Module 2

Installation d'un contrôleur de domaine sur une installation minimale de Windows Server 2012 :

→Install-Windowsfeature -name AD-Domain- Services:

•Exécutez la commande Windows PowerShell **Install-ADDSDomainController –domainname "Adatum.com"** avec d'autres arguments, selon les besoins.

• Créez un fichier de réponses et exécutez **dcpromo /unattend:"D:\answerfile.txt"** à une invite de commandes où "D:\answerfile.txt" est le chemin d'accès au fichier de réponses.

•Exécutez **dcpromo /unattend** à une invite de commandes avec les commutateurs appropriés,

par exemple :

dcpromo /unattend /InstallDns:yes /confirmglobal catalog:yes /replicaOrNewDomain:replica /replicadomaindnsname:"nouveau_domaine.com" /databasePath:"c:\ntds" /logPath:"c:\ntdslogs" /sysvolpath:"c:\sysvol" /safeModeAdminPassword:Pa$$w0rd /rebootOnCompletion:yes

•Sur le contrôleur de domaine complet, ouvrez une invite de commandes d'administration, tapez les commandes suivantes (où *C:\IFM* est le répertoire de destination qui contiendra la capture instantanée de la base de données AD DS) et appuyez sur Entrée après chaque ligne :

Ntdsutil

activate instance ntds

ifm

create SYSVOL full C:\IFM

Module 3

Gestion des objets de services de domaine Active Directory

Outils de ligne de commande

•**Dsadd** : Pour créer des objets.

Exemple *:* *Dsadd ou '' ou=casa,dc=TRI,dc=MA ''*

• **Dsget** : Pour afficher des objets et leurs propriétés.

Exemple : *dsget user –tel ''cn=karim,ou=casa,dc=TRI,dc=MA''*

• **Dsmod** : Pour modifier des objets et leurs propriétés.

Exemple *:* *dsmod user ''cn=salim,ou=casa,dc=TRI,dc=MA''-dept compta*

• **Dsmove.**:Pour déplacer des objets.

Exemple : *dsmove user ''cn=salim,ou=casa,dc=TRI,dc=MA'' –newparent '' ou=khouribga ,dc=TRI ,dc=MA* **''**

• **Dsquery :** Pour demander à AD DS des objets qui correspondent à des critères que vous fournissez.

Exemple : dsquery user –name John* | dsget user –office

•**Dsrm :** Pour supprimer des objets

Exemple : *dsrm ''cn=salim,ou=khouribga,dc=TRI,dc=MA''*

•**Djoin.exe** : Jonction de domaine hors connexion

•**Redircmp.exe** : Modification du conteneur d'ordinateur par défaut

•**DSACLS** ; Affichage et modification des autorisations AD DS

• **netdom :** lié machine au domaine

Exemple : netdom reset *MachineName* /domain *DomainName* /UserO *UserName* /PasswordO {*Password* | *}

•**NLTEST :** Pour réinitialiser le canal sécurisé

Exemple : NLTEST /SERVER:SERVERNAME /SC_RESET:DOMAIN\DOMAINCONTROLLER

réinitialiser le mot de passe d'un ordinateur distant avec Windows PowerShell :

invoke-command -*computername* Workstation1 -scriptblock {reset-*computermachinepassword*

Module 4 :

Automatisation de l'administration des domaines de services Active Directory

Leçon 1 :

Utilisation des outils en ligne de commande pour l'administration d'AD DS

Csvde : est un outil en ligne de commande qui exporte ou importe des objets Active Directory dans ou à partir d'un fichier de valeurs séparées par une virgule (.csv).

Les options que vous pouvez utiliser avec csvde sont répertoriées dans le tableau suivant :

Option	Description
-d RootDN	Spécifie le nom unique de conteneur à partit duquel l'exportation commencera. La valeur par défaut est le domaine.
-p SearchScope	Spécifie l'étendue de recherche relative au conteneur spécifié par l'option **-d**. L'option **SearchScope** peut avoir la valeur base (cet objet uniquement), **onelevel** (objets de ce conteneur) ou **subtree** (ce conteneur et tous les sous-conteneurs). La valeur par défaut est **subtree**.
-r Filter	Limite les objets retournés à ceux qui correspondent au filtre. Le filtre est basé sur la syntaxe de requête du protocole LDAP (Lightweight Directory Access Protocol).
-l ListOFAtrributes	Spécifie les attributs à exporter. Utilisez le nom LDAP pour chaque attribut et séparez-les par une virgule.
-f Filename	spécifier le nom du fichier .csv vers lequel les données seront exportées. Avec uniquement le nom de fichier spécifié, tous les objets du domaine seront exportés.

