Homelab Documentation

By Cody Wimbert

Overview

This document details a homelab environment I've cultivated in order to gain technical knowledge and improve my IT skillset. In this document, you will read about the installation, configuration, and management of a multi-user Windows Active Directory environment using virtual machines deployed via VirtualBox. This lab intends to simulate an enterprise environment and has been built with knowledge gained from my experiences in the field as well as through self-study. I consider this a living document, as I intend to revise it as more features are tested and configured within the environment. The goal of this project is to demonstrate my understanding of administration, networking, and security, my passion for the IT field, and my capacity to learn and implement new technologies.

Network Addressing Scheme

Windows Server 2022 (Domain Controller / DHCP Server / NAT)

- Hostname: *ADDC01*
- Internal NIC
  - IP: *172.16.0.1*
  - Subnet: *255.255.255.0*
  - Gateway: N/A (not required, server routes internal network)
  - DNS: *127.0.0.1* (loopback, resolves to itself as DNS/DC)
- External NIC (Internet)
  - IP: *10.0.2.1*
  - Gateway: *10.0.2.2* (for outbound internet)

Windows 10 Pro Client

- Hostname: *CLIENT1*
  - IP (from DHCP): *172.16.0.100*
  - Subnet: *255.255.255.0*
  - Gateway: *172.16.0.1*
  - DNS (static for reliability): *172.16.0.1*

VirtualBox Setup & Configuration

I chose VirtualBox as my virtualization software as it is widely utilized across the industry and is an open-source solution, making it free to install and widely available:

Initial Setup

1. **Installed VirtualBox** at official website
   - *Verified file integrity via Get-FileHash (compared to checksum value)*
2. **Installed Windows ISOs** at official website

3. **Configured VMs** (*Windows Server 2022, Windows 10 Pro*)
   Gen 2 > 4096 memory (8192 server) > 50 gb > select ISO
4. **Created NAT & Internal Networks**: Attached Adapter 1 on *ADDC01* to NAT for Internet access, all other Adapters on Internal Network
5. **Configured static IP addresses** (IP, subnet mask, DNS) via Open LAN Icon in
   Taskbar > Open Network & Internet Settings > Change Adapter Options > NIC 2 (INTERNAL) > Properties

Insecure Install Location Error

*I initially encountered the "Insecure Install Location" error upon attempting to install VirtualBox in a non-default location; troubleshooting steps detailed are adapted from [this Reddit post](): *

1. **Created new folder** *F:\Oracle Virtualbox*
2. **Edited folder permissions** *Right click > Properties > Security > Advanced > Change Permissions > 'Disable Inheritance' > 'Convert inherited permissions into explicit permissions on this object'*
3. **Edited *User* permissions to *Read & Execute*, removed *Authenticated Users* from list**
   'Users' list entry > 'Edit' > Uncheck box next to 'Write' option > Click OK

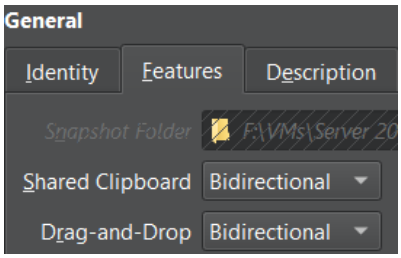
I was now able to install VirtualBox to the desired location!

Enable Copy & Paste Between Host Machine and VMs

As I progressed through my configuration, I found it annoying that I could not copy & paste between my host machine and my VMs. A quick Google search provided the following solution:

While the VM is booted...

1. **Inserted Guest Additions CD**
   Devices > Insert Guest Additions CD Image...
2. **Installed Guest Additions CD**, rebooted at prompt
3. **Enabled bidirectional Shared Clipboard & Drag-and-Drop**
   VirtualBox Manager > Settings... > General > Features
4. *Success!*



Installing Windows Active Directory on DC

In order to simulate a real enterprise environment, I installed Active Directory Domain Services on my DC. This would provide centralized management of all my VMs and allow me to experiment with GPO provisioning:

Initial Setup

1. **Installed Windows on *ADDC01* using default settings** (*Windows Server 2022 VM*)
2. **Set static IP settings** (according to "*Network Addressing Scheme*" section)
3. **Renamed server to *ADDC01*** *and rebooted when prompted*
   Server Manager > Local Server Computer name > Change

