Windows Server

Administration Windows Server 2012

Chapitre 4:Automatisation de l'administration des domaines de services Active Directory

AIT MOULAY

Vue d'ensemble du module

- Utilisation des outils en ligne de commande pour l'administration d'AD DS
- Utilisation de Windows PowerShell pour l'administration d'AD DS
- Exécution d'opérations en bloc avec Windows PowerShell

Partie 1 : Utilisation des outils en ligne de commande pour l'administration d'AD DS

- Avantages de l'utilisation des outils en ligne de commande pour l'administration d'AD DS
- L’outil Csvde
- L’outil Ldifde
- les commandes DS

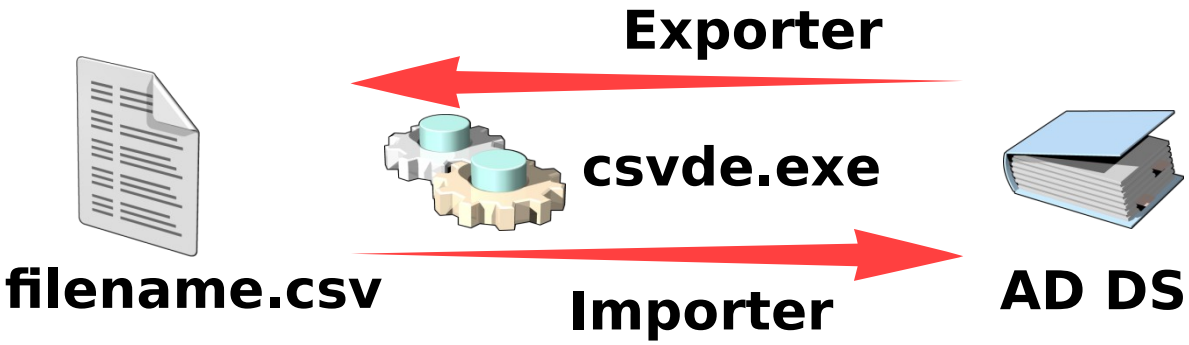
Avantages de l'utilisation des outils en ligne de commande pour l'administration d'AD DS

Les outils en ligne de commande vous permettent d'automatiser l'administration d'AD DS

Avantage des outils en ligne de commande

- Implémentation plus rapide des opérations en bloc
- Processus personnalisés pour l'administration d'AD DS
- Administration d'AD DS dans une installation minimale

L’outil Csvde



- 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)
- La principale limite de csvde est qu'il ne peut pas modifier les objets Active Directory existants. Il ne peut que créer de nouveaux objets.
- Pour exporter des objets à l'aide de csvde,on doit spécifier le nom du fichier .csv vers lequel les données seront exportées.par défaut tous les objets du domaine seront exportés.

```
csvde -f filename
```

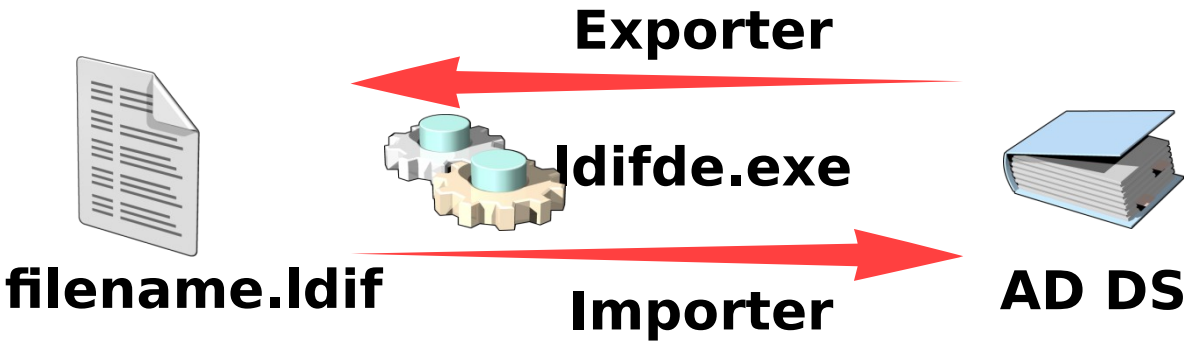
L’outil Csvde

Les autres options d’exportation de csvde sont répertoriées dans le tableau suivant.

Option	Description
-d RootDN	Spécifie le nom unique du conteneur à partir 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.

