Information Technology Institute

MCSA PROJECT

Implementation of Multi-Domain Enterprise Services and Centralized Management

Project Team

Ahmed Hamdy
Tarek Abdelrahman
Yousef Mohamed Aboelata
Omar Alaa El-Din
Donia Sobhy
Fatma Ahmed

Under Supervision of:
Eng: Mohamed Abosehely

Table of Contents

1. Network Topology & Overview

This project demonstrates the design and implementation of a complex Windows Server infrastructure for ITI.Local, using a multi-domain forest architecture to simulate real-world enterprise networking scenarios. The environment integrates core services including Active Directory, DNS, DHCP, IIS, and Windows Deployment Services (WDS), providing centralized management, security, and automation.

The project focuses on three key areas:

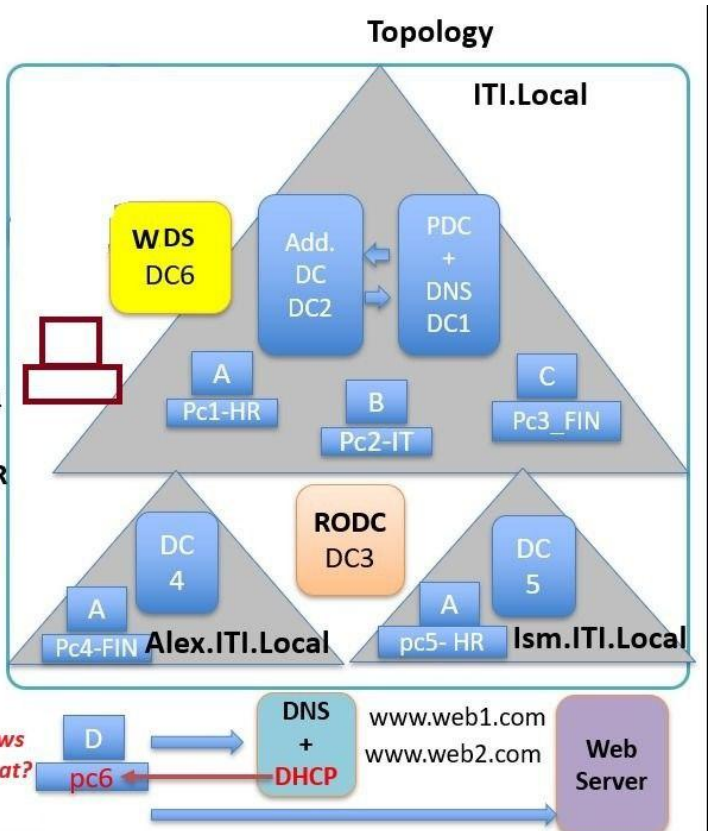
- Active Directory Hierarchy – implementing a root domain (ITI.Local) with child domains (Alex.ITI.Local and Ism.ITI.Local) to represent organizational branches.
- Policy Management – using Group Policy Objects (GPOs) for software deployment, desktop restrictions, and security settings, including password replication for RODCs.
- Service Automation & Administration – leveraging WDS for rapid deployment of users and computers, and enabling secure remote management while adhering to the principle of least privilege.

This setup provides a realistic environment for testing enterprise-level administration, delegation, and automated service management.

DC1 is a primary Domain Controller
DC2 is an additional Domain Controller
DC3 is a RODC,DC4&DC5 are Chilled DC

A@ITI.local can only login to PC1 but can't login to pc1 on Fridays
help@ITI.local can login to Rodc & his PSWD is replicated to Rodc
c@ITI.local can't access Flash memory& control Panel & his wallpaper is ITI logo
A@Ism.ITI.Local can login to **PC5-PC1-PC4** (ROMING PROFILE)**
DOMAIN ADMIN need to install **WINRAR** on pc2 using GPO (how)**
DOMAIN ADMIN delegate to B@iti.local to login remotely to DC1 (not member of administrators) **
A@ITI.local check the website **https**:\\www.web2.com from pc1

you need to add 50 new computers with windows and 50 user to the domain (how to automate that? WDS



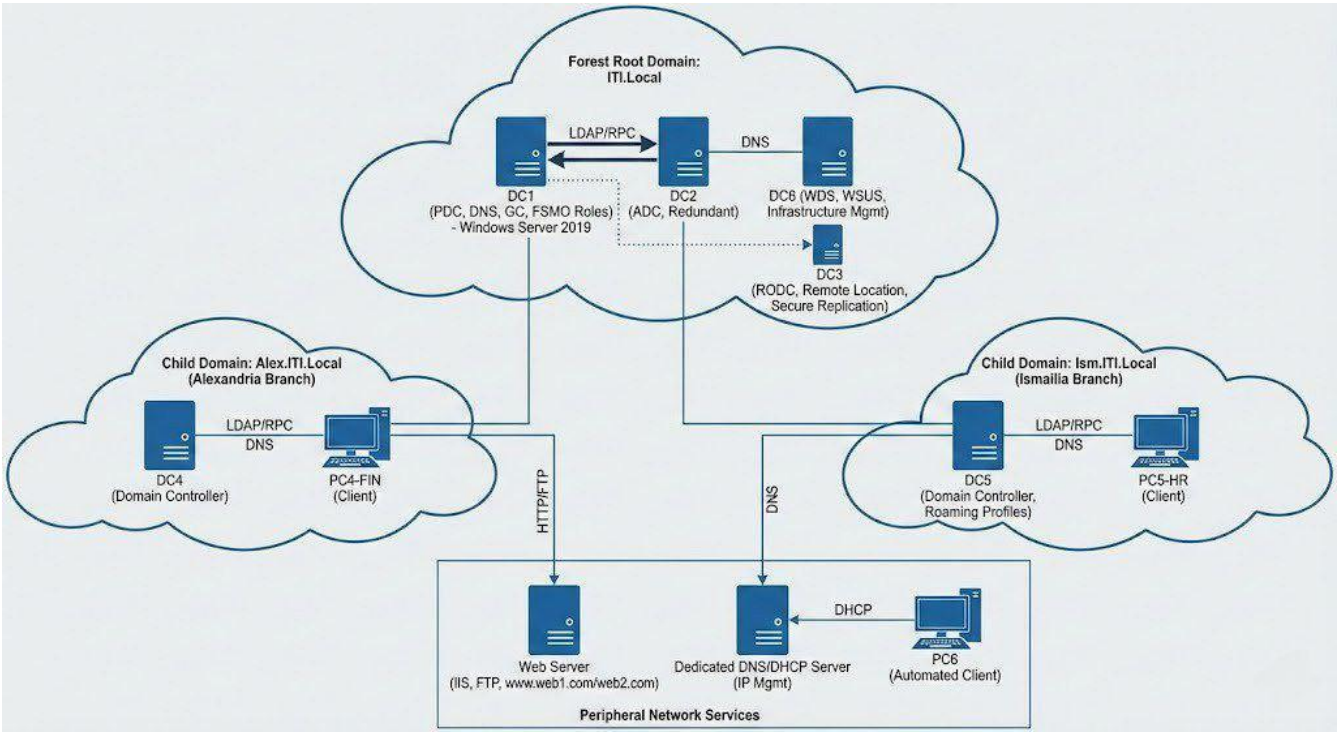
D is a local user on **pc6** but he can manage remotely (**RDP**) the webserver with administrative privileges ,his responsibilities is to check http:\\ www.web1.com and get a **copy** of it using **FTP**

Infrastructure overview:

- **Forest Root Domain (Top Cloud):**
  - Hosting the critical identity infrastructure.
  - **DC1 & DC2:** Connected via LDAP/RPC to ensure synchronous replication of the Active Directory database.
  - **DC6 & DC3:** Services like WDS and the RODC are linked to the core via secure channels to minimize risk.

- **Branch Offices (Left & Right Clouds):**
  - Alex.ITI.Local (DC4) and Ism.ITI.Local (DC5) maintain a two-way transitive trust with the root domain.
  - Traffic flow for authentication and DNS queries utilizes standard RPC and DNS protocols to route requests back to the PDC when necessary.

- **Peripheral Services (Bottom Box):**
  - This zone isolates public-facing services from the core identity servers.
  - **Web Server:** Accessible via HTTP/FTP for hosting the corporate intranet and file transfers.



2. Domain Infrastructure (The Backbone)

2.1 Primary & Additional Domain Controllers

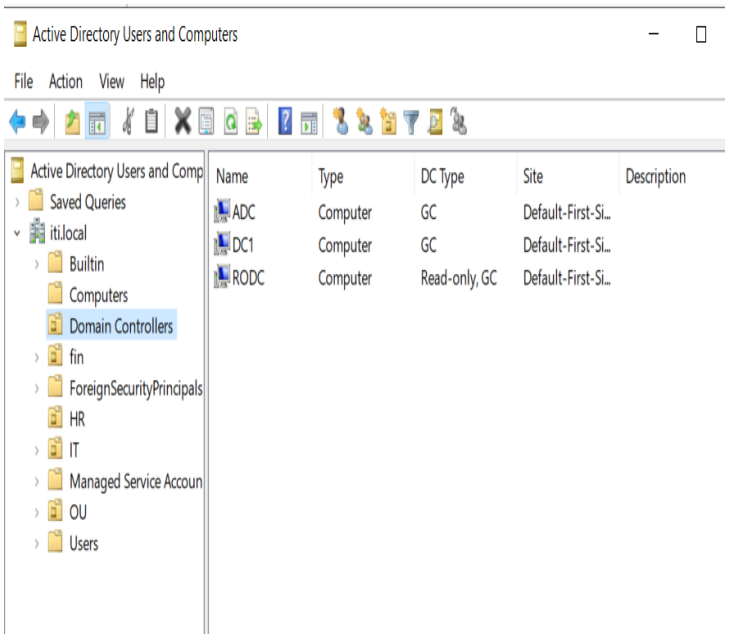
DC1 (PDC): The Root DC (ITI.Local) serves as the central authority for the entire forest infrastructure. Its primary functions include:

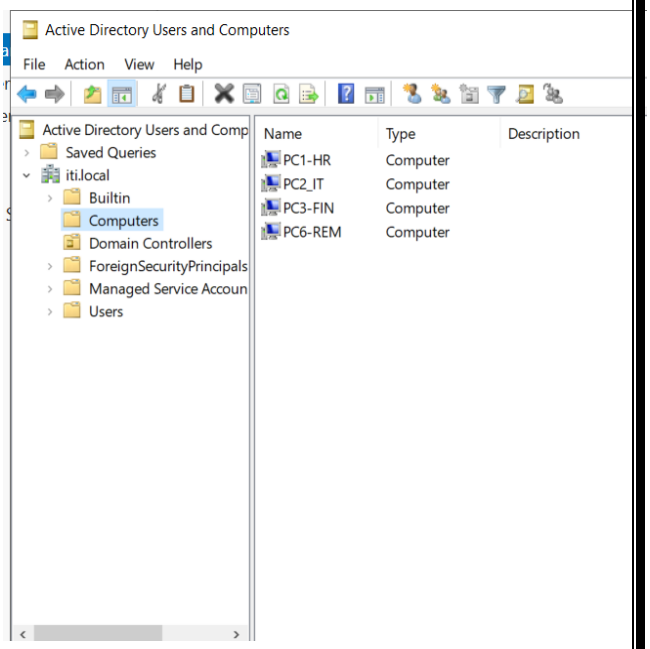
- **Trust Management:** Facilitates the Parent-Child Trust, allowing User A to authenticate across both ITI and Ism domains.
- **Policy Synchronization:** Manages the PDC Emulator role to ensure WinRAR GPO updates are replicated and enforced on all targets.
- **Global Catalog:** Locates Roaming Profile paths for cross-domain users, ensuring data accessibility regardless of the workstation's domain.
- **Centralized Security:** Validates Logon Workstation restrictions to prevent unauthorized access to restricted network resources.

The Primary DC acts as the centralized management point, ensuring consistent policy enforcement and secure resource sharing between the Root and Child domains.

DC2 (ADC): Promotion of the Additional Domain Controller to establish High Availability and eliminate a "Single Point of Failure" within the network.

- **Redundancy:** Prevents network downtime if the primary server fails.
- **Fault Tolerance:** Ensures users can still log in even if DC1 is offline.
- **Load Balancing:** Distributes the workload of processing user logons between two servers.





2.2 Child Domains Implementation

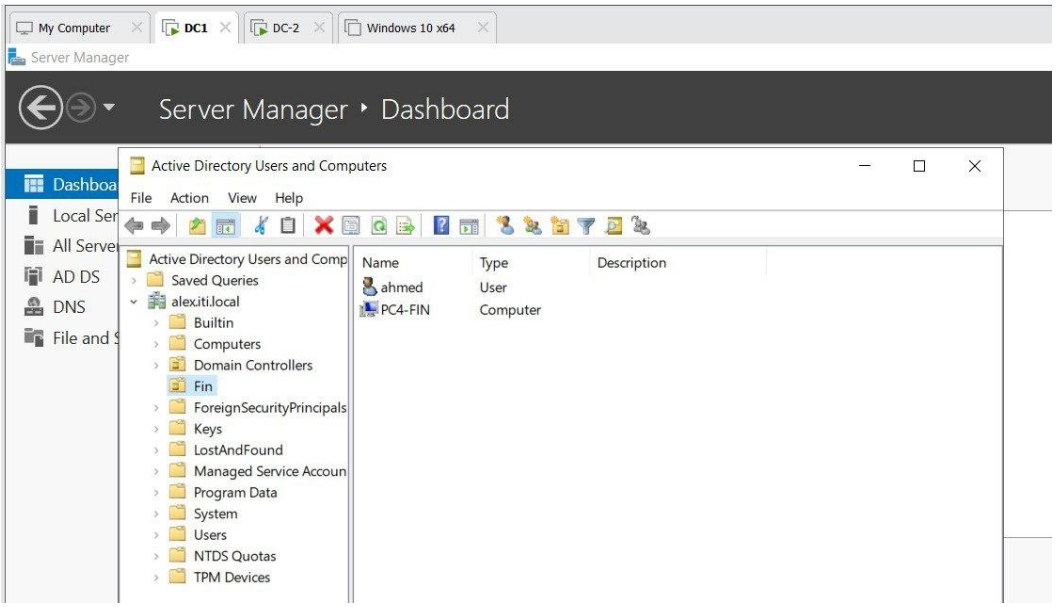
We created two child domains under the main forest: alex.iti.local and ism.iti.local, to simulate a multi-branch organizational structure and centralized identity management

Alex.ITI.Local (Alex):

We also created a dedicated Finance Organizational Unit (OU) that contains the finance department's user accounts and computers, allowing for structured administration and policy control.

Ism.ITI.Local (Ism):

We also created a dedicated HR Organizational Unit (OU) that contains the HR department's user accounts and computers, allowing for structured administration and policy control.



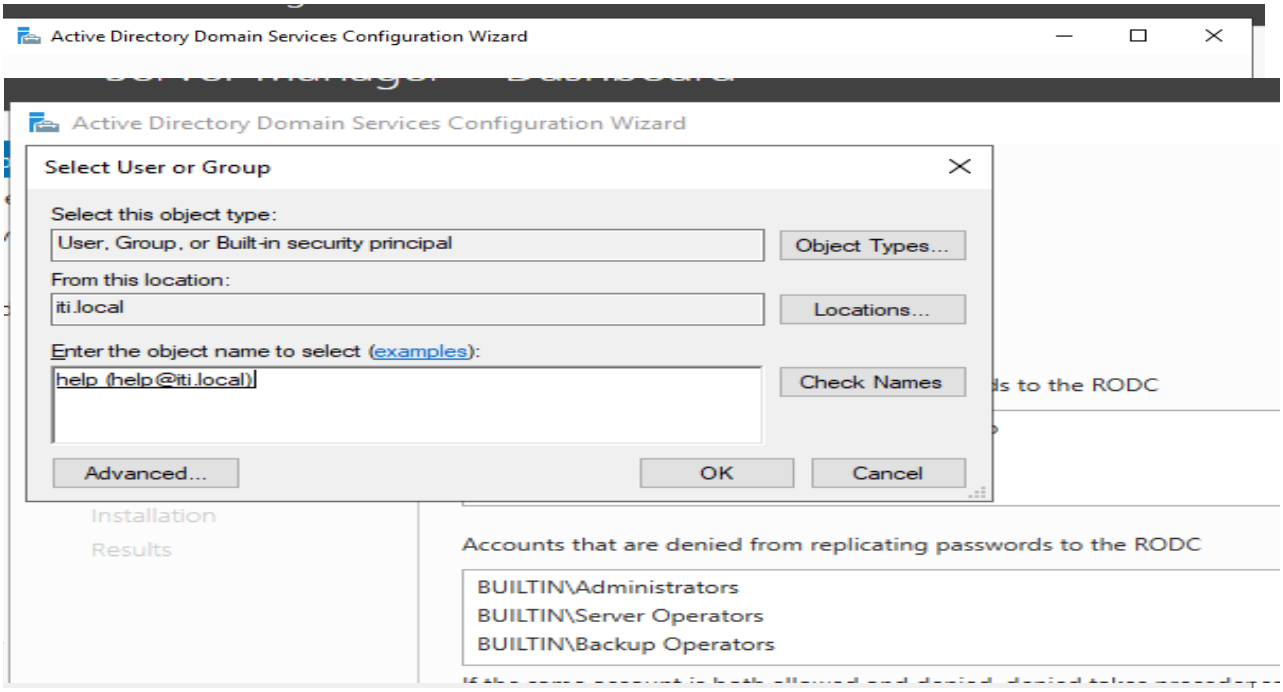
2.3 Read-Only Domain Controller (RODC)

