

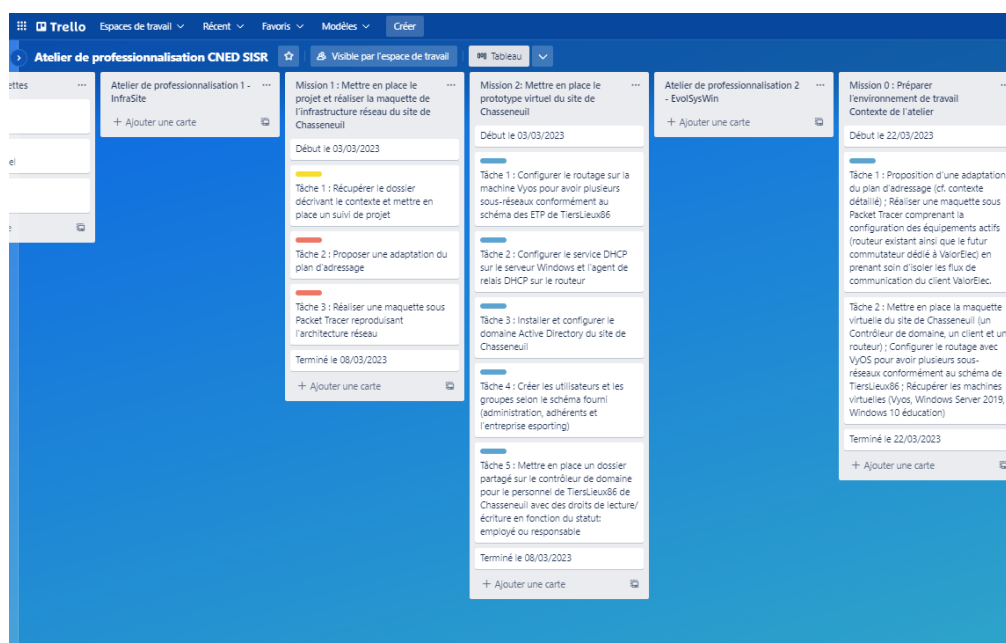
Atelier de professionnalisation 2

EvolSysWin

Sommaire

Contexte.....	2
Mission 0 : Mettre en place le projet et réaliser la maquette de l'infrastructure réseau (Chasseneuil)	3
Mission 1 : Créer la maquette de l'architecture système	4
Mission 2 : Mettre en place un serveur de fichiers	8
Problème rencontrés.....	9
Mission 3 : Automatiser la mise en place de sécurité des partages.....	20
Mission 4 : Mettre en place des stratégies de groupes GPO	23
Qu'est ce qu'une GPO ?.....	23
Sources	39

Cet atelier de professionnalisation se concentre sur l'évolution de l'architecture du système (Windows Server et Active Directory) pour accueillir un nouveau client sur le site de Chasseneuil de TiersLieux86. Pour un suivi du projet reportez vous au Trello en cliquant [ici](#) ou sur l'image.



Contexte

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

En tant qu'assistant du responsable Système et Réseaux d'IT Services 86, nous recevons cet e-mail urgent de votre 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...

Nous sommes chargés de préparer le système d'information de TiersLieux86 pour accueillir le nouveau client, vous devrez intégrer ces personnes au site de Chasseneuil. Le service informatique d'IT Services 86 dispose de la console LAPS pour effectuer des interventions à distance sur les postes de travail.

Mission 0 : Préparer l'environnement de travail

Les prérequis de cet AP sont présentés dans la mission 0

A savoir :

Une adaptation du plan d'adressage après l'étude du dossier documentaire ;
Configurer le routage avec Vyos pour avoir plusieurs sous-réseaux conformément au schéma de TiersLieux86 ;

Ces points ont été abordés et développés dans l'AP 1, je vous invite donc à prendre connaissance du compte rendu.

Mission 1 : Créer la maquette de l'architecture système

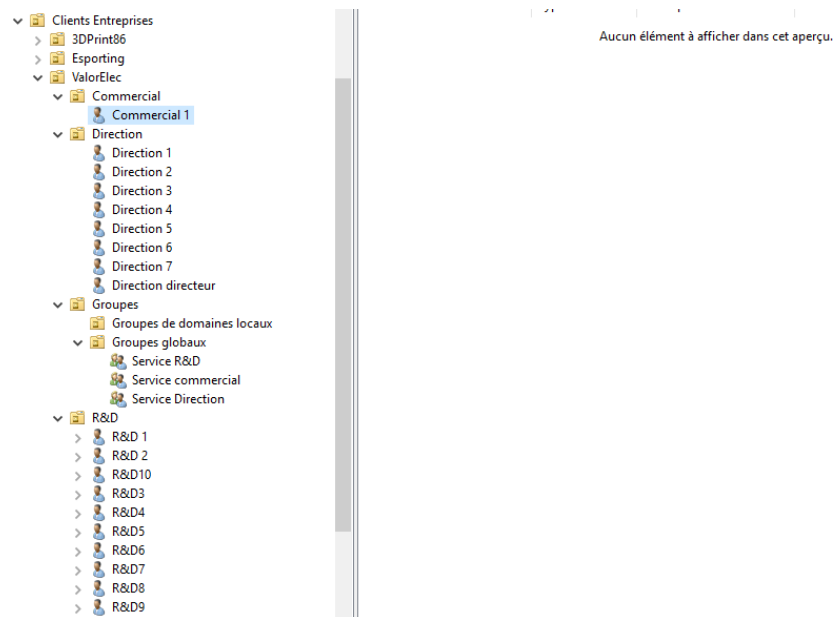
Cette mission se décompose en 2 tâches et vise à intégrer le client ValorElec au site de Chasseneuil, sur l'Active Directory.

Tâche 1

Nous devons élaborer une organisation en unité d'organisation, utilisateurs et groupes pour le client ValorElec, intégré à TiersLieux86. Le client attend l'arrivée de 19 collaborateurs, répartis comme suit : 10 pour le service de recherche et développement, 1 commercial et 8 pour le service de direction (dont le directeur commercial).

Nous proposons de créer trois unités d'organisation, à savoir "Commercial", "Direction" et "R&D", dans l'OU ValorElec. Chacune de ces OU contiendra les utilisateurs de chaque service. Ces utilisateurs seront affectés à des groupes spécifiques : "Service R&D", "Service Commercial" et "Service Direction". Les noms d'utilisateurs iront de R&D1 à R&D10, Commercial 1 sera le seul pour le moment et Direction 1 à Direction 7, incluant le directeur de la direction.

Un screenshot de l'AD est disponible ci-dessous pour avoir un aperçu de l'organisation proposée :



Screenshot Active Directory ValorElec

Tâche 2

Cette tâche vise à automatiser l'administration donc la création d'OU, d'utilisateurs et de groupes tout en générant un document avec les informations personnelles tel que les identifiants de connexion et mots de passe via scripting.

L'objectif est de créer de manière automatique des utilisateurs, des unités d'organisations ou encore des groupes sur l'Active Directory via le lancement d'un script PowerShell par exemple. En effet la création de ces objets est chronophage et amène à l'erreur notamment dans la saisie de nom ou bien même de mots de passe par faute d'inattention. Le but est donc d'éviter cela via un script qui gère la création via un fichier .csv contenant les informations que nous voulons garder. Ainsi le temps passer sur le script sera amorti par l'automatisation et la possibilité de réutiliser celui-ci.

```
New-ADOrganizationalUnit "Commercial2" -Path  
"OU=ValorElec,OU=Clients Entreprises,DC=CHASSENEUIL,DC=FR"
```

Création d'une nouvelle OU

```
New-ADGroup -Name "Service R&D" -Path "OU=ValorElec,Clients  
Entreprises,DC=CHASSENEUIL,DC=FR" -GroupScope Global -Description  
"Service recherche et développemennt"
```

Script Powershell pour la création de groupes

```

#Déclaration du fichier .csv qui sert de base à l'automatisation
$CSVFile = "C:\Scripts\AD_USERS\Utilisateurs.csv"
$CSVData = Import-CSV -Path $CSVFile -Delimiter ";" -Encoding Default

foreach($Utilisateur in $CSVData){

$UtilisateurPrenom = $Utilisateur.Prenom
$UtilisateurNom = $Utilisateur.Nom
$UtilisateurLogin = ($UtilisateurPrenom).Substring(0,1).ToLower() + "." +
$UtilisateurNom.ToLower()
$UtilisateurEmail = "$UtilisateurLogin@chasseneuil.fr"
$UtilisateurMotDePasse = "SacCEVv2"
$UtilisateurGroupe = Utilisateur.Groupe

#Vérifier la présence de l'utilisateur dans l'AD
if (Get-ADUser -Filter {SamAccountName -eq $UtilisateurLogin})
{
Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'annuaire"
}
else
{
New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom" `
-DisplayName "$UtilisateurNom $UtilisateurPrenom"
`
-GivenName $UtilisateurPrenom `
-Surname $UtilisateurNom `
-SamAccountName $UtilisateurLogin `
-UserPrincipalName
"$UtilisateurLogin@chasseneuil.fr" `
-EmailAddress $UtilisateurEmail `
-Path OU=ValorElec,OU=Clients
}
}

```

```

Entreprises,DC=CHASSENEUIL,DC=FR`
    -AccountPassword(ConvertTo-SecureString
$UtilisateurMotDePasse -AsPlainText -Force) `
    -ChangePasswordAtLogon $false `
    -Enabled $true `
    -AdGroupeMember $UtilisateurGroupe
    Write-Output "Création de l'utilisateur : $UtilisateurLogin
($UtilisateurNom $UtilisateurPrenom $UtilisateurMotDePasse)"
    $Utilisateur | Select-Object Prenom, Nom, Login, Email,
MotDePasse | Export-Csv -Path "utilisateurs_creés.csv"
-NoTypeInfoInformation -Append
    }
}

```

Script PowerShell pour la création d'utilisateur avec un fichier .csv

```

$Utilisateur | Select-Object Prenom, Nom, Login, Email,
MotDePasse | Export-Csv -Path
"C:\Users\Scripts\utilisateurs_creés.csv" -NoTypeInfoInformation
-Append

```

Script pour exporter au format .csv l'identifiant de connexion, le mot de passe et d'autres infos

Ainsi, un fichier csv peut permettre via le bon script et les bons paramètres de créer un nombre d'utilisateurs important dans un temps restreint.

