Lab Report - Lab 5

Name: Tyler Burleson Date: 2/19/2024

Summary

We started our lab by RDP'ing into our Windows server named FluxWinDC01. This server is going to be our domain controller. Once we were connected to the machine, we navigated to the Advanced System Properties. Here we modified our machine's name to FluxWinDC01. Once this was complete, we repeated the same process with our FluxWinMS01 server. We then moved into the Active Directory piece of our lab.

We started by installing AD onto our domain controller server. Once this was installed, we promoted our server to officially be a domain controller. We then had to set up our DNS role by using the provided wizard. Once AD DS was installed and our instance was promoted, we needed to add a domain administrator to our system. We did this by launching server manager and accessing the AD users and computers. We clicked on the users file and added Bob Smith as a new user with "bsmith" in his email field. Next, we set his password to be Passw0rd! and for it to never expire. Once he was added to our system, we navigated to his accounts properties and added him to our Domain Admins group. Next, we set Domain Admins as our primary group and repeated these same steps for Alice Goodall. After we created these accounts were created, we needed to manage our administrator account so we wouldn't be locked out of our DC a month from now. We did this by navigating to the administrator properties and the account tab. We then unlocked the account and set the password to never expire.

After changing the administrator properties, we needed to RDP into our member server. Once we were in we navigated to the network adapter properties and added a private IP. This private IP connected our member server to our domain controller so we can use the DC for DNS lookups. Once this was done, we used the "nslookup" command in PowerShell to confirm our MS was reaching our DC. We then used a PowerShell command to add our DC to the Domain and restarted the machine. Once this was complete,

we connected back to our DC and ensured Bob's account had the desired privileges we gave it. Finally, we tested our DNS by RDP'ing from the DC server into the MS server through PowerShell with fluxwinms01.flux.loc as the computer name. Once this was confirmed to work we were finished with the lab.

