

# Atelier de professionnalisation 1

**Mettre en place l'infrastructure système (Windows Server et Active Directory) et réseau du site de Chasseneuil de TiersLieux86 .**

## **Mission 0:Préparé l'environnement de travail**

**Tache 1 :** mettre en place le projet et réaliser la maquette de l'infrastructure réseau du site de Chasseneuil

**Tache 2 :** mettre en place le prototype virtuel du site de Chasseneuil

## **Mission 1 créer la maquette de l'architecture système**

**Tâche 1:**Proposer une organisation en OU, utilisateurs et groupes pour le client *ValorElec* intégrée à TiersLieux86.

**Tâche 2:**Automatiser les tâches d'administration (créations des OUs, utilisateurs et groupes, peuplement des groupes et création d'un document Word avec leurs informations personnelles login mot de passe...) par l'écriture de scripts.

## **Mission 2 : mettre en place un serveur de fichiers**

**Tâche 1:**Mettre en place un serveur de fichiers basé sur du stockage iSCSI

**Tâche 2:**Réaliser une étude sur l'implémentation d'une racine dédiée DFS (avantages et inconvénients) pour le client ValorElec.

## **Mission 3 : automatiser la mise en place de la sécurité sur les partages**

**Tâche 1:**Proposer sous forme de tableau les utilisateurs, groupes et droits associés sur les partages.

**Tâche 2:**Écrire un script PowerShell qui vous permettra d'automatiser l'ensemble des tâches pour mettre en place la sécurité sur les partages.

## **Mission 4 : mettre en place des stratégies de groupe (GPO)**

**Tâche 1:**Installer via une GPO le logiciel AcrobatReader.msi pour le client ValorElec.

**Tâche 2:**Mettre en place un ensemble de restrictions par stratégies de groupe,

Le but de cet AP est l'étude et la mise en place des pré requis pour les ateliers de professionnalisation suivants. L'analyse est basée sur le Dossier documentaire: description du site de TiersLieux86 à Chasseneuil

**Tache 1:**Mettre en place le projet et réaliser la maquette de l'infrastructure réseau du site de Chasseneuil

## Objectifs de cette mission:

- Récupérer le dossier décrivant le contexte et mettre en place un suivi de projet
- Rédiger la documentation du contexte et proposer une adaptation du plan d'adressage
- Réaliser une maquette sous Packet Tracer reproduisant l'architecture réseau

## **Documentation du Contexte de l'ETP de Chasseneuil**

### **Document du Contexte : Infrastructure Réseau de l'ETP de Chasseneuil**

#### **1. Introduction**

Ce document décrit l'infrastructure réseau de l'ETP de Chasseneuil "B2". Il détaille les aspects physiques et logiques du réseau, et les services essentiels.

#### **2. Description de l'Infrastructure**

- **2.1. Bâtiments et Agencement**
  - L'ETP de Chasseneuil est réparti sur deux bâtiments (A et B).
  - Chaque bâtiment dispose de deux étages hébergeant les bureaux des adhérents.
  - Les rez-de-chaussée accueillent des espaces mutualisés (salles de réunion, espace de convivialité, reprographie, etc.).
- **2.2. Équipements Réseau**
  - **Routeur WAN :**
    - Assure la connexion Internet mutualisée (fibre 100 Mb/s).
    - Possède une adresse IP publique : 192.36.253.20
  - **Commutateurs :**
    - Distribution : Centralisée (bâtiment B) et secondaire par étage (bâtiment A).
    - Type : Gigabit Ethernet (10/100/1000) avec ports combo RJ-45/SFP.
  - **Points d'Accès WiFi :**
    - Couverture : Déploiement en quinconce sur les étages pour une couverture optimale.
  - **Pare-feu :**
    - Type : Pare-feu Stormshield.

- Rôle : Protection du réseau, gestion des accès à la DMZ et de l'accès à Internet.
- **Serveur d'impression :**
  - Un serveur d'impression relié aux différents moyens d'impression des bureaux et de la salle de repro-graphie qui fait également office de serveur antiviral.
- **2.3. Serveurs**
  - **Serveur Physique (LAN Serveurs) :**
    - Services :
      - Active Directory.
      - DHCP.
      - DNS.
      - Gestion des configurations et des incidents.
      - NAS.
      - Serveur d'impression (également serveur antiviral).
  - **Serveur Virtuel (DMZ) :**
    - Machine Debian
    - Services :
      - DNS.
      - Serveur Web.
      - Serveur de messagerie.
- **2.4. Baies de Brassage**
  - **Bâtiment A :**
    - Une armoire de brassage secondaire par étage.
    - 22 prises Ethernet par armoire (20 vers les bureaux, 1 vers la borne WiFi, 1 vers la salle de réunion).
    - 1 commutateur 26 ports (24 ports 10/100/1000 + 2 ports Giga combo RJ-45/SFP) par armoire.

- Connexion en fibre à l'armoire centralisatrice au rez-de-chaussée.
- **Bâtiment B :**
  - Une armoire de brassage centralisée au premier étage.
  - 64 prises Ethernet (32 par étage, 3 par bureau, 1 pour la salle de réunion, 1 pour la borne WiFi).
  - 2 commutateurs stackés (32 ports Gigabit Ethernet chacun).
  - Connexion en fibre à l'armoire centralisatrice au rez-de-chaussée.
- **Armoire Centralisatrice (Rez-de-Chaussée, Bâtiment B) :**
  - 2 commutateurs 24 ports.
  - Routeur.
  - Armoire des serveurs.
  - Connexion des salles du RDC et des bornes WiFi.
- **2.5. Services Associés**
  - Accès Internet mutualisé (fibre 100 Mb/s).
  - WiFi "visiteurs" avec clé WPA2.
  - Téléphonie IP.
  - Services d'impression (facturation au coût).

### 3. Réseaux et Sous-Réseaux

- **LAN Bureaux:**
  - Objectif : Connexion des adhérents, de l'administration et des équipements WiFi.
- **LAN Serveurs:**
  - Objectif : Infrastructure des serveurs internes.
- **DMZ:**
  - Objectif : Hébergement des serveurs exposés à Internet (Web, DNS, Messagerie).
- **Réseaux des Juniors Entreprises :**

- Objectif : Isolement et accès réseau pour chaque junior entreprise.
- **Réseau Evénement :**
  - Objectif : Créer un réseau lors d'un évènement.

## 5. Services Réseau

- **DHCP :**
  - Rôle : Attribution automatique des adresses IP dans le LAN Bureaux et les réseaux des juniors entreprises.
  - Serveur DHCP : Hébergé sur le serveur Active Directory.
- **DNS :**
  - Rôle : Résolution de noms de domaine internes et externes.
  - Serveurs DNS : Hébergés sur le serveur Active Directory et dans la DMZ .

## 6. Sécurité

- **Pare-feu :** Pare-feu Stormshield assurant la sécurité des accès.
- **Segmentation VLAN :** Projet en cours pour améliorer la sécurité en segmentant les réseaux.

## Plan d'Adressage IP – ETP de Chasseneuil ("B2")

Ce plan d'adressage définit les plages d'adresses IP utilisées dans l'infrastructure réseau de l'ETP de Chasseneuil. Il a été conçu en respectant la numérotation du site (2).

### 1. Réseaux

Nom du Réseau	Plage d'Adresses
LAN Bureaux	192.168.2.0/24
WiFi (Visiteurs)	192.168.3.0/24
LAN Serveurs	10.2.0.0/24
DMZ	172.16.2.0/24
Réseaux Juniors Entreprises	172.17.2ent.0/24 (variable)
Réseau Evénement	172.17.2reu.0/24 (variable)

### 2. Adresses IP Statiques

Équipement	Adresse IP Réseau
Routeur/Pare-feu (Interface LAN - LAN Bureaux)	192.168.2.254 LAN Bureaux
Routeur/Pare-feu (Interface LAN - WiFi)	192.168.3.254 WiFi
Routeur/Pare-feu (Interface LAN - DMZ)	172.16.2.254 DMZ
Serveur Active	10.2.0.1 LAN Serveurs

Directory/DHCP/DNS		
Serveur de gestion configurations/incidents	10.2.0.2	LAN Serveurs
Serveur NAS	10.2.0.3	LAN Serveurs
Serveur d'impression	10.2.0.4	LAN Serveurs
Serveur DNS (domaine x.net)	172.16.2.10	DMZ
Serveur Web	172.16.2.11	DMZ
Serveur de messagerie	172.16.2.12	DMZ
Routeur/Pare-feu (Interface LAN - LAN Serveurs)	10.2.0.254	LAN Serveurs
Routeur/Pare-feu (Interface Internet)	192.36.253.20	Internet

### 3. DHCP

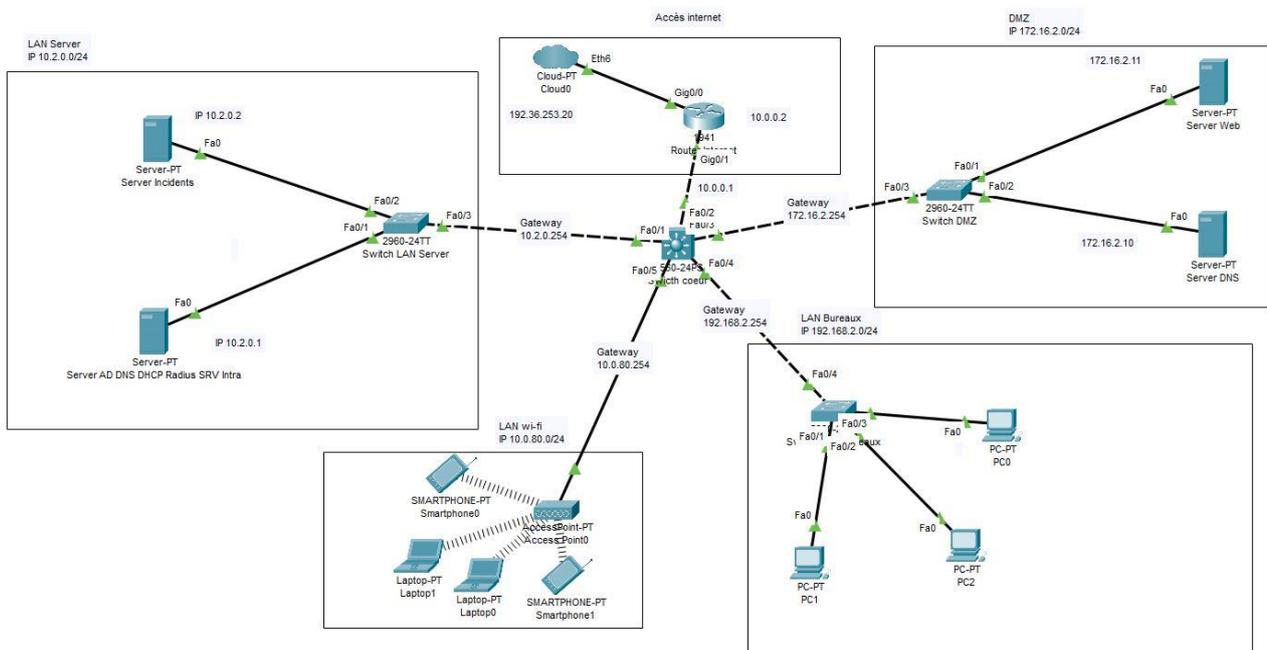
- LAN Bureaux: 192.168.2.10 - 192.168.2.200
- WiFi: 192.168.3.10 - 192.168.3.200

### 4. Commentaires

- **WiFi:** Plage distincte pour la sécurité, bail court.
- **Juniors :** Sous-réseau unique par entreprise.
- **LAN Serveurs :** Pas de passerelle, isolé.
- **DMZ :** Passerelle pour accès externe.

## Schéma illustratif Packet Tracer

La maquette Packet Tracer doit suivre le schéma logique d'un site ETP



## Tache 2: Mettre en place le prototype virtuel du site de Chasseneuil

Objectifs de cette mission:

- Mettre en place un prototype virtuel reproduisant l'architecture système.

Récupérer ou installer les machines virtuelles suivantes :

- une machine virtuelle Vyos
- une machine virtuelle Windows Server 2019
- une machine virtuelle Windows 10 Education.

La virtualisation se fera via Virtualbox.

### Consigne

- configurer le routage sur la machine VyOS pour avoir plusieurs sous-réseaux conformément au schéma des ETP de TiersLieux86 ;
- configurer le service DHCP sur le serveur Windows et l'agent de relais DHCP sur le routeur
- installer et configurer le domaine Active Directory du site de Chasseneuil ;

- créer les utilisateurs et les groupes selon le schéma fourni (administration, adhérents et l'entreprise esporting) ;
- mettre en place un dossier partagé sur le contrôleur de domaine pour le personnel de TiersLieux86 de Chasseneuil avec des droits de lecture/écriture en fonction du statut : employé ou responsable.