Mission 2 : Mettre en place un serveur de fichiers

Cette mission est portée sur le besoin pour les entreprises de pouvoir stocker les informations ainsi que de partager leurs travaux et cela entre les différents collaborateurs qui la constituent. Elle est divisée en 2 tâches, premièrement mettre en place un serveur de fichiers basé sur du stockage iSCSI et deuxièmement réaliser une étude sur l'implémentation d'une racine dédiée DFS pour le client ValorElec.

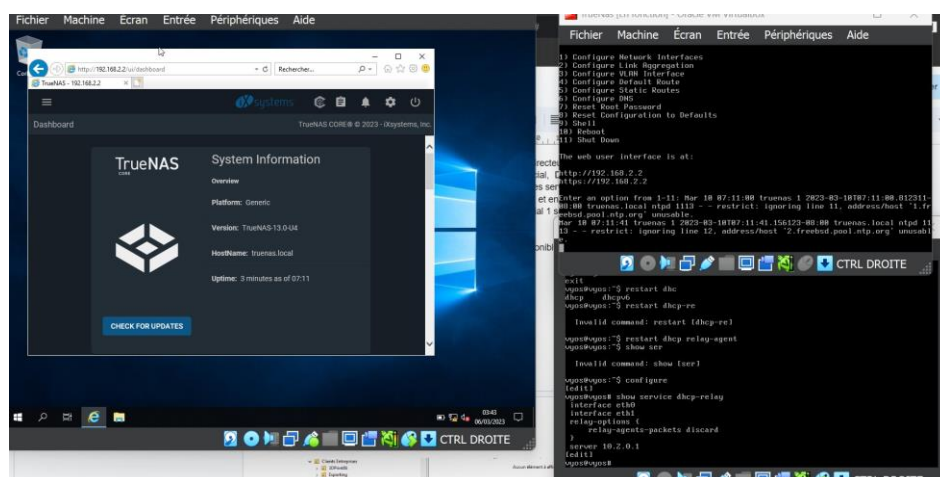
Tâche 1

Qu'est-ce que le protocole iSCSI ?

iSCSI ou Internet Small Computer System Interface est un protocole de la couche 4 du modèle OSI soit de la couche transport. Cela permet donc de partager des fichiers et des données via le protocole internet et de les stocker sur un serveur annexe permettant de mettre à disposition des utilisateurs les données stockées.

Nous devons donc configurer une machine virtuelle avec l'image ISO de TrueNAS. Faire en sorte d'allouer assez de ressources pour le serveur de données. Par la suite nous pouvons renseigner l'adresse IP qui est grâce au relais DHCP dynamiquement allouée. Ensuite nous créons un volume basé sur un disque ajouter préalablement. Pour ma configuration j'ai mis le RAID 1 soit le mirroring qui permet d'avoir une réplication, un clonage en temps réel des données d'un disque sur l'autre amenant une sécurité en cas de dysfonctionnement d'un disque. Une fois cela configuré nous devons réserver une adresse IP sur le pool DHCP via l'interface en renseignant l'adresse IP qui à été donnée par le relai DHCP visible directement sur la console. Pour moi, ayant eu de nombreux problèmes, ce sera l'adresse 192.168.2.9. Pour bénéficier du relai, il faut placer le serveur TrueNAS sur le LAN Bureau.

Installation et configuration du service TrueNAS



Problèmes rencontrés

Pour des raisons de performances, certaines des images illustrant les démarches sont tirées d'internet, des images de mes VM et des tests seront disponibles lors de la conclusion.

Impossibilité de créer un pool : Bien que les paramètres soient bons, la création du volume une fois validé tourne indéfiniment. Pour éviter cela, nous devons configurer TrueNas depuis une machine cliente, le problème est la consommation de ressources de l'ordinateur hôte qui avec 4 vm ne suit plus trop.

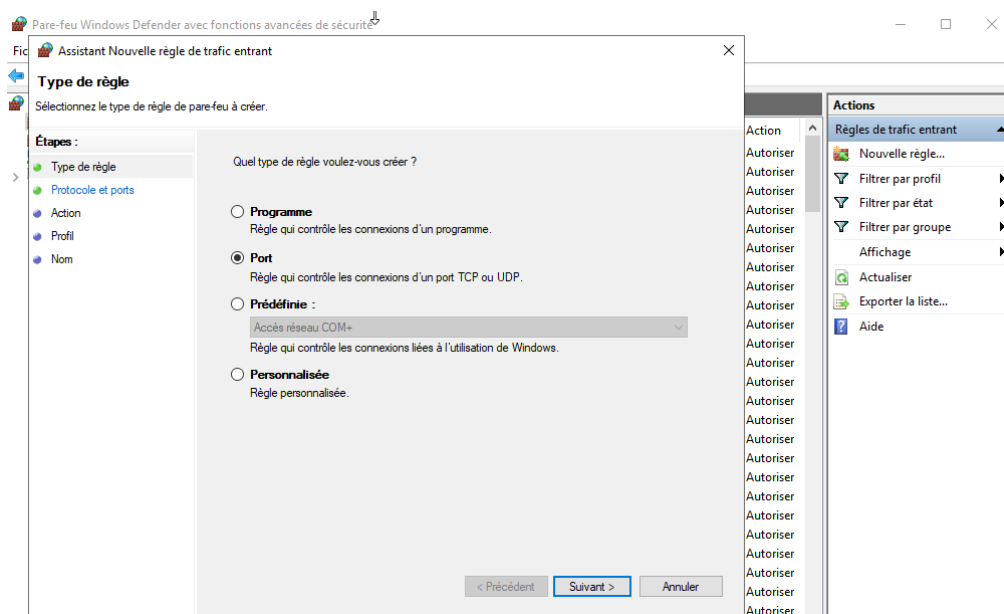
Impossibilité d'incorporer le TrueNas au domaine : En effet l'authentification sur l'active directory se fait en partie via Kerberos. Qui n'aime pas du tout la différence de temps entre deux machines. D'une manière générale, nous aurions simplement dû synchroniser les horloges des deux machines en fonction d'un même serveur NTP (Network Time Protocol) à l'image de ntp.u-strasbg.fr hors nous sommes en réseau local, ce qui rends la tâche un peu plus compliquée. Nous devons donc configurer un service NTP sur le serveur Windows Server 2019. Pour cela rendez-vous sur l'éditeur de registre via win+r "regedit" :

"Computer\HKEY_LOCAL_MACHINE\SYSTEM\NtpServer vérifier que Enabled finis par un 1 sinon clic droit>modifier>1 dans ValueData

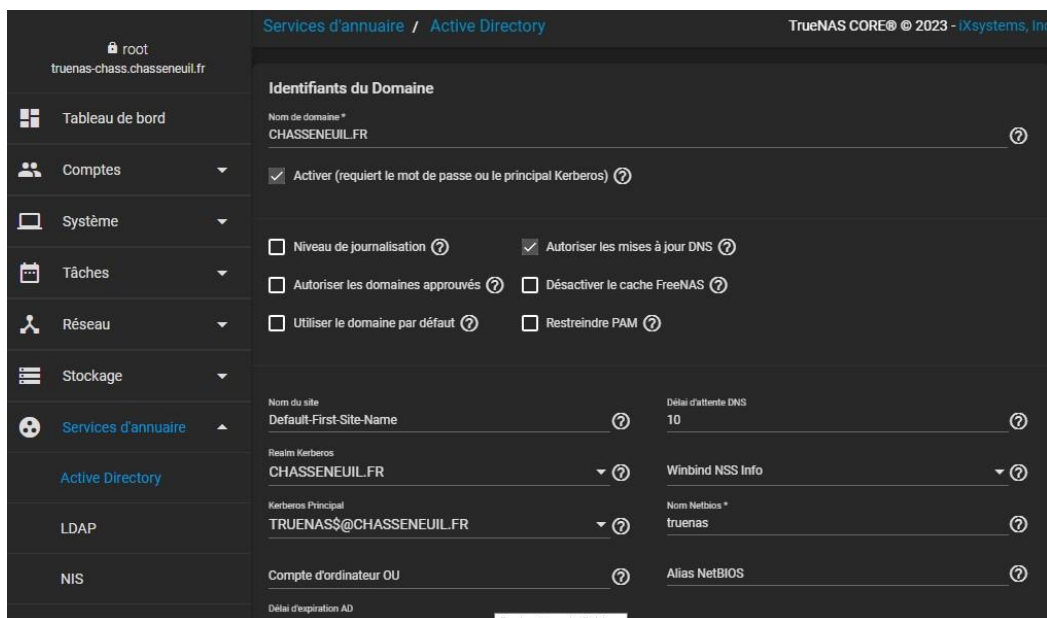
"Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Win32\Time\Config">AnnounceFlags doit avoir comme valeur 5 dans ValueData

Ensuite, nous devons redémarrer le service "Windows Time" pour cela win+r "Service", nous recherchons "windows time" dans la liste et clic droit>démarrer.

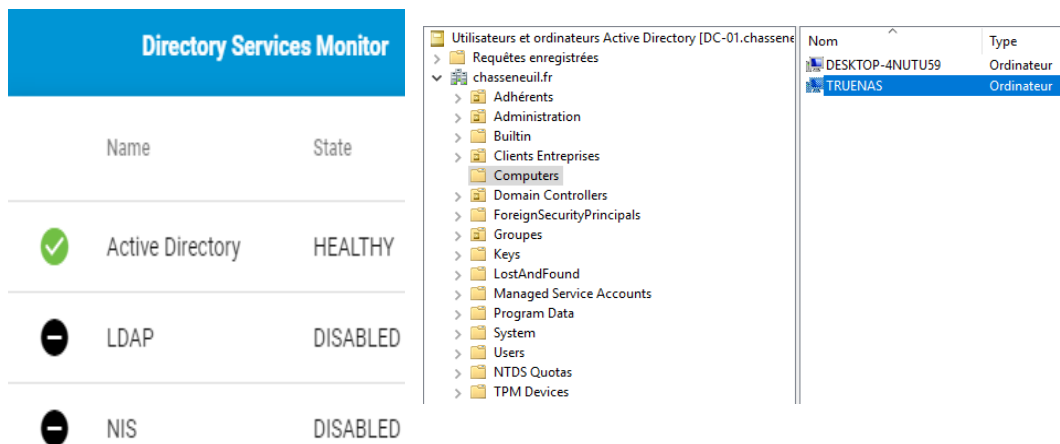
De plus, pour éviter tout problème de firewall, j'ai ouvert le port UDP 123 qui permet au NTP de fonctionner.