Screen Shots

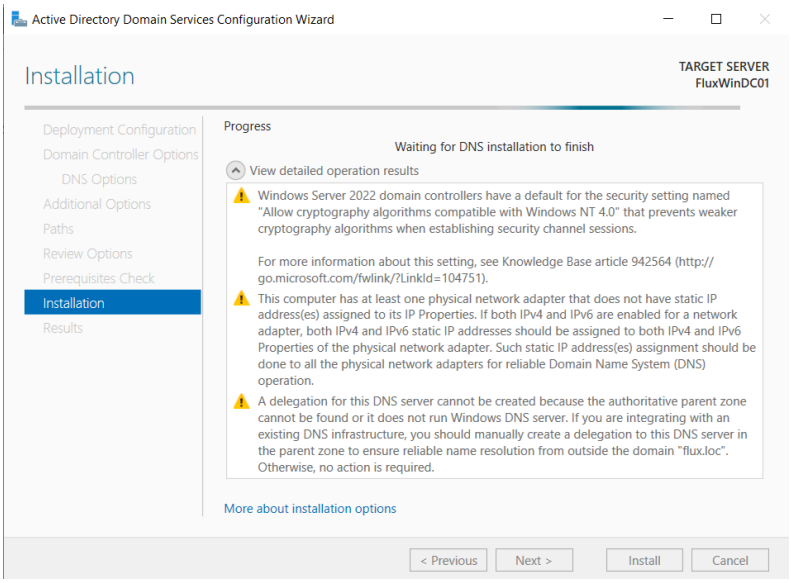

Figure 1

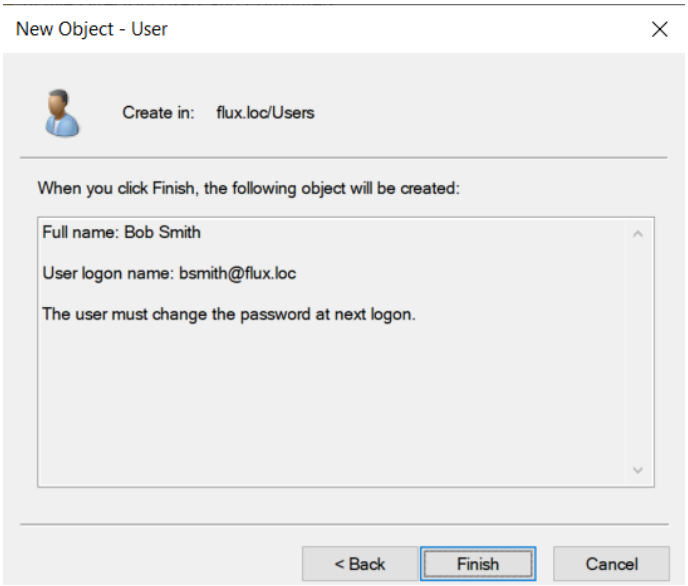

Figure 2

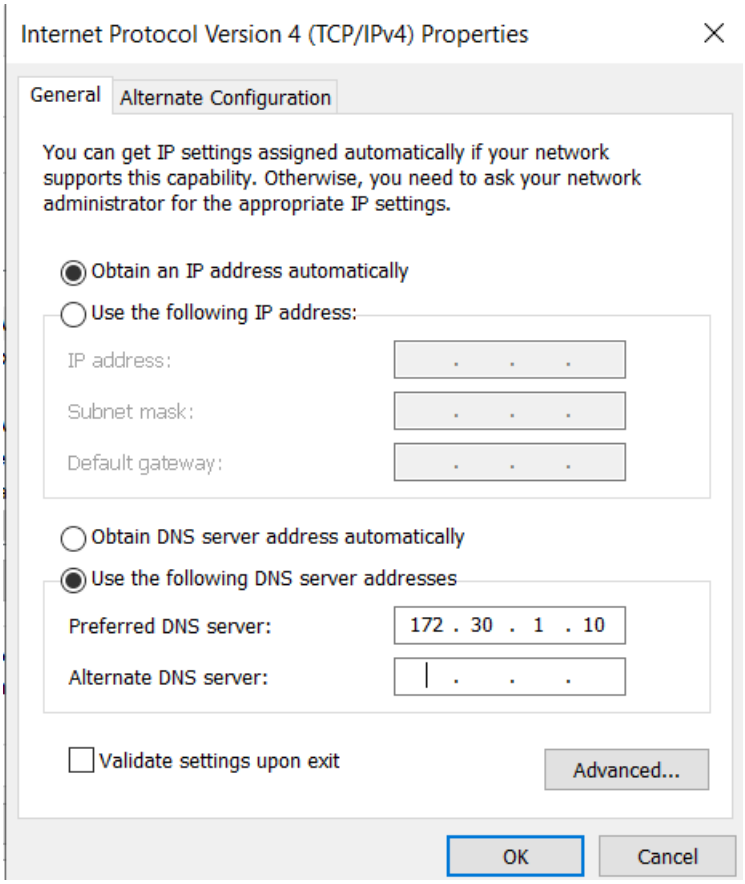

Figure 3

```
PS C:\Users\Administrator> nslookup flux.loc
Server:  ip-172-30-1-10.ec2.internal
Address:  172.30.1.10

Name:    flux.loc
Address:  172.30.1.10

PS C:\Users\Administrator>
```

Figure 4

```
PS C:\Windows\system32> ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be report
ed in the Event Viewer in 15 minutes.
PS C:\Windows\system32>
```

Figure 5

Research Questions

1. What is Active Directory Domain Controller?
   Servers that have the AD DS server role installed; this is used to authenticate users.
2. What is a Domain in Active Directory?
   A domain provides a partition to house objects in an AD.
3. In Active Directory, what is the schema?
   Defines objects and the information pertaining to those objects that can be stored in Active Directory.
4. What is the Global Catalog? What does it do?
   Global Catalog stores information about every object within forest. It is also used for authentication, Forest-wide searches, replication of key AD elements, and keeps a copy of the most used attributes.
5. When we promoted the domain controller, one of the wizard windows asked for the location of the SYSVOL folder. We left the default folder C:\Windows\SYSVOL. What is the SYSVOL folder and what does it do?
   It provides a default location for files that are replicated throughout the domain.
6. What is LDAP?
   Lightweight directory access protocol | This protocol maintains and accesses services within a network.
7. Briefly explain how Active Directory authentication works
   The client starts by requesting an authentication ticket from the AD server. The server then sends a ticket to the client. The client then sends that ticket to the endpoint server. Finally, the server returns an acknowledgement of authentication to the client.
8. What is Kerberos?
   Kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network.
9. What are the components of Active Directory?
   The main components are Forest, Trees, Domains, OU's, and sites.
10. What is the difference between domain admin groups and enterprise admins group in AD?
    The enterprise group is in the root domain of the forest while domain admins have full control of the root domain.