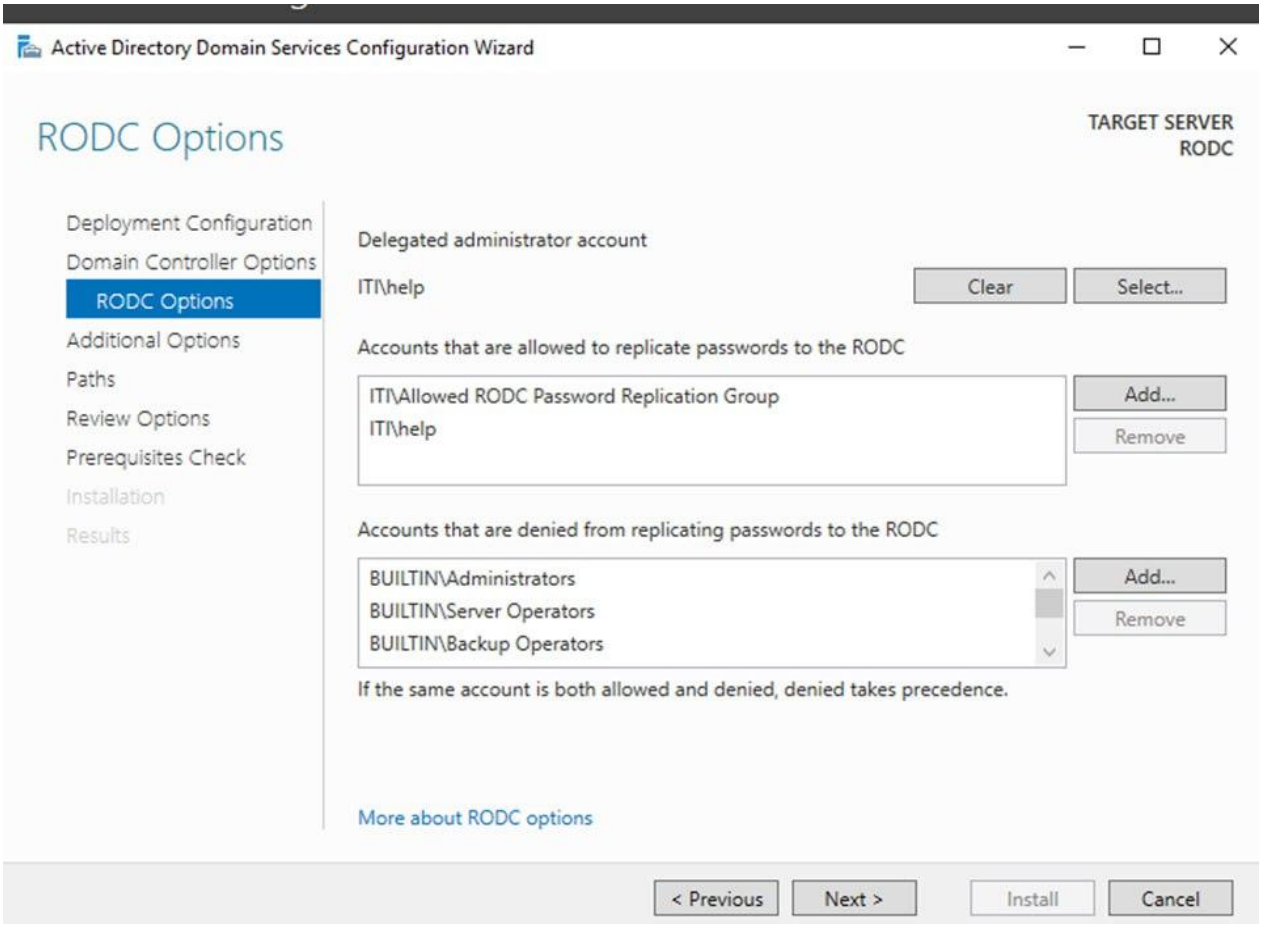
The primary goal was to deploy a Read-Only Domain Controller (RODC) to a remote site while delegating administrative tasks to a non-Domain Admin user.

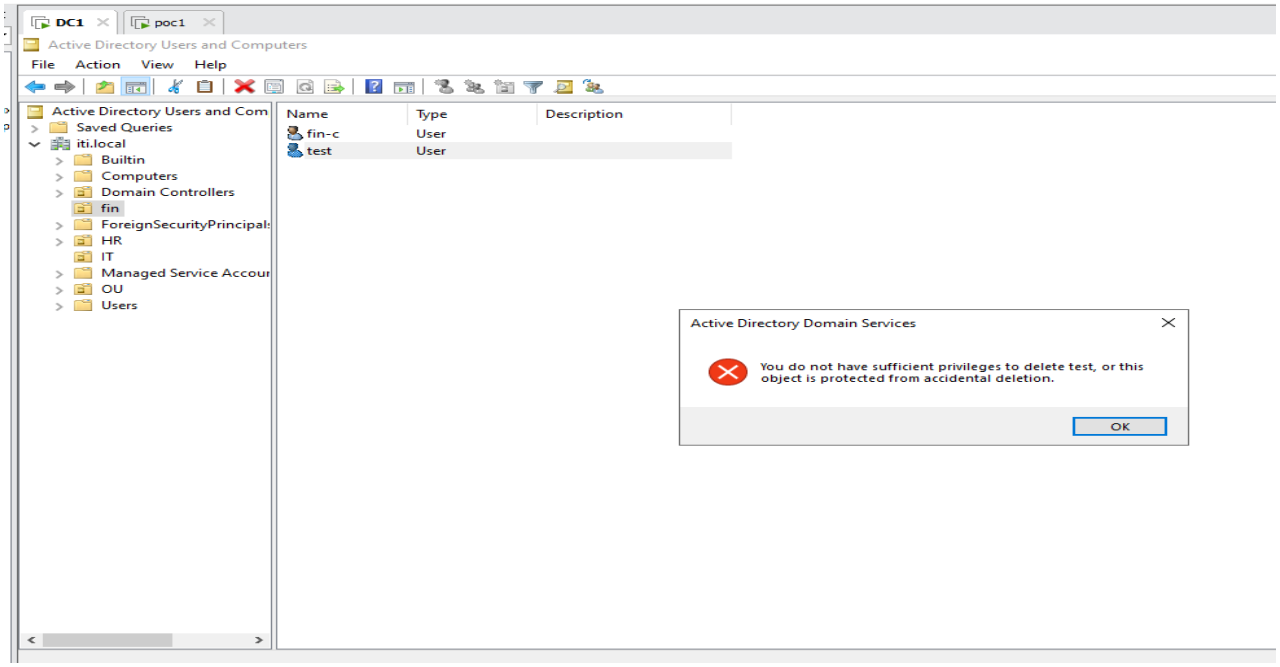
- **Delegated Administrator Account:** The user help@ITI.local was designated as the local administrator for the RODC. This allows the user to manage the server (updates, troubleshooting) without granting them permissions over the entire forest.
- **Password Replication Policy (PRP):** To ensure that the help user can authenticate locally even if the connection to the Primary Domain Controller (DC1) is lost, the account was explicitly added to the "Allowed RODC Password Replication Group".

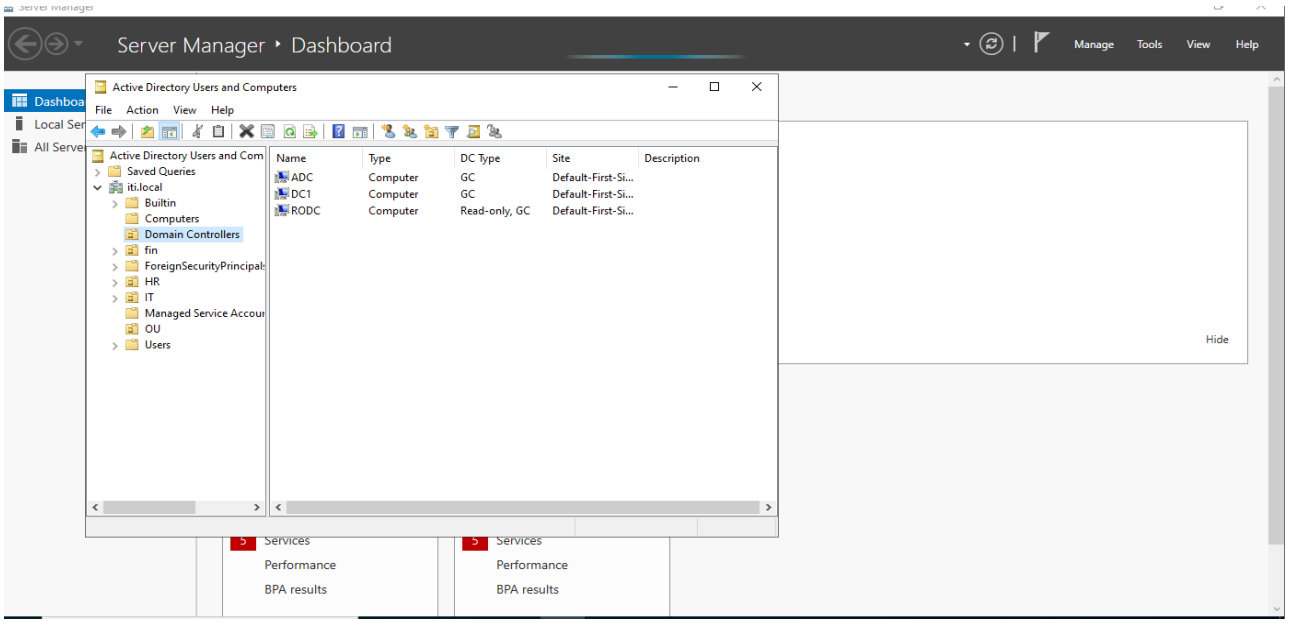
- **Security Hardening:** By default, high-privilege groups (e.g., Administrators, Server Operators) are placed in the "Denied" replication list. This ensures that even if the RODC is physically stolen, the credentials of the Domain Admins are not stored on its drive.

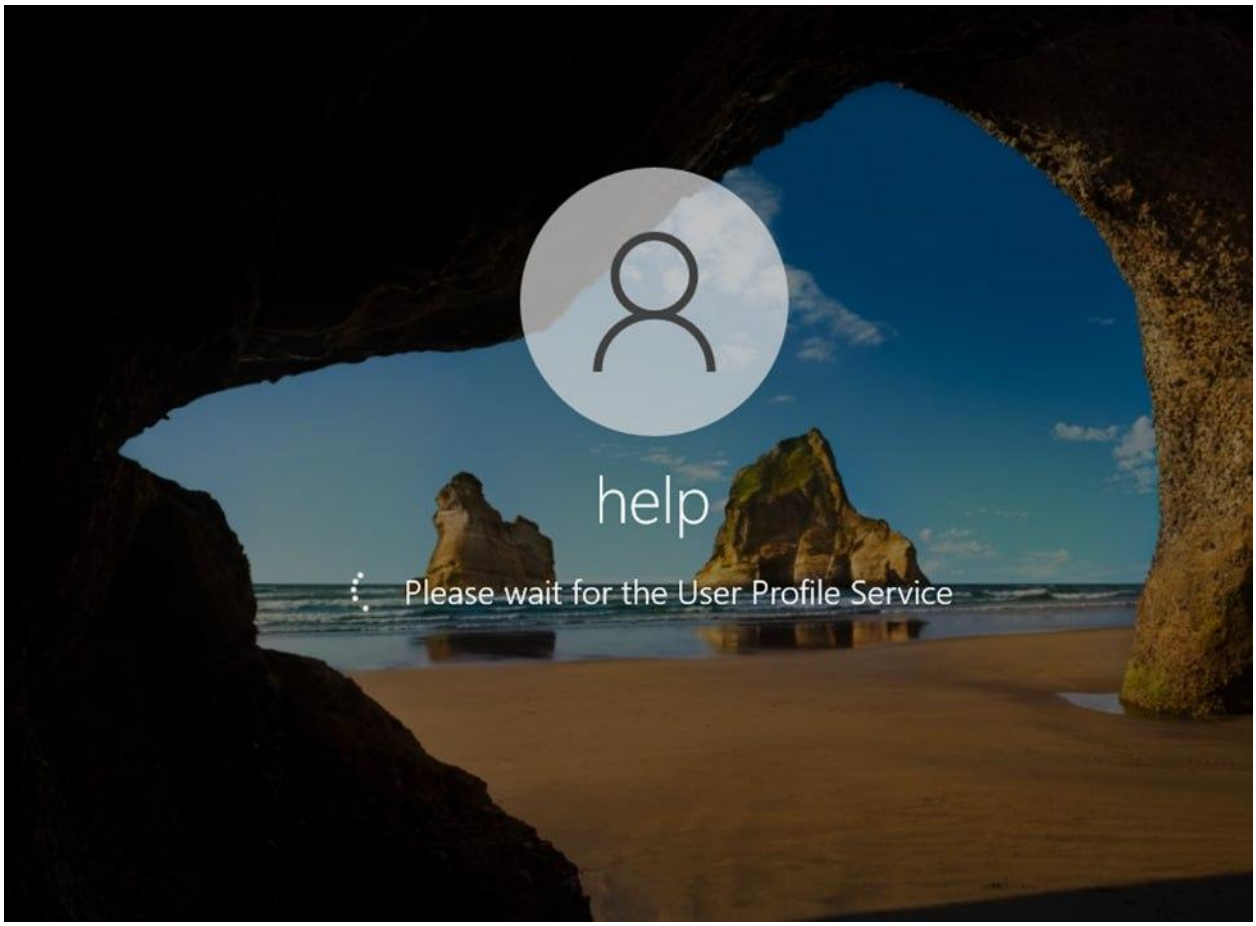
And it can be seen from the screens that the user help cannot delete or add any user as it doesn't have the administrative privileges




Active Directory Domain Services Configuration Wizard
RODC Options
TARGET SERVER
RODC
Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Delegated administrator account
ITI\help
Clear
Select...
Accounts that are allowed to replicate passwords to the RODC
ITI\Allowed RODC Password Replication Group
ITI\help
Add...
Remove
Accounts that are denied from replicating passwords to the RODC
BUILTIN\Administrators
BUILTIN\Server Operators
BUILTIN\Backup Operators
Add...
Remove
If the same account is both allowed and denied, denied takes precedence.
More about RODC options
< Previous
Next >
Install
Cancel


DC1
poc1
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
iti.local
Builtin
Computers
Domain Controllers
fin
ForeignSecurityPrincipals
HR
IT
Managed Service Accour
OU
Users
Name
Type
Description
fin-c
User
test
User
Active Directory Domain Services
You do not have sufficient privileges to delete test, or this object is protected from accidental deletion.
OK


Server Manager ‣ Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
iti.local
Builtin
Computers
Domain Controllers
fin
ForeignSecurityPrincipal
HR
IT
Managed Service Accou
OU
Users
Name
Type
DC Type
Site
Description
ADC
Computer
GC
Default-First-Si...
DC1
Computer
GC
Default-First-Si...
RODC
Computer
Read-only, GC
Default-First-Si...
Hide
Services
Performance
BPA results
Services
Performance
BPA results


help
Please wait for the User Profile Service

3. Web Services (IIS) Implementation

Server Role: IIS Web Server Hosting Multiple Sites on Single IP (Host Headers)

3.1 Role Configuration

The Internet Information Services (IIS) role was deployed to support the organization's requirement for two distinct web portals.

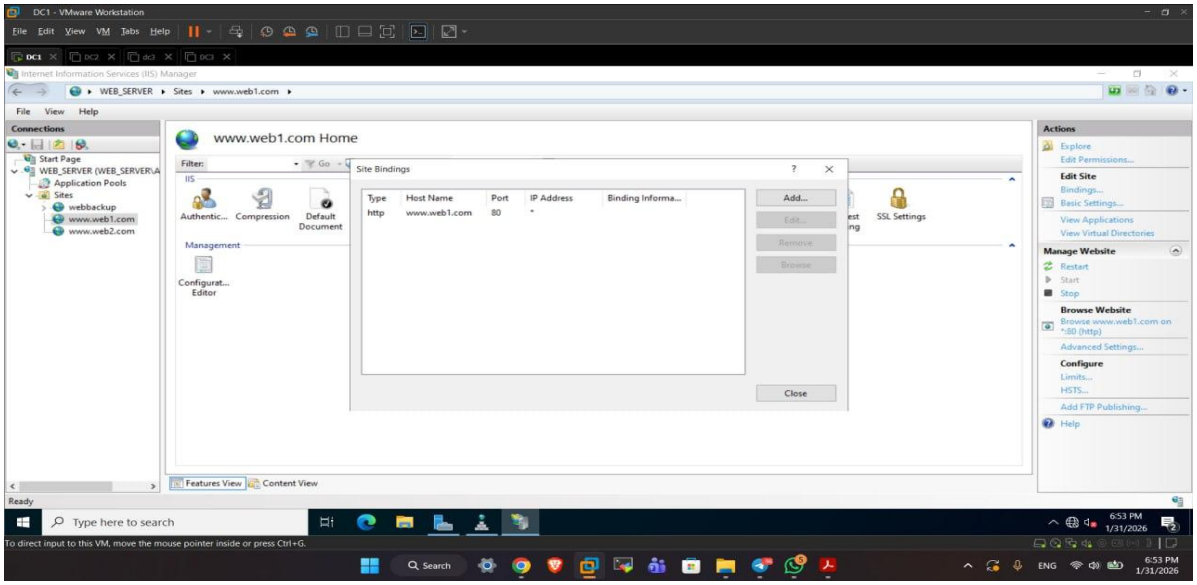
- **Static Content:** Directory browsing was disabled for security.
- **Default Documents:** Configured index.html as the primary landing page for both sites.