Ouverture du port 123 UDP pour le service NTP



Configuration de la rubrique Active Directory

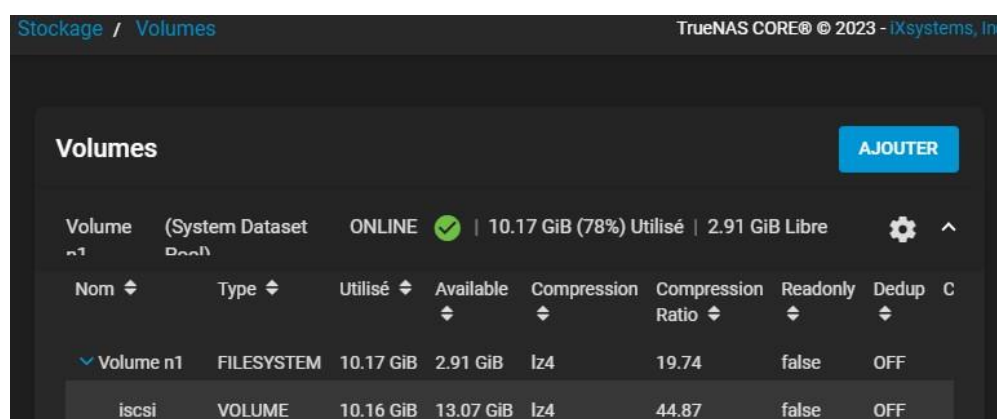


Vérification de l'intégration à l'AD

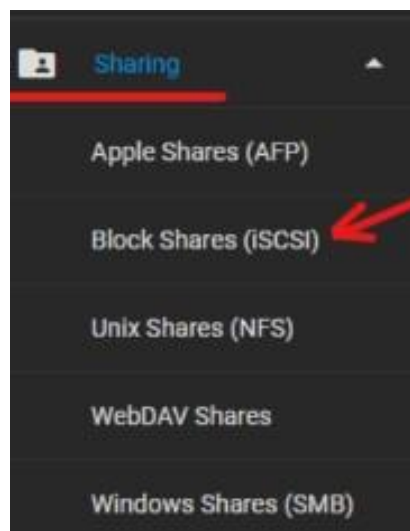
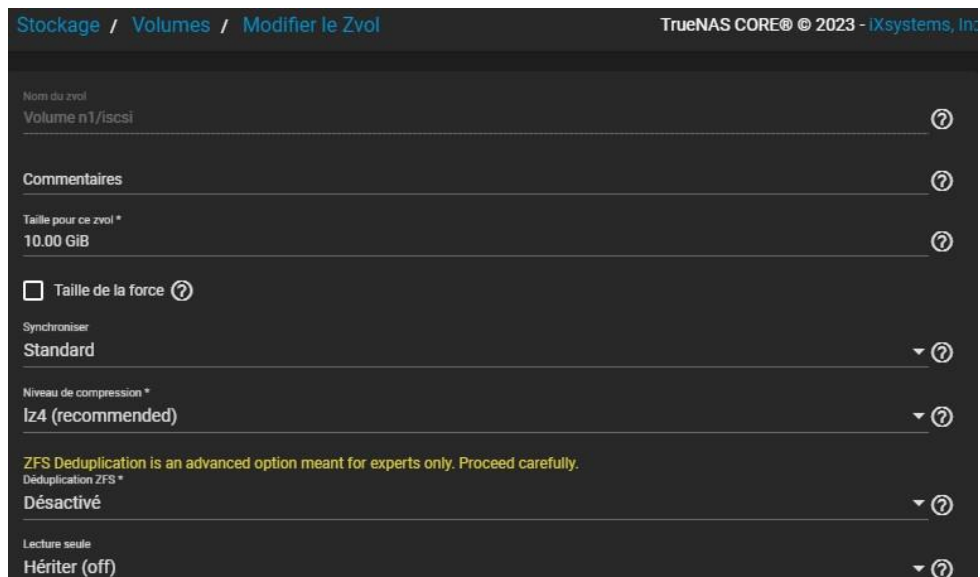
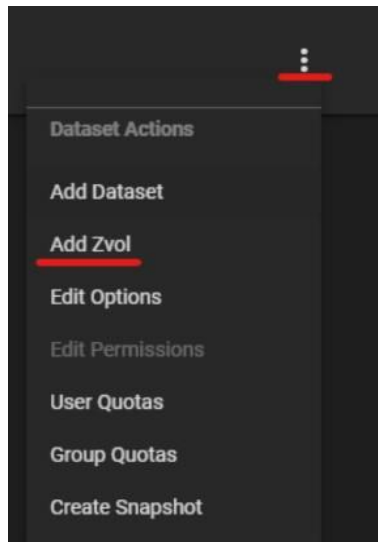
Nous pouvons constater que TrueNas est bien intégré au site de Chasseneuil.

Continuité du projet

Une fois ces problèmes corrigés, nous pouvons passer à la création du partage iSCSI, pour cela nous devons configurer le serveur TrueNas et ensuite nous devons configurer les clients. Pour cela nous devons configurer le pool ou volume de stockage initialement créé. Nous devons ajouter un Zvol et le configurer. Nous devons ensuite nous rendre dans les partages iSCSI et le configurer là aussi. Pour les adresses IP nous pouvons mettre l'IP 0.0.0.0 qui écouterait toutes les IP. Nous devons ensuite créer une cible dans l'onglet Target puis l'onglet extents où nous devons déclarer le nom que notre Zvol va utiliser. (Pour voir en détail les configurations effectuées, des screenshots sont présentés ci-dessous).



Création du Zvol



WIZARD

Target Global Configuration

Portals

Initiators Groups

Authorized Access

Cibles

Extents

Associated Targets

Configuration globale

Nom de base *

iqn.2005-10.org.freenas.cti

?

Serveurs ISNS

?

Seuil d'espace disponible dans le volume (%)

?

ENREGISTRER

Infos de base

Description

Portail

?

Méthode et groupe d'authentification

Méthode d'authentification de découverte

NONE

?

Groupe d'authentification de découverte

?

Adresse IP

Adresse IP *

0.0.0.0

?

Port

3260

?

AJOUTER

ENREGISTRER

ANNULER

Infos de base

Nom de la cible *

lun1

Alias de la cible

lun1

groupe iSCSI

ID de groupe du portail *

1 (Portail)

ID de groupe de l'initiateur

Méthode d'Authentification

Aucun

Numéro du groupe d'authentification

AJOUTER

ENREGISTRER ANNULER

Cible associée

Cible *

lun1

ID LUN

0

Etendre *

lzvol1

ENREGISTRER ANNULER

Infos de base

Nom *

lzvol1

Description

☒ Activé

Type

Type d'étendue

Périphérique

Périphérique *

Volume n1/iscsi (10.0G)

Numéro de série

0800274d141b000

Taille du bloc logique

512

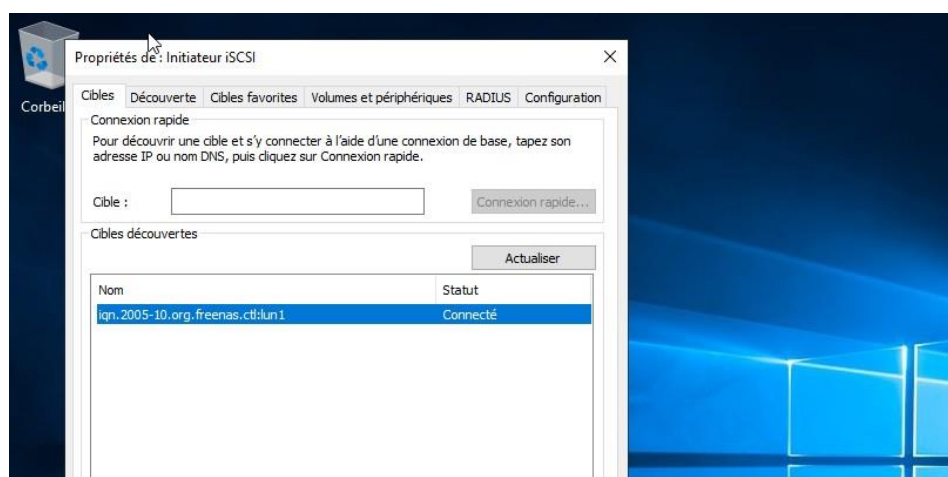
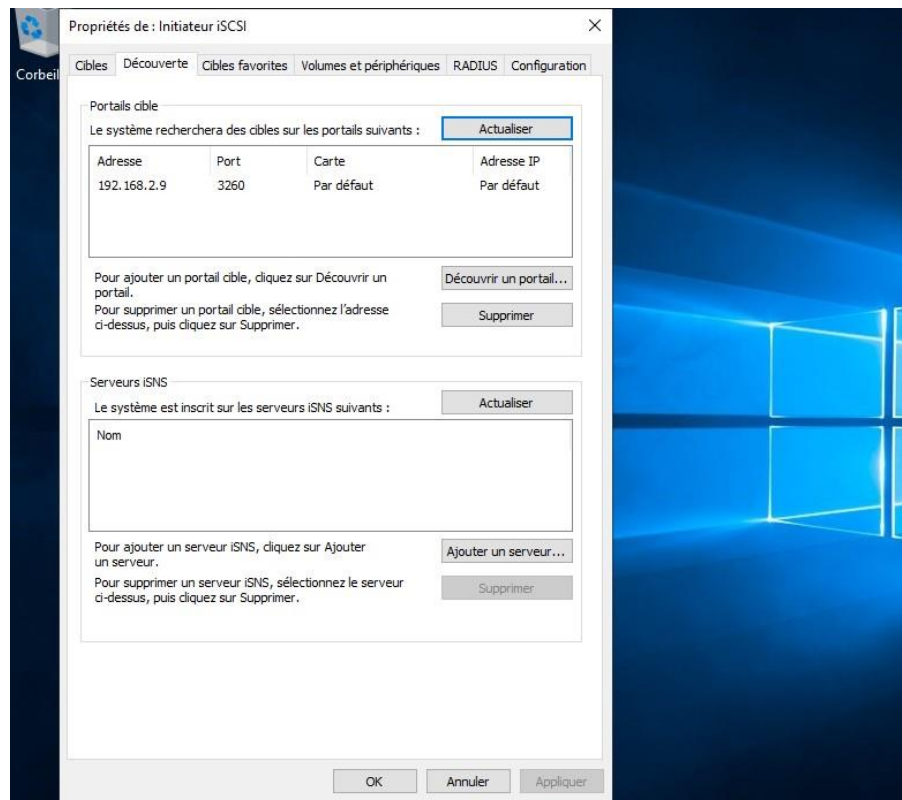
☐ Désactiver le rapport sur la taille des blocs physiques

