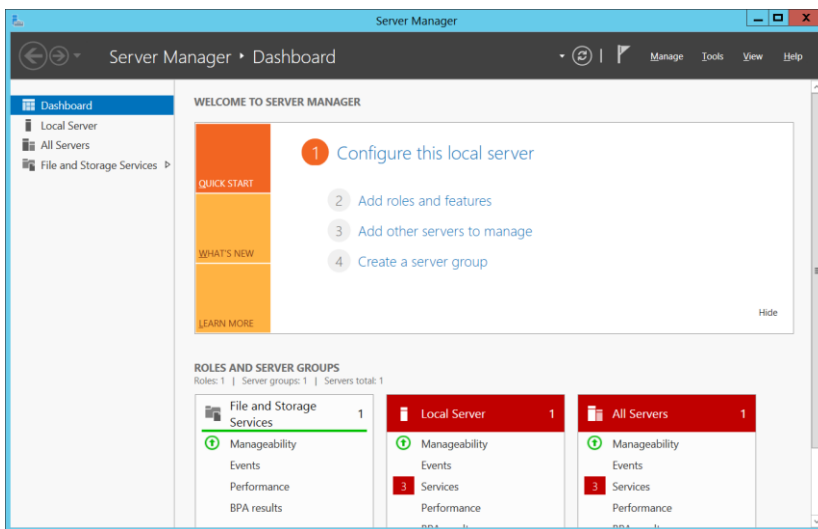


## Homework #5: Active Directory and Group Policy Objects

- This is an individual assignment, and is worth 20 points.
- The due date is Thursday, February 27<sup>th</sup>.
- You need to provide your answers to the “Homework #5 – Tasks.docx” file. Change the file name following the naming convention suggested below.
- Naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Homework #5\_ImG.docx).
- If you do not zoom in your screenshots, I will penalize you.

### Installing the Active Directory Domain Services role<sup>1</sup>

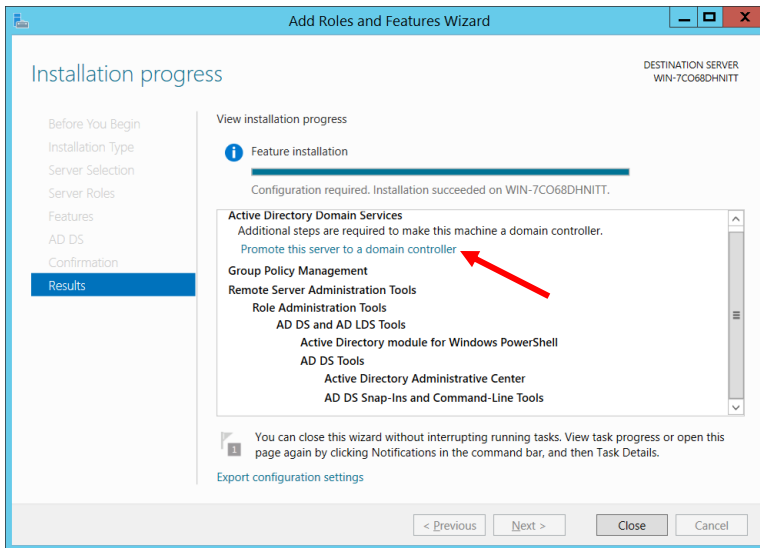
- Logon to Windows Server 2012 VM in Proxmox.



- In **Server Manager, Dashboard** > (2) select **Add Roles and Features** > On the **Add Roles and Features Wizard**, click **Next**.
- On the **Select Installation Type** page, select the **Role-Based or Feature-Based Installation** option > **Next**.
- On the **Select Destination Server** page, choose **Select a server from the pool** (we have only one server) > **Next**.
- On the **Select Server Roles** page, select the **Active Directory Domain Service** role > **Add Features**.
- On the **Select Features** page, click **Next** > On the **Active Directory Domain Services** page, click **Next** > On the **Confirm Installation Selections** page, click **Install**.
- After the installation of the role, a **Promote This Server to A Domain Controller** link is shown. Do not close the wizard.

