Sommaire

I. Contexte

Le site de Chasseneuil de TiersLieux86 accueille plusieurs entreprises au sein d'une infrastructure informatique mutualisée reposant sur Windows Server et Active Directory. Dans ce cadre, l'entreprise ValorElec doit être intégrée à l'environnement existant afin de permettre l'accueil d'une vingtaine de collaborateurs répartis entre les services Direction, Développement et Commercial. L'objectif de la réalisation est de faire évoluer l'architecture système du site pour fournir à ce nouveau client une organisation d'annuaire cohérente, un espace de stockage centralisé, une gestion sécurisée des accès aux ressources et une administration homogène des postes de travail. Les missions officielles de l'atelier 2 portent précisément sur la création de la maquette de l'architecture système, la mise en place d'un serveur de fichiers, l'automatisation de la sécurité sur les partages et le déploiement de stratégies de groupe.

La solution a été mise en œuvre dans un environnement virtualisé sous VMware, choix pertinent pour reproduire une architecture professionnelle tout en conservant une grande souplesse de test, de modification et de validation. L'infrastructure s'appuie sur un contrôleur de domaine Windows Server déjà présent dans le domaine chasseneuilx86.local, sur un serveur de stockage TrueNAS déployé en machine virtuelle, ainsi que sur un poste client Windows utilisé pour les vérifications de fonctionnement. Cette approche permet de distinguer les rôles de chaque machine et de simuler une organisation réaliste de l'infrastructure, sans mobiliser plusieurs serveurs physiques. Le compte rendu montre notamment l'utilisation d'une machine TrueNAS dédiée, raccordée au domaine réseau du site et configurée pour exposer un volume de stockage au serveur Windows.

Le socle d'administration repose sur Active Directory, technologie centrale des environnements Windows professionnels. Son rôle est de centraliser la gestion des utilisateurs, des groupes, des ordinateurs et des stratégies de sécurité. Dans cette réalisation, l'annuaire doit être structuré pour intégrer ValorElec de manière propre, avec une organisation en unités d'organisation (OU) distinctes selon les services et les types d'objets. Cette structuration facilite l'administration, prépare l'application des GPO et sert de base à la gestion des autorisations sur les partages. Afin de rendre le déploiement reproductible et plus fiable, plusieurs tâches sont automatisées avec PowerShell, notamment la création des OU, des comptes et des groupes. Ce choix répond à une logique professionnelle d'industrialisation des opérations d'administration.

Pour le stockage des données, la solution retenue repose sur TrueNAS avec exposition d'un volume au serveur Windows via le protocole iSCSI. Ce choix technique permet de séparer le stockage de la gestion des partages. TrueNAS fournit un espace disque centralisé, tandis que Windows Server conserve la maîtrise du système de fichiers, des permissions NTFS et des partages SMB. Cette architecture rapproche la maquette d'une infrastructure d'entreprise dans laquelle la couche de stockage et la couche de services de fichiers sont dissociées pour améliorer l'administration, la sécurité et l'évolutivité. La sécurisation des accès aux dossiers est ensuite organisée selon la méthode AGDLP, qui consiste à attribuer les permissions aux groupes plutôt qu'aux utilisateurs directement. Enfin, l'administration des postes est renforcée par les GPO, utilisées ici pour déployer un logiciel, restreindre certaines actions locales et appliquer des politiques de mot de passe différenciées selon les profils.

II. Objectifs

L’objectif de cet atelier est de concevoir et déployer une infrastructure système permettant d’intégrer l’entreprise ValorElec dans l’environnement informatique du site de Chasseneuil, en garantissant une administration centralisée, une gestion sécurisée des ressources et une homogénéisation des postes de travail.

La solution mise en place doit permettre de :

- Structurer l’intégration de ValorElec dans Active Directory par la création d’une arborescence d’unités d’organisation adaptée aux services Direction, Développement et Commercial.
- Automatiser la création des OU, des utilisateurs et des groupes à l’aide de PowerShell afin de fiabiliser le déploiement et de rendre les opérations reproductibles.
- mettre en place un espace de stockage centralisé à l’aide d’un serveur TrueNAS, exposé au serveur Windows via le protocole iSCSI.
- configurer un serveur de fichiers capable d’héberger les dossiers de travail de l’entreprise et de distinguer clairement la couche de stockage de la couche de partage.
- appliquer une gestion des autorisations conforme à la méthode AGDLP, afin d’assurer une attribution lisible, évolutive et sécurisée des droits d’accès.
- déployer automatiquement les permissions NTFS et les partages SMB sur les dossiers de service et sur l’espace commun.
- mettre en œuvre des stratégies de groupe (GPO) pour automatiser certains paramétrages des postes, notamment le déploiement d’un logiciel, la restriction du panneau de configuration et l’application de politiques de mot de passe différenciées.
- vérifier le bon fonctionnement global de l’infrastructure à l’aide de tests sur les postes clients et sur les ressources partagées.

III. Réalisations professionnelles

1. Création de l'Active Directory

La première phase de la réalisation a consisté à intégrer l’entreprise ValorElec dans l’annuaire Active Directory existant du site de Chasseneuil. L’objectif était de structurer les utilisateurs, les ordinateurs et les groupes dans une arborescence claire, afin de faciliter l’administration du domaine et de préparer la mise en place des droits d’accès, des partages réseau et des stratégies de groupe. La solution retenue repose sur une organisation par unités d’organisation (OU) distinctes selon les services et les types d’objets, ainsi que sur l’automatisation de la création des objets avec PowerShell.

1.1 Proposition d'organisation du Client ValorElec dans l’annuaire

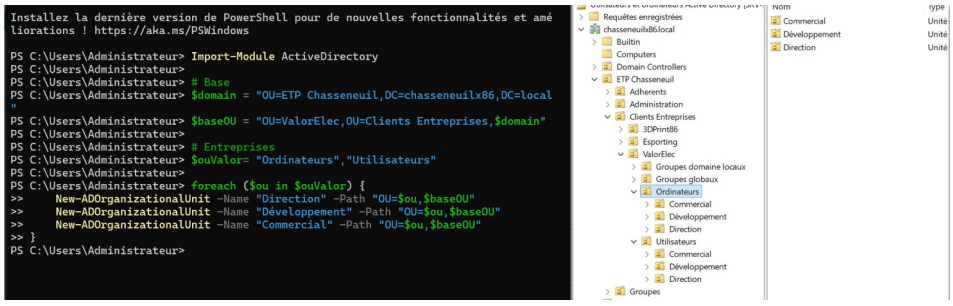
Une OU racine ValorElec a été créée sous l’OU Clients Entreprises afin d’intégrer proprement ce nouveau client dans l’environnement mutualisé du site. Cette OU a été structurée en sous-unités dédiées aux utilisateurs, aux ordinateurs, aux groupes globaux et aux groupes domaine locaux. Les OU Utilisateurs et Ordinateurs ont ensuite été subdivisées selon les services Direction, Développement et Commercial. Cette organisation améliore la lisibilité de l’annuaire, facilite l’administration quotidienne et prépare l’application ultérieure des GPO et des autorisations sur les ressources partagées.

L’arborescence retenue est la suivante :

```
OU=ValorElec
│
├── OU=Utilisateurs
│   ├── OU=Direction
│   ├── OU=Développement
│   └── OU=Commercial
├── OU=Ordinateurs
│   ├── OU=Direction
│   ├── OU=Développement
│   └── OU=Commercial
├── OU=Groupes globaux
└── OU= Domain Locaux
```

1.2 Automatisation avec PowerShell

La création de l’arborescence Active Directory a été automatisée à l’aide de scripts PowerShell exploitant le module ActiveDirectory. Ce choix permet de fiabiliser le déploiement, de limiter les erreurs de saisie et de rendre les opérations reproductibles. Les scripts ont servi à créer les unités d’organisation nécessaires à l’intégration de ValorElec dans le domaine chasseneuilx86.local, en respectant la structure définie lors de la phase de conception. Cette méthode s’inscrit dans une logique d’industrialisation des tâches d’administration.

