Active Directory

September 3, 2023

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 Deployment

This step is very easy but Chris said I had to document it. Go to the add roles and features wizard, server roles, and check "Active Directory Domain Services." After it finishes downloading, click the yellow warning icon in the top right of the Server Manager. The yellow icon says "Post Deployment Configuration".

2.1 Making a new forest

In the Deployment Configuration, select "Add a few forest".

In the text field that says "Root domain name", you will put the Fully Qualified Domain Name (FQDN).

FQDN guidelines:

1. **Naming**:
   - Use a subdomain of a domain you own, e.g., `ad.example.com`.
   - Avoid using the exact public domain name.
2. **Length and Characters**:
   - FQDN should be 155 characters or fewer.
   - Use letters (A-Z, a-z), numbers (0-9), and hyphens. No special characters.
3. **Uniqueness**:
   - Ensure no conflicts with existing names on your network.

4. **NetBIOS Name**:
   - The NetBIOS name is a legacy computer name format, typically shorter and without domain suffixes.
   - For AD DS, it's a non-FQDN version of your domain name, often the prefix of your FQDN. Example: For `corp.example.com`, the NetBIOS name could be `CORP`.
   - It's used for backward compatibility with older systems and applications that don't recognize FQDNs.
   - Ensure it's unique within your network to prevent conflicts.
5. **Avoid**:
   - Names like `www`, `public`, `com`, `net`, `org`.

After the domain is created, the built-in local "Administrator" account of the server becomes the domain "Administrator" account for that domain.

Directory Services Restore Mode A special boot mode for Windows Domain Controllers used for repairing, restoring, or analyzing Active Directory. In the event of a compromise or corruption of the domain controller, DSRM provides an isolated environment to restore from backups, conduct forensic analysis, or manually rectify issues. It's essential for maintaining the integrity and security of Active Directory services.

2.2 Adding to an existing forest

When adding a new Domain Controller to an existing forest, you should first join the machine to the domain. The two machines must have different SIDs. Use the SIDCHGL program as described in the deployment section.

3 Network

To edit your network settings, follow these directions:

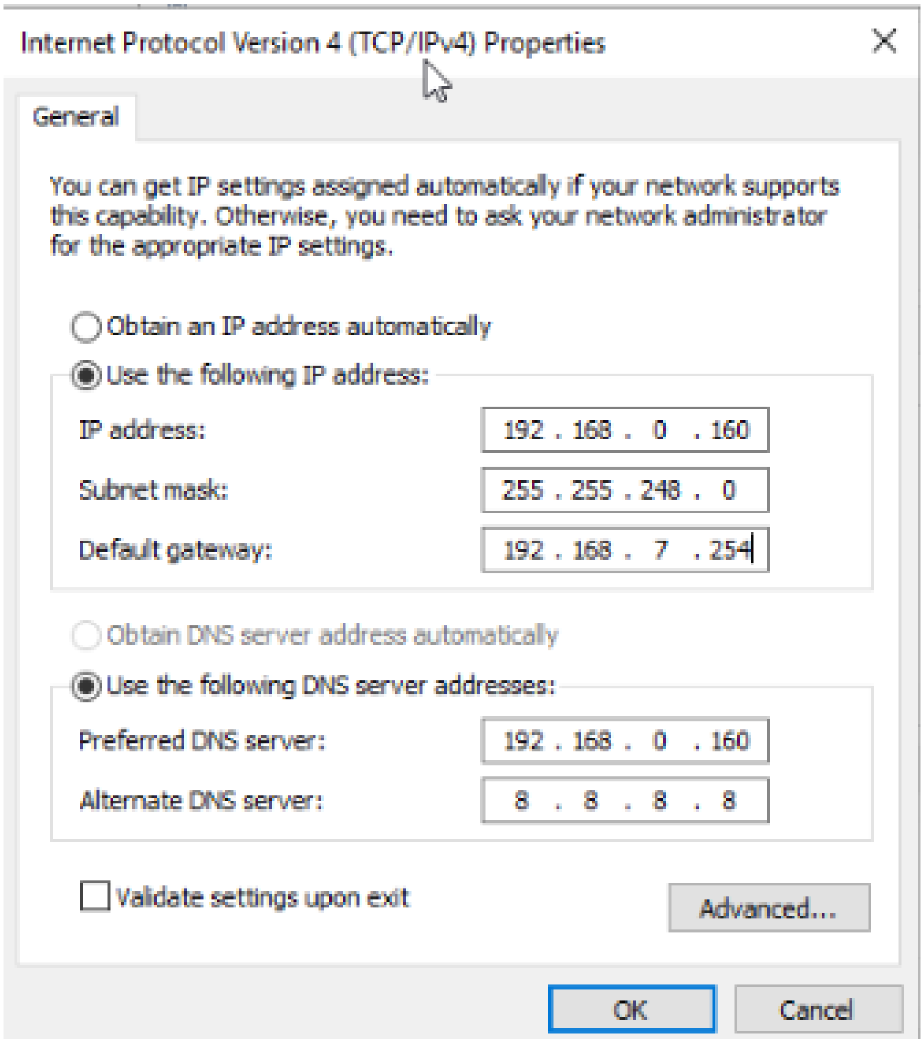
Control Panel → Network and Sharing Center → Change Adapter Settings → Click "Internet Protocol Version 4 (TCP/IPv4)

