Théo Humbert

Réalisation N°1 – Infrastructure Système

Table des matières

Annexes

- Script utilisateurs PowerShell ;
- Script permissions PowerShell ;
- Vidéo de démonstration ;
- Maquette Cisco Packet Tracer ;
- Dossier contexte détaillé.

Contexte

Mise en situation :

En tant que technicien système et réseau opérant au sein de l'entreprise IT Services 86, l'un de nos clients TiersLieux86 nous contacte pour une raison urgente, car ils viennent de recevoir un nouveau client nommé ValorElec dont le siège a été détruit à la suite d'un incendie et vont devoir le relocalisé dans leur établissement afin que ValorElec puisse continuer son activité.

TiersLieux86 nous demande donc de préparer leur système d'information afin d'accueillir ce nouveau client.

Dans le mail, certaines directives sont communiqués, on sait que ValorElec n'a pas perdu ses données car elles sont répliquées sur d'autres sites, ils nous indiquent aussi que le siège comptait plusieurs services dont la Direction, le service commercial et celui chargé de la R&D, en tous ces services comptaient 20 personnes, qui vont être relocalisées sur le site de TiersLieux86, on nous informe que ces utilisateurs auront besoin d'une connexion internet pour travailler avec leur sites distants.

Mon responsable me confie donc la tâche d'agrandir et de préparer le système d'information de TiersLieux86 dans le but d'accueillir son nouveau client.

Contexte du client :

TiersLieux86 met à ma disposition un document comprenant des informations utiles au bon déroulement de ma mission notamment :

- L'implémentation des bâtiments sur site ;
- L'existant des actifs informatiques ;
- Des informations sur son activité ;
- L'organisation type du réseau informatique d'un de leur site d'ETP (d'Espace de Travail Partagé) ;
- Ainsi que des informations sur l'agencement du domaine active directory.

Dans ce compte rendu je ferais un court résumé du contexte du client en rappelant les informations essentielles, en annexe de ce document se trouve le dossier que le client a transmis afin de prendre connaissances de ces informations.

TiersLieux86, est une association régionale qui gère des Espaces de Travail Partagés (ETP) mis à disposition par des communes auprès de leurs administrés (entreprises et particuliers). Pour installer, déployer et administrer l'infrastructure informatique des espaces gérés par TiersLieux86, elle fait appel à des sociétés d'infogérance prestataires de services qui répondent à des appels d'offres.

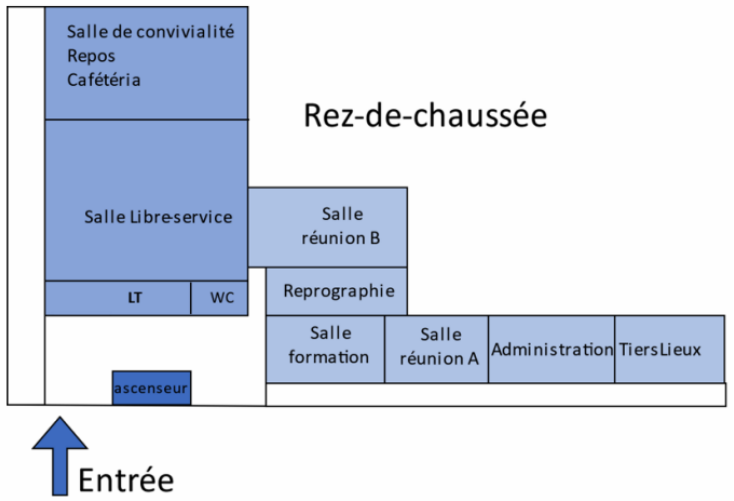
Prestations réalisées par TiersLieux86

Les services proposés par TiersLieux86 aux entreprises :

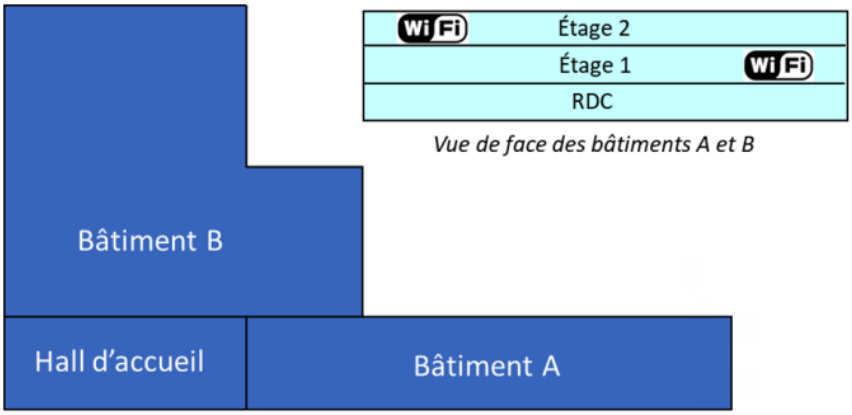
- Accès à internet ;
- Accès Wifi ;
- Téléphonie IP ;
- Impression et photocopie ;
- Salles de réunion et bureaux ;
- Gestion de parc informatique.

Implémentation des bâtiments

TiersLieux86 nous a même fournit un plan de leur bâtiment que voici :



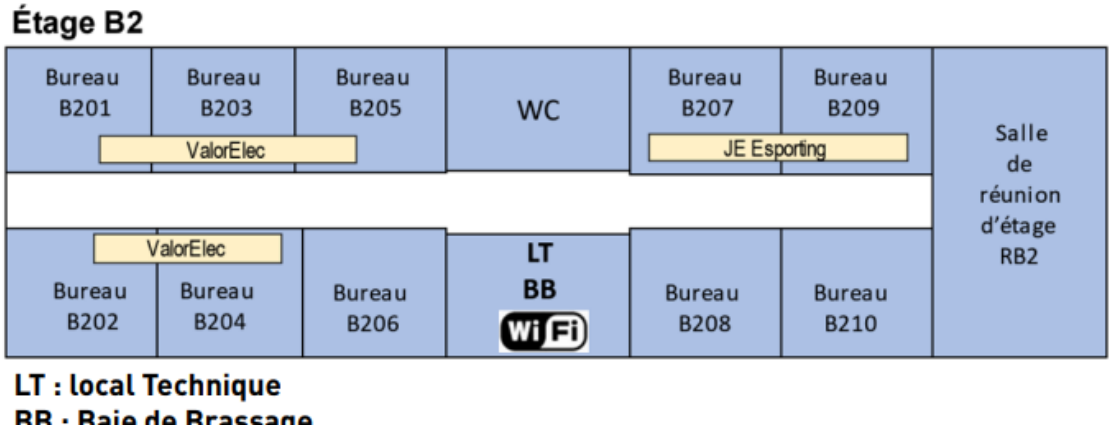
Ce bâtiment est divisé en deux : le bâtiment A et le bâtiment B sur 3 niveaux, tel que :



Vue de face des bâtiments A et B

Implantation des locaux en rez-de-chaussée des bâtiments A et B

Chaque étage est réparti de la manière suivante :



Equipements informatiques

Le site possède 5 points d'accès wifi dont 3 au rez de chaussée et 1 par étage.

Dans le bâtiment A, il y a une armoire de brassage à chaque étage, elles possèdent 22 prises Ethernet ainsi qu'un commutateur 24 ports RJ45 + 2 ports SFP

Pour le bâtiment B, une armoire se situe au premier étage, elle réunit 64 prises répartis équitablement entre les deux étages et comporte deux switch stackés dont tous les ports sont en gigabit.

Toutes ces armoires sont connectées à celle du RDC qui est la principale, en son sein sont regroupé l'accès a internet et l'accès de téléphonie IP. Elle est composée de 2 commutateurs 24 ports de niveau 3 stacké ainsi que d'un routeur.

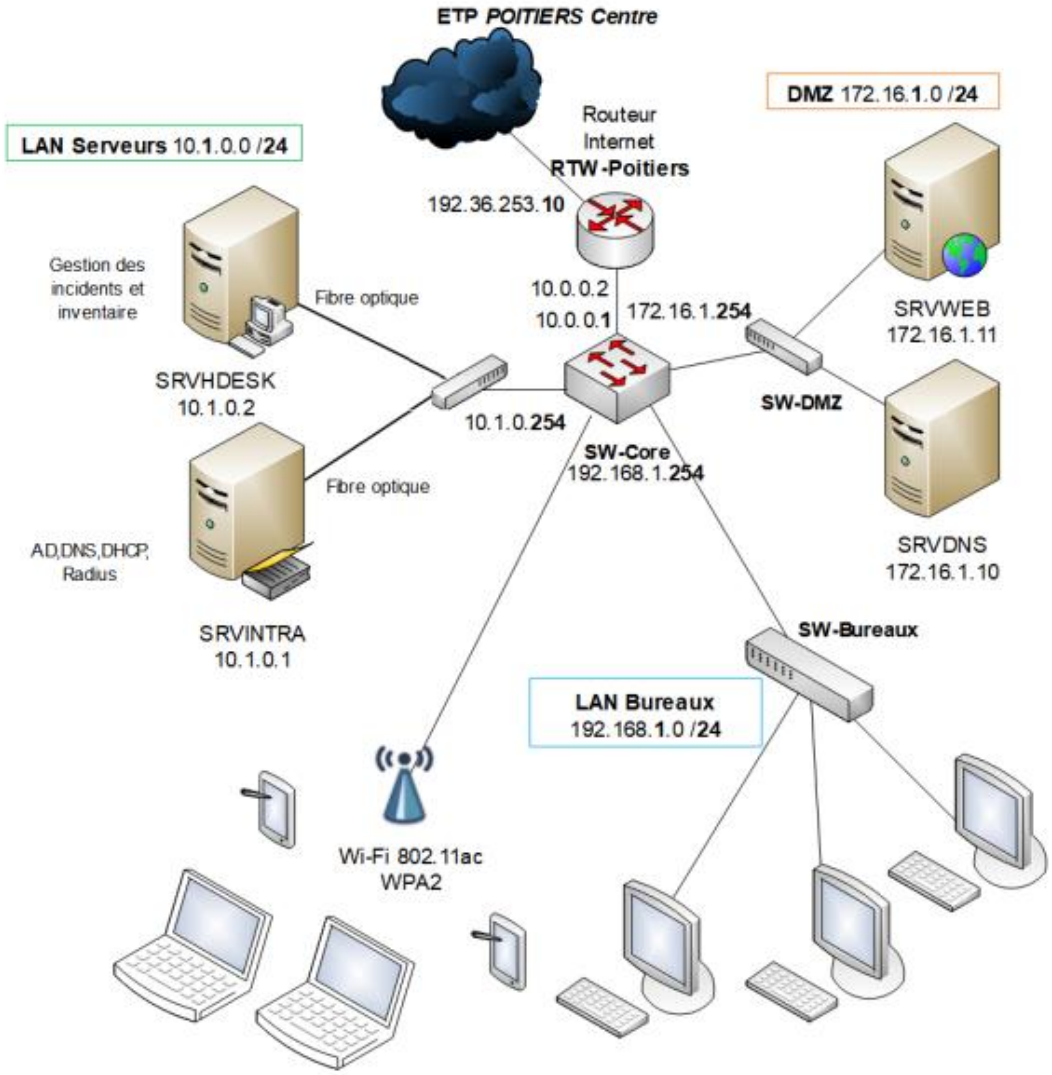
Plan d'adressage du site

Chaque entreprise accueillit se voit attribuer un chiffre, qui est intégré dans l'adressage de celle-ci, par exemple une entreprise se voit attribuer le chiffre **3** alors son réseau sera 172.17.1**3**.0/24, le fonctionnement pour les réseaux de réunion est similaire.

