TP WINDOWS SERVER

Administration et création d'objets ADDS

PARTIE 1 : ACTIVATION DE LA CORBEILLE AD

Il est possible d'activer la corbeille AD (irréversible). En fonction d'une liste de tous les objets supprimés, l'administrateur pourra sélectionner ceux dont il souhaite la récupération. Pour se faire :

1. Depuis votre DC, lancer la console *Centre d'administration Active Directory* depuis les outils d'administration.
2. Dans le menu de gauche, double cliquer sur votre domaine « *VotreNom* » (local).
3. Cliquer sur *Activer la corbeille* dans le bandeau « *Tâches »*., puis sur « OK » afin de lancer l'activation.
4. Créer des unités d'organisation, des groupes et des utilisateurs de test puis les supprimer afin de les placer dans la corbeille.
5. Dans la console *Centre d'administration Active Directory*, double cliquer sur « *Deleted Objects »*. Les objets supprimés précédemment apparaissent.
6. Sélectionner les objets supprimés puis cliquer sur *« Restaurer »*. Les attributs des comptes devraient être restaurés.

PARTIE 2 : CREATION D'OBJETS (via interface graphique)

A. Création d'une OU test :

1. Ouvrir une session sur SDC01 avec un compte avec privilèges.
2. Ouvrir l'outil d'administration *Utilisateurs et Ordinateurs Active Directory*
3. Développer le nœud correspondant au domaine. Cliquer avec le bouton droit sur le nœud Domaine, choisir *Nouveau* puis sélectionner *Unité d'organisation* et saisir le nom de l'unité d'organisation : Test-TP.
4. Cocher la case *Protéger le conteneur contre une suppression accidentelle*. Cliquer sur OK.
5. Cliquer avec le bouton droit sur l'OU et choisir Propriétés.
6. Dans le champ *Description,* saisir *OU test de préparation au TP*. Cliquer sur OK.

B. Création d'un utilisateur test :

1. Sous votre session sur SDC01 toujours dans le composant logiciel enfichable *Utilisateurs et ordinateurs Active Directory*, développer le nœud du domaine, *VotreNom.local,* et sélectionner l'unité d'organisation *Test-TP*. Cliquer avec le bouton droit sur l'OU *Test-TP*, choisir Nouveau puis sélectionner Utilisateur. La boîte de dialogue *Nouvel objet- Utilisateur* s'affiche.
2. Dans la zone Prénom, saisir le prénom de l'utilisateur : Jean.
3. Dans la zone Nom, saisir le nom de l'utilisateur : BON.
4. Dans la zone Nom d'ouverture de session de l'utilisateur, saisir : jbon.
5. Dans la zone Nom d'ouverture de session de l'utilisateur antérieur à (Windows2000), saisir : jbon
6. Cliquer sur Suivant. Saisir un mot de passe initial pour l'utilisateur et le confirmer.

La stratégie de mot de passe par défaut d'un domaine AD exige sept caractères au moins, et doit contenir trois de ces quatre types de caractères : majuscules (A-Z), minuscules (a-z), numérique (0-9) et non alphanumérique (comme!@#$%). Le mot de passe ne peut contenir aucun des attributs de nom d'utilisateur ou de nom d'ouverture de session. Il est recommandé de créer des mots de passe uniques, même dans le cadre d'un exercice, afin d'utiliser les meilleures pratiques, y compris dans un environnement d'essai.