---

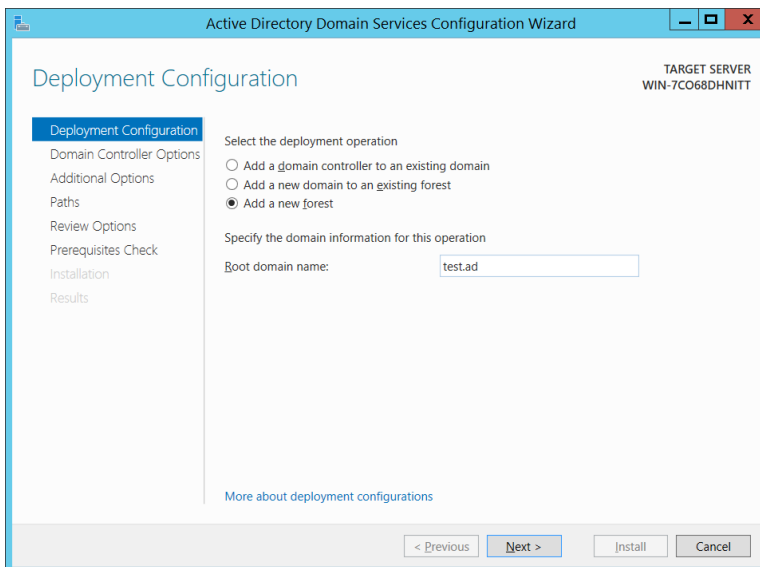
<sup>1</sup> Installing and Configuring Windows Server 2012 R2 by Craig Zacker



## Creating a new forest

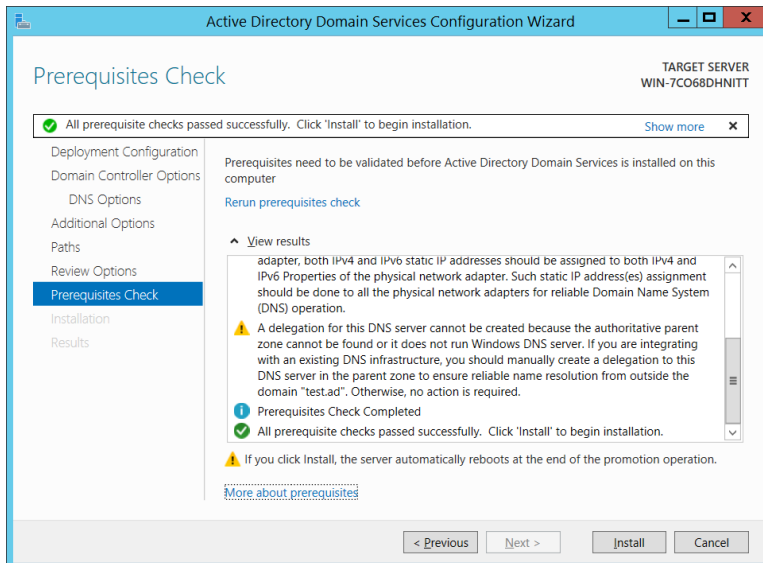
For a new AD DS installation, we should create a new forest, by creating the first domain in the forest (forest root domain).

- On the **Installation Progress** page, click the **Promote This Server to A Domain Controller** hyperlink.
- On the **Deployment Configuration** page, select the **Add a new forest** option > Type “test.ad” as shown below > Next.