3.2 Website Configuration

We configured two separate sites pointing to different physical directories on the server:

- **Site A:** Web1 (Public HTTP)
  - **Site Name:** www.web1.com
  - **Physical Path:** C:\MyWebsites\web1
  - **Binding:** Port 80 (HTTP)
  - **Access Level:** Anonymous Authentication enabled.

- **Site B:** Web2
  - **Site Name:** www.web2.com
  - **Physical Path:** C:\MyWebsites\web2
  - **Binding:** Port 80

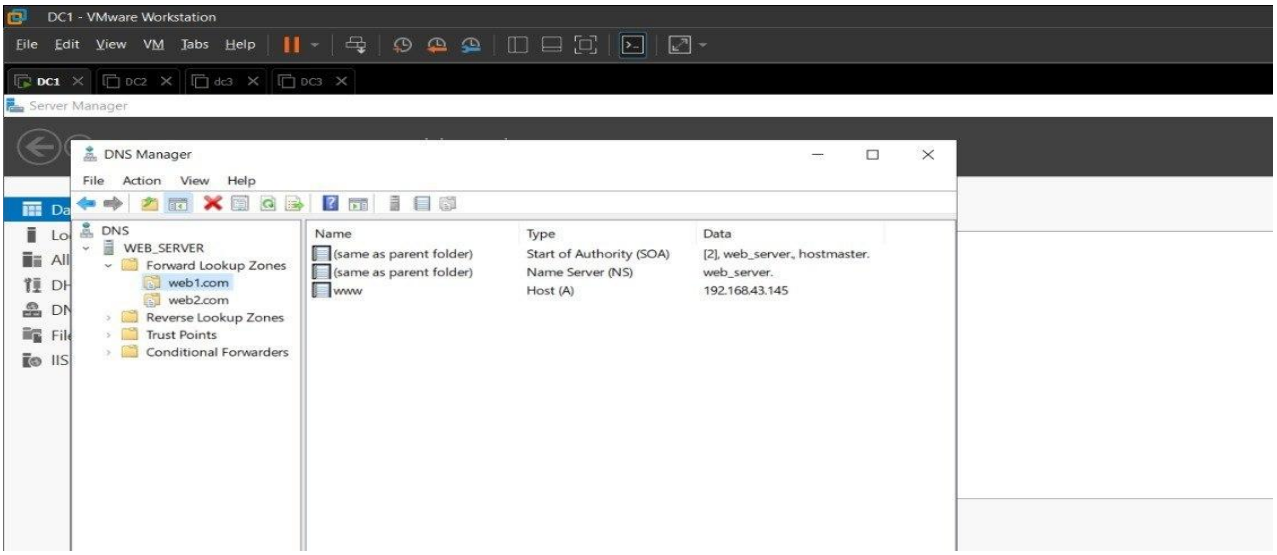


4. Network Services (DNS & DHCP)

4.1 DNS Configuration

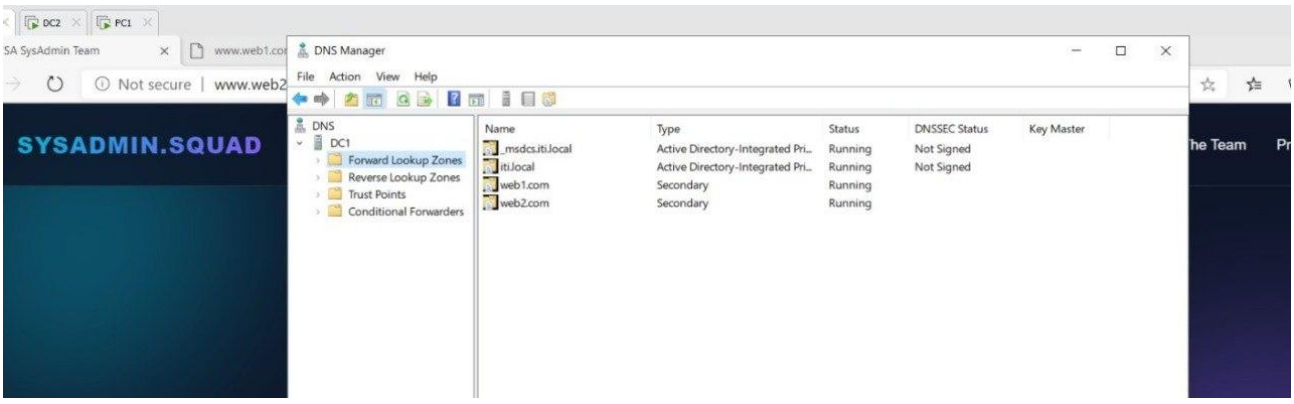
Primary DNS Server:

A Primary DNS server was configured to host the main DNS zones for www.web1.com and www.web2.com. This server is responsible for storing and managing the original zone records, handling name resolution, and processing updates related to both website



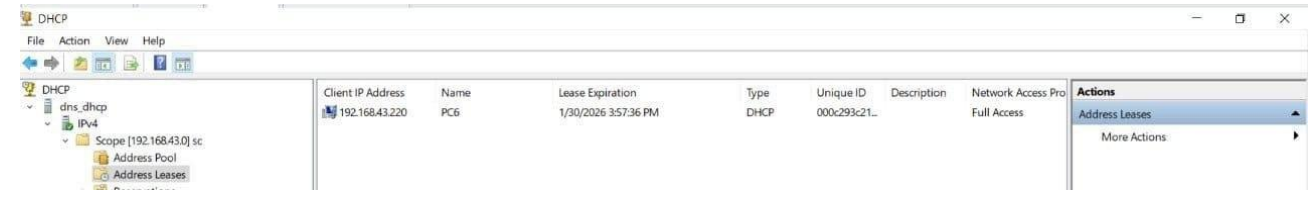
Secondary DNS Server:

A Secondary DNS server was deployed on a separate machine (DC1) to provide redundancy and fault tolerance. It receives zone copies from the Primary DNS server through zone transfer, ensuring continuous availability and load distribution in case the primary server becomes unavailable.



4.2 DHCP Scope Implementation

A DHCP server was configured on the same machine hosting the Primary DNS server. The DHCP service is dedicated to assigning IP configuration to PC6 only, and it automatically provides the Primary DNS server address as the DNS resolver to ensure proper name resolution.




```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : PC6
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-3C-21-F2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.43.220(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, January 29, 2026 3:57:36 PM
   Lease Expires . . . . . . . . . . : Friday, January 30, 2026 3:57:35 PM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.43.239
   DNS Servers . . . . . . . . . . . : 192.168.43.145
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Administrator>
```

5. Automation & Mass Deployment

5.1 Mass User Creation

The purpose of this step is to automate the creation of 50 domain users in Active Directory using a PowerShell script. This approach reduces manual effort, ensures naming consistency, and minimizes configuration errors.

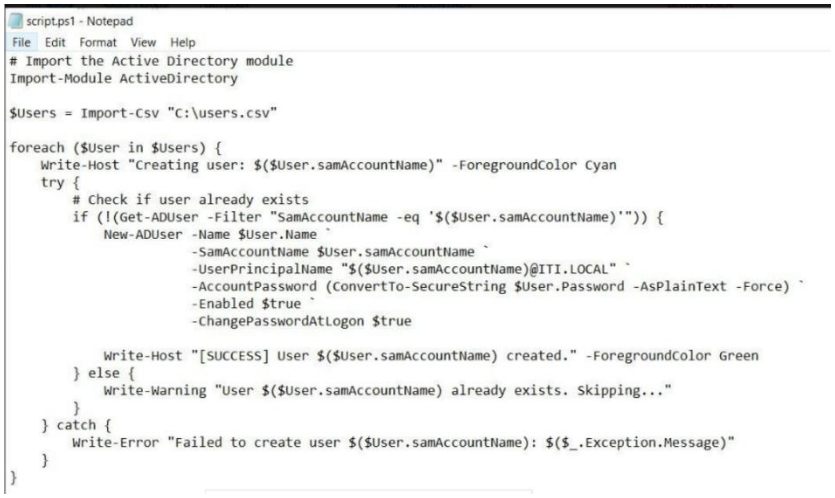
◆ Script Explanation

PowerShell script was used to generate 50 user accounts automatically in the iti.local domain.

The script performs the following actions:

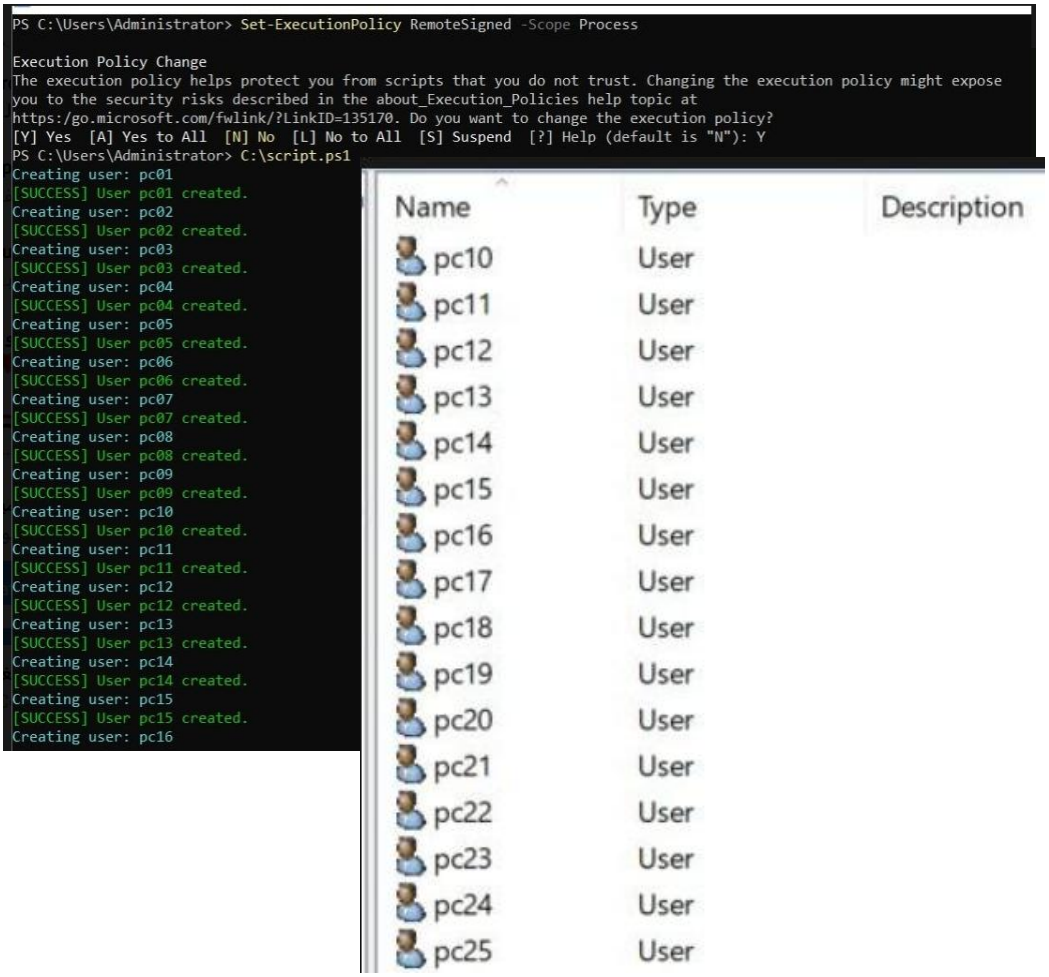
- Connects to Active Directory using the ActiveDirectory PowerShell module.
- Creates 50 user accounts with a predefined naming convention (e.g., pc01 to pc50).
- **Existence Check:** It runs Get-ADUser to see if the SamAccountName (the login ID) already exists in your network.
- If the user doesn't exist, it uses New-ADUser with several parameters:
  - **UserPrincipalName:** Sets the login email format (pc01@iti.local).
  - **AccountPassword:** Converts the plain text password from your CSV into a "Secure String" so Windows can handle it safely.
  - **ChangePasswordAtLogon $true:** Forces the new employee to pick a new password the first time they sign in.
  - Enables the user accounts after creation.

Script:



```
samAccountName,Name,Password
pc01,pc01,iti@iti1
pc02,pc02,iti@iti1
pc03,pc03,iti@iti1
pc04,pc04,iti@iti1
pc05,pc05,iti@iti1
pc06,pc06,iti@iti1
pc07,pc07,iti@iti1
pc08,pc08,iti@iti1
pc09,pc09,iti@iti1
```

AD Users showing the list of 50 created users:



5.2 Windows Deployment Services (WDS)

Environment: Windows Server 2022 (DHCP/WDS)
Target OS: Windows 10

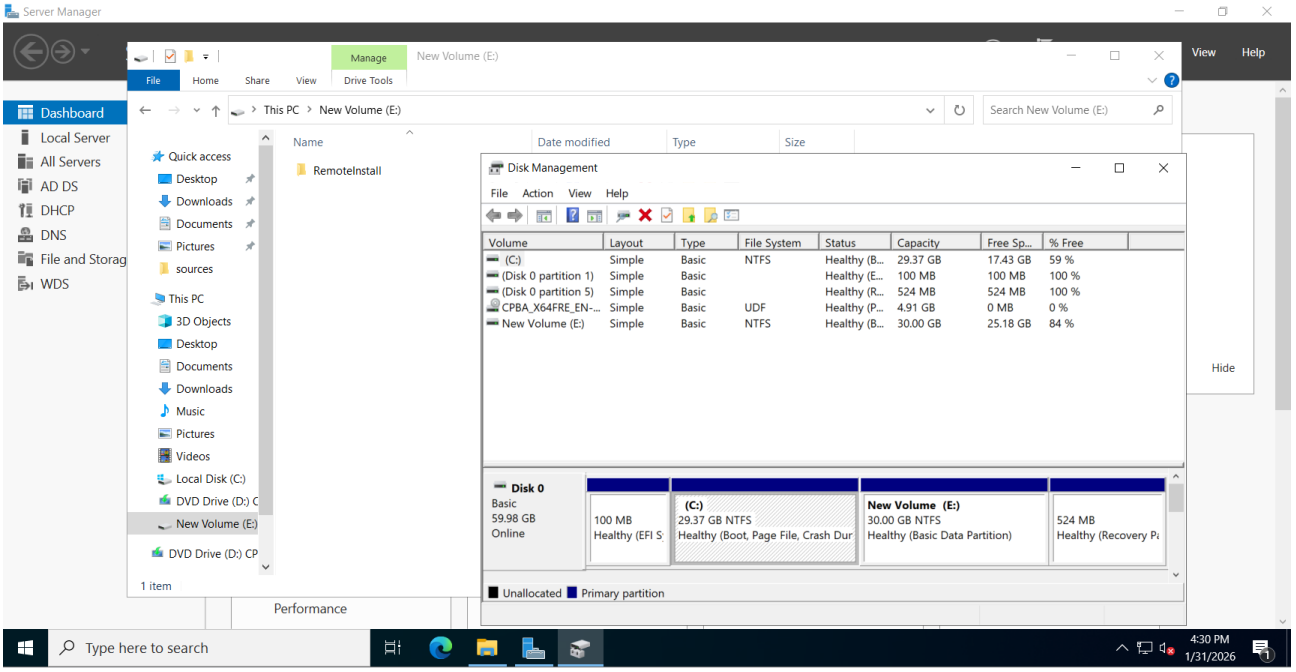
◆ Phase 1: Infrastructure Prerequisites

Before WDS can be initialized, the following infrastructure must be verified:

1.1 Dedicated Storage (NTFS)

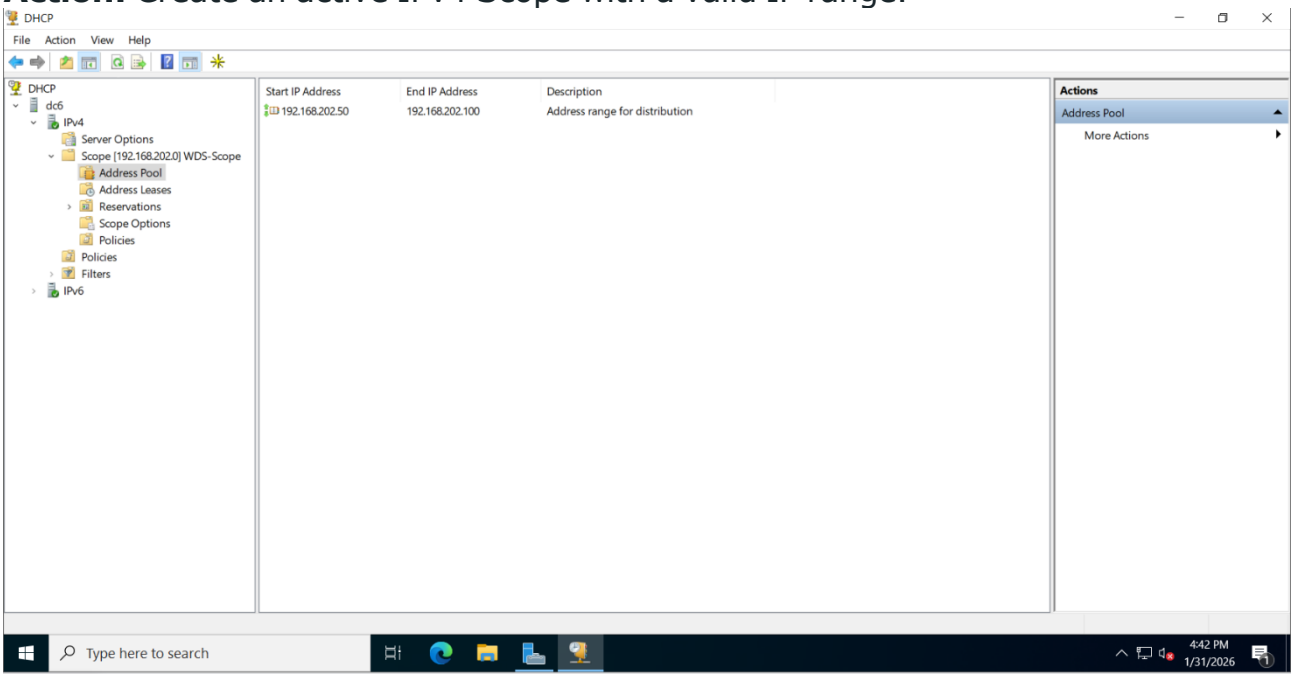
Requirement: WDS images cannot reside on the C: drive.

