Active Directory & DNS Configuration for Network Management

By: Michael Emil Santos

Introduction:

This project demonstrates the setup and configuration of Windows Server 2016 as an Active Directory (AD) and DNS server, with a Windows 10 workstation joined to the domain. This setup centralizes network management, ensuring secure user authentication and streamlined access to network resources.

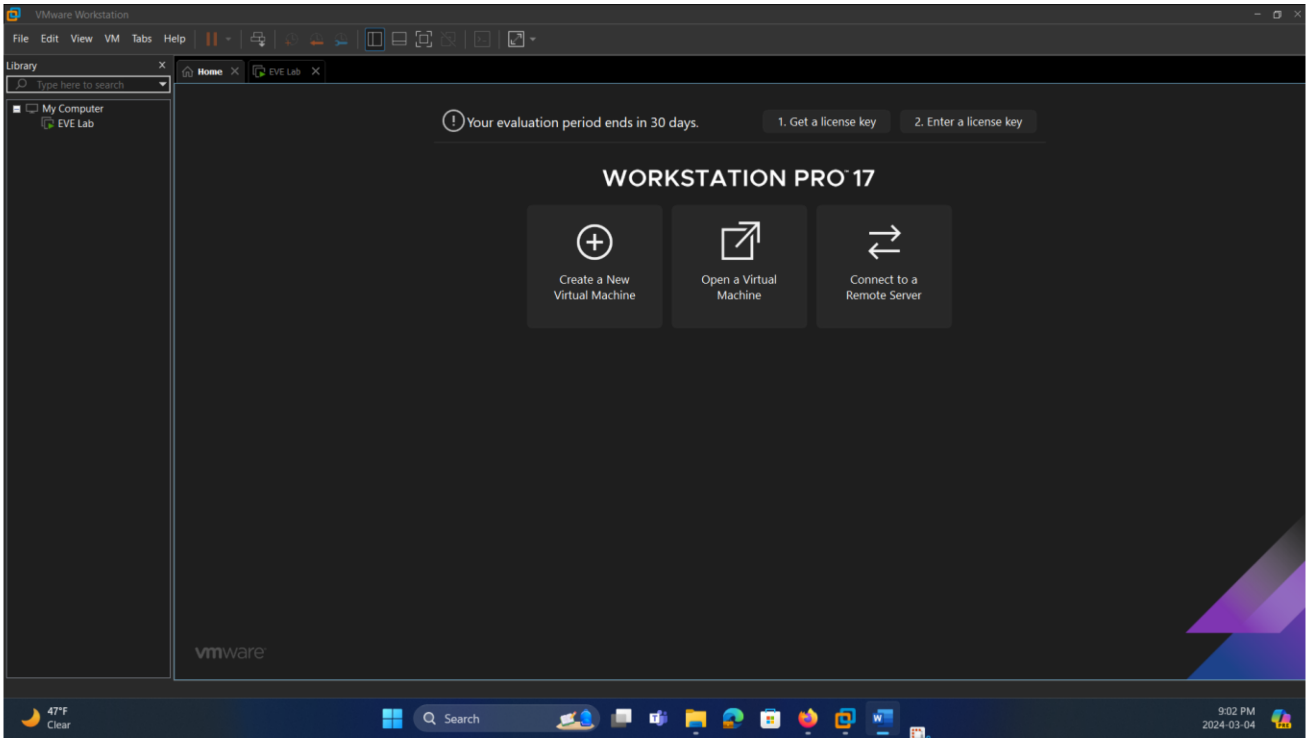
Objectives:

In this lab the procedure of installing and configuring Windows server 2016 as an Active directory is applied. To configure the server as an AD and install another node as a workstation (Windows 10Pro); which will be connected to the server. The following are the main objectives of this lab:

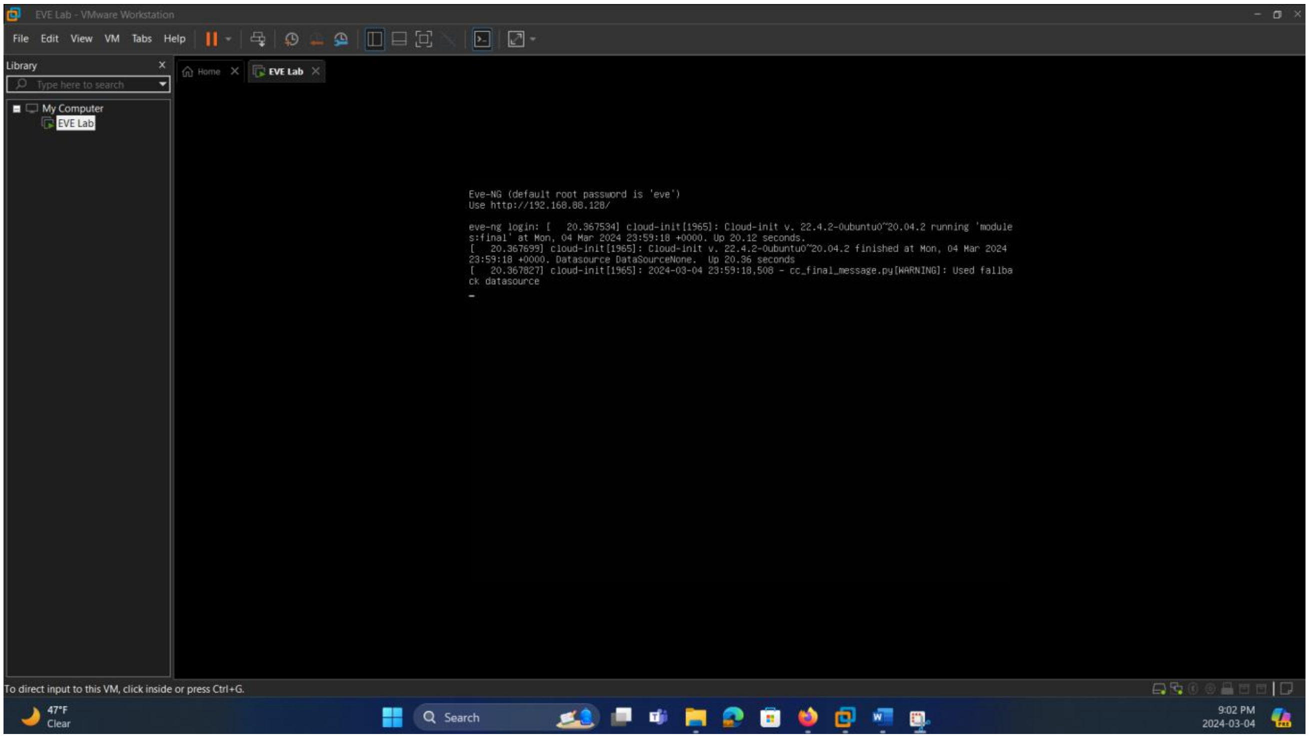
- Configure windows server 2016 as Active Directory and DNS
- Create a user under Active Directory
- Add Windows 10 to the domain
- Login using a domain account

Installation and Setup:

1. **Installation of VMWare Workstation Pro and EVE-NG for Creation of AD & DNS Lab Scenario**

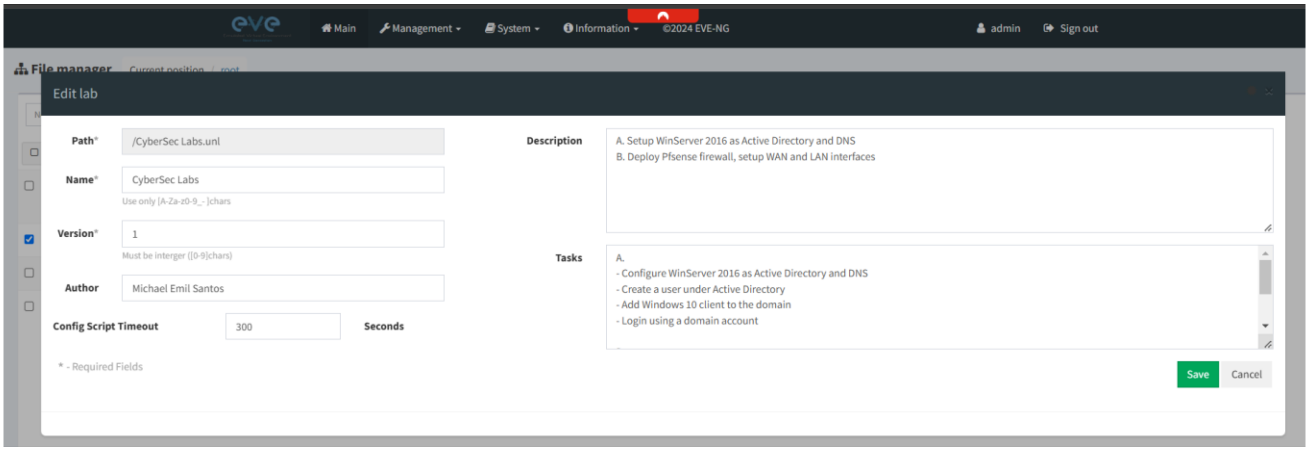


Your evaluation period ends in 30 days.


EVE Lab - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
EVE Lab
Home
EVE Lab
To direct input to this VM, click inside or press Ctrl+G.
47°F
Clear
Search
9:02 PM
2024-03-04

```
Eve-NG (default root password is 'eve')
Use http://192.168.88.128/

eve-ng login: [   20.367534] cloud-init[1965]: Cloud-init v. 22.4.2-0ubuntu0~20.04.2 running 'module
s:final' at Mon, 04 Mar 2024 23:59:18 +0000. Up 20.12 seconds.
[   20.367699] cloud-init[1965]: Cloud-init v. 22.4.2-0ubuntu0~20.04.2 finished at Mon, 04 Mar 2024
23:59:18 +0000. Datasource DataSourceNone.  Up 20.36 seconds
[   20.367827] cloud-init[1965]: 2024-03-04 23:59:18,508 - cc_final_message.py[WARNING]: Used fallba
ck datasource
_
```

This screenshot showcases the initial interface of VMware Workstation Pro 17, which is the platform used to host EVE-NG, a network emulator that allows the creation and configuration of virtual lab environments. Also, displayed is the console output of EVE-NG after its initial boot within VMware Workstation Pro. The screen provides essential information such as the default root password ('eve') and the URL to access the EVE-NG web interface (`http://192.168.88.128`). This console is crucial for initial setup and configuration tasks.



