

CS 240W - Lab 3 - Active Directory

Name: _____

Topic: Introduction to Active Directory (AD) and Setting Up a Virtual Server as an Active Directory Domain Controller

Total Points: 25

Section 1: Active Directory Basics (5 Points) (Be sure to do the reading for the week)

Imagine you are an IT Administrator for a small company, and your manager has asked you to explain Active Directory and its potential threats. Write a short (200-300 words) email explaining:

- What Active Directory is and how it helps the company manage users and resources.
- The risks and threats to Active Directory, and why they should be addressed.
- A brief mention of steps the company can take to improve security.

Ans:

Active Directory is a database containing information about all users on a network and what services they are allowed to access. Since AD is the keeper of all permissions, it provides threat actors a valuable target for gaining access to a company's data. One could attack AD and, perhaps, slowly gain greater permissions to services on the network. To improve security, companies should focus on enforcing best security practices (like using strong passwords, installing security updates, and configuring permissions properly), conducting regular audits of the AD environment, training staff, and using new technologies (like Machine Learning) to analyze potentially harmful behavior on the network.

Section 2: Create NAT Network /Static IP (3 Points)

We are going to end up creating other virtual machines to add to our network. To do this we'll need a NAT Network.

- If using Oracle VirtualBox
 - Files > Tools > Network
 - Setup a NAT Network
- Update your Server to that Network.
 - Select your Server
 - Select Settings
 - Select Network

- Select NAT Network created above.
- Boot up your Server and switch to Static IP
 - Open Network & Internet Settings
 - Change Adapter Settings
 - Select your network
 - Properties
 - Edit IPv4 and create Static

The screenshot shows the Windows Server Manager interface. The top navigation bar includes File, Machine, View, Input, Devices, Help, and a Server Manager icon. Below the navigation bar, the title bar says "Server Manager > Dashboard". On the left, there's a sidebar with "Dashboard" selected, "Local Server", and "All" (Administrator: Windows PowerShell). The main content area displays a PowerShell session output:

```

ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1

Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

Host Name . . . . . : McLainServer
Primary Dns Suffix . . . . . : mcclainc.lab3
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : mcclainc.lab3

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address . . . . . : 08-00-27-B9-E4-DC
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::701c:e76c:a80d:d7d7%9(PREFERRED)
IPv4 Address. . . . . : 10.0.2.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.1
DHCPv6 IAID . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-12-0B-A9-08-00-27-B9-E4-DC
DNS Servers . . . . . : 1.1.1.1
NetBIOS over Tcpip. . . . . : Enabled

PS C:\Users\Administrator>

```

- **Section 3: Setting Up an Active Directory Domain Controller (10 Points)**

Objective: Set up a Windows Server as a Domain Controller with Active Directory installed and configured.

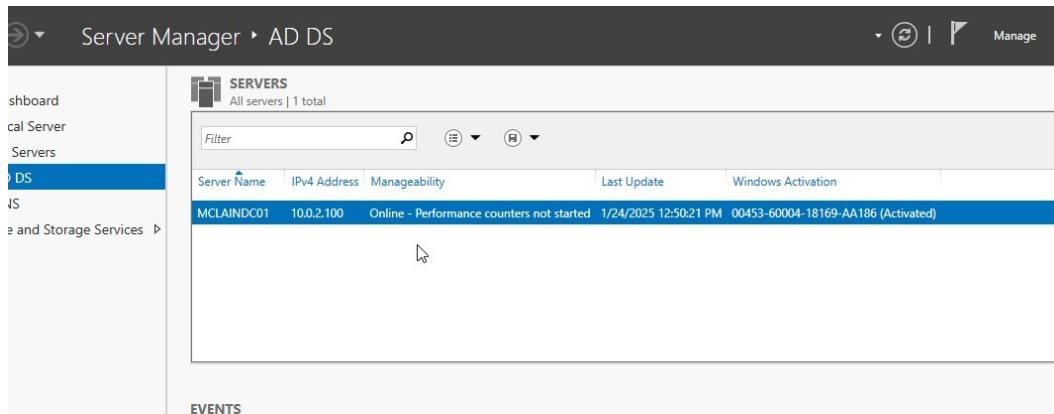
Lab Environment:

- You will use your virtual server from Lab2.
- I suggest you clone your server for future weeks when we create a non-AD server. (If you have the hard drive space).