Seuil d'espace disponible (%)

Compatibilité

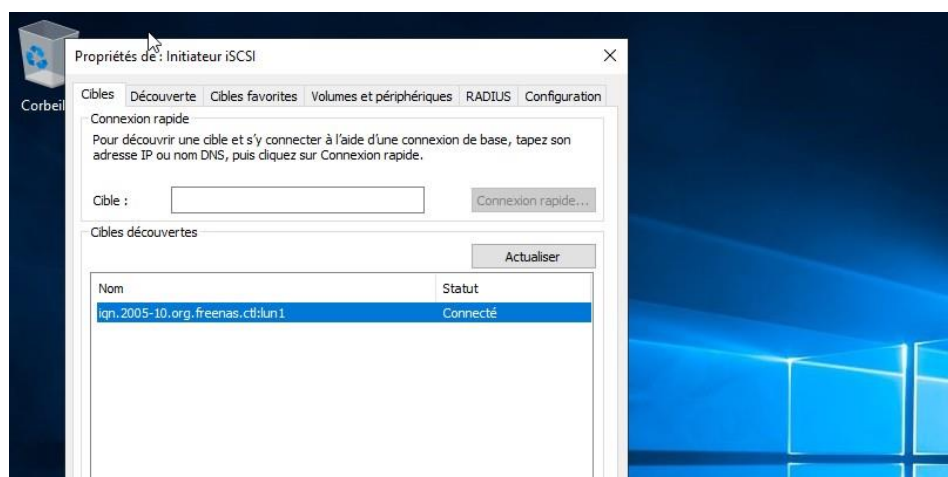
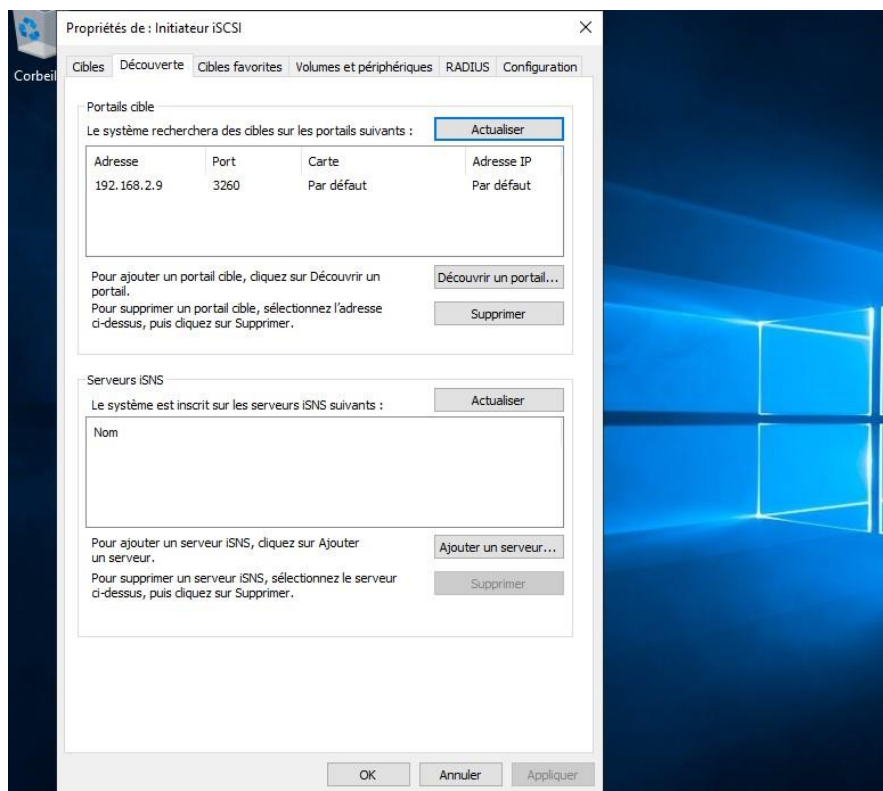
Configuration du partage iSCSI

Nous devons par la suite configurer les clients. Ceux-ci doivent recevoir une configuration de l'initiateur iSCSI. Nous devons pour découvrir notre serveur TrueNas renseigner l'adresse IP qui pour moi est 192.168.2.9 dans "Découvrir un portail".



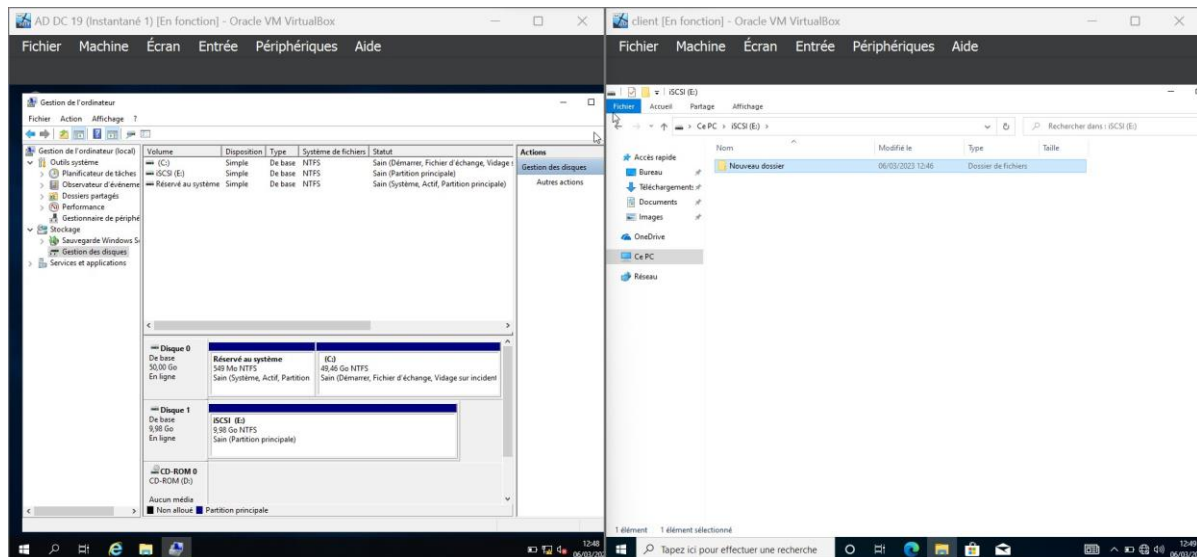
Propriété de l'initiateur iSCSI

Nous devons par la suite configurer les clients. Ceux-ci doivent recevoir une configuration de l'initiateur iSCSI. Nous devons pour découvrir notre serveur TrueNas renseigner l'adresse IP qui pour moi est 192.168.2.9 dans "Découvrir un portail".



Propriété de l'initiateur iSCSI

Par la suite le disque n'est pas alloué, nous devons donc nous rendre sur le contrôleur de domaine et dans le gestionnaire de l'ordinateur, le disque nouvellement intégré n'est pas en ligne, pour cela clic droit>mettre en ligne. Ensuite nous allouons la partition et ainsi le disque en ligne apparaît dans notre environnement pas sous l'interface réseau, mais bien sur l'interface "ce pc", donc en local. Le serveur iSCSI est donc bien configuré.



Présence dans l'environnement client du disque E, après paramétrage de l'initiateur iSCSI.

- ☒ Mettre en place un serveur de fichier basé sur du stockage iSCSI

Tâche 2

L'objectif de cette tâche est de réaliser une étude sur l'implémentation d'une racine dédiée DFS (avantages et inconvénients) pour le client ValorElec.

Qu'est ce que le DFS ?

Le DFS pour Distributed File System ou Système de fichier distribués est un système de fichier hiérarchisé. C'est-à-dire qu'il permet de structurer les fichiers partagés sur différents serveurs du réseau de manière logique. Ainsi, l'utilisateur final ne visualise pas le nom du serveur sur lequel il accède. Si le serveur vient à changer alors le chemin restera le même.

Qu'est ce qu'une racine DFS ?

La racine DFS est le point d'entrée principal d'un système, elle contient le chemin d'accès aux différentes liaisons DFS qui lui sont associées.

Points positifs et négatifs

Ainsi, créer une racine DFS serait optimale pour l'organisation de ValorElec, une racine permettant de créer des dossiers et sous dossier pour une meilleure organisation. Ces dossiers pourraient cibler un serveur tel que le TrueNas créé précédemment.

De plus, le DFS a d'autres points positifs à l'image de la simplicité d'administration en effet, celui-ci est intégré à windows, de plus un déplacement du chemin vers un autre serveur si l'un est défaillant est possible, la performance via la mise en cache pour augmenter les performances ou encore l'équilibrage de charge mais aussi la tolérance aux pannes, par ailleurs, l'évolutivité est un point important puisque un espace disque peut-être ajouté si l'espace de stockage est saturé et la sécurité de celui-ci.

Le problème étant la mise en place, la mise à disposition d'un serveur pour ValorElec à lui seul et la demande. L'entreprise reste tout de même petite voir moyenne et la génération de données n'est peut-être pas assez importante pour privatiser, créer une racine. Sachant qu'avec un serveur TrueNas joint au domaine comme vue plus haut, cela pourrait suffire.

Mission 3 : Automatiser la mise en place desécurité des partages

Tâche 1

Proposer sous forme de tableau les utilisateurs, groupes et droits associés sur les partages. Le but d’une telle manipulation est de donner les bon droit d’accès sur les partages de fichiers aux bonnes personnes. Une étude préalable doit donc être faite et cela via des tableurs. Nous allons nous concentrer sur le cas de ValorElec puisque c’est le sujet de cet AP. ValorElec est découpé en 3 services, un service de direction comportant 8 employés dont un directeur, un service de recherche et développement composé de 10 employés et un service commercial comportant 1 employé.