Edit lab

Path* /CyberSec Labs.unl

Name* CyberSec Labs
Use only [A-Za-z0-9_-]chars

Version* 1
Must be interger ([0-9]chars)

Author Michael Emil Santos

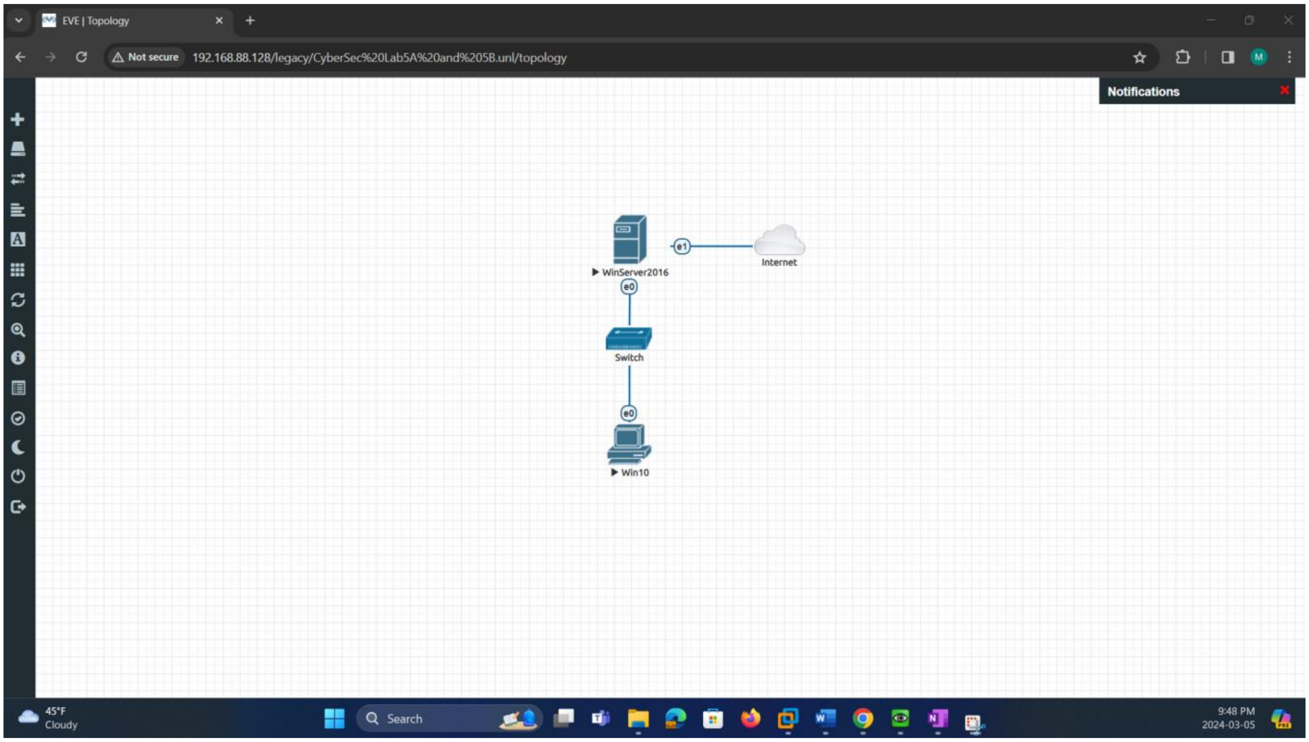
Config Script Timeout 300 Seconds

Description
A. Setup WinServer 2016 as Active Directory and DNS
B. Deploy Pfsense firewall, setup WAN and LAN interfaces

Tasks
A.
- Configure WinServer 2016 as Active Directory and DNS
- Create a user under Active Directory
- Add Windows 10 client to the domain
- Login using a domain account

* - Required Fields

Here we can see the EVE-NG web interface with the lab details outlined. This web-based topology viewer is where the network scenario for the AD & DNS lab is configured and managed. The left pane details the lab ID and lists the key steps for setting up Windows Server 2016 as an Active Directory and DNS, which are critical components of the lab.

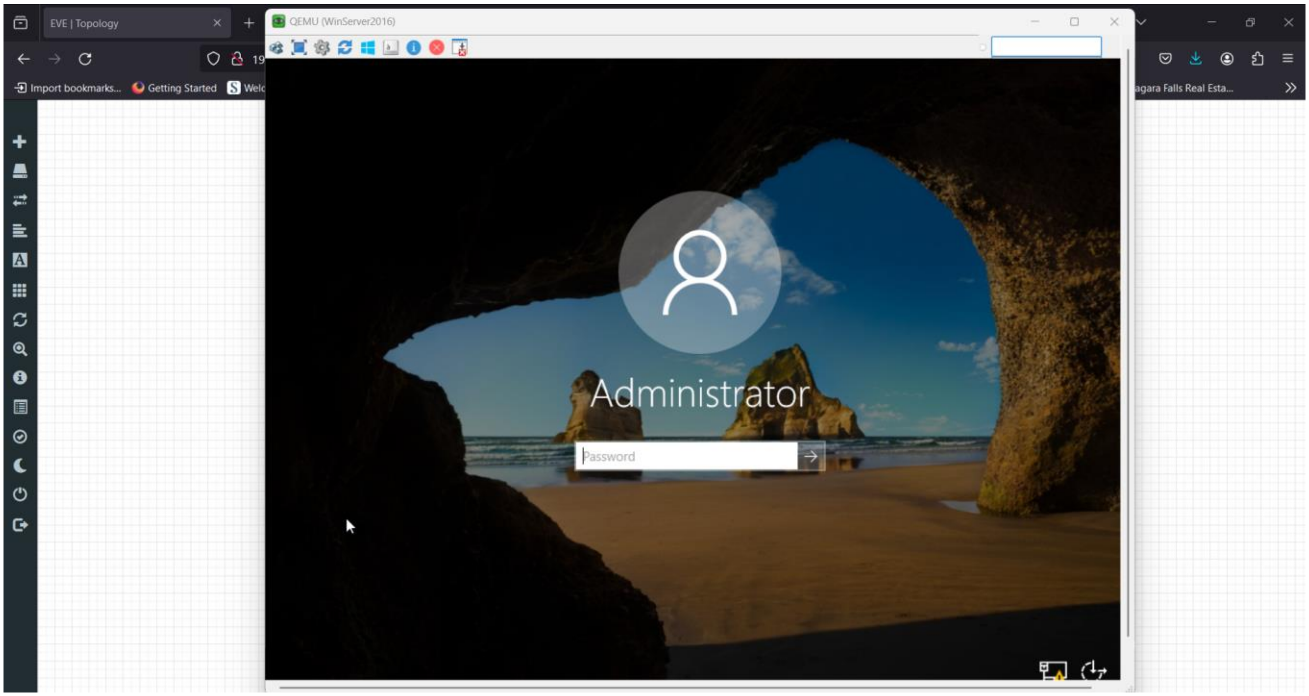


This screenshot shows the EVE-NG network topology window with a basic setup for a lab environment. In this topology:

- **WinServer2016**: The Windows Server 2016 virtual machine, which is typically used as a Domain Controller in Active Directory setups and can also serve as a DNS server. It is connected to the "Internet" cloud node, which suggests it has external network access, possibly for internet connectivity or updates.
- **Switch**: This represents a virtual switch that provides network connectivity within the virtual lab environment. It acts as a central point to which other virtual devices connect and can communicate.
- **Win10**: The Windows 10 virtual machine, serving as a client within the Active Directory domain. It is connected to the switch, indicating it's on the same local network as the Windows Server 2016 VM.
- **Internet Cloud**: The cloud icon named "Internet" typically represents a node that provides NAT (Network Address Translation) services, allowing the connected devices to access external networks including the internet.

The configuration indicates a straightforward network where the Windows Server 2016 VM can communicate with the Windows 10 VM and reach outside networks. This setup is suitable for testing AD DS and DNS functionalities, where the server needs internet access, and the client requires local network connectivity to the server.

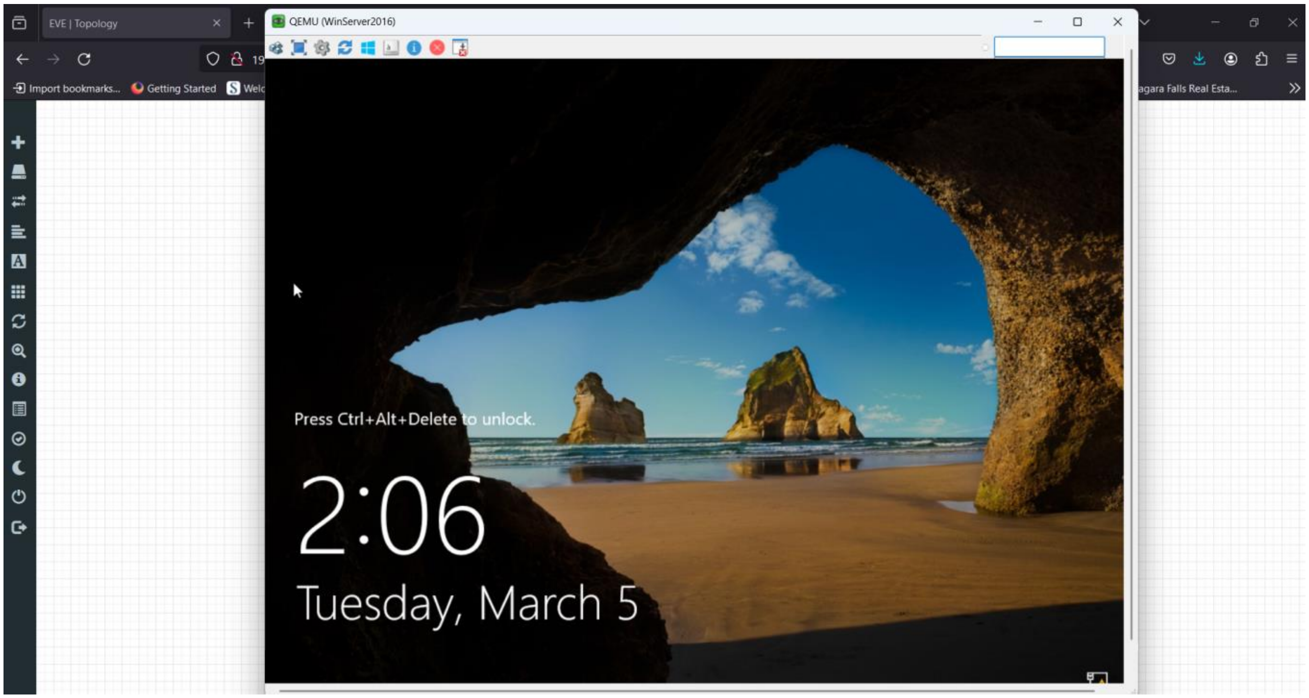
2. Installation and Configuration of WinServer 2016 as Active Directory and DNS Server



Administrator

Password

Shown here is the lock screen of the Windows Server 2016 VM, captured just before the login process. This stage precedes administrative access, which is necessary for the setup and management of server roles and features.