Ldifde : Ldifde est un outil en ligne de commande que vous pouvez utiliser pour exporter, créer, modifier ou supprimer des objets AD DS. Comme csvde, ldifde utilise les données enregistrées dans un fichier.

Les options que vous pouvez utiliser lors de l'exportation des objets sont répertoriées dans le tableau suivant :

Option	Description
-d RootDN	Racine de la recherche LDAP. La valeur par défaut est la racine du domaine.
-r Filter	Filtre de recherche LDAP qui limite les résultats retournés.
-p SearchScope	Étendue ou intensité de la recherche. Valeur possible : • **subtree** (conteneur et tous les conteneurs enfants) ; • **base** (objets enfants immédiats du conteneur uniquement) ; • **onelevel** (conteneur et ses conteneurs enfants immédiats).
-l ListOfAttributes	Liste d'attributs à inclure dans l'exportation, séparés par une virgule
-o ListOfAttributes	Liste d'attributs à exclure de l'exportation, séparés par une virgule.
-f filename	vous devez fournir au minimum un nom de fichier pour contenir les données.

Les commandes DS :

Outil	Description
DSadd	Crée des objets AD DS.
Dsget	Affiche les propriétés des objets AD DS.
Dsquery	Recherche les objets AD DS.
Dsmod	Modifie les objets AD DS.
DSrm	Supprime les objets AD DS.
DSmove	Déplace les objets AD DS.

Exemples de commandes de gestion des utilisateurs :

Pour modifier le service d'un compte d'utilisateur, tapez :
dsmod user "cn=Joe Healy,ou=Managers,dc=adatum,dc=com" -dept IT

Pour afficher le courrier électronique d'un compte d'utilisateur, tapez :
dsget user "cn=Joe Healy,ou=Managers,dc=adatum,dc=com" –email

Pour supprimer un compte d'utilisateur, tapez :
dsrm "cn=Joe Healy,ou=Managers,dc=adatum,dc=com"

Pour créer un compte d'utilisateur, tapez :
dsadd user "cn=Joe Healy,ou=Managers,dc=adatum,dc=com"

Leçon 2

Utilisation de Windows PowerShell pour l'administration d'AD DS

Applet de commande	Description
New-ADUser	Crée des comptes utilisateurs.
Set-ADUser	Modifie les propriétés des comptes utilisateurs.
Remove-ADUser	Supprime des comptes utilisateurs.
Set-ADAccountPassword	Réinitialise le mot de passe d'un compte utilisateur.
Set-ADAccountExpiration	Modifie la date d'expiration d'un compte utilisateur.
Unlock-ADAccount	Déverrouille un compte d'utilisateur lorsqu'il a été verrouillé après le dépassement du nombre autorisé de tentatives incorrectes d'ouverture de session.
Enable-ADAccount	Active un compte d'utilisateur.
Disable-ADAccount	Désactive un compte d'utilisateur.

Certains paramètres couramment utilisés pour l'applet de commande **New-ADUser** sont répertoriés dans le tableau suivant :

Paramètre	Description
AccountExpirationDate	Définit la date d'expiration du compte d'utilisateur.
AccountPassword	Définit le mot de passe du compte d'utilisateur.
ChangePasswordAtLogon	Requiert le compte d'utilisateur pour modifier les mots de passe à la prochaine connexion.
Service	Définit le service du compte d'utilisateur.
Activé	Définit si le compte d'utilisateur est activé ou désactivé.
HomeDirectory	Définit l'emplacement du répertoire de base d'un compte d'utilisateur.
HomeDrive	Définit les lettres de lecteur mappées au répertoire de base d'un compte d'utilisateur.
GivenName	Définit le prénom d'un compte d'utilisateur.
Surname	Définit le nom d'un compte d'utilisateur.
Chemin d'accès	Définit l'unité d'organisation ou le conteneur dans lequel le compte d'utilisateur est créé.

