Managing Access Control in Windows Servers

(CompTIA Security + SY – 601)

Objectives:

To implement identity and account management controls

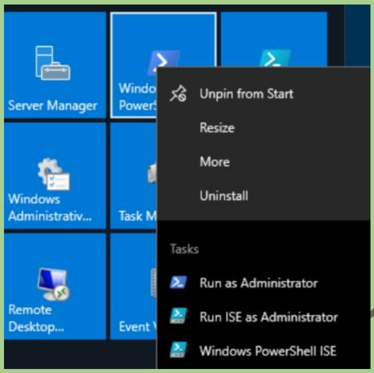
Resources:

- Windows VM (DC1)

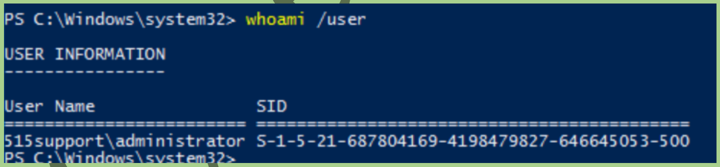
Instructions:

<u>Examine Administrator account properties</u>

- Log-in to **DC1 VM**
- Select the Start menu, right-click **Windows Powershell** and then select **Run as Administrator**. Confirm the UAC prompt by selecting **Yes**



- Run the following command to display the security ID (SID) on the other information for current user: **whoami /user**

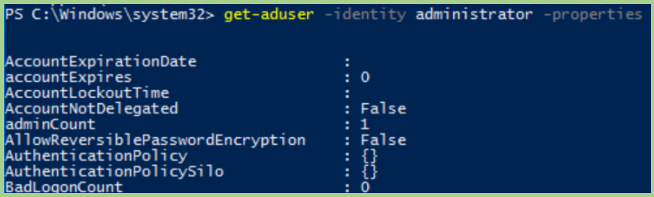


```
PS C:\Windows\system32> whoami /user

USER INFORMATION
----------------

User Name                 SID
========================= ============================================
515support\administrator S-1-5-21-687804169-4198479827-646645053-500
PS C:\Windows\system32>
```

- Run the **get-aduser** cmdlet to display account information



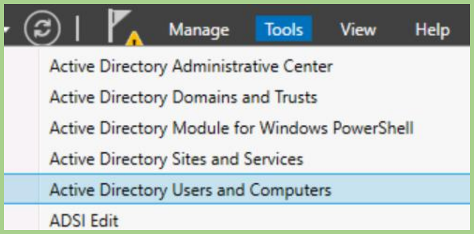
```
PS C:\Windows\system32> get-aduser -identity administrator -properties


AccountExpirationDate                   :
accountExpires                          : 0
AccountLockoutTime                      :
AccountNotDelegated                     : False
adminCount                              : 1
AllowReversiblePasswordEncryption       : False
AuthenticationPolicy                    : {}
AuthenticationPolicySilo                : {}
BadLogonCount                           : 0
```

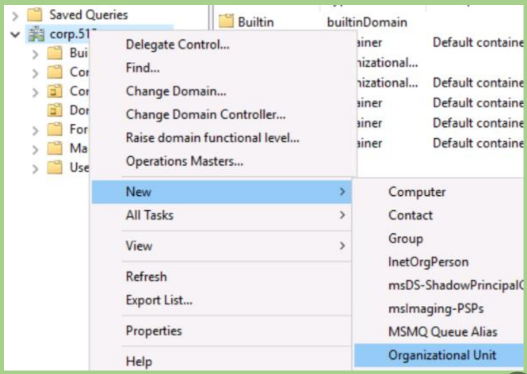
- Minimize the **Administrator: Windows PowerShell** window

Manager user, group and computer objects

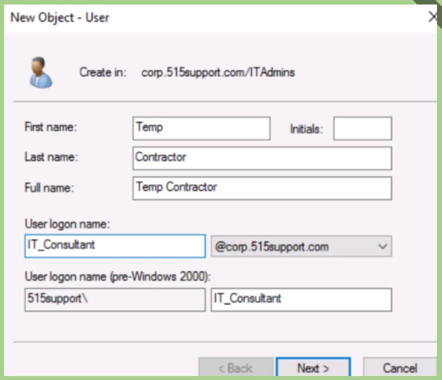
- In Server Manager, from the Tools menu, open the **Active Directory Users and Computers** console


