



Active Directory et PowerShell





Le protocole LDAP



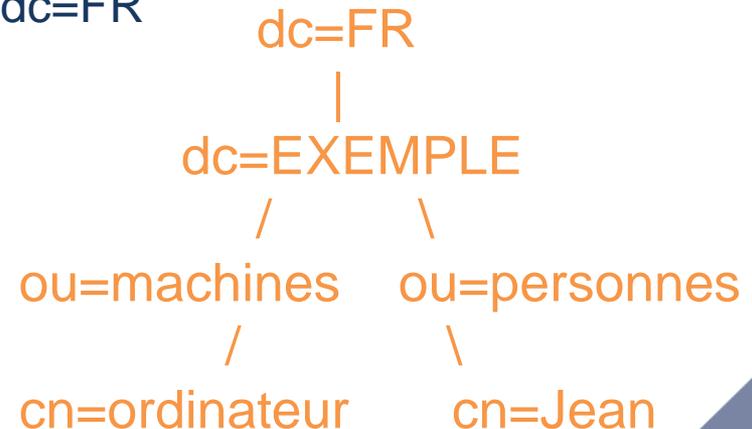
V. Présentation de LDAP

- ▶ 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 (ldapmodify)
 - 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





Le module Active Directory de Powershell

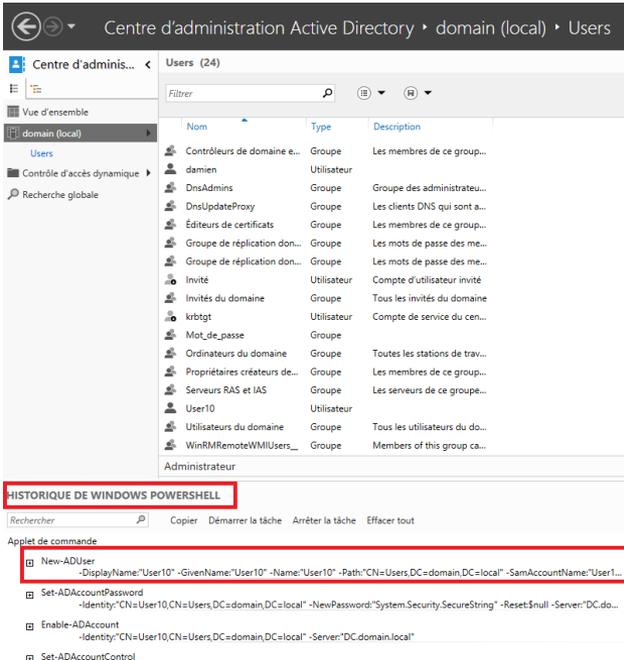


Le module Active Directory

- ▶ Utilisé pour gérer 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 objet → **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**



The screenshot shows the Active Directory Users and Groups console for the 'domain (local)' domain, specifically the 'Users (24)' view. The 'Administrateur' user is selected. Below the user list, the 'HISTORIQUE DE WINDOWS POWERSHELL' window is open, displaying a list of PowerShell commands executed in the console. A large blue arrow points from the left towards the console window.

Nom	Type	Description
Contrôleurs de domaine e...	Groupe	Les membres de ce group...
damien	Utilisateur	
DnsAdmins	Groupe	Groupe des administrateu...
DnsUpdateProxy	Groupe	Les clients DNS qui sont a...
Éditeurs de certificats	Groupe	Les membres de ce group...
Groupe de réplication don...	Groupe	Les mots de passe des me...
Groupe de réplication don...	Groupe	Les mots de passe des me...
Invité	Utilisateur	Compte d'utilisateur invité
Invités du domaine	Groupe	Tous les invités du domaine
krbtgt	Utilisateur	Compte de service du cen...
Mot_de_passe	Groupe	
Ordinateurs du domaine	Groupe	Toutes les stations de trav...
Propriétaires créateurs de...	Groupe	Les membres de ce group...
Serveurs RAS et IAS	Groupe	Les serveurs de ce groupe...
User10	Utilisateur	
Utilisateurs du domaine	Groupe	Tous les utilisateurs du do...
WinRMRemoteWMIUsers_...	Groupe	Members of this group ca...
Administrateur		

HISTORIQUE DE WINDOWS POWERSHELL

Rechercher [] Copier Démarrer la tâche Arrêter la tâche Effacer tout

Applet de commande

- [-] New-ADUser
-DisplayName>User10 -GivenName>User10 -Name>User10 -Path'CN=Users,DC=domain,DC=local' -SamAccountName>User1...
- [-] Set-ADAccountPassword
-Identity'CN=User10,CN=Users,DC=domain,DC=local' -NewPassword:'System.Security.SecureString' -Reset\$null -Server:'DC.do...
- [-] Enable-ADAccount
-Identity'CN=User10,CN=Users,DC=domain,DC=local' -Server:'DC.domain.local'
- [-] Set-ADAccountControl



Rappel Powershell



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 | Modification 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/>