P2 - EvolSysWin

Contexte de l'Atelier Professionnel 2 – ValorElec / TiersLieux86

L’entreprise **TiersLieux86**, spécialisée dans l'accompagnement d'initiatives numériques locales, a récemment intégré une nouvelle structure partenaire :

ValorElec, une société dédiée à la recherche et développement dans le domaine de l'électronique.

Dans le cadre de cette intégration, TiersLieux86 souhaite mettre en place une **infrastructure système complète** pour le site de **Chasseneuil**, incluant :

- **La structuration d'un Active Directory** avec une organisation logique en unités organisationnelles (OU), groupes et utilisateurs.**La configuration d'un serveur de fichiers** sécurisé et accessible via iSCSI.
- **L'automatisation des tâches administratives** à l'aide de scripts PowerShell.
- **La mise en place de stratégies de sécurité** via des GPO adaptées aux besoins métiers de ValorElec.
- **Une étude sur la mise en œuvre de DFS** pour centraliser les partages.

Le projet vise à garantir la **sécurité**, la **centralisation des accès** et l'**efficacité des services IT** pour une vingtaine de nouveaux collaborateurs répartis en services (R&D, Direction, Commercial).

Il s'inscrit dans une démarche d'industrialisation des déploiements et de fiabilisation des configurations, en vue de **normaliser l'infrastructure** du site et d'accompagner la croissance de ValorElec.

Rappel des missions

Mission 1 : Créer la maquette de l'architecture système

- Proposer une **organisation des unités organisationnelles (OU)** pour ValorElec.
- Créer les **utilisateurs et groupes** selon la répartition des collaborateurs :
  - 10 pour le service Recherche & Développement
  - 8 pour le service Direction
  - 1 pour le service Commercial
  - 1 Directeur commercial appartenant à deux services

- Écrire un **script PowerShell** pour automatiser la création des OUs, des utilisateurs, des groupes et l'export des identifiants.

Mission 2 : Mettre en place un serveur de fichiers

- Installer et configurer un **serveur de fichiers iSCSI** (via TrueNAS).
- Réaliser une **étude sur l'implémentation d'une racine DFS dédiée** à ValorElec (avec avantages/inconvénients).

Mission 3 : Sécuriser les partages

- Proposer un **tableau d'affectation des droits** selon les services.
- Écrire un **script PowerShell** pour créer les partages, gérer les droits NTFS, créer les groupes nécessaires (domain local) et attribuer les permissions adaptées.

Mission 4 : Mettre en place des stratégies de groupe (GPO)

- Mettre en place des **politiques de sécurité** :
  - Interdiction d'accès au panneau de configuration.
  - Mot de passe avec complexité, durée, historique, verrouillage du compte.
- Bonus : implémenter une **stratégie d'audit** (comptes, AD, partages).
- Tester les GPO sur une **VM cliente Windows**.

Mission 1 : Création de la maquette de l'architecture système - ValorElec

Objectif

Mettre en place l'organisation Active Directory de l'entreprise **ValorElec**, client de TiersLieux86, via une maquette intégrée au domaine `chasseneuil.local`.

Cette architecture devra inclure :

- Une organisation en Unités d'Organisation (OU)
- Des groupes Active Directory par service
- Des comptes utilisateurs correspondant à la structure de l'entreprise
- Une automatisation par script PowerShell

Tâche 1 : Organisation Active Directory proposée pour ValorElec

Structure logique sous : `OU=Clients Entreprises,OU=ETP Chasseneuil,OU=TiersLieux86.fr,DC=chasseneuil,DC=local`

```
OU=ValorElec
|__ OU=Utilisateurs
|   |__ Comptes utilisateurs (20)
|
|__ OU=Groupes globaux
|   |__ GG_ValorElec_RnD
|   |__ GG_ValorElec_Direction
|   |__ GG_ValorElec_Commercial
|
|__ OU=Ordinateurs
```

Détail des collaborateurs :