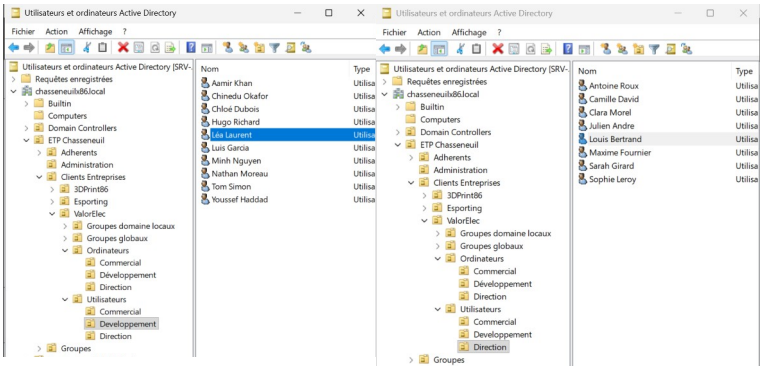


* Détails en annexe 1.

1.3 Organisation de l'annuaire

Les comptes utilisateurs ont ensuite été générés automatiquement pour les différents services de l’entreprise. Une convention de nommage homogène a été retenue pour produire les identifiants de connexion, puis chaque utilisateur a été positionné dans l’OU correspondant à son service. Cette organisation facilite le ciblage des stratégies de groupe, l’affectation des droits d’accès et l’administration des ressources par service. Elle constitue également une base cohérente pour la suite de l’atelier, notamment pour la mise en œuvre des groupes de sécurité et des autorisations sur les dossiers partagés.

Principe retenu : création automatisée des comptes et répartition par service dans les OU Direction, Développement et Commercial.



* Détails en annexe 2.

1.4 Vérification

Une vérification a été réalisée dans la console Utilisateurs et ordinateurs Active Directory afin de contrôler la bonne création des unités d’organisation et des comptes utilisateurs. Le résultat obtenu est conforme à la structure attendue : l’arborescence ValorElec est présente dans l’annuaire, les utilisateurs sont placés dans les bons emplacements et l’organisation retenue constitue une base exploitable pour la mise en place des groupes, des partages et des stratégies de groupe.

Outil de contrôle : Utilisateurs et ordinateurs Active Directory.

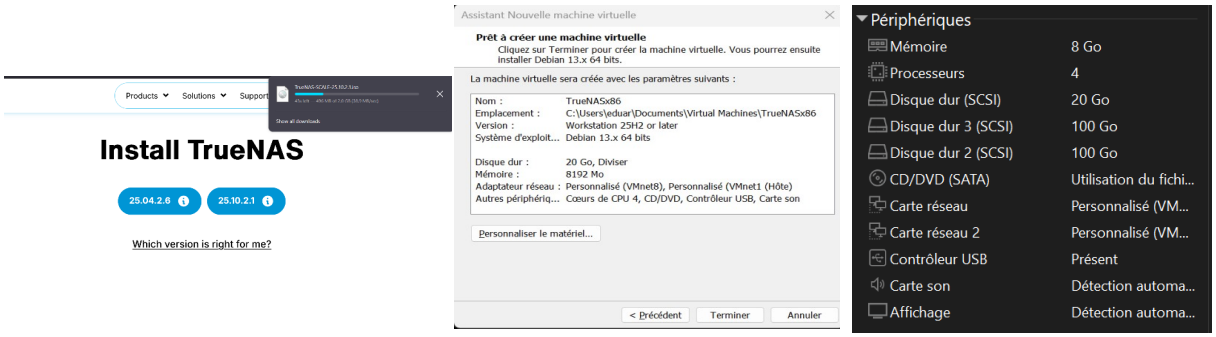
2. Mise en place d’un serveur de fichiers avec TrueNAS

La deuxième phase de la réalisation a consisté à mettre en place une solution de stockage centralisé destinée à héberger les données de l’entreprise ValorElec. L’architecture retenue repose sur un serveur TrueNAS déployé dans l’environnement VMware, chargé de fournir un volume de stockage au serveur Windows via le protocole iSCSI. Ce choix permet de dissocier la couche de stockage de la couche de partage de fichiers, tout en conservant sur Windows Server la gestion du système de fichiers, des permissions NTFS et des partages SMB. Cette organisation rapproche la maquette d’une architecture d’entreprise plus réaliste et plus administrable.

2.1 Déploiement de la machine virtuelle

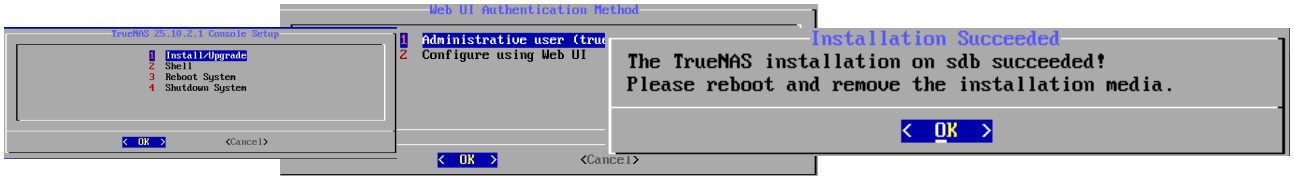
Le serveur TrueNAS a été déployé sous forme de machine virtuelle dans VMware. La configuration retenue comprend 4 vCPU, 8 Go de mémoire vive, un disque système de 20 Go ainsi que deux disques de 100 Go destinés au stockage des données. Cette répartition permet de distinguer le système de la zone de données et de simuler une baie de stockage dédiée, adaptée à un usage de type serveur de fichiers.

Paramètres : 4 vCPU, 8 Go RAM, 1 disque système de 20 Go et 2 disques de données de 100 Go.



2.2 Installation de TrueNAS

L'installation de TrueNAS a été réalisée à partir de l'image ISO officielle, en sélectionnant l'option Install/Upgrade. Le système a été déployé sur le disque de 20 Go, puis un compte administrateur a été défini afin de sécuriser l'accès à l'interface d'administration. Cette étape permet de disposer d'un serveur de stockage dédié, distinct du serveur Windows qui assurera ensuite la publication des partages.

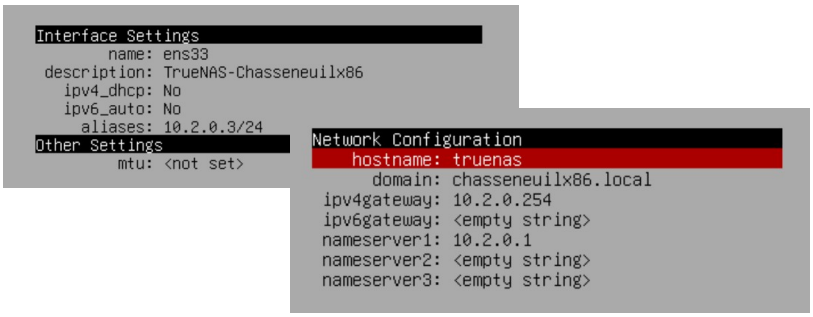


* Détails en Annexe 3.

2.3 Configuration réseau en mode console

Après installation, une configuration réseau statique a été appliquée depuis la console de TrueNAS. Le serveur a reçu l'adresse 10.2.0.3, avec le nom d'hôte TrueNAS, le domaine chasseneuilx86.local, la passerelle 10.2.0.254 et le serveur DNS 10.2.0.1. Cette configuration garantit l'accessibilité de l'interface web de TrueNAS et la disponibilité du service iSCSI sur le réseau serveur.

Paramètres : IP 10.2.0.3, passerelle 10.2.0.254, DNS 10.2.0.1, domaine chasseneuilx86.local.

