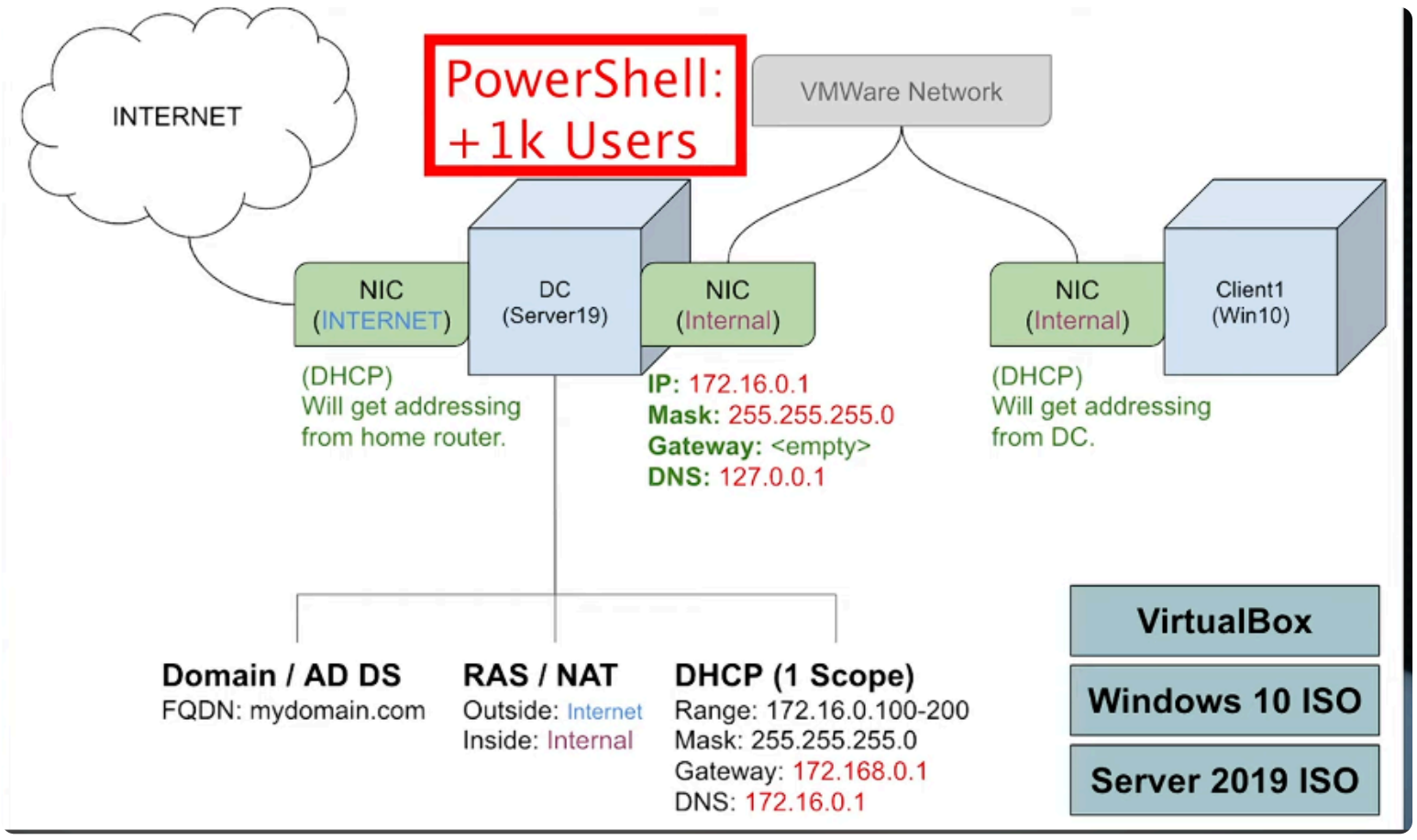
HOME LAB

Step 1: Active Directory Setup

Reference: How to Setup a Basic Home Lab Running Active Directory (Oracle VirtualBox) | Add Users w/PowerShell - YouTube



1. Windows Server Installation

Objective: Deploy a Windows Server 2019 instance to serve as the **Domain Controller (DC)** for the TradeGuard lab.

VM Configuration

Setting	Value
VM Name	`TradeGuard-DC`
Base ISO	Windows Server 2019 Evaluation
Virtual Disk	60 GB
Memory (RAM)	4 GB
CPU Cores	1
Password	`#Ckhandor123`
Network	Dual Adapters: NAT (Internet) + Host-Only (Internal Lab)

2. Network Configuration

We configure two network adapters to ensure:

- The server can access the internet (for updates and package installs)
- The internal lab VMs (Kali, Ubuntu SIEM, Windows clients) can communicate securely with the DC.

Adapter	Type	Purpose	Example IP	Notes
Adapter 1	NAT (`VMnet8`)	Provides internet access through host	Dynamic	Used for Windows updates and downloads
Adapter 2	Host-Only (`VMnet1`)	Internal lab network	`172.16.0.1`	Used for AD, DNS, and internal VM communication

Network Verification

After installation:

1. Open **Command Prompt** → Run:

```powershell
ipconfig /all
```

   Ensure both adapters appear (NAT + Host-Only).
2. Set a **static IP** for the internal adapter (`Ethernet1`):
   - IP: `172.16.0.1`
   - Subnet mask: `255.255.255.0`
   - Default gateway: *(leave blank or use `127.0.0.1`)*
   - DNS server: `127.0.0.1` *(will later point to local DNS once AD DS is installed)*
3. Verify connectivity:

```powershell
ping 8.8.8.8          # Internet connectivity via NAT
ping 172.16.0.1   # Loopback / local connectivity
```

3. System Configuration Summary

Parameter	Value
Hostname	`TRADEGUARD-DC`
IP Address	172.16.0.1
Domain	`tradeguard.com`
Default Gateway	*(None – DC will serve as DNS)*
DNS Server	`127.0.0.1`
Admin Account	`Administrator`
Password	`#Ckhandor123`

