MCSA Project Documentation

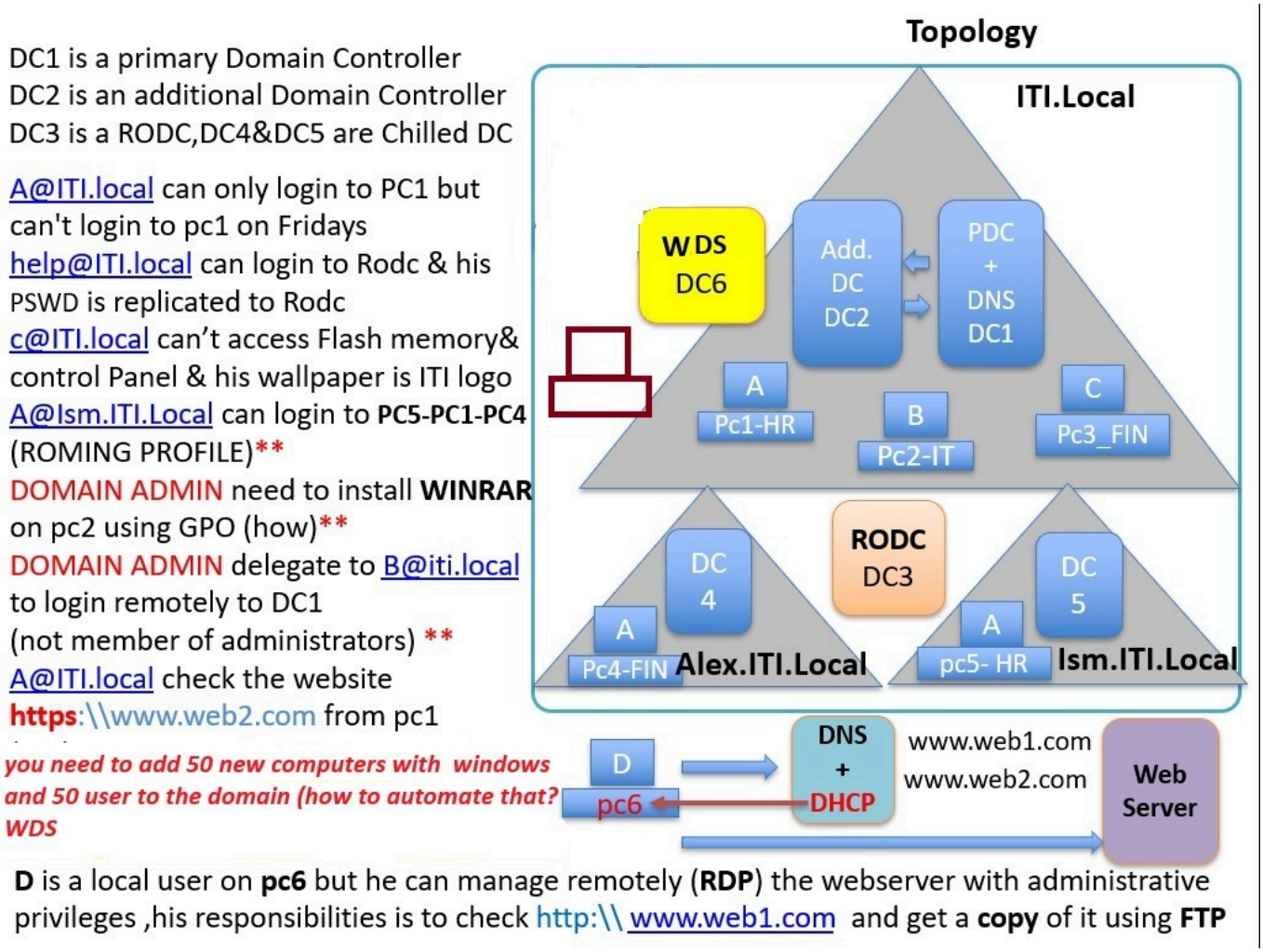
Team Members

Abdelrahim Badr
Emad Singab
Islam Yasser
Tasneem Adel
Yasmeen Mohamed

Overview

This project presents the implementation of a **Windows Server Active Directory infrastructure** that simulates a real enterprise environment. It applies key **MCSA concepts** including **Active Directory Domain Services (AD DS)**, **DNS**, **DHCP**, **Group Policy**, and **Domain Controller roles**.

The environment is based on a **root domain (ITI.local)** with multiple Domain Controllers to ensure **security, redundancy, and centralized management**. Client computers and user accounts are organized into departments, with **Group Policy Objects (GPOs)** used to enforce security settings and administrative control. The project demonstrates effective **domain design, service integration, and user management** within a Microsoft-based network.

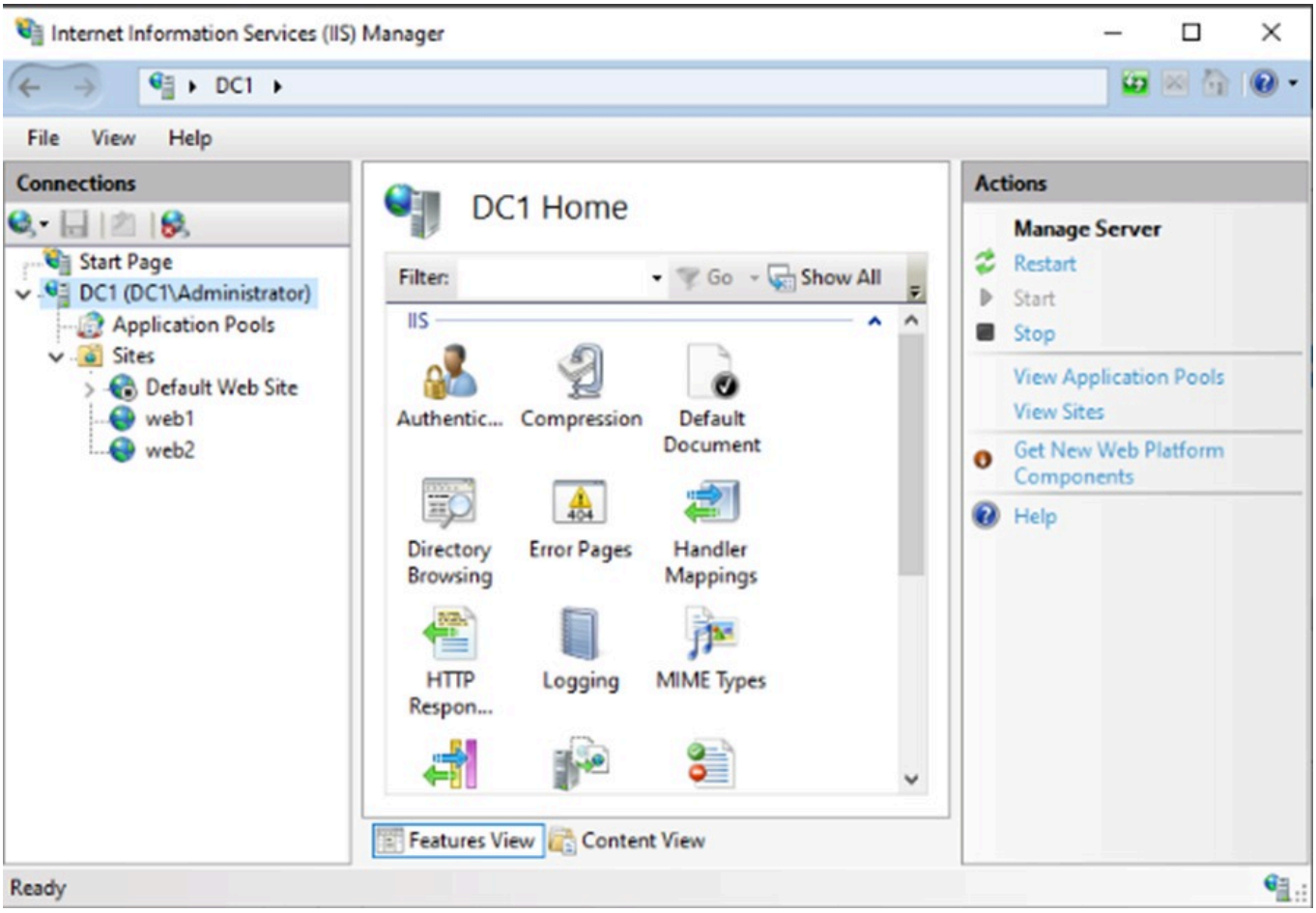


1. Web Server - DNS - DHCP

1.1. IIS Web Server Configuration (DC1)

The **IIS Manager** on **DC1** is the primary host for the project's internal websites.

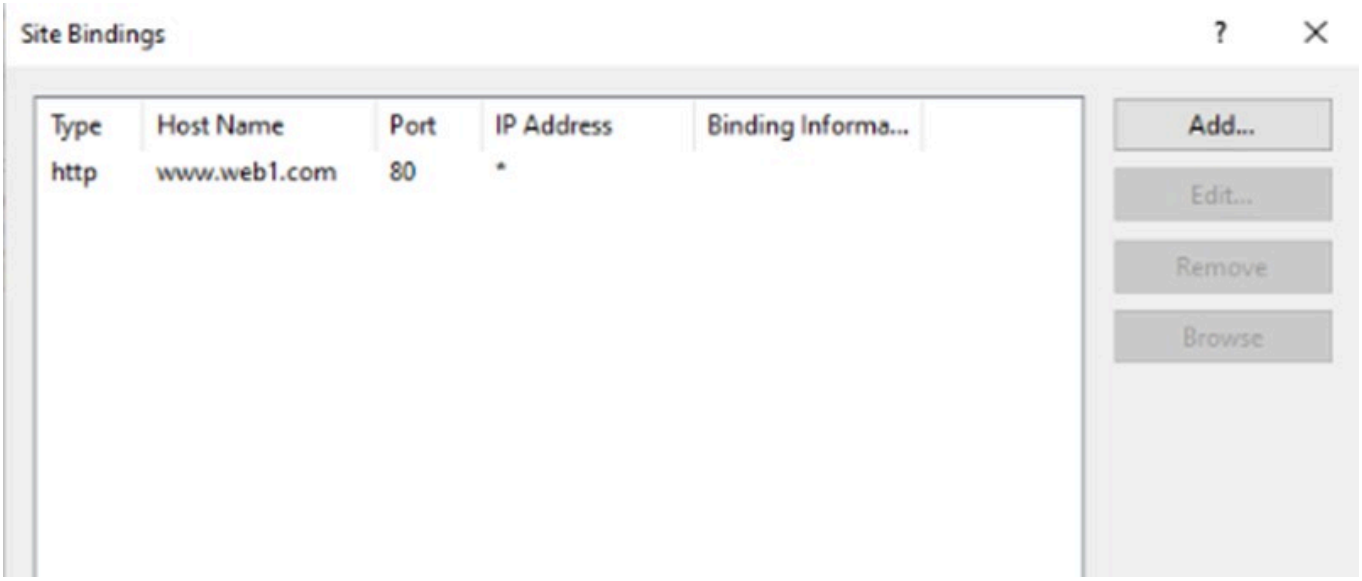
- **Hosted Sites**: The console confirms that **web1** and **web2** are active and managed on this server.

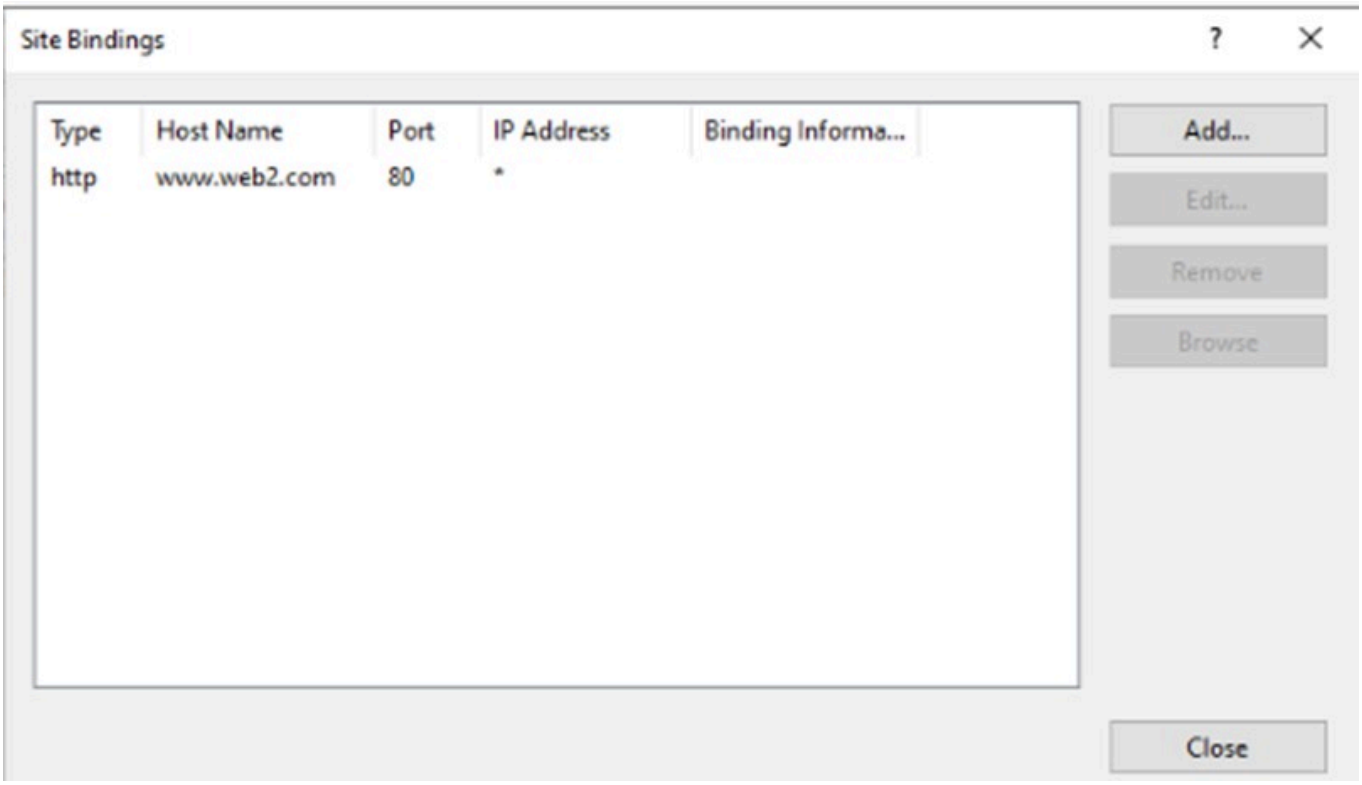


1.2. Bindings

Specific bindings are set up so that users like A@ITI.local can access the sites from **pc1**.

- **web1 Binding**: The site **www.web1.com** is configured on **Port 80** via **http**.
- **web2 Binding**: The site **www.web2.com** is also configured on **Port 80** via **http**.



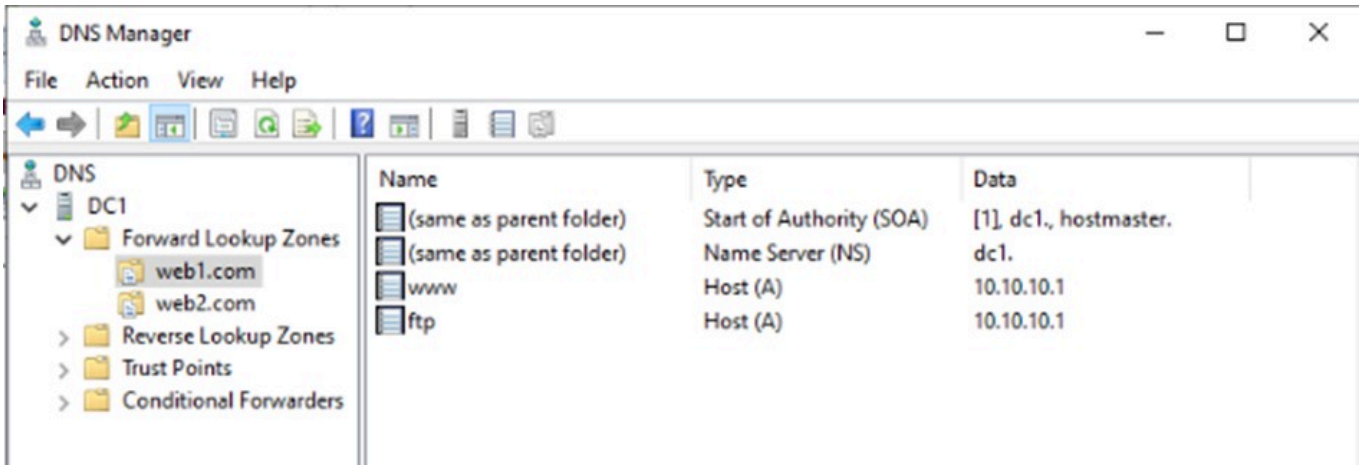


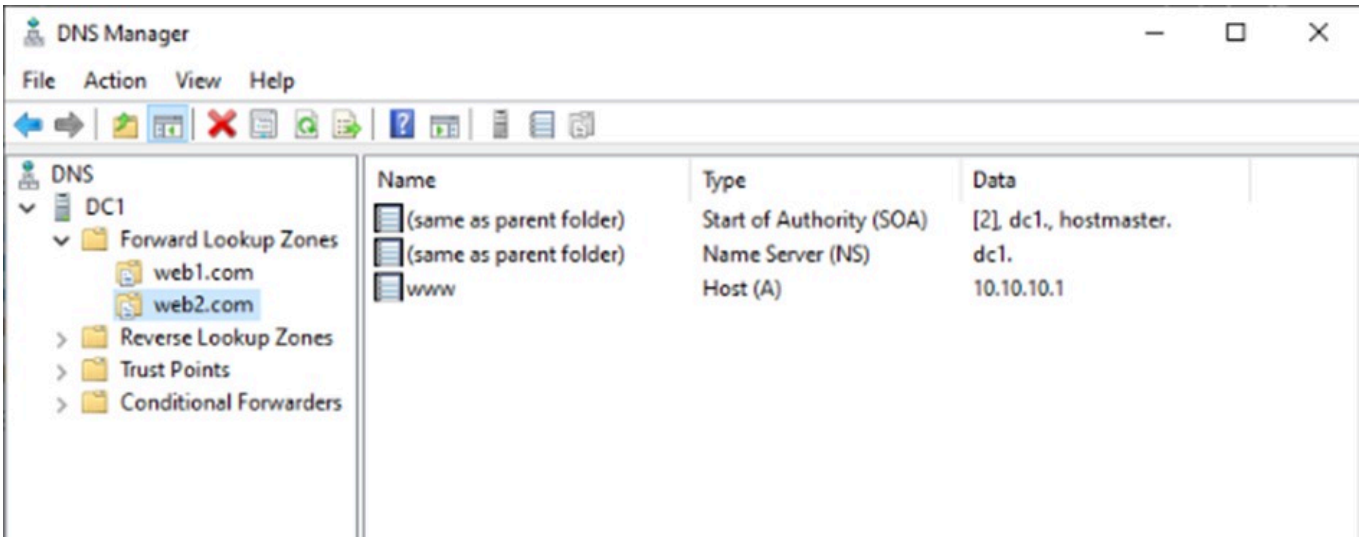
1.3. DNS

The **DNS Manager** on **DC1** handles name resolution and zone forwarding for the forest.

- **Forward Lookup Zones**: Authoritative zones are active for **web1.com** and **web2.com**.
- **web1.com Records**:
  - **www**: A **Host (A)** record points to the server IP **10.10.10.1**.
  - **ftp**: A **Host (A)** record points to **10.10.10.1**, enabling the requirement to retrieve site copies via FTP.
- **Conditional Forwarding**: A forwarder for **web2.com** is configured to point to **10.250.159.151**. This satisfies the requirement for **DC1** to act as the authoritative "Second

Z" for that domain.