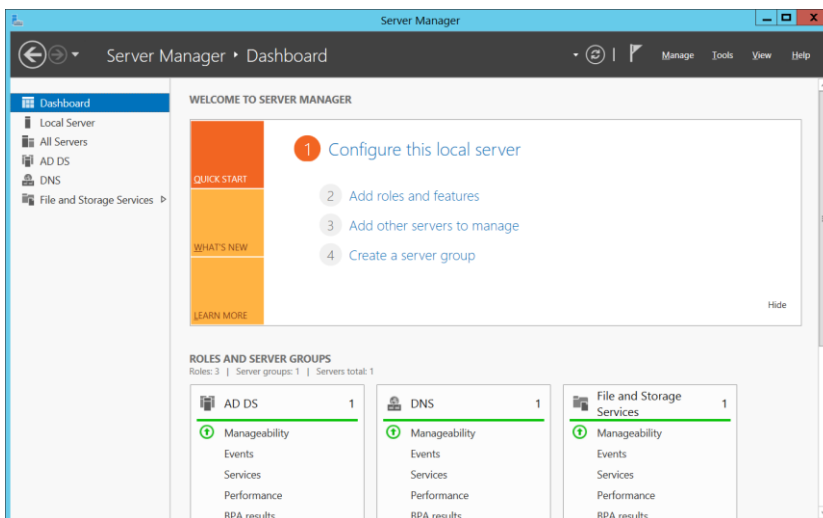


- On the **Domain Controller Options** page, type the password “WinOly@PC2018” for Directory Services Restore Mode (DSRM) > Next.
- We see a warning message about a delegation for the DNS server > Next.
- The **Additional Options** page shows the NetBIOS domain name which is equivalent of the domain name you specified > Next.

- On the **Paths** page, click Next.
- On the **Review Options** page, click Next.
- On the **Prerequisites Check** page, we see the wizard conducting a series of environment tests to evaluate whether the workstation can become a domain controller.
- You should see “**All prerequisites passed successfully**” > Install > A new forest is created and the server is configured to function as a domain controller.



- Restart the computer. When you need to change the password, make sure you change it systematically so that you can remember the new one. I recommend the following: “**WinOly@PC2019**”.



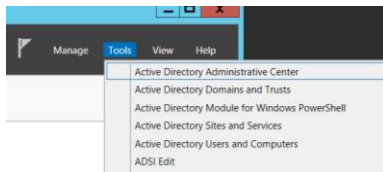
# Create and manage Active Directory groups and organizational units (OUs)

## Creating OUs

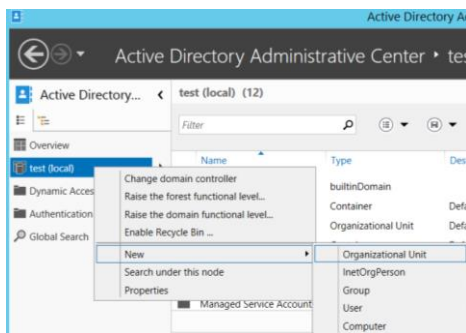
- FYI: How to delete an OU from Windows Server 2012 Domain Controller:

<https://www.manageengine.com/products/active-directory-audit/kb/how-to/how-to-delete-organizational-units-ous-in-active-directory-2012.html>

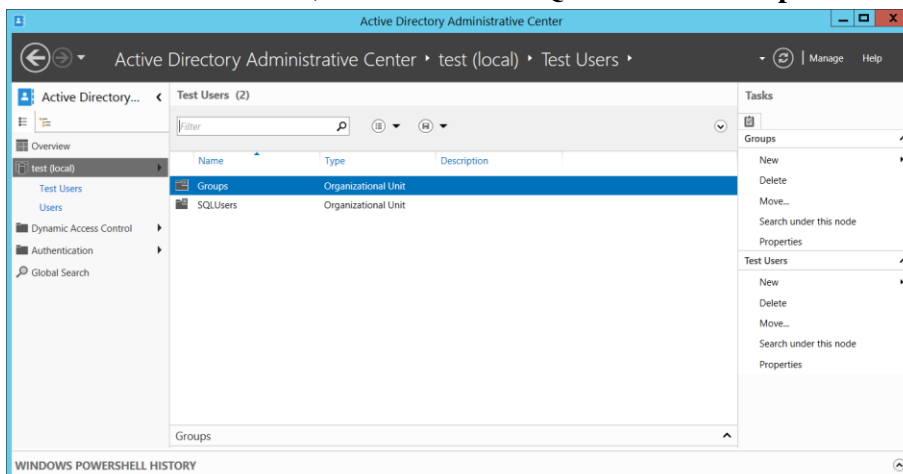
- In **Server Manager**, go to **Tools > Active Directory Administrative Center**.



- Right-click on **test (local) > New > Organizational Unit**.



- Create the Organizational Unit **“Test Users”**.
- Within the Test Users OU, create two OUs: **SQLUsers** and **Groups**.



