

Deploying Active Directory

Written by Tyler Weiss

Deploy Active Directory (GUI)

In this exercise, you'll deploy Active Directory (AD) on Windows Server 2019, capturing the essence of creating a Windows Domain. Along the way, take at least four screenshots to document key moments.

After deployment, reflect on the process in a brief narrative. Discuss the purpose of each step, highlighting the role of AD in centralizing domain management and enhancing network security. Your explanation should tie the screenshots to the deployment stages, offering insights into the significance of each action and its impact on the network environment.

This reflection will demonstrate not only your technical capability but also your understanding of AD's pivotal role in network infrastructure.

Exercise 1 uses the writeup:

<https://petri.com/how-to-install-active-directory-in-windows-server-2019-server-manager/>

Exercise 2 uses the writeup:

<https://petri.com/how-to-install-active-directory-in-windows-server-2019-using-powershell/>

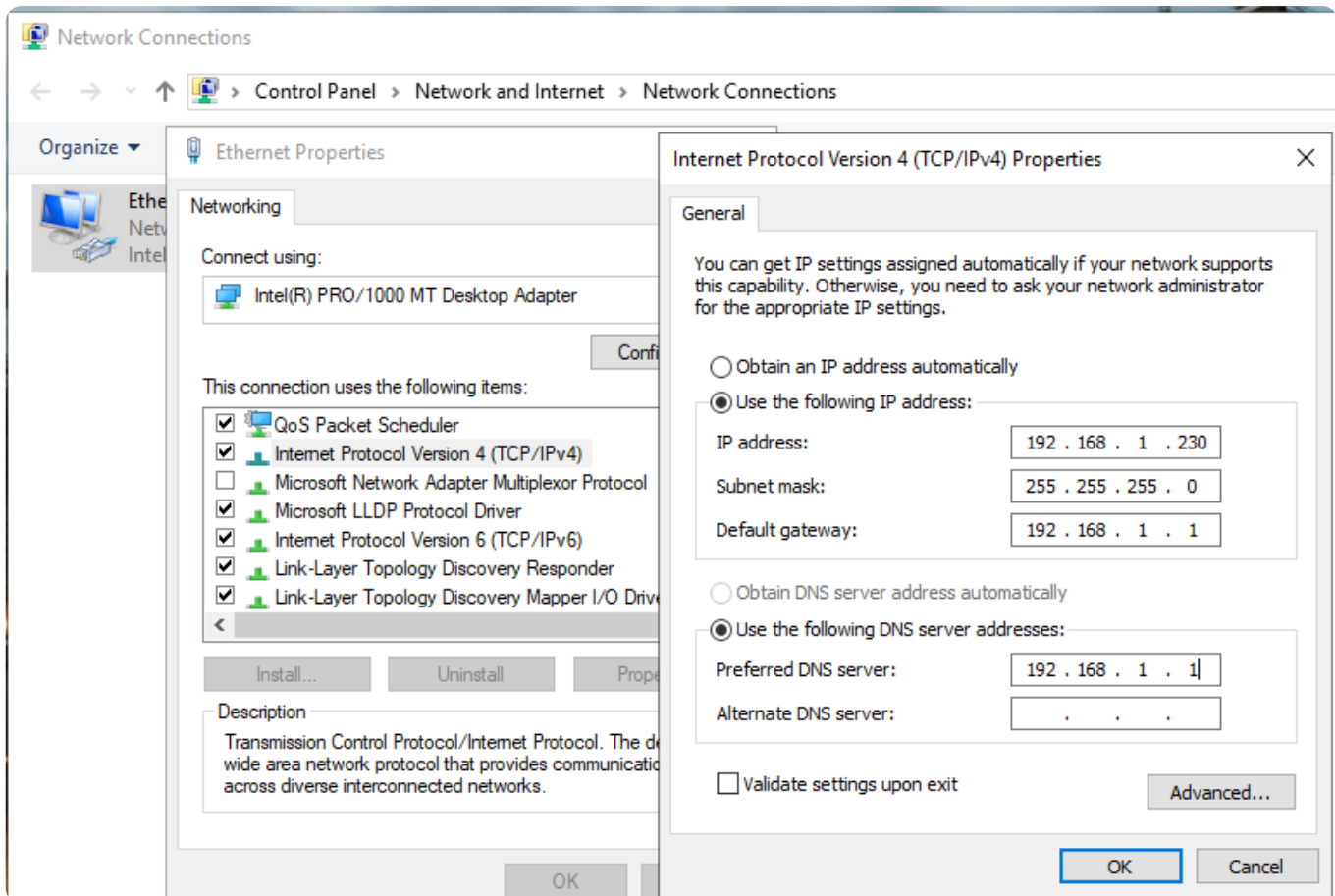
Exercise 1

Two major steps are involved in the setup process. First is the installation of Active Directory Domain Services (AD DS). The second is the setup of the Domain Controller (DC). A Domain must have at least one DC to manage the Domain. In this exercise the the server we are installing AD DS on will also be the first DC in the domain.

The first step when installing Active Directory Domain Services and setting up the Domain Controller is to set a static IP address and rename the server. It's important for the