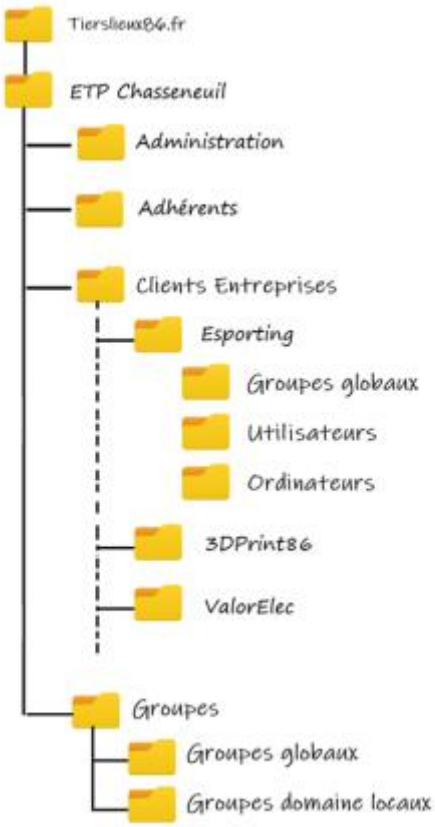
Plages réseaux		
RESEAU	ADRESSE	Vlan ID
Bureaux	192.168.2.0/24	2
Serveurs	10.2.0.0/24	10
WIFI	172.17.80.0/24	80
Entreprises	172.17.11.0 à 172.17.19.0/24	11 à 19
Réunion	172.17.21.0 à 172.17.29/24	21 à 29
DMZ	172.16.2.0/24	99
IP PUBLIQUE	192.36.253.20	

Serveurs		
NOM	ADRESSE IP	Vlan ID
AD/DNS/DHCP	10.2.0.1	10
NAS	10.2.0.2	10
DNS_WEB	172.16.2.3	99
SRV_WEB	172.16.2.1	99
SRV_MAIL	172.16.2.2	99

Schéma de l'infrastructure réseau de l'ETP Chasseneuil fourni par le client



Organisation actuelle de l'annuaire Active Directory de TiersLieux86



Objectifs

Déploiement de l'environnement

- Créer une maquette représentative du site ;
- Déployer un contrôleur de domaine Active directory, un routeur et un client ;
- Configurer le routage et segmenter en sous réseau en suivant le plan d'adressage ;
- Mettre en place le serveur DHCP sur le contrôleur de domaine et l'agent relais sur le routeur ;
- Configurer le domaine, créer les utilisateurs et les groupes selon les indications de TiersLieux86 ;
- Mettre en place un dossier partagé sur le contrôleur de domaine et configurer les autorisations.

Mission 1

- Modifier l'arborescence active directory pour accueillir ValorElec ;
- Automatiser à l'aide d'un script la création d'utilisateurs, de leur service et des groupes globaux en fonction d'un fichier CSV.

Mission 2

- Mettre en place une solution de partage de fichier ISCSI ;
- Etudier un système de partage de fichier DFS

Mission 3

- Définir les autorisations NTFS à mettre en place sur les partages ;
- Automatiser l'attribution des autorisations via un script PowerShell.

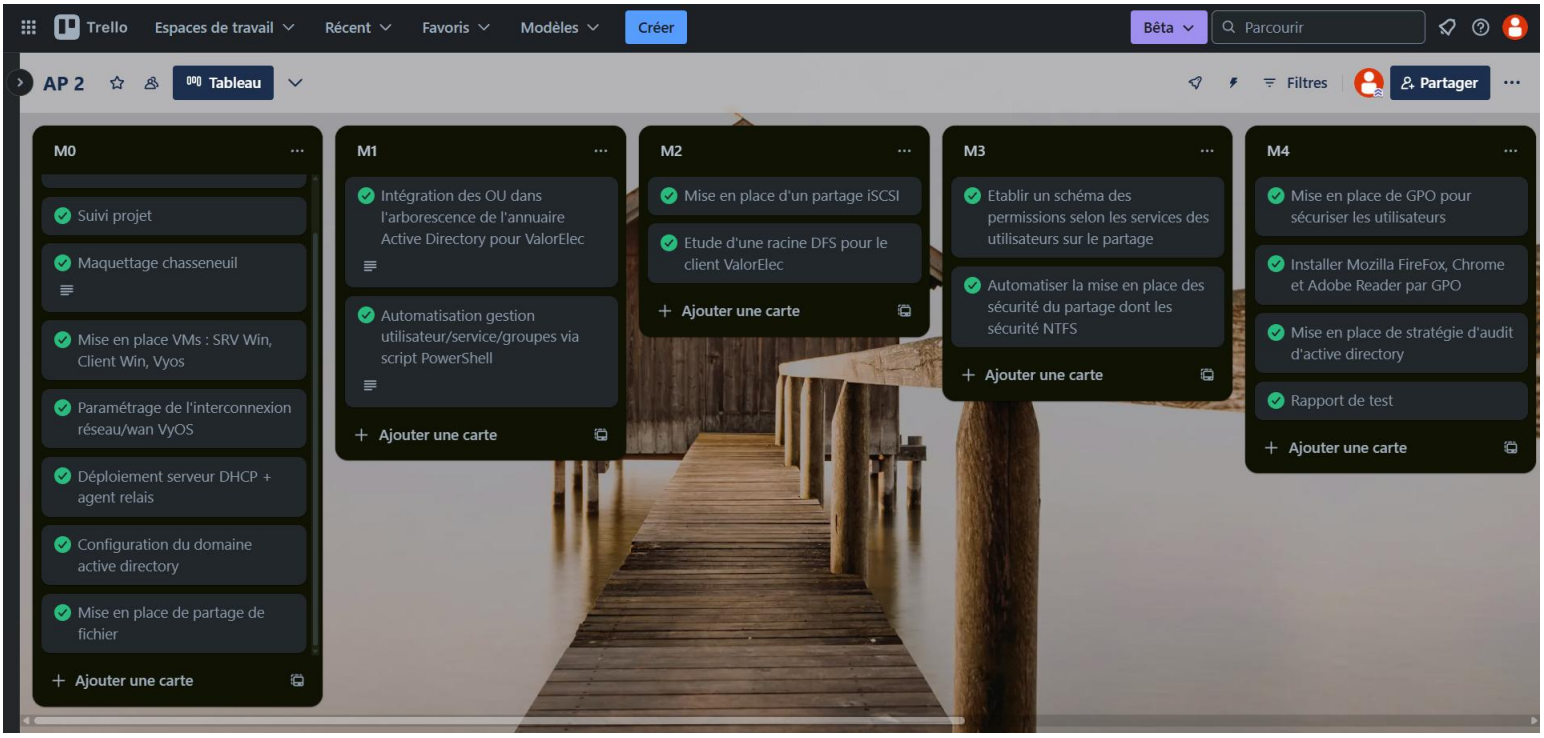
Mission 4

- Mise en place de l'installation automatique des logiciels demandés ;
- Déploiement des GPO portant sur la sécurité des postes (Mot de passe utilisateurs, interdiction d'accéder au panneau de configuration) ;
- Mise en place de stratégie d'audit lié à la journalisation d'évènement ;
- Réaliser un rapport de test sur la mise en place effectuée.

Suivi de projet

L'organisation des différentes étapes de réalisation de ce projet s'est faite sur un web service dénommé Trello, qui est accessible en ligne et permet d'avoir un tableau de bord des objectifs à court ou moyen terme de son projet.

Afin d'établir le suivi de mon projet j'ai tout d'abord divisé les différentes parties le composant, dans le but de me fixer de petits objectifs plus rapide et plus simple à réaliser, ensuite j'ai déterminé un ordre chronologique de réalisation de ces tâches puis tout au long de la production de ce projet je mettais à jour le suivis de tâches.



Mise en place de l'environnement

Objectif

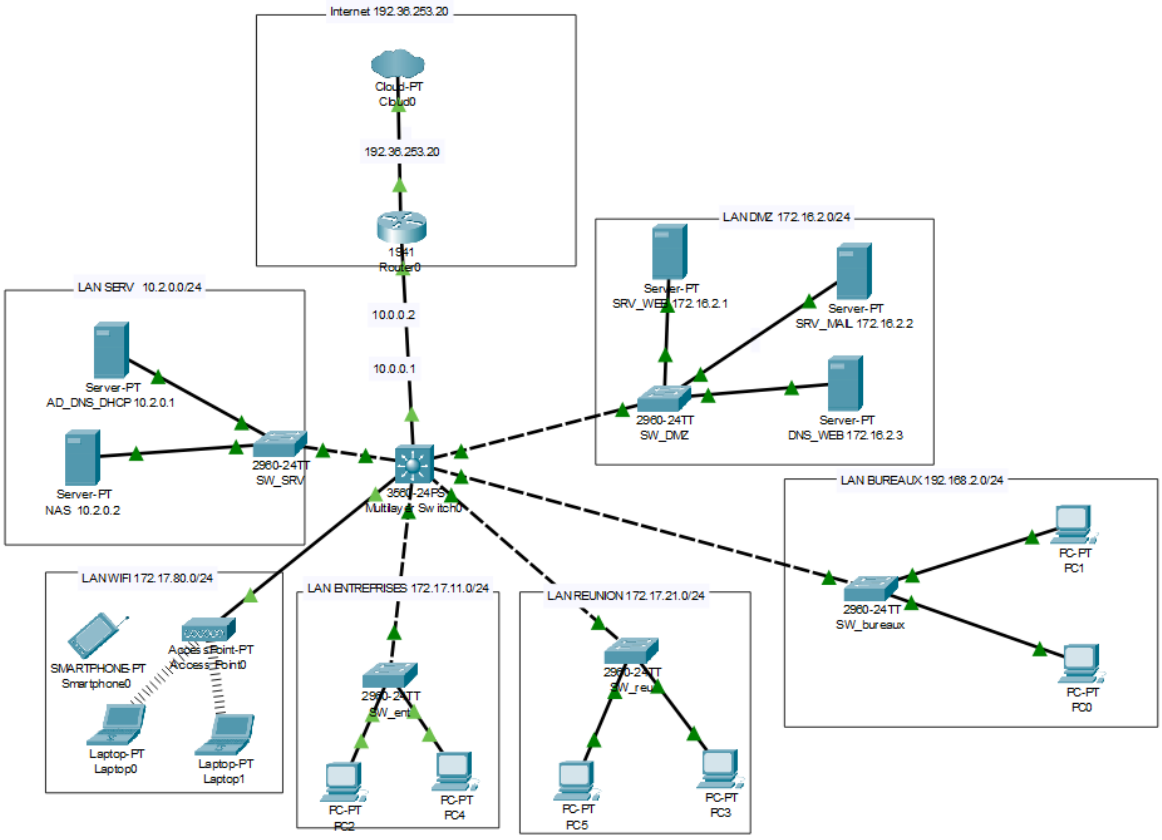
Mettre en place les bases de l'infrastructure système et réseau afin de la faire évoluer au long de ce projet.

Tâche 1 : Maquette de l'architecture

Cette tâche consiste à mettre en place une simulation du réseau de l'ETP Chasseneuil, afin de pouvoir visionner avec du recul l'infrastructure. De plus cette maquette nous accompagnera pour les prochaines réalisations à venir.

Elle comprend notamment la mise en place des VLANs, le routage de ces derniers ainsi que celui jusqu'au routeur passerelle, un point d'accès wifi et la représentation des différents réseaux.

Voici un aperçu de la maquette :



Le fichier packet tracer est disponible sur mon portfolio ou à cette adresse :

https://drive.google.com/file/d/1xOJWETPEdP-Y_O1syUwb8jayzBiKM8LI/view?usp=drive_link/

Tâche 2 : Déploiement des machines virtuelles

Sur mon PC hôte, grâce au logiciel VMWare Workstation Pro dans sa version 17 je vais installer plusieurs machines :

- Un serveur Windows 2022 avec les roles de : DNS, active directory et de serveur DHCP ;
    - Avec les ressources matérielles suivante : 8Gb de ram 4 Core de CPU, 50Go d'espace disque ;
- Un client windows 11 ;
    - Avec : 4Gb de RAM, 2 Core, 40Go d'espace disque ;
- Un routeur virtuel VyOS 1.4 ;
    - Avec : 724 Mb de RAM, 2 Core, 5 Go d'espace disque.