C. Création d'un ordinateur test :

1. Toujours dans l'arborescence de la console *Utilisateurs et ordinateurs Active Directory*, développer le nœud du domaine *VotreNom.local,* et sélectionner l'unité d'organisation *Test-TP*.
2. Cliquer avec le bouton droit sur l'OU *Test-TP*, choisir Nouveau puis sélectionner Ordinateur. La boîte de dialogue Nouvel objet- Ordinateur s'affiche. Dans la zone Nom de l'ordinateur, saisir le nom de l'ordinateur : **DSK01.** La saisie remplit automatiquement la zone Nom d'ordinateur (antérieur à Windows 2000). Ne pas changer le nom dans la zone Nom d'ordinateur (antérieur à Windows 2000).
3. Noter le compte spécifié dans la zone de texte Utilisateur ou groupe. Ne pas changer cette valeur pour l'instant. Ne pas cocher la case intitulée Attribuer ce compte d'ordinateur à un ordinateur antérieur à Windows 2000. Cliquer sur OK.
4. Cliquer avec le bouton droit sur l'ordinateur et choisir Propriétés. Examiner les propriétés disponibles pour un ordinateur. Ne changer aucun attribut pour l'instant. Cliquer sur OK.

D. Création d'un groupe test :

1. Sous votre session sur SDC01, dans l'arborescence de la console *Utilisateurs et ordinateurs Active Directory*, développer le nœud du domaine, *VotreNom.local,* et sélectionner l'OU *Test-TP*.
2. Cliquer avec le bouton droit sur l'OU *Test-TP*, choisir Nouveau puis sélectionner Groupe. La boîte de dialogue *Nouvel objet- Groupe* s'affiche. Dans la zone Nom du groupe, saisir le nom du nouveau groupe : *Test*. Ne pas changer le nom dans la zone Nom du groupe (antérieur à Windows 2000).
3. Sélectionner le Type de groupe *Sécurité* et l'étendue du groupe *Globale*. Cliquer sur OK.
4. Cliquer avec le bouton droit sur le groupe et choisir Propriétés. Compléter le champ Description pour le groupe par « Service financier ». Ne changer aucun autre attribut pour l'instant. Cliquer sur OK.

E. Ajout d'un membre au groupe *Test* :

1. Sous votre session sur SDC01, dans l'arborescence de la console *Utilisateurs et ordinateurs Active Directory*, ouvrir les propriétés de votre compte utilisateur dans l'unité d'organisation *Test-TP*. Cliquer sur l'onglet *Membres de*, puis sur le bouton Ajouter.
2. Dans la boîte de dialogue Sélectionner Groupes, saisir le nom *Test*. Cliquer sur OK.

PARTIE 3 : CREATION D'OBJETS (automatisation via commandes)

A. Automatiser la création de comptes d'utilisateurs

Utiliser une méthode pour créer un grand nombre de comptes d'utilisateurs via une feuille de calcul Excel ou un Bloc-Notes qui servira de base de données et contiendra les comptes d'utilisateurs.

La 1ère ligne du tableau doit contenir les attributs LDAP suivants (virgule = séparateur) :

dn(distinguishedName),objectClass,givenName,sn,sAMAccountName,userAccountControl. Les données à remplir sont les objets utilisateur suivants à créer, dans l'unité d'organisation ***Test-TP***, à raison d'une ligne par objet : Jean PEUPLU, Elie HARIVRA, Medhi TUNPEUX, Ella REUSSI, Alain PROVISTE, Alex AMIN et Alex SEPSION. La valeur de l'attribut *userAccountControl* est égale à 514 afin que les nouveaux comptes créés soient désactivés. Enregistrer le fichier au format .csv et utiliser la commande CSVDE pour importer tous les objets dans l'AD. Aide pour créer le fichier .csv dans le *bloc-notes* :

exemplesUsers-OU.csv

Fichier Modifier Affichage

```
Exemple pour automatiser la création d'OU :

dn,objectClass,description
"OU=Admins,DC=ggbb,DC=local",OrganizationalUnit,"Domain OU"

Exemple pour automatiser la création d'utilisateurs :

dn,objectClass,givenName,sn,sAMAccountName,userPrincipalName,userAccountControl,Department,title,initials,displayName,description
"CN=Bart ABA,OU=Utilisateurs,DC=ggbb,DC=local",user,Bart,ABA,BA101,BA101@ggbb.local,514,Commerce,VRP,BA,"Bart BA ABA","Domain user"


----> Exemples de fichiers .csv qui s'utilise avec la commande CSVDE (CSVDE /?)

Pour exporter tous les objets et attributs correspondants depuis l'AD vers un fichier .csv :
CSVDE -f C:\emplacement\fichierDomaineExport.csv
```