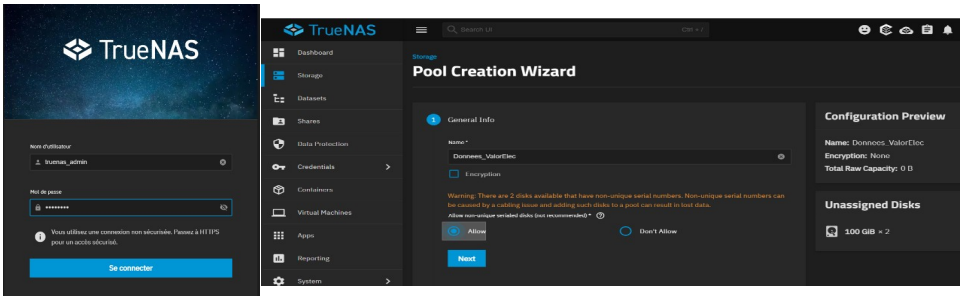


2.4 Configuration du stockage dans TrueNAS

Depuis l'interface web de TrueNAS, un espace de stockage dédié à ValorElec a été préparé à partir des deux disques de données. Un pool nommé Donnees_ValorElec a été créé, puis un volume de type zvol a été configuré afin d'être exposé au serveur Windows via le service iSCSI. Cette approche permet à TrueNAS de jouer le rôle de baie de stockage, sans exposer directement de partages utilisateurs. Les partages et les droits restent ainsi administrés côté Windows Server.

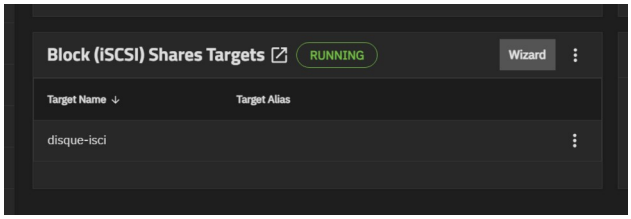
2.4.1 Création du pool

Le pool de stockage Donnees_ValorElec a été créé à partir des deux disques de 100 Go ajoutés à la machine virtuelle. Cette étape constitue la base du stockage centralisé utilisé ensuite pour publier un volume au serveur Windows. Le pool permet d'agréger l'espace disque disponible dans une structure administrable depuis l'interface de TrueNAS.



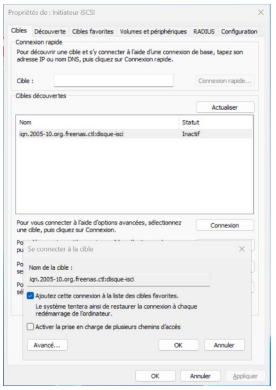
2.4.2 Configuration du disque iSCSI

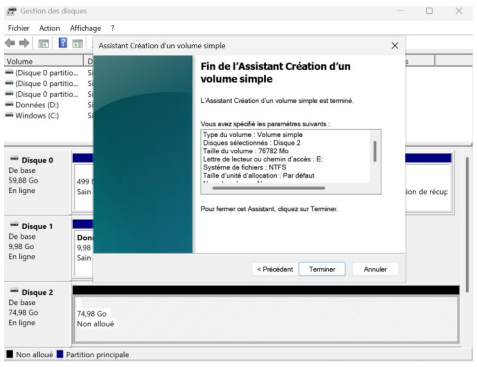
Un volume de type zvol a ensuite été créé dans le pool, puis publié par le service iSCSI de TrueNAS. Cette configuration permet de présenter au serveur Windows un disque réseau brut, qui sera ensuite initialisé, partitionné et formaté côté système Microsoft. Ce choix technique sépare clairement la gestion du stockage de la gestion des permissions et des partages utilisateurs.

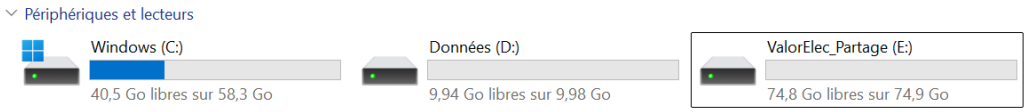


2.5 Connexion du disque iSCI sur Windows Server

Le serveur Windows Server a été configuré avec l'initiateur iSCSI afin de se connecter à la cible publiée par TrueNAS. Une fois la connexion établie, le disque est apparu dans la Gestion des disques de Windows, où il a été initialisé, partitionné et formaté. Il a ensuite pu être utilisé comme support des futurs partages de l'entreprise ValorElec. Cette étape finalise l'intégration du stockage au serveur de fichiers Windows.







3. Automatisation de la mise en place des droits sur les dossiers

La troisième phase de la réalisation a consisté à mettre en place une gestion structurée et automatisée des autorisations sur les dossiers de l'entreprise ValorElec. L'objectif était de créer une arborescence de travail cohérente, de définir les groupes de sécurité associés aux services et d'appliquer automatiquement les permissions sur les ressources du serveur de fichiers. La solution retenue repose sur la méthode AGDLP, qui permet d'attribuer les droits aux groupes plutôt qu'aux utilisateurs directement, afin d'améliorer la lisibilité, la sécurité et l'évolutivité de l'administration.

3.1 Création de l'arborescence de dossiers

Une arborescence dédiée a été créée sur le volume de données du serveur de fichiers dans le répertoire E:\Partages. Quatre dossiers ont été définis : Direction, Développement, Commercial et Commun. Cette organisation permet à chaque service de disposer de son propre espace de travail tout en prévoyant un dossier partagé commun. La création de cette structure a été automatisée avec PowerShell afin de rendre l'opération reproductible et plus rapide à déployer.

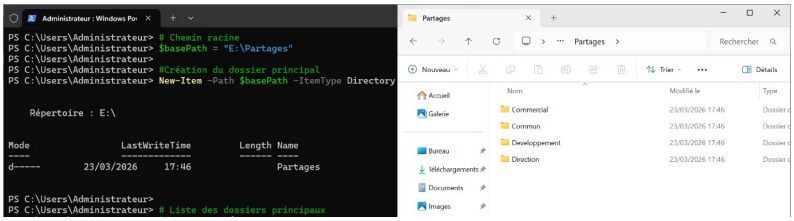
3.1.1 Proposition de l'arborescence de dossiers

L'arborescence retenue repose sur un répertoire racine E:\Partages, contenant les dossiers de chaque service ainsi qu'un dossier commun accessible selon les droits définis. Cette organisation prépare directement la mise en place des permissions NTFS et des partages SMB.

E:\Partages\
├── Direction
├── Developpement
├── Commercial
└── Commun

3.1.2 Création des dossiers avec PowerShell

La création des répertoires a été automatisée à l'aide d'un script PowerShell. Ce choix permet de garantir une création homogène de l'arborescence et de limiter les manipulations manuelles sur le serveur. L'ensemble des dossiers nécessaires a ainsi été généré depuis un chemin racine unique sur le volume de données du serveur de fichiers.



* Détails en Annexe 4.

3.2 Mise en œuvre de la méthode AGDLP

La sécurisation des accès a été organisée selon la méthode AGDLP. Les utilisateurs ont d'abord été regroupés dans des groupes globaux correspondant à leur service, puis ces groupes ont été intégrés dans des groupes domaine locaux auxquels les permissions ont été attribuées. Cette méthode évite l'affectation directe de droits aux utilisateurs, simplifie l'administration des accès et facilite les évolutions futures de l'organisation.

Principe retenu : Utilisateurs → Groupes globaux → Groupes domaine locaux → Permissions NTFS et SMB.

Groupes globaux et domaine locaux

Groupes globaux (utilisateurs)	Groupes Domain Local (droits)
GG_Direction_VE	DL_Direction_VE_M
GG_Developpement_VE	DL_Developpement_VE_M
GG_Commercial_VE	DL_Commercial_VE_M
	DL_Commun_VE_L

Tableau des droits

Dossier	Groupe	Type	Droits
Direction	GG_Direction_VE → DL_Direction_VE_M	M	Lecture/Écriture
Developpement	GG_Developpement_VE → DL_Developpement_VE_M	M	Lecture/Écriture
Commercial	GG_Commercial_VE → DL_Commercial_VE_M	M	Lecture/Écriture
Commun	Tous → DL_Commun_VE_L	R	Lecture seule

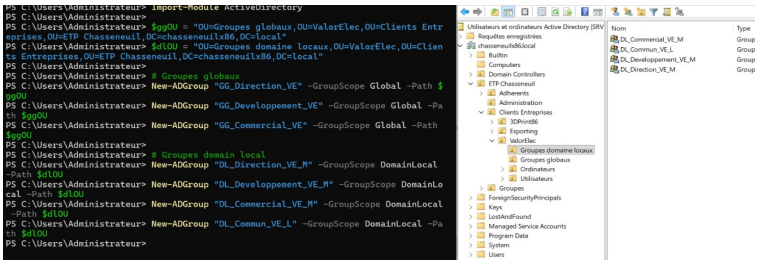
3.3 Création et peuplement des groupes

Les groupes de sécurité nécessaires à l'application des droits ont été créés dans l'annuaire Active Directory. Les groupes GG_Direction_VE, GG_Developpement_VE et GG_Commercial_VE ont été utilisés pour représenter les utilisateurs de chaque service. Des groupes domaine locaux dédiés aux permissions ont ensuite été créés pour porter les droits sur les dossiers partagés. Les utilisateurs ont été ajoutés automatiquement à leur groupe global, puis les groupes globaux ont été intégrés dans les groupes domaine locaux correspondants.