Installing Roles & Features

1. Opened **Server Manager** > **Add Roles and Features**
2. **Clicked Next** until reaching **Server Roles**
3. Selected **Active Directory Domain Services**
4. Continued through the wizard and clicked **Install**

DC Promotion

1. Selected ***'Promote server to a domain controller'*** in *Server Manager (yellow flag icon, pictured)*
2. Selected ***Add a new forest*** (Root domain name: *mytest.local*)
3. Selected **default settings and rebooted**

Installing RAS/NAT

To reach the Internet from my internal network, I configured a RAS/NAT server on my external NIC (attached to my ADDC01 DC). This would allow internal clients to connect to the Internet using one public IP address:

1. Selected *Add Roles & Features > Next > Next > Select server > Next > Selected "Remote Access" Role > Next > Selected "Routing" & Left Defaults > Next > Finish*
2. Progressed to *Tools > Routing & Remote Access*
3. Selected *Configure and Enable Routing and Remote Access*
4. Selected *Install NAT*
5. "Use this public interface to connect to the Internet" (Selected "INTERNET" NIC) > Finish
6. Green arrow (Up) indicated *Success!*

Installing & Configuring DHCP Server

Though DHCP is probably unnecessary for my needs in a small lab environment, I configured this server to better simulate an enterprise environment. DHCP reduces the need for manual, static provisioning of IP configurations and thus makes networks more easily scalable:

Installation

1. **Server Manager > Add Roles and Features > Role-based installation > ADDC01**
2. **Selected DHCP Server** on Server Roles page > Install

Authorizing DHCP Server

1. *Server Manager > Tools > DHCP*
2. *Right-click > Authorize*
3. **Refreshed** — Green arrow indicates *Success!*

Creating a Scope (Address Range)

1. DHCP Manager > right-click IPv4 > New Scope

Name: 172.16.0.100-200

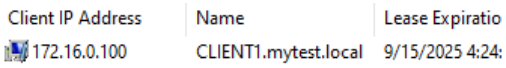
2. Defined address range
   Start: 172.16.0.100
   End: 172.16.0.200
   Subnet mask: 255.255.255.0
3. **Did not reserve any addresses** within this range (no need)
4. **Lease duration: Default 8 days** (should not be an issue on lab network)

Configuring Scope Options

- Router (Default Gateway): *172.16.0.1*
- DNS Server: *172.16.0.1*
- DNS Domain Name: *mytest.local*
- *Right-click > Scope Options > Configure Options*
- **Enabled 003 Router, 006 DNS Servers, 015 DNS Domain Name**

Verification

Released and renewed IP on CLIENT1 via ipconfig /release and ipconfig /renew:



- *Server Manager > Tools > addc01.mytest.local > IPv4 > Scope (172.16.0.100-200) > Address Leases*
- Client was assigned IP *172.16.0.100*, which is within the DHCP pool, indicating *Success!*

OU Creation & User Provisioning

*The magic happens in **Active Directory Users and Computers**. From there, it's as simple as creating a new object by right clicking and entering desired attributes in the provided fields. However, provisioning one OU or User at a time is a time-consuming process. [Josh Madakor's PowerShell script] allowed me to generate 1,000+ users and showed me the potential for automation in an enterprise environment:*

1. **Modified *names.txt* file** to suit my needs
2. **Ran script in *PowerShell ISE***
   Pulls from names.txt to create user objects, assigns them a default password (Password1), and places them into a newly generated _USERS OU
3. **Verified object creation via GUI** (*Server Manager > AD Users and Computers*)

General Troubleshooting

I encountered many issues through my installation and configuration of these virtual machines and have done my best to document my troubleshooting methodology here:

Network Connectivity

- Upon setting up my VMs, **pinged IP** for both to confirm network connectivity

- **Ping echo request didn't go through from server to client, but client to server worked fine**
- Both **could access basic URLs** in browser
- After some searches, discovered that **Client implicitly denies ICMP echo requests due to no inbound rule on firewall** (Windows Defender blocks ping to reduce attack surface (stops malicious actors from performing network scans))
- **Disabled Firewall temporarily** > ping succeeded
- **Created inbound firewall rule** (*Windows Defender Firewall > Advanced settings > Inbound Rules > New Rule... > Custom > Protocol type (ICMPv4) (other settings default) > Name "Allow ICMP Echo"*)
- **Pinged client from server**... *Success!*

