Windows Server & Active Directory

By Benjamin Brewster

Why You Need to Care

- Because someday you'll have to:
  - Work at a job somewhere; practically all medium-size businesses and larger use Windows Server in some capacity
  - Restrict users from breaking things
  - Organize and categorize devices and users on your network
  - Know the difference between local and domain accounts

Just Shut Up and Listen For a Moment

- Listen, I know we give Microsoft a lot of grief, for good reason, but...
- Imma let you finish, but Active Directory and Windows Server are some of the best pieces of management software ever written

-Kanye

Some Microsoft History

- Windows had a server all the way back in 1993's Windows NT 3.1 Advanced Server

- Active Directory premiered in 1999 with Windows 2000 Server

- Desktop OS and Server releases generally coincide because of shared code:
  - Windows XP & Windows Server 2003
  - Windows Vista & Windows Server 2008
  - Windows 8 & Windows Server 2012
  - Windows 10 Windows Server 2016

What Windows Server Does

- Runs ***ALL KINDS*** of services:
  - Desktop Services (as in, remote desktops running on the server)
  - Anti-malware via Windows Defender
  - Storage services: file server, replication, backup, RAID, software volume/block drives, etc.
  - Server failover clustering
  - Web proxy server
  - Internet Information Services (web server)
  - Windows Server Containers (managed by Docker!)
- Provides a platform to host AD

What AD Does

- High Level: Manage users, computers, groups, security, and files
- Elements:
  - **Domain Services:** Tracks information about members of the domain, including computers and users; also defines access rights to the devices, files, and services on the domain
  - **Certificate Services:** Generates and maintains a public key infrastructure
  - **Federation Services** (also known as Single-Sign-On, or SSO): Sign in one place, have access to all resources across the domain *and* with other connected services, domains, or technologies
  - **Rights Management Services:** Encrypted file management and access services

AD Domain Services (AD DS)

- Stores information about Computers
  - Security, usability, access rights (per User), network data (with DNS), allowed software, usage hours, etc.
- Stores information about Users
  - Username, password, access rights, other custom directory info, etc.
- Hierarchical: everything can be grouped
- Domains have an extension, because some can be internet visible:
  - Ours is: `cs312domain.local`

AD Domain Services (AD DS)

- PCs are "joined" to a domain by a domain administrator, and then become subject to the Group Policies defined on that domain
  - "Pro" versions of Windows only, not Home!
- PCs cannot leave the domain unless a domain administrator performs the action
  - You have to reinstall Windows if you've lost access to the domain and want to remove the PC from it
  - Domain User directories on the PC become unreadable after leaving the domain
- Local User Accounts can still be used, but the PC is still subject to Group Policies

Certificate Services (AD CS)

- This is a full-on Certificate Authority system
- Certs are given to authenticate websites, documents, and other communications

- Group Policies can control who gets access to which certs

- Certificates tend to expire, and take bandwidth to fetch: AD CS provisions and renews certificates automatically for the PCs connected to it

Federation Services (AD FS)

- Federation means that your login is accepted outside of the typical scope for which it was defined.
- Common examples are the use of your Google or Facebook accounts to access an untold number of services online, or how we use ONID here at OSU for even our external services

1. You first login to AD, and receive authentication token A; token A can be used anywhere in your AD domain
2. When you try to log in to a federated service, that service receives your token A, sends it to your original AD server for verification, then allows you to log in, giving you token B; token B can be used anywhere in the federated service

Rights Management Services (AD RMS)

- This is a built-in system for encrypting files, and for keeping the decryption and viewing of those files restricted, based on User permissions set in AD

- Documents can even be set to be decrypted only in certain environments, under certain conditions, for specific periods of time...

- Because it's specific to certain file formats only, like Office; this is very much an application extension

Our Windows Server 2016 VM

- Going to want to set 4GB of RAM and 2 or 3 processor cores
- Occupies 10GB of space
- Has a dedicated router for the network (pfSense, no DHCP on LAN)
- I have installed Windows Server 2016 plus the following actions:
  - Disabled automatic updates using sconfig (a cmd line tool)
  - Set static IP
  - Added AD DS Role (plus the other dependencies; auto-adds DNS to itself, which isn't too surprising, since AD DS is all about being a directory)
  - Set up Domain as CS312DOMAIN
  - Added DHCP server for the LAN

Windows Server 2016 Hands-On

Say

- Here's Windows Server 2016!