3.3.1 Création de groupes globaux et de domaine locaux

Les groupes ont été créés par PowerShell dans les unités d'organisation prévues dans l'annuaire. Cette automatisation garantit une nomenclature homogène et une préparation cohérente de l'application des droits sur les ressources du serveur de fichiers.

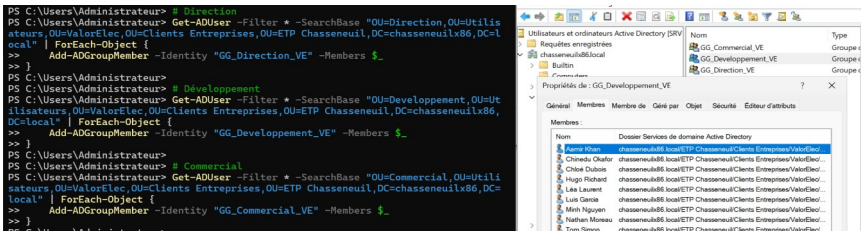
Groupes créés :
GG_Direction_VE, GG_Developpement_VE, GG_Commercial_VE
DL_Direction_VE_M, DL_Developpement_VE_M, DL_Commercial_VE_M, DL_Commun_VE_L



* Détails en Annexe 5.

3.3.2 Peuplement des groupes globaux

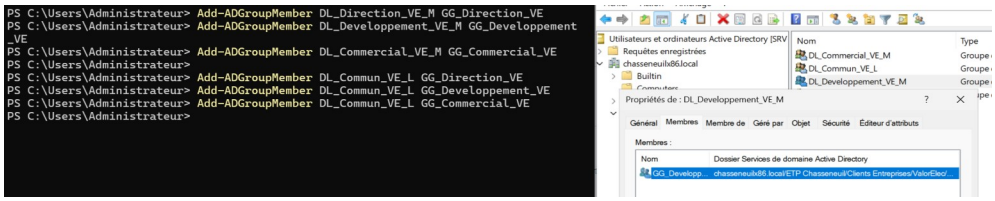
Les utilisateurs ont ensuite été ajoutés automatiquement à leur groupe global en fonction de leur service et de leur emplacement dans l'annuaire. Cette opération permet de relier directement l'organisation des comptes à la gestion des accès sur les dossiers partagés.



* Détails en Annexe 6.

3.3.3 Liaison AGDLP des groupes de domaine local

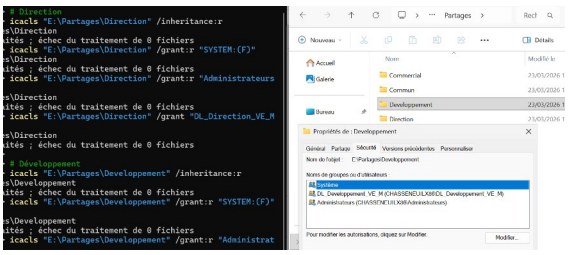
Les groupes globaux ont été intégrés dans les groupes domaine locaux afin de finaliser la chaîne AGDLP. Les groupes de service reçoivent ainsi indirectement les permissions appliquées aux dossiers. Le dossier Commun a été configuré de manière à être accessible en lecture à l'ensemble des services, tandis que les dossiers métiers restent associés à leur groupe dédié.



3.4 Application des Droits NTFS

Les autorisations NTFS ont été configurées sur chaque dossier du serveur de fichiers. L'héritage a été désactivé afin de maîtriser précisément les droits appliqués. Les comptes SYSTEM et Administrateurs conservent un contrôle total, tandis que les groupes domaine locaux reçoivent les autorisations adaptées : modification pour les dossiers de service et lecture pour le dossier commun. Cette configuration permet d'assurer l'isolation des services tout en maintenant un espace partagé contrôlé.

Principe retenu :
dossiers de service : droit Modification pour le groupe domaine local correspondant ;
dossier commun : droit Lecture pour le groupe domaine local partagé.

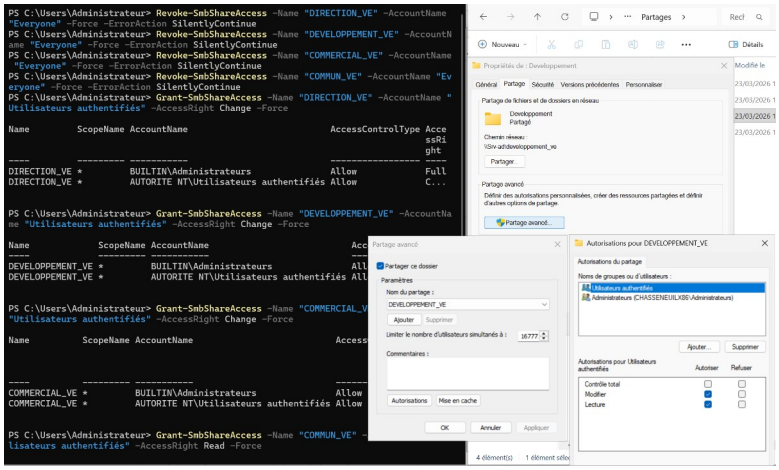


* Détails en Annexe 7.

3.5 Application des Droits SMB

Les dossiers ont ensuite été publiés sous forme de partages SMB sur le serveur Windows. Les partages ont été créés avec une administration centralisée, en supprimant les autorisations trop larges par défaut, notamment pour Everyone, puis en appliquant des autorisations cohérentes avec l'organisation retenue. Les services métiers disposent d'un accès en modification, tandis que le dossier commun est publié en lecture seule. Cette étape complète la mise en œuvre des permissions NTFS en assurant la cohérence entre droits de partage et droits de fichier.

Partages créés : DIRECTION_VE, DEVELOPPEMENT_VE, COMMERCIAL_VE, COMMUN_VE.
Principe retenu : accès en modification pour les dossiers métiers, accès en lecture pour le dossier commun.



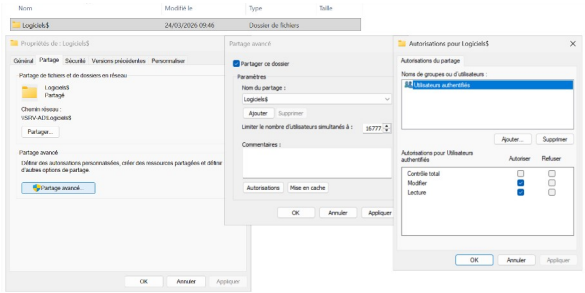
4. Mettre en place des stratégies de GPO

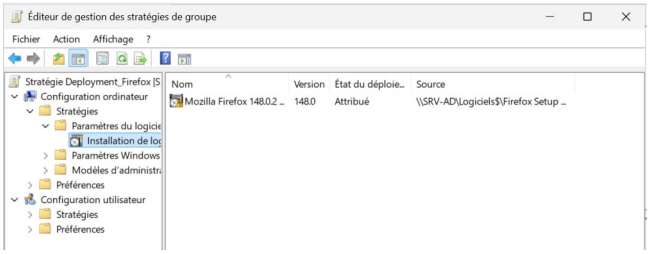
La dernière phase de la réalisation a consisté à mettre en place des stratégies de groupe afin d'automatiser certains paramétrages sur les postes de ValorElec, de renforcer la sécurité des utilisateurs et d'homogénéiser l'environnement de travail. Les GPO déployées portent sur l'installation automatisée d'un logiciel, la restriction de certaines fonctions locales et l'application de politiques de mot de passe affinées selon les profils. Cette approche permet de centraliser l'administration des postes et de limiter les opérations manuelles sur chaque machine.