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit

- Expand the **corp.515support.com** domain node
- Right-click the corp.515support.com domain node. Select New and then select **Organizational Unit**. Name the New OU



- Right-click the ITAdminOU, select New, and select User. Create a new user named: **IT_consultant**


New Object - User

Create in: corp.515support.com/ITAdmins

First name: Temp

Initials:

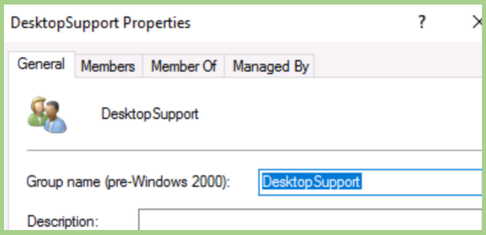
Last name: Contractor

Full name: Temp Contractor

User logon name: IT_Consultant @corp.515support.com

User logon name (pre-Windows 2000): 515support\ IT_Consultant

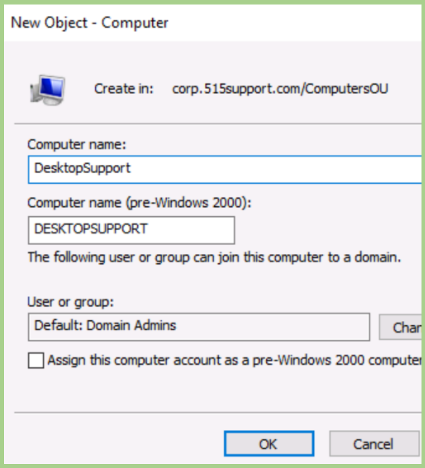
- Create a global security group within the ITAdminOU and name it **DesktopSupport**



Group name (pre-Windows 2000): DesktopSupport

Description:

- Add the **IT_Consultant** account to the **DesktopSupport** group



Create in: corp.515support.com/ComputersOU

Computer name: DesktopSupport

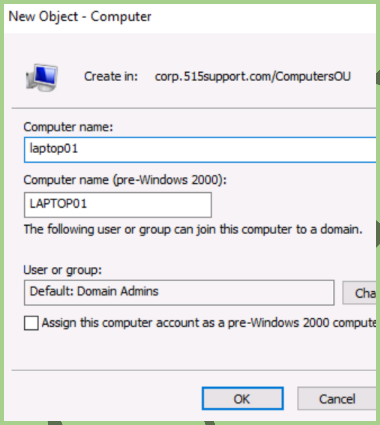
Computer name (pre-Windows 2000): DESKTOPSUPPORT

The following user or group can join this computer to a domain.

User or group: Default: Domain Admins

□ Assign this computer account as a pre-Windows 2000 compute

- From the corp.515support.com domain object, browse to the **ComputersOU** Organizational unit, right-click it. Select **New** and then create a new computer account named **laptop01**



Create in: corp.515support.com/ComputersOU

Computer name: laptop01

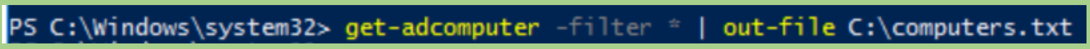
Computer name (pre-Windows 2000): LAPTOP01

The following user or group can join this computer to a domain.

User or group: Default: Domain Admins

□ Assign this computer account as a pre-Windows 2000 compute

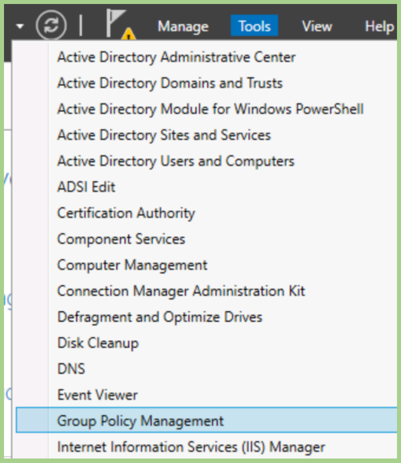
- Run the following PowerShell cmdlet to generate a report of all computer objects in the domain



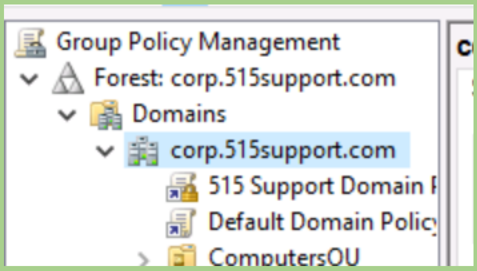
```
PS C:\Windows\system32> get-adcomputer -filter * | out-file C:\computers.txt
```