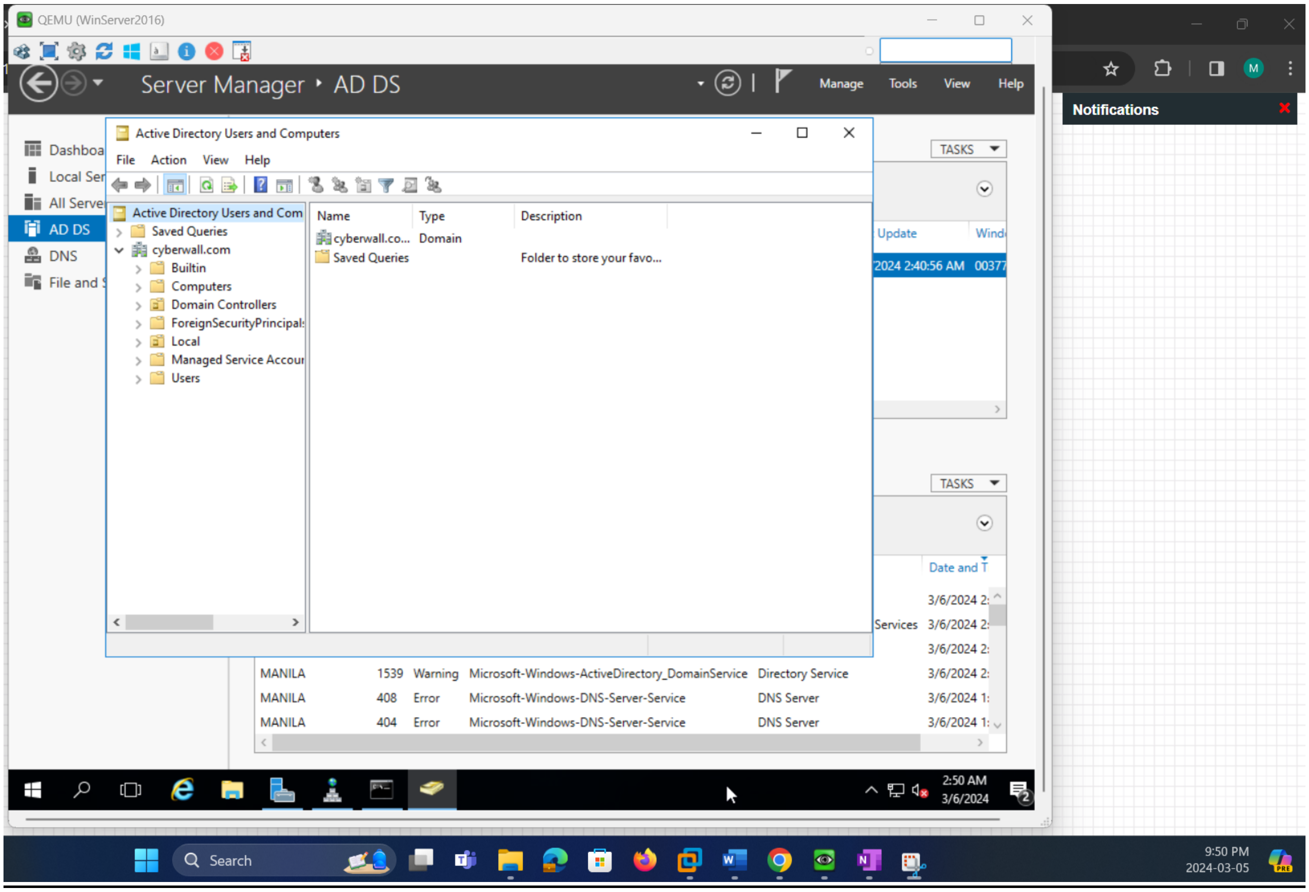


Press Ctrl+Alt+Delete to unlock.

2:06

Tuesday, March 5

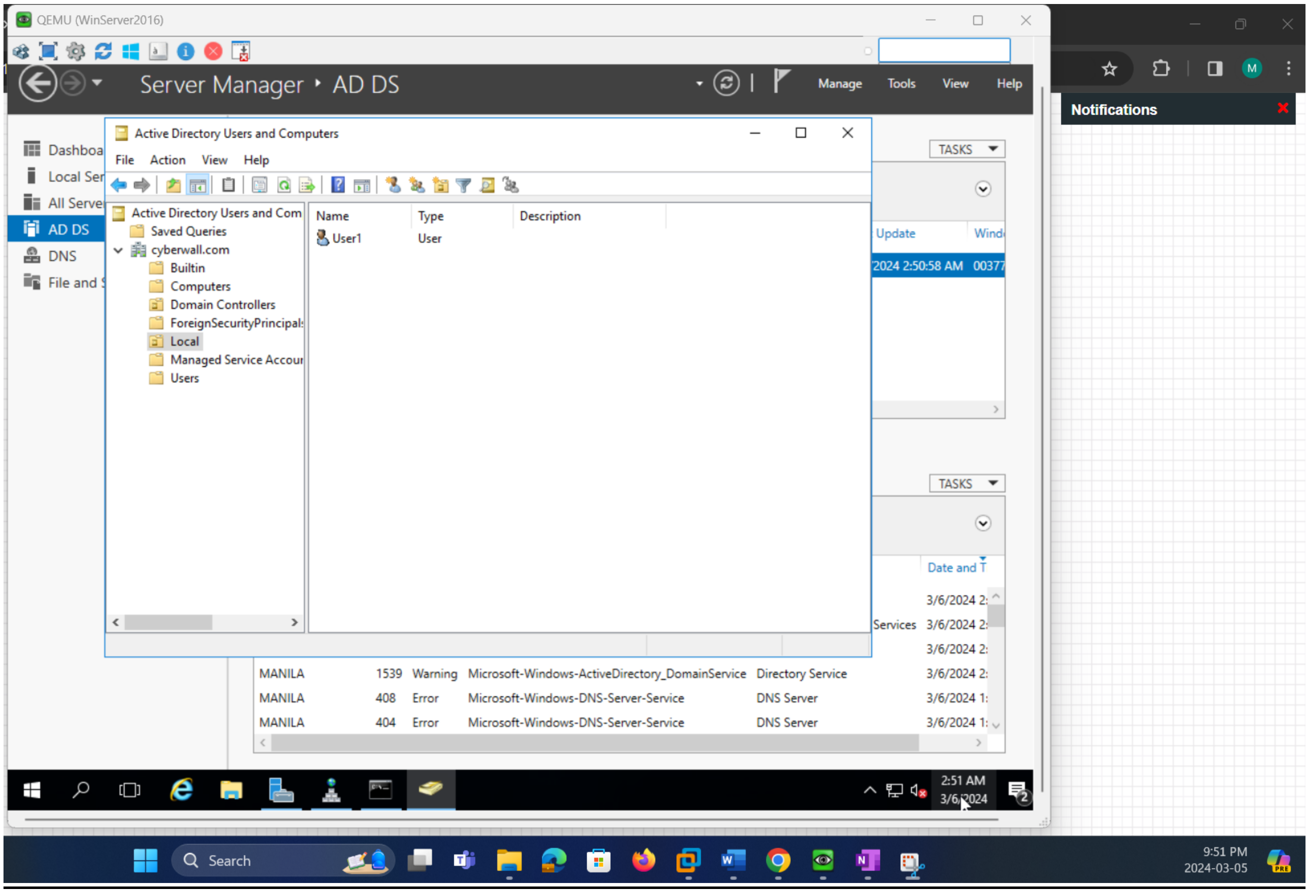
This image displays the login screen of a Windows Server 2016 virtual machine, indicating readiness for administrator login. It demonstrates the initial stage of accessing the server environment where Active Directory and DNS Server roles will be configured.



Name	Type	Description
cyberwall.co...	Domain	
Saved Queries		Folder to store your favo...

MANILA	1539	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	3/6/2024 2:
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:
MANILA	404	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:

Here we have the DNS Manager displaying DNS records for 'cyberwall.com'. Visible are the SOA (Start of Authority) and NS (Name Server) records, which are critical for the DNS functioning within an AD domain. Also, the ADUC console, a management tool used for creating and managing users, groups, computers, and organizational units within the Active Directory environment. In this context, the ADUC is open to the 'Users' container, where new user accounts can be created and managed for domain access.

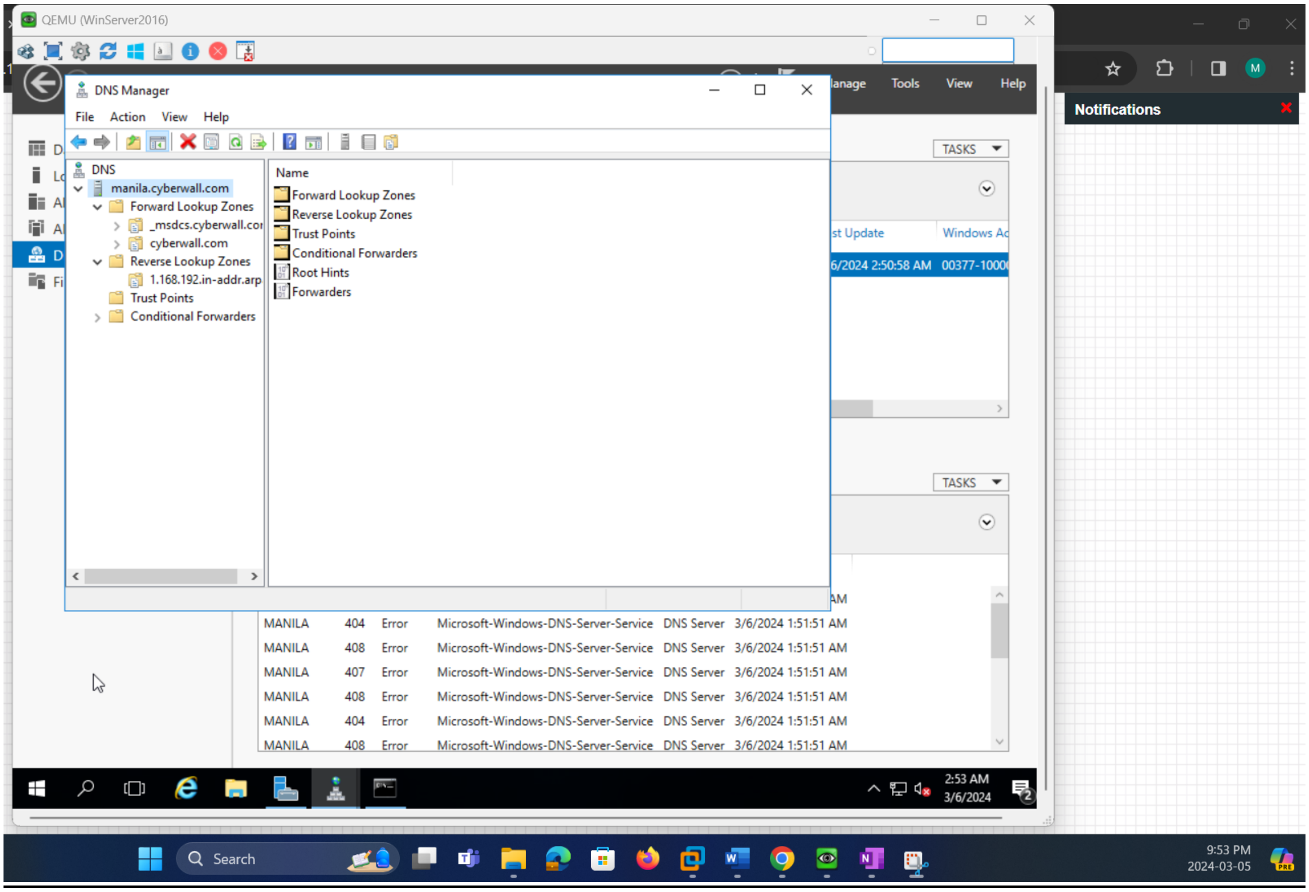


Active Directory Users and Com
- Saved Queries
- cyberwall.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal:
  - Local
  - Managed Service Accour
  - Users

Name	Type	Description
User1	User	

```
2024 2:50:58 AM   00377
                                                                    Services   3/6/2024 2:
MANILA   1539  Warning  Microsoft-Windows-ActiveDirectory_DomainService  Directory Service  3/6/2024 2:
MANILA   408   Error    Microsoft-Windows-DNS-Server-Service             DNS Server         3/6/2024 1:
MANILA   404   Error    Microsoft-Windows-DNS-Server-Service             DNS Server         3/6/2024 1:
```

The Active Directory Users and Computers (ADUC) console is showcased in this image, where 'User1' is visible under the domain 'cyberwall.com'. This tool is central to managing users, computers, and other objects within an AD domain. User1 was created for the purpose of this laboratory exercise.