La VM Windows Serveur reçoit donc comme le plan d'adressage le prévoit, l'adresse IP 10.2.0.1 Le service DHCP a aussi été installé et un pool d'IP pour le LAN bureau a été configuré comme vous pouvez le constater ci-dessous.

The image shows two screenshots. The top one is a Windows PowerShell window with the following content:

```

Administrateur: Windows PowerShell
- i TTL           Durée de vie.
- v TOS           Type de service (IPv4 uniquement. La
                  configuration de ce paramètre n'a aucun effet sur le type
                  de service dans l'en-tête IP).
- r count        Itinéraire d'enregistrement du nombre de sauts (IPv4
                  uniquement).
- s count        Horodatage du nombre de sauts (IPv4 uniquement).
- j host-list     Itinéraire source libre parmi la liste d'hôtes (IPv4
                  uniquement).
- k host-list     Itinéraire source strict parmi la liste d'hôtes (IPv4
                  uniquement).
- w timeout      Délai d'attente pour chaque réponse, en millisecondes.
- R             Utilise l'en-tête de routage pour tester également
                  l'itinéraire inverse (IPv6 uniquement).
                  D'après la RFC 5095, l'utilisation de cet en-tête de routage
                  est déconseillée. Certains systèmes peuvent supprimer des
                  demandes d'écho si cet en-tête est utilisé.
- S srcaddr      Adresse source à utiliser.
- c compartiment Identificateur de compartiment de routage.
- p             Effectue un test ping sur l'adresse de fournisseur
                  de la virtualisation réseau Hyper-V.
- 4             Force l'utilisation d'IPv4.
- 6             Force l'utilisation d'IPv6.

PS C:\Users\Administrateur> ping chasseneuil.fr

Envoi d'une requête 'ping' sur chasseneuil.fr [10.2.0.1] avec 32 octets de données :
Réponse de 10.2.0.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 10.2.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
PS C:\Users\Administrateur>

```

The bottom screenshot shows the DHCP console in Windows Server. The left pane shows the hierarchy: DHCP > dc-01.chasseneuil.fr > IPv4. The right pane shows the DHCP server configuration for the IPv4 scope:

- Contenu du serveur DHCP
- État
- Étendue [192.168.2.0] LAN Bureaux (État: \*\* Actif \*\*)
- Options de serveur
- Stratégies
- Filtres

Below the console, a table shows the IP address pool configuration:

Pool d'IP		
Adresse IP de début	Adresse IP de fin	Description
192.168.2.1	192.168.2.253	Plage d'adresses

Nous devons configurer un relais DHCP sur les différents routeurs du réseau. En effet, cela permettra aux requêtes DHCP de ne pas s'arrêter au niveau du routeur principal, mais d'être relayées vers les autres sous-réseaux. Ainsi, les équipements réseau et les postes utilisateurs pourront recevoir une adresse IP allouée dynamiquement par le serveur DHCP.

Pour cela, les deux interfaces créées dans VirtualBox doivent être configurées en tant que passerelles, chacune dédiée à un LAN spécifique :

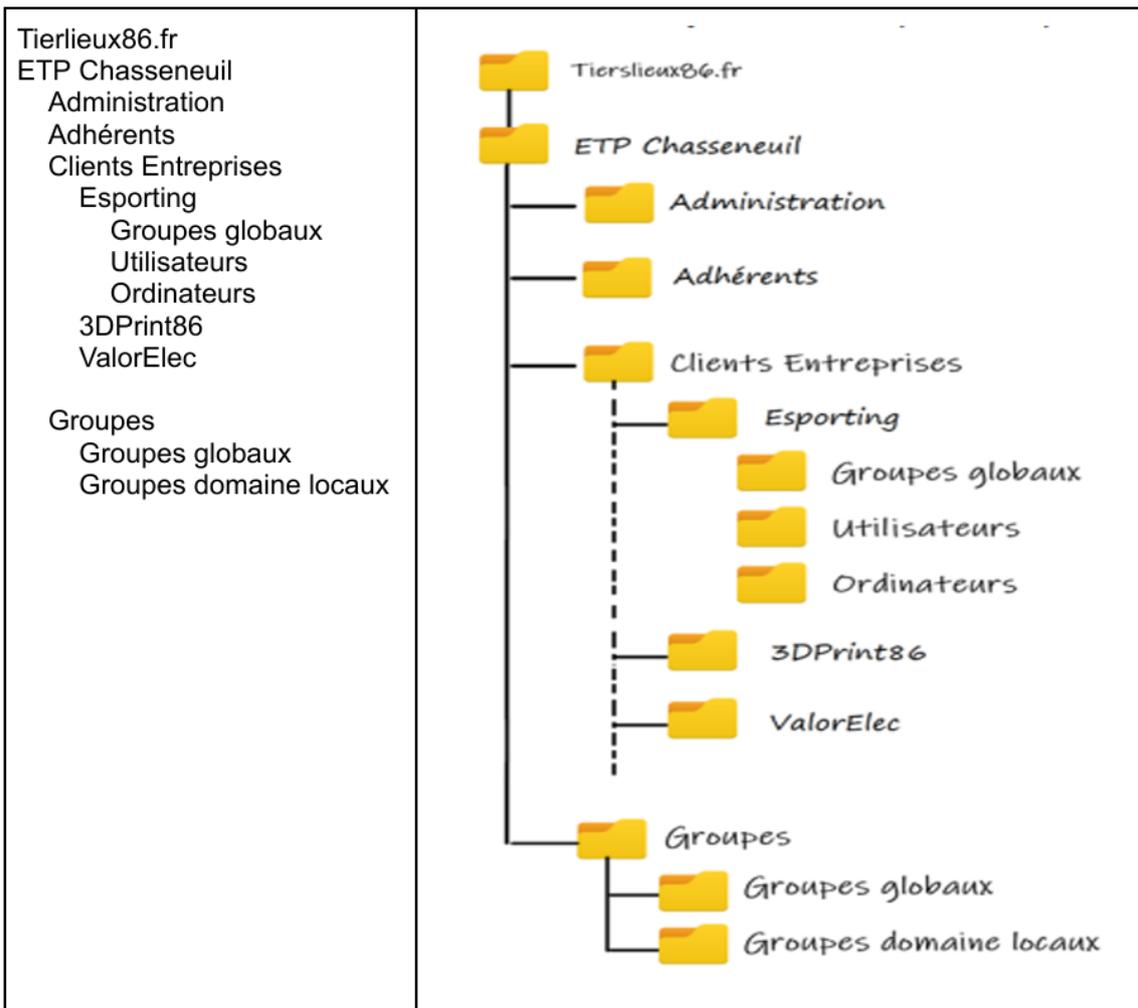
- Le LAN Serveur, avec l'adresse passerelle 10.2.0.254
- Le LAN Bureaux, avec l'adresse passerelle 192.168.2.254

Via les commandes:

```
configure
#set interfacesetherneteth0address
"10.2.0.254/24"
#set interfacesetherneteth1address
"192.168.2.254/24"
#commit
#save
#exit
```

Nous devons par la suite configurer le relai dhcp via les commandes:

```
configure
#setservicedhcp-relayinterfaceeth0
#setservicedhcp-relayinterfaceeth1
#setservicedhcp-relayserver10.2.0.1
#setservicedhcp-relayrelay-options
relay-agent-packetsdiscard
#commit
#save
#exit
```



## Organisation de l'AD

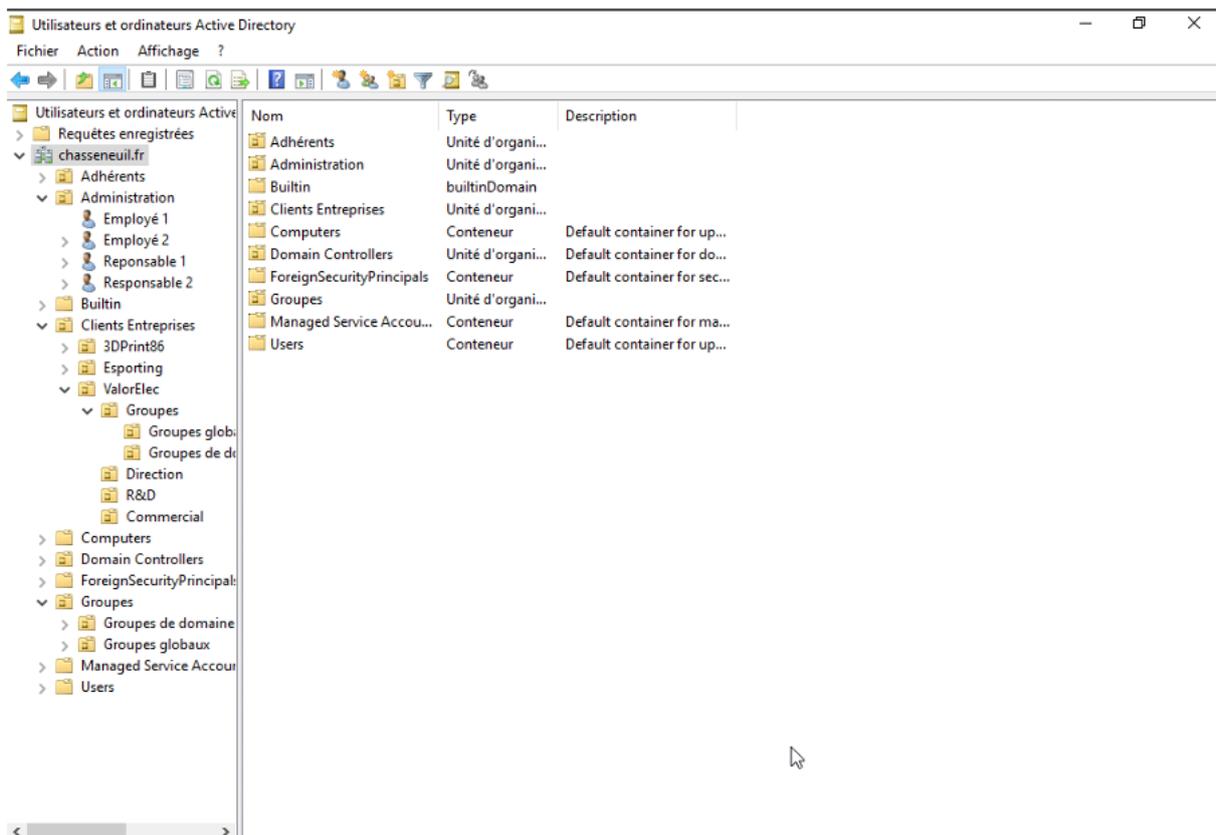
Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Nom	Type	Description
Adhérents	Unité d'organi...	
Administration	Unité d'organi...	
Builtin	builtinDomain	
Clients Entreprises	Unité d'organi...	
Computers	Conteneur	Default container for up...
Domain Controllers	Unité d'organi...	Default container for do...
ForeignSecurityPrincipals	Conteneur	Default container for sec...
Groupes	Unité d'organi...	
Managed Service Accou...	Conteneur	Default container for ma...
Users	Conteneur	Default container for up...