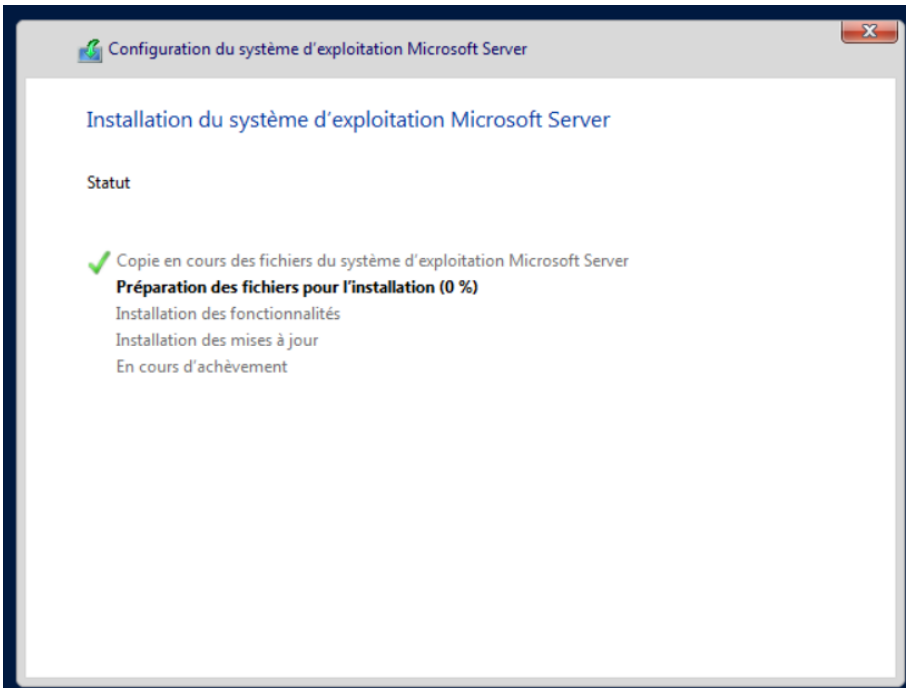
Sur le routeur 4 interfaces réseaux sont actives, une interface WAN permettant l'accès a internet, une interface sur le réseau des bureaux, une pour la DMZ et une dernière pour le réseau des serveurs.

L'adressage IP est fait en fonction du plan établie dans la documentation du contexte, mais voici un récapitulatif du plan a notre échelle :

Réseau	Adresses	Interface Routeur
WAN	192.36.253.20	ETH0
Bureaux	192.168.2.0/24	ETH1
DMZ	172.16.2.0/24	ETH2
SRV	10.2.0.0/24	ETH3

Machine	Nom d'hôte	Adresses
Windows Serveur	AD-DNS-DHCP Domaine : ap.local	10.2.0.1
Client windows	PC1	DHCP
Routeur VyOS	Vyos	10.2.0.254 192.168.2.254 172.16.2.254 Bridge WAN

Dans un premier temps on installe le serveur Windows ainsi que la machine cliente sous Windows qui se font toutes les deux de manière classique.



A l'issue de celles-ci, il faut configurer le Windows serveur, plus précisément :

- Créer un compte d'administration local ;
    - Qui se nommera : Administrateur ;

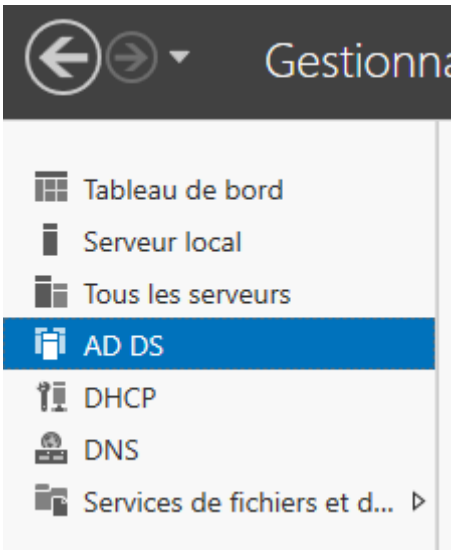
- Lui donner un nom d'hôte ;

```
C:\Users\Administrateur>hostname
AD-DNS-DHCP
```

- Une configuration IP ;

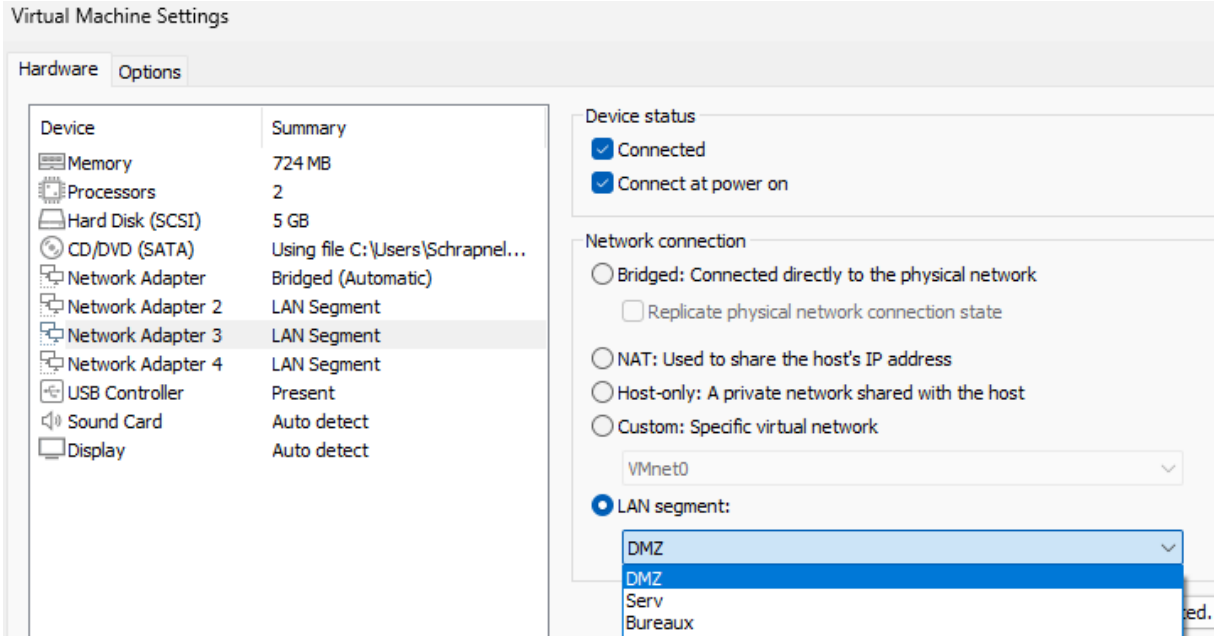
```
Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . .: fe80::3e99:25d:64ae:c09a%13
Adresse IPv4. . . . . . . . . . . . . .: 10.2.0.1
Masque de sous-réseau. . . . . . . . . : 255.255.255.0
Passerelle par défaut. . . . . . . . . : 10.2.0.254
```

- Lui installer le rôle de serveurs DNS,DHCP et le service AD DS afin que ce serveur passe de simple machine virtuelle à contrôleur de domaine ici le nom de domaine sera ap.local.



Tâche 3 : Configuration VyOS

Préalablement il faut dans un premier temps installé l'OS de VyOS qui ressemble a une installation linux classique, ensuite il faut créer les interfaces dans le logiciel hyperviseur, ici VMWARE de façon à obtenir les sous réseaux de notre plan d'adressage, il faut bien spécifier que nous voulons créer des segments LAN :



Puis il faut ajouter 4 interfaces réseaux à notre routeur, et leurs attribuer le segment LAN adéquat. La dernière interface sera configurée soit en mode Bridge (pont) ou en mode NAT afin d'obtenir une connexion WAN vers internet.

Une fois VyOS installé et ses cartes réseaux attribuées, on peut commencer à paramétrer la partie software du routeur, pour cela il suffit d'attribuer une configuration IP à chaque interface grâce à cette commande :

#set interfaces ethernet nom_interfaces address "IP/MASQUE"

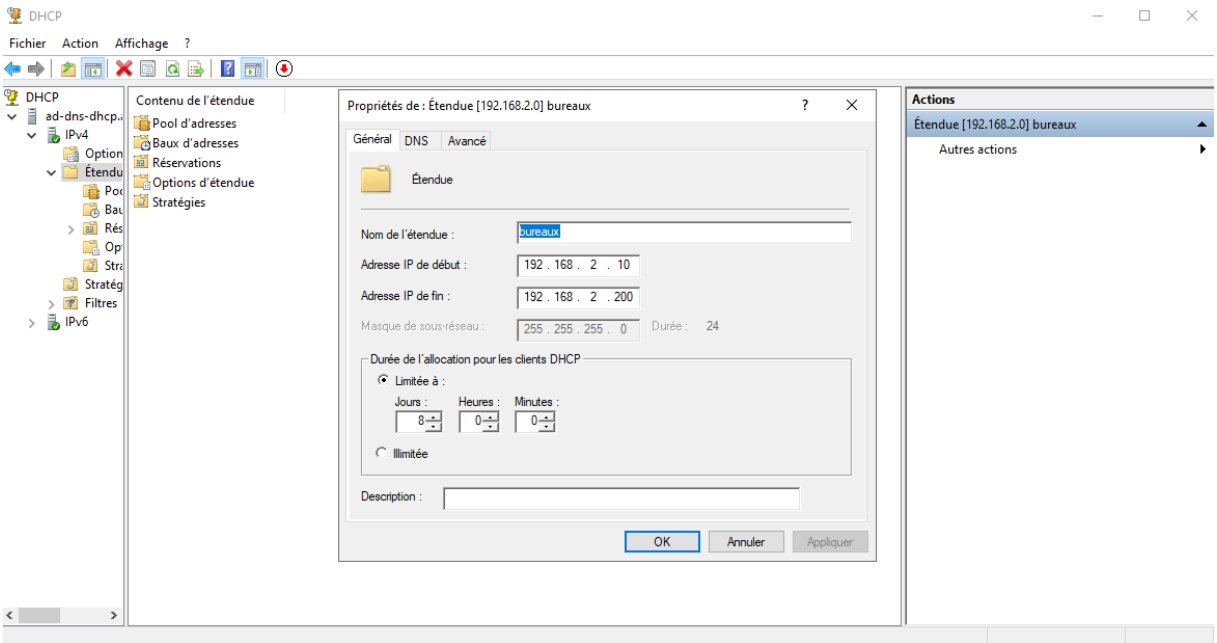
Cette configuration correspond à l'adressage de la passerelle de chaque réseau

```
Interface    IP Address          MAC                VRF        MTU  S/L    Descrip
tion
-----------  ------------------  -----------------  -------  -----  -----  -------
------
eth0         -                   00:50:56:24:1a:60  default   1500  u/u    WAN
eth1         192.168.2.254/24    00:50:56:25:52:68  default   1500  u/u    LAN_BUR
eth2         172.16.2.254/24     00:50:56:2d:4f:52  default   1500  u/u    DMZ
eth3         10.2.0.254/24       00:50:56:23:e5:b0  default   1500  u/u    SERV
lo           127.0.0.1/8         00:00:00:00:00:00  default  65536  u/u
```

Tâche 4 : DHCP

Désormais le serveur DHCP est déjà installé sur notre contrôleur domaine, il reste plus qu'a configurer les plages de distribution DHCP ainsi que le relais DHCP sur le routeur.

Voici les paramètres de l'étendu DHCP, il faut bien préciser la passerelle du routeur lors de la création ici : 192.168.2.254 pour que le serveur soit a l'écoute sur les paquets en provenance de ce réseau mais aussi pour qu'il sache vers ou envoyé les réponses.