B. Création d'un groupe avec DSadd

La commande `DSadd` permet de créer un groupe et même de peupler ses appartenances en une seule ligne de commande :

1. Ouvrir une session sur le DC avec un compte privilège. Dans une invite de commande, saisir la commande puis appuyer ensuite sur *Entrée* :

```
dsadd group "CN=DSTest,OU=Test-TP,DC=VotreNom,DC=local" -samid DSTest -
secgrp yes -scope g
```

2. Ouvrir le composant logiciel enfichable *Utilisateurs et ordinateurs Active Directory* et vérifier que le groupe a été créé. Si le composant était déjà ouvert, rafraîchir l'affichage.
3. A quoi servent les options –secgrp et –scope utilisées pour cette commande ?

C. Modification des appartenances au groupe avec DSmod

Ajouter un utilisateur et un groupe au groupe *Test* à l'aide de la commande DSmod :

1. Ouvrir une invite de commandes. Afin de modifier les appartenances au groupe Finance, saisir la commande : `dsmod group "CN=Test,OU=Test-TP,DC=VotreNom,DC=local" -addmbr "CN=Jean PEUPLU,OU=Test-TP,DC=VotreNom,DC=local" "CN=DSTest,OU=Test-TP,DC=VotreNom,DC=local"`
2. Dans le composant logiciel enfichable *Utilisateurs et ordinateurs Active Directory*, s'assurer que le groupe *Test* contient *Jean PEUPLU* et le groupe *DSTest*.
3. Sur le même modèle ajouter *Jean BON* et Alex AMIN comme membres du groupe *DSTest* en saisissant les commandes correspondantes.

D. Affichage des appartenances au groupe avec DSget

Avec le composant logiciel enfichable *Utilisateurs et ordinateurs Active Directory*, il est difficile d'évaluer les appartenances au groupe. La commande *DSget* simplifie considérablement la tâche, en permettant à la fois l'examen des appartenances complètes d'un groupe et celles d'un utilisateur :

1. Ouvrir une invite de commandes. Afficher les membres directs du groupe *Test* en saisissant la commande suivante puis appuyer sur *Entrée* :

```
dsget group "CN=Test,OU=Test-TP,DC=VotreNom,DC=local" -members
```

2. Sur le même modèle afficher les membres directs du groupe *DSTest* en saisissant la commande correspondante.
3. Afficher la liste complète des membres du groupe *Test* en saisissant la commande suivante puis appuyer sur *Entrée* :

```
dsget group "CN=Test,OU=Test-TP,DC=VotreNom,DC=local" -members -expand
```

4. Afficher les appartenances directes d'Elie HARIVRA aux groupes, en saisissant la commande suivante puis appuyer sur *Entrée* :

```
dsget user "CN=Elie HARIVRA,OU=Test-TP,DC=VotreNom,DC=local" -memberof
```

5. Sur le même modèle afficher l'appartenance complète d'Alex AMIN au groupe.

E. Modification de l'appartenance aux groupes avec LDIFDE

Contrairement à CSVDE, LDIFDE peut modifier l'appartenance aux groupes existants. Utiliser LDIFDE pour modifier l'appartenance du groupe Test.

