

# Building an Active Directory Lab - Part 1

---

blog.spookysec.net/ad-lab-1

05 Nov 2021

Have you ever done an Active Directory machine on TryHackMe, HackTheBox, Pentester Academy, or any other platform and thought, “Huh, that was really fun!”?

Well, I certainly have. One of Penetration Testing’s most interesting topics (to me) is Active Directory. New security flaws are being discovered every day, this makes it incredibly useful to have an environment on-hand already built out. To do this, you’re going to need several things on hand, let’s go over them real quick:

- A Windows Server ISO
- A Windows Client ISO
- Virtualization Software
- Organization

## Windows Server/Client ISO

These are relatively easy to acquire, you can do so with the Microsoft Evaluation Center. This can be found at the following URL:

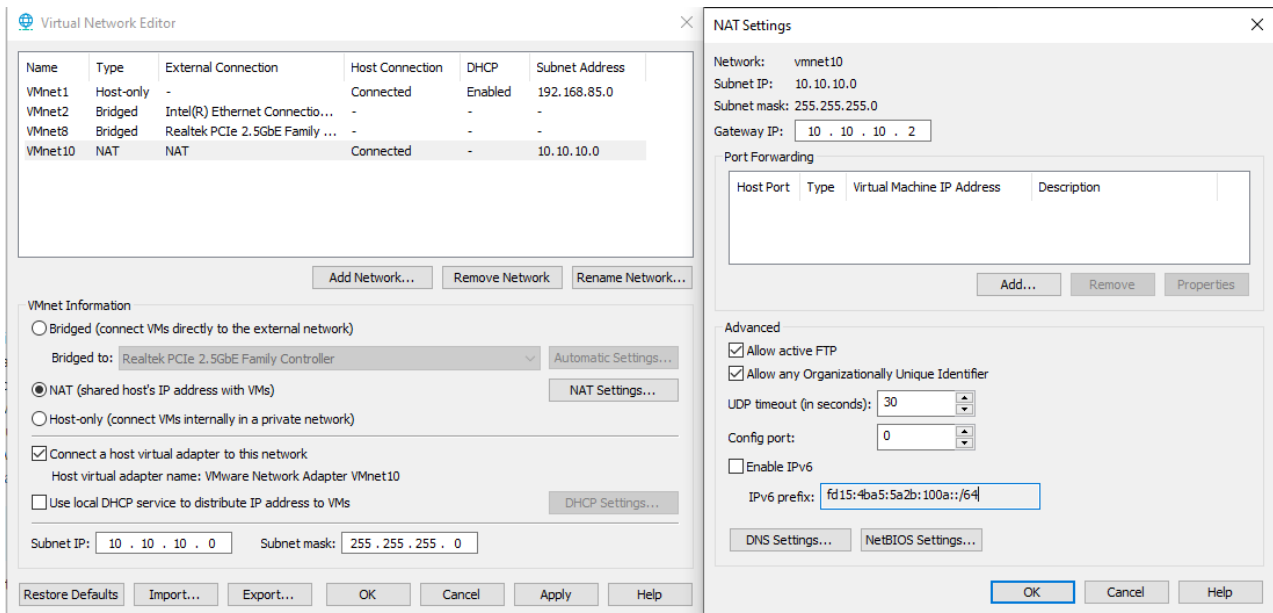
<https://www.microsoft.com/en-us/evalcenter/>

At the time of writing, you can download either Windows 10 or 11, or Server 2019 or 2022. These are completely **free** to download, and have a trial range between **180** and **90** days. However, it is possible to extend this trial with the `slmgr /rearm` command. This is a general reminder – these devices are not designed to be used in a production environment. It is highly recommended that you download Server 20XX first. Setting up an Active Directory Environment is generally the same across all Windows Server versions. For the purpose of this post, I will be using Windows 10 and Server 2019.

## Virtualization Software

This is another key thing that you should have – It is not *required*, you can use real metal, but this will take a considerably amount of time. I will personally be using VMWare Workstation, but just about any virtualization software will work as long as you can add VMs into an isolated network.

I have done this by creating a “NAT” network in the 10.10.10.0/24 Subnet with a Default Gateway of 10.10.10.2.



I have went ahead and disabled DHCP, this is because DHCP will be handeld by Active Directory Sites and Services. We will go into this in detail a little bit later.

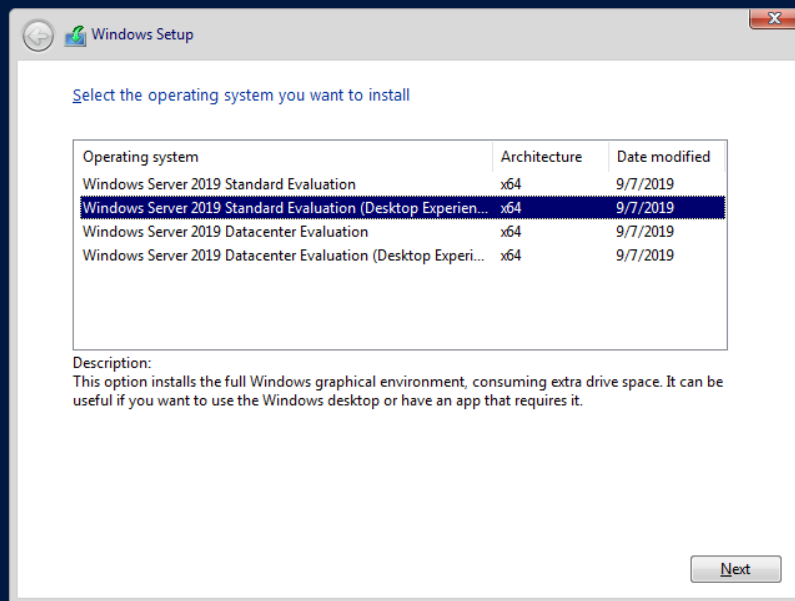
## Organization

This is arguably the most important thing; having an Active Directory environment is good, but if you can't remember the credentials for anything, can't remember the IP Addresses, or don't remember your chosen naming scheme, you're gonna have a bad time. I highly recommend keeping credentials for your Lab environment in someplace like a KeyPass vault or a Spreadsheet.

## Installing Windows Server

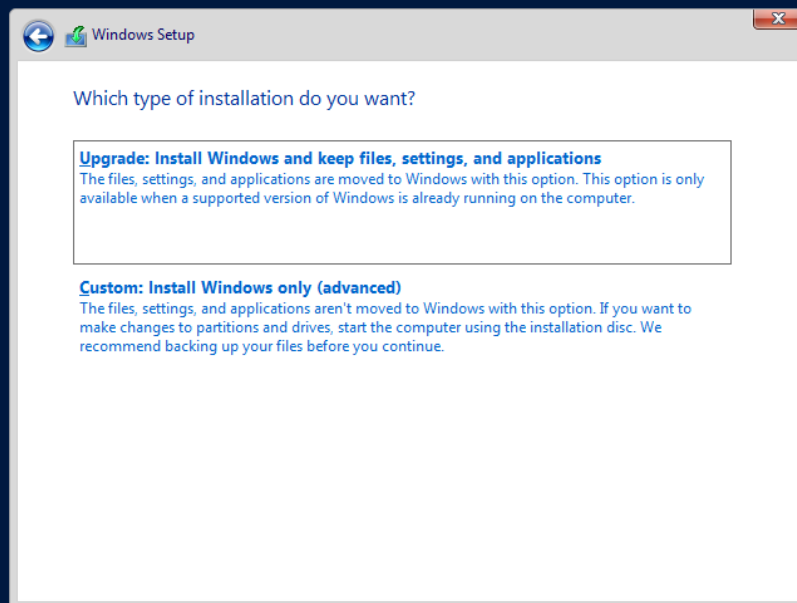
The Windows Server install and setup process is relatively straight forward, because Windows Server is running, it means that the device can run on a lot less hardware resources. In fact, an Enterprise Domain Controller can run on roughly 2 CPU Cores, 8GB of RAM, and 90-120GB of Disk Space for approximately 20,000 users and computers.

After inserting the ISO and powering on the Virtual Machine, you will be presented with 4 or so options, it is very important which one you pick – two are labeled “Desktop Experience” and two are not. If you're comfortable with managing the device via Powershell, it's okay to choose this option, however, it's not for the faint of heart. I highly recommend choose “Standard Evaluation”, depicted below.



