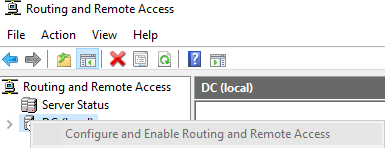
**Windows Server Setup:**

Using VirtualBox, I created the VM that will act as the domain controller as a Windows Server 2022 machine. In the VM settings, you have to add a second Network Adapter that is attached to an Internal Network, which will act as an organization’s internal network. After launching the machine, I then navigate to the Network and Sharing Center in the Control Panel, and click the “change adapter settings”. Determine which is the “External” connection and which is the “Internal” by viewing the status of each. One will have an IP address assigned via APIPA, which is the internal network’s connection, and the other has connections to the router. Assign a static IP so that all clients within the internal network will always be able to find the Domain Controller. Since Active Directory automatically installs DNS, the loopback address can be assigned as the DNS.

**AD Setup:**

In Server Manager, add AD Domain Services through the Add Roles and Features selection. Afterwards, the Server Manager prompts the administrator to promote the machine to the domain controller. In the deployment wizard, since this is a new lab, I added a new forest, and gave the root domain name “mydomain.com”.

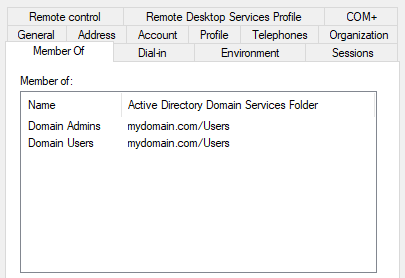
I next added Remote Access as a feature, additionally adding the Routing feature. This is done to map the internal clients’ IP addresses to the public address, so that each client can access the internet under one public IP address. Navigate to the Routing and Remote Access tool, configure the NAT on the local domain controller, and choose the external network adapter.



Finally, I added the DHCP feature, so that clients can get an IP address for the internal network. Once finished, you must navigate to the DHCP button under “Tools”, and authorize and refresh the server.

**“Organization” Setup:**

My next step is to create an administrator account, which is done through the tool “Active Directory users and computers”. Right click the domain and add a new organizational unit for the administrator accounts. After creating the user, make them a member of “Domain Admins” by editing the user’s properties.



I then logged into the admin account to make sure it was set up properly. I ran a powershell script that grabs randomized names from a .txt file and makes them into user accounts in the domain.

Finally, I need a Client machine to simulate having another computer connected to the organization’s network. Similar to the setup of the Windows Server 2022 machine, I set up a Windows 10 Pro machine. Since it is connected to the internal network already, the next step is to navigate to Settings -> System -> About -> Rename this PC (advanced), and access the change button to change both the computer name as well as the domain/workgroup. After typing mydomain.com into the domain textbox, it prompts for a domain administrator’s credentials, and can now be used by any domain user.

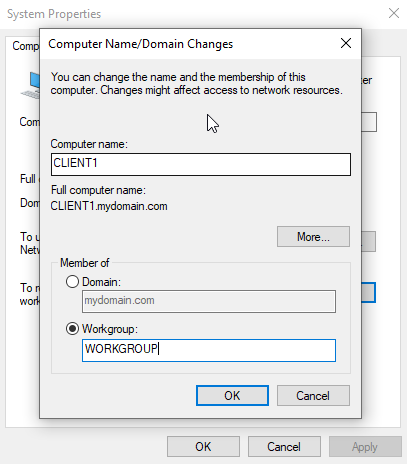
**User lockouts and password resets:**

To disable an account, navigate to Active Directory Users and Computers, find them within their OU, right click, and choose the “Disable Account” option.

To change a password, you can right click the user and choose the “Reset Password” option. Here, it allows you to give a new password to the user, as well as make them change it on their next login. This is the method I chose, because if a user forgot their password, the administrator could set and send them the temporary password, and having the user change it at next login ensures only the user themselves will know the password.

**Removing client from the domain:**

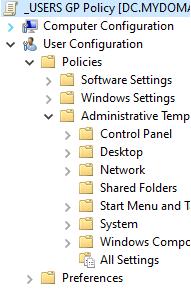
To remove a client from the Active Directory, on the client computer, go to Settings -> System -> About -> Rename this PC (advanced). Click the Change button, and change from the domain to a workgroup, and type in “WORKGROUP”.



After a restart, the computer is effectively disconnected from the domain, and no accounts from the domain can log in to the computer. Due to the connection of the virtual machine environment, the DNS and DHCP stay connected. In a real situation, these should be disconnected when the client is no longer within range of the network, and change once connected to another network. I confirmed this by changing the name of the virtual machine’s internal network adapter, as well as changing the adapter to NAT, which connects the machine to my home network. For practice, I changed the DNS server of the client to Google’s DNS (8.8.8.8). After doing this, I could no longer run the command >ping DC.mydomain.com, however the command >ping DC still pinged the virtual machine of the domain controller.

**Group Policy:**

Within the Group Policy Management tool, I right clicked the Organizational Unit to add the policy in, and created and linked the GPO. I then edited the policy and navigated under User Configuration, and changed basic settings within the Administrative Templates folder, like removing access to windows update, not allowing the store app on the taskbar, and hiding items on the desktop.



After running the command gpupdate /force in the command prompt, and relogging in as a user, the changes were in effect.