

The Comprehensive Active Directory Penetration Testing & Lab

By Muhammad Sada Mainasara

CCNA R&S, CCNP SECURITY, CISCO SECURITY
SPECIALIST, CEH, CHFI, MCSA, OSCP

Lab Preparation and Setup

Tools of the Trade

1 Windows Server 2019

2 Windows 10 Enterprise Edition

3 Metasploitable3 on Windows Server 2008

4 Microsoft Sql Server 2017

Domain Enumeration Tools

Tools of the Trade

1 Remote Server Administration Tools (RSAT) AD PowerShell Module

2 PowerView

3 PowerUpSql

4 SharpHound

5 BloodHound

6 SQLRecon

Exploitation, Post Exploitation and Lateral Movement

Tools of the Trade

1 PowerView

2 PowerUpSql

3 Inveigh

4 SQLRecon

5 Mimikatz

6 Rubeus

7 SharpSpray

Exploitation, Post Exploitation and Lateral Movement Cont...

8 DomainPasswordSpray

9 PsExec

10 Netcat

11 Invoke-SqlServer-Escalate-ExecuteAs

12 john-the-ripper

13 Hashcat

14 Kekeo

15 Invoke-SqlServer-Escalate-Dbowner

Exploitation, Post Exploitation and Lateral Movement Cont...

16 Invoke-BruteForce

17 PrintSpoofer

Lab Setup

Downloading Virtual Machines

1 Windows Server 2019 Evaluation Copy from Microsoft website

<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019>

2 Windows Enterprise Evaluation Copy from Microsoft website

<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise>

3 MetaSploitable3 VM from Rapid7 Github Repo

<https://github.com/rapid7/metasploitable3>

Lab Setup

Downloading Virtual Machines

4 MicroSoft SQL Server Express edition from Microsoft Website

<https://www.microsoft.com/en-us/download/details.aspx?id=55994>

5 Downloading VirtualBox

<https://download.virtualbox.org/virtualbox/7.0.12/VirtualBox-7.0.12-159484-Win.exe>

Downloading VirtualBox Extension Pack

[https://download.virtualbox.org/virtualbox/7.0.12/Oracle VM VirtualBox Extension Pack-7.0.12.vbox-extpack](https://download.virtualbox.org/virtualbox/7.0.12/Oracle_VM_VirtualBox_Extension_Pack-7.0.12.vbox-extpack)

Lab Setup

Installing Windows Server 2019

Create Virtual Machine

Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: ✓

Folder:

ISO Image:

Edition:

Type: 

Version: 

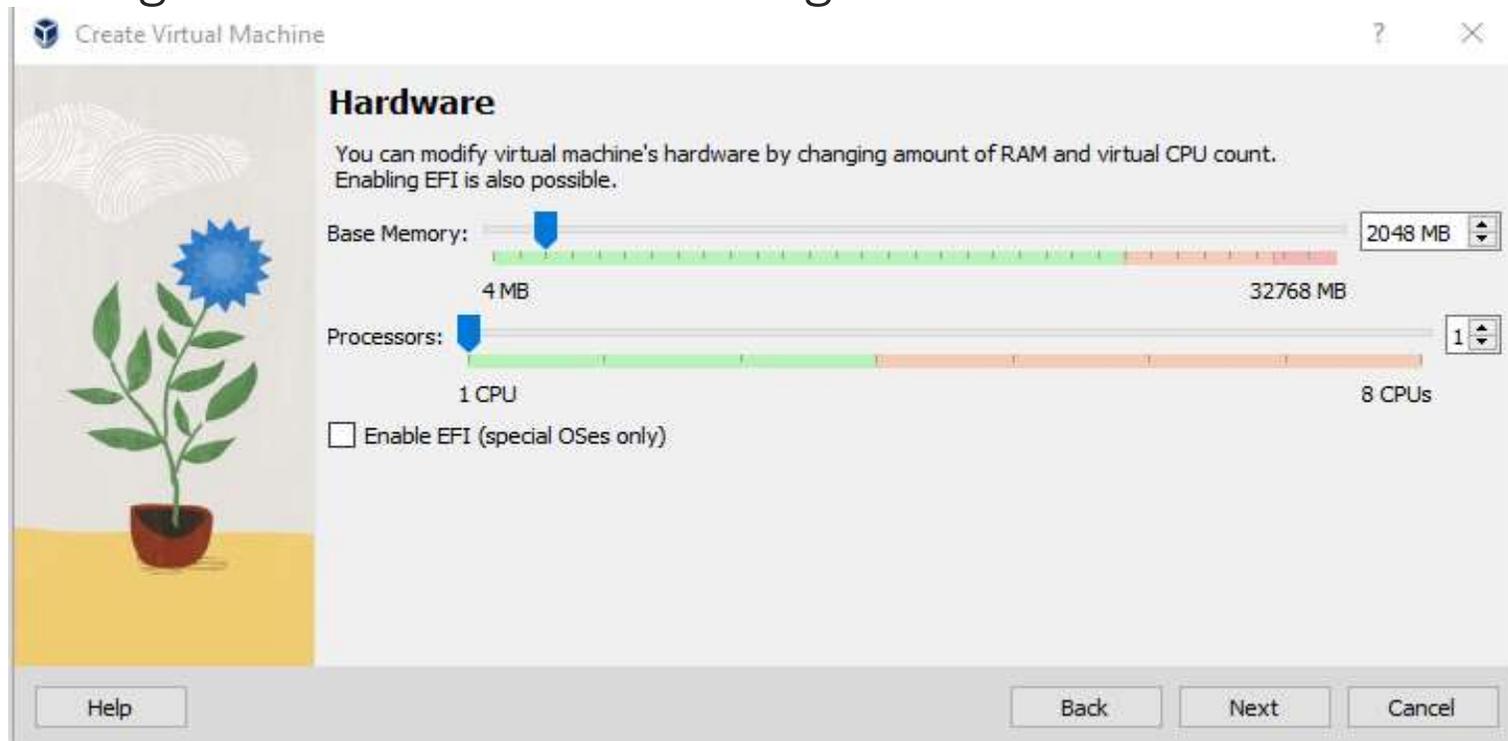
Skip Unattended Installation

 No ISO image is selected, the guest OS will need to be installed manually.