Demonstrate

- Boot:
  - WinServer2016Router
  - WindowsServer2016_Reference
  - Win10_DomainPC

- When booted, the first thing we see is that it looks like Windows 10, and acts like it
- Note that the login is of the form DOMAIN\USERNAME
- The web browser is fairly locked down - you have to add lots of security exceptions, or disable the entire "protected access" thing.
  - On the other hand, you shouldn't be browsing the web on a server
- The Server Manager, which gives us access to all the roles installed, shows us the status of everything

- Show Roles on left side of Server Manager, click on a few

Windows Server 2016: DHCP

Say	Demonstrate
• Let's look at the DHCP Server	• Tools -> DHCP • Drill down: DHCP -> <server> -> IPv4 -> Scope
• This is the range of dynamic addresses • This is who has an address already • Let's reserve our PC! • This reserves that IP as a reservation: note that in Windows, this address is kept in the pool (reducing your pool side), while in pfSense, this reservation must be for an address outside the pool (which keeps the pool size the same)	• Examine Address Pool • Examine Address Leases • Reservations is for reserved dynamic addresses • Right-click PC in Leases, Click Add Reservation
• Scope Options lists the default gateway (here called "Router"), DNS Servers, and DNS Domain Name that are handed out to clients when they register via DHCP	• Click Scope Options • In PC, run "ipconfig /all" at command line, show these values have been acquired

Windows Server 2016: DNS

Say

- Let's look at the DNS Server
- Here is the actual A record that maps the server name (win-h9bs8biaqkf) to its IP address (192.168.1.2)
- There is a LOT of complexity to DNS that we don't have time to go into, but you can dig into this to find the SRV records that inform clients where various servers can be found: all these entries point to this server

Demonstrate

- Tools -> DNS
- Drill down: DNS -> <server> -> Forward Lookup Zones -> cs312domain.local

Windows Server 2016: Joining the Domain

Say

- We can join the domain, and then control the PC from the domain controller (our server)

- Search for System

- Now, we change domain ownership!

- This only works if DNS is set up correct on the server, and this PC is getting its address info from the server

Demonstrate

- Search for System -> Advanced system settings -> Computer Name tab
- Click Change... button
- Select "Domain" in "Member of" control
- Type in name of Domain: "CS312DOMAIN"
- Enter Domain Administrator credentials:
  - u: CS312DOMAIN\Administrator
    p: Password!
- Click OK and cross your fingers
- Click the OK button of victory!
- Restart

Windows Server 2016: Remote Management

Say

- We can connect from another server to manage our reference server
- Log in first as a user with rights to administrate; you can log in as any user (by default) to domain-connected computers!
- First, I've opened up a few ports on the server (which ones to open is given to you by the software when you try to use them)
- Then, I've downloaded and installed the Remote Server Administration Tools from Microsoft
- Lots of Groups are in here, but really one Domain User: the Domain Administrator. This super-ultra-admin account can do anything anywhere, on any part of the domain.

Demonstrate

- Log in to Windows 10 PC as the Domain Admin
- Start -> Windows Administrative Tools -> Active Directory Users and Computers
- Expand down to Users

Windows Server 2016: Create a Domain User

Say

- Let's create a Domain User
- Domain Users can log in anywhere, but local user accounts are per-machine.
- You can still have local machine Administrator accounts that can do anything to the non-Domain accounts, and to the computer itself

Demonstrate

- Action -> New -> User
- Fill in details, hit Next
- Enter "Password!" as the password, uncheck "User must change password...", hit Next
- Hit Finish
- Log Out
- Switch to "Other User" in the lower left
- Log in as new user

- Note that the new user can't do jack, unless you log in as an Administrator, log in as a user who can do just that one task, or elevate the new user's permissions.

- Try to run Command Prompt as Administrator

Conclusion

- Active Directory and Windows Server are excellent - don't underestimate these products and the good that they do!

- One of the most important perks you get with a domain of PCs is that the Users are much less likely to be able to do damage to their systems: this might be the most important factor of them all