

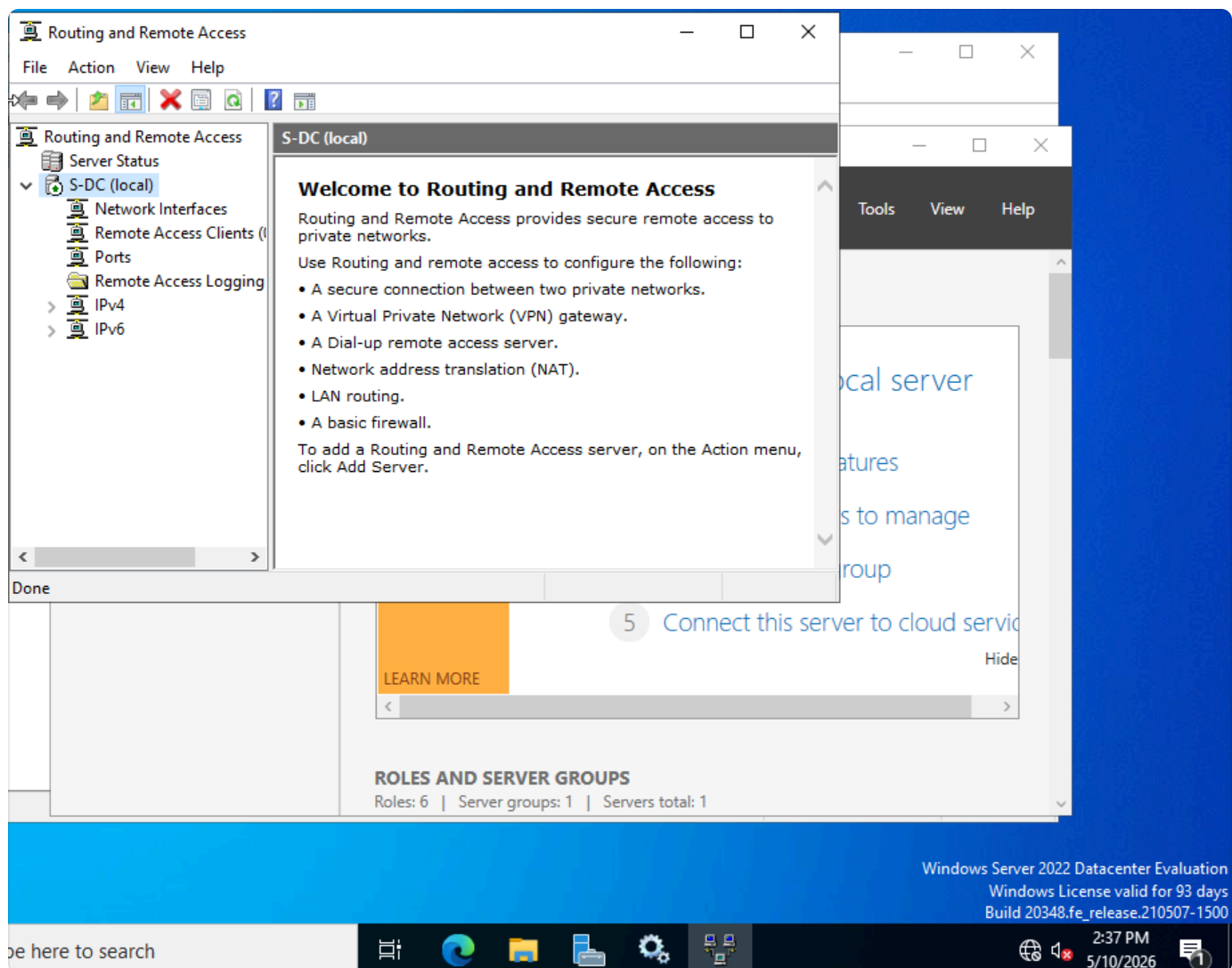
Network Infrastructure Configuration

Introduction

This report clearly shows the configuration and testing of a multi-network infrastructure developed for ACCA5023-Networking Operating Systems and Services are described in this report. Using services such as Active Directory, DNS, DHCP, RRAS, IIS, and shared network storage, the project required setting up both a Windows & Debian server and client across a Swansea and London network.

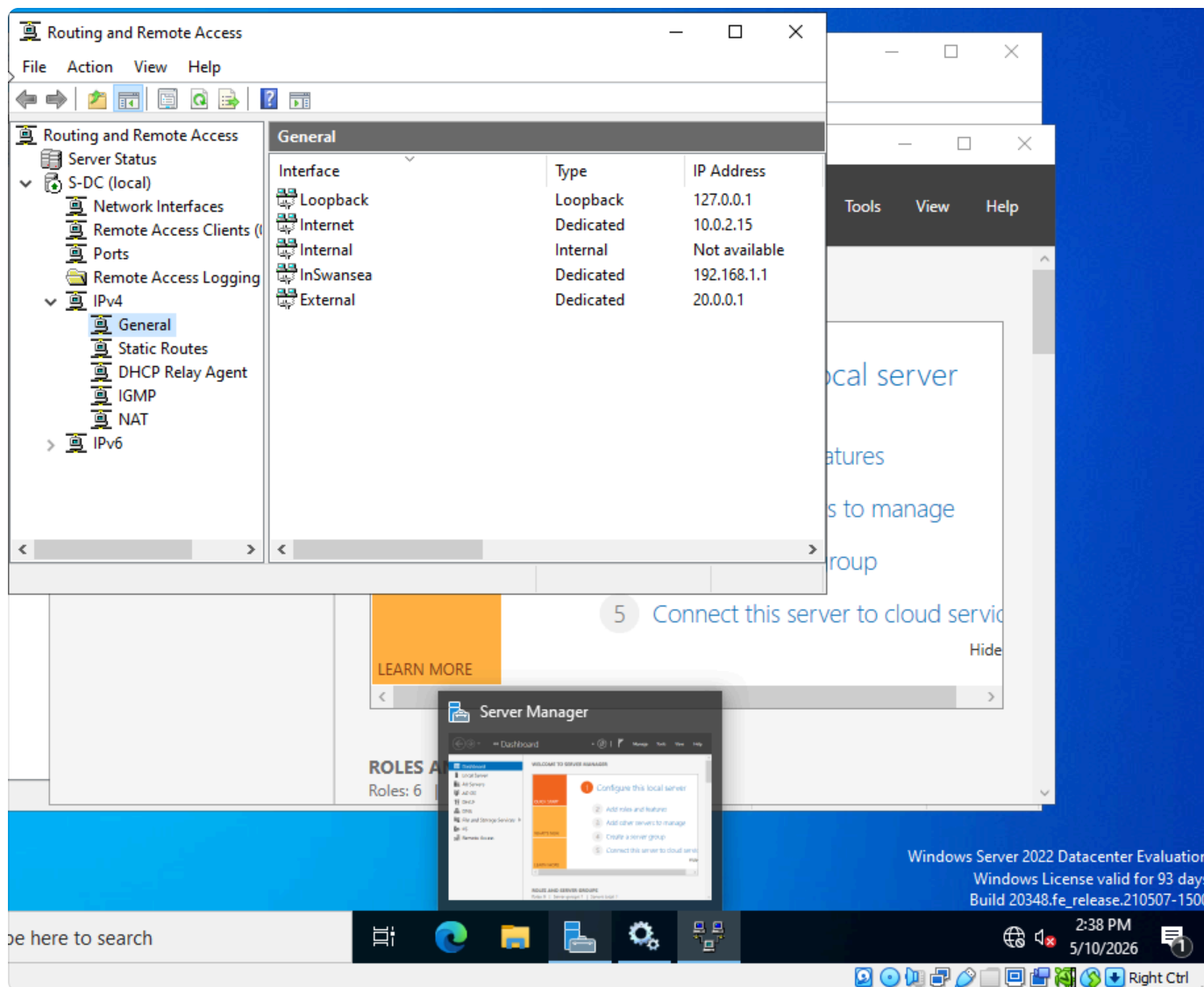
1. Routing Configuration

Figure 1 – RRAS Successfully Configured on S-DC



Caption: This screenshot shows Routing and Remote Access Services configured on the Swansea Domain Controller.

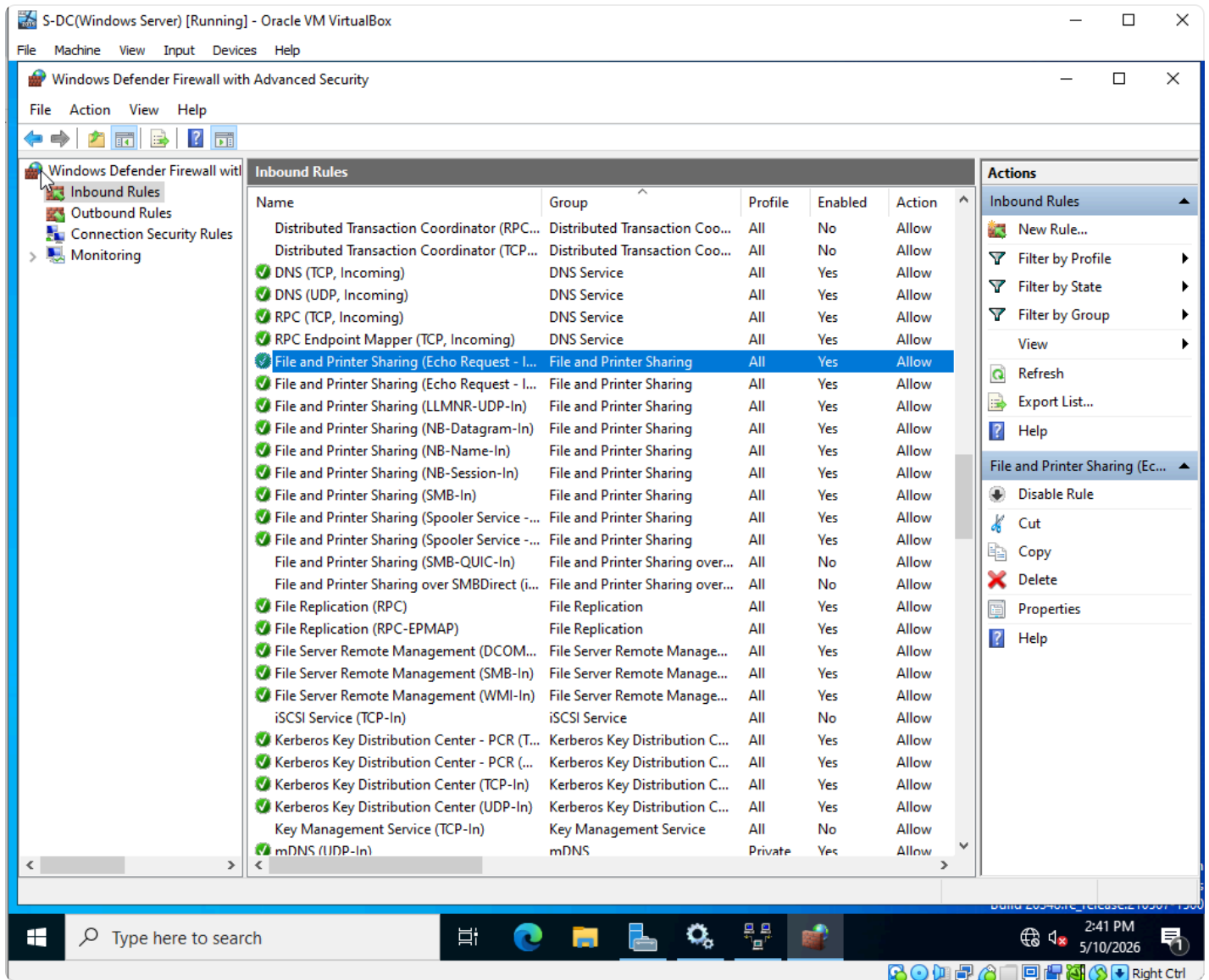
Figure 2/3 – RRAS IPv4 Configuration-RRAS Network Interfaces



Caption: This screenshot shows IPv4 routing configured within RRAS.

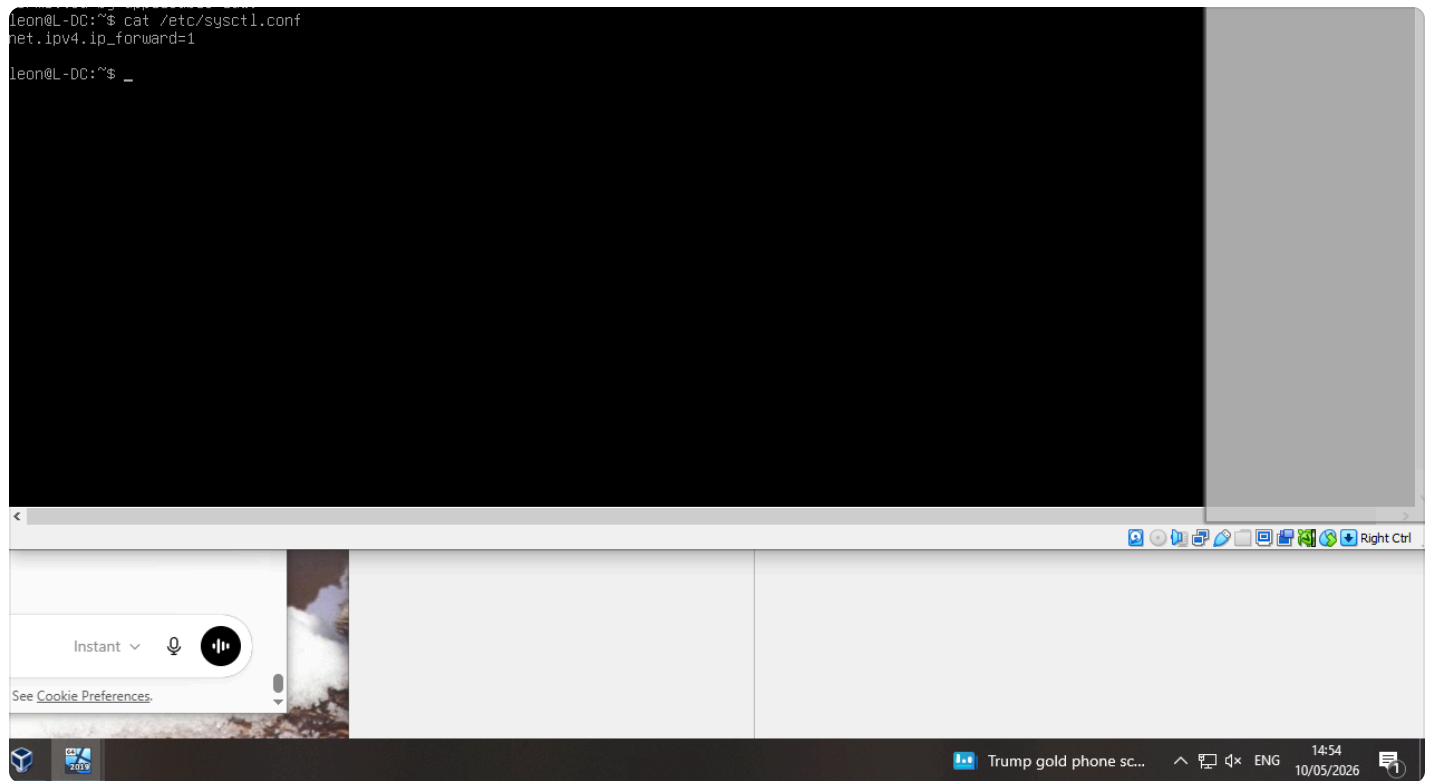
Caption: This screenshot shows configured RRAS network interfaces.

Figure 4 – ICMP Firewall Rules Enabled



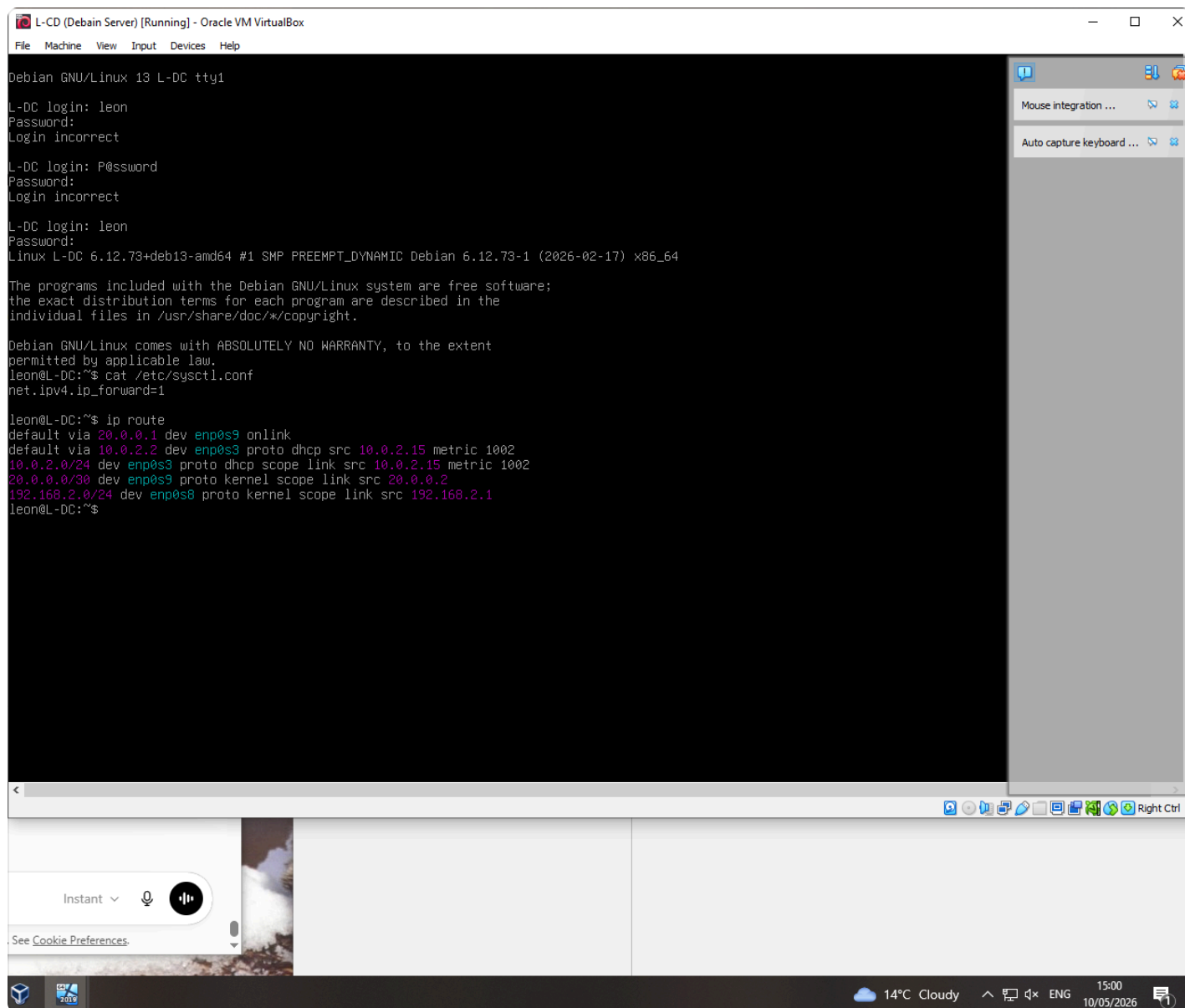
Caption: This screenshot shows ICMP traffic enabled within Windows Defender Firewall to allow successful ping communication between devices.

Figure 5 – Debian IP Forwarding Configuration



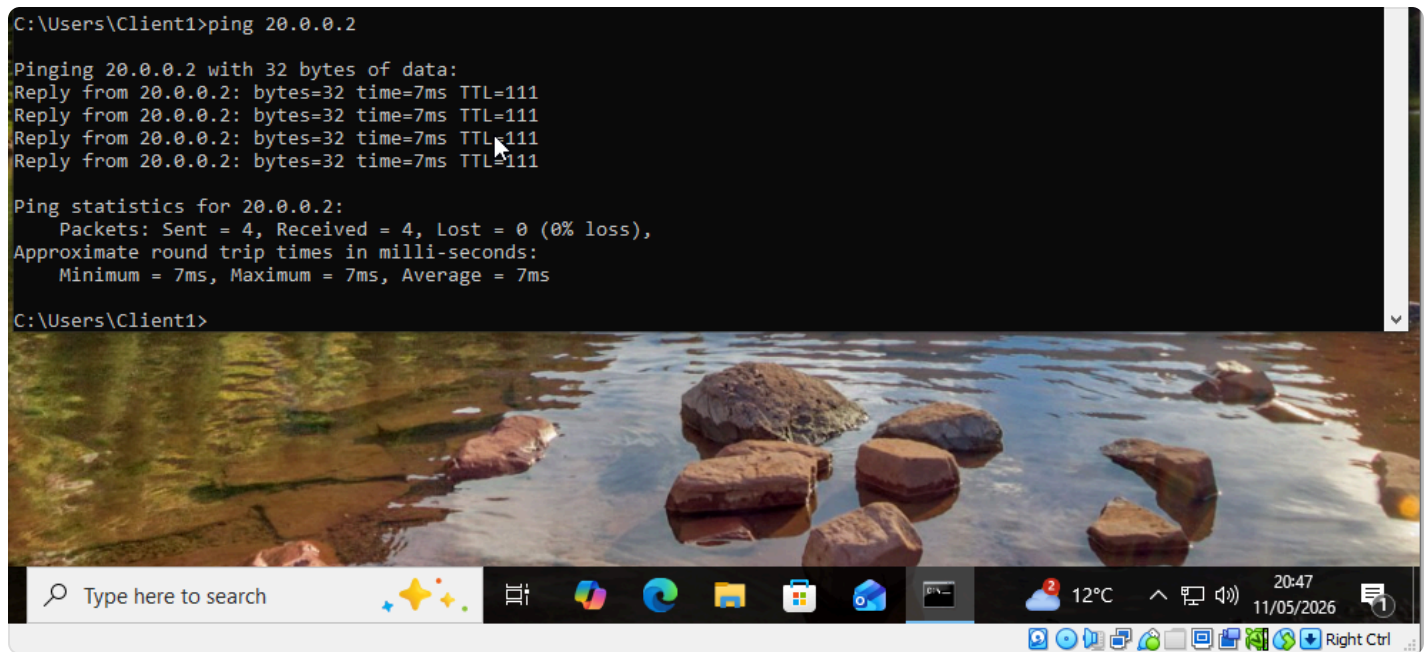
Caption: This screenshot shows IP forwarding configured on the Debian London router.

Figure 6 – Debian Routing Table



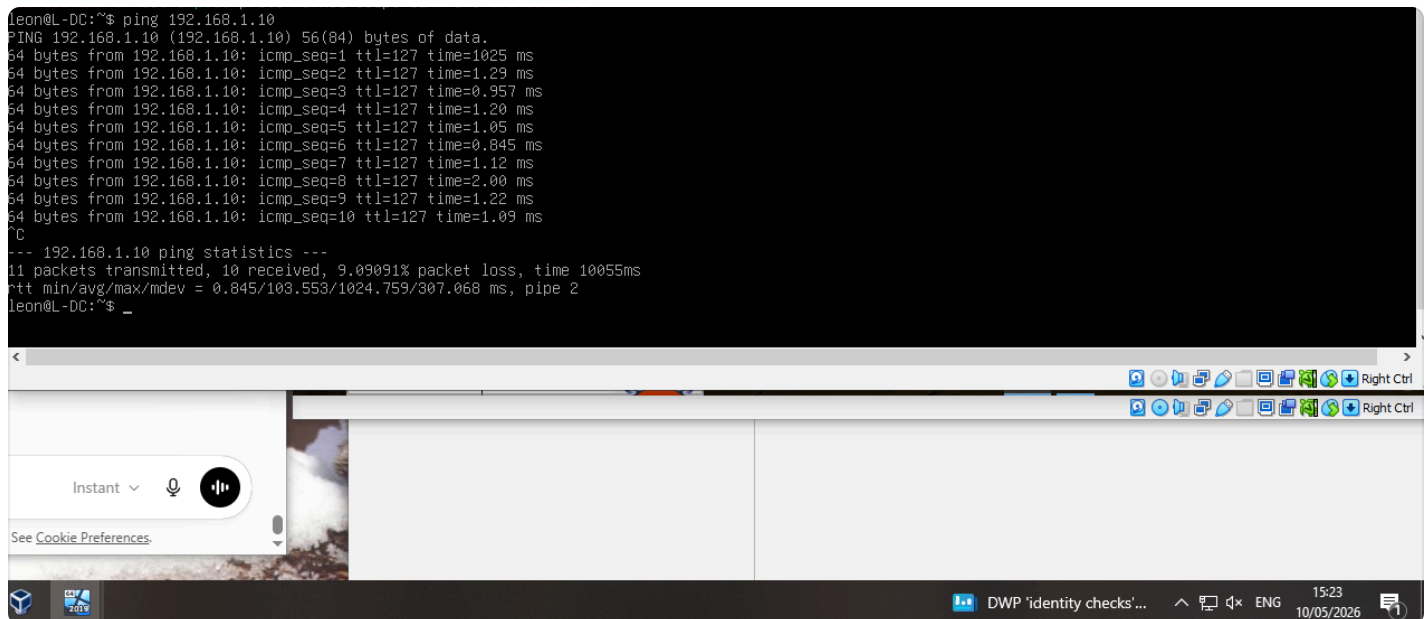
Caption: This screenshot shows the configured routing table on the Debian London router.