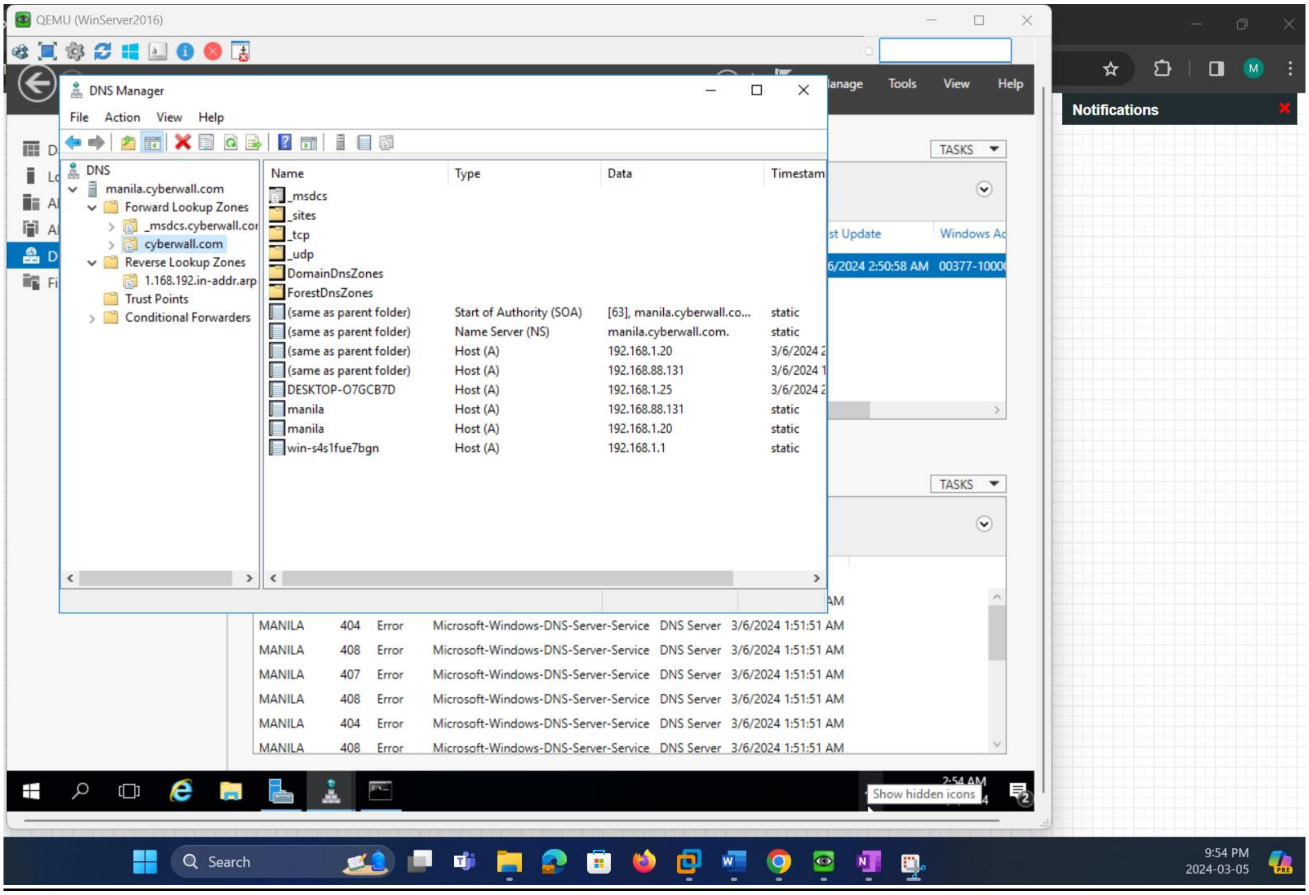
DNS
manila.cyberwall.com
Forward Lookup Zones
_msdcs.cyberwall.cor
cyberwall.com
Reverse Lookup Zones
1.168.192.in-addr.arp
Trust Points
Conditional Forwarders

Name
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Root Hints
Forwarders

st Update | Windows Ac
6/2024 2:50:58 AM | 00377-1000(

MANILA	404	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	407	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	404	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM

This screenshot displays the DNS Manager with a detailed view of the Forward Lookup Zones. It highlights the DNS entries associated with the Active Directory domain, such as the A (Host) records, which are essential for the proper resolution of domain names to IP addresses. These records are crucial for domain computers to locate domain controllers and other services.

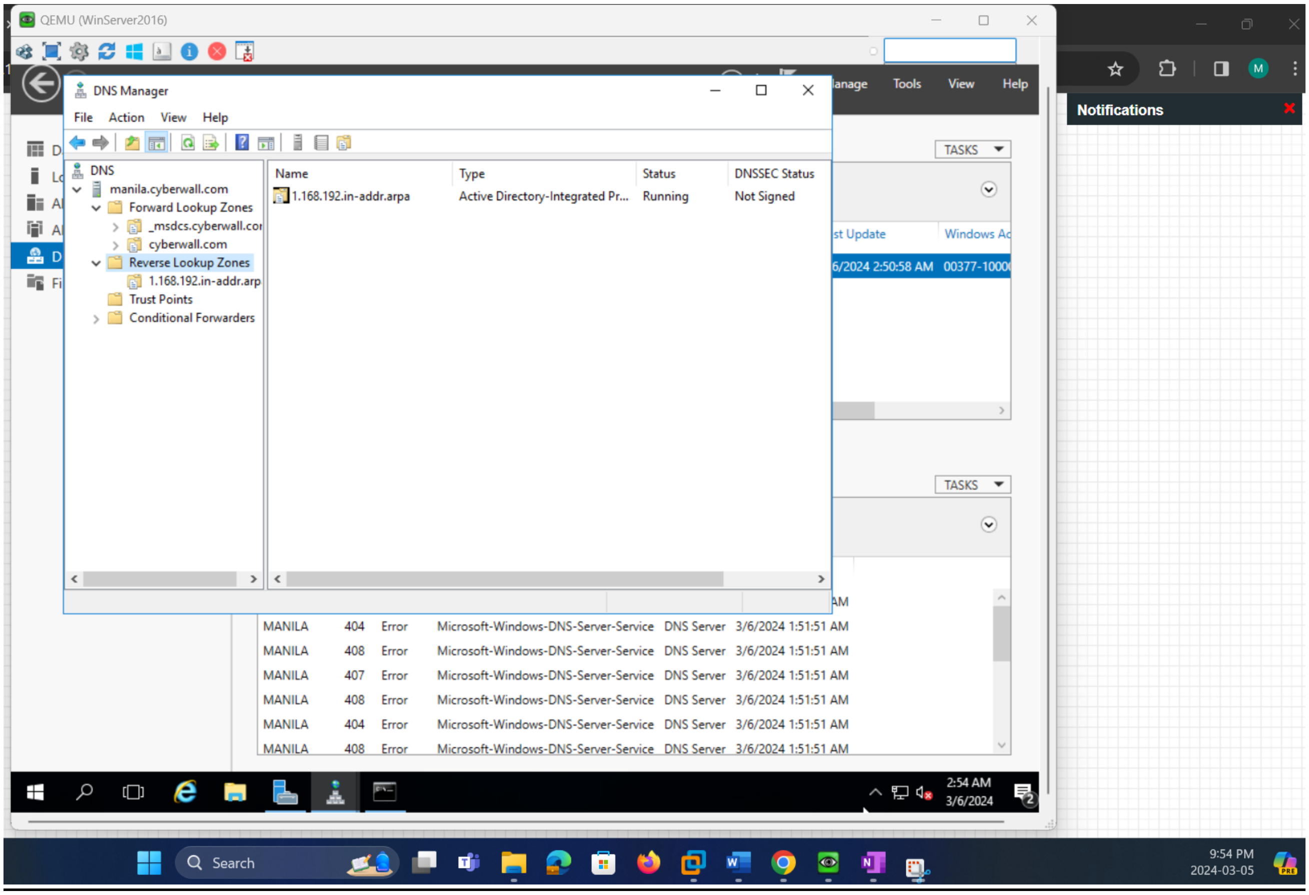


DNS
- manila.cyberwall.com
  - Forward Lookup Zones
    - _msdcs.cyberwall.co
    - cyberwall.com
  - Reverse Lookup Zones
    - 1.168.192.in-addr.arp
  - Trust Points
  - Conditional Forwarders

Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[63], manila.cyberwall.co...	static
(same as parent folder)	Name Server (NS)	manila.cyberwall.com.	static
(same as parent folder)	Host (A)	192.168.1.20	3/6/2024 2
(same as parent folder)	Host (A)	192.168.88.131	3/6/2024 1
DESKTOP-O7GCB7D	Host (A)	192.168.1.25	3/6/2024 2
manila	Host (A)	192.168.88.131	static
manila	Host (A)	192.168.1.20	static
win-s4s1fue7bgn	Host (A)	192.168.1.1	static