**Dossier partagé**

**Domaine Active Directory configuré**



**Le domaine est bien sur l'IP 10.2.0.1, il respecte le plan d'adressage**

```

l'itinéraire inverse (IPv6 uniquement).
D'après la RFC 5095, l'utilisation de cet en-tête de routage
est déconseillée. Certains systèmes peuvent supprimer des
demandes d'écho si cet en-tête est utilisé.
-S srcaddr Adresse source à utiliser.
-c compartiment Identificateur de compartiment de routage.
-p Effectue un test ping sur l'adresse de fournisseur
de la virtualisation réseau Hyper-V.
-4 Force l'utilisation d'IPv4.
-6 Force l'utilisation d'IPv6.

PS C:\Users\Administrateur> ping chasseneuil.fr

Envoi d'une requête 'ping' sur chasseneuil.fr [10.2.0.1] avec 32 octets de données :
Réponse de 10.2.0.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 10.2.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
PS C:\Users\Administrateur>

```

**Routage et DHCP mis en place:**

**L'IP de l'utilisateur est bien donnée par le serveur DHCP**

```
Invite de commandes

Configuration IP de Windows

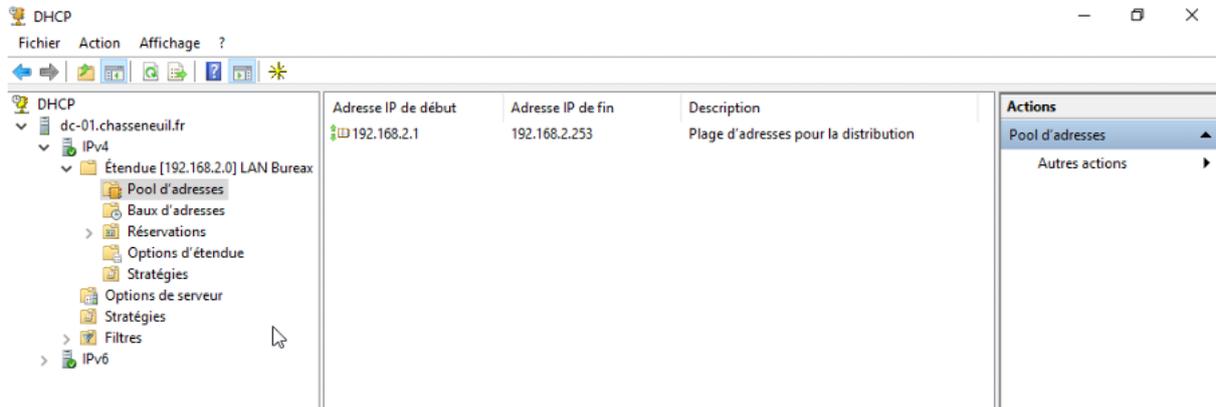
Nom de l'hôte . . . . . : DESKTOP-4MUTU59
Suffixe DNS principal . . . . . : chasseneuil.fr
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: chasseneuil.fr

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . : chasseneuil.fr
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-27-68-63
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::ada6:24f7:4b02:62c8%8(préféré)
Adresse IPv4. . . . . : 192.168.2.1(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : dimanche 5 mars 2023 22:48:56
Bail expirant. . . . . : lundi 13 mars 2023 23:11:57
Passerelle par défaut. . . . . : 192.168.2.254
Serveur DHCP . . . . . : 10.2.0.1
IAID DHCPv6 . . . . . : 101187623
DUID de client DHCPv6. . . . . : 00-01-00-01-2B-97-80-84-08-00-27-27-68-63
Serveurs DNS. . . . . : 10.2.0.1
NetBIOS sur Tcpip. . . . . : Activé

C:\Users\responsable2>
```

## DHCP sur le serveur



## Ping du poste utilisateur vers l'interface du serveur sur le VyoS

```
Invite de commandes

Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-27-68-63
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::ada6:24f7:4b02:62c8%8(préféré)
Adresse IPv4. . . . . : 192.168.2.1(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : dimanche 5 mars 2023 22:48:56
Bail expirant. . . . . : lundi 13 mars 2023 23:11:57
Passerelle par défaut. . . . . : 192.168.2.254
Serveur DHCP . . . . . : 10.2.0.1
IAID DHCPv6 . . . . . : 101187623
DUID de client DHCPv6. . . . . : 00-01-00-01-2B-97-80-84-08-00-27-27-68-63
Serveurs DNS. . . . . : 10.2.0.1
NetBIOS sur Tcpip. . . . . : Activé

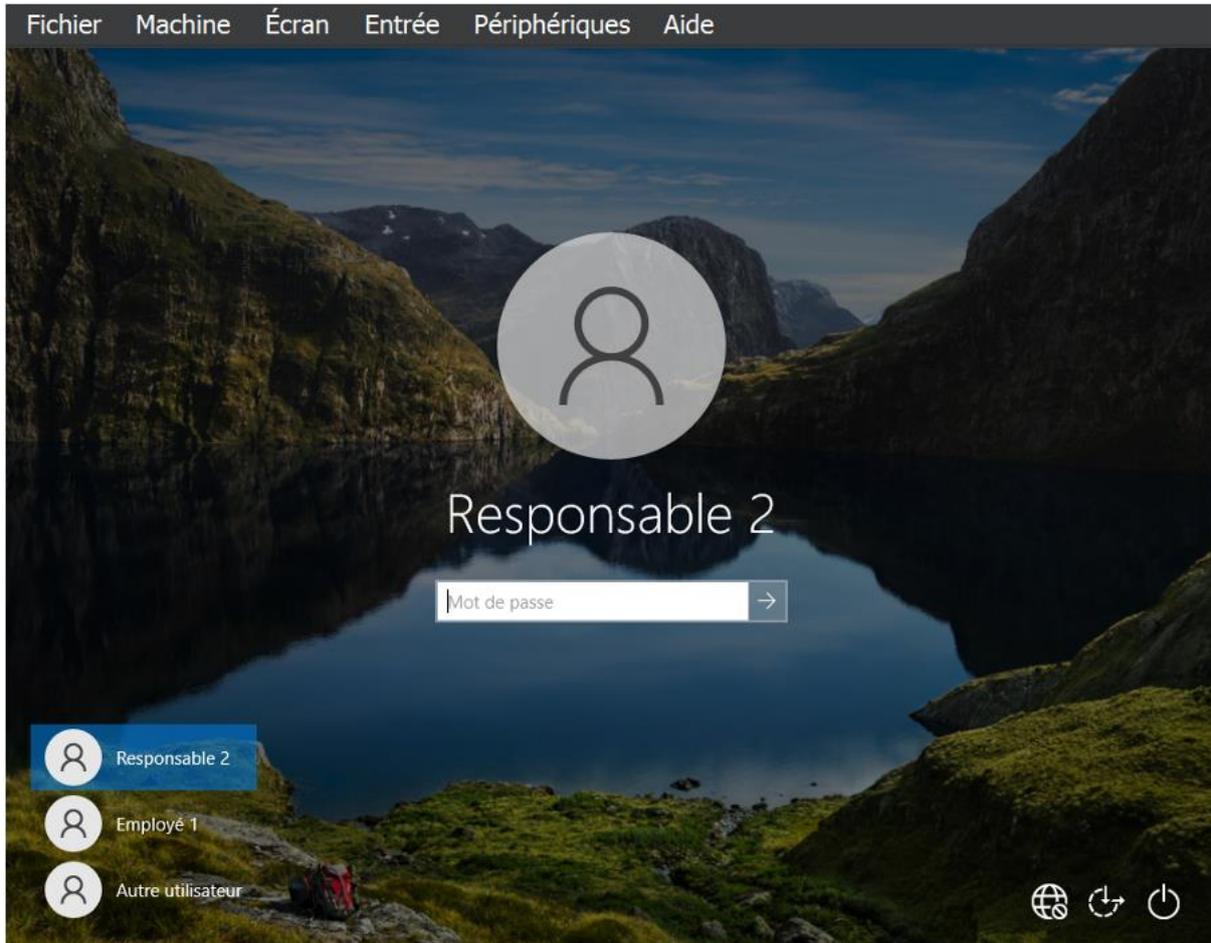
C:\Users\responsable2>ping 10.2.0.254

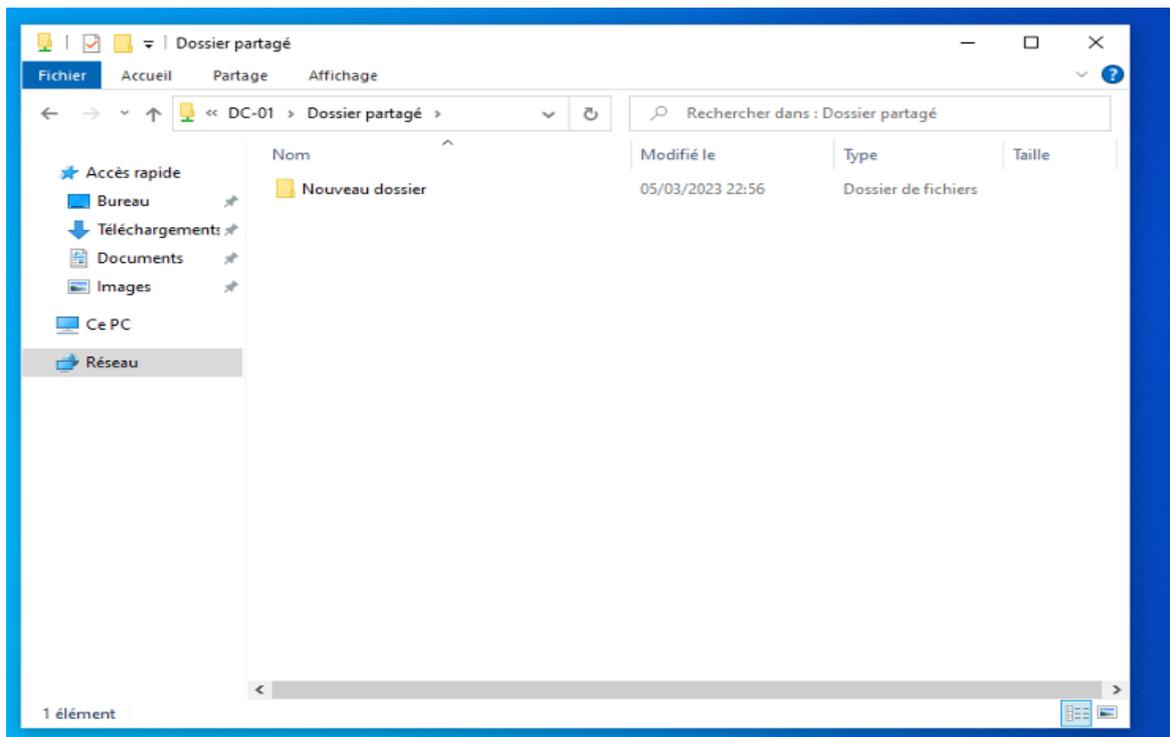
Envoi d'une requête 'Ping' 10.2.0.254 avec 32 octets de données :
Réponse de 10.2.0.254 : octets=32 temps=1 ms TTL=64
Réponse de 10.2.0.254 : octets=32 temps=1 ms TTL=64
Réponse de 10.2.0.254 : octets=32 temps=1 ms TTL=64
Réponse de 10.2.0.254 : octets=32 temps=2 ms TTL=64

Statistiques Ping pour 10.2.0.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\responsable2>
```

## Utilisateurs et partage configurés





## Situation de professionnalisation 2

**Faire évoluer l'architecture système (Windows Server et Active Directory) pour accueillir un nouveau client sur le site de Chasseneuil de TiersLieux86.**

### **Contexte**

InfoTech Services 86 (ITS 86) est une Entreprise de Services Numériques (ESN) spécialisée dans le développement informatique (applications de bureau, web et mobile), l'hébergement de sites web, l'infogérance, la gestion de parcs informatiques, l'ingénierie système et réseau ainsi que la cybersécurité. Elle répond régulièrement à des appels d'offres en tant que prestataire de services informatiques et société d'infogérance.

En tant qu'assistante du responsable Système et Réseaux d'ITS 86, je reçois un e-mail urgent de notre client, TiersLieux86.

Objet : intégration d'un nouveau client à notre site de Chasseneuil

TiersLieux86 doit mettre à jour son SI car dans quelques jours nous allons devoir accueillir un nouveau client ValorElec spécialisé dans la collecte, le traitement et la valorisation de déchets d'équipements électriques et électroniques (DEEE). Leur siège a été détruit à la suite d'un incendie, ils n'ont heureusement pas perdu de données car elles étaient répliquées sur les sites de production. Le siège accueillait le service Direction de l'entreprise, le service Commercial et le service de Recherche et développement. Les services et les utilisateurs du

site de Chasseneuil (20 personnes) vont être relocalisés sur notre site de Chasseneuil qui est en cours d'agrandissement. Le client ValorElec a comme particularité d'être multi sites, il comporte un siège, quatre sites de production (Lyon, Marseille, Lens et Rennes) et 8 agences commerciales réparties sur le territoire. Ils devront avoir la possibilité de continuer à travailler avec leurs sites distants depuis notre site de Chasseneuil. Nous pouvons accueillir momentanément dans la salle libre-service leurs 20 collaborateurs, mais il faudra prévoir de nous fournir 20 nouveaux ordinateurs et un nouveau commutateur dédié pour aménager la salle en cours de création.

Nous attendons votre proposition que nous adjoindrons à la réponse à notre client

Bien cordialement...

**Je suis chargée de préparer le système d'information de TiersLieux86 afin d'accueillir le nouveau client. Je devrai intégrer ces personnes au site de Chasseneuil. Le service informatique d'IT Services 86 dispose de la console LAPS pour réaliser des interventions à distance sur les postes de travail.**

## **Mission 1 : créer la maquette de l'architecture système**

### **Objectifs de cette mission:**

- Créer la maquette reproduisant l'architecture système du site de Chasseneuil.

### **Tâche 1**

Proposer une organisation en OU, utilisateurs et groupes pour le client *ValorElec* intégrée à TiersLieux86. Une vingtaine de collaborateurs vont arriver ils sont répartis de la manière suivante :

- 10 personnes pour le service recherche et développement ;
- 1 commercial ;
- 8 personnes pour le service de Direction (dont le directeur commercial).