Figure 7 – Successful Ping from Swansea to London



Caption: This screenshot shows successful communication between the Swansea and London networks.

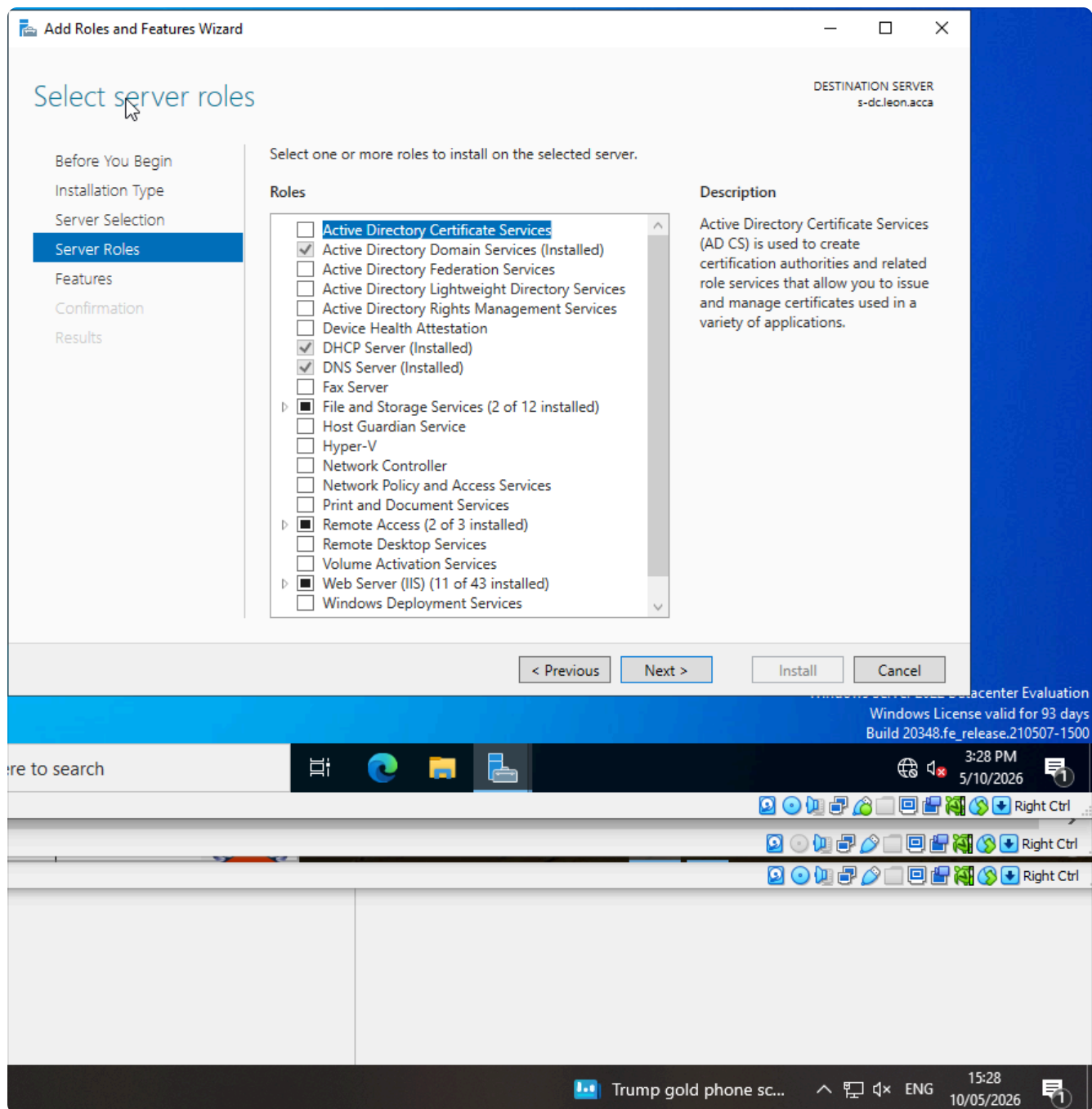
Figure 8 – Successful Ping from London to Swansea



Caption: This screenshot shows successful communication between the London and Swansea networks.

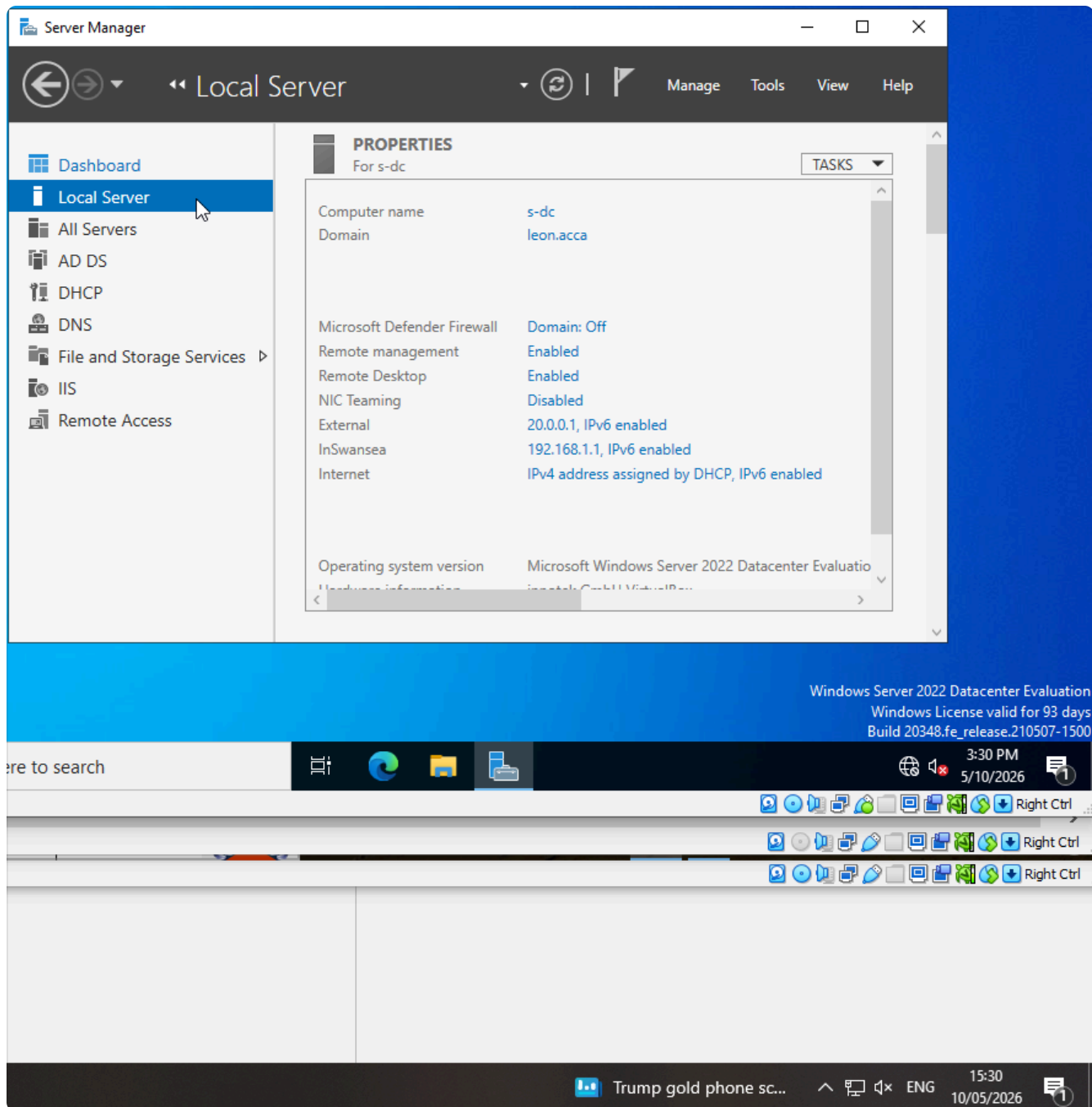
2. Active Directory Domain Services (ADDS)

Figure 9 – ADDS Role Installation



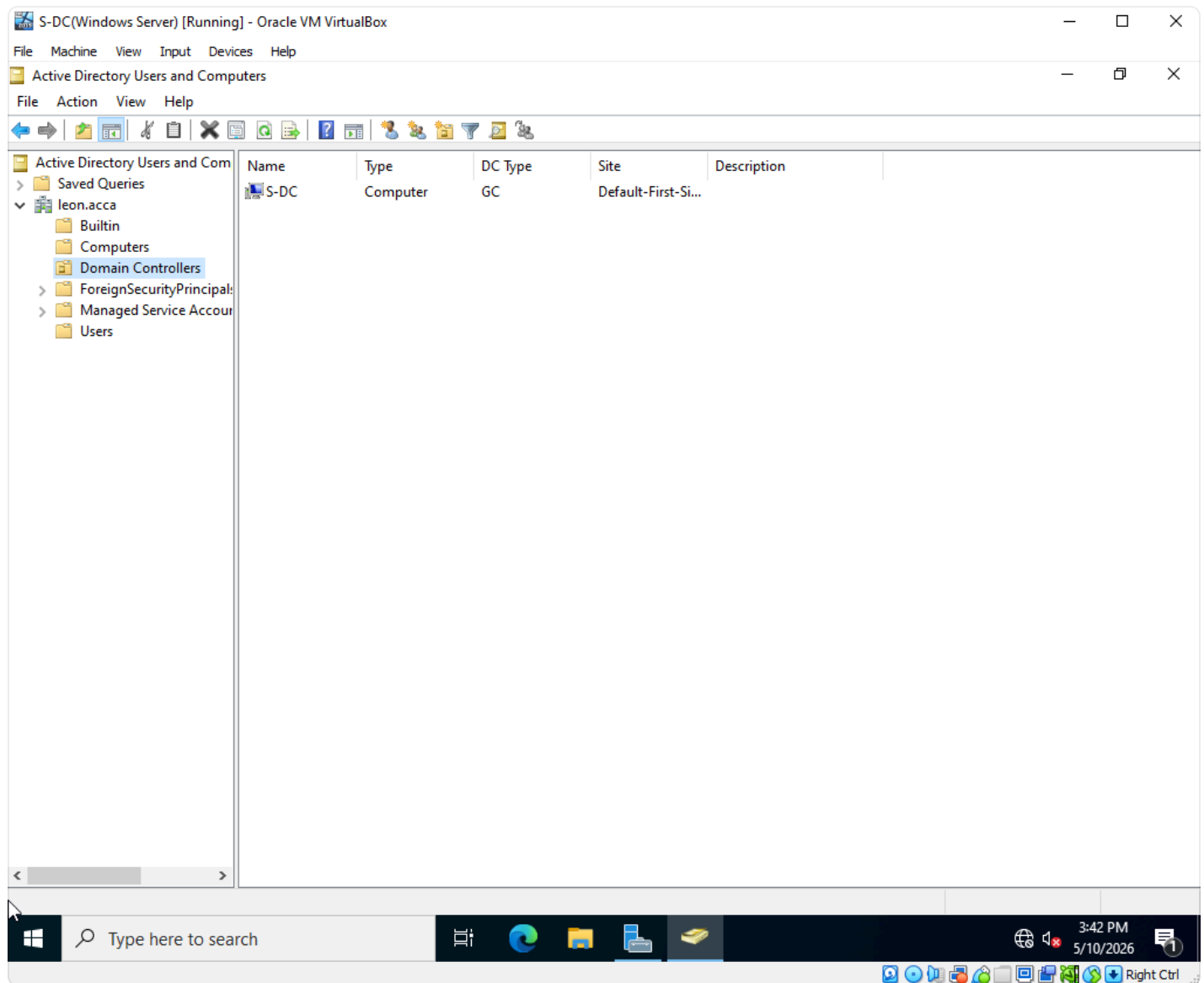
Caption: This screenshot shows Active Directory Domain Services installed on S-DC.

Figure 10 – Domain Creation (leon.acca)



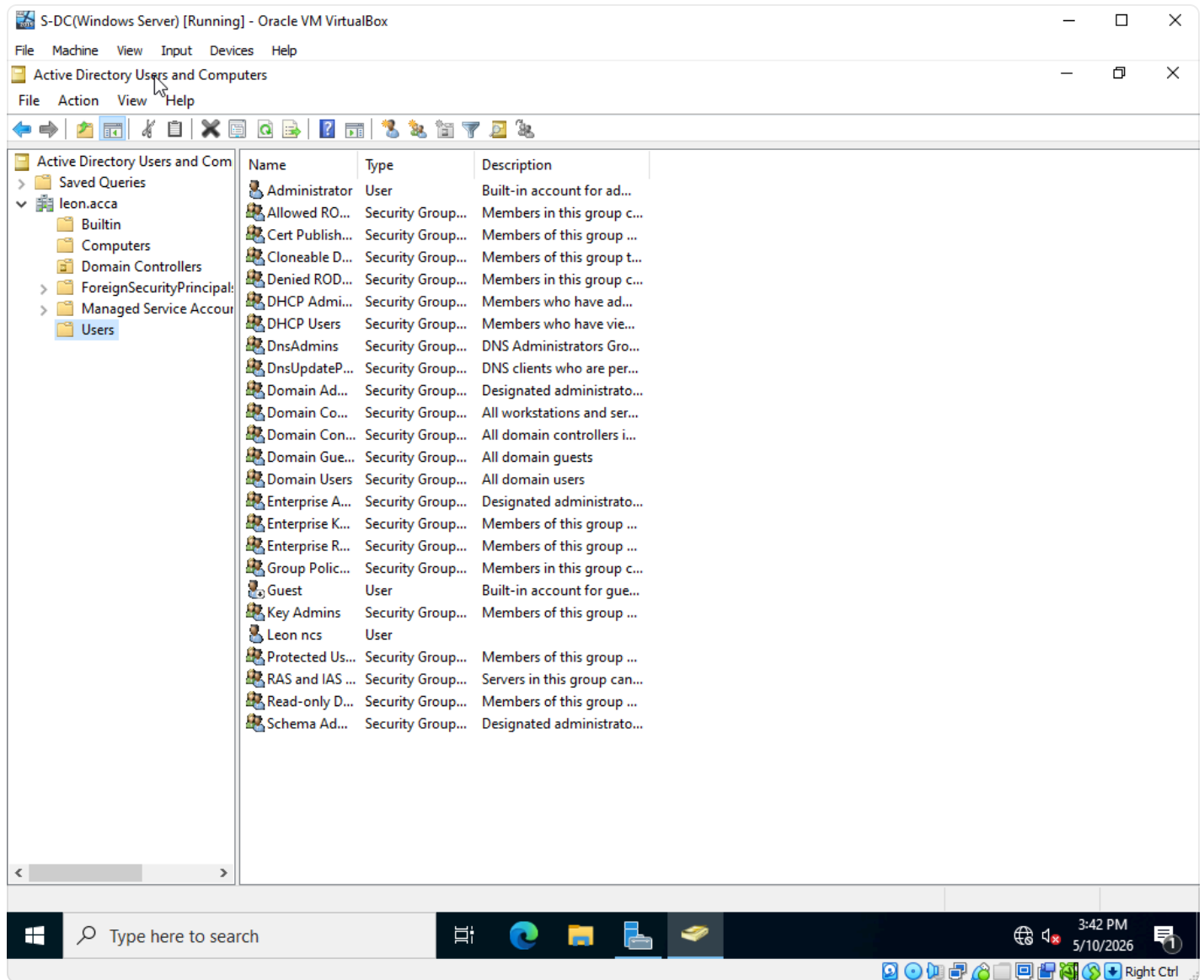
Caption: This screenshot shows the successful creation of the leon.acca domain.

Figure 11 – Domain Controller Configuration



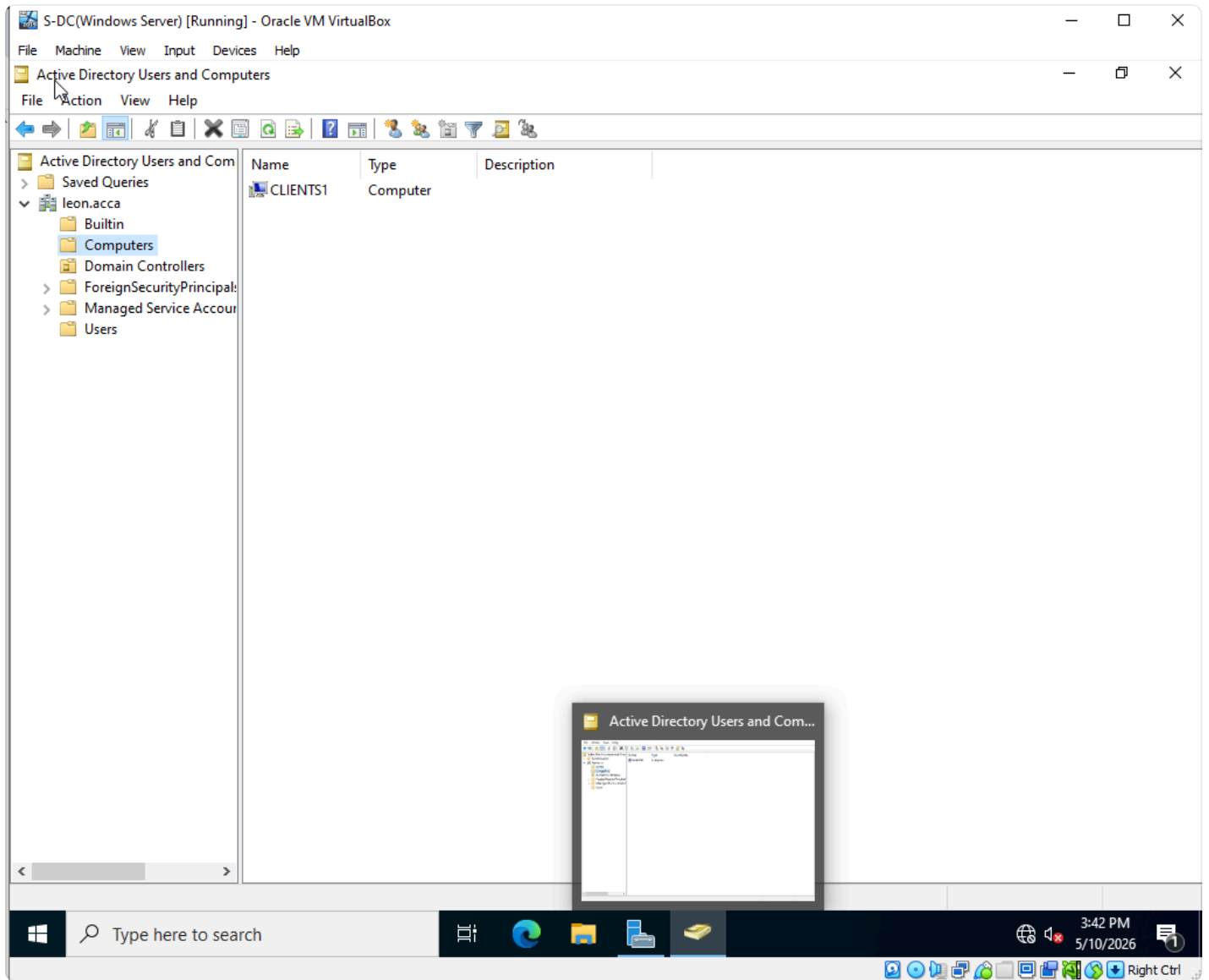
Caption: This screenshot shows S-DC configured as the Domain Controller.

Figure 12 – Active Directory Users and Computers Console



Caption: This screenshot shows the Active Directory Users and Computers management console.

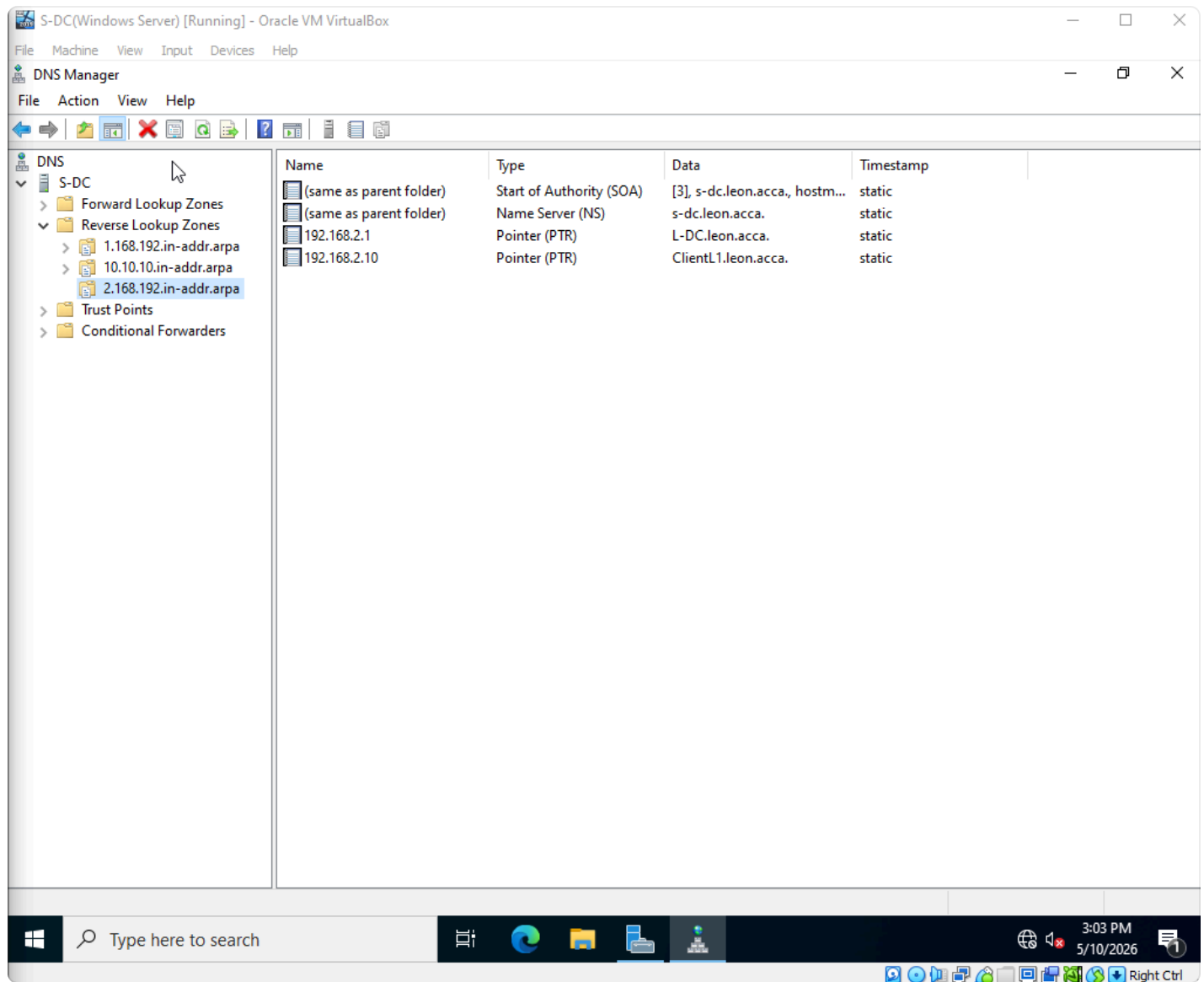
Figure 13 – Organisational Units Configuration



Caption: This screenshot shows the configured organisational units within Active Directory.