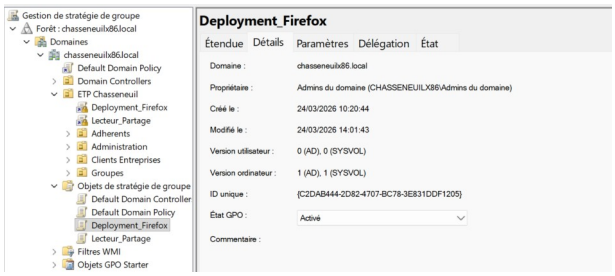
4.1 Déploiement d'un logiciel par GPO

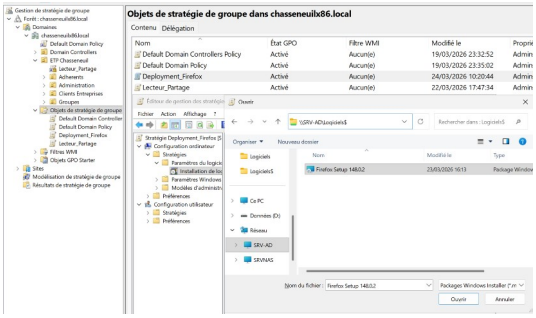
Une stratégie de groupe a été créée pour déployer automatiquement un logiciel sur les postes du domaine. Le package Firefox.msi a été placé dans un dossier partagé accessible aux ordinateurs concernés, puis la stratégie a été configurée dans la section Configuration ordinateur > Stratégies > Paramètres du logiciel avec un déploiement en mode Attribué. La GPO a ensuite été liée à l'unité d'organisation ValorElec afin d'automatiser l'installation du logiciel sur les postes ciblés. Cette méthode permet d'assurer un déploiement homogène sans intervention manuelle sur chaque poste.

Logiciel déployé : Firefox.msi
Principe retenu : déploiement automatique par GPO via un partage réseau dédié.





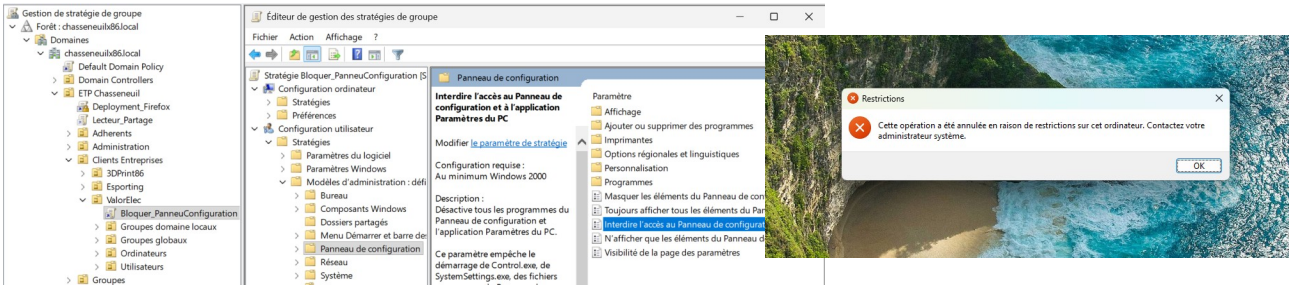




* Détails en Annexe 8.

4.2 Restriction du panneau de configuration

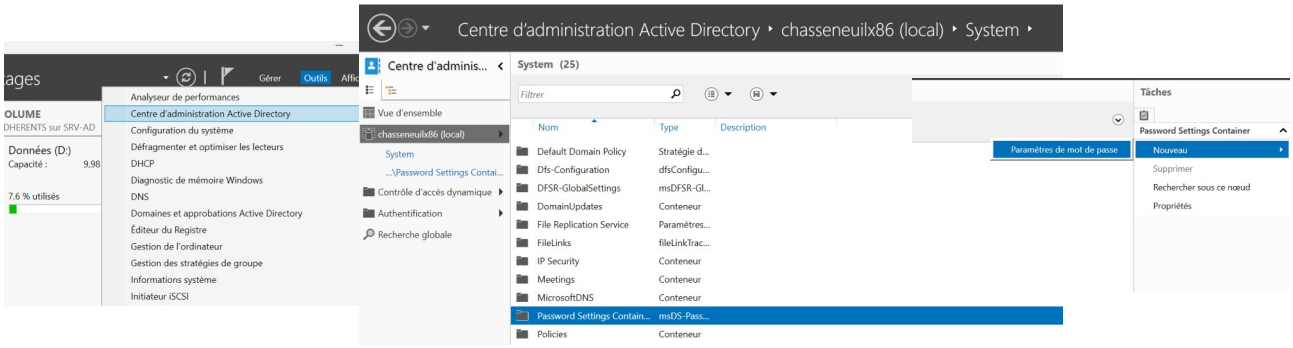
Une stratégie de groupe utilisateur a également été mise en place afin d'empêcher l'accès au panneau de configuration. Cette mesure permet de limiter les modifications locales non maîtrisées sur les postes et de conserver un meilleur contrôle de l'environnement utilisateur. Elle contribue à renforcer la cohérence de la configuration des postes de travail en réduisant la possibilité de changements manuels par les utilisateurs.



4.3 Stratégies de mot de passe affiné

Des politiques de mot de passe différenciées ont été configurées afin d'adapter le niveau de sécurité au profil des utilisateurs. Pour les utilisateurs standards, une politique impose un mot de passe d'au moins 8 caractères, un historique de 12 mots de passe et un verrouillage après deux tentatives infructueuses pendant 10 minutes. Pour la direction, une politique plus stricte a été définie avec un mot de passe d'au moins 12 caractères, un historique de 24 mots de passe et un verrouillage dès la première tentative infructueuse pendant 5 minutes. Ces réglages ont été mis en place dans le Password Settings Container du Centre d'administration Active Directory.

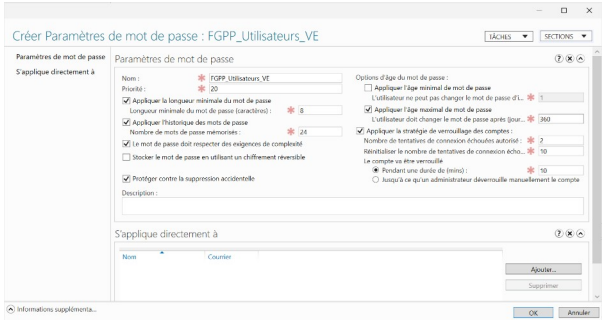
Outil utilisé : Centre d'administration Active Directory > System > Password Settings Container.

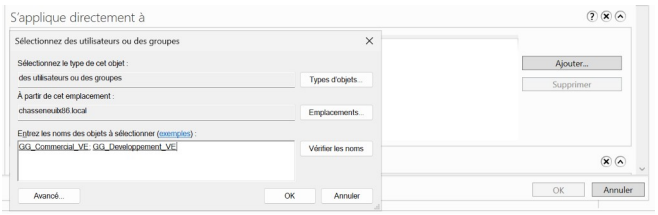


* Détails en annexe 10

4.3.1 Configuration pour les utilisateurs

Une première politique de mot de passe affiné a été appliquée aux utilisateurs standards de l'entreprise. Cette stratégie vise à renforcer le niveau de sécurité tout en restant compatible avec un usage quotidien classique. Elle définit une longueur minimale de 8 caractères, un historique de 12 mots de passe et un verrouillage temporaire du compte après plusieurs échecs d'authentification