La syntaxe de base permettant d'utiliser csvde pour créer des objets est la suivante :
csvde -i -f filename -k
Le paramètre -i spécifie le mode d'importation.
Le paramètre -f identifie le nom de fichier à partir duquel l'importation s'effectue.
Le paramètre -k indique à csvde d'ignorer les messages d'erreur

L’outil Ldifde



- Ldifde est un outil en ligne de commande utilisé pour exporter, créer, modifier ou supprimer des objets AD DS
- ldifde utilise les données enregistrées dans un fichier. Le fichier doit être au format LDIF (LDAP Data Interchange Format)
- Lorsque on utilise ldifde pour exporter des objets,on doit fournir un nom de fichier vers lequel les données seront exportées.
- Par défaut tous les objets du domaine sont exportés.
- La syntaxe de base pour l'exportation des objets à l'aide de LDIFE est la suivante :

```
Ldifde f filename
```

L’outil Ldifde

Autres option d’exportation de ldifde

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.

L’outil Ldifde

Importer des objets à l'aide de Ldifde

- Lorsque on utilise ldifde pour importer des objets, on doit spécifier l'opération à effectuer sur l'objet.Pour chaque opération d'un fichier LDIF, la ligne changetype définit l'opération à effectuer.
- La syntaxe de base permettant d'utiliser ldifde pour importer des objets est la suivante :

```
ldifde -i -f filename -k
```

- Le paramètre -i spécifie le mode d'importation.
- Le paramètre -f identifie le nom de fichier à partir duquel l'importation s'effectue.
- Le paramètre -k indique à ldifde d'ignorer les erreurs, y compris l'erreur « L'objet existe déjà ».

Qu'est-ce que les commandes DS ?

- Windows Server 2012 inclut des outils en ligne de commande, appelés commandes DS, qui sont appropriées pour une utilisation dans les scripts.
- On peut utiliser les outils en ligne de commande DS pour créer, afficher, modifier et supprimer des objets AD DS. Le tableau suivant décrit les outils en ligne de commande DS.

Qu'est-ce que 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.

Qu'est-ce que les commandes DS ?

- Exemples
  - Pour modifier le service d'un compte d'utilisateur, tapez

```
Dsmod user "cn=Ahmed Fahmi,ou=Managers, dc=ofppt,dc=org" –dept IT
```

  - Pour afficher le courrier électronique d'un compte d'utilisateur, tapez

```
Dsget user "cn=Ahmed Fahmi,ou=Managers,dc=ofppt,dc=org" –email
```

  - Pour supprimer un compte d'utilisateur, tapez

```
Dsrm "cn=Ahmed Fahmi,ou=Managers,dc=ofppt,dc=org"
```

  - Pour créer un compte d'utilisateur, tapez

```
Dsadd user "cn=Ahmed Fahmi,ou=Managers,dc=ofppt,dc=org"
```

Partie 2 : Utilisation de Windows PowerShell pour l'administration d'AD DS

- gérer les comptes d'utilisateurs
- gérer les groupes
- gérer les comptes d'ordinateurs
- gérer les unités d'organisation

gérer les comptes d'utilisateurs:les applets power shell

Applet de commande	Description
New-ADUser	Crée des comptes d'utilisateurs
Set-ADUser	Modifie les propriétés des comptes d'utilisateurs
Remove-ADUser	Supprime des comptes d'utilisateurs
Set-ADAccountPassword	Réinitialise le mot de passe d'un compte d'utilisateur
Set-ADAccountExpiration	Modifie la date d'expiration d'un compte d'utilisateur
Unlock-ADAccount	Déverrouille un compte d'utilisateur après qu'il soit devenu verrouillé après que trop de tentatives incorrectes d'ouverture de session
Enable-ADAccount	Active un compte d'utilisateur
Disable-ADAccount	Désactive un compte d'utilisateur

gérer les comptes d'utilisateurs:paramètre de l’applet New-ADUser

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.
Department	Définit le service du compte d'utilisateur.
Enabled	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.
Path	Définit l'unité d'organisation ou le conteneur dans lequel le compte d'utilisateur est créé.

Exemple

```
New-ADUser “Ahmed Fahmi” –AccountPassword (Read-Host
–AsSecureString “Entrez le mot de passe”) -Department IT
```

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

Paramètre	Description
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.
Path	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.
Name	Définit le nom du groupe.