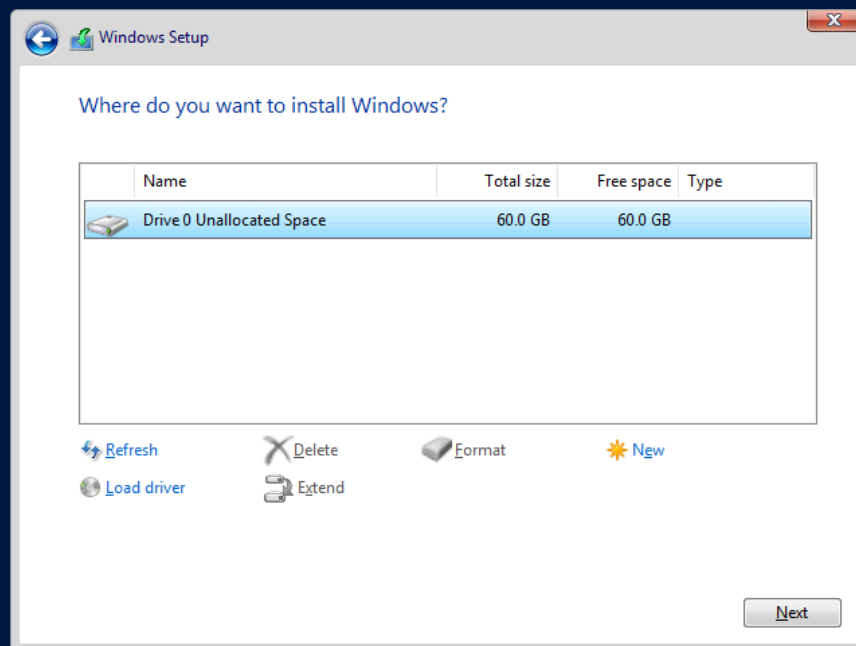
1 Collecting information 2 Installing Windows

Afterwards, you will be brought to the Microsoft “Terms and Conditions” screen, it’s important to be aware of these terms because it is a trial, generally if you do not use this device for production services, you will be fine.



1 Collecting information 2 Installing Windows

Next up, we will be presented with the Installation type, here we want to choose “Custom: Install Windows only (Advanced)”. You will be brought to the Windows Disk Partitioning screen. Here, you should see “Drive 0 Unallocated Space”, if you don’t, click “Delete” on each partition, then click “Next”.



1 Collecting information

2 Installing Windows

Lastly, Windows will begin installing. After the installation finishes, Windows will reboot and you will be presented with a screen to enter the Administrator Password. This is where you should start your Password table.

## Customize settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name	<input type="text" value="Administrator"/>
Password	<input type="password"/>
Reenter password	<input type="password"/>