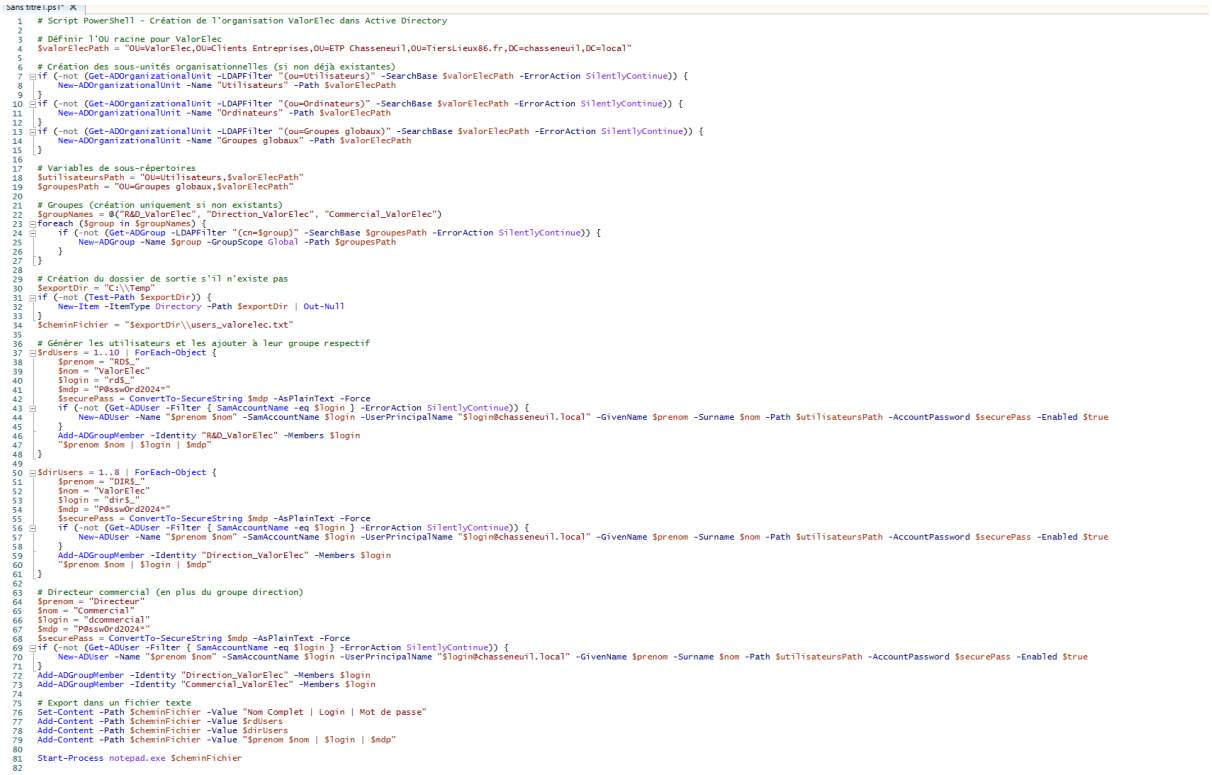
- **10** en **Recherche et Développement**
- **8** en **Direction**, dont **1 Directeur Commercial**
- **1** en **Commercial**

Tâche 2 : Script PowerShell d’automatisation

Le script à créer devra permettre de :