## Creating Users

- Within the **SQLUsers** OU, create a user: **sqluser1**. When you create a new user, uncheck **“User must change password at next logon”**. For convenience, type the password **“Pa\$\$w0rd”**.

Create User: SQL User1

Account

Organization

Member Of

Password Settings

Profile

Policy

Silo

First name: SQL

Middle initials: User1

Last name: SQL User1

User UPN logon: @

User SamAccountName L: test \\* sqluser1

Password: \*\*\*\*\*

Confirm password: \*\*\*\*\*

Create in: OU=SQLUsers,OU=Test Users,DC=test,DC=ad [Change...](#)

☐ Protect from accidental deletion

Log on hours... Log on to...

Account expires: ☒ Never ☐ End of

Password options:

☐ User must change password at next log on

☒ Other password options

☐ Smart card is required for interactive log on

☐ Password never expires

☐ User cannot change password

Encryption options:

Other options:

Display name: SQL User1

Office:

E-mail:

Web page:

Job title:

Department:

Company:

Manager:

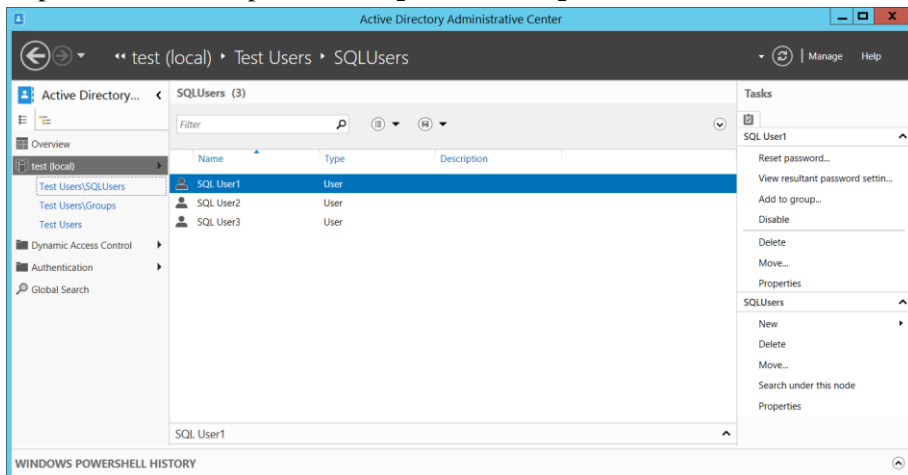
Direct reports:

[Other web pages...](#)

[More Information](#)

OK Cancel

- Repeat the above step to create **sqluser2** and **sqluser3**.



- Within the **Groups** OU, create a group (not user): **sqlgroup**. Accept the default for Group scope and Group type.

**Create Group: SQL Group**

**Group**

Group name: \* SQL Group

Group (SamAccountName): \* sqlgroup

Group type: ☒ Security ☐ Distribution

Group scope: ☐ Domain local ☒ Global ☐ Universal

☐ Protect from accidental deletion

E-mail:

Create in: OU=Groups, OU=Test Users, DC=test, DC=ad [Change...](#)

Description:

Notes:

**Managed By**

Managed by: [Edit...](#) [Clear](#)

☐ Manager can update membership list

Phone numbers: Main: Mobile: Fax:

Office:

Address: Street City State/Province Zip/Postal code Country/Region:

**Member Of**

[More Information](#) [OK](#) [Cancel](#)

- Click **Members** on the same screen, add **sqluser1** to the **sqlgroup** group. For this, click **Add...** on the Members screen. Type **sqluser1** in the box and click **Check Names**.

**Select Users, Contacts, Computers, Service Accounts, or Groups**

Select this object type: Users, Service Accounts, Groups, or Other objects [Object Types...](#)

From this location: test.ad [Locations...](#)

Enter the object names to select (examples): SQL User1 [Check Names](#)

[Advanced...](#) [OK](#) [Cancel](#)

- Go to **sqluser1** and add it to the group **Domain Admins**. If you do not add sqluser1 to Domain Admins, **sqluser1** cannot logon to this domain controller.