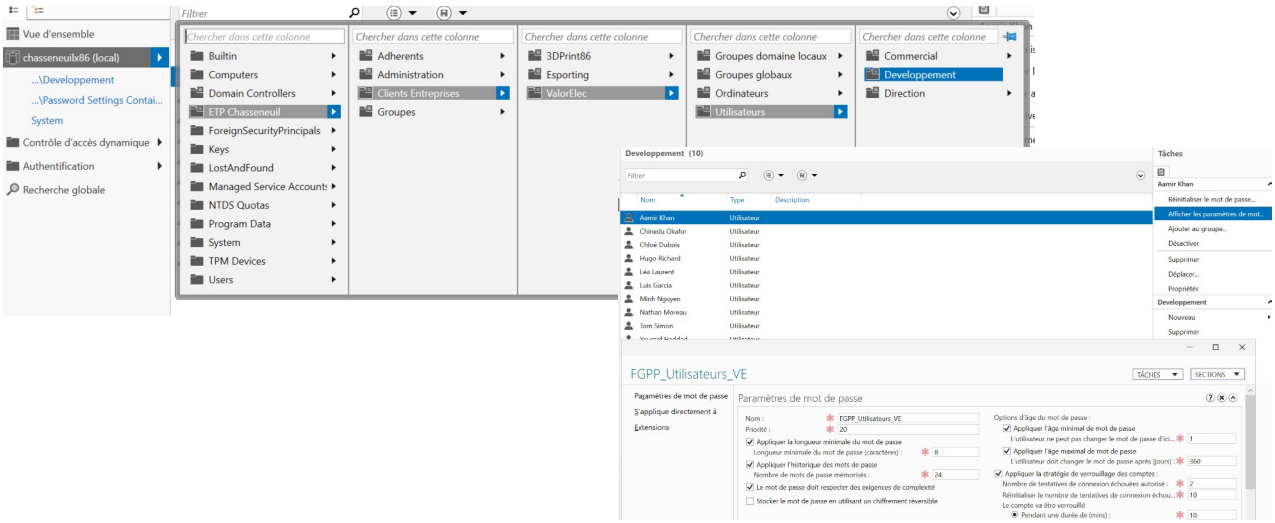


4.3.2 Configuration pour la direction

Une seconde politique, plus restrictive, a été appliquée aux comptes de la direction. Cette distinction permet de renforcer la sécurité des profils les plus sensibles de l'organisation. La stratégie impose un mot de passe d'au moins 12 caractères, un historique de 24 mots de passe et un verrouillage plus rapide en cas d'échec de connexion.

4.3.3 Vérifier l'application du politique de mot de passe

Une vérification a été réalisée afin de s’assurer que les politiques de mot de passe affinées s’appliquent correctement selon le profil de l’utilisateur. Cette validation permet de confirmer que les paramètres de sécurité définis dans l’annuaire sont bien pris en compte lors de l’authentification et que la différenciation entre utilisateurs standards et direction est effective.



IV. Scénarios de tests

Les tests suivants permettent de valider le bon fonctionnement de l'infrastructure ValorElec : annuaire Active Directory, stockage TrueNAS/iSCSI, droits d'accès sur les partages et application des GPO.

Test 1. Structure Active Directory
Objectif : vérifier la création de l'OU ValorElec, des sous-OU et des comptes utilisateurs.
Procédure : contrôler l'arborescence dans Utilisateurs et ordinateurs Active Directory.
Résultat attendu : la structure et les comptes sont présents aux bons emplacements.

Test 2. Stockage TrueNAS et disque iSCSI
Objectif : vérifier la connexion du volume TrueNAS sur Windows Server.
Procédure : contrôler la cible iSCSI puis la présence du disque dans Gestion des disques.
Résultat attendu : le disque iSCSI est visible, initialisé et utilisable.

Test 3. Arborescence de dossiers
Objectif : vérifier la création des dossiers métiers.
Procédure : contrôler la présence de Direction, Développement, Commercial et Commun dans E:\Partages.
Résultat attendu : l'arborescence prévue est bien créée.

Test 4. Groupes et liaison AGDLP
Objectif : vérifier la création des groupes et leur association.
Procédure : contrôler les groupes globaux, domaine locaux et leur liaison dans Active Directory.
Résultat attendu : les groupes sont présents et la chaîne AGDLP est correctement appliquée.

Test 5. Droits NTFS
Objectif : vérifier les permissions sur les dossiers.
Procédure : consulter les propriétés de sécurité des dossiers de service et du dossier commun.
Résultat attendu : modification sur les dossiers métiers, lecture sur le dossier commun.

Test 6. Accès SMB selon le profil
Objectif : vérifier l'accès aux partages selon le service de l'utilisateur.
Procédure : ouvrir une session avec plusieurs profils et tester les partages.
Résultat attendu : accès en modification sur le partage métier, lecture sur COMMUN_VE.

Test 7. Déploiement de Firefox par GPO
Objectif : vérifier l'installation automatique du logiciel.
Procédure : redémarrer un poste client ciblé et contrôler la présence de Firefox.
Résultat attendu : Firefox est installé après application de la GPO.

Test 8. Restriction du panneau de configuration
Objectif : vérifier le blocage de l'accès au panneau de configuration.
Procédure : tenter d'ouvrir le panneau de configuration depuis une session utilisateur.
Résultat attendu : l'accès est refusé avec un message de restriction.

Test 9. Politique de mot de passe affiné
Objectif : vérifier l'application des politiques selon le profil.
Procédure : afficher les paramètres appliqués à un utilisateur standard puis à un membre de la direction.
Résultat attendu : chaque profil reçoit la politique de mot de passe prévue.

IV. Bilan

La mise en œuvre de cette infrastructure a permis d'intégrer l'entreprise ValorElec dans l'environnement système du site de Chasseneuil de manière cohérente et centralisée. L'organisation de l'annuaire Active Directory a été structurée par services afin de faciliter l'administration des utilisateurs, des ordinateurs et des groupes. Cette base a ensuite permis de déployer une gestion des accès rigoureuse sur le serveur de fichiers, reposant sur une séparation claire entre les rôles d'administration, les groupes de sécurité et les permissions appliquées aux ressources.

La solution de stockage mise en place avec TrueNAS et iSCSI a permis de dissocier la couche de stockage de la couche de partage, tandis que le serveur Windows a conservé la maîtrise du système de fichiers, des permissions NTFS et des partages SMB. L'application de la méthode AGDLP a rendu l'attribution des droits plus lisible, plus évolutive et plus conforme aux bonnes pratiques d'administration. Les tests réalisés ont confirmé le bon accès aux dossiers selon les profils définis, ainsi que le fonctionnement global de l'infrastructure.

La mise en place des GPO a également permis d'automatiser plusieurs paramètres d'exploitation, avec le déploiement d'un logiciel, la restriction de certaines fonctions utilisateur et l'application de politiques de mot de passe affinées selon les profils. Ces éléments montrent l'intérêt d'une administration centralisée pour améliorer la sécurité, homogénéiser les postes et limiter les opérations manuelles. L'utilisation de PowerShell a enfin contribué à fiabiliser le déploiement en rendant plusieurs opérations reproductibles et plus rapides à exécuter.

Cette solution reste toutefois perfectible. L'absence de mécanismes de sauvegarde, de redondance du stockage ou de haute disponibilité constitue une limite en cas d'incident. Dans une perspective d'évolution, il serait pertinent de compléter l'infrastructure par une stratégie de sauvegarde automatisée, un renforcement de la résilience du stockage et une supervision plus poussée des services. L'ensemble réalisé constitue néanmoins une infrastructure fonctionnelle, administrable et sécurisée, répondant aux objectifs fixés pour l'intégration de ValorElec.