1. Créer l’arborescence OU ci-dessus
2. Créer les groupes globaux (GG_*)

3. Générer 20 comptes utilisateurs avec des mots de passe aléatoires
4. Ajouter les utilisateurs dans les bons groupes selon leur service
5. Exporter les informations (Nom, Login, Mot de passe, Groupe) dans un fichier Word (.docx)



```powershell
# Script PowerShell - Création de l'organisation ValorElec dans Active Directory

# Définir l'OU racine pour ValorElec
$valorElecPath = "OU=ValorElec,OU=Clients Entreprises,OU=ETP Chasseneuil,OU=TiersLieux86.fr,DC=chasseneuil,DC=local"

# Création des sous-unités organisationnelles (si non déjà existantes)
if (-not (Get-ADOrganizationalUnit -LDAPFilter "(ou=Utilisateurs)" -SearchBase $valorElecPath -ErrorAction SilentlyContinue)) {
    New-ADOrganizationalUnit -Name "Utilisateurs" -Path $valorElecPath
}
if (-not (Get-ADOrganizationalUnit -LDAPFilter "(ou=Ordinateurs)" -SearchBase $valorElecPath -ErrorAction SilentlyContinue)) {
    New-ADOrganizationalUnit -Name "Ordinateurs" -Path $valorElecPath
}
if (-not (Get-ADOrganizationalUnit -LDAPFilter "(ou=Groupes globaux)" -SearchBase $valorElecPath -ErrorAction SilentlyContinue)) {
    New-ADOrganizationalUnit -Name "Groupes globaux" -Path $valorElecPath
}

# Variables de sous-répertoires
$utilisateursPath = "OU=Utilisateurs,$valorElecPath"
$groupesPath = "OU=Groupes globaux,$valorElecPath"

# Groupes (création uniquement si non existants)
$groupNames = @("R&D_ValorElec", "Direction_ValorElec", "Commercial_ValorElec")
foreach ($group in $groupNames) {
    if (-not (Get-ADGroup -LDAPFilter "(cn=$group)" -SearchBase $groupesPath -ErrorAction SilentlyContinue)) {
        New-ADGroup -Name $group -GroupScope Global -Path $groupesPath
    }
}

# Création du dossier de sortie s'il n'existe pas
$exportDir = "C:\\Temp"
if (-not (Test-Path $exportDir)) {
    New-Item -ItemType Directory -Path $exportDir | Out-Null
}
$cheminFichier = "$exportDir\\users_valorelec.txt"

# Générer les utilisateurs et les ajouter à leur groupe respectif
$rdUsers = 1..10 | ForEach-Object {
    $prenom = "RD$_"
    $nom = "ValorElec"
    $login = "rd$_"
    $mdp = "P@sswOrd2024*"
    $securePass = ConvertTo-SecureString $mdp -AsPlainText -Force
    if (-not (Get-ADUser -Filter { SamAccountName -eq $login } -ErrorAction SilentlyContinue)) {
        New-ADUser -Name "$prenom $nom" -SamAccountName $login -UserPrincipalName "$login@chasseneuil.local" -GivenName $prenom -Surname $nom -Path $utilisateursPath -AccountPassword $securePass -Enabled $true
    }
    Add-ADGroupMember -Identity "R&D_ValorElec" -Members $login
    "$prenom $nom | $login | $mdp"
}

$dirUsers = 1..8 | ForEach-Object {
    $prenom = "DIR$_"
    $nom = "ValorElec"
    $login = "dir$_"
    $mdp = "P@sswOrd2024*"
    $securePass = ConvertTo-SecureString $mdp -AsPlainText -Force
    if (-not (Get-ADUser -Filter { SamAccountName -eq $login } -ErrorAction SilentlyContinue)) {
        New-ADUser -Name "$prenom $nom" -SamAccountName $login -UserPrincipalName "$login@chasseneuil.local" -GivenName $prenom -Surname $nom -Path $utilisateursPath -AccountPassword $securePass -Enabled $true
    }
    Add-ADGroupMember -Identity "Direction_ValorElec" -Members $login
    "$prenom $nom | $login | $mdp"
}

# Directeur commercial (en plus du groupe direction)
$prenom = "Directeur"
$nom = "Commercial"
$login = "dcommercial"
$mdp = "P@sswOrd2024*"
$securePass = ConvertTo-SecureString $mdp -AsPlainText -Force
if (-not (Get-ADUser -Filter { SamAccountName -eq $login } -ErrorAction SilentlyContinue)) {
    New-ADUser -Name "$prenom $nom" -SamAccountName $login -UserPrincipalName "$login@chasseneuil.local" -GivenName $prenom -Surname $nom -Path $utilisateursPath -AccountPassword $securePass -Enabled $true
}
Add-ADGroupMember -Identity "Direction_ValorElec" -Members $login
Add-ADGroupMember -Identity "Commercial_ValorElec" -Members $login

# Export dans un fichier texte
Set-Content -Path $cheminFichier -Value "Nom Complet | Login | Mot de passe"
Add-Content -Path $cheminFichier -Value $rdUsers
Add-Content -Path $cheminFichier -Value $dirUsers
Add-Content -Path $cheminFichier -Value "$prenom $nom | $login | $mdp"

Start-Process notepad.exe $cheminFichier
```

Script d'intégration de l'organisation ValorElec dans Active Directory

---

1. Objectif du script

Ce script PowerShell a pour but d'automatiser la création de la structure Active Directory pour l'entreprise **ValorElec**, cliente de l'ETP de Chasseneuil. Il permet de créer les unités organisationnelles (OU), les groupes, les utilisateurs, et d'organiser ces derniers selon leur service. Il automatise également l'export des identifiants (login + mot de passe) dans un fichier texte.

