Operaciones básicas de AD con Powershell

LDAP nombres distintivos

• Active Directory utiliza el Lightweight Directory Access Protocol (LDAP). Este protocolo utiliza los nombres distintivos (Distinguished Name) para identificar de forma única todos los objetos dentro del directorio. Antes de seguir viendo como creamos dichos objetos, tenemos que comprender como funcionan estos nombres distintivos (DN).

• El formato DN usa varias parejas Tipo_Objeto=Nombre_Objeto separadas por coma para identificar cada objeto. Por ejemplo, nuestro dominio dominioASO.net tiene dos componentes de dominio (DC) que son dominioASO y net y su nombre DN sería el siguiente:

dc=dominioASO, dc=net

• El tipo de una unidad organizativa es OU, así que una unidad organizativa Cuentas tendría el siguiente nombre DN:

ou=cuentas, dc=dominioASO, dc=net

• Vemos como los nombres DN van ordenados de izquierda a derecha, de modo que siempre terminan con el dc.

• Los contenedores (Usuarios, equipos) se identifican como de tipo CN (common name, nombre común). Así, el contenedor Users tiene el siguiente nombre DN:

cn=Users, dc=dominioASO, dc=net

La **diferencia** entre contenedores y unidades organizativas son las siguientes:

- Los contenedores se crean automáticamente al crear o promover un servidor a controlador de dominio, mientras que las unidades organizativas tenemos que crearlas manualmente.
- No se pueden aplicar políticas de grupo a los contenedores, sí a las unidades organizativas.
- No se pueden crear UO dentro de los contenedores, sí dentro de otras UO.

• Los usuarios del sistema también se consideran objetos del dominio, de modo que también tienen su nombre DN(Distinguished Name). El tipo de cuentas de usuario y grupo son cn (common name).

• Así, si creamos una cuenta de usuario Ines.Garcia dentro de nuestra UO OficinasCentrales que está dentro de Cuentas, esta cuenta tendrá un nombre DN como el siguiente:

CN=Inés IG. García,OU=OficinasCentrales,OU=Cuentas,DC=dominioASO,DC=net

• Una cuenta con nombre usuario, creado dentro del contenedor Users, tendría el nombre DN:

cn=usuario, cn=Users, dc=dominioASO, dc=net

• Si el nombre DN tiene espacios en blanco tiene que estar encerrado entre comillas. Los nombres DN no distinguen mayúsculas de minúsculas, por lo que los siguientes nombres DN son los mismos:

cn=pedro,ou=Administrativo,ou=Alumnos,dc=dominioASO,dc=net

CN=Pedro,Ou=ADMINISTRATIVO,Ou=ALUMNOS,DC=dominioASO,DC=net

Unidades organizativas

- El comando para crear unidades organizativas es New-ADOrganizationalUnit. El comando para crear unidades organizativas desde PowerShell es **New-ADOrganizationalUnit** donde le tenemos que indicar el nombre de la nueva OU, en que servidor se va a crear y el path dentro del directorio donde se va a crear.

La línea completa para crear una OU Recursos dentro de dominioASO.net en nuestro servidor sería la siguiente:

```
New-ADOrganizationalUnit -Name Recursos -Path "dc=dominioASO,dc=net"
```

DDD

Si queremos ver información sobre una OU utilizaríamos el comando **Get-ADOrganizationalUnit** y si quisiermos borrar una OU el comando **Remove-ADOrganizationalUnit**.

Cuentas de usuario

- El comando de PowerShell que usamos para crear usuarios es **New-ADUser**.

Los comandos de PowerShell los podemos ejecutar sin pasarles parámetros, con lo que nos pedirá los parámetros obligatorios directamente por teclado. El único parámetro que pide para el nuevo usuario es el Nombre.
Podremos comprobar como se ha creado una cuenta de usuario del dominio, sin ningún otro dato, que cuelga directamente del contenedor Users y que está deshabilitada, ya que no se puede habilitar una cuenta de Dominio a menos que cuente con una contraseña.
Para crear una cuenta con parámetros de inicialización podemos ejecutar el comando New-ADUser del siguiente modo:

```
New-ADUser
       -Name Rosa
       -Path “OU=Marketing,DC=dominioASO,DC=net”
       -Givenname Rosa
       -Surname “Cortés García”
       -UserPrincipalName Rosa@dominioASO.net
       -AccountPassword (Read-Host –AsSecureString “Contraseña para Rosa: “)
       -Enabled 1
       -ChangePasswordAtLogon 1
```

La mayoría de las opciones es fácil de entender lo que hacen, vamos a detenernos en la de la contraseña. Esa línea le indica que la contraseña de la cuenta debe ser pedida por teclado (Read-Host) que debe pedirse como una cadena segura (no verse por pantalla y guardarse internamente como cadena segura o cifrada) y que el mensaje que verá el usuario será “Contraseña : “.

Podríamos de igual modo asignar directamente la contraseña sin pedirla al usuario escribiéndola a continuación del parámetro -AccountPassword del siguiente modo para que se convierta en un objeto SecureString y no nos dé error al pasarle una cadena:

```
-AccountPassword (ConvertTo-SecureString contraseñ@0 –AsPlainText –force)
```

Para eliminar un usuario usaremos el comando **Remove-ADUser Rosa** desde PS (PowerShell).

Grupos

- El comando de PowerShell que usamos para crear grupos es **New-ADGroup**.

Un ejemplo de uso de este comando:

```
New-ADGroup
    -Description:"Descripcion del grupo"
    -GroupCategory:"Security"
    -GroupScope:"DomainLocal"
    -Name:"nombre del grupo"
    -Path:"OU=Cuentas,DC=DominioASO,DC=net"
    -SamAccountName: "nombre del grupo"
    -Server: "nombreDelServer.DominioASO.net"
```

- Para eliminar grupos tenemos el comando **Remove-ADGroup nombreGrupo**.