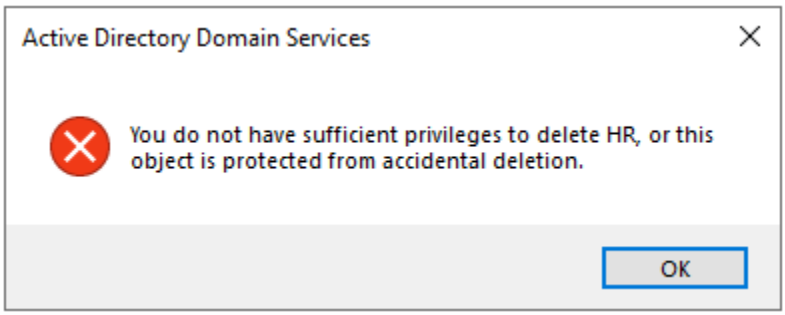
Client Domain Join

- ***CLIENT1* failed to join *mytest.local* domain**
- **Received error** *"Some DNS records may be missing"*
- **Checked DNS records in Server Manager**... Found nothing abnormal
- **Checked IP configuration using /ipconfig** to confirm configuration

    DNS set to "Auto-obtain"... Discovered that DNS needs to be set statically to DC in this configuration, not to an external or auto-obtained server
- **Set DNS to static (*172.16.0.1*)** and was able to *successfully* join client to domain

Disable "Protect Object from Accidental Deletion"

Received the following error upon attempt to delete OU when trying to restructure hierarchy

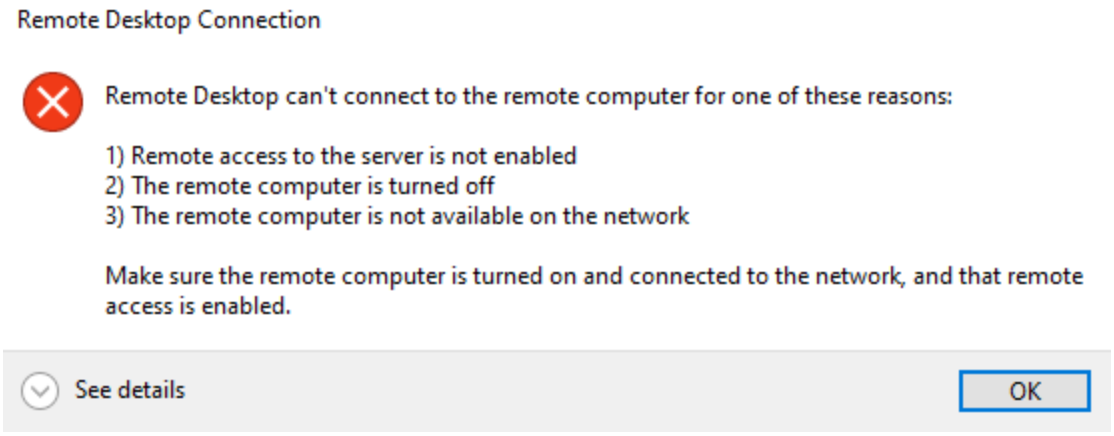


Since I was logged into an Administrative account, I knew I had privileges to delete the OU. However, I needed to investigate "object is protected from accidental deletion" error:

- *Right clicked > Properties > Object > Protect object from accidental deletion (Disable)*
- Verified by attempting to delete OU again... *Success!*

Configuring Remote Desktop Connection

Initial failure to connect to remote client:



- **"Allow remote connections" in Windows settings toggled off and could only be enabled with an Administrative account**
    I wondered if this configuration could be pushed out with Group Policy...
- **Created GPO "Enable-RDP"** for user workstations within *mytest.local\Endpoints\Workstations*
- **Applied to Domain Computers group**
- **GPO defines Inbound Firewall Rules** (Remote Desktop - User Mode (TCP-In), Remote Desktop - User Mode (UDP-In), Remote Desktop - Shadow (TCP-In)) **and Allow Remote Connections** "Allow users to connect remotely by using Remote Desktop Services"
    To create Firewall rules within GPMC: *Edit rule "Enable-RDP" > Windows Settings > Security Settings > Windows Defender Firewall with Advanced Security > Inbound Rules > Right click empty space > New rule > Predefined > Remote Desktop)*
- **Achieved successful RDP connection to and from client**

Slow Client Machine

While ADDC01 ran well, CLIENT1 experienced frequent slowness and freezing. I performed some basic troubleshooting to resolve this issue:

- **Performed restart & applied Windows updates**
- **Checked hardware resource allocation on VirtualBox** (Good)
- **Checked task manager**
    Disabled News & Interests since it is an unnecessary feature and was spiking CPU

I decided this would be a good opportunity to experiment with another Group Policy. After some Googling, I discovered that the News and Interests service could be disabled with an option under Edit > Policies > Administrative Templates. However, upon creation of my "Disable News & Interests" GPO, I found that "News & Interests" was not an option in that path... After more Google queries, I discovered that these files are not always included with Windows Server 2022 installs, but that an updated repository of administrative templates could be installed from Microsoft's website...