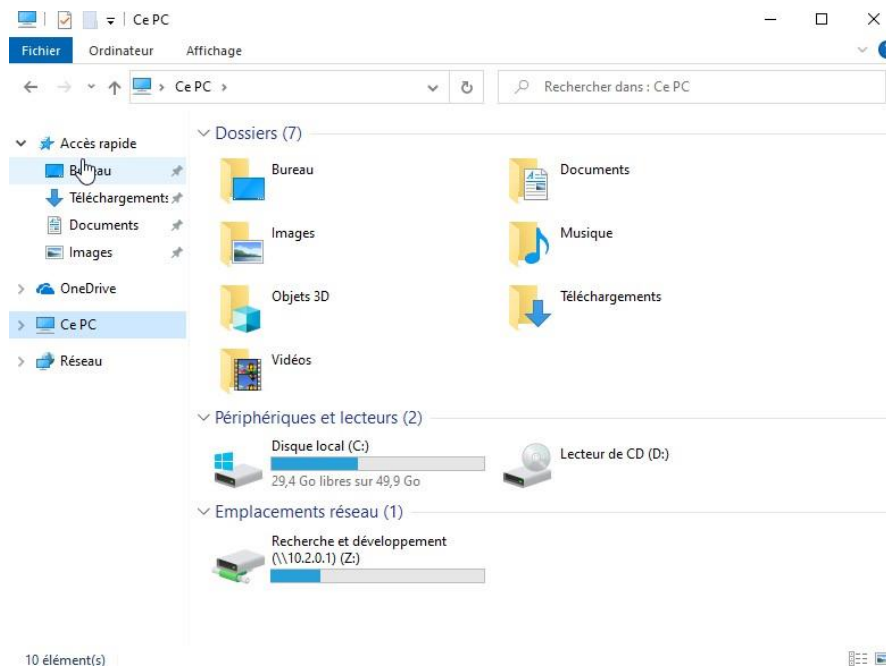
Nous pouvons donc imaginer un partage commun aux différents services, ainsi qu’un partage par services.

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	

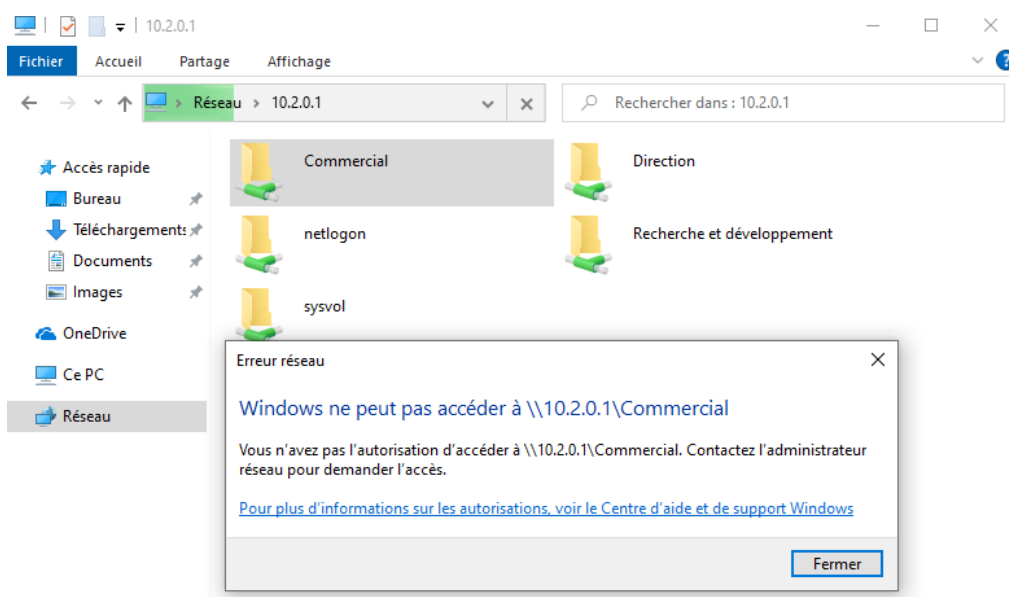
Appartenances des utilisateurs au groupes en fonction des services		Groupes Globaux		
		Service Recherche et développement	Service Commercial	Service Direction
Utilisateurs	R&D 1 à 10	X		
	Direction 1 à 7			X
	Directeur direction	X	X	X
	Commercial 1		X	

Légende : X Membre de ...

Tableau de synthèse des droits



Session retd du groupe service R&D après la mise en place du dossier partagé



Session retd du groupe service R&D, impossibilité d'accéder au partage du groupe commercial

Nous devons donc essayer de reproduire la même chose de manière automatisée en ne renseignant que les informations nécessaires et donc en évitant toutes les manipulations via l'interface graphique.

Tâche 2

Le but est donc d'automatiser la création de dossier partagé avec powershell tout en incorporant les droit d'accès pour augmenter la sécurité.

Pour pouvoir créer un partage SMB sous windows et automatiser la sécurité des partages nous pouvons utiliser le script New-SmbShare -Name Partage\$ -Path "C:\Dossier partagés\Commercial" -FullAccess "Service commercial" -ReadAccess "Utilisateurs".

Nous pouvons de plus chercher à lister les droits actuels sur un dossier avec Get-NTFSAccess -Path "C:\Dossier partagés\Commercial" par exemple. Or nous devons installer au préalable le module NTFS Security avec la commande Install-Module NTFSSecurity. Dans mon cas des messages d'erreurs sont retournés lors de la tentative d'installation du module, j'ai donc opter pour une autre solution.

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

# Créer le dossier
New-Item -ItemType Directory -Path $folderPath

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

# Définir les règles d'accès pour le groupe
$group1 = "Service Commercial"

# Définir les autorisations pour le groupe 1
$group1Permission = "Modify"
$group1AccessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule($group1,
$group1Permission, "ContainerInherit, ObjectInherit", "None", "Allow")
$folderSecurity.SetAccessRule($group1AccessRule)

# Appliquer les modifications à l'objet de sécurité pour le dossier
Set-Acl -Path $folderPath -AclObject $folderSecurity

# Partager le dossier
$shareName = "C:/Dossier Partagé/"
New-SmbShare -Name $shareName -Path $folderPath -FullAccess
$group1,$group2,$group3
```

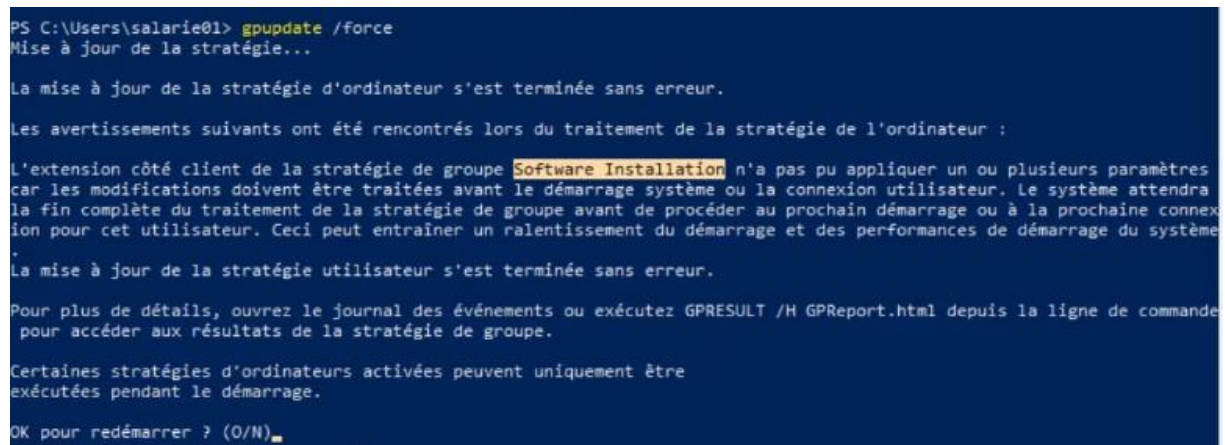

Tâche 1

Le but de cette tâche est l'installation automatique du logiciel Acrobat Reader via une stratégie de groupe donc un GPO. L'objectif est le gain de temps, il n'est pas nécessaire de faire les manipulations sur chaque machine et dans une situation où les machines ne se trouveraient pas dans le même bâtiment. Cela simplifie donc l'administration du parc informatique.

La première étape est le téléchargement du fichier .msi de Acrobat Reader. Je l'ai fait via mon pc Hôte qui est isolé de mon lab virtuel. J'ai ensuite partagé le dossier entre mon hôte et ma machine Windows Server 2019 pour avoir accès au fichier.

Pour créer une GPO d'installation de logiciels, nous devons créer un dossier partagé qui permettra à nos ordinateurs de récupérer le chemin du fichier à installer. Nous devons ensuite nous rendre dans l'Éditeur de gestion des stratégies de groupe>Configuration ordinateur>Stratégies>Paramètre du logiciel>Clic droit>Nouveau>Chemin du fichier .msi sur le partage>Ouvrir>Attribué>Ok

Nous pouvons ensuite nous rendre sur un client windows 10, nous forçons la mise à jour de notre stratégie de groupe via la commande `gpupdate /force` qui peut être tant exécuter sur CMD que PowerShell. Nous pouvons constater un retour avec la mention Software Installation et une demande pour redémarrer la machine, nous entrons O et l'installation s'exécute lors du redémarrage. Nous pouvons constater via les screenshot suivant que l'installation a bien eu lieu.



```
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.

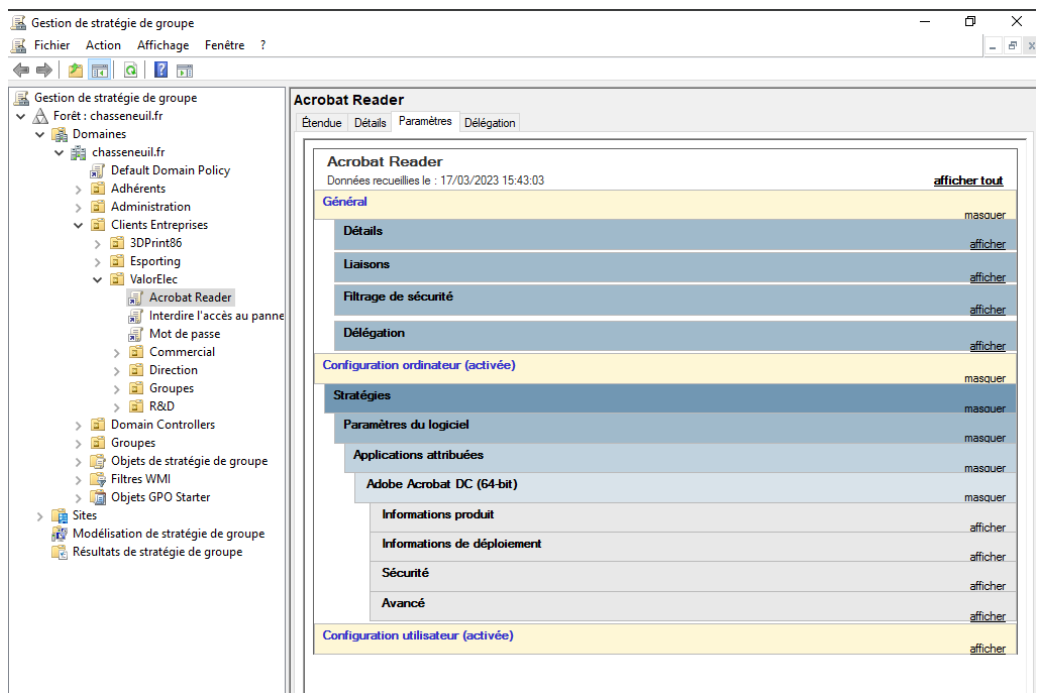
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