Domain Controller to have a reserved IP address so that the Domain Controller can be accessed reliably.

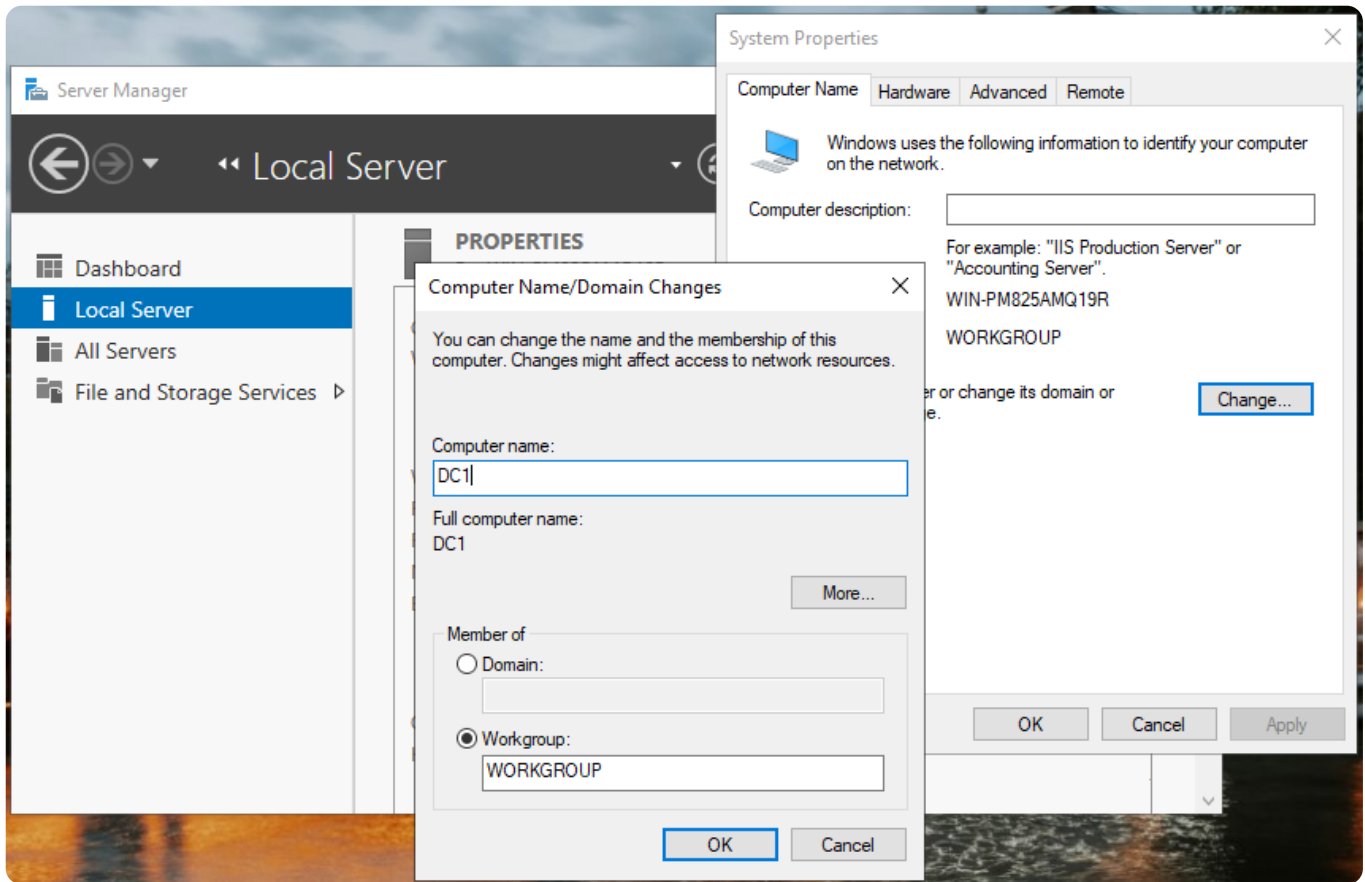
Open the 'Network and Internet' settings window. Click on 'Change adapter options'. Right click on the network the network interface and choose properties on in the menu. Select 'Internet Protocol Version 4' and click the 'Properties' button. Select the 'Use the following IP address' radio button. If the network is using DHCP, choose a static IP address that is outside of DHCP range. Input the subnet mask, default gateway and DNS server of the network. Click the okay and close in the windows to save the settings. All the above information can retrieved using `ipconfig /all` in the command prompt.