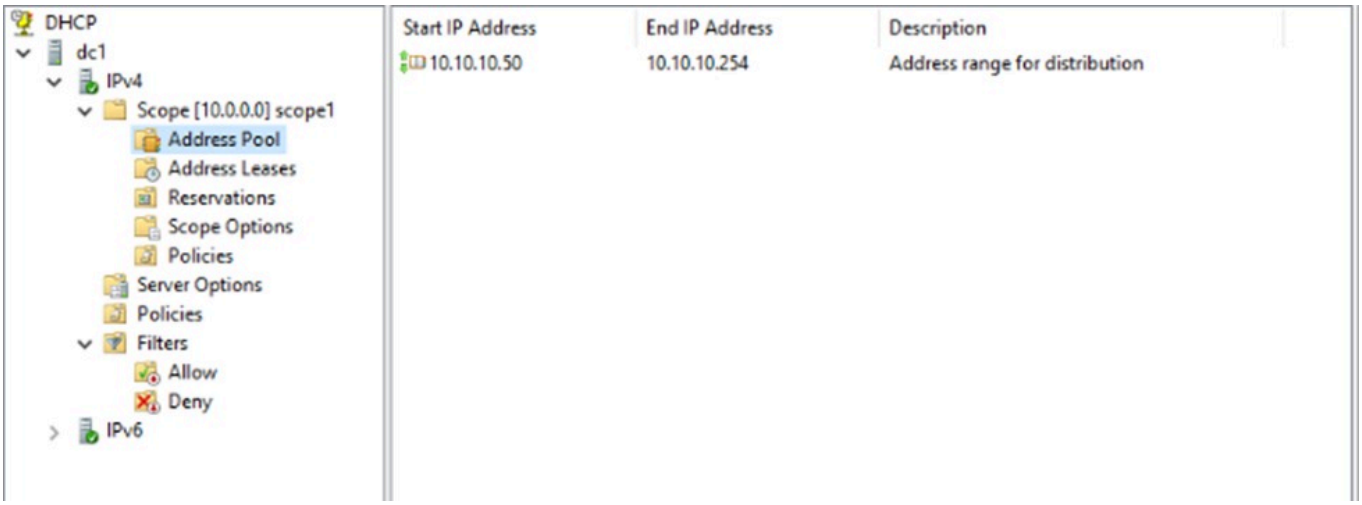


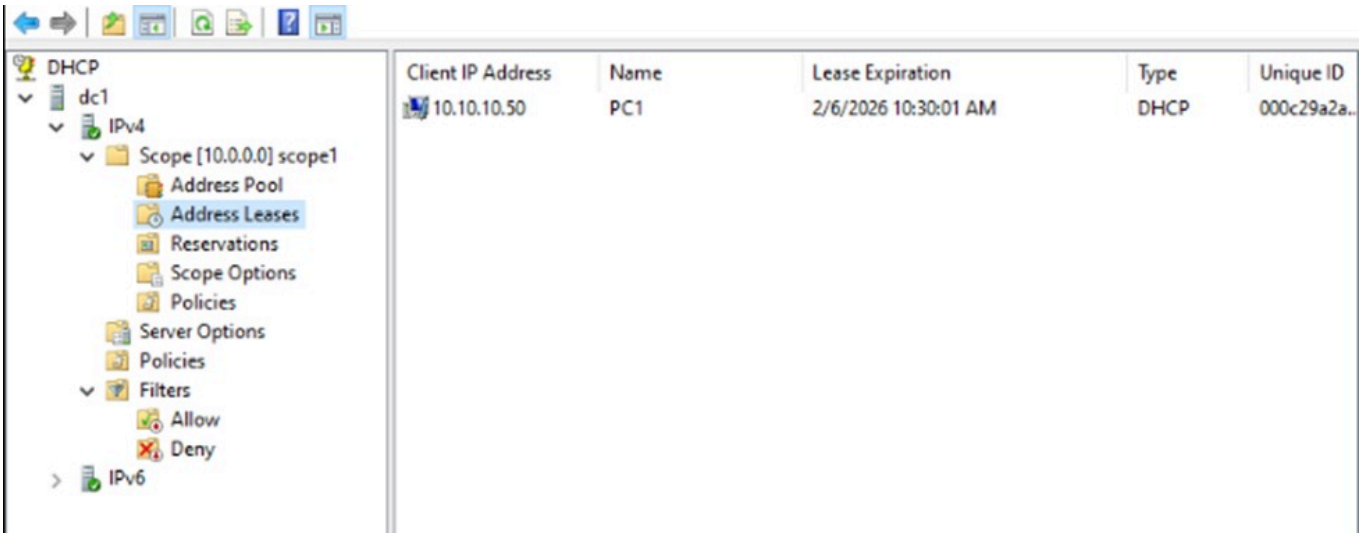


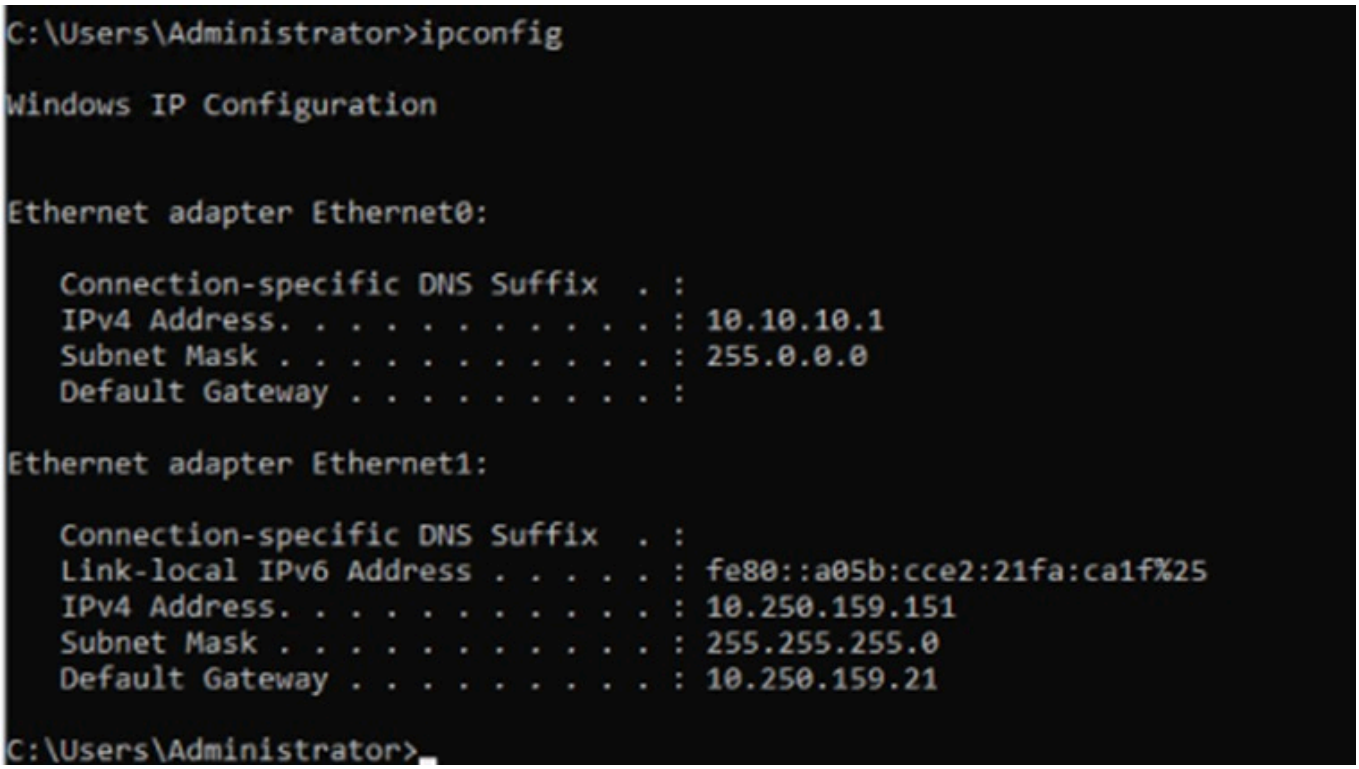
1.4. DHCP

The **DHCP** console on **DC1** provides dynamic IP management for the entire topology.

- **Scope**: A scope named **scopel** is defined for the **10.0.0.0** network.
- **Address Pool**: IPs are distributed from **10.10.10.50** to **10.10.10.254**.
- **Active Lease**: The "Address Leases" table confirms **PC1** has successfully leased IP **10.10.10.50**.
- **Verification**: The lease is valid until **2/6/2026**, confirming the network is live and updating correctly.


DHCP
dc1
IPv4
Scope [10.0.0.0] scope1
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
Allow
Deny
IPv6
Start IP Address
End IP Address
Description
10.10.10.50
10.10.10.254
Address range for distribution


DHCP
dc1
IPv4
Scope [10.0.0.0] scope1
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
Allow
Deny
IPv6
Client IP Address
Name
Lease Expiration
Type
Unique ID
10.10.10.50
PC1
2/6/2026 10:30:01 AM
DHCP
000c29a2a..

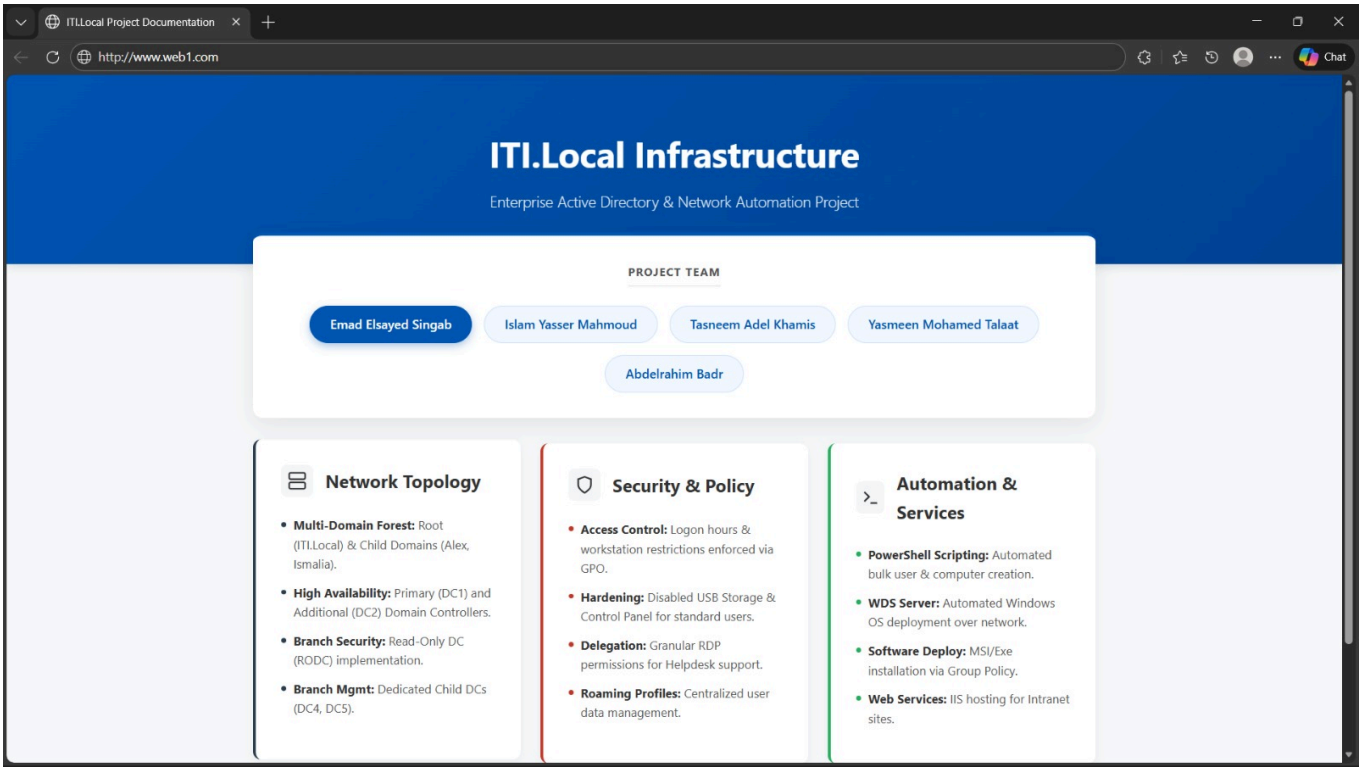

C:\Users\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 10.10.10.1
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . :
Ethernet adapter Ethernet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::a05b:cce2:21fa:ca1f%25
IPv4 Address. . . . . : 10.250.159.151
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.250.159.21
C:\Users\Administrator>

1.5. Websites

This section confirms the successful deployment of the web infrastructure on **DC1** as verified by the active browser results.

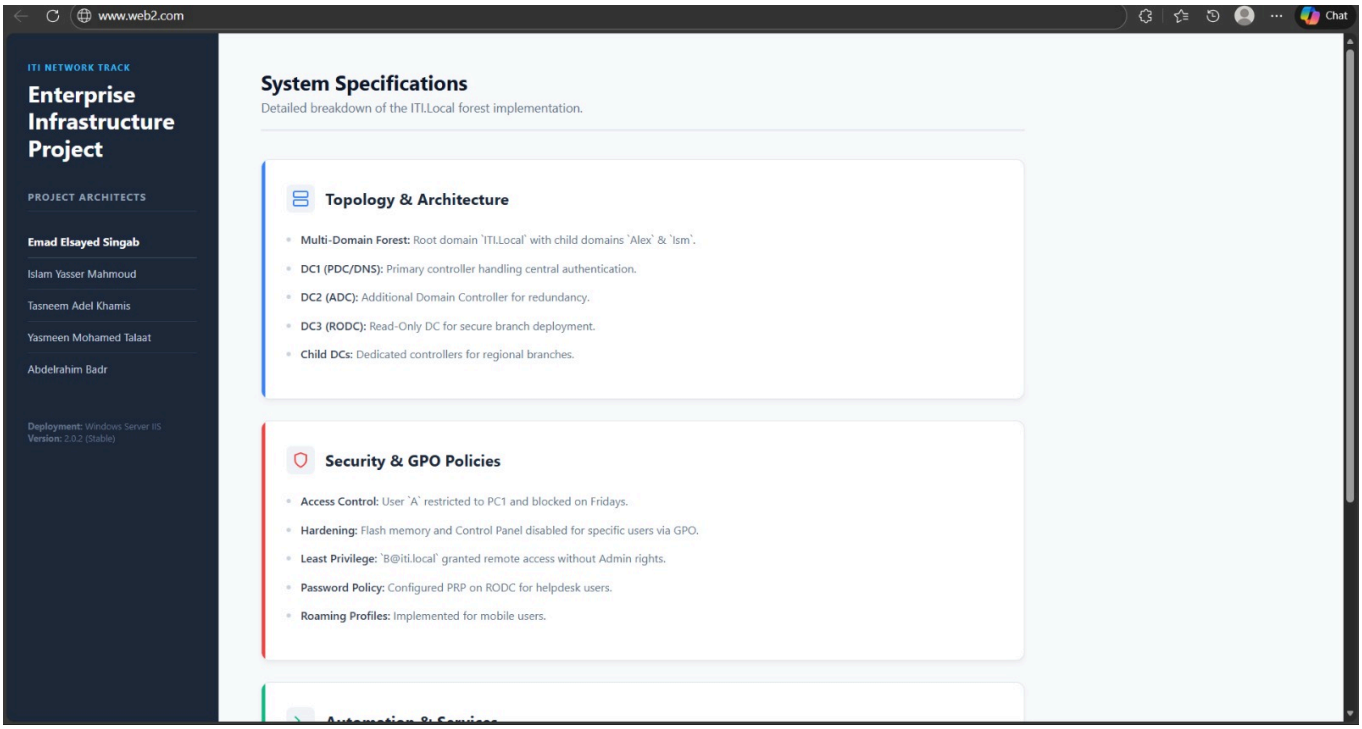
Web 1

Accessing http://www.web1.com confirms the primary project site is live and reachable from the domain workstations.



web2

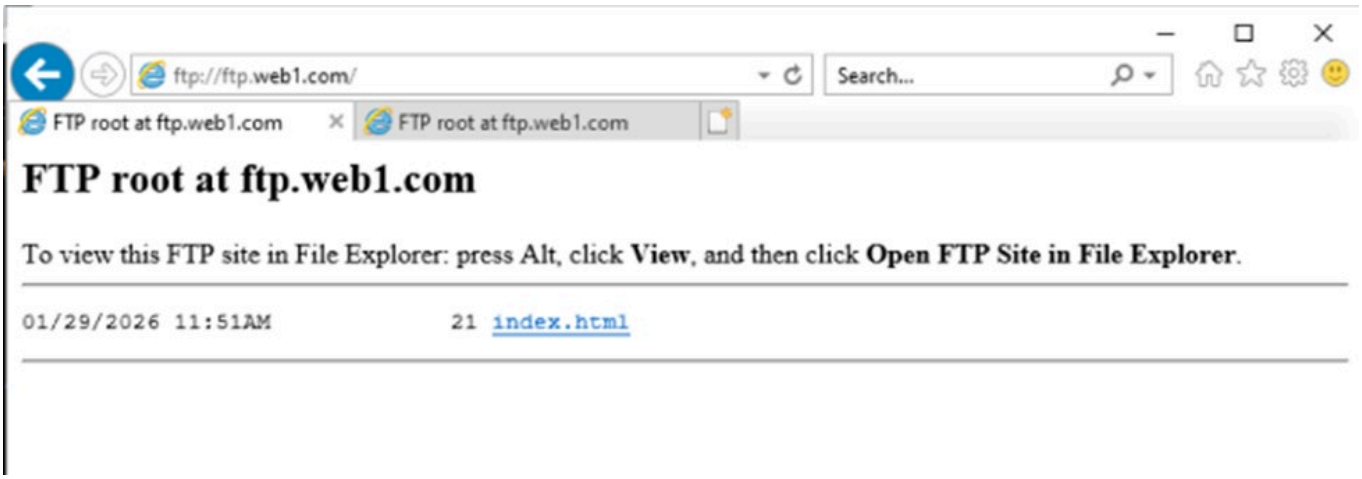
Accessing http://www.web2.com confirms that the secondary authoritative zone and its content are correctly deployed.



1.6. FTP

This section verifies that the **FTP service** is functional and configured according to the project requirements.

The **DNS Manager** on **DC1** confirms a **Host (A) record** for `ftp` pointing to the server IP **10.10.10.1**.



2. Parent Active Domain Directory

The root of the infrastructure is the **iti.local** domain, which serves as the forest parent for all subordinate branches.

- **iti.local**: This represents the top-level namespace for the entire Active Directory environment.

2.1. Active Domain Hierarchy

The organizational structure is defined by a parent-child relationship between the root and regional branch domains.

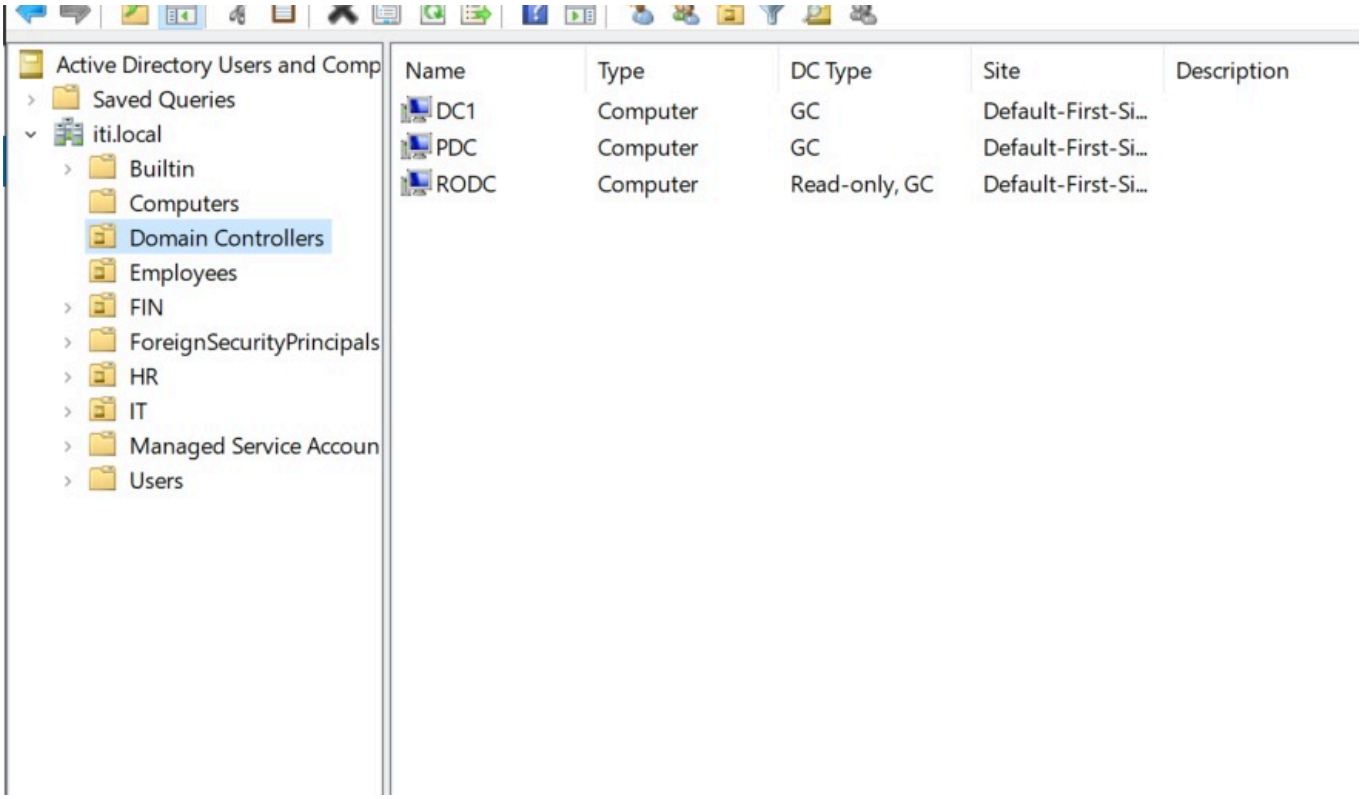
- **Domain Relationships**: The hierarchy displays **ALEX.iti.local** and **ISMAILIA.iti.local** as child domains under the **iti.local** root.