### **Tâche 2**

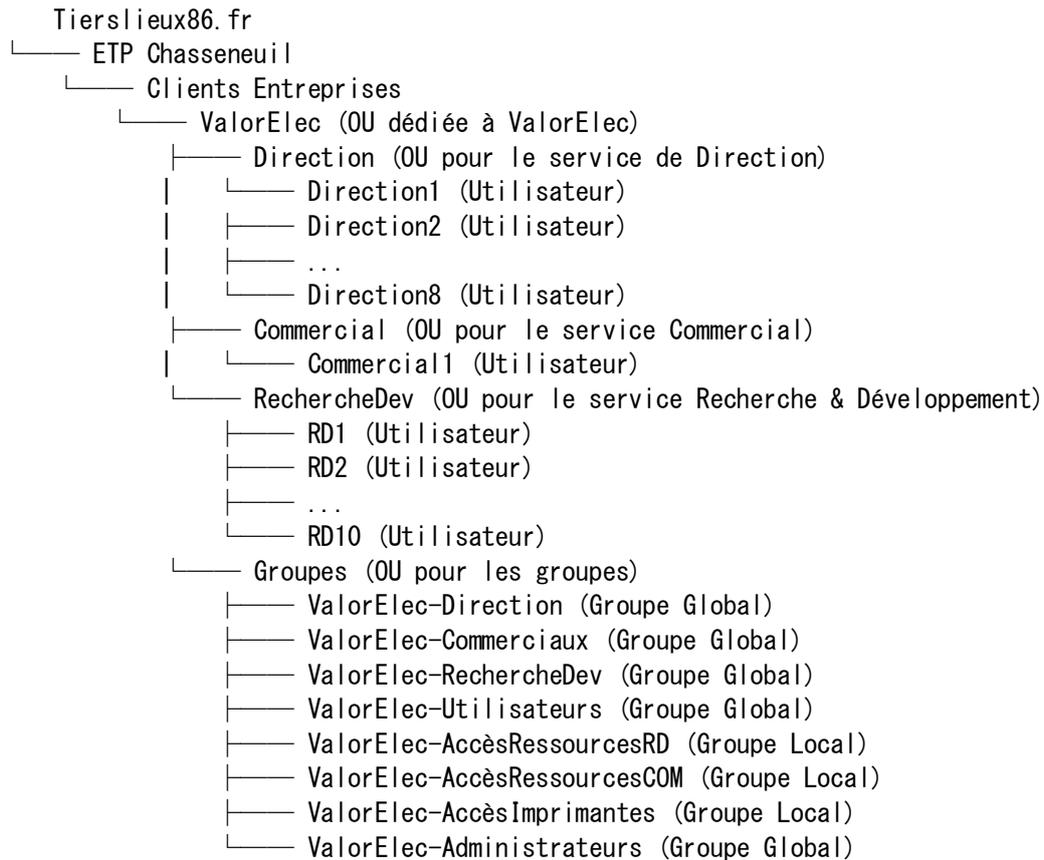
Automatiser les tâches d'administration (créations des OUs, utilisateurs et groupes, peuplement des groupes et création d'un document Word avec leurs informations personnelles login mot de passe...) par l'écriture de scripts.

### **Tâche 1**

#### **Organisation en OU, Utilisateurs et Groupes pour ValorElec**

Cette proposition décrit l'organisation des unités d'organisation (OU), des groupes et des comptes utilisateurs pour le client ValorElec au sein de l'Active Directory de TiersLieux86. L'objectif est de créer une structure claire, sécurisée et facile à gérer, permettant d'appliquer des politiques de sécurité et des autorisations spécifiques à ValorElec et à ses différents services.

## 1. Structure des OU



### Explication de la structure :

- **ValorElec** : L'OU racine dédiée à ValorElec contient toutes les sous-OU et les ressources spécifiques à ce client.
- **Direction, Commercial, RechercheDev** : Ces OU contiennent les comptes utilisateurs de chaque service.
- **Groupes** : Cette OU contient tous les groupes utilisés pour gérer les permissions et les droits d'accès.

## 2. Description des Groupes

**Groupes Globaux** (ValorElec-Direction, Commerciaux, RechercheDev) : Définissent l'appartenance aux services et octroient des droits spécifiques.

- ValorElec-Direction : Droits spécifiques Direction.
- ValorElec-Commerciaux : Droits spécifiques Commerciaux.
- ValorElec-RechercheDev : Droits spécifiques R&D.
- ValorElec-Utilisateurs : Droits communs à tous.

- ValorElec-Administrateurs : Administration du domaine.

ValorElec-Utilisateurs :Regroupe tous les utilisateurs ValorElec pour les droits communs.

ValorElec-Administrateurs :Réservé à l'administration.

**Groupes Locaux** (AccèsRessourcesRD/COM, AccèsImprimantes) :Contrôlent l'accès aux ressources partagées (lecture/écriture) et aux imprimantes.

- ValorElec-AccèsRessourcesRD : Accès R&D.
- ValorElec-AccèsRessourcesCOM : Accès Commercial.
- ValorElec-AccèsImprimantes : Accès imprimantes.

### 3. Convention de Nommage des Utilisateurs

- Service Recherche & Développement : RD1, RD2, ..., RD10
- Service Commercial : Commercial1
- Service Direction : Direction1, Direction2, ..., Direction8 (dont DirectionDirecteur pour le directeur commercial)

## Tâche 2

L'objectif est d'automatiser la création d'unités d'organisation (OU), d'utilisateurs et de groupes dans Active Directory via un script PowerShell. Cette automatisation permet de réduire les erreurs humaines et de gagner du temps en s'appuyant sur un fichier CSV contenant les informations nécessaires. Le script générera également un document avec les identifiants de connexion et mots de passe des utilisateurs, facilitant ainsi la gestion et le déploiement des comptes.

```

Import-Module ActiveDirectory
# Définition du domaine et de l'unité principale
$domain = "DC=CHASSENEUIL, DC=FR"
$baseOU = "OU=Clients Entreprises, DC=CHASSENEUIL, DC=FR"
$valorElecOU = "OU=ValorElec, $baseOU"

# Création des OUs principales
$OUs = @(

```

```

    "Direction", "Commercial", "RechercheDev", "Groupes"
)
foreach ($ou in $OUs) {
    New-ADOrganizationalUnit -Name $ou -Path $valorElecOU -ErrorAction SilentlyContinue
}

# Création des utilisateurs
$users = @(
    @{Name="Direction1"; OU="Direction"},
    @{Name="Commercial1"; OU="Commercial"},
    @{Name="RD1"; OU="RechercheDev"},
    @{Name="RD2"; OU="RechercheDev"}
)

$securePassword = ConvertTo-SecureString "P@sswOrd123" -AsPlainText -Force

foreach ($user in $users) {
    $ouPath = "OU=$(($user.OU), OU=ValorElec, $baseOU"
    New-ADUser -Name $user.Name -SamAccountName $user.Name -UserPrincipalName "$($user.Name)@chasseneuil.fr" -Path
    $ouPath -AccountPassword $securePassword -Enabled $true
}

# Création des groupes
$groups = @(
    "ValorElec-Direction", "ValorElec-Commerciaux", "ValorElec-RechercheDev", "ValorElec-Utilisateurs",
    "ValorElec-AccèsRessourcesRD", "ValorElec-AccèsRessourcesCOM", "ValorElec-AccèsImprimantes", "ValorElec-
    Administrateurs"
)

foreach ($group in $groups) {
    New-ADGroup -Name $group -GroupScope Global -Path "OU=Groupes, OU=ValorElec, $baseOU" -ErrorAction SilentlyContinue
}

# Génération d'un fichier Word avec les informations des utilisateurs
$word = New-Object -ComObject Word.Application
$word.Visible = $false
$doc = $word.Documents.Add()

```

```
$selection = $word.Selection

$selection.TypeText("Liste des utilisateurs et leurs identifiants")
$selection.TypeParagraph()

foreach ($user in $users) {
    $selection.TypeText("Nom: $($user.Name), Login: $($user.Name), Mot de passe: P@ssw0rd123")
    $selection.TypeParagraph()
}

$doc.SaveAs("C:\¥¥Users¥¥Public¥¥Users_Credentials.docx")
$doc.Close()
$word.Quit()

Write-Host "Script terminé. Toutes les OUs, utilisateurs et groupes ont été créés."
```

## **Mission 2 : mettre en place un serveur de fichiers**

*Les services doivent pouvoir stocker leurs informations ainsi que partager leur travail entre leurs collaborateurs.*

### **Objectifs de cette mission:**

- Mettre en place un serveur de fichiers

### **Tâche 1**

Mettre en place un serveur de fichiers basé sur du stockage iSCSI (TrueNas par exemple).

### **Tâche 2**

Réaliser une étude sur l'implémentation d'une racine dédiée DFS (avantages et inconvénients) pour le client ValorElec.

## Tâche 1

### □ Qu'est-ce que le protocole iSCSI ?

L'iSCSI (Internet Small Computer System Interface) est un protocole de stockage en réseau fonctionnant sur la couche transport (couche 4 du modèle OSI). Il permet de transférer des données entre des serveurs et des dispositifs de stockage distants en utilisant le protocole Internet (TCP/IP). Grâce à iSCSI, un serveur peut accéder à un espace de stockage distant comme s'il s'agissait d'un disque local, facilitant ainsi le partage des fichiers et la centralisation des données pour les utilisateurs.

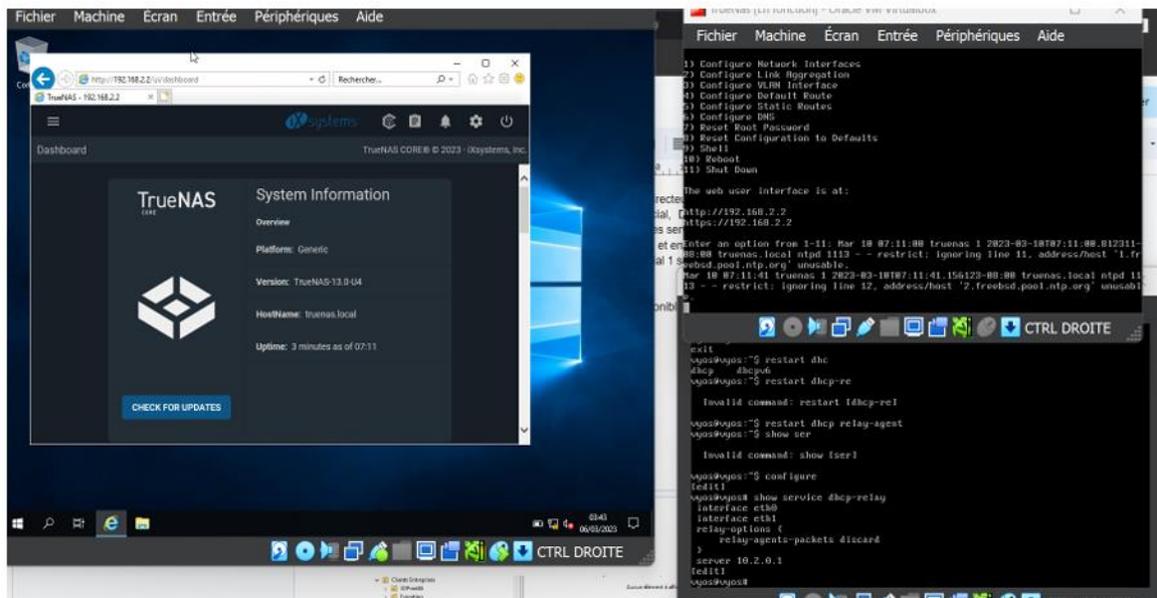
### Réalisation de la Tâche 1 : Mise en place du serveur de fichiers sur stockage iSCSI

*Pour mettre en place le serveur de fichiers pour ValorElec sur stockage iSCSI, j'ai suivi ces étapes principales :*