Step: Use Disk Management to create a new NTFS volume (e.g., E:\RemoteInstall).

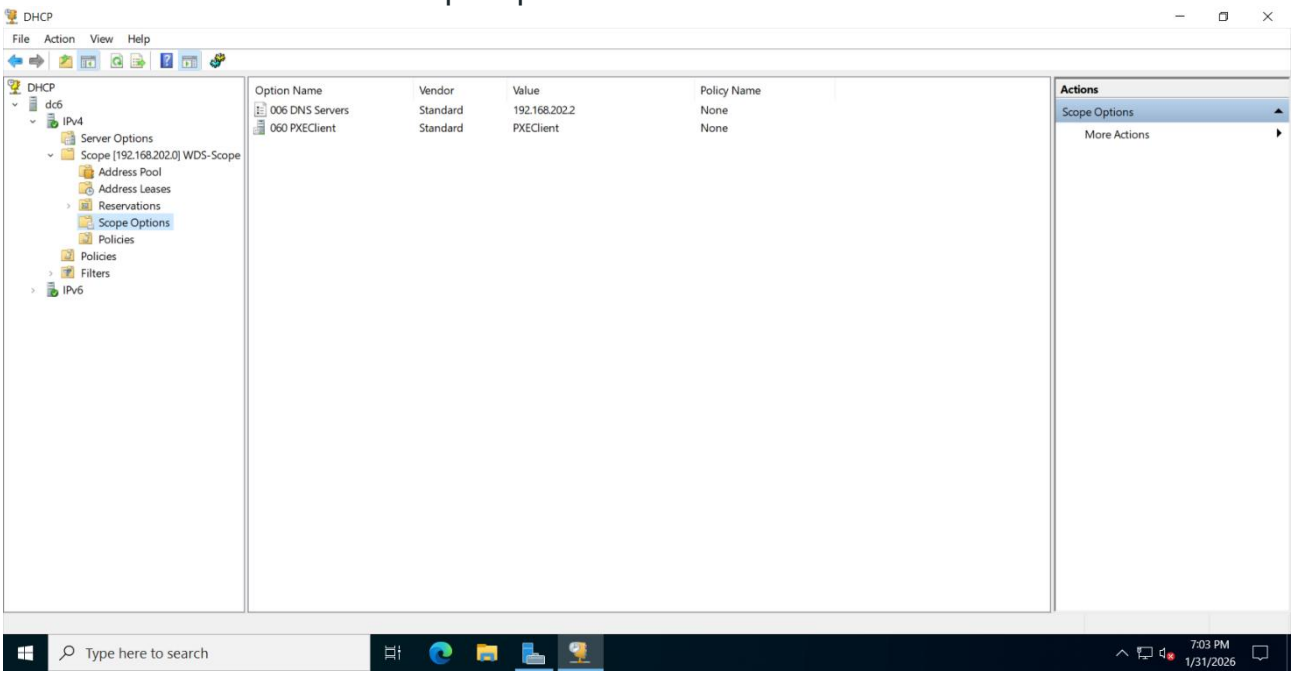


1.2 DHCP Configuration

Action: Create an active IPv4 Scope with a valid IP range.



Constraint: Ensure the Scope Options include the DNS Server IP.



◆ Phase 2: WDS and DHCP Coexistence (Same Server)

Because both services use Port 67, these steps are mandatory to prevent service failure.

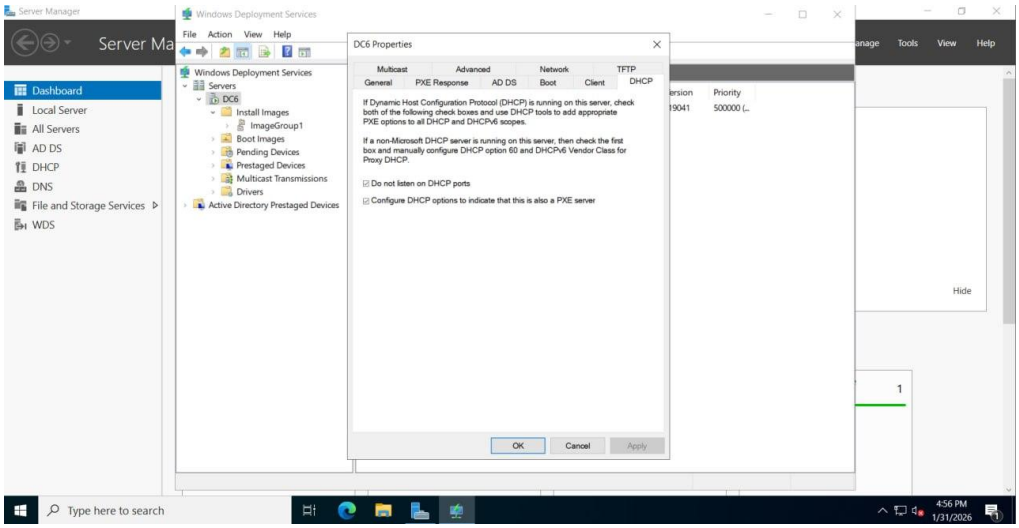
2.1 Install the WDS Role

1. Open Server Manager > Add Roles and Features.

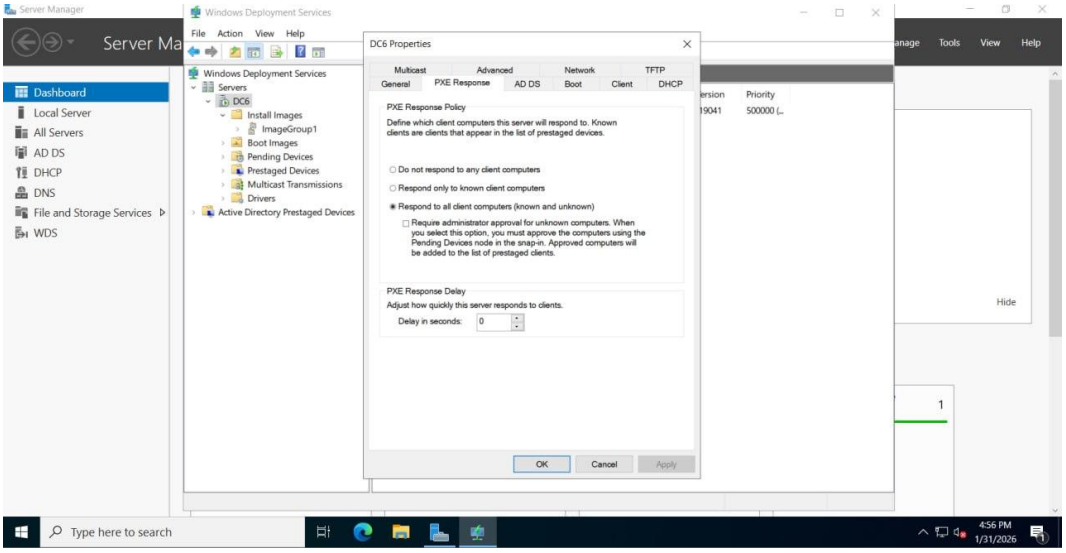
2. Select Windows Deployment Services.

2.2 Configure Port Exclusion & Option 60

1. Open WDS Console > Right-click Server > Properties.
2. Navigate to the DHCP tab.
3. Check: Do not listen on DHCP and DHCPv6 ports (Port 67).
4. Check: Configure DHCP options for ProxyDHCP (Option 60).



5. Navigate to PXE Response tab > Select Respond to all client computers.

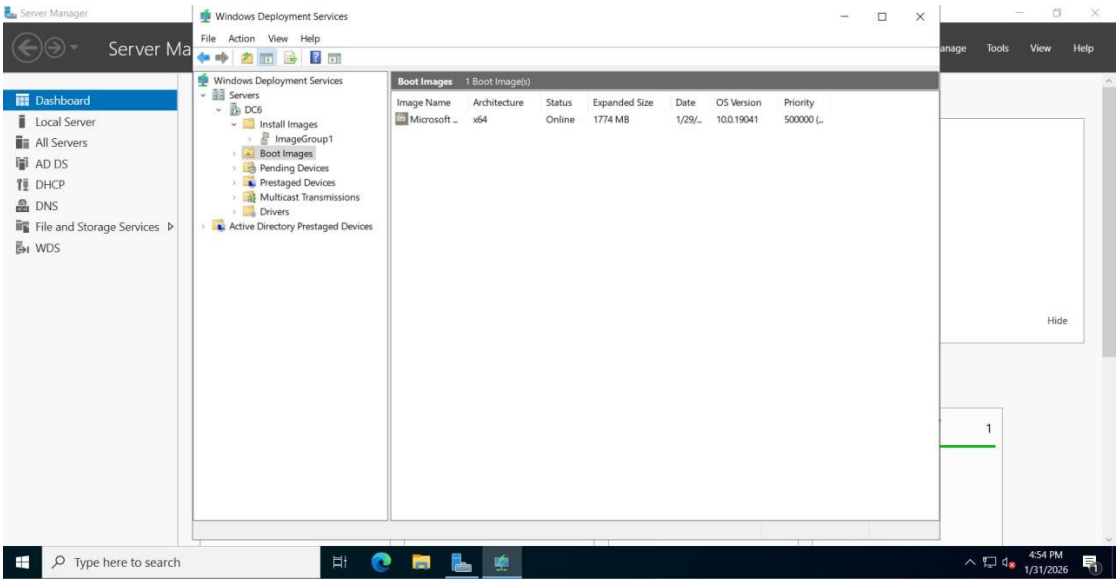


◆ Phase 3: WDS Post-Installation Configuration

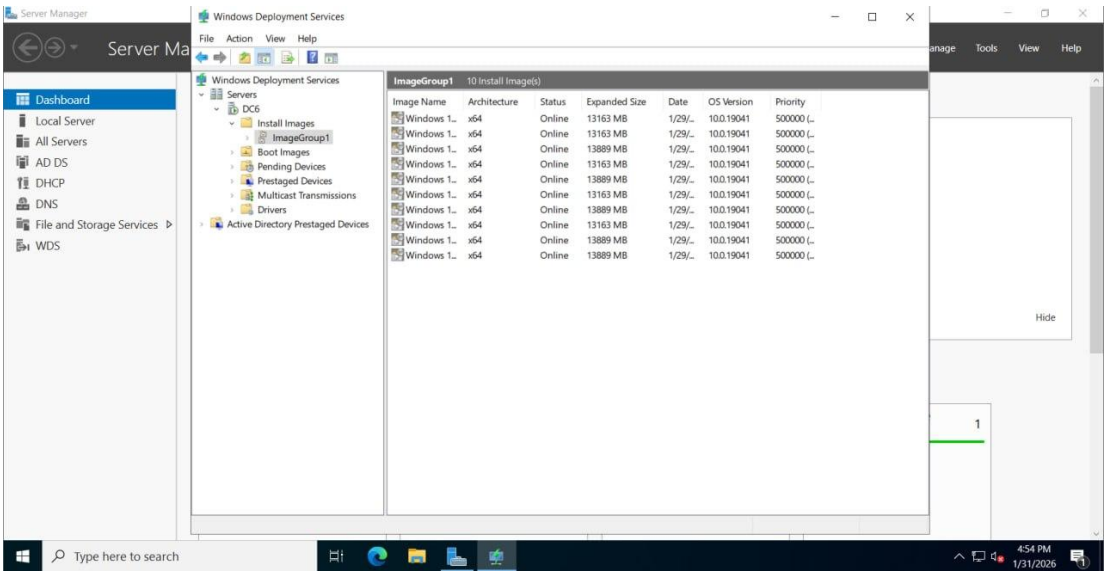
Once the roles are set, the server must be initialized to hold the OS files.