Ensuite il ne reste plus qu'a configurer l'agent relais sur le routeur de cette façon :

1. Saisir la ou les interfaces d'écoute DHCP (donc les réseaux clients) :
   #set service dhcp-relay listen-interface eth1
2. Puis l'interface d'envoie (le réseau serveur) :
   #set service dhcp-relay upstream-interface eth3
3. Et définir l'adresse du serveur DHCP :
   # set service dhcp-relay server 10.2.0.1

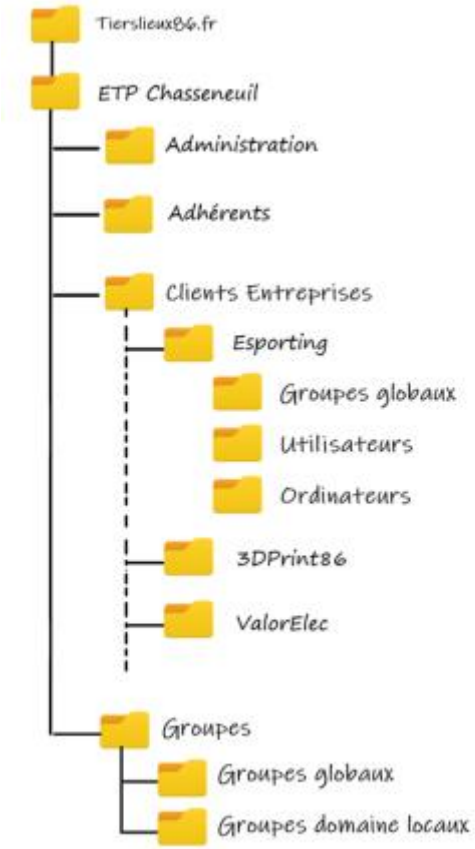
On fait un show service dhcp-relay :

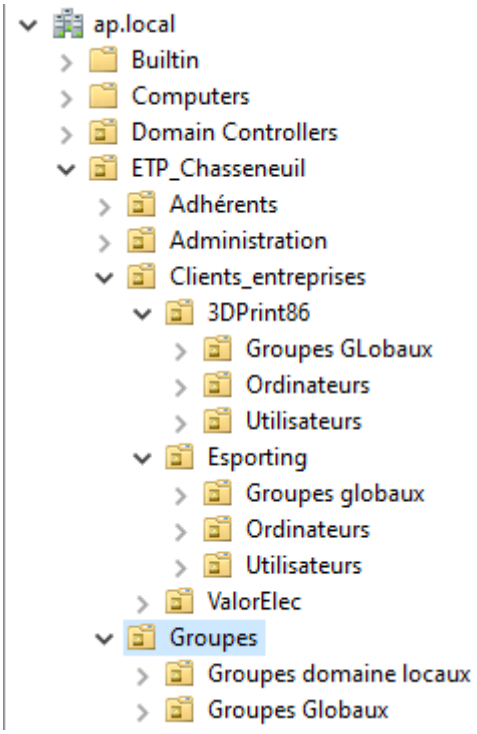
```
vyos@vyos# sh service dhcp-relay
 listen-interface eth1
 server 10.2.0.1
 upstream-interface eth3
```

Le routeur est configuré comme souhaité.

Tâche 5 : Annuaire Active Directory

Ici il suffit d'appliquer le schéma organisationnel de l'active directory fournit par le client sur notre infrastructure :



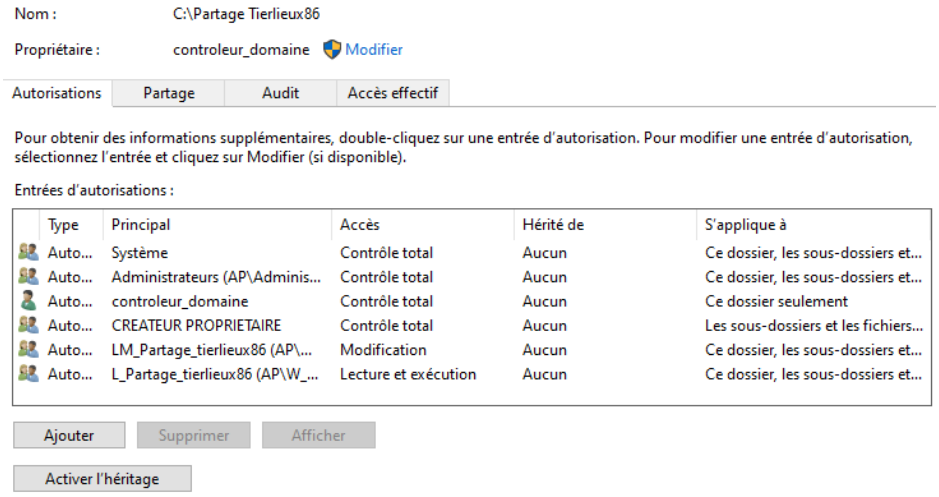


Tâche 6 : Partage de fichiers

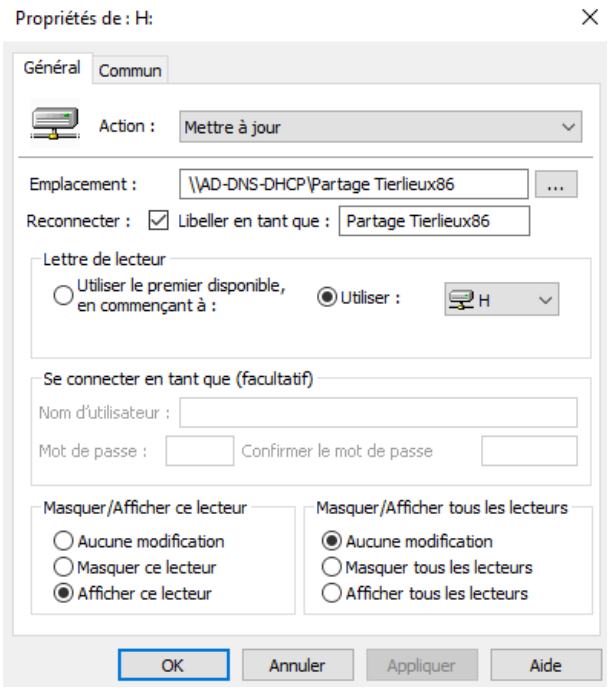
Afin que les utilisateurs puissent accéder a différent dossier de manière rapide, il faut mettre à leur disposition un partage de fichiers.

Pour cela il a fallu :

1. Créer un dossier ;
2. Activer le partage sur celui-ci ;
3. Donner les autorisations NTFS nécessaire aux personnes selon leurs statuts et leurs rôles ;



4. Créer une GPO afin de mapper automatiquement un lecteur réseau a la connexion de l'utilisateur puis la lier un OU.



Tâche 7 : Rapport de test

Dans cette partie on procèdera aux différents tests afin de vérifier si tout ce que l'on a mit en place est fonctionnel.

Connectivité

Vérification de la communication entre les machines virtuelles grâce à des pings.

PC1 > Contrôleur de domaine :

```
C:\Users\admin.AP.000>ping 10.2.0.1

Envoi d'une requête 'Ping'  10.2.0.1 avec 32 octets de données :
Réponse de 10.2.0.1 : octets=32 temps<1ms TTL=127
Réponse de 10.2.0.1 : octets=32 temps=3 ms TTL=127
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
```

Contrôleur de domaine > PC1 :

```
C:\Users\Administrateur>ping 192.168.2.10

Envoi d'une requête 'Ping'  192.168.2.10 avec 32 octets de données :
Réponse de 192.168.2.10 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.2.10 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.2.10 : octets=32 temps<1ms TTL=127
Réponse de 192.168.2.10 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 192.168.2.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 3ms, Moyenne = 1ms
```

Puis du contrôleur de domaine vers les différentes passerelles :

Passerelle serveur :

```
C:\Users\Administrateur>ping 10.2.0.254

Envoi d'une requête 'Ping'  10.2.0.254 avec 32 octets de données :
Réponse de 10.2.0.254 : octets=32 temps<1ms TTL=64
Réponse de 10.2.0.254 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.2.0.254:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Passerelle Bureaux :

```
C:\Users\Administrateur>ping 192.168.2.254

Envoi d'une requête 'Ping'  192.168.2.254 avec 32 octets de données
Réponse de 192.168.2.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.2.254 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.2.254:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Passerelle DMZ :

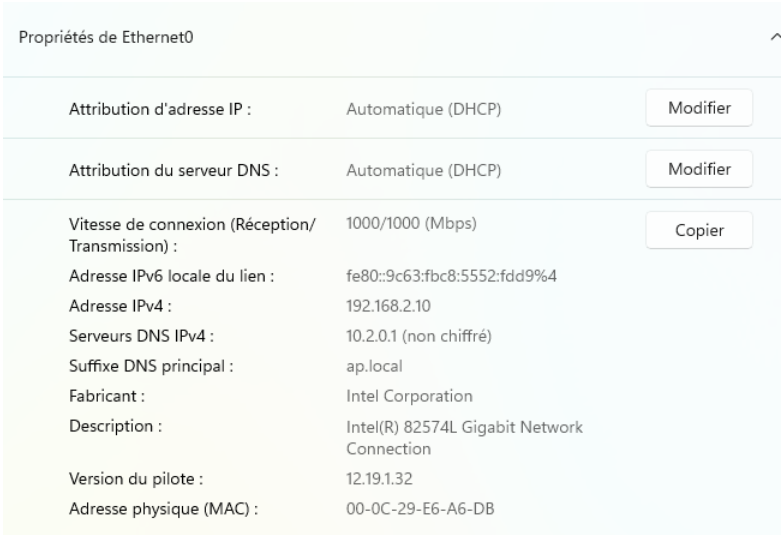
```
C:\Users\Administrateur>ping 172.16.2.254

Envoi d'une requête 'Ping'  172.16.2.254 avec 32 octets de données :
Réponse de 172.16.2.254 : octets=32 temps<1ms TTL=64
Réponse de 172.16.2.254 : octets=32 temps<1ms TTL=64
Réponse de 172.16.2.254 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.16.2.254:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Connexion internet :

```
C:\Users\admin.AP.000>ping www.google.com

Envoi d'une requête 'ping' sur www.google.com [172.217.19.132] avec 32 octets de données :
Réponse de 172.217.19.132 : octets=32 temps=9 ms TTL=127
Réponse de 172.217.19.132 : octets=32 temps=16 ms TTL=127
Réponse de 172.217.19.132 : octets=32 temps=10 ms TTL=127
Réponse de 172.217.19.132 : octets=32 temps=8 ms TTL=127