Vous trouverez ci-dessous un exemple de commande que vous pouvez utiliser pour créer un compte d'utilisateur avec une invite vous demandant d'entrer un mot de passe :
New-ADUser "Sten Faerch" -AccountPassword (Read-Host -AsSecureString "Entrez le mot de passe") -Department IT

Utilisation des applets de commande Windows PowerShell pour gérer les groupes :

Applet de commande	Description
New-ADGroup	Crée des groupes.
Set-ADGroup	Modifie les propriétés des groupes.
Get-ADGroup	Affiche les propriétés des groupes.
Remove-ADGroup	Supprime des groupes.
Add-ADGroupMember	Ajoute des membres aux groupes.
Get-ADGroupMember	Affiche l'appartenance des groupes.
Remove-ADGroupMember	Supprime des membres des groupes.
Add-ADPrincipalGroupMembership	Ajoute l'appartenance au groupe aux objets.
Get-ADPrincipalGroupMembership	Affiche l'appartenance au groupe des objets.
Remove-ADPrincipalGroupMembership	Supprime l'appartenance au groupe d'un objet.

Créer des groupes :

Paramètre	Description
Nom	Définit le nom du groupe.
GroupScope	Définit l'étendue du groupe comme **DomainLocal**, **Global** ou **Universal**. Vous devez fournir ce paramètre.
DisplayName	Définit le nom complet LDAP de l'objet.
GroupCategory	Définit s'il s'agit d'un groupe de sécurité ou d'un groupe de distribution. Si vous n'en spécifiez aucun, un groupe de sécurité est créé.
ManagedBy	Définit un utilisateur ou un groupe qui peut gérer le groupe.
Chemin d'accès	Définit l'unité d'organisation ou le conteneur dans laquelle ou lequel le groupe est créé.
SamAccountName	Définit un nom qui a une compatibilité descendante avec les systèmes d'exploitation plus anciens.

La commande suivante est un exemple de ce que vous pouvez taper à une invite Windows PowerShell pour créer un groupe :
New-ADGroup -Name "CustomerManagement" -Path "ou=managers,dc=adatum,dc=com" –GroupScope Global -GroupCategory Security

Utilisation des applets de commande Windows PowerShell pour gérer les comptes d'ordinateurs :

Applet de commande	Description
New-ADComputer	Crée un compte d'ordinateur.
Set-ADComputer	Modifie les propriétés d'un compte d'ordinateur.
Get-ADComputer	Affiche les propriétés d'un compte d'ordinateur.

Remove-ADComputer	Supprime un compte d'ordinateur.
Test-ComputerSecureChannel	Vérifie ou répare la relation d'approbation entre un ordinateur et le domaine.
Reset-ComputerMachinePassword	Réinitialise le mot de passe d'un compte d'ordinateur.

Créer des comptes d'ordinateurs :

Paramètre	**Description**
Nom	Définit le nom d'un compte d'ordinateur.
Chemin d'accès	Définit l'unité d'organisation ou le conteneur dans lequel le compte d'ordinateur sera créé.
Activé	Définit si le compte d'ordinateur est activé ou désactivé. Par défaut, le compte d'ordinateur est activé et un mot de passe aléatoire est généré.

Voici un exemple de script que vous pouvez utiliser pour créer un compte d'ordinateur : **New-ADComputer -Name LON-SVR8 -Path "ou=marketing,dc=adatum,dc=com" -Enabled $true**

Utilisation des applets de commande Windows PowerShell pour gérer les unités d'organisation :

Applet de commande	**Description**
New-ADOrganizationalUnit	Crée des unités d'organisation.
Set-ADOrganizationalUnit	Modifie les propriétés des unités d'organisation.
Get-ADOrganizationalUnit	Affiche les propriétés des unités d'organisation.
Remove-ADOrganizationalUnit	Supprime des unités d'organisation.

Créer des unités d'organisation :

Paramètre	**Description**
Nom	Définit le nom d'une nouvelle unité d'organisation.
Chemin d'accès	Définit l'emplacement d'une nouvelle unité d'organisation.
rotectedFromAccidentalDeletion	Permet d'empêcher la suppression accidentelle de l'unité d'organisation. La valeur par défaut est **$true**.

Voici un exemple de script que vous pouvez utiliser si vous voulez créer une unité d'organisation : **New-ADOrganizationalUnit -Name Sales -Path "ou=marketing,dc=adatum,dc=com" -ProtectedFromAccidentalDeletion $true**

Leçon3 :
Exécution d'opérations en bloc avec Windows PowerShell

Que sont les opérations en bloc ?