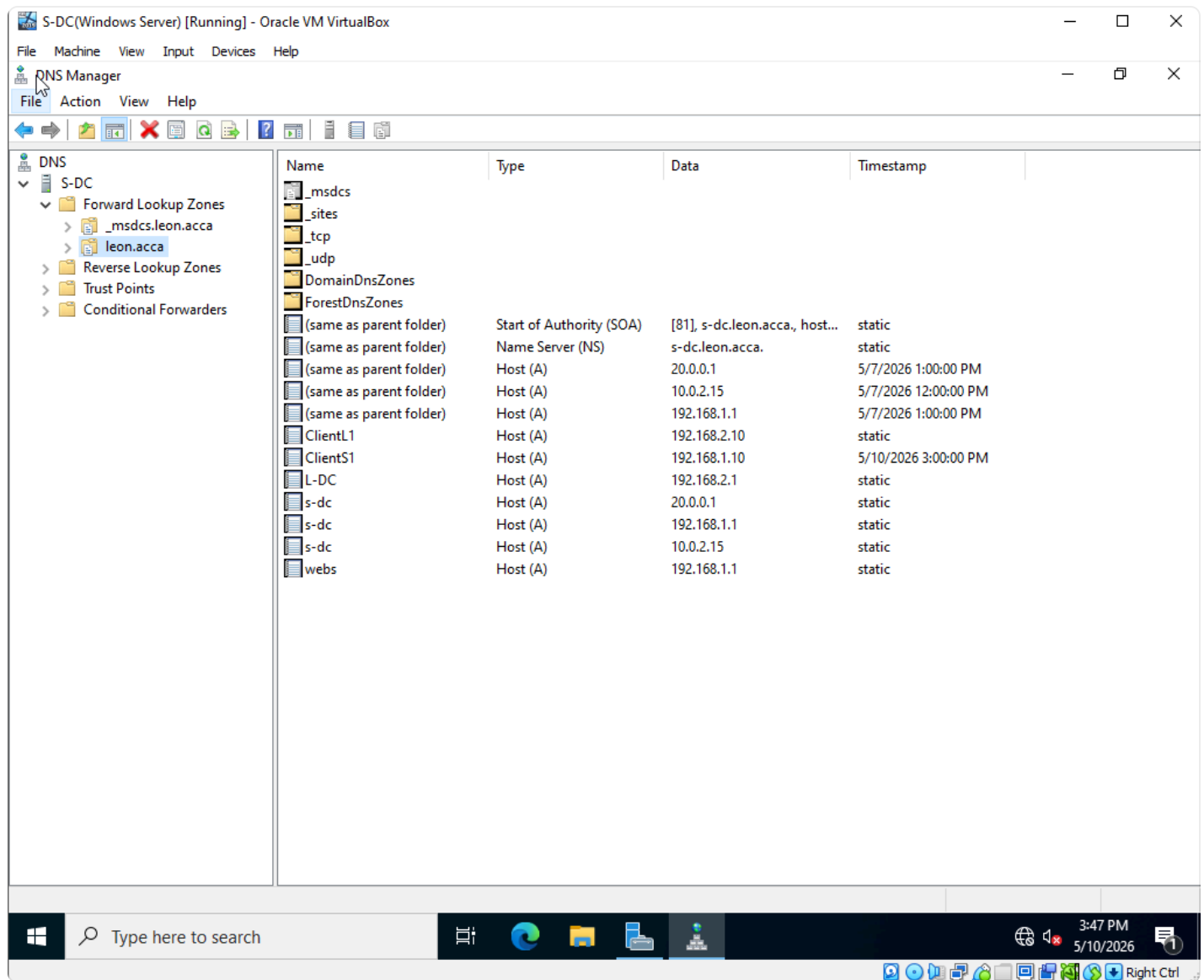
3. DNS Configuration

Figure 14 – DNS Manager Overview



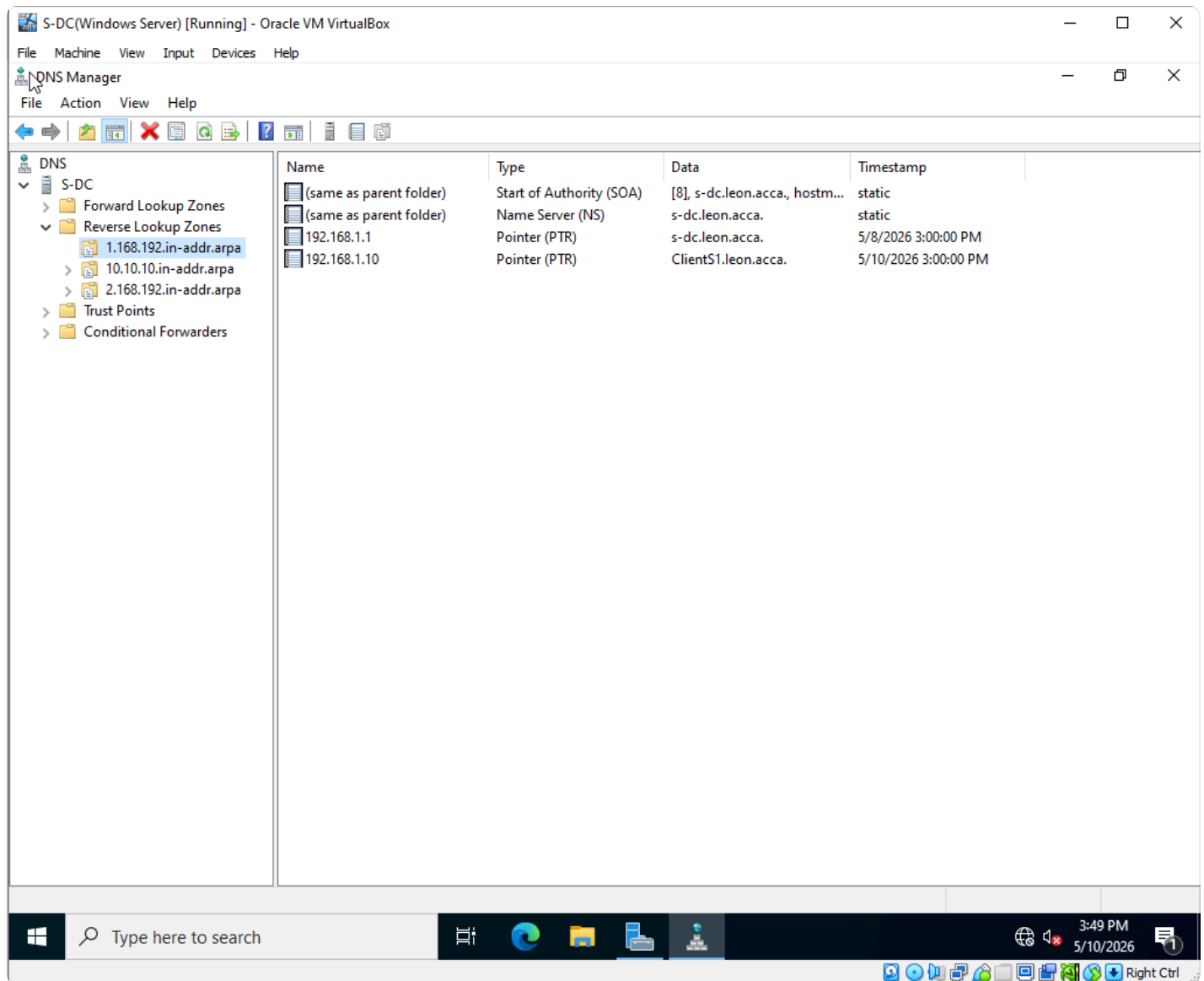
Caption: This screenshot shows the DNS Manager overview including all configured zones.

Figure 15 – Forward Lookup Zone



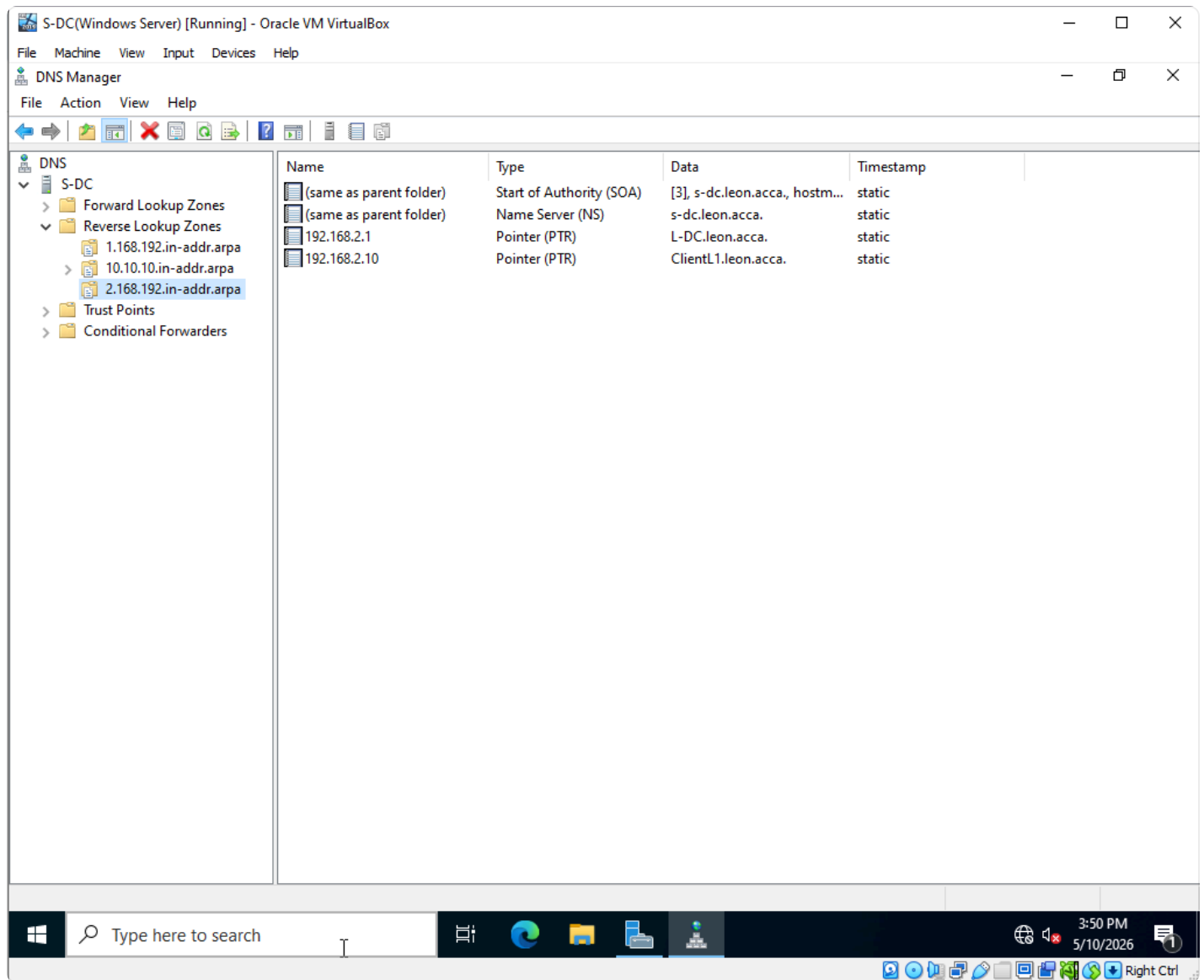
Caption: This screenshot shows the forward lookup zone for leon.acca.

Figure 16 – Reverse Lookup Zone (192.168.1.0)



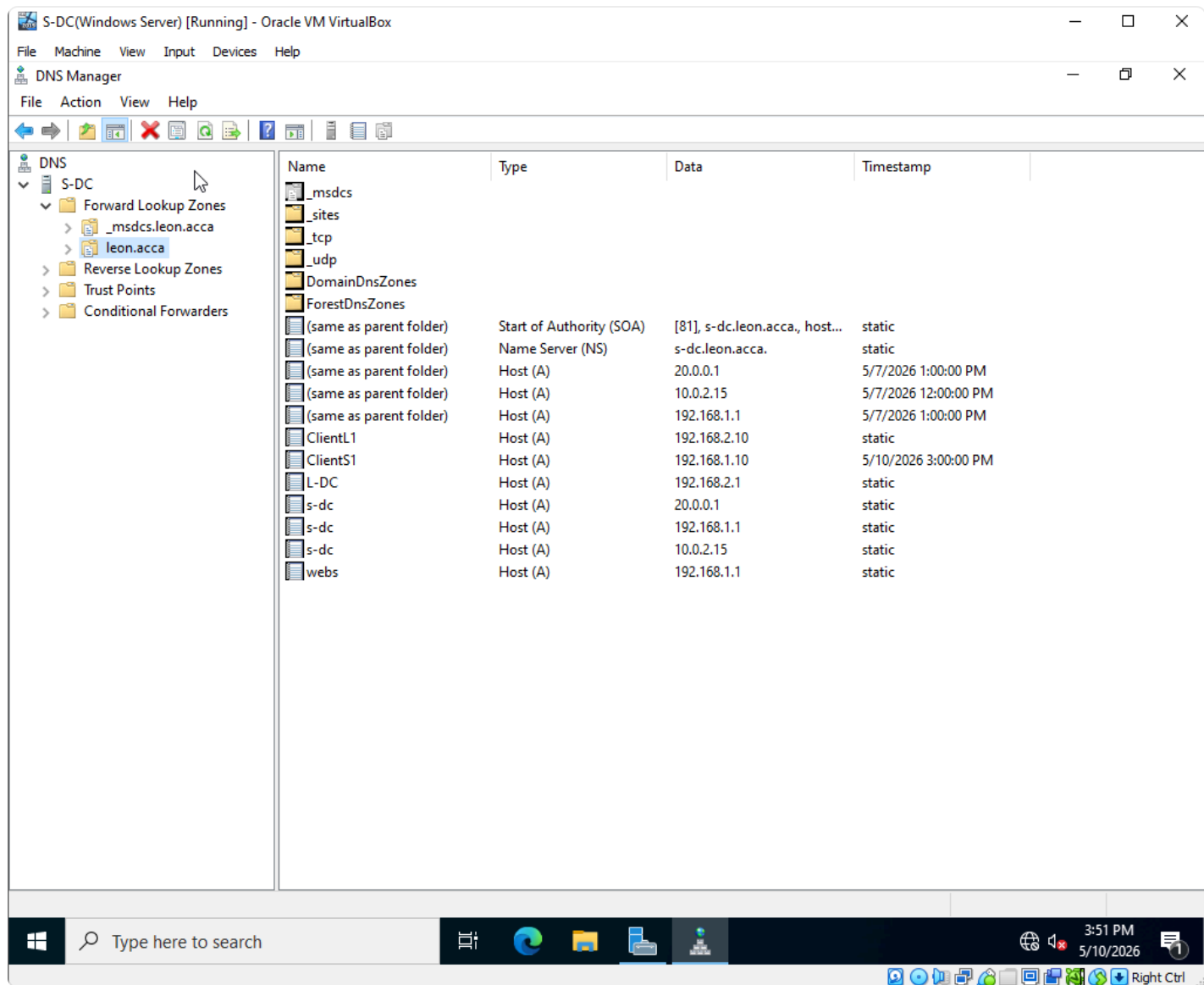
Caption: This screenshot shows the reverse lookup zone configured for the Swansea network.

Figure 17 – Reverse Lookup Zone (192.168.2.0)



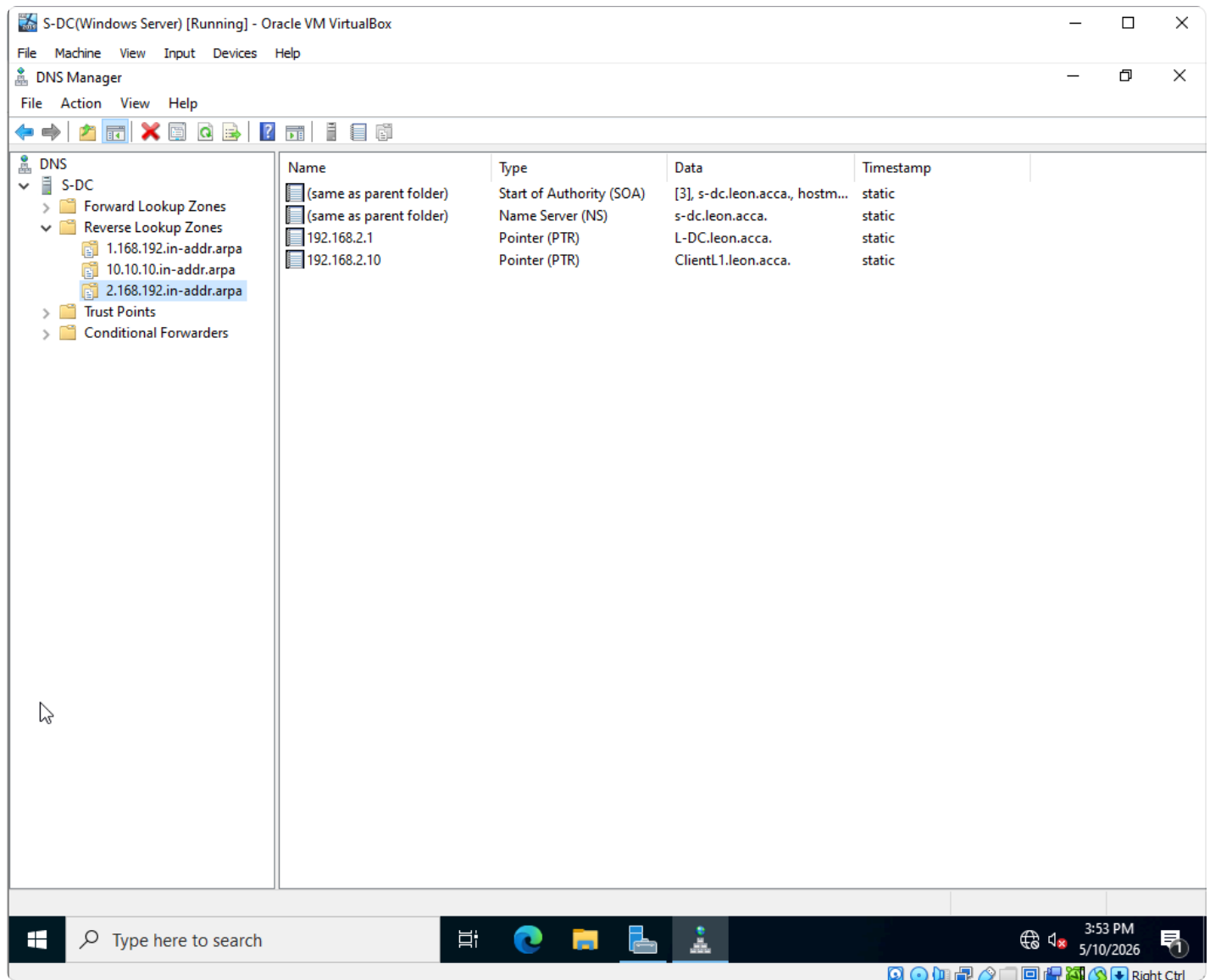
Caption: This screenshot shows the reverse lookup zone configured for the London network.

Figure 18 – DNS Host (A) Records



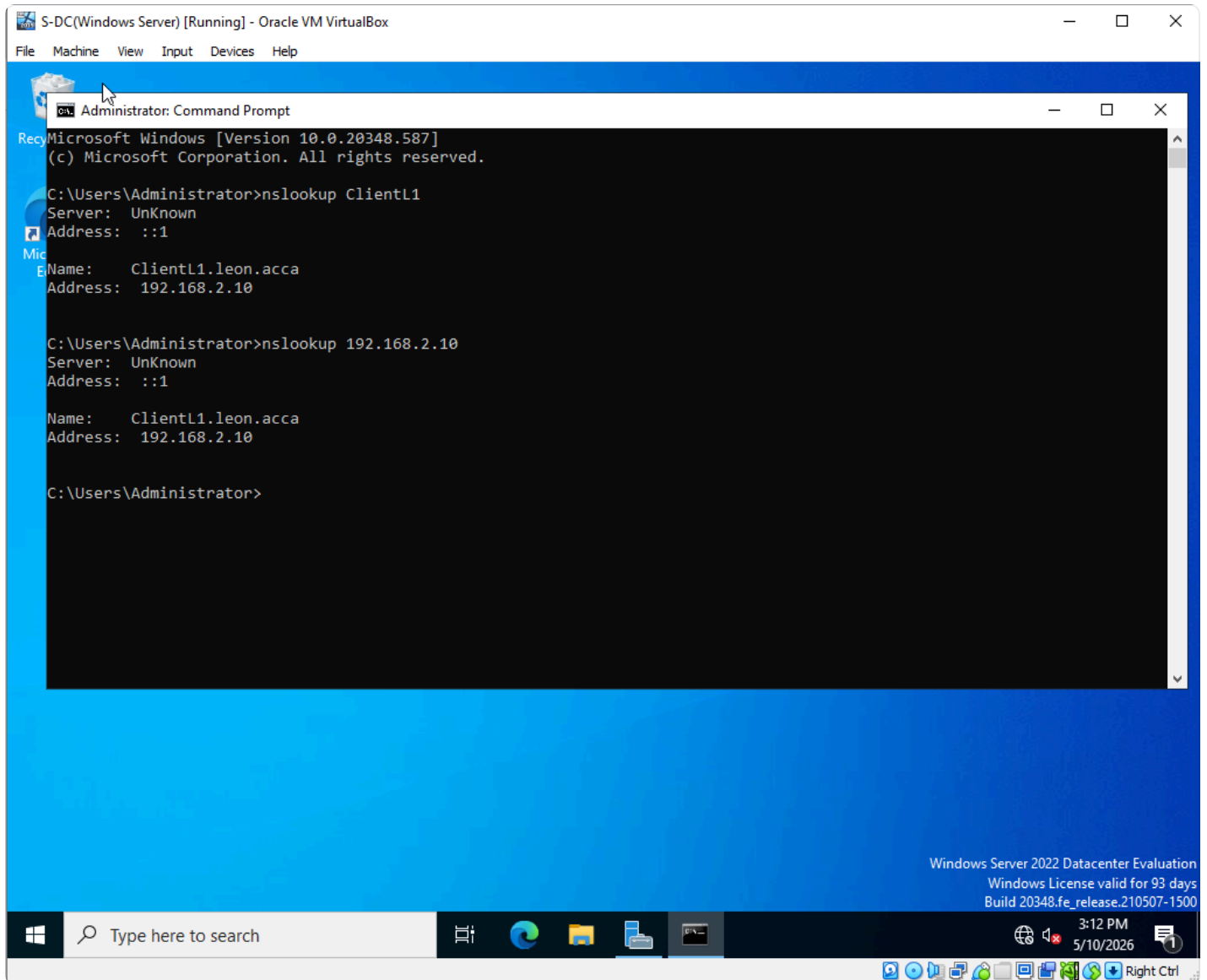
Caption: This screenshot shows the configured DNS A records for all devices.

Figure 19 – DNS PTR Records



Caption: This screenshot shows the configured PTR records used for reverse DNS lookups.

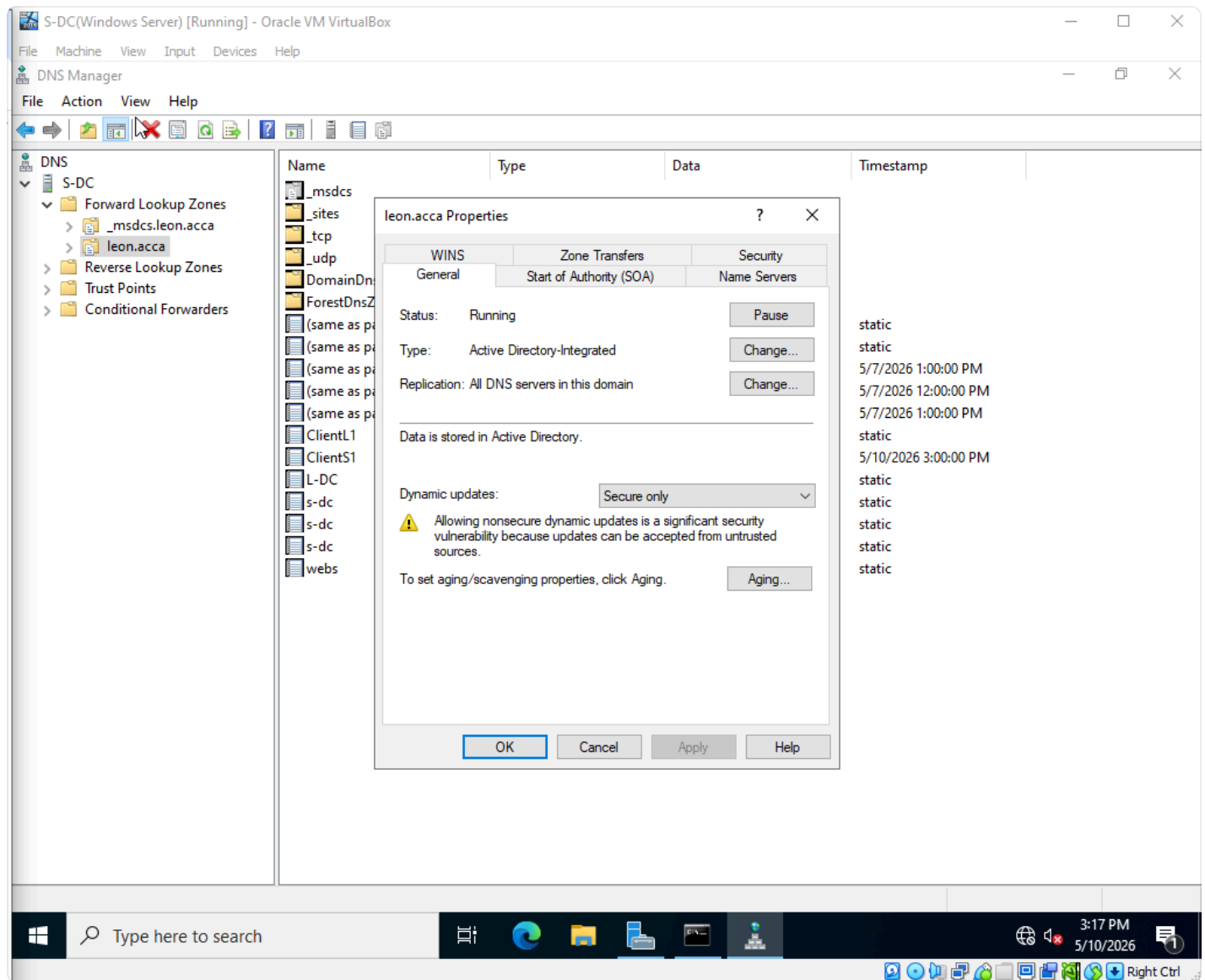
Figure 20 – nslookup Testing



Caption: This screenshot shows successful DNS resolution using nslookup.