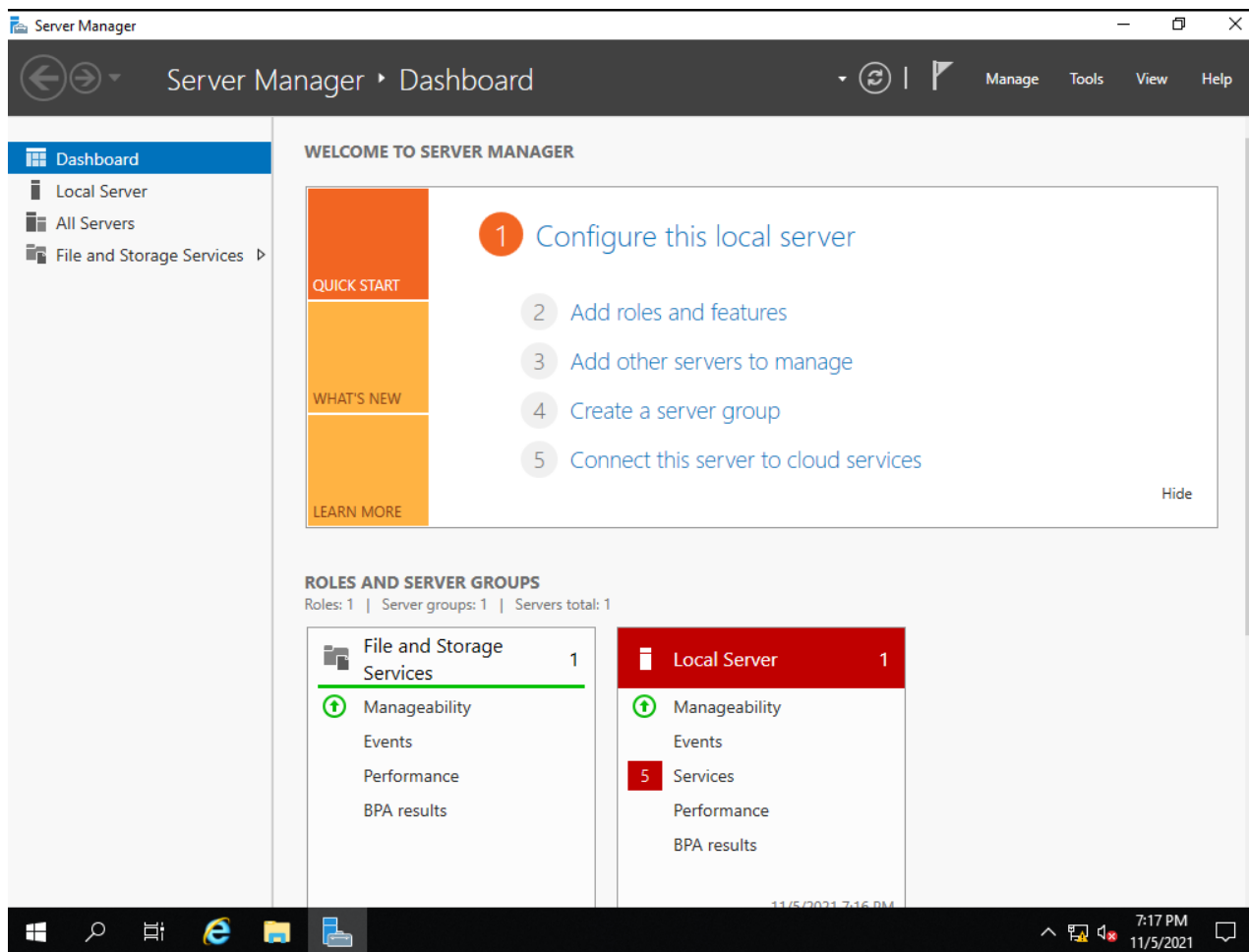


Finish

Username	Password
----------	----------

Administrator	S3cur3P@ssw0rd123!
---------------	--------------------

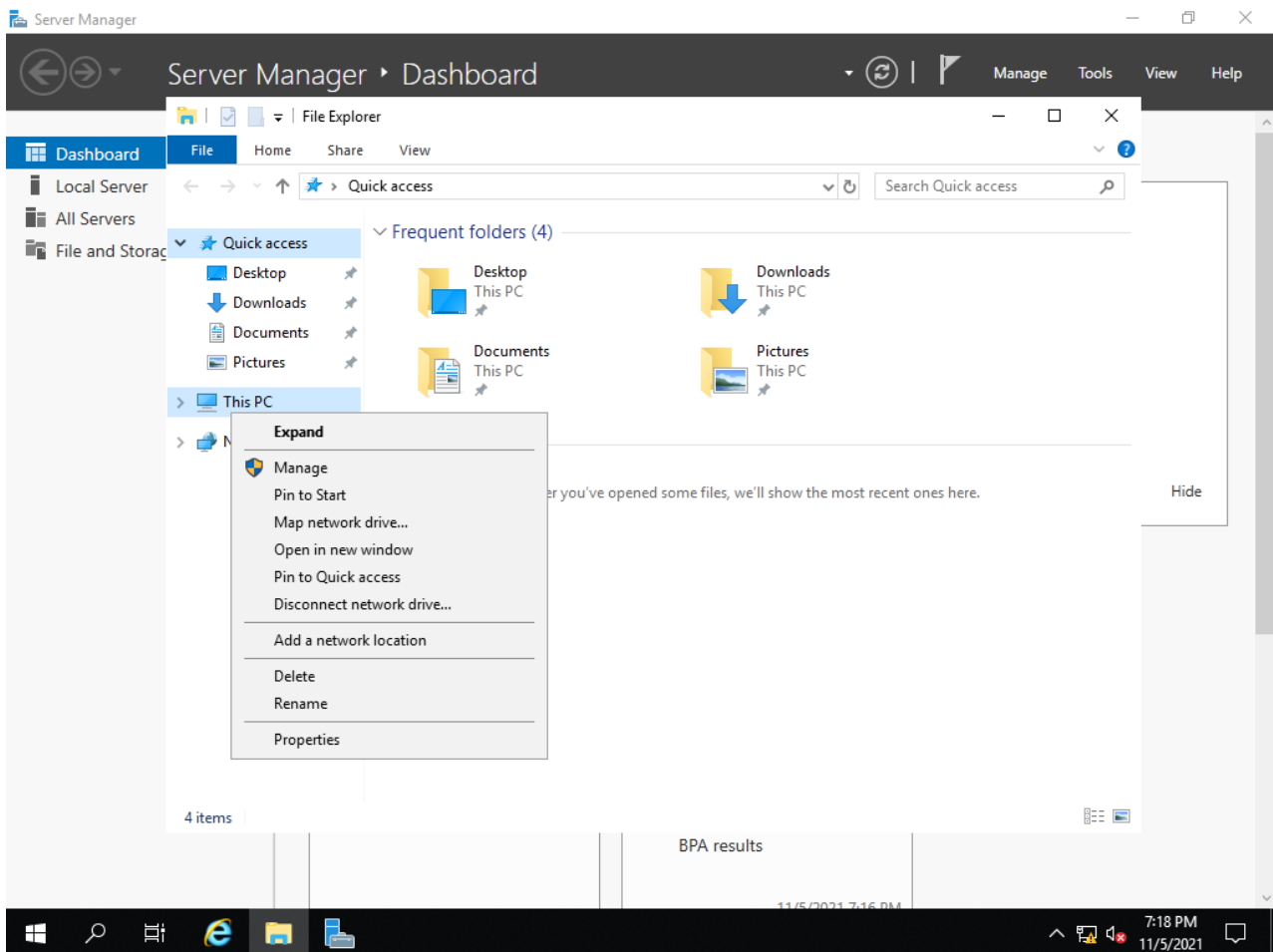
After entering the new Password, you will be brought to the login screen. Enter your password and the installation will finally be finished!



## Building out the Server

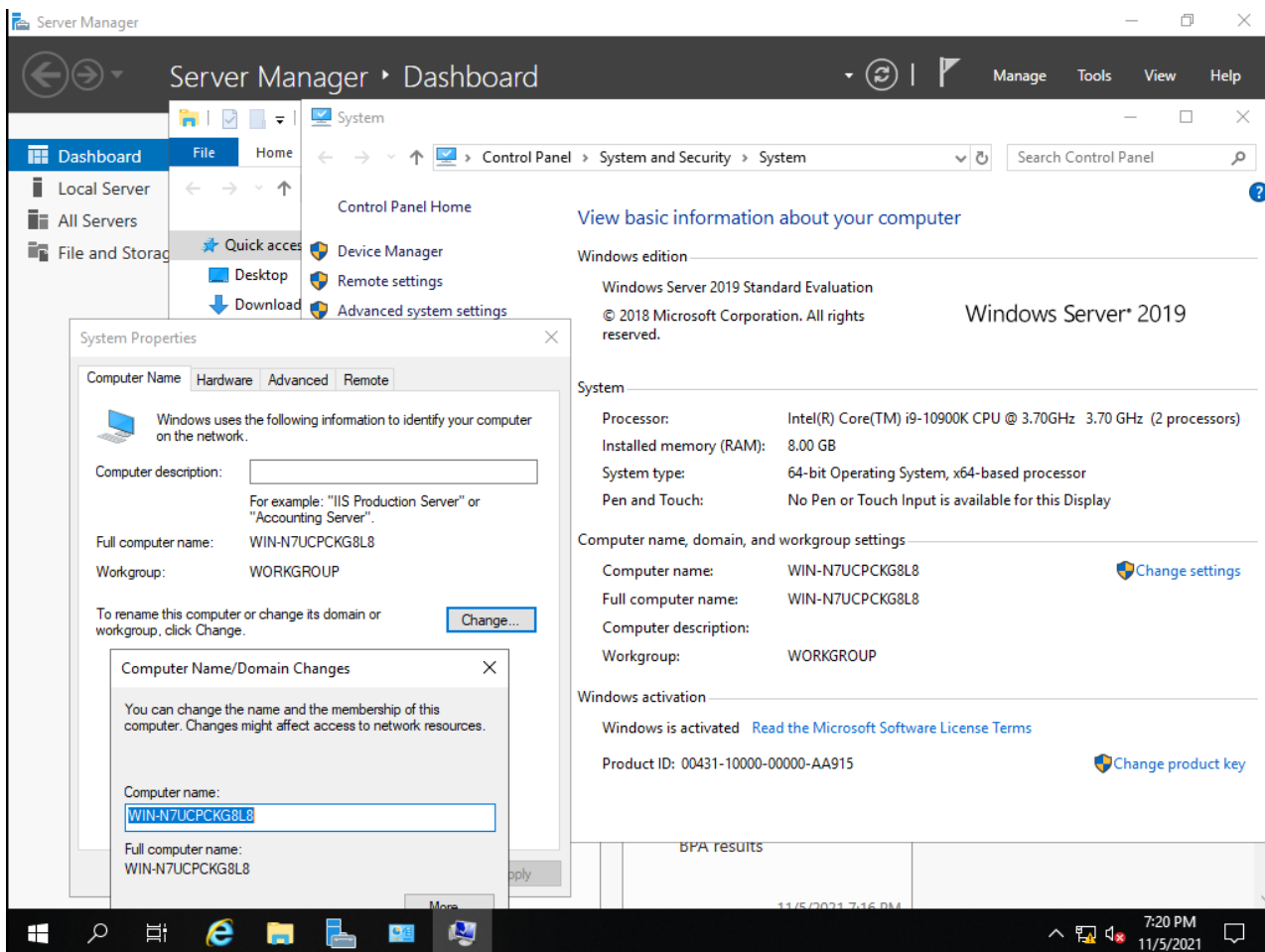
### Naming your Devices

To start, we're going to reconfigure the Hostname as well as configure the Networking settings on the DC. To start, open the File Explorer, right click on "This PC", and click "Properties".



This will bring you to the “System Settings” panel, here we can update the Hostname of the device by clicking “Change Settings” next to “Computer Name, Domain, and Workgroup settings”. Next, click “Change” next to “To rename this computer or change its domain or workgroup, click Change”.





Here, you can update the hostname to whatever you please. Note: It's incredibly important to set a good naming scheme. Here, you want it to be both descriptive and meaningful. Generally, if this is **not** a lab, you want to create a naming scheme that represents the location of the device type, the device location and the device number.

For example:

SRV-GAVATLDC01

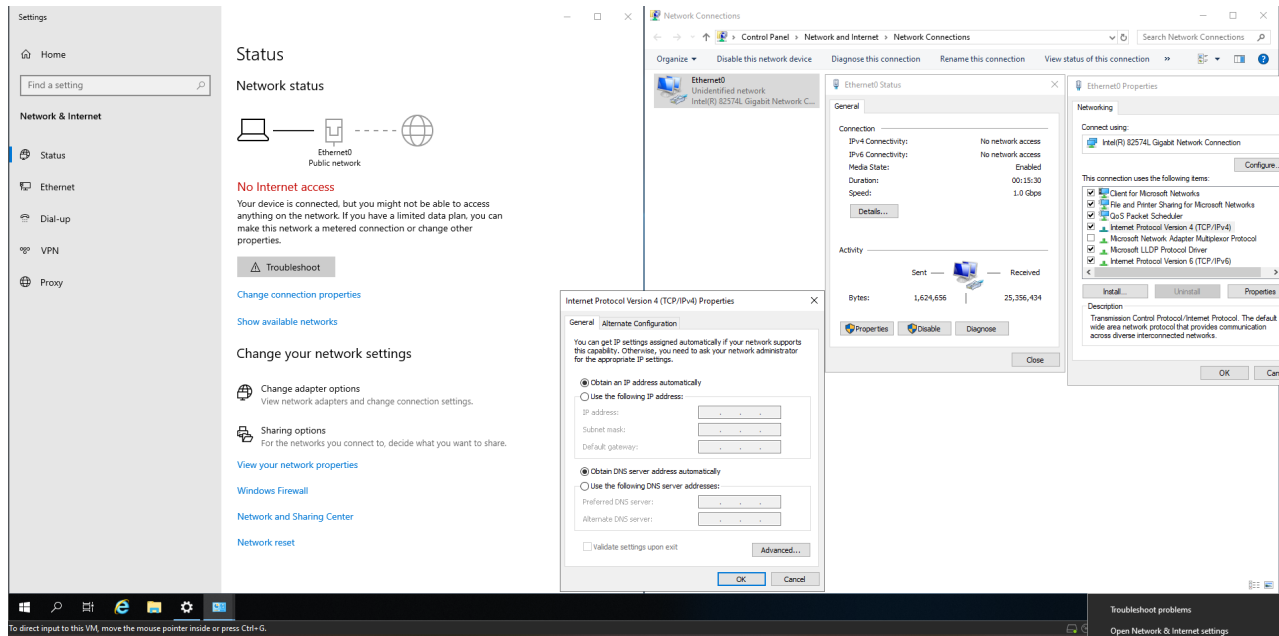
This breaks down to the following:

