Windows server project

Under supervision: **Eng Mohamed Abosehly**

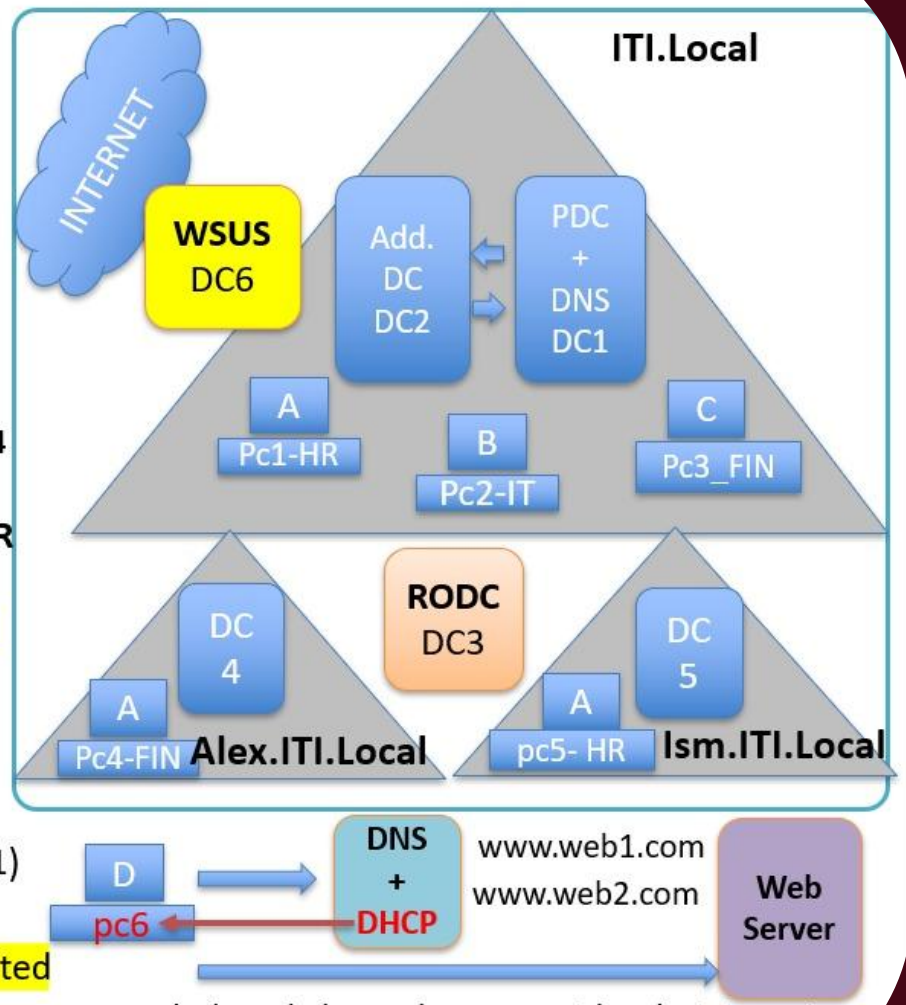
Project Overview

C1 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 (authoritative -web2.com Second Z (DC1)

Bonus , tray to configure a WSUS to make sure that your topology is updated

Topology



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 FT

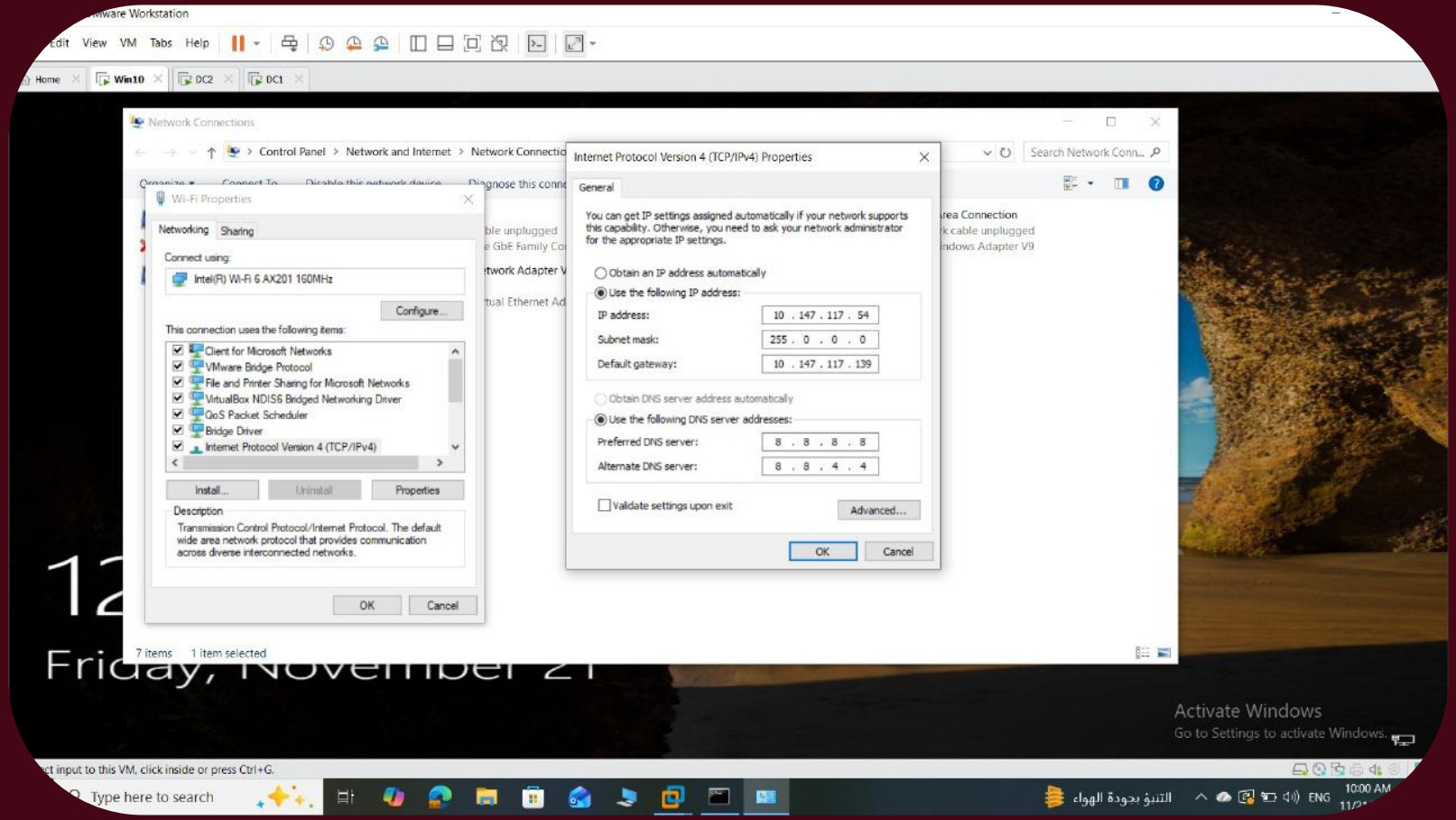
Network Setup Overview

We connected all devices using a **unified local network** created from a mobile hotspot.

To ensure **network stability and consistent communication**, we assigned **static IP addresses** to all physical PCs and virtual machines

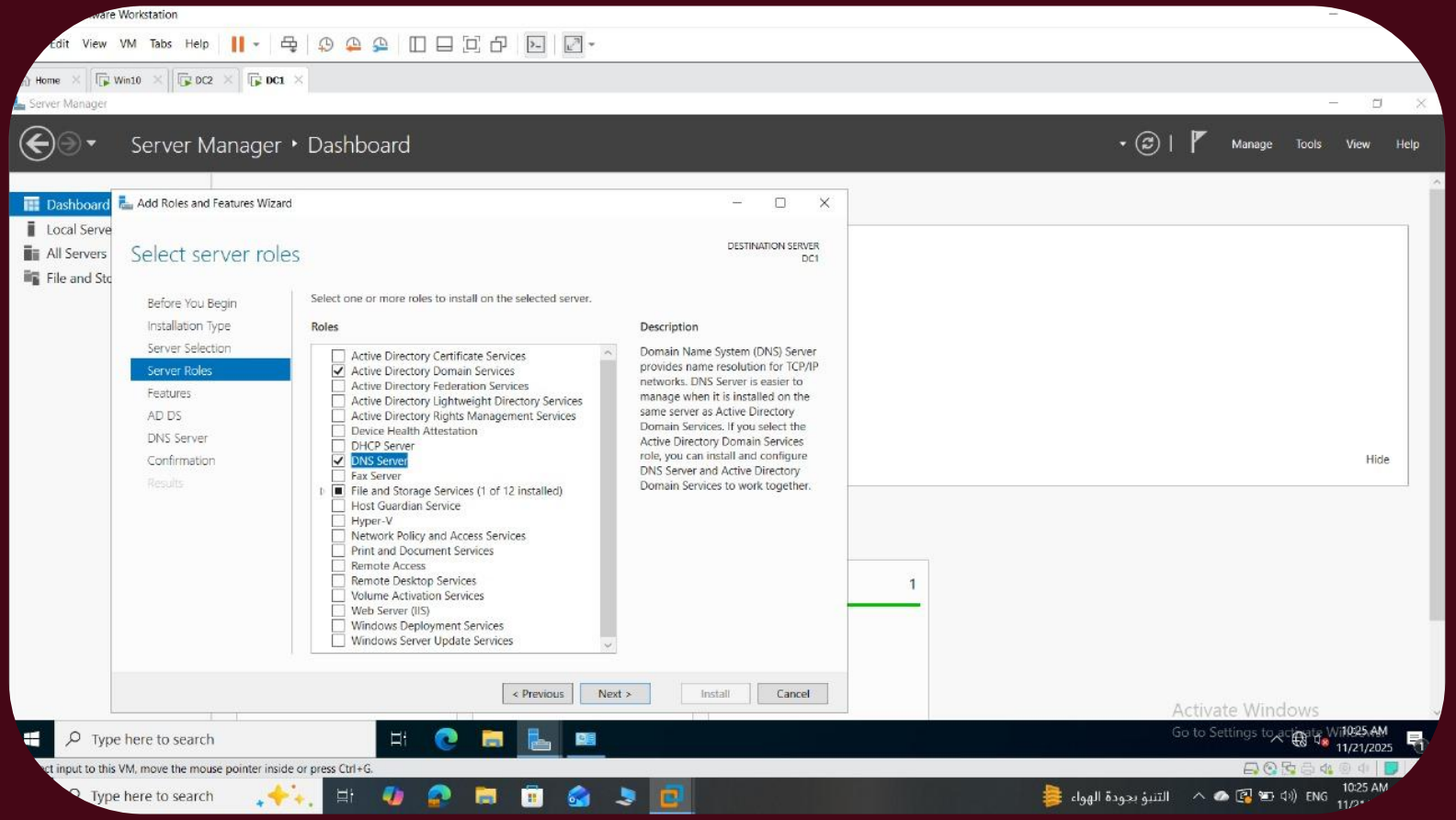
Domain Controllers Overview

"The primary Domain Controller (DC1) was assigned a static IP address to ensure stable Active Directory and DNS services across the network."



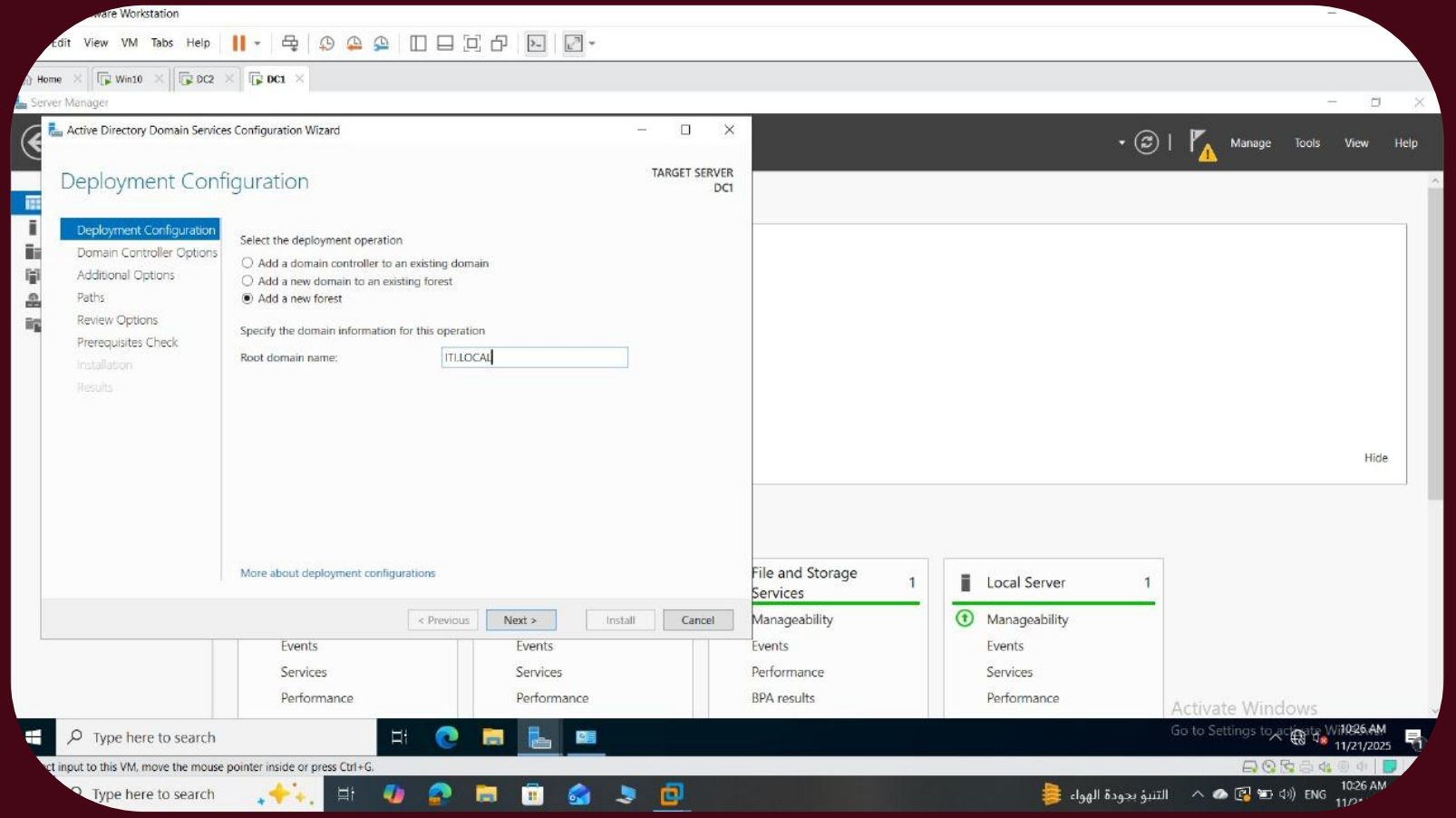
Domain Controllers Overview

"After assigning a static IP address to DC1, we installed the Active Directory Domain Services (AD DS) role to prepare the server to function as a Domain Controller."