**Select Groups**

Select this object type: Groups or Built-in security principals [Object Types...](#)

From this location: test.ad [Locations...](#)

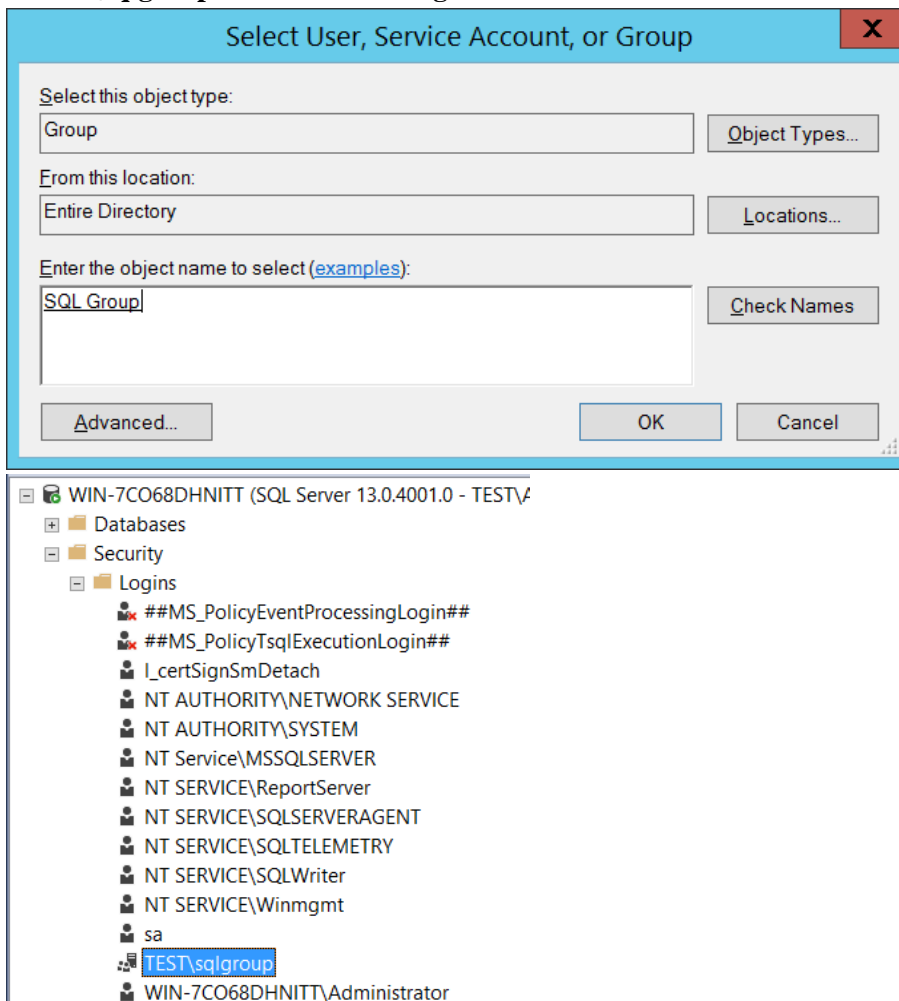
Enter the object names to select (examples): Domain Admins [Check Names](#)

[Advanced...](#) [OK](#) [Cancel](#)

- (**Task 1**) Show in a screenshot that the three domain users (sqluser1, sqluser2, sqluser3) are created in **SQLUsers** OU. Also show in a screenshot that **sqlgroup** is created in the **Groups** OU.
- (**Task 2**) Go to sqluser1 properties and show in a screenshot that sqluser1 is a member of **Domain Admins** and **sqlgroup**.