Applying Group Policy

Creating GPO to Disable News and Interests

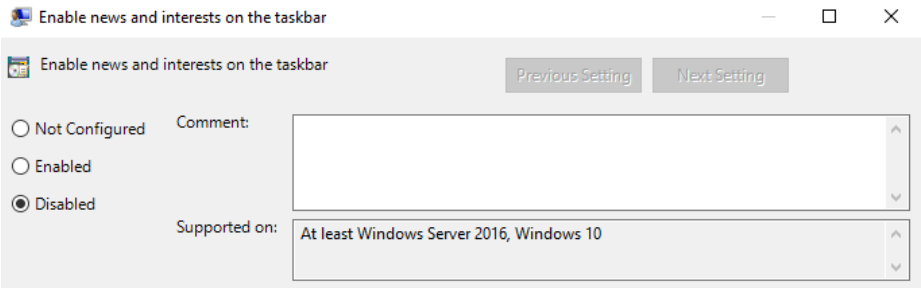
… I visited Microsoft's website to install the necessary administrative templates so I could create and implement the "Disable News and Interests" GPO:

- **Obtained updated .ADMX and .ADML files** from Microsoft's website > Ran installer (Wizard) > Installed to default path (pictured):

Location:	C:\Program Files (x86)\Microsoft Group Policy\Windows Server 2022 August 2021 Update \PolicyDefinitions\

- **Refreshed Domain in GPMC** thinking it would show the new options, but instead it showed no options…

  I suspected that the file path was somehow modified or that there was an issue with the default install location based on past experiences…
- With more investigation, I learned that the **relevant files would needed to be moved** to a preferred location on the DC to reliably appear in GPMC (***C:\Windows\PolicyDefinitions***)
- Once I confirmed that the files populated, I **refreshed and edited *"Disable News & Interests" GPO*** *> Applied to user group "Domain Users" & machine group "Domain Computers" > client side gpupdate /force > Restart*
- ***gpresult /r confirmed that the GPO was applied to CLIENT1*** *and News & Interests no longer started, indicating Success!*



Installing Google Chrome to Client Machine via GPO

Knowing how frequently users need software applied to systems, I wanted to practice pushing out a simple application, Google Chrome, to clients within my domain. I expected this to be a relatively easy process, but it proved to be more challenging than expected due to NTFS/Security permission configurations:

On DC

- **Installed** Google Chrome **.msi file** from browser
- **Created folder** *C:\Software* and shared

  Right click > Properties > Sharing > Advanced Sharing > Permissions > Everyone > Security > Edit > Domain Users (Read & Execute, List Folder Contents, Read)
- **Copied .msi file** into *C:\Software*

On Client

- **Confirmed share folder access** (*\\ADDC01\Software*)

On DC

- **Created GPO "Google Chrome"** linked to mytest.local > Add… *Authenticated Users* in Security Filtering > Right click > Edit > Computer Configuration > Policies > Software Settings > Software Configuration > Software Installation > Right click > New > Package… > Selected .msi file in *\\ADDC01\Software*

On Client

- ***gpupdate /force* > restart client machine…** *Success!*

Though I performed these actions using only my DC and client machine, I'd like to set up a dedicated file server for future software rollouts. I'd also like to include some troubleshooting techniques and lessons learned during this process…

- Reset permissions to ensure NTFS matches Security: **takeown /f "C:\Software" /r /d y**, **icacls "C:\Software" /reset /t /c /q**
- DC & domain shares are ***NOT*** the same… The folder *C:\ Software* was not showing the application .msi on *\\mytest.local\Software* but did on *\\ADDC01\Software*, so **ensure GPO points to correct path**
- Run **gpresult /r** on client machine **to confirm group membership** and compare with NTFS/Security Permissions on shared folder