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



Contenue de la GPO de déploiement d'Adobe Reader

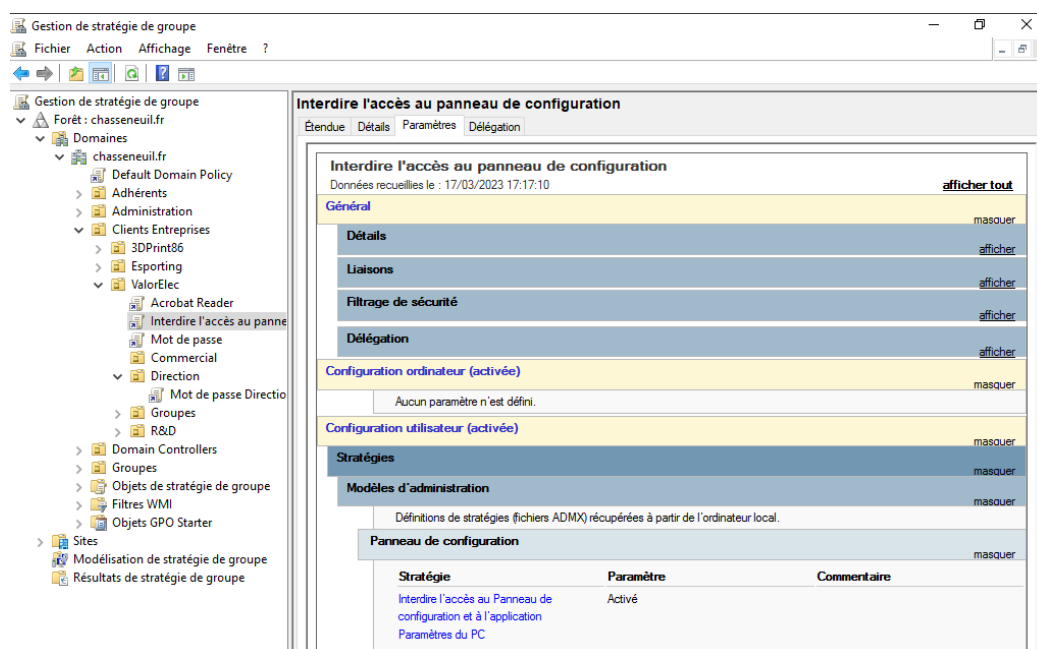


Présence du logiciel sur l'environnement ValorElec

Tâche 2

La tâche numéro deux consiste en la création de restriction pour les utilisateurs, pour éviter des mauvaises manipulations ou des intentions malveillantes. Pour cela différentes GPO doivent être mises en place. Une GPO interdisant l'accès au panneau de configuration devra être appliquée, deux GPO relatives à la politique de mot de passe en fonction des services seront configurées, l'une pour les utilisateurs classiques et l'autre pour les utilisateurs du groupe Direction.

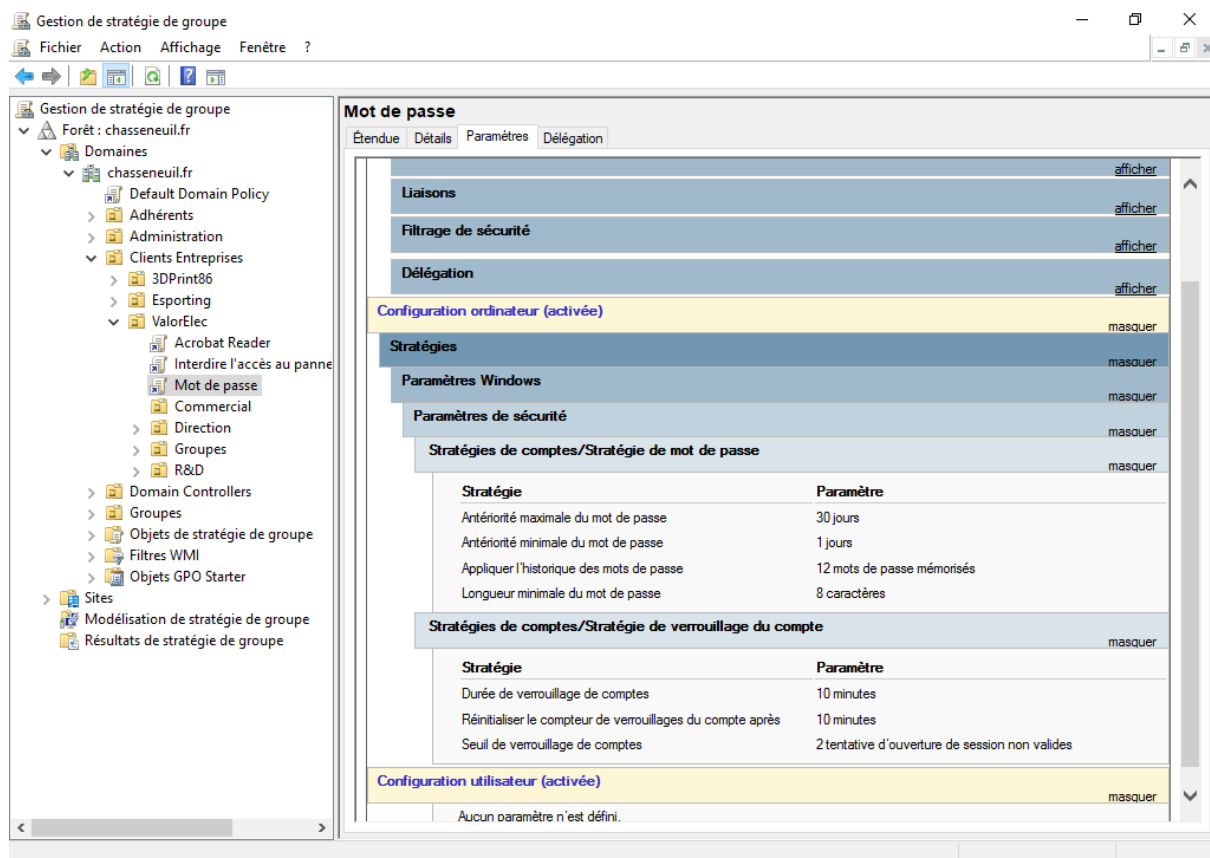
Nous réalisons premièrement la restriction sur le panneau de configuration. Pour cela nous nous rendons dans l'Éditeur de stratégie de groupe et créons une nouvelle stratégie sur l'OU de ValorElec. Sa fonction sera d'interdire l'accès au panneau de configuration. Pour cela nous allons dans Configuration utilisateur>Stratégie>Modèle d'administration>Panneau de configuration>Double clic sur Interdire l'accès au Panneau de configuration et à l'application paramètre du PC>Activé.



GPO Interdire l'accès au panneau de configuration

☒ Les utilisateurs ne doivent pas avoir accès au panneau de configuration;

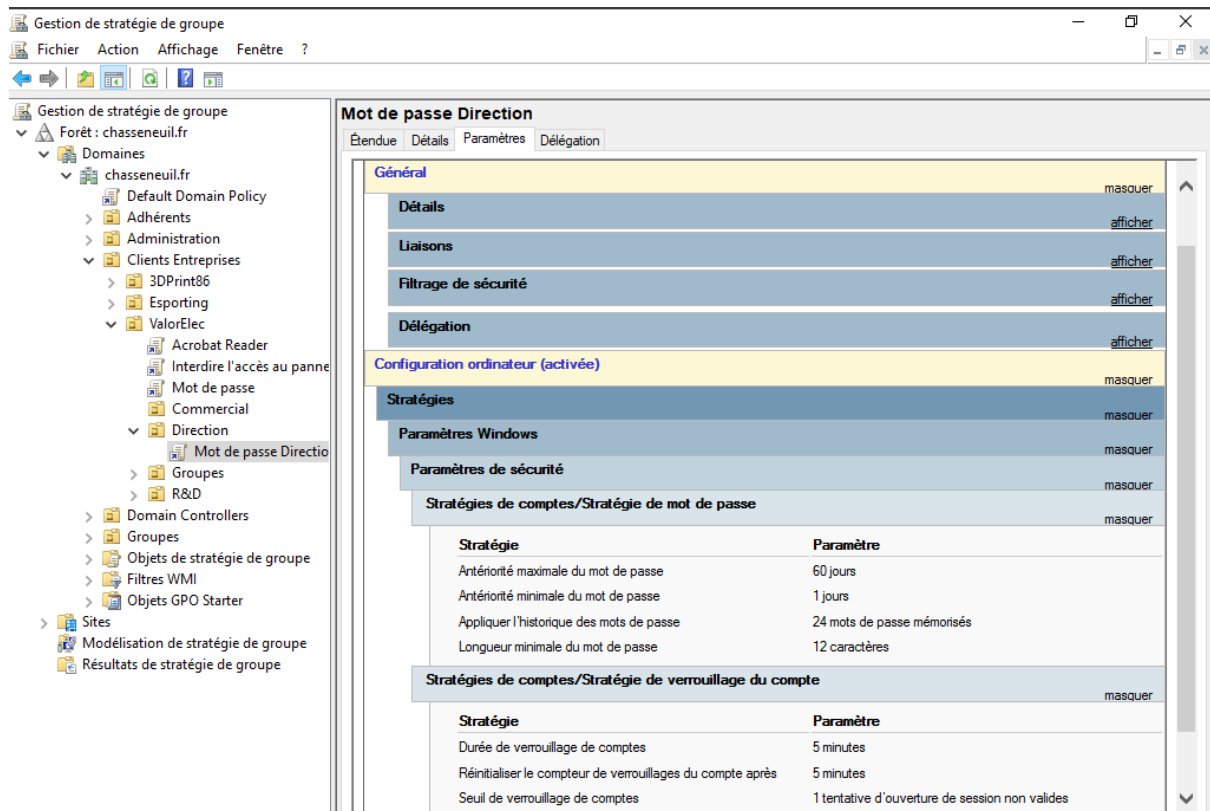
Pour ce qui est de la politique de mot de passe nous devons créer une nouvelle GPO sur l'OU ValorElec et nous rendre dans Configuration de l'ordinateur>Stratégies>Paramètres Windows>Paramètre de sécurité>Stratégies de comptes/Stratégie de mot de passe (nous renseignons les paramètres pour des utilisateurs classiques, ne faisant pas partie de la direction voir screenshot).