### **Actions Réalisées pour la Mise en Place de TrueNAS et iSCSI :**

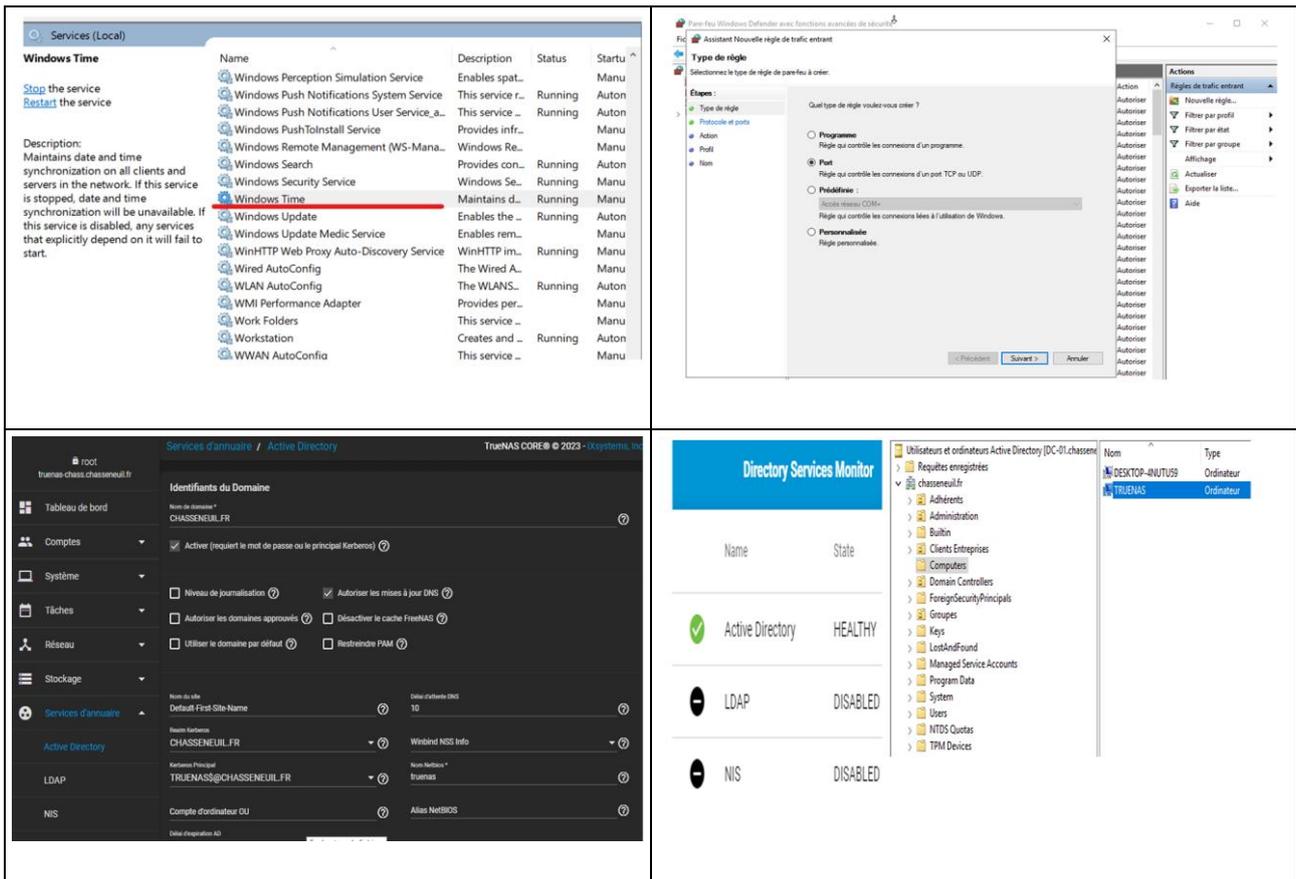
#### **I. Installation et Configuration Initiale de TrueNAS :**

- Machine virtuelle (VM) créée avec l'image ISO TrueNAS.
- Ressources suffisantes **allouées** à la VM (CPU, RAM, disques).
- VM **placée** sur le segment réseau LAN Bureau pour accès au relais DHCP.
- Adresse IP **obtenue** dynamiquement via relais DHCP au démarrage.
- Réserve DHCP **créée** sur le serveur DHCP pour l'IP obtenue (192.168.2.9).
- Pool de stockage **créé** dans TrueNAS (configuration Mirror/RAID 1 utilisée).



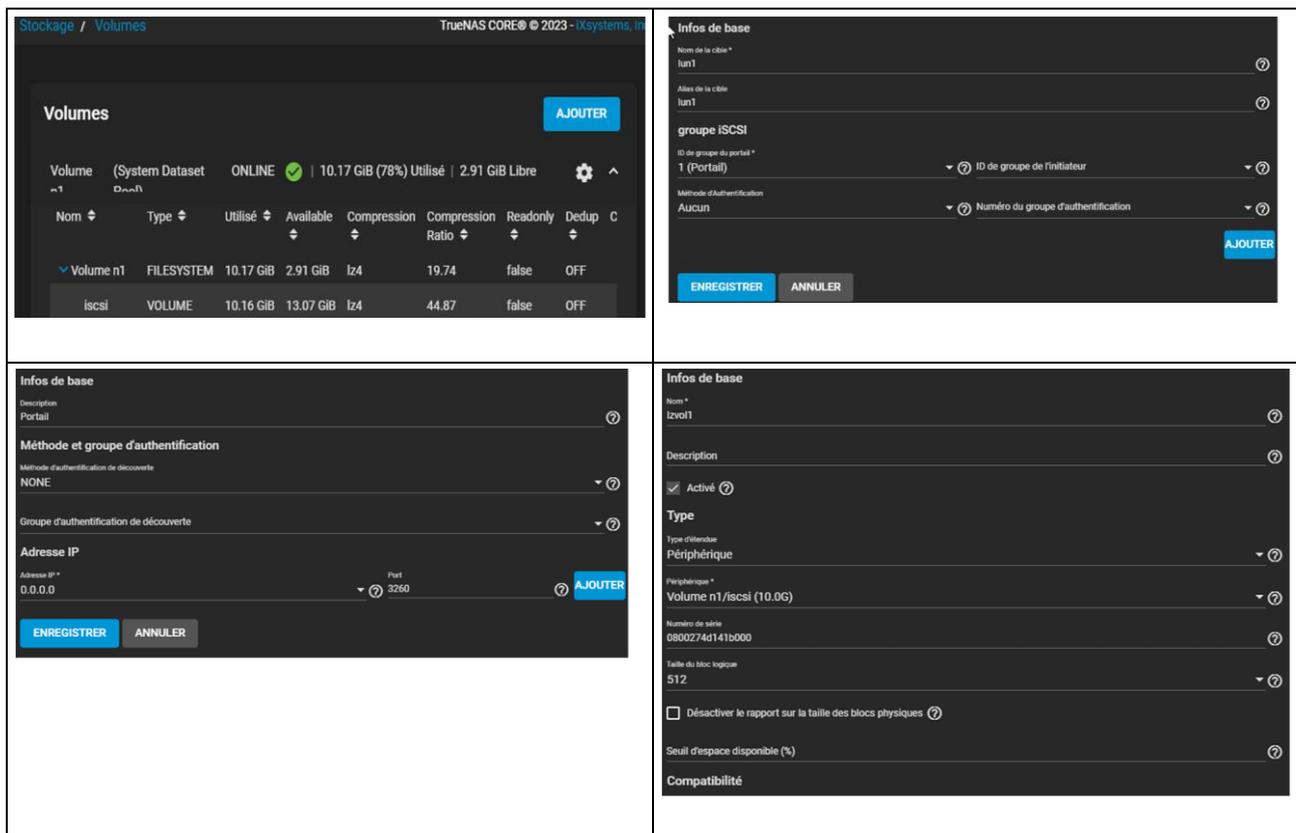
#### **II. Synchronisation Horaire (NTP) et Intégration Active Directory :**

- Service Windows Time **démarré** sur le serveur Windows désigné comme source NTP.
- TrueNAS **configuré** pour utiliser ce serveur Windows comme serveur NTP.
- Port UDP 123 **ouvert** (pare-feu) pour le trafic NTP.
- Synchronisation horaire entre TrueNAS et le serveur NTP **établie**.
- TrueNAS **intégré** avec succès au domaine Active Directory.
- Intégration AD **vérifiée** (présence confirmée dans le site AD de Chasseneuil).



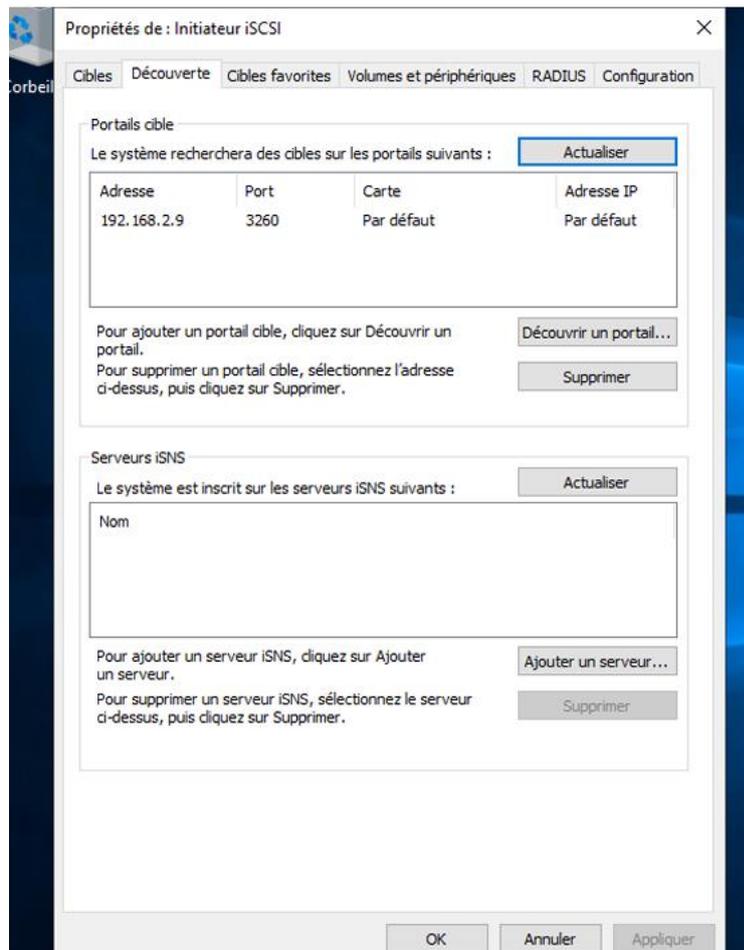
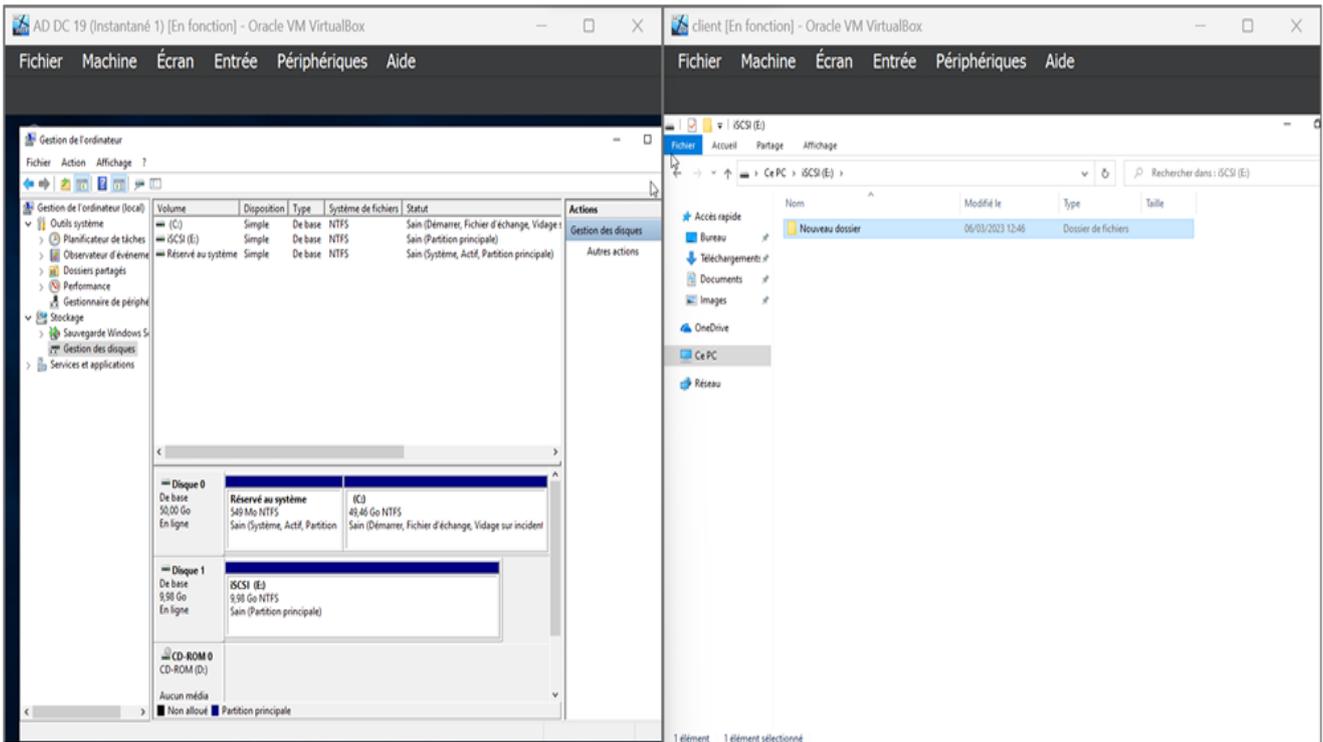
### III. Configuration du Partage iSCSI sur TrueNAS :

- Zvol iSCSI **créé** sur le pool de stockage existant.
- Portail iSCSI **configuré** (écoute sur toutes les IP : 0.0.0.0).
- Target iSCSI **créée**.
- Extent iSCSI **créé** (liaison entre le Zvol et la LUN établie).