4. (Optional) Disable Firewall Temporarily

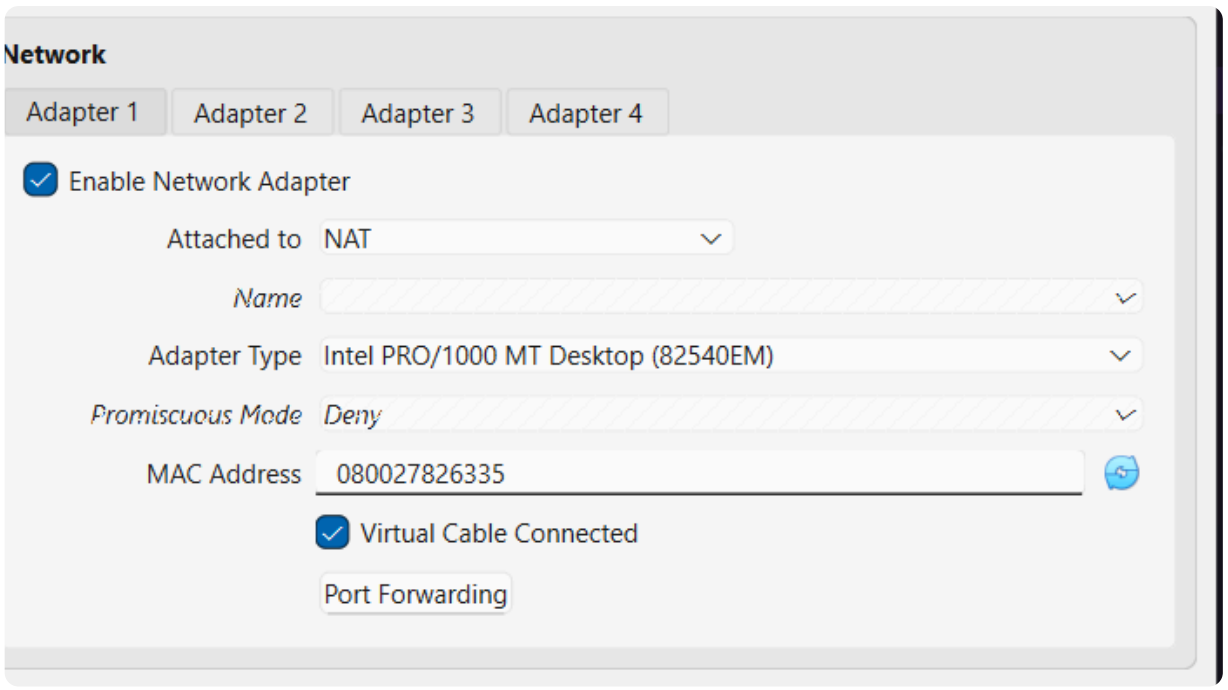
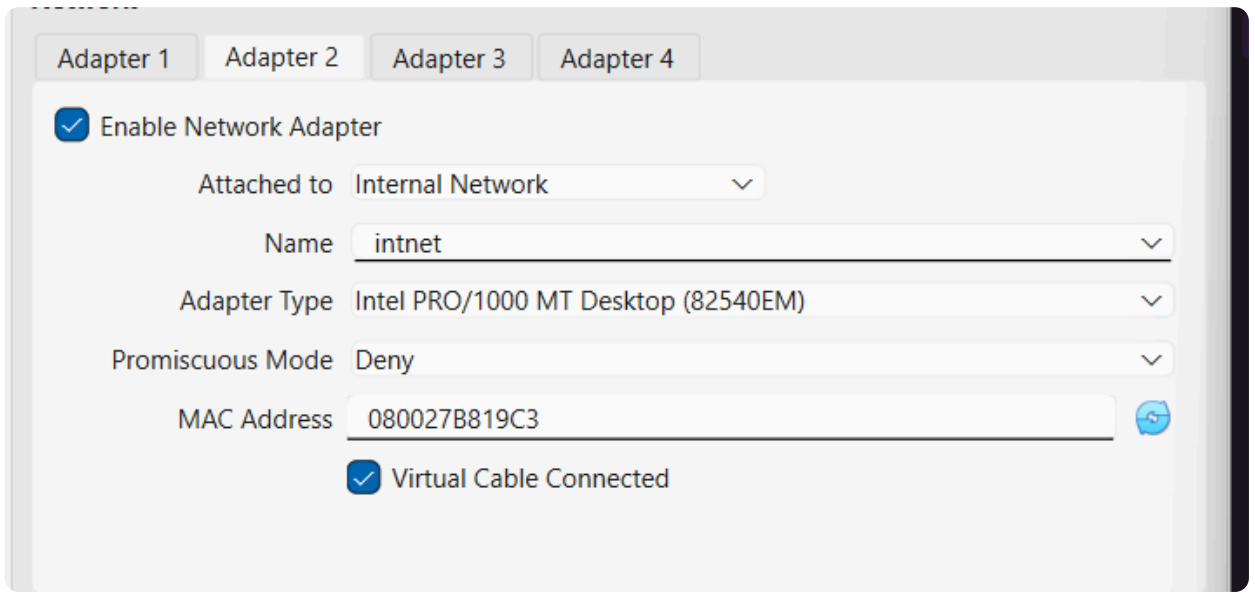
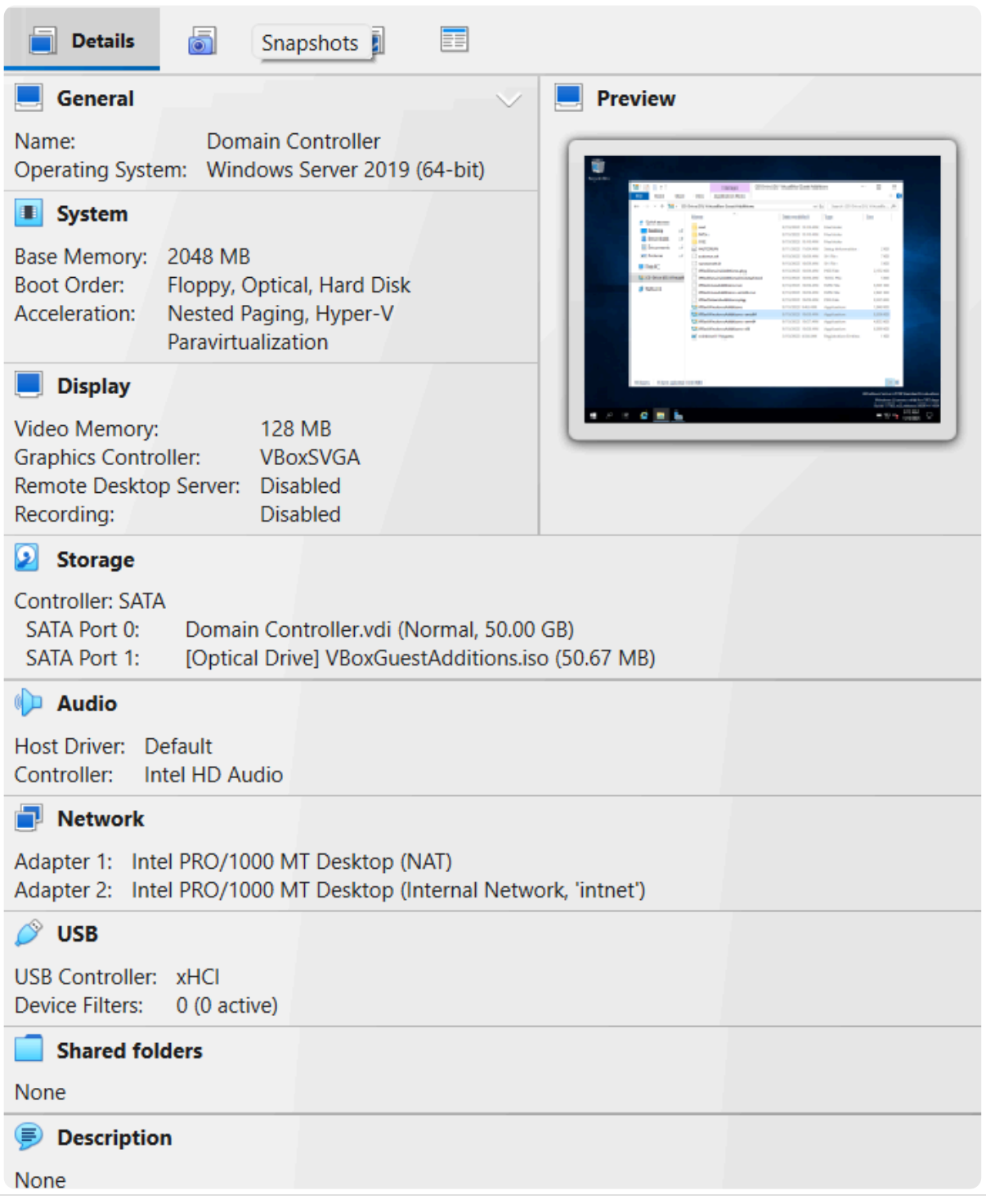
To simplify testing and avoid connectivity issues during setup:

1. Open **Windows Defender Firewall → Turn Windows Defender Firewall on or off**
2. Turn **off** for:
   - Domain Network
   - Private Network
   - Public Network

5. Pre-Setup Validation

Before installing **Active Directory Domain Services (AD DS)**:

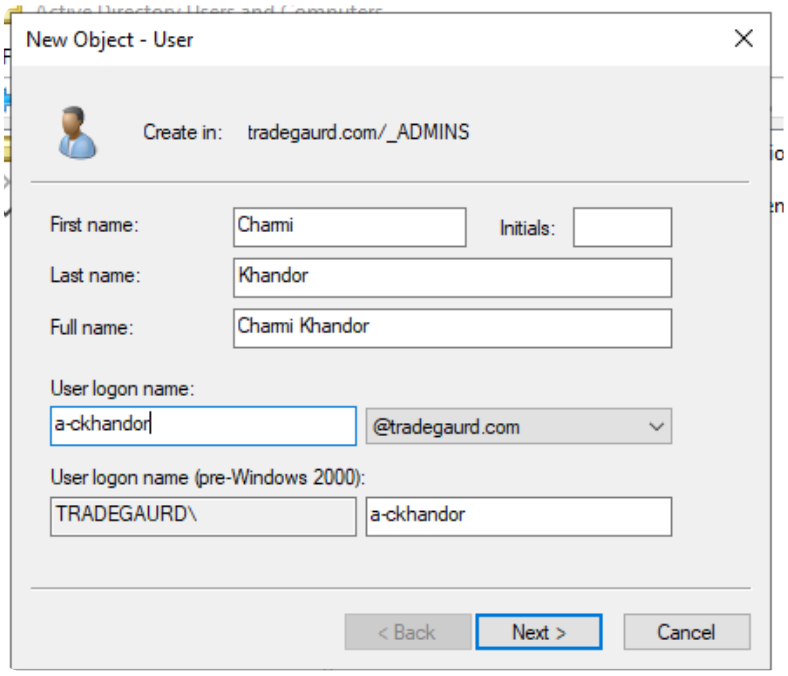
Renamed the server → `TRADEGUARD-DC`
Set static IP → `172.16.0.1`
Verified NAT and internal connectivity
Took VM snapshot → *"Pre-AD Setup"*