1. Ouvrir le Bloc-notes et saisir les lignes suivantes (Inclure les tirets après chaque bloc et la ligne vide entre les deux blocs) :

```
dn: CN=Test,OU=Test-TP,DC=VotreNom,DC=local
changetype: modify
add: member
member: CN= Elie HARIVRA,OU=Test-TP,DC=VotreNom,DC=local
member: CN=Medhi TUNPEUX,OU=Test-TP,dc=VotreNom,dc=local
-

dn: CN=Test,OU=Test-TP,DC=VotreNom,DC=local
changetype: modify
delete: member
member: CN=Jean BON,OU=Test-TP,DC=VotreNom,DC=local
-
```

2. Enregistrer le fichier dans votre dossier Documents et le nommer "GroupModif.ldf".
3. Ouvrir une invite de commandes. Saisir la commande suivante et appuyer sur Entrée :

```
ldifde -i -f "%userprofile%\documents\GroupModif.ldf"
```

4. Dans le composant logiciel enfichable *Utilisateurs et ordinateurs Active Directory*, s'assurer que les appartenances au groupe *Test* ont changé selon les instructions du fichier LDIF. Il devrait contenir à présent Elie HARIVRA, Medhi TUNPEUX et Jean BON.

F. Création d'un ordinateur avec *DSadd*

DSadd permet d'ajouter un ordinateur en une seule ligne de commande, uniquement grâce à son *DN*, tout en créant automatiquement les attributs *sAMAccountName* et *userAccountControl* .

1. Ouvrir une session sur le DC avec privilège. En CMD, saisir la commande suivante, et appuyer ensuite sur *Entrée* : `dsadd computer "CN=DESKTOP301,OU=Test-TP,DC=VotreNom,DC=local"`
2. Ouvrir le composant logiciel enfichable *Utilisateurs et ordinateurs Active Directory* et vérifier que l'ordinateur a bien été créé.

PARTIE 4 : CREATION D'OBJETS SELON UNE NOMENCLATURE ETABLIE (automatisation via script et/ou commandes)

Dans cette partie, en tant que nouvel administrateur d'une organisation fictive, vous allez suivre la nomenclature décidée par la DSI, et donc déjà établie avant votre arrivée.

A. Création d'OU

Les conteneurs par défaut Utilisateurs et Ordinateurs sont proposés pour faciliter la configuration et la migration vers un domaine Active Directory. Il est conseillé de créer des unités d'organisation qui reflètent un modèle d'administration, à utiliser ensuite pour créer et gérer ses propres objets dans le service d'annuaire.

À partir du schéma suivant, via la méthode d'automatisation de votre choix, créer les unités d'organisation nécessaires depuis la racine de votre domaine *VotreNom*.local en respectant les niveaux définis et en renseignant leur description pour chacune dans l'attribut prévu à cet effet :

DC=*VotreNom*,DC=local

- OU=Domain Controllers ← Contrôleurs de domaine (T0)
- OU=Admin
  - OU=Tier 0
    - OU=Accounts ← Admin-T0, comptes spécifiques admin serveurs T0
    - OU=Groups ← Groupes T0 (ex : GG-Admin-T0)
    - OU=Devices ← PAW T0, serveurs PKI, hyperviseurs
    - OU=Service Accounts ← Comptes de service critiques (AAD Connect …)
  - OU=Tier 1
    - OU=Accounts ← Admin-T1, comptes spécifiques admins serveurs, sauvegarde

- OU=Groups ← GG-Admin-Serveurs, GG-Admin-Web
- OU=Devices ← PAW T1, serveurs fichiers, web, sauvegarde, DNS
- OU=Service Accounts ← Comptes applicatifs (ex : SQL Server, IIS, …)

- OU=Tier 2
  - OU=Accounts ← Admin-T2, comptes spécifiques support T2 (ex: jdupont-admin)
  - OU=Groups ← GG-Admin-Postes
  - OU=Devices ← PAW T2
  - OU=Service Accounts ← Comptes de service standard

- OU=Utilisateurs
  - OU=Standard ← Utilisateurs métiers (comptes standard)
  - OU=Support ← Comptes standard des techniciens (ex: jdupont-user)

- OU=Groupes ← Groupes fonctionnels (ex: GG-Compta, GG-RH)
- OU=Postes ← Ordinateurs utilisateurs (non-admin)
- OU=Serveurs ← Serveurs non critiques (impression, etc.)

