ERCOM

Active Directory et PowerShell

Le protocole LDAP

12/0
3/20
18

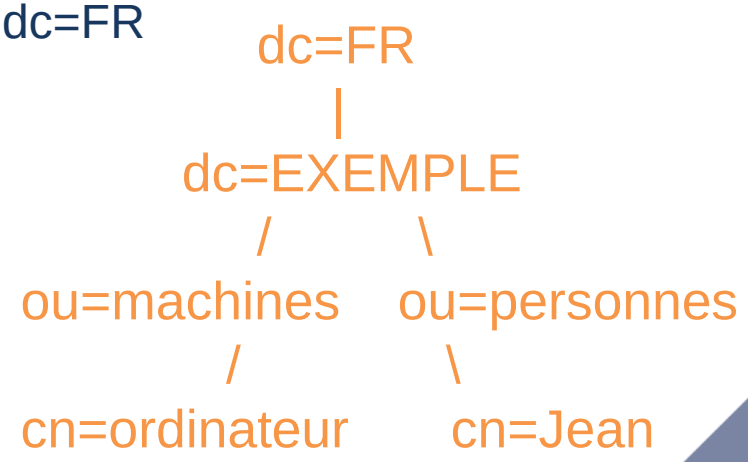
V. Présentation de LDAP

- Active Directory est un annuaire basé sur le protocole LDAP.
- LDAP est un protocole permettant l'interrogation et la modification des services d'annuaire.

- LDAP fournit à l'utilisateur des méthodes lui permettant de :
  - se connecter/ déconnecter
  - rechercher des informations (ldapsearch)
  - comparer des informations
  - insérer des entrées (ldapadd)
  - modifier des entrées (ldapmodifiy)
  - supprimer des entrées (ldapdelete)

V. L'arborescence d'informations de LDAP

- LDAP présente les informations sous forme d'une arborescence d'informations hiérarchique :
  - Domaine
  - OU
  - Nom de l’objet
- L'assemblage de tous les composants (**du plus précis au plus général**) d'un nom forme son *distinguished name*, l'exemple suivant en présente deux :
  - cn=ordinateur,ou=machines,dc=EXEMPLE,dc=FR
  - cn=Jean,ou=personnes,dc=EXEMPLE,dc=FR