st Update | Windows Ac
6/2024 2:50:58 AM | 00377-1000

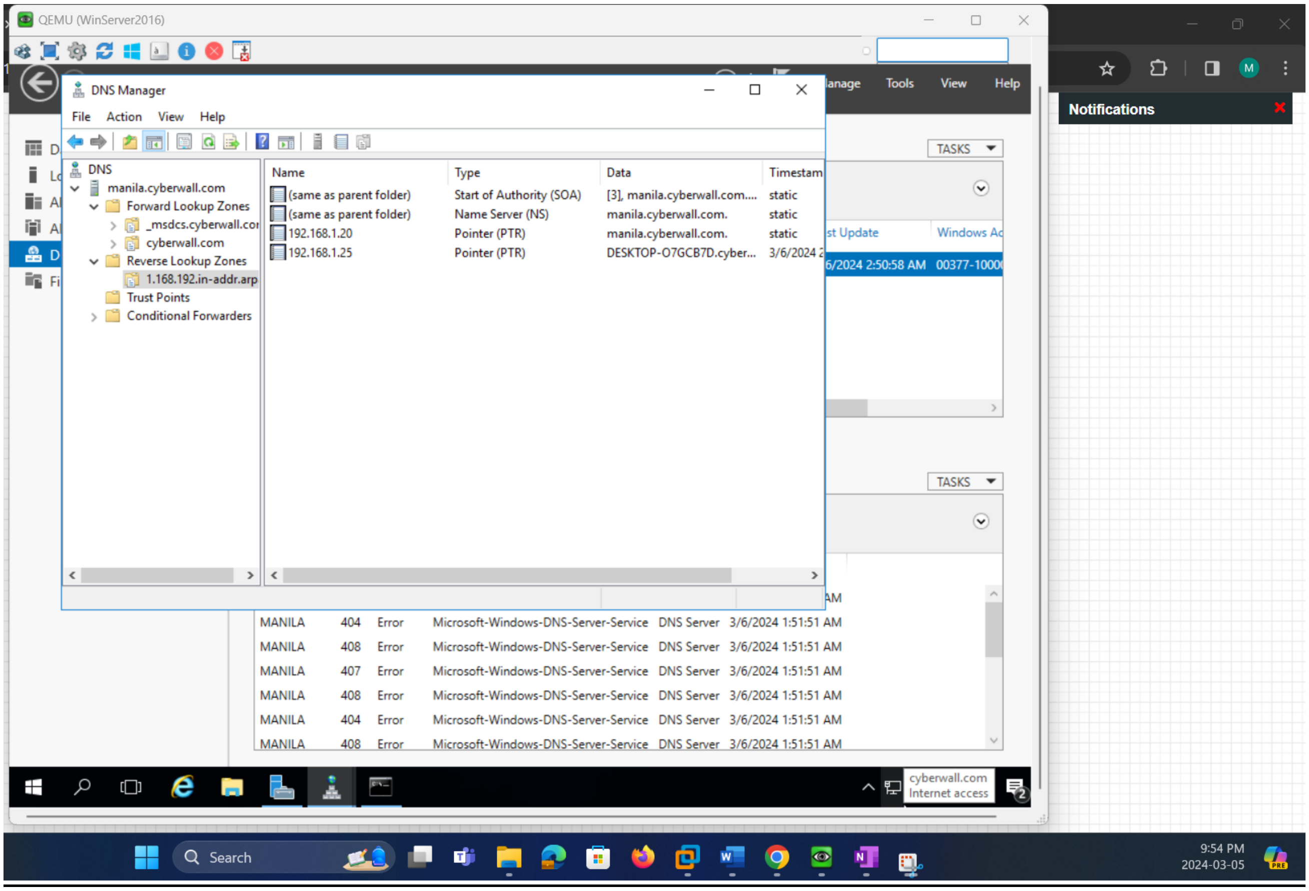
```
MANILA   404   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   408   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   407   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   408   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   404   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   408   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
```



Name	Type	Status	DNSSEC Status
1.168.192.in-addr.arpa	Active Directory-Integrated Pr...	Running	Not Signed

MANILA	404	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	407	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	404	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM

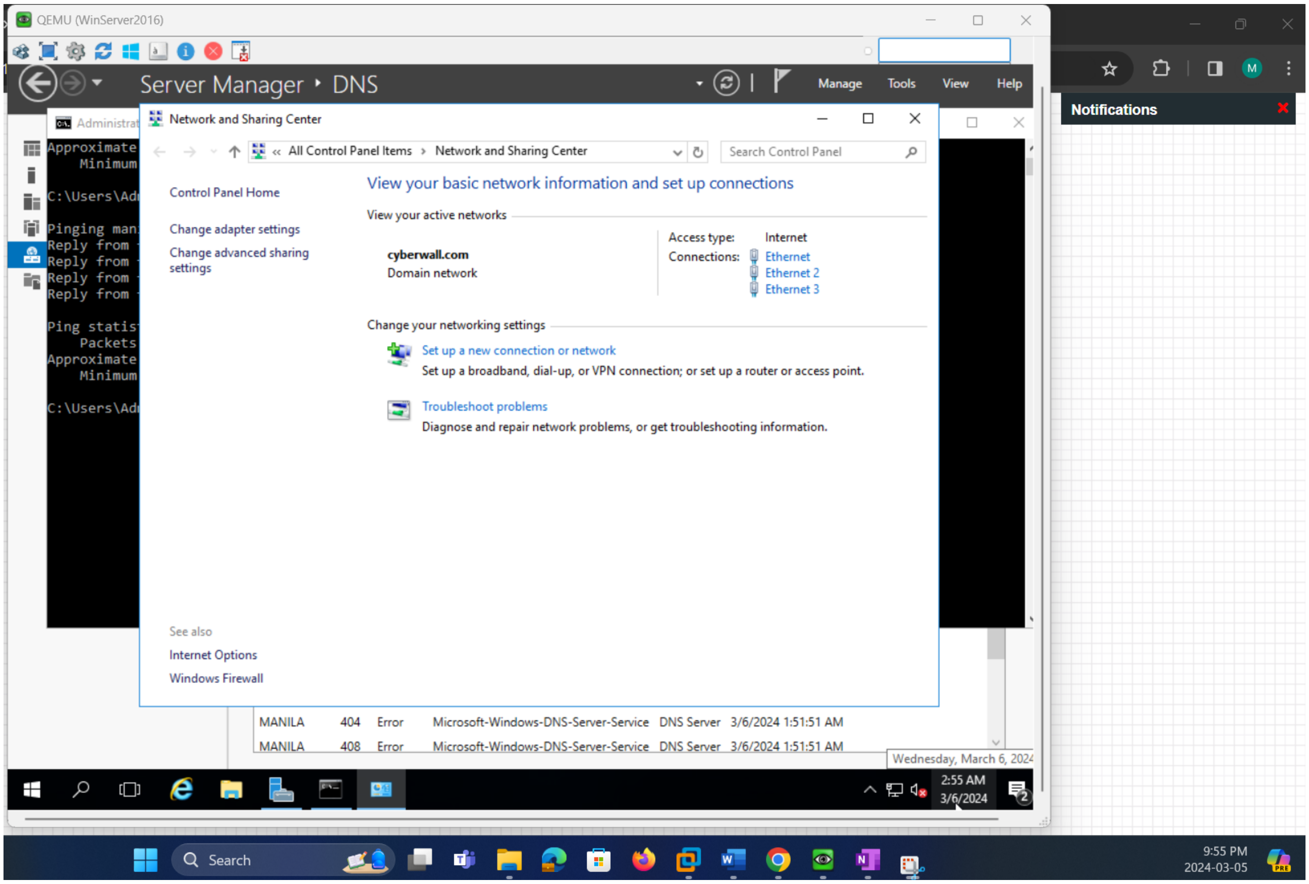
The Reverse Lookup Zones in the DNS Manager, shown in this screenshot, are responsible for mapping IP addresses back to domain names. The presence of PTR (Pointer) records here is important for certain network services and applications that rely on reverse name resolution.



Name	Type	Data	Timestam
(same as parent folder)	Start of Authority (SOA)	[3], manila.cyberwall.com....	static
(same as parent folder)	Name Server (NS)	manila.cyberwall.com.	static
192.168.1.20	Pointer (PTR)	manila.cyberwall.com.	static
192.168.1.25	Pointer (PTR)	DESKTOP-O7GCB7D.cyber...	3/6/2024 2

```
MANILA   404   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   408   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   407   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   408   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   404   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   408   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
```

This screenshot displays the DNS Manager with detailed DNS records for the domain "cyberwall.com" within the Windows Server 2016 environment. Specifically shown are the Start of Authority (SOA) and Name Server (NS) records for the domain, along with various Host (A) records that map domain names to IP addresses. The presence of these records is integral to the functionality of Active Directory, as they help in the resolution of domain names within the network. Correct configuration of these DNS records is crucial for the Active Directory services to function properly, enabling resources to be located and utilized by users and computers within the domain.



```
Approximate
    Minimum
C:\Users\Adm
Pinging man
Reply from
Reply from
Reply from
Reply from

Ping statis
    Packets
Approximate
    Minimum

C:\Users\Adm
```

View your basic network information and set up connections

View your active networks

cyberwall.com
Domain network

Access type: Internet
Connections: Ethernet
Ethernet 2
Ethernet 3

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

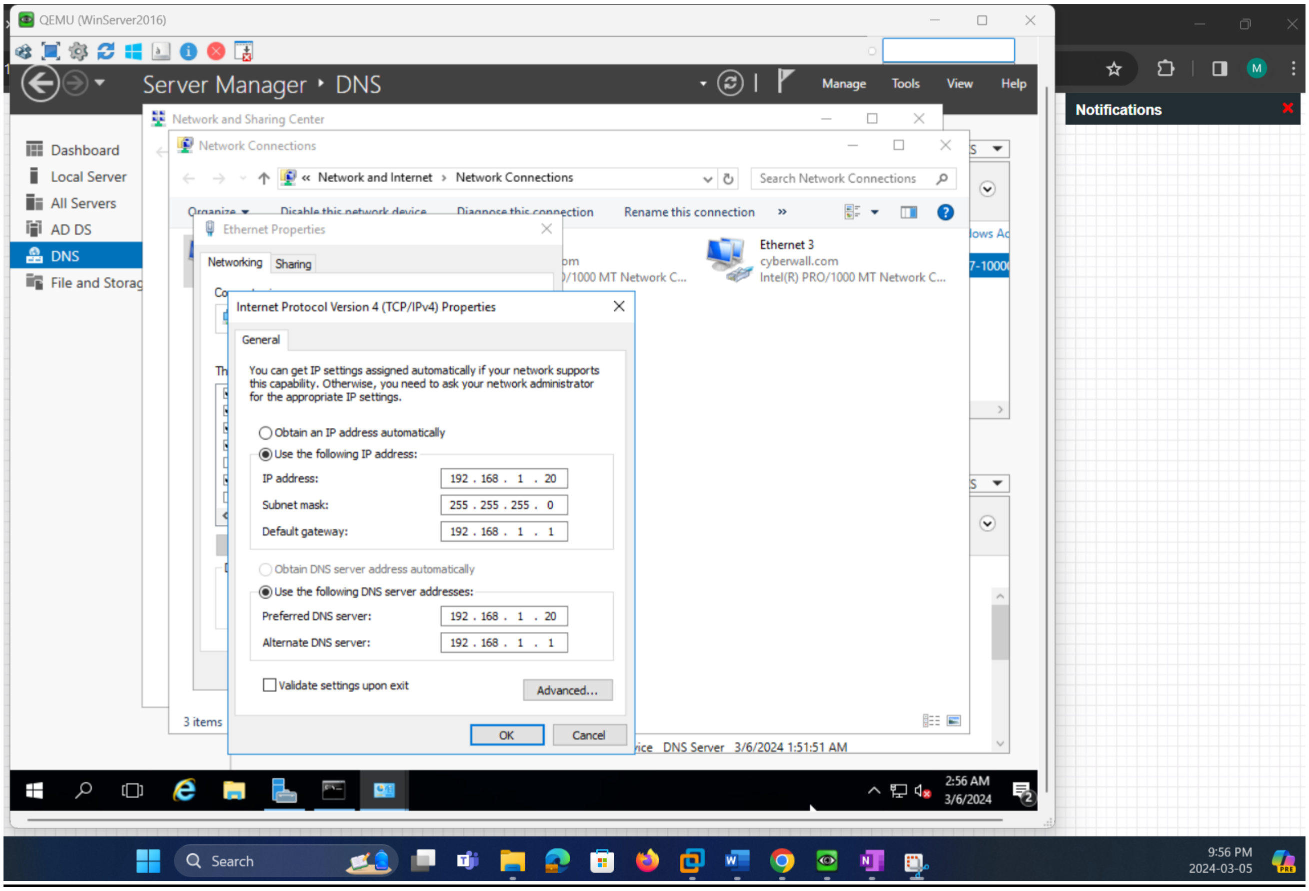
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

```
MANILA   404   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
MANILA   408   Error   Microsoft-Windows-DNS-Server-Service   DNS Server   3/6/2024 1:51:51 AM
```