B. Création d'utilisateurs

1. Créer manuellement un compte utilisateur spécifique administrateur de serveur Tier 0 à votre nom (désactivé par défaut à la création), dans l'OU correspondante, en respectant la nomenclature de l'entreprise, et en incluant tous les attributs suivants :

- CN : *VotrePrénom VotreNom*
- Prénom : *VotrePrénom*
- Nom : *VotreNom*
- Initiales : *VosInitiales*
- Nom d'affichage : *VotrePrénom VosInitiales VotreNom*
- Nom d'ouverture de session de l'utilisateur : *LettreN°1PrénomLettresN°123Nom*.AT0 (ex. : LPAR.AT0 pour Léo PART)
- Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : *LettreN°1PrénomLettresN°123Nom*.AT0@*VotreNom*.local
- Description : Compte personnel d'administration T0
- Service : Informatique IT
- Fonction : Administrateur Systèmes

2. Sur le même modèle avec **DSadd**, toujours en respectant la nomenclature de l'entreprise, reprendre les mêmes attributs et valeurs qu'à la question précédente pour créer manuellement un compte utilisateur spécifique administrateur de serveur Tier 1 à votre nom (désactivé par défaut à la création), dans l'OU correspondante. Seules les valeurs suivantes changent :

- Nom d'ouverture de session de l'utilisateur : *LettreN°1PrénomLettresN°123Nom*.AT1 (ex. : LPAR.AT1 pour Léo PART)
- Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : *LettreN°1PrénomLettresN°123Nom*.AT1@*VotreNom*.local
- Description : Compte personnel d'administration T1

3. Toujours sur le même modèle, reprendre les mêmes attributs et valeurs qu'à la question 1 pour créer un compte utilisateur Standard à votre nom (désactivé par défaut à la création), dans l'OU `OU=Utilisateurs,OU=Support`. Choisir votre méthode (manuelle, DSadd ou l'ajouter au script en question 5). Seules les valeurs suivantes changent :

- Nom d'ouverture de session de l'utilisateur : *LettreN°1PrénomLettresN°123Nom*.SPT
- Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : *LettreN°1PrénomLettresN°123Nom*.SPT@*VotreNom*.local
- Description : Compte personnel Standard

4. Sur le même modèle, créer un compte Tier 2 dans l'OU correspondante pour Ella REUSSI. Choisir votre méthode (manuelle, DSadd ou l'ajouter au script en question 5).

5. Dans le tableau suivant, respecter la nomenclature de l'entreprise et rechercher les attributs aux objets correspondants (console dsa.msc via l'onglet « Editeur d'attribut » ou la console ADSI), afin de créer les utilisateurs indiqués, via la méthode d'automatisation de votre choix (sachant que les comptes doivent être désactivés par défaut à l'état de création), dans `OU=Utilisateurs,OU=Standard` (pour HCAN.STD, AHAL.STD, ATER.STD, SSEK.STD), `OU=Utilisateurs,OU=Support` (SCRO.STD), et l'OU Tier 2 correspondante (SCRO.SPT) :