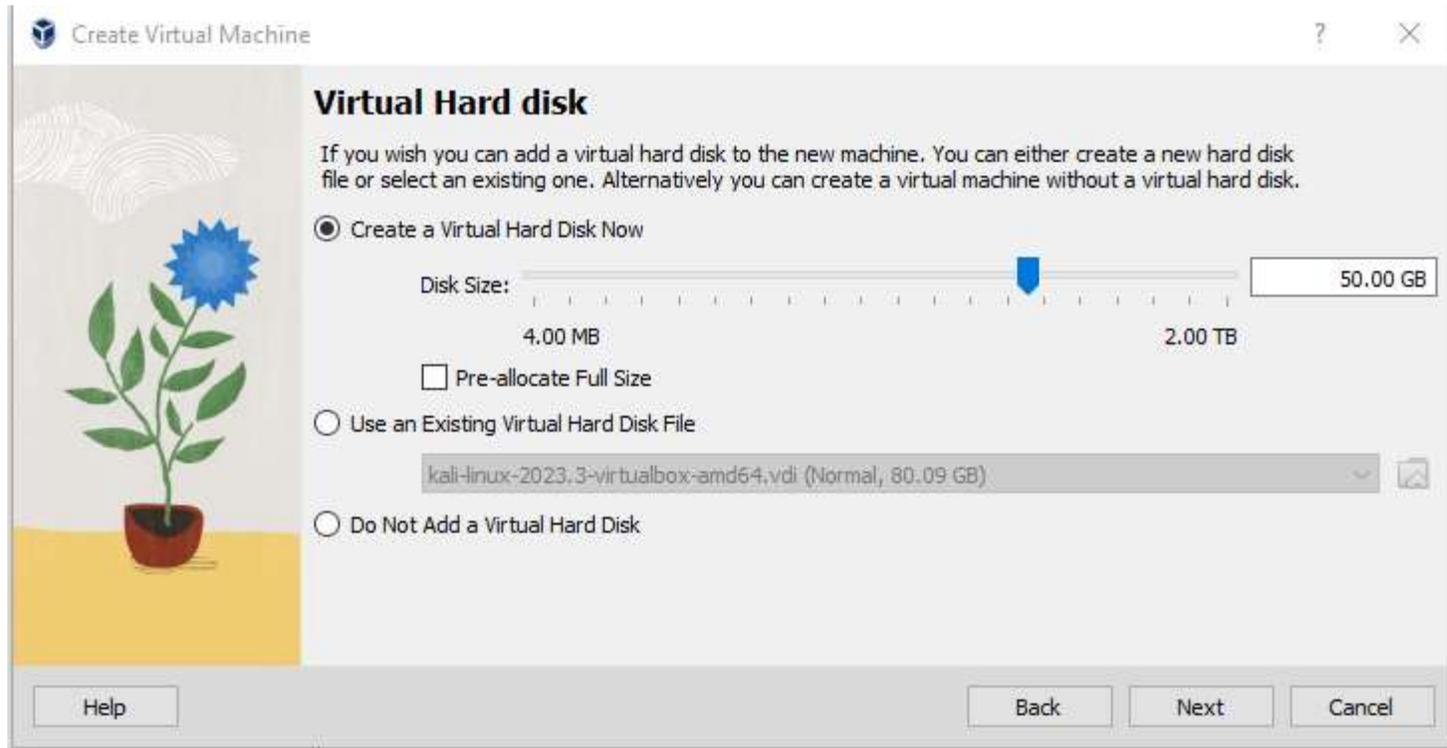
Help Expert Mode Back Next Cancel

Lab Setup

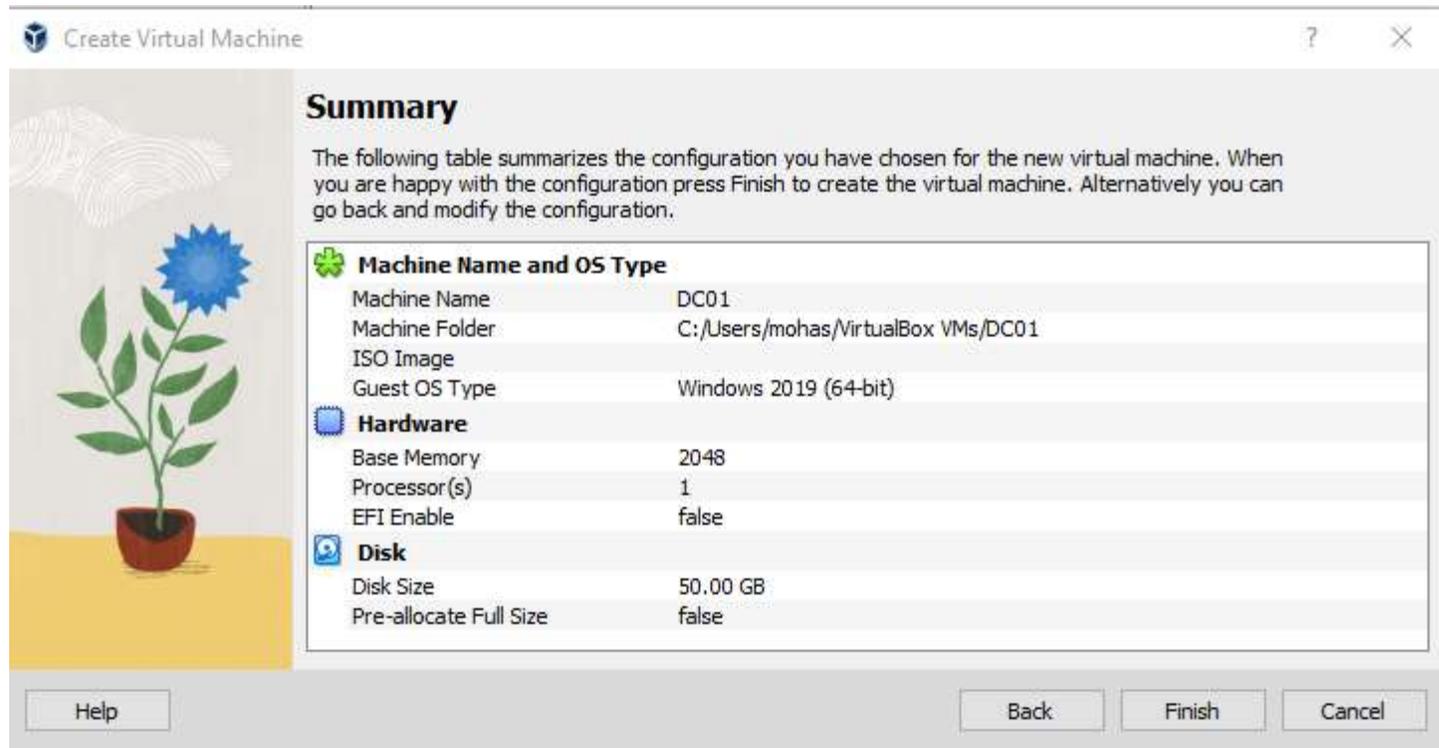
Let's go with the Default Setting



Lab Setup

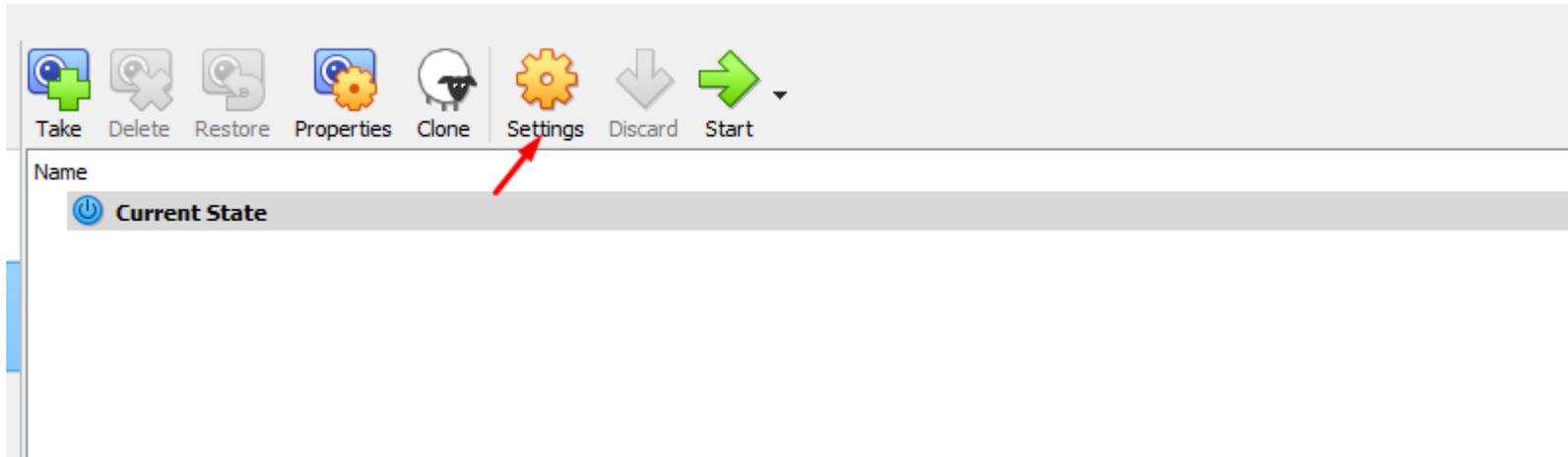


Lab Setup



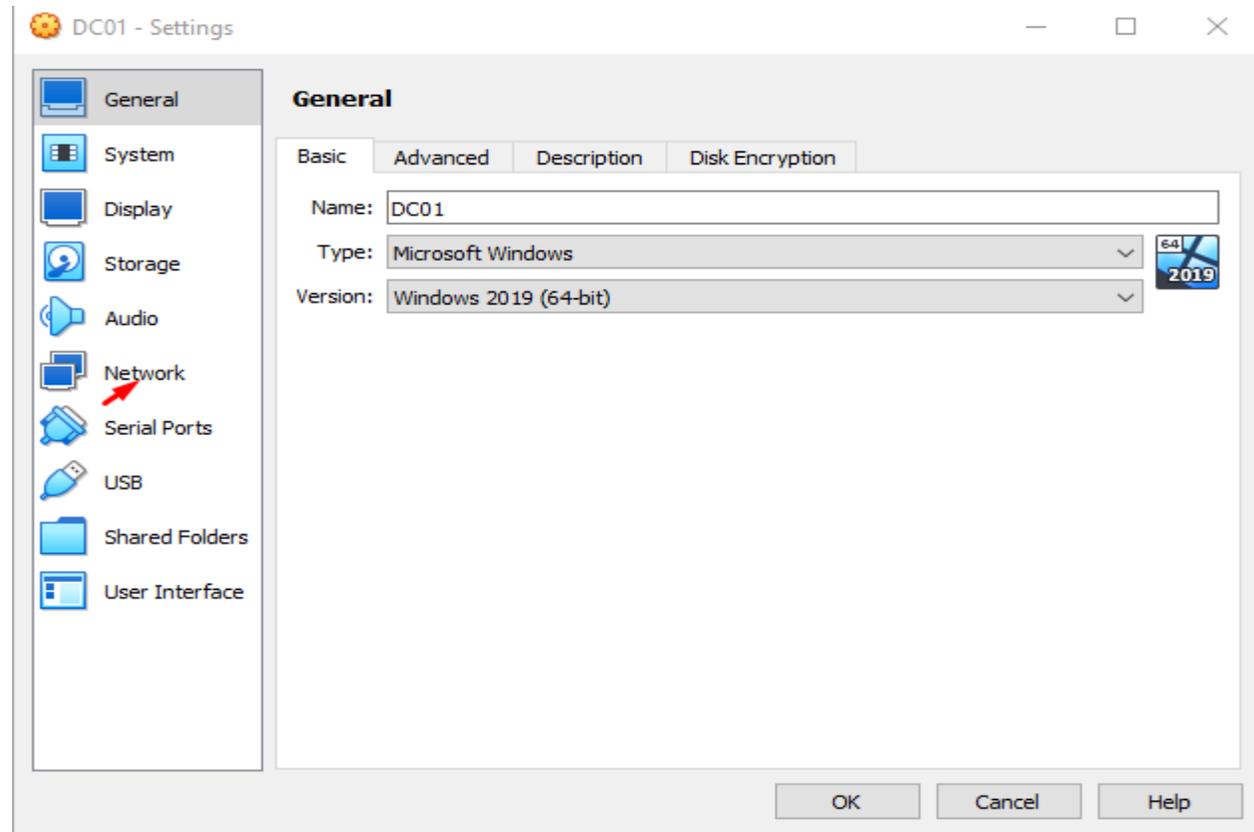
Lab Setup

Let's Change Some Settings



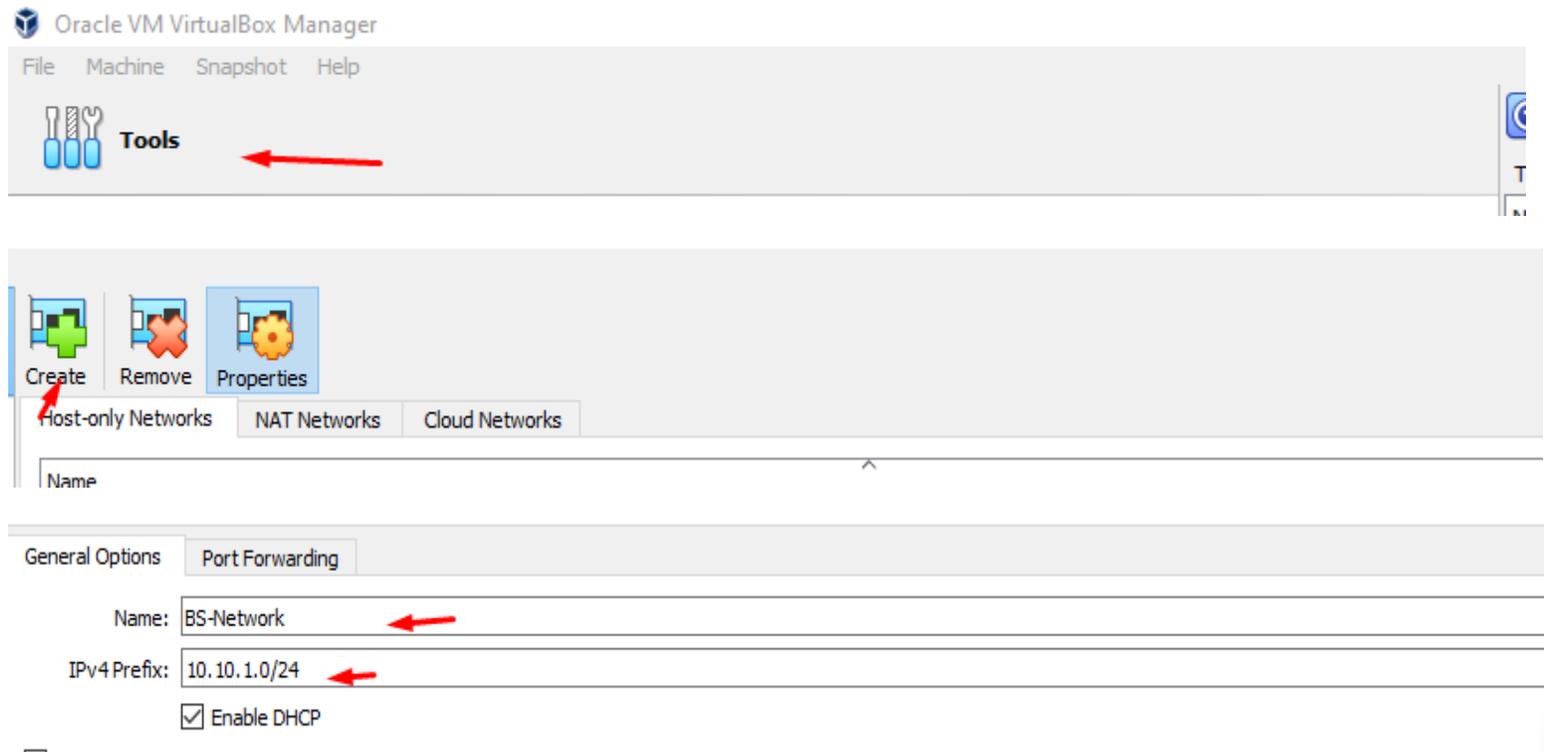
Lab Setup

Network Adapter Settings

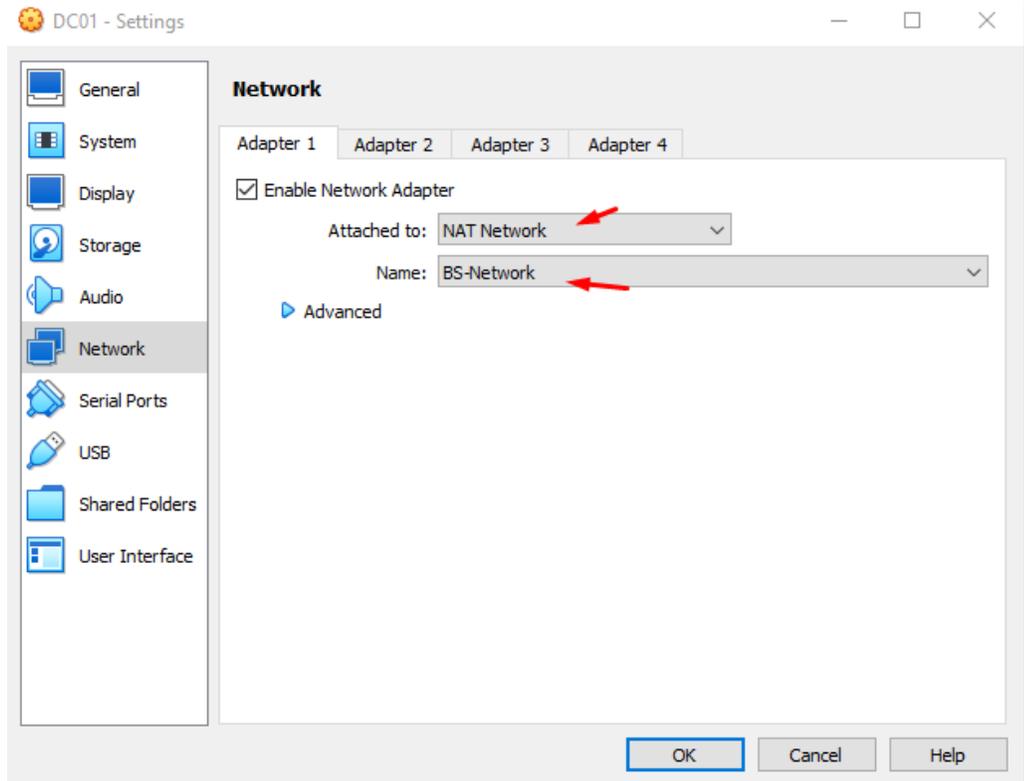


Lab Setup

Creating New Nat Network

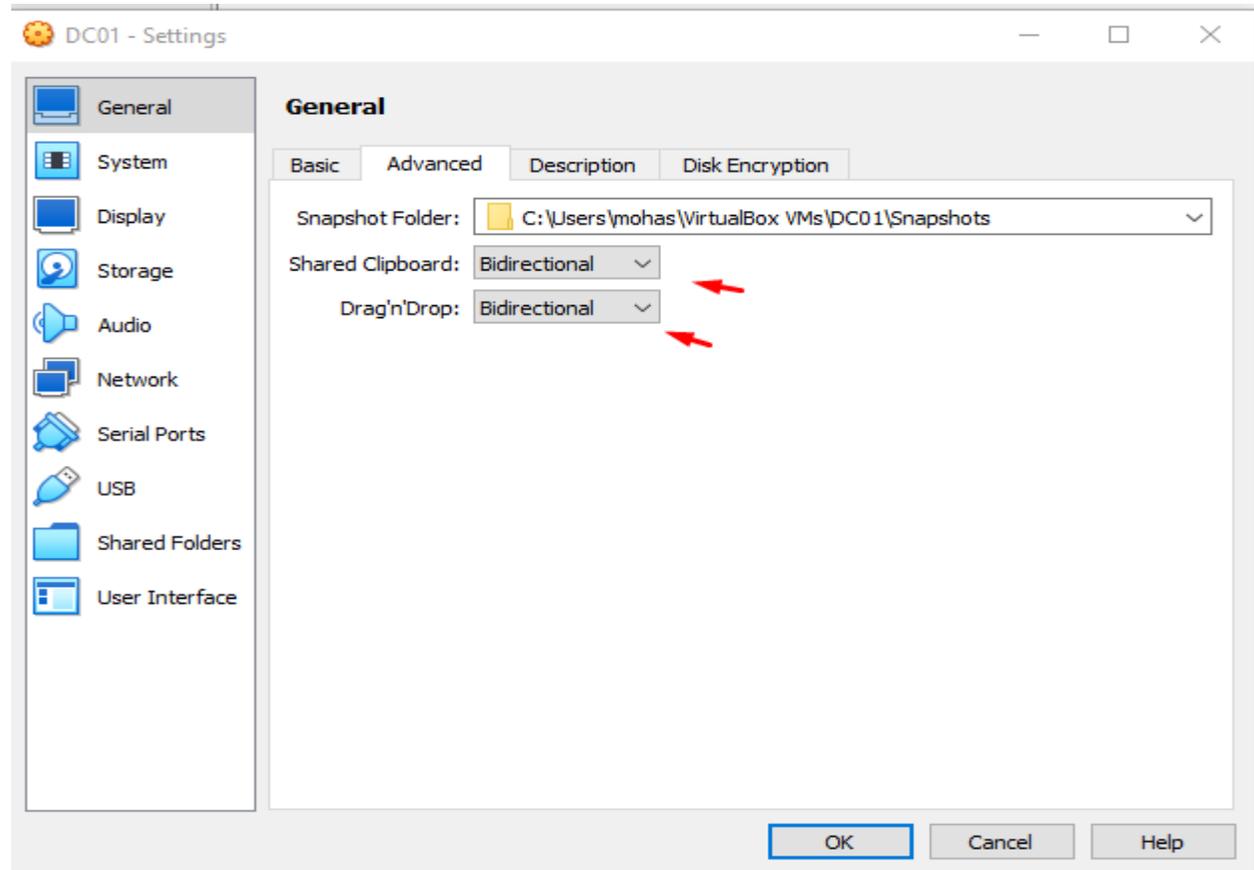


Lab Setup



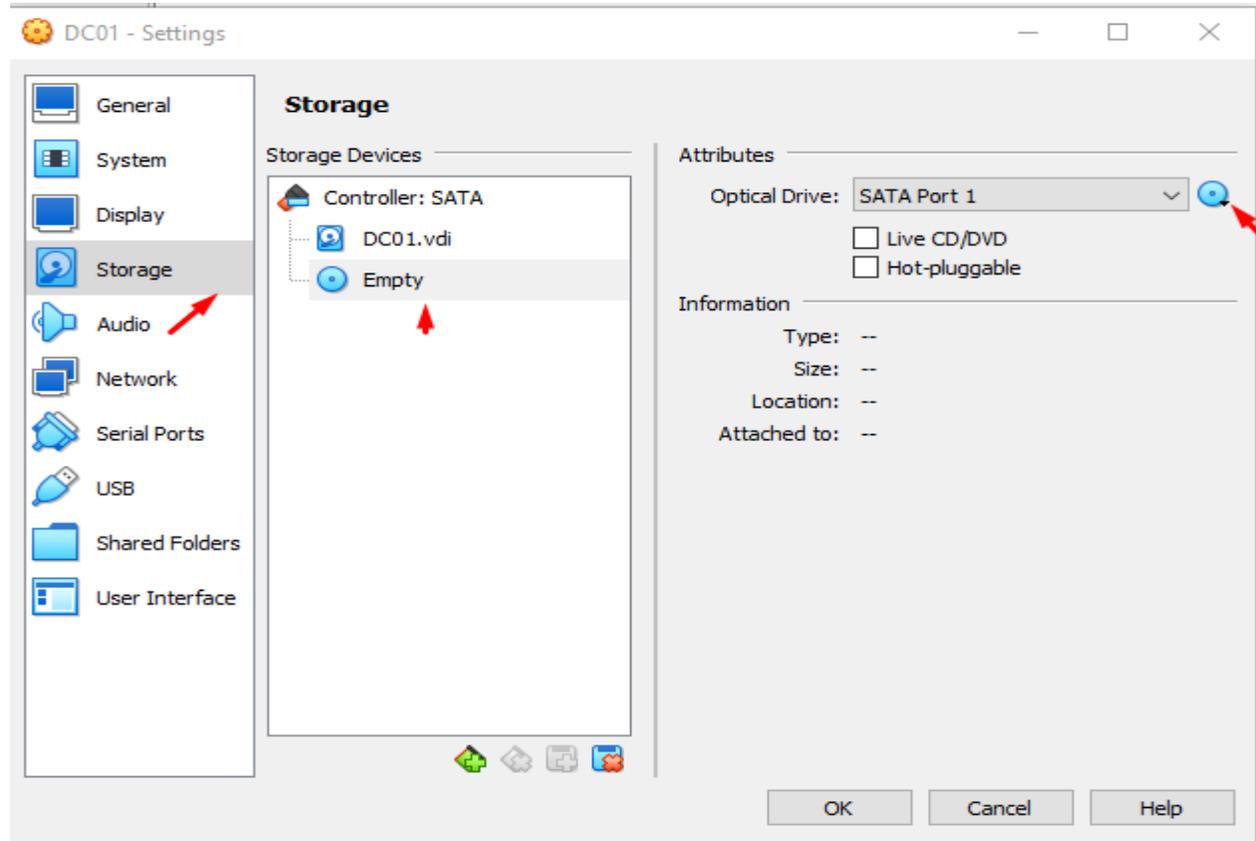
Lab Setup

Clipboard Sharing and Drag and Drop between guest and host Operating system



Lab Setup

Installing the OS



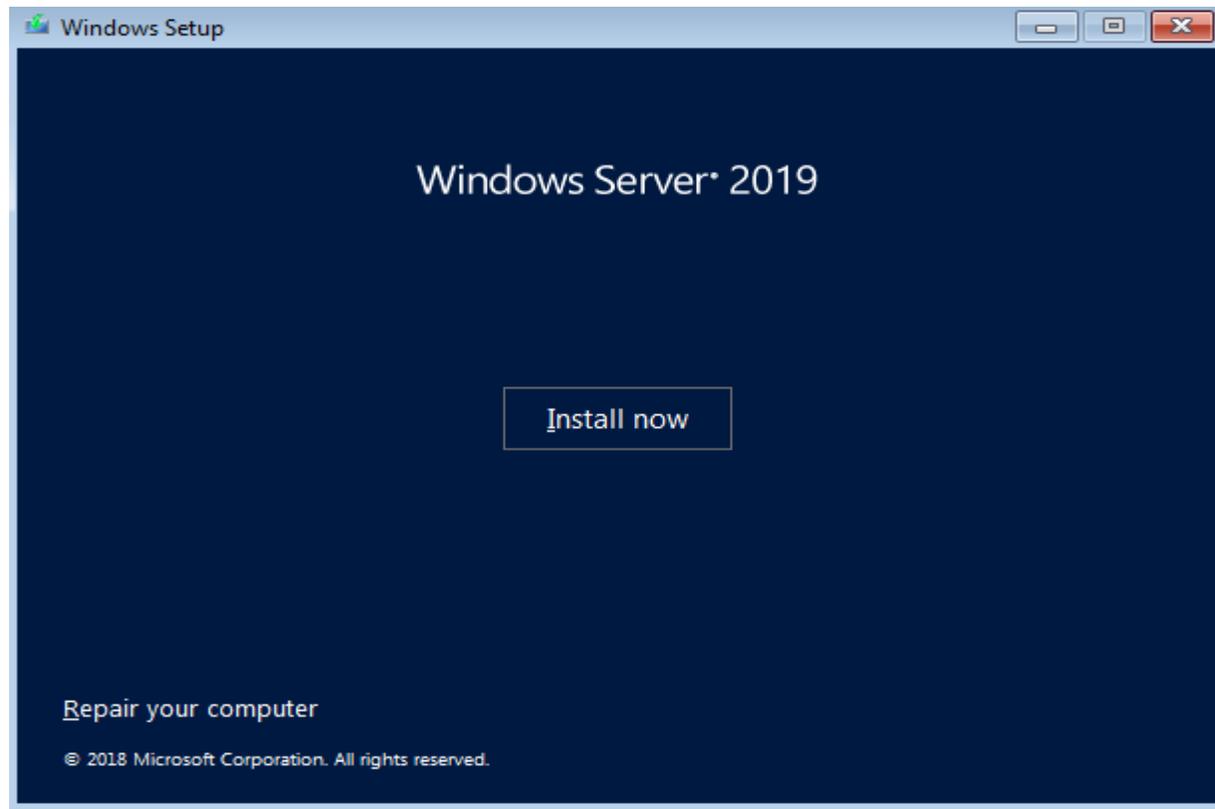
Lab Setup

Installing the OS



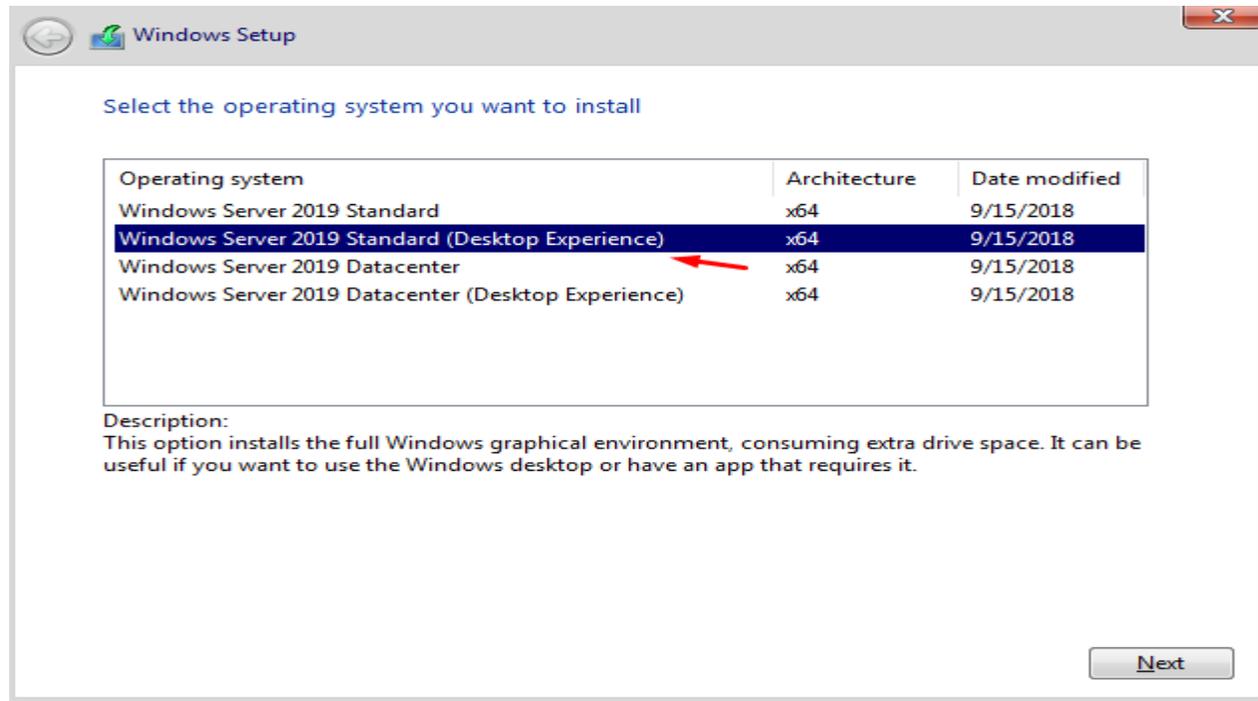
Lab Setup

Install now



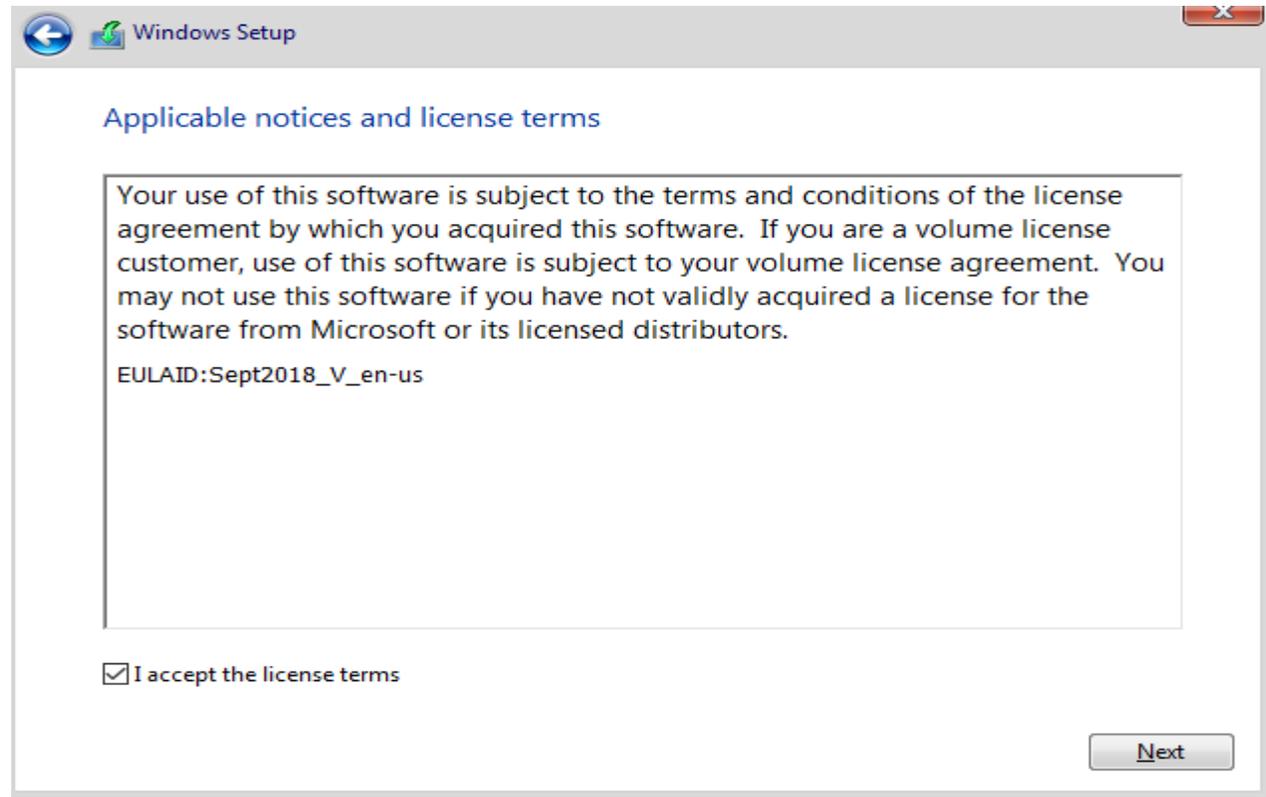
Lab Setup

Choose windows server with Desktop Experience



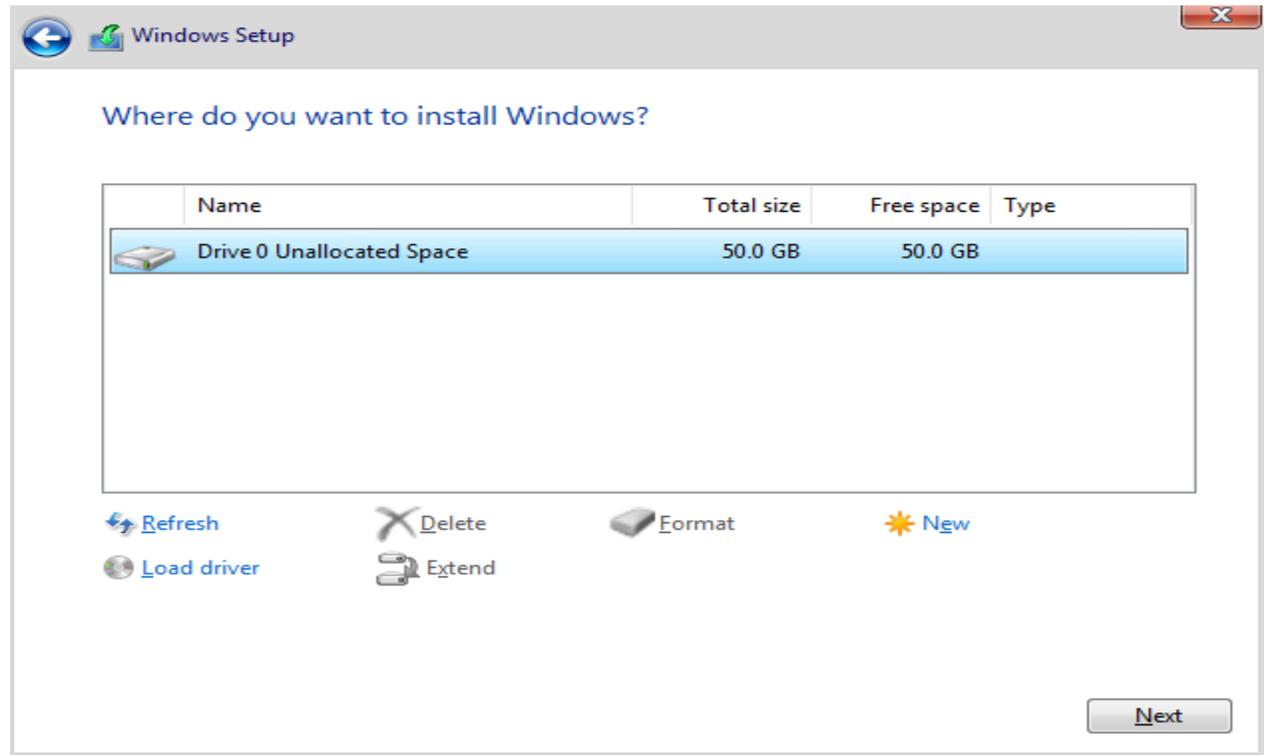
Lab Setup

Accept and Click Next



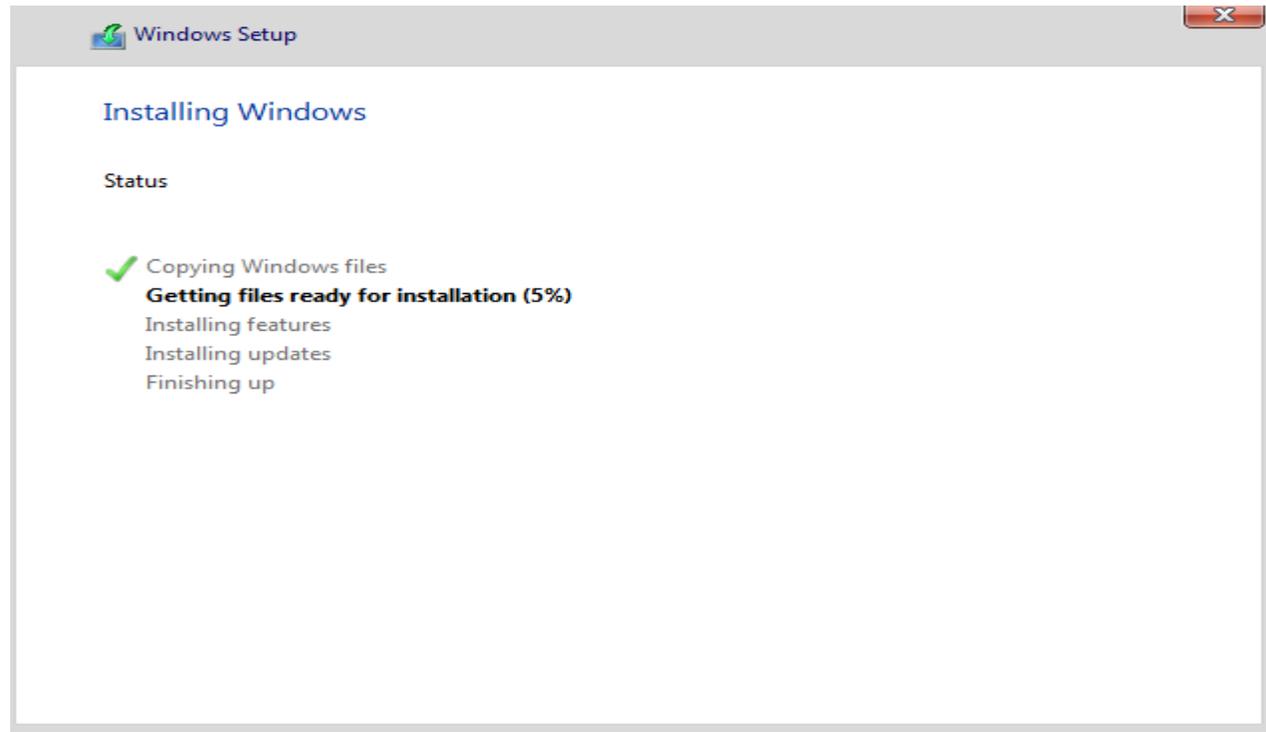
Lab Setup

Choose Custom install and Click Next



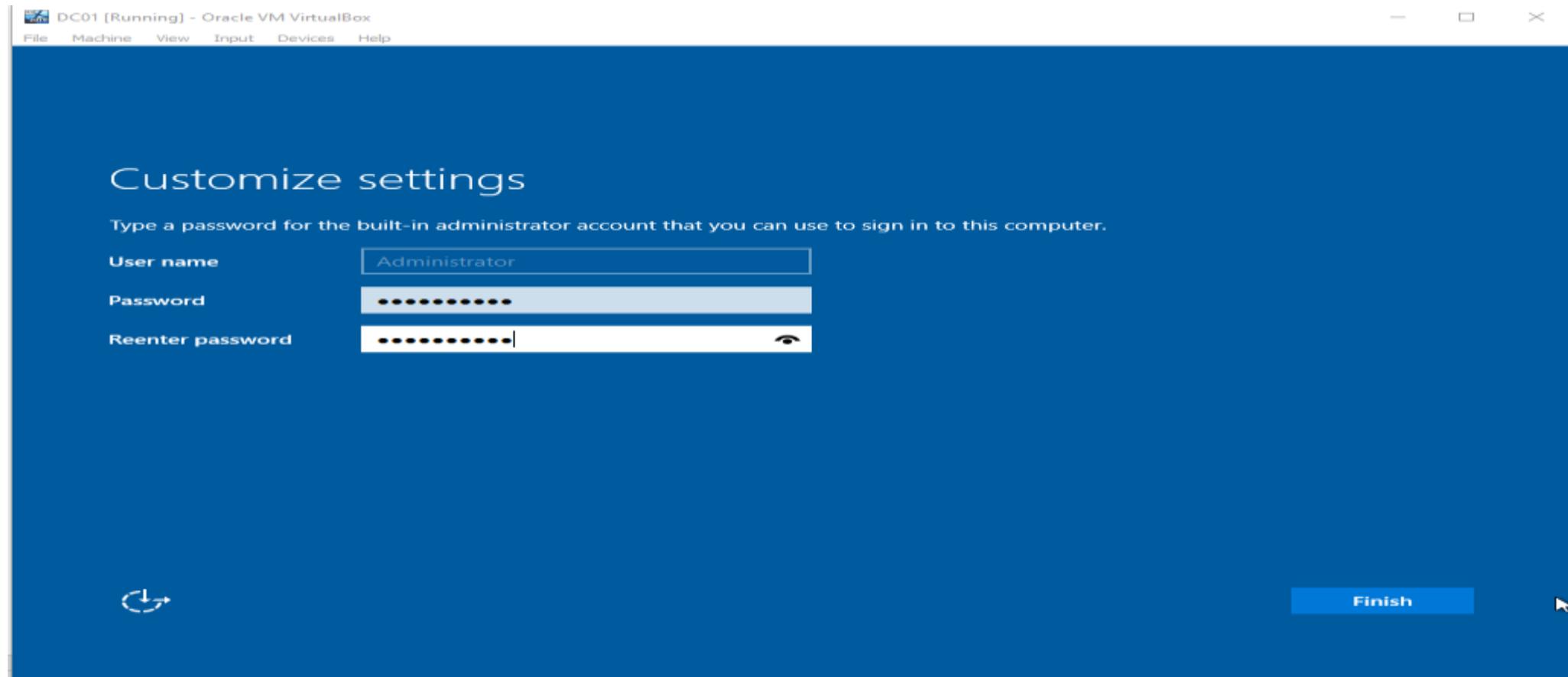
Lab Setup

Now allow the OS to be copied the VM we created



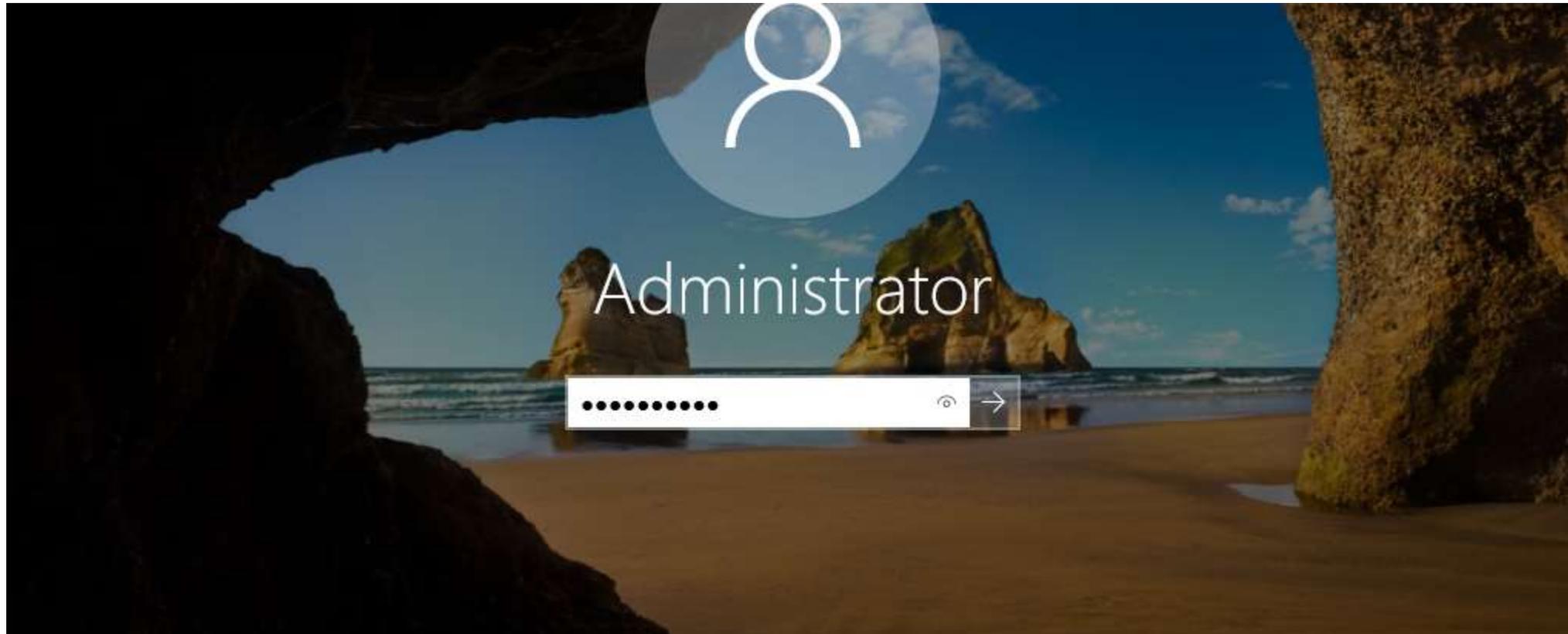
Lab Setup

Here we will Create the Administrator's Password and Click Finish



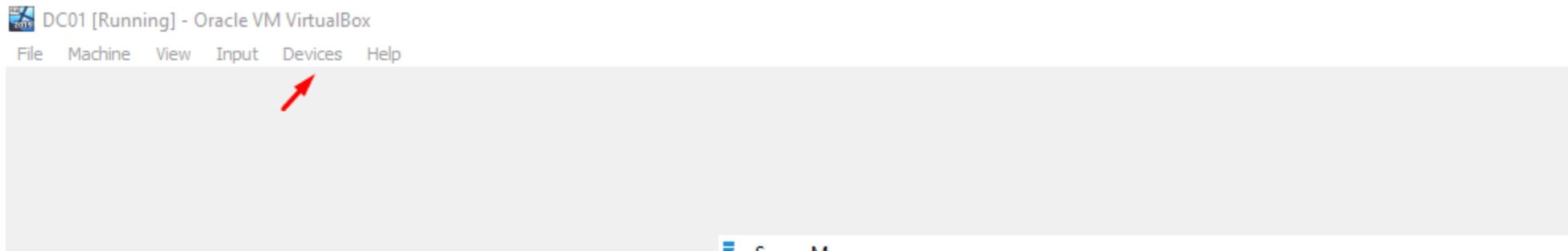
Lab Setup

Successfully Installed the OS



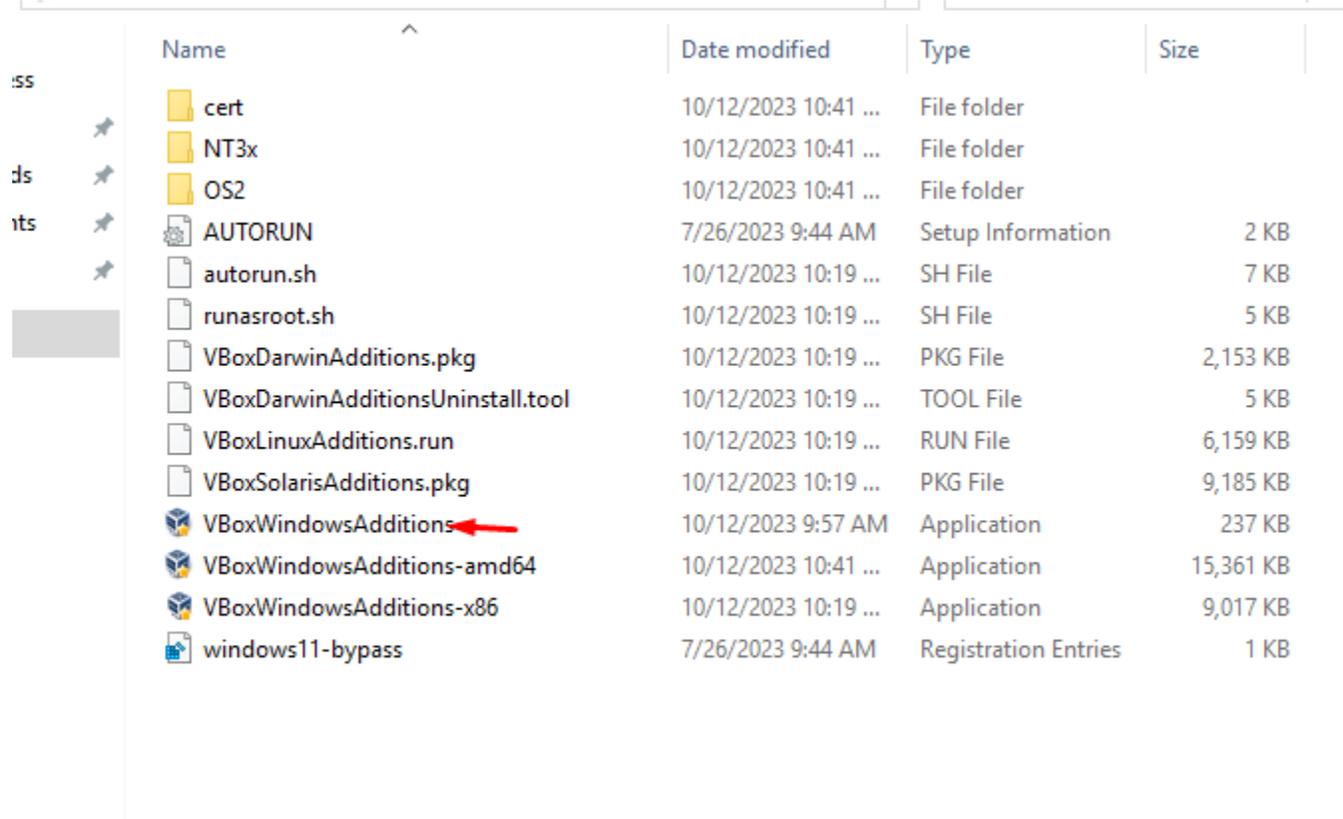
Lab Setup

Go Devices and Click insert guest edition CD image



Lab Setup

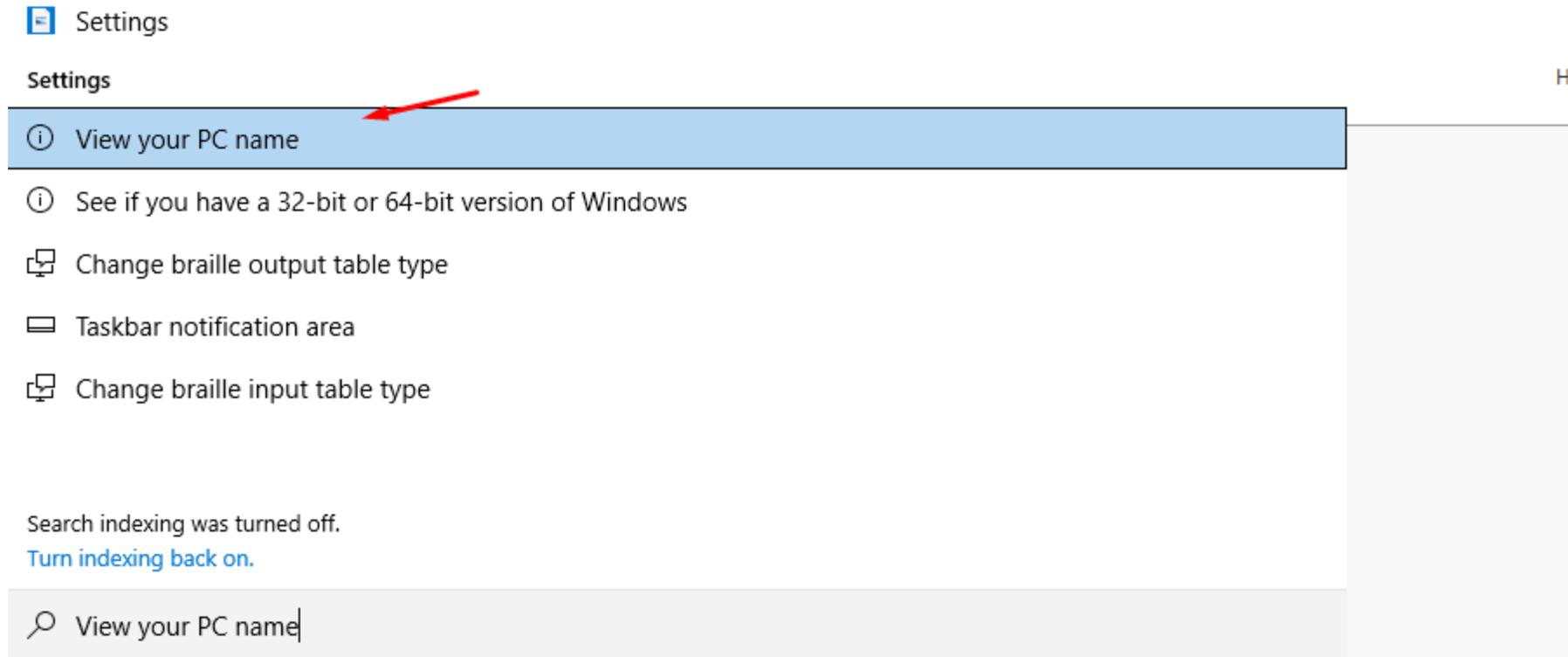
Double Click on it and follow the installation wizard to install it



Name	Date modified	Type	Size
cert	10/12/2023 10:41 ...	File folder	
NT3x	10/12/2023 10:41 ...	File folder	
OS2	10/12/2023 10:41 ...	File folder	
AUTORUN	7/26/2023 9:44 AM	Setup Information	2 KB
autorun.sh	10/12/2023 10:19 ...	SH File	7 KB
runasroot.sh	10/12/2023 10:19 ...	SH File	5 KB