Adding Boot and Install Images

1. Mount the Windows 10 ISO.
2. Boot Image: Right-click Boot Images > Add Boot Image > Browse to \sources\boot.wim.

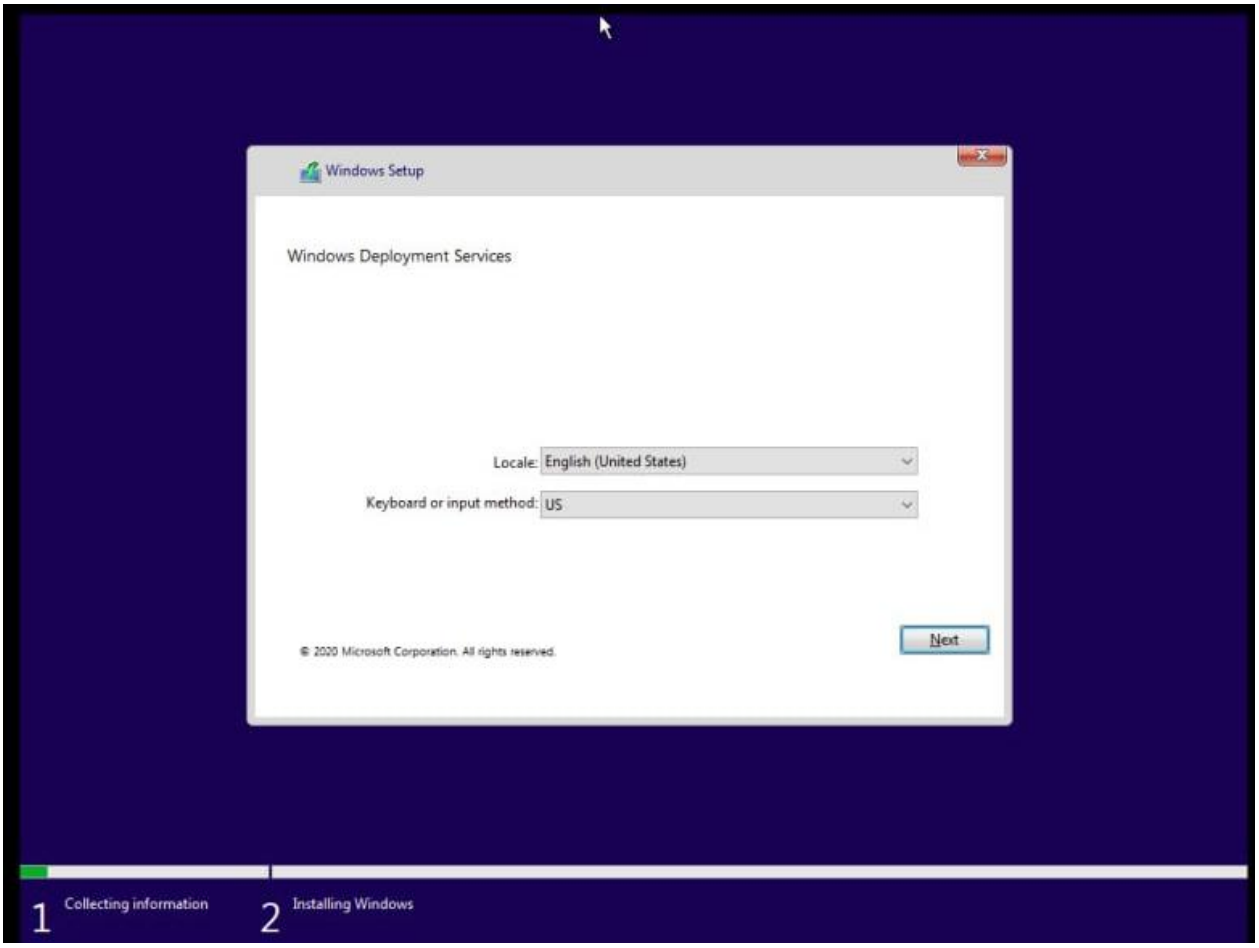


3. Install Image: Right-click Install Images > Add Image Group > Add Install Image > Browse to \sources\install.wim.



◆ Phase 4: Client Execution

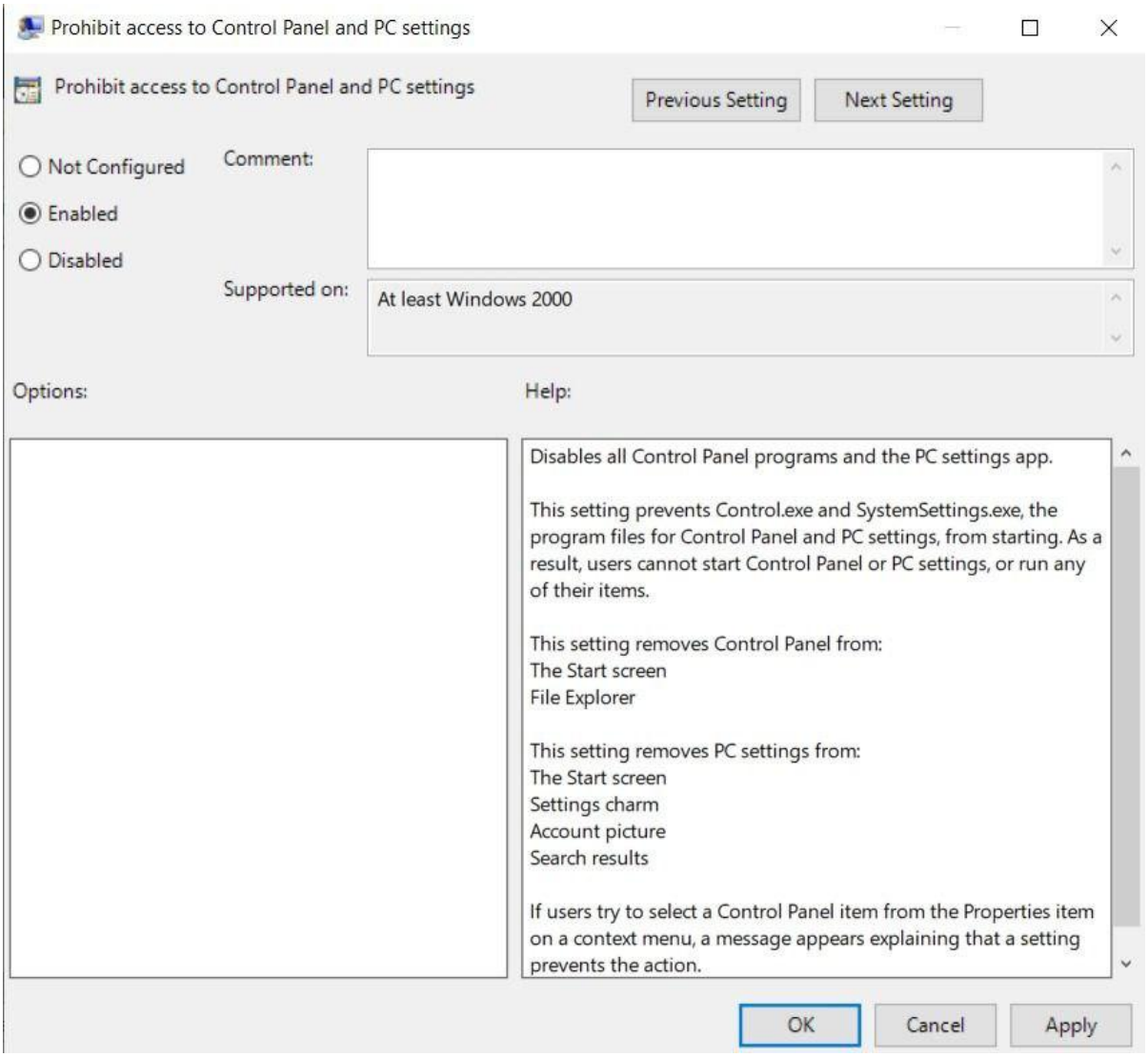
1. Boot the Windows 10 PC.
2. Enter BIOS/UEFI and enable Network Boot (PXE).
3. Press F12 on startup to initiate the WDS boot process.



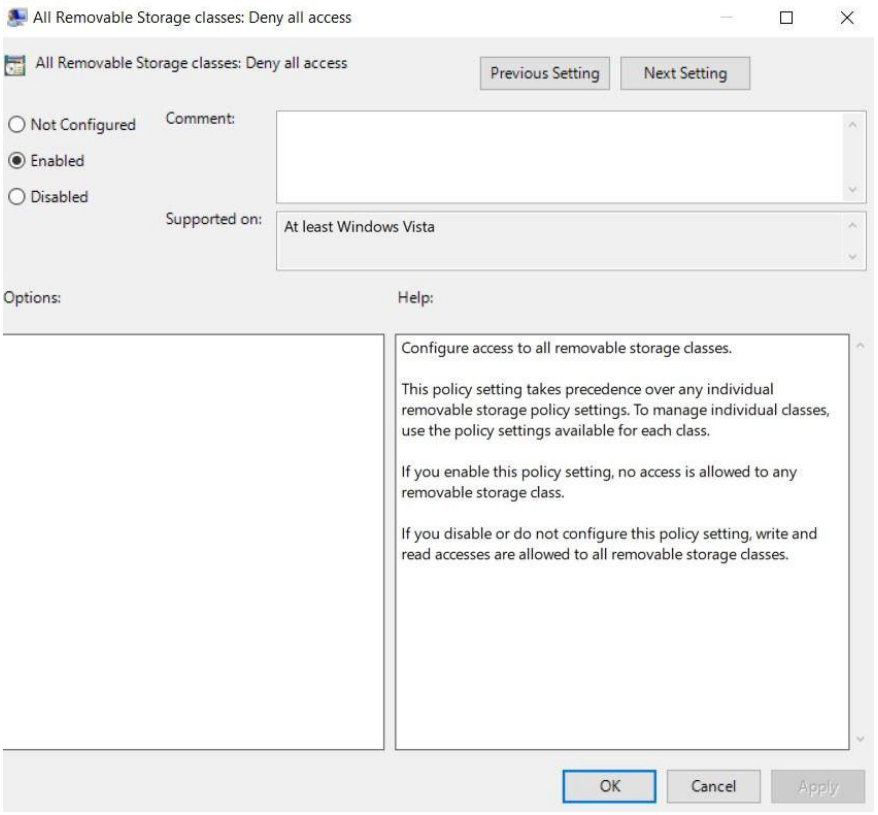
6. Group Policy & Client Management

6.1 Security Restrictions (User fin-c)

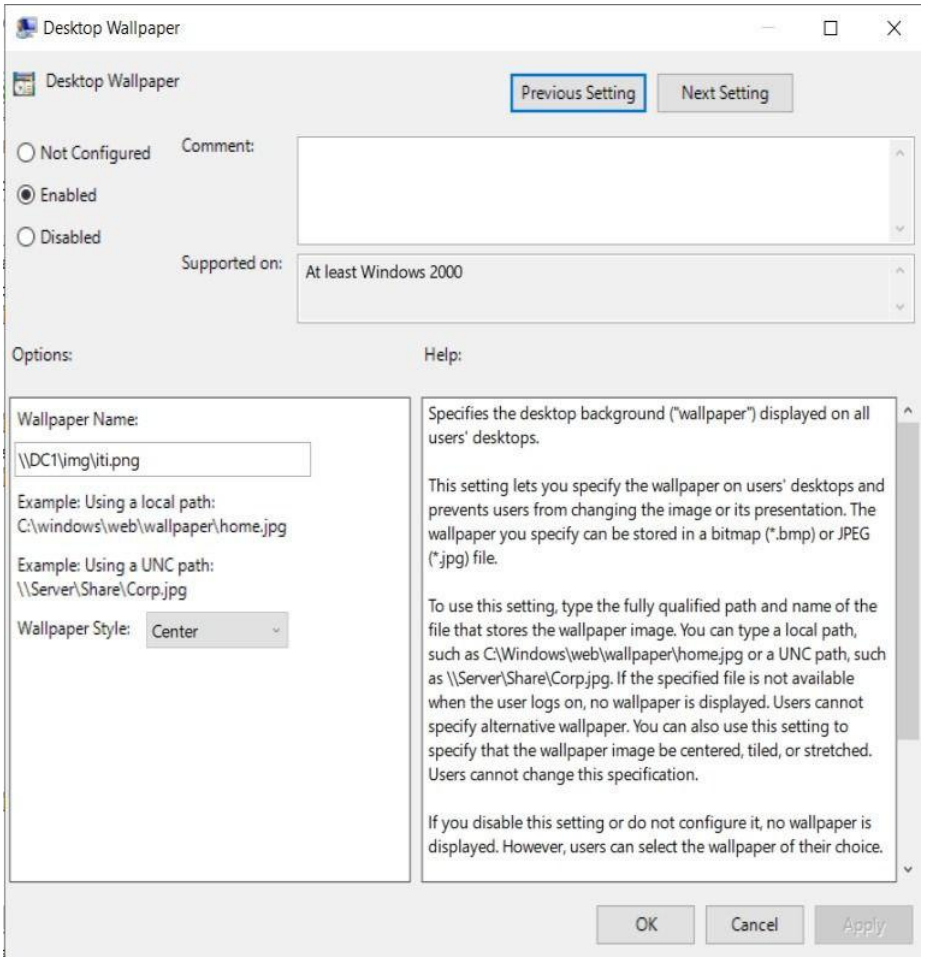
- Prevent Access to Control Panel.



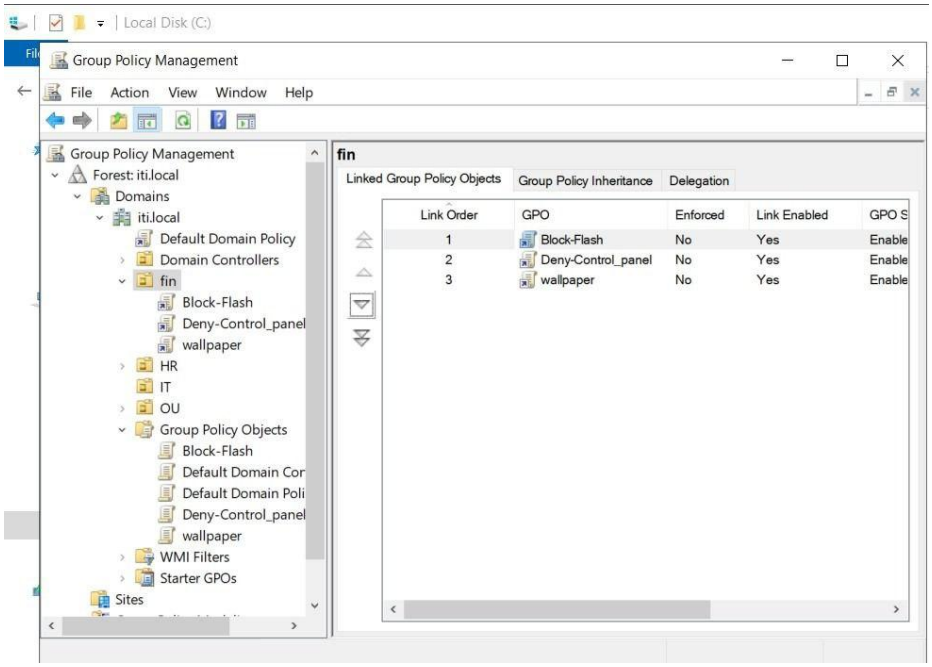
- Prevent Access to Flash Memory (Removable Storage)



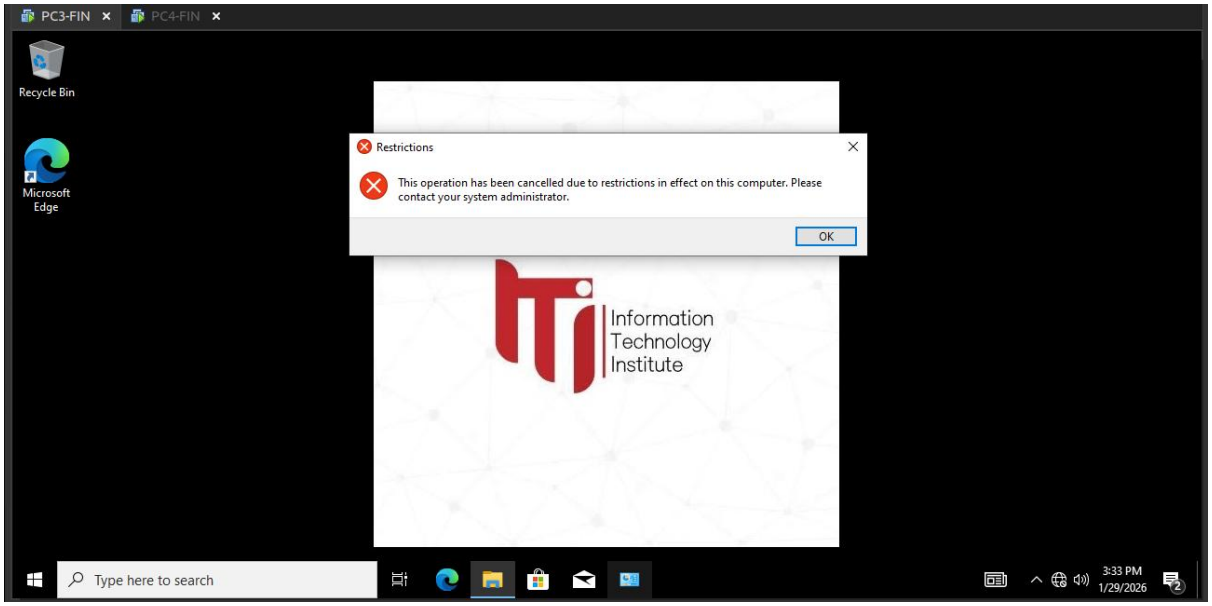
- Enforce ITI Logo Wallpaper.

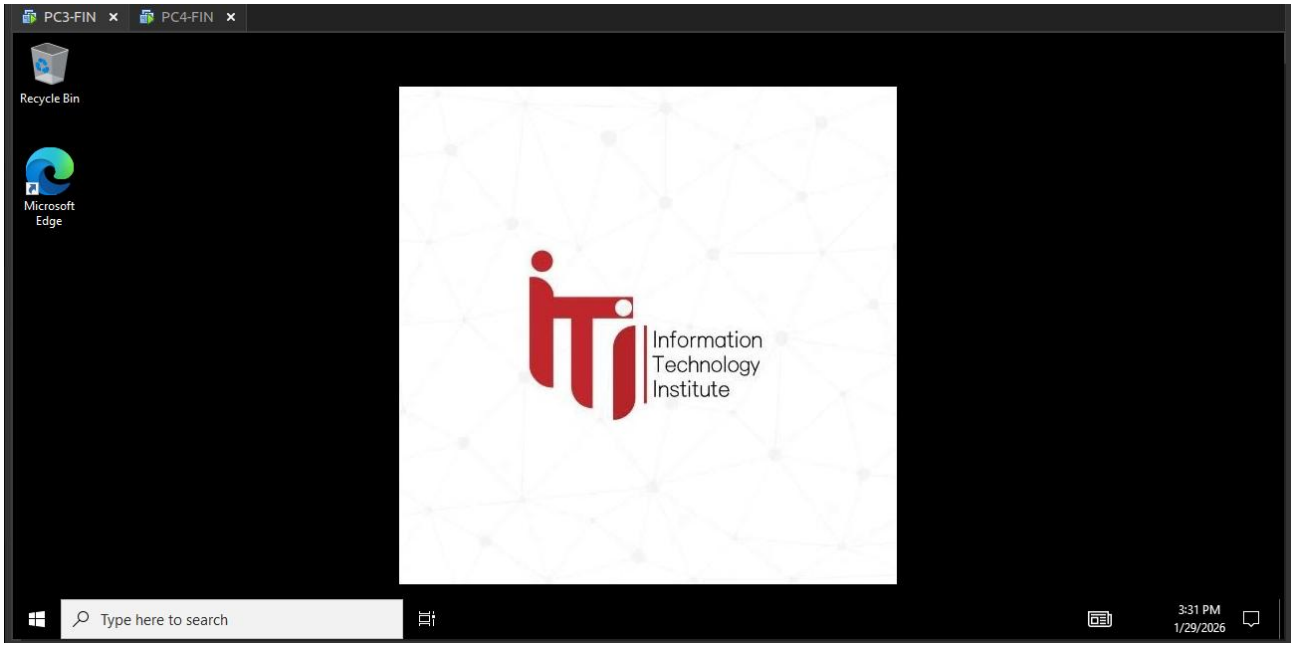


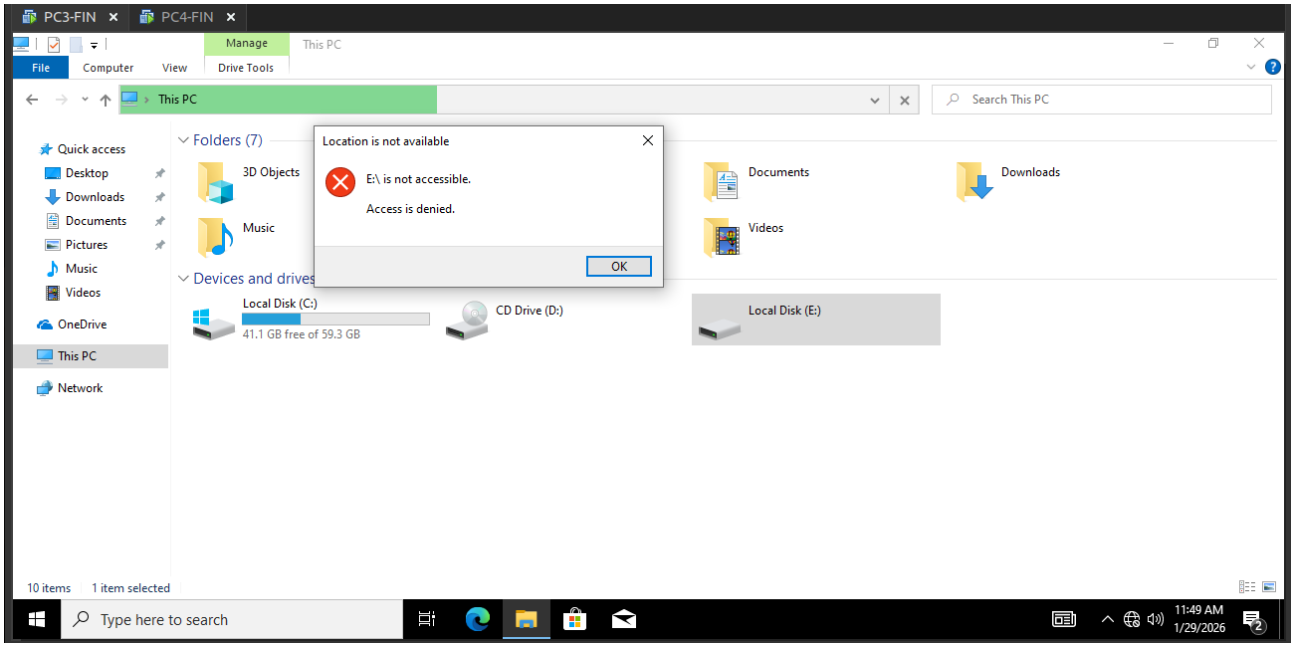
Linked the GPO to the specific On U fin that contains User fin-c