---

2. Ce que fait le script

a. Création de l'arborescence Active Directory

- **OU parent** : ValorElec

- **Sous-OUs** :
  - Utilisateurs
  - Ordinateurs
  - Groupes globaux

b. Création des groupes globaux

- R&D_ValorElec
- Direction_ValorElec
- Commercial_ValorElec

c. Création des utilisateurs

- **10 utilisateurs** pour le service **R&D** : rd1 à rd10
- **8 utilisateurs** pour la **Direction** : dir1 à dir8
- **1 Directeur commercial** : dcommercial (fait partie des groupes Direction et Commercial)
- Chaque utilisateur a un mot de passe par défaut : `P@ssw0rd2024*`
- Le compte est créé, activé, et assigné au groupe correspondant.

d. Export dans un fichier texte

- Le fichier `users_valorelec.txt` est créé dans `C:\Temp` et contient les informations suivantes pour chaque utilisateur :
  - Nom complet
  - Login
  - Mot de passe

---

3. Commandes de vérification utilisées

a. Vérifier les utilisateurs créés

```
Get-ADUser -SearchBase "OU=Utilisateurs,OU=ValorElec,OU=Clients Entreprises,OU=ETP Chasseneuil,OU=TiersLieux86.fr,DC=chasseneuil,DC=local" -Filter * | Select-Object Name, SamAccountName
```

b. Vérifier les membres d'un groupe

```
Get-ADGroupMember "R&D_ValorElec" | Select-Object Name, SamAccount
Name
Get-ADGroupMember "Direction_ValorElec" | Select-Object Name, SamAcc
ountName
Get-ADGroupMember "Commercial_ValorElec" | Select-Object Name, Sam
AccountName
```

---

4. Remarques

- Le script inclut un test de présence des OUs avant leur création pour éviter les erreurs.
- Il vérifie également la présence du dossier `C:\Temp` avant l'export.
- Le fichier est automatiquement ouvert dans Notepad à la fin du script.
- Le script est relanceable, mais si des utilisateurs ou groupes existent déjà, des erreurs de doublon peuvent apparaître (gérables en supprimant les objets ou en modifiant le script pour tester leur existence).

Mission 2 : Mise en place d'une VM TrueNAS (serveur de stockage)

Objectif

Mettre en place un serveur de fichiers pour le client ValorElec, via une VM TrueNAS installée sur VirtualBox, avec du stockage iSCSI.

---

1. Création de la VM TrueNAS sur VirtualBox

1.1 Paramètres de base

- **Nom** de la VM : `SERVER TRUENAS`
- **Type** : BSD

- **Version** : FreeBSD (64-bit)

1.2 Matériel

- **RAM** : 4 Go recommandés
- **Processeur** : 2 cœurs

1.3 Disques

- **Disque Système** : `SERVER TRUENAS.vdi` (taille recommandée : 16 Go minimum)
- **Disque iSCSI** : `iscsi_disk.vdi` (taille recommandée : 20 Go ou plus)

1.4 ISO

- **Image ISO TrueNAS** montée sur le contrôleur IDE : `TrueNAS-13.0-U6.7.iso`

1.5 Réseau

- **Mode réseau** : Accès par pont (bridge) ou Adaptateur réseau interne (réseau LAN Clients selon le contexte du projet)

---

2. Installation et configuration initiale de TrueNAS

2.1 Installation

- L'installation se fait via l'ISO TrueNAS lancée au démarrage de la VM.
- Choisir le disque système (ex : `ada0`) pour installer TrueNAS.
- Définir un mot de passe `root`. **Mot de passe utilisé :** **`stqnd`**

2.2 Configuration réseau

- Choix de l'interface réseau : `em0`
- DHCP : **Oui**
- IPv6 : **Non**
- Le serveur obtient automatiquement une IP locale (ex : `192.168.2.100`)

2.3 Accès à l'interface Web

- Se rendre sur l'adresse : `http://192.168.2.100`
- Identifiants :

- **Utilisateur :** `root`
- **Mot de passe :** `stqnd`

Etude sur l'implémentation d'une racine DFS pour le client ValorElec

Objectif

Proposer une architecture de partage de fichiers basée sur DFS (Distributed File System) pour centraliser les données de l'entreprise ValorElec.