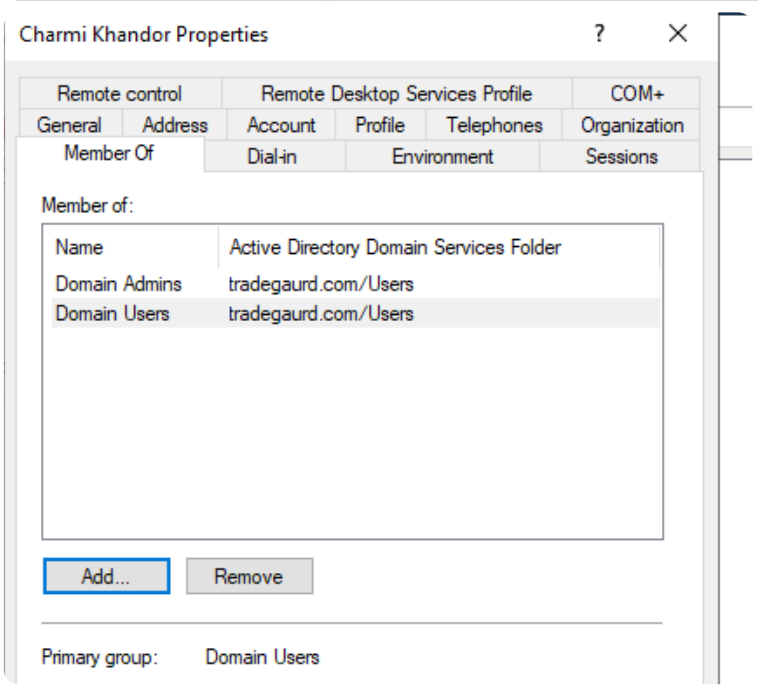
Description	Example
showing both adapters	
Network Adapter settings	
Server Manager overview	

1. Download and Configure Active Directory Domain Services (AD DS)

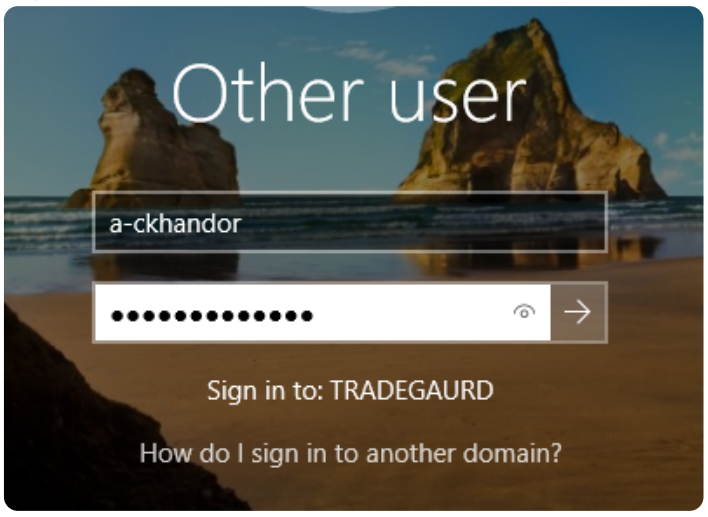
Steps:

1. **Set up the Domain Controller (DC)**
   - **Domain Name:** `tradegaurd.com`
   - **Password for the default admin:** `#TradeGaurd123`
   - During setup, make this server the **default domain controller** for the domain.
2. **Create a Custom Domain Admin Account**
   - Instead of using the default administrator account, create a custom domain admin.
   - Navigate to **Active Directory Users and Computers (ADUC)** → **Organizational Units (OUs)** → Create a new OU named `_ADMINS`.





   - Inside `_ADMINS`, create a new user.
     - **Password:** `Password1`
   - Make this user a **domain admin**.
   - Sign in with the new domain admin account.



Explanation:
Using a separate domain admin account improves security and avoids using the default admin account, which is a common attack target.