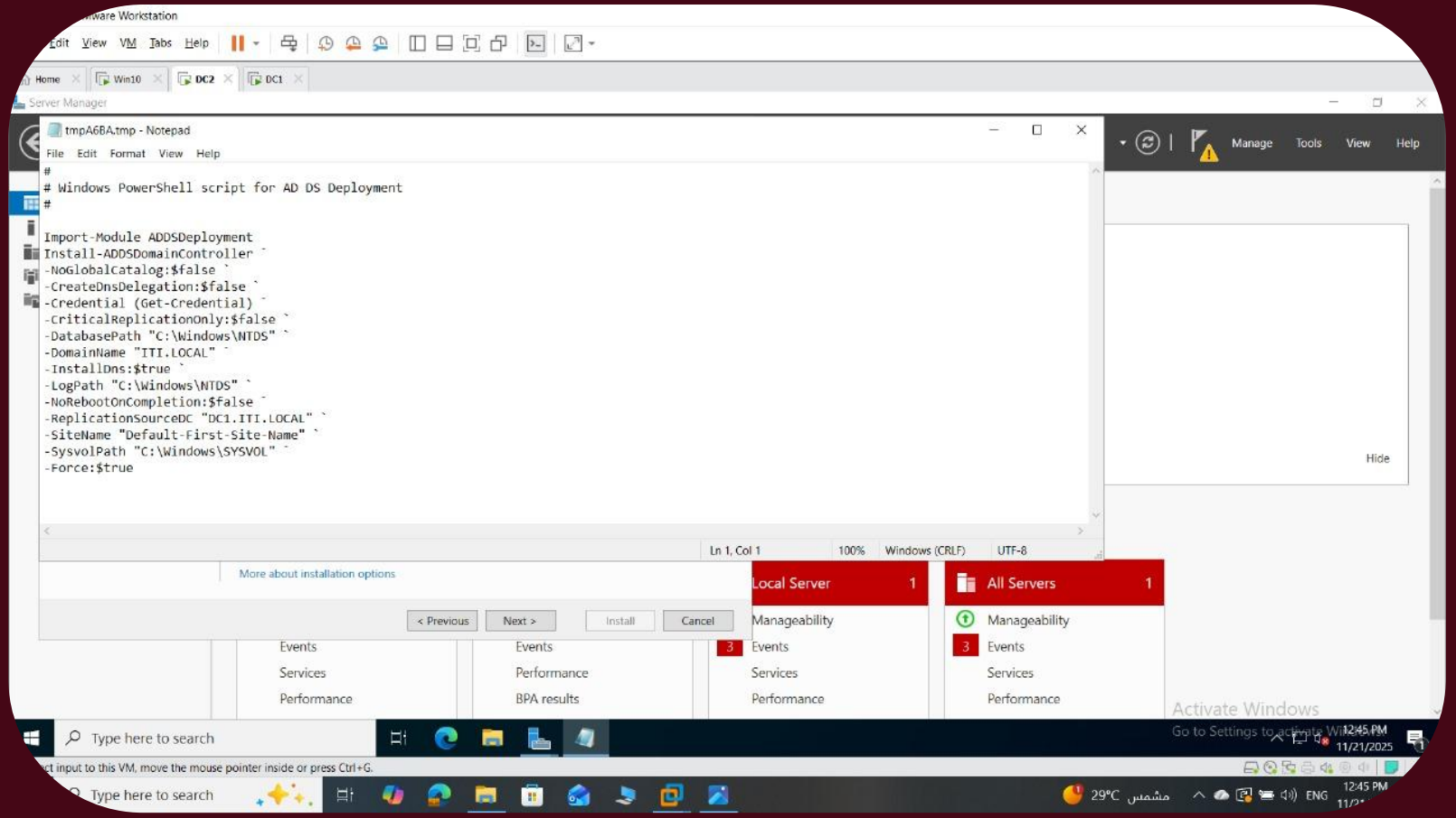
Domain Controllers Overview

"After installing the AD DS role, we configured the new domain and named it ITI.local."



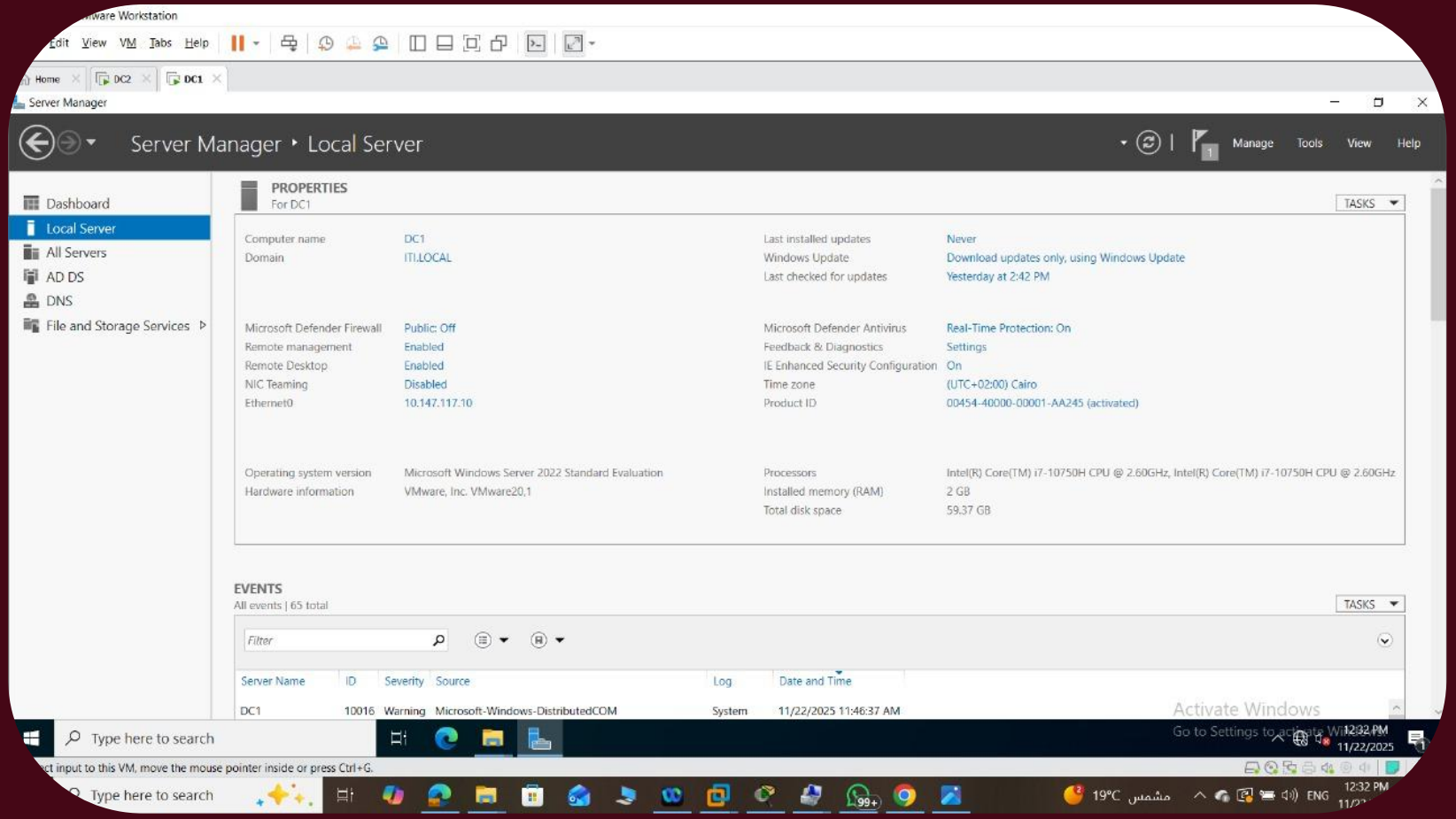
Domain Controllers Overview

"After creating the ITI.local domain, we completed the initial configuration by disabling the firewall, adjusting the time and time zone settings, and enabling Remote Desktop access on DC1."



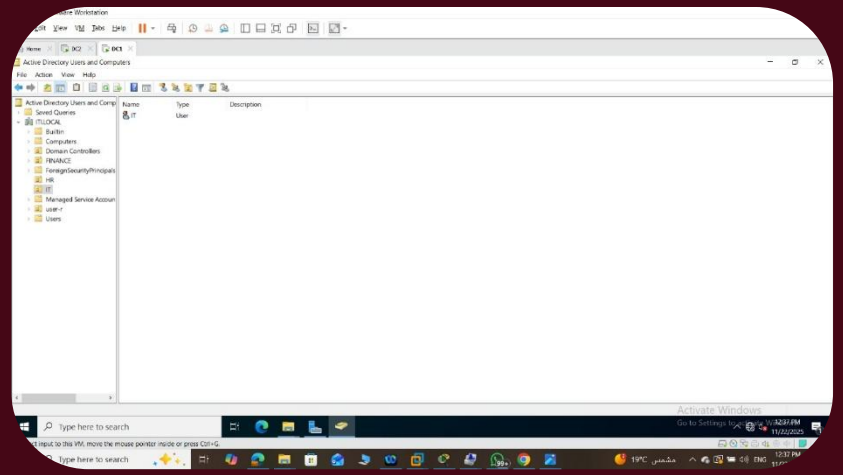
Domain Controllers Overview

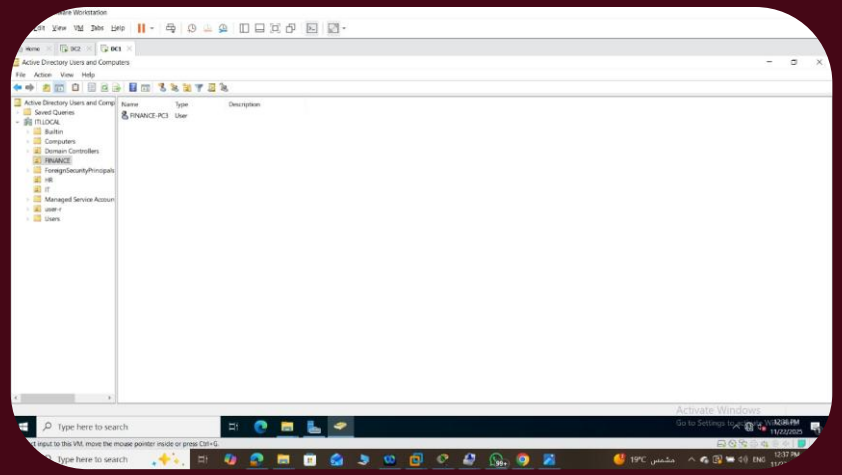
"After creating the ITI.local domain, we completed the initial configuration by disabling the firewall, adjusting the time and time zone settings, and enabling Remote Desktop access on DC1."

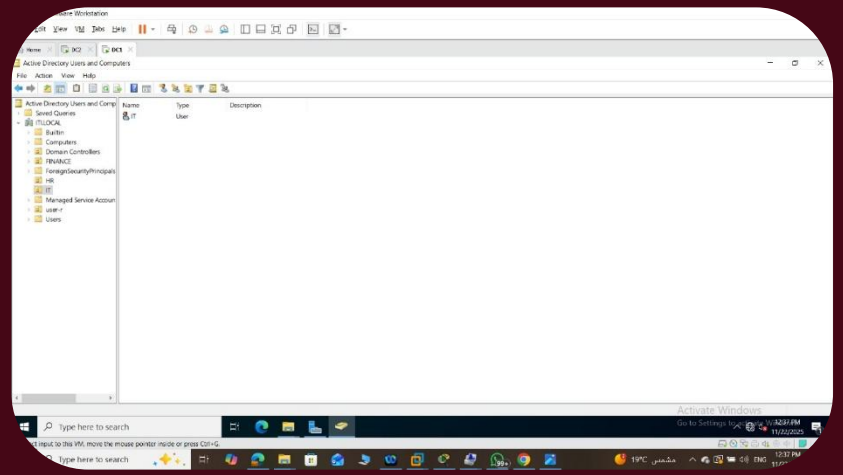


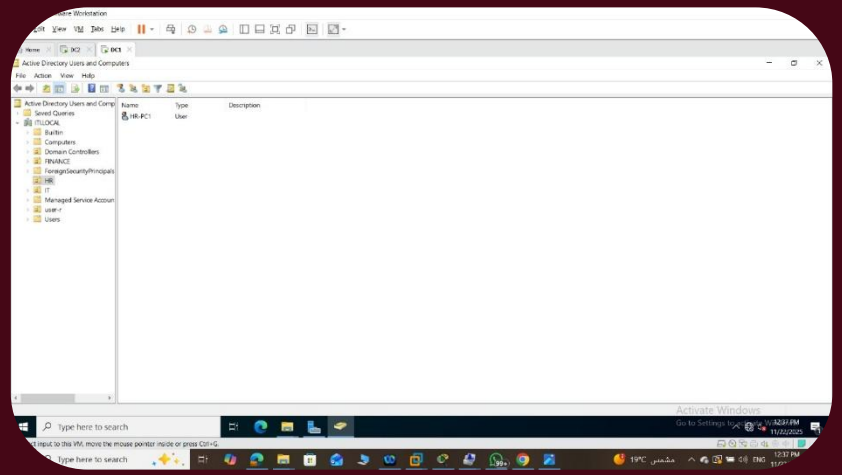
Domain Controllers Overview

Creating Organizational Units (OUs) and Users



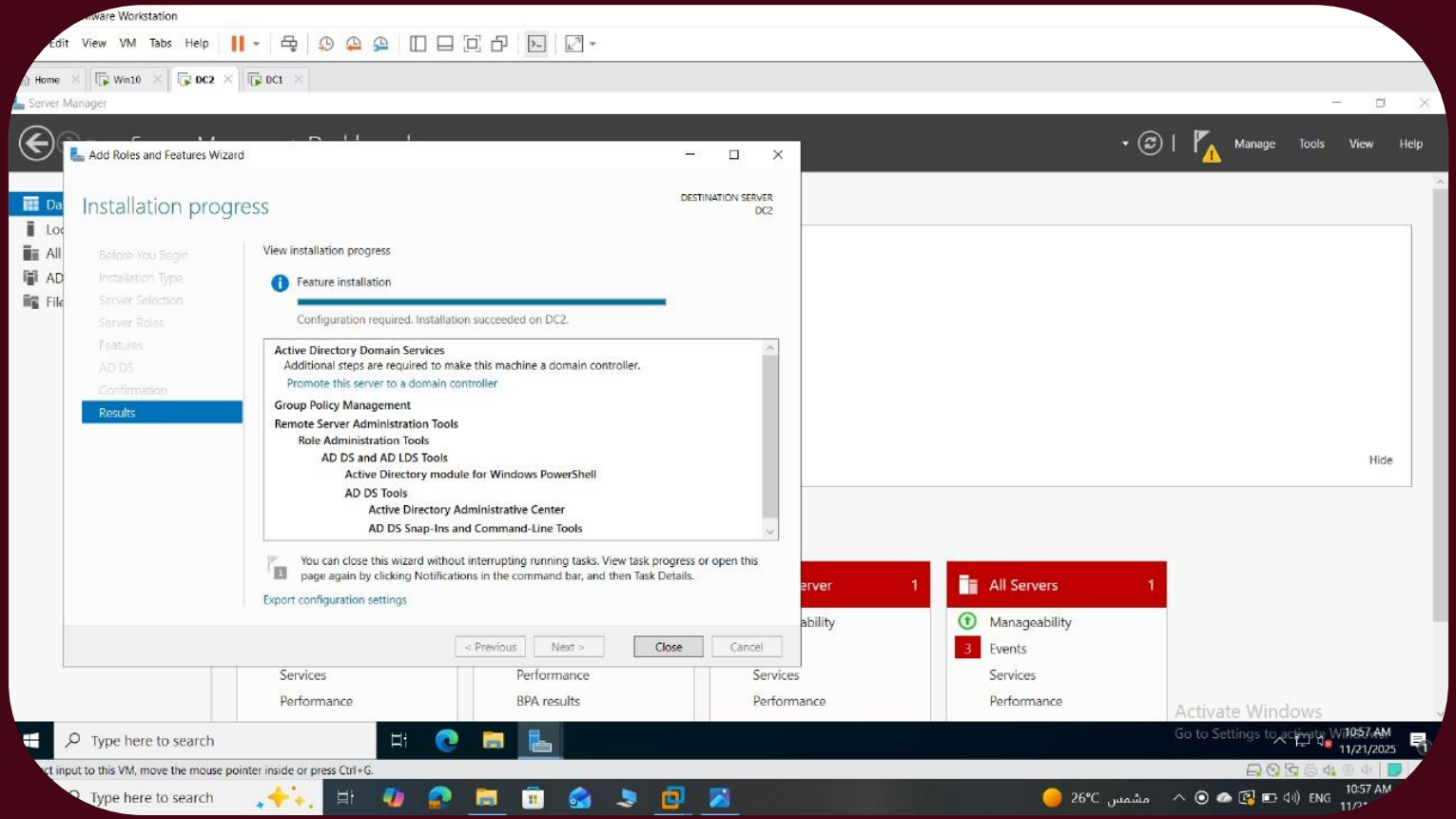






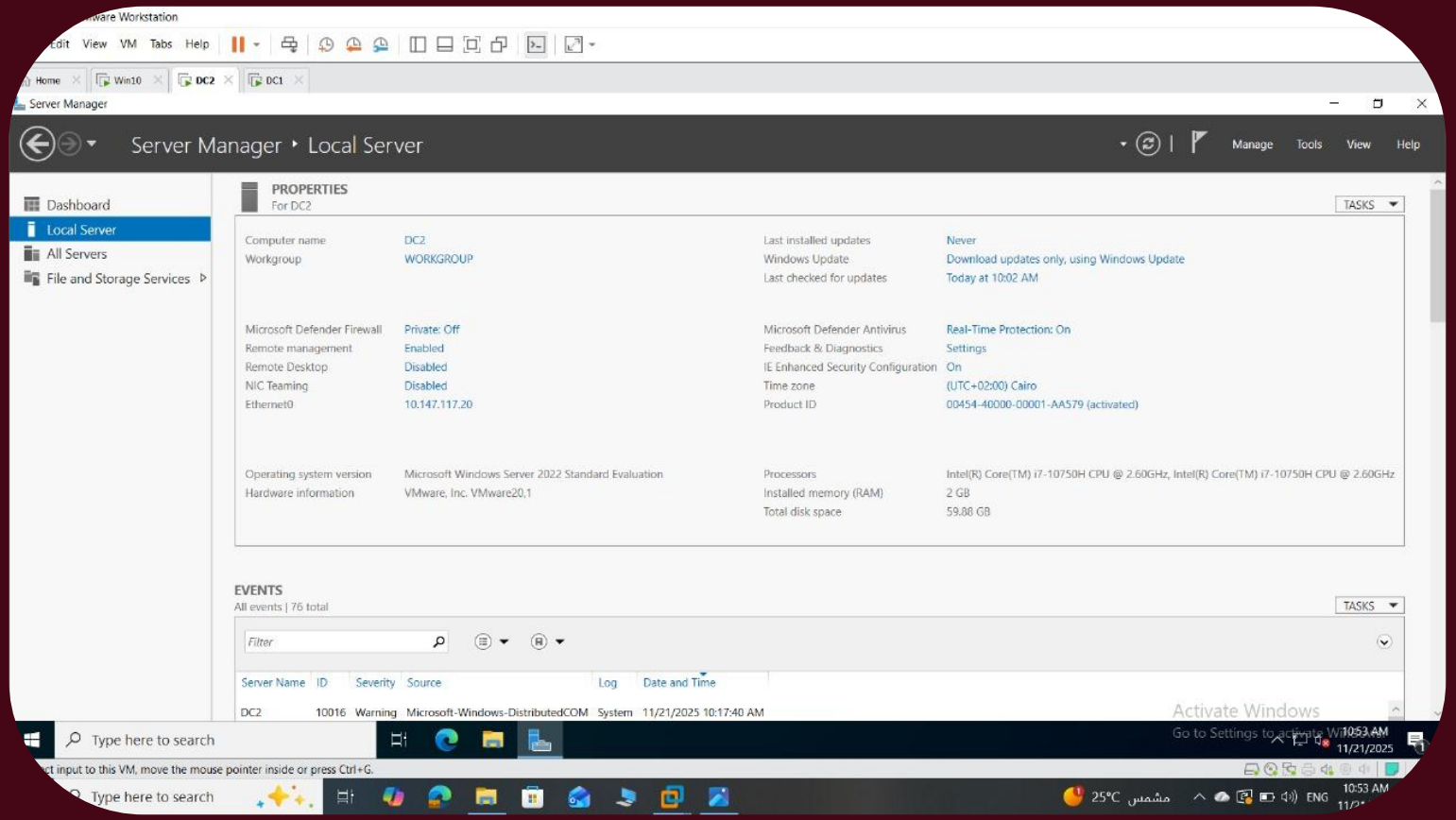
Configuring the Additional Domain Controller (DC2)

"After preparing the primary domain controller (DC1), we promoted the second server to act as an Additional Domain Controller (DC2). This step ensures redundancy, load balancing, and increased reliability for the ITI.local domain."