- Device Type: SRV (Server)
- State: GA (Georgia)
- Device Characteristics: V (Virtualized or Physical)
- City: ATL (Atlanta)
- Device Type: DC (Domain Controller)
- Device Number: 01

Once again, for the purpose of the lab, we can arbitrarily name devices, but if you're training to become a System Administrator, it's immensely important to establish a good naming scheme that works for you. We're going to follow the K.I.S.S. methodology – Keep It Simple Stupid and name our device SRV-DC01.

## Configuring Network Settings

After this is done, we're going to establish the Network Settings on the VM. To do so, right click on the Network Adapter and click on "Open Network and Internet Settings", click "Change Adapter Options", double click on the Ethernet Interface, and click "Internet Protocol version 4", and the IP configuration settings window should now be open.



Here, you should configure your IP Settings, in accordance to what was set in your VM Network settings config. For me, I configured the following:

IP Address Range	Subnet	Default Gateway
10.10.10.0	255.255.255.0	10.10.10.2

After this is configured on your VM, you should then validate your network connectivity by attempting to ping a public server like **1.1.1.1**.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=20ms TTL=128
Reply from 1.1.1.1: bytes=32 time=18ms TTL=128
Reply from 1.1.1.1: bytes=32 time=17ms TTL=128
Reply from 1.1.1.1: bytes=32 time=16ms TTL=128