The Client PC logged in as fin-c@iti.local




PC3-FIN
PC4-FIN
Recycle Bin
Microsoft Edge
Information Technology Institute
Type here to search
3:31 PM
1/29/2026


PC3-FIN
PC4-FIN
Manage
This PC
File
Computer
View
Drive Tools
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Folders (7)
3D Objects
Documents
Downloads
Music
Videos
Devices and drives
Local Disk (C:)
41.1 GB free of 59.3 GB
CD Drive (D:)
Local Disk (E:)
Location is not available
E:\ is not accessible.
Access is denied.
OK
10 items
1 item selected
Type here to search
11:49 AM
1/29/2026

6.2 Logon Restrictions (User A)

Setup & Configuration: To enhance security and control access across the domain, specific Logon Workstations restrictions were applied to User A:

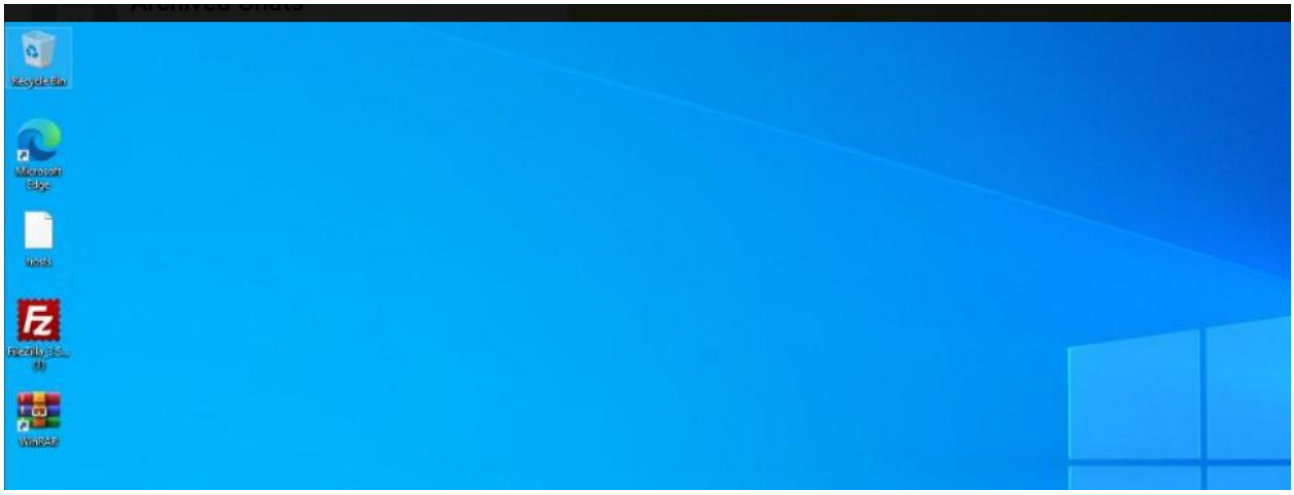
- **Policy:** User A is restricted to logging in only on authorized machines (PC4, PC5, and PC1).
- **Security Benefit:** If User A attempts to log into any other machine (like a Server or a Guest PC), the domain controller will deny the request, even if the password is correct.
- **Result:** Windows displayed an error message stating: "Your account is configured to prevent you from using this PC. Please try another PC."

6.3 Software Deployment (WINRAR.msi)

Setup & Configuration: To automate software management, WinRAR was deployed to PC2 using Group Policy (GPO):

- **Package Preparation:** The WinRAR .msi installer was placed in a shared network folder with Read permissions for "Domain Computers."
- **GPO Creation:** A new Group Policy Object was created and linked to the Organizational Unit (OU) containing PC2.
- **Deployment Policy:** Configured under Computer Configuration > Software Installation as an Assigned package to ensure the software installs automatically during the next system boot.

Verification:



- **Reboot:** PC2 was restarted to trigger the GPO update.
- **Installation Check:** Logged into PC2 and verified that WinRAR appears in

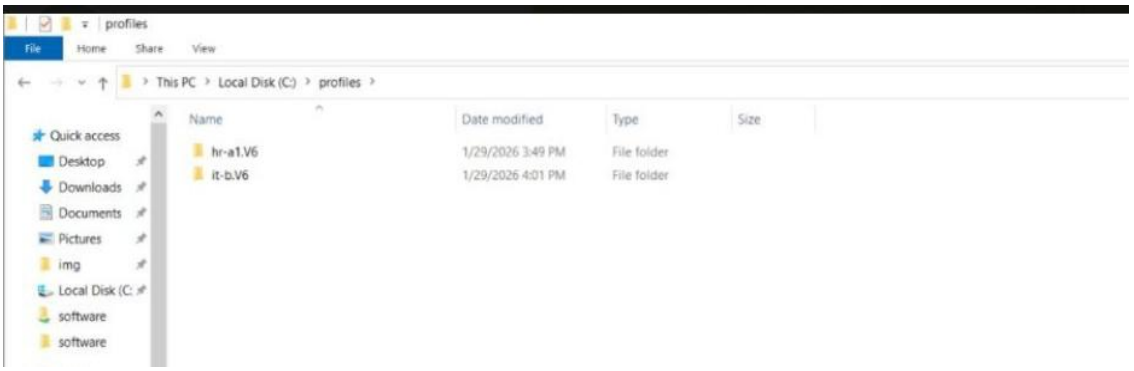
the "Programs and Features" list.

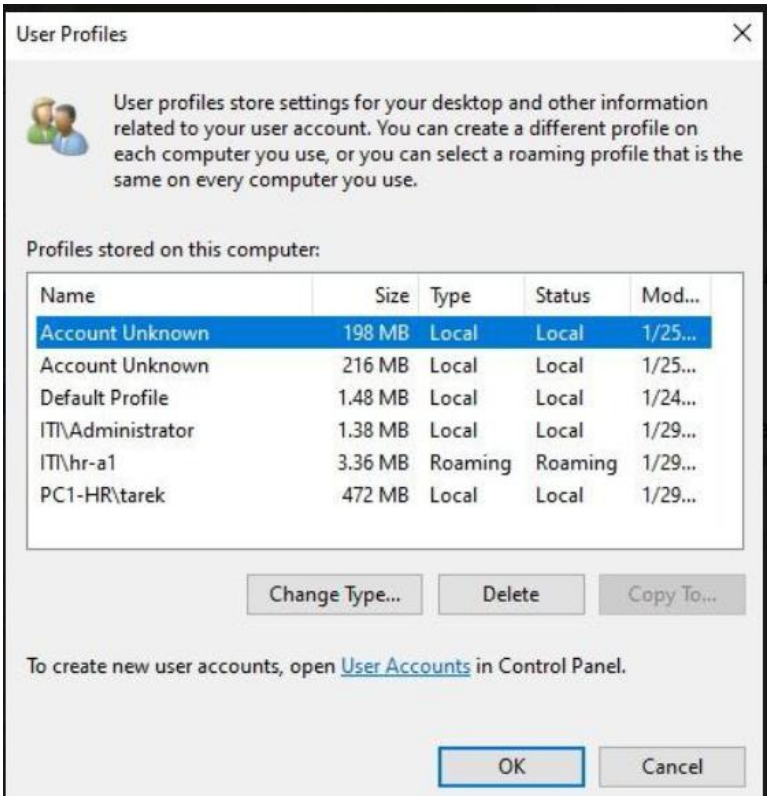
- **Functionality:** Confirmed the application opens and is ready for use by any user logging into that machine.

6.4 Roaming Profiles

Setup & Configuration: To allow User A to access their files from any assigned machine (PC4, PC5, PC1), a Roaming Profile was configured:

- **Network Share:** A central folder was created on the server with shared access.
- **AD Integration:** In Active Directory, the user's "Profile Path" was set to \\<ServerName>\<ShareName>\%username%.
- **Result:** This ensures that when the user logs off, their data (Desktop, Documents, etc.) is saved to the server instead of just the local PC





7. Security Delegation & Remote Access

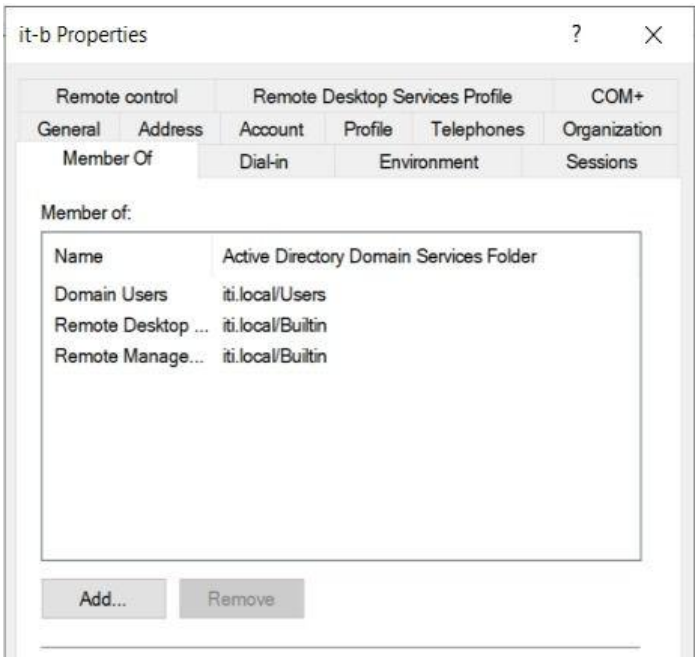
(Responsible: Admin handling User B and User D)

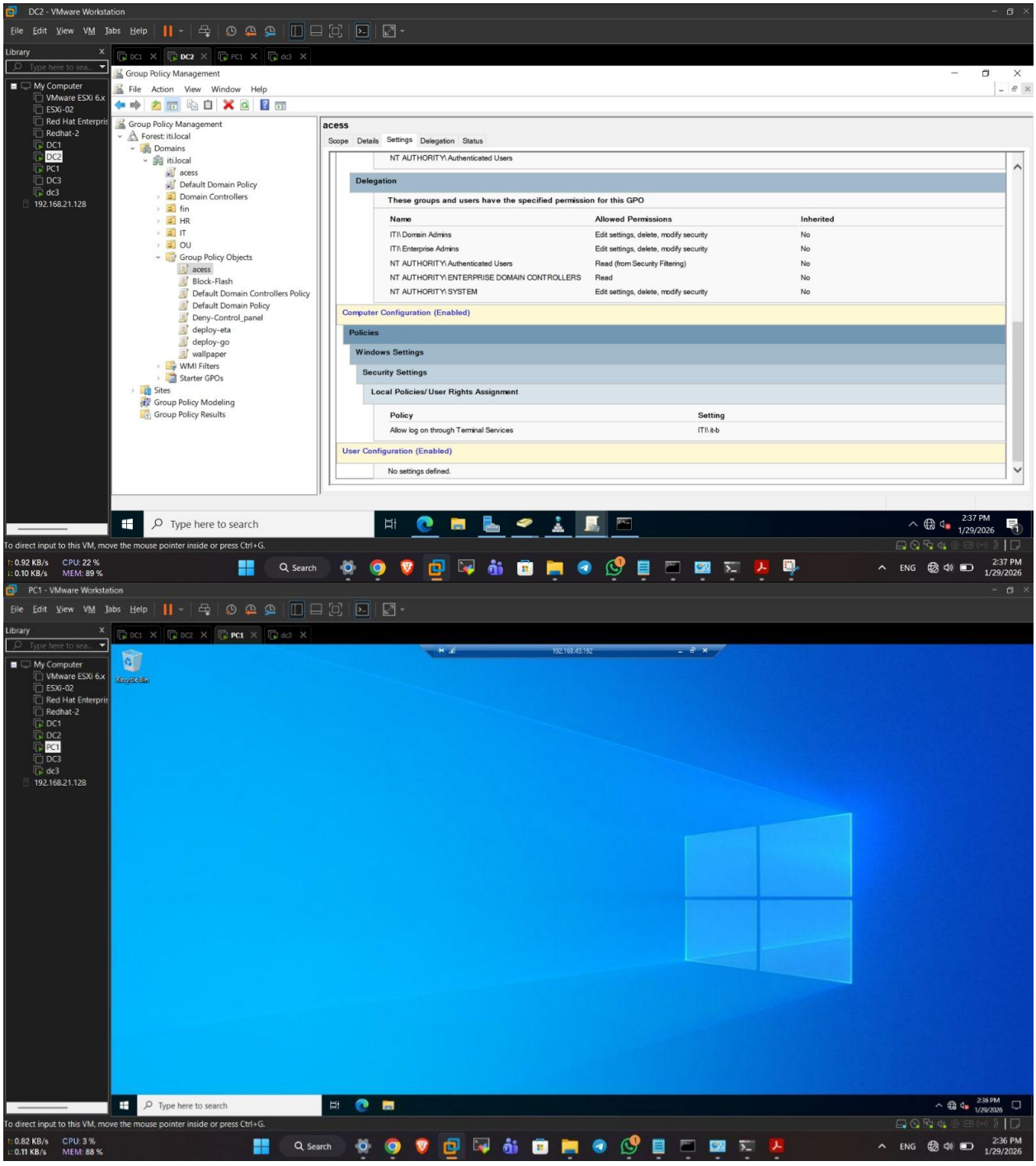
7.1 Server Administration Delegation

To maintain a "least privilege" security model, User B (ITI\it-b) was granted the ability to manage DC1 remotely without being added to the Domain Admins or local Administrators groups.

- **Group Policy Configuration:** A specific Group Policy Object (GPO) named "access" was created and linked within the iti.local domain structure.
- **User Rights Assignment:** Within this GPO, the policy "Allow log on through Terminal Services" (also known as "Allow log on through Remote Desktop Services") was modified.
- **Target Assignment:** The user account ITI\it-b was explicitly added to this policy setting.

Technical Result: This configuration allows User B to establish an RDP session to the Domain Controller to perform authorized tasks while the system continues to deny access to other non-administrative users."