2.2. Primary Domain

This section lists the specific servers responsible for authentication within the root domain.

- **PDC**: This is the parent server and primary controller for the domain.

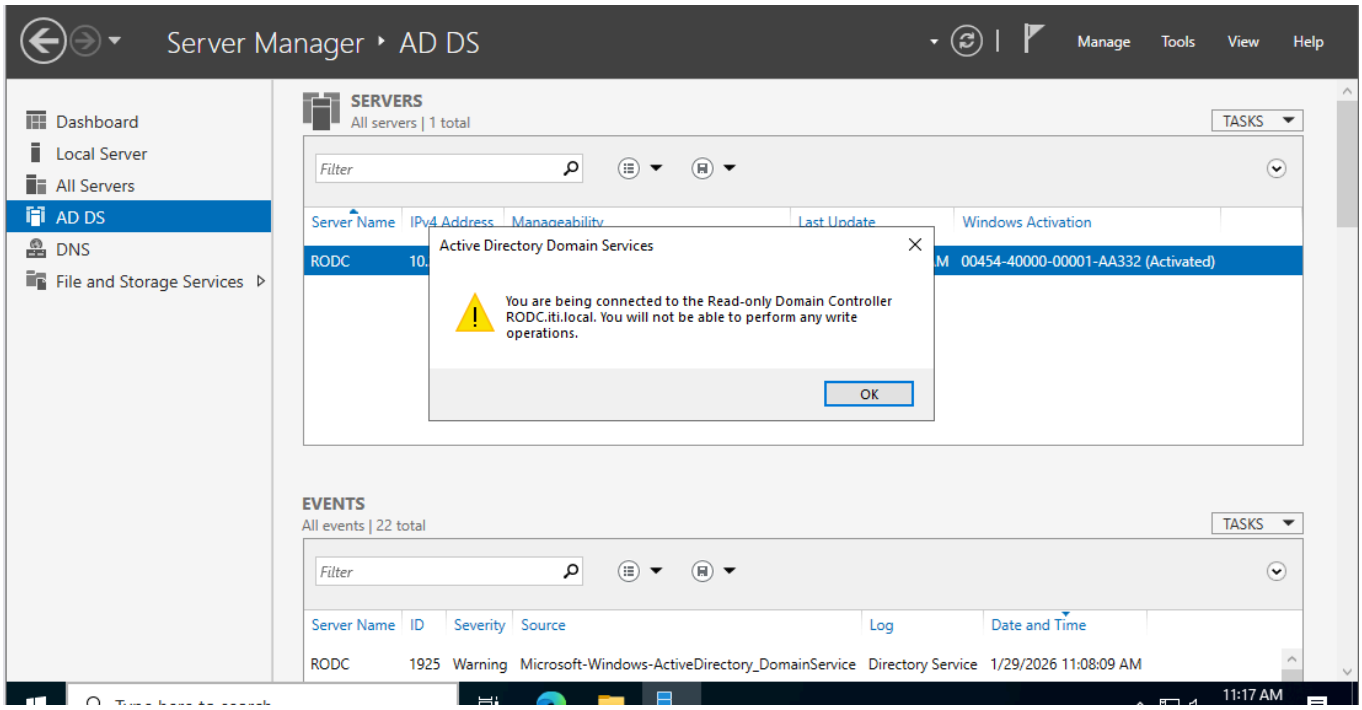
- **DC1**: This server is configured as the additional domain controller to provide redundancy.
- **Global Catalog (GC)**: Both the **PDC** and **DC1** are designated as **GC** servers, allowing them to provide resource information across the entire forest.



2.3. RODC

The implementation of a Read-Only Domain Controller provides secure identity services to remote branches.

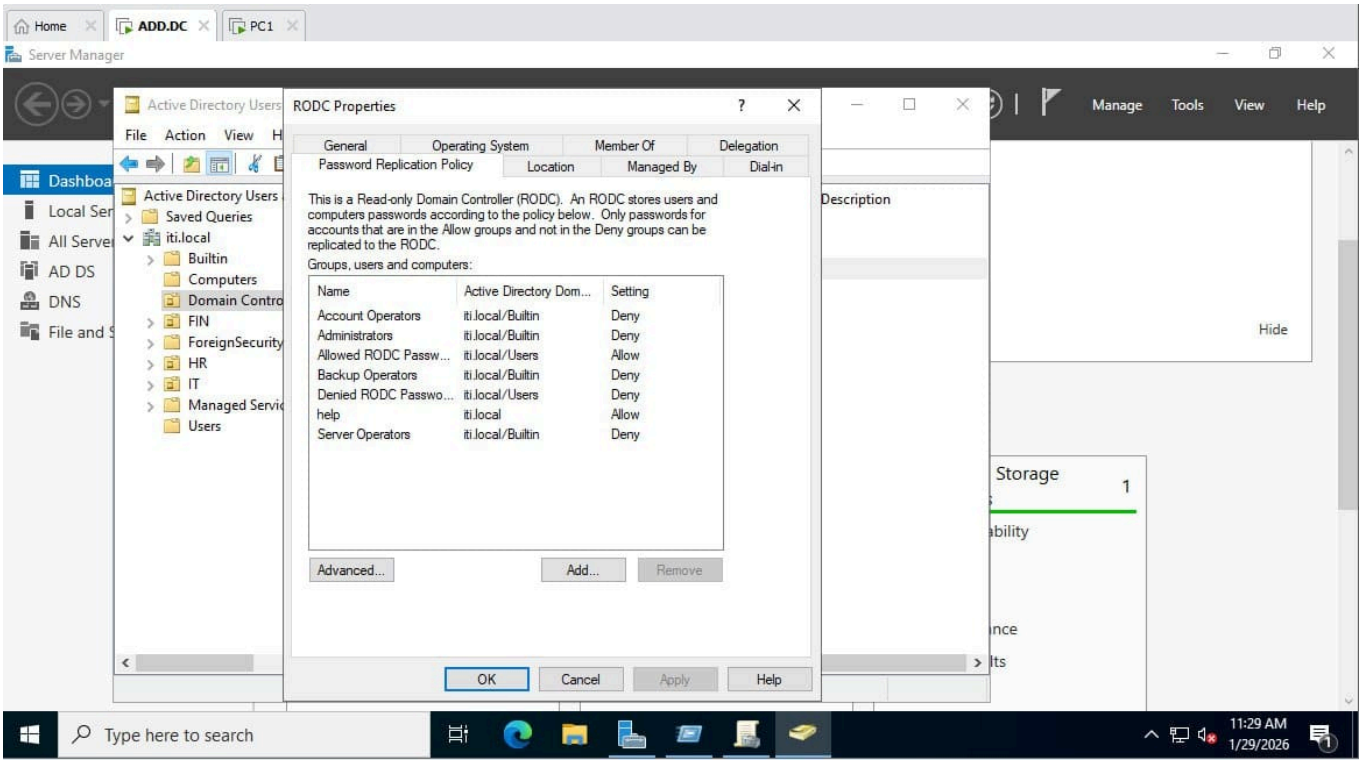
- **RODC Identity**: The server named **RODC** is the dedicated read-only controller for **iti.local**.
- **Write Restrictions**: The system identifies this machine as read-only and explicitly prevents any write operations to the Active Directory database.



2.3.1. Help user

The **help** user is a dedicated account within the domain hierarchy used to test branch accessibility and replication.

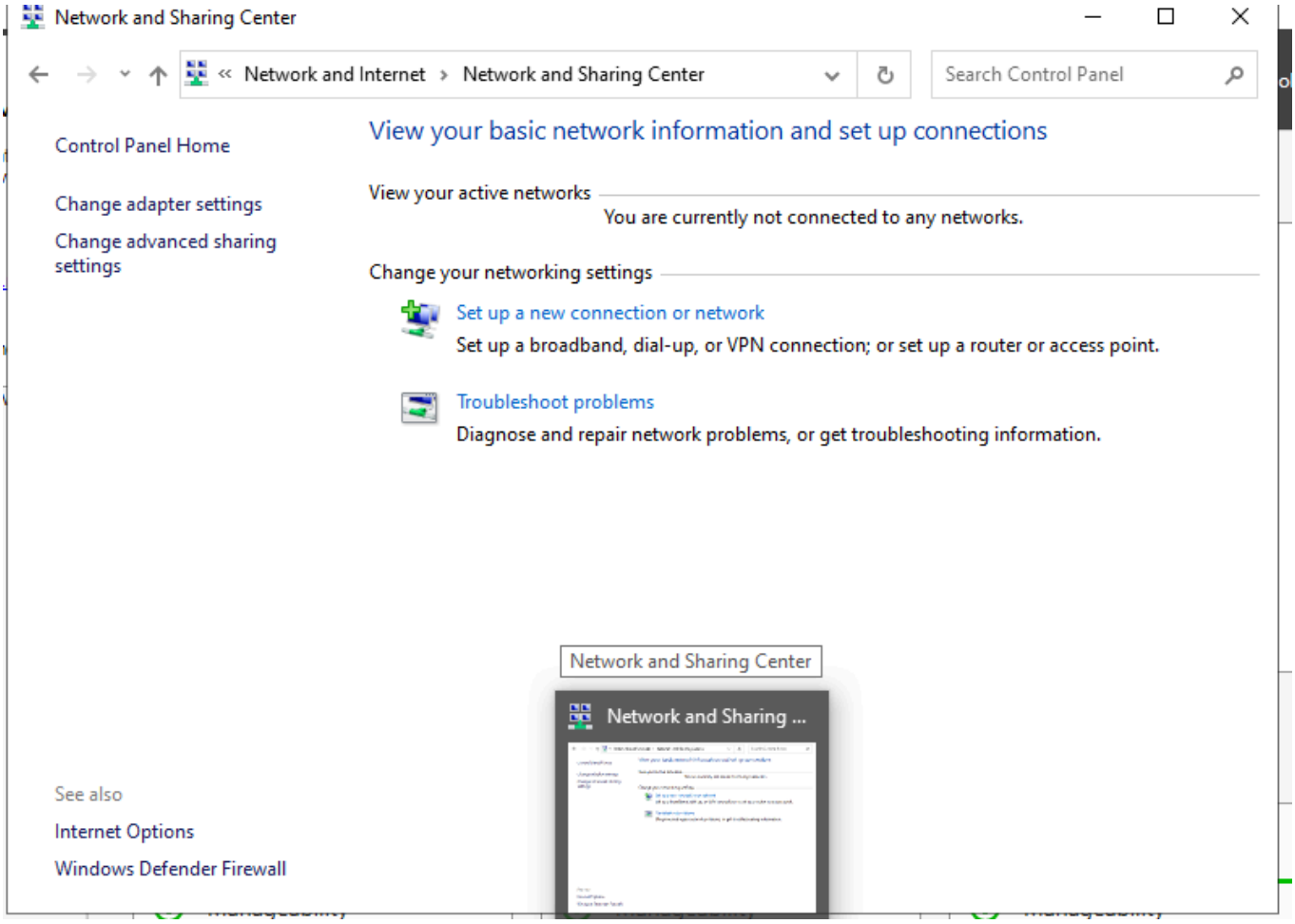
- **Account Status**: The user is identified as help@ITI.local.
- **Server Access**: This user is granted the necessary permissions to log in and authenticate on the **RODC** server.

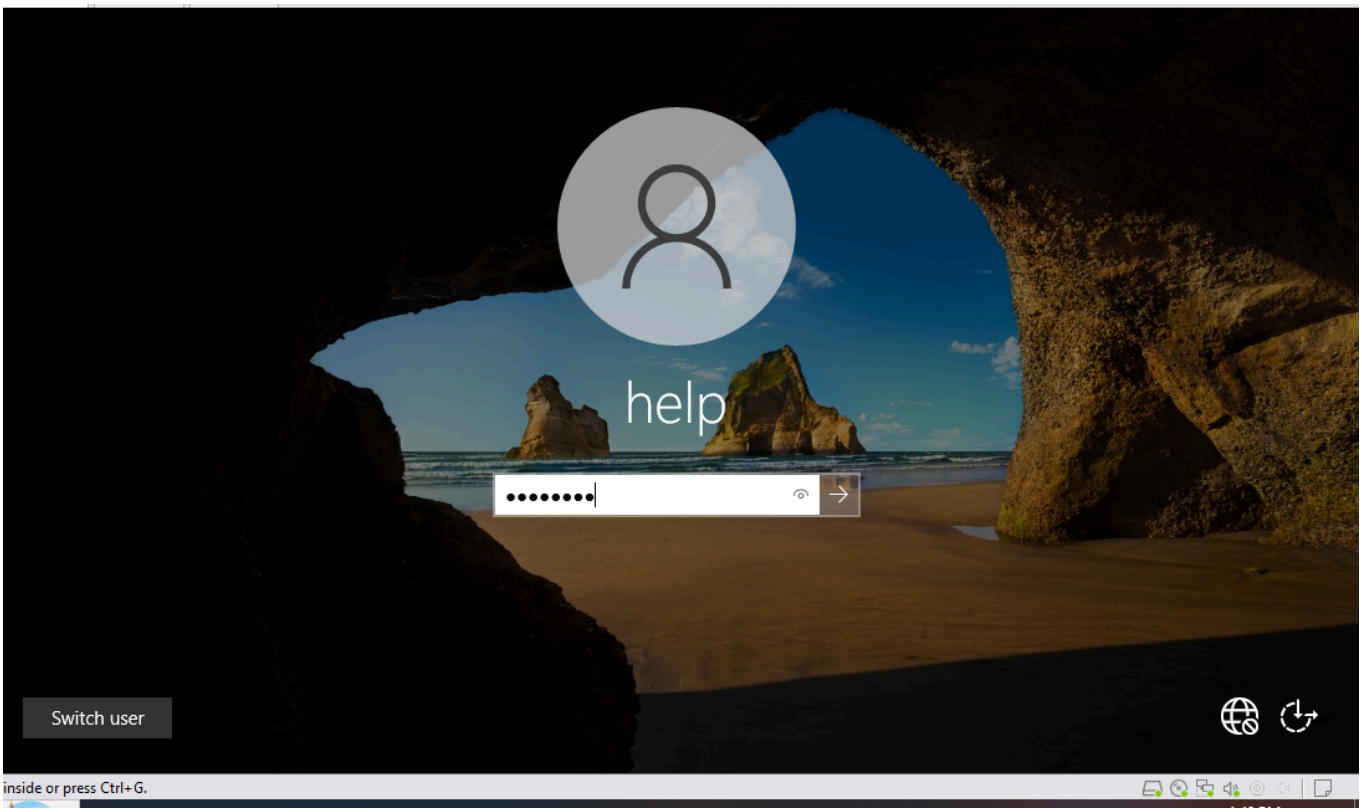


2.3.2. Password Replication

This policy manages credential caching to ensure branch users can log in even if the connection to the parent domain is lost.

- **Help Account**: Credentials for the **help** user are set to **"Allow"**, permitting their password to be replicated locally to the **RODC**.
- **Standard Allowed Group**: The **Allowed RODC Password Replication Group** is also granted permission to replicate.
- **Restricted Groups**: High-privilege accounts, such as **Administrators**, **Backup Operators**, and **Server Operators**, are strictly set to **"Deny"** to prevent their passwords from being stored on branch hardware.



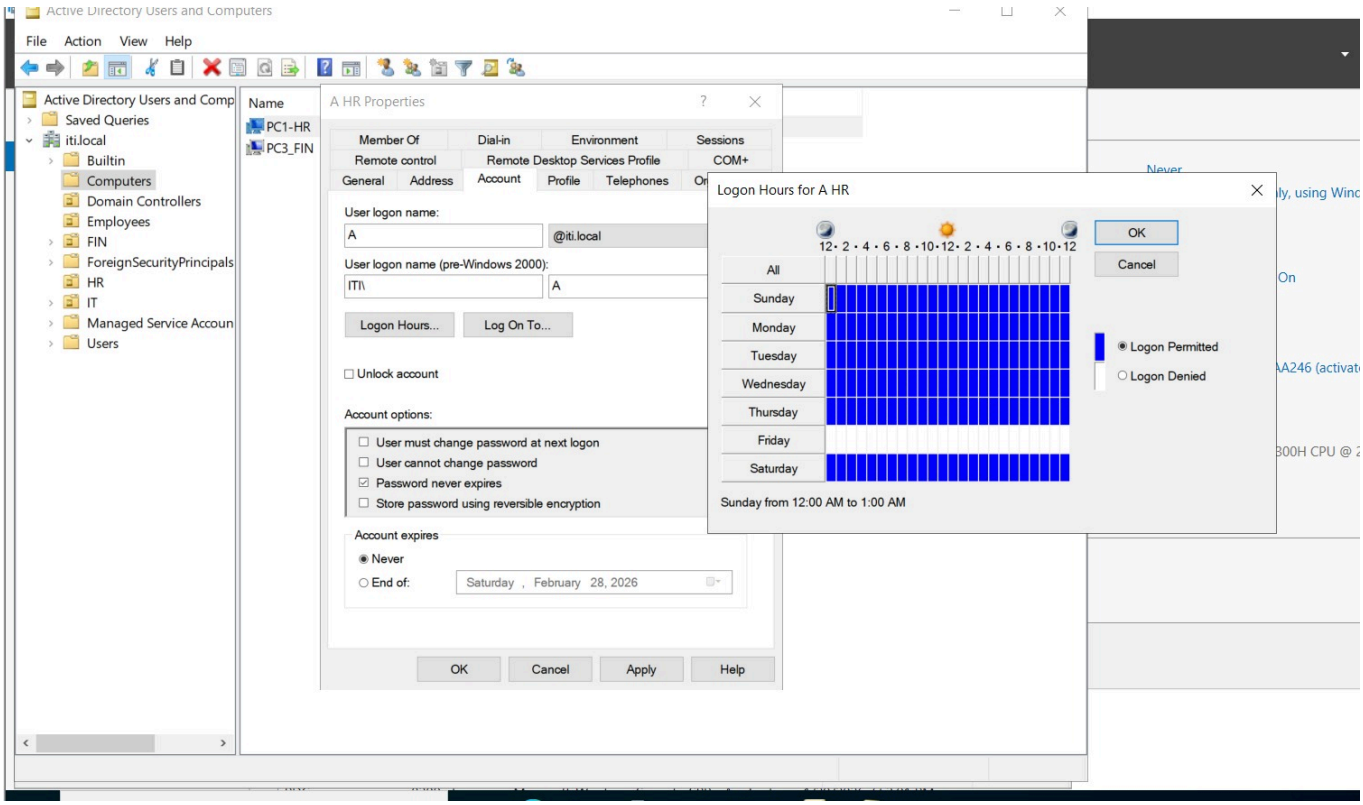


3. Policies

3.1. Blocking The User From Accessing PC on Friday

This policy implements time-based access control for the user A@ITI.local within the domain.