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 20ms, Average = 17ms

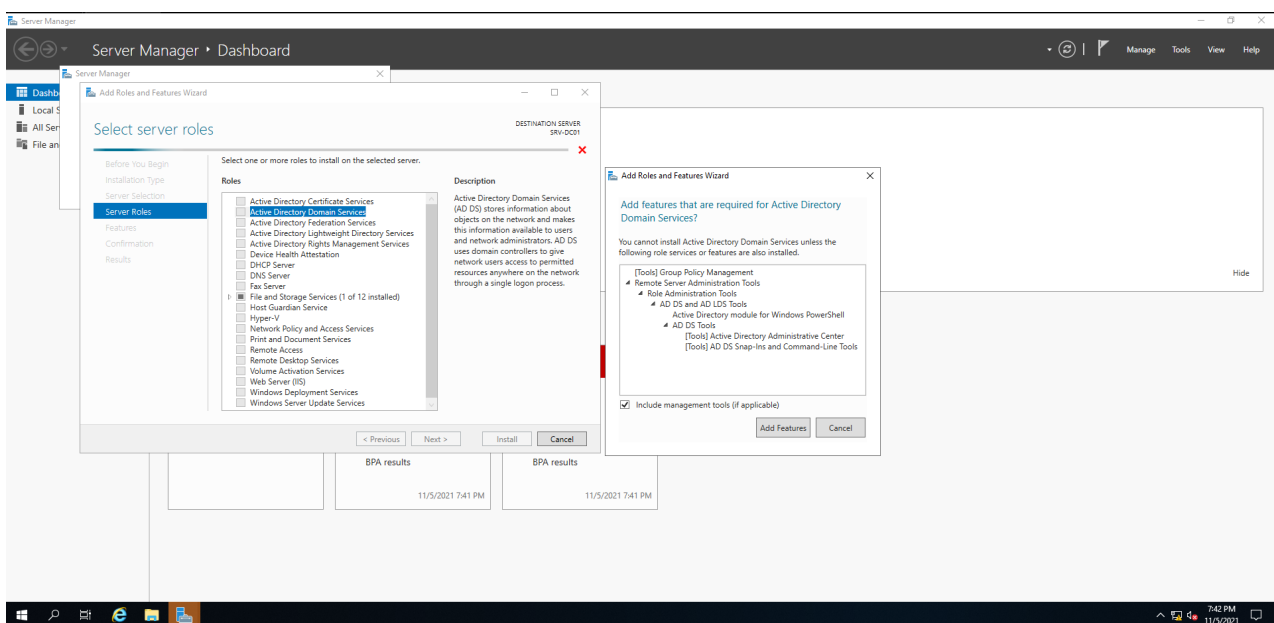
C:\Users\Administrator>
```

After this is setup, this concludes the basic Server Admin components. Next, we're going to start to build out the Active Directory components of the Server.

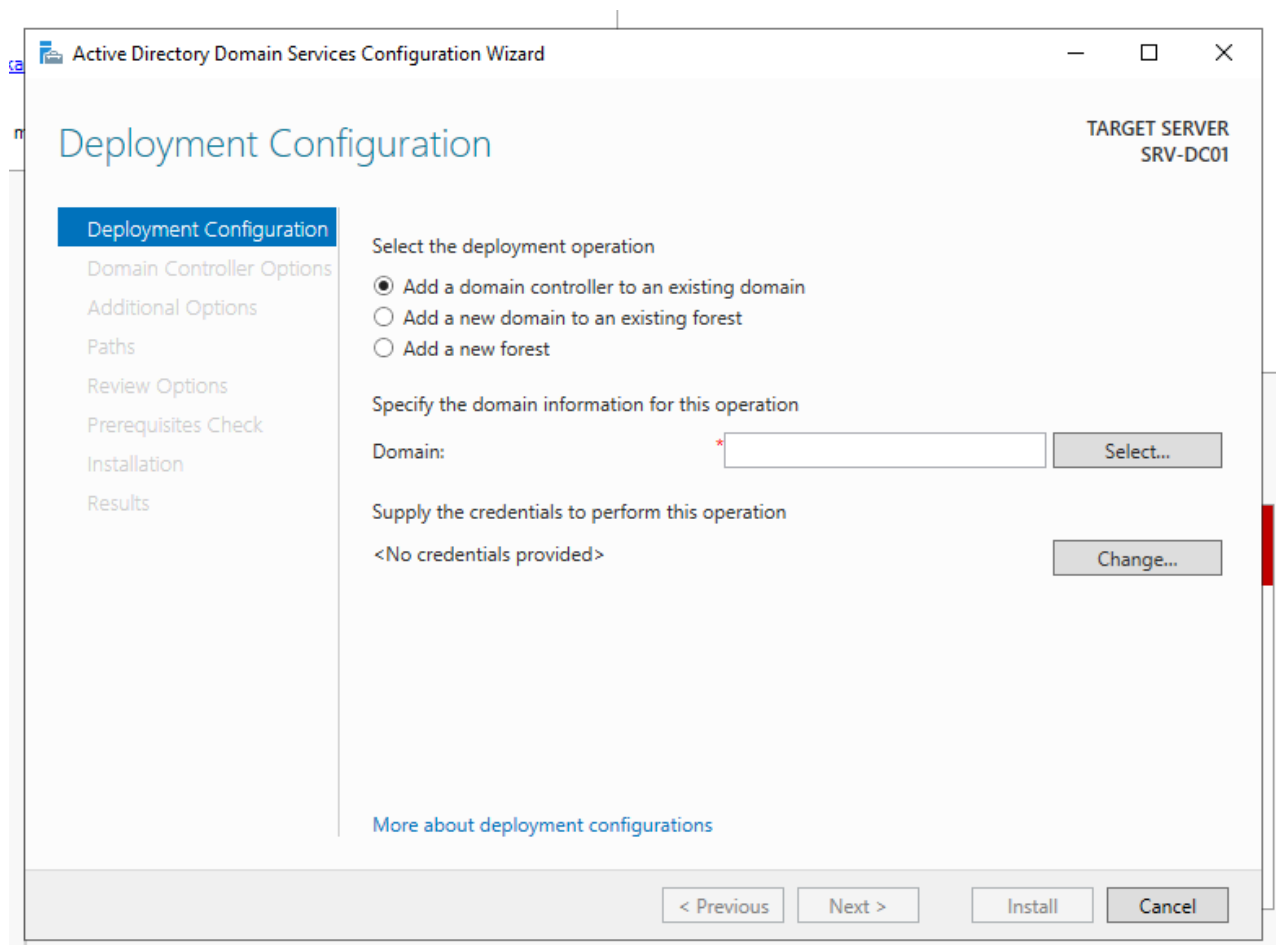
## Building the Forest

### Installing ADDS

To start, we're going to open the "Server Manager", this is where you can perform some basic monitoring of AD and Server services. Additionally, the Server Manager allows us to install packages. To do this, we go to "Manage" and then "Add Roles and Features". Click "Next" three times and we should be at the "Select Server Roles" tab. Here we want to install "Active Directory Domain Services", or ADDS for short.



Next, we will click “Next”, “Next”, and “Install” to finish up the ADDS install. This installation shouldn’t take too long to finish. After it finishes, click Close. You should notice a new yellow informational triangle next to the “Manage” icon, clicking on this, you should see a pending Post-deployment Configuration option called “Promote this server to a Domain Controller”. A new window should pop open as seen below:



By default, the “Add a Domain Controller to an existing domain” option will be selected, we need to change this to “Add a new Forest”. Here you will provide a Domain Name – for example contoso.com is a fictional company that Microsoft uses. This should *ideally* be a valid domain name that you own if this is being deployed in Production. However, in the Lab, unless you’re looking to expand out to Office365, you can use whatever you like. I will be using banana.corp. Clicking Next will bring you to a few technical options that I won’t dive into – however, you will be required to provide a DSRM restore password. This password is normally used to correct any problems or go into a restore mode with Active Directory.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER  
SRV-DC01

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: .....

[More about domain controller options](#)

< Previous   Next >   Install   Cancel

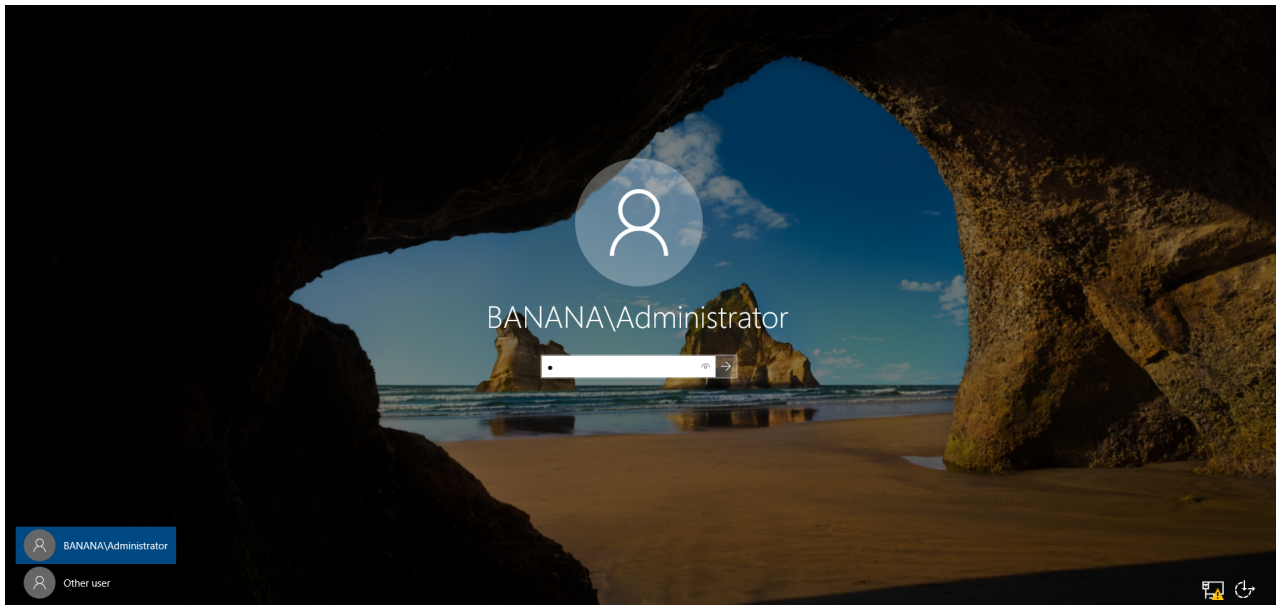
I personally have never had to use this before, however, that doesn't mean you shouldn't arbitrarily set this or forget this. You should add this password to your password list.

#### **Username      Password**

Administrator    S3cur3P@ssw0rd123!

DSRM              DSRMRestoreP@ssw0rd123!

Click "Next" on the DNS Options tab, since this is our first device in the Domain Controller in the environment, we can keep the default settings. Under the next "Additional Options" tab, we will be providing the NetBIOS Domain Name. This is normally seen in the DOMAIN\USER format in AD. You typically use this when logging into a device. I am going to set this to BANANA. The last few tabs you can click through "Next" and then finally "Install". After this finishes installing, this will bring you back to the Windows Login screen.



## Configuring a Conditional Forwarder

After logging in, the ADDS installation is now officially complete. Next up we will be covering how to configure DNS forwarding – This is important, when you configure the DNS server on the client workstation as the Domain Controller, the Domain Controller will not know where to forward appropriate DNS queries. In our case, if a user currently tries to query Google.com, it will not know where to go (as depicted below).

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup google.com
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: ::1

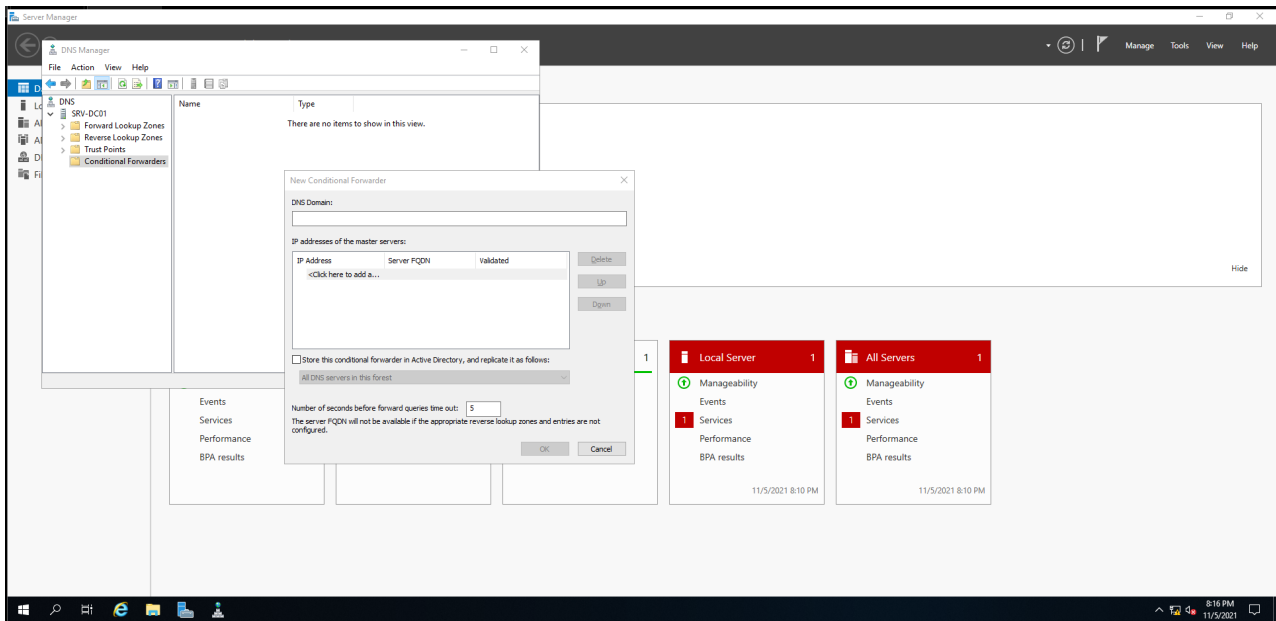
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\Administrator>
C:\Users\Administrator>
```