ERCOM

Le module Active Directory de Powershell

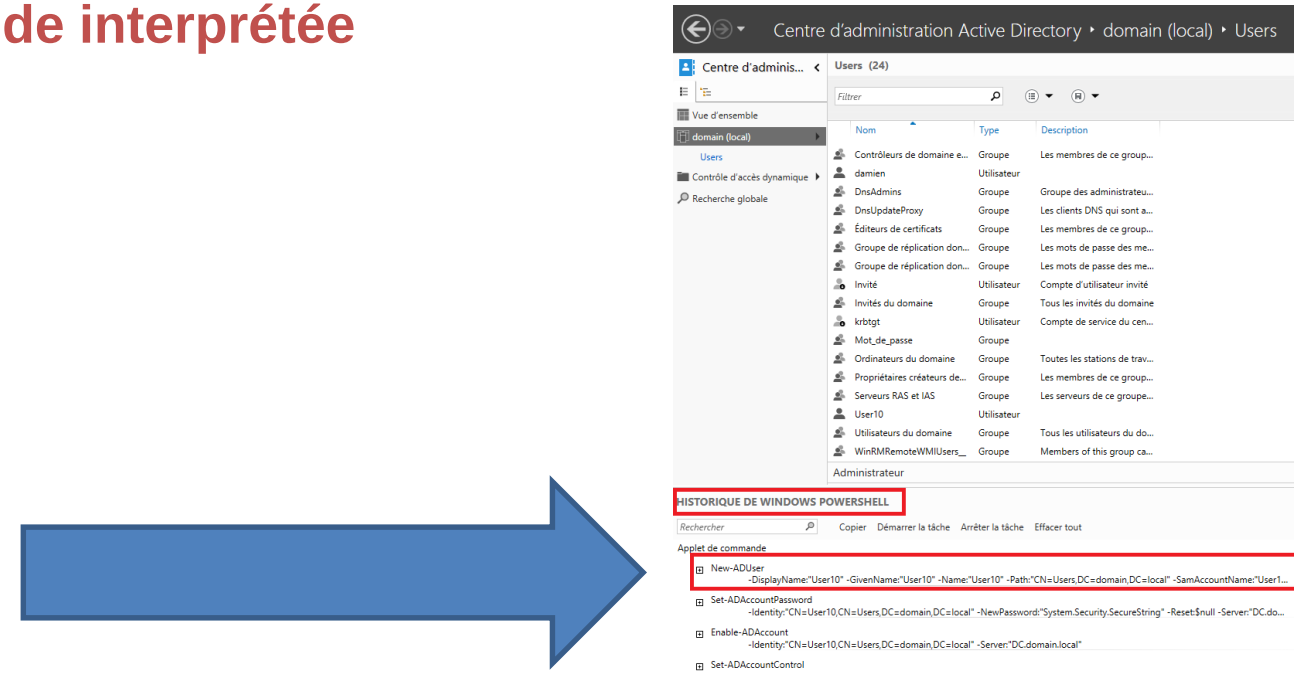
12/0
3/20
18

Le module Active Directory

- Utilisé pour géré Active Directory via Powershell
- Les objets les plus couramment gérés avec ce module :
  - Les comptes utilisateurs → ADUSER
  - Les comptes ordinateurs → ADCOMPUTER
  - Les groupes → ADGROUP
  - Les OU → ADOrganizationalUnit
- Les actions les plus courantes sur ces objets :
  - Création → NEW
  - Suppression → REMOVE
  - L'affichage d'attributs → GET
  - La modification d'attributs → SET
- Pour effectuer une opération sur un objet :
  - Création d'un nouveau compte utilisateur → NEW-ADUSER
  - Affichage d'un compte ordinateur → GET-ADCOMPUTER
  - Autres actions sur un object → ACTION-TypeObjet

Historique de Windows Powershell

- Comme vous le savez, toutes les actions que vous réalisez avec une interface graphique Windows est ensuite interprété en PowerShell.
  - (Par ailleurs, de nombreuses d'actions sont maintenant uniquement réalisable avec Powershell)
- **Lorsque vous effectuez des actions avec le centre d'administration Active Directory, vous pouvez afficher la commande interprétée**



ERCOM

Rappel Powershell

12/0
3/20
18

2 types d’utilisation

- En script (.ps1)
  - Pour automatiser les tâches
- Avec mode console
  - Pour effectuer des tâches d’administration courantes
    - Création d’un compte utilisateur par exemple.

Principe du pipeline

- Le pipeline est symbolisé par le caractère « | »
- C'est une fonctionnalité qui a été reprise du bash. Ex:
  - cat /etc/passwd | grep www-data
  - ls | cat
- Il se place entre deux commandes. Il lit la sortie de la première commande pour l'envoyer dans la seconde.
- Souvent, quand je souhaite modifier plusieurs objets en même temps je procède de la manière suivante :
  - Sélection des objets | Modication des objets sélectionnés
  - Get-XXXX | SET-XXXX
  - Ex : Get-ADUser –searchbase "OU=test,DC=Dom" | REMOVE-ADUSER

- Pour aller plus loin : http://igm.univ-mlv.fr/~dr/XPOSE2008/Introduction%20au%20Powershell/pipeline.html

Sources

- http://www.commentcamarche.com/contents/525-le-protocole-ldap
- https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
- https://docs.microsoft.com/en-us/powershell/module/addsadministration/?view=win10-ps
- https://www.supinfo.com/articles/single/3941-active-directory-avec-powershell-base
- https://blogs.technet.microsoft.com/samdrey/2011/09/26/bulk-populate-an-ad-using-a-csv-file-and-new-aduser-including-passwords/