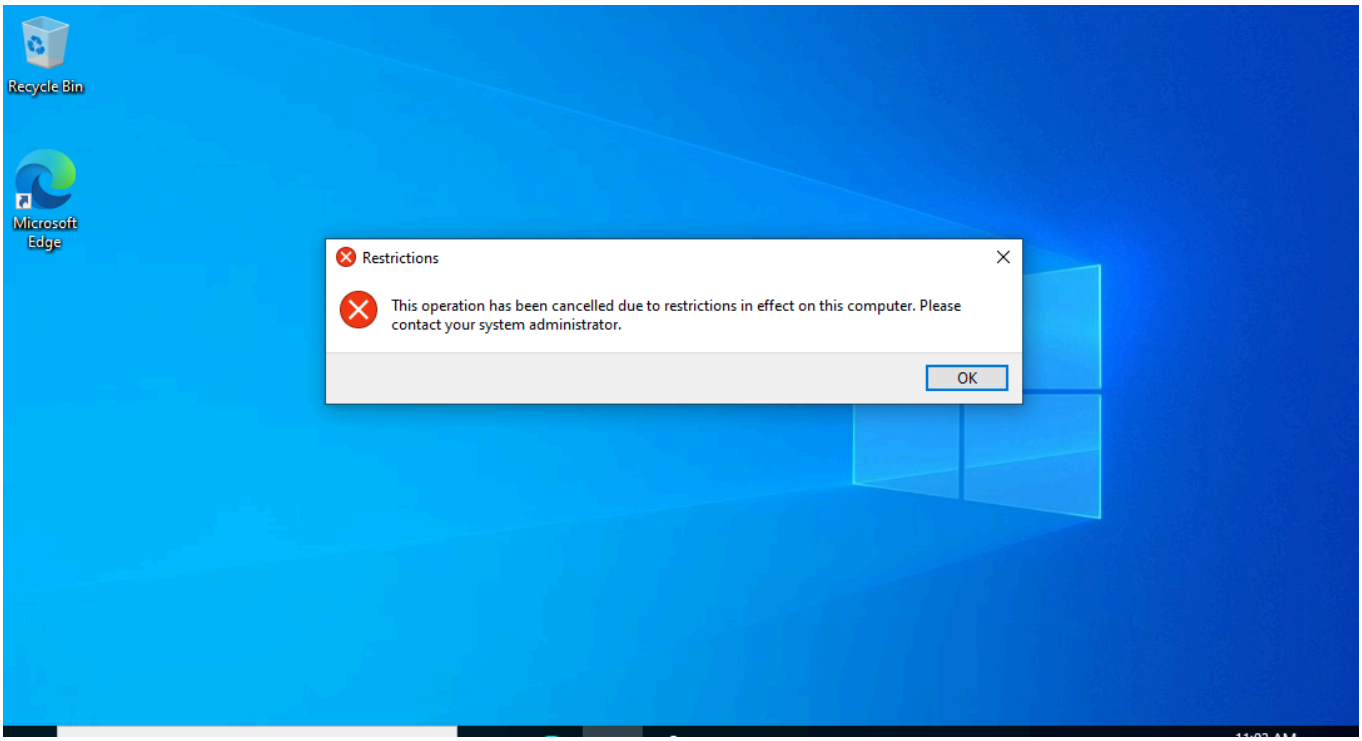
- **Logon Hours**: The configuration grid in Active Directory shows that logon is permitted from Sunday through Thursday.
- **Restriction**: The schedule for **Friday** is explicitly marked as "Logon Denied" for all 24 hours.
- **Result**: This ensures that User A is unable to authenticate or access the system on Fridays as per the project requirements.



3.2 Prevent Opening Control Panel

This Group Policy Object (GPO) is applied to secure the operating system environment for **User C**.

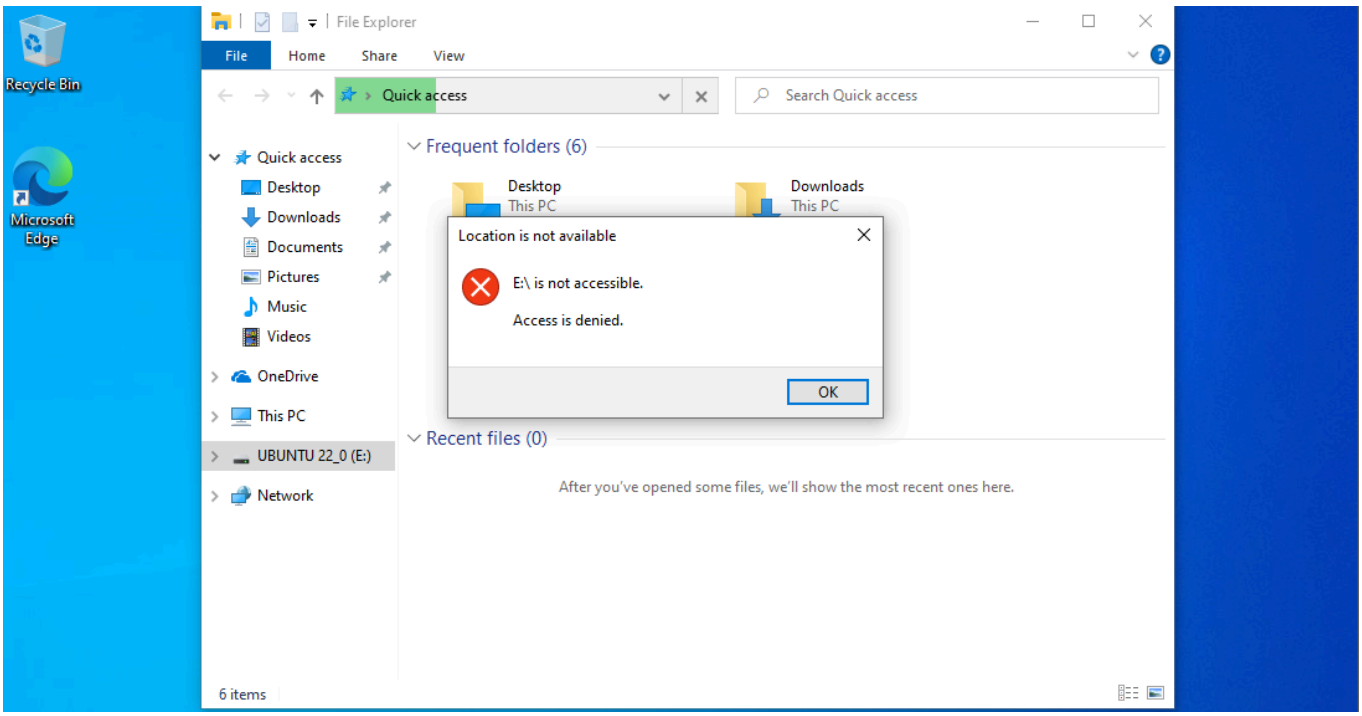
- **GPO Enforcement**: The policy **"Prohibit access to Control Panel and PC settings"** is enabled and linked to the **FIN** OU.
- **System Result**: When User C attempts to open the Control Panel, the system displays a **"Restrictions"** error message stating: "This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator."



3.3 Can't Access Flash

Hardware security measures are enforced to prevent data exfiltration via removable storage.

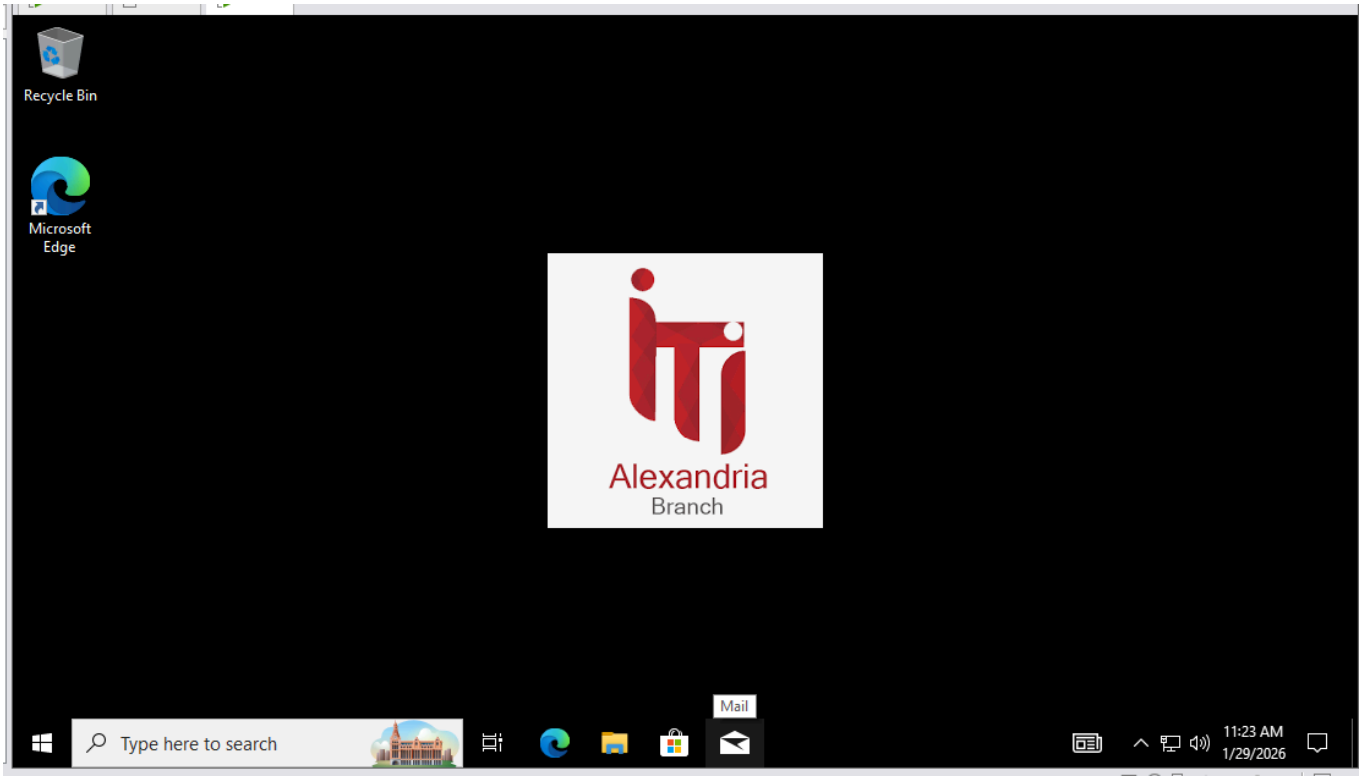
- **Removable Storage Block**: A GPO named **"can't access Flash memory"** is configured to deny read/write access to removable disks.
- **Verification Result**: When attempting to access an attached USB drive (E:), the system returns an **"Access is denied"** prompt, confirming the policy is active.



3.4 Wallpaper is ITI Logo

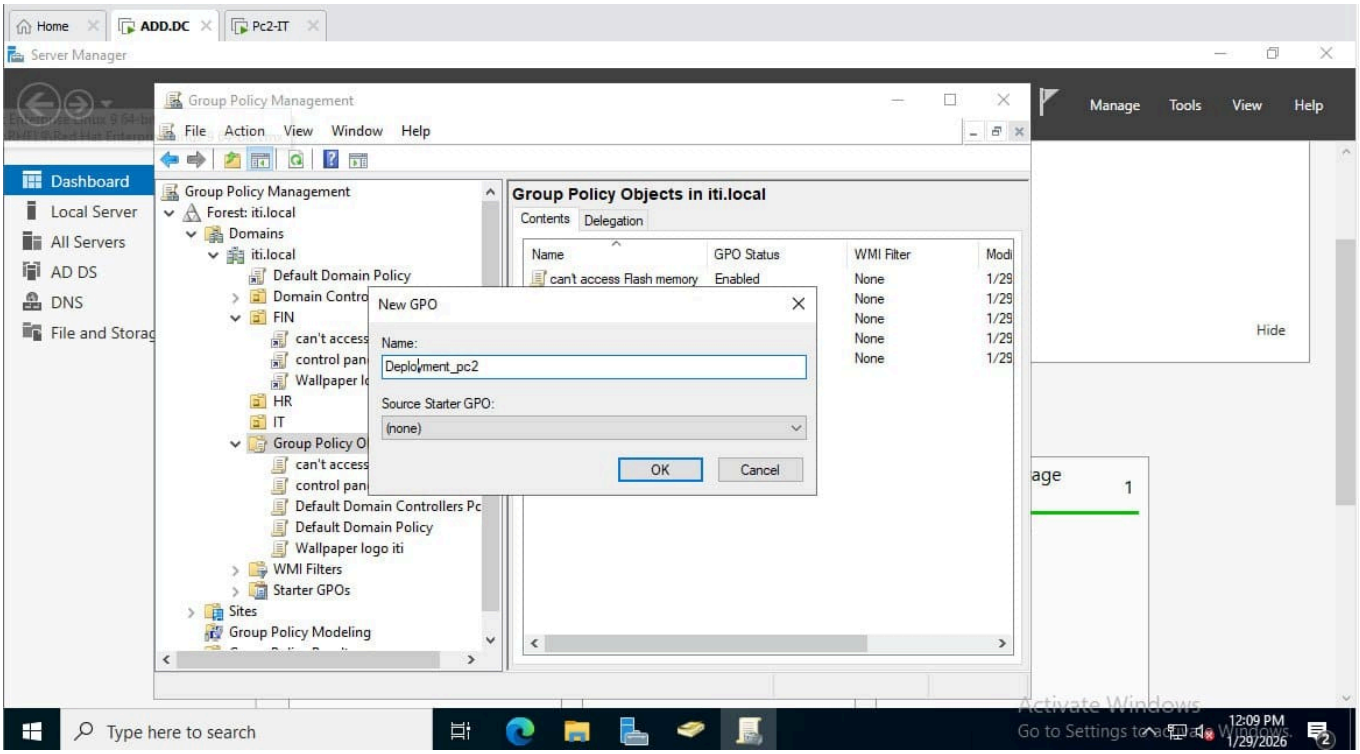
Mandatory branding is applied via GPO to maintain a uniform corporate identity across branch workstations.

- **Desktop Wallpaper Policy**: The **"Desktop Wallpaper"** setting is enabled within the GPO, pointing to the local path of the **ITI Alexandria Branch logo**.
- **Visual Result**: The specified ITI logo is locked as the desktop background for User C and cannot be changed by the end user.

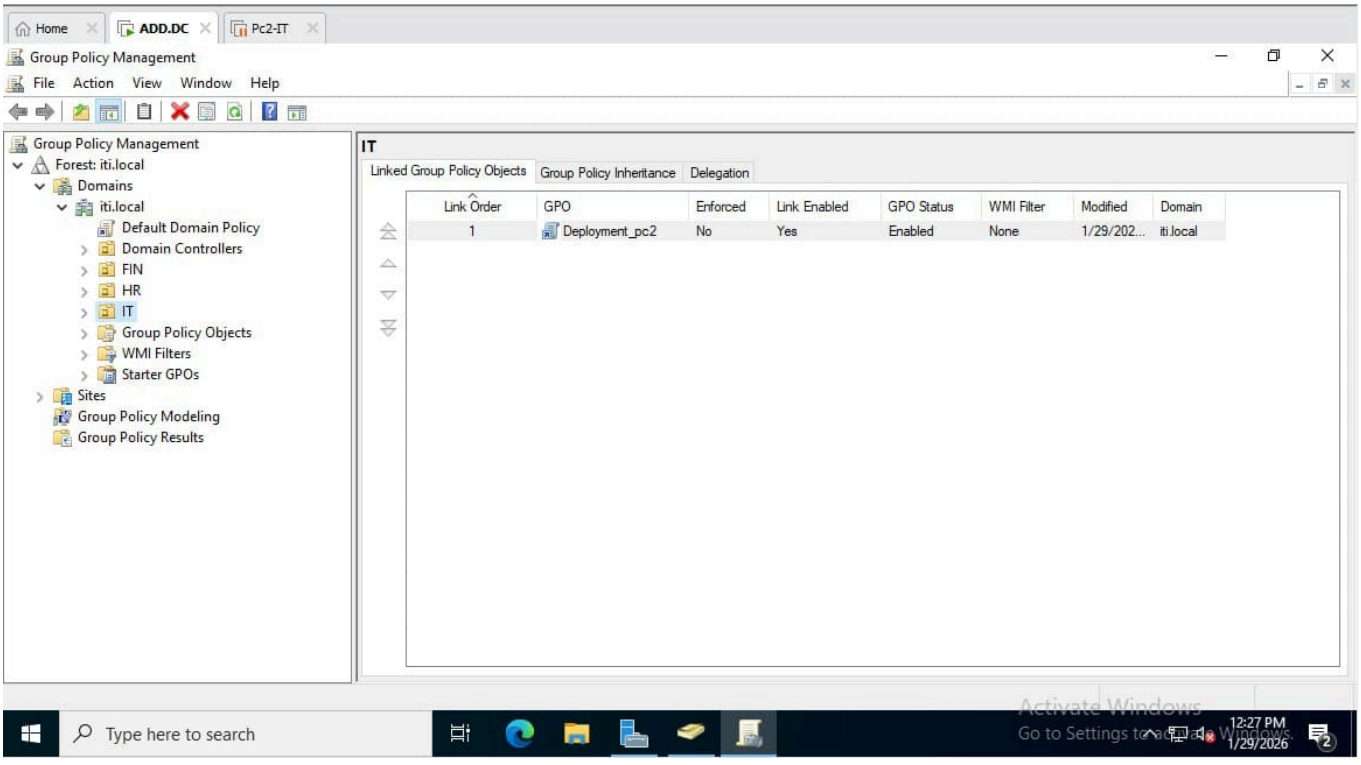


3.5 Installing WinRAR

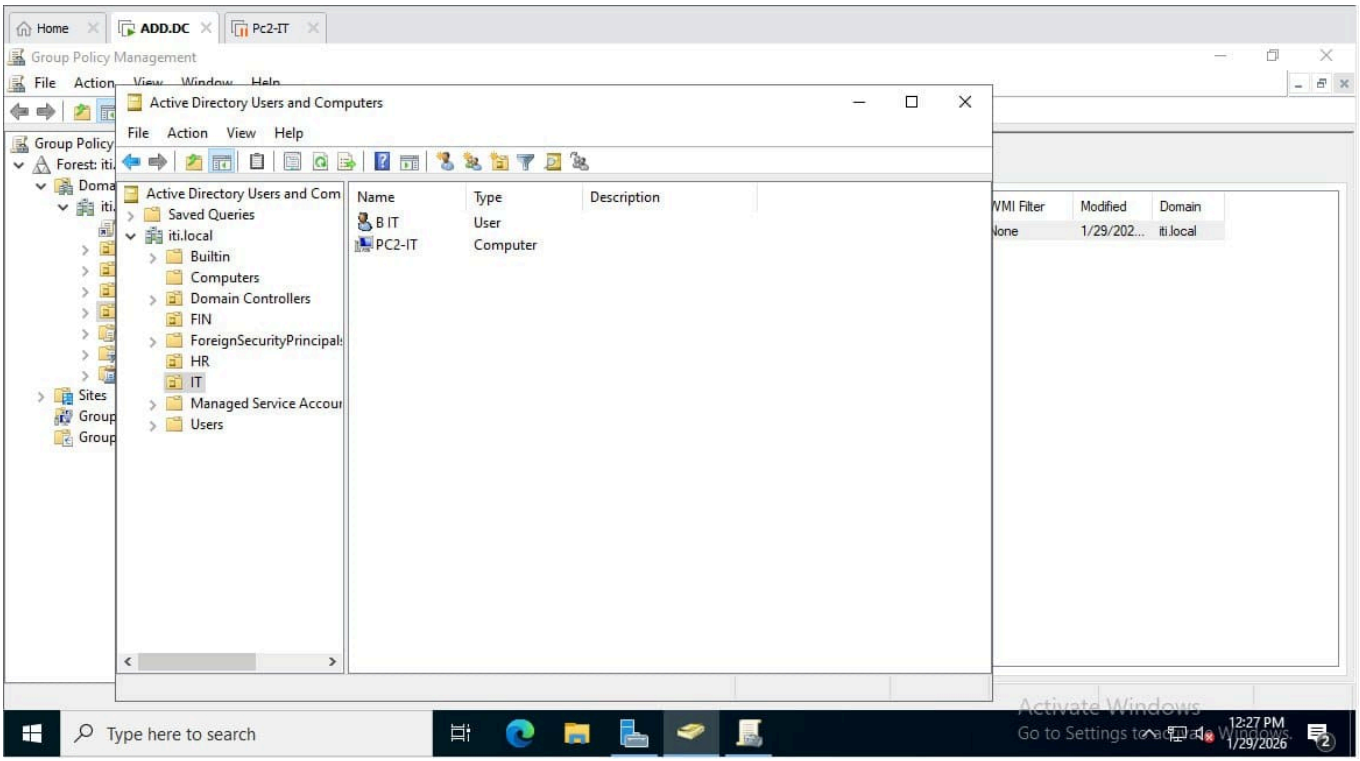
The **Group Policy Management Editor** shows the configuration of the software package. Under **Computer Configuration > Policies > Software Settings**, the WinRAR installation is established. This ensures that the deployment is handled at the machine level, targeting the computer's operating system environment.