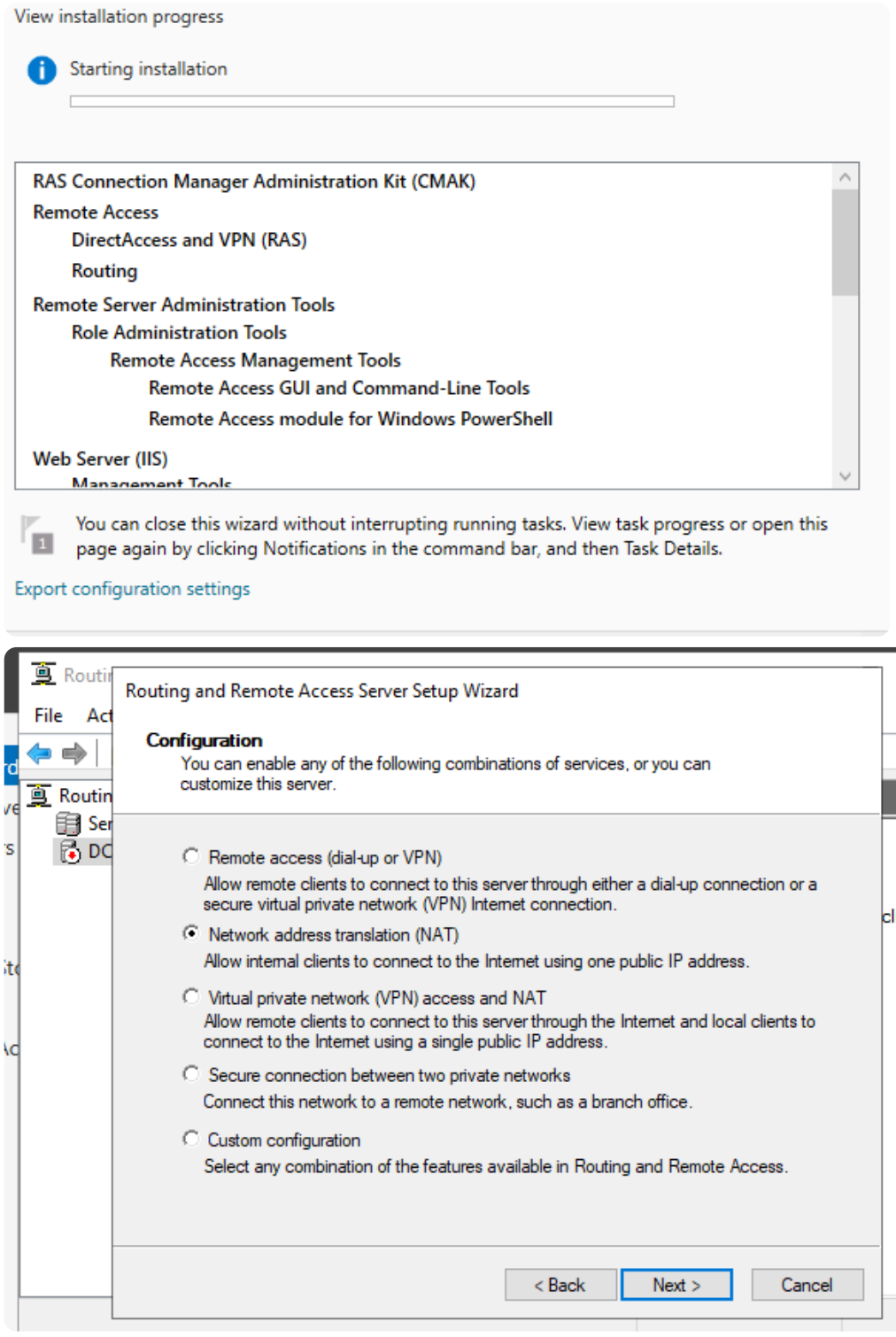
---

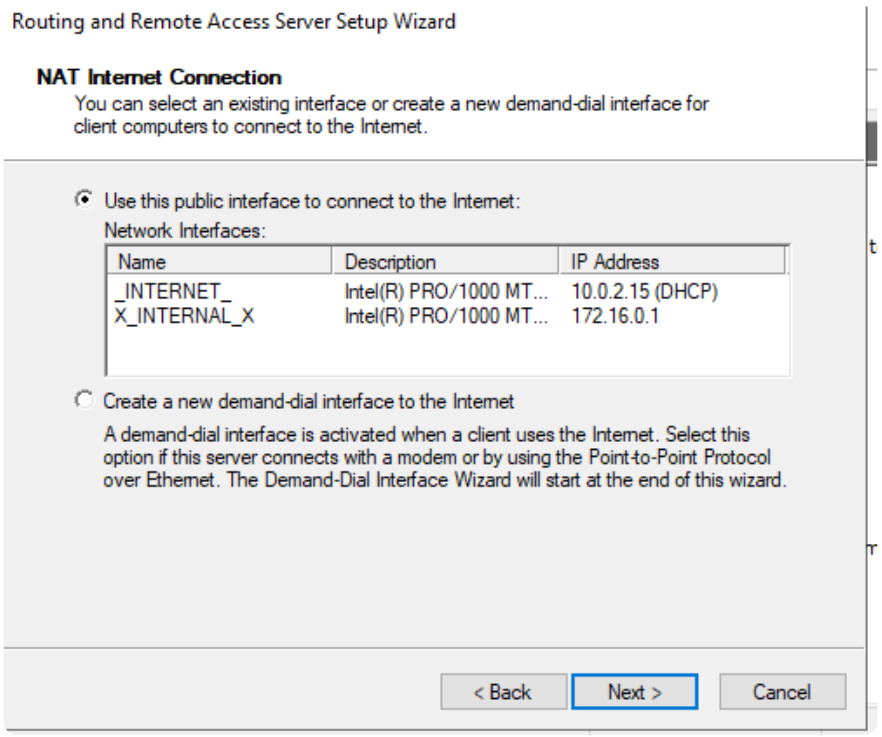
2. Install Routing and Remote Access Service (RAS/NAT)

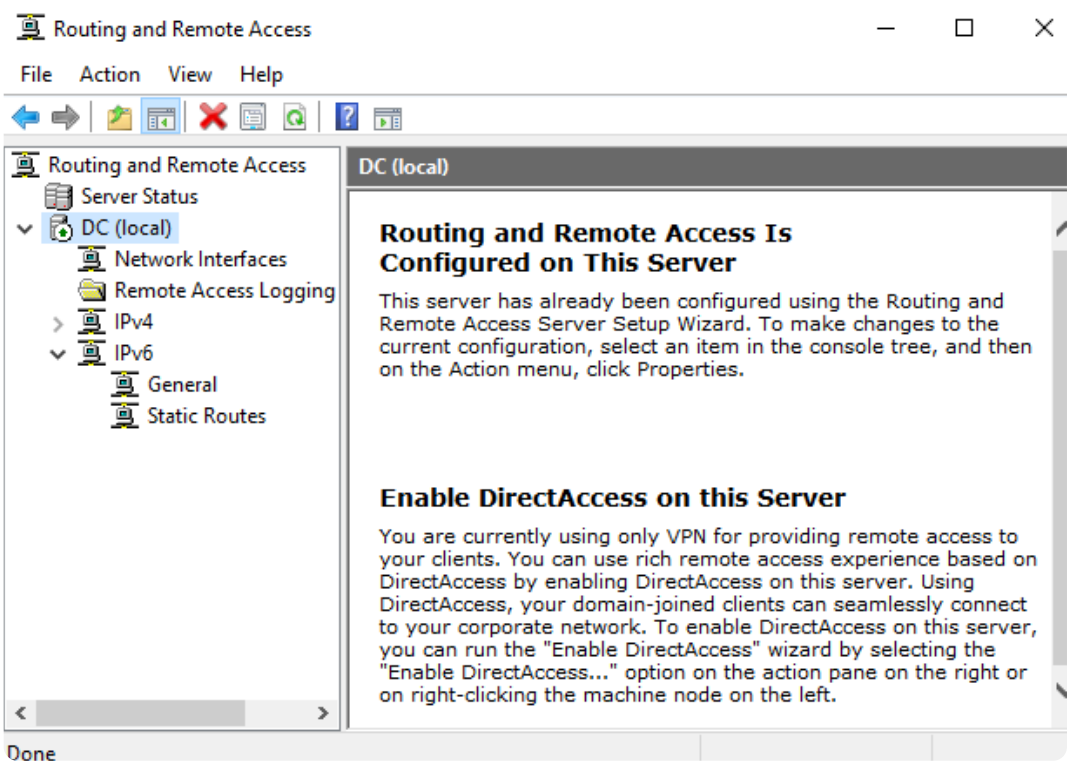
Purpose:
Allows Windows 10 clients on the internal network to access the internet through the virtual network.

Steps:

1. Open **Routing and Remote Access** tool.
2. Configure NAT (Network Address Translation) for the internal network.







Explanation:

NAT allows multiple clients on a private network to share a single public IP address for internet access. This is essential for testing virtual clients while keeping them isolated from external networks.

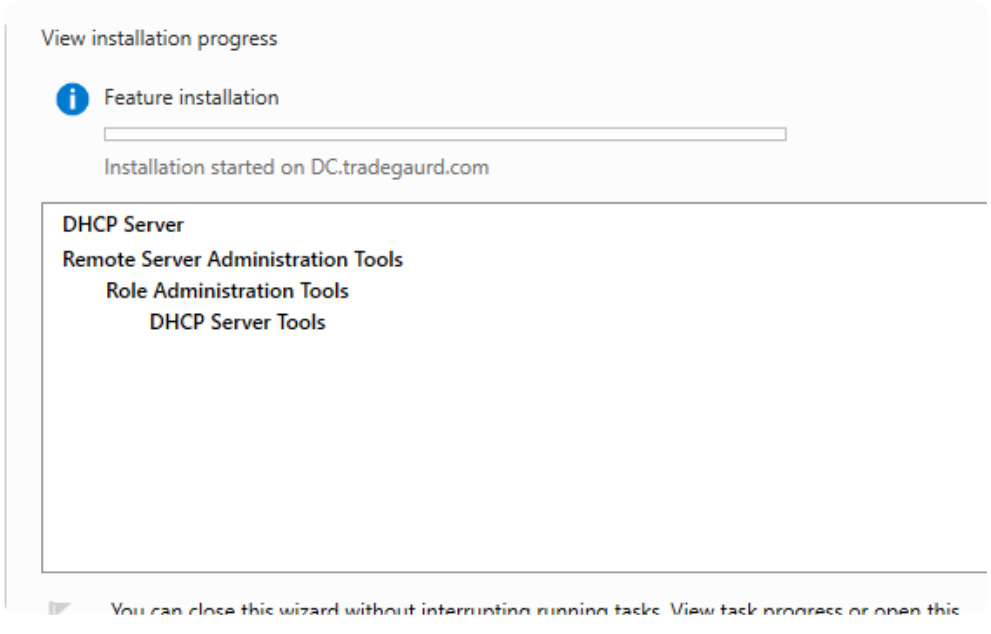
3. Set Up DHCP Server on the Domain Controller

Purpose:

Automatically assign IP addresses to clients on the internal network so they can communicate internally and access the internet.

Steps:

1. Open **DHCP Server** in the server manager.



2. Create a new **DHCP scope**:
   - **Range:** `172.16.0.100 – 172.16.0.200`

- **Subnet Mask:** `255.255.255.0`
- **Router IP:** Use the domain controller’s IP (since NAT is configured)
- **DNS Server:** Domain Controller
- No exclusions needed
- Lease duration can remain default for lab purposes

Explanation:
DHCP automates IP configuration, preventing conflicts and simplifying network management. Assigning the DC as the router and DNS ensures all internal clients route traffic properly and resolve domain names.