Une opération en bloc est une action unique qui modifie plusieurs objets. L'exécution d'une opération en bloc est beaucoup plus rapide que la modification de plusieurs objets individuellement.

Interrogation d'objets avec Windows PowerShell

Paramètre	Description
SearchBase	Définit le chemin d'accès AD DS pour commencer à rechercher, par exemple, le domaine ou une unité d'organisation.
SearchScope	Définit le niveau inférieur à SearchBase auquel une recherche doit être effectuée. Vous pouvez choisir de rechercher uniquement dans la base, un niveau en dessous ou dans l'ensemble de la sous-arborescence.
ResultSetSize	Définit le nombre d'objets à retourner en réponse à une requête. Pour vérifier que tous les objets sont retournés, vous devez lui affecter la valeur $null.
Propriétés	Définit les propriétés d'objet à retourner et à afficher. Pour retourner toutes les propriétés, tapez un astérisque (*). Vous n'avez pas besoin d'employer ce paramètre afin d'utiliser une propriété pour le filtrage.

Opérateur	Description
-eq	Égal à
-ne	Différent de
-lt	Inférieur à
-le	Inférieur ou égal à
-gt	Supérieur à
-ge	Supérieur ou égal à
-like	Utilise des caractères génériques pour les critères spéciaux

Vous pouvez utiliser la commande suivante pour afficher toutes les propriétés d'un compte d'utilisateur :

Get-ADUser Administrateur -Properties *

Vous pouvez utiliser la commande suivante pour retourner tous les comptes d'utilisateurs dans l'unité d'organisation Marketing et toutes ses unités d'organisation enfants :

Get-ADUser -Filter * -SearchBase "ou=Marketing,dc=adatum,dc=com" -SearchScope subtree

Vous pouvez utiliser la commande suivante pour afficher tous les comptes d'utilisateurs avec une dernière date de connexion antérieure à une date spécifique :
Get-ADUser -Filter {lastlogondate -lt "Mars 29, 2013"}
Vous pouvez utiliser la commande suivante pour afficher tous les comptes d'utilisateurs du service Marketing qui ont une dernière date de connexion antérieure à une date spécifique :
Get-ADUser -Filter {(lastlogondate -lt "Mars 29, 2013") -and (department -eq"Marketing")}

Modification d'objets avec Windows PowerShell

Pour exécuter une opération en bloc, vous devez passer la liste d'objets interrogés à une autre applet de commande pour modifier les objets. Dans la plupart des cas, vous utilisez les applets de commande **Set-AD*** pour modifier les objets.

Vous pouvez utiliser la commande suivante pour ces comptes dont l'attribut Company n'est pas défini. Elle génèrera une liste de comptes d'utilisateurs et donnera à l'attribut Company la valeur **A.Datum**.
Get-ADUser -Filter {company -notlike "*"} | Set-ADUser -Company "A. Datum"
Vous pouvez utiliser la commande suivante pour générer une liste de comptes d'utilisateurs qui n'ont pas ouvert de session depuis une date spécifique, puis les désactiver :
Get-ADUser -Filter {(lastlogondate -lt "Mars 29, 2013") -and (department -eq"Marketing")}

Module 5

Les commandes	Explication	Exemple
PING (Test-connection)	il envoie des paquets de requete d'écho ICMP à un ordinateur pour determiner si un ordinateur peut être contacté via un réseau IP.	Ping Lon-DC1
Tracert (test-NetConnection)	Affiche l'itinéraire IP au la route d'un pakcet vers n hôte ,y compris tous les sauts entre un ordinateur et ce hôte.	Test-NetConnection Lon-DC1 -Traceroute
IPCONFIG	Cette commande comporte de nombreuse option,mais l'utilisation la plus courante consiste simplement à affiche l'addresse IP,le masque de sous-réseau et la passrelle par défaut dechaque adapteur réseau d'une machine.	Ipconfig /all

Get-NetRoute	Il affiche les informations de routage IP à partir de la table de routage IP, y compris les préfixes de réseau de destination, les addresses IP de saut suivant et les métriques de routage	Get-NetRoute
Remove-NetRoute-DestinationPrefix x.x.x.x	Supprime les route IP de la table de routage IP et l'option **(DestinationPrefix)** Indique l'addresse IP de destination souhaité supprimer	Remove-NetRoute-DestinationPrefix 172.16.0.0/16