Instructions:

1. Initial Configuration:

- o Set up the server's hostname to reflect its role, add to the end of your last name, DC01. (Example: GoudreauDC01)



2. Install Active Directory Role:

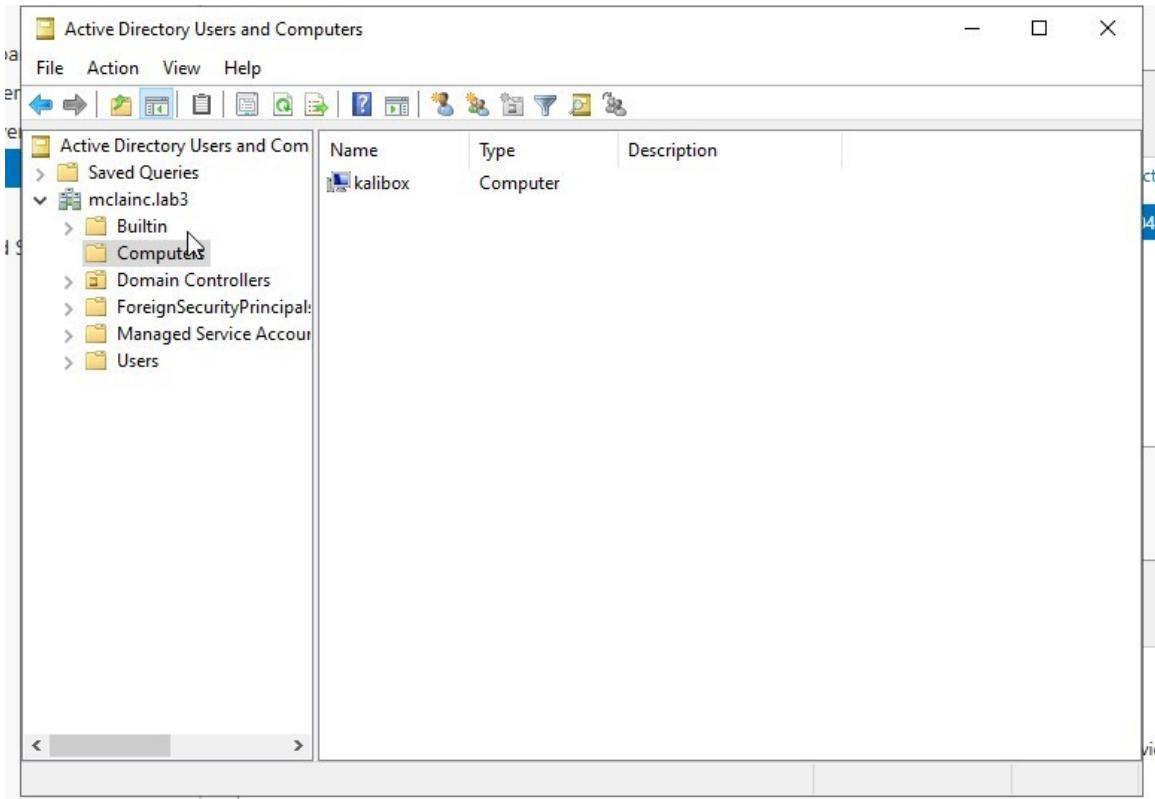
- o Add the "Active Directory Domain Services" role using Server Manager.

3. Promote the Server to a Domain Controller:

- o Create a new domain with your last name. (e.g., YourLastName.lab).

4. Verify Active Directory Installation:

- o Open the "Active Directory Users and Computers" console and confirm the domain is listed.
- o Open Computers and show there are no computers on your Domain.



Note: Should show your domain name and no computers listed.

NOTE: Please forgive me, I didn't notice this was supposed to be empty until after reading the assignment. This computer is a Linux machine I added.

Section 4: Create a new Windows 11 VM (5 Points)

Using the Education license from Azure. Create a Windows VM. Use the best options for your environment for this VM.