VBoxDarwinAdditions.pkg	10/12/2023 10:19 ...	PKG File	2,153 KB
VBoxDarwinAdditionsUninstall.tool	10/12/2023 10:19 ...	TOOL File	5 KB
VBoxLinuxAdditions.run	10/12/2023 10:19 ...	RUN File	6,159 KB
VBoxSolarisAdditions.pkg	10/12/2023 10:19 ...	PKG File	9,185 KB
VBoxWindowsAdditions	10/12/2023 9:57 AM	Application	237 KB
VBoxWindowsAdditions-amd64	10/12/2023 10:41 ...	Application	15,361 KB
VBoxWindowsAdditions-x86	10/12/2023 10:19 ...	Application	9,017 KB
windows11-bypass	7/26/2023 9:44 AM	Registration Entries	1 KB

Lab Setup

Open the Computer Search bar and Type computer, View your PC name



The screenshot shows the Windows Settings application with a search bar at the top. The search results are displayed in a list. The first result, 'View your PC name', is highlighted in blue and has a red arrow pointing to it. Below the search results, there is a message: 'Search indexing was turned off. Turn indexing back on.' At the bottom, there is a search bar with the text 'View your PC name' entered.

Settings

Settings H

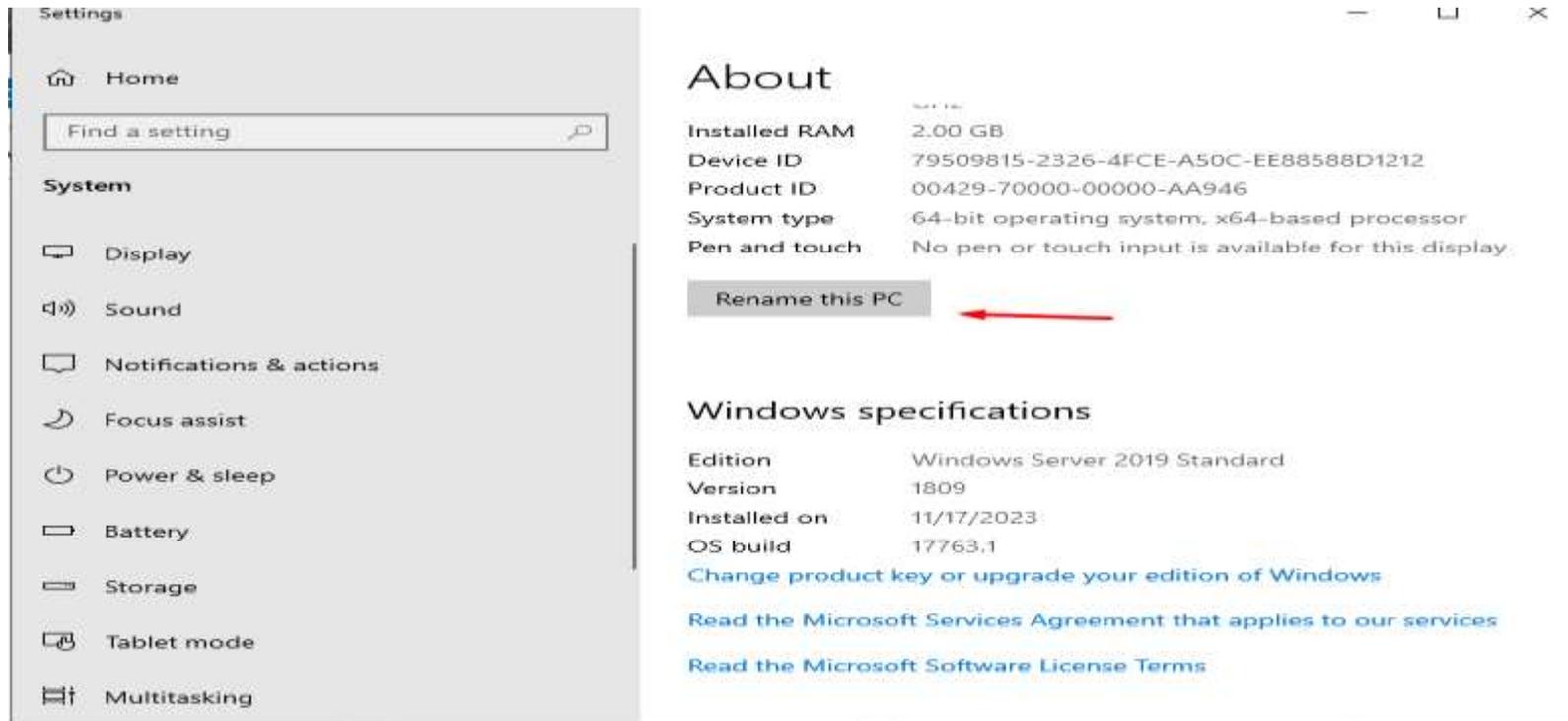
- View your PC name
- See if you have a 32-bit or 64-bit version of Windows
- Change braille output table type
- Taskbar notification area
- Change braille input table type

Search indexing was turned off.
[Turn indexing back on.](#)

View your PC name

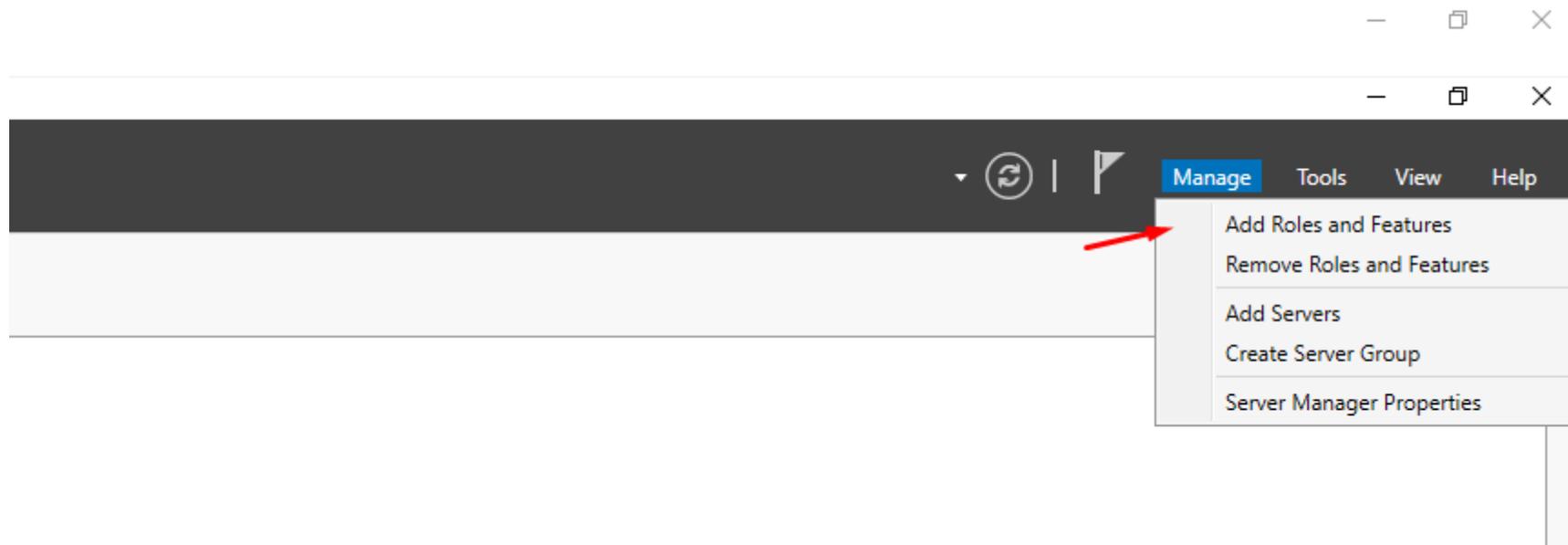
Lab Setup

Click on rename this pc and enter DC01 in the name, click Next and restart the Vm



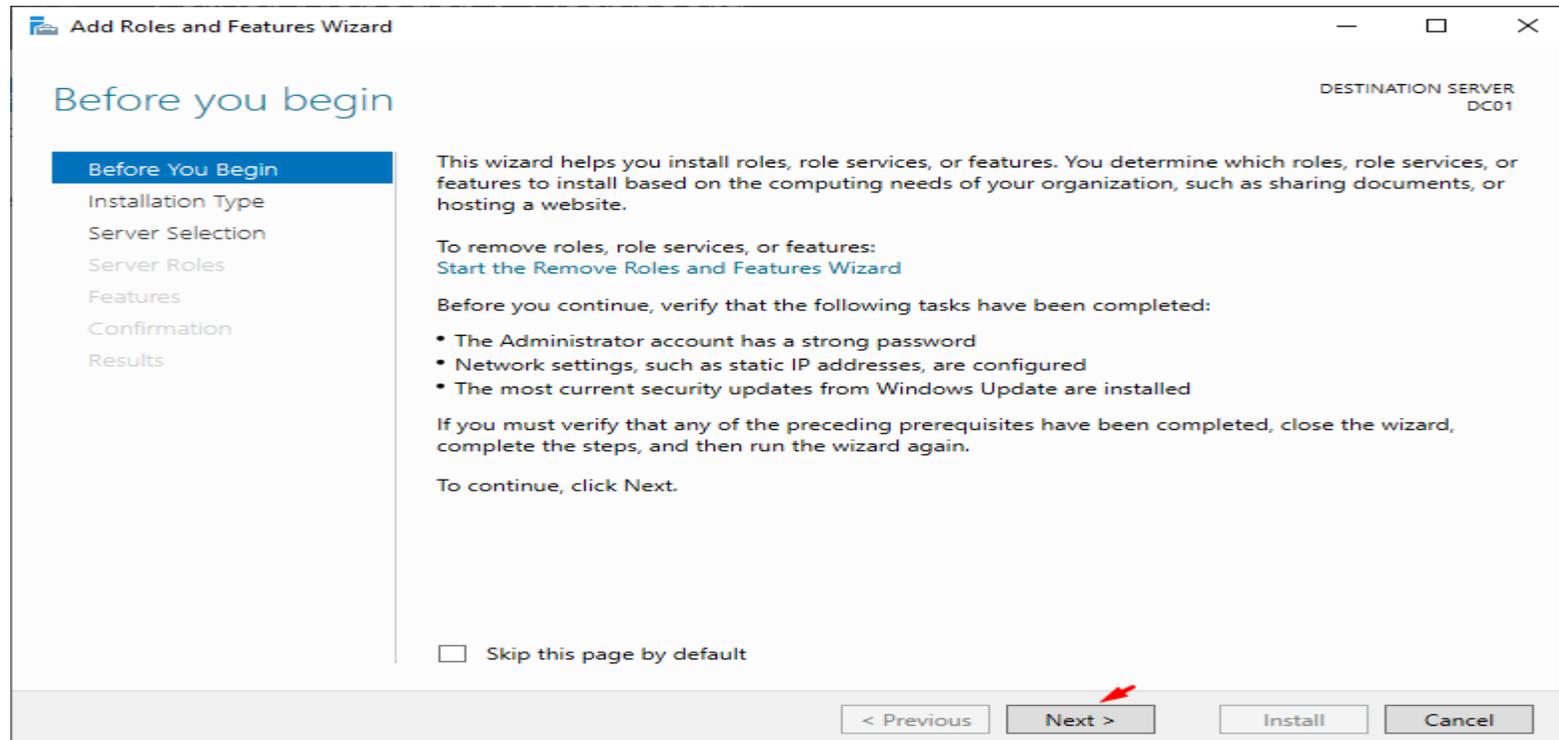
Lab Setup

Installing AD-DS and Domain Controller on the Server



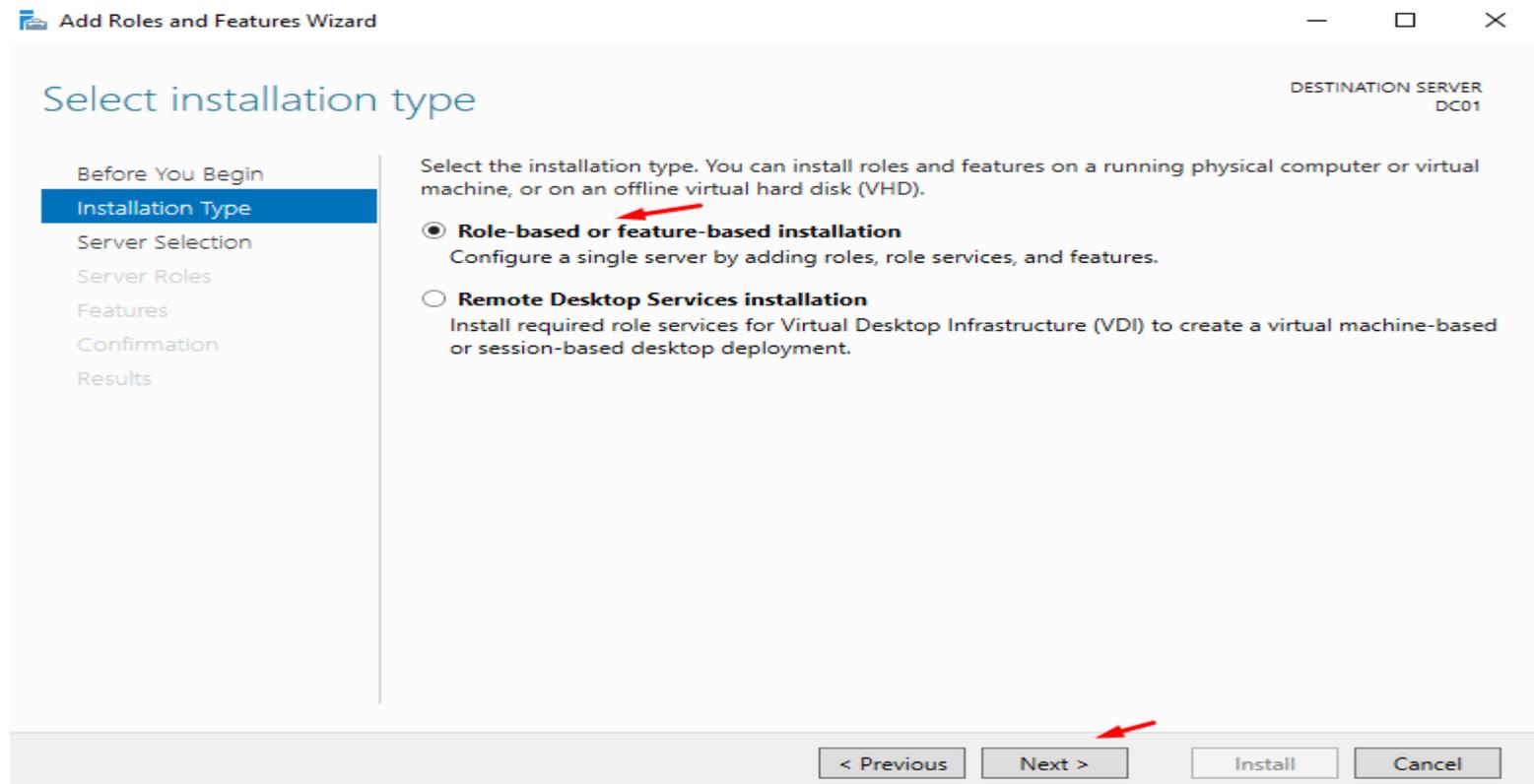
Lab Setup

Next



Lab Setup

Next



Lab Setup

Next

Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
DC01

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

Select a server from the server pool
 Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
DC01	10.10.1.4	Microsoft Windows Server 2019 Standard