#### IV. Configuration du Client iSCSI (Serveur Windows) :

- Outil Initiateur iSCSI **lancé** sur le serveur Windows client.
- Adresse IP du serveur TrueNAS (192.168.2.9) **ajoutée** à la Découverte de portail.
- Connexion à la cible iSCSI **établie**.
- Disque iSCSI **apparu** dans le Gestionnaire de disques Windows (hors connexion).
- Disque iSCSI **mis en ligne**.
- Disque **initialisé** (en GPT).
- Nouveau volume simple **créé** sur le disque iSCSI.
- Volume **formaté** en NTFS.
- Disque iSCSI **rendu accessible** comme un disque local sur le client Windows.



## Tâche 2

### Étude sur l'Implémentation d'une Racine DFS pour ValorElec

#### 1. Le Besoin de ValorElec et la Solution DFS

ValorElec dispose d'un serveur de fichiers avec des partages dédiés (Direction, Commercial, RechercheDev, Commun) hébergés. Pour simplifier l'accès à ces ressources et pérenniser l'infrastructure, nous pouvons utiliser la technologie **DFS (Distributed File System)** de Microsoft. Elle permet de créer une vue unifiée et logique de ces partages.

#### 2. Qu'est-ce qu'une Racine (ou Espace de Noms) DFS pour ValorElec ?

Il s'agit de créer un point d'entrée virtuel unique pour tous les partages de ValorElec, intégré au domaine **CHASSENEUIL.FR**. Au lieu d'accéder à `\\NomServeurFichiers\Direction`, les utilisateurs accéderont à quelque chose comme `\\CHASSENEUIL.FR\ValorElecData\Direction`. L'avantage est que ce chemin `\\CHASSENEUIL.FR\ValorElecData` ne changera jamais, même si le serveur physique (`NomServeurFichiers`) est remplacé un jour.

#### 3. Implémentation Proposée pour ValorElec

- **Type** : Espace de noms basé sur le domaine **CHASSENEUIL.FR**.
- **Nom de la racine** : `\\CHASSENEUIL.FR\ValorElecData`.
- **Structure** :(cibles des dossiers)

`\\CHASSENEUIL.FR\ValorElecData\Direction` pointera vers `\\NomServeurFichiers\Direction`

`\\CHASSENEUIL.FR\ValorElecData\Commercial` pointera vers `\\NomServeurFichiers\Commercial`

`\\CHASSENEUIL.FR\ValorElecData\RechercheDev` pointera vers `\\NomServeurFichiers\RechercheDev`

`\\CHASSENEUIL.FR\ValorElecData\Commun` pointera vers `\\NomServeurFichiers\Commun`

#### 4. Avantages Spécifiques pour ValorElec

- **Accès Simplifié** : Les utilisateurs n'auront qu'un chemin racine à retenir ou à mapper (`\\CHASSENEUIL.FR\ValorElecData`) pour accéder à tous leurs fichiers partagés.
- **Administration Simplifiée (Transparence Majeure)** : Si il faut faire une migrations de données vers un nouveau serveur de fichiers à l'avenir, il n'y aura pas besoin de reconfigurer les postes clients. Seule la configuration DFS sera à mettre à jour, de manière transparente pour les utilisateurs.
- **Organisation Claire** : Fournit une vue logique et organisée des ressources pour tous les services (Direction, Commercial, R&D).
- **Préparation à l'Avenir** : Pose les bases si ValorElec souhaite un jour mettre en place de la haute disponibilité pour ses fichiers (avec DFS-Replication).

## 5. Inconvénients Potentiels dans le Contexte de ValorEle

- **Gestion Additionnelle** : Cela ajoute une console de gestion (Gestion DFS) et un concept à maîtriser pour l'administration IT de ValorElec.
- **Dépendance à AD** : Le bon fonctionnement de \\CHASSENEUIL.FR\ValorElecData dépendra de la bonne santé de l'Active Directory.
- **Dépannage** : En cas de problème d'accès, il faudra aussi penser à vérifier la configuration DFS, en plus des permissions classiques.

## 6. Conclusion et Recommandation pour ValorElec

Pour l'infrastructure actuelle et future de ValorElec, l'implémentation de cette racine DFS **est une solution pertinente et recommandée**. La simplification de l'accès utilisateur et, surtout, l'énorme gain en flexibilité pour les évolutions futures (migration de serveur sans impact utilisateur) justifient pleinement l'ajout de cette technologie.

## **Mission 3 : automatiser la mise en place de la sécurité sur les partages**

*Le serveur de fichiers doit être configuré pour gérer la sécurité sur les partages dédiés à l'entreprise ValorElec*

Objectifs de cette mission:

- Automatiser la mise en place de la sécurité sur les partages.

### Tâche 1

Proposer sous forme de tableau les utilisateurs, groupes et droits associés sur les partages. Comme l'exemple suivant.

### Tâche 2

Écrire un script PowerShell qui vous permettra d'automatiser l'ensemble des tâches pour mettre en place la sécurité sur les partages.

## **Tâche 1**

L'objectif de cet exercice est de **définir précisément les droits d'accès** aux dossiers partagés de ValorElec, qui comprend **trois services** (Direction, R&D, Commercial) et nécessite à la fois des **partages spécifiques à chaque service et un partage commun**.

Pour réaliser cela de manière **structurée et sécurisée**, nous utiliserons la méthode **AGDLP** (Utilisateurs -> Groupes Globaux -> Groupes Locaux de Domaine -> Permissions). Cette approche permet d'attribuer les bons droits aux bonnes personnes et de **simplifier l'administration** des permissions à long terme, en suivant les bonnes pratiques Active Directory.

Le résultat de cette étude sera présenté sous forme de **tableaux**, détaillant les utilisateurs, les groupes et les droits associés pour chaque partage.

Partage en fonction des services		Groupes Domaines Locaux		
		Partage commercial	Partage direction	Partage R&D
Groupes Globaux	Service R&D			X
	Service Commercial	X		
	Service Direction		X	

Appartenances des utilisateurs au groupes en fonction des services		Groupes Globaux		
		Service Recherche et développement	Service Commercial	Service Direction
Utilisateurs	R&D 1 à 10	X		
	Direction 1 à 7			X
	Directeur direction	X	X	X
	Commercial 1		X	

## Tâche 2

Un script PowerShell permettant d'automatiser la mise en place de la sécurité sur les partages offre plusieurs avantages :

- Gagner du temps – Évite la configuration manuelle de chaque partage et de ses permissions.
- Assurer une sécurité cohérente – Applique des règles d'accès uniformes, réduisant les erreurs humaines.
- Gérer efficacement les droits d'accès – Attribue automatiquement les permissions NTFS et de partage aux groupes d'utilisateurs.
- Faciliter l'administration – Permet aux administrateurs IT de gérer les partages de manière centralisée.
- Automatiser la gestion des partages – Supprime et recrée les partages si nécessaire, applique des audits et enregistre les actions.

```
# Définir le chemin du dossier à créer et partager
$folderPath = "C:\DossierPartagé"

# Vérifier si le dossier existe, sinon le créer
if (!(Test-Path $folderPath)) {
    New-Item -ItemType Directory -Path $folderPath -Force
}

# Obtenir l'objet de sécurité pour le dossier
$folderSecurity = Get-Acl -Path $folderPath

# Définir les groupes et leurs permissions
$permissions = @(
```

```

    @{ Group = "Domain\%Service Commercial"; Rights = "Modify" }
    @{ Group = "Domain\%Service IT"; Rights = "FullControl" }
    @{ Group = "Domain\%Service Comptabilité"; Rights = "ReadAndExecute" }
)

# Appliquer les permissions NTFS
foreach ($perm in $permissions) {
    $accessRule = New-Object System.Security.AccessControl.FileSystemAccessRule(
        $perm.Group, $perm.Rights, "ContainerInherit, ObjectInherit", "None", "Allow"
    )
    $folderSecurity.SetAccessRule($accessRule)
}

# Appliquer la configuration des permissions
Set-Acl -Path $folderPath -AclObject $folderSecurity

# Définir le nom du partage
$shareName = "DossierPartagé"

# Vérifier si le partage existe déjà et le supprimer avant de le recréer
if (Get-SmbShare -Name $shareName -ErrorAction SilentlyContinue) {
    Remove-SmbShare -Name $shareName -Force
}

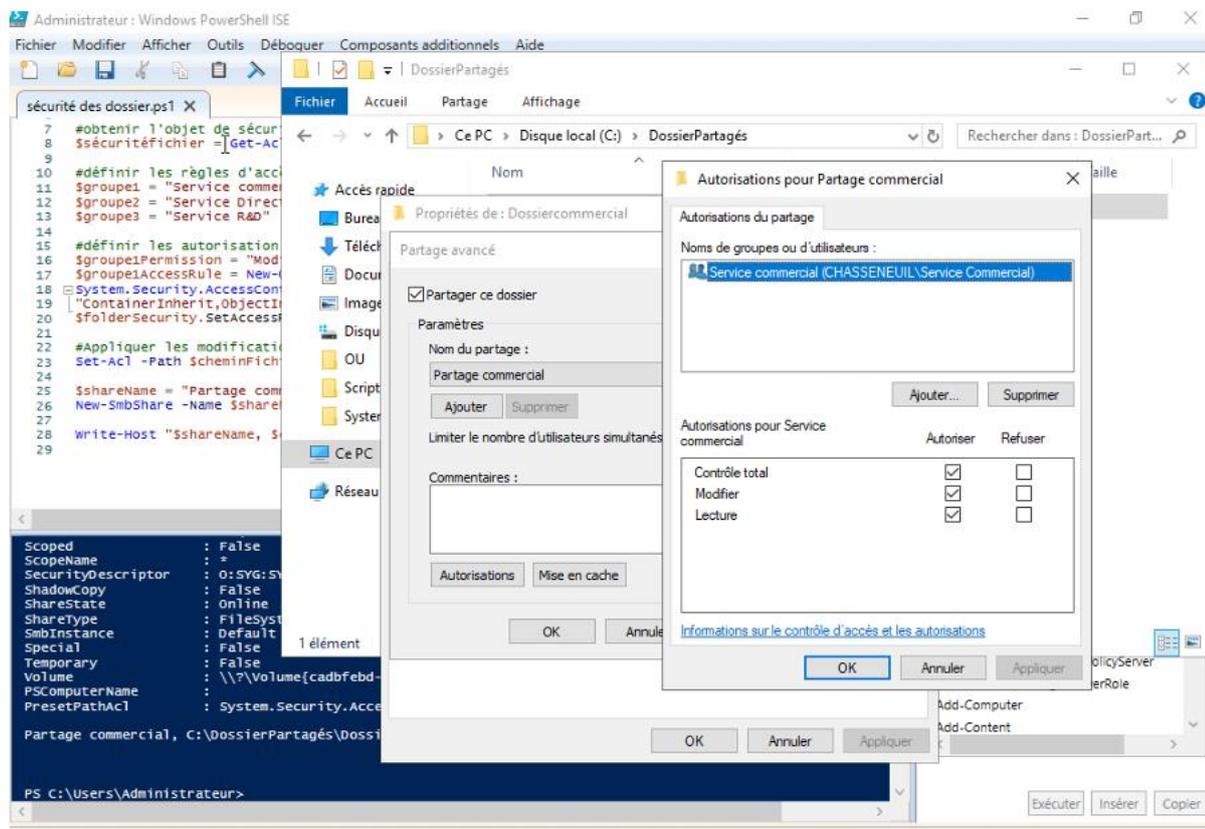
# Créer le partage avec les permissions de partage (différentes des permissions NTFS)
New-SmbShare -Name $shareName -Path $folderPath -FullAccess "Domain\%Service IT" -
ChangeAccess "Domain\%Service Commercial" -ReadAccess "Domain\%Service Comptabilité"

Write-Host "Le partage '$shareName' a été créé avec succès avec les permissions de
sécurité."

```

*Création du partage commercial, accessible que par le groupe Service Commercial*

## **Mission 4 : mettre en place des stratégies de groupe**



### **(GPO)**

*Vous devez mettre en place des stratégies de groupe, afin de répondre aux différents besoins du client ValorElec.*

Objectifs de cette mission:

- Mettre en place des stratégies de groupe (GPO).

#### **Tâche 1**

Installer via une GPO le logiciel **AcrobatReader.msi** pour le client ValorElec.

#### **Tâche 2**

Mettre en place un ensemble de restrictions par stratégies de groupe, comme décrites ci-après.