GPO stratégie de mot de passe Utilisateur

☒ 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 ce qui est de la politique de mot de passe de la direction nous devons créer une stratégie directement sur l'OU du groupe Direction et faire la même recherche que précédemment et adapter les paramètres en fonction du groupe Direction, comme demander. (voir screenshot ci-dessous)



GPO stratégie de mot de passe Utilisateur

☒ 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

L'objectif de cette tâche est la mise en place d'une stratégie d'audit, générant des logs dans le journal d'événement du serveur, témoignant de l'ouverture de session infructueuse, la modification d'objet AD ou encore la modification du dossier partagé contenant Acrobat Reader.

Pour cela rendez-vous sur le serveur Active Directory>Gestion de stratégie de groupe>Clic droit sur le domaine>Créer un objet GPO dans ce domaine et le lier ici>Donner le nom souhaité>Clic droit sur la GPO>Modifier>Sur le panneau de gauche de l'Éditeur de gestion de stratégie de groupe>Configuration ordinateur>Stratégies>Paramètres Windows>Paramètres de sécurité>Stratégies locales>Stratégie d'audit

Nous pouvons aussi nous rendre dans la configuration avancée de la stratégie d'audit>stratégie d'audit>échec et réussite sur les paramètres qui semblent pertinent pour auditer les sessions, la modification des objets active directory tant ordinateurs qu'utilisateurs, ainsi que les dossier partagés et applications. Pour pouvoir observer ses logs un phénomène auditer par la GPO doit se passer.



GPO d'audit 1

Stratégies locales/Options de sécurité		m350.07
Audit		m350.07
Stratégie	Paramètre	
Audit : auditer l'accès des objets systèmes globaux	Activé	
Audit : auditer l'utilisation des privilèges de sauvegarde et de restauration	Activé	
Autre		m350.07
Stratégie	Paramètre	
Audit : forcer les paramètres de sous-catégorie de stratégie d'audit (Windows Vista ou version ultérieure) à se substituer aux paramètres de catégorie de stratégie d'audit	Activé	
Configuration avancée de l'audit		m350.07
Connexion de compte		m350.07
Stratégie	Paramètre	
Auditer la validation des informations d'identification	Succès, échec	
Auditer le service d'authentification Kerberos	Succès, échec	
Auditer les opérations de ticket du service Kerberos	Succès, échec	
Auditer d'autres événements d'ouverture de session	Succès, échec	
Accès DS		m350.07
Stratégie	Paramètre	
Auditer la réplication du service d'annuaire détaillé	Succès, échec	
Auditer l'accès au service d'annuaire	Succès, échec	
Auditer les modifications du service d'annuaire	Succès, échec	
Auditer la réplication du service d'annuaire	Succès, échec	

GPO d'audit 2

Stratégie d'audit

Écran

Détails

Paramètres

Délégation

Stratégie d'audit

Données recueillies le : 18/03/2023 11:14:57

Général

Détails

Liasons

Filtrage de sécurité

Délégation

Configuration ordinateur (active)

Stratégies

Paramètres Windows

Paramètres de sécurité

Stratégie locale/Stratégie d'audit

Stratégie

Auditer l'accès au service d'annuaire

Auditer l'accès aux objets

Auditer l'utilisation des privilèges

Auditer la gestion des comptes

Auditer le suivi des processus

Auditer les événements de connexion

Auditer les événements de connexion aux comptes

Auditer les événements système

Auditer les modifications de stratégie

Paramètre

Succès, Échec

Succès, Échec

Succès, Échec

Succès, Échec

Succès, Échec

Succès, Échec

Succès, Échec

Succès, Échec

Succès, Échec

afficher tout

masquer

afficher

afficher

afficher

masquer

masquer

masquer

masquer

GPO d'audit 3

Ouvrir/fermer la session		
Stratégie	Paramètre	masquer
Auditer le verrouillage du compte	Succès, échec	
Auditer la fermeture de session	Succès, échec	
Auditer l'ouverture de session	Succès, échec	
Auditer d'autres événements d'ouverture/fermeture de session	Succès, échec	
Auditer l'ouverture de session spéciale	Succès, échec	
Accès à l'objet		
Stratégie	Paramètre	masquer
Auditer l'application générée	Succès, échec	
Auditer le partage de fichiers	Succès, échec	
Utilisation de privilège		
Stratégie	Paramètre	masquer
Auditer l'utilisation de privilèges non sensibles	Succès, échec	
Auditer d'autres événements d'utilisation de privilèges	Succès, échec	
Auditer l'utilisation de privilèges sensibles	Succès, échec	

GPO d'audit 4

Les stratégie d'audit mises en place vont générer des logs avec des numéros d'événements qui peuvent sembler abstraits. Voici une liste non exhaustive de numéros de logs avec leurs correspondances. Ces logs seront centralisés dans le journal d'événement du serveur Windows Server 2019.

Tableau de correspondance de logs

L'événement n°	correspond à
4713	la stratégie Kerberos à été modifiée
4716	les informations de domaine approuvé ont été modifiée
4739	la stratégie de domaine à été modifiée
4867	une entrée d'information de forêt à été modifiée
4741	un compte d'ordinateur à été créé
4742	un compte d'ordinateur à été modifié
4713	la stratégie Kerberos à été modifiée
4716	les informations de domaine approuvé ont été modifiée
4739	la stratégie de domaine à été modifiée
4867	une entrée d'information de forêt à été modifiée

4741	un compte d'ordinateur à été créé
4742	un compte d'ordinateur à été modifié
4743	un compte d'ordinateur à été supprimé
4692	la sauvegarde de la clé principale de protection des données à été tentée
4768	un ticket d'authentification Kerberos (TGT) à été demandé
4771	échec de la pré-authentification Kerberos
4769	un ticket de service Kerberos a été demandé
4634	un compte à été déconnecté
4624	un compte à été correctement connecté

4625	échec d'ouverture de session d'un compte
4648	une tentative d'ouverture de session à été effectuée à l'aide d'informations d'identification explicite
4743	un nouveau processus à été créé
4728	introuvable
4610	un package d'authentification a été chargé par l'autorité de sécurité locale
4697	un service à été installer dans le système
4769	un ticket de service Kerberos a été demandé
4634	un compte à été déconnecté
4624	un compte à été correctement connecté
4672	privilège spéciaux attribués à la nouvelle ouverture de session
4673	un service privilégié à été appelé
4674	une opération à été tentée sur un objet privilégié

4964	des groupes spéciaux ont été affecté à une nouvelle ouverture de session
4720	un compte utilisateur à été créé
4722	un compte utilisateur à été activé
4723	une tentative de modification du mot de passe d'un compte à été effectué
4738	un compte d'utilisateur à été modifié
4964	des groupes spéciaux ont été affecté à une nouvelle ouverture de session
4765	l'historique sid à été ajouté à un compte
4766	une tentative d'ajout de l'historique du SID à un compte a échoué
4780	la liste de contrôle d'accès a été définis sur les comptes qui sont membres de groupes d'administrateur
4794	une tentative à été effectuée pour définir le mot de passe administrateur du mode de restauration des services d'annuaire

Journal d'événement du server

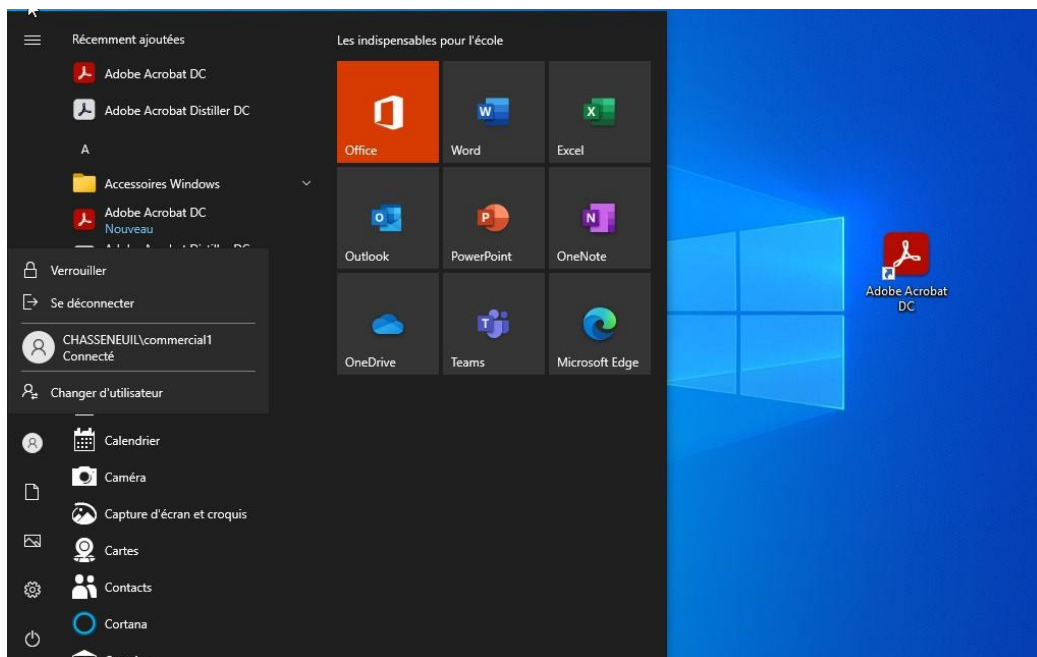
Mots clés	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Succès de l'audit	18/03/2023 11:24:19	Microsoft Windows security auditing.	4634	Logoff
Succès de l'audit	18/03/2023 11:24:19	Microsoft Windows security auditing.	4624	Logon
Succès de l'audit	18/03/2023 11:24:19	Microsoft Windows security auditing.	4672	Special Logon
Succès de l'audit	18/03/2023 11:23:42	Microsoft Windows security auditing.	4674	Sensitive Privilege Use
Succès de l'audit	18/03/2023 11:23:42	Microsoft Windows security auditing.	4674	Sensitive Privilege Use
Succès de l'audit	18/03/2023 11:23:38	Microsoft Windows security auditing.	4634	Logoff
Succès de l'audit	18/03/2023 11:23:30	Microsoft Windows security auditing.	4634	Logoff
Succès de l'audit	18/03/2023 11:23:30	Microsoft Windows security auditing.	4624	Logon
Succès de l'audit	18/03/2023 11:23:30	Microsoft Windows security auditing.	4634	Logoff
Succès de l'audit	18/03/2023 11:23:30	Microsoft Windows security auditing.	4624	Logon
Succès de l'audit	18/03/2023 11:23:30	Microsoft Windows security auditing.	4769	Kerberos Service Ticket Operations
Succès de l'audit	18/03/2023 11:23:30	Microsoft Windows security auditing.	5140	File Share
Échec de l'audit	18/03/2023 11:23:28	Microsoft Windows security auditing.	4674	Sensitive Privilege Use
Échec de l'audit	18/03/2023 11:23:28	Microsoft Windows security auditing.	4674	Sensitive Privilege Use
Échec de l'audit	18/03/2023 11:23:28	Microsoft Windows security auditing.	4674	Sensitive Privilege Use
Échec de l'audit	18/03/2023 11:23:28	Microsoft Windows security auditing.	4674	Sensitive Privilege Use
Succès de l'audit	18/03/2023 11:23:28	Microsoft Windows security auditing.	4634	Logoff
Succès de l'audit	18/03/2023 11:23:28	Microsoft Windows security auditing.	4634	Logoff
Succès de l'audit	18/03/2023 11:23:28	Microsoft Windows security auditing.	4634	Logoff
Succès de l'audit	18/03/2023 11:23:28	Microsoft Windows security auditing.	5140	File Share
Succès de l'audit	18/03/2023 11:23:28	Microsoft Windows security auditing.	4624	Logon