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).

3.1 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



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

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.

3.1.1 Setting the DNS Servers

For an image, see Figure 1

I assume you have 2 Domain Controllers.

The Domain Controllers should have their DNS set to

1. IP of the other Domain Controller
2. Own IP (aka the static IP you set)
3. Some other DNS that can go on the internet, i.e. 1.1.1.1 or 8.8.8.8

To set more than 2 DNS servers, go to "Advanced" and then the DNS tab.

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

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

Do not worry if you disconnect after doing this!!! The IP address of the server has changed, of course your rdp connection to it will be cut.

4 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
5. More Sean Metcalf Active Directory
6. Even more Sean Metcalf Active Directory

5 Enabling LDAPS

Run the command certutil -verifystore MY

6 Why do forests exist?

6.1 What is a forest

A forest is a collection of one or more domains that share a common schema, configuration, and global catalog. The forest represents the highest level of logical container in Active Directory.

Trusts can be manually configured between different forests if required.

Certain forest-wide data, like the schema, is replicated to all domain controllers in all domains within the forest.

They can be used for replication and for easier management across multiple geographic regions.

6.2 What is a domain

"A domain represents a database. That database holds records about network services-things like computers, users, groups and other things that use, support, or exist on a network. The domain database is, in effect, Active Directory." - Robert R. King

A domain is associated with a single DNS namespace (e.g., example.com).

By default, all domains within a forest have two-way, transitive trusts, meaning resources can be easily shared across domains in the same forest.

6.3 What is a schema?

Active Directory Schema:

- Serves as the blueprint for permissible objects and attributes within Microsoft's Active Directory (AD).

Key Elements:

- *Object Classes:* Define permissible objects like users, groups, and computers.
- *Attributes:* Specify properties an object can have, e.g., first name, last name for a user.
- *Syntax:* Dictates the type of data an attribute can contain.
- *Constraints:* Apply rules or limitations on attributes, such as mandatoriness.
- *Object Identifiers (OIDs):* Ensure global uniqueness for object classes and attributes.

Importance of Schema:

- *Standardization:* Enforces consistent creation and management of objects.

- *Extensibility:* Allows for custom object classes and attributes.
- *Search Optimization:* Enables efficient querying via well-designed indexing.
- *Security:* Restricted to administrators with special permissions.
- *Interoperability:* Facilitates uniform interpretation of object data by various applications.

Schema Modification:

- Sensitive, forest-wide operation requiring careful planning, testing, and coordination.

6.4 Historical limits of domains

In old versions of AD, a single domain could handle up to around 10 million objects. However, these were not strict limits and more of an operational guideline.

For Active Directory Domain Services in Windows Server 2008 and later, Microsoft stated that the maximum supported number of objects in Active Directory is 2.15 billion objects.

There is a limit of $2^{30} \approx 10^9$ billion security identifiers (SIDs) over the life of a domain due to the size of the global relative identifier (RID) pool of 30 bits that makes each SID (that is assigned to user, group, and computer accounts) in a domain unique