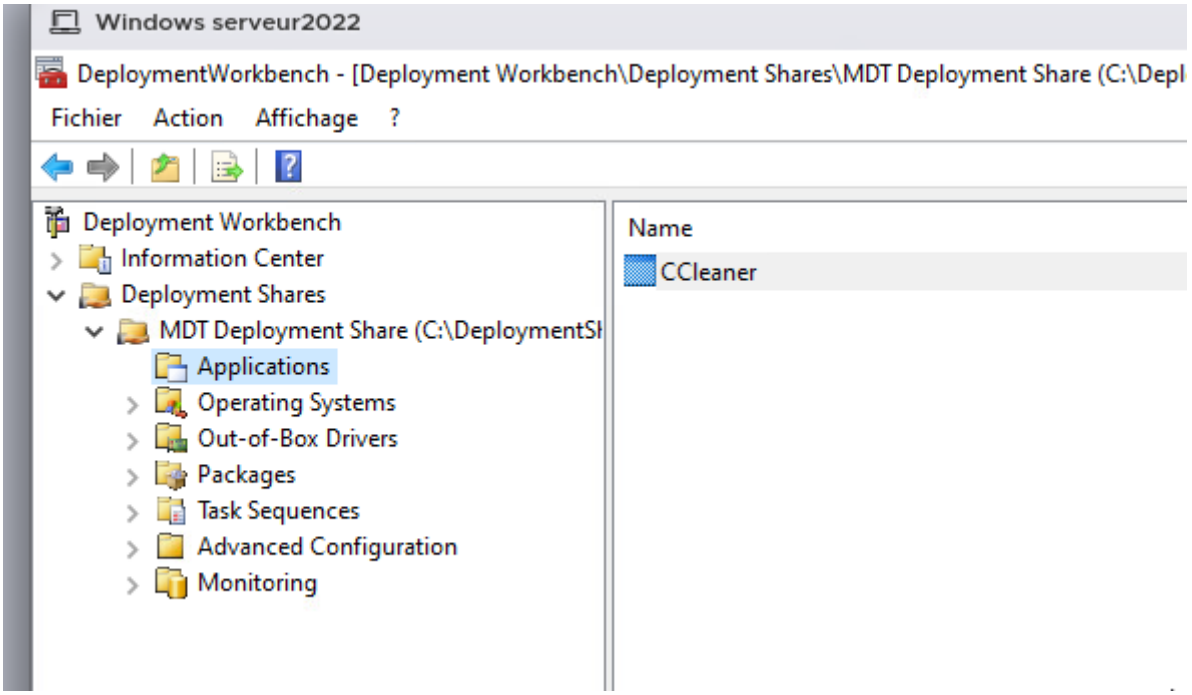
Ici, on a mis en place un workbench qui va permettre de faire des tâches de séquence de déploiement d'images iso ou de logiciels (comme CCleaner dans notre cas).