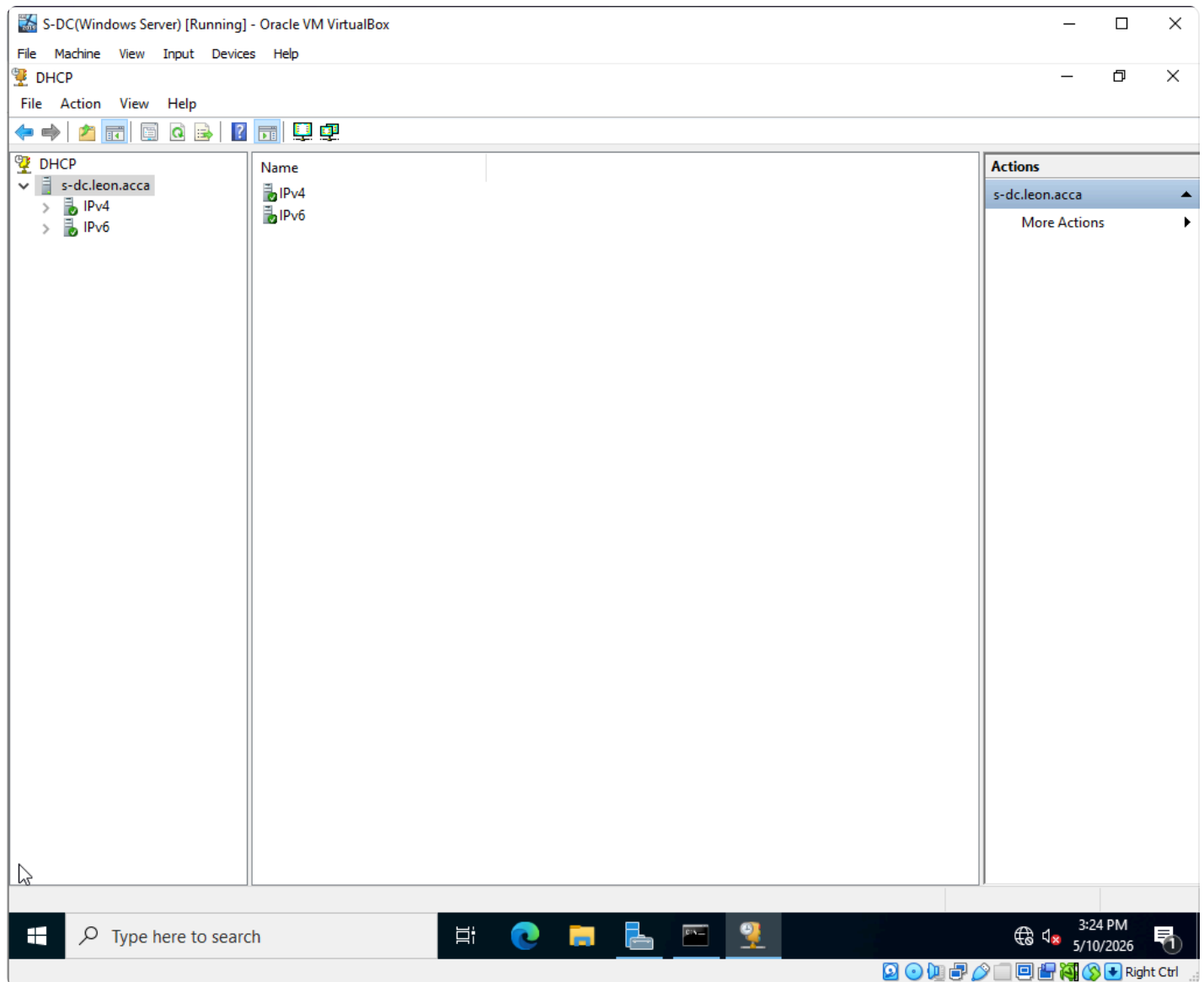
4. DHCP Configuration

Figure 21 – DHCP Role Installation



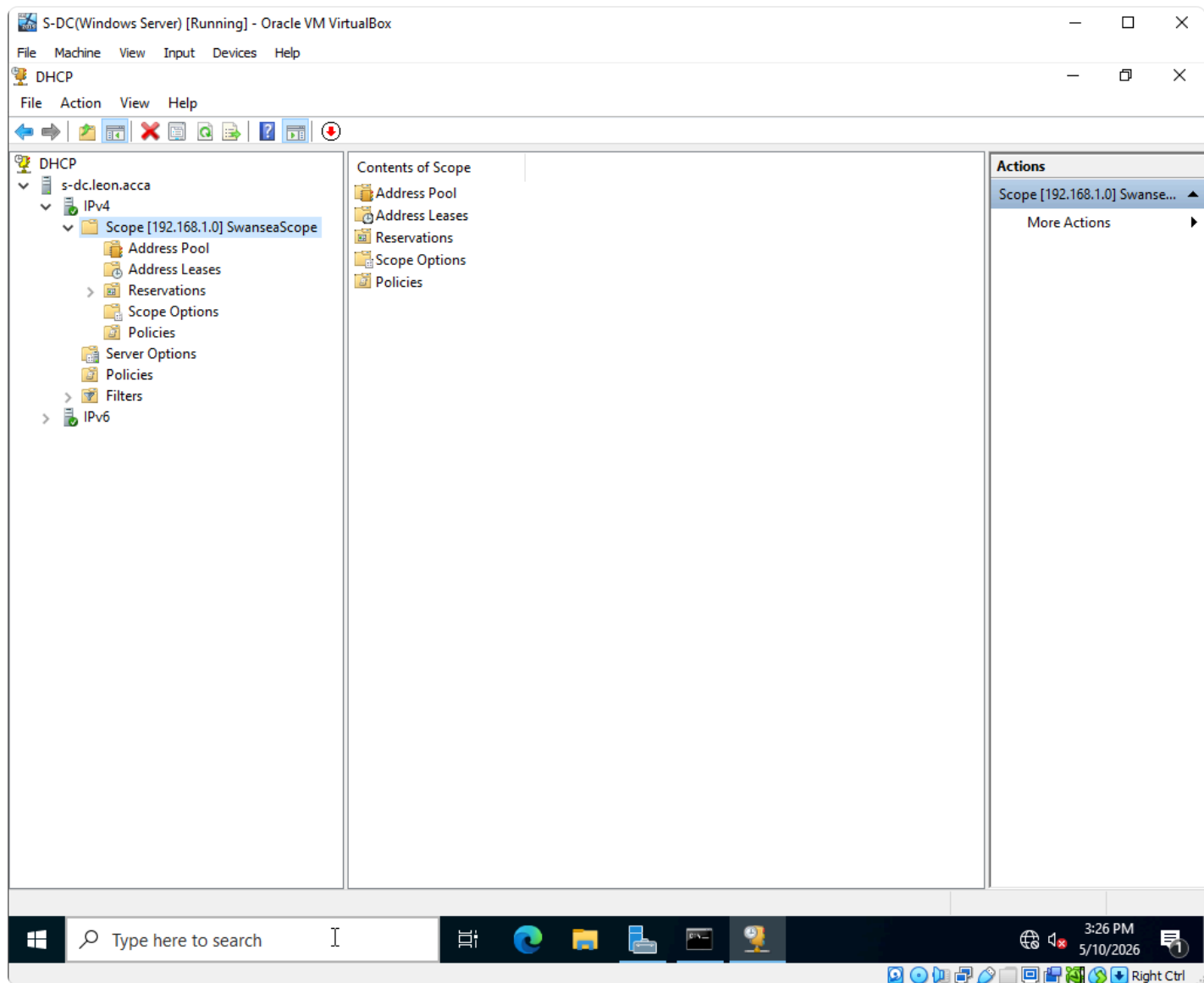
Caption: This screenshot shows the DHCP Server role installed on S-DC.

Figure 22 – DHCP Server Authorisation



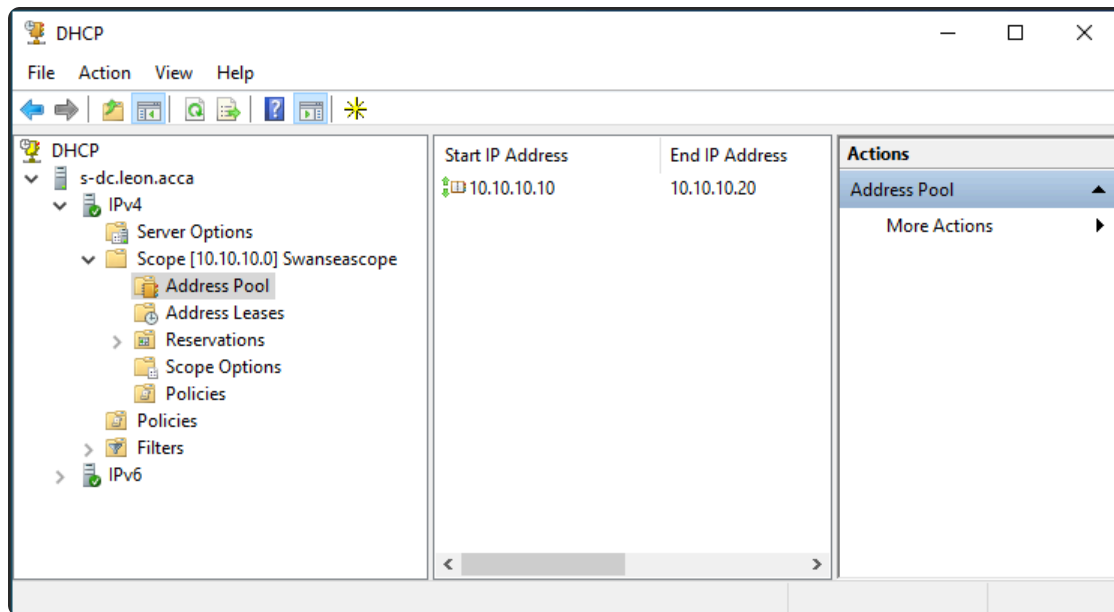
Caption: This screenshot shows the DHCP server authorised within Active Directory.

Figure 23 – DHCP Scope Configuration



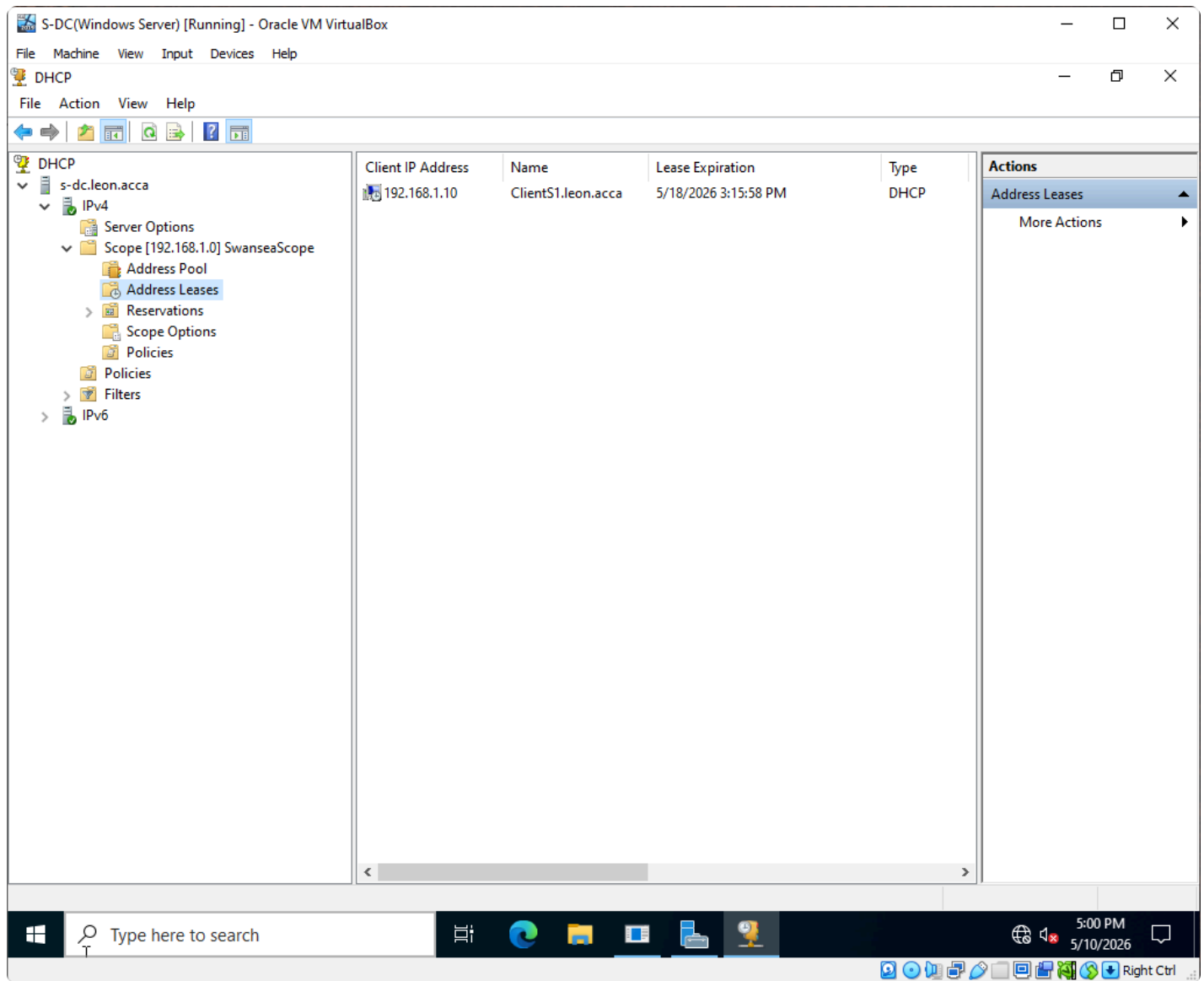
Caption: This screenshot shows the DHCP scope configured for the Swansea network.

Figure 24 – DHCP Address Pool



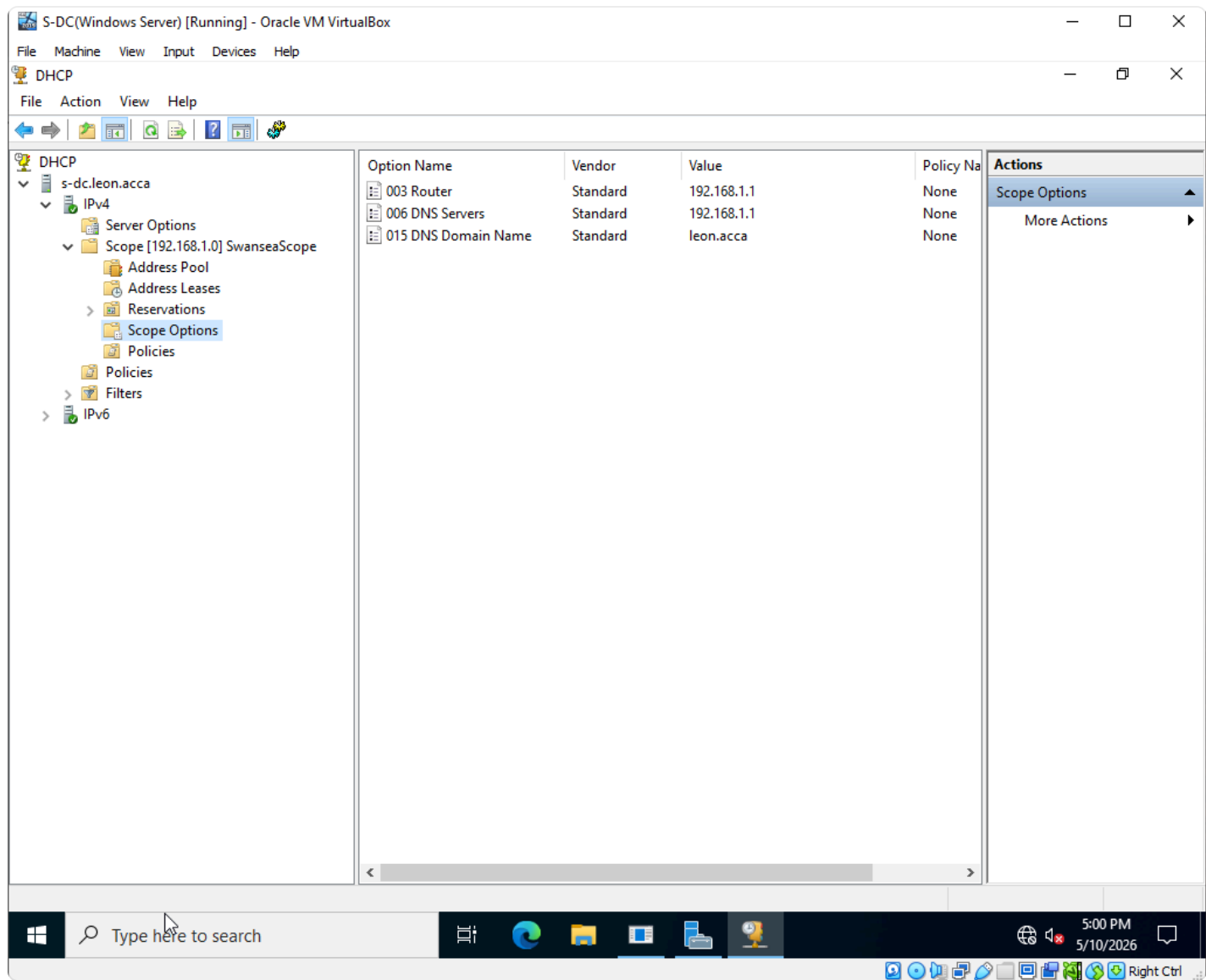
Caption: This screenshot shows the configured DHCP address pool.

Figure 25 – DHCP Scope Options



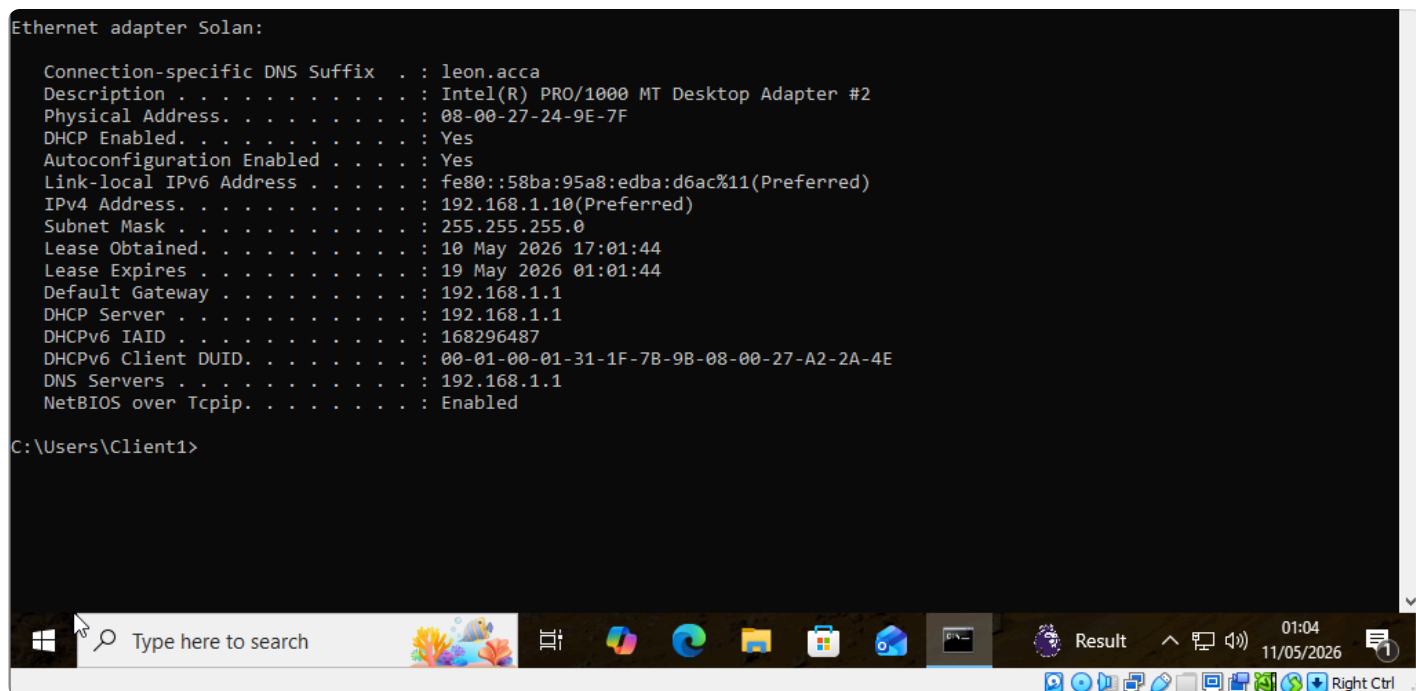
Caption: This screenshot shows the configured DHCP scope options, including gateway and DNS settings.

Figure 26 – DHCP Lease Allocation



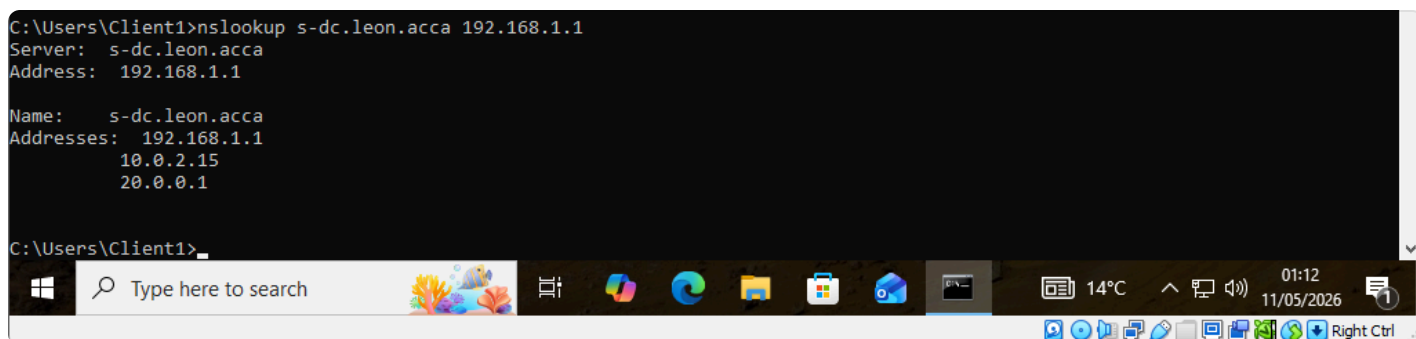
Caption: This screenshot shows DHCP successfully assigning IP addresses to client devices.

Figure 27 – DHCP Relay Configuration



Caption: This screenshot shows DHCP relay configuration between Swansea and London networks.

Figure 28 – DNS Name Resolution Test



This screenshot shows successful DNS name resolution from the client workstation to the domain controller using the internal DNS server, confirming correct DNS functionality within the enterprise network.