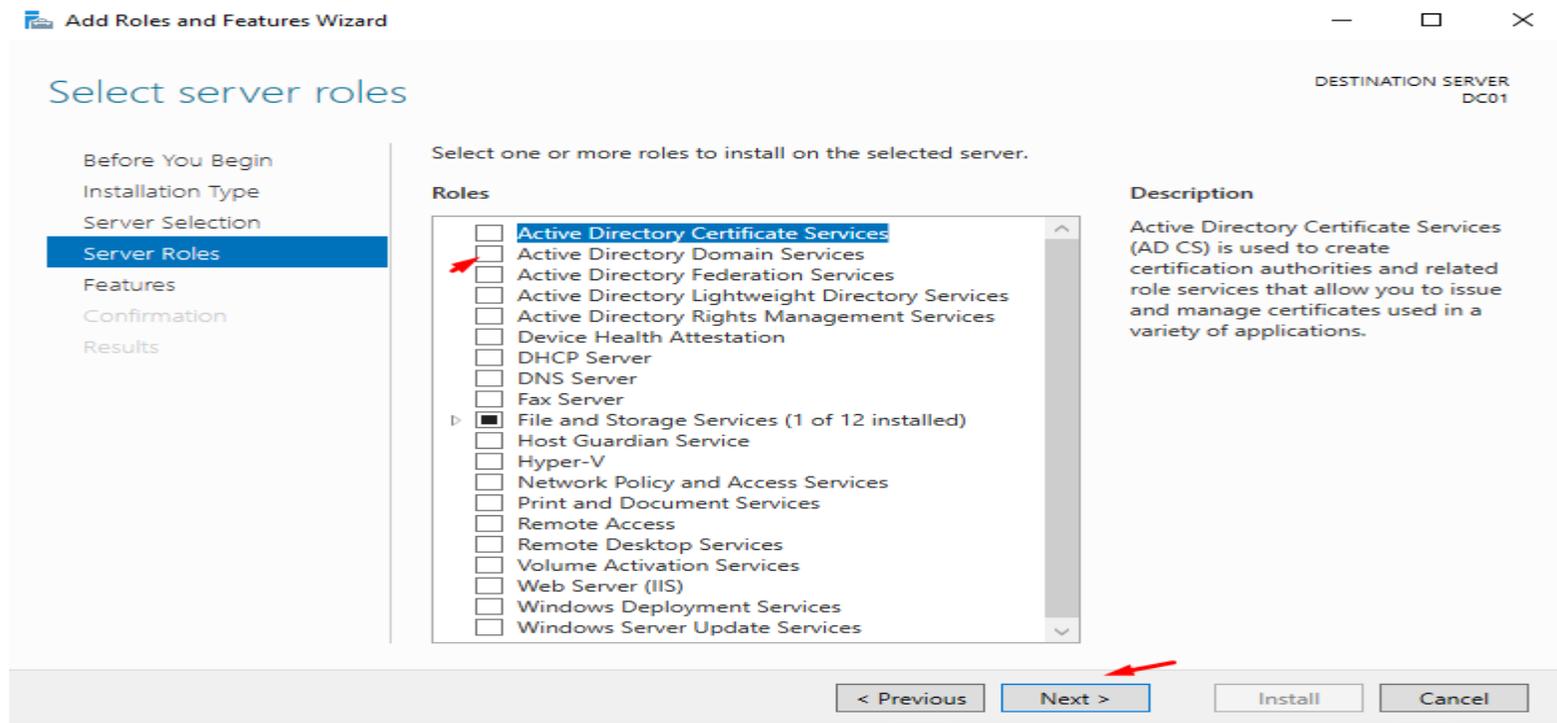
1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

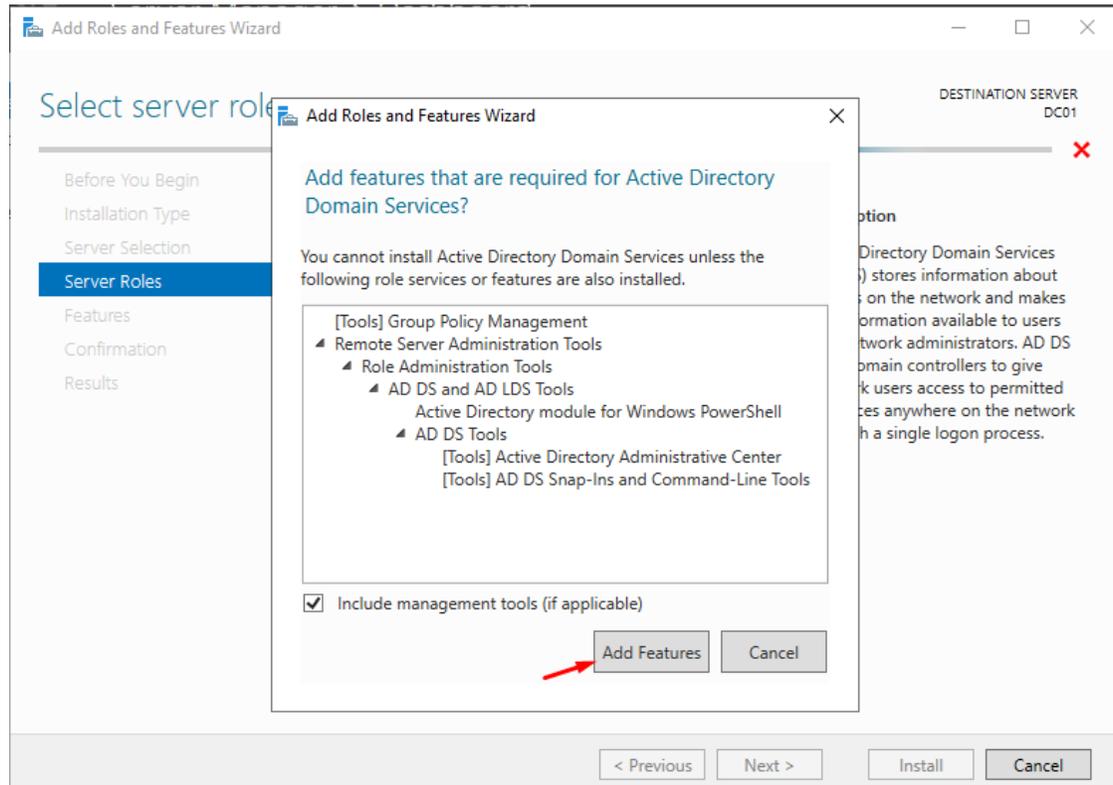
< Previous Next > Install Cancel

Lab Setup

Select Active Directory DomainService and Click add features

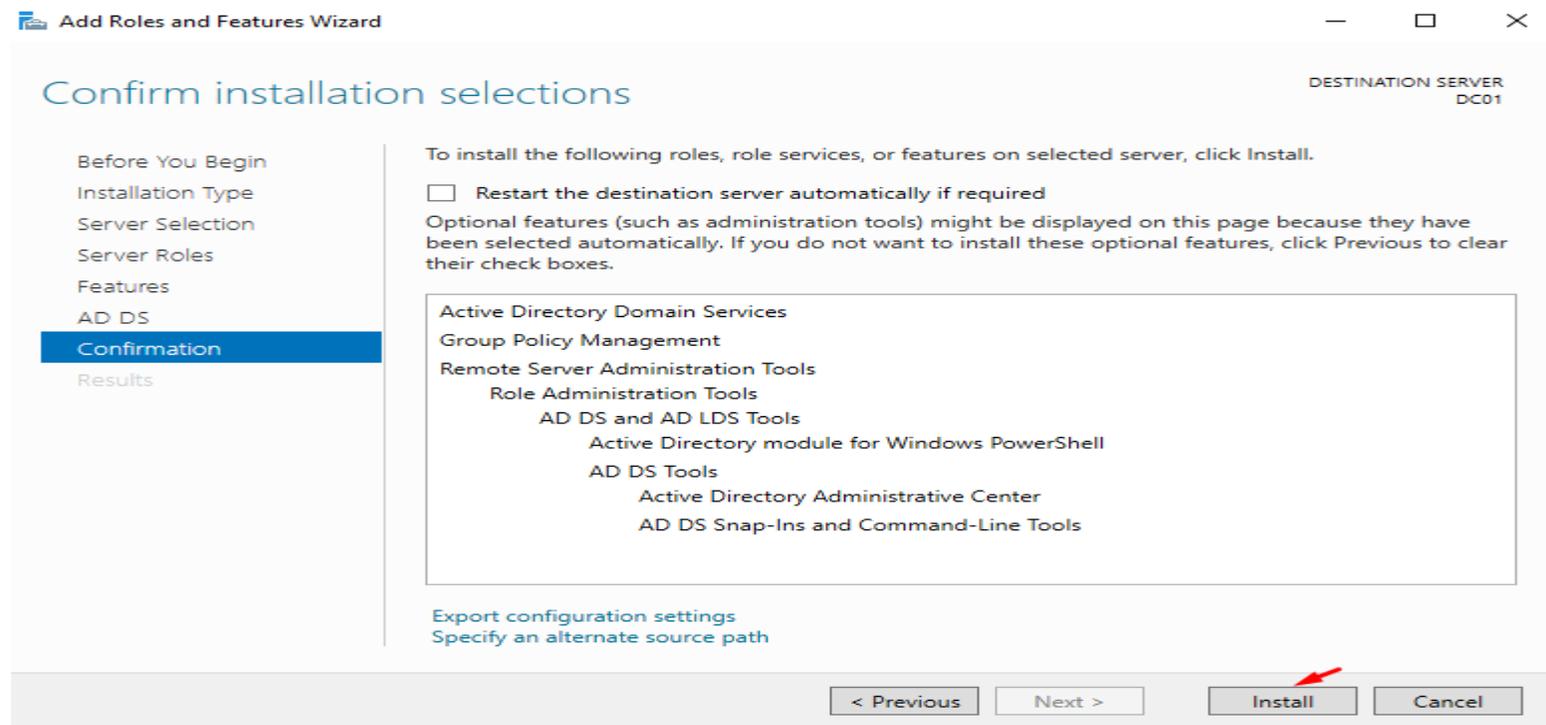


Lab Setup



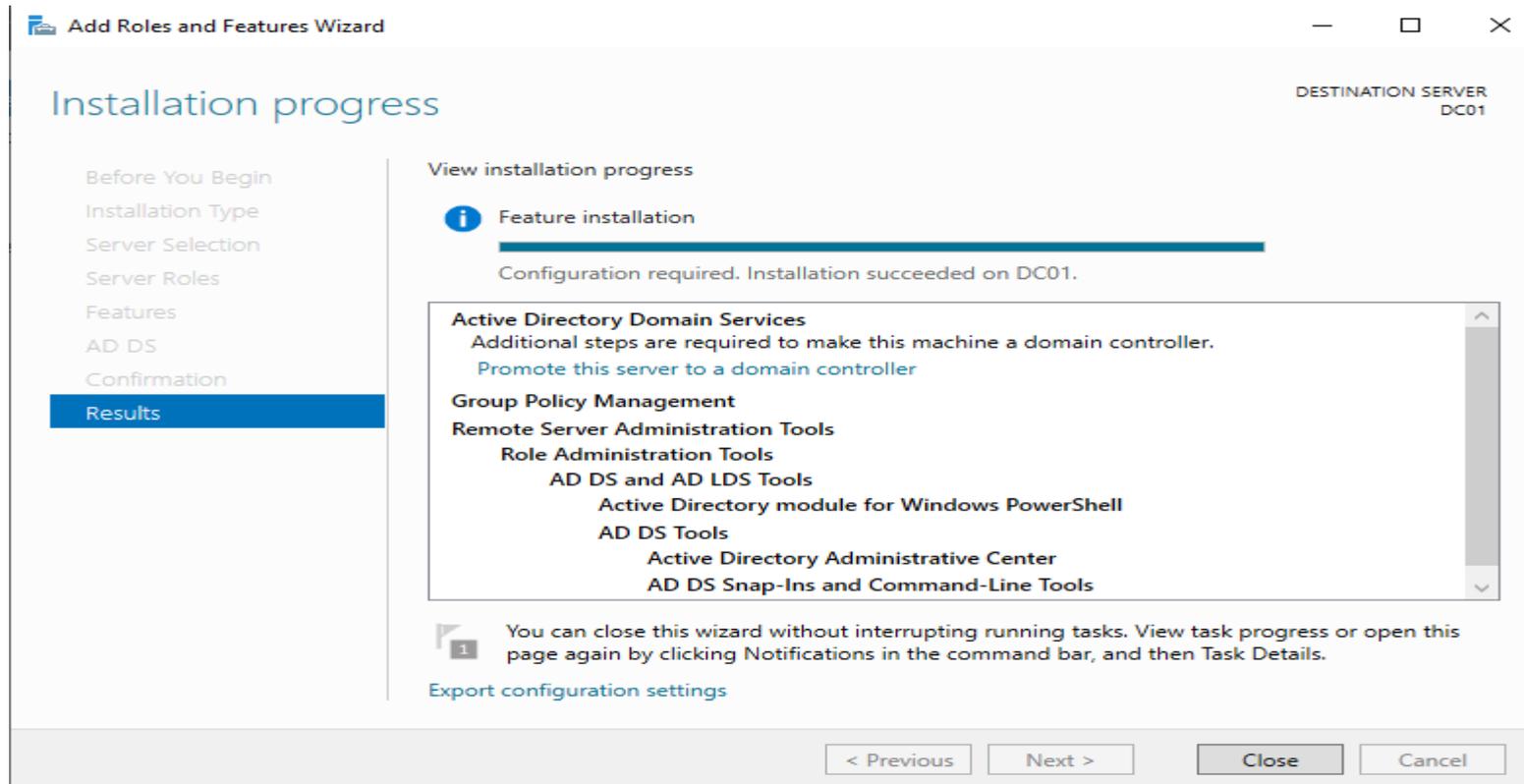
Lab Setup

Next to Install



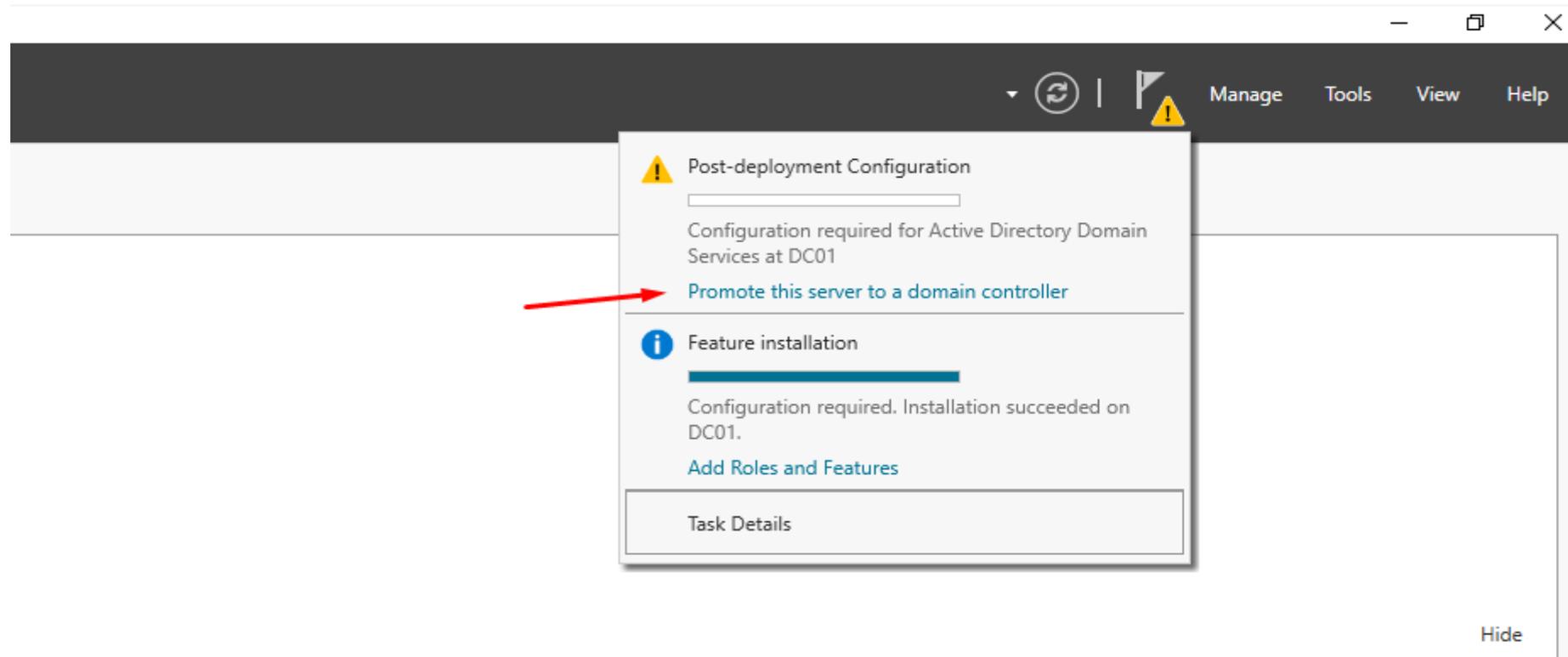
Lab Setup

After the installation click close



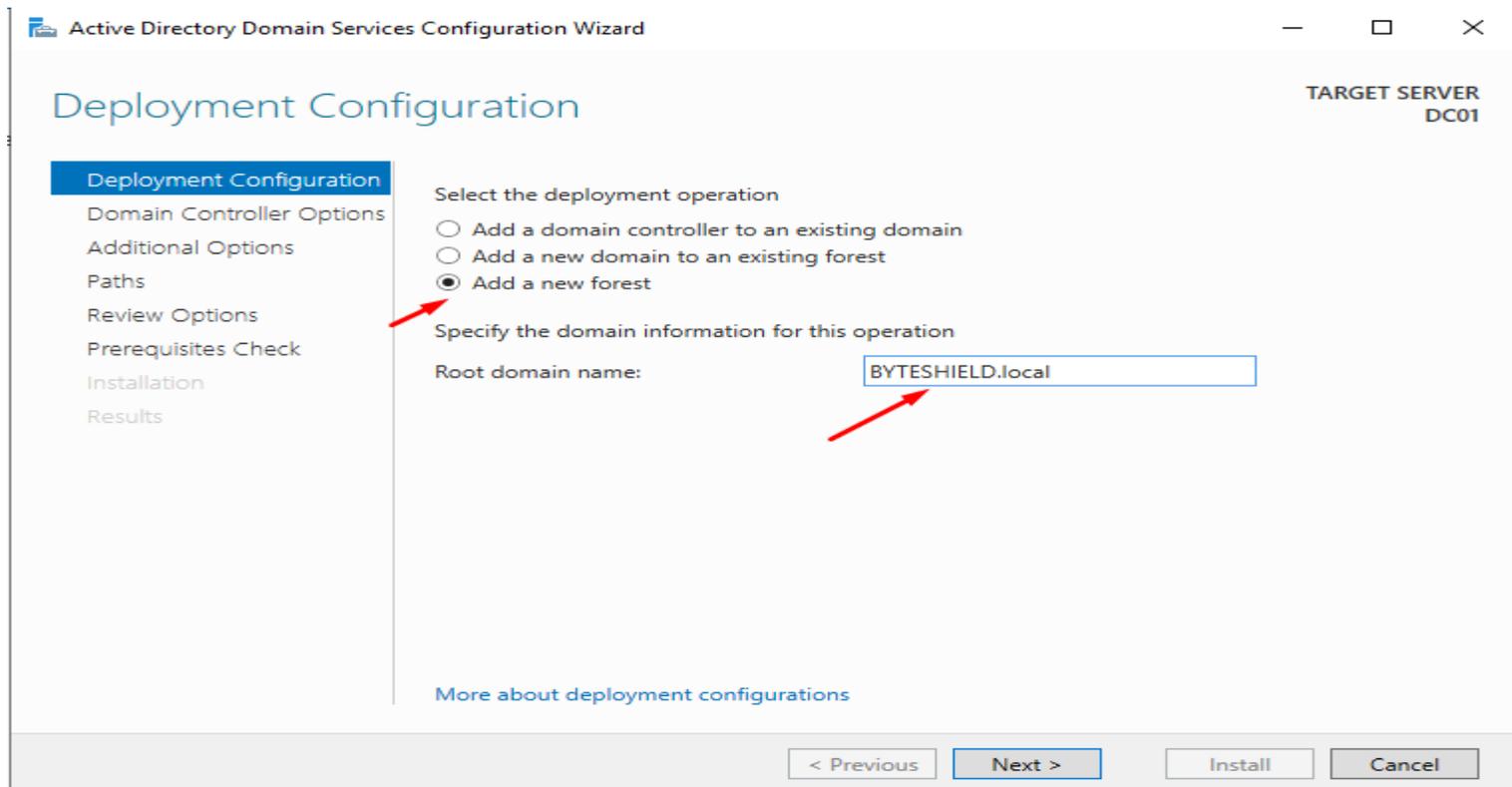
Lab Setup

Installing Domain Controller



Lab Setup

Adding new forest and FQDN



Active Directory Domain Services Configuration Wizard

TARGET SERVER
DC01

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:

[More about deployment configurations](#)

< Previous Next > Install Cancel

Lab Setup

Creating a memorable Domain Services Recovery mode password (DSRM)

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the application name and standard window controls. The main title is 'Domain Controller Options' for 'TARGET SERVER DC01'. A left-hand navigation pane lists steps: Deployment Configuration, Domain Controller Options (highlighted), DNS Options, Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. The main area is titled 'Select functional level of the new forest and root domain' and contains two dropdown menus: 'Forest functional level' and 'Domain functional level', both set to 'Windows Server 2016'. Below this is the 'Specify domain controller capabilities' section with three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). The 'Type the Directory Services Restore Mode (DSRM) password' section has two password input fields, both filled with dots. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
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:

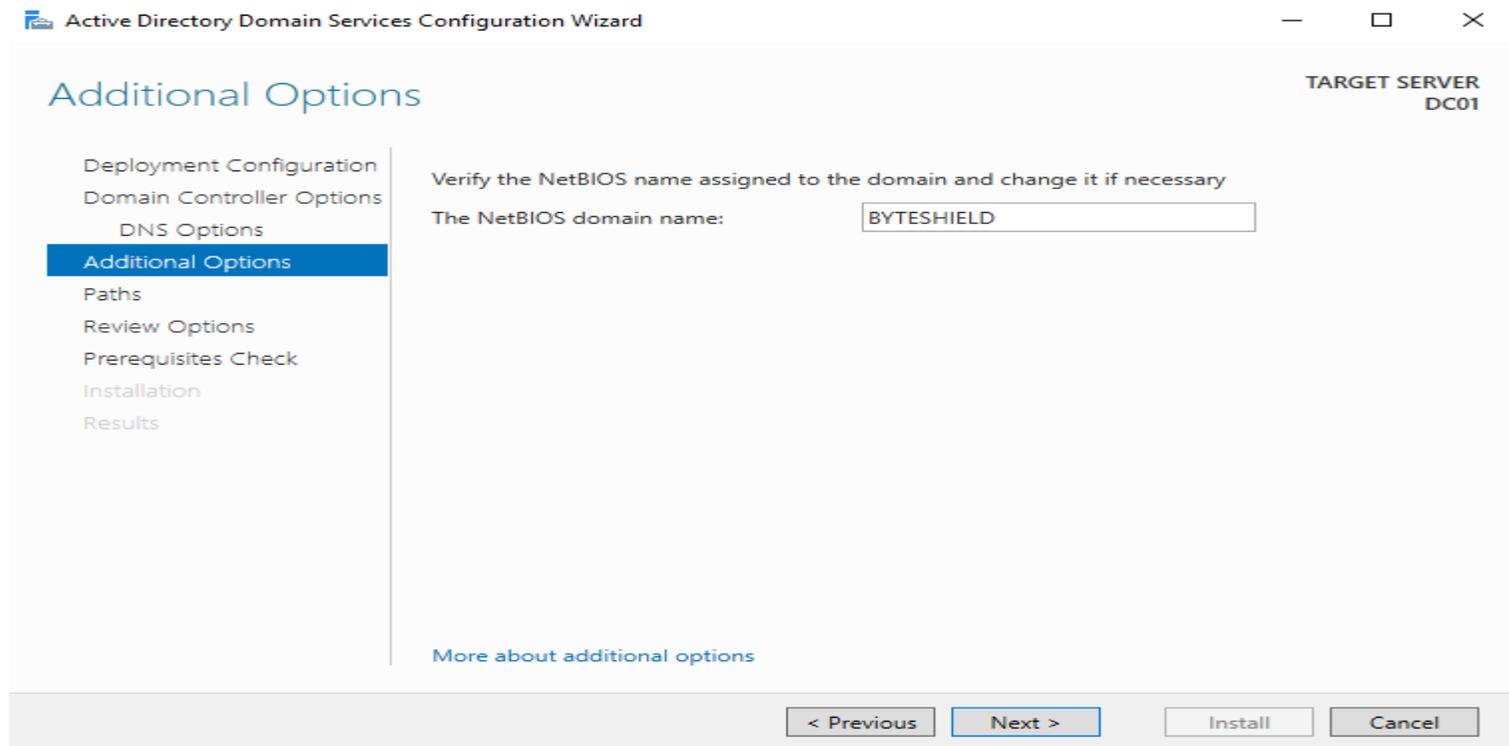
Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

Lab Setup

Next > Next > Install to Finish



Lab Setup

AD-DS and Domain Controller has been Successfully installed



Lab Setup

Network Configuration, ipconfig shows the dynamic ip address, let's make it static