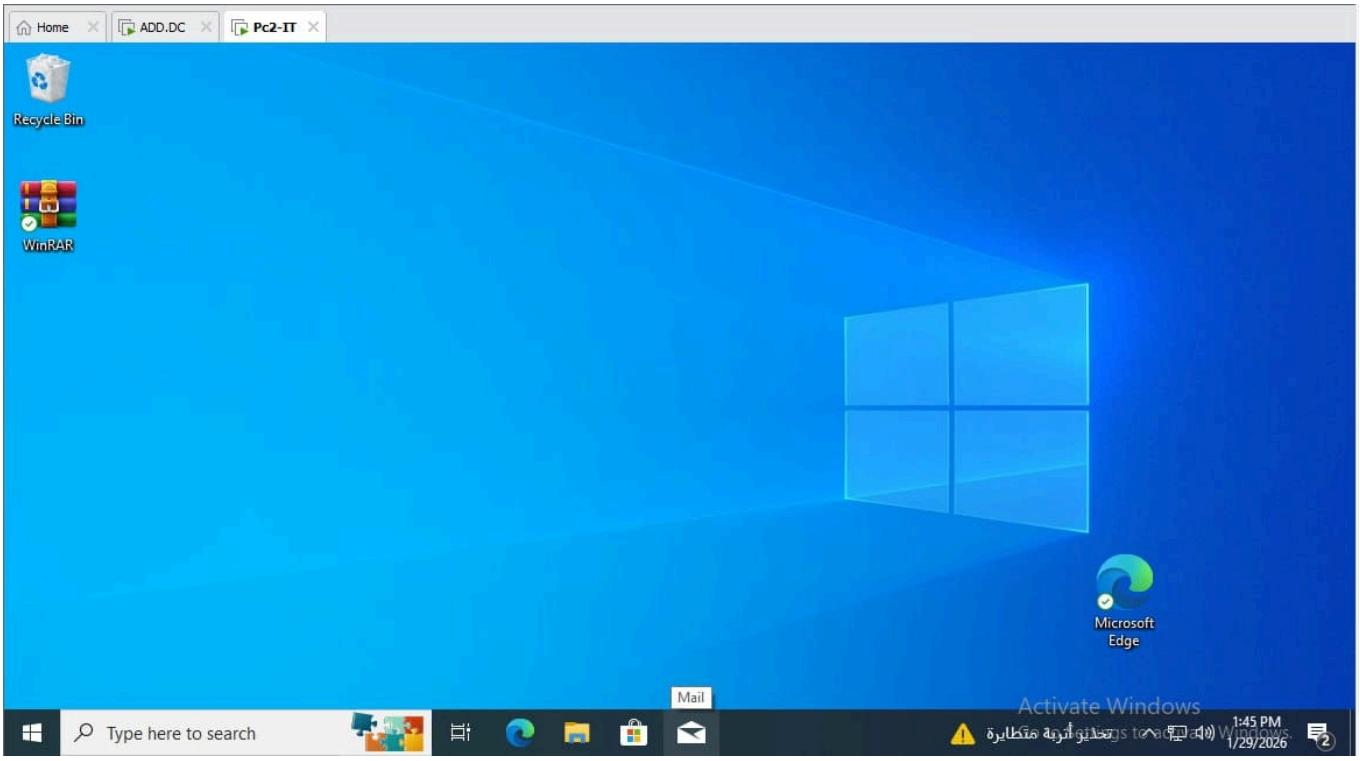
The deployment properties window confirms that the WinRAR package is set to **Assigned**. This specific configuration triggers the automatic installation of the software, ensuring that the package is deployed to the system without requiring any interaction from the user during the setup process.



The **Group Policy Management** console displays the **"Deploy_pc2"** GPO as it is linked to the target Organizational Unit (OU) IT. This confirms the logical scope of the policy, ensuring that the software deployment is directed specifically to the computers within that defined container.



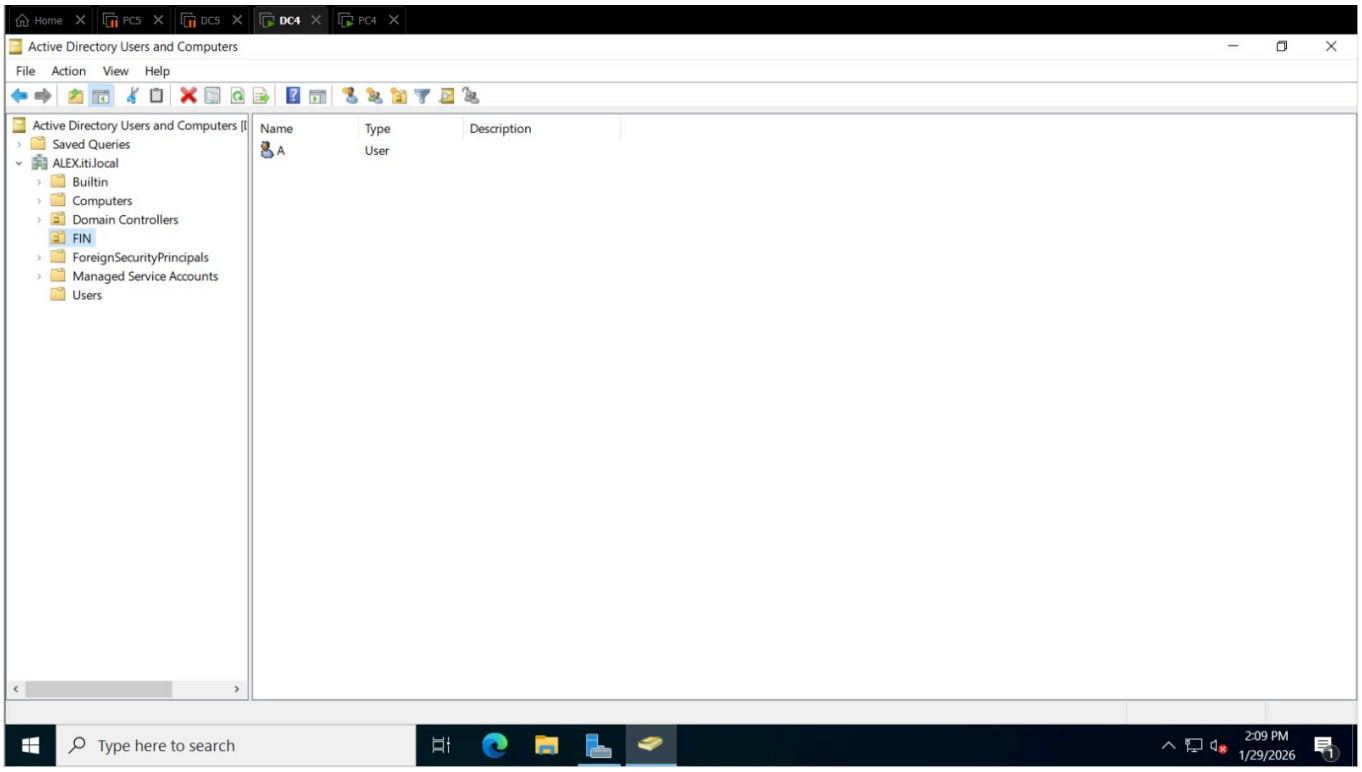
The result is verified on **PC1**, showing the **Start Menu** and **File Explorer** after the policy has been processed. **WinRAR** is present in the application list and fully integrated into the Windows shell, confirming that **PC1** successfully received the policy and completed the installation.



4. Child Domain

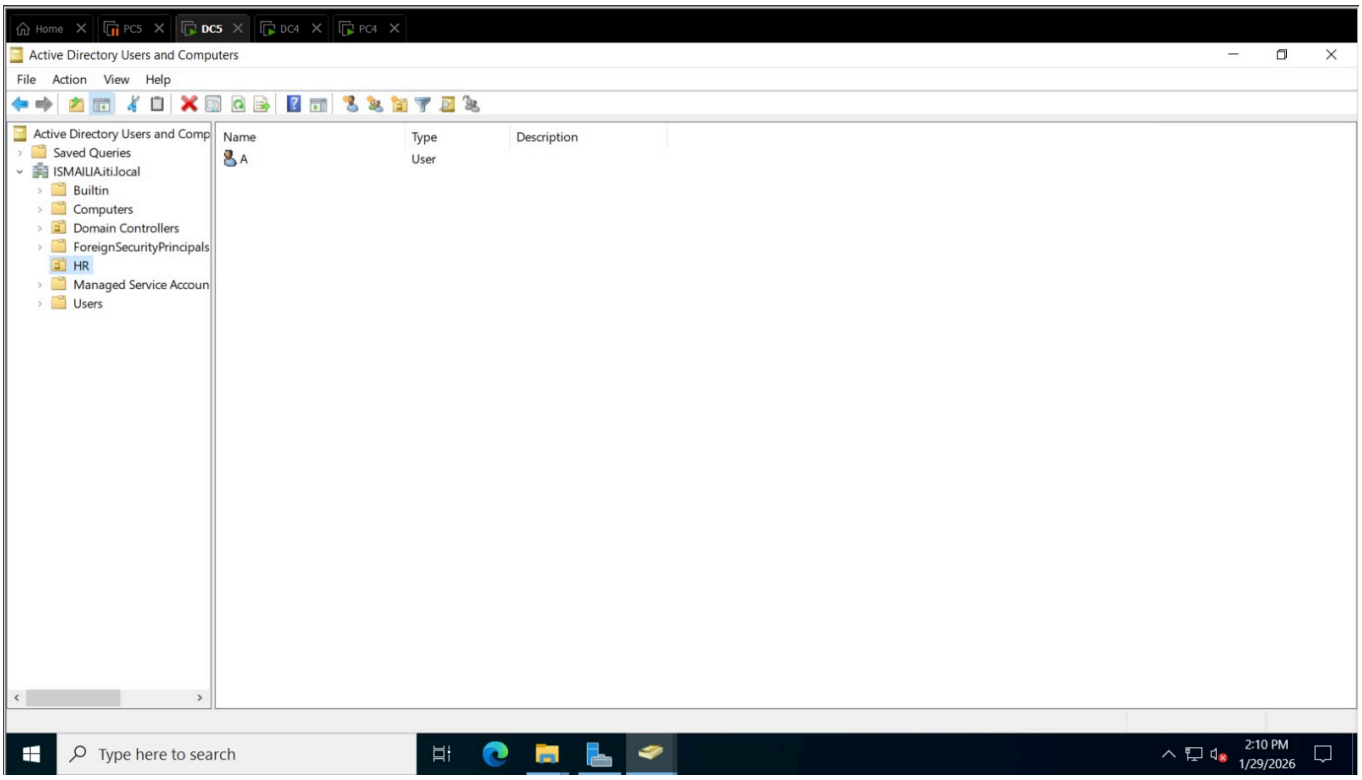
4.1. Alex

ALEX.iti.local This is the child domain established for the Alexandria branch with **DC4** as its domain controller. Inside this domain, a specific Organizational Unit (OU) named **FIN** has been created to manage the users and resources of the Alexandria finance department.



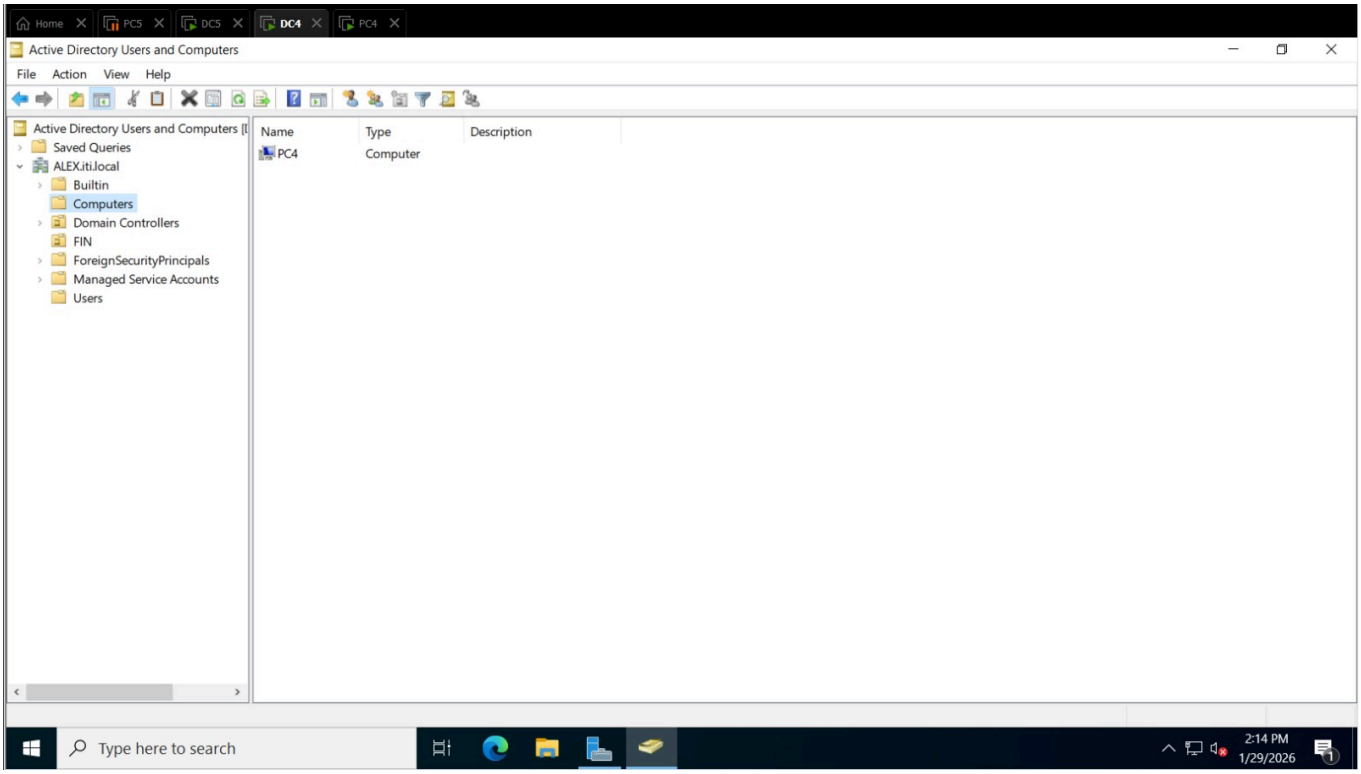
4.2. Ismailia

This is the child domain established for the Ismailia branch with **DC5** as its domain controller. Similarly, it contains an Organizational Unit (OU) named **FIN** to centralize and manage the accounts for the finance department in the Ismailia branch.

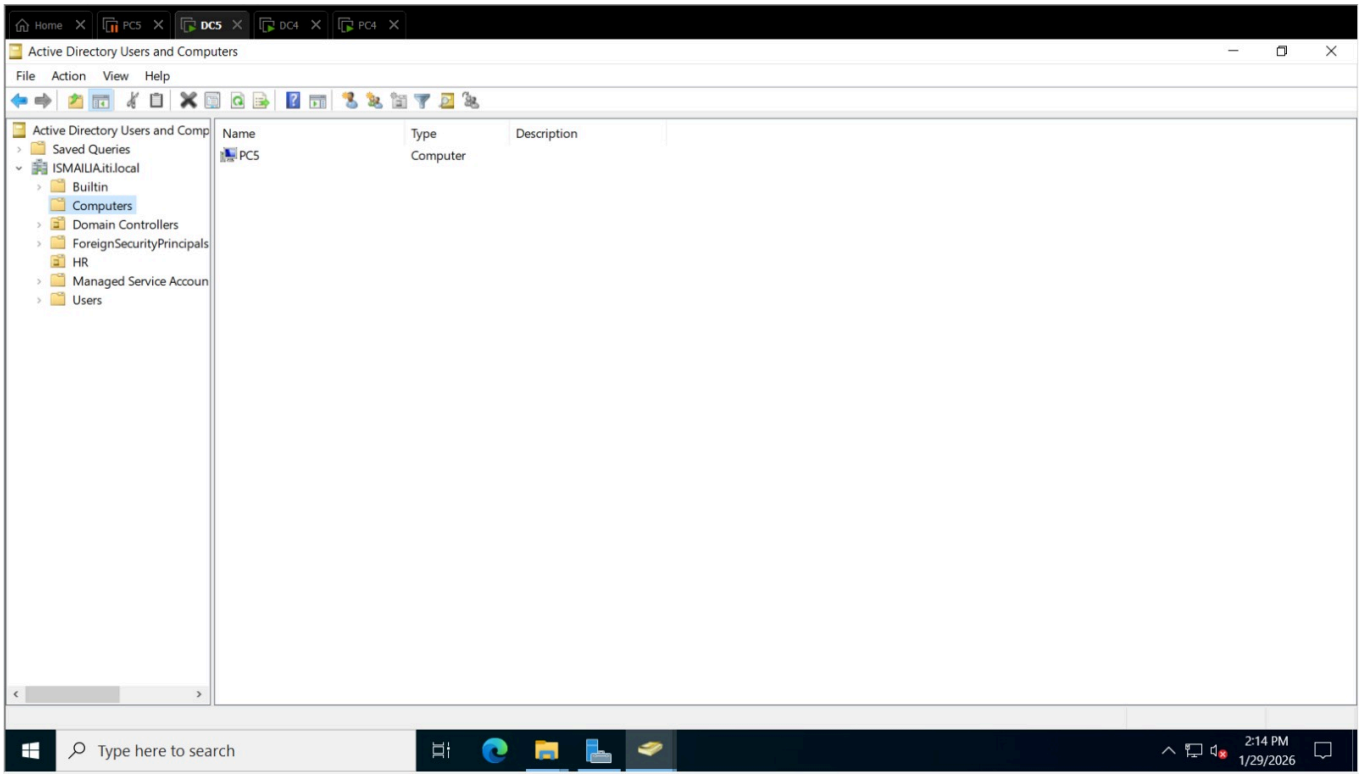


4.3. Branch Workstation Domain Integration

PC4 Joined ALEX Domain PC4 functions as a member workstation within the **ALEX.iti.local** child domain.



PC5 Joined Ismailia Domain PC5 is integrated into the **ISMAILIA.iti.local** child domain as a managed workstation.