Figure 29 – Network Connectivity Verification

```
C:\Users\Client1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

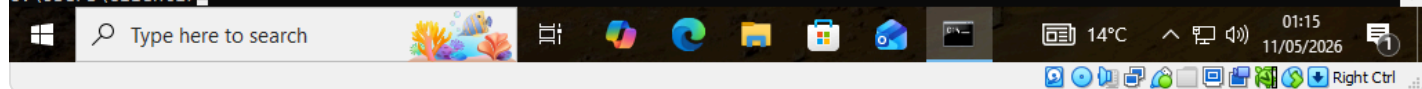
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Client1>ping s-dc.leon.acca

Pinging s-dc.leon.acca [192.168.1.1] with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

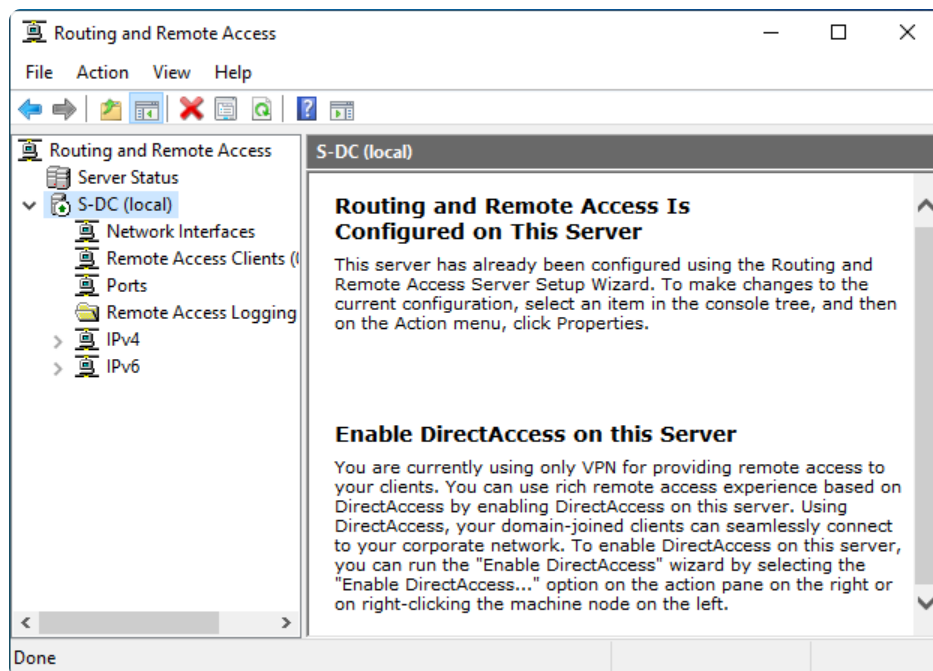
C:\Users\Client1>
```



This screenshot shows successful network connectivity tests between the client workstation and the domain controller using both direct IP addressing and DNS hostname resolution.

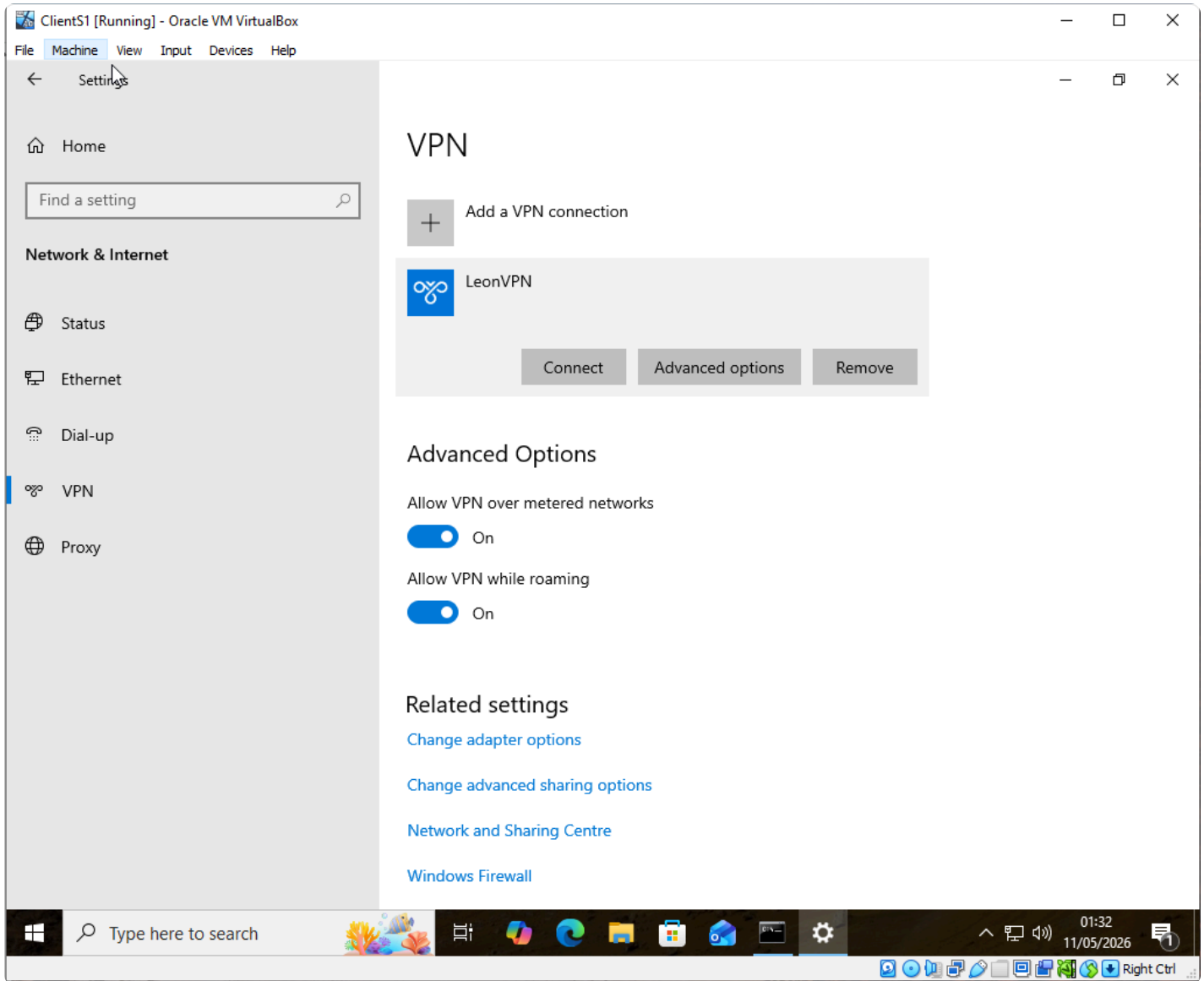
5. VPN Configuration

Figure 28 – RRAS VPN Configuration



Caption: This screenshot shows VPN configuration within Routing and Remote Access Services.

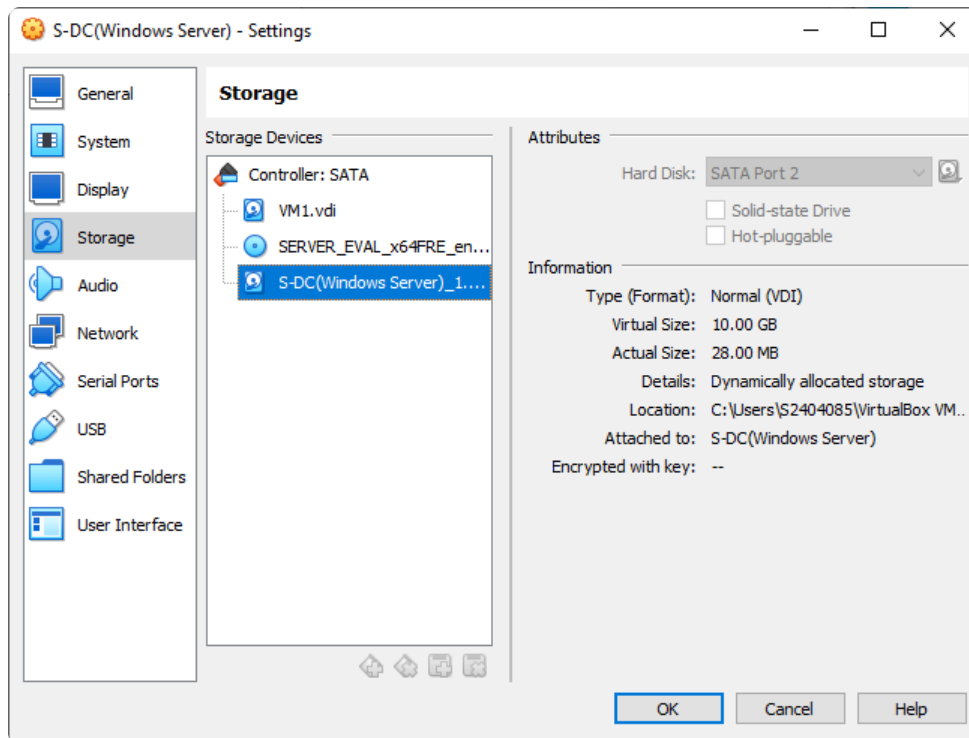
Figure 29 – VPN Connectivity Testing



Caption: This screenshot shows the VPN client connection configured on the workstation for secure remote access testing to the RRAS server.

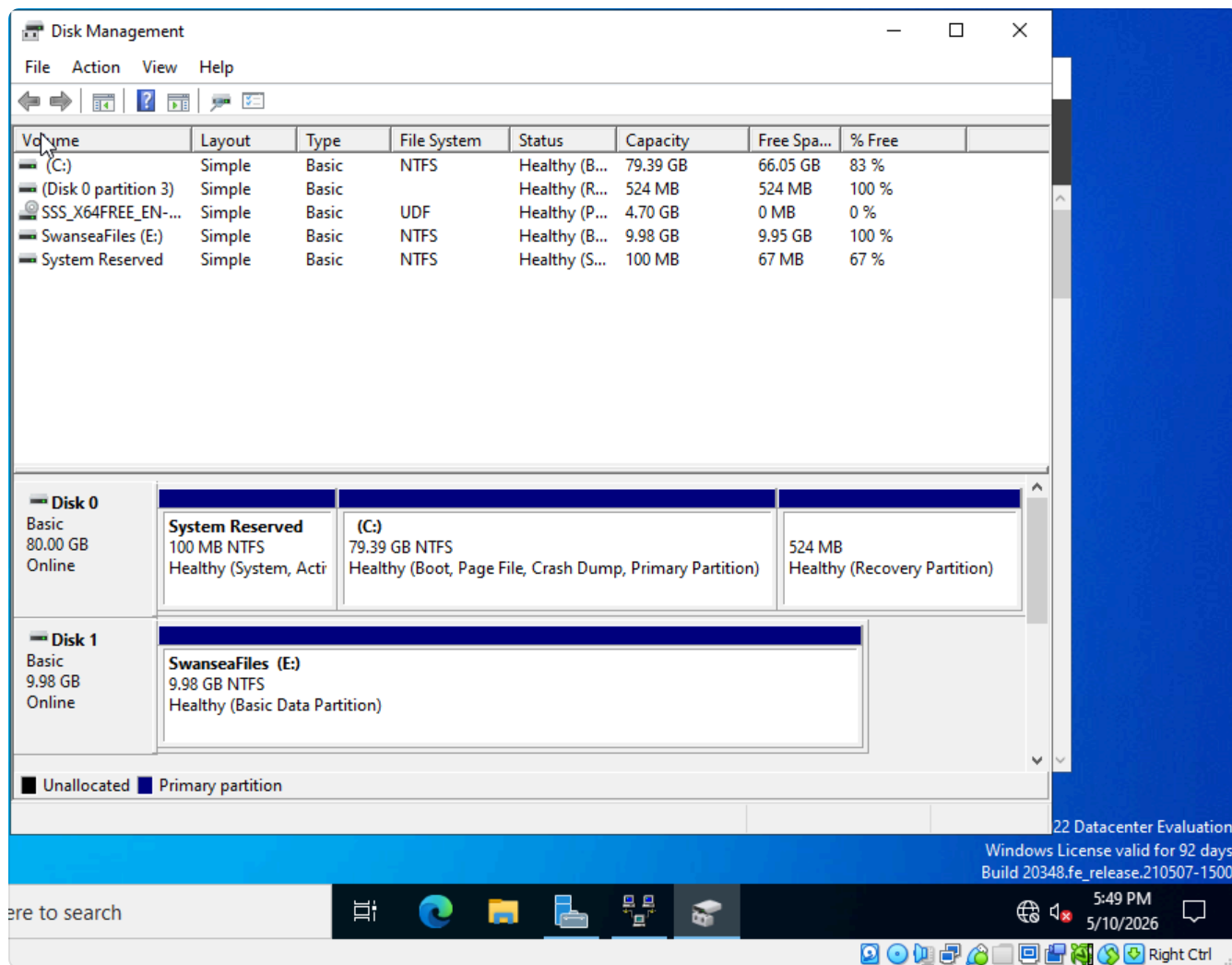
6. Shared Drive Configuration

Figure 30 – Additional Virtual Disk Configuration



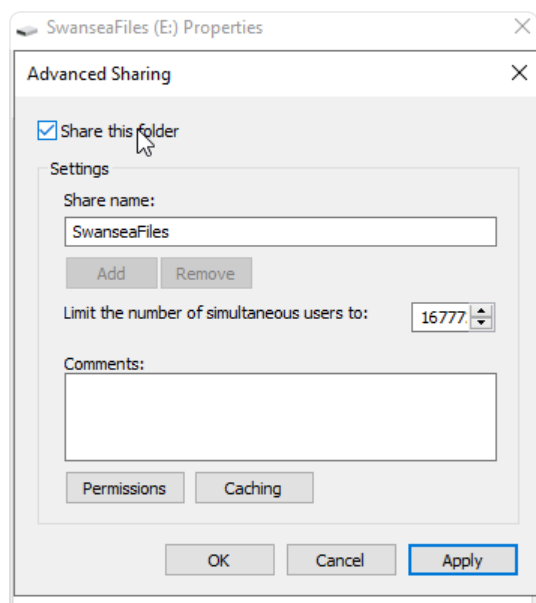
Caption: This screenshot shows the additional virtual hard disk configured on the server.

Figure 31 – E: Drive Successfully Mounted



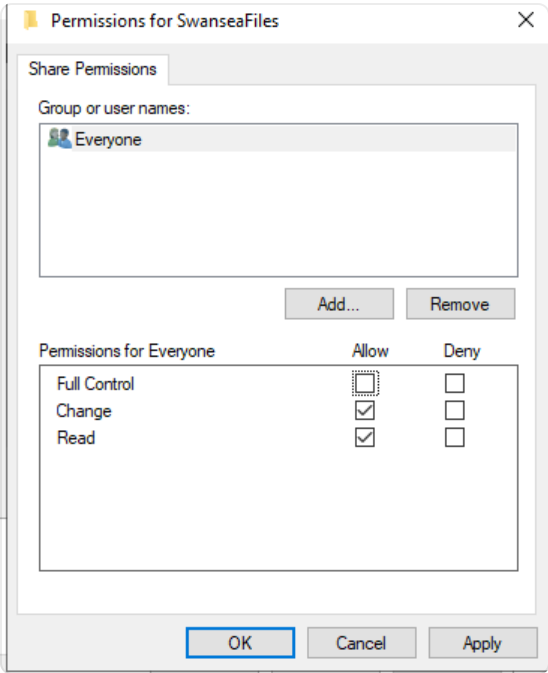
Caption: This screenshot shows the E: drive successfully mounted on S-DC.

Figure 32 – Shared Folder Creation



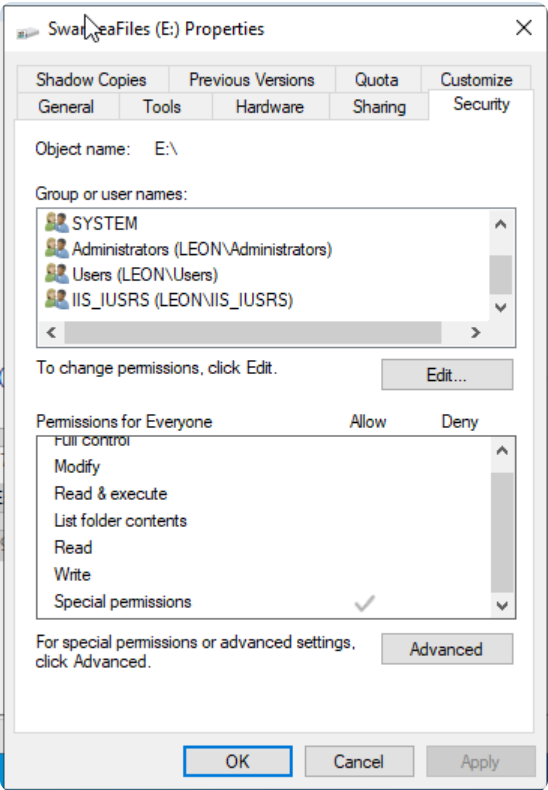
Caption: This screenshot shows the SwanseaFiles shared folder created on the E: drive.

Figure 33 – Shared Folder Permissions



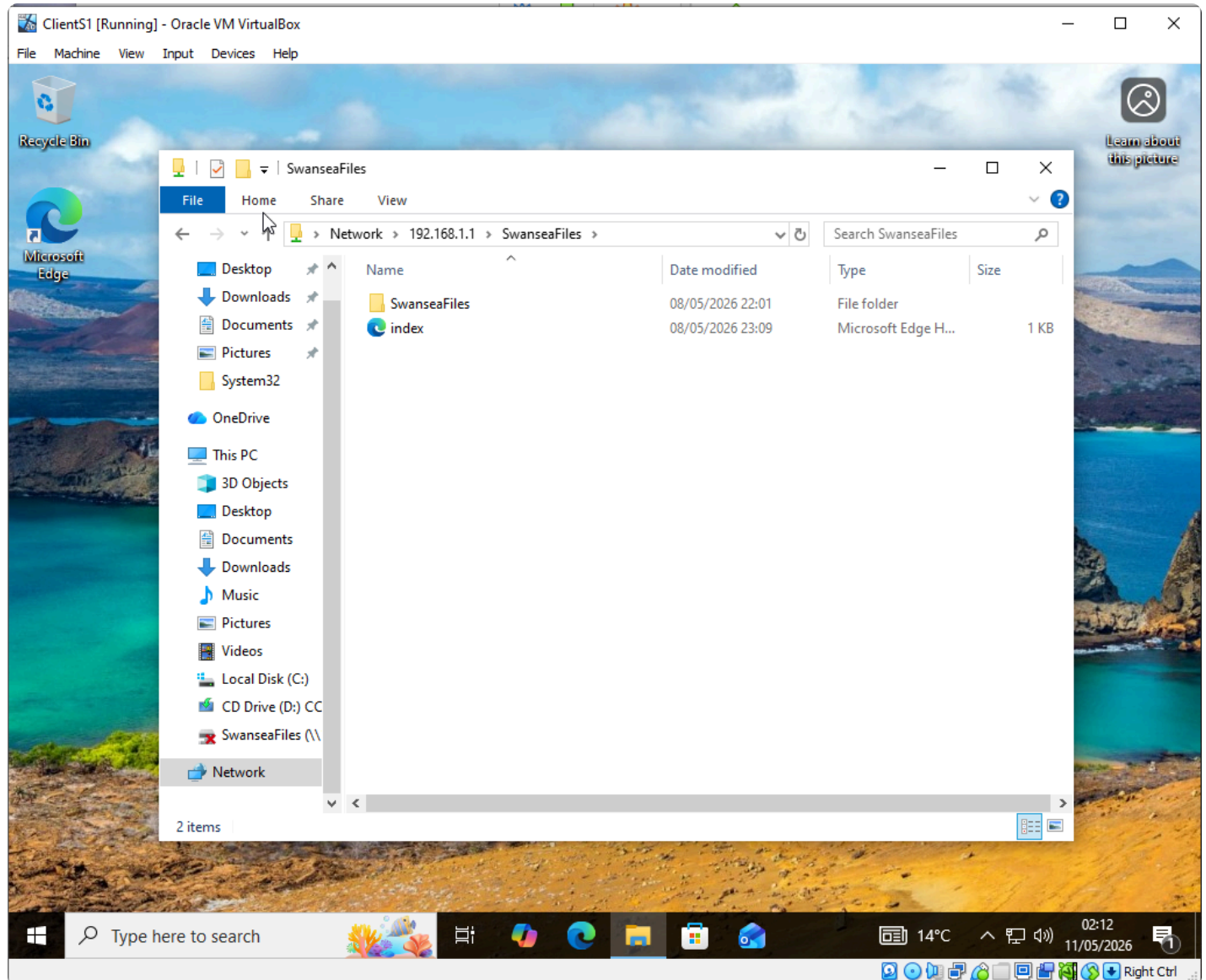
Caption: This screenshot shows the configured share permissions for the SwanseaFiles shared folder.

Figure 34 – NTFS Security Permissions



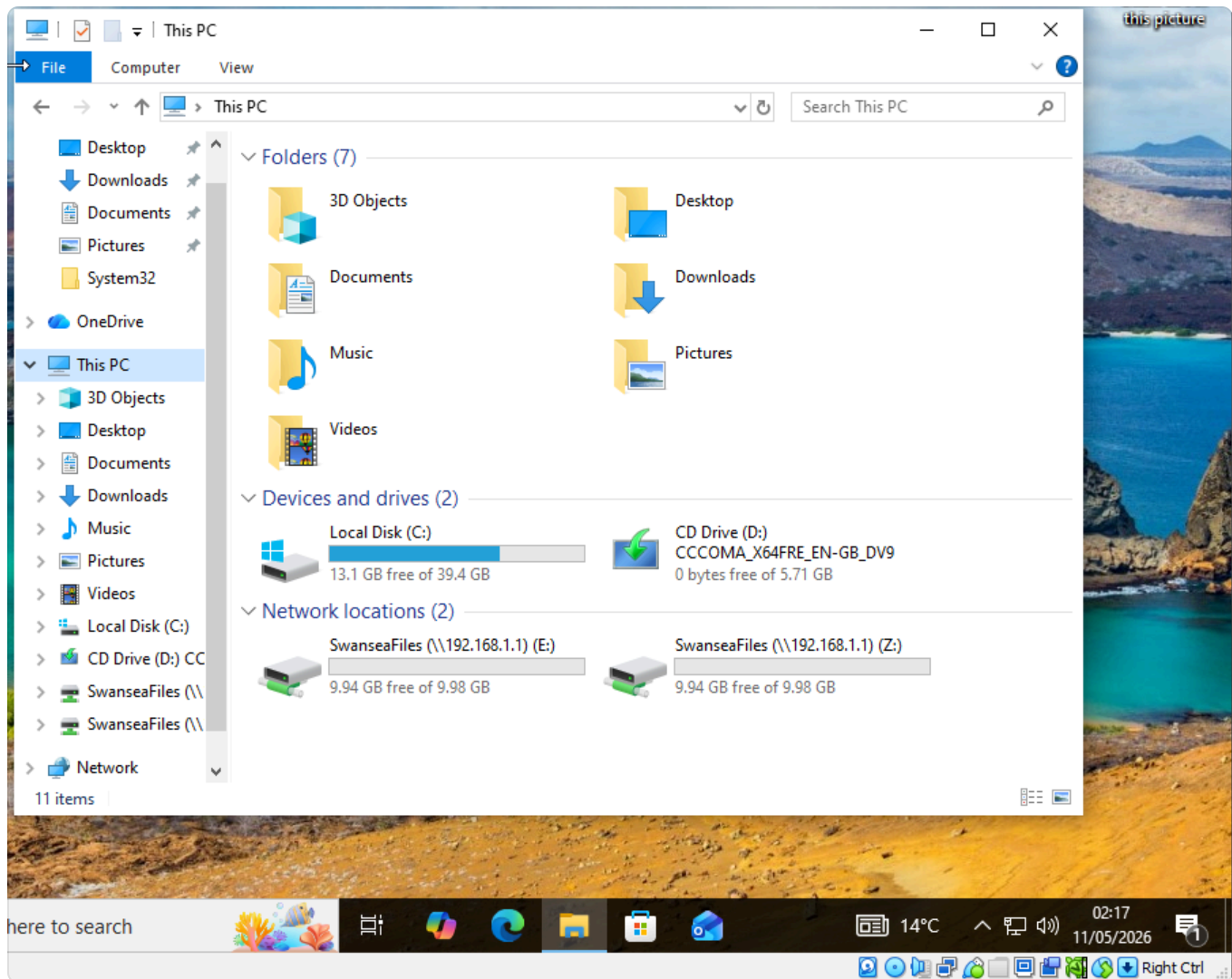
Caption: This screenshot shows NTFS security permissions configured on the shared folder.

Figure 35 – Shared Drive Access from Client



Caption: This screenshot shows the shared drive successfully accessed from ClientS1.