- o Ensure that your VM is on the same NAT Network as your server.
- o Change your DNS to your Server.
- o Open a Command Prompt window and ping the domain you created above: Yourlastname.lab

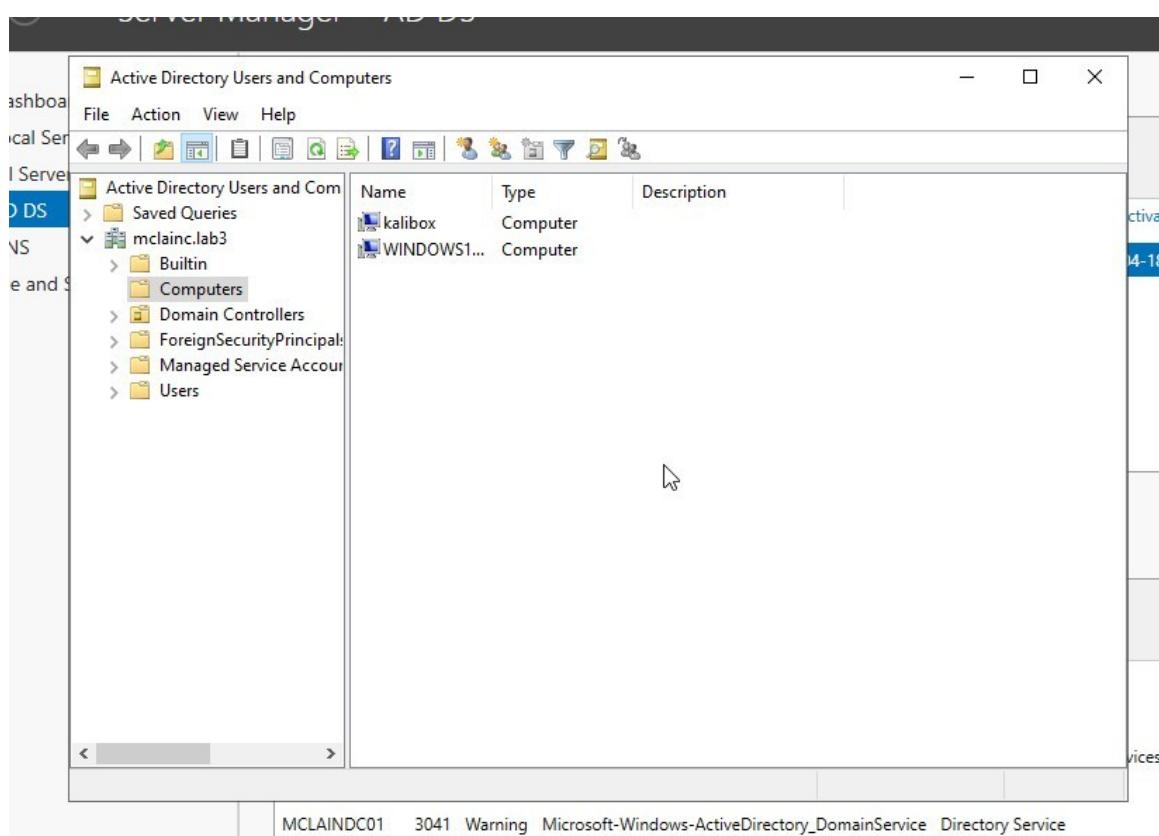
```
Administrator: Windows PowerShell
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : lanecc.edu
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-3E-34-85
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::cccd1:8079:2ad3:4e7a%14(Preferred)
IPv4 Address. . . . . : 10.0.2.7(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, January 24, 2025 12:51:52 PM
Lease Expires . . . . . : Friday, January 24, 2025 1:01:52 PM
Default Gateway . . . . . : 10.0.2.1
DHCP Server . . . . . : 10.0.2.3
DHCPv6 IAID . . . . . : 84410407
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-25-AB-14-08-00-27-3E-34-85
DNS Servers . . . . . : 10.0.2.100
NetBIOS over Tcpip. . . . . : Enabled
PS C:\WINDOWS\system32> ping mclainc.lab3

Pinging mclainc.lab3 [10.0.2.100] with 32 bytes of data:
Reply from 10.0.2.100: bytes=32 time<1ms TTL=128
Reply from 10.0.2.100: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.2.100:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
PS C:\WINDOWS\system32>
```

- o Change the Domain of your Windows 11 machine to be on your Domain.
 - o Note: This will require your Admin username and password from your domain server.
 - o Note2: You will need to reboot for the changes to take effect.
- o On your Windows 2022 Server should show that your pc is now a computer on the network.



Note: Should show your domain name and your new computer listed.

Section 5: Turn into Moodle (2 points)

Save the completed document as a PDF. Name it as Lab1_YourlastnameFirstInitial.pdf. Be sure to have your name on the top line in this document. Upload to Moodle.