### Creating sqlgroup Login in SQL Server

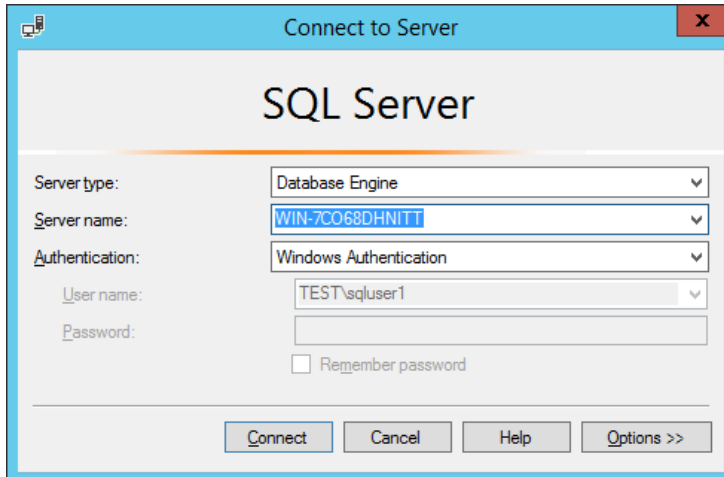
- Login to SQL Server with Windows Authentication.
- Go to **Security** > Right-click on **Logins** > **New Login...**
- On **Login – New** screen, click on **Search...** (located on the top-right)
- On **Select this object type** screen, click on **Object Types...** > Check **Groups** and uncheck the others.
- Enter **sqlgroup** in the box and click on **Check Names**. Save the setting and make sure “**TEST\sqlgroup**” is included in **Logins**.



- Exit the SQL Server.
- Log off Windows 2012 completely and log back on with **sqluser1** domain admin account. For this you should switch user on the Windows logon screen.



- Logon to SQL Server with Windows Authentication. You have to have Windows Authentication with the username “TEST\sqluser1”.



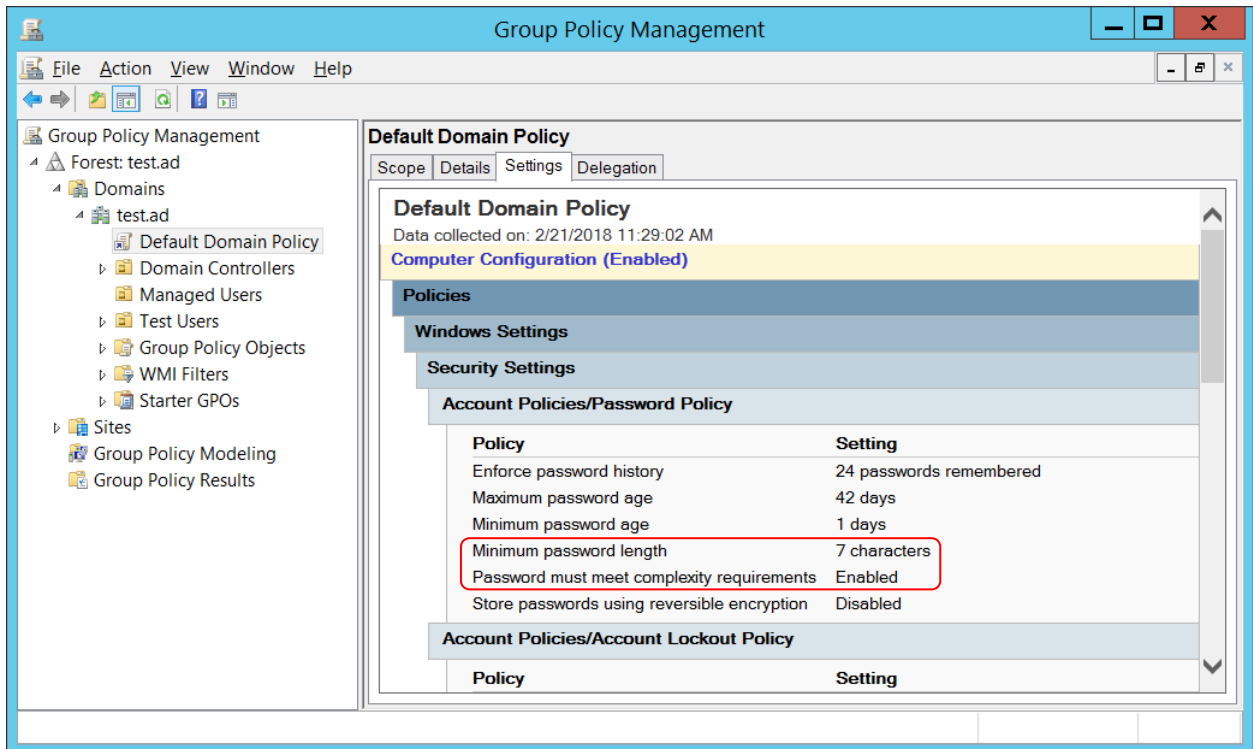
- (**Task 3**) Run the following query on SQL Server and show in a screenshot that you indeed logged-on with sqluser1.  

```
SELECT SUSER_NAME ( )
```
- Restart Windows 2012 Server with the **Administrator** (domain admin account).