Statistiques Ping pour 172.217.19.132:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 8ms, Maximum = 16ms, Moyenne = 10ms
```

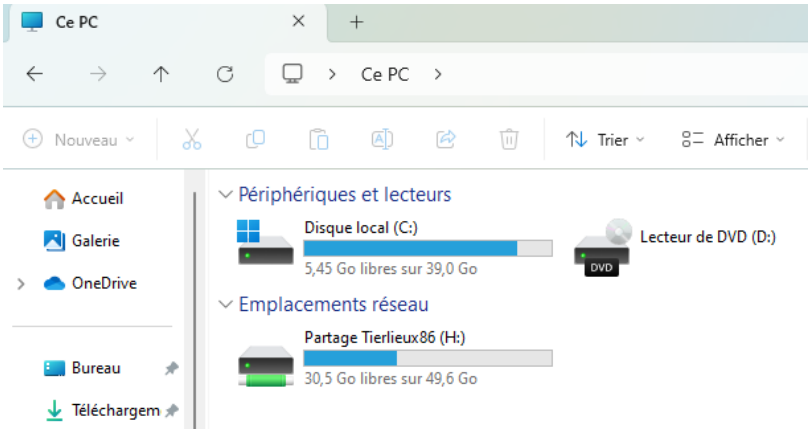
DHCP

Pour vérifier la configuration DHCP il suffit modifier les paramètres d'un client aifn de voir si il se voit attribuer une configuration IP :



Partage de fichier

En se connectant sur le client avec un compte active directory disposant des droits d'accès au partage créer on peut s'apercevoir que le partage est bien présent :



Bilan

Désormais les fonctions basiques de notre infrastructure sont en place, notre infrastructure propose un annuaire d'organisation, un serveur DNS, un contrôleur de domaine, un serveur DHCP ainsi que les relais nécessaires, un routage inter réseau, une connexion internet et un partage de fichier.

Nous allons pouvoir améliorer ce prototype en y ajoutant maintes fonctionnalités.

Mission 1

Objectif

Préparer l'architecture Active Directory afin d'accueillir ValorElec puis automatiser ces tâches grâce à un script PowerShell.

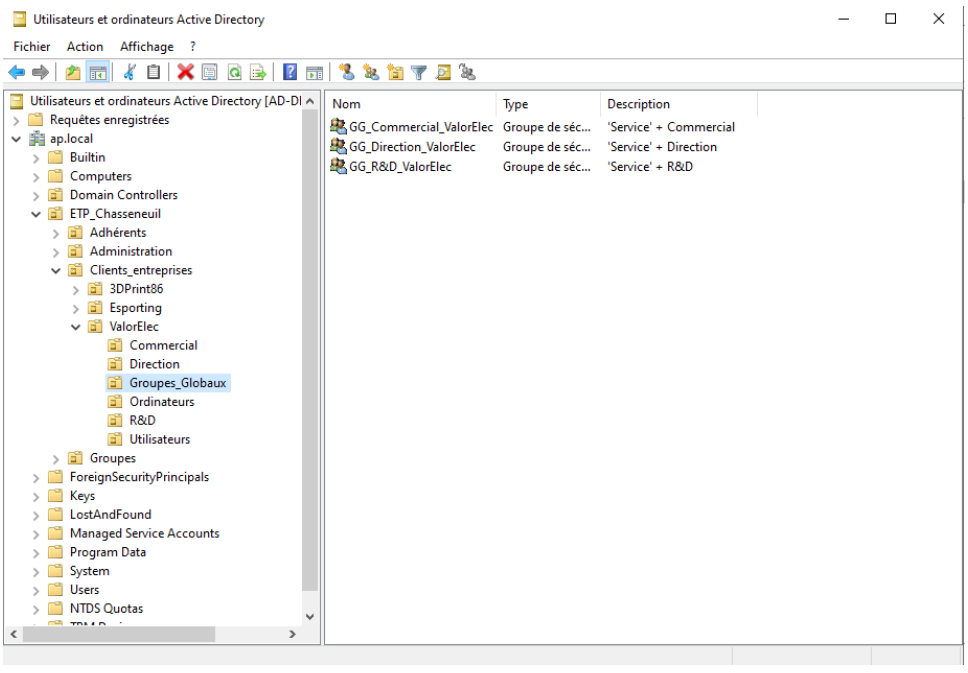
Tâche 1 : Evolution de l'arborescence Active Directory

L'organisation de l'entreprise au sein de l'annuaire du contrôleur de domaine sera organisé comme suit :

- OU Commercial
  - Employés commerciaux
- OU Direction
  - Employés direction
- OU R&D
  - Employés R&D

Dans l'OU « Groupe_Globaux » se situeront les Groupes de sécurité global en fonction du service concerné, cela en suivant la pratique AGDLP pour Account > Global > Domain Local > Permissions.

Les utilisateurs seront répartis en fonction de leur service dans les OU correspondantes.



Tâche 2 : Automatisation de l'administration AD via PowerShell

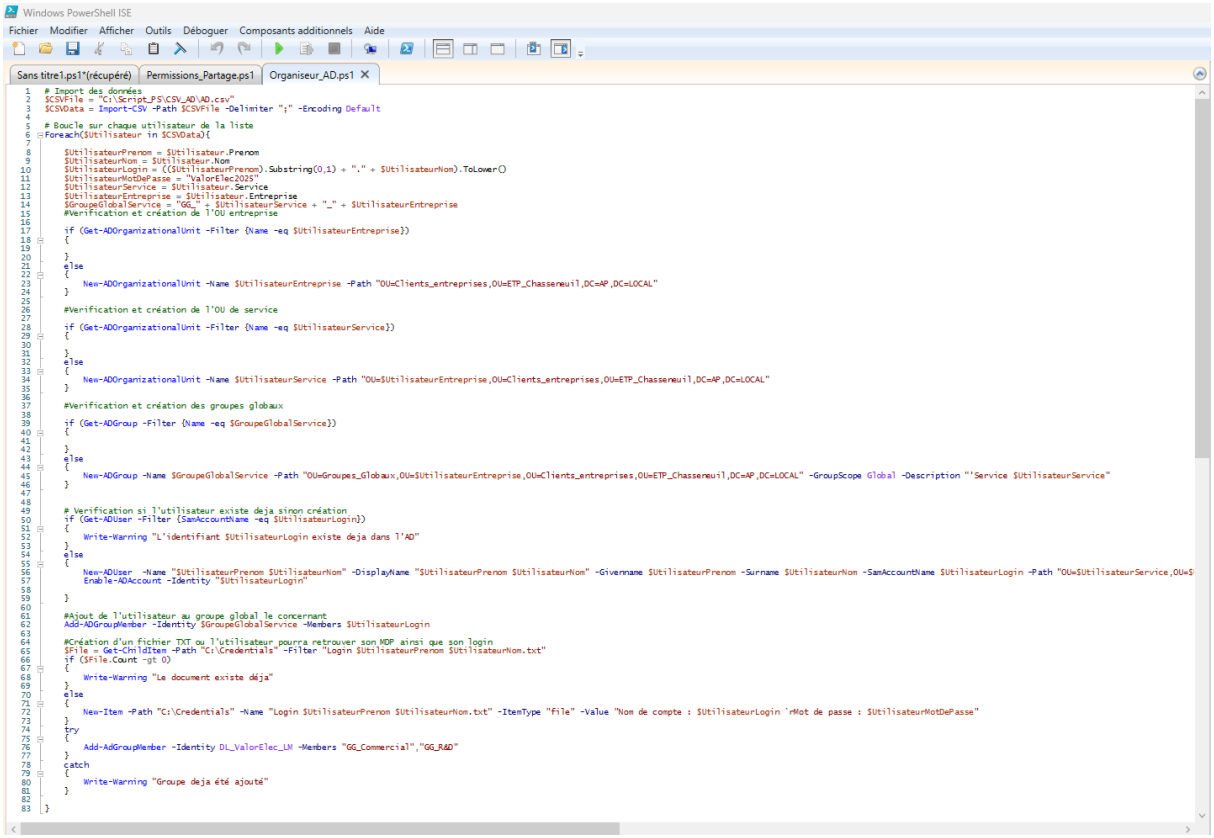
Le script est écrit en PowerShell, il nécessite en entrer un document « .csv » lui indiquant les informations suivantes : nom, prénom, services et entreprise de l'utilisateur.

Ensuite il créer tout en vérifiant l'existence une OU du service ainsi que de l'entreprise de l'utilisateur.

Puis il créer un groupe de sécurité global propre au service et a l'entreprise de l'utilisateur.

Et pour finir il créer l'utilisateur en l'ajoutant dans les OU et Groupes concernés en lui attribuant un mot de passe par défaut avec un changement automatique a la première connexion et met les combos login/mot de passe dans un document texte au nom et prénom de l'employé.

Une version plus « lisible » est disponible en téléchargement sur mon portfolio.



En partant de ce modèle il est possible de rendre ce script bien plus performant en investissant plus de temps.

Mission 2

Objectif

Mise en place d'un serveur de fichiers iSCSI et étude d'une racine DFS.

Tâche 1 : Partage iSCSI

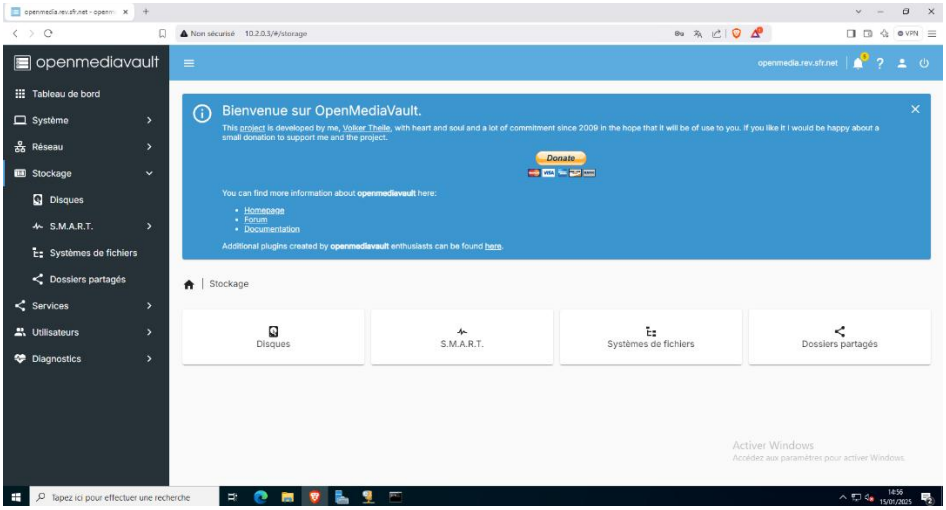
Je me suis orienté vers OpenMediaVault qui est une solution open sources avec beaucoup de documentation, une grande polyvalence en termes de plugins et possède une communauté assez étendue.

(De plus cet OS est plus simple a utiliser mais cela reste subjectif)

Je créer une VM avec deux disque virtuel un pour le système d'OMV et un autre pour le partage.

Il suffit de télécharger l'ISO, de réaliser l'installation en paramétrant correctement les options de réseau et si nécessaire ne pas hésiter à configurer manuellement dans /etc/networks/interface.conf.

À la suite de cela on peut accéder à l'interface d'administration web de l'application via l'adresse IP du serveur.



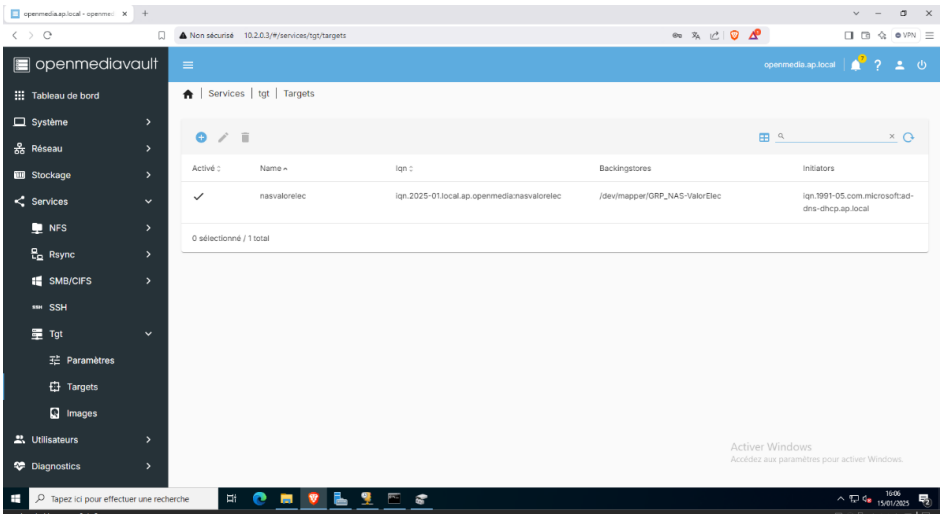
Ensuite je change le mot de passe par défaut de l'utilisateur admin.

OMV ne gère pas de façon native les partages iSCSI il faut donc installer deux plugins qui pourront gérer le format iSCSI :

- « Openmediavaultlvm »
- « Openmediavault-tgt »

On créer donc un volume physique de notre disque que l'on met dans un groupe de volume qui se nomme : « GRP_NAS »

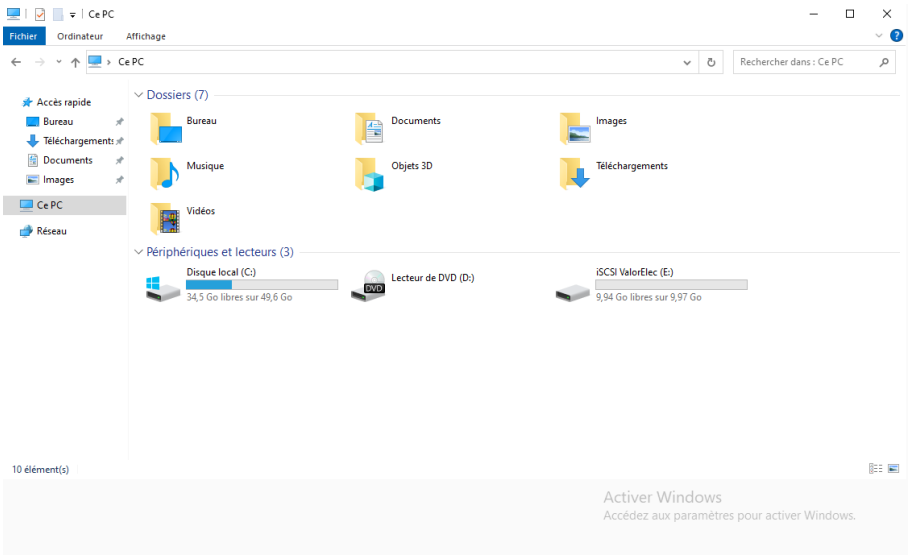
Puis à partir de ce groupe de volumes on créer un volume logique qui s'appellera « valorelec ».



On crée la target, on récupère l'adresse de l'initiator iSCSI du contrôleur de domaine, on mappe le volume ISCI et on enregistre.

De retour sur le contrôleur de domaine on ajoute notre cible iSCSI puis on initialise le disque et on le formate.

Voilà notre partage iSCSI est prêt à être utilisé



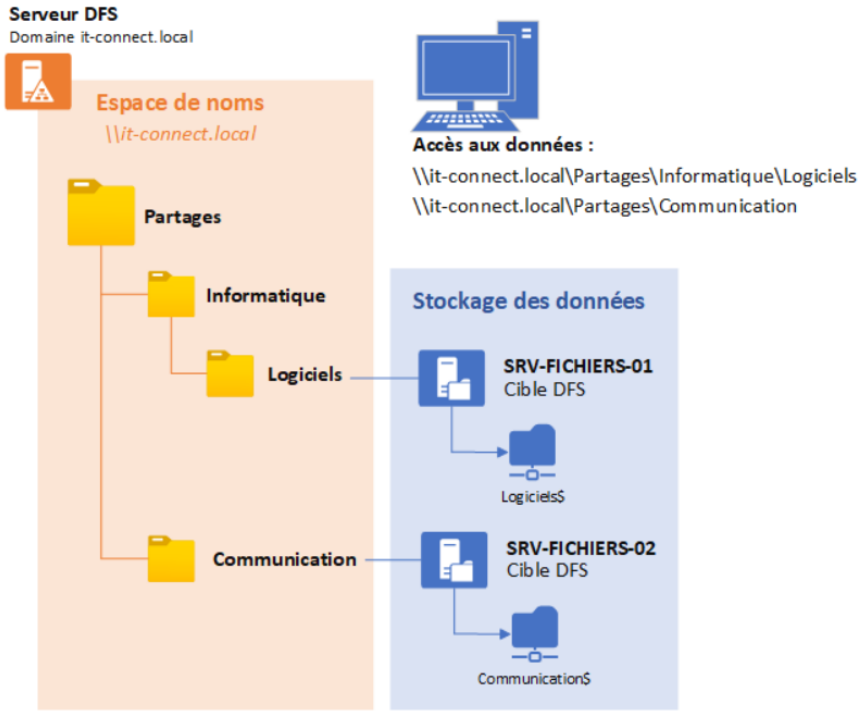
Tâche 2 : Etude solution DFS

Distributed File System

DFS est un ensemble de services client et serveur qui permet d'organiser de nombreux partages de fichiers dans un regroupement logique en liant de manière transparente les partages à un seul espace de noms.

Par exemple si le serveur de partage doit changer suite a une panne ou autre, le chemin d'accès restera le même, ce sera donc transparent pour les utilisateurs

Cette image illustre assez bien le principe du DFS :



Avantages/Inconvénients du DFS

Avantages	Inconvénients
Forte redondance	Mise en place assez complexe
Améliore la disponibilité, le temp d'accès et l'efficacité du réseau	Non approprié aux besoins de ValorElec
Système adaptable	Cout financier plus élevé

Mission 3

Objectif

Etablir un plan des autorisations à accorder aux utilisateurs puis procéder à son automatisation via un script PowerShell

Tâche 1 : Schéma des permissions

Dans un premier temps j'ai répertorié tous les utilisateurs ainsi que leur groupe global et mis ces groupes globaux dans des groupes de domaine local tel que suivant :

Partage N°1		Groupes Domaines Locaux		
		DL_ValorElec_L	DL_ValorElec_LM	DL_ValorElec_CT
Groupes Globaux	GG_Direction			X
	GG_Commercial	X		
	GG_R&D		X	
	GG_admin_Tierslieux86			X

Légende : X Membre de ...

		Groupes Globaux		
		GG_Commercial	GG_R&D	GG_Direction
Utilisateurs	Pierre Un		X	
	André Deux		X	
	Michel Trois		X	
	Adrien Quatre		X	
	Théo Cinq		X	
	Tiffany Sic		X	
	Gérard Sette		X	
	Kamel Ouitte		X	
	Louis Neuffe		X	
	Henri Disse		X	
	Alexandre Onz	X		
	Antoine Douse			X
	Jean Treze			X
	Jacqueline Katorz			X
	Valerie Quainze (Directrice Commercial)	X		X
	Philippe Saize (Directeur)	X	X	X
	Nadine Diset			X
	Odette Diouite			X
	Alfred Disseneuf			X
	...			
	...			

Tâche 2 : Automatisation de la sécurité du partage

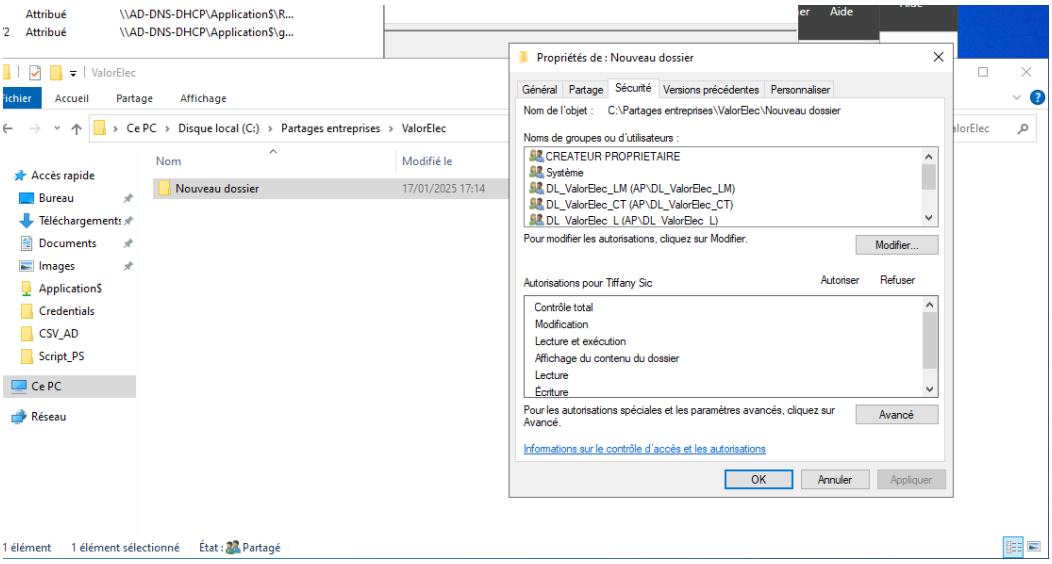
Ensuite j'ai écrit un petit script PowerShell qui permet de créer un partage samba puis ajoute les groupes globaux dans les groupes DL, qui donne les permissions de partage et NTDS aux groupes DL et qui supprime les utilisateurs « Tout le monde » et « Utilisateurs ».

En investissant plus de temps sur le script il peut être améliorer de sorte à prendre en charge n'importe quelle entreprise et peut aussi être optimiser en créant des fonctions, mais comme c'est un script relativement léger il n'a pas besoin d'être optimiser et il remplit la tâche demandée.

Je précise que la gestion de la sécurité NTFS nécessite l'installation d'un module PowerShell.

Ce script est de même disponible sur mon portfolio en téléchargement.