---

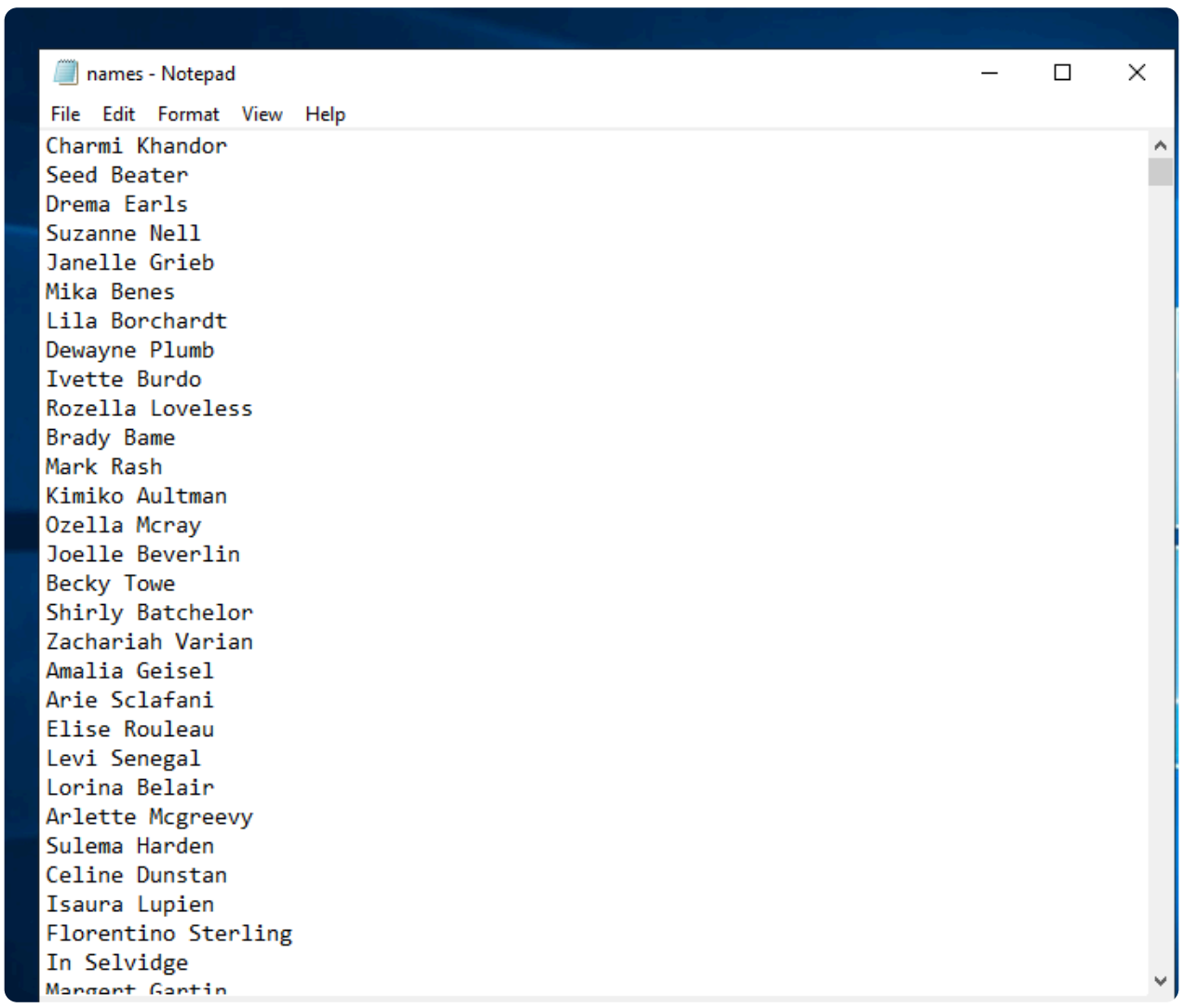
4. Create Users Using PowerShell

Purpose:
Automate bulk user creation in Active Directory with consistent credentials and organizational structure.

Steps:

1. **Prepare a text file** `names.txt` with user names, one per line:

```
John Doe
Jane Smith
```



2. **Set Execution Policy** to allow scripts:

```powershell
Set-ExecutionPolicy Unrestricted
```

3. **Run PowerShell Script**:

```powershell
# Password to assign to all users
$PASSWORD_FOR_USERS = "Password1"

# Get list of users from text file
$USER_FIRST_LAST_LIST = Get-Content .\names.txt

# Convert password to a secure object that AD can use
$password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force

# Create a new organizational unit called _USERS
New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false

foreach ($n in $USER_FIRST_LAST_LIST) {
    $first = $n.Split(" ")[0].ToLower()
    $last = $n.Split(" ")[1].ToLower()
```

```
    # Username format: first letter of first name + last name
    $username = "$($first.Substring(0,1))$($last)".ToLower()
    Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan

    # Create AD user
    New-AdUser -AccountPassword $password `
               -GivenName $first `
               -Surname $last `
               -DisplayName $username `
               -Name $username `
               -EmployeeID $username `
               -PasswordNeverExpires $true `
               -Path "ou=_USERS,$(([ADSI]`"").distinguishedName)" `
               -Enabled $true
}
```

Explanation:

- Automates creation of multiple users.
- Sets a secure, consistent password.
- Organizes users in `_USERS` OU for better management.
- Usernames follow a predictable format (`first initial + last name`), simplifying login conventions.

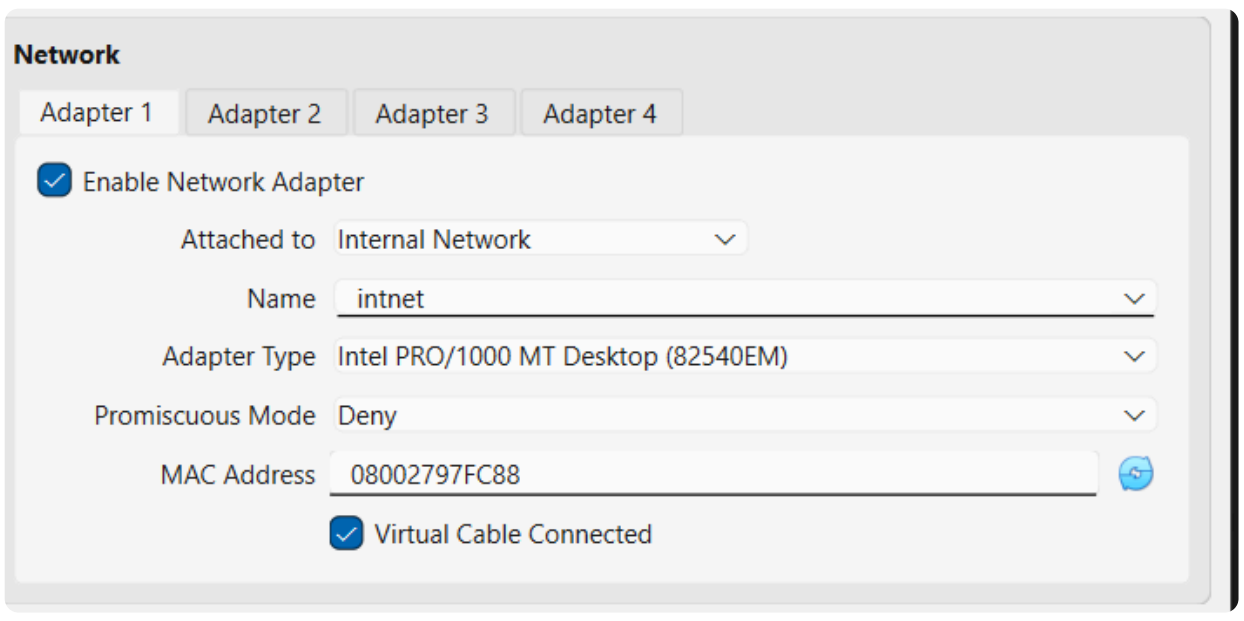
5. Creating a user client1 to test our internal network

1. Windows 10 Pro VM Configuration

Create a new VM with the following settings:

Setting	Value
VM Name	CLIENT1
OS	Windows 10 Pro
Network Adapter	Host-Only (VMnet1) - Internal network only
RAM	2-4 GB (recommended)
Disk	40-60 GB