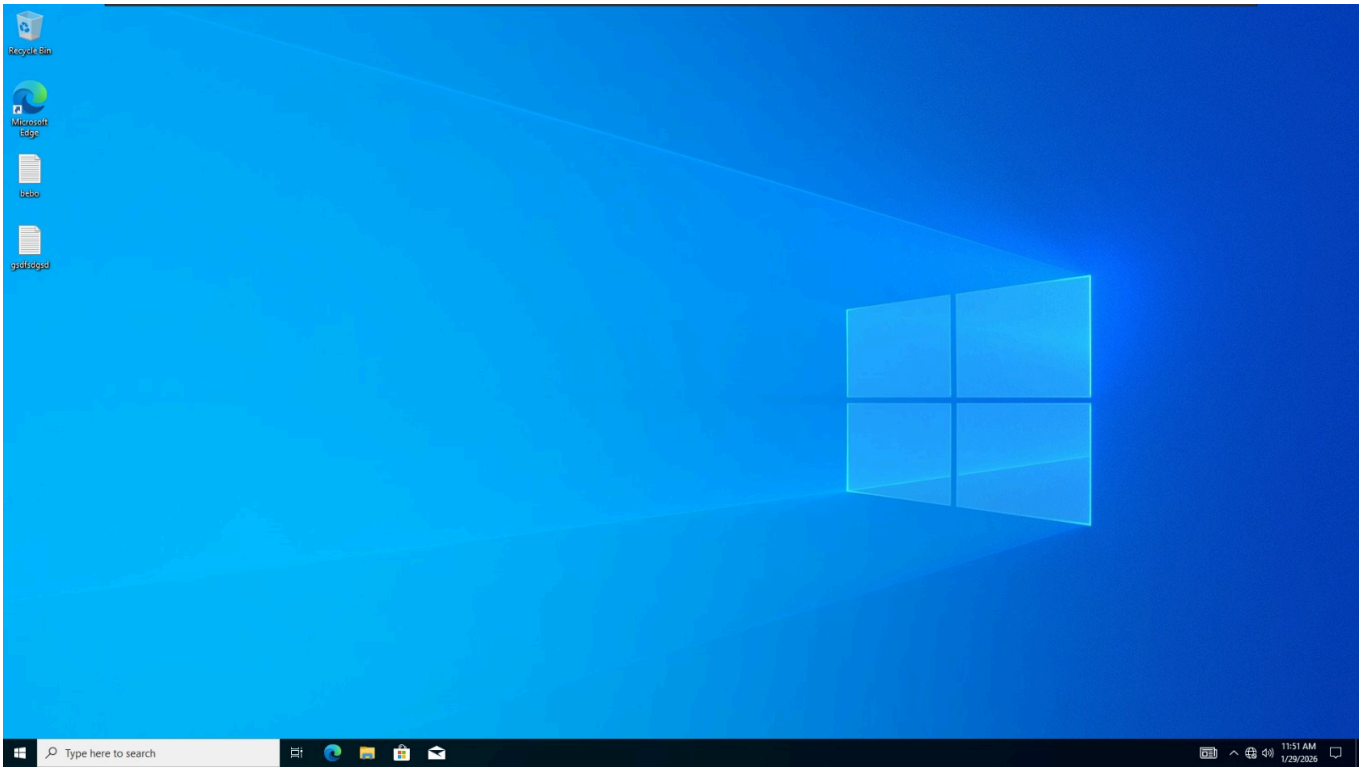


5. Roaming

A shared folder is created on the server to act as the central repository for user data. The sharing and NTFS permissions are configured to allow "Domain Users" to create their own profile folders while ensuring data privacy and security across the **iti.local** forest.

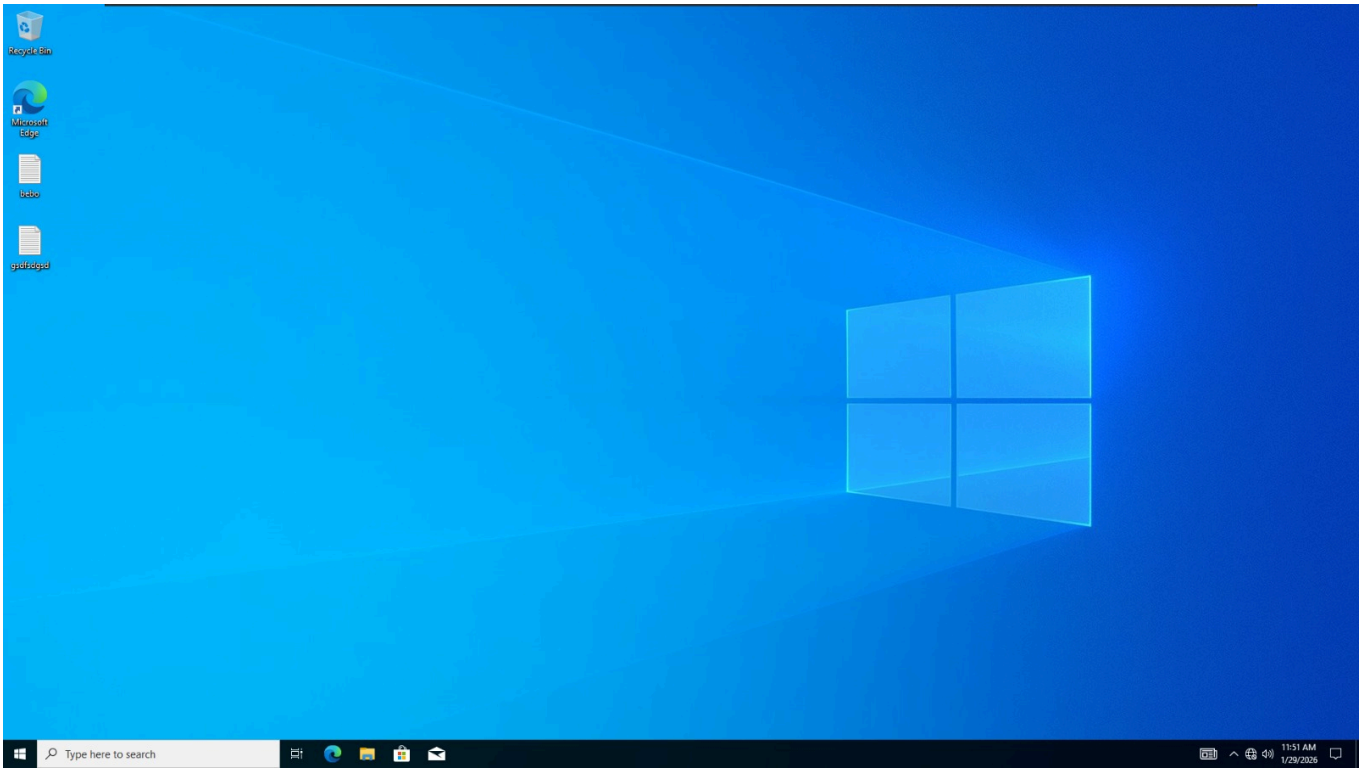
5.1. Environment Creation on PC1

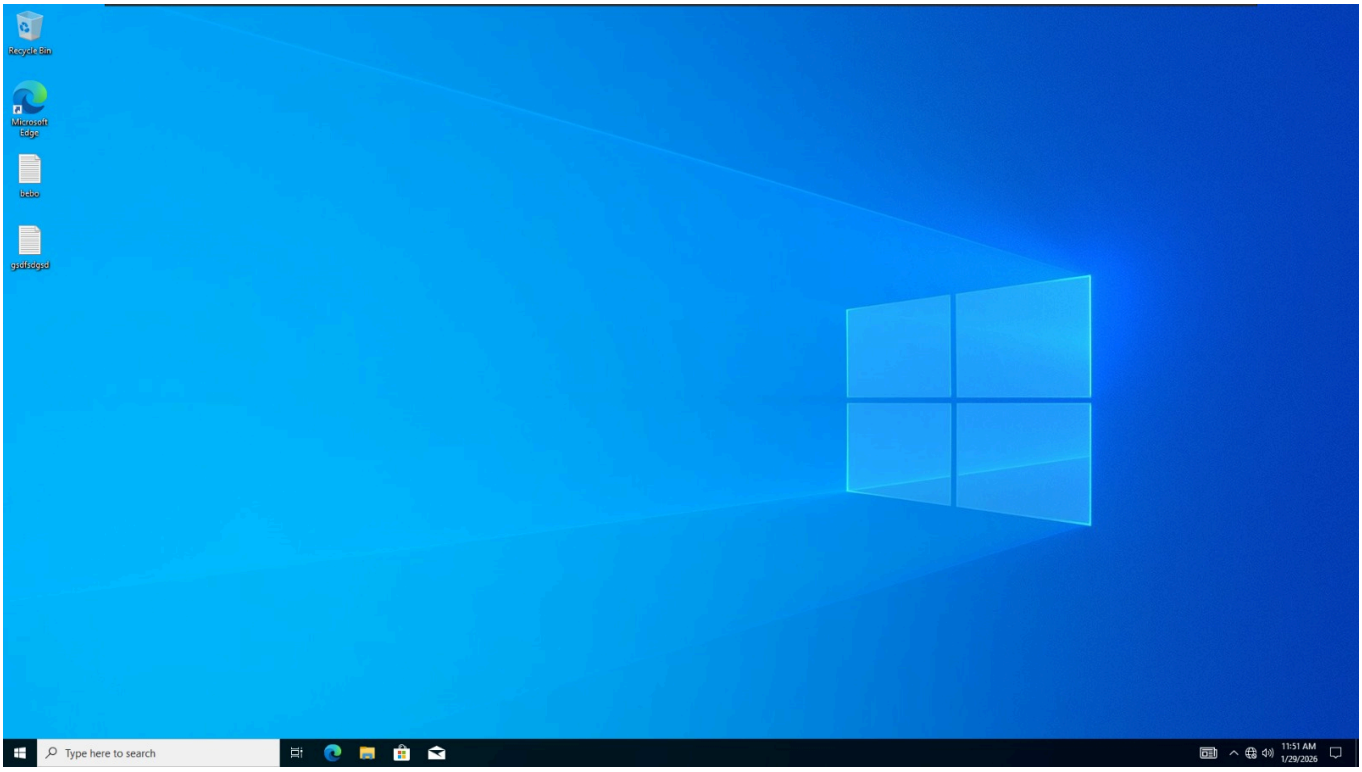
The user performs an initial login on **PC1**. During this session, a test file or folder is created on the desktop. When the user logs out, the local profile is synchronized and uploaded to the centralized **Profiles** folder on the server.



5.2. Roaming Verification on PC4 and PC5

The user signs into **PC4** in the **ALEX** domain and **PC5** in the **ISMAILIA** domain. In both instances, the desktop files created on PC1 are immediately visible and accessible. This demonstrates that the roaming profile is successfully retrieved across different child domains, providing a consistent user experience on both branch workstations.

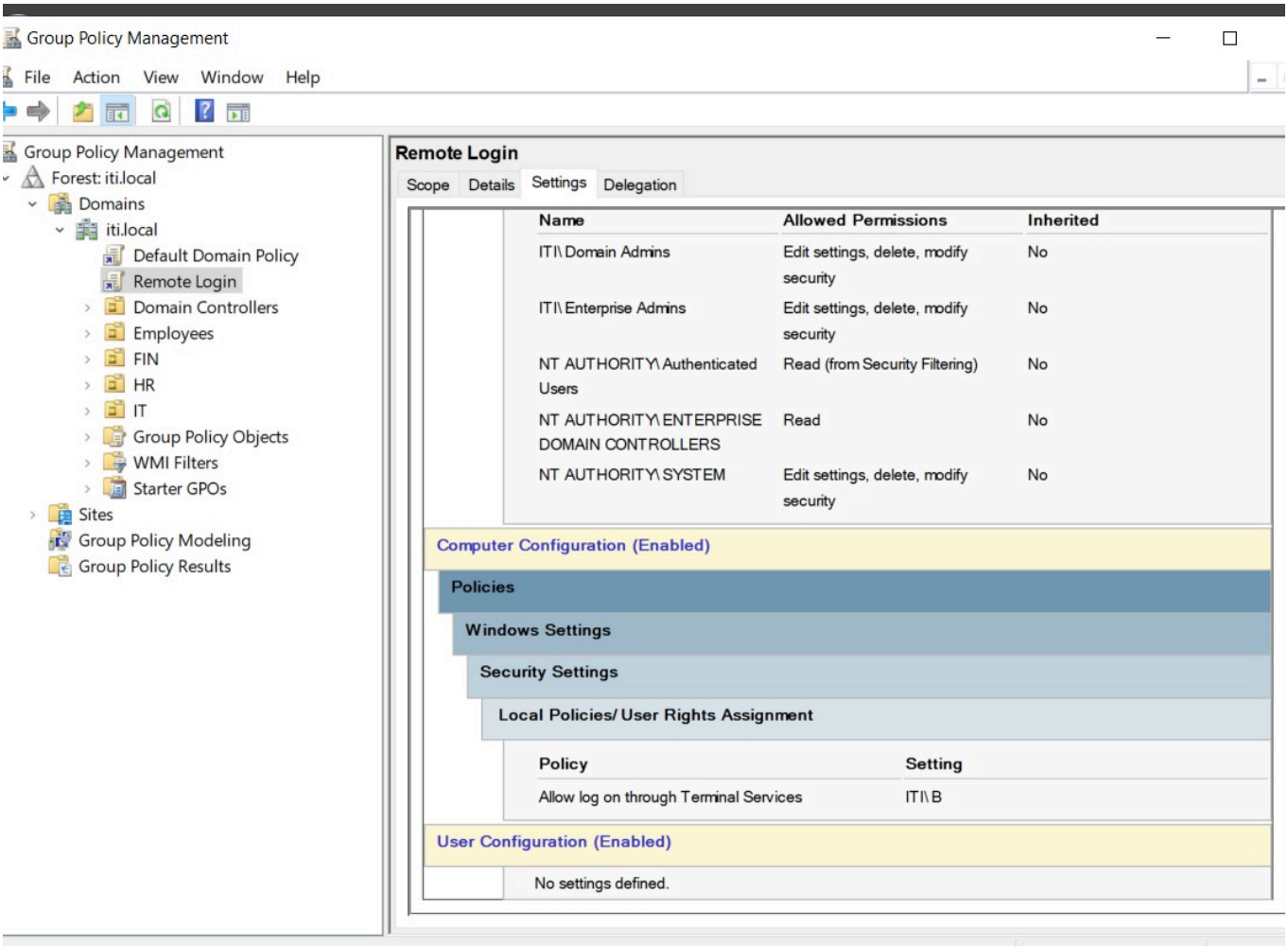




6. Delegation

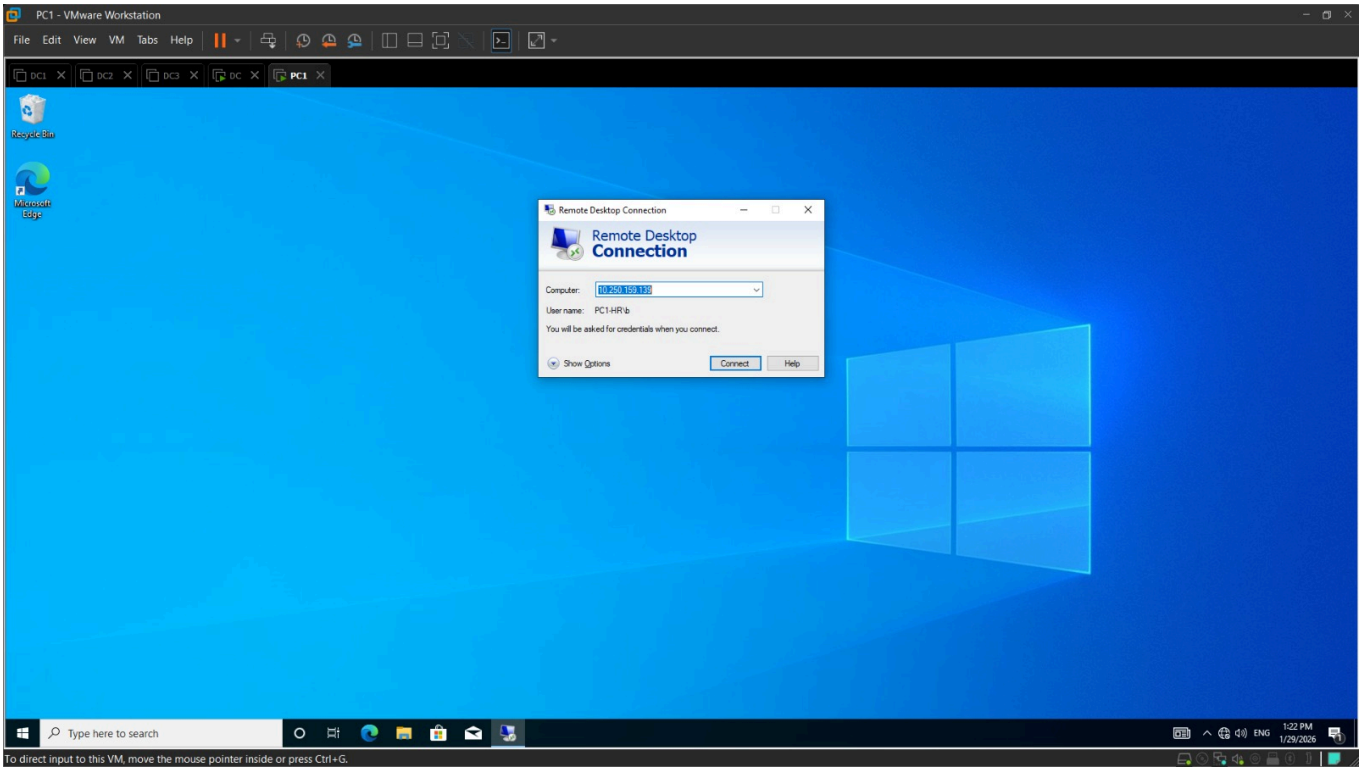
6.1 Group Policy Configuration for RDP

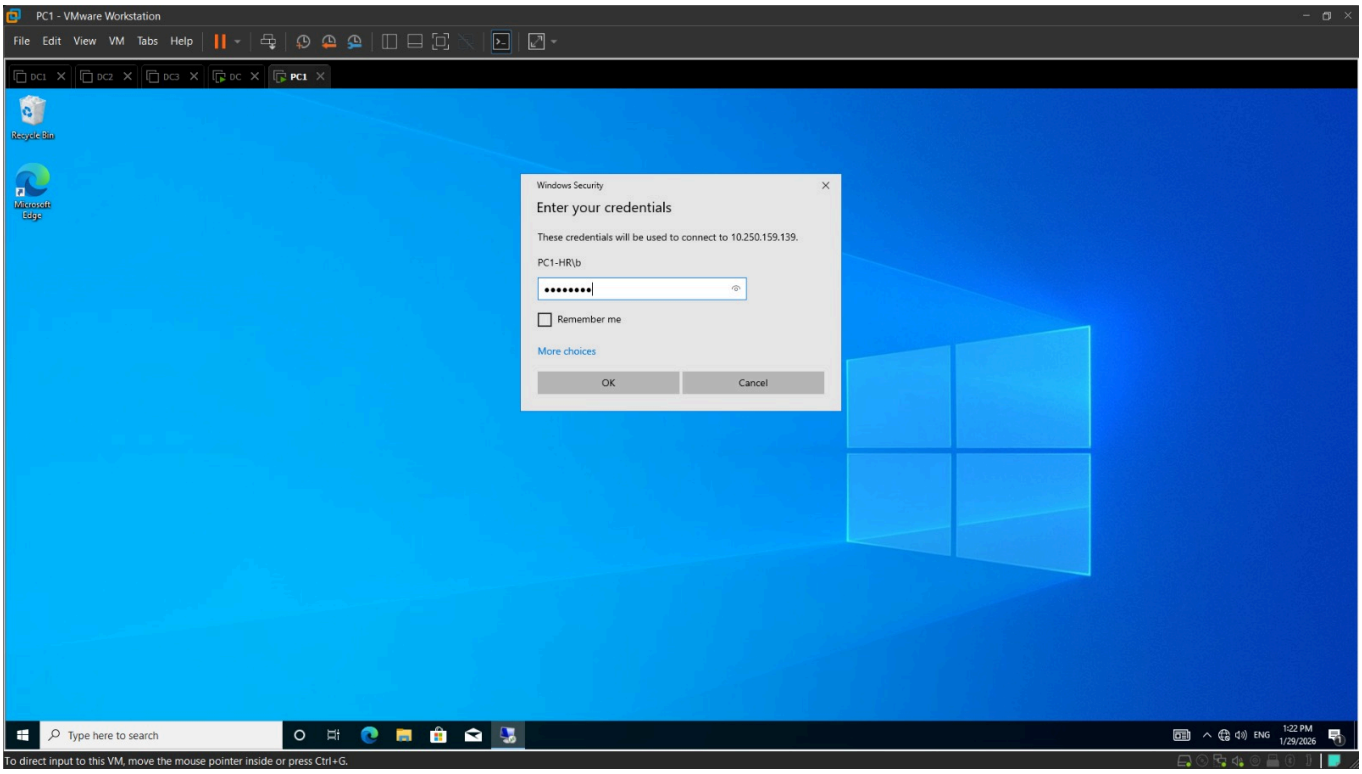
In the **Group Policy Management Editor**, the policy **"Allow log on through Remote Desktop Services"** is modified. **User B** is explicitly added to this security setting within the GPO linked to the Domain Controllers. This administrative step overrides the default restriction that prevents non-administrators from logging into a domain controller remotely.



