**Active Directory Domain Project**

Steps:

1. I installed Windows Server 2025 on one VM in VMWare Workstation, which acted as the Domain Controller for the network. I created 2 additional VMs to be members of the domain using Windows Education.
2. I configured a static IP address on the Windows Server (192.168.171.10/24). I used VMWare’s default gateway for the network and assigned the DNS server as the loopback for the server, 127.0.0.1. I changed the hostname of the **Windows Server to DC1 (Domain Controller1).**
3. I installed Active Directory, DHCP and DNS services on DC1. I named the **domain “mydomain**”. I configured a DHCP pool in the 192.168.171.150-192.168.171.254/24 network.
4. I changed the **hostname of the VM running Windows Education to FileServer**. I then configured FileServer to use DHCP to receive its IP address configuration. I pinged the Domain Controller (DC1) to ensure that I had network connectivity. I then added the FileServer computer to be a member of “mydomain”.
5. I configured the second domain member to use DHCP, named it **PC1,** and added it to be a member of “mydomain”.
6. In the Active Directory Users and Groups management tool, I created an Organizational Unit under the main domain named “MainOffice”. Then, I created 2 more OUs under “MainOffice” to hold the users and computers, named “MainUsers” and “MainComputers”.
7. I wrote a Powershell script “new\_users.ps”, that would create 3 security groups, “NetworkAdmins”, “NetworkShare”, and “Employees”. First, I created user accounts in Active Directory and placed them in the “MainUsers” OU by pulling from a CSV file with employee information. I created a network share on the FileServer VM with the path “[\\FileServer\NetworkShare](file:///\\FileServer\NetworkShare)” and gave the “NetworkShare” group full access to it. Also, I moved PC1 and FileServer to the “MainComputers” OU. Lastly, I created roaming profiles for all the users.
8. Next, I created Group Policies to restrict software downloads, create a warning logon banner, install 7zip for all users on the network share, create a custom password policy, and configure firewall rules.
9. I configured the password policy to have a password history of 5, age of 42 days, and minimum length of 9 characters. I configured an account lockout policy that would lock users out of their account after 5 incorrect attempts for 10 minutes. I configured a software restriction policy that would apply to all software, restrict all users including administrators and enforce certificate rules. I created a firewall GPO that would block inbound traffic by default unless it met the rules. I restricted both inbound and outbound traffic on unsecure ports 21, 23, 25, 80, 110 and 389 to block FTP, Telnet, SMTP, HTTP, POP3, and RDP traffic.

The firewall, logon banner, password, and software restriction GPOs were Computer Configuration GPOs applied to the MainComputers OU, while the 7zip GPO that installed the application on the network share was a User Configuration GPO that was applied to the MainUsers OU.

1. To verify the users, security groups, and GPOs were created, I wrote another PowerShell script named “validate\_AD.ps” that displayed the output of the AD users, security groups and GPOs that I created. I created a CSV file with the output of the details of the GPOs I created. I then imported the CSV file into Excel and made a table that listed the details of the GPOs.

**The Group Policies I created in “mydomain”**

A screenshot of a computer

AI-generated content may be incorrect.

**The OUs, security groups and users I created in “mydomain”**

A screenshot of a computer

AI-generated content may be incorrect.

**The output of the “validate\_AD.ps” script showing the users, computers, and groups in “mydomain”**

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.