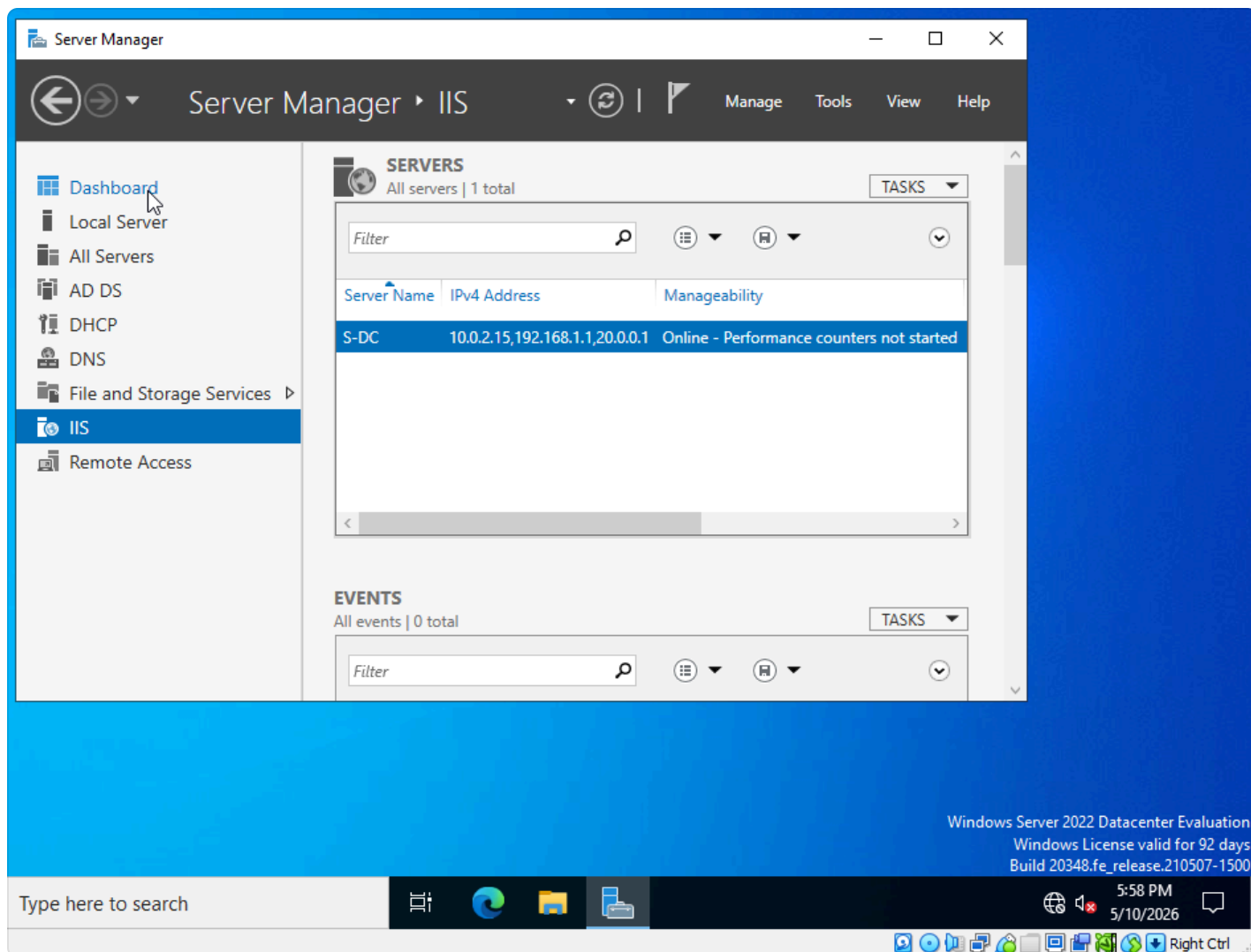
Figure 36 – Mapped Network Drive



Caption: This screenshot shows the shared drive mapped within This PC on ClientS1.

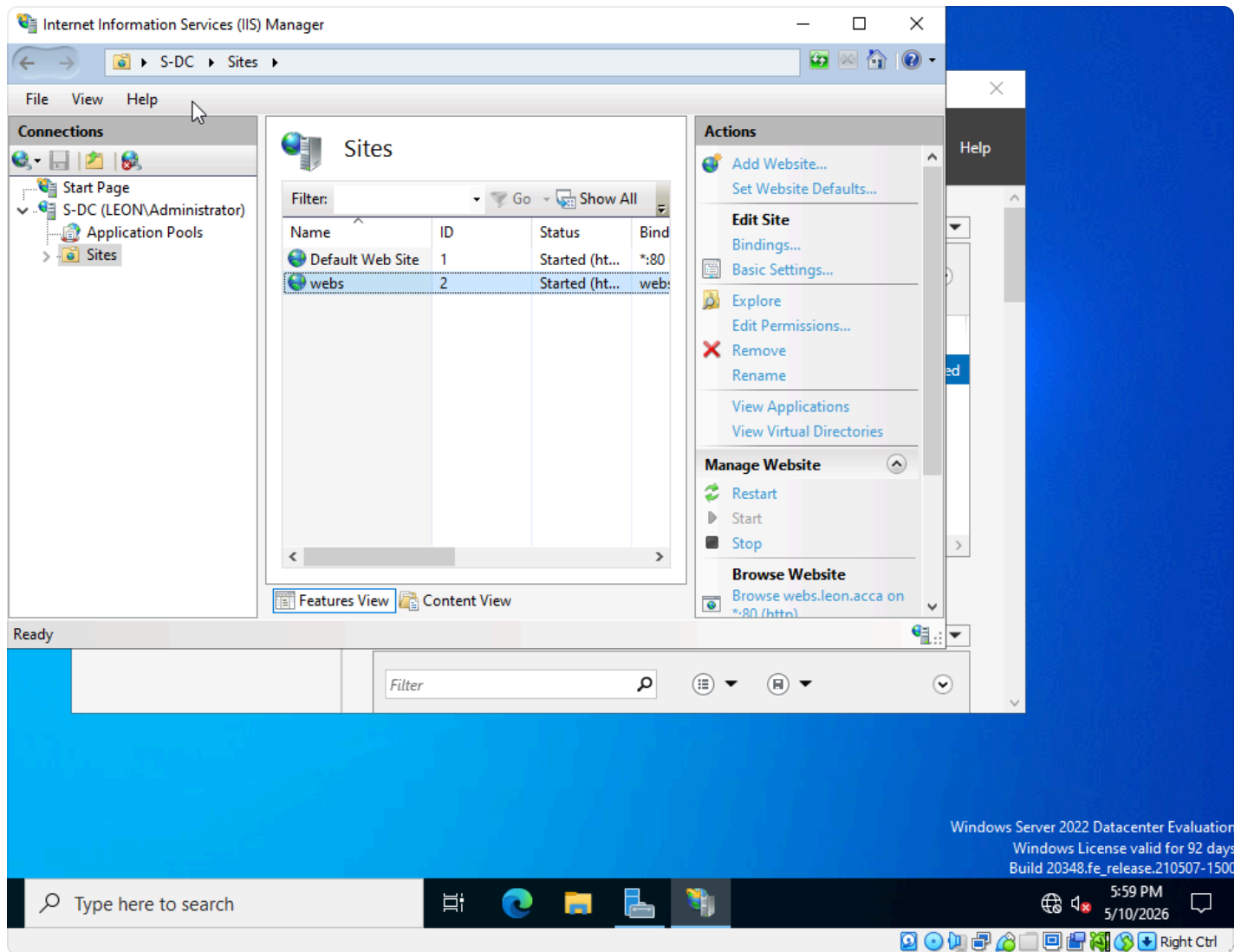
7. IIS Web Server Configuration

Figure 37 – IIS Role Installation



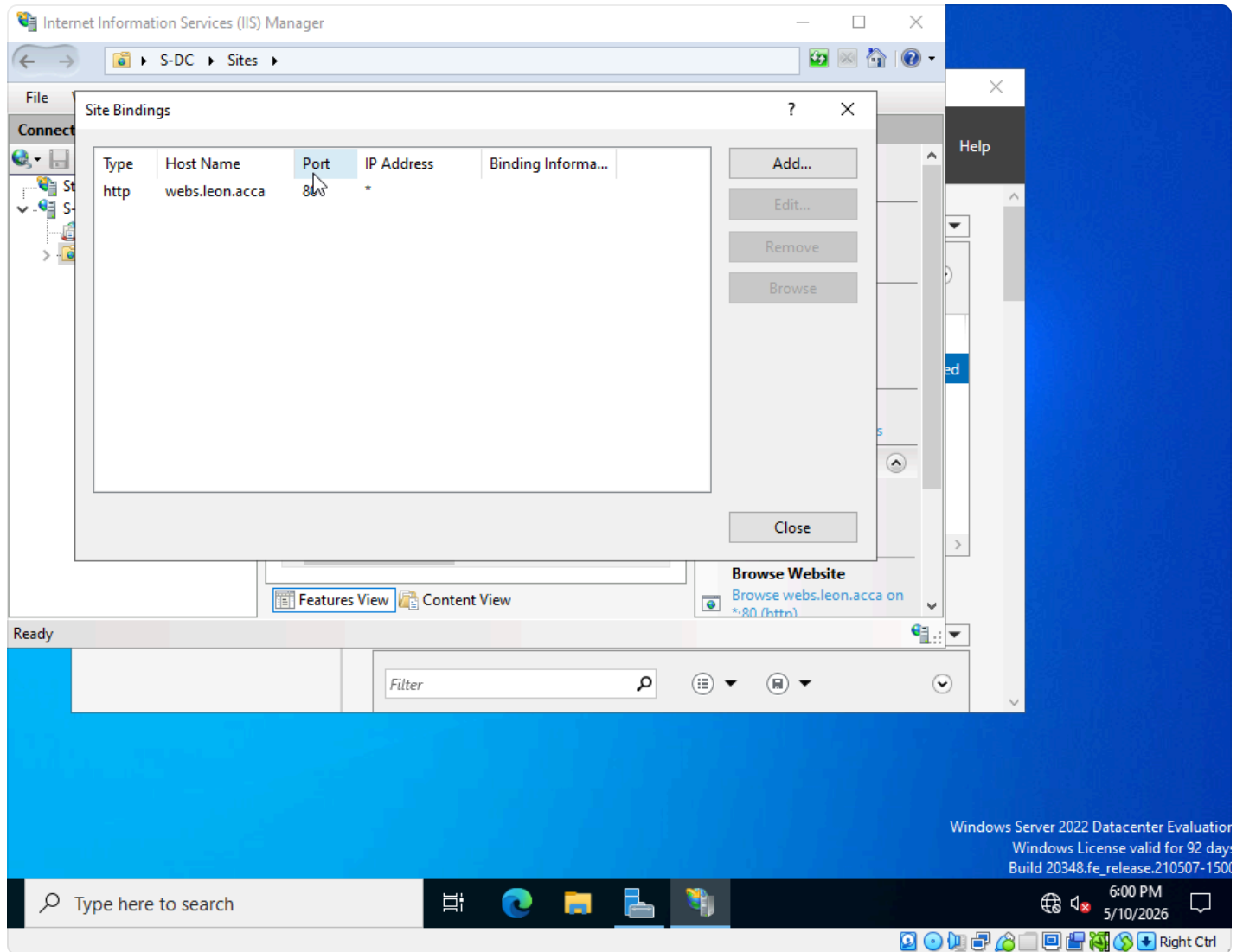
Caption: This screenshot shows Internet Information Services installed on S-DC.

Figure 38 – Website Configuration



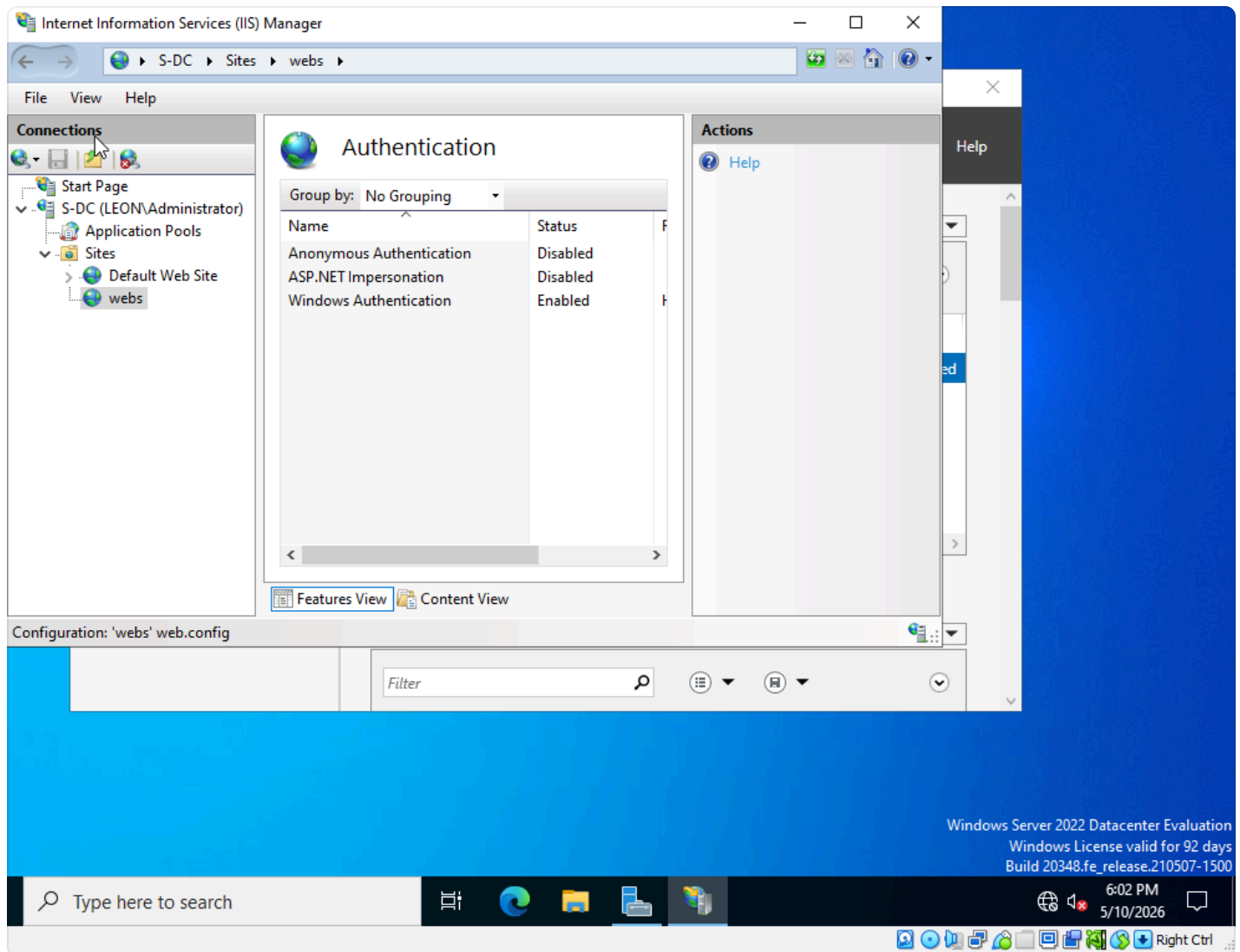
Caption: This screenshot shows the configured webs website within IIS Manager.

Figure 39 – IIS Bindings Configuration



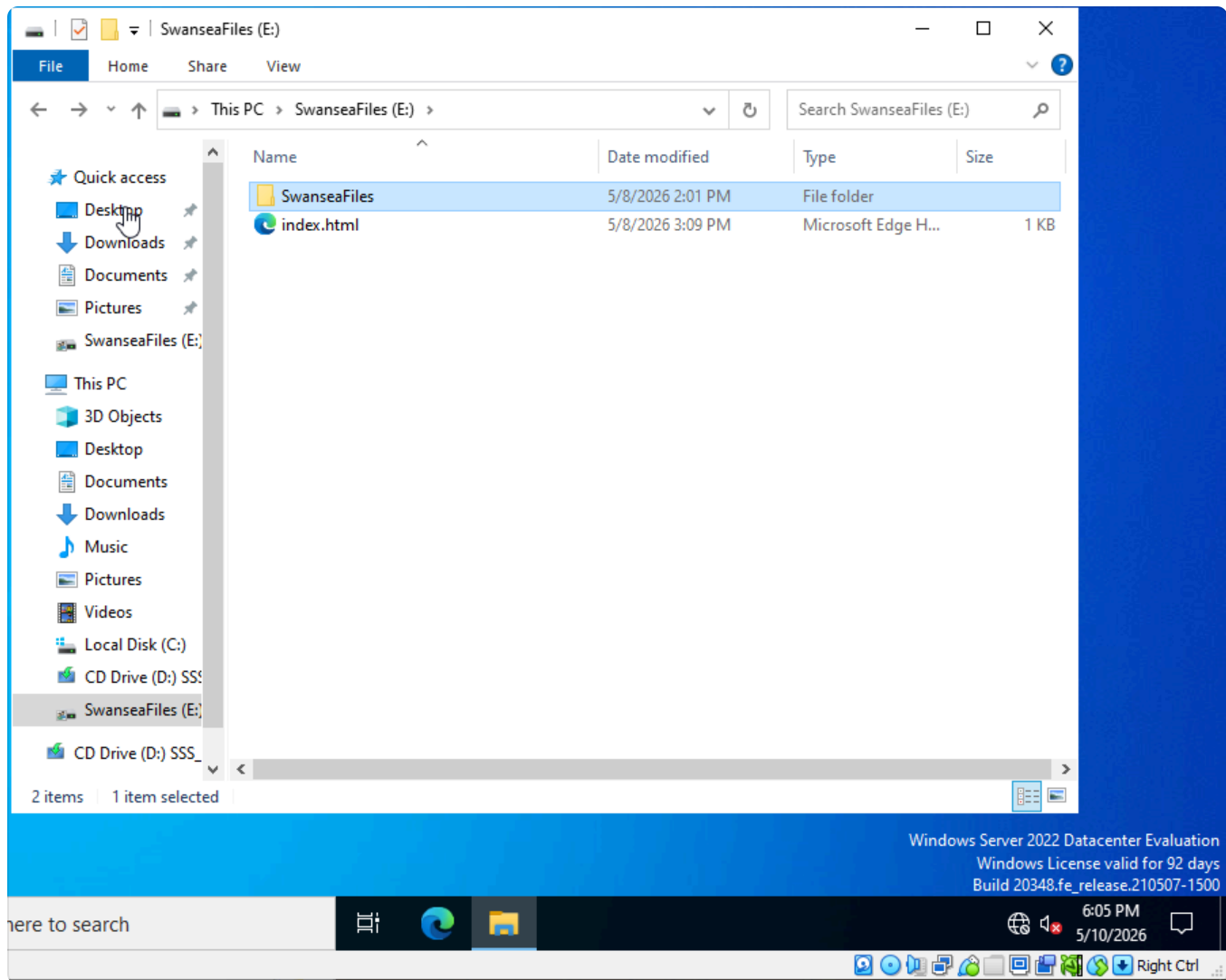
Caption: This screenshot shows the configured IIS website bindings.

Figure 40/41 – Windows Authentication Enabled - Anonymous Authentication Disabled



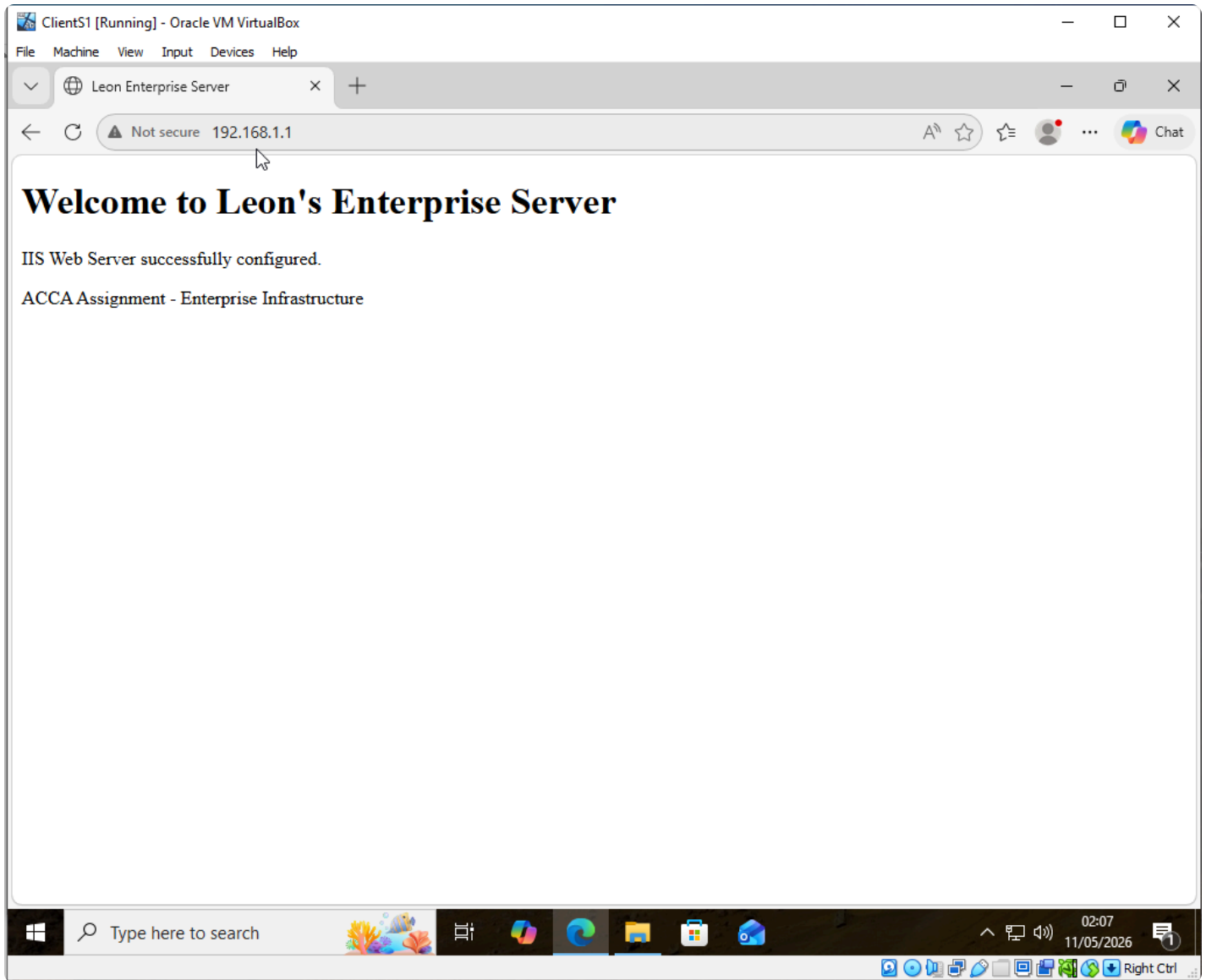
Caption: This screenshot shows Windows Authentication enabled for the IIS website. This screenshot also shows Anonymous Authentication disabled for the IIS website.

Figure 42 – Website Files Stored in Shared Directory



Caption: This screenshot shows website files stored within the SwanseaFiles shared directory.

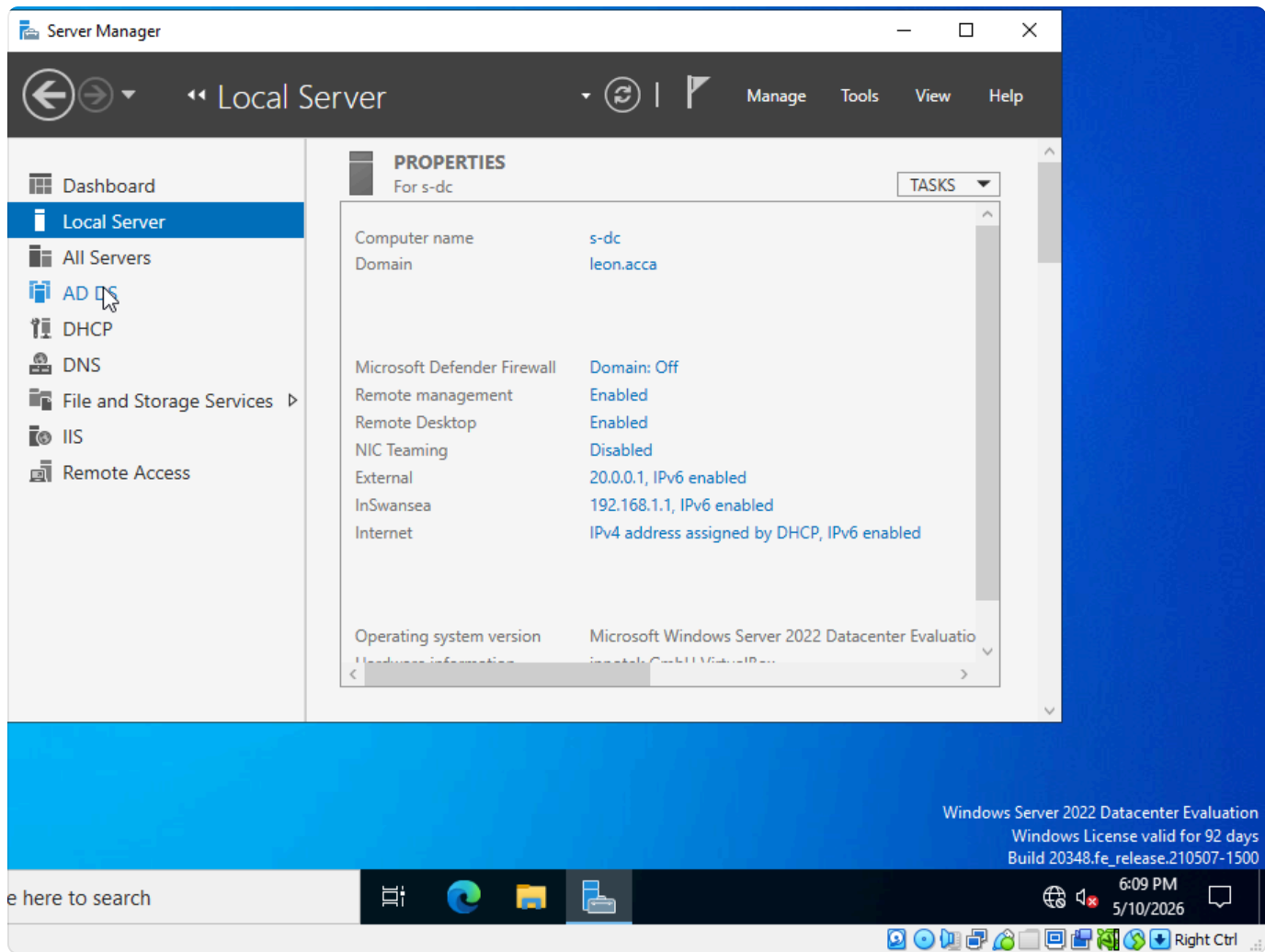
Figure 43 – Website Successfully Accessed



Caption: This screenshot shows the enterprise website successfully accessed from ClientS1.