- Les utilisateurs ne doivent pas avoir accès au panneau de configuration ;
- le mot de passe des utilisateurs doit avoir 8 caractères minimum, changer tous les mois avec un historique de 12 mots de passe qui ne peuvent pas être réutilisés et enfin le compte doit être bloqué à deux tentatives infructueuses d'identification pendant une durée de 10 minutes ;

- pour le service de direction, le mot de passe des utilisateurs doit avoir des caractéristiques plus contraignantes : doit avoir 12 caractères minimum, changer tous les deux mois avec un historique de 24 mots de passe qui ne peuvent pas être réutilisés et enfin le compte doit être bloqué à chaque tentative infructueuse d'identification pendant une durée de 5 minutes

### Tâche 3

Tester l'application des stratégies de groupe sur une machine virtuelle cliente.

## **Définition d'une GPO (Group Policy Object)**

Une **GPO (Group Policy Object)**, ou **stratégie de groupe**, est un ensemble de règles et de configurations appliquées aux **ordinateurs** et aux **utilisateurs** dans un environnement **Microsoft Active Directory**. Elle permet aux administrateurs **d'automatiser, sécuriser et standardiser** la gestion des postes de travail et des serveurs.

Dans notre laboratoire, qui dispose d'un annuaire **Active Directory**, les GPO sont particulièrement utiles pour :

- ✓ **Déployer des logiciels** en utilisant des fichiers **.msi** (contrairement aux **.exe**, qui nécessitent un script de déploiement en **.bat** ou **PowerShell**).
- ✓ **Appliquer des restrictions** (stratégies de mot de passe, limitation des accès aux fonctionnalités des appareils).
- ✓ **Activer l'audit** (suivi des connexions, modifications d'Active Directory, logs Kerberos).

Grâce aux GPO, il est également possible de :

- ✓ **Configurer les paramètres système** (mappage d'imprimantes, connexions réseau).
- ✓ **Appliquer des stratégies de sécurité avancées** (chiffrement des fichiers, blocage de périphériques USB).
- ✓ **Gérer les ressources réseau de manière centralisée** (partages, scripts d'ouverture de session).

Les stratégies de groupe sont essentielles pour assurer une **gestion efficace, sécurisée et homogène** d'un parc informatique, réduisant ainsi les interventions manuelles et les erreurs humaines.

## **Tâche 1**

### Installation automatique d'Acrobat Reader via une GPO

L'objectif est de **déployer automatiquement** le logiciel **Acrobat Reader** sur plusieurs machines sans intervention manuelle. Cette méthode permet **un gain de temps considérable** et évite les déplacements, notamment lorsque les machines sont réparties sur plusieurs sites.

#### *Étapes du déploiement*

##### **1. Téléchargement du fichier d'installation**

- J'ai récupéré le fichier **.msi** d'Acrobat Reader sur un poste isolé.

- Je l'ai ensuite transféré vers **Windows Server 2019** via un dossier partagé.

## 2. Création du dossier partagé pour le déploiement

- J'ai créé un dossier partagé contenant le fichier **.msi**, accessible aux machines clientes.

## 3. Configuration de la GPO

- J'ai ouvert l'**Éditeur de gestion des stratégies de groupe**.
- Je me suis rendu dans :  
**Configuration ordinateur > Stratégies > Paramètres du logiciel.**
- J'ai fait un clic droit > **Nouveau** > J'ai sélectionné le fichier **.msi** sur le partage > **Attribué** > OK.

## 4. Application de la GPO sur une machine cliente

- Sur un **poste Windows 10**, j'ai exécuté la commande suivante pour appliquer immédiatement la stratégie :

```
gpupdate /force
```

- Un message m'a indiqué la prise en compte de l'installation et a demandé un redémarrage.
- Après le redémarrage, Acrobat Reader a été installé automatiquement.

```

PS C:\Users\salarie01> gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.

Les avertissements suivants ont été rencontrés lors du traitement de la stratégie de l'ordinateur :

L'extension côté client de la stratégie de groupe Software Installation n'a pas pu appliquer un ou plusieurs paramètres car les modifications doivent être traitées avant le démarrage système ou la connexion utilisateur. Le système attendra la fin complète du traitement de la stratégie de groupe avant de procéder au prochain démarrage ou à la prochaine connexion pour cet utilisateur. Ceci peut entraîner un ralentissement du démarrage et des performances de démarrage du système.

La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

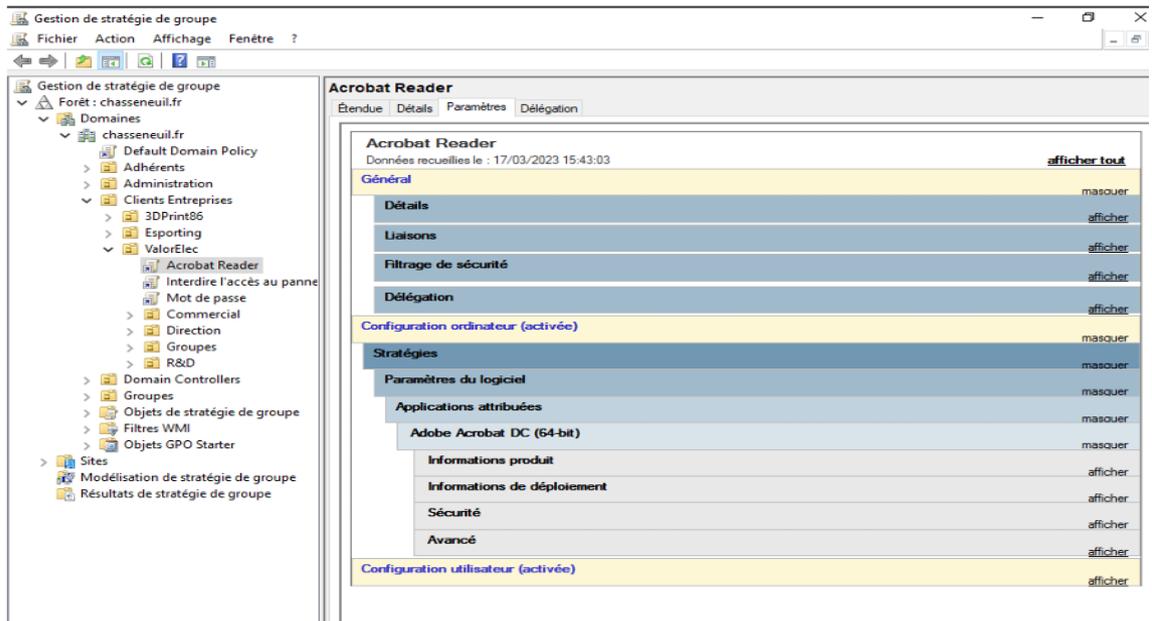
Pour plus de détails, ouvrez le journal des événements ou exécutez GPREsult /H GPREport.html depuis la ligne de commande pour accéder aux résultats de la stratégie de groupe.

Certaines stratégies d'ordinateurs activées peuvent uniquement être exécutées pendant le démarrage.

OK pour redémarrer ? (O/N)

```

*gpupdate /force*



## Tâche 2

Mise en place des restrictions via des GPO

1. Restriction de l'accès au panneau de configuration

Pour interdire l'accès au Panneau de configuration, voici les étapes que j'ai suivies :

1. **J'ai créé une GPO** dans l'Éditeur de gestion des stratégies de groupe pour l'OU **ValorElec**.
2. **J'ai modifié la GPO** :
  - **Chemin** : Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration.
  - **Paramètre** : Interdire l'accès au Panneau de configuration et à l'application Paramètres PC → **Activé**.
3. **J'ai lié la GPO** à l'OU **ValorElec** pour l'appliquer.

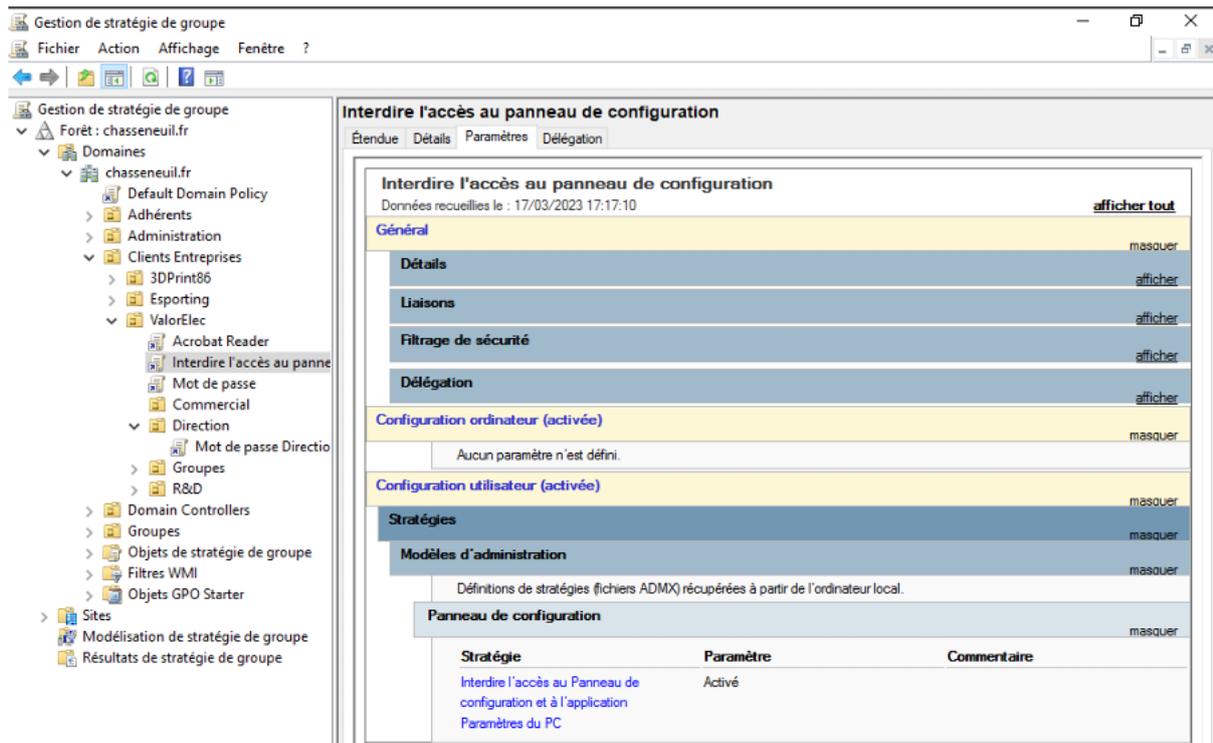
Cette restriction empêche l'accès au Panneau de configuration et aux paramètres du PC pour tous les utilisateurs de l'OU.

## 2. Application de la GPO :

- Sur les machines clientes, **j'ai exécuté** la commande suivante pour forcer l'application immédiate de la GPO :

gpupdate /force

## GPO Interdire l'accès au panneau de configuration



## Politique de mot de passe pour les utilisateurs classiques

Pour configurer la politique de mot de passe des utilisateurs classiques, voici les étapes que j'ai suivies :