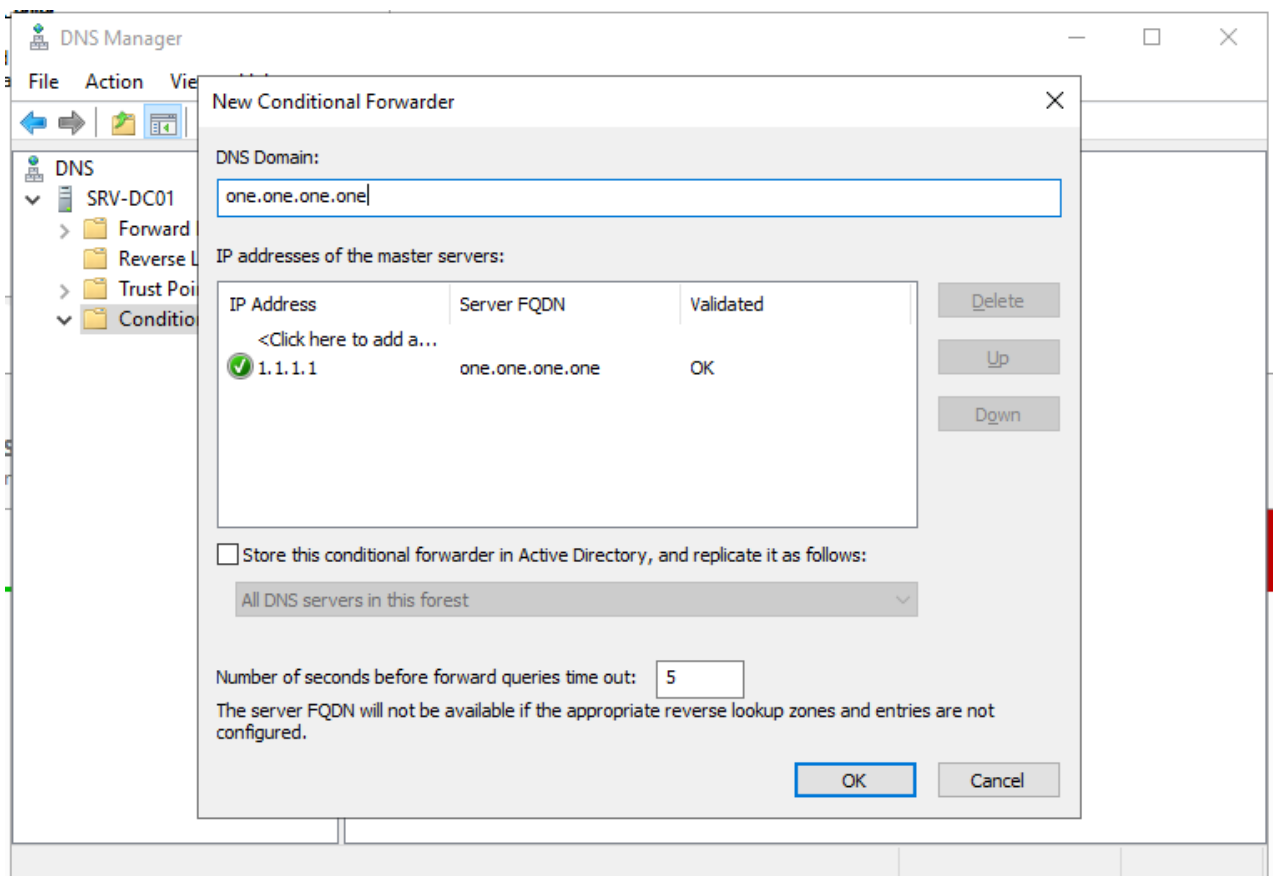
To remedy this, we have to setup a DNS conditional forwarder. To do so, search for DNS in the Windows Search bar, or open Server Manager, click Tools, then click DNS. Expanding the dropdowns you will see several options:

- Forward Lookup Zones
- Reverse Lookup Zones
- Trust Points
- and Conditional Forwarders

Expand the Conditional Forwarders tab and right click and click the “New Conditional Forwarder button”.



This new menu will open – here we are going to give the Domain of choice (for Cloudflare, they use one.one.one.one, and for Google they use dns.google)



After clicking “Ok”, using nslookup to query the IP address for Google, we should see that we are now able to resolve the DNS record. If you’d like, you can also add several more DNS servers to forward to (ex. Google).

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup google.com
Server: localhost
Address: 127.0.0.1

Non-authoritative answer:
Name: google.com
Addresses: 2607:f8b0:4002:800::200e
          172.217.13.14