La création de politique d'audit permet d'analyser les faits et gestes commis sur le domaine après coup, permettant de corriger une faille ou bien de trouver la cause du problème.

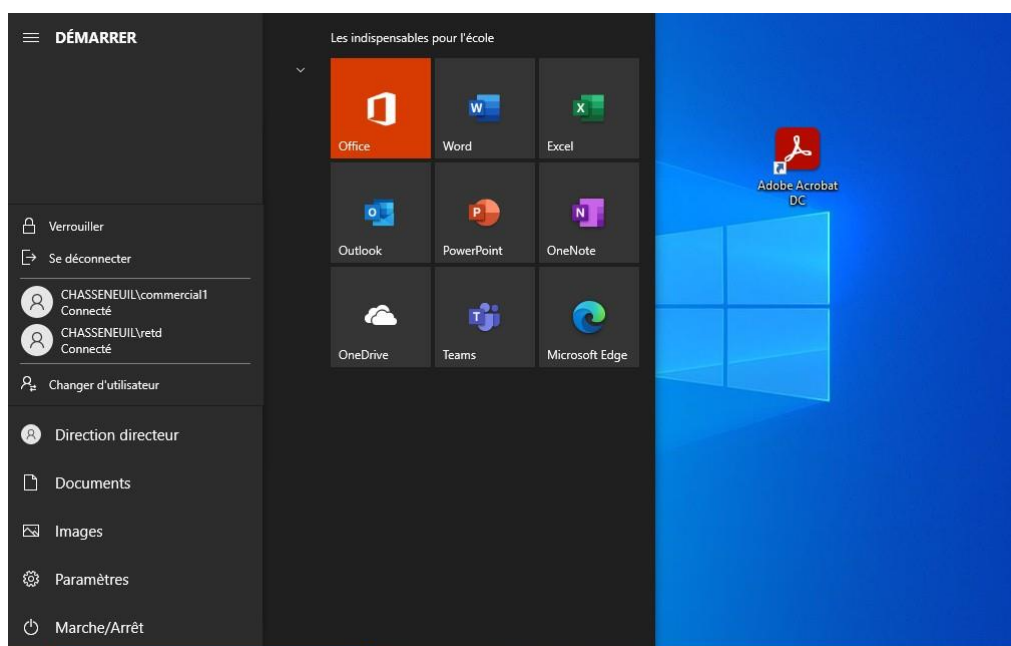
Tâche 4

Cette dernière tâche est une conclusion basée sur des tests via un environnement client. Pour cela différents screenshot seront disponible témoignant du bon fonctionnement des GPO mise en place

Nous devons premièrement vérifier le bon déploiement du logiciel Acrobat Reader via GPO. Nous pouvons constater que sur le bureau des différentes sessions utilisateurs ValorElec, le raccourci du logiciel est présent témoignant de la bonne installation de celui-ci. Nous pouvons donc conclure que la gpo fonctionne normalement.

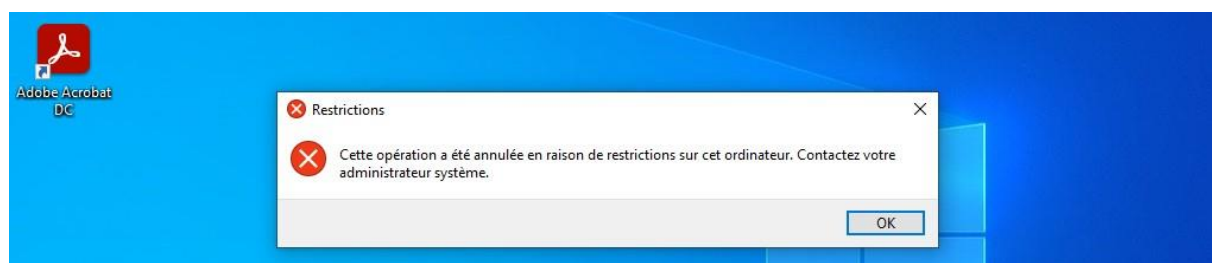


Session Commercial1 acrobat reader



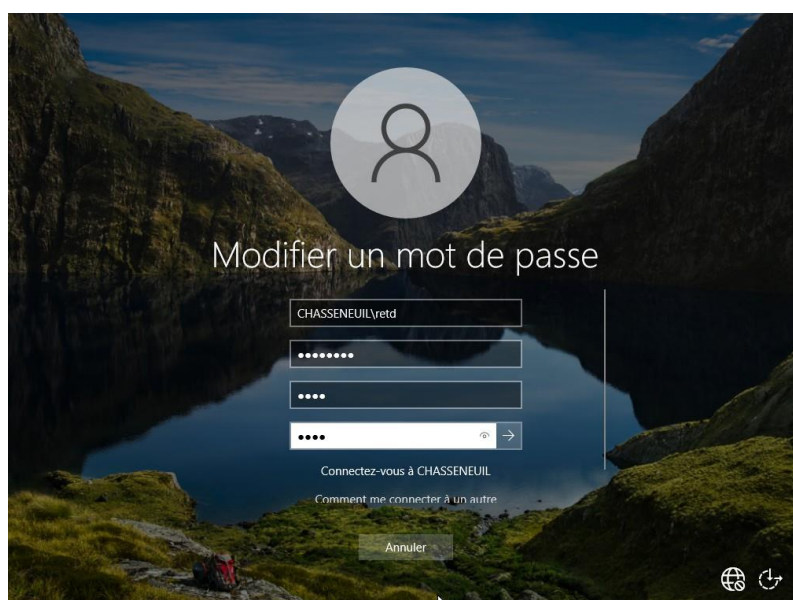
Session Direction Directeur acrobat reader

Nous devons donc vérifier dans un premier temps si la restriction du panneau de configuration fonctionne. Si oui, un message d'erreur doit être retourné, rendant impossible l'accès au panneau de configuration. En se connectant sur le compte "retld" qui est le premier compte du groupe Service R&D, qui subit donc cette restriction. En effet, la GPO à bien été appliquée, nous pouvons le voir via le screenshot ci-dessous.

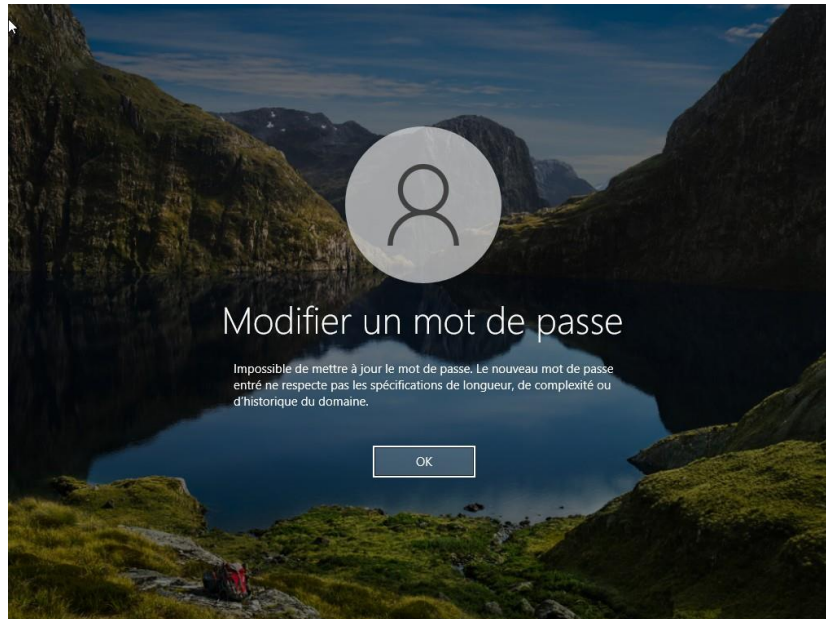


Impossibilité d'accès au panneau de configuration

Nous devons désormais vérifier l'application de la stratégie de mot de passe. Nous pouvons voir dans les screenshot suivant qu'il est impossible de mettre un mot de passe non conforme à la politique qui s'applique sur le compte. Le test à été fait ici sur le compte "retld". Le mot de passe est censé contenir au moins 8 caractères. Nous pouvons voir que le nouveau mot de passe ne fait que 4 caractères, ce qui entraîne une erreur que nous pouvons voir dans le deuxième screenshot.



Changement de mot de passe 1



Changement de mot de passe 2

Les différentes GPO mises en place sont donc actives et remplissent leurs missions.

Pour mieux comprendre le fonctionnement de cette infrastructure virtualisée, je vous invite à prendre connaissance de la vidéo de démonstration qui justifie la bonne communication entre les machines et la configuration des différents comptes, des différentes GPO ainsi que du serveur de fichier et des partages pour les services de Valor Elec.

Sources

Sites internet :

[Comment installer TrueNas](#)

Forum Officiel TrueNas :

[How to fix incorrect time](#)

[Time on machine constantly out of sync](#)

Articles microsoft et en relation avec windows server :

[How to configure ntp server on windows server 2019 Paramètres et outils du service de temps windows](#)

Site internet :

[IT Connect C'est quoi le DFS ? ActualitéInformatique Définition DFS Correspondance des numéros de logs Microsoft](#)