Important: Ensure the VM is connected **only to the internal network** (Host-Only adapter) - no NAT adapter needed as it will route through the Domain Controller



- Windows 10 pro Virtual machine client

2. Verify Network Connectivity

After Windows 10 installation, verify the network is working properly:

Check IP Address Assignment:

cmd

```
ipconfig
```

You should see:

- **IP Address:** 172.16.0.x (assigned by DHCP from range 172.16.0.100-200)
- **Subnet Mask:** 255.255.255.0
- **Default Gateway:** 172.16.0.1 (Domain Controller)
- **DNS Server:** 172.16.0.1 (Domain Controller)

```
thernet adapter Ethernet:

  Connection-specific DNS Suffix  . : tradegaurd.com
  Link-local IPv6 Address . . . . . : fe80::7823:3019:39e0:1a37%4
  IPv4 Address. . . . . . . . . . . : 172.16.0.100
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 172.16.0.1
```

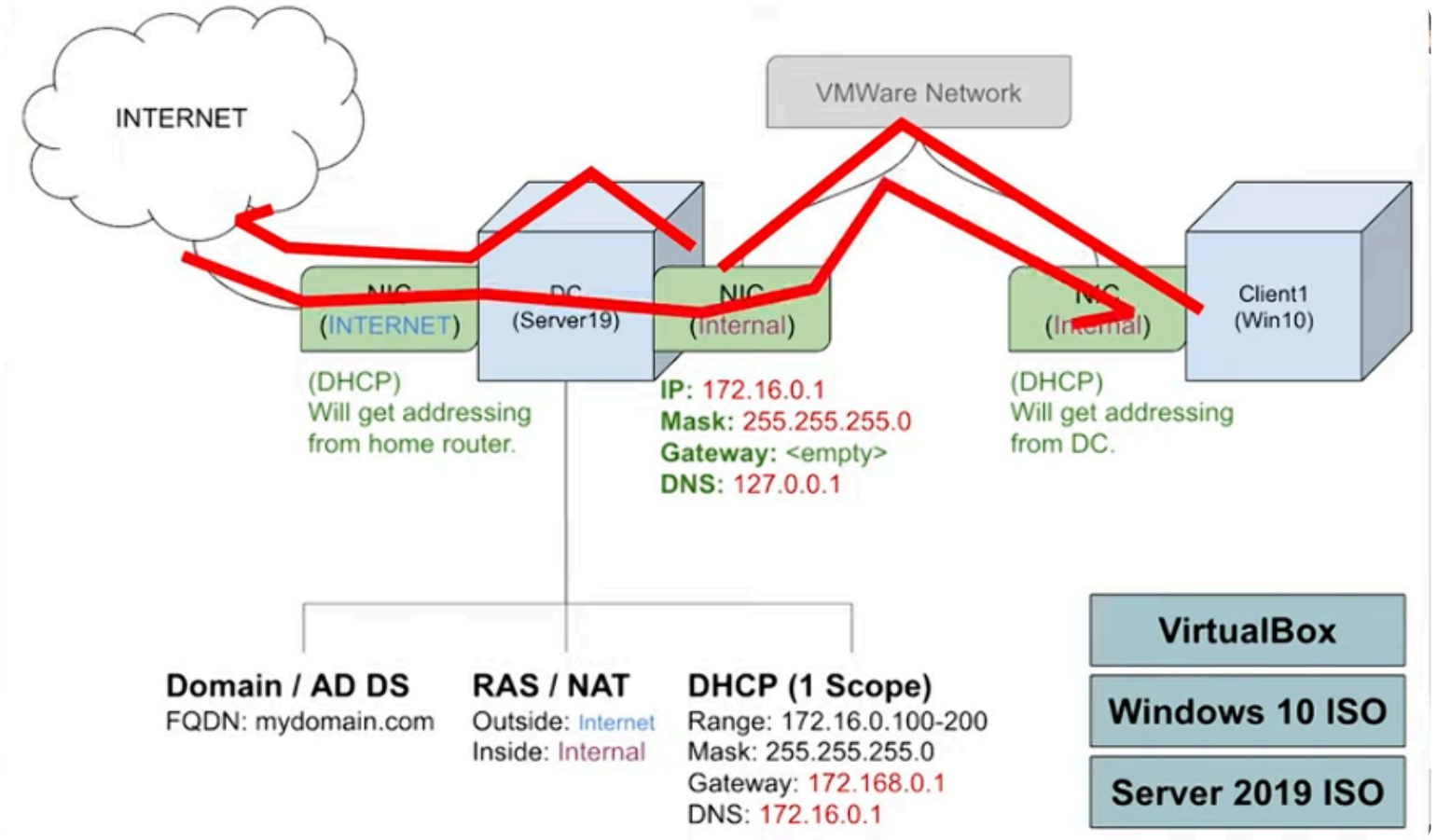
Test Internet Connectivity:

If you can ping the internet successfully, your entire network diagram is working correctly:

- Client → Domain Controller (NAT/RAS) → Internet

cmd

```
ping 8.8.8.8
ping google.com
```



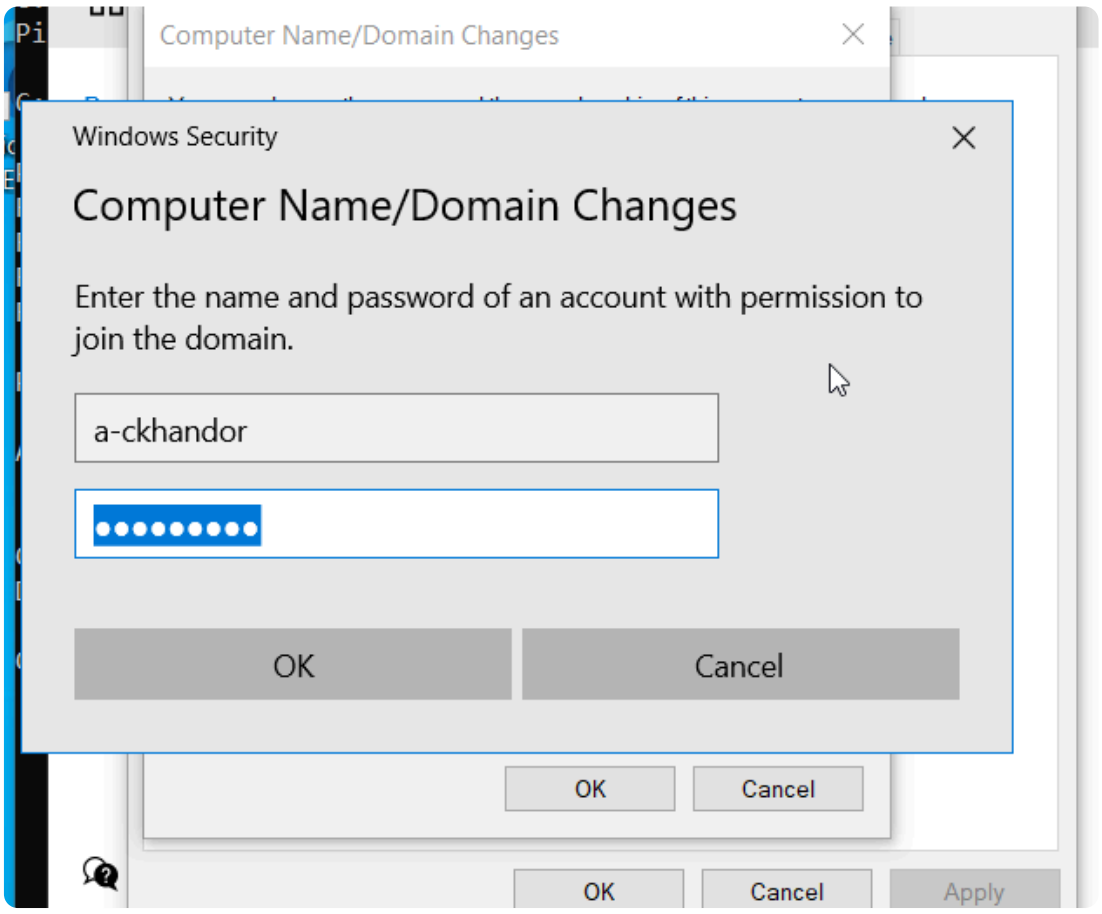

```
C:\Windows\system32>ping tradegaurd.com

Pinging tradegaurd.com [172.16.0.1] with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time=17ms TTL=128
Reply from 172.16.0.1: bytes=32 time=3ms TTL=128
Reply from 172.16.0.1: bytes=32 time=3ms TTL=128
Reply from 172.16.0.1: bytes=32 time=9ms TTL=128

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 17ms, Average = 8ms
```

