

Powershell

Para ejecutar el powershell desde el cuadro buscar→ powershell o desde consola ejecutamos

```
Powershell
```

El prompt cambiará y aparecerá como **PS C:\>**

Sacar información del directorio activo

Lo primero es carga el módulo del AD desde el powershell con

```
import-module ActiveDirectory
```

y si queremos sacar un listado po pantalla de equipos de nuestro dominio

```
Get-ADComputer -Filter * -Property * | Format-Table  
Name,OperatingSystem,OperatingSystemServicePack,OperatingSystemVersion -Wrap  
-Auto
```

que queremos el mismo listado para abrirlo desde un excel

```
Get-ADComputer -Filter * -Property * | Select-Object  
Name,OperatingSystem,OperatingSystemServicePack,OperatingSystemVersion |  
Export-CSV AllWindows.csv -NoTypeInfoation -Encoding UTF8
```

Equipos que no han cambiado la password en 30 días

```
$d = [DateTime]::Today.AddDays(-30)  
Get-ADComputer -Filter 'PasswordLastSet -lt $d' -Properties  
PasswordLastSet | FT Name,PasswordLastSet
```

Usuarios que no han cambiado su contraseña en tres 180 días

```
$d = [DateTime]::Today.AddDays(-180)  
Get-ADUser -Filter 'PasswordLastSet -lt $d' -Properties PasswordLastSet  
| FT Name,PasswordLastSet
```

Usuarios que no requieren password

```
Get-ADUser -Filter 'userAccountControl -band 32' | FT Name
```

Otro valores que podemos utilizar en vez de 32

```
Active Directory userAccountControl Values:
```

```
Normal Day to Day Values:
```

```
=====  
512 – Enable Account  
514 – Disable account  
544 – Account Enabled – Require user to change password at first logon  
4096 – Workstation/server  
66048 – Enabled, password never expires  
66050 – Disabled, password never expires  
262656 – Smart Card Logon Required  
532480 – Domain controller
```

All Other Values:

```
=====  
1 – script  
2 – accountdisable  
8 – homedir_required  
16 – lockout  
32 – passwd_notreqd  
64 – passwd_cant_change  
128 – encrypted_text_pwd_allowed  
256 – temp_duplicate_account  
512 – normal_account  
2048 – interdomain_trust_account  
4096 – workstation_trust_account  
8192 – server_trust_account  
65536 – dont_expire_password  
131072 – mns_logon_account  
262144 – smartcard_required  
524288 – trusted_for_delegation  
1048576 – not_delegated  
2097152 – use_des_key_only  
4194304 – dont_req_preauth  
8388608 – password_expired  
16777216 – trusted_to_auth_for_delegation
```

referencias

- <http://blogs.itpro.es/rtejero/2014/10/13/algunos-cmdlets-interesantes-de-directorio-activo-gracias-a-un-rap-as-a-service/>
- <http://blogs.technet.com/b/askds/archive/2010/02/04/inventorying-computers-with-ad-powershell.aspx>

From:

<https://intrusos.info/> - **LCWIKI**

Permanent link:

<https://intrusos.info/doku.php?id=windows:powershell&rev=1414155119>

Last update: **2023/01/18 14:00**