Wednesday, March 6, 2024
2:55 AM
3/6/2024

Search
9:55 PM
2024-03-05

The Network and Sharing Center is open on the Windows Server 2016 desktop. It is instrumental in managing network connections and indicates the server is part of the 'cyberwall.com' domain network with Internet access, aligning with the lab's objectives.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 20
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

○ Obtain DNS server address automatically

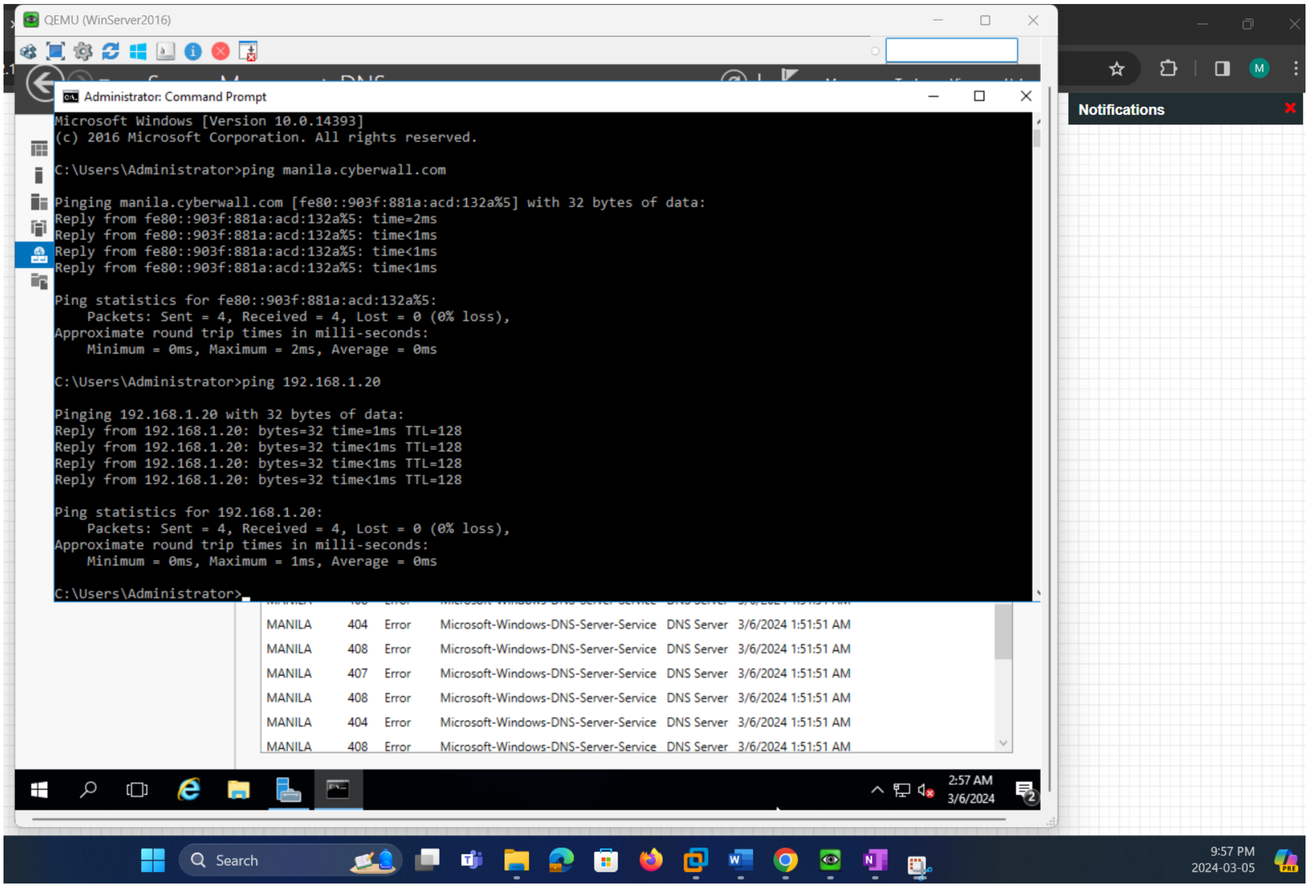
● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 1 . 20
Alternate DNS server:	192 . 168 . 1 . 1

□ Validate settings upon exit

Ethernet 3
cyberwall.com
Intel(R) PRO/1000 MT Network C...

The screenshot displays the "Internet Protocol Version 4 (TCP/IPv4) Properties" configuration window for a network interface on the Windows Server 2016. It shows that the server has been assigned a static IP address (192.168.1.20) with a subnet mask of 255.255.255.0 and a default gateway of 192.168.1.1. The DNS server settings are also manually configured with the preferred DNS server address pointing to itself (192.168.1.20) and an alternate DNS server address (192.168.1.1). This setup is typical for a domain controller, ensuring that the server uses its own DNS service for resolution and providing an alternate DNS server for redundancy or external name resolution. This configuration is essential for Active Directory and DNS services to operate correctly and reliably within the network.

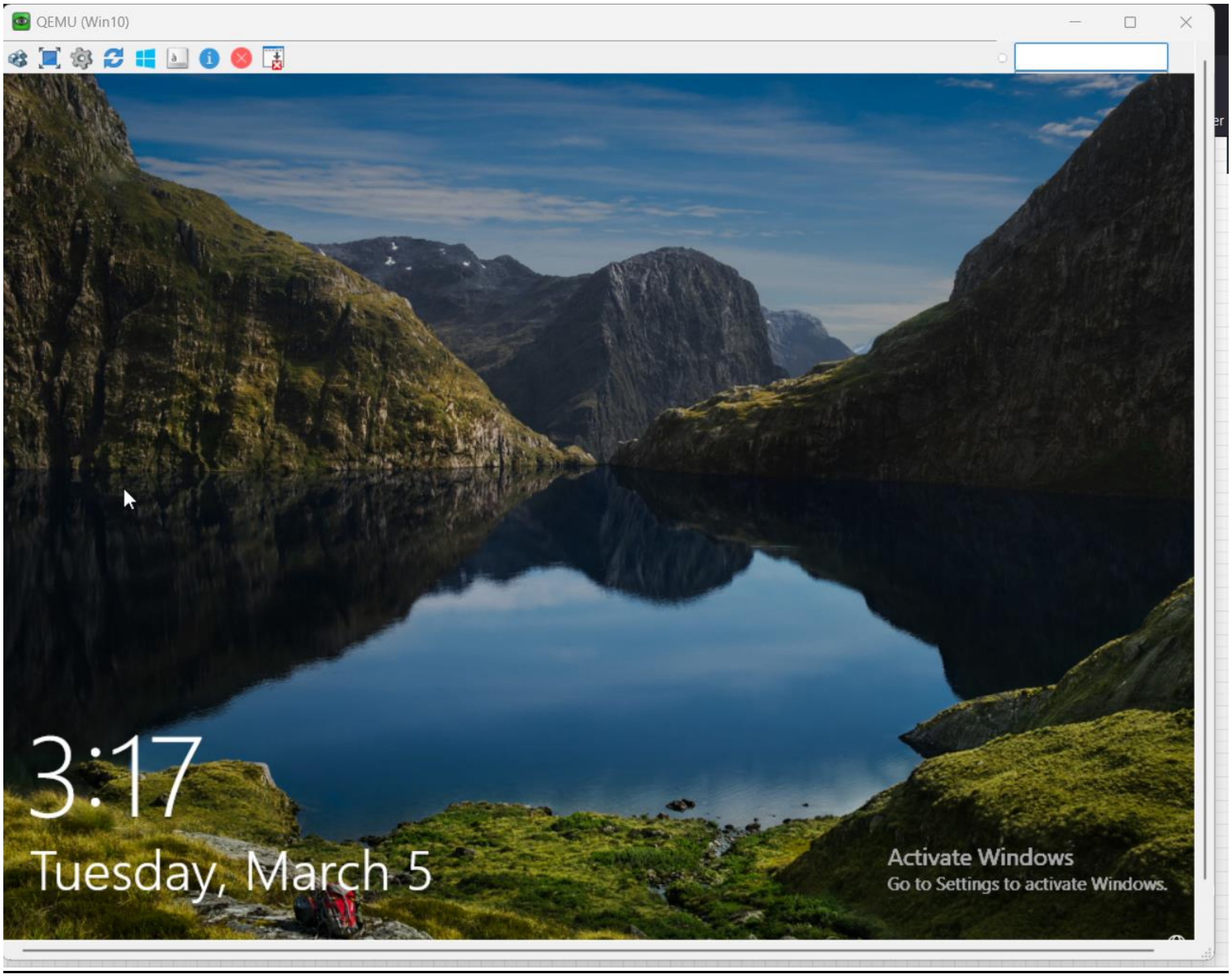


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping manila.cyberwall.com

Pinging manila.cyberwall.com [fe80::903f:881a:acd:132a%5] with 32 bytes of data:
Reply from fe80::903f:881a:acd:132a%5: time=2ms
Reply from fe80::903f:881a:acd:132a%5: time<1ms
Reply from fe80::903f:881a:acd:132a%5: time<1ms
Reply from fe80::903f:881a:acd:132a%5: time<1ms