```powershell
$GG_RD = "CN=GG_ValorElec_R&D,OU=Groupes_Globaux,OU=ValorElec,OU=Clients_entreprises,OU=ETP_Chasseneuil,DC=ap,DC=local"
$GG_DIR = "CN=GG_ValorElec_Direction,OU=Groupes_Globaux,OU=ValorElec,OU=Clients_entreprises,OU=ETP_Chasseneuil,DC=ap,DC=local"
$GG_COMM = "CN=GG_ValorElec_Commercial,OU=Groupes_Globaux,OU=ValorElec,OU=Clients_entreprises,OU=ETP_Chasseneuil,DC=ap,DC=local"
$GG_ADM_TL86= "CN=GG_Admin_TierLieux86,OU=Groupes Globaux,OU=Groupes,OU=ETP_Chasseneuil,DC=ap,DC=local"
$Path_Dir = "C:\Partages entreprises\ValorElec"

#Création des groupes de domaines locaux
New-ADGroup -Name "DL_ValorElec_L" -Path "OU=Groupe_DL,OU=ValorElec,OU=Clients_entreprises,OU=ETP_Chasseneuil,DC=AP,DC=LOCAL" -GroupScope DomainLocal -Description "Lecture"
New-ADGroup -Name "DL_ValorElec_LM" -Path "OU=Groupe_DL,OU=ValorElec,OU=Clients_entreprises,OU=ETP_Chasseneuil,DC=AP,DC=LOCAL" -GroupScope DomainLocal -Description "Modification"
New-ADGroup -Name "DL_ValorElec_CT" -Path "OU=Groupe_DL,OU=ValorElec,OU=Clients_entreprises,OU=ETP_Chasseneuil,DC=AP,DC=LOCAL" -GroupScope DomainLocal -Description "Contrôle Total"

#Ajout de memebres aux groupes DL
Add-AdGroupMember -Identity DL_ValorElec_LM -Members $GG_RD
Add-AdGroupMember -Identity DL_ValorElec_LM -Members $GG_COMM
Add-AdGroupMember -Identity DL_ValorElec_CT -Members $GG_DIR
Add-AdGroupMember -Identity DL_ValorElec_CT -Members $GG_ADM_TL86

#Création du partage
try
    {
        New-SmbShare -Name "ValorElec" -Path $Path_Dir
    }
catch
    {
        Write-Warning "Le Partage existe déjà"
    }


#Permissions NTFS
Disable-NTFSAccessInheritance -Path $Path_Dir
Remove-NTFSAccess -Path $Path_Dir  -Account "Utilisateurs" -AccessRights FullControl
Add-NTFSAccess -Path $Path_Dir -Account "DL_ValorElec_LM" -AccessRights Modify
Add-NTFSAccess -Path $Path_Dir -Account "DL_ValorElec_L" -AccessRights Read
Add-NTFSAccess -Path $Path_Dir -Account "DL_ValorElec_CT" -AccessRights FullControl