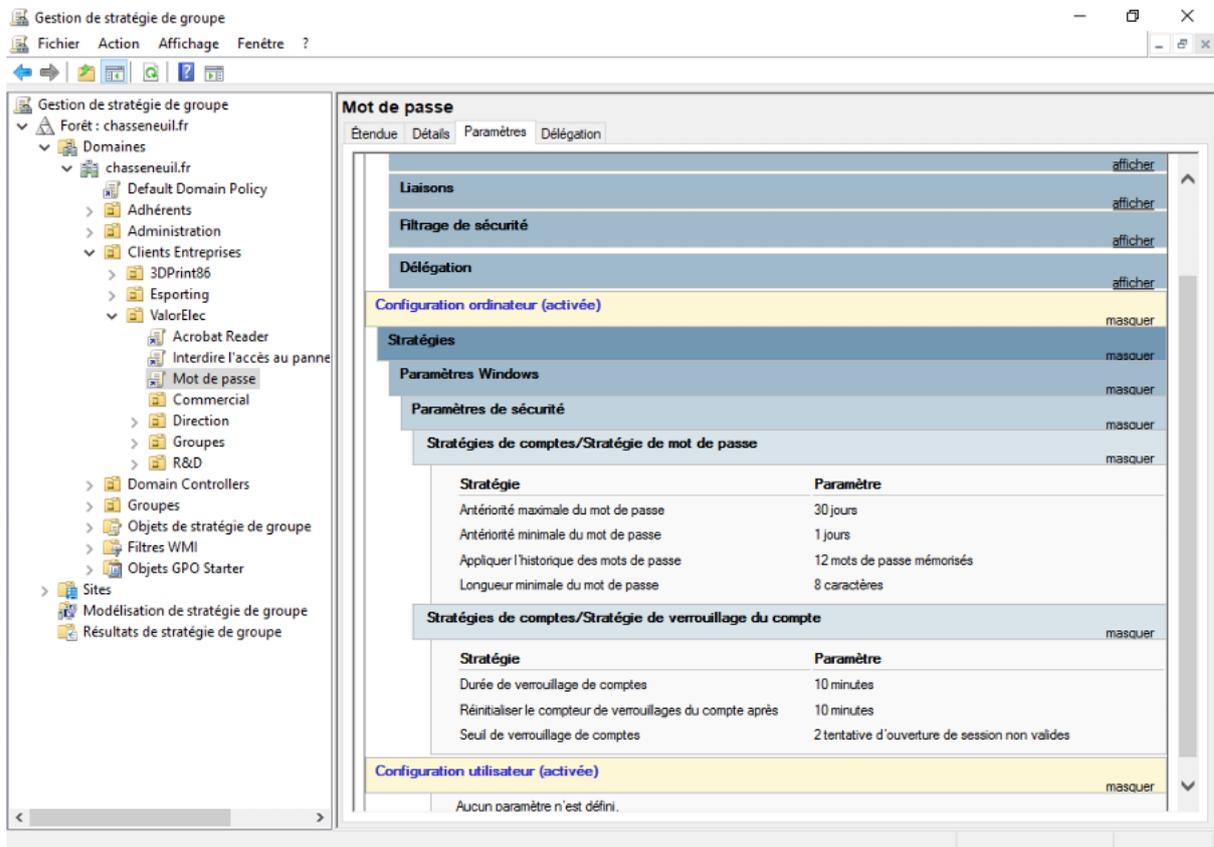
1. **J'ai créé une nouvelle GPO** sur l'OU **ValorElec** dans l'**Éditeur de gestion des stratégies de groupe**.
2. **J'ai configuré les paramètres** de la politique de mot de passe :
  - **Chemin** : Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de mot de passe.
  - **Paramètres appliqués pour les utilisateurs classiques** :
    - **Longueur minimale du mot de passe** → 8 caractères.
    - **Durée de vie maximale du mot de passe** → 30 jours.
    - **Historique des mots de passe** → 12 anciens mots de passe mémorisés.

- **Verrouillage après échec** → 2 tentatives infructueuses, durée du verrouillage 10 minutes.

3. **J'ai lié cette GPO** à l'OU **ValorElec** pour qu'elle s'applique aux utilisateurs classiques.

Cela permet de garantir une sécurité minimum pour les mots de passe des utilisateurs non-direction.

## GPO stratégie de mot de passe Utilisateur



## Politique de mot de passe pour les utilisateurs du groupe Direction

Pour appliquer une politique de mot de passe spécifique aux utilisateurs du groupe **Direction**, voici les étapes que j'ai suivies :

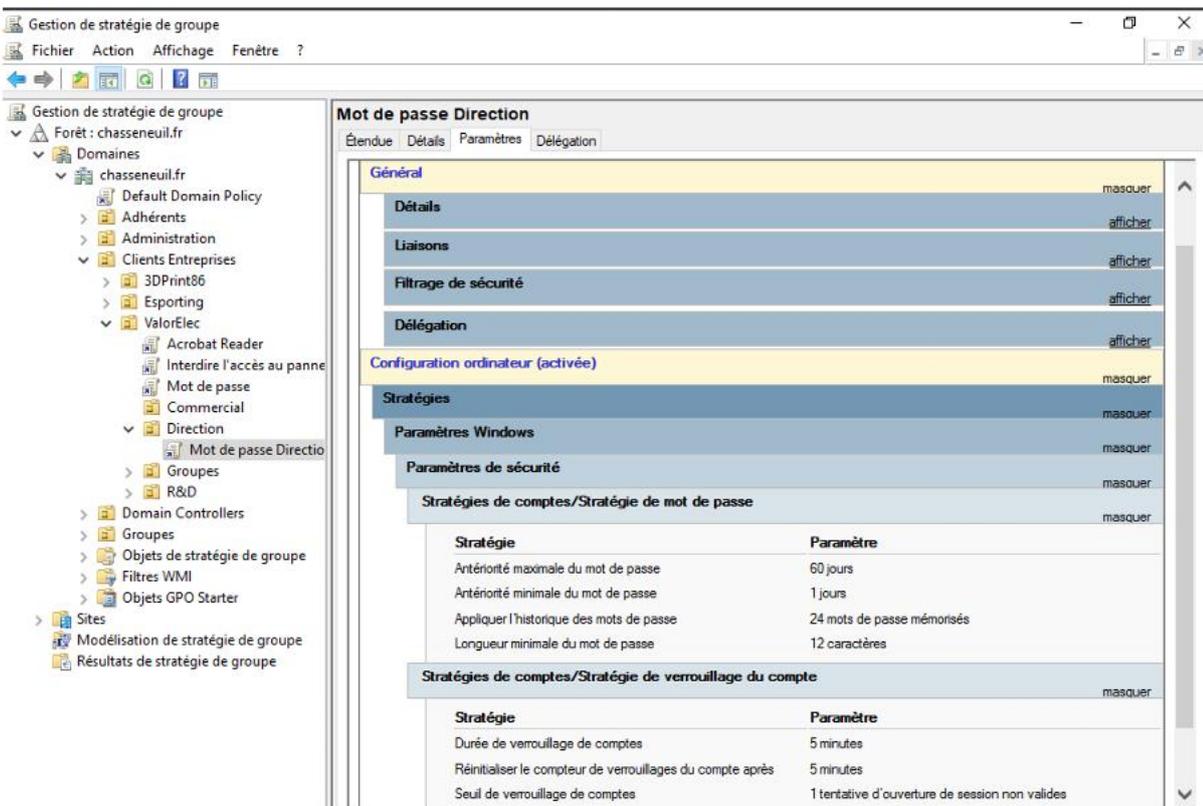
1. **J'ai créé une nouvelle GPO** directement sur l'OU du groupe **Direction** dans l'**Éditeur de gestion des stratégies de groupe**.
2. **J'ai configuré les paramètres** de la politique de mot de passe comme suit :
  - **Chemin** : Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de mot de passe.
  - **Paramètres appliqués pour les utilisateurs de la Direction** :
    - **Longueur minimale du mot de passe** → 12 caractères.

- **Durée de vie maximale du mot de passe** → 60 jours.
- **Historique des mots de passe** → 24 anciens mots de passe mémorisés.
- **Verrouillage après échec** → 1 tentative infructueuse, durée du verrouillage 5 minutes.

3. **J'ai lié cette GPO** à l'OU **Direction** pour que les utilisateurs du groupe bénéficient de ces paramètres renforcés.

Cela permet de renforcer la sécurité des comptes des utilisateurs du groupe **Direction** avec des exigences plus strictes pour les mots de passe.

### GPO stratégie de mot de passe Utilisateur



### Tâche 3

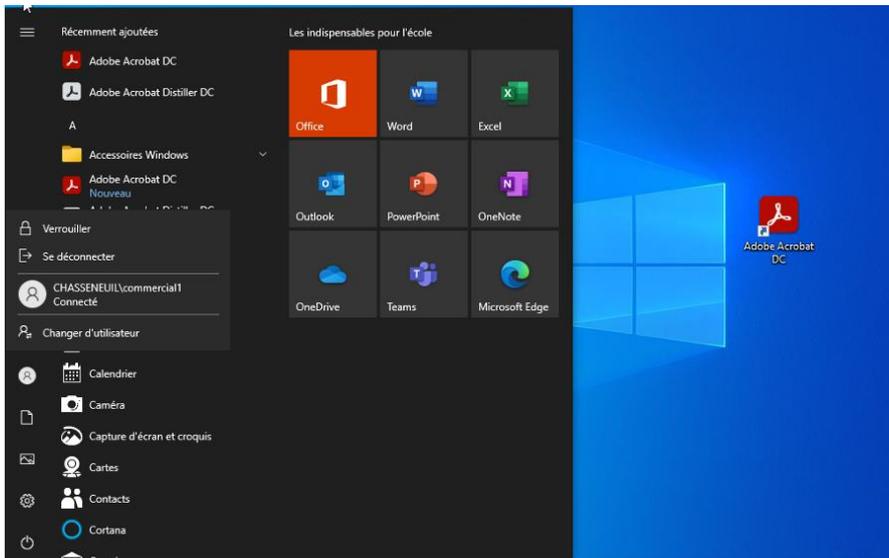
#### Vérification des GPO via un environnement client

Pour cette dernière tâche, j'ai effectué des tests dans un environnement client afin de valider le bon fonctionnement des GPO mises en place. Les résultats sont confirmés par plusieurs captures d'écran disponibles, qui attestent du bon déploiement.

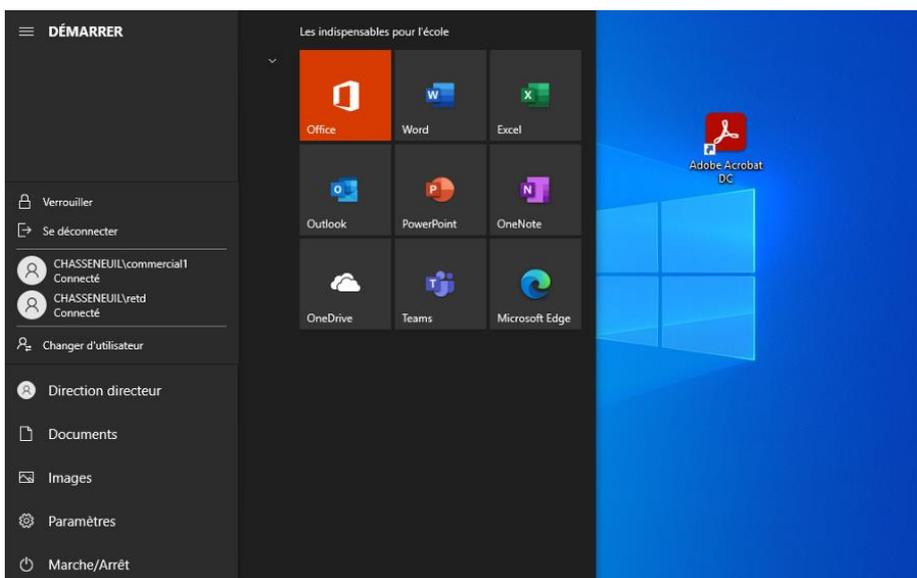
D'abord, j'ai vérifié l'installation du logiciel **Acrobat Reader** via GPO. Sur les bureaux des sessions utilisateurs de **ValorElec**, j'ai constaté que le raccourci du logiciel était présent, ce qui témoigne de

son installation réussie. Cela confirme que la GPO a bien fonctionné et a permis le déploiement correct du logiciel.

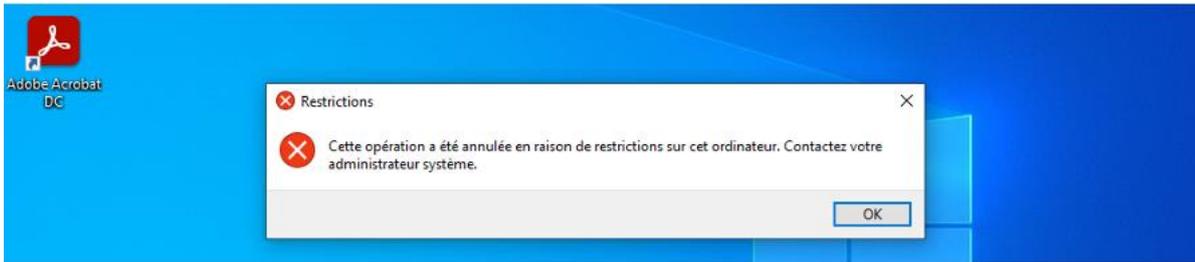
### Session Commercial1 acrobat reader



### Session Direction Directeur acrobat reader



Nous devons d'abord vérifier si la restriction d'accès au panneau de configuration est effective. Si la restriction fonctionne correctement, un message d'erreur doit apparaître, empêchant l'accès au panneau de configuration. Pour cela, je me suis connecté avec le compte "retd", qui fait partie du groupe Service R&D et est soumis à cette restriction. Comme prévu, la GPO a bien été appliquée, ce qui est confirmé par le message d'erreur et le screenshot ci-dessous.



Nous

devons maintenant vérifier l'application de la stratégie de mot de passe. Comme le montre les captures d'écran suivantes, il est impossible de définir un mot de passe qui ne respecte pas la politique en vigueur. Le test a été effectué sur le compte "retld". La politique exige que le mot de passe contienne au moins 8 caractères. Dans ce test, le mot de passe ne comporte que 4 caractères, ce qui entraîne une erreur, comme le montre le deuxième screenshot.

Changement de mot de passe 1

Changement de mot de passe 2