VII. Annexes

Annexe 1. Script : Création des OU

```
# Création des OU à l'aide de Powershell

Import-Module ActiveDirectory

# Base
$domain = "OU=ETP Chasseneuil,DC=chasseneuilx86,DC=local"
$baseOU = "OU=ValorElec,OU=Clients Entreprises,$domain"

# Entreprises
$ouValor= "Ordinateurs","Utilisateurs"

foreach ($ou in $ouValor) {
   New-ADOrganizationalUnit -Name "Direction" -Path "OU=$ou,$baseOU"
   New-ADOrganizationalUnit -Name "Développement" -Path "OU=$ou,$baseOU"
   New-ADOrganizationalUnit -Name "Commercial" -Path "OU=$ou,$baseOU"
}
```

Annexe 2. Script : Création des utilisateurs de l'annuaire

```
# Création des utilisateurs dans Developpement
Import-Module ActiveDirectory
# Base
$domain = "OU=ETP Chasseneuil,DC=chasseneuilx86,DC=local"
$devOU = "OU=Developpement,OU=Utilisateurs,OU=ValorElec,OU=Clients Entreprises,$domain"

# Mot de passe
$Password = ConvertTo-SecureString "Sio1234*" -AsPlainText -Force

# Liste utilisateurs (10)
$devs = @(
   @{Nom="Khan"; Prenom="Aamir"},
   @{Nom="Okafor"; Prenom="Chinedu"},
   @{Nom="Garcia"; Prenom="Luis"},
   @{Nom="Nguyen"; Prenom="Minh"},
   @{Nom="Haddad"; Prenom="Youssef"}
   @{Nom="Richard"; Prenom="Hugo"},
   @{Nom="Dubois"; Prenom="Chloé"},
   @{Nom="Moreau"; Prenom="Nathan"},
   @{Nom="Laurent"; Prenom="Léa"},
   @{Nom="Simon"; Prenom="Tom"}
)

foreach ($user in $devs) {
   $login = ($user.Prenom.Substring(0,1) + $user.Nom).ToLower()

   New-ADUser `
      -Name "$($user.Prenom) $($user.Nom)" `
      -GivenName $user.Prenom `
      -Surname $user.Nom `
      -SamAccountName $login `
      -UserPrincipalName "$login@chasseneuilx86.local" `
      -Path $devOU `
      -AccountPassword $Password `
      -Enabled $true `
      -PasswordNeverExpires $true
}

# Création des utilisateurs dans Direction

Import-Module ActiveDirectory

# Base
$domain = "OU=ETP Chasseneuil,DC=chasseneuilx86,DC=local"
$dirOU = "OU=Direction,OU=Utilisateurs,OU=ValorElec,OU=Clients Entreprises,$domain"

# Mot de passe
$Password = ConvertTo-SecureString "Sio1234*" -AsPlainText -Force
```

```
# Liste utilisateurs (8)
$dirs = @(
    @{Nom="Leroy"; Prenom="Sophie"},
    @{Nom="Roux"; Prenom="Antoine"},
    @{Nom="David"; Prenom="Camille"},
    @{Nom="Bertrand"; Prenom="Louis"},
    @{Nom="Morel"; Prenom="Clara"},
    @{Nom="Fournier"; Prenom="Maxime"},
    @{Nom="Girard"; Prenom="Sarah"},
    @{Nom="Andre"; Prenom="Julien"}
)

foreach ($user in $dirs) {
    $login = ($user.Prenom.Substring(0,1) + $user.Nom).ToLower()

    New-ADUser `
        -Name "$($user.Prenom) $($user.Nom)" `
        -GivenName $user.Prenom `
        -Surname $user.Nom `
        -SamAccountName $login `
        -UserPrincipalName "$login@chasseneuilx86.local" `
        -Path $dirOU `
        -AccountPassword $Password `
        -Enabled $true `
        -PasswordNeverExpires $true
}

# Création des utilisateurs dans Commercial

Import-Module ActiveDirectory

# Base
$domain = "OU=ETP Chasseneuil,DC=chasseneuilx86,DC=local"
$comOU = "OU=Commercial,OU=Utilisateurs,OU=ValorElec,OU=Clients Entreprises,$domain"

# Mot de passe
$Password = ConvertTo-SecureString "Sio1234*" -AsPlainText -Force

# Utilisateur
$user = @{Nom="Mercier"; Prenom="Thomas"}

$login = ($user.Prenom.Substring(0,1) + $user.Nom).ToLower()

New-ADUser `
    -Name "$($user.Prenom) $($user.Nom)" `
    -GivenName $user.Prenom `
    -Surname $user.Nom `
    -SamAccountName $login `
    -UserPrincipalName "$login@chasseneuilx86.local" `
    -Path $comOU `
    -AccountPassword $Password `
    -Enabled $true `
    -PasswordNeverExpires $true
```

Annexe 3. Mise en place du stockage TrueNAS et connexion iSCSI

1. Installer TrueNAS sur la machine virtuelle
Démarrer la machine virtuelle TrueNAS depuis l'image ISO officielle.
Sélectionner l'option Install/Upgrade, choisir le disque système de 20 Go, puis définir le mot de passe administrateur de l'interface.

2. Configurer le réseau en mode console
Depuis la console TrueNAS, appliquer une configuration réseau statique.
Paramètres :

- Adresse IP : 10.2.0.3
- Passerelle : 10.2.0.254
- DNS : 10.2.0.1
- Nom d'hôte : truenas
- Domaine : chasseneuilx86.local

3. Créer le pool de stockage
Depuis l'interface web TrueNAS :
Chemin : Storage > Pools > Add

Créer un pool avec les deux disques de données de 100 Go.
Nom du pool :
Donnees_ValorElec

4. Créer le volume iSCSI de type zvol
Dans le pool créé, ajouter un volume de type zvol destiné à être publié au serveur Windows.

Principe retenu :

publication d'un volume bloc à destination du serveur Windows ;
gestion des partages et permissions conservée côté Windows Server.

5. Activer et configurer le service iSCSI

Depuis l'interface TrueNAS, activer le service iSCSI, puis créer :

- un portal
- une target
- un extent
- une association target/extent

Associer ensuite le zvol créé à la cible iSCSI.

6. Connecter le disque iSCSI sur Windows Server
Sur Windows Server, ouvrir l'outil Initiateur iSCSI.
Ajouter le portail cible correspondant à l'adresse :
10.2.0.3
Se connecter à la cible publiée par TrueNAS.

7. Initialiser et formater le disque
Ouvrir Gestion des disques sur Windows Server.
Initialiser le disque détecté, créer un volume simple, le partitionner puis le formater en NTFS.

8. Vérifier le résultat
Contrôler que le disque est bien visible dans la Gestion des disques et qu'il peut être utilisé comme support du serveur de fichiers.

Annexe 4. Script : Création des dossiers

```
# Chemin racine
$basePath = "E:\Partages"

#Création du dossier principal
New-Item -Path $basePath -ItemType Directory -Force

# Liste des dossiers principaux
$dossiers = @(
    "Direction", "Developpement", "Commercial", "Commun"
)

# Création des dossiers
foreach($dossier in $dossiers) {
    New-Item -Path "$basePath\$dossier" -ItemType Directory -Force
}
```

Annexe 5. Script : Création des groupes AGDLP

```
Import-Module ActiveDirectory

$ggOU = "OU=Groupes globaux,OU=ValorElec,OU=Clients Entreprises,OU=ETP Chasseneuil,DC=chasseneuilx86,DC=local"
$dlOU = "OU=Groupes domaine locaux,OU=ValorElec,OU=Clients Entreprises,OU=ETP Chasseneuil,DC=chasseneuilx86,DC=local"

# Groupes globaux
New-ADGroup "GG_Direction_VE" -GroupScope Global -Path $ggOU
New-ADGroup "GG_Developpement_VE" -GroupScope Global -Path $ggOU
New-ADGroup "GG_Commercial_VE" -GroupScope Global -Path $ggOU

# Groupes domain local
New-ADGroup "DL_Direction_VE_M" -GroupScope DomainLocal -Path $dlOU
New-ADGroup "DL_Developpement_VE_M" -GroupScope DomainLocal -Path $dlOU
New-ADGroup "DL_Commercial_VE_M" -GroupScope DomainLocal -Path $dlOU
New-ADGroup "DL_Commun_VE_L" -GroupScope DomainLocal -Path $dlOU
```