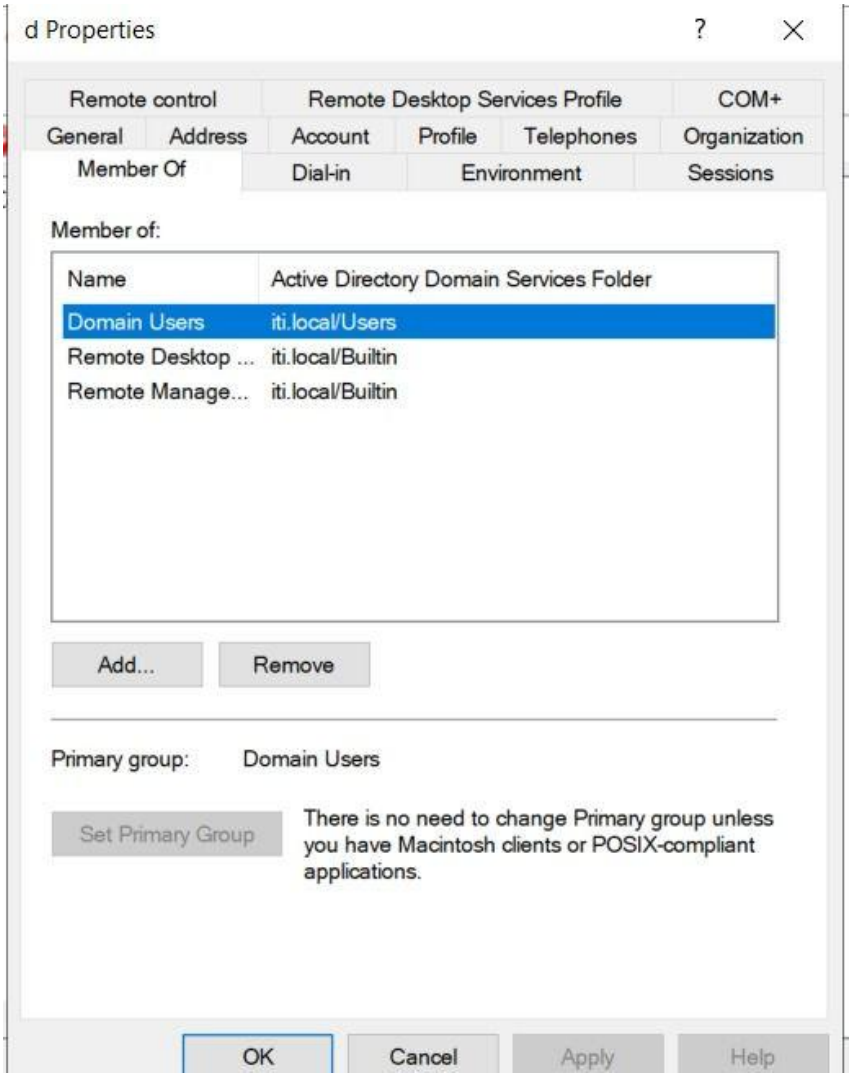


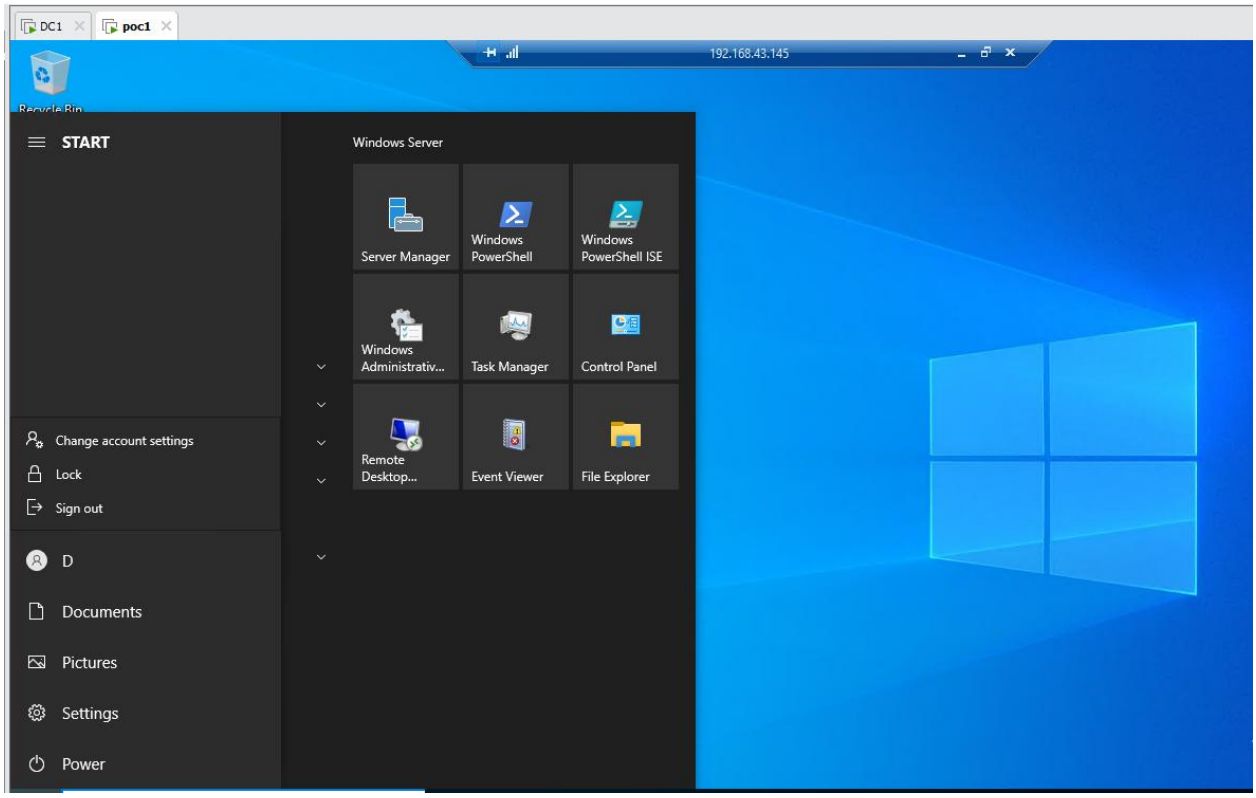

DC2 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
VMware ESXi 6.x
ESXi-02
Red Hat Enterpris
Redhat-2
DC1
DC2
PC1
DC3
dc3
192.168.21.128
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: iti.local
Domains
iti.local
acess
Default Domain Policy
Domain Controllers
fin
HR
IT
OU
Group Policy Objects
acess
Block-Flash
Default Domain Controllers Policy
Default Domain Policy
Deny-Control_panel
deploy-eta
deploy-go
wallpaper
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
acess
Scope Details Settings Delegation Status
NT AUTHORITY\Authenticated Users
Delegation
These groups and users have the specified permission for this GPO
Name
Allowed Permissions
Inherited
ITI\Domain Admins
Edit settings, delete, modify security
No
ITI\Enterprise Admins
Edit settings, delete, modify security
No
NT AUTHORITY\Authenticated Users
Read (from Security Filtering)
No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Read
No
NT AUTHORITY\SYSTEM
Edit settings, delete, modify security
No
Computer Configuration (Enabled)
Policies
Windows Settings
Security Settings
Local Policies/ User Rights Assignment
Policy
Setting
Allow log on through Terminal Services
ITI\it-b
User Configuration (Enabled)
No settings defined.
Type here to search
2:37 PM
1/29/2026
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
0.92 KB/s
0.10 KB/s
CPU: 22 %
MEM: 89 %
Search
ENG
2:37 PM
1/29/2026
PC1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
VMware ESXi 6.x
ESXi-02
Red Hat Enterpris
Redhat-2
DC1
DC2
PC1
DC3
dc3
192.168.21.128
Recycle Bin
Type here to search
2:36 PM
1/29/2026
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
0.82 KB/s
0.11 KB/s
CPU: 3 %
MEM: 88 %
Search
ENG
2:36 PM
1/29/2026

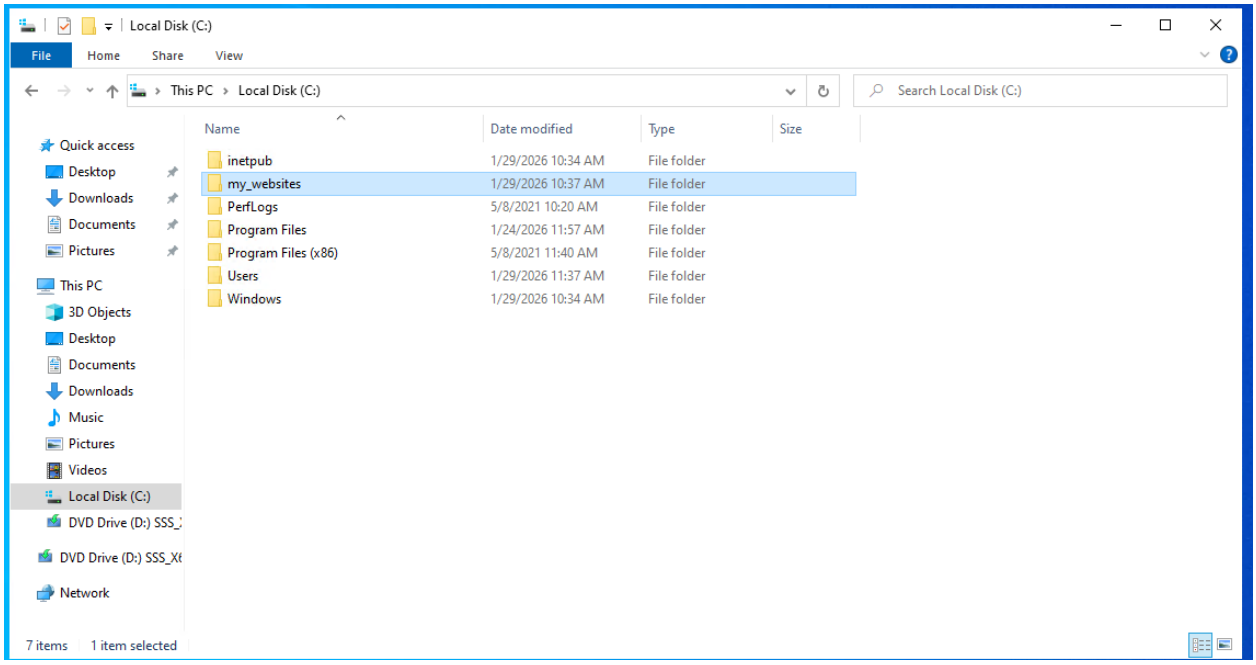
7.2 Web Server Administration (User D)

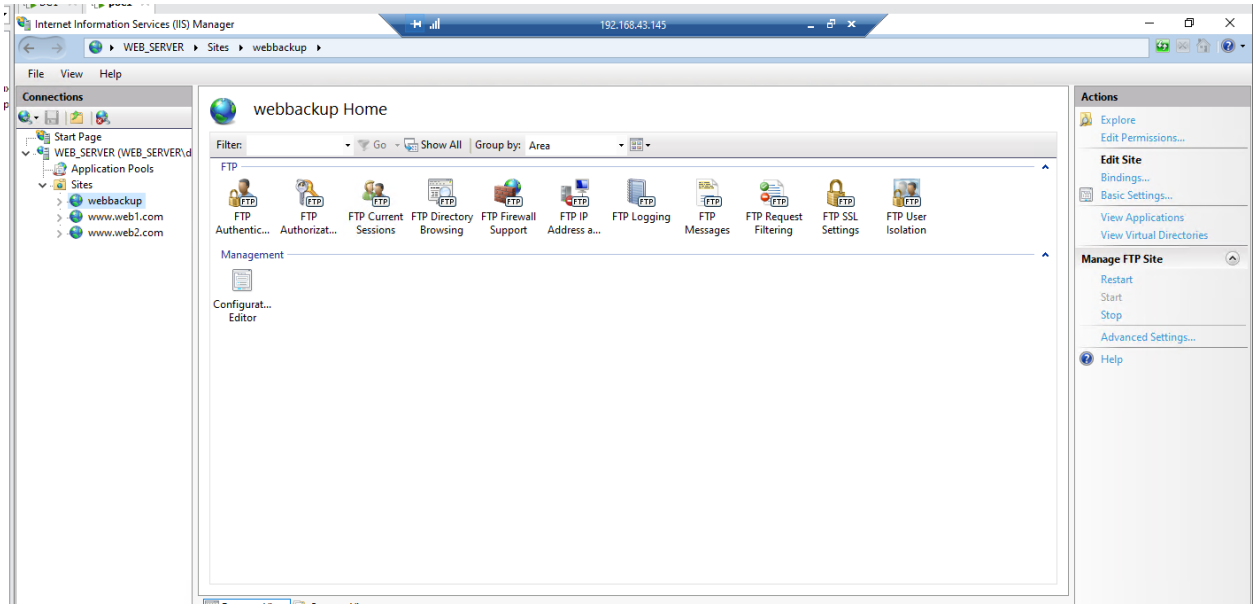
User D is responsible for the remote administration of the Windows Server infrastructure, specifically targeting the Web Server environment.

- **Access Credentials:** D operates as a local user on pc6 but maintains authorized access to manage the Web Server remotely via RDP.
- **Establishment of Session:** RDP sessions are established using the destination IP address 192.168.43.145.
- **Administrative Interface:** Upon successful connection, D has access to the Server Manager and Windows Administrative Tools to perform system-level configurations




DC1
poc1
192.168.43.145
Recycle Bin
START
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer
Change account settings
Lock
Sign out
D
Documents
Pictures
Settings
Power

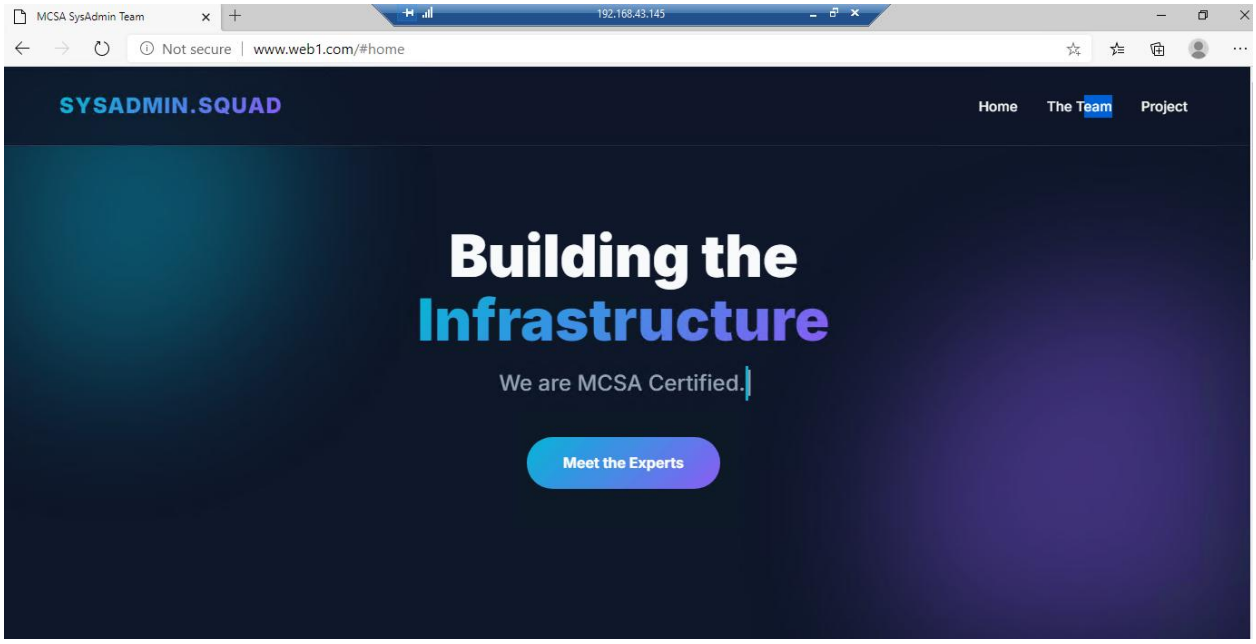

Local Disk (C:)
File
Home
Share
View
This PC
Local Disk (C:)
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
DVD Drive (D:) SSS_X
Network
Name
Date modified
Type
Size
inetpub 1/29/2026 10:34 AM File folder
my_websites 1/29/2026 10:37 AM File folder
PerfLogs 5/8/2021 10:20 AM File folder
Program Files 1/24/2026 11:57 AM File folder
Program Files (x86) 5/8/2021 11:40 AM File folder
Users 1/29/2026 11:37 AM File folder
Windows 1/29/2026 10:34 AM File folder
7 items
1 item selected

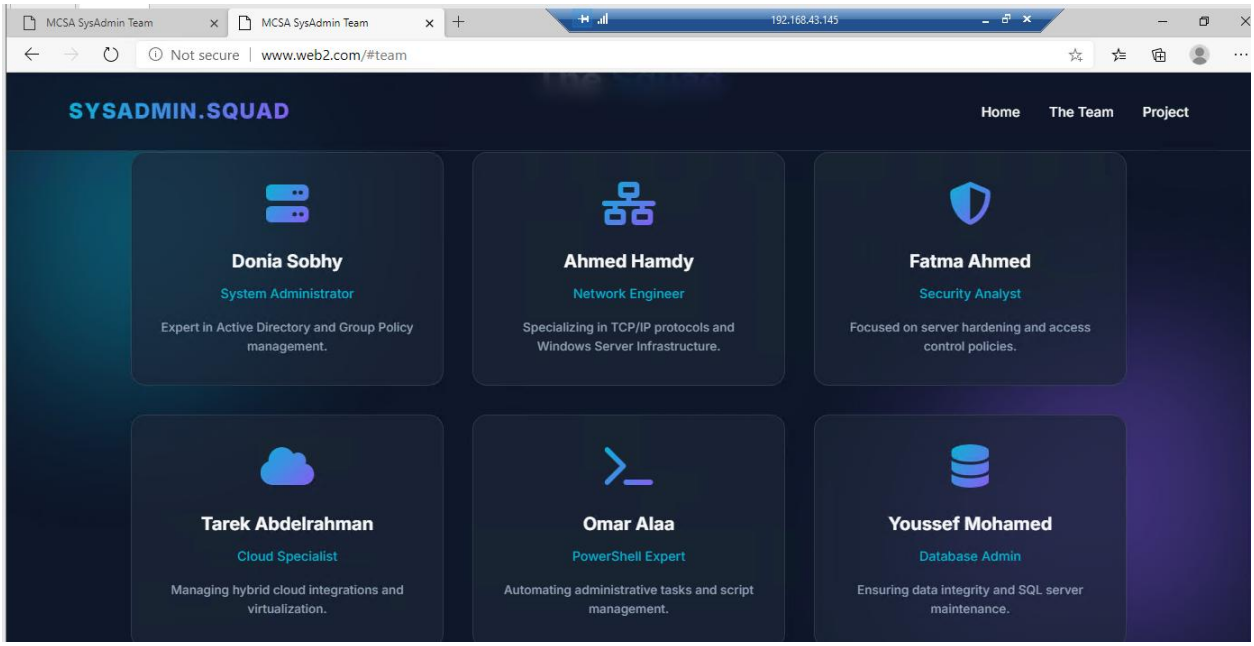


In addition to system-level management, User D is responsible for ensuring the availability and accuracy of hosted web services.

- **Site Validation:** Primary responsibility includes verifying the live status of the following sites:
  - **www.web1.com:** Verified as operational with the header "Building the Infrastructure".
  - **www.web2.com:** Verified as operational, showcasing the "SYSADMIN.SQUAD" team.

- **Directory Structure:** Web content is locally organized within the C:\my_websites directory on the server for management and local staging.