The server, which will also be the first DC in the domain, needs to be renamed to something that makes sense. In this example the servers name will be 'DC1'.

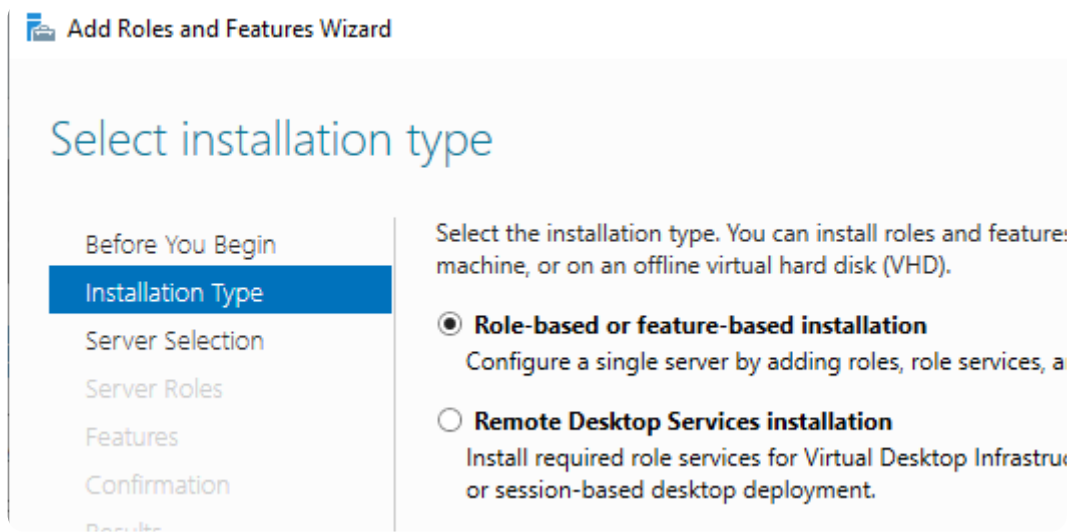
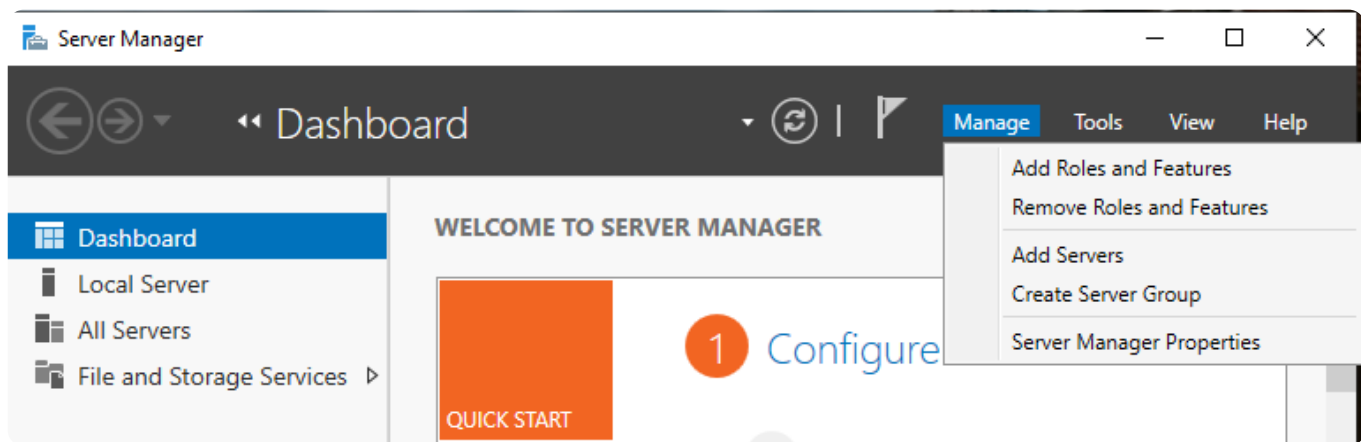
Open the 'Server Manager' and select 'Local Server'. Click the 'Computer Name'. Click the 'Change' button and Input the new computer name then click 'OK'. A popup alert will appear informing you that the computer needs to be restarted for the changes to take place. Click 'OK' and close the 'System Properties' window. Click 'Restart Now' in the

popup dialog.



The next step is to install Active Directory Domain Services. Installing AD DS on the local server will allow it to be connected and managed by an active directory. AD DS will allow the management and organization of objects and members. It is the set of software that facilitates the hierarchical relationships between the objects within a domain or forest so that they can be managed.

Sign in to the server with the Administrator account and open the 'Server Manager'. Click manage and choose 'Add Roles and Features' in the drop down menu. Make sure the 'Role-based or feature-based installation' radio button is selected.



Adding features and roles will allow the selection of a server and what applications to install on it. We will be installing Active Directory Domain Services.

Select the server from the server pool in 'Server Selection'. Select the 'Active Directory Domain Services' role along with 'Include management tools (if applicable)'. Click 'Add Features'.

Read the information under 'AD DS' and proceed to 'Confirmation'. Click 'Install'.

Active Directory Domain Services

DESTINATION SERVER
DC1

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS


Confirmation

Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.



Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

[Learn more about Azure Active Directory](#)

[Configure Office 365 with Azure Active Directory Connect](#)

Before You Begin

Installation Type

Server Selection

Server Roles


Features

AD DS

Confirmation

Results

View installation progress

 Feature installation

Configuration required. Installation succeeded on DC1.

Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

[Promote this server to a domain controller](#)

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

Active Directory module for Windows PowerShell

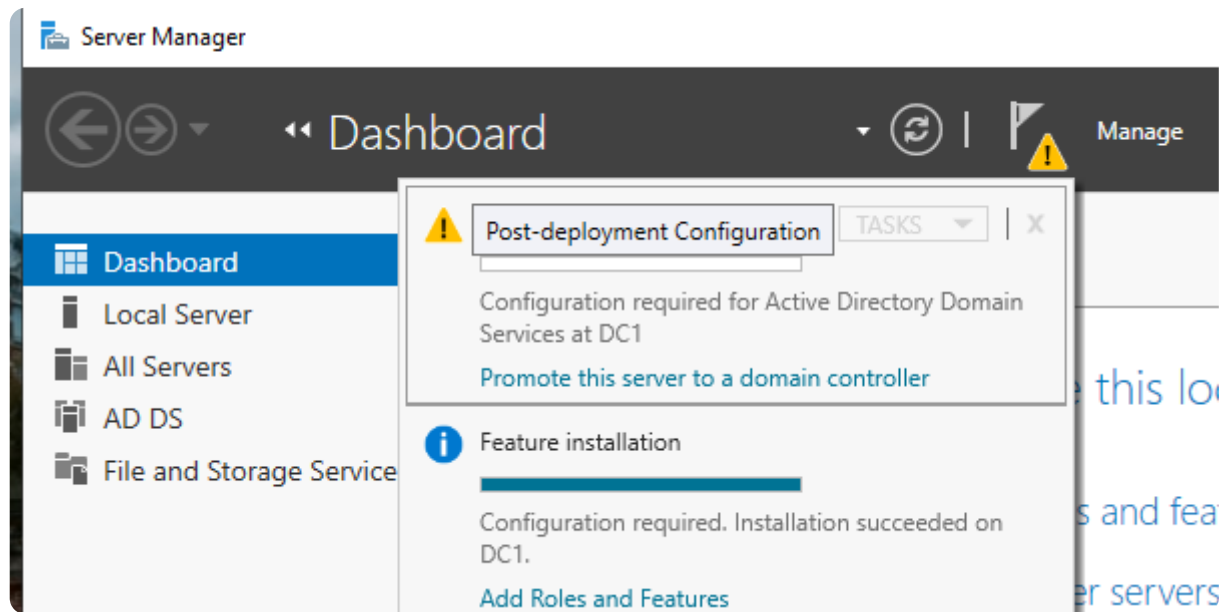
AD DS Tools

Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools

The next step is to configure AD DS on the new DC which will the define a Forest and a Domain. The DC actually facilitates the centralized management and network access of a

domain. Under alerts choose 'Promote this server to a domain controller'.



Under 'Deployment Configuration' select 'Add a new forest' enter the 'Root domain name'. You should own the top level domain (TLD) but in this example 'controller.com' will be used. Under 'Domain Controller Options' enter a restore password. This password can be used to take the server offline for emergency maintenance, particularly restoring backups of AD objects. Notice that the DC will also serve as the Domain Name System (DNS) server.

Deployment Configuration

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

- ☐ Add a domain controller to an existing domain
- ☐ Add a new domain to an existing forest
- ☒ Add a new forest

Specify the domain information for this operation

Root domain name:

contoller.com

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level:

Windows Server 2016

Domain functional level:

Windows Server 2016

Specify domain controller capabilities

- ☒ Domain Name System (DNS) server
- ☒ Global Catalog (GC)
- ☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

••••••••••

Confirm password:

••••••••••

Under 'Additional Options' review the NetBIOS domain name and click 'Next'. The NetBIOS domain name is typically the TLD and will be used as the Domain reference when logging in to the network. Review each section and click 'Next'. Once the prerequisite checks are passed click 'Install'. After the installation the server will automatically restart.

Deployment Configuration	Verify the NetBIOS name assigned to the domain and change it if necessary
Domain Controller Options	The NetBIOS domain name: <input type="text" value="CONTROLLER"/>
DNS Options	
Additional Options	
Paths	
Review Options	
Prerequisites Check	
Installation	

All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#)

Deployment Configuration	Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Domain Controller Options	Rerun prerequisites check
DNS Options	View results
Additional Options	<div> Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions. For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751). A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "contoller.com". Otherwise, no action is required.</div>
Paths	If you click Install, the server automatically reboots at the end of the promotion operation.
Review Options	More about prerequisites
Prerequisites Check	
Installation	
Results	

After the server reboots sign-in to the domain administrator account. The domain name preceding the account name show that a user is now logging into the domain

'CONTROLLER'.