Exemple:

```
New-ADGroup –Name “CustomerManagement” –Path
“ou=managers,dc=ofppt,dc=org” –GroupScope Global
–GroupCategory Security
```

```
Add-ADGroupMember CustomerManagement –Members “Ahmed”
```

gérer les comptes d'ordinateurs

Applet de commande	Description
New-ADComputer	Crée des comptes d'ordinateurs
Set-ADComputer	Modifie les propriétés des comptes d'ordinateurs
Get-ADComputer	Affiche les propriétés des comptes d'ordinateurs
Remove-ADComputer	Supprime des comptes d'ordinateurs
Reset-ComputerMachinePassword	Réinitialise le mot de passe d'un compte d'ordinateur

Exemple:

```
New-ADComputer –Name LON-SVR8 -Path
“ou=marketing,dc=ofppt,dc=org” -Enabled $true
```

Vous pouvez utiliser l'applet de commande **Test-ComputerSecureChannel** avec le paramètre **-Repair** pour réparer une relation d'approbation perdue entre un ordinateur et le domaine. Vous devez exécuter l'applet de commande sur l'ordinateur avec la relation d'approbation perdue.

```
Test-ComputerSecureChannel -Repair
```

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
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

```
New-ADOrganizationalUnit –Name Sales
–Path “ou=marketing,dc=ofppt,dc=org”
–ProtectedFromAccidentalDeletion $true
```

Partie 3 : Exécution d'opérations en bloc avec Windows PowerShell

- Que sont les opérations en bloc ?
- Démonstration : Utilisation des outils graphiques pour exécuter des opérations en bloc
- Interrogation d'objets avec Windows PowerShell
- Modification d'objets avec Windows PowerShell
- Utilisation des fichiers CSV
- Démonstration : 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**

- **Processus permettant d'effectuer une opération en bloc**
  1. Définir une requête
  2. Modifier les objets définis par la requête

- **Vous pouvez exécuter des opérations en bloc en utilisant**
  - Des outils graphiques
  - Outils en ligne de commande
  - Scripts

- Dans Windows PowerShell, vous utilisez les applets de commande Get-* pour obtenir des listes d'objets, tels que des comptes d'utilisateurs.
- Vous pouvez également utiliser ces applets de commande pour générer des requêtes pour des objets sur lesquels vous pouvez exécuter des opérations en bloc.
- Le tableau suivant répertorie les paramètres couramment utilisés avec les applets de commande Get-AD*.

Paramètre	Description
SearchBase	Définit le chemin d'accès AD DS où commencer à rechercher
SearchScope	Définit le niveau inférieur à SearchBase auquel une recherche doit être effectuée
ResultSetSize	Définit le nombre d'objets à retourner en réponse à une requête
Properties	Définit les propriétés d'objet à retourner et à afficher

- Vous pouvez utiliser le paramètre **Filter** pour créer des requêtes pour les objets avec les applets de commande **Get-AD*.**
- Le tableau suivant répertorie les opérateurs couramment utilisés dans les requêtes Windows PowerShell.

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

Interrogation d'objets avec Windows PowerShell

Afficher toutes les propriétés d'un compte d'utilisateur

```
Get-ADUser Administrateur –Properties *
```

Afficher tous les comptes d'utilisateurs de l'unité d'organisation Marketing et tous ses sous-conteneurs

```
Get-ADUser –Filter * –SearchBase
"ou=Marketing,dc=ofppt,dc=org" –SearchScope subtree
```

Afficher tous les comptes d'utilisateurs dont la dernière date de connexion est antérieure à une date spécifique

```
Get-ADUser -Filter {lastlogondate –lt "Mars 29, 2013"}
```

Afficher tous les comptes d'utilisateurs du service Marketing dont la dernière date de connexion est antérieure à une date spécifique

```
Get-ADUser -Filter {(lastlogondate –lt "Mars 29, 2013") –and
(department –eq "Marketing")}
```

- 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.
- Pour passer la liste des objets interrogés à une autre applet de commande en vue d'un traitement ultérieur, vous utilisez le caractère de barre verticale (|). Le caractère de barre verticale passe chaque objet de la requête à une deuxième applet de commande, qui exécute ensuite une opération spécifiée sur chaque objet.
- Au lieu d'utiliser une liste d'objets à partir d'une requête pour effectuer une opération en bloc,on peut aussi utiliser une liste d'objets dans un fichier texte.

Modification d'objets avec Windows PowerShell

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 OFPPT.

```
Get-ADUser -Filter {company -notlike "*"} |
Set-ADUser -Company "OFPPT"
```

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"} | Disable-ADAccount
```

Vous pouvez utiliser la commande suivante pour désactiver les comptes d'utilisateurs répertoriés dans un fichier texte :

```
Get-Content C:\users.txt | Disable-ADAccount
```

Utilisation des fichiers CSV

La première ligne d'un fichier .csv définit les noms des colonnes

```
FirstName,LastName,Department
Ahmed,Fahmi,Informatique
Said,Alami,Recherche
Mourad,Majidi,Marketing
```

Une boucle Foreach traite le contenu d'un fichier .csv qui a été importé dans une variable

```
$users=Import-CSV C:\users.csv
Foreach ($i in $users) {
     Write-Host “Le premier nom est :” $i.FirstName
     }
```