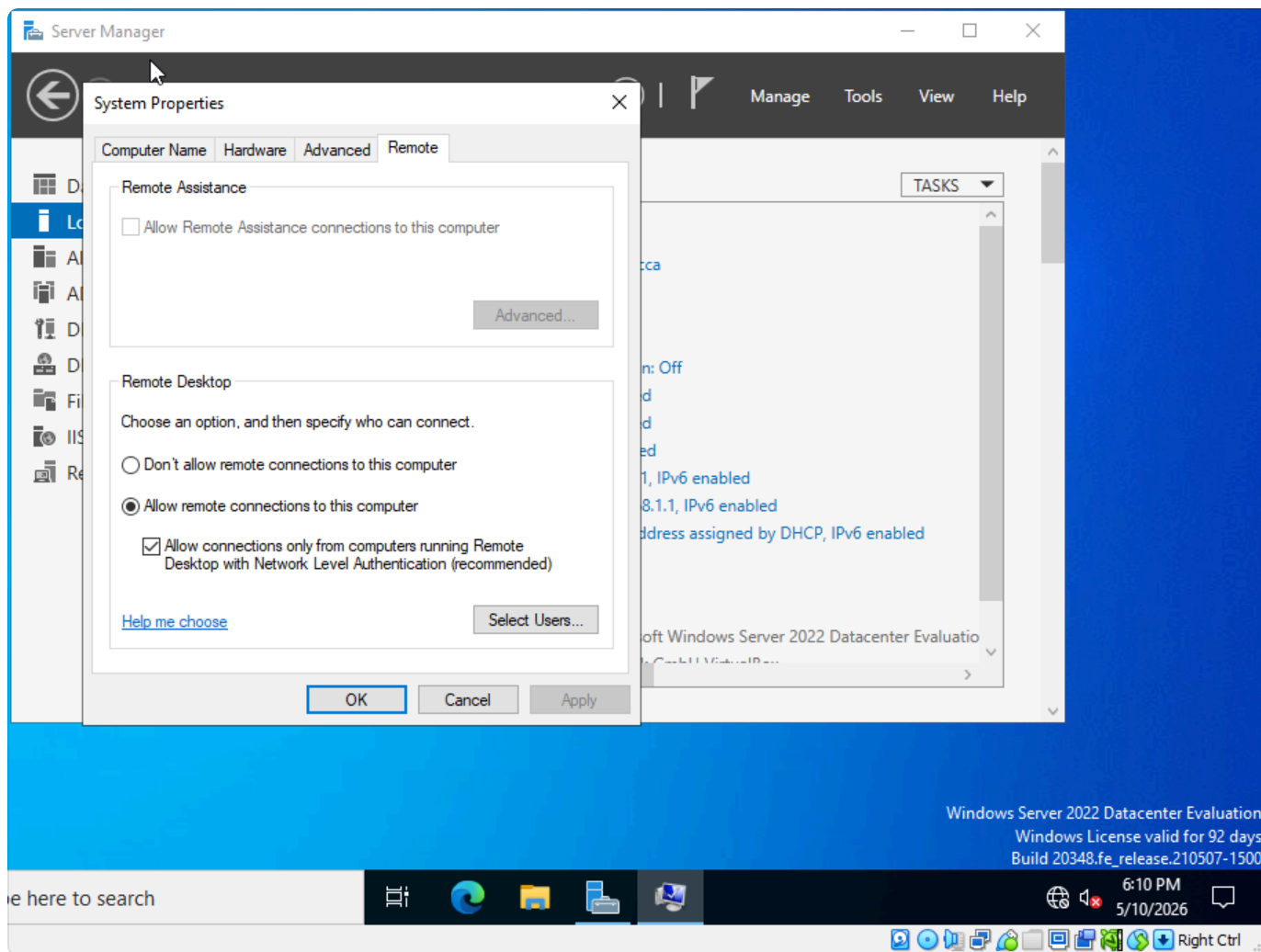
8. Remote Desktop Services

Figure 44 – Remote Desktop Enabled



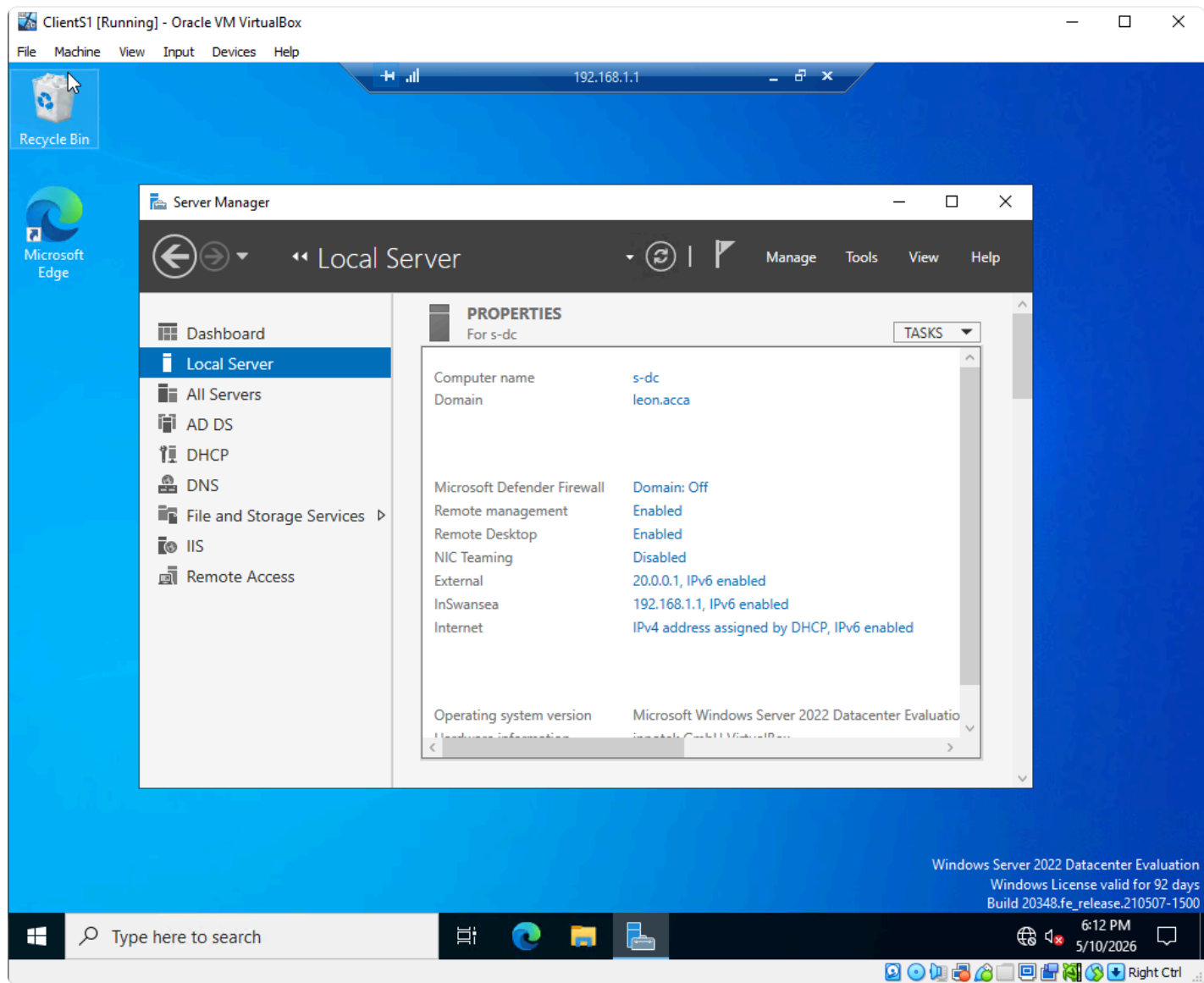
Caption: This screenshot shows Remote Desktop enabled on the server.

Figure 45 – Remote Desktop System Settings



Caption: This screenshot shows Remote Desktop enabled within system settings.

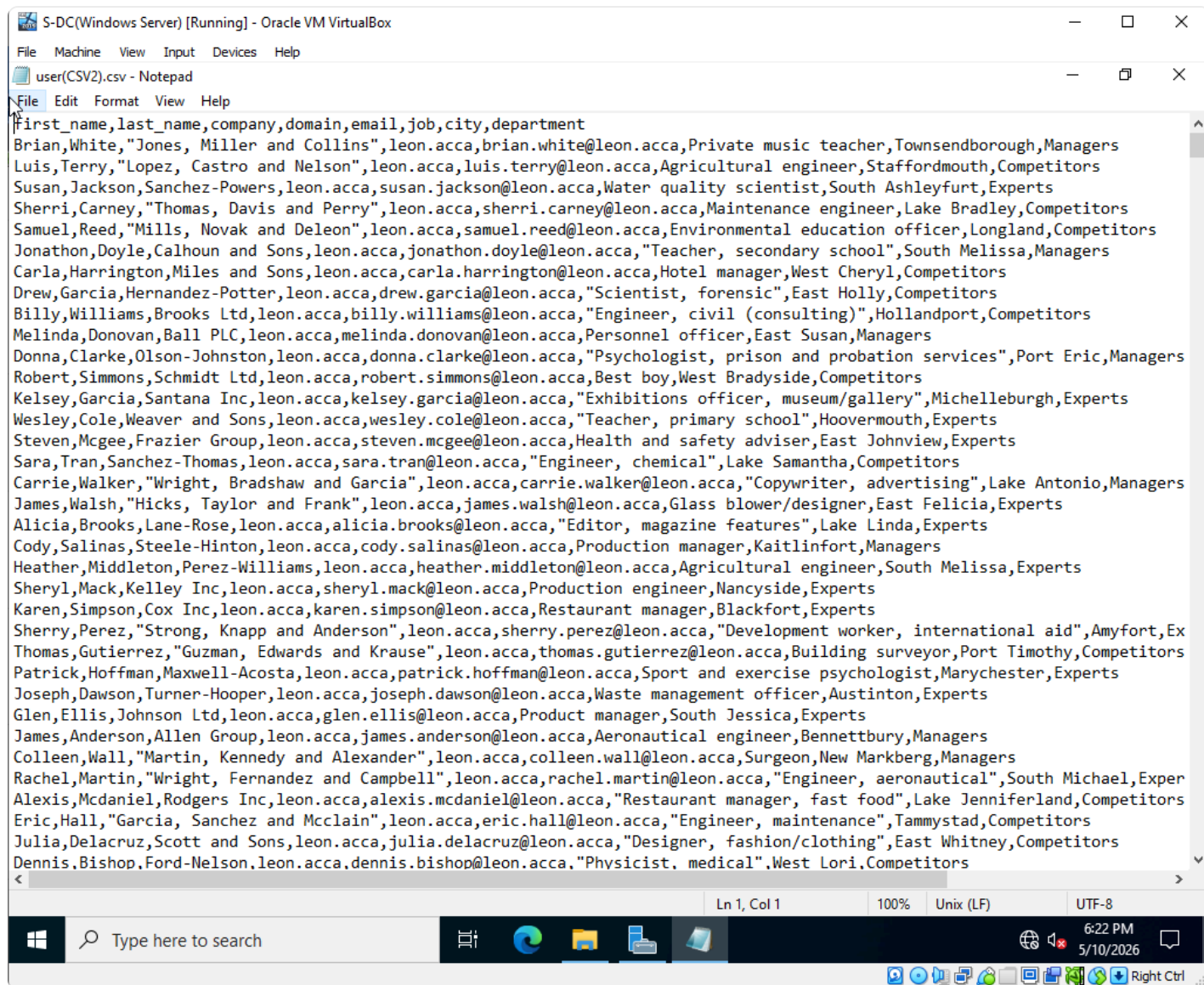
Figure 46 – Successful Remote Desktop Connection



Caption: This screenshot shows a successful Remote Desktop connection to the server.

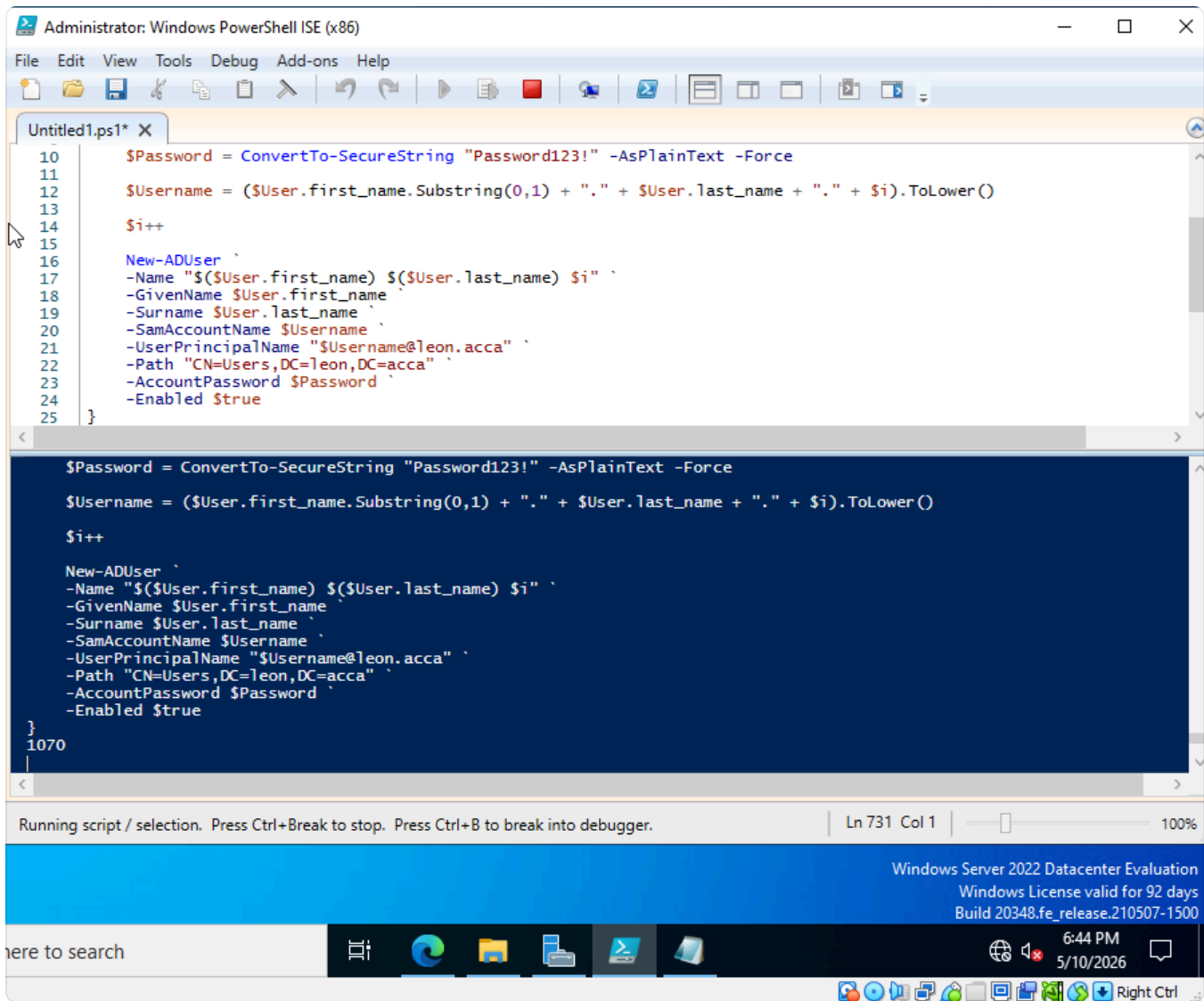
9. User Account Configuration

Figure 47 – User CSV File



Caption: This screenshot shows the provided CSV file containing user account information.

Figure 48 – PowerShell User Import Script



The screenshot displays the Windows PowerShell ISE (x86) interface. The main window shows a PowerShell script in a file named 'Untitled1.ps1'. The script is designed to bulk import user accounts into an Active Directory. It starts by converting a plain text password to a secure string. Then, it iterates through a collection of users (implied by the loop variable \$i). For each user, it constructs a username by combining the first name, last name, and a domain suffix. The script then uses the 'New-ADUser' cmdlet to create each user with specific attributes: Name, GivenName, Surname, SamAccountName, UserPrincipalName, Path, AccountPassword, and Enabled status. The console window at the bottom shows the execution of the script, with the same commands being run. The status bar indicates the script is running, and the taskbar at the bottom shows the system clock and various icons.

```
10 $Password = ConvertTo-SecureString "Password123!" -AsPlainText -Force
11
12 $Username = ($User.first_name.Substring(0,1) + "." + $User.last_name + "." + $i).ToLower()
13
14 $i++
15
16 New-ADUser `
17 -Name "$($User.first_name) $($User.last_name) $i" `
18 -GivenName $User.first_name `
19 -Surname $User.last_name `
20 -SamAccountName $Username `
21 -UserPrincipalName "$Username@leon.acca" `
22 -Path "CN=Users,DC=leon,DC=acca" `
23 -AccountPassword $Password `
24 -Enabled $true
25 }
```

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger. Ln 731 Col 1 100%

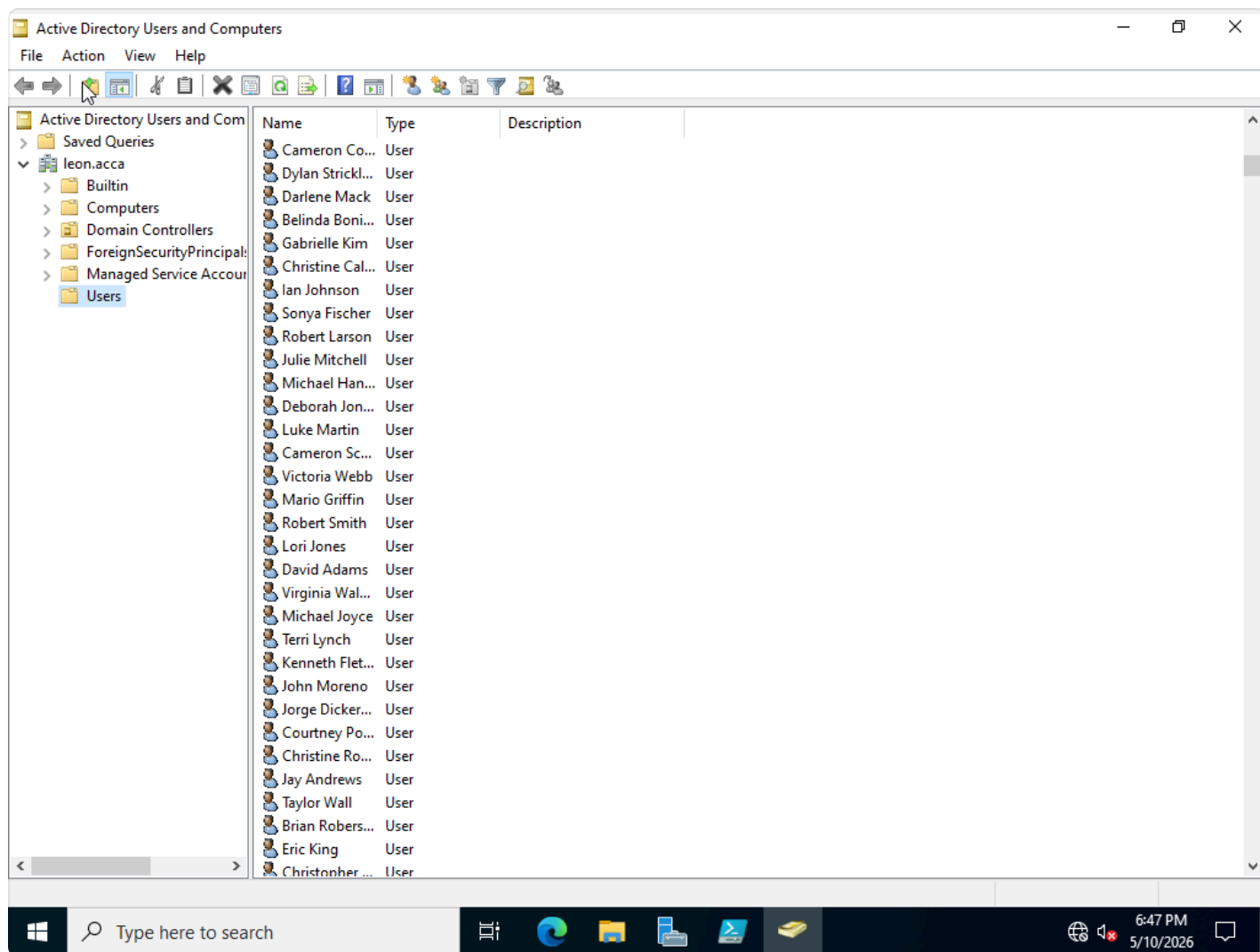
Windows Server 2022 Datacenter Evaluation
Windows License valid for 92 days
Build 20348.fe_release.210507-1500

6:44 PM
5/10/2026

Right Ctrl

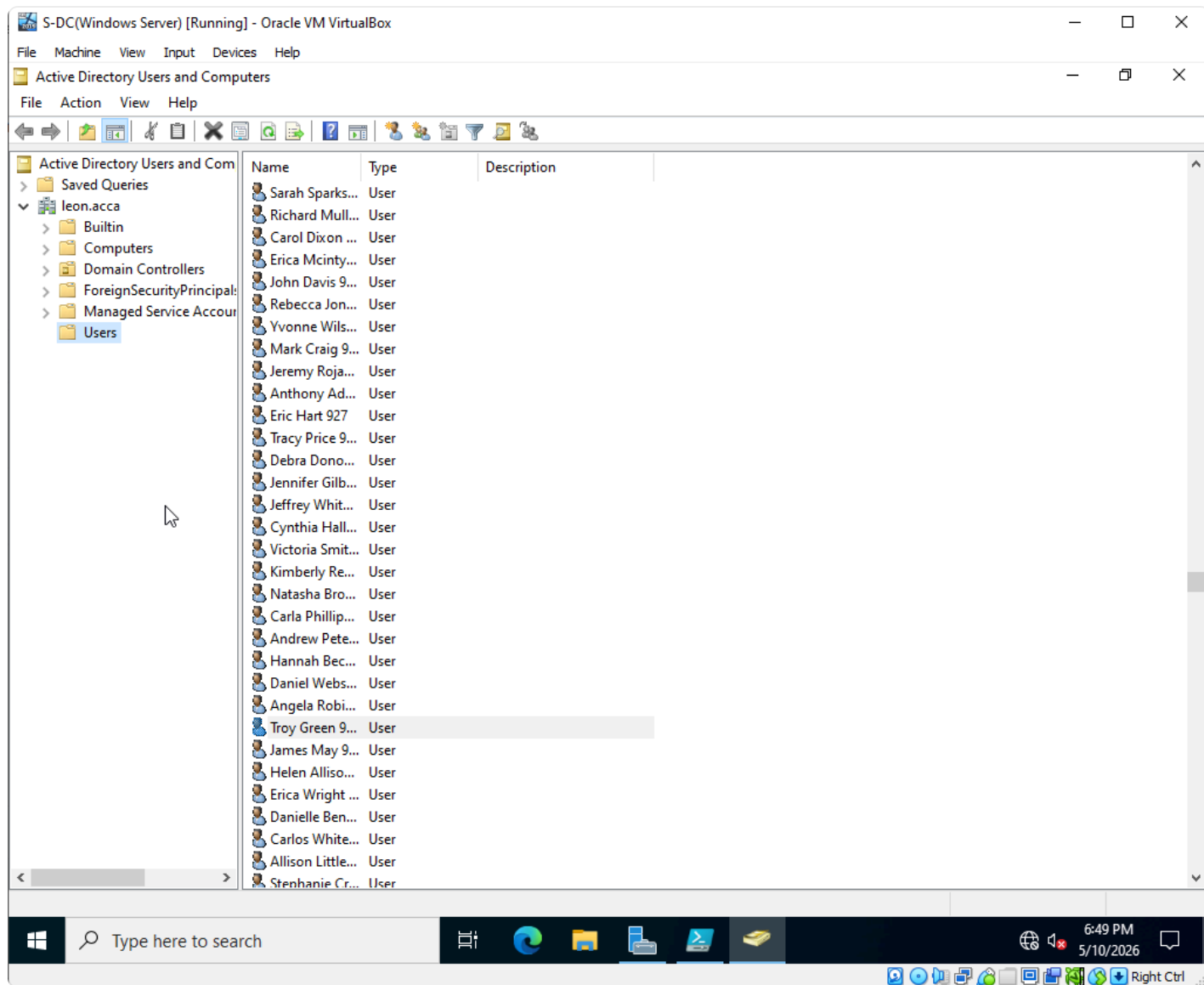
Caption: This screenshot shows the PowerShell script used to bulk import user accounts.