Qu'est-ce que DFS ?

DFS (Distributed File System) est une fonctionnalité de Windows Server permettant :

- La création d'une **arborescence logique de dossiers** (espace de noms DFS).
- La **centralisation des partages** répartis sur un ou plusieurs serveurs.
- La **réplication des données** (optionnelle) entre serveurs via DFS-R.
- Une **meilleure accessibilité** pour les utilisateurs via un point d'accès unique.

✅ Avantages de DFS pour ValorElec

Avantage	Description
🗂️ Organisation centralisée	Tous les fichiers accessibles via `\\chasseneuil.local\ValorElec`
🔒 Gestion des droits simplifiée	Droits NTFS liés aux groupes AD (R&D, Direction, Commercial)
🖥️ Point d'accès unique	Les utilisateurs ne connaissent pas l'emplacement réel des fichiers
🔄 Redondance possible	DFS-R permet une réplication sur plusieurs serveurs (optionnel ici)
🔧 Flexible	Ajout/modification des partages sans impacter les utilisateurs

---

❌ Inconvénients de DFS

Inconvénient	Description
⚙️ Mise en place complexe	Requiert des compétences AD, DFS-N, DFS-R
🚧 Surveillance nécessaire	Suivi des réplications, journaux, synchronisation
⚠️ SPOF potentiel	Un seul serveur DFS = risque si absence de réplication ou de sauvegarde
📊 Performance à surveiller	En cas de volume important, charge sur les disques ou le réseau

📂 Espace de noms DFS proposé pour ValorElec

Racine DFS : `\\chasseneuil.local\ValorElec`

Dossier DFS	Destination	Groupe AD concerné
`\R&D`	Partage pour le service R&D	`R&D_ValorElec`
`\Direction`	Partage pour la direction	`Direction_ValorElec`
`\Commercial`	Partage pour le commercial	`Commercial_ValorElec`

🔢 Recommandations techniques

Composant	Détail
Serveur DFS	Contrôleur de domaine ou serveur de fichiers (TrueNAS/SMB)
Type de racine DFS	Domaine-based namespace `\\domaine.local\...`
Droits d'accès	ACL par groupe AD (droits NTFS)
Réplication DFS-R	Optionnelle mais recommandée en production

Conclusion

Mettre en place un DFS pour ValorElec permet d'assurer une organisation claire, un accès centralisé, une gestion simplifiée des droits, et une évolution facilitée de l'infrastructure.

Son implémentation nécessite toutefois une planification précise, notamment si une réplication multi-site ou un environnement haute disponibilité est envisagé.

Mission 3 : Mise en place de la sécurité sur les partages de fichiers - ValorElec

Objectif

Mettre en place une automatisation de la sécurité sur les partages de fichiers pour le client ValorElec à l'aide de PowerShell, avec une gestion des droits NTFS et des partages réseau conformes à l'organisation Active Directory mise en place.

---

1. Structure prévue des partages

Trois services disposent chacun de leur dossier partagé :

- **Partage_RD** (Recherche & Développement)
- **Partage_Direction** (Direction)
- **Partage_Commercial** (Commercial)

Pour chaque dossier, les droits suivants sont attribués via des groupes de sécurité :

Droit	Groupe	Nom du groupe
Lecture seule	Groupe domaine local	DL_[Service]_L
Lecture / Écriture	Groupe domaine local	DL_[Service]_LM
Contrôle total	Groupe domaine local	DL_[Service]_CT

Chaque groupe global de service est membre du groupe domaine local avec droit Lecture/Écriture.

---

2. Script PowerShell utilisé

Un script PowerShell a été écrit pour automatiser :

- La création des dossiers
- La création des groupes domaine locaux si non existants
- L'ajout du groupe global du service au groupe domaine local LM
- L'application des droits NTFS
- Le partage réseau du dossier (New-SmbShare)

Le répertoire de base utilisé est : `C:\Partages\ValorElec`

---

3. Problèmes rencontrés

- **Erreur sur le chemin d'OU** : les groupes domaine locaux étaient censés être créés dans `OU=Groupes domaine locaux`, mais l'OU n'existait pas. Cela a provoqué des erreurs `ObjectNotFound` lors de la création des groupes.
- **Nom de partage invalide** : erreur de type `Windows System Error 123` car le nom de partage ou chemin contenait une syntaxe incorrecte.
- **Erreur dans New-Object pour les droits NTFS** : problème de syntaxe à corriger (paramètre mal utilisé).