3. Join Client to Domain

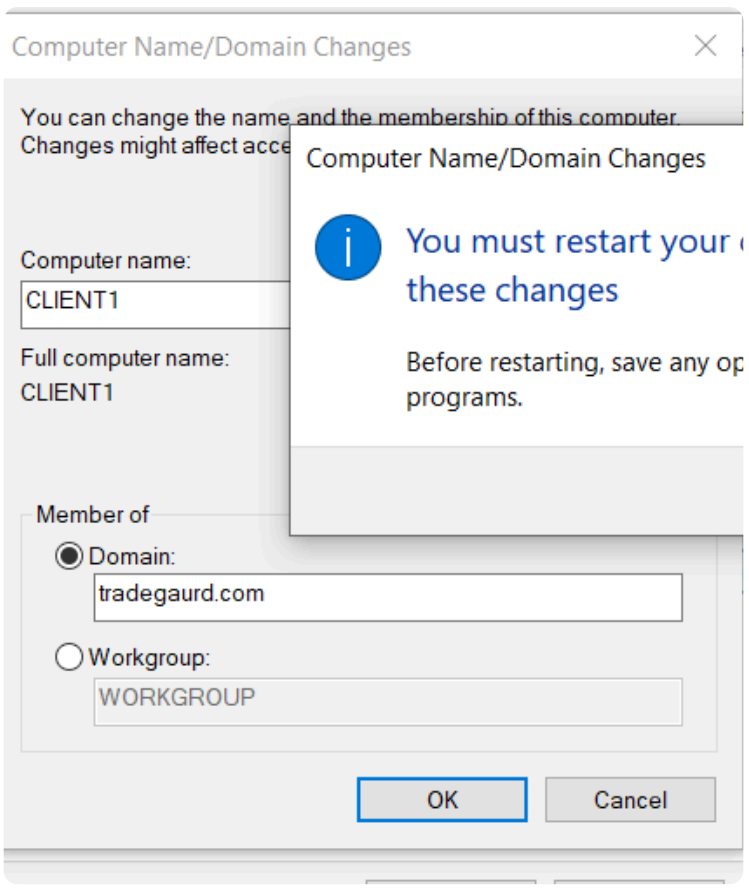
Change Computer Name and Add to Domain:

1. **Open System Properties:**
   - Right-click **This PC** → **Properties**
   - Click **"Change settings"** next to computer name
   - Click **"Change..."** button
2. **Configure Domain Membership:**
   - **Computer name:** CLIENT1
   - Select **"Domain"** radio button
   - Enter: **tradeguard.com**

- Click **OK**



3. **Enter Domain Admin Credentials:**
   - When prompted, use your domain admin account created earlier
   - Username: `a-ckhandor` (or your admin username)
   - Password: `Password1`

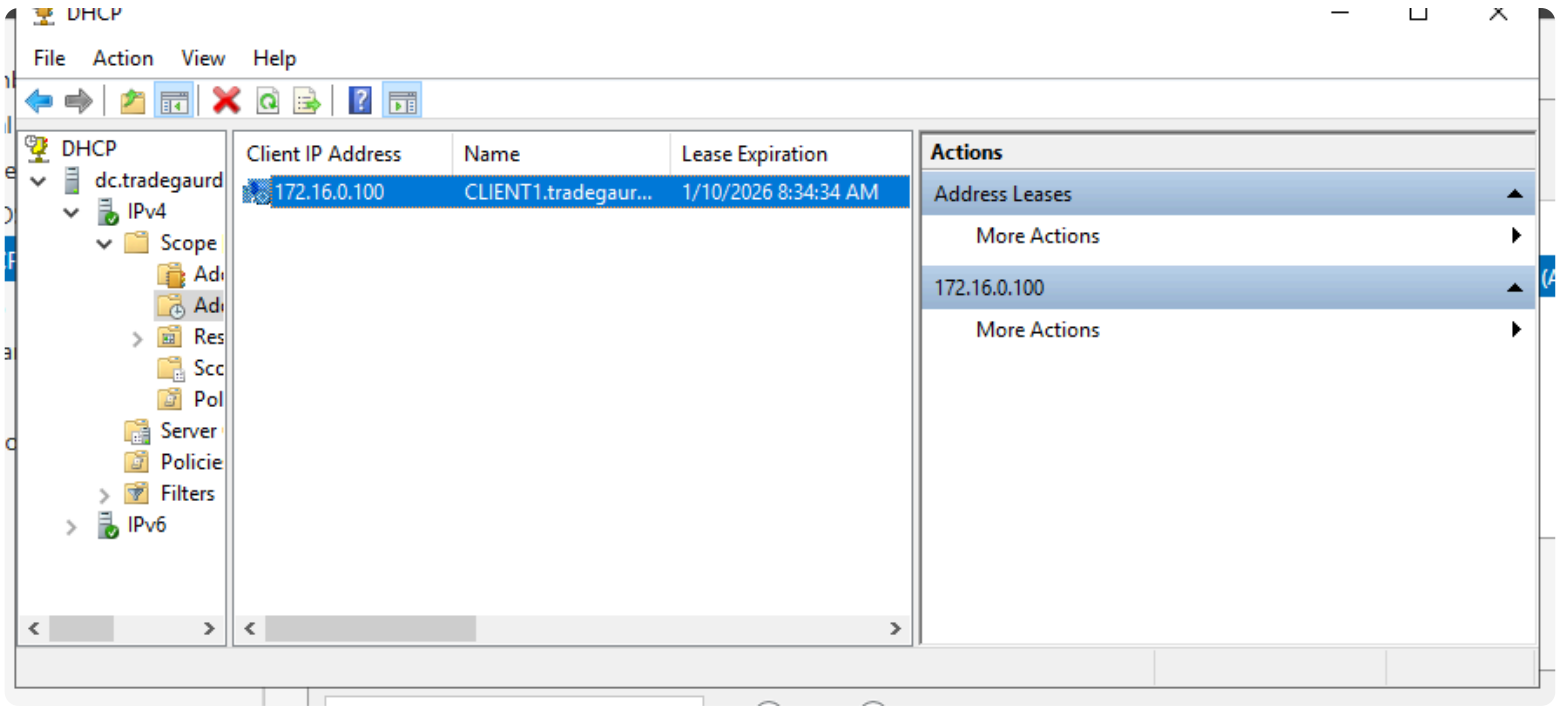


4. Verify Client Appears in Active Directory

On the Domain Controller (TRADEGUARD-DC):