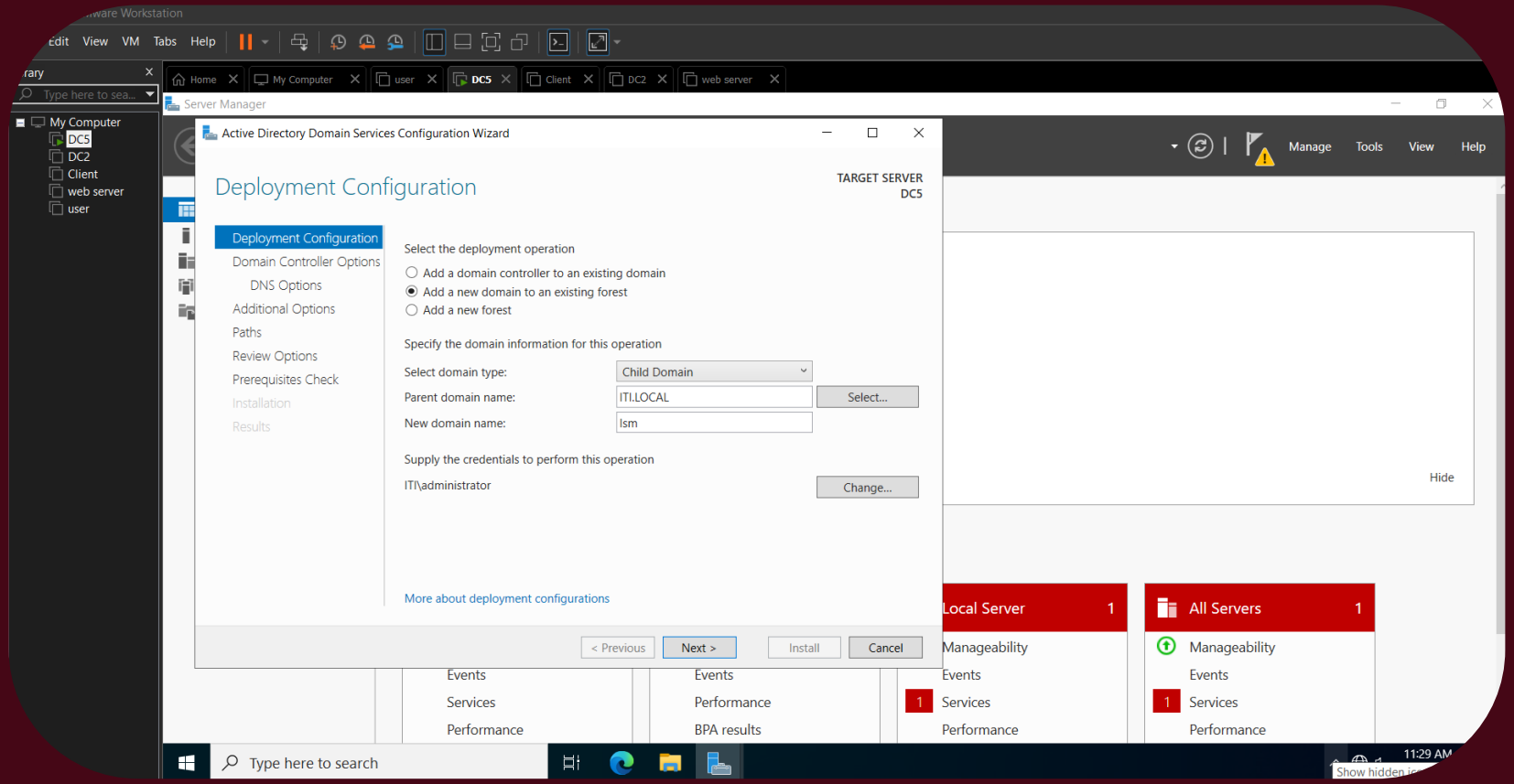
Configuring the Additional Domain Controller (DC2)

"After preparing the primary domain controller (DC1), we promoted the second server to act as an Additional Domain Controller (DC2). This step ensures redundancy, load balancing, and increased reliability for the ITI.local domain."



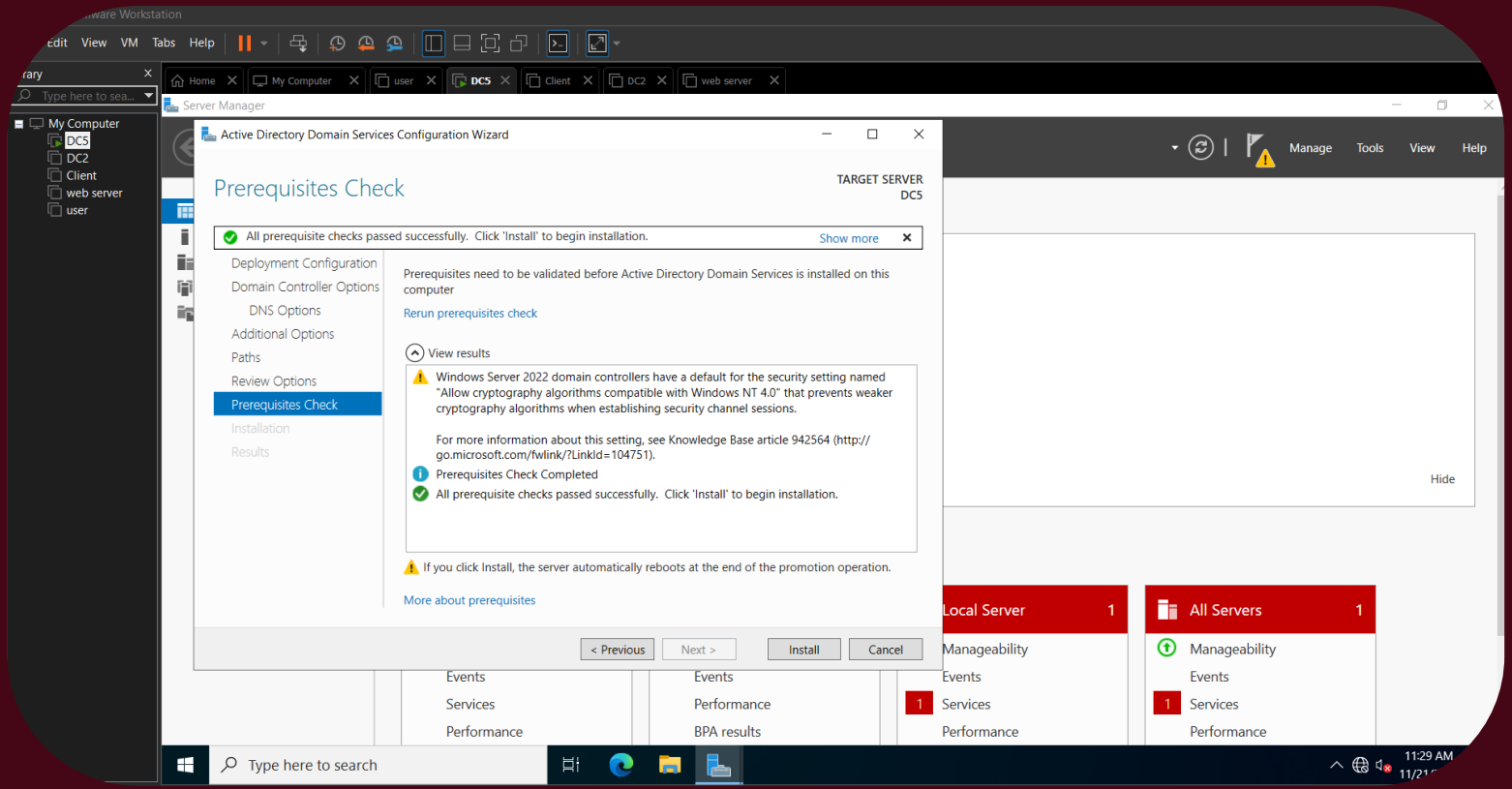
Child Domain Controller Overview

“We created the Ismailia Child Domain (Ism.ITI.local) to extend the forest, enable local authentication, improve performance, and provide administrative separation for the Ismailia branch.”



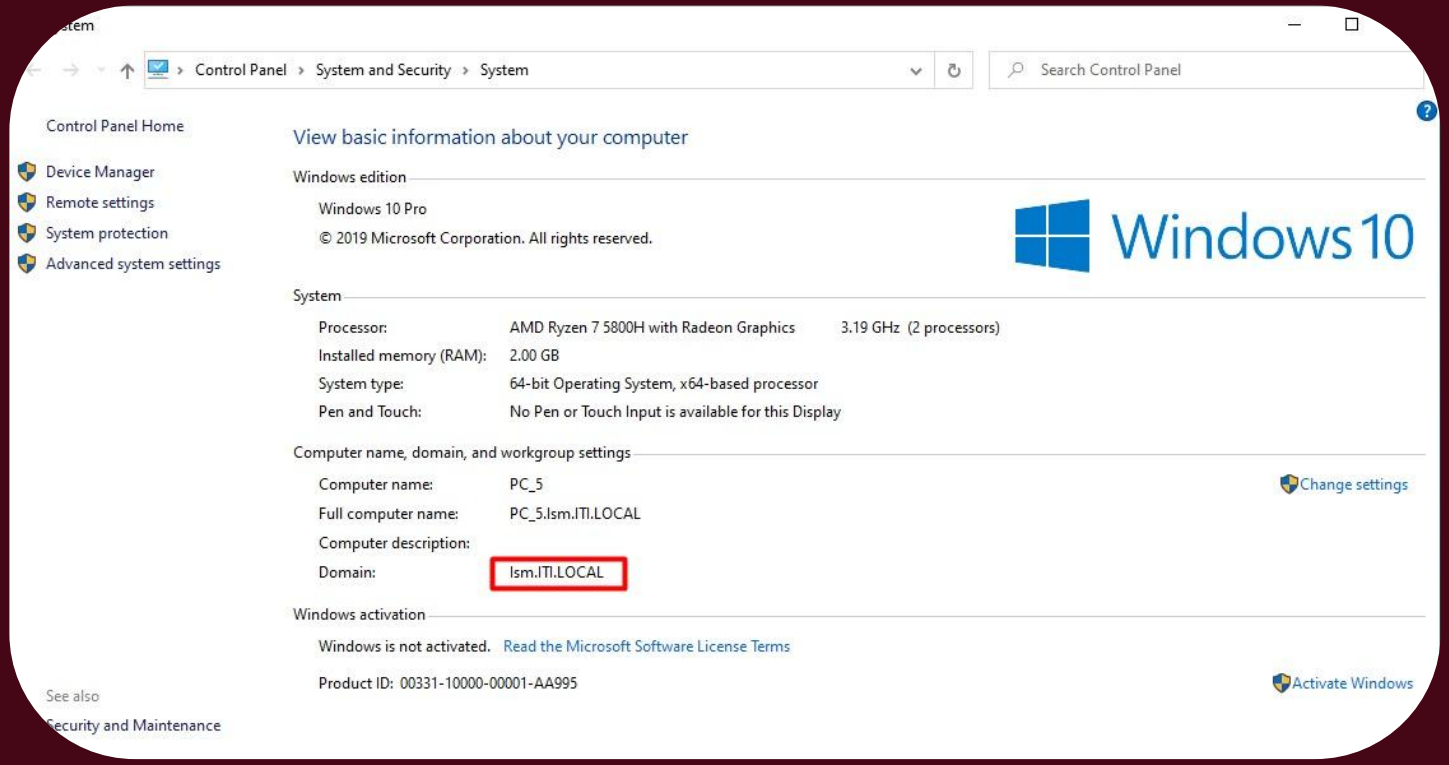
Child Domain Controller Overview

“We created the Ismailia Child Domain (Ism.ITI.local) to extend the forest, enable local authentication, improve performance, and provide administrative separation for the Ismailia branch.”



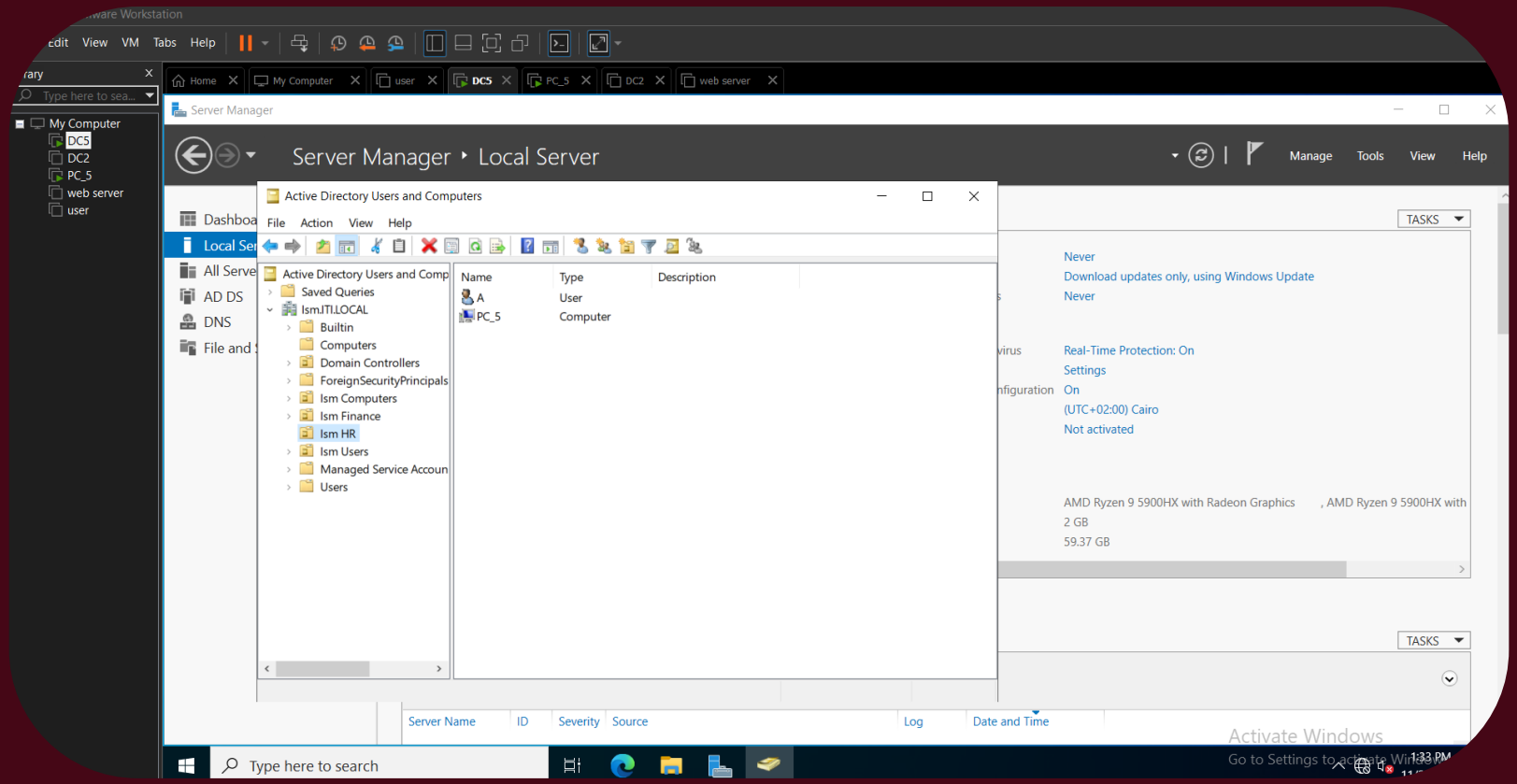
Child Domain Controller Overview

"PC5 was joined to the Ism.ITI.local child domain".