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::16c:55bb:130f:60e1%3
    IPv4 Address. . . . . : 10.10.1.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.1.1
PS C:\Users\Administrator>
```

Lab Setup

Network Settings

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: 10 . 10 . 1 . 4

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 10 . 1 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 127 . 0 . 0 . 1

Alternate DNS server: 8 . 8 . 8 . 8

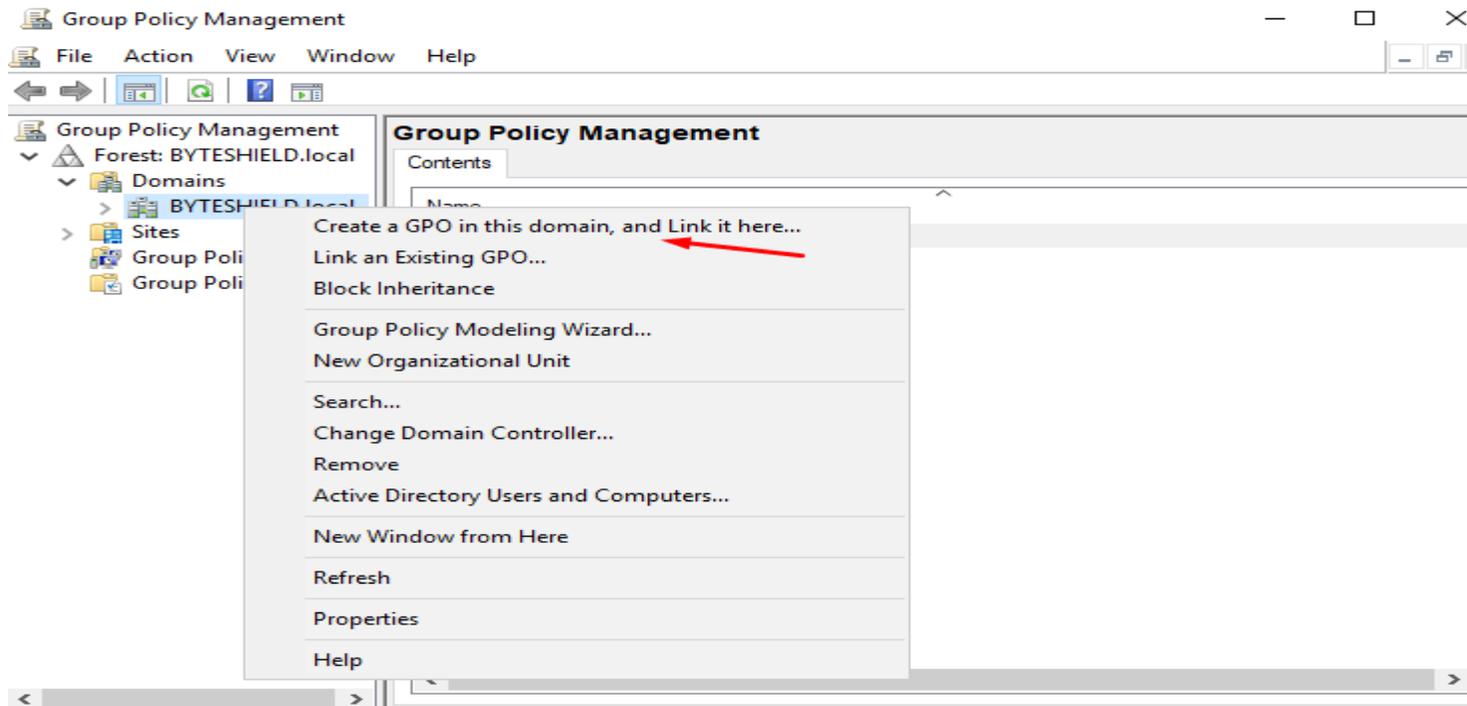
Validate settings upon exit

Advanced...

OK Cancel

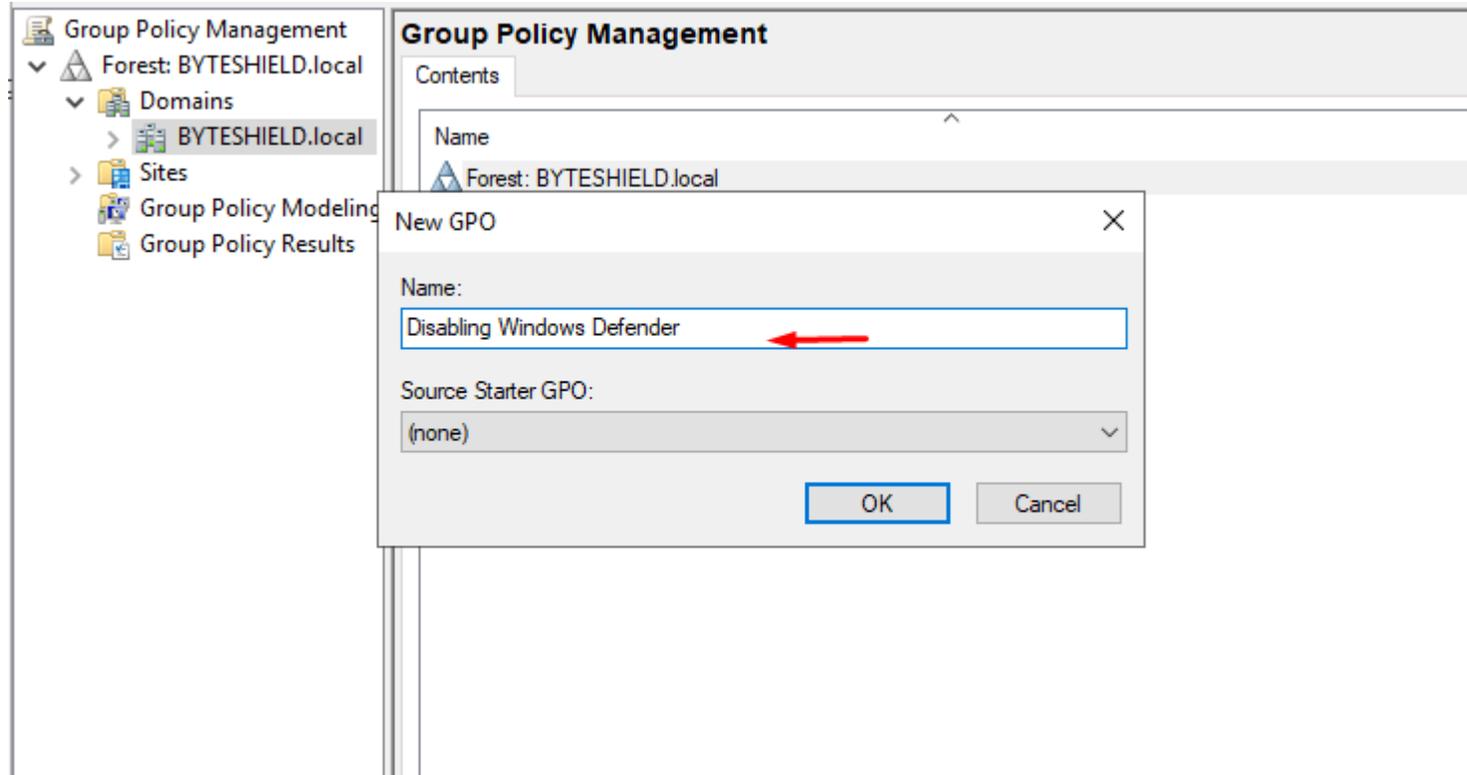
Lab Setup

Creating Policy to Disable Windows Defender



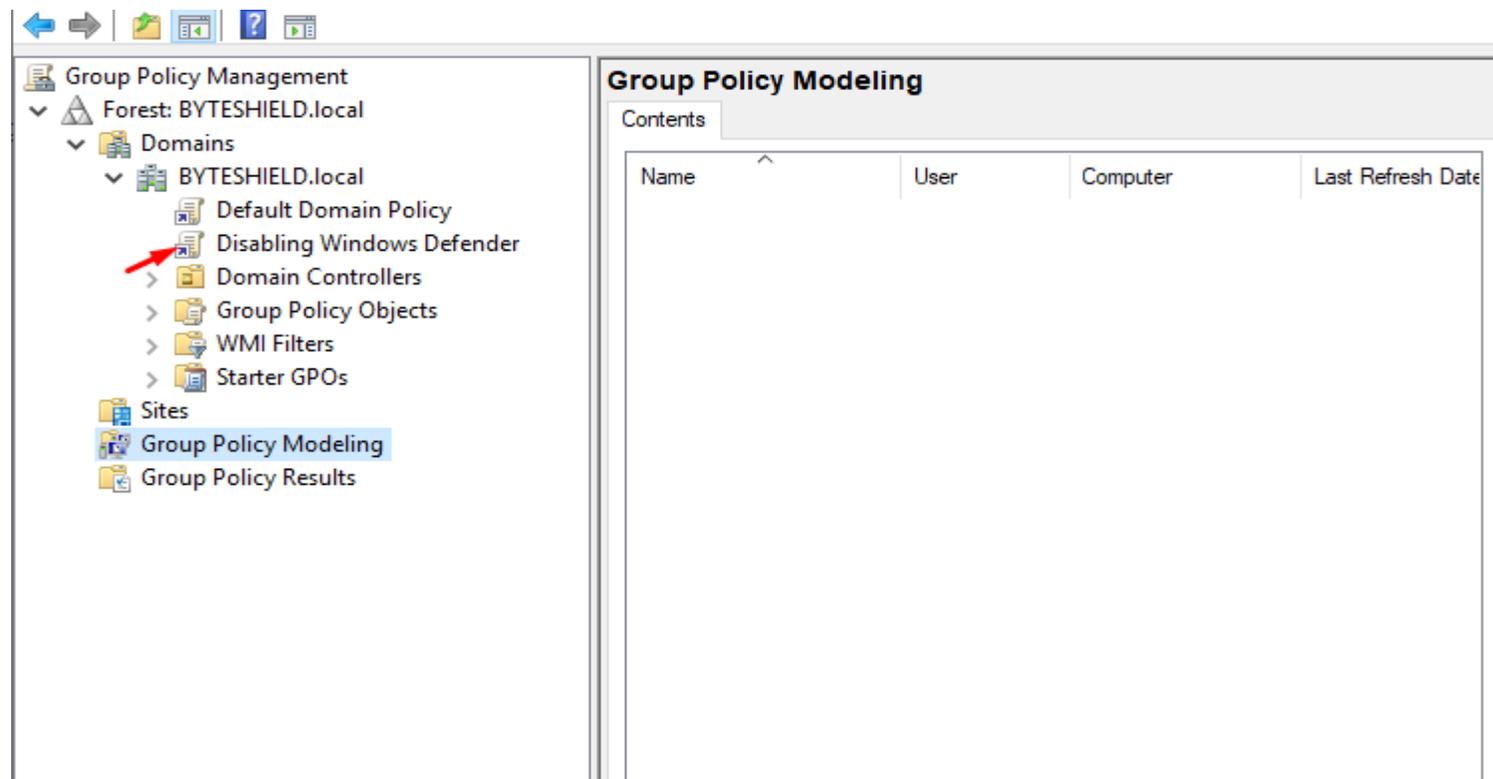
Lab Setup

Naming the Policy

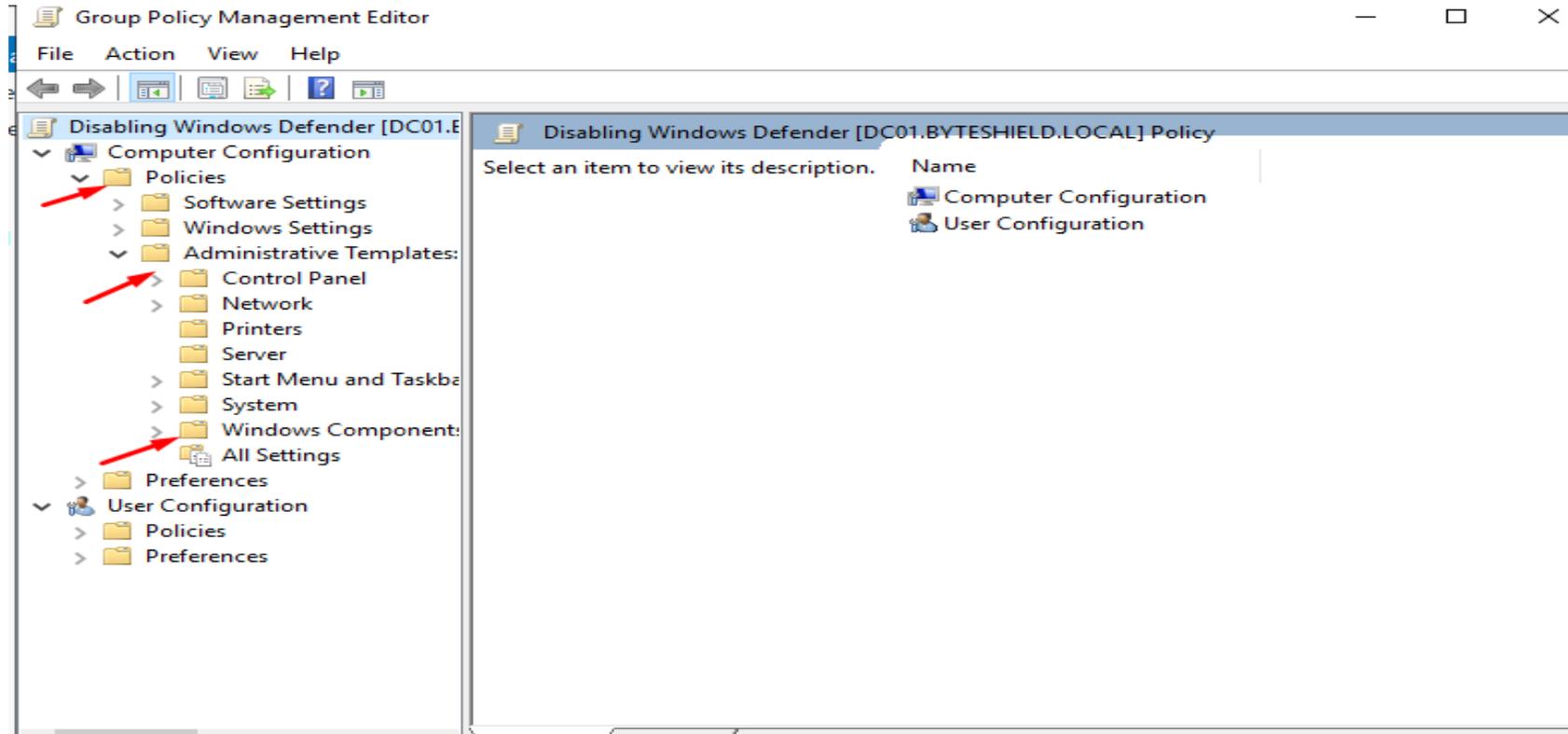


Lab Setup

Now right click on the policy you just created and click edit to edit it

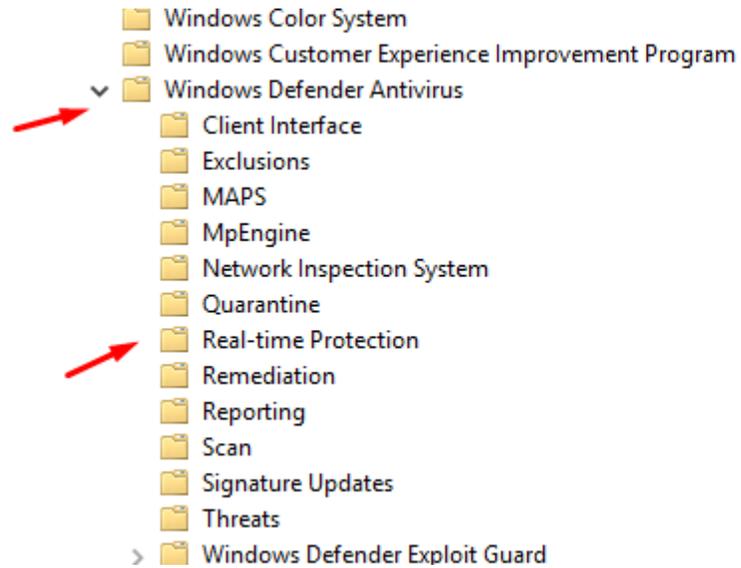


Lab Setup



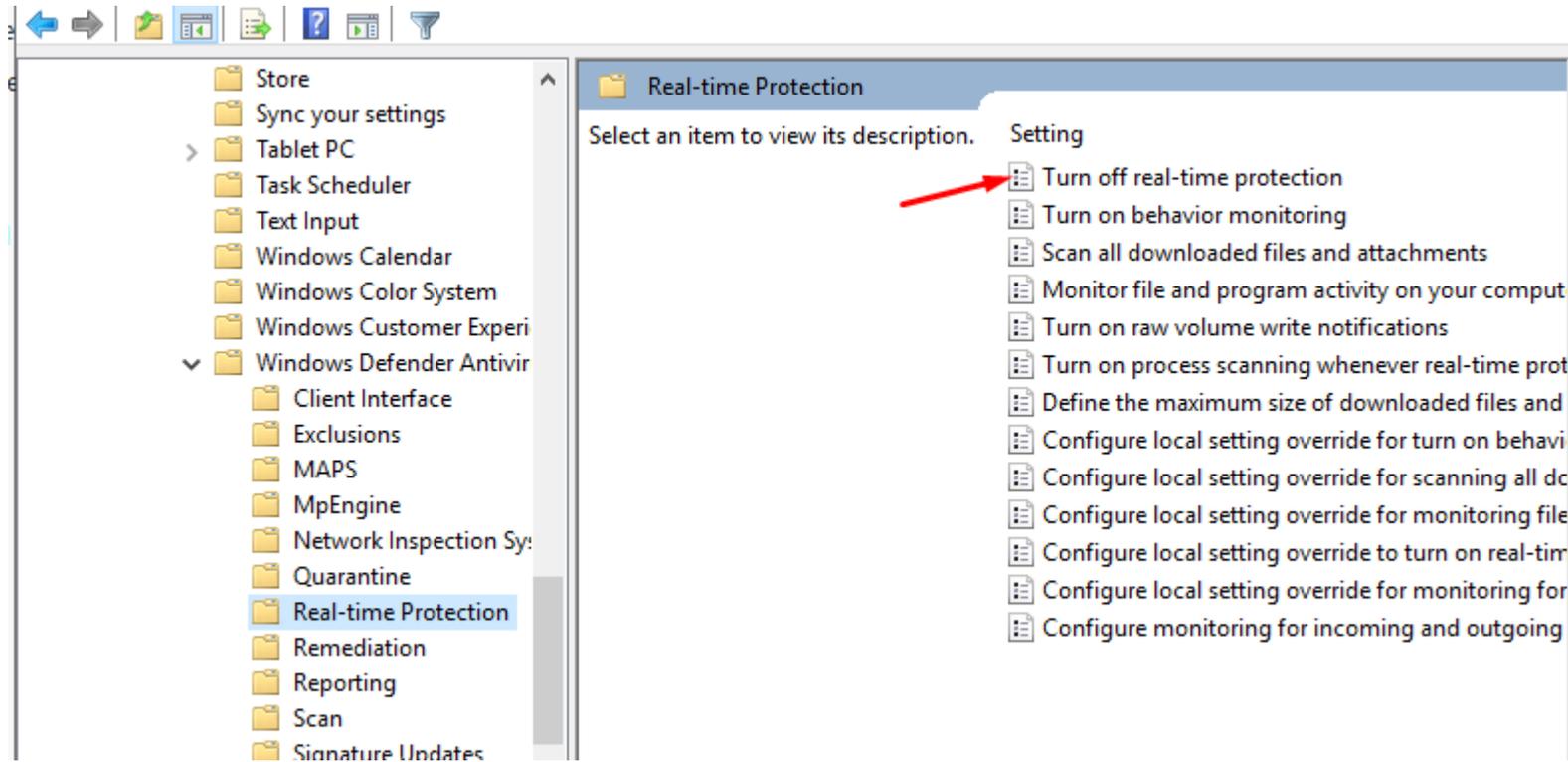
Lab Setup

Scroll Down to Select windows defender antivirus and real-time protection



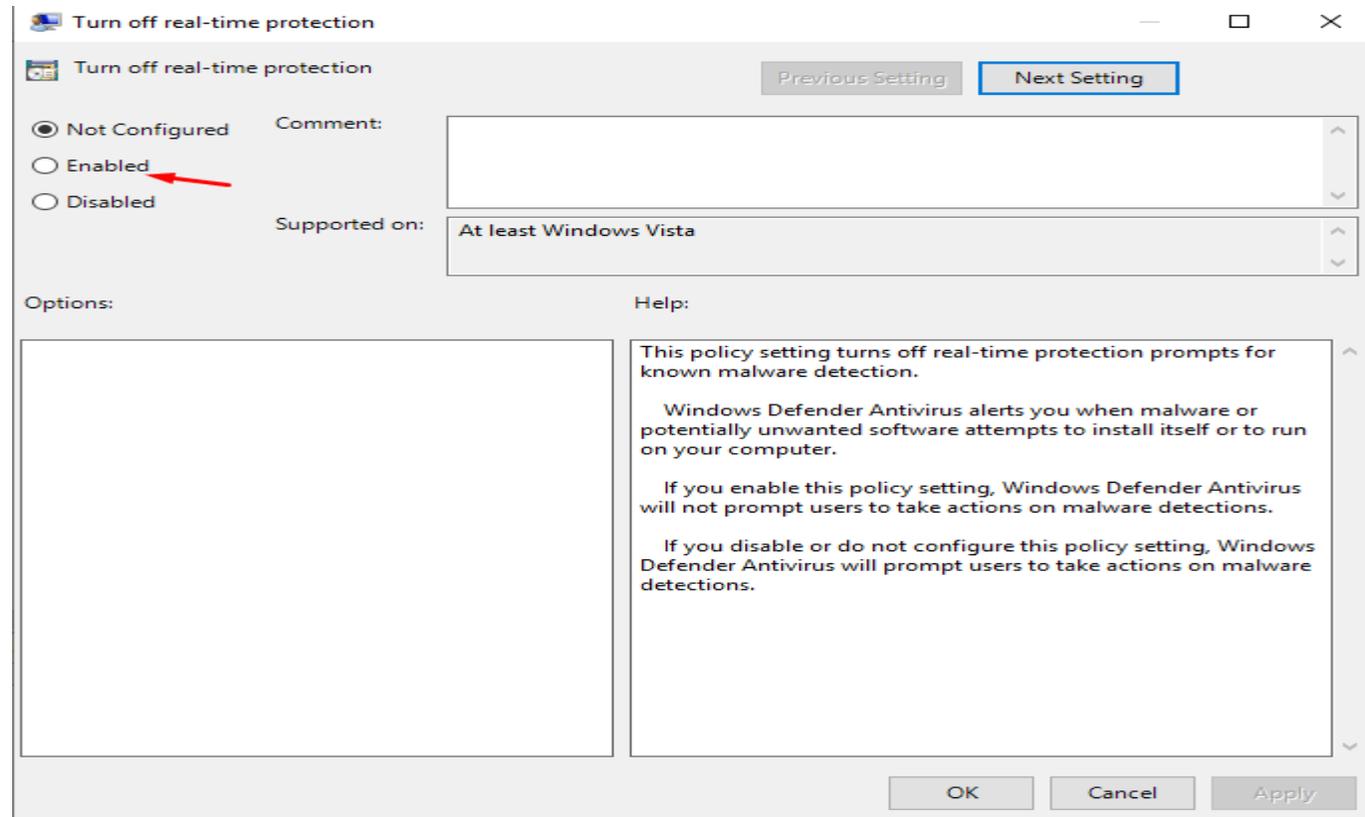
Lab Setup

Double Click on turn off real-time Protection



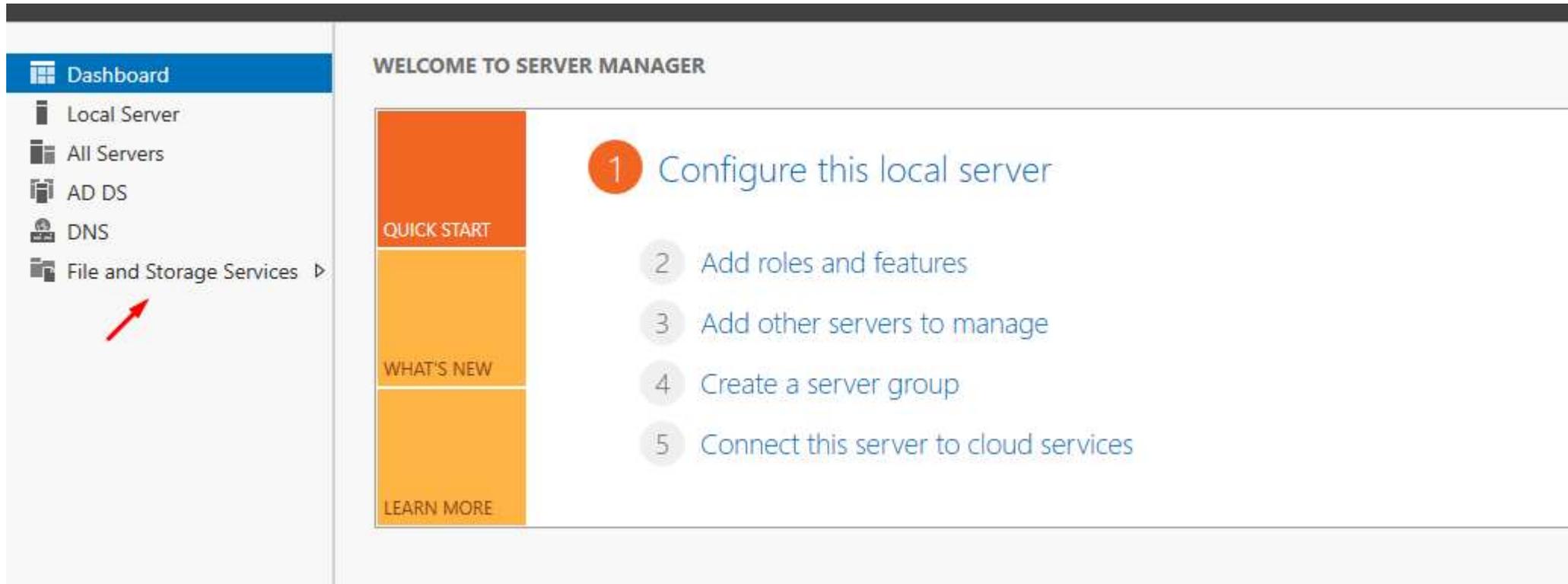
Lab Setup

Select enable and Ok



Lab Setup

Creating Smb Share



The screenshot displays the Windows Server Manager interface. On the left, a navigation pane lists several options: Dashboard, Local Server, All Servers, AD DS, DNS, and File and Storage Services. A red arrow points to the 'File and Storage Services' option. The main area of the interface is titled 'WELCOME TO SERVER MANAGER' and features a 'QUICK START' section with a numbered list of five steps:

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

Below the 'QUICK START' section, there are two additional sections: 'WHAT'S NEW' and 'LEARN MORE'.

Lab Setup

SERVERS
All servers | 1 total

Filter 🔍

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
DC01	10.10.1.4	Online - Performance counters not started	11/17/2023 4:32:51 PM	Not activated

Lab Setup

The screenshot shows the Windows File Explorer interface for the 'SHARES' section. The top bar includes a search filter, view icons, and a 'TASKS' dropdown menu. A red arrow points to the 'TASKS' menu, which is open, showing options for 'New Share...' and 'Refresh'. Below the top bar is a table of shares, and to the right is a 'VOLUME' section for 'NETLOGON on DC01' showing a progress bar for disk usage.

SHARES
All shares | 2 total

Filter [] [] [] []

TASKS ▼

- New Share...
- Refresh

Share	Local Path	Protocol	Availability Type
DC01 (2)			
NETLOGON	C:\Windows\SYSVOL\sysvo\BYTE...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered

VOLUME
NETLOGON on DC01

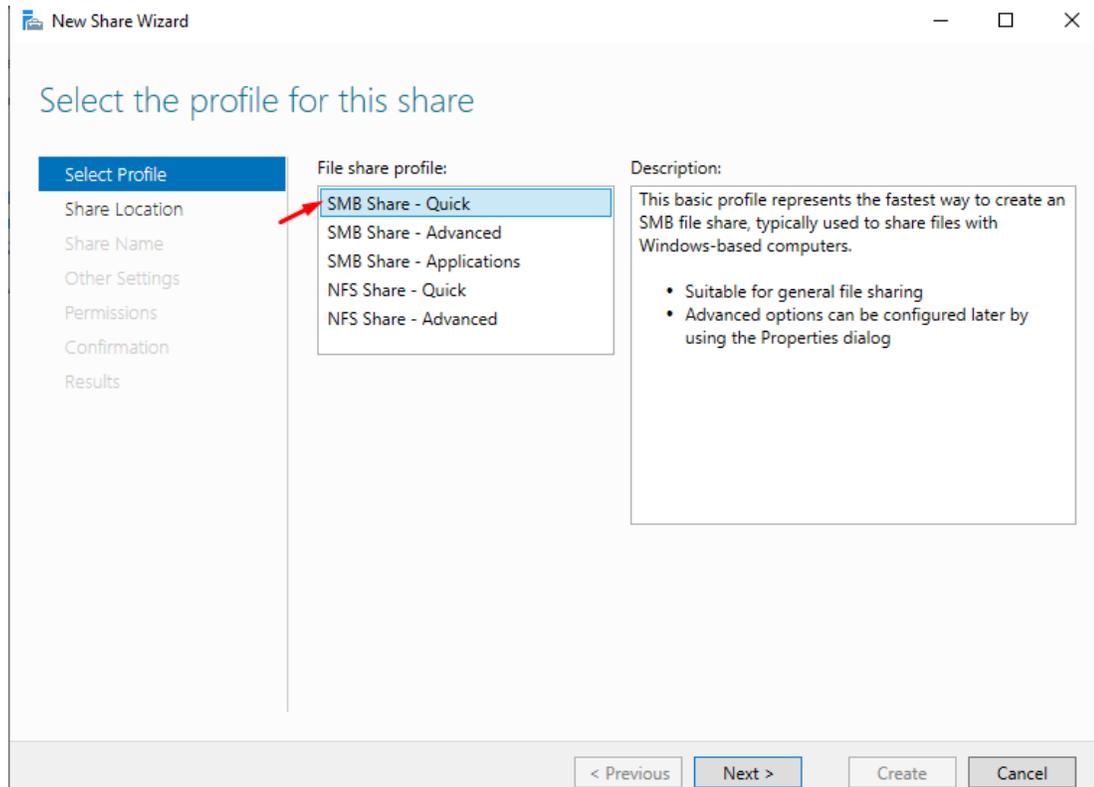
49.5 GB

20.6% Used

10.2 GB Used Space

39.3 GB Free Space

Lab Setup



Lab Setup

New Share Wizard

Specify share name

Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results

Share name:

Share description:

Local path to share:
i If the folder does not exist, the folder is created.

Remote path to share:

< Previous Next > Create Cancel

Lab Setup

Next > Next > Create

Confirm selections

Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results

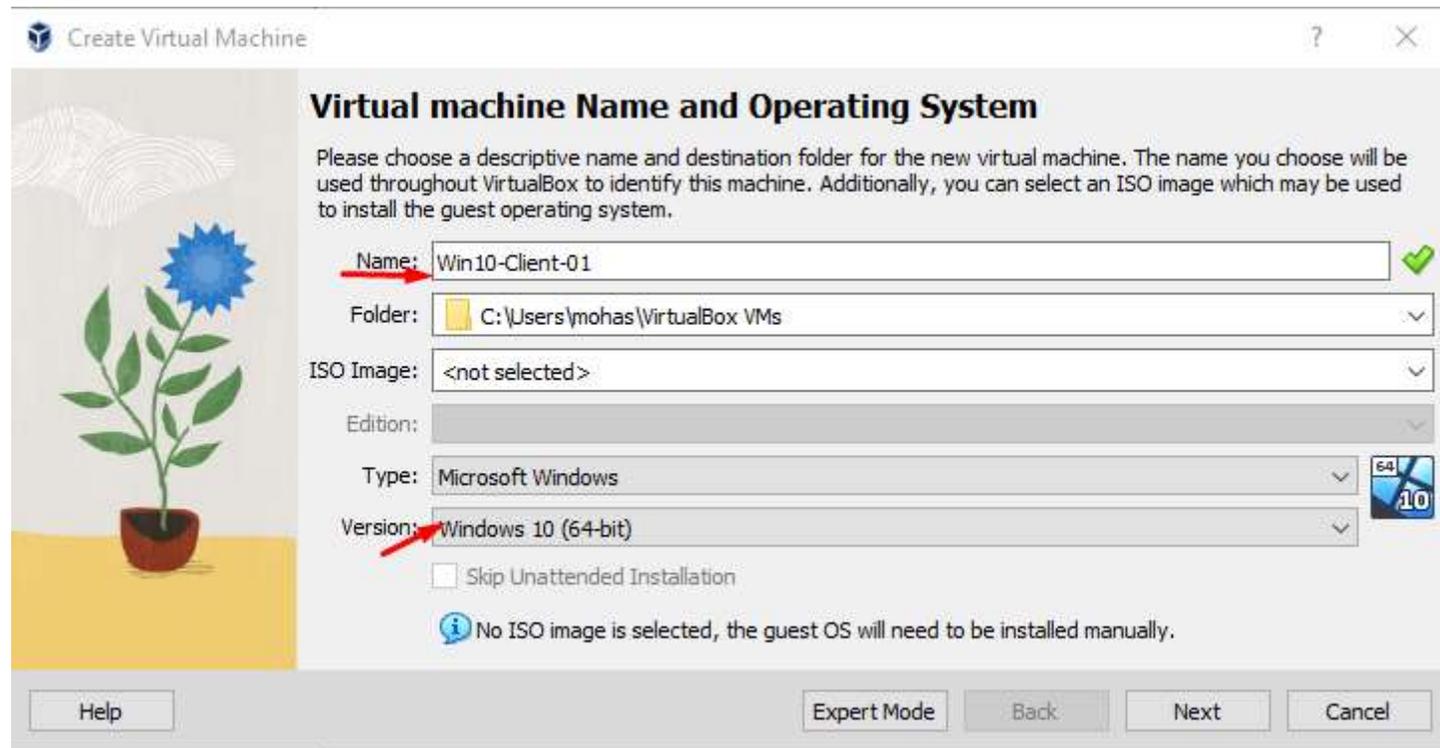