6.2 Remote Desktop Connection Setup

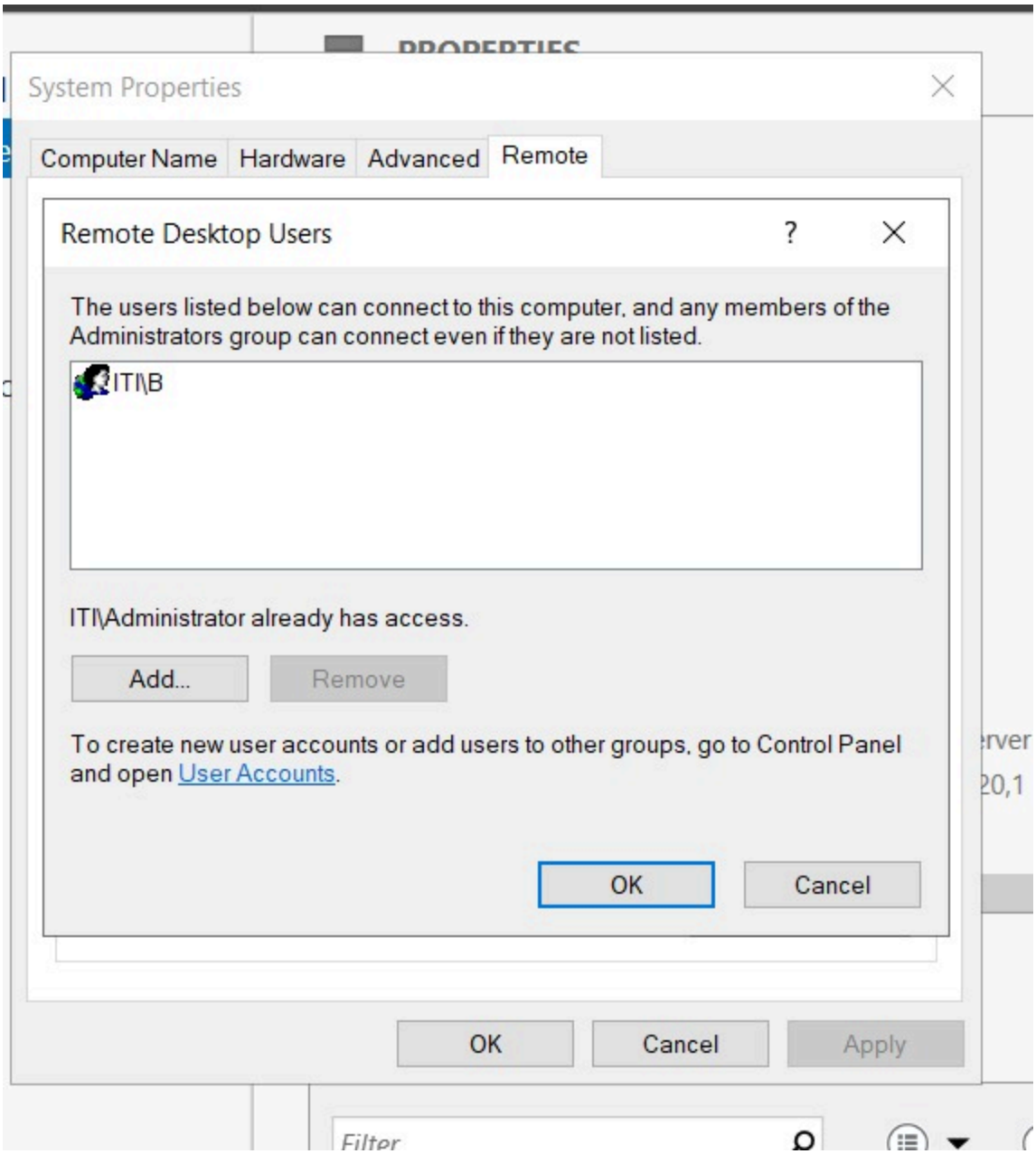
The **Remote Desktop Connection** utility is opened on a client workstation, with the target address set to **DC1**. **User B** enters their domain credentials, initiating the authentication process. This visualizes the practical application of the delegation, where a standard user account is used to access server-side resources.





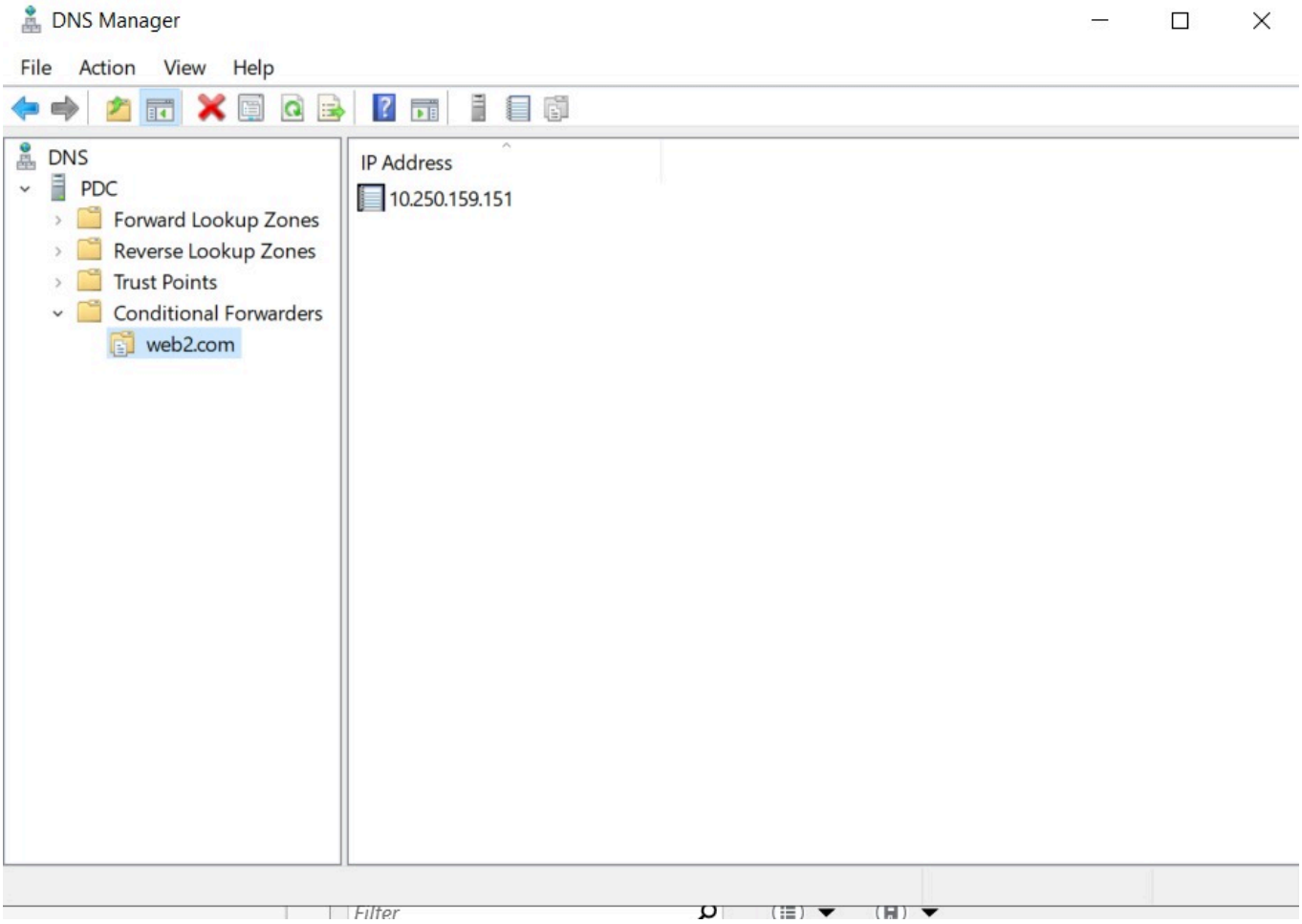
6.3. Verification of Remote Access on DC1

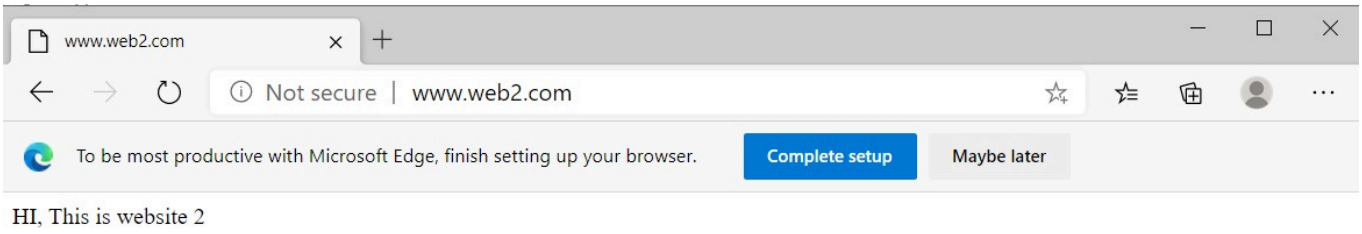
The successful remote session on **DC1** is shown, with the desktop environment active for **User B**. This confirms that the delegation settings are correctly applied and that the user can perform managed tasks on the domain controller within their restricted permission set, proving the security configuration is functional.



7. Website Check Using Conditional Forwarding

The **DNS Manager** on the **PDC** shows a conditional forwarder configured for the domain **web2.com**. This setting ensures that any DNS queries for this specific domain are automatically forwarded to the IP address **10.250.159.151**, allowing the local network to resolve names for that external or separate infrastructure correctly.


DNS Manager
File
Action
View
Help
DNS
PDC
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
web2.com
IP Address
10.250.159.151
Filter

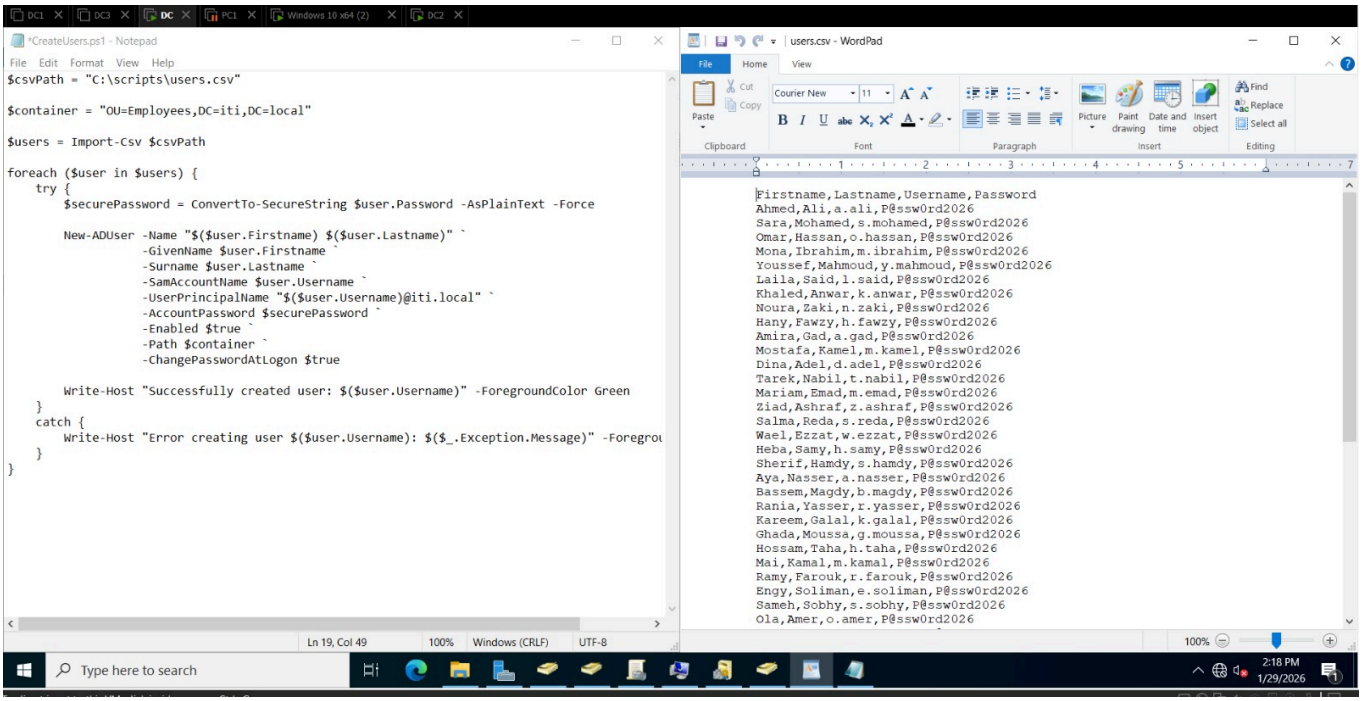


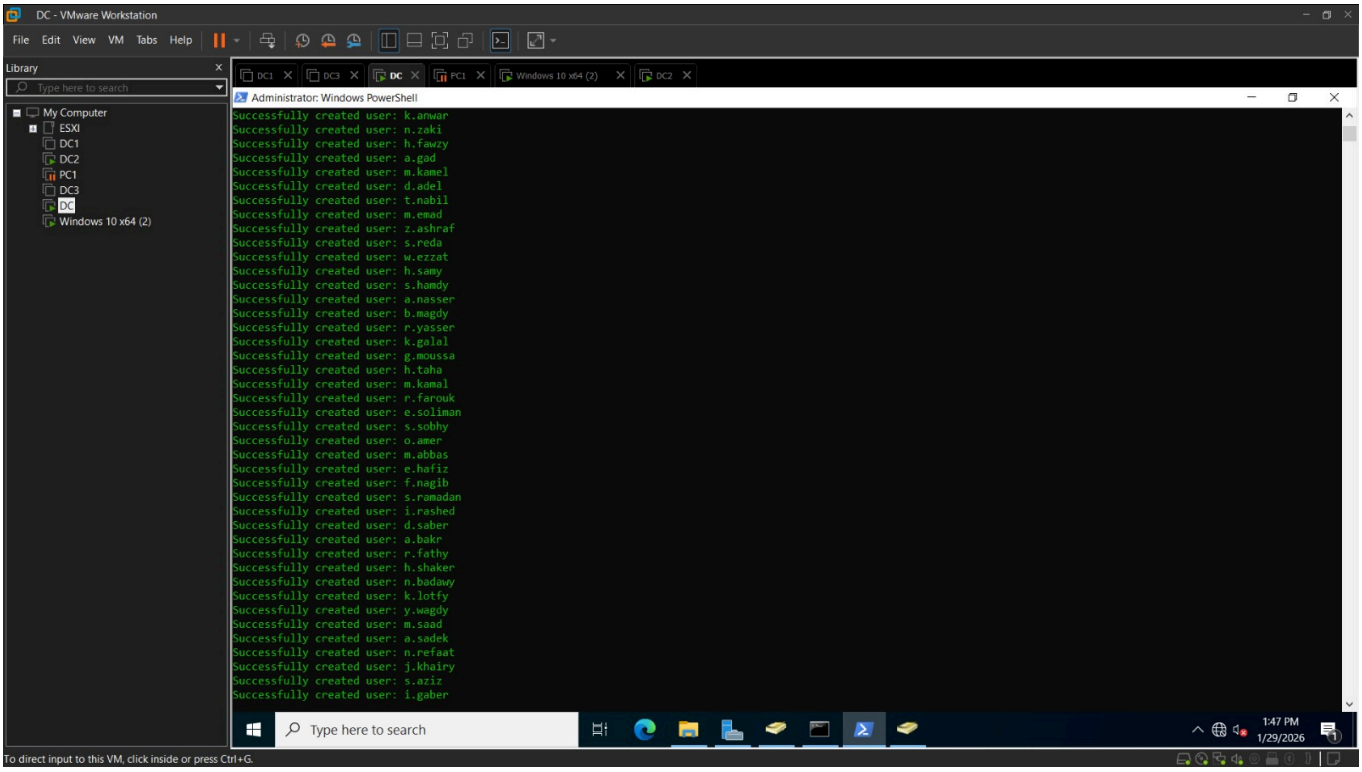
---

8. Script For Creating 50 Users

Automation is implemented using a **PowerShell** script designed to bulk-create user accounts from a CSV file.

- **Script Logic**: The script imports data from `users.csv` and iterates through each entry to create a new Active Directory user with properties including **First Name**, **Last Name**, **Username**, and a secure **Password**.
- **Target Container**: Users are automatically placed within the **OU=Employees,DC=iti,DC=local** organizational unit.
- **Execution Verification**: The PowerShell console displays "Successfully created user" messages for accounts such as **k.anwar**, **n.zaki**, and **h.fawzy**, confirming the batch process completed without errors.



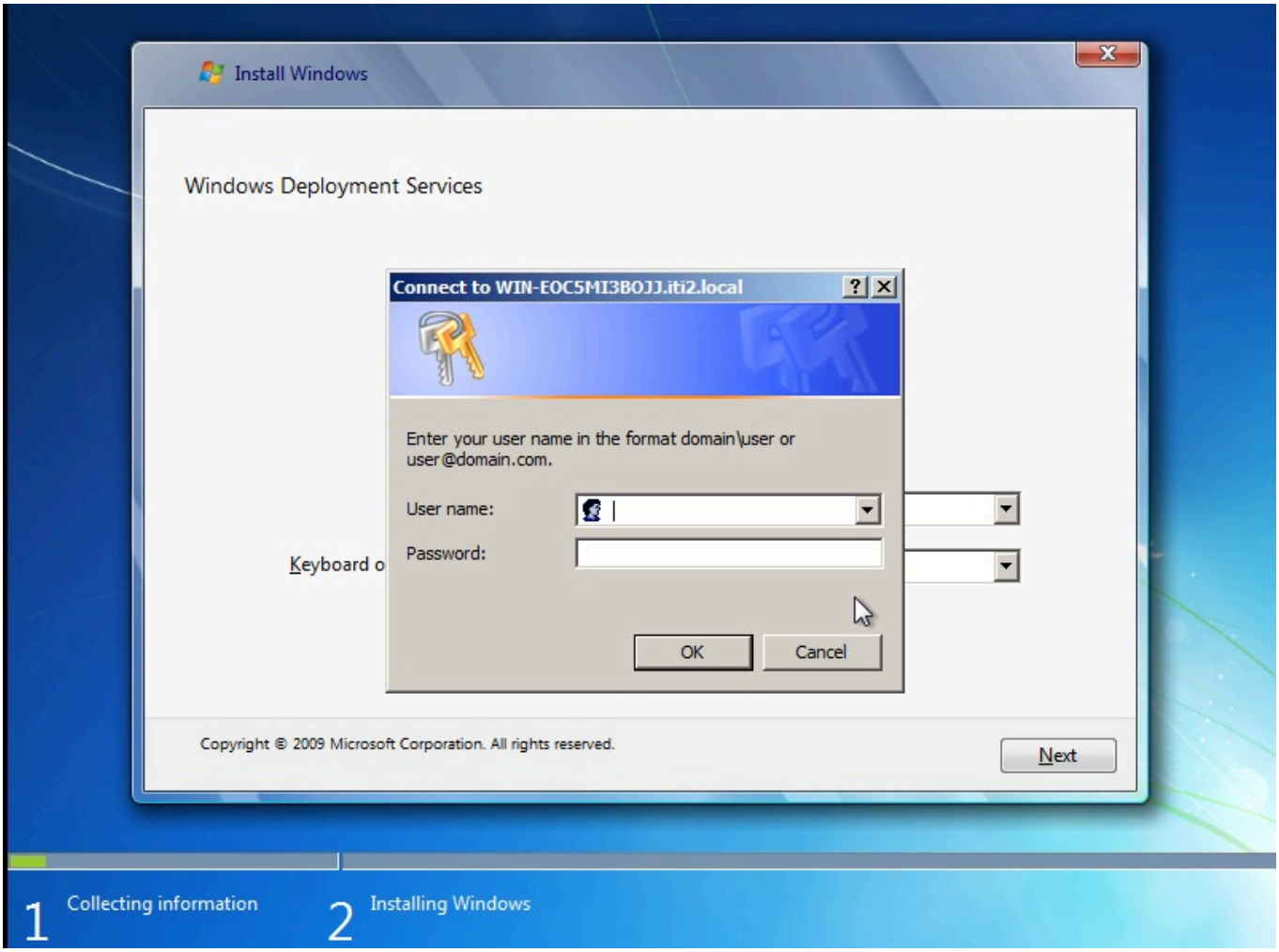


9. Windows Deployment Services

Windows Deployment Services (WDS) is a server role that enables the remote deployment of Windows operating systems. Instead of installing an OS on each machine manually using a physical disk or USB, WDS allows you to "push" the installation over the network to multiple computers simultaneously.