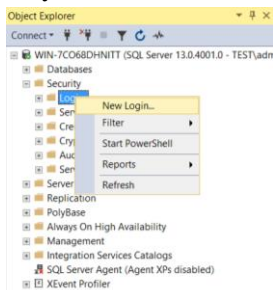
## Applying GPOs to SQL Server

- We are going to apply a GPO – password policy – to SQL Server.
- In Server Manager, go to **Tools > Group Policy Management > Forest > Domains > test.ad > Default Domain Policy**.
- On the right screen, click on **Settings**. Remember the two conditions **minimum password length** and **password complexity**.

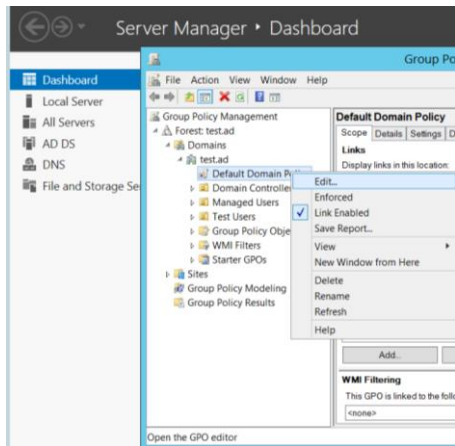




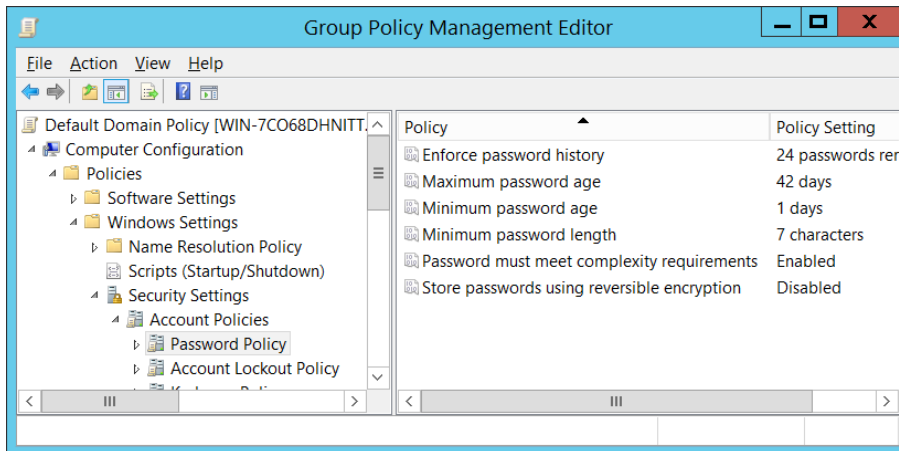
- **(Task 4)** Logon to SQL Server. Create a login “**Cardinal1**”. Select **SQL Server authentication**. Enter the password “1234567”, and show in a screenshot that the login cannot be created. Explain why?



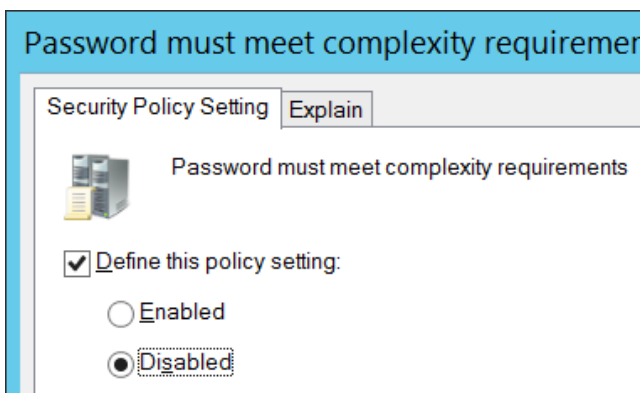
- Exit SQL Server.
- Go to Server Manager > Right-click **Default Domain Policy** > Click on **Edit...**



- You will see **Group Policy Management Editor**.
- Go to **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**.