<u>Modify an existing GPO to match password requirements</u>

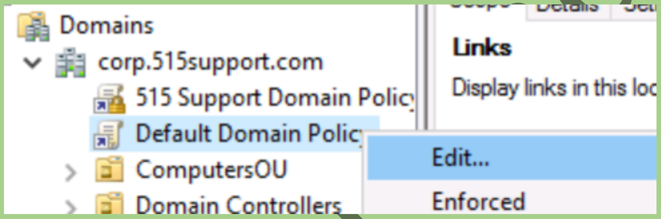
- In the **Server Manager**, select Tools > **Group Policy Management**


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Component Services
Computer Management
Connection Manager Administration Kit
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager

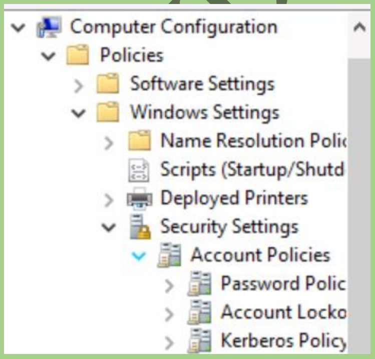
- ➢ In the Group Policy Management console, expand **Forest > Domains > corp515support.com** and select the **Default Domain Policy**



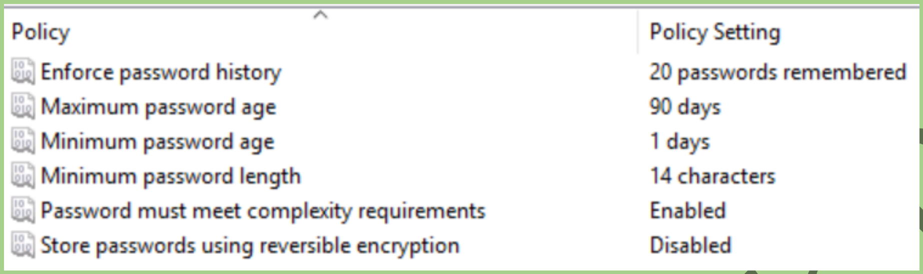
- ➢ Right-click the **Default Domain Policy** and then select Edit



- ➢ Browse to the Password Policy node by following this path: **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies**

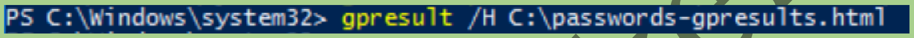


- You have reviewed your company’s written security policy regarding passwords. You must now configure the **Default Domain Policy** to match the following requirements:
- Minimum Password Length -**14 charachters**
- Complexity Requirements - **Enabled**
- Maximum Password Age - **90 days**
- Minimum Password Age - **1 day**
- Enforce Password History - **20**
- Enforce Reversible Encryption – **Displayed**



Policy	Policy Setting
Enforce password history	20 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

- In the Administrator: Windows Powershell window, run the following command to produce a report of the password policy settings to updating configuration documentation



```
PS C:\Windows\system32> gpresult /H C:\passwords-gpresults.html
```

Observations:

- **Identity and Account Management Controls:**

- Administrator account properties examined using PowerShell commands.
- New user and security group created in Active Directory.
- Computer object created in the domain.
- Password policy updated to enforce security standards.

- **Tools and Commands Used:**

- Windows PowerShell and Active Directory Users and Computers console.
- `whoami /user` and `get-aduser` PowerShell cmdlets.
- Group Policy Management for password policy adjustments.

Results:

- **User Management:**

- IT_Consultant user created and added to DesktopSupport group.
- New computer account, laptop01, successfully created.

- **Password Policy:**

- Default Domain Policy updated to enforce:
    - Minimum Password Length: 14 characters
    - Complexity Requirements: Enabled
    - Maximum Password Age: 90 days
    - Minimum Password Age: 1 day
    - Enforce Password History: 20
    - Enforce Reversible Encryption: Enabled

Conclusion:

- Successfully implemented identity and account management controls.
- Updated password policy to enhance security as per organizational requirements.

Future Work:

- **Further Enhancements:**

- Regular audits to ensure compliance with updated policies.
- Implement additional security measures like multi-factor authentication.
- Continuous training for IT staff on managing and securing Active Directory environments.