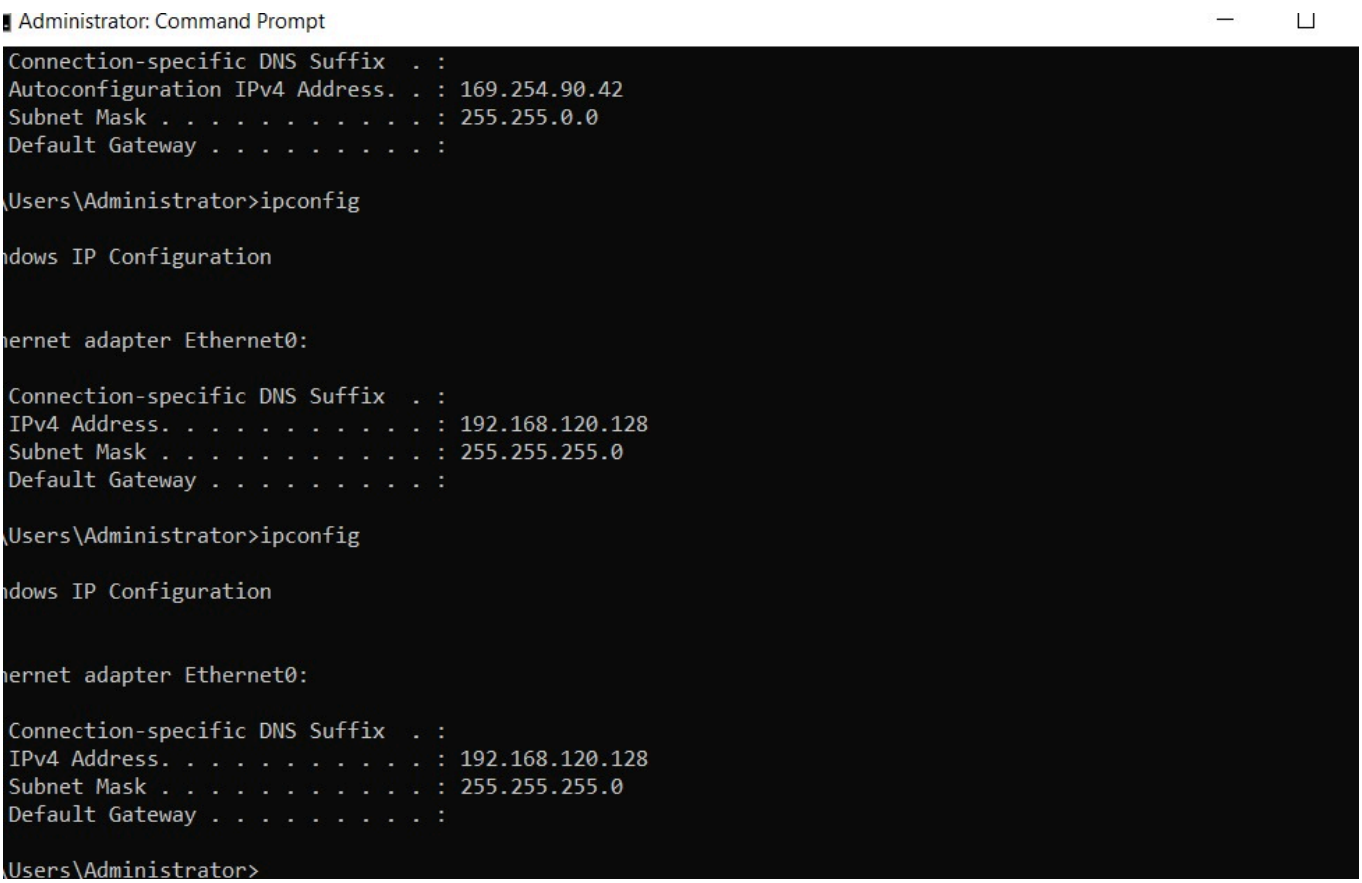
9.1. WDS Authentication

This is the **WDS Authentication** screen on the client machine. It requires a user to enter domain credentials (in `domain\user` format) to authorize the connection to the WDS server (**WIN-EOC5MI3BOJJ.iti2.local**) and start the installation.



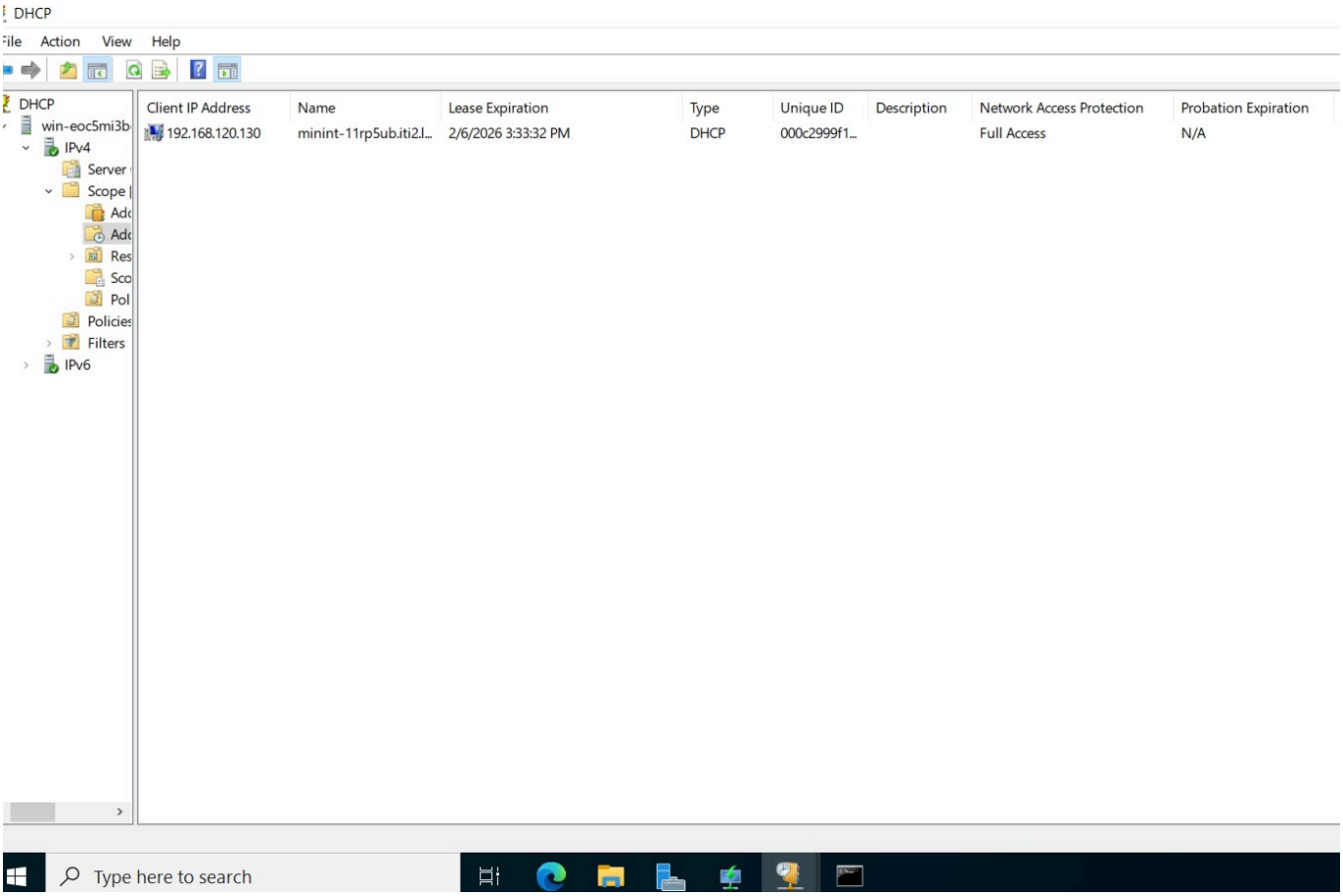
9.2. IP Address Acquisition

A command prompt window shows the results of the **ipconfig** command. It captures the transition from a self-assigned APIPA address (**169.254.90.42**) to a valid network IP address (**192.168.120.128**) provided by the DHCP server.



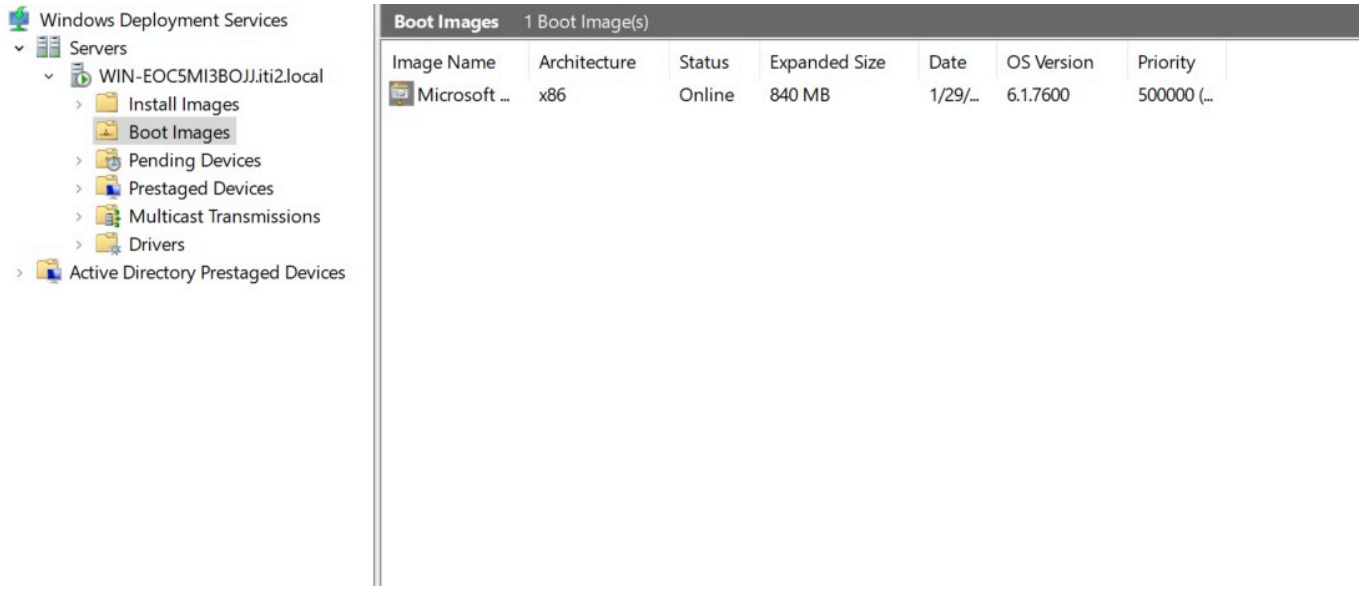
9.3. DHCP Lease Verification

The **DHCP Management** console shows the **Address Leases** for the network. It lists a specific client (**minint-11rp5ub.iti2...**) that has been assigned the IP address **192.168.120.130**, which is necessary for the client to communicate during the WDS process.

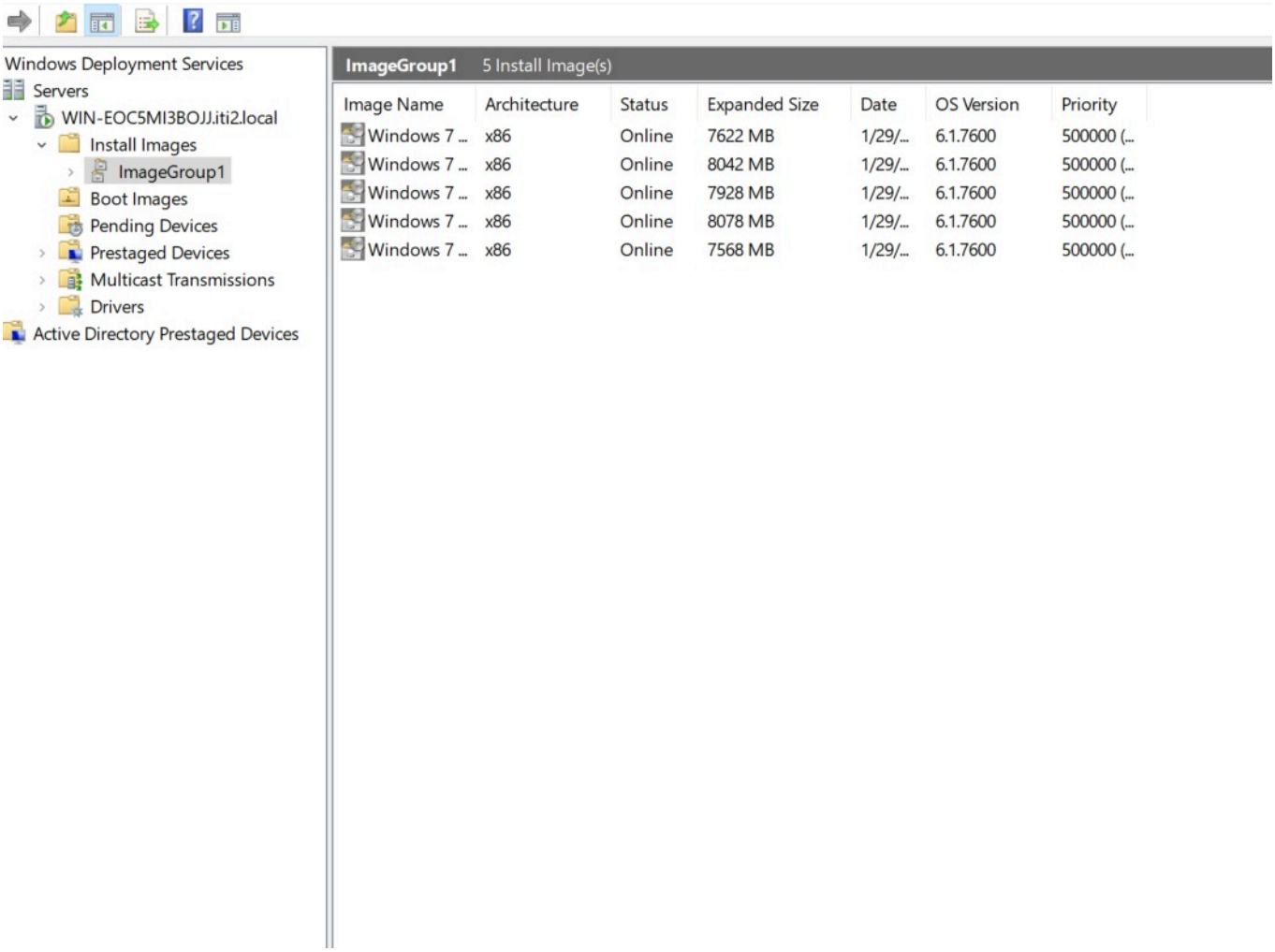


9.4. Boot and Install Image Configuration

The **WDS Manager** displays the **Boot Images** section. It shows one Microsoft Windows Setup (x86) image is "Online" and ready to be used by client computers to boot into the deployment environmen

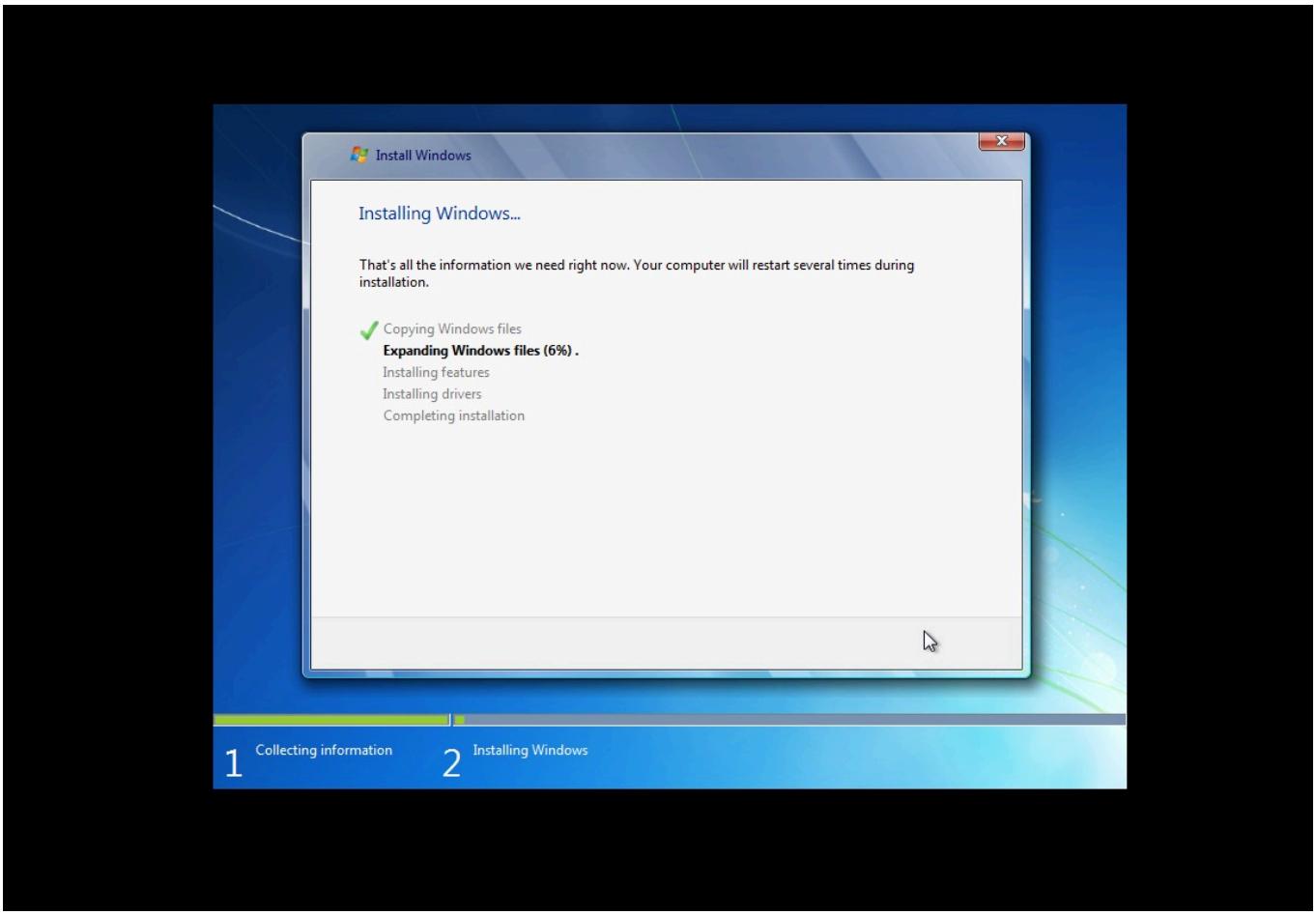


The **WDS Manager** shows the **Install Images** grouped under **ImageGroup1**. It lists five different versions of Windows 7 (x86) that are available for deployment to workstations on the network.



9.5. Deployment Progress

This is the **Installing Windows** progress screen on the client workstation. It confirms that the deployment is active.


Install Windows
Installing Windows...
That's all the information we need right now. Your computer will restart several times during installation.
Copying Windows files
Expanding Windows files (6%) .
Installing features
Installing drivers
Completing installation
1 Collecting information
2 Installing Windows