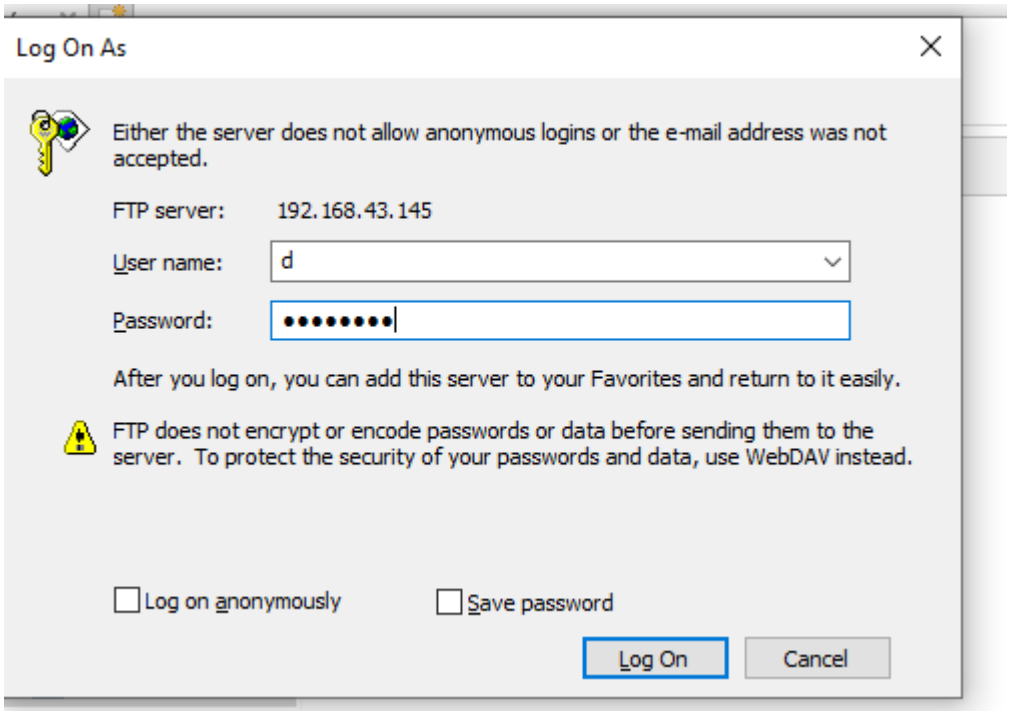


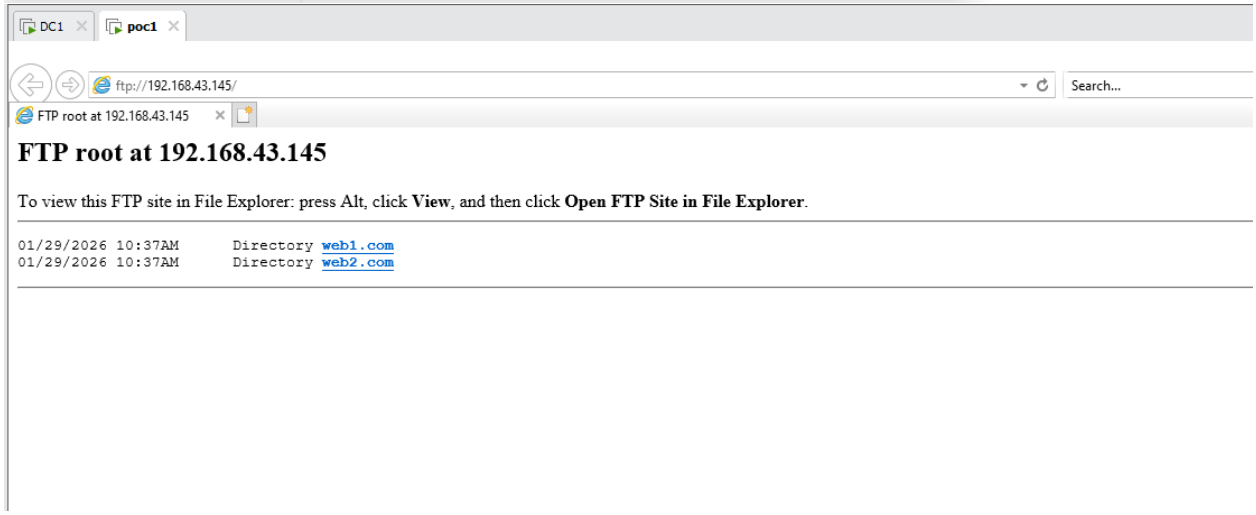
To maintain data integrity and facilitate off-site backups, User D manages the File Transfer Protocol (FTP) lifecycle for the web assets.

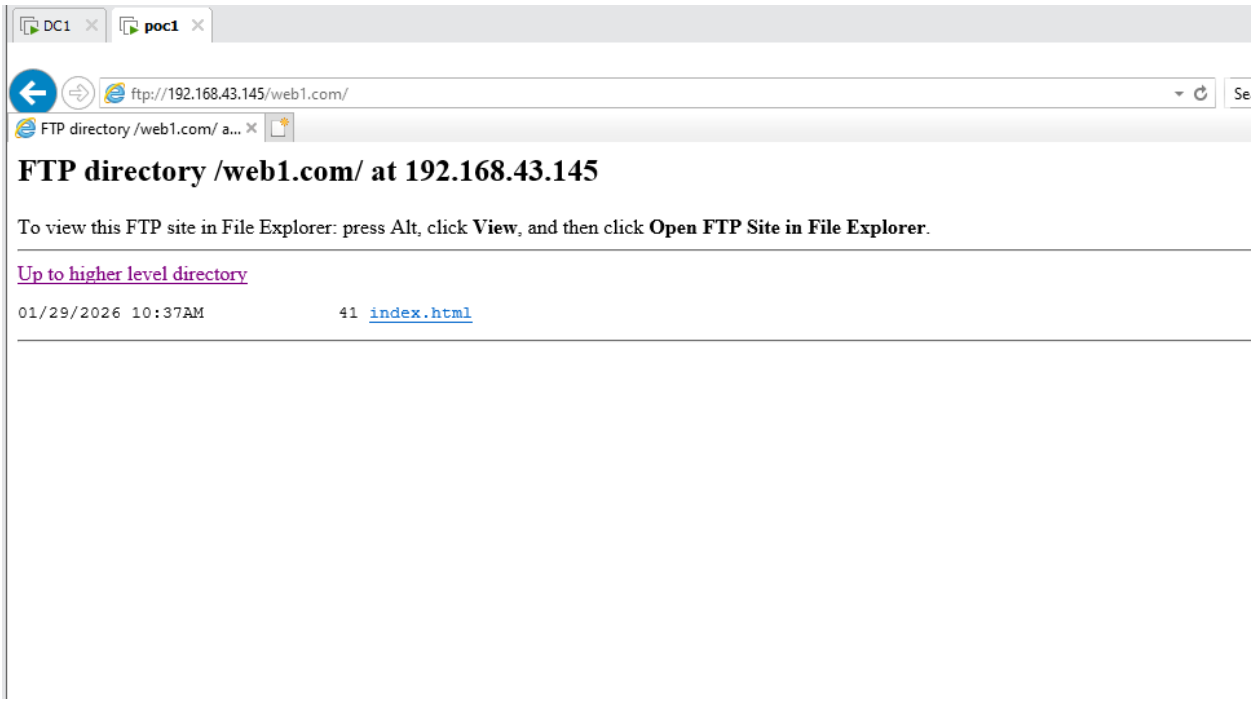
- **FTP Authentication:** Secure access is maintained through the FTP server at 192.168.43.145, where User D must provide credentials to gain access to the file root.
- **Site Management (IIS):** A dedicated FTP site named "webbackup" is managed through Internet Information Services (IIS) Manager to handle directory browsing and SSL settings.

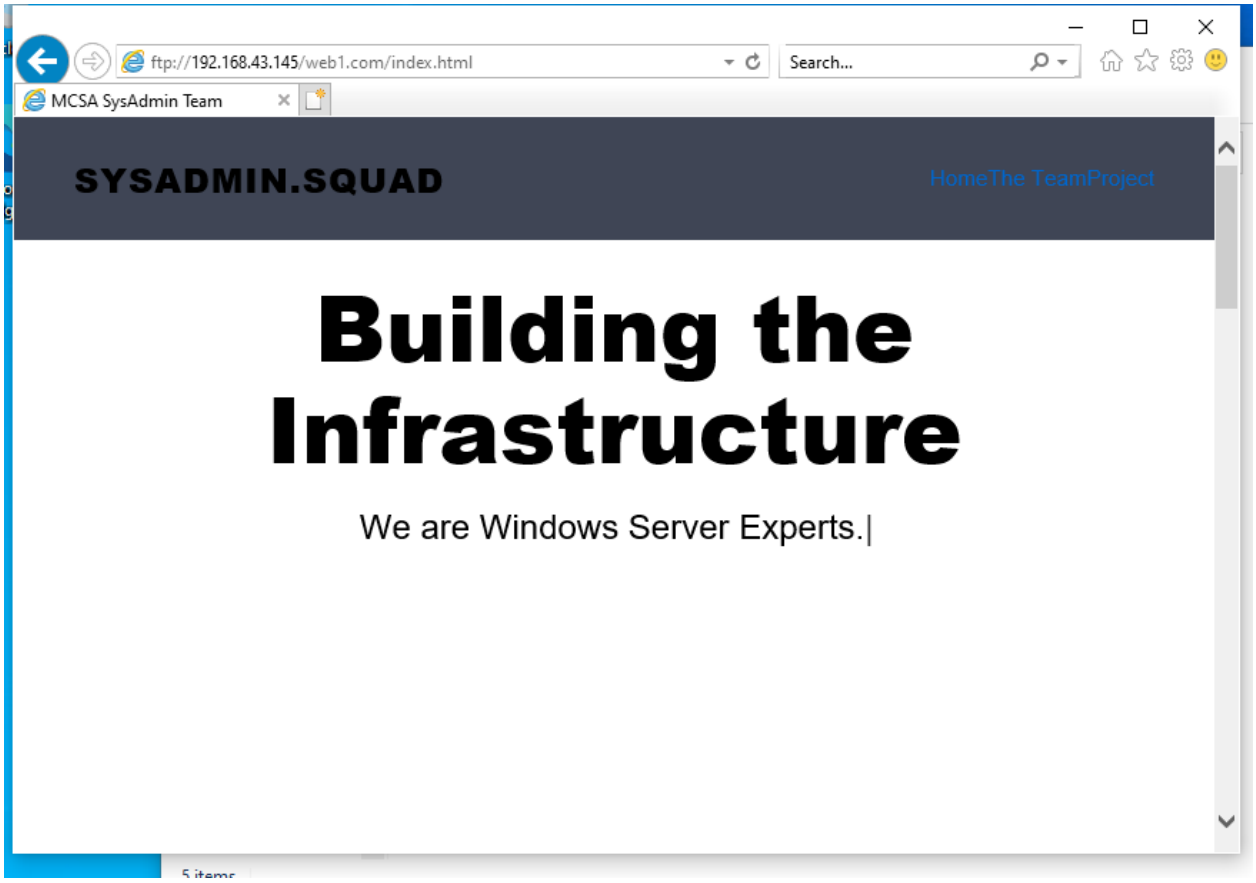
- *Content Retrieval and Backup:*
  - User D accesses the FTP root to view directories for web1.com and web2.com.
  - Individual files, such as index.html, are retrieved from the FTP server.

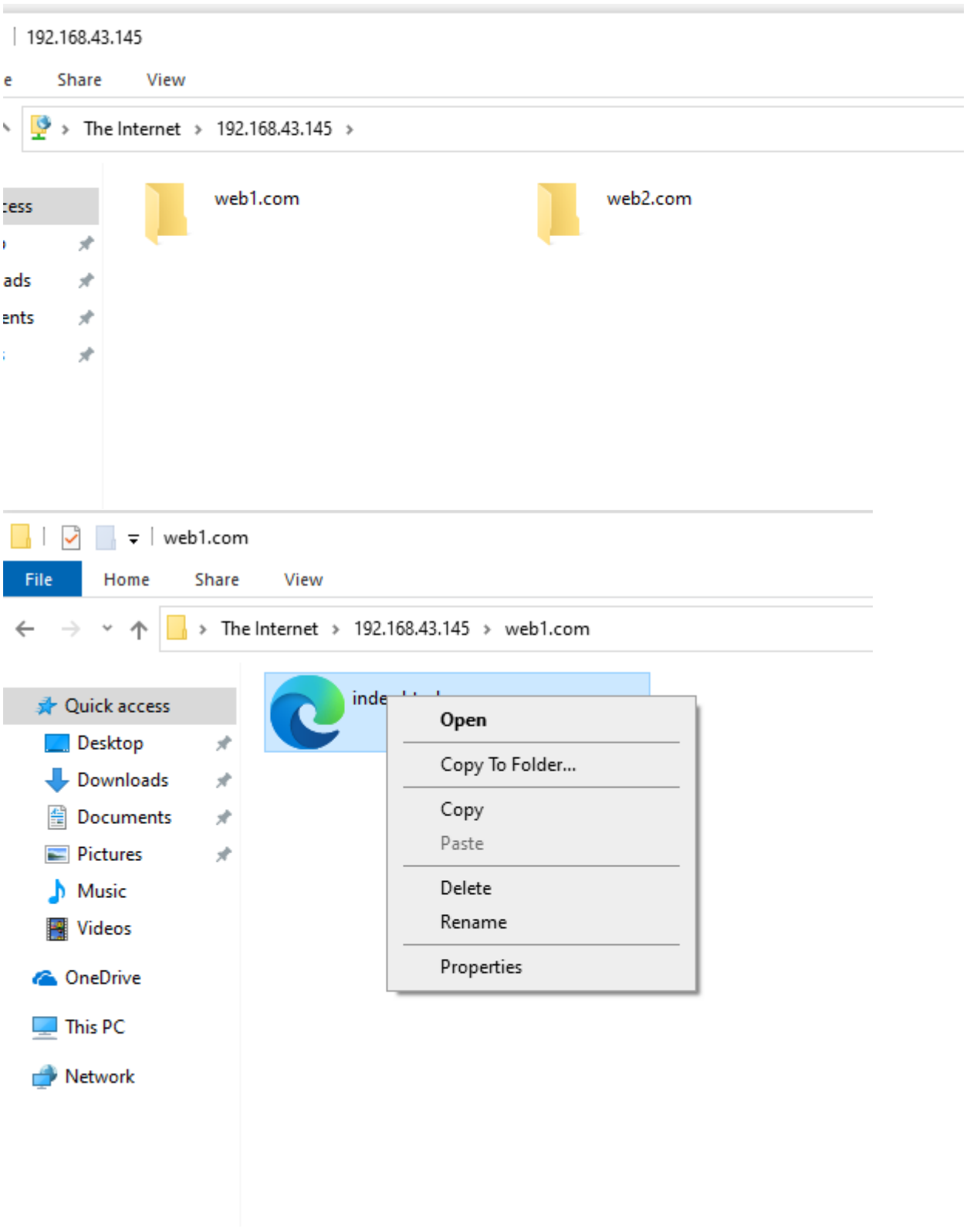
Data Copying: Verified workflows include copying files from the FTP server and storing them in local backup directories like C:\web1_copy to ensure redundancy.

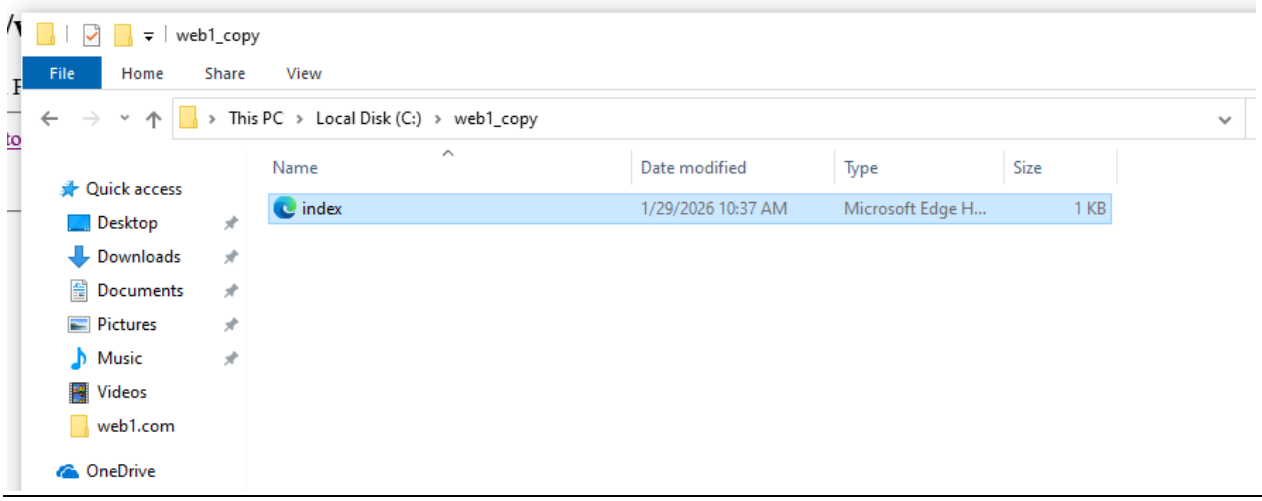





DC1
poc1
ftp://192.168.43.145/web1.com/
FTP directory /web1.com/ a...
FTP directory /web1.com/ at 192.168.43.145
To view this FTP site in File Explorer: press Alt, click View, and then click Open FTP Site in File Explorer.
Up to higher level directory
01/29/2026 10:37AM 41 index.html


ftp://192.168.43.145/web1.com/index.html
Search...
MCSA SysAdmin Team
SYSADMIN.SQUAD
HomeThe TeamProject
Building the Infrastructure
We are Windows Server Experts.
5 items


192.168.43.145
Share
View
The Internet › 192.168.43.145 ›
web1.com
web2.com
web1.com
File
Home
Share
View
The Internet › 192.168.43.145 › web1.com
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Open
Copy To Folder...
Copy
Paste
Delete
Rename
Properties



8. Conclusion

- **Forest Architecture:** established a Root Domain with two regional Child Domains to satisfy geographical administrative requirements.
- **High Availability:** Eliminated single points of failure by deploying an Additional Domain Controller (ADC) and configuring proper replication paths.
- **Operational Automation:** Successfully reduced administrative overhead by automating the creation of 50 users/computers and standardizing OS deployment via WDS.
- **Service Integration:** Achieved full interoperability between internal infrastructure services (DNS/DHCP) and public-facing Web Servers (IIS), ensuring reliable name resolution and connectivity across all zones.