Domain Controller Configuration

Pretty much every organization I've worked with has leveraged an Active Directory Domain in some at least some capacity. Active Directory (AD) is a centralized database for managing users and computers in a company's network. Both of these can be added to groups and used to assign permissions, centrally control identities which can be tied into authentication using various components, set minimum password requirements, and leverage Group Policy which allows you to manage thousands of settings to ensure a consistent experience without manually configuring them.

A domain needs to have at least one Domain Controller (DC) which runs the Active Directory Domain Services role. Ideally two or more will exist for redundancy and load balancing. At the most basic level, getting a domain set up involves installing the role through PowerShell or the Add Roles and Features wizard. Once completed, the server needs to be promoted to a domain controller which can also be done through a wizard where you can either create a new domain and forest, set the functional level, and get things up and running. The local Administrator account gets converted to your first Domain Administrator account and once the server reboots at the end of the process, you have a functioning domain. DNS will need to be configured for clients to find the domain controller and allow other servers and workstations to be joined to the domain.

To install the necessary roles:

1. Log into the server and Launch Server Manager.
2. Go to Manage > Install Roles and Features.
3. Click Next until you can select the roles and select Active Directory Domain Services and DNS Server (install management tools as well).
4. Before clicking on Install, you can export the configuration settings to an .xml file which can be imported on future systems with `Install-WindowsFeature -ConfigurationFilePath c:\example\configuration.xml`.

Alternatively, the roles can be installed entirely through PowerShell without the .xml file. The name of the features can be obtained by running `Get-WindowsFeature` which will also confirm which are installed.

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
Install-WindowsFeature -Name DNS -IncludeManagementTools
```

Once the roles are installed, Server Manager will show a ! in Notifications stating configuration is required for ADDS on the DC with a link to the DC Promo wizard. To do this through the UI:

1. Select Add a new forest as this is the first server in the domain. Specify the fully qualified root domain name (domain.com or domain.local). There is plenty of debate whether this should be an internet routable domain or not and both have their advantages but as this is a lab I'm not worried.
2. Select the Forest/Domain Functional level. This controls which features are available and despite there being a Server 2019 and Server 2022 released, Server 2016 is the latest new functional level. This should be the latest unless there are older servers which are no longer supported. The Directory Services Restore Mode (DSRM) password also needs to be specified. This is hopefully something never needed as it helps recover a corrupt database and do other offline maintenance. It is one of those things that should be documented and secured well in hopes it is never needed. This can be changed later using ntdsutil.
3. Skip setting up DNS delegation.
4. Verify the NetBIOS domain (the short name).
5. Leave the default locations for the database, log, and SYSVOL folders.
6. Click Next through the rest of the wizard until you can select Install.
7. The server will reboot automatically upon completion. You can no longer sign in with the local account which is now your Domain Administrator.

Again, this can also be exported to a PowerShell file that can be used instead of the wizard. This will prompt for the DSRM password and will also reboot automatically upon completion.

```
Import-Module ADDSDeployment
Install-ADDSForest -CreateDNSDelegation:$false -DatabasePath "C:\Windows\NTDS" -DomainMode "WinThreshold" `
  -DomainName "DOMAIN.LOCAL" -DomainNetbiosName "DOMAIN" -ForestMode "WinThreshold" `
  -InstallDNS:$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$fasle `
  -SysvolPath "C:\Windows\SYSVOL" -Force:$true
```

Revision #4
Created 30 December 2023 00:00:12 by Matthew B.
Updated 30 December 2023 03:13:05 by Matthew B.