DESIGNATION Propriétés (ATTRIBUTS)	UTILISATEUR STD (VALEURS D'ATTRIBUT)	UTILISATEUR STD (VALEURS D'AT-TRIBUT)	UTILISATEUR STD (VALEURS D'ATTRIBUT)	UTILISATEUR STD (VALEURS D'ATTRIBUT)	UTILISATEUR STD (VALEURS D'ATTRIBUT)	UTILISATEUR SPT (VALEURS D'ATTRIBUT)
Nom commun	Henri CANTONEY	Anne HALFABETH	Alex TERRIEUR	Sylvie SEKILE-PAMOR	Sarah CROCHE	Sarah CROCHE
Prénom	Henri	Anne	Alex	Sylvie	Sarah	Sarah
Nom	CANTONEY	HALFABETH	TERRIEUR	SEKILE-PAMOR	CROCHE	CROCHE
Initiales	HC	AH	AT	SS	SC	SC
Nom d'affichage	Henri HC CANTONEY	Anne AH HALFABETH	Alex AT TERRIEUR	Sylvie SS SEKILE-PAMOR	Sarah SC CROCHE	Sarah SC CROCHE
Nom d'ouverture de session de l'utilisateur	HCAN.STD	AHAL.STD	ATER.STD	SSEK.STD	SCRO.STD	SCRO.SPT
Nom d'ouverture de session de l'utilisateur	HCAN.STD@ *VotreNom*. local	AHAL.STD@ *VotreNom*. local	ATER.STD@ *VotreNom*. local	SSEK.STD@ *VotreNom*.local	SCRO.STD@ *VotreNom*.local	SCRO.SPT@ *VotreNom*.local
Description	Domain user	Domain user	Domain user	Domain user	Domain user	Support User
Service	Restaura-tion	Entretien	Entretien	Medical	Informatique	Informatique
Fonction	Chef cuisinier	Technicienne de surface	Technicien espaces verts	Médecin infirmière	Tech. support téléphonique	Tech. support téléphonique

6. Ajouter les comptes de Tier aux groupes de sécurité existants :

T0 > Admins du domaine, Admins de l'entreprise, Administrateurs

T1 > Opérateurs de serveur

D'autres groupes peuvent être ajouté en fonction des besoins à condition d'intégrer certaines règles de sécurité supplémentaires …

C. Création d'ordinateurs

Créer les comptes d'ordinateurs suivants au préalable (pas encore joints au domaine), via la méthode d'automatisation de votre choix :

NOM	*UNITÉ D'ORGANISATION*	*DESCRIPTION*
PKI01	*VotreNom*.local>Admin>Tier0>Devices>**Servers**	Autorité de Certification
PKI02	*VotreNom*.local>Admin>Tier0>Devices>**Servers**	Autorité de Certification
FIL01	*VotreNom*.local>Admin>Tier1>Devices>**Servers**	Serveur de fichier
FIL02	*VotreNom*.local>Admin>Tier1>Devices>**Servers**	Serveur de fichier
MEX01	*VotreNom*.local>Admin>Tier1>Devices>**Servers**	Serveur de messagerie
MEX02	*VotreNom*.local>Admin>Tier1>Devices>**Servers**	Serveur de messagerie
PRT01	*VotreNom*.local>**Servers**	Serveur d'impression
LAB01	*VotreNom*.local>**Servers**	Serveur de test (experimental)
LAP00	*VotreNom*.local>Admin>Tier0>Devices>**PAW**	Ordinateur portable T0
LAP01	*VotreNom*.local>Admin>Tier0>Devices>**PAW**	Ordinateur portable T1
LAP02	*VotreNom*.local>Admin>Tier0>Devices>**PAW**	Ordinateur portable T2
LAP11	*VotreNom*.local>Postes>**Laptop**	Ordinateur portable STD
LAP12	*VotreNom*.local>Postes>**Laptop**	Ordinateur portable STD
WKS11	*VotreNom*.local>Postes>**Desktop**	Ordinateur de bureau STD
WKS12	*VotreNom*.local>Postes>**Desktop**	Ordinateur de bureau STD

D. Création de groupes

Plutôt que de gérer les objets individuellement, créer les groupes (de sécurité globale) suivants, via la méthode d'automatisation de votre choix, y incluant leur attribut description dans l'AD et leurs appartenances respectives comme ci-suivent :