#Permissions Partage
Revoke-SmbShareAccess -Name "ValorElec" -AccountName "Tout le monde" -Force
Grant-SmbShareAccess -Name "ValorElec" -AccountName DL_ValorElec_LM -AccessRight Change -Force
Grant-SmbShareAccess -Name "ValorElec" -AccountName DL_ValorElec_CT -AccessRight Full -Force
Grant-SmbShareAccess -Name "ValorElec" -AccountName DL_ValorElec_L -AccessRight Read -Force
```



Mission 4

Objectif

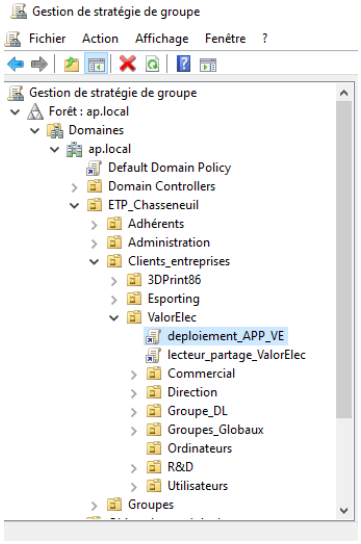
Déploiement de stratégie de group dans le but d'améliorer la gestion et la sécurité de l'infrastructure.

Tâche 1 : Installation de logiciel via GPO

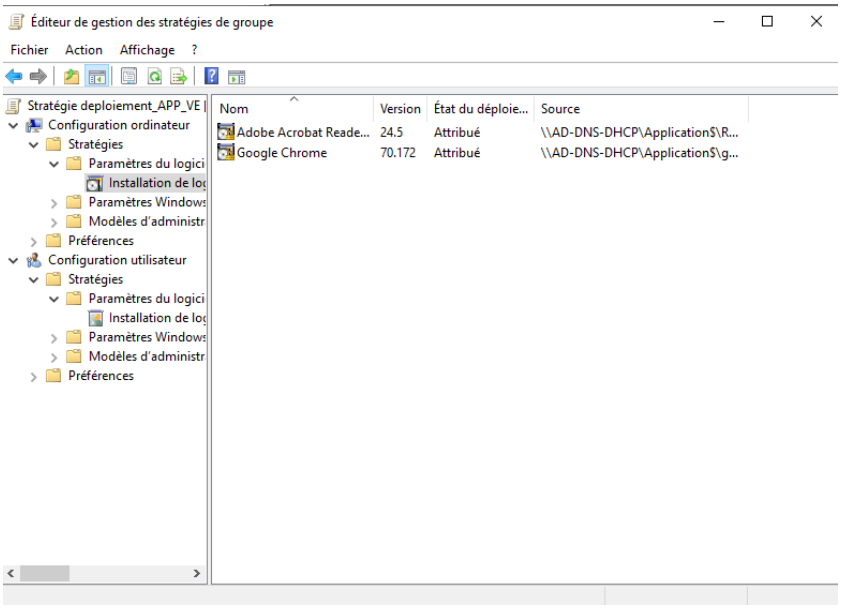
Il faut dans un premier temps obtenir la version .MSI de l'application que l'on souhaite installer automatiquement, ici Adobe Acrobat Reader ainsi que Mozilla et Google Chrome.

Ensuite il suffit de créer un partage afin d'y stocker les exécutables des logiciels, de paramétrer les permissions de sorte que les ordinateurs du domaine aient un droit de lecture et d'exécution puis récupérer l'adresse réseau de ce partage dans le but de l'inclure dans notre stratégie.

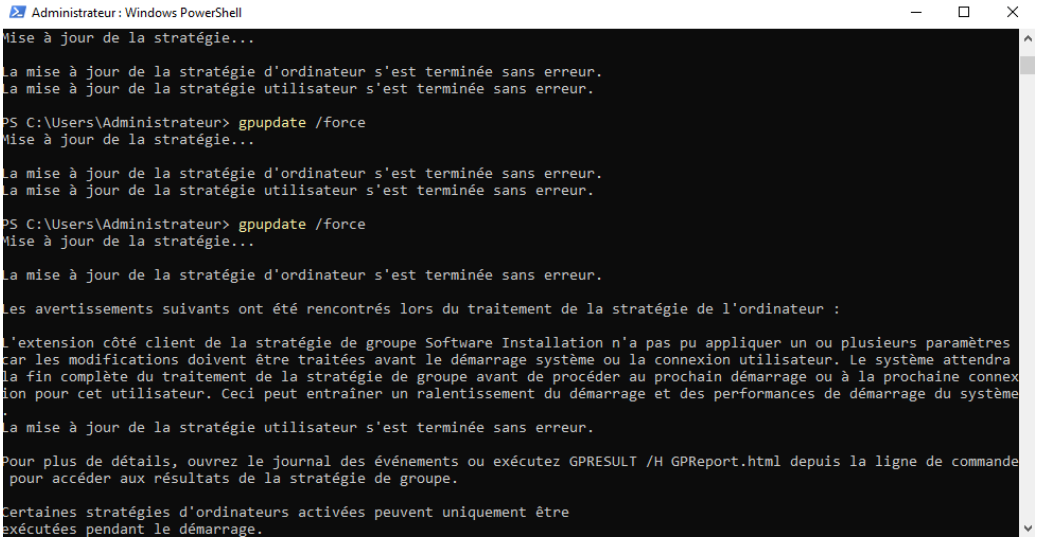
Dans un second temps, on se positionne sur l'unité d'organisation avec laquelle on veut que la stratégie interagisse puis on crée la GPO.



On la modifie pour qu'elle prenne en paramètre les applications précédemment configurer et placées dans le bon dossier on pense bien a la mettre en mode attribué pour qu'elle installe de façon complétement automatique les logiciels sur les ordinateurs affectés.



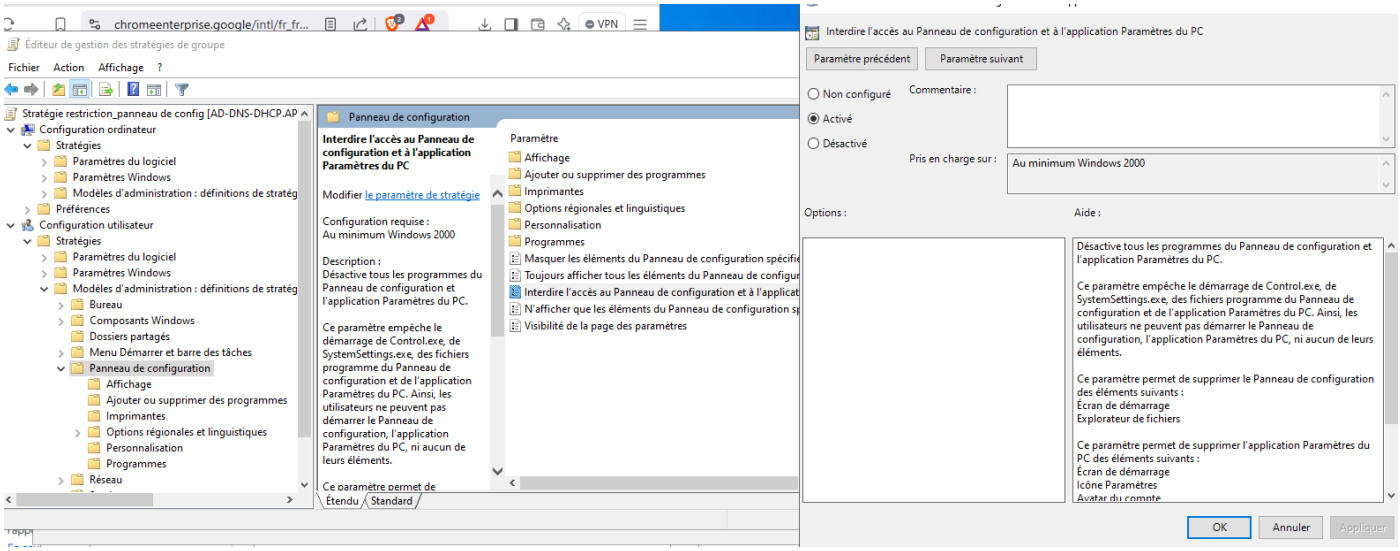
Sur le PC client on ouvre une ligne de commande et on force la mise à jour des GPO le PC va nous demander de redémarrer afin d'appliquer les stratégies.



A la suite du redémarrage les applications sont installées.

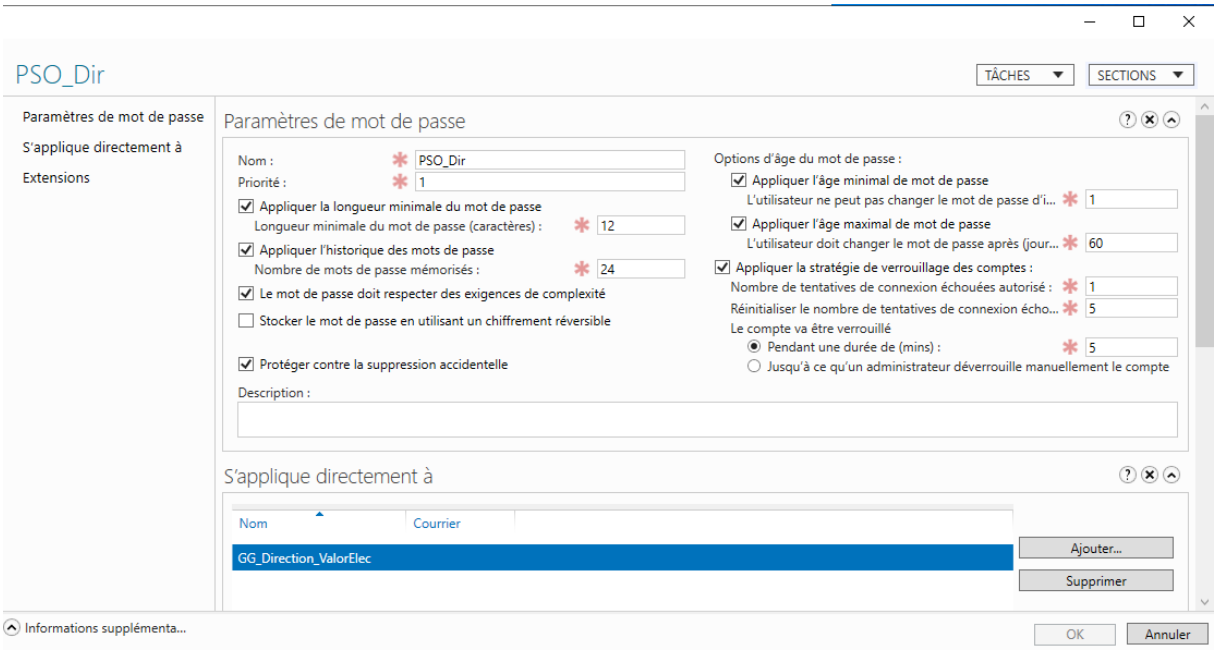
Tâche 2 : Stratégies de sécurisation

Dans un premier temps on désactive l'accès au panneau de configuration via les GPO

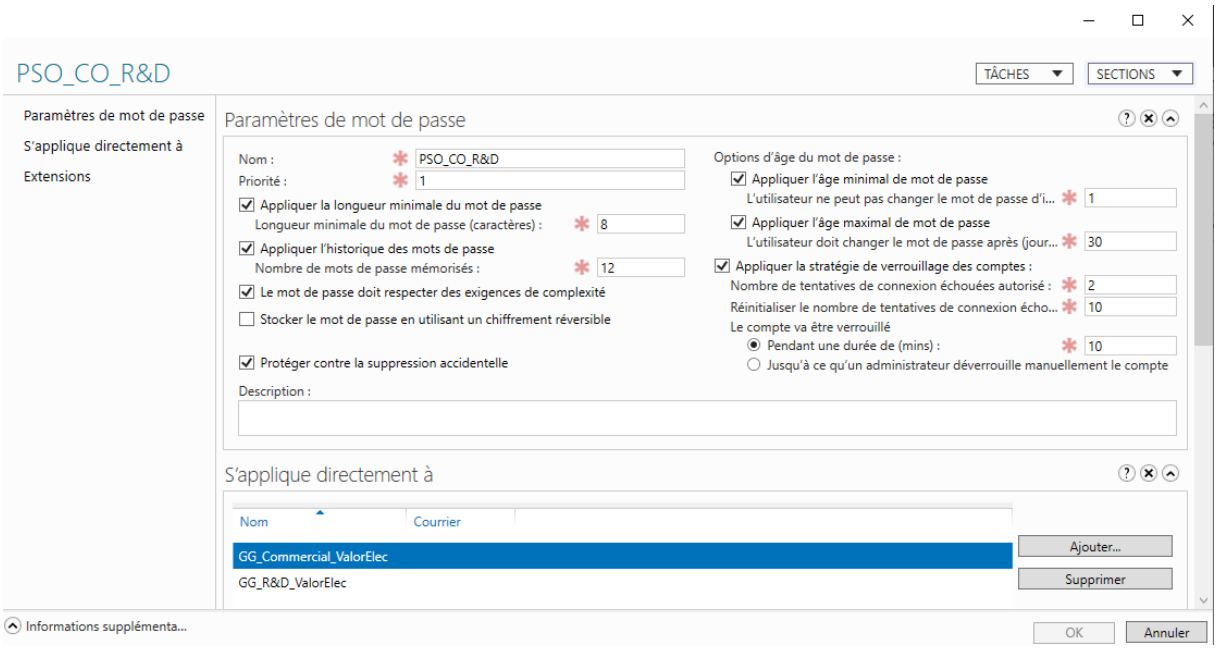


Ensuite on met en place des Password Setting Object qui permettent d'appliquer des politiques de mot de passe pour différents groupes.

Pour le groupe de direction :



Et pour les groupes R&D et Commercial :



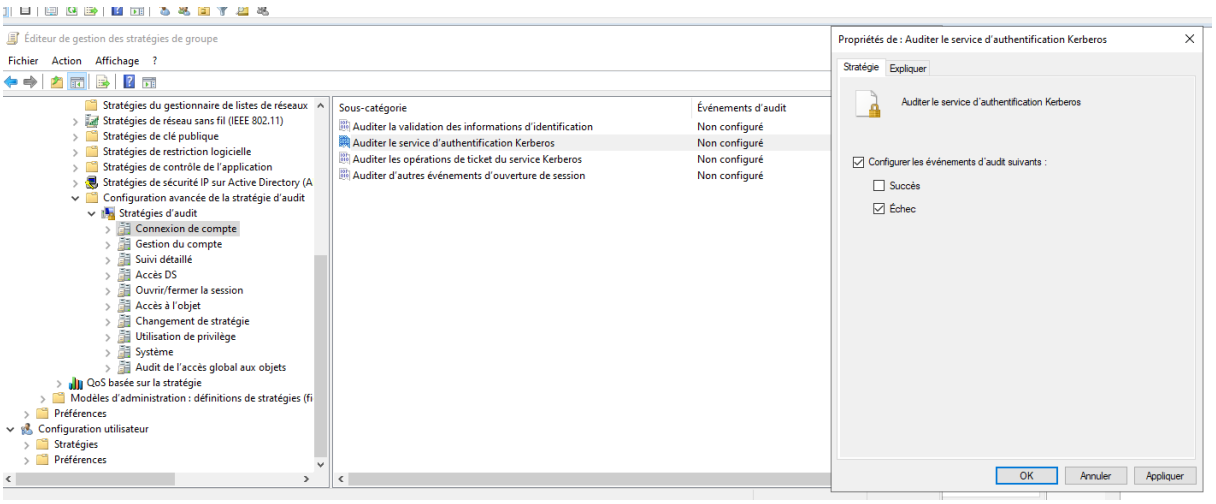
Tâche 3 : Mise en place de stratégie d'audit

Nous allons mettre en place un audit sur les ouvertures de compte infructueuse, les modifications d'objets AD et un audit aussi sur les partages existants.

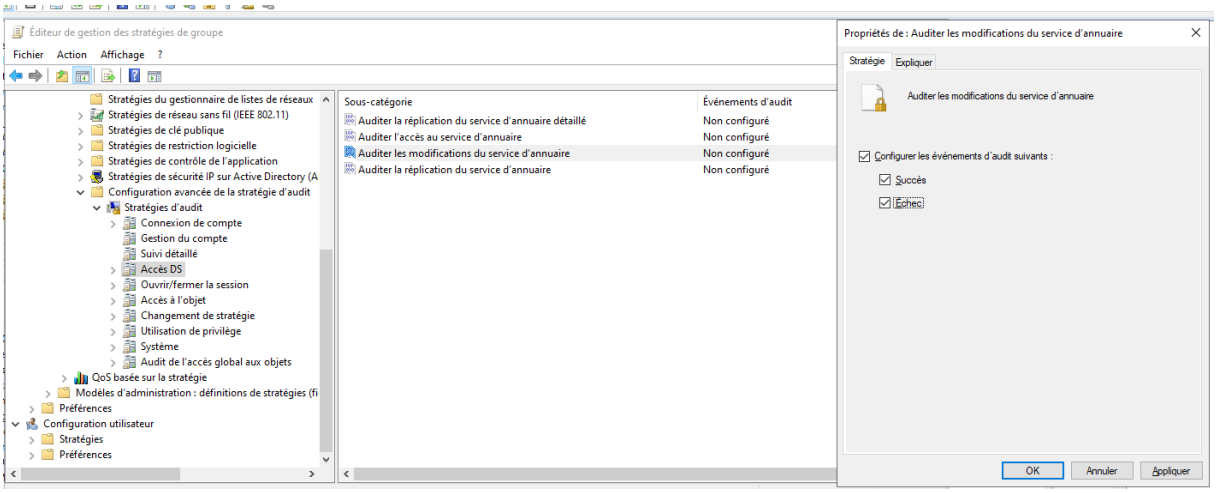
Cet audit permettra au système de journaliser les évènements souhaités afin de garder une traçabilité.

Il faut pour cela se rendre dans gestion de stratégie de groupe > configuration Ordinateurs > Stratégies > Paramètres Windows > Paramètres de sécurité > Configuration avancée de la stratégie d'audit > Stratégie d'audit et de sélectionné les éléments qui nous correspondent.

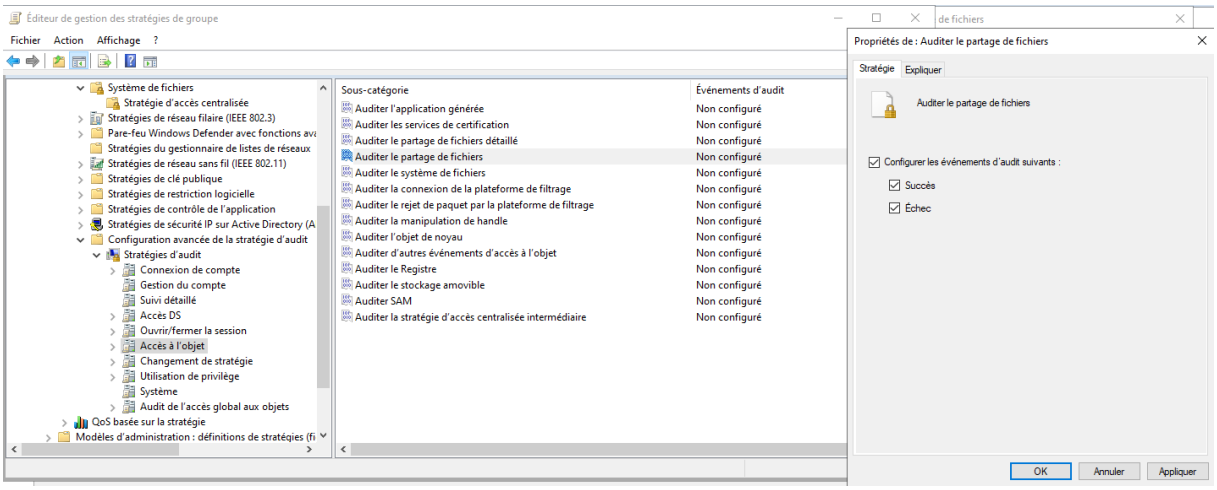
Pour les tentatives de connexion infructueuse :



Les modifications d'objets AD :

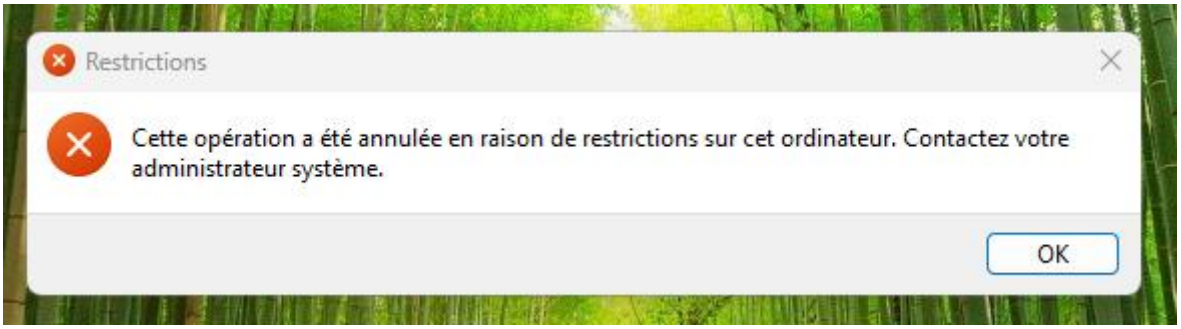


Et les partages de fichiers :



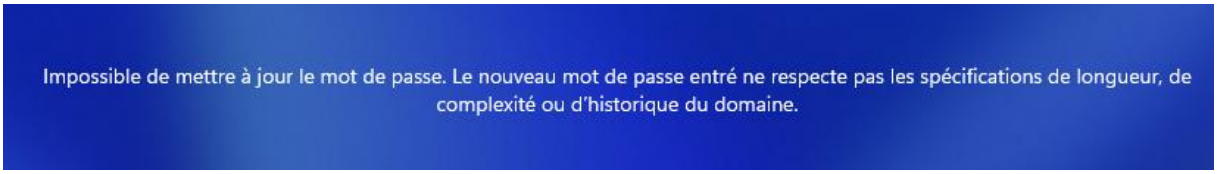