Deploying Active Directory (Powershell)

For this assignment, you will set up Active Directory (AD) on Windows Server 2019 using PowerShell commands, giving you hands-on experience with the command line interface. Make sure to take screenshots of each command you use and the success message at the end showing that AD is deployed.

Along with your screenshots, write a short explanation for each PowerShell command you used. Talk about what each command does and why it's important for setting up your Windows Domain. This part of the assignment will show that you not only know how to do the task but also understand what each step is for.

Exercise 2

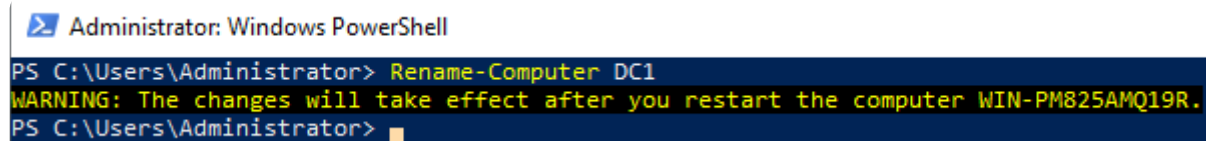
The previous exercise has a more in-depth description of each step of the deployment process so I will instead be referencing the descriptions in exercise one, assuming that exercise 1 has been reviewed by the reader. I will however restate the following.

Two major steps are involved in the setup process. First is the installation of Active Directory Domain Services (AD DS). The second is the setup of the Domain Controller (DC). A Domain must have at least one DC to manage the Domain. In this exercise the the server we are installing AD DS on will also be the first DC in the domain.

As stated in the previous exercise we need to set a proper name for the server, which will be our Domain Controller (DC), and a static IP address to make the server reliably available to the AD forest.

Type the following command in powershell to rename the server to 'DC1' or which ever name you choose then restart the server.

```
Rename-Computer -NewName DC1
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Rename-Computer DC1
WARNING: The changes will take effect after you restart the computer WIN-PM825AMQ19R.
PS C:\Users\Administrator> █
```

Once logged back in set a static IP address for the server. Type the following command using a proper reserved IP address from your own network. The '--PrefixLength' option is the length of the subnet mask. Note that the network adapter interface is referenced by index. The 'Get-NetAdapter' cmdlet and method 'InterfaceIndex' allows retrieval of this information.

```
New-NetIPAddress -IPAddress 192.168.1.230 -DefaultGateway 192.168.1.1 -
PrefixLength 24 -InterfaceIndex (Get-NetAdapter).InterfaceIndex
```

```

PS C:\Users\Administrator> Get-NetAdapter

Name                InterfaceDescription          ifIndex Status    MacAddress          LinkSpeed
-----                -
Ethernet            Intel(R) PRO/1000 MT Desktop Adapter      8 Up          08-00-27-6B-FD-E7 ...ps

PS C:\Users\Administrator> (Get-NetAdapter).InterfaceIndex
8

PS C:\Users\Administrator> New-NetIPAddress -IPAddress 192.168.1.230 -DefaultGateway 192.168.1.1 -PrefixLength
24 -InterfaceIndex (Get-NetAdapter).InterfaceIndex

IPAddress           : 192.168.1.230
InterfaceIndex      : 8
InterfaceAlias       : Ethernet
AddressFamily        : IPv4
Type                 : Unicast
PrefixLength         : 24
PrefixOrigin         : Manual
SuffixOrigin         : Manual
AddressState         : Tentative
ValidLifetime        : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime    : Infinite ([TimeSpan]::MaxValue)
SkipAsSource         : False
PolicyStore          : ActiveStore

IPAddress           : 192.168.1.230
InterfaceIndex      : 8
InterfaceAlias       : Ethernet
AddressFamily        : IPv4
Type                 : Unicast
PrefixLength         : 24
PrefixOrigin         : Manual
SuffixOrigin         : Manual
AddressState         : Invalid
ValidLifetime        : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime    : Infinite ([TimeSpan]::MaxValue)
SkipAsSource         : False
PolicyStore          : PersistentStore

PS C:\Users\Administrator>