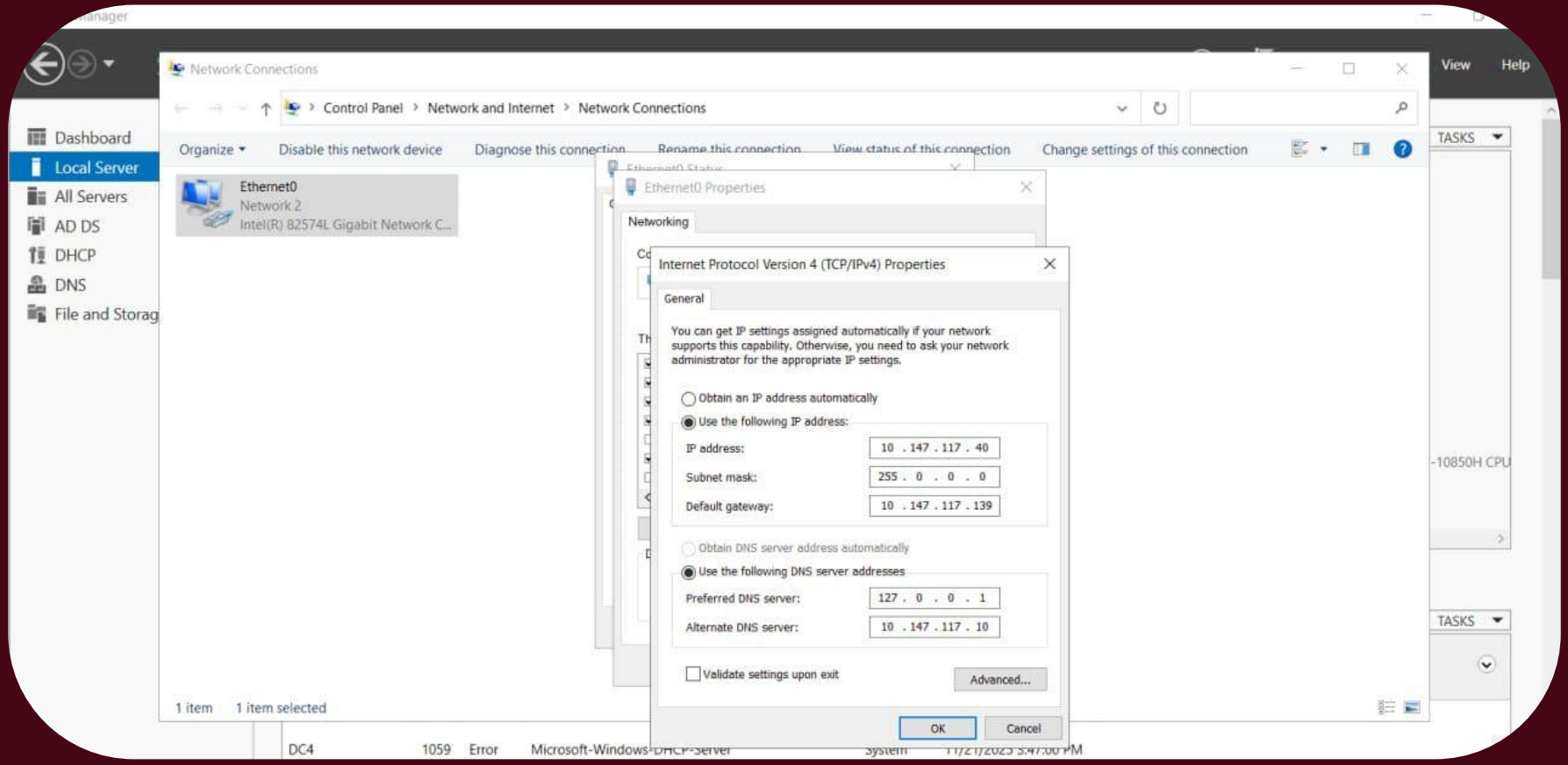
Child Domain Controller Overview

"After configuring the Ismailia child domain, we created the necessary Organizational Units and added users and computers to structure the environment properly. PC5 was joined to the Ism.ITI.local domain and assigned to the appropriate user for login and policy application."



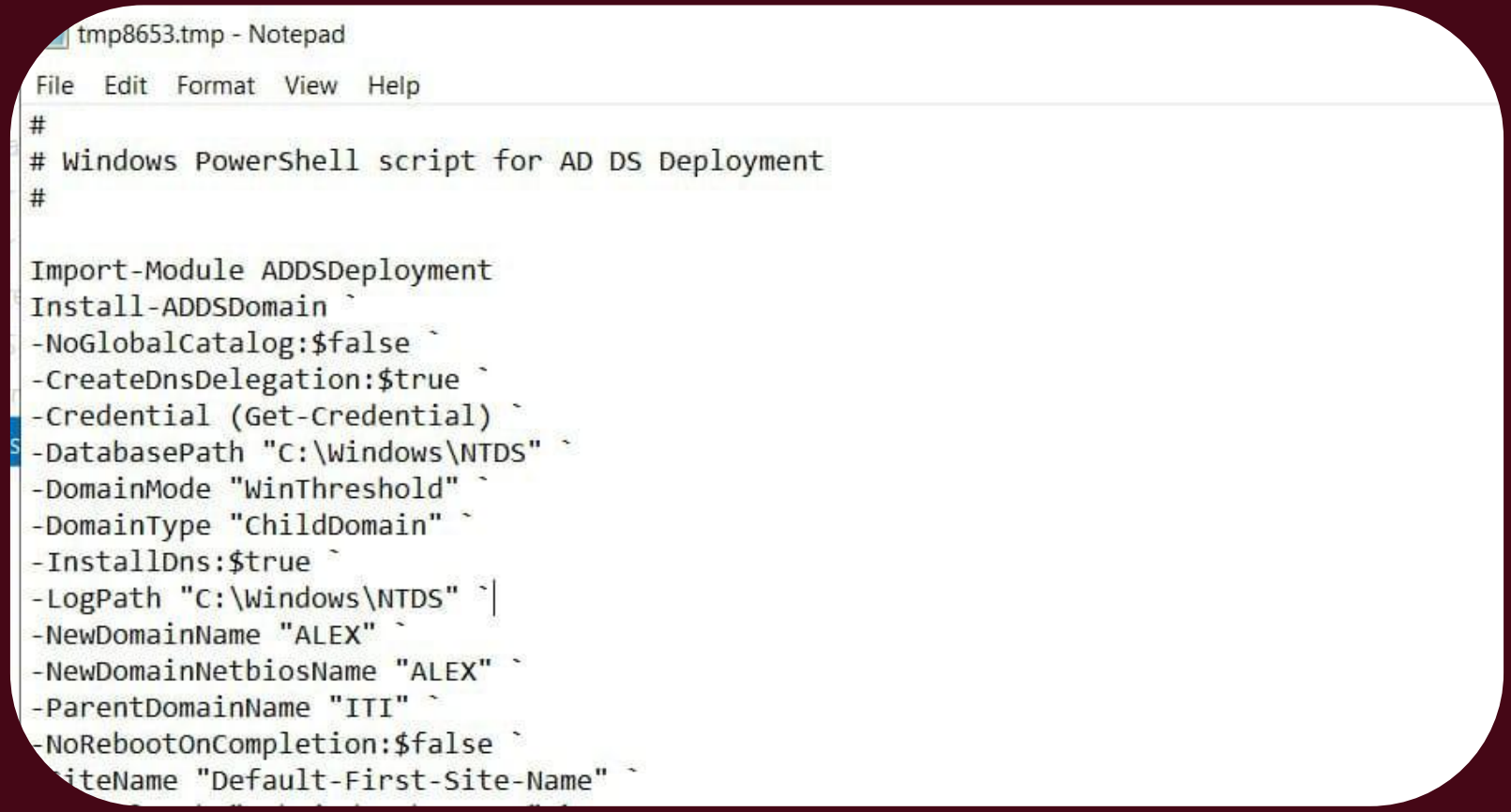
Child Domain Controller Overview

“We created the Alexandria Child Domain (Alex.ITI.local) to extend the forest, enable local authentication, improve performance, and provide administrative separation for the Alexandria branch.”



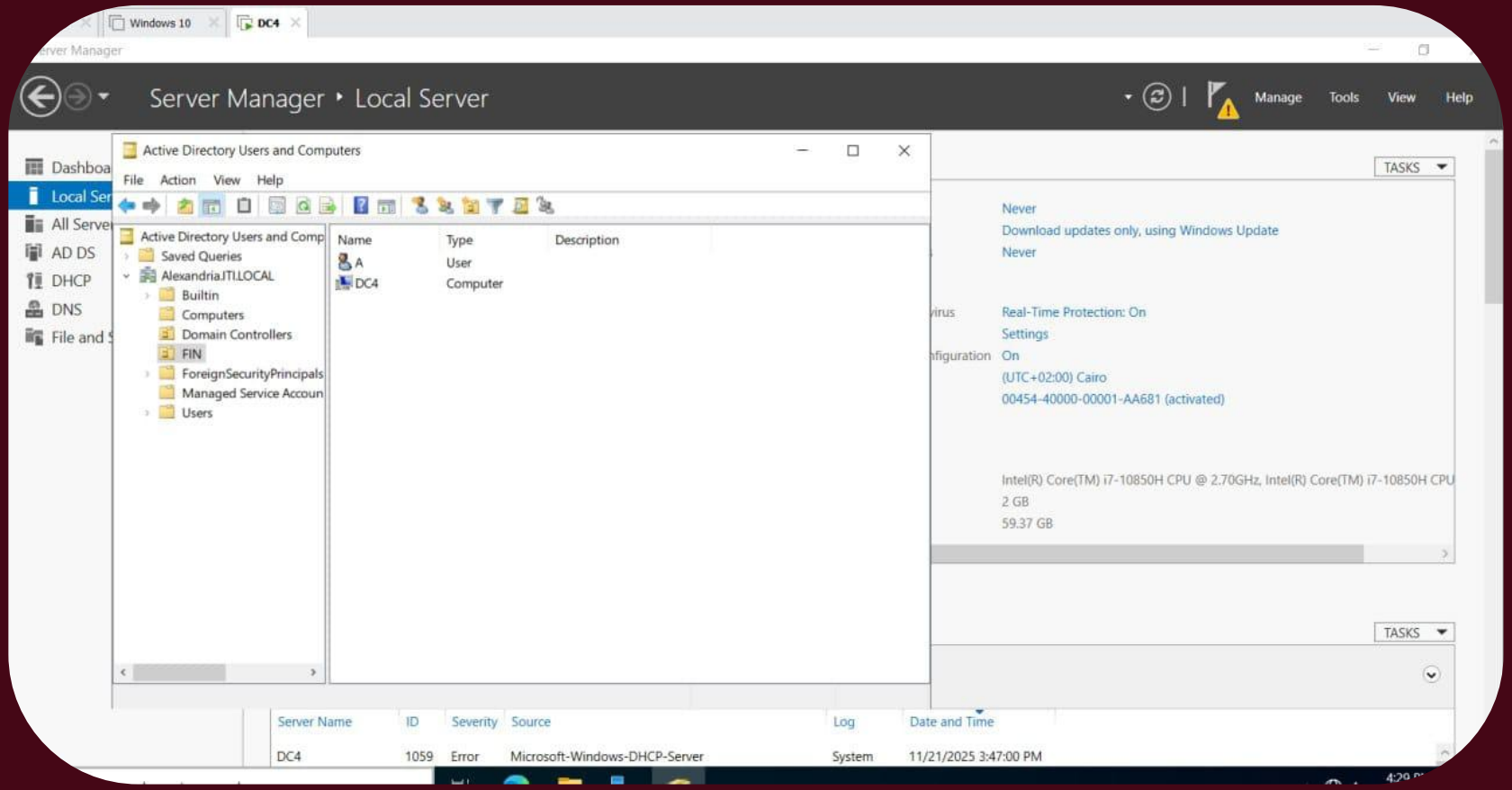
Child Domain Controller Overview

“We created the Alexandria Child Domain (Alex.ITI.local) to extend the forest, enable local authentication, improve performance, and provide administrative separation for the Alexandria branch.”



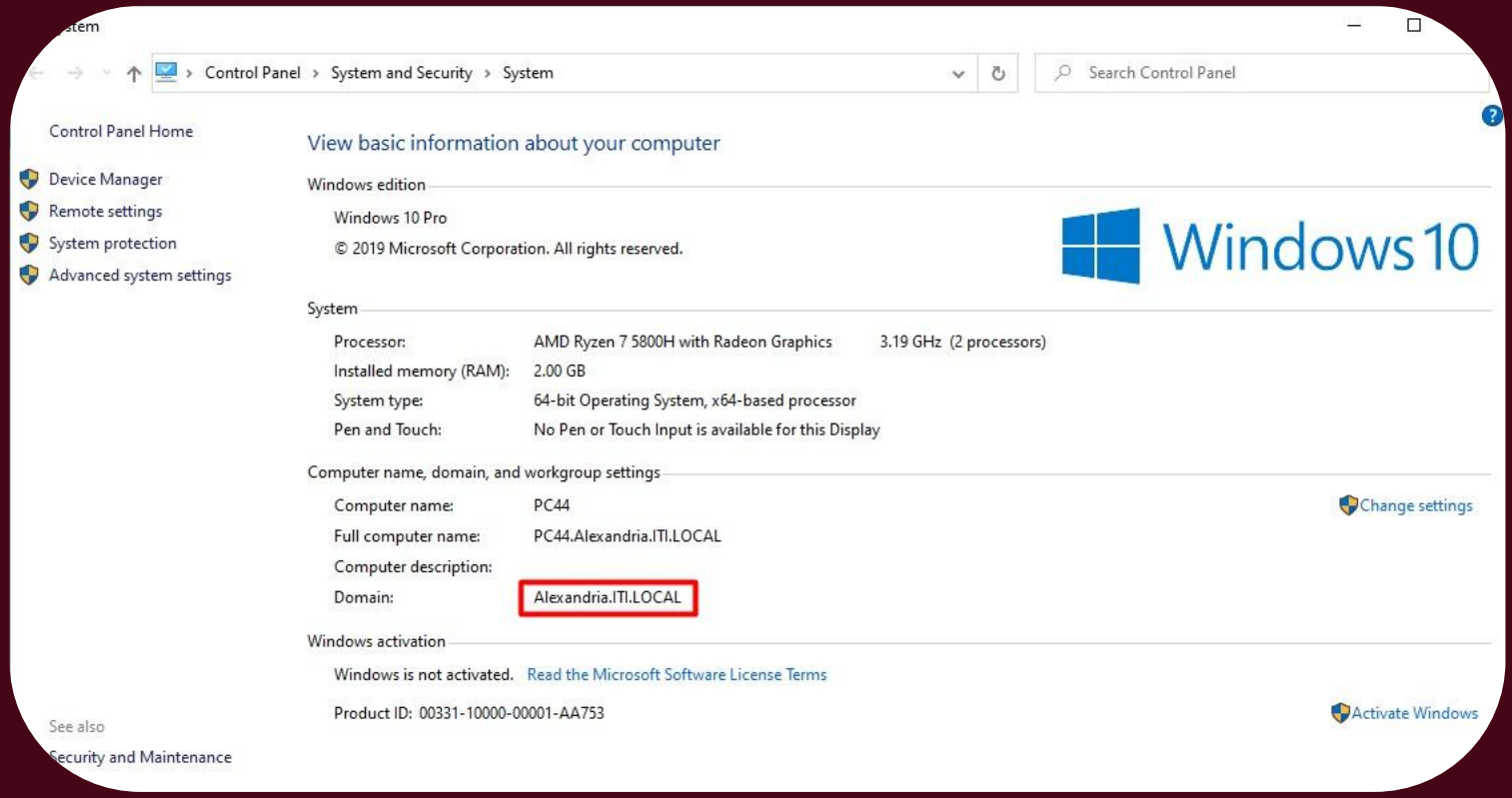
Child Domain Controller Overview

"After configuring the Alex child domain, we created the necessary Organizational Units and added users and computers to structure the environment properly. PC5 was joined to the Alex.ITI.local domain and assigned to the appropriate user for login and policy application."