Annexe 6. Script : Peuplement des groupes globaux et liaison AGDLP

```
# Peuplement des groupes globaux
# Direction
Get-ADUser -Filter * -SearchBase "OU=Direction,OU=Utilisateurs,OU=ValorElec,OU=Clients Entreprises,OU=ETP
Chasseneuil,DC=chasseneuilx86,DC=local" | ForEach-Object {
    Add-ADGroupMember -Identity "GG_Direction_VE" -Members $_
}

# Développement
Get-ADUser -Filter * -SearchBase "OU=Developpement,OU=Utilisateurs,OU=ValorElec,OU=Clients Entreprises,OU=ETP
Chasseneuil,DC=chasseneuilx86,DC=local" | ForEach-Object {
    Add-ADGroupMember -Identity "GG_Developpement_VE" -Members $_
}

# Commercial
Get-ADUser -Filter * -SearchBase "OU=Commercial,OU=Utilisateurs,OU=ValorElec,OU=Clients Entreprises,OU=ETP
Chasseneuil,DC=chasseneuilx86,DC=local" | ForEach-Object {
    Add-ADGroupMember -Identity "GG_Commercial_VE" -Members $_
}

# Liaison AGDLP
Add-ADGroupMember DL_Direction_VE_M GG_Direction_VE
Add-ADGroupMember DL_Developpement_VE_M GG_Developpement_VE
Add-ADGroupMember DL_Commercial_VE_M GG_Commercial_VE

Add-ADGroupMember DL_Commun_VE_L GG_Direction_VE
Add-ADGroupMember DL_Commun_VE_L GG_Developpement_VE
Add-ADGroupMember DL_Commun_VE_L GG_Commercial_VE
```

Annexe 7. Script : Application des droits NTFS et SMB

```
# Application des droits NTFS
# Direction
icacls "E:\Partages\Direction" /inheritance:r
icacls "E:\Partages\Direction" /grant:r "SYSTEM:(F)"
icacls "E:\Partages\Direction" /grant:r "Administrateurs:(F)"
icacls "E:\Partages\Direction" /grant "DL_Direction_VE_M:(M)"

# Développement
icacls "E:\Partages\Developpement" /inheritance:r
icacls "E:\Partages\Developpement" /grant:r "SYSTEM:(F)"
icacls "E:\Partages\Developpement" /grant:r "Administrateurs:(F)"
icacls "E:\Partages\Developpement" /grant "DL_Developpement_VE_M:(M)"

# Commercial
icacls "E:\Partages\Commercial" /inheritance:r
icacls "E:\Partages\Commercial" /grant:r "SYSTEM:(F)"icacls "E:\Partages\Commercial" /grant:r "Administrateurs:(F)"
icacls "E:\Partages\Commercial" /grant "DL_Commercial_VE_M:(M)"

# Commun
icacls "E:\Partages\Commun" /inheritance:r
icacls "E:\Partages\Commun" /grant:r "SYSTEM:(F)"
icacls "E:\Partages\Commun" /grant:r "Administrateurs:(F)"
icacls "E:\Partages\Commun" /grant "DL_Commun_VE_L:(R)"

# Création de partage SMB
New-SmbShare -Name "DIRECTION_VE" -Path "E:\Partages\Direction" -FullAccess "Administrateurs"
New-SmbShare -Name "DEVELOPPEMENT_VE" -Path "E:\Partages\Developpement" -FullAccess "Administrateurs"
New-SmbShare -Name "COMMERCIAL_VE" -Path "E:\Partages\Commercial" -FullAccess "Administrateurs"
New-SmbShare -Name "COMMUN_VE" -Path "E:\Partages\Commun" -ReadAccess "Administrateurs"# Revocation de "Tout le monde"
Revoke-SmbShareAccess -Name "DIRECTION_VE" -AccountName "Everyone" -Force -ErrorAction SilentlyContinue
Revoke-SmbShareAccess -Name "DEVELOPPEMENT_VE" -AccountName "Everyone" -Force -ErrorAction SilentlyContinue
Revoke-SmbShareAccess -Name "COMMERCIAL_VE" -AccountName "Everyone" -Force -ErrorAction SilentlyContinue
Revoke-SmbShareAccess -Name "COMMUN_VE" -AccountName "Everyone" -Force -ErrorAction SilentlyContinue

# Attribution
Grant-SmbShareAccess -Name "DIRECTION_VE" -AccountName "Utilisateurs authentifiés" -AccessRight Change -Force
Grant-SmbShareAccess -Name "DEVELOPPEMENT_VE" -AccountName "Utilisateurs authentifiés" -AccessRight Change -Force
Grant-SmbShareAccess -Name "COMMERCIAL_VE" -AccountName "Utilisateurs authentifiés" -AccessRight Change -Force
Grant-SmbShareAccess -Name "COMMUN_VE" -AccountName "Utilisateurs authentifiés" -AccessRight Read -Force
```

Annexe 8. Déploiement d’un logiciel par GPO

1. Préparer le package d’installation
Copier le fichier Firefox.msi dans un dossier partagé accessible aux ordinateurs du domaine.

Partage utilisé :
Logiciels$

2. Vérifier les autorisations du partage
Attribuer au minimum les droits de lecture aux ordinateurs du domaine sur le partage contenant le package MSI.

3. Créer une nouvelle GPO
Ouvrir la console de gestion des stratégies de groupe.

Chemin : Console AD > Outils > Gestion de stratégies de groupe

Créer un nouvel objet GPO.
Nom : Deployment_Firefox

4. Configurer le déploiement du logiciel
Modifier la GPO créée.
Chemin : Configuration ordinateur > Stratégies > Paramètres du logiciel
Ajouter le package Firefox.msi depuis le partage réseau, puis choisir le mode : Attribué

5. Lier la GPO à l’unité d’organisation
Lier la GPO à l’unité d’organisation ValorElec afin qu’elle s’applique aux postes concernés.

6. Affecter les postes si nécessaire
Si un filtrage plus précis est retenu, créer un groupe pour les ordinateurs cibles puis l’utiliser dans le filtrage de sécurité de la GPO.

7. Mettre à jour les stratégies sur le poste client
Sur le poste Windows concerné : redémarrer l’ordinateur ou forcer l’actualisation des stratégies.

8. Vérifier l’installation
Après redémarrage, contrôler que Firefox est bien installé sur le poste client.

Annexe 9. Restriction de l’accès au panneau de configuration par GPO

1. Créer une GPO dédiée
Ouvrir la console de gestion des stratégies de groupe et créer une nouvelle stratégie dédiée à la restriction du panneau de configuration.

2. Modifier la stratégie utilisateur
Modifier la GPO créée.

Chemin d’accès :
Configuration utilisateur > Stratégies > Modèles d’administration > Panneau de configuration

3. Activer le paramètre de restriction
Activer la stratégie permettant d’interdire l’accès au panneau de configuration.

Paramètre à activer :
Interdire l’accès au Panneau de configuration et à l’application Paramètres du PC

4. Lier la GPO à l’unité d’organisation concernée
Lier la stratégie à l’OU contenant les utilisateurs ValorElec.

5. Mettre à jour les stratégies sur le poste client
Sur le poste utilisateur :

fermer puis rouvrir la session ;
ou forcer la mise à jour des stratégies de groupe.

6. Vérifier côté client
Depuis la session utilisateur, tenter d’ouvrir le panneau de configuration ou l’application Paramètres.

Annexe 10. Mise en place des stratégies de mot de passe affiné

1. Ouvrir le conteneur des politiques de mot de passe
Depuis le Centre d'administration Active Directory, accéder au conteneur des stratégies de mot de passe.

Chemin : Centre d'administration Active Directory > System > Password Settings Container

2. Créer une politique pour les utilisateurs standards
Créer une première stratégie de mot de passe affiné.
Nom :FGPP_Utilisateurs_VE

Paramètres :

- longueur minimale : 8 caractères
- historique : 12 mots de passe
- verrouillage après : 2 tentatives échouées
- durée de verrouillage : 10 minutes

Appliquer cette stratégie aux groupes représentant les utilisateurs standards.

3. Créer une politique pour la direction

Créer une seconde stratégie plus restrictive.
Nom : FGPP_Direction_VE

Paramètres :

- longueur minimale : 12 caractères
- historique : 24 mots de passe
- verrouillage après : 1 tentative échouée
- durée de verrouillage : 5 minutes

Appliquer cette stratégie au groupe GG_Direction_VE.

4. Vérifier l'application des politiques
Depuis le Centre d'administration Active Directory, afficher les paramètres de mot de passe appliqués à un utilisateur standard puis à un utilisateur de la direction.