Ping statistics for fe80::903f:881a:acd:132a%5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Administrator>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>_
```

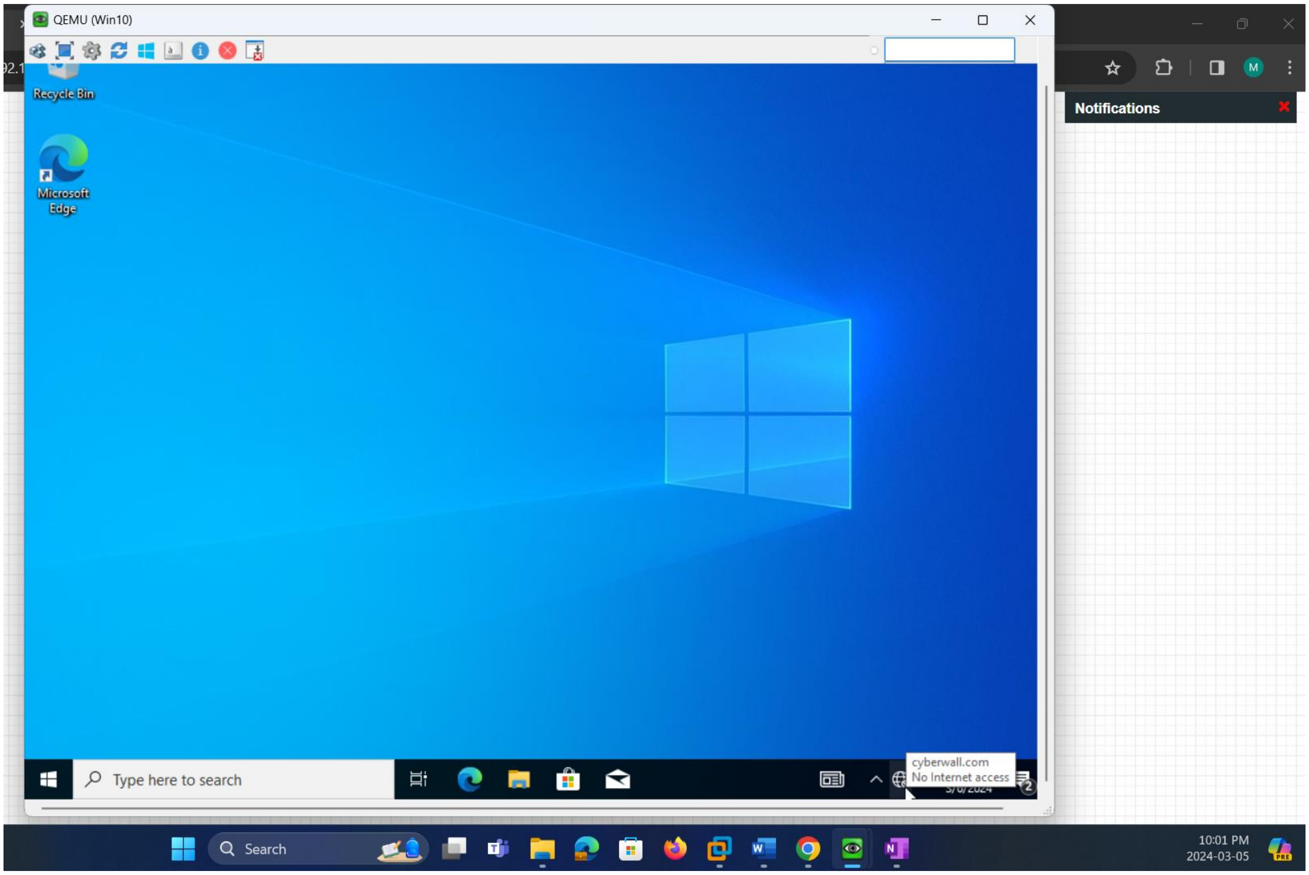
MANILA	404	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	407	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	404	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM
MANILA	408	Error	Microsoft-Windows-DNS-Server-Service	DNS Server	3/6/2024 1:51:51 AM

This screenshot presents the Command Prompt window on the Windows Server 2016 virtual machine displaying the results of a ping test conducted on the domain name "manila.cyberwall.com" and its associated IP address "192.168.1.20". The successful ping results to both the domain name and the IP address indicate that DNS resolution is working correctly for the domain within the local network, which is a key aspect of the DNS server functionality. The absence of packet loss in the statistics shows a healthy network communication between the server and the domain resources. This is an important verification step to ensure that the Active Directory domain controller can be reached by its name, a crucial requirement for domain operation and services accessibility.

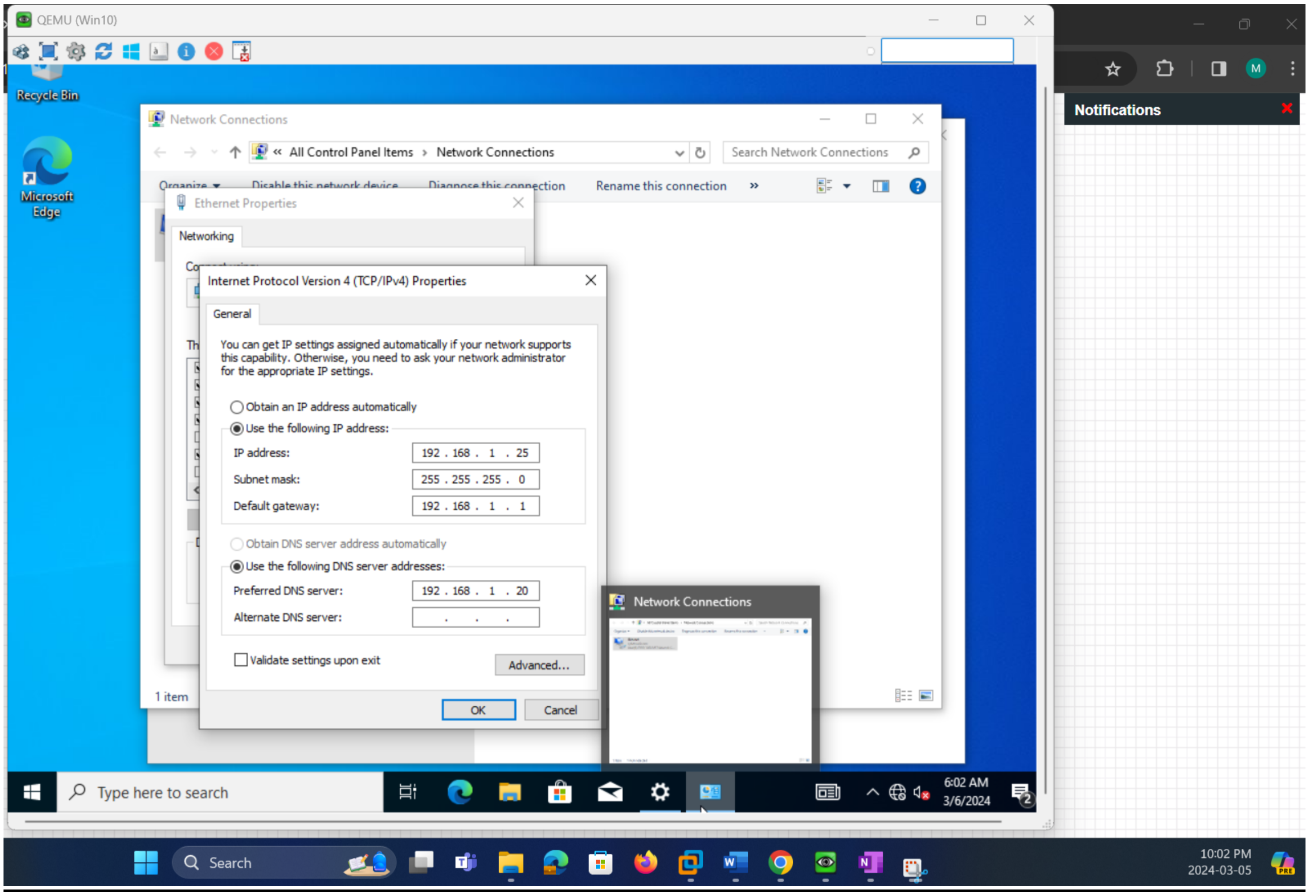
3. Installation and Configuration of Windows 10 Pro Client



The initial lock screen of a newly booted Windows 10 system, indicating the operating system is up and ready for user sign-in.



The desktop interface of Windows 10, demonstrating that the installation process has completed successfully, and the system is at a ready state for further configuration or use.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 25
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

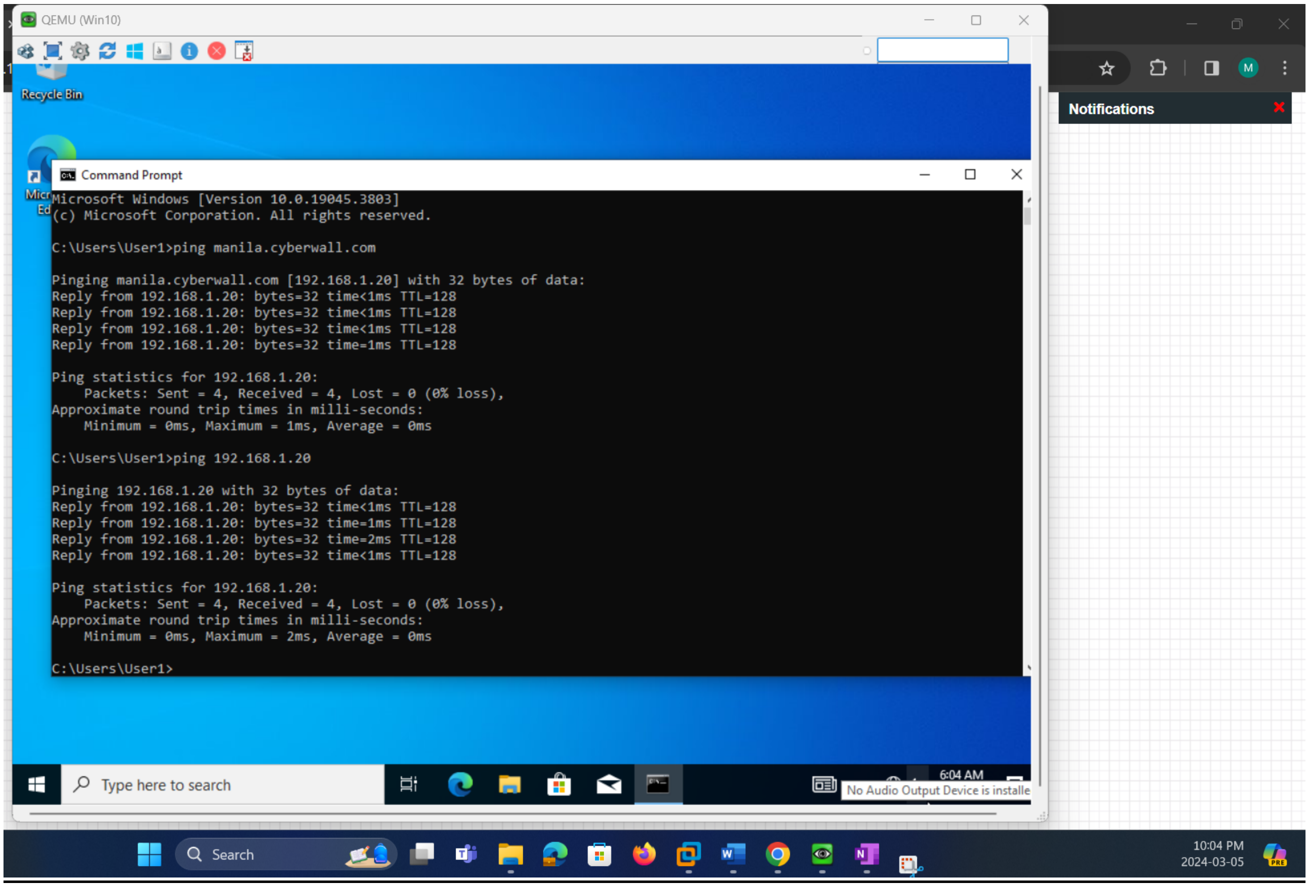
Preferred DNS server:	192 . 168 . 1 . 20
Alternate DNS server:	. . .

□ Validate settings upon exit

Advanced...

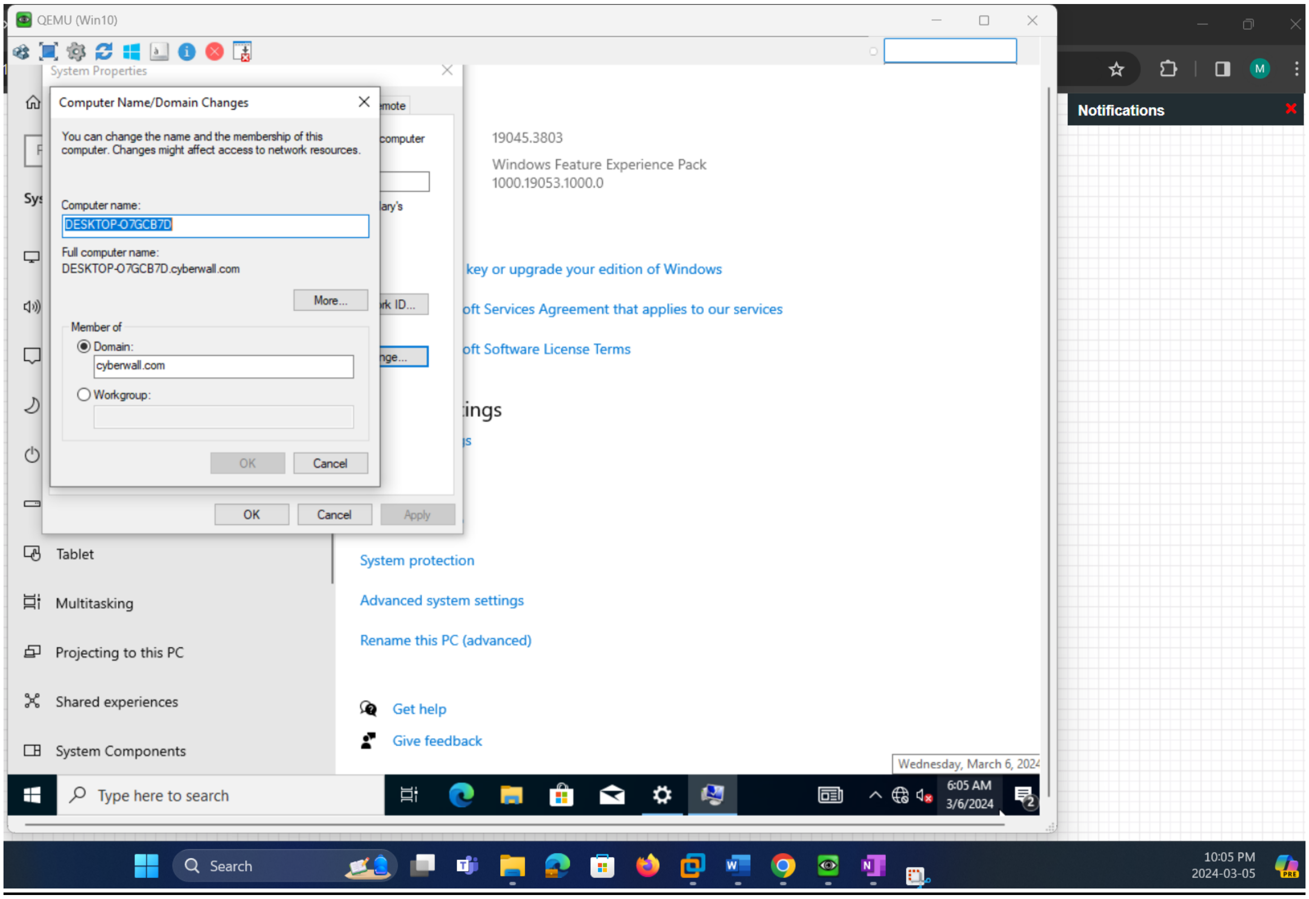
OK Cancel

The network configuration settings of the Windows 10 client, where a static IP address has been assigned to the machine to ensure consistent network communication within your domain environment. It's also set to use the Windows Server 2016 machine as its preferred DNS server, indicating integration with the domain for DNS resolution.