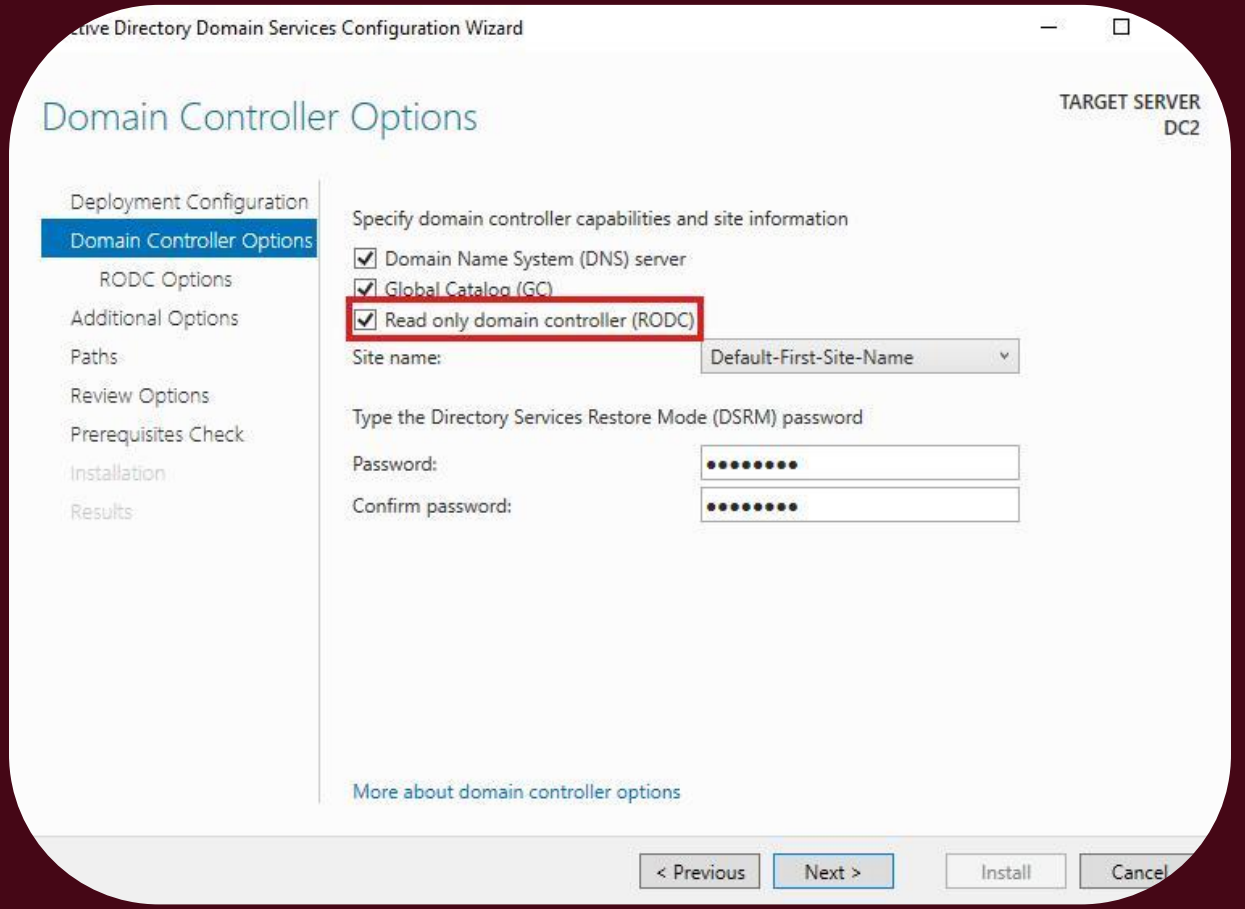
Child Domain Controller Overview

"PC4 was successfully joined to the Alex.ITI.local child domain to allow user authentication and policy application within the Alexandria branch."



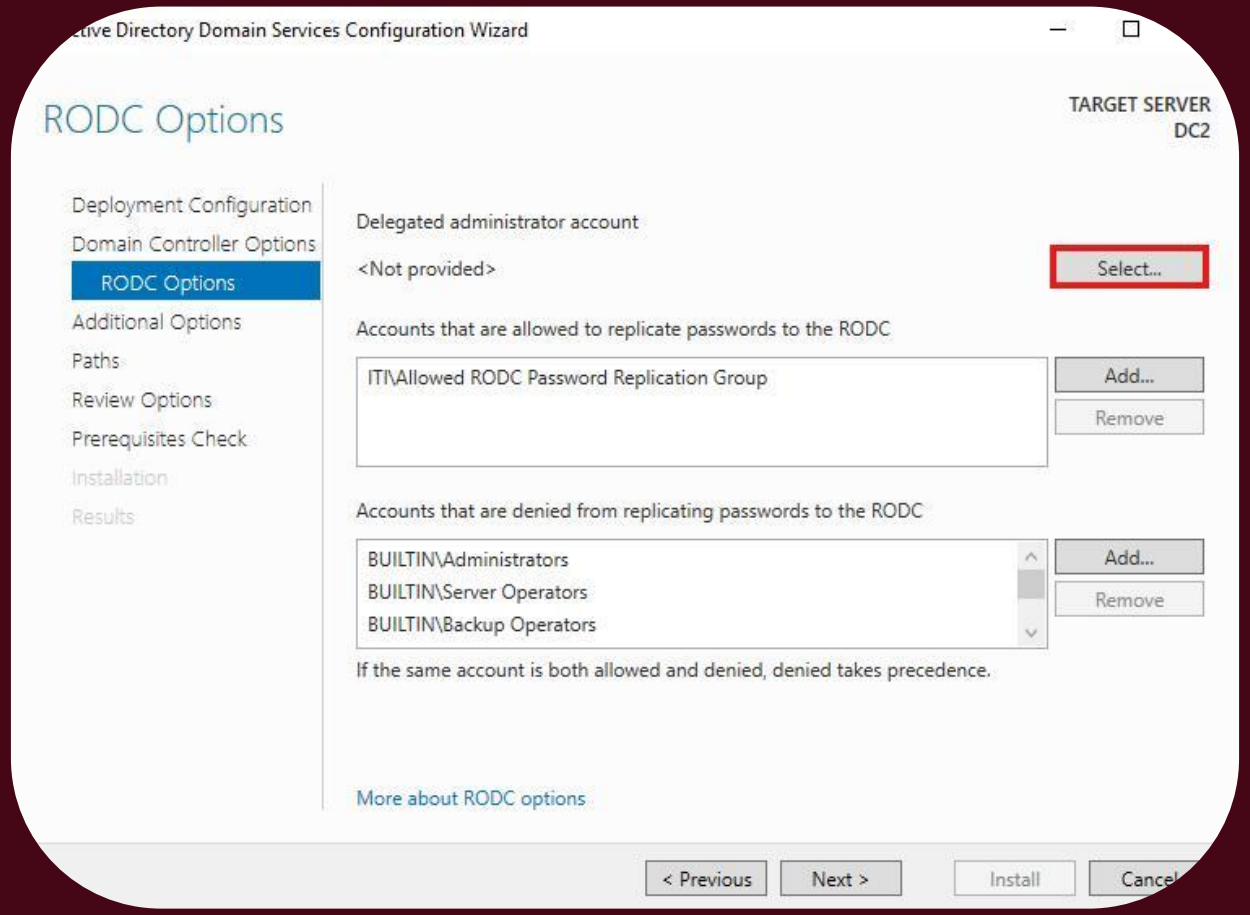
Read-Only Domain Controller(RODC)

"The RODC (DC3) was deployed to provide secure authentication services in branch locations.
It stores a read-only copy of the Active Directory database, reducing security risks while still allowing users to authenticate locally."



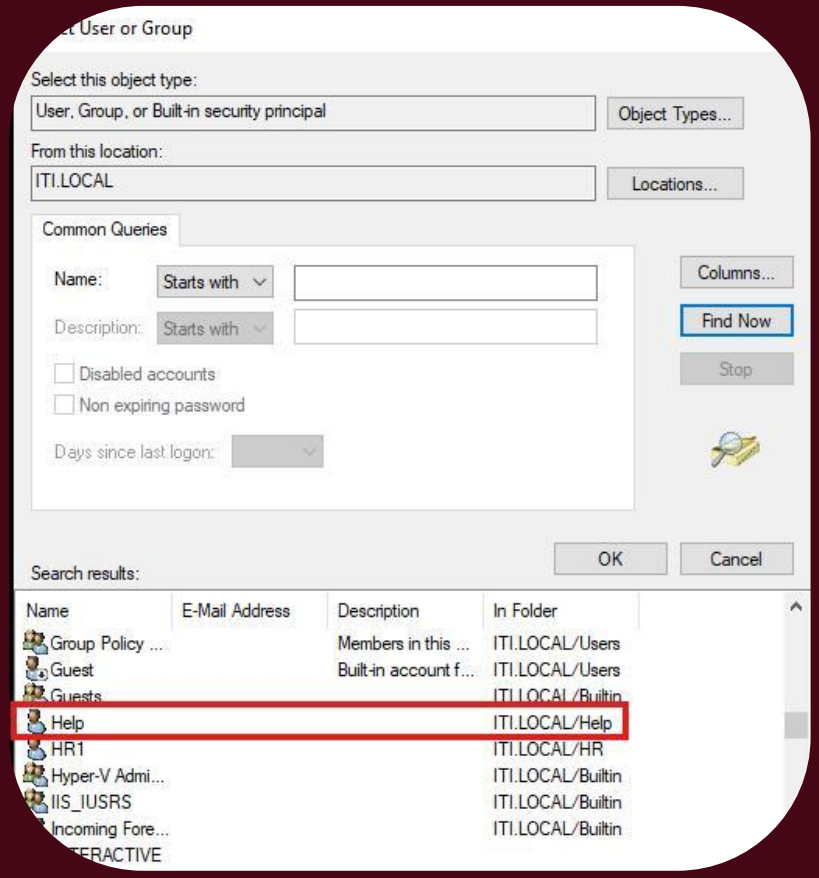
Read-Only Domain Controller(RODC)

"The RODC (DC3) was deployed to provide secure authentication services in branch locations.
It stores a read-only copy of the Active Directory database, reducing security risks while still allowing users to authenticate locally."



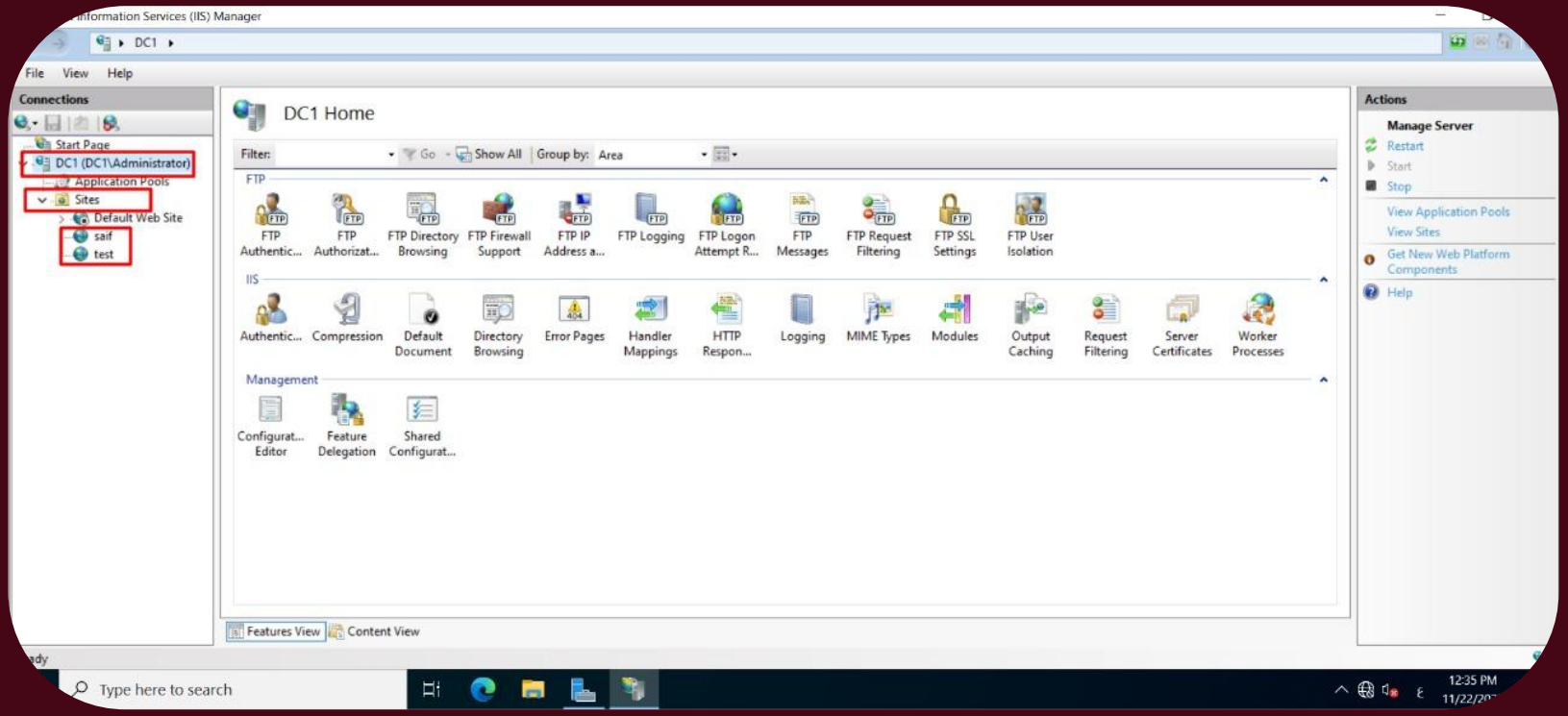
Read-Only Domain Controller(RODC)

"After creating the *Help* user in Active Directory, we assigned its credentials in the RODC settings so that it becomes the only account authorized to manage and administer the RODC."



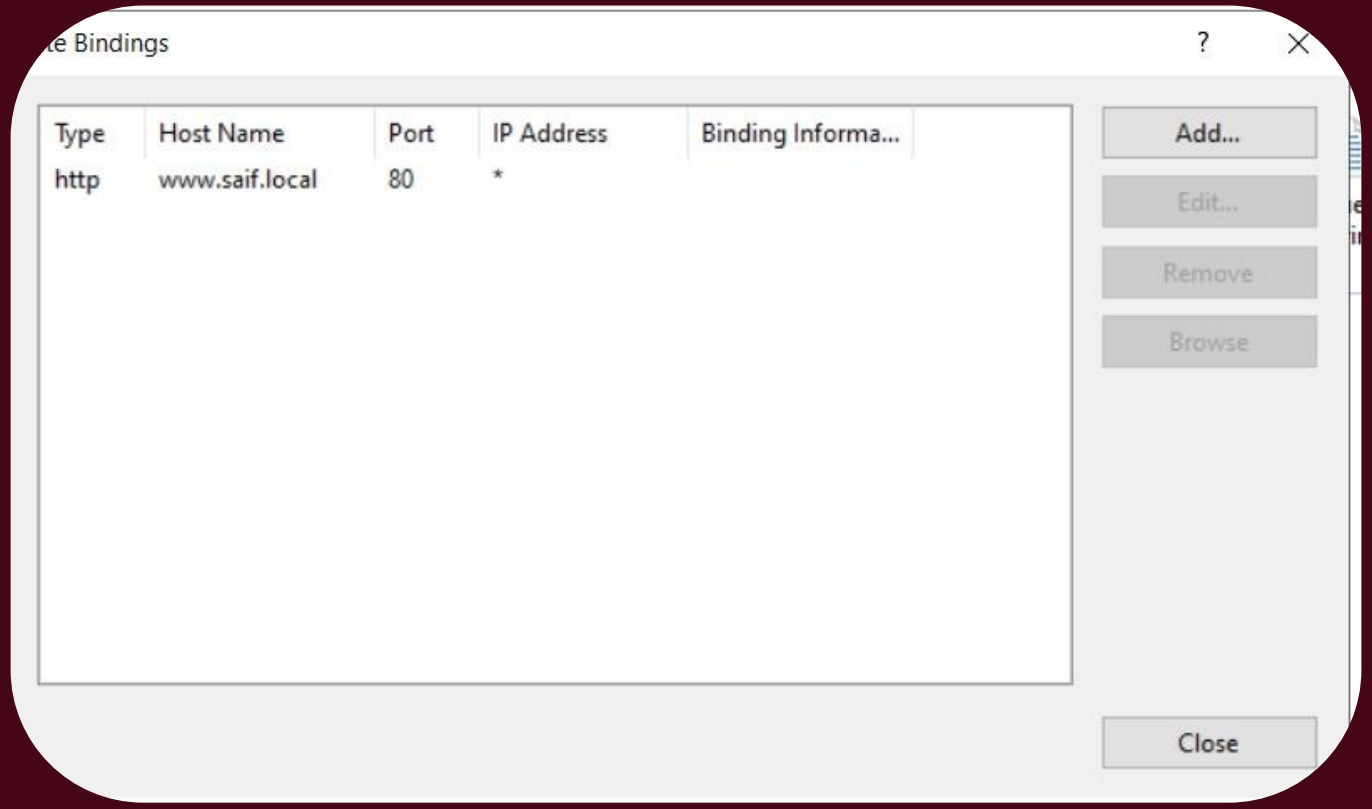
Web Server Overview

"We configured two web servers: an HTTP server hosting www.saif.local and an HTTPS server hosting www.testing.local."