---

4. Actions correctives effectuées

- Création manuelle de l'OU `Groupes domaine locaux` dans Active Directory.
- Vérification et correction de la syntaxe des noms de partage.
- Correction du script pour la gestion propre des objets ACL avec `FileSystemAccessRule`.

---

5. État actuel

- Les dossiers `Partage_RD`, `Partage_Direction` et `Partage_Commercial` sont bien créés.
- Les droits sont appliqués selon le niveau d'accès requis.
- Les partages réseau sont créés et visibles.
- Le script peut être rejoué si besoin, une fois les OU correctement créées.

---

6. Commandes utiles

Création manuelle d'une OU si manquante :

```
New-ADOrganizationalUnit -Name "Groupes domaine locaux" -Path "OU=Groupes,OU=TiersLieux86.fr,DC=chasseneuil,DC=local"
```

Vérifier l'existence d'un groupe :

```
Get-ADGroup -Filter {Name -eq "DL_RD_LM"}
```

Afficher les partages SMB :

```
Get-SmbShare
```

Vérifier les droits d’accès d’un dossier :

```
Get-Acl "C:\Partages\ValorElec\Partage_RD" | Format-List
```

Conclusion

Cette mission a permis d’appliquer de manière automatisée une organisation sécuritaire des accès aux partages pour chaque service de ValorElec, en s’appuyant sur les groupes Active Directory. Une fois les erreurs corrigées, le script est fonctionnel et permet de gagner un temps précieux dans la gestion des partages et des droits utilisateurs.

Mission 4 : Mise en place des stratégies de groupe (GPO) pour ValorElec

Objectifs

Mettre en place un ensemble de stratégies de groupe afin de répondre aux besoins de sécurité et de gestion du parc informatique de l'entreprise ValorElec.

Contexte

Dans le cadre de l'intégration de ValorElec à TiersLieux86, des politiques de groupe doivent être appliquées aux utilisateurs et aux machines afin de :

- Renforcer la sécurité des mots de passe et du système
- Empêcher les utilisateurs d'accéder à certaines fonctions critiques du système (comme le panneau de configuration)
- Mettre en place une stratégie d'audit

Tâche 1 : Restrictions par stratégie de groupe

Interdiction d'accès au panneau de configuration

1. Créer une GPO `Restriction_PanneauConfig`
2. Aller dans `Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration`
3. Activer : `Interdire l'accès au panneau de configuration et aux Paramètres du PC`
4. Lier cette GPO à l'OU ValorElec

Tâche 2 : Politique de mot de passe générale (tous utilisateurs)

1. Aller dans `Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Politique de mot de passe` :
   - Longueur mini : 8
   - Durée de vie max : 30 jours
   - Historique : 12 mots de passe
2. Aller dans `Verrouillage de compte` :
   - Tentatives avant verrouillage : 2
   - Durée de verrouillage : 10 min
   - Réinitialisation du compteur : 10 min

Tâche 3 : Stratégie d'audit

1. Créer une GPO `Audit_ValorElec`
2. Aller dans `Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Stratégie d'audit`
3. Activer :
   - Audit des échecs de connexion
   - Audit de la gestion des comptes
   - Audit d'accès aux objets (dossier Acrobat Reader)

4. Aller dans `Audit avancé` pour spécifier des journaux plus précis

Tâche 4 : Tests sur une machine cliente

1. Redémarrer la machine cliente
2. Lancer dans PowerShell : `gpresult /r` ou `gpupdate /force`
3. Vérifier :
    - L'interdiction d'accès au panneau de configuration
    - Les stratégies de mot de passe (avec un changement de mot de passe test)
    - La création de logs dans `Observateur d'événements`

Conclusion

Les GPO ont permis d'automatiser l'application des politiques de sécurité pour ValorElec. Ces mesures renforcent la protection du SI tout en facilitant la gestion des utilisateurs et des postes de travail par l'administrateur.