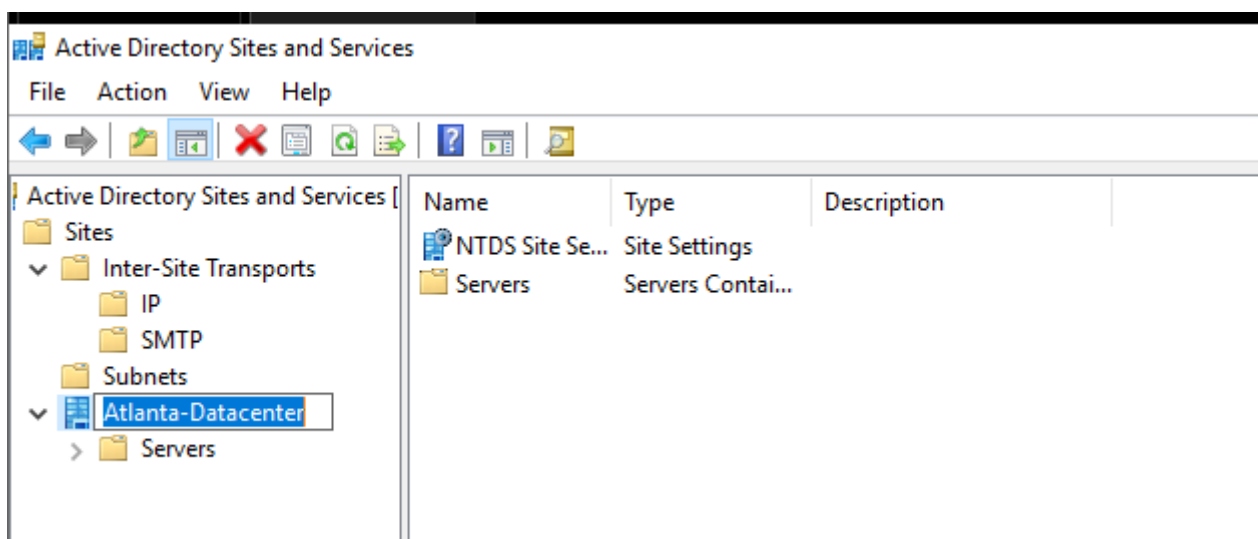
C:\Users\Administrator>
```

## Configuring Sites and Services

The next portion only applies to those who do not have DHCP enabled within their Network. AD Sites and Services provides a variety of AD heavy features, for example, which server is the Global Catalog, which servers live in which sites, which SMTP server to choose if you're in this site, which Subnets belong to these sites, etc. Having basic awareness of this section is incredibly important – here you can configure advanced features such as Site Replication which can allow you to control how often AD-Sites sync.

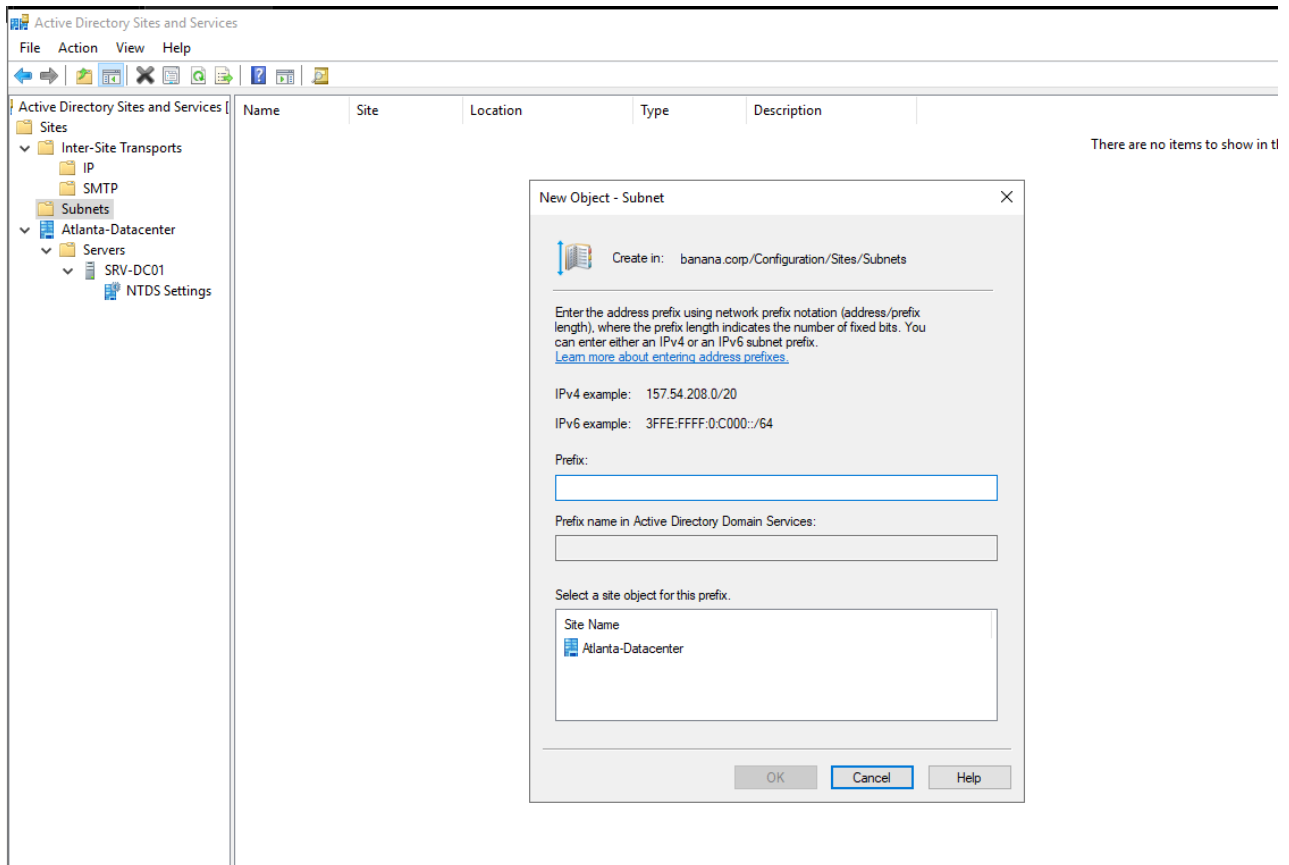
Let's say you have 10,000 employees in Albany, New York and things are constantly changing, you may want a lower sync time so consistency is achieved across both sites and at the end of the day there won't be massive levels of data transferring between sites. This can cause link saturation which could potentially lead to issues.

To start, we are going to rename the first site – by default, it is named "Default-First-Site-Name", I'm going to change this site name to Atlanta-Datacenter. This can be done by right clicking and selecting "Rename".





Next up, we're going to head over to the "Subnets" tab, here we are going to right click and "Add a New Subnet" as seen below.



Here, we are going to add our IPv4 address range and select our new Site.

New Object - Subnet

Create in: banana.corp/Configuration/Sites/Subnets

Enter the address prefix using network prefix notation (address/prefix length), where the prefix length indicates the number of fixed bits. You can enter either an IPv4 or an IPv6 subnet prefix.  
[Learn more about entering address prefixes.](#)

IPv4 example: 157.54.208.0/20  
IPv6 example: 3FFE:FFFF:0:C000::/64

Prefix:

Prefix name in Active Directory Domain Services:

Select a site object for this prefix.

Site Name
Atlanta-Datacenter

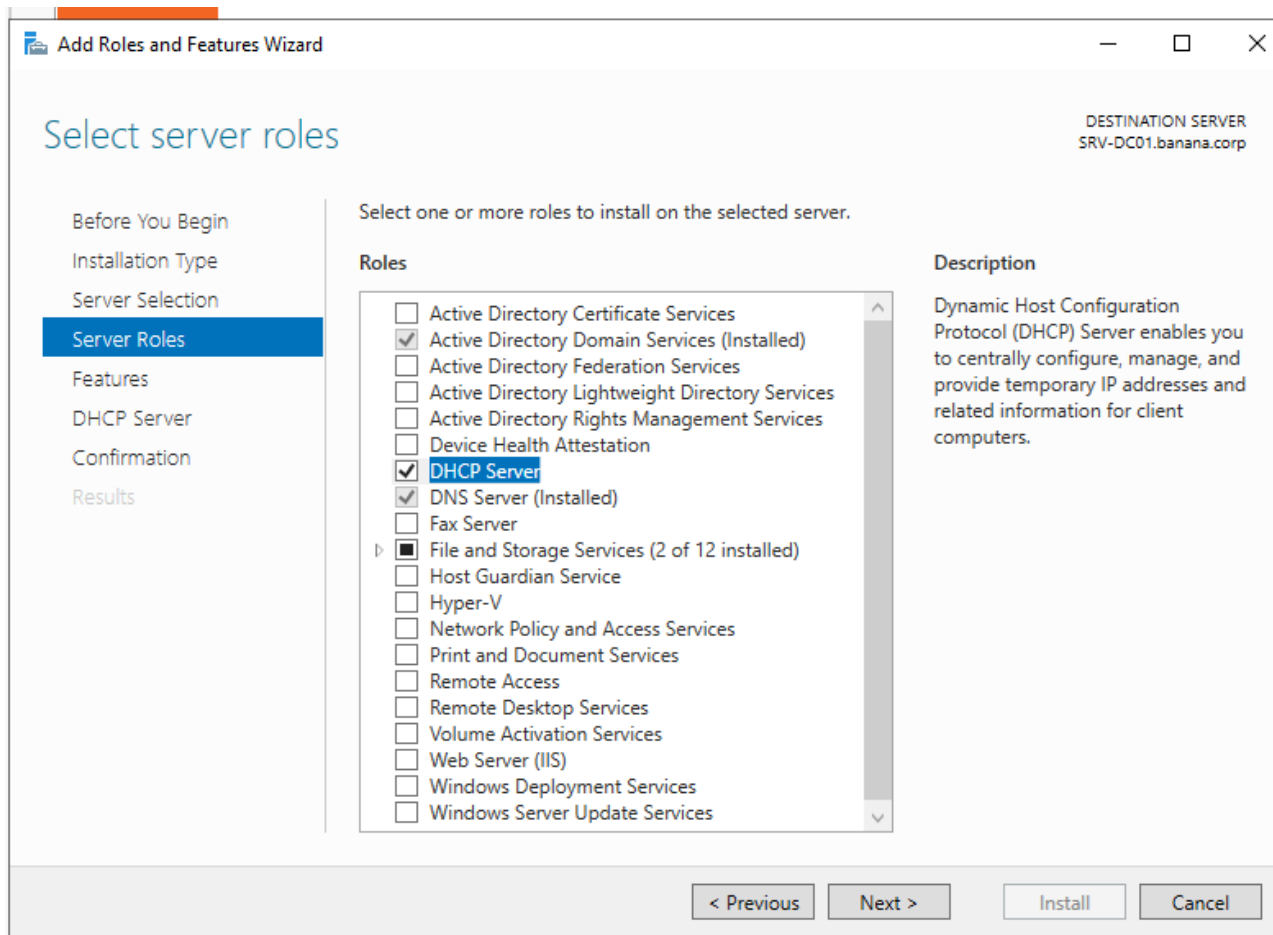
OK Cancel Help

To recap what we have configured:

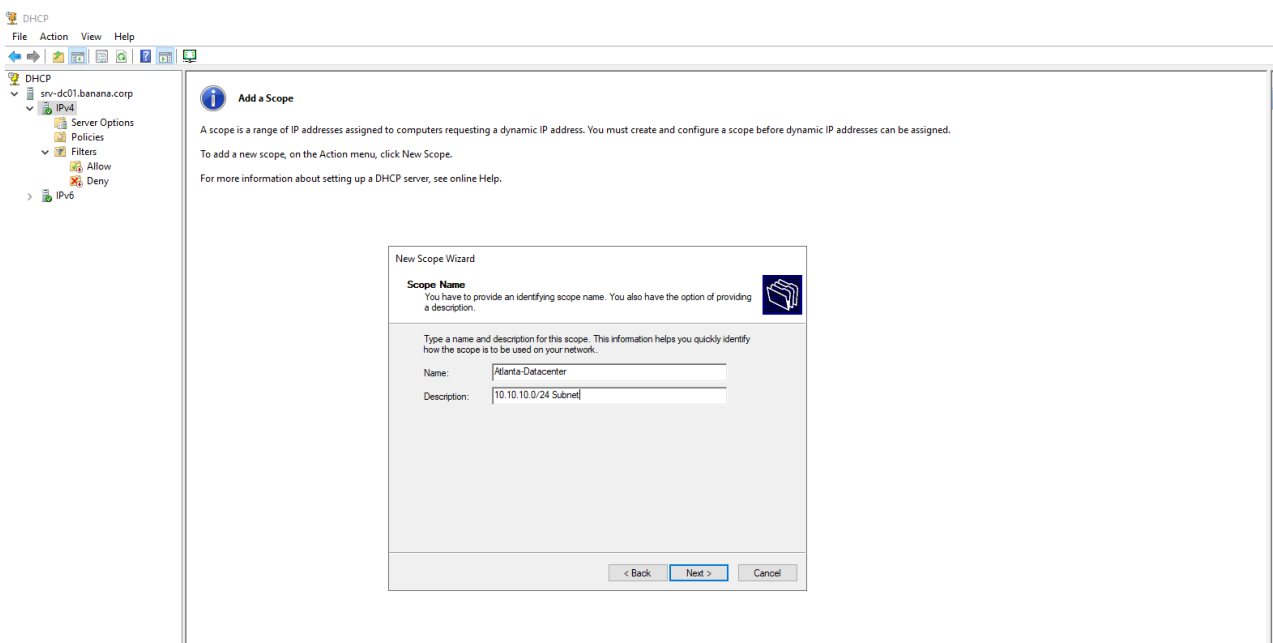
- We have configured a Site (Atlanta Datacenter)
- That site contains the 10.10.10.0/24 Address Range  
On a large enterprise network, this may be tens or possibly hundreds of different addresses

## Configuring DHCP

Next, we are going to move onto configuring DHCP, first we must install the DHCP service through the Server Manager, to do this, we must go to Manage -> Roles and Features -> Server Selection -> Server Roles and select "DHCP Server".

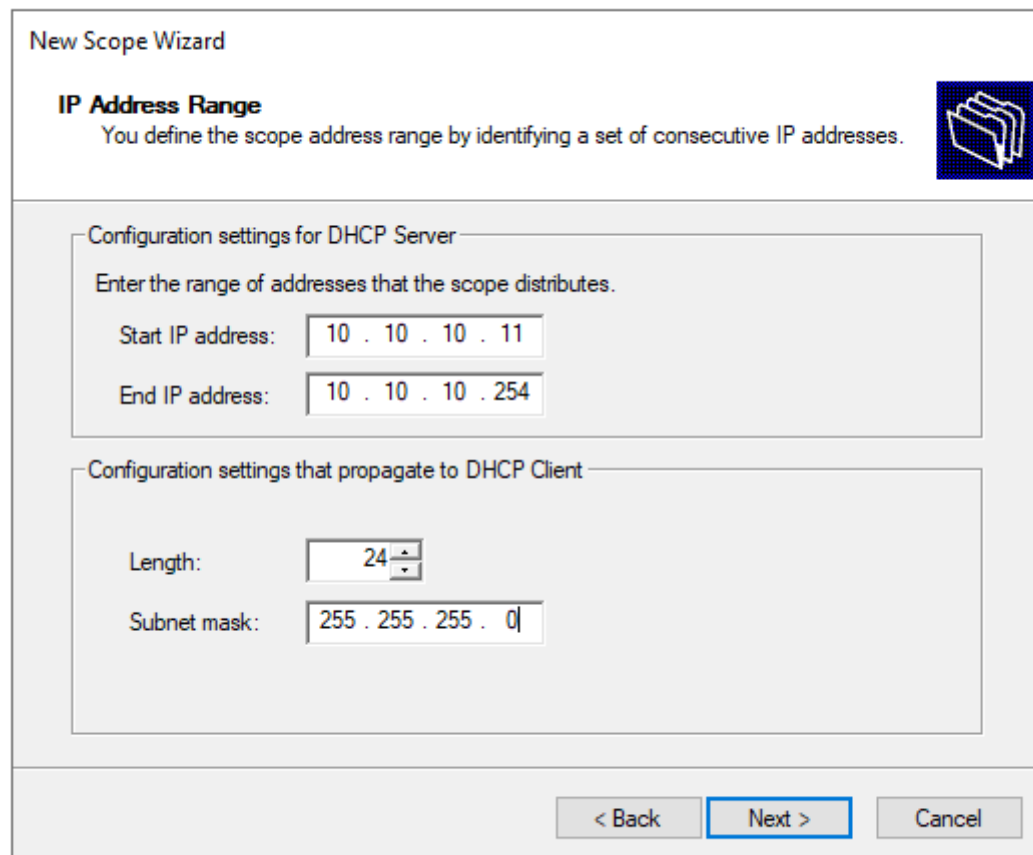


After this is installed, we will have another Post Deployment Operation required – this being to configure the DHCP server. We must authorize the deployment of a DHCP server with our Administrator credentials. After this is finished. To configure DHCP, you must go to Tools -> and select DHCP. Expand out the DHCP panel as well as the IPv4 settings.



I recommend that you provide a relatively verbose description, for example, what Subnet you will be serving via the specific DHCP service.

After clicking “Next”, we will be configuring the scope of our DHCP pool – I’m going to exclude the first ten IP Addresses of the subnet for Servers, Firewalls and any other objects that might be important in the future that should require a static IP Address.