```

Using 'hostname' and 'ipconfig' verifies that the proper changes have been made.

```

PS C:\Users\Administrator> HOSTNAME.EXE
DC1
PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f48f:8a48:4fc9:1a65%8
    IPv4 Address. . . . . : 192.168.1.230
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
PS C:\Users\Administrator> █

```

Set the preferred DNS server. If this is the going to be the DC then set use the IP address of the DC. The DNS server for my network happens to be '192.168.1.1'.

```

Set-DNSClientServerAddress -InterfaceIndex (Get-
NetAdapter).InterfaceIndex -ServerAddresses 192.168.1.1

```

```
PS C:\Users\Administrator> Set-DNSClientServerAddress -InterfaceIndex (Get-NetAdapter).InterfaceIndex -ServerAddresses 192.168.1.1
```

The next step is to install Active Directory Domain Services (AD DS). The previous exercise describes the purpose of the AD DS installation and what this collection of software does. The name of the 'WindowsFeature' that will be installed is 'AD-Domain-Services' and the option '-IncludeManagementTools' makes sure management tools are added as well.

```
Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools
```

```
Start Installation...
24%
[ooooooooooooooooooooooooooooo]

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f48f:8a48:4fc9:1a65%8
    IPv4 Address. . . . . : 192.168.1.230
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
PS C:\Users\Administrator> Set-DNSClientServerAddress -InterfaceIndex (Get-NetAdapter).InterfaceIndex -ServerAddresses 192.168.1.230
PS C:\Users\Administrator> Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools

PS C:\Users\Administrator> Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
-----
True      No              Success      {Active Directory Domain Services, Group P...
```

The last step is to configure the DC in a new AD Forest. In the prior exercise we accomplished this by clicking on the alert flag in the Server Manager Interface and selecting 'Promote this server to a domain controller'. As previously stated the '-DomainName' would be the Top Level Domain (TLD) with the root domain and the '-DomainNetBIOSName' usually your TLD. The NetBIOS Name will be name used to reference the domain which you will see on the login screen once the AD is properly deployed. You will be asked to input a 'SafeModeAdministratorPassword'. For information on what this password is used for refer to exercise 1 but just keep in mind that this password is extremely important. Once the password is input after running the following command type 'Y' to continue configuration of the AD forest.

```
Install-ADDSForest -DomainName controller.com -DomainNetBIOSName CONTROLLER -InstallDNS
```

```
PS C:\Users\Administrator> Install-ADDSForest -DomainName controller.com -DomainNetBIOSName CONTROLLER -InstallDNS
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
```

```
PS C:\Users\Administrator> Install-ADDSForest -DomainName controller.com -DomainNetBIOSName CONTROLLER -InstallDNS
SafeModeAdministratorPassword: *****
```

Install-ADDSForest

Validating environment and user input

All tests completed successfully

[oo]

Installing new forest

Configuring the DNS Server service on this computer...

For more information about this setting, see Knowledge Base article 942564
(<http://go.microsoft.com/fwlink/?LinkId=104751>).

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "controller.com". Otherwise, no action is required.

WARNING: Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564
(<http://go.microsoft.com/fwlink/?LinkId=104751>).

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "controller.com". Otherwise, no action is required.

After the AD Forest and DC are configured the server will automatically restart.



Notice the difference in time saved using powershell vs the GUI. For a better insight and description the the AD deployment process the GUI method may be more beneficial. On

the other hand, using powershell is obviously much faster and simpler but you have to know what you want to do exactly. Choose which method most supports your needs.