Confirm that the following are the correct settings, and then click Create.

SHARE LOCATION	
Server:	DC01
Cluster role:	Not Clustered
Local path:	C:\Shares\IT-DEPT
SHARE PROPERTIES	
Share name:	IT-DEPT
Protocol:	SMB
Access-based enumeration:	Disabled
Caching:	Enabled
BranchCache:	Disabled
Encrypt data:	Disabled

< Previous Next > Create Cancel

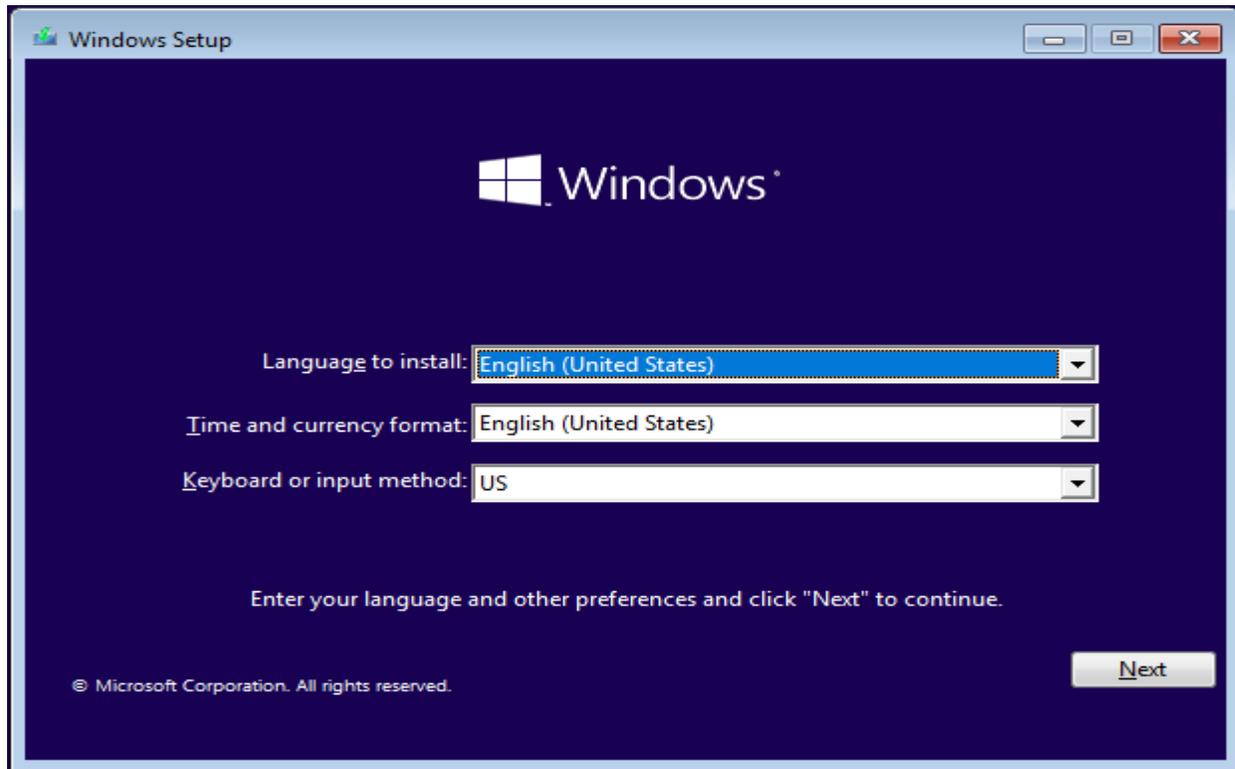
Lab Setup

Installing Windows 10 Enterprise edition



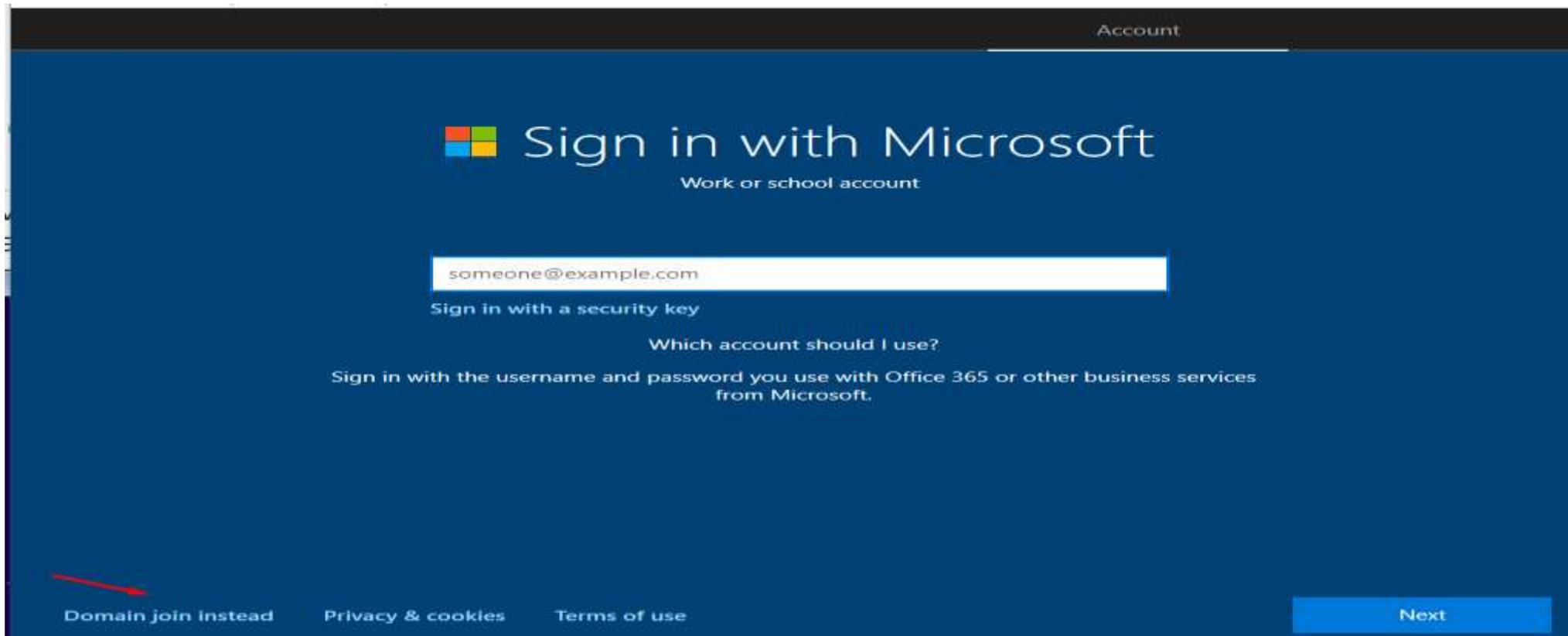
Lab Setup

We are going to go with the default setting as we did on the Domain Controller, the same way we installed the DC



Lab Setup

When you get to this level instead of Creating a local user click join domain instead



Lab Setup

Creating User

Who's going to use this PC?
What name do you want to use?



Or, even better, use an online account

Next

Lab Setup

Create a memorable Password and Confirm it



A white circular icon containing a stylized human figure, representing a user profile, centered on a dark blue background.

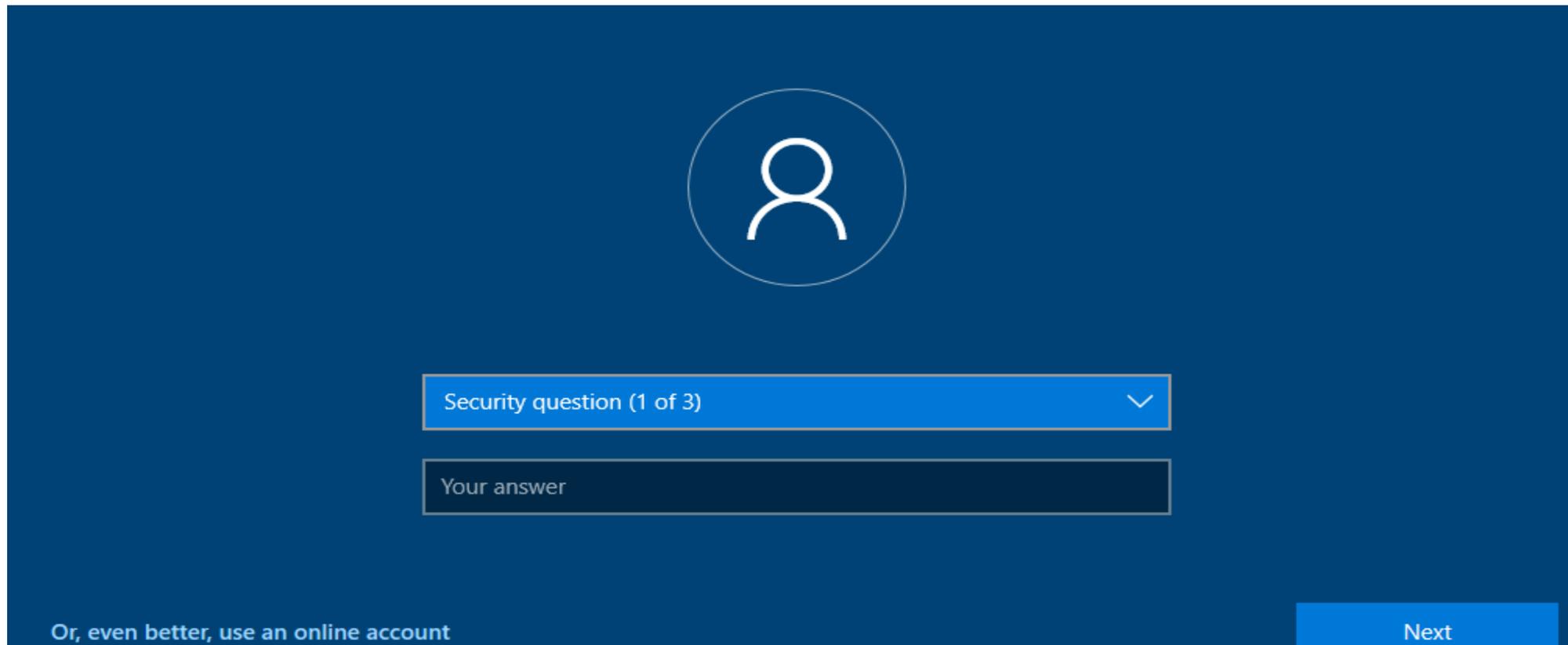
A white password input field with a blue border. The field contains ten black dots representing a masked password and a vertical cursor line at the end. A small eye icon is visible on the right side of the field.

Or, even better, use an online account

Next

Lab Setup

Select 3 memorable Security question and move on



Security question (1 of 3) ▾

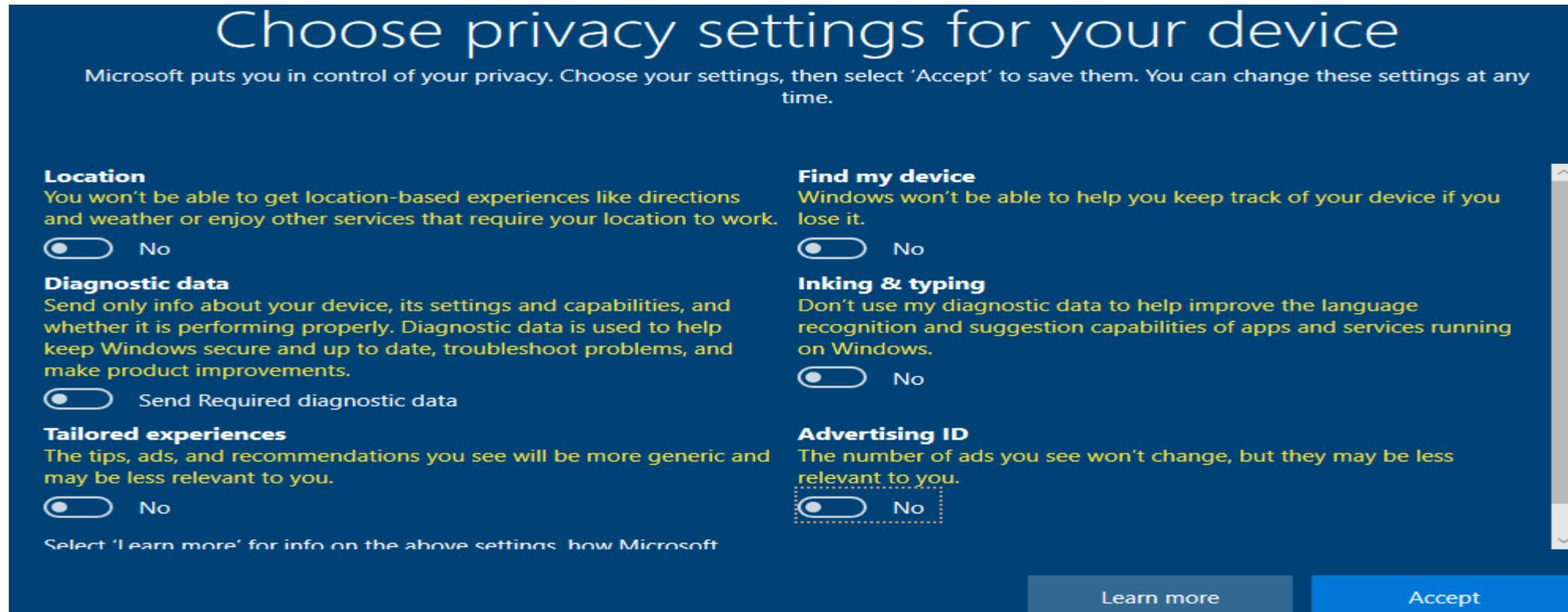
Your answer

Or, even better, use an online account

Next

Lab Setup

Accept

A screenshot of a Windows privacy settings screen with a dark blue background and white text. The title is "Choose privacy settings for your device". Below it is a sub-header: "Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time." There are six settings sections, each with a description and a toggle switch. The "Advertising ID" toggle is highlighted with a dashed white box. At the bottom right are two buttons: "Learn more" and "Accept".

Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.

Location
You won't be able to get location-based experiences like directions and weather or enjoy other services that require your location to work.
 No

Diagnostic data
Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements.
 Send Required diagnostic data

Tailored experiences
The tips, ads, and recommendations you see will be more generic and may be less relevant to you.
 No

Select 'Learn more' for info on the above settings, how Microsoft

Find my device
Windows won't be able to help you keep track of your device if you lose it.
 No

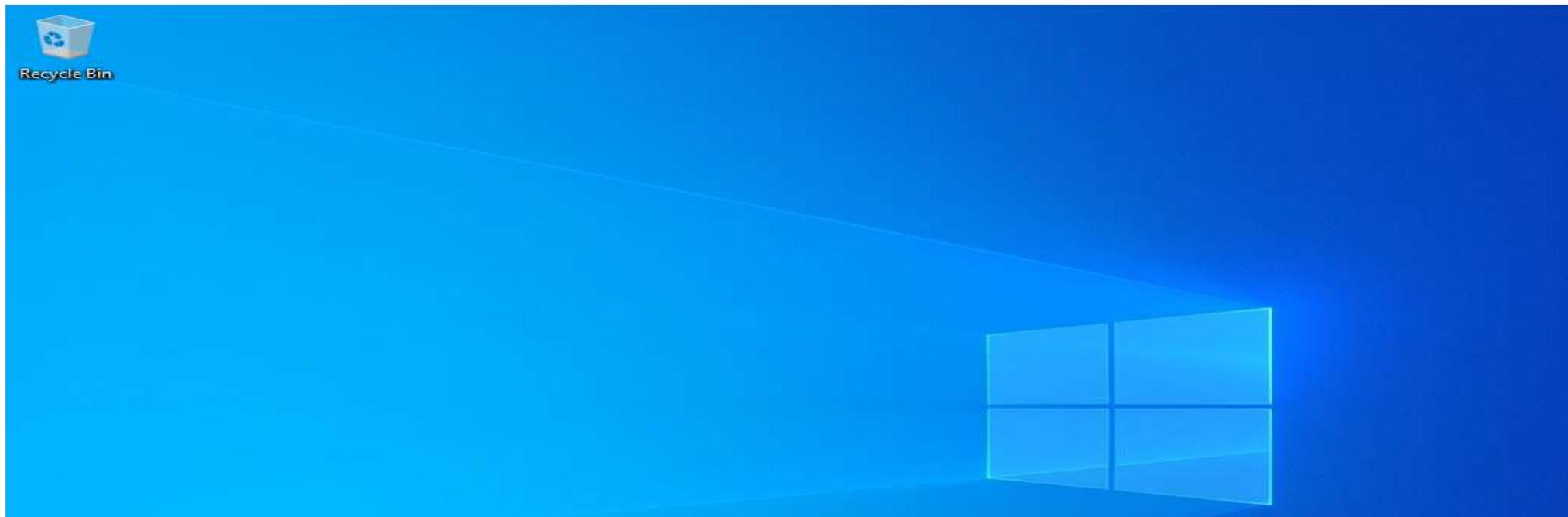
Inking & typing
Don't use my diagnostic data to help improve the language recognition and suggestion capabilities of apps and services running on Windows.
 No

Advertising ID
The number of ads you see won't change, but they may be less relevant to you.
 No

Learn more Accept

Lab Setup

Windows Successfully Installed, you can install guest edition cd and change PC name as Win10-Client-01 the same way you did on the Domain Controller



Lab Setup

Joining the Client to the Domain, Let's Assign static ip address to the Client

Select Windows PowerShell



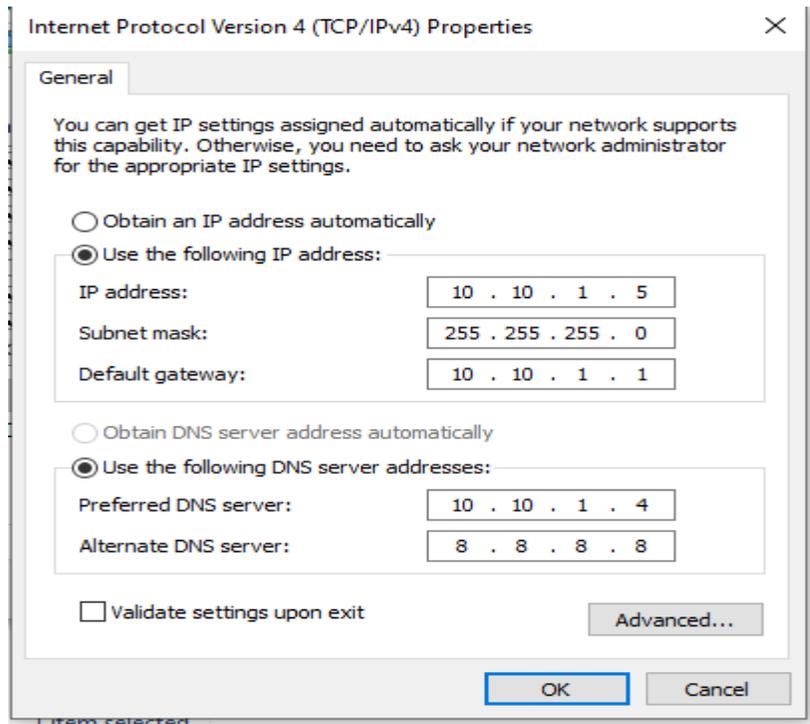
```
Ethernet adapter Ethernet:
```