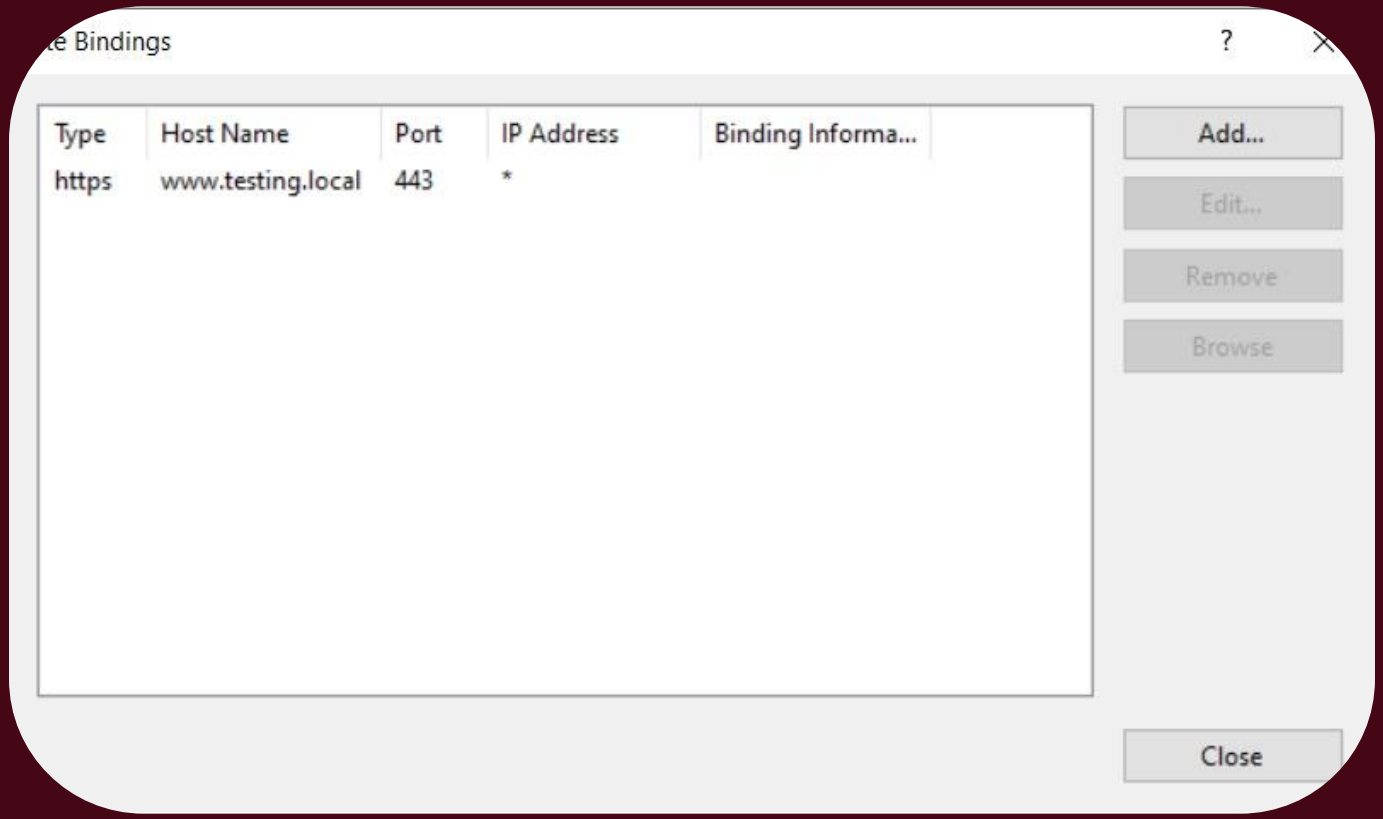
Web Server Overview

HTTP server hosting www.saif.local



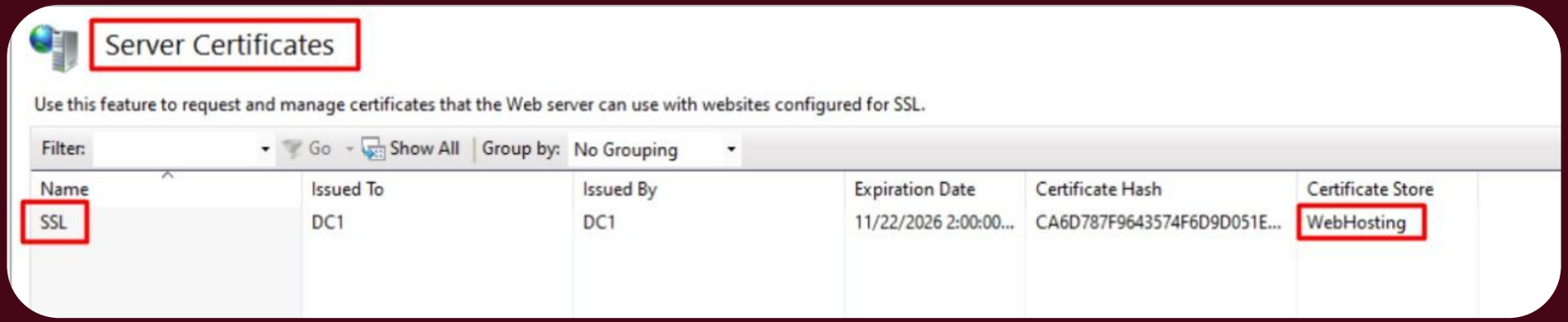
Web Server Overview

HTTPS server hosting www.testing.local



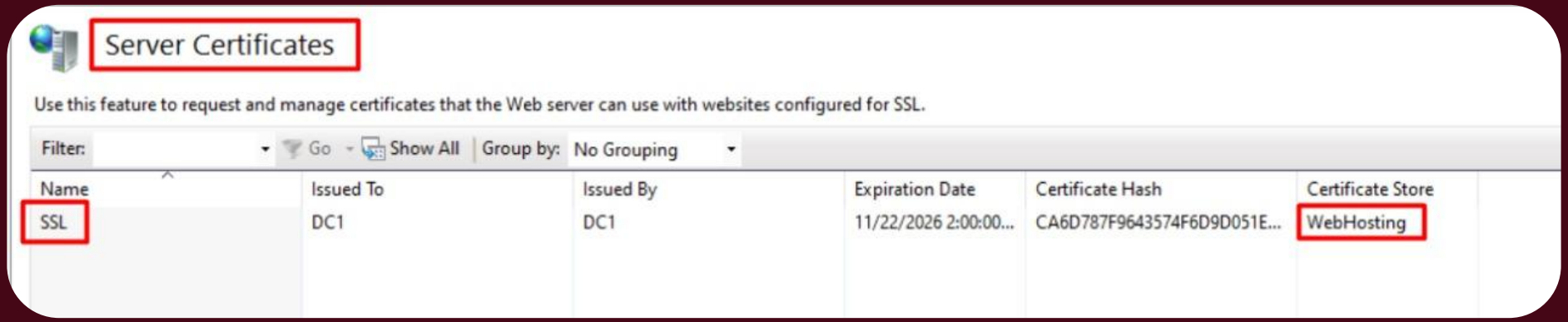
Web Server Overview

SSL certificate for the secure website



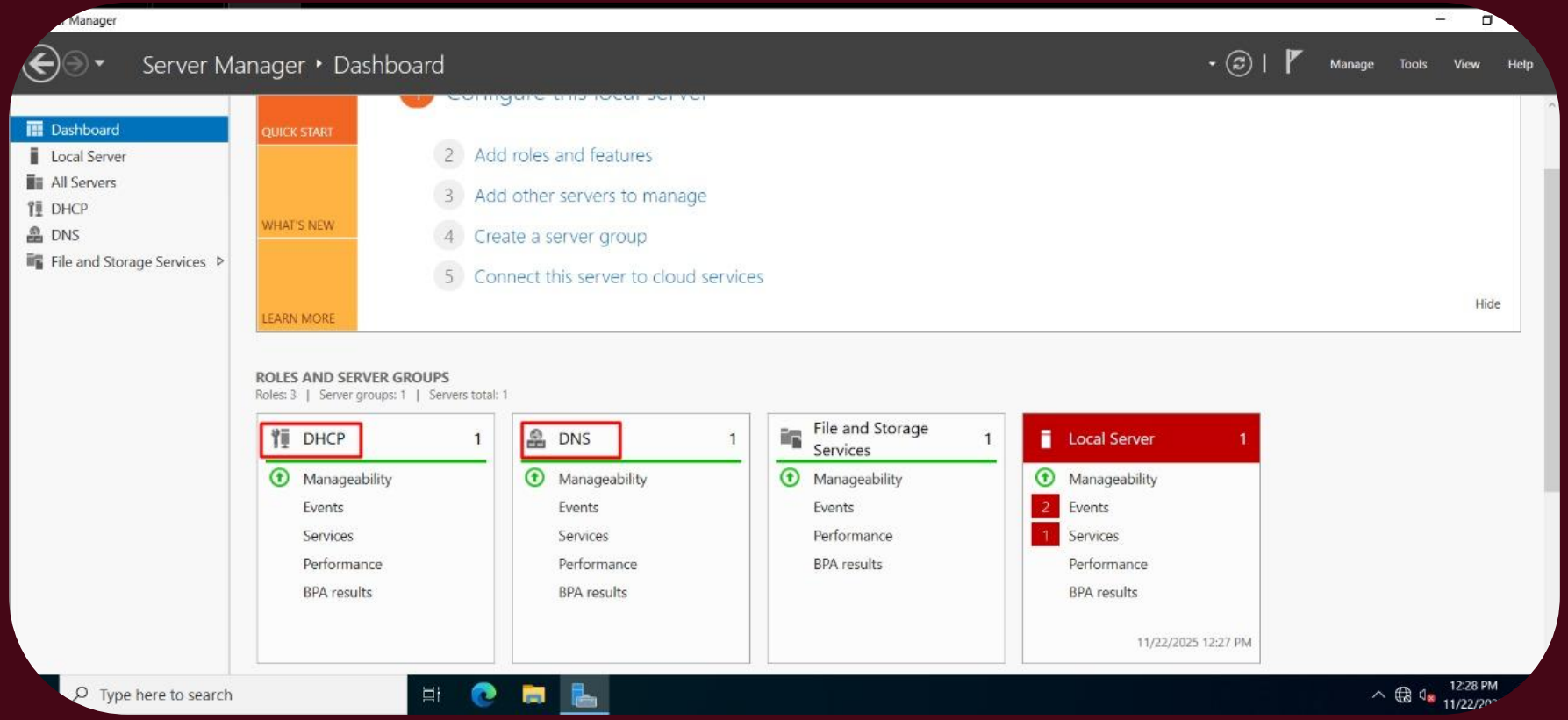
Web Server Overview

SSL certificate for the secure website



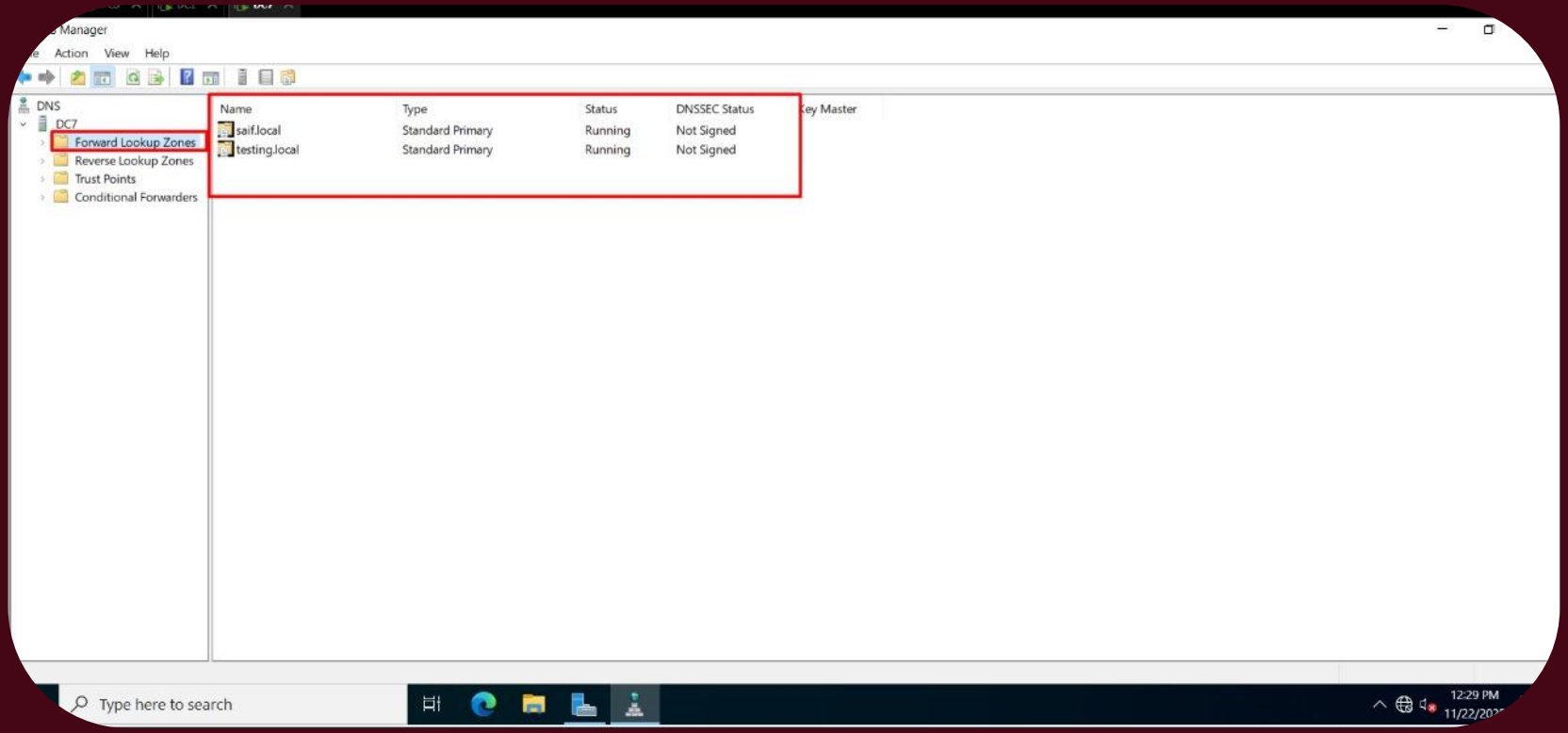
DNS Overview

“DNS: Translates human-readable domain names into IP addresses to enable accurate and efficient network communication.”



