Contents

1 Introduction

It took me far too long to realize the significance of the word ”Directory” in Active Directory. So that never happens, again, here is Mr. Bing:

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. A directory, in the context of AD, is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators.

AD is both a database and a set of services that connect users with the network resources they need to get their work done. The database (or directory) contains critical information about your environment, including what users and computers there are and who’s allowed to do what. AD DS is a distributed database that stores and manages information about network resources as well as application-specific data from directory-enabled applications. The Active directory database uses the “Extensible Storage Engine (ESE)” which is an indexed and sequential access method (ISAM) database.

LDAP (Lightweight Directory Access Protocol) is an application protocol for working with various directory services. Directory services, such as Active Directory, store user and account information, and security information like passwords. The service then allows the information to be shared with other devices on the network. LDAP orchestrates searching in Active Directory. When a user searches for a user, computer, or printer, LDAP runs a search and finds the results. Based on multiple levels of permissions on Active Directory, users get access to information and resources through LDAP authentication. LDAP administrators require elevated permissions to add or manipulate information in your AD repository database.

2 Domain Controller

2.1 Network

To edit your network settings, follow these directions:

Control Panel → Network and Sharing Center → Change Adapter Settings → Click "Internet Protocol Version 4 (TCP/IPv4)

We have two goals in this menu: setting a static IP (to whatever) and setting the DNS servers. On non domain controllers, the DNS should be set to use DC1 and DC2. On the domain controllers, the DNS should be set to use the other domain controller and the internet (e.g. 8.8.8.8 for Google's DNS).

2.1.1 Setting a Static IP

For an image, see Figure 1

You can set the static IP to any IP not currently in use. (Maybe you can kick machines off of their IP, but that is probably not advised.) Once you have picked your IP, put it in the **IP Address** field. I am not sure how to determine the subnet mask manually, so I run **ipconfig** in powershell and use the subnet mask it gives. To determine the default gateway, you can run **ipconfig** or **route print**. It is also possible to find the default gateway by running **ip route show** in the Proxmox console.

2.1.2 Setting the DNS Servers

For an image, see Figure 1

This step is less complicated than the last step. However, you can Red-Team yourself (I speak from experience...), so be careful.

On the Domain Controller, the first DNS server should be itself (the same as the machine's static IP). The second should be an actual internet DNS server. In this case 8.8.8.8 is Google's DNS Server.

On non domain controllers, both DNS servers should point to the domain controllers.

3 Useful Videos

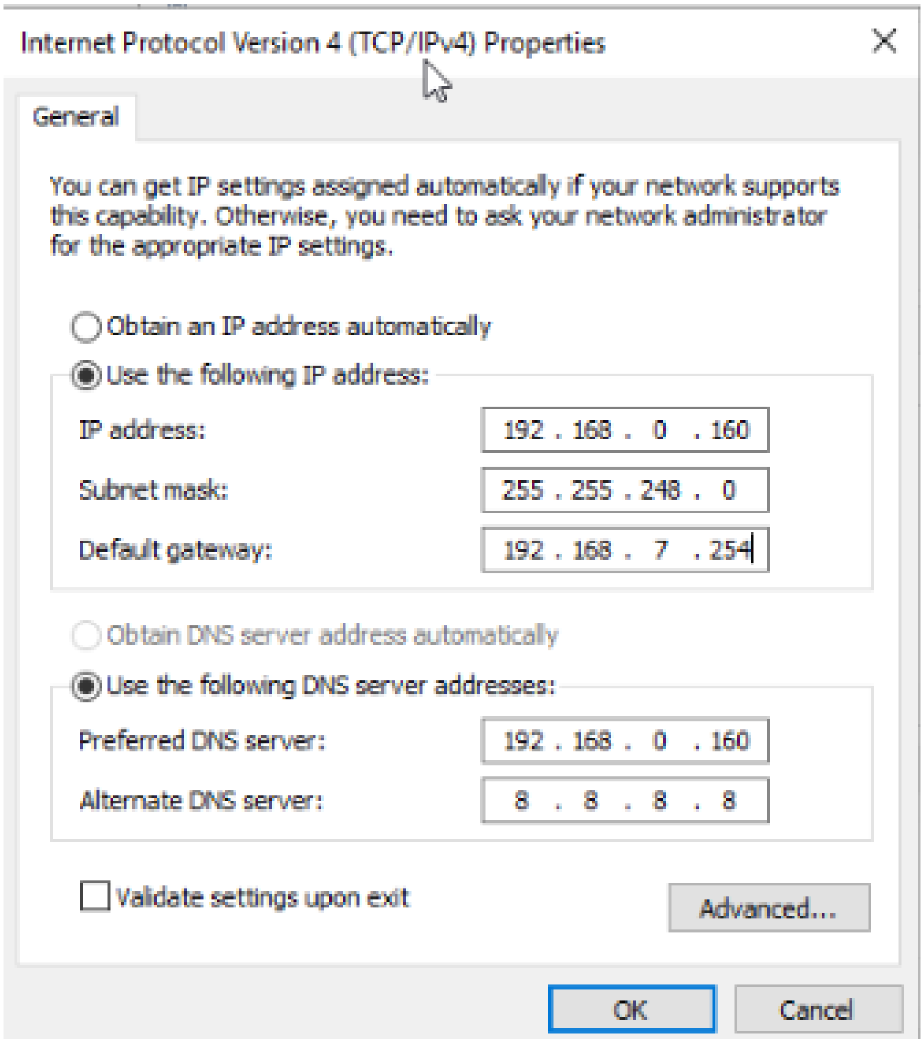
This is a list of useful videos for understanding active directory. At some point I should watch all of the videos, take notes on them, and put them in the document.

1. FSMO Roles (not very good but idk what FSMO role are and it is important)

2. Professor Messer LDAP/LDAPS

3. Sean Metcalf Active Directory Overview

4. Sean Metcalf Active Directory Attacks



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 160

Subnet mask: 255 . 255 . 248 . 0

Default gateway: 192 . 168 . 7 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 160

Alternate DNS server: 8 . 8 . 8 . 8

□ Validate settings upon exit

Figure 1: Example IPv4 Settings

5. More Sean Metcalf Active Directory

6. Even more Sean Metcalf Active Directory

7.