```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User1>ping manila.cyberwall.com

Pinging manila.cyberwall.com [192.168.1.20] with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User1>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=2ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\User1>
```

The command prompt showing successful ping tests to both the domain name and the server's IP address, confirming network connectivity and DNS resolution from the client side.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: DESKTOP-O7GCB7D

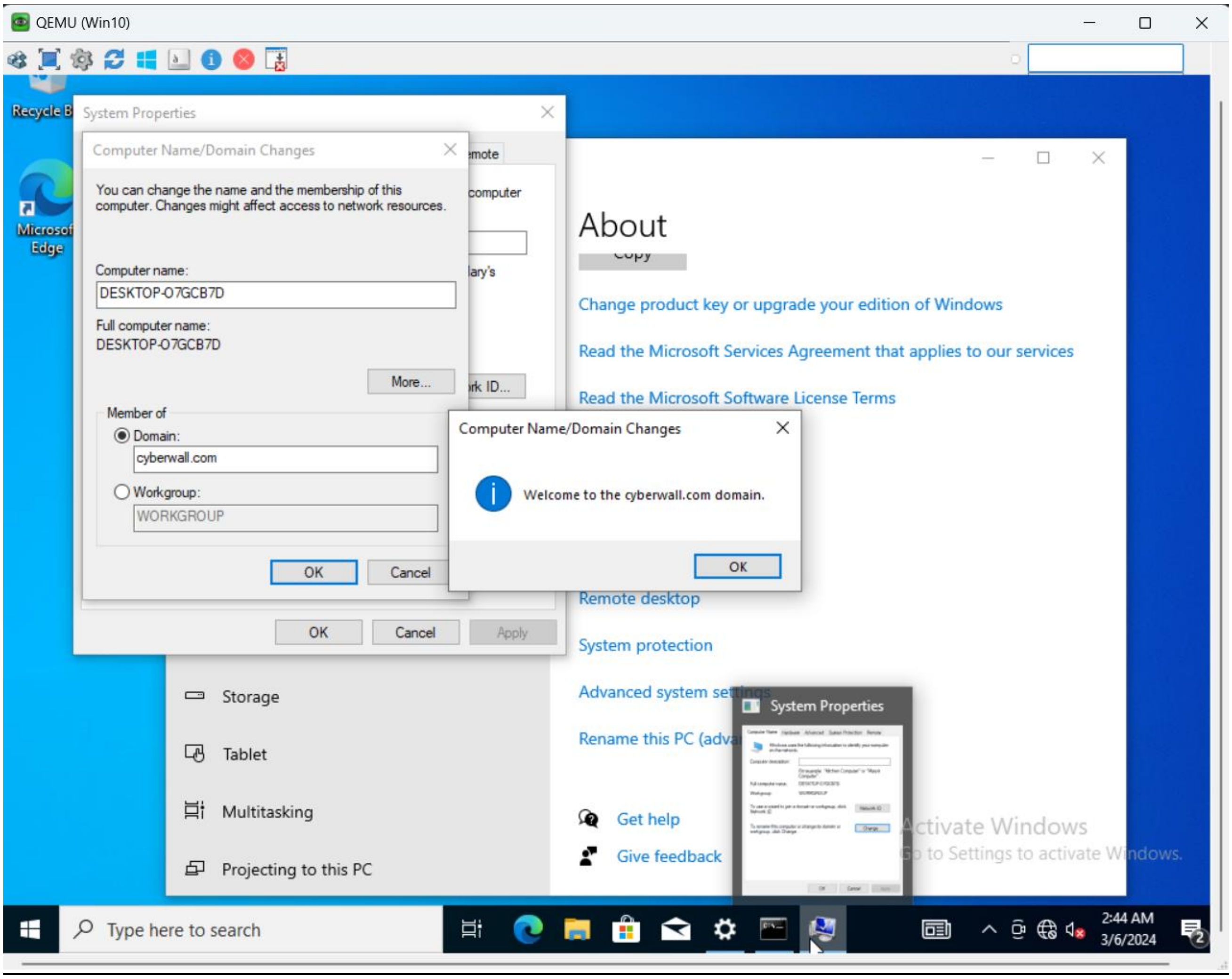
Full computer name: DESKTOP-O7GCB7D.cyberwall.com

Member of

● Domain: cyberwall.com

○ Workgroup:

The system properties window with the 'Computer Name/Domain Changes' dialog open, showing that the client machine is being joined to the 'cyberwall.com' domain. This is a critical step in integrating the client into the Active Directory domain, allowing for centralized management and authentication.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: DESKTOP-07GCB7D

Full computer name:
DESKTOP-07GCB7D

Member of
● Domain: cyberwall.com
○ Workgroup: WORKGROUP

Computer Name/Domain Changes

Welcome to the cyberwall.com domain.

The image shows the 'System Properties' dialog box on a Windows 10 Pro virtual machine with the 'Computer Name/Domain Changes' window open. This window is used to add the computer to a domain; in this case, the domain "cyberwall.com" has been entered. When a computer is joined to a domain, it can leverage the centralized management and security settings provided by Active Directory. This step is crucial in setting up a client machine to work within a corporate network, allowing it to access shared resources and adhere to organizational policies. The computer name "DESKTOP-07GCB7D" is displayed, indicating it is the default name given to the machine before joining the domain.

4. Challenges Faced and How they were Overcome:

Throughout the lab scenario, I encountered several technical challenges, particularly in managing system resources such as memory, RAM, and HDD space. The resource constraints sometimes resulted in lag and occasional crashes or freezes of the virtual machines. However, leveraging my prior experience with similar scenarios in my previous job, I was able to navigate these challenges effectively.

In addition, I optimized the VM allocations, ensuring that each virtual machine had only the necessary resources, which was crucial for the smooth running of the Active Directory and DNS configuration tasks. I frequently saved my work to prevent data loss and closed any non-essential applications to free up additional resources. My familiarity with virtualization and network configuration allowed me to anticipate potential issues and troubleshoot them promptly, ensuring the success of the lab exercise.

Conclusion and Recommendations

The general objective of configuring Active Directory (AD) and Domain Name System (DNS) in a cybersecurity exercise is to understand the foundational role these services play in the security infrastructure of an organization. AD is crucial for managing user access, implementing security policies, and administering permissions across networked resources. DNS, on the other hand, is integral to the functioning of the internet and intranet services within an organization, including the resolution of domain names into IP addresses.

By setting up and configuring these services, one gains practical insights into securing identity management and network services, which are common targets for cyber attacks. This hands-on practice is vital in learning how to harden these systems against threats, understand potential vulnerabilities, and how to monitor and respond to security incidents involving identity and access management as well as network traffic.

The lab exercise provided a comprehensive understanding of how Active Directory and DNS function within a network and their importance in cybersecurity. It demonstrated the critical nature of secure configuration and the potential impact of system resources on network operations. The hands-on experience gained is invaluable for any cybersecurity professional, as it reflects real-world situations where one must optimize limited resources while ensuring robust network security and functionality. The ability to overcome technical challenges and apply theoretical knowledge in a practical environment is a testament to the effectiveness of such exercises in preparing cybersecurity practitioners for the field.

For individuals undertaking similar lab exercises, it is recommended to approach the task with patience and a readiness to apply troubleshooting skills. Anticipating challenges with system resources and preparing for potential software issues can greatly reduce the frustration that might come with unexpected problems. Additionally, those with prior experience should draw upon their knowledge while remaining open to learning from new situations that lab scenarios may present. The practice of saving work frequently and documenting steps as you go can not only save time in the event of a system failure but also serve as a learning tool for future reference.