Tâche 4 : Rapport de test stratégie de groupes

GPO sur le panneau de configuration depuis un poste client:



Verrouillage de compte :

Caractéristique mot de passe :



Conclusion

Désormais nous avons une infrastructure virtuel évolué qui contient :

- Un AD structuré en plusieurs OU avec les utilisateurs d'une entreprise cliente dont l'administration peut se faire de façon automatiser ou du moins très faciliter ;
- Un serveur de fichier NAS est disponible pour les utilisateurs de l'entreprise ValorElec, les dossiers partagés sont protégés par des sécurité d'habilitations et des droits NTFS ce qui peut aussi s'administrer de façon assister grâce à un script ;
- Des GPO ont été déployées afin d'installer automatiquement certains logiciels dès l'ouverture d'une session utilisateurs ;
- Des politiques de sécurité utilisateurs en instaurant des barrières de façon a ce que les utilisateurs ne puissent pas accéder au panneau de configuration ;
- L'utilisateur doit changer sont mots de passe lors de la première ouverture de session pour un mot de passe plus sécuriser, en fonction des responsabilités de chaque utilisateur ;
- Pour finir nous avons éditer des stratégies d'audit Active Directory afin d'être informer en fonction de certains éléments.

Compétences couvertes

Bloc 1

- Gérer le patrimoine informatique ;
- Répondre aux incidents et aux demandes d'assistance et d'évolution ;
- Travailler en mode projet ;
- Mettre à disposition des utilisateurs un service informatique.

Bloc 2

- Concevoir une solution d'infrastructure réseau ;
- Installer, tester et déployer une solution d'infrastructure réseau ;
- Exploiter, dépanner et superviser une solution d'infrastructure réseau.

Bloc 3

- Sécuriser les équipements et les usages des utilisateurs ;
- Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service (spécifique à l'option SISR).

Sources

https://www.malekal.com/powershell-gerer-les-partages-reseaux-et-de-dossiers-de-windows-10/

https://www.it-connect.fr/comment-connecter-une-cible-iscsi-sous-windows/

https://www.youtube.com/watch?v=xqM8A1gM5wI

https://www.it-connect.fr/cest-quoi-le-dfs-windows-server/#:~:text=Racine%20DFS%20%3A%20le%20point%20d,les%20espaces%20de%20noms%20autonome.

https://www.cohesity.com/fr/glossary/distributed-file-system/#:~:text=Voici%20quelques%20avantages%20%C3%A0%20utiliser,physiquement%20les%20donn%C3%A9es%20des%20fichiers.

https://www.it-connect.fr/chapitres/creer-un-groupe-active-directory-avec-powershell/

https://www.malekal.com/powershell-creer-ecrire-fichier/#:~:text=Le%20cmdlet%20pour%20cr%C3%A9er%20un,l'on%20souhaite%20%C3%A9crire%20dedans.&text=Voici%20un%20exemple%20d'utilisation,txt%20avec%20du%20texte.

https://www.it-connect.fr/chapitres/creer-un-utilisateur-dans-lactive-directory-avec-powershell/

https://www.it-connect.fr/audit-des-groupes-de-securite-de-lactive-directory/

https://www.it-connect.fr/comment-deployer-un-logiciel-au-format-msi-par-gpo/

https://www.it-connect.fr/strategie-de-mot-de-passe-affinee-sous-windows-server-2012-r2/

https://github.com/letsdoautomation/group-policy/tree/main/Deploy%20Adobe%20Acrobat%20Reader%20DC