```
Connection-specific DNS Suffix . . :  
Link-local IPv6 Address . . . . . : fe80::a935:2bad:755:652c%6  
IPv4 Address. . . . . : 10.10.1.5  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.10.1.1
```

```
PS C:\Users\p.brown> █
```

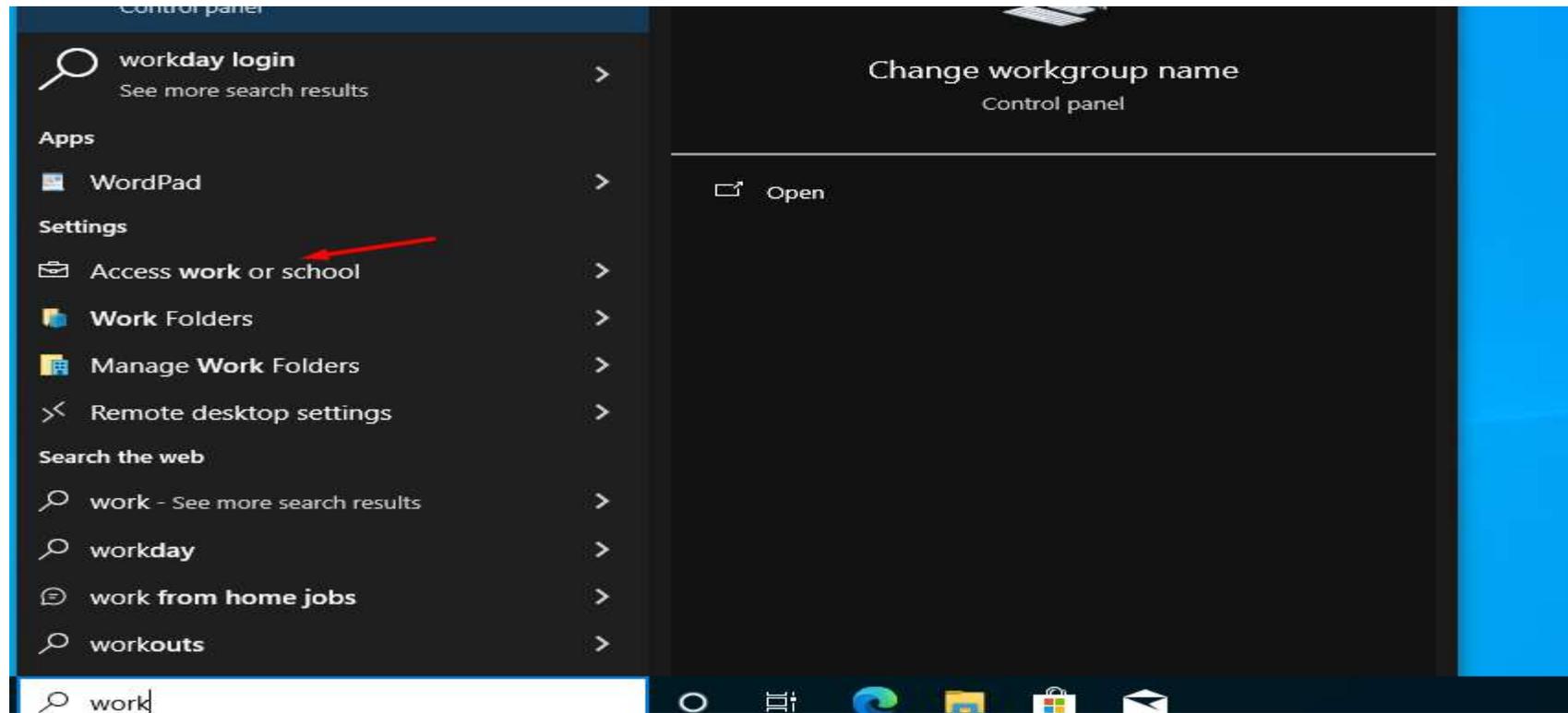
Lab Setup

Here is the network configuration with the Domain Controller as DNS Server



Lab Setup

Joining the Client, search for work or school



Lab Setup

Connect

Accounts

- Your info
- Email & accounts
- Sign-in options
- Access work or school
- Family & other users
- Sync your settings

such as which settings you can change. For specific info about this, ask them.



Related settings

[Add or remove a provisioning package](#)

[Export your management log files](#)

[Set up an account for taking tests](#)

Lab Setup

Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

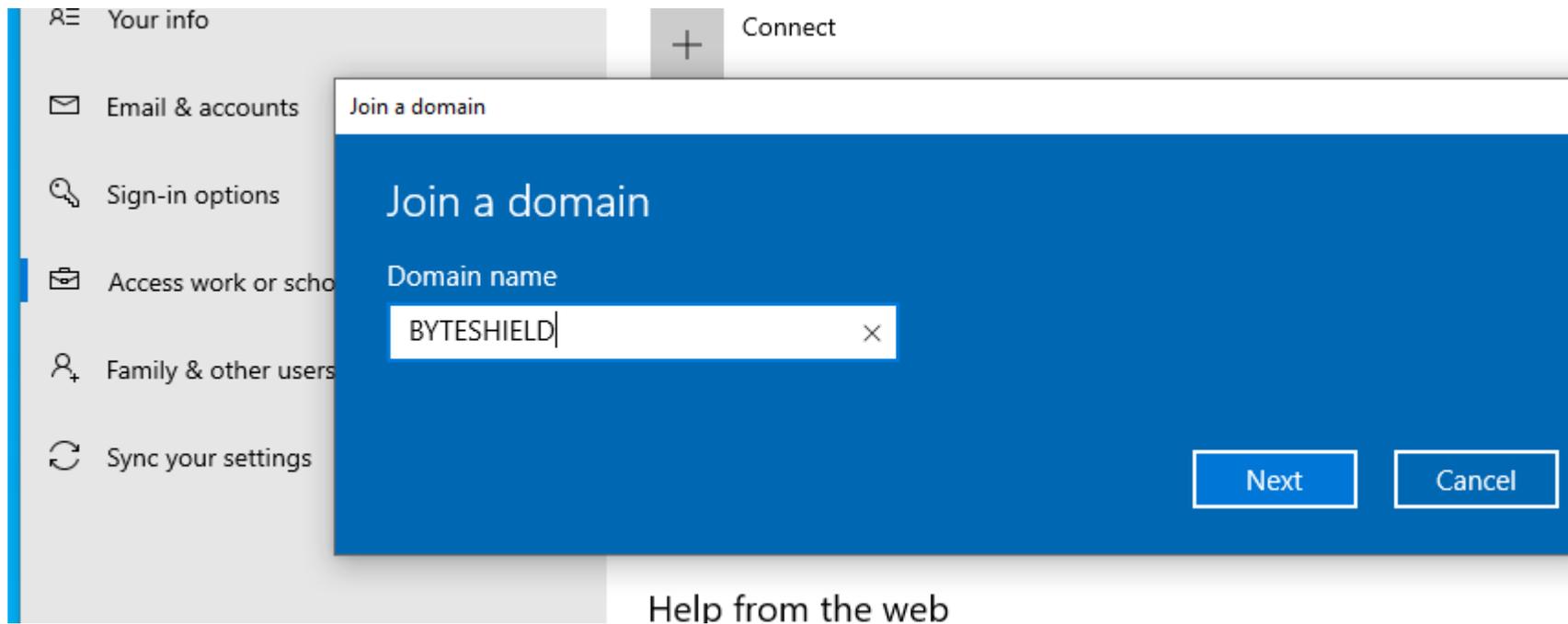
[Join this device to Microsoft Entra ID](#)

[Join this device to a local Active Directory domain](#)

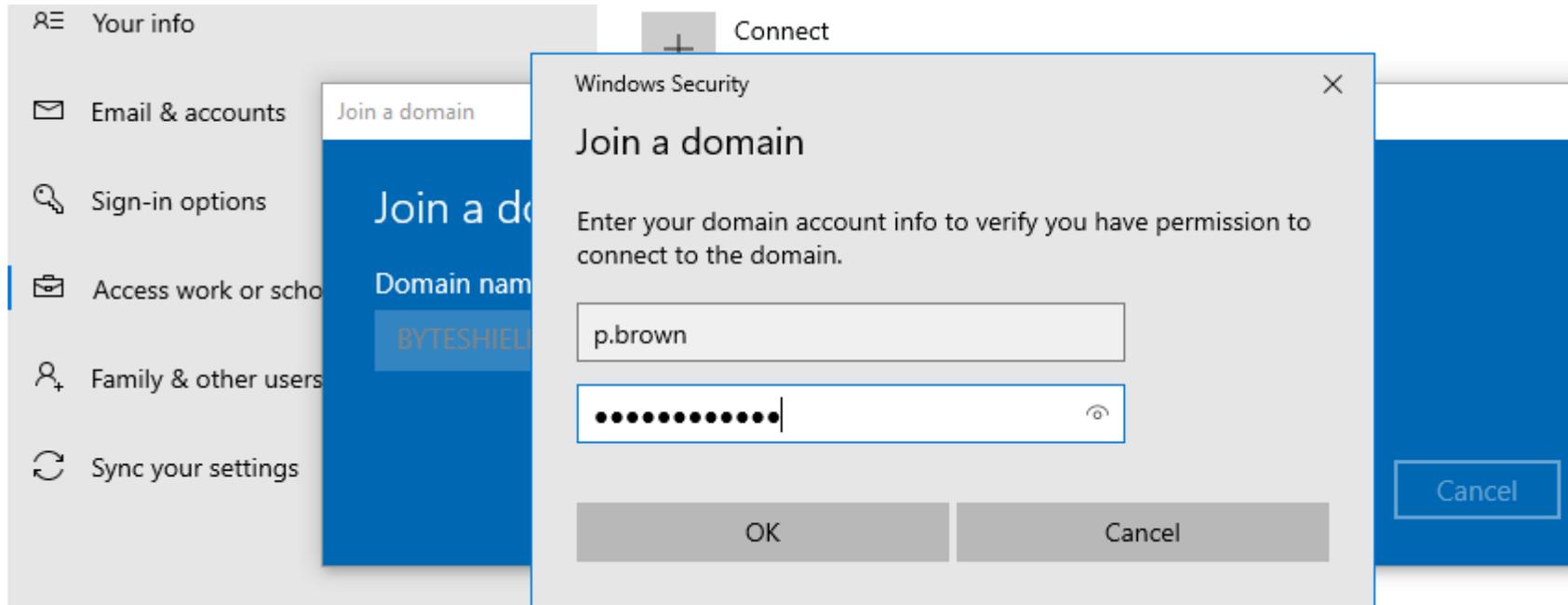


Next

Lab Setup



Lab Setup



Lab Setup

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Family & other users

Sync your settings

such as which settings you can change. For specific info about this, ask them.

Add an account

Add an account

Enter the account info for the person who'll be using this PC. If you skip this step, the person will have default permissions for the domain.

User account

p.brown

Account type

Administrator

Next

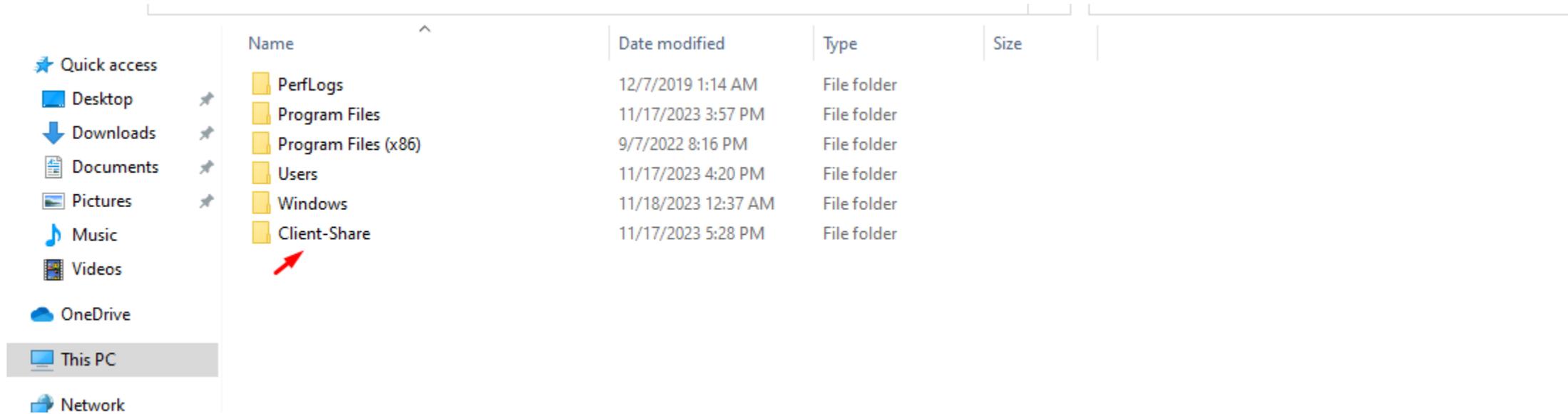
Skip

Solving PC problems remotely

Using Remote Desktop

Lab Setup

Creating Smb Share on Windows Client

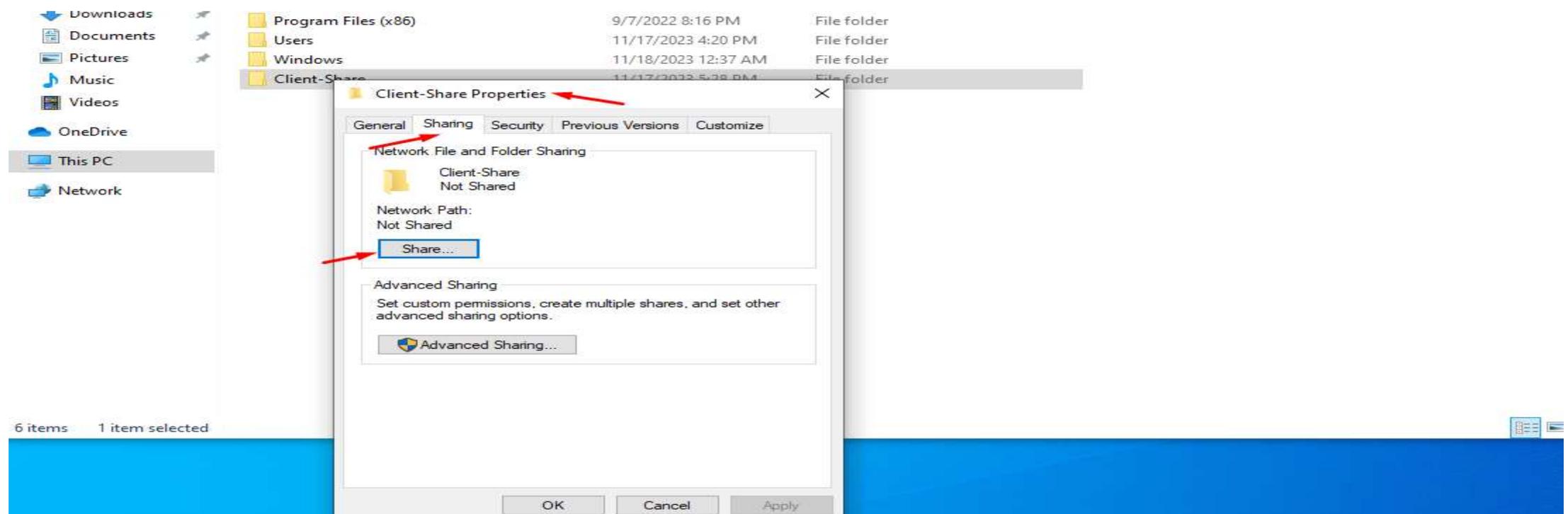


The screenshot shows the Windows File Explorer interface. On the left, the 'This PC' view is selected, showing a sidebar with 'Quick access' and 'This PC' options. The main pane displays a table of folders in the 'C:\' drive. The 'Client-Share' folder is highlighted with a red arrow.

Name	Date modified	Type	Size
PerfLogs	12/7/2019 1:14 AM	File folder	
Program Files	11/17/2023 3:57 PM	File folder	
Program Files (x86)	9/7/2022 8:16 PM	File folder	
Users	11/17/2023 4:20 PM	File folder	
Windows	11/18/2023 12:37 AM	File folder	
Client-Share	11/17/2023 5:28 PM	File folder	

Lab Setup

Right Click and go the Properties and share it



Lab Setup

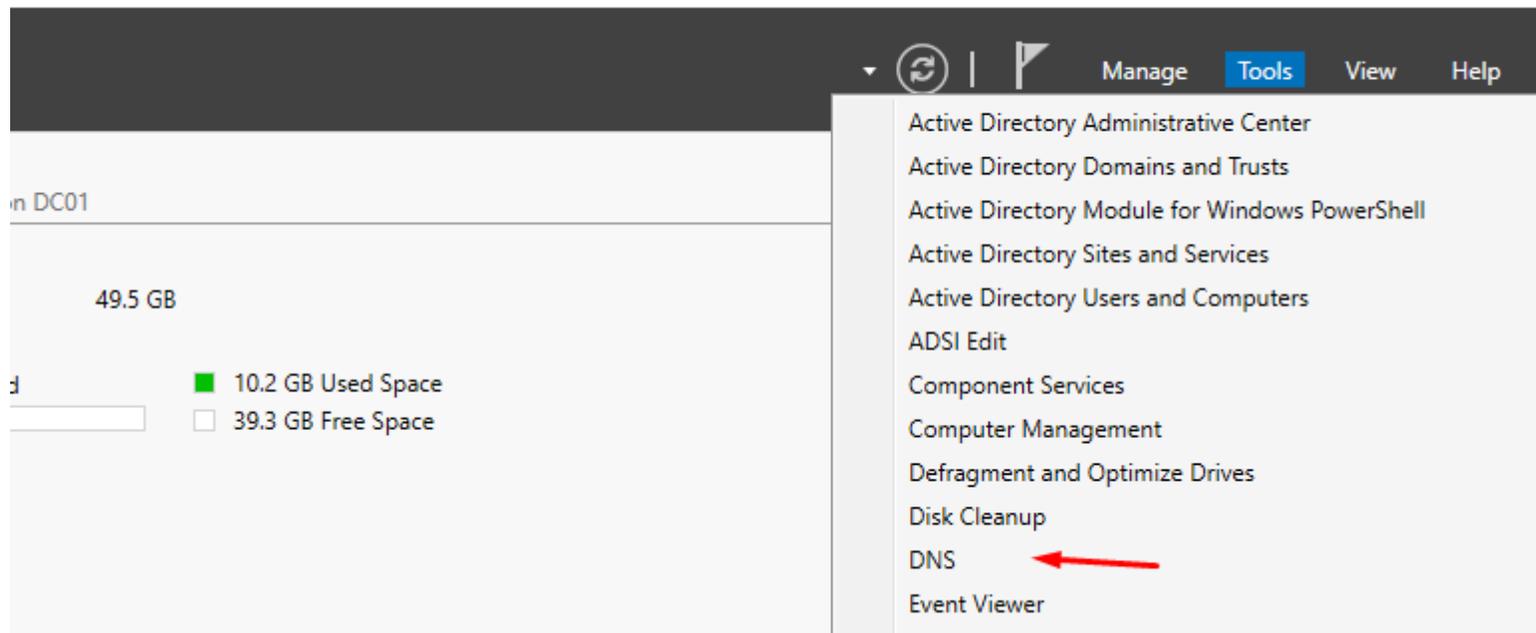
Now we are done setting up Win10-Client-01 Machine

Instruction

Replicate the same process to create another Machine and name it Win10-Client-02

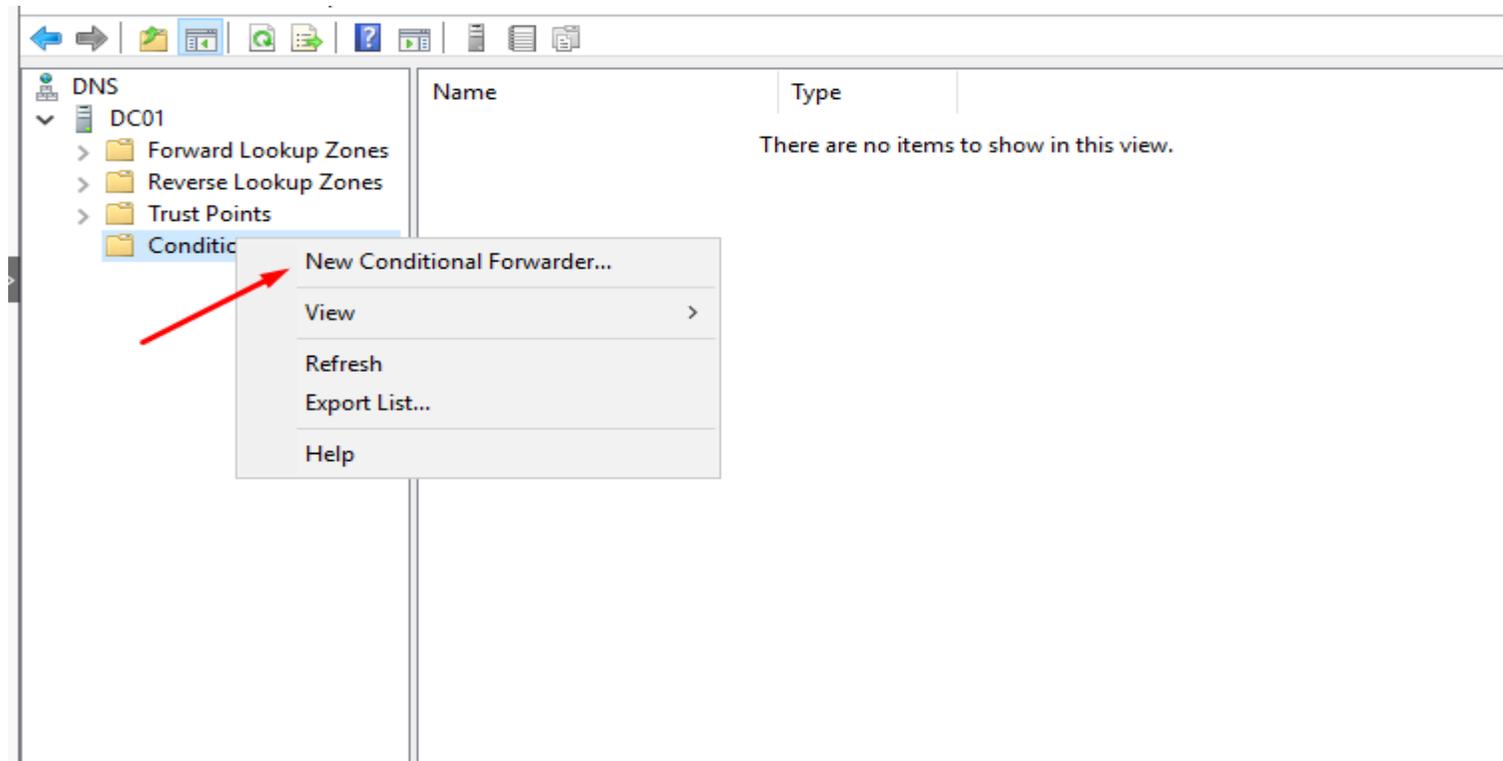
Lab Setup

Setting up DNS conditional forwarders for both side



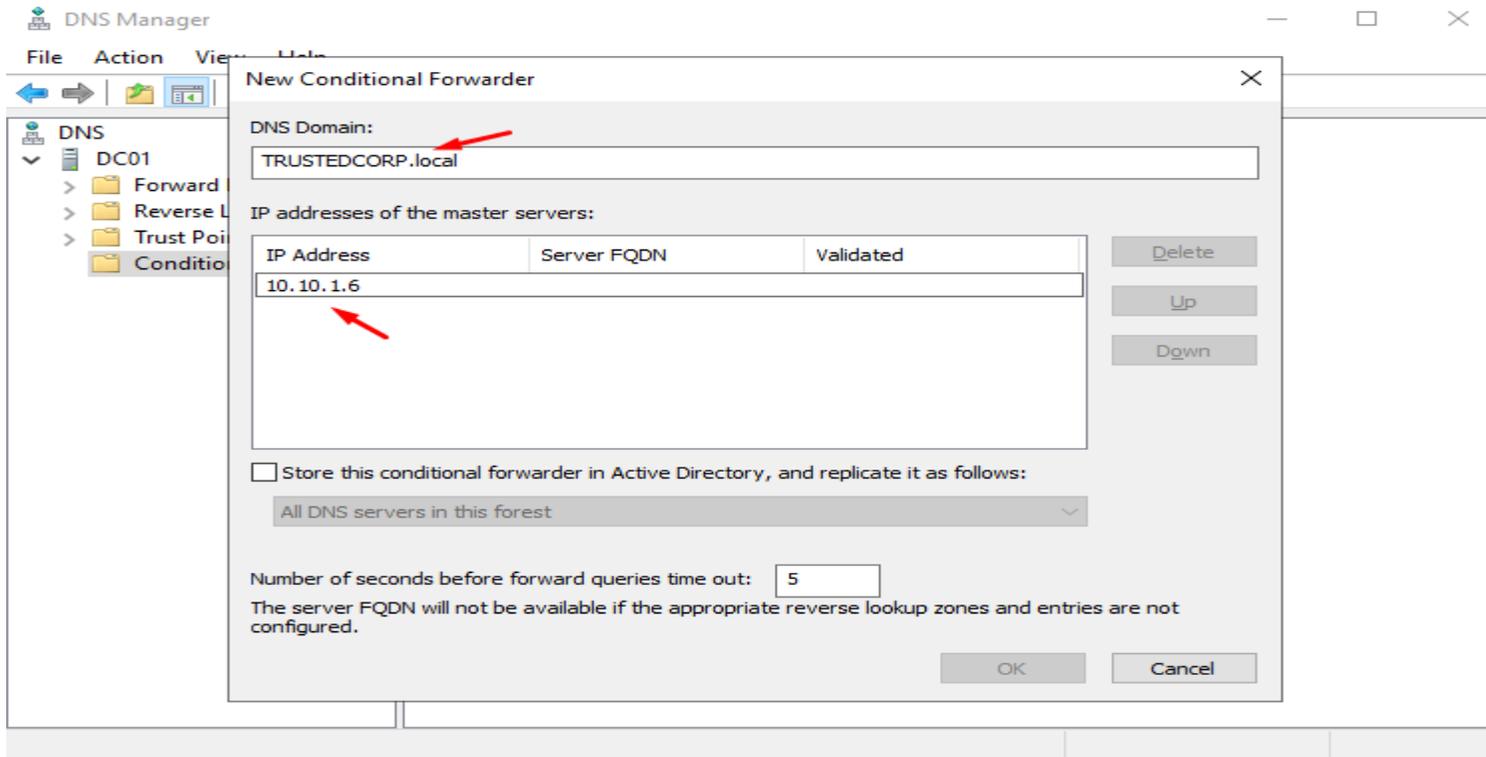
Lab Setup

Adding Forwarder



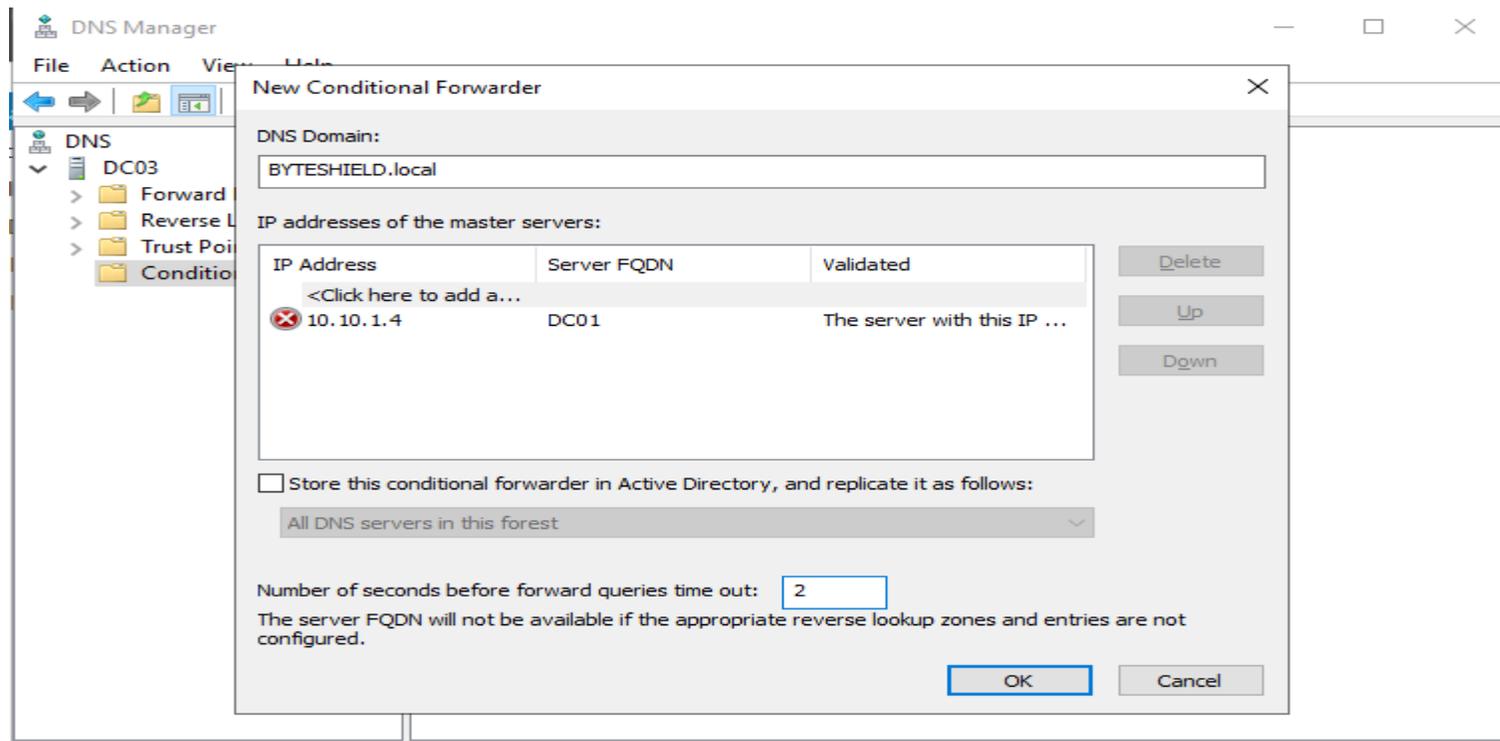
Lab Setup

Here we add the FQDN and IP address pointing to the target domain



Lab Setup

Doing the same from the other side pointing to Byteshield



Lab Setup

We can now ping the DC by its hostname