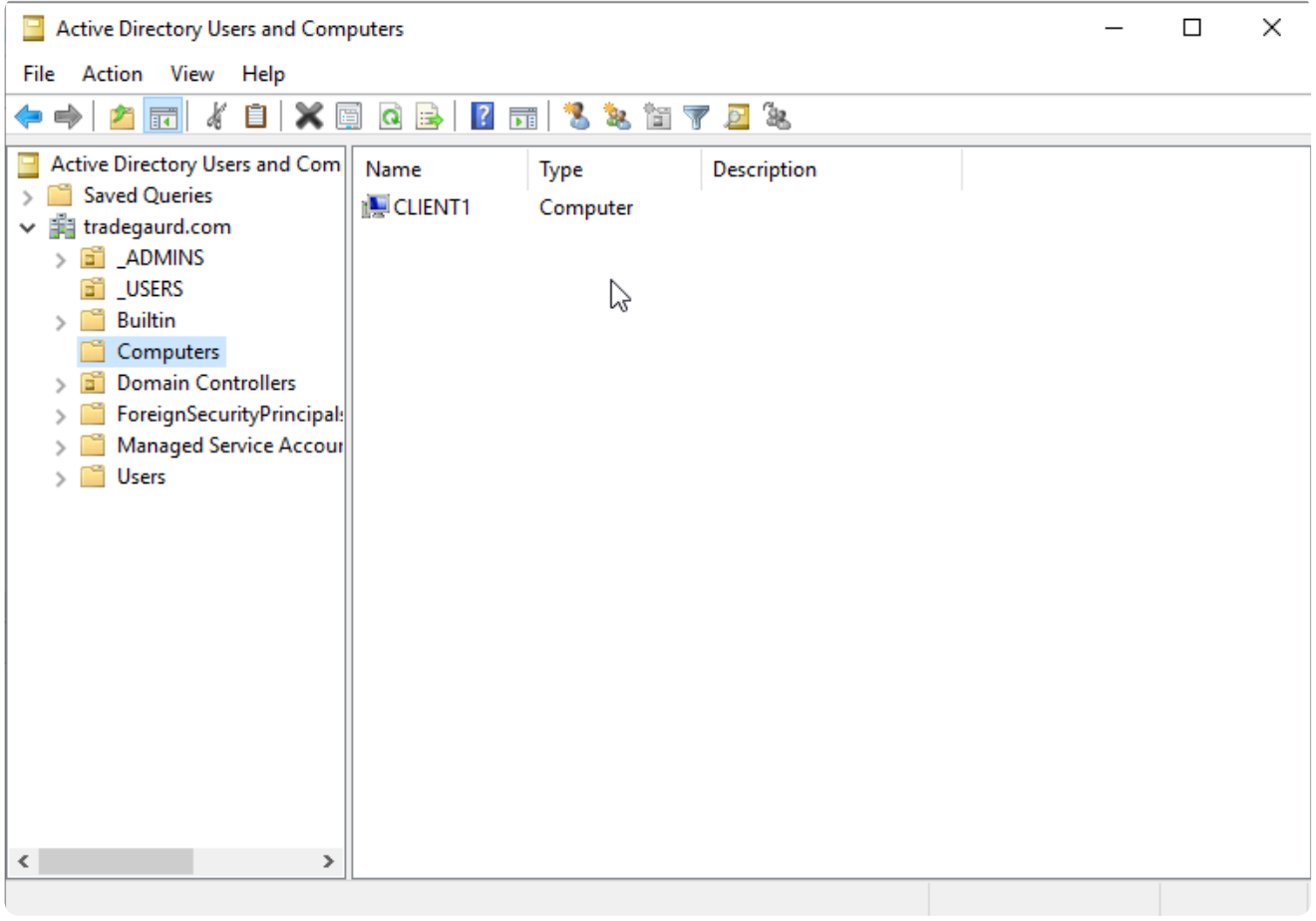
Check DHCP Lease:

- Open **Server Manager** → **Tools** → **DHCP**
- Navigate to: **DHCP** → **TRADEGUARD-DC** → **IPv4** → **Scope [172.16.0.0] tradeguard.com** → **Address Leases**
- CLIENT1 should appear with its leased IP address



Check Active Directory Computers:

- Open **Server Manager** → **Tools** → **Active Directory Users and Computers**
- Navigate to: **tradeguard.com** → **Computers**
- CLIENT1 should be listed here

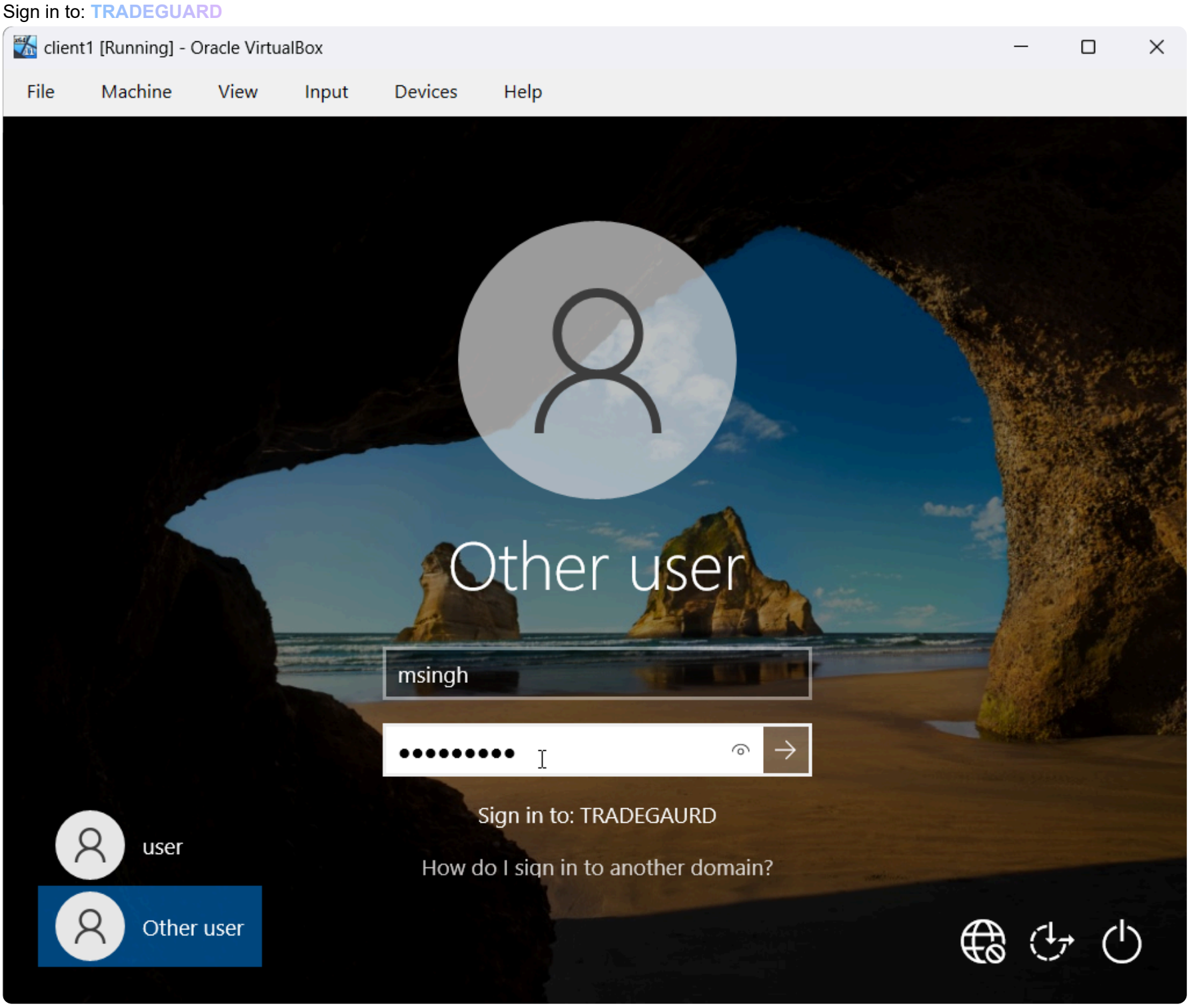


5. Test Domain User Login

Log in with PowerShell-Created Users:

1. **On CLIENT1**, restart and at the login screen:
   - Click **"Other user"**
   - Username: Use one of the users created via PowerShell (e.g., `jdoe` for John Doe)
   - Password: `Password1`

- Sign in to: TRADEGUARD



- Now we have created a mini corporate network with this

Step 2: Ubuntu SIEM

Now that the Active Directory environment and Windows client are operational, we deploy a **standalone Ubuntu Server** to act as the **Security Information and Event Management (SIEM)** system.
This SIEM will **monitor the domain externally** by collecting logs from Windows hosts via **Winlogbeat**, without being joined to the Active Directory domain.

1. Ubuntu Server Virtual Machine Configuration

Create a new virtual machine in **Oracle VirtualBox** with the following settings:

Setting	Value
VM Name	`TRADEGUARD-SIEM`
OS Type	Linux
Version	Ubuntu (64-bit)
ISO	Ubuntu Server LTS
Memory	2 GB (minimum)
CPU	1
Disk	40–60 GB (VDI, dynamically allocated)

Network Adapter Configuration

Adapter	Mode	Purpose
Adapter 1	Host-Only (VMnet1)	Internal lab communication

> ⚠ **Do NOT attach a NAT adapter**

The SIEM must reside **only on the internal network** and receive traffic from the domain via controlled routing.