*UNITÉ D'ORGANISATION>**NOM***	*DESCRIPTION*	*MEMBRE*
VotreNom.local>Groupes>**Medical**	Personnel médical	Sylvie SEKILE-PAMOR
VotreNom.local>Groupes> **Entretien**	Personnel d'entretien	Alex TERRIEUR ; Anne HALFABETH
VotreNom.local>Groupes> **Resto**	Personnel de restauration	Henri CANTONEY
*VotreNom.local>Groupes> Support>***Hotline**	Assistance technique support télephonique	Sarah CROCHE (SPT)
*VotreNom.local>Groupes> Support>***Tech1**	Personnel technique support IT	Sarah CROCHE (SPT)
*VotreNom.local>Admin>Tier2>Groups>Support>***Tech2**	Personnel technique support IT - Admin postes	Ella REUSSI (AT2)
*VotreNom.local>Admin> Tier1>Groups>***Adm-Servers**	Administration des serveurs T1	Votre compte : *Prénom NOM* (AT1)
*VotreNom.local>Admin> Tier1>Groups>***Adm-T0**	Administration des serveurs T0	Votre compte : *Prénom NOM* (AT0)

PARTIE 5 : PAW (PRIVILEGED ACCESS WORKSTATIONS)

Recommandé par l'ANSSI dans le cadre du modèle Tier 0. Ce mode permet à un administrateur de se connecter en RDP à un serveur sans exposer ses tickets Kerberos ou ses identifiants en mémoire claire, réduisant ainsi le risque de vol de privilèges (ex. attaque Pass-the-Hash).

Pour configurer un ***PAW*** (poste dédié, durci) pour l'administration T0, il faut activer ***Restricted Admin Mode*** via une clé de registre ou une stratégie de groupe :

- GPO : ***Sécurité*** -> ***Authentification locale*** -> ***Autoriser le mode administrateur restreint***.
- Clé de registre : `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa` et ajouter `DisableRestrictedAdmin = 0 (DWORD)`

PARTIE 6 : DELEGUATION DE CONTROLE

Cette partie aide à gérer la délégation des tâches administratives au sein du domaine *VotreNom*.local, en autorisant l'assistance technique à prendre en charge des utilisateurs par la réinitialisation des mots de passe et le déverrouillage des comptes utilisateurs dans l'OU Utilisateurs.

1. Depuis l'OU Utilisateurs de votre domaine *VotreNom*.local, (clic droit) choisir *Délégation de contrôle* pour lancer l'Assistant Délégation de contrôle.

2. Sur la page *Utilisateurs ou groupes*, cliquer sur le bouton *Ajouter*, et dans la boîte de dialogue *Sélectionnez…*, saisir `Tech2` et cliquer sur OK.

3. Dans la page *Tâches à déléguer*, sélectionner *Réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session*.
Cliquer sur *Suivant*, passer en revue le résumé des actions accomplies et cliquer sur *Terminer*.

4. Pour repérer les changements apportés aux ACL accordées à `Tech2`, ouvrir les propriétés de l'OU Utilisateurs et choisir l'onglet *Sécurité* →bouton *Avancé*.
Dans la liste *Entrées d'autorisations*, sélectionner la première autorisation attribuée à `Tech2` →bouton *Modifier*.
Dans la boîte de dialogue *Autorisation pour Utilisateurs*, l'autorisation assignée au groupe précédemment doit apparaitre cochée. Quelles sont les autorisations et propriétés assignées ?
Cliquer ensuite sur OK pour fermer la boîte de dialogue.

5. Répéter l'étape précédente pour la deuxième entrée d'autorisation attribuée à `Tech2`, en prenant soin de répondre également à la question.

6. Répéter l'étape précédente pour afficher l'ACL d'un utilisateur au choix de l'OU Utilisateurs et examiner les autorisations héritées attribuées à `Tech2`. Que remarquez-vous ?

7. Pour repérer les changements apportés aux ACL en invite de commandes, entrer :
```
dsacls "ou=Utilisateurs,dc=VotreNom,dc=local"
```

Pour aller plus loin …

PARTIE 7 : AMELIORATION DE LA SECURITE

1) Réfléchir aux améliorations possibles de l'organisation de votre domaine AD, et proposer des axes de progressions afin de faire évoluer l'infrastructure AD en matière de sécurité.
2) Proposer des solutions techniques à appliquer sur l'infrastructure AD créée afin de renforcer et garantir la sécurité des ressources déployées.