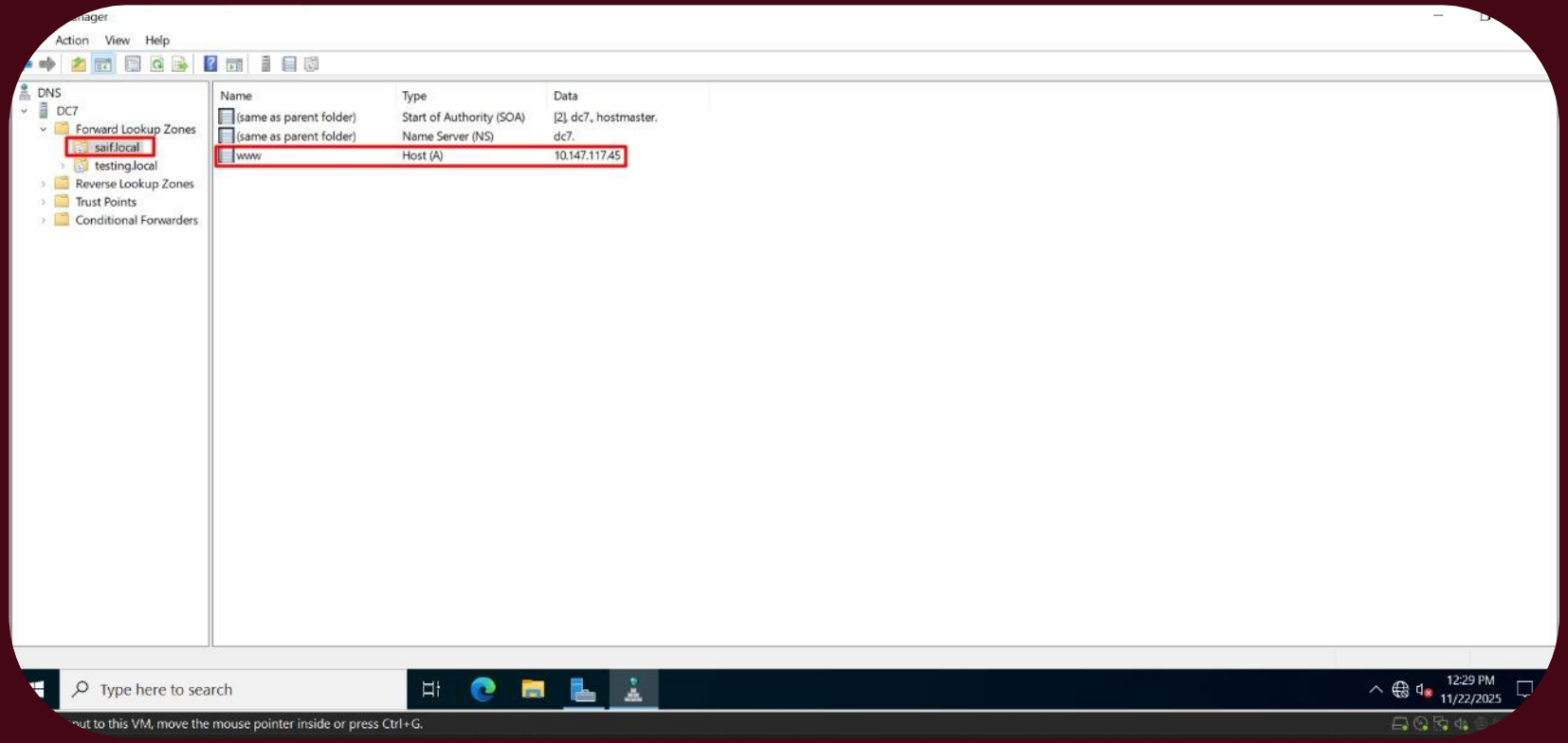
DNS Overview

The forward lookup zones to the websites



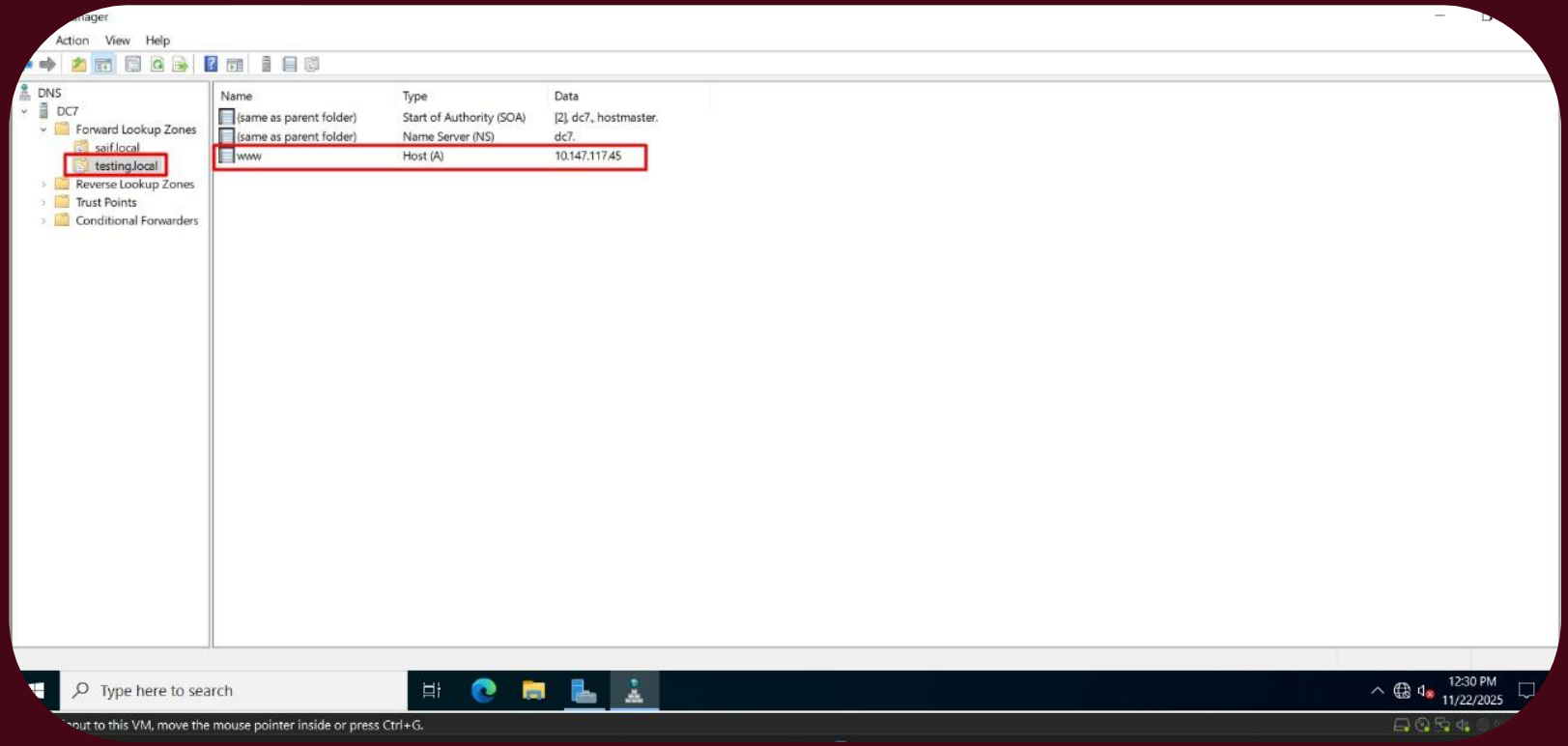
DNS Overview

The host on the saif.local zone



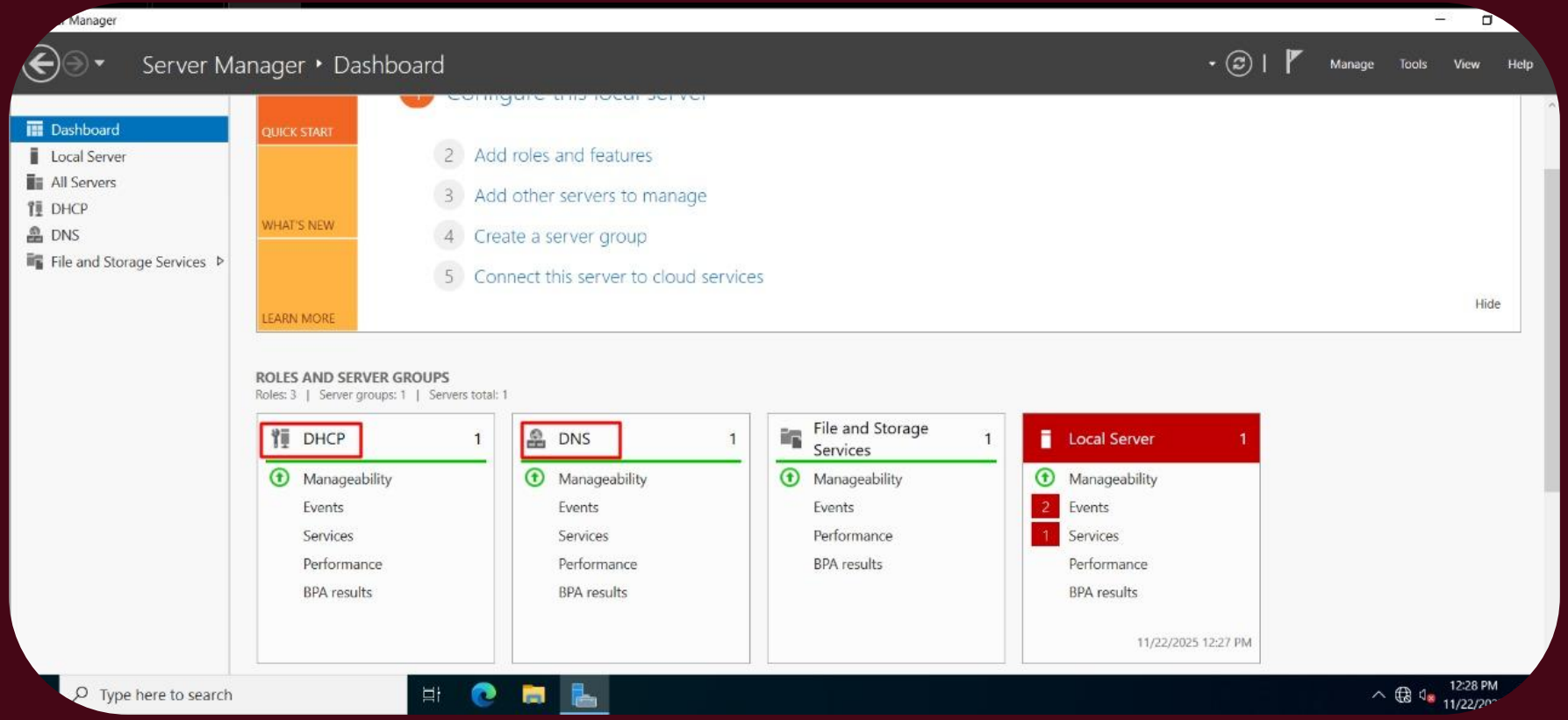
DNS Overview

The host on the testing.local zone



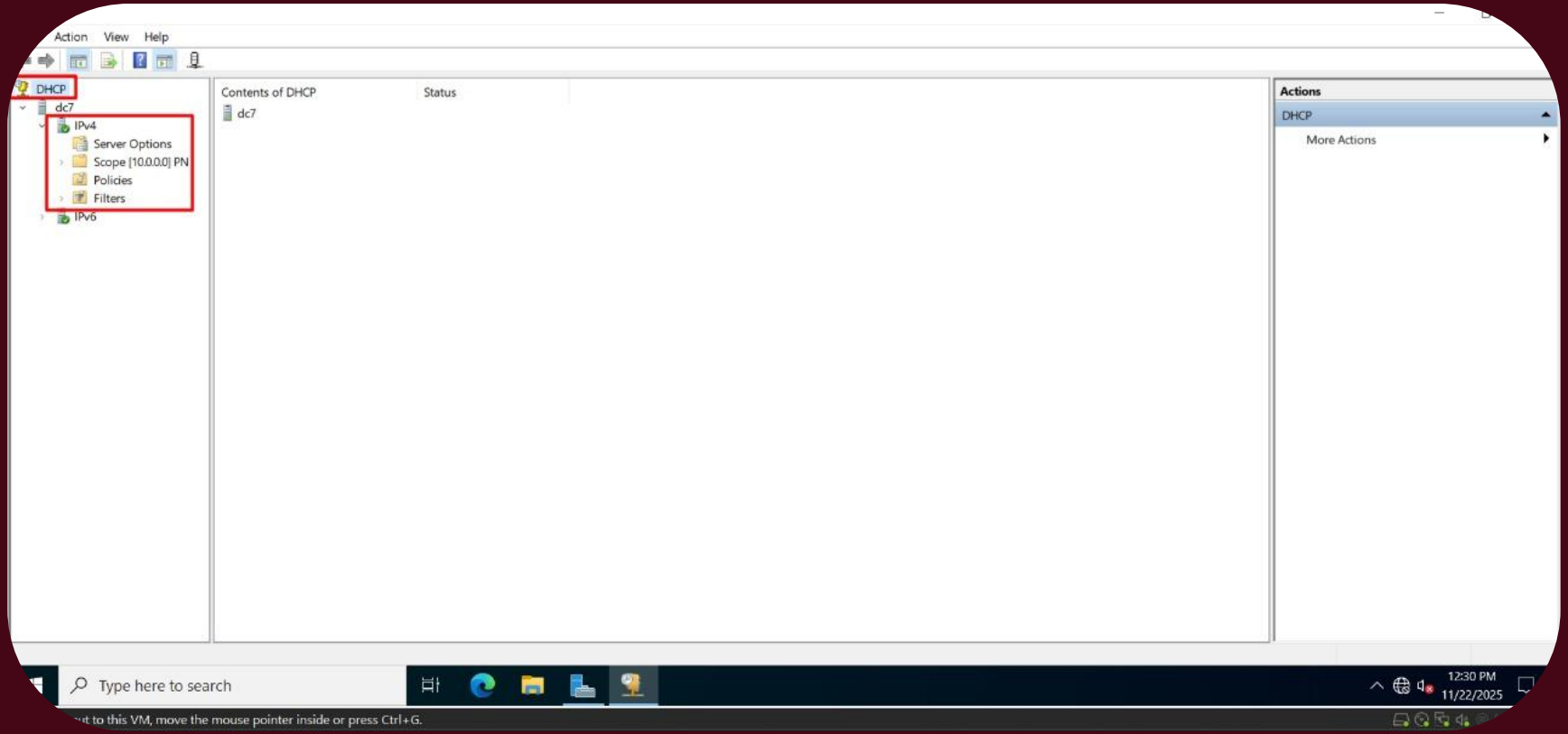
DHCP Overview

“DHCP Server: Automatically assigns IP addresses and network configuration parameters to client devices, ensuring efficient and centralized IP management.”