```
PS C:\Users\p.brown.BYTESHIELD> ping DC01

Pinging DC01.BYTESHIELD.local [10.10.1.4] with 32 bytes of data:
Reply from 10.10.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\p.brown.BYTESHIELD> ■
```

Lab Setup

We can also ping back from the DC

```
PS C:\Users\Administrator> ping win10-client-01

Pinging win10-client-01.BYTESHIELD.local [10.10.1.5] with 32 bytes of data:
Reply from 10.10.1.5: bytes=32 time<1ms TTL=128
Reply from 10.10.1.5: bytes=32 time<1ms TTL=128
Reply from 10.10.1.5: bytes=32 time=1ms TTL=128
Reply from 10.10.1.5: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Lab Setup

We have Successfully Installed windows server 2019, installed AD-DS and domain Controller on it, also installed Windows 10 enterprise edition as a client and joined to it to the domain,

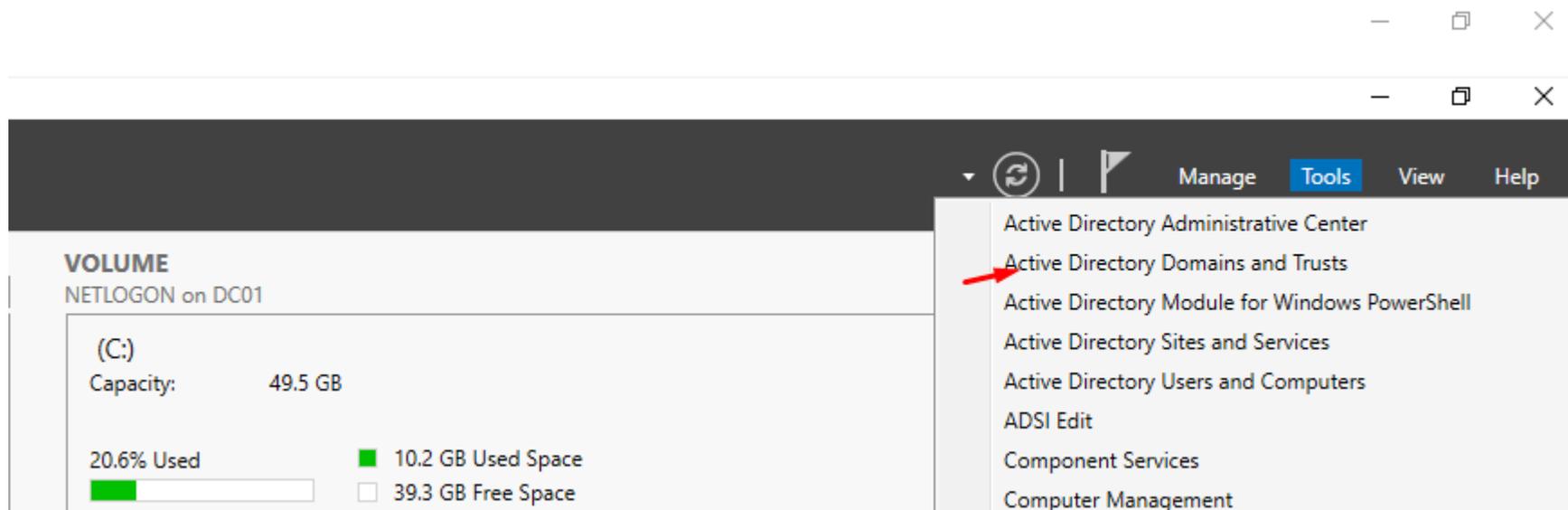
INSTRUCTION

Install 2 Domain Controllers DC02 and DC03, the DC03 should be installed the same way you installed DC01, but with different Domain name as TRUSTEDCORP.local, but every other thing should be the same,

DC02 should only be installed without installing AD-DS and Domain Controller, because we are going to make it a child to DC01 as the Parent or Root Domain, while DC03 would later be as a trusted domain to DC01, aTransitive/bidirectional Trust

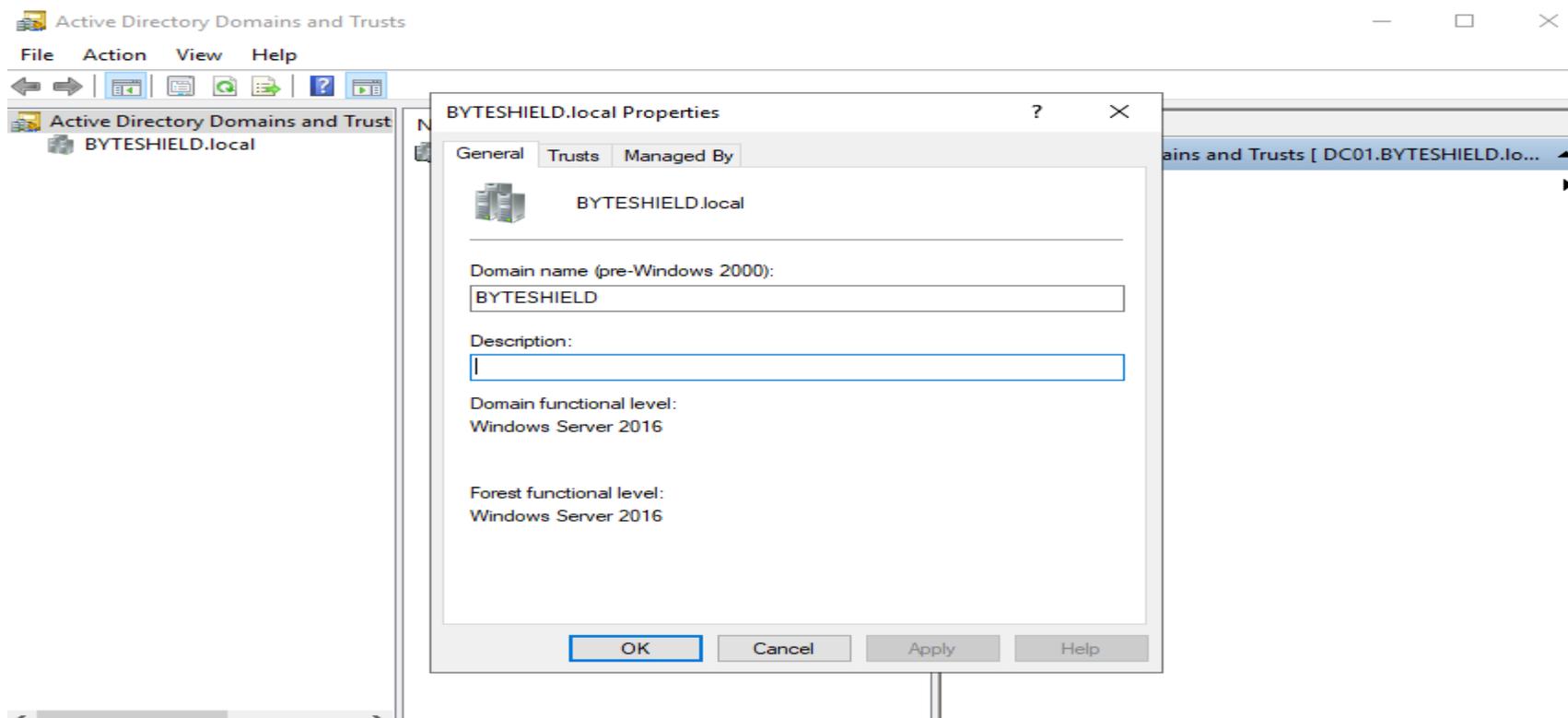
Lab Setup

If you have Successfully done what you're instructed in the last section, it is now time to create forest bidirectional trust between BYTESHIELD and TRUSTEDCORP



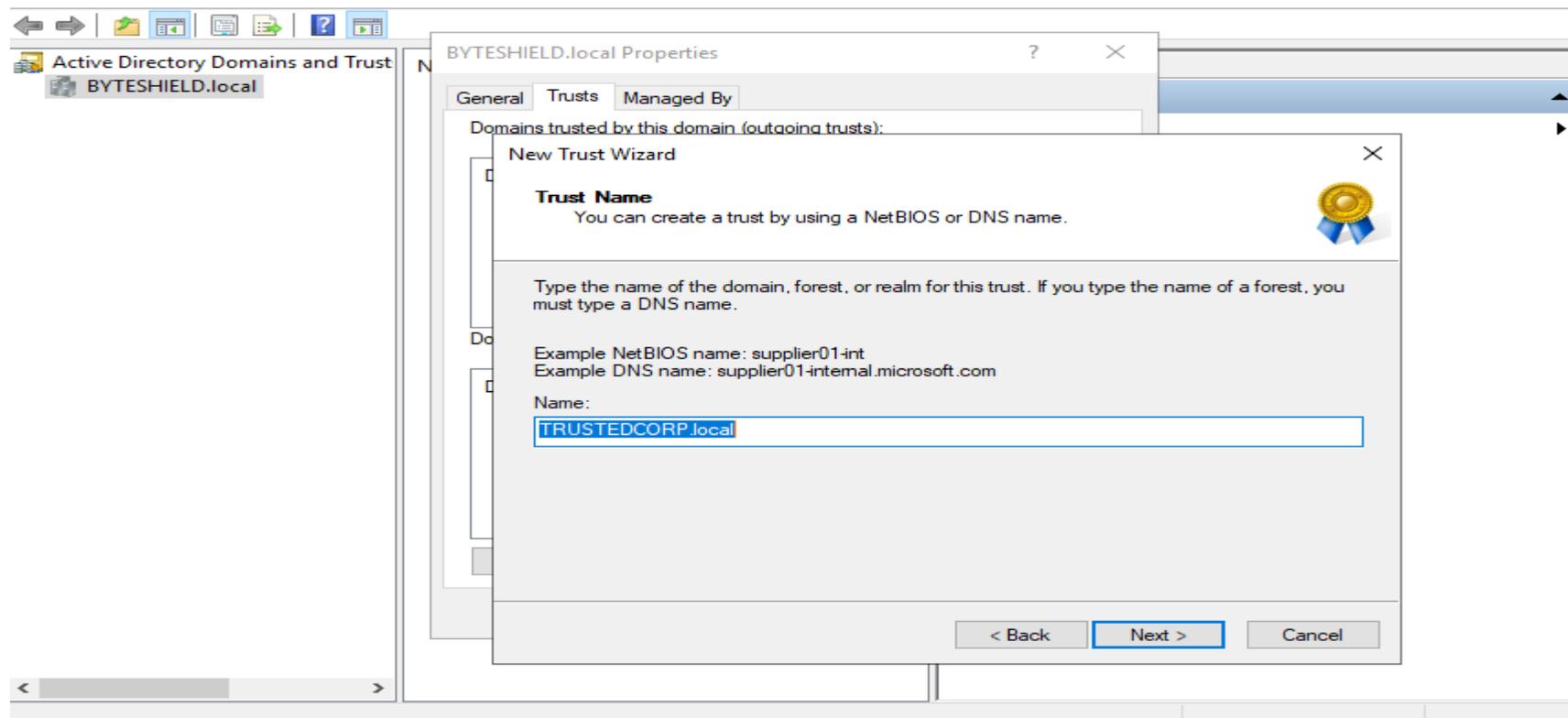
La Setup

Right click on the Domain name and go to properties, select trusts tab to start



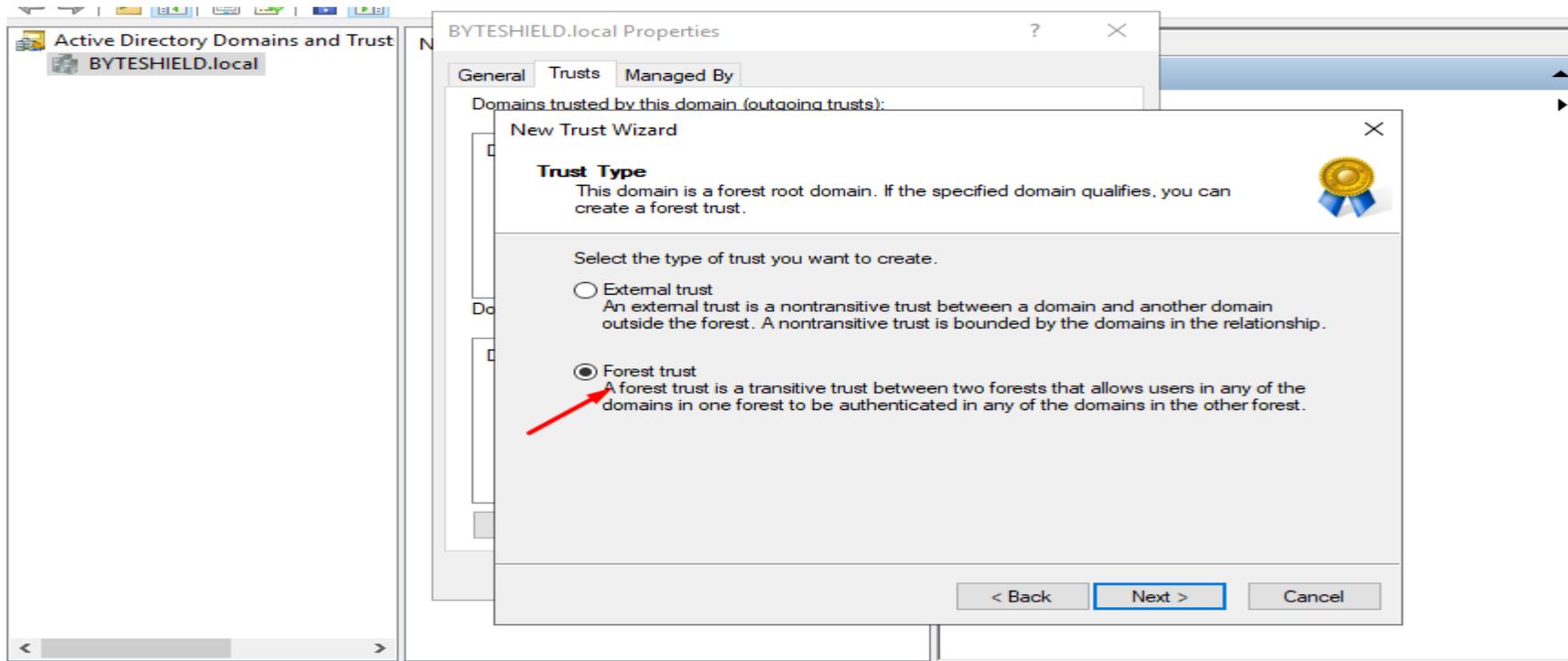
Lab Setup

Enter the Domain



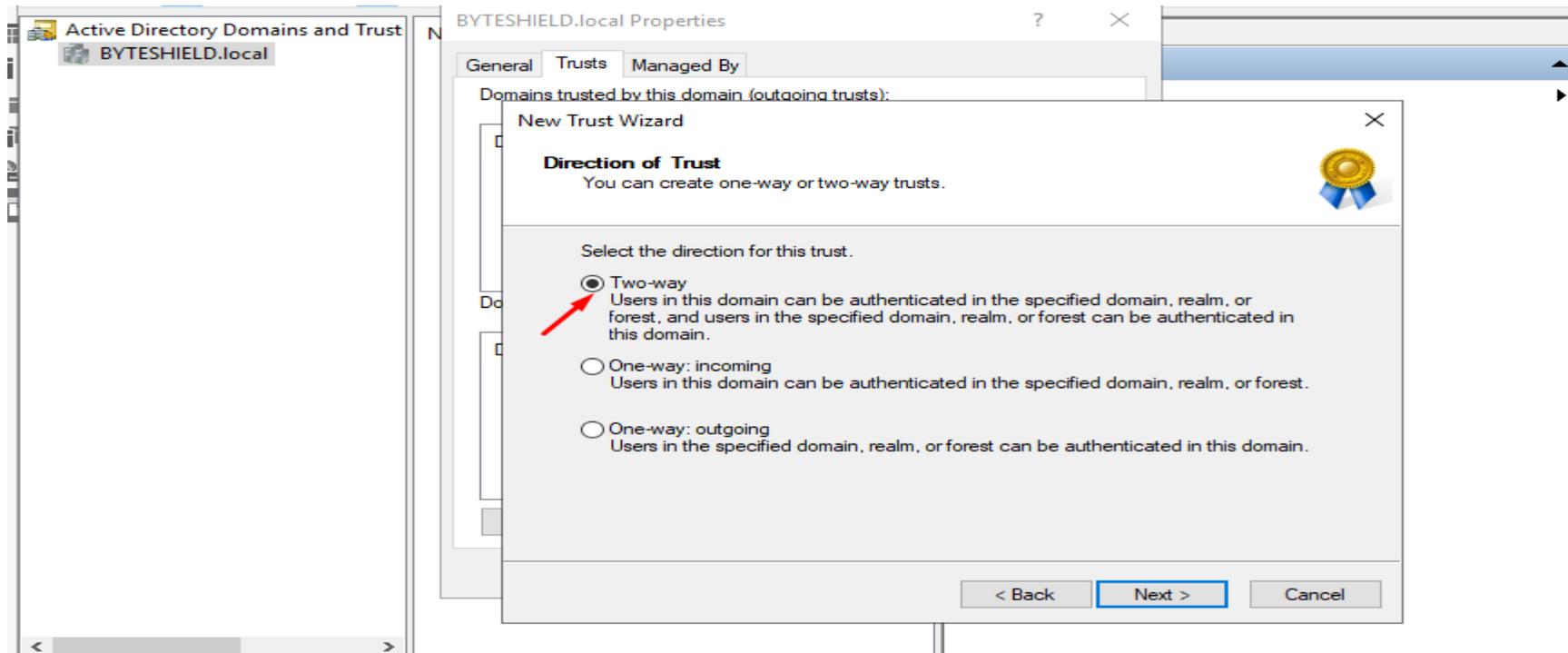
Lab Setup

Forest trust

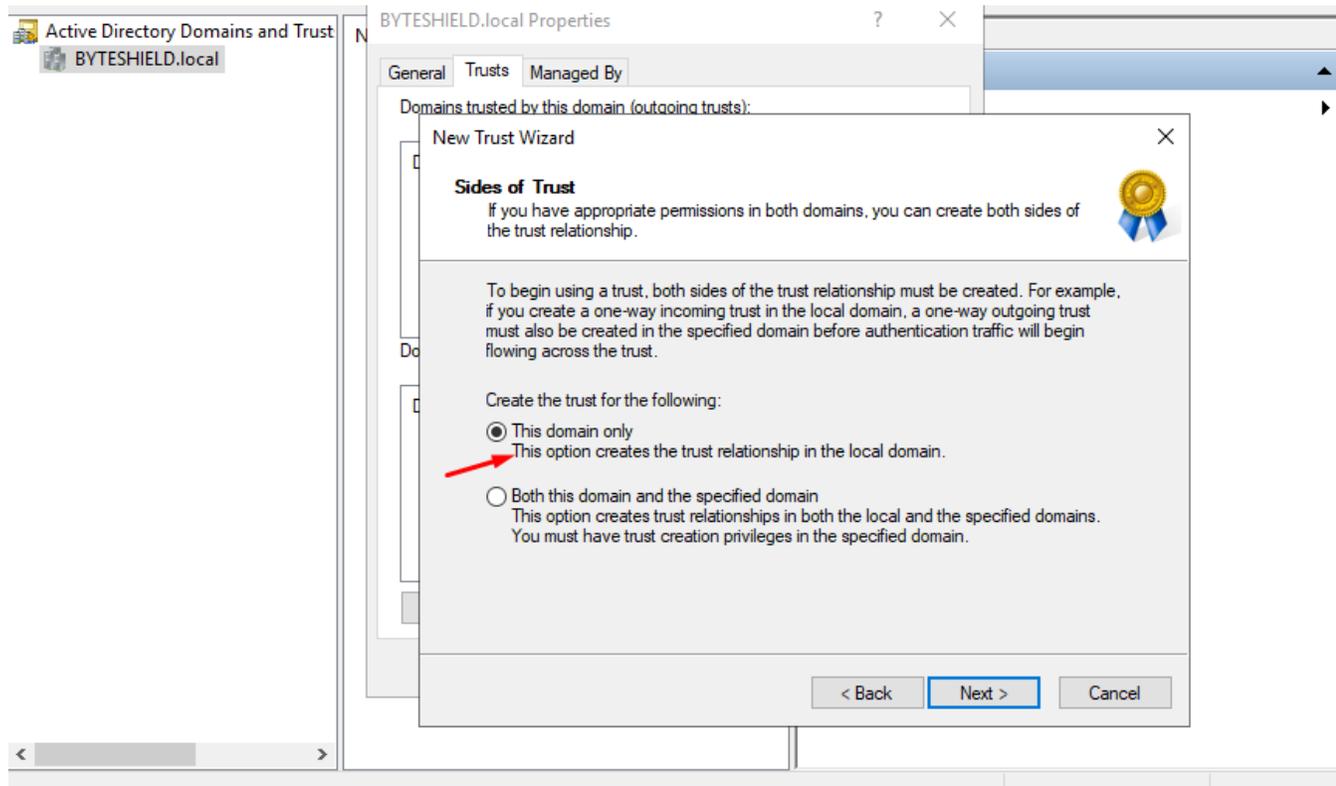


Lab Setup