The image shows a 'New Scope Wizard' dialog box. At the top, it says 'New Scope Wizard' and 'IP Address Range'. Below this, it says 'You define the scope address range by identifying a set of consecutive IP addresses.' There is a folder icon on the right. The main area is divided into two sections: 'Configuration settings for DHCP Server' and 'Configuration settings that propagate to DHCP Client'. In the first section, it says 'Enter the range of addresses that the scope distributes.' and has two input fields: 'Start IP address:' with the value '10 . 10 . 10 . 11' and 'End IP address:' with the value '10 . 10 . 10 . 254'. In the second section, it has two input fields: 'Length:' with the value '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

New Scope Wizard

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 10 . 10 . 10 . 11

End IP address: 10 . 10 . 10 . 254

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

In the next section, it's possible to create a reserved IP Address range, we're going to exclude an extra set of IP Addresses (11-20) *just in case*.

New Scope Wizard

**Add Exclusions and Delay**

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:  End IP address:

Excluded address range:

10.10.10.11 to 10.10.10.20	<input type="button" value="Remove"/>
----------------------------	---------------------------------------

Subnet delay in milli second:

< Back Next > Cancel

Clicking "Next" leads us to the Lease Duration section where we can control how long each DHCP lease is issued for. I recommend lowering the DHCP lease time for the purpose of the lab. However, that is ultimately up to you.

Next, we will be creating a couple of new special DHCP options, like the Default Gateway, DNS server.

In order to add the Default Gateway, you need to type in the IP Address (in my case it will be 10.10.10.2), then we will click "Add".

**New Scope Wizard**

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

10 . 10 . 10 . 2    Add

10.10.10.2    Remove

Up

Down

< Back    **Next >**    Cancel

The DNS server section is already pre-populated for us, so we just need to click “Next”.

**New Scope Wizard**

**Domain Name and DNS Servers**  
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain: banana.corp

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:    IP address:

Resolve    Add

10.10.10.10    Remove

Up

Down

< Back    **Next >**    Cancel

We can skip the WINS server section, lastly we will be presented with the “Activate Scope section”. Click “Activate the Scope now”, then “Next” and we will be finished!

The screenshot shows a 'New Scope Wizard' window. The title bar says 'New Scope Wizard'. Inside, the section is titled 'Activate Scope' with a subtext: 'Clients can obtain address leases only if a scope is activated.' There is a folder icon in the top right corner. Below this, a question is asked: 'Do you want to activate this scope now?'. There are two radio button options: 'Yes, I want to activate this scope now' (which is selected) and 'No, I will activate this scope later'. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

After the scope is configured, we have some new options we can check out, these being the following:

- Address Pool  
This displays the address ranges allowed to be issued and the excluded addresses
- Address Leases  
This displays all currently leased IP Addresses
- Reservations  
DHCP reservations based on MAC address
- Scope Options  
Here, we can add some additional services that we can send out with DHCP, for example, NTP Servers, IRC Servers, and many others
- Lastly, Policies  
For example, we can create a policy that issues IPs to Cisco devices based on their MAC address OUI.

This concludes the first part of building out an AD Lab. In the next post we will cover User Accounts, Group Policy Objects, Joining PCs to the Domain and much much more!

## Comments

---