- Disable the **password complexity requirement policy**.



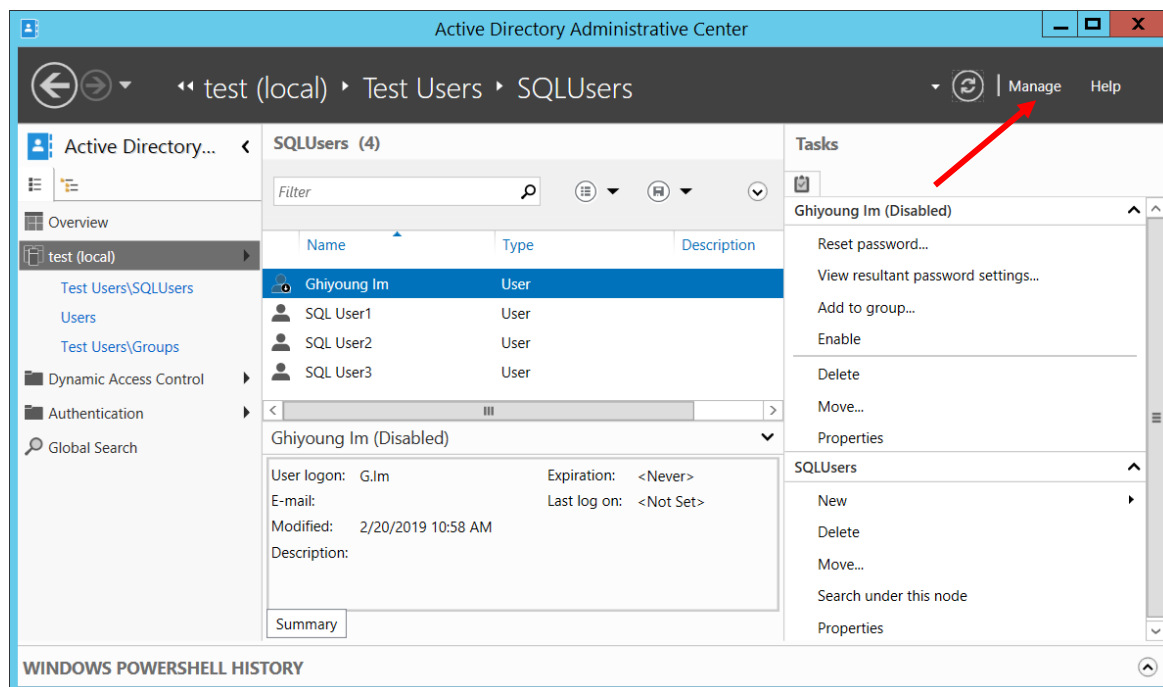
- Restart SQL Server.
- **(Task 5)** Create a login "**Cardinal2**". Select **SQL Server authentication**. Enter the password "1234567", and show in a screenshot that the login is created. Explain why this was possible. Explain also the relationship between the GPO and the SQL Server password policy.

- Delete the SQL Server **logins** you have created.
- Enable the **password complexity requirement policy**.
- Now you can add clients (e.g., Windows 7 workstations) to the domain.

## Creating a new AD user using PowerShell

- You are going to create a new AD user using PowerShell. First, you need to read the following document: *Netwrix Windows PowerShell Tutorial for Beginners.pdf*.
- **(Task 6)** Create a new AD account using the command **New-ADUser** explained on pp 12-13. Refresh after running the command. Show in a screenshot that the account is indeed created (example below). Also, attach a screenshot that displays the PowerShell execution.
- The account has the following attributes:
  - Name: *your full name*
  - Given Name: *your given name*
  - Surname: *your surname*
  - Account Name: *first\_initial.last\_name* (e.g., G.Im)
  - User Principal Name: *first\_initial.last\_name@test.ad* (e.g., *G.Im@test.ad*)
  - Path: *OU=SQLUsers,OU=Test Users,DC=test,DC=ad*

When you run the command, make sure you place the entire command in one single line.



**FOLKS, GREAT JOB!! YOU DID IT!!**