Figure 49 – Active Directory User Accounts



Caption: This screenshot shows successfully created Active Directory user accounts.

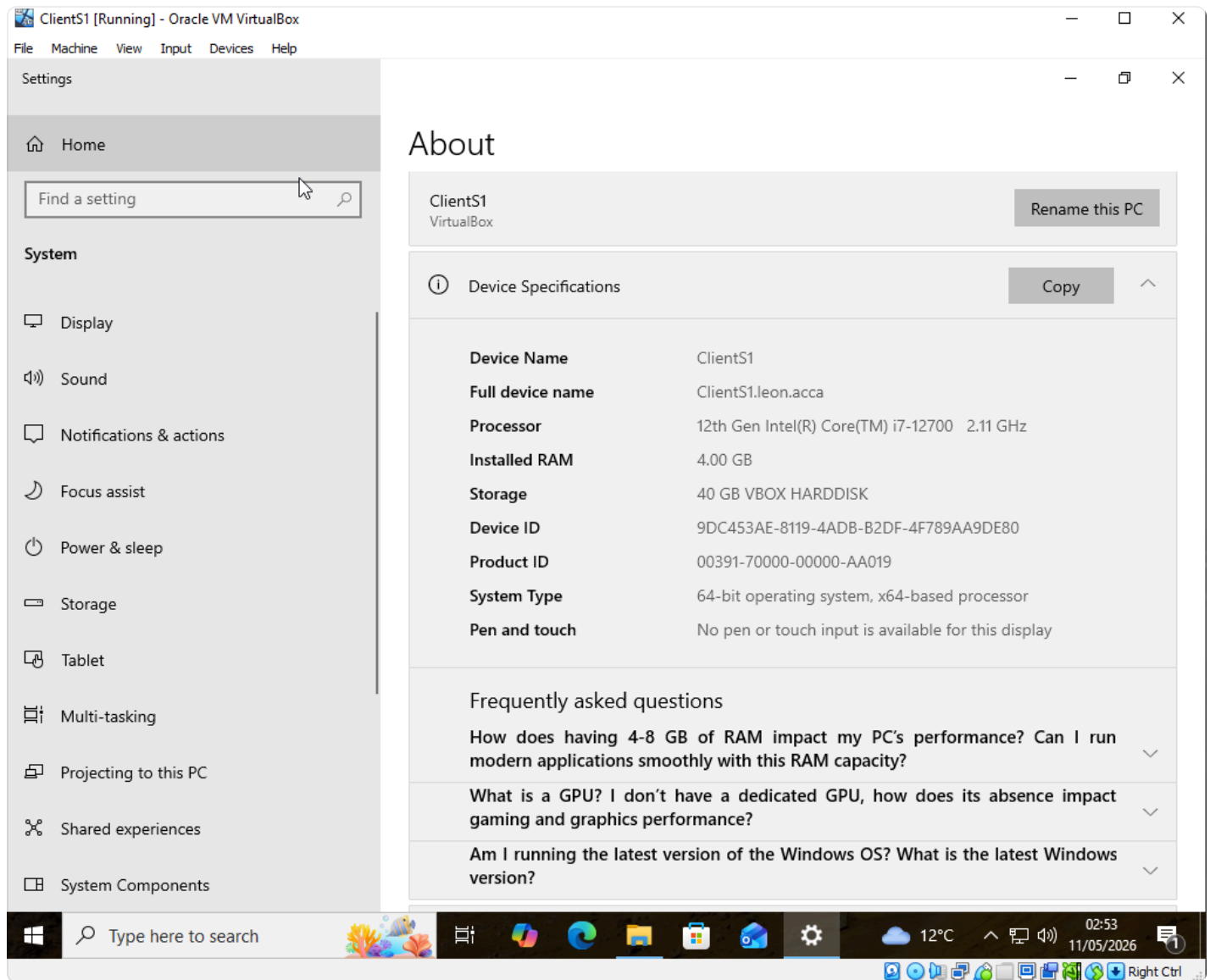
Figure 50 – Imported User Naming Convention



Caption: This screenshot shows imported users following the required naming convention.

10. Domain Membership

Figure 51/52 – ClientS1 Joined to Domain - System Properties Domain Membership



Caption: This screenshot shows ClientS1 successfully joined to the leon.acca domain .This screenshot also shows the system properties confirming domain membership

Figure 53 – Linux Hostname Configuration

```
leon@L-DC:~$ hostnmectl
Failed to query product UUID, ignoring: Access denied
Failed to query hardware serial, ignoring: Access denied
Static hostname: L-DC
    Icon name: computer-vm
    Chassis: vm
    Machine ID: 6dc5aed8e25642a080e51d7c866dffc7
    Boot ID: ed4008d02d894d4f8d833613afe58817
    AF_VSOCK CID: 1
Virtualization: oracle
Operating System: Debian GNU/Linux 13 (trixie)
    Kernel: Linux 6.12.73+deb13-amd64
    Architecture: x86_64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Firmware Version: VirtualBox
    Firmware Date: Fri 2006-12-01
    Firmware Age: 19y 5month 1w 1d
leon@L-DC:~$
```

Caption: This screenshot shows the configured hostname on the Linux Debian server.

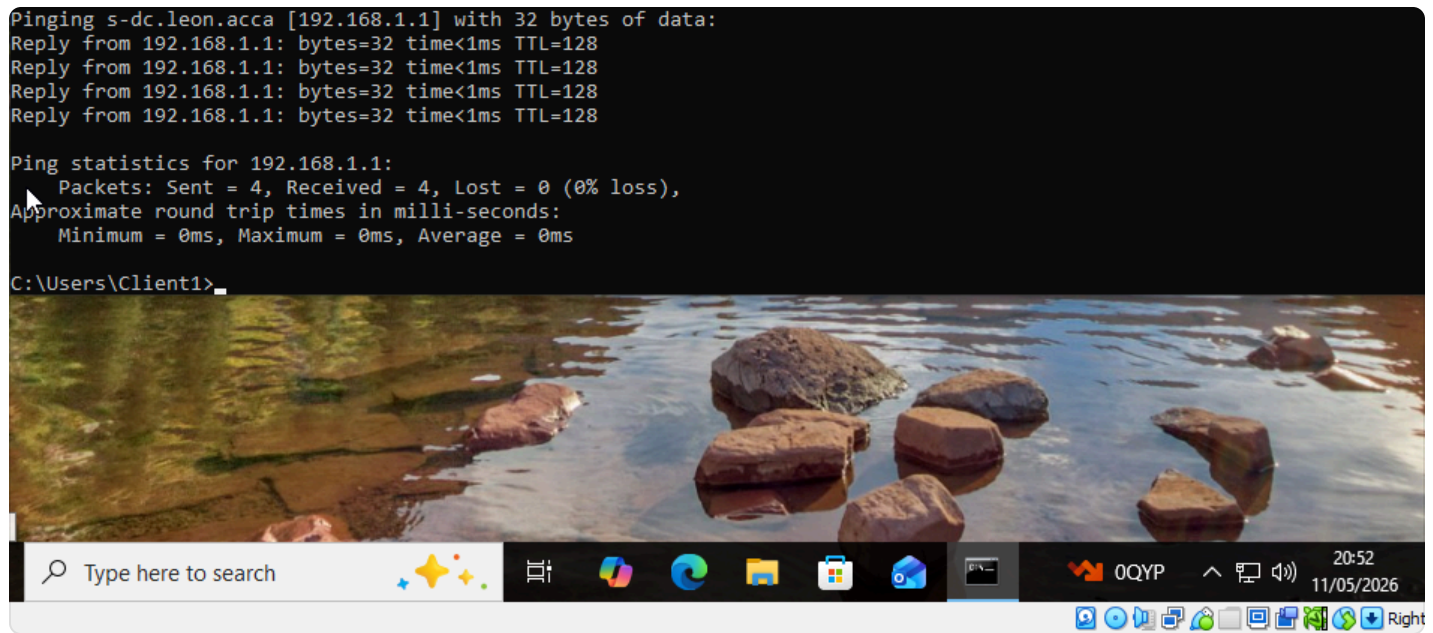
Figure 54 – Full Domain Name Verification

```
leon@L-DC:~$ hostname -f
L-DC.leon.acca
leon@L-DC:~$
```

Caption: This screenshot shows successful verification of the Linux fully qualified domain name.

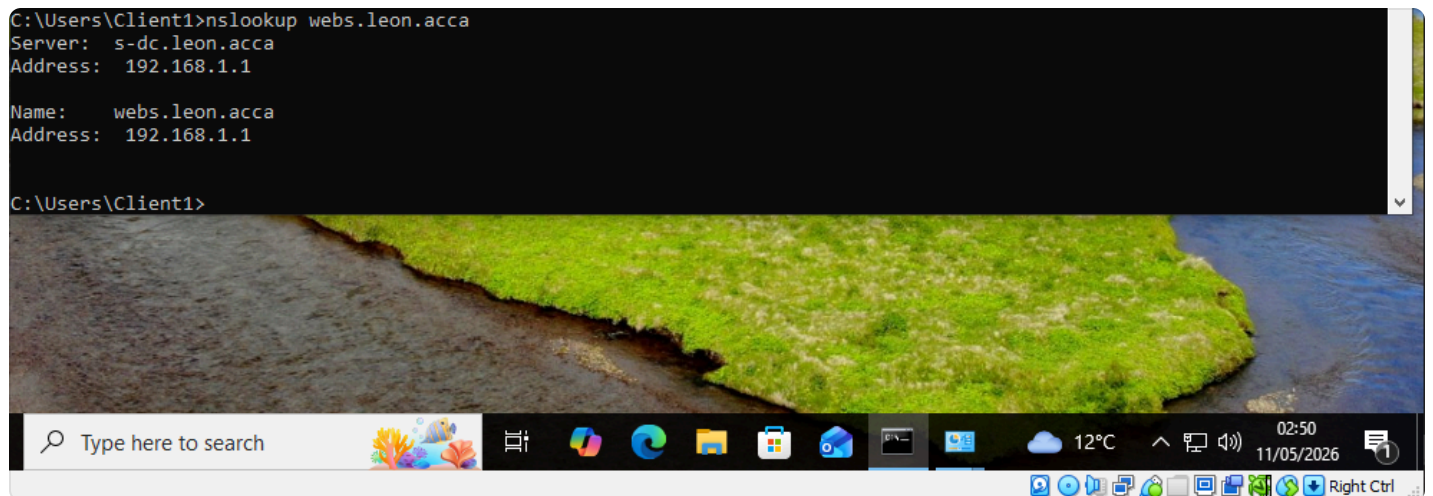
11. Testing and Troubleshooting

Figure 55 – Successful DNS Resolution



Caption: This screenshot shows successful DNS resolution between devices.

Figure 56 – Successful Website DNS Resolution



Caption: This screenshot shows successful resolution of webs.leon.acca.

Figure 57 – ping Test from ClientS1 to S-DC

```
Command Prompt
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Client1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Client1>tracert 192.168.2.1

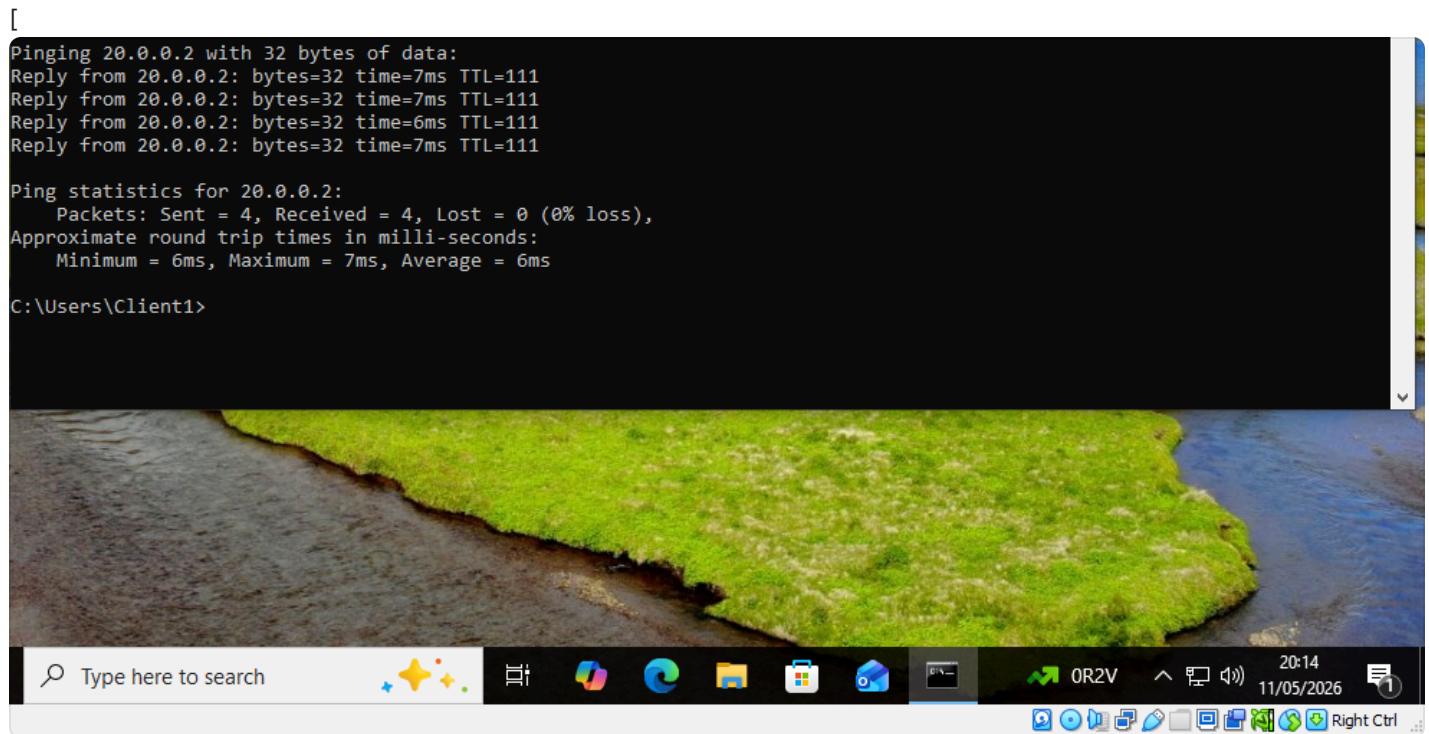
Tracing route to L-DC.leon.acca [192.168.2.1]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    10.0.2.2
  1  <1 ms    <1 ms    <1 ms    172.29.1.254
  2  <1 ms    <1 ms    <1 ms    172.30.2.254
  3  *         *         *         Request timed out.
  4  ^C

C:\Users\Client1>
C:\Users\Client1>
```

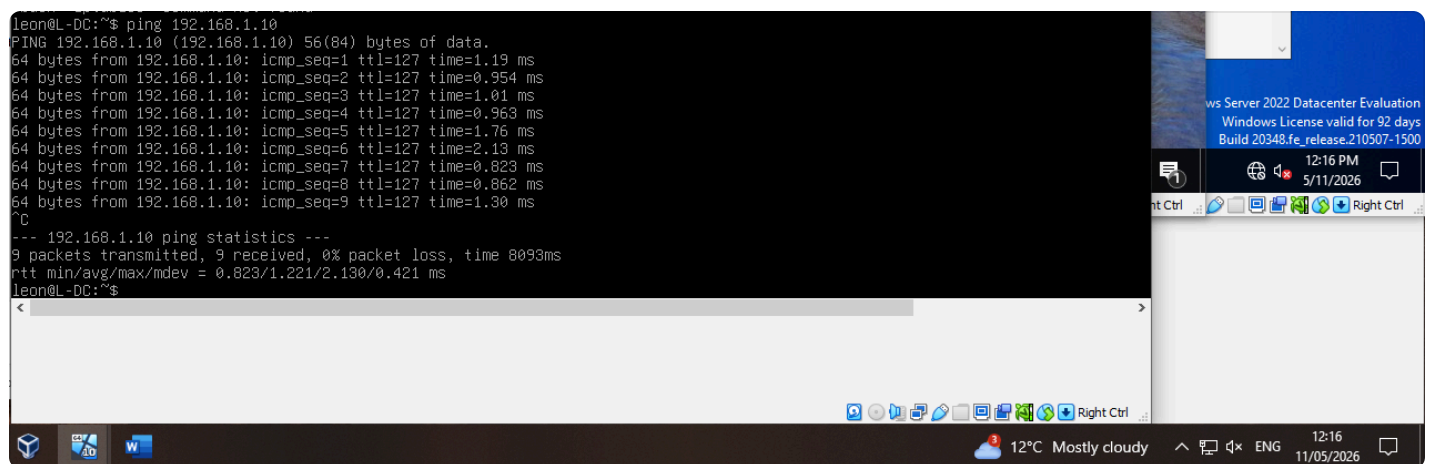
Caption: This screenshot shows successful communication from ClientS1 to S-DC.

Figure 58 – ping Test from ClientS1 to L-DC



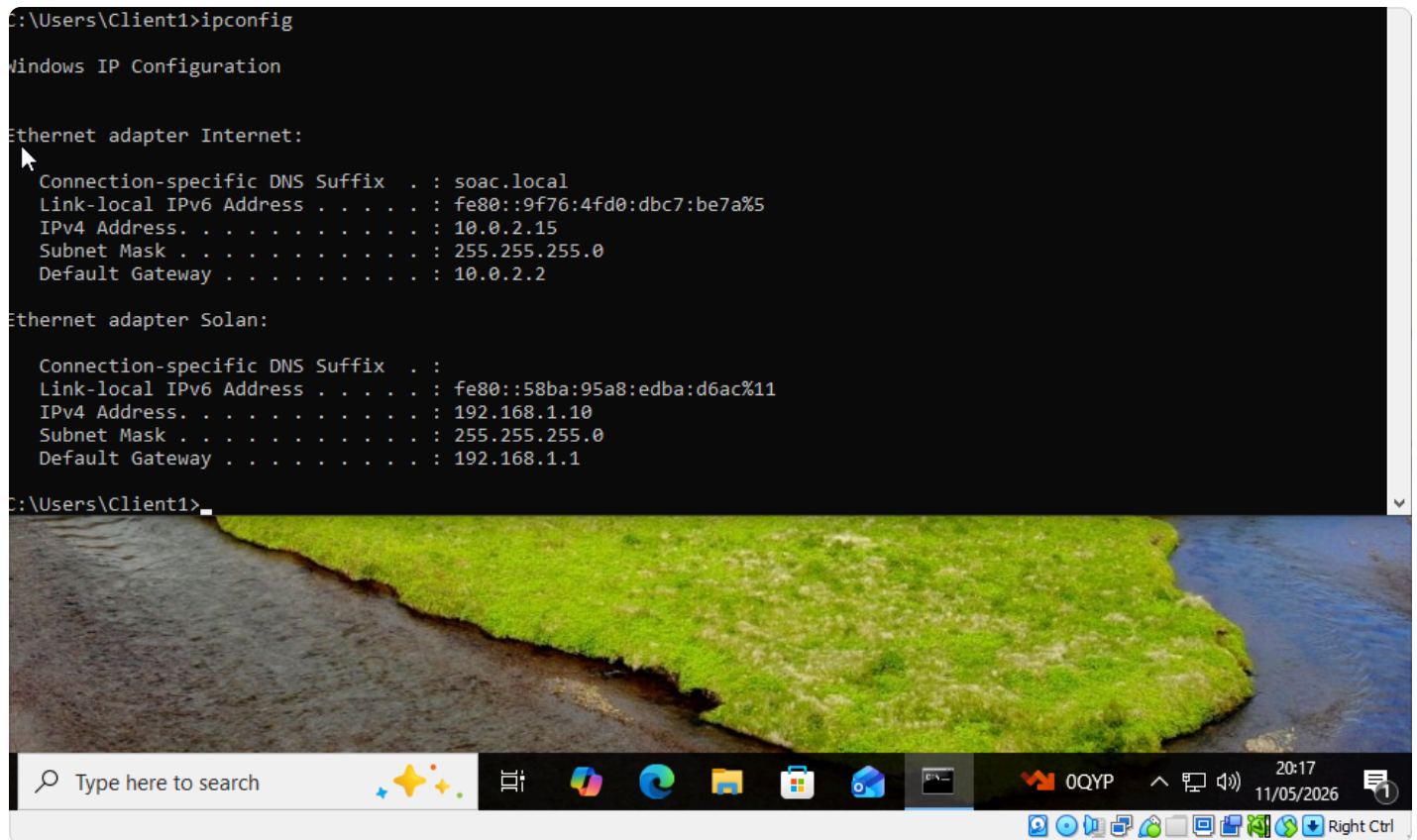
Caption: This screenshot shows successful communication from ClientS1 to L-DC.

Figure 59 – ping Test from L-DC to ClientS1



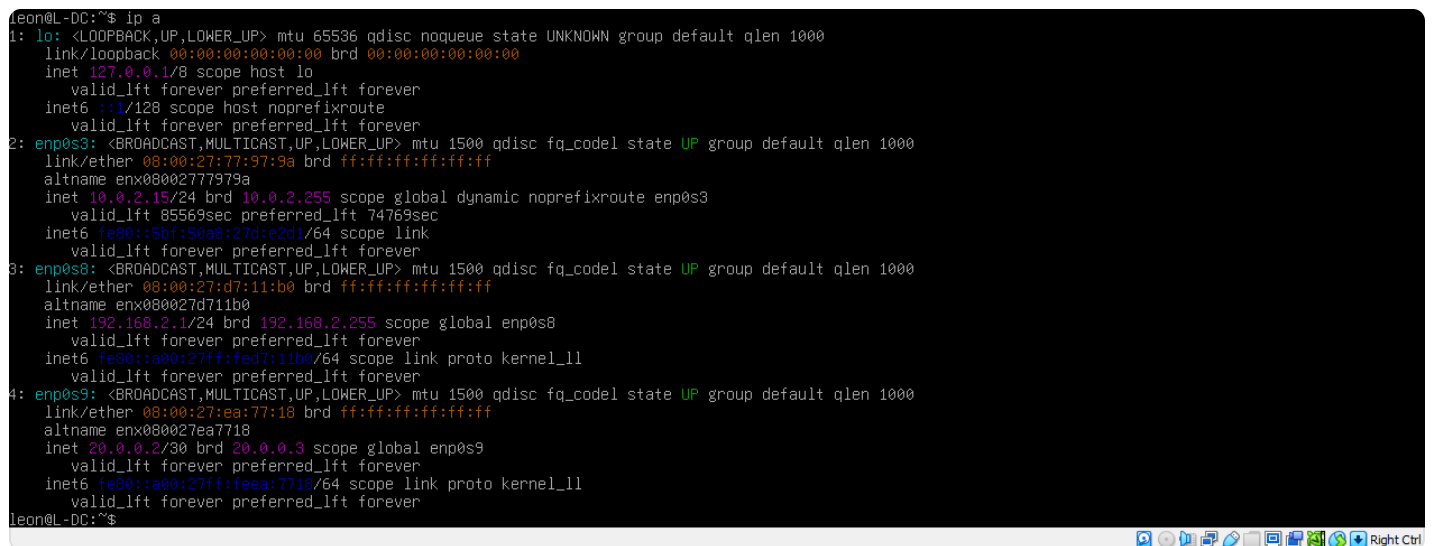
Caption: This screenshot shows successful communication from L-DC to ClientS1.

Figure 60 – ipconfig Verification



Caption: This screenshot shows IP configuration details on ClientS1.

Figure 61 – Linux ip route Verification



Caption: This screenshot shows the Linux routing table configuration.

Figure 62 – Troubleshooting Evidence

```
Command Prompt
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Client1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Client1>tracert 192.168.2.1

Tracing route to L-DC.leon.acca [192.168.2.1]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    10.0.2.2
  1  <1 ms    <1 ms    <1 ms    172.29.1.254
  2  <1 ms    <1 ms    <1 ms    172.30.2.254
  3  *         *         *         Request timed out.
  4  ^C

C:\Users\Client1>
C:\Users\Client1>
```

Caption: This screenshot shows troubleshooting steps performed during infrastructure configuration.

Conclusion

To sum up, this assignment effectively illustrated how to set up and test a multi-site network system. Throughout the assignment, real-world testing and troubleshooting techniques were used to configure and validate networking services, routing, domain management, and client communication.