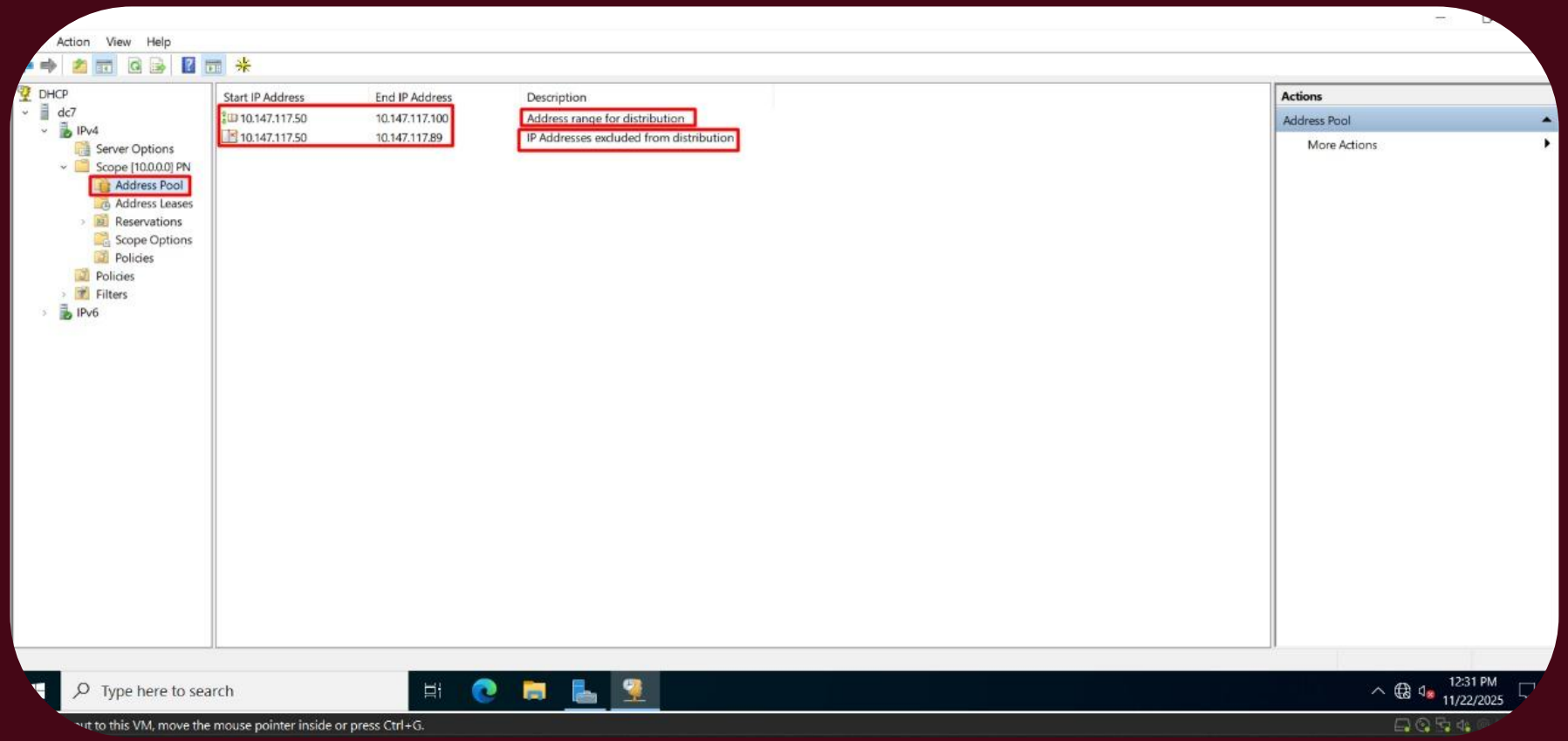
DHCP Overview

The scope of the DHCP server



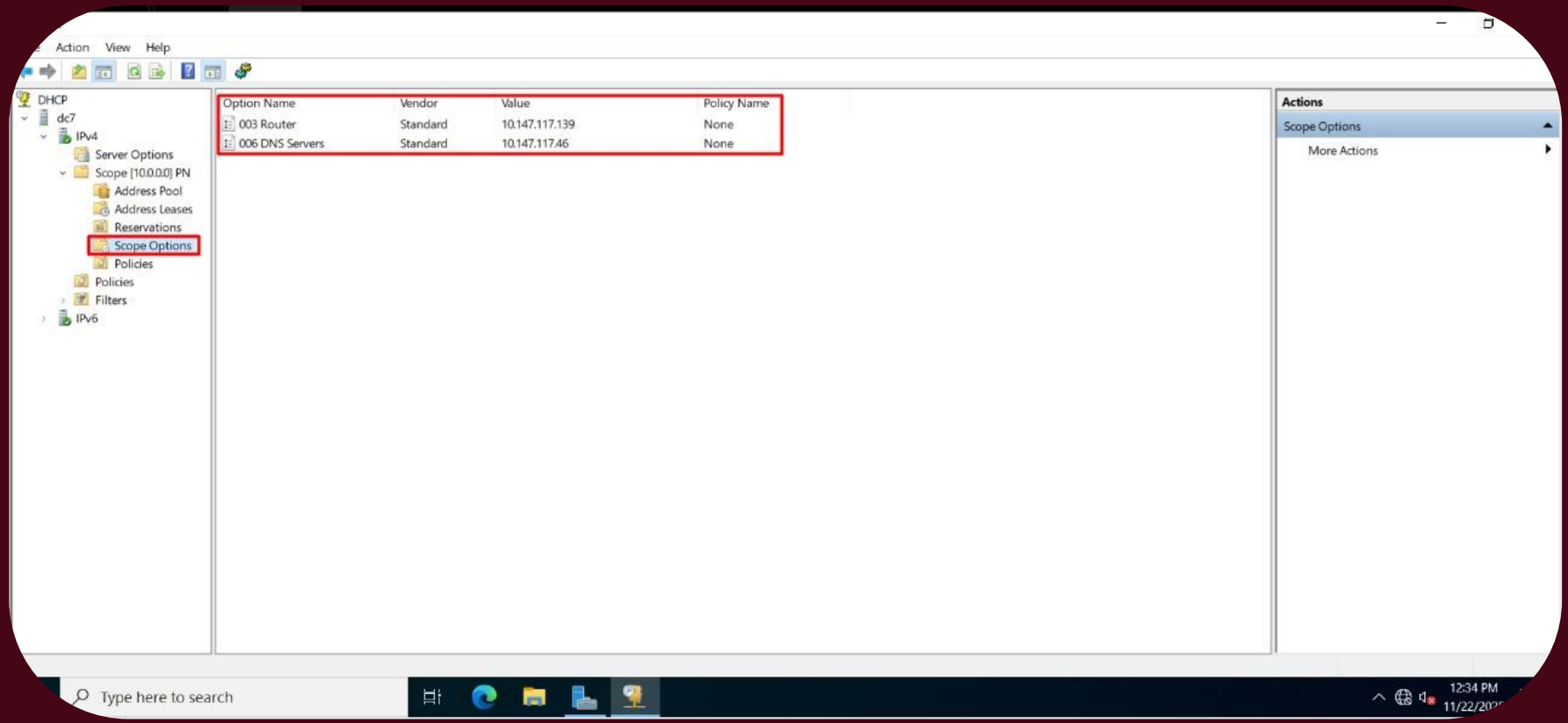
DHCP Overview

The address pool of the scope and the excluded IPs



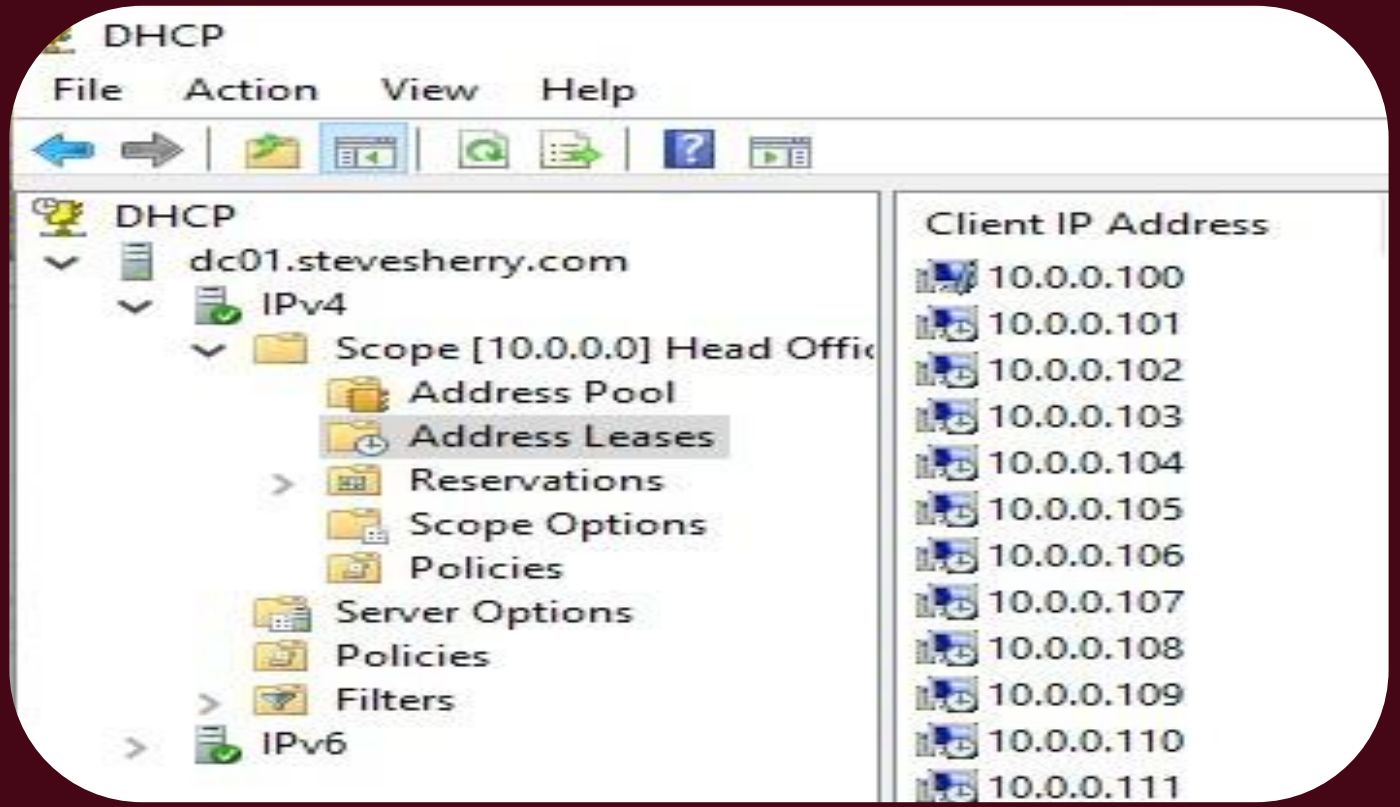
DHCP Overview

The scope options like the default gateway and the DNS server



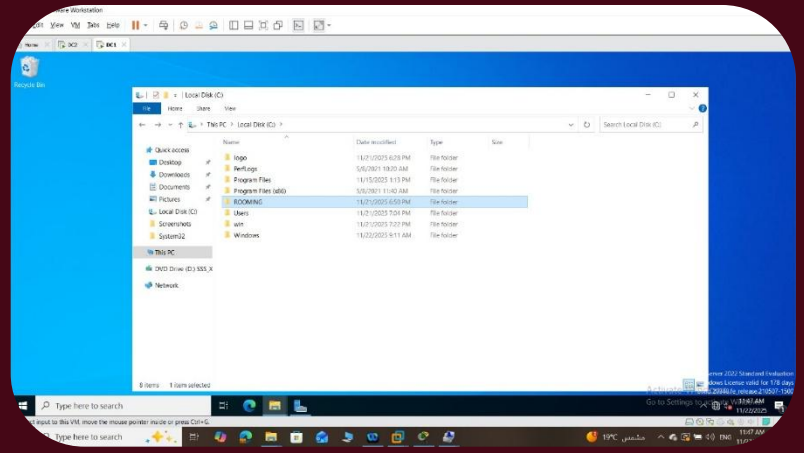
DHCP Overview

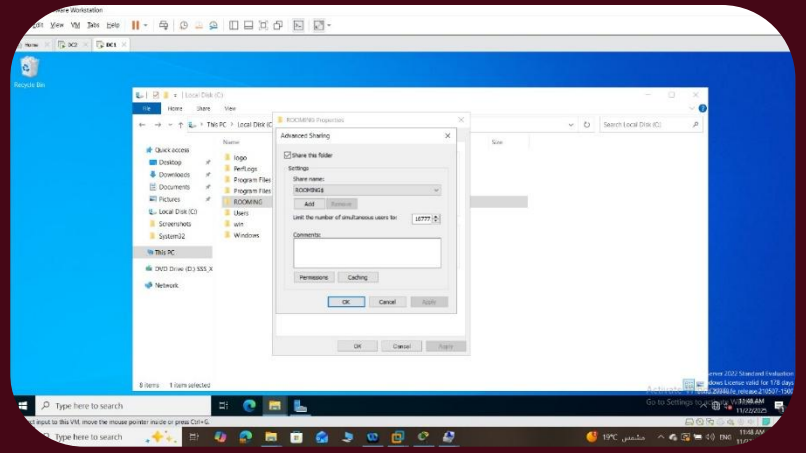
The devices that took configuration from DHCP server

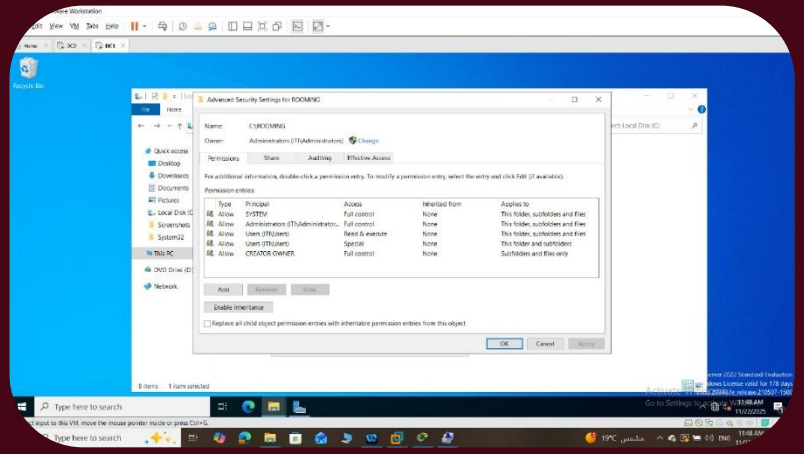


Roaming Profile Configuration

“Roaming Profile: keeps the user’s settings consistent across all domain computers.”

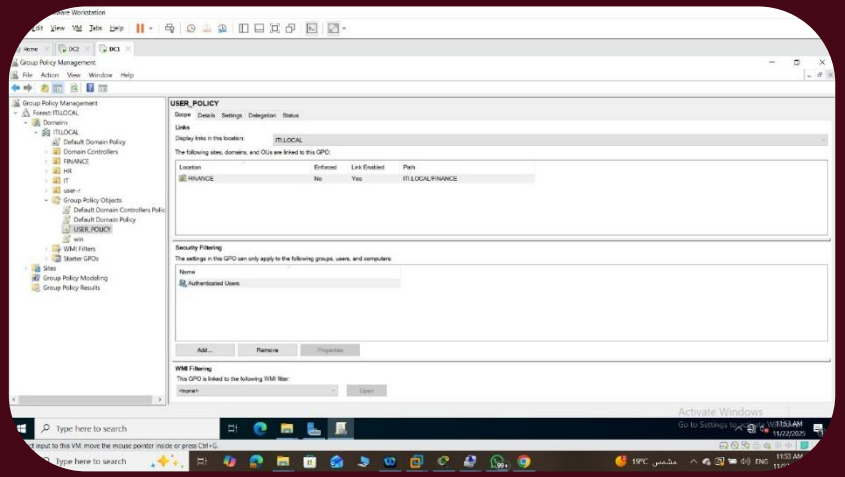


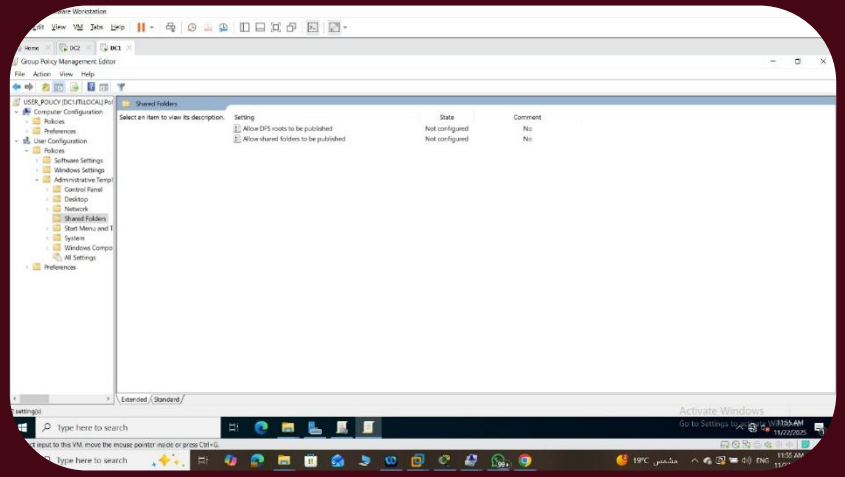


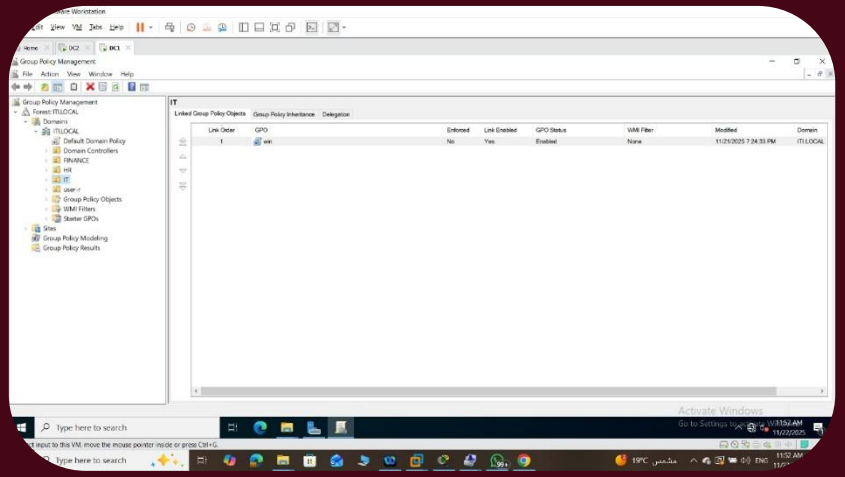


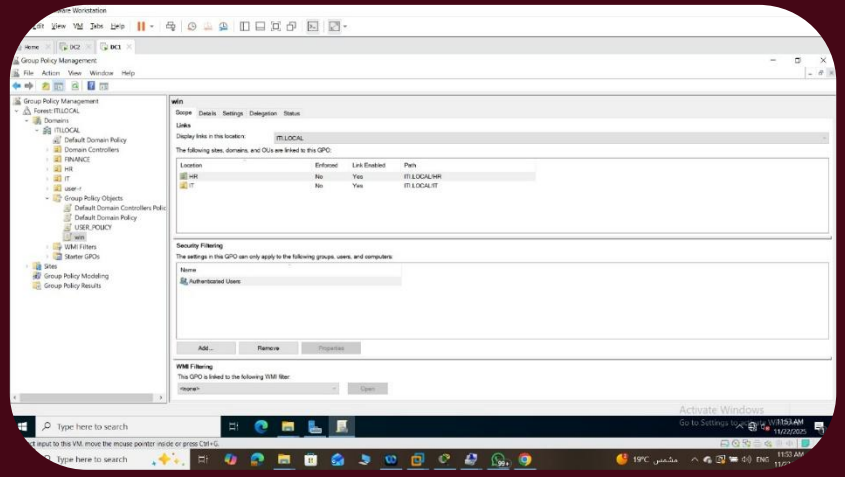
Policies Configuration

“All Group Policies were configured to control user permissions, apply security rules, customize the desktop environment, and automatically deploy required software across the domain.”









Challenges

1- Network Connectivity Issues
Connection problems between sites or domain controllers due to DNS or routing failures.

2- Domain Controller Failure
Failure of PDC or RODC is causing login issues and replication problems.

3- Network Card Misconfiguration
Incorrect IP/DNS settings or a disabled network adapter.

4- Roaming Profile Issues
Slow or failed profile loading due to permissions or weak network links.

5- WSUS Configuration Problems
Clients are not receiving updates, or GPO settings are not being applied correctly.

6- GPO Deployment Issues
Slow replication, wrong security filtering, or policy conflicts.

7- Delegation & Permission Challenges
Difficulty assigning limited permissions without giving full admin access.


Learn
Think
1017 ATOG 9SM