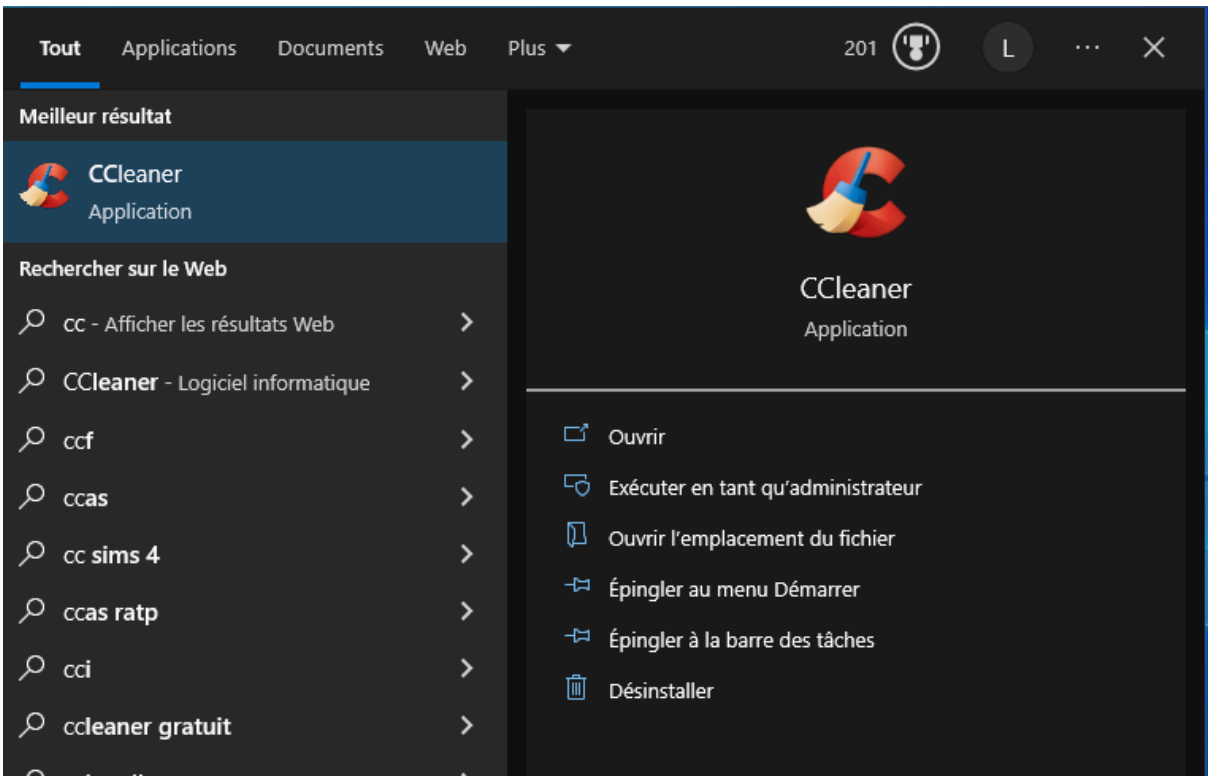
Le dossier “Operating Systems” va permettre de stocker les différents systèmes d’exploitation en image iso.



Voici la création d’un “Task Sequence” qui a pour but de déployer un Windows 10 Pro.



Ici, on a mis en place le logiciel CCleaner dans le dossier “Applications” avec le fichier exécutable du logiciel qui va s’installer quand il sera déployé sur le client.



Voici le résultat, on a bien déployé Windows 10 avec le logiciel CCleaner qui a été installé en arrière-plan pendant le déploiement.

Tableau des avantages et inconvénients de Windows Deployment Services :

Avantages	Inconvénients
Rapidité	Le temps entre le moment du démarrage et le chargement de l'image est d'environ 2 ou 3 minutes
Déploiement en masse facilité	Utilisation importante du réseau
Interface graphique	Le déploiement pour les images de types GNU/Linux et Mac OS X n'est pas possible
Possibilité d'apporter des modifications aux images créées	Augmentation coûts fixes relatifs au matériel (Achat Serveur)
Les images sont indépendantes du matériel	X
Automatisation complète possible au niveau des installations (XML)	X
Simplicité d'utilisation	X
Meilleur contrôle de la gestion de pilotes	X
Réduire les complexités liées aux déploiements matériels	X

Sources :

https://aydinet.fr/quest-ce-que-le-windows-deployment-services/

https://fr.wikipedia.org/wiki/Windows_Deployment_Services

Diagramme des tâches

https://docs.google.com/spreadsheets/d/1-feYv_8hors8d9_HRultEwm1s4Y_uZVFYC29Rq6S7Ac/edit?gid=1115838130#gid=1115838130

Conclusion

Pour conclure, ce TP nous a permis d'apprendre à travailler en équipe puisqu'il fallait se répartir les tâches avec l'aide d'un diagramme des tâches (diagramme de Gantt). Malgré les difficultés de communication, de compréhension dans l'équipe, nous sommes parvenus à réaliser les tâches entièrement. Nous avons appris à mettre en place Windows Server 2022, à introduire un serveur DHCP, à manipuler WDS avec le complément MDT et ADK et à créer des unités organisationnelles, groupes d'utilisateurs, dossiers partagés et GPOs (Lecteur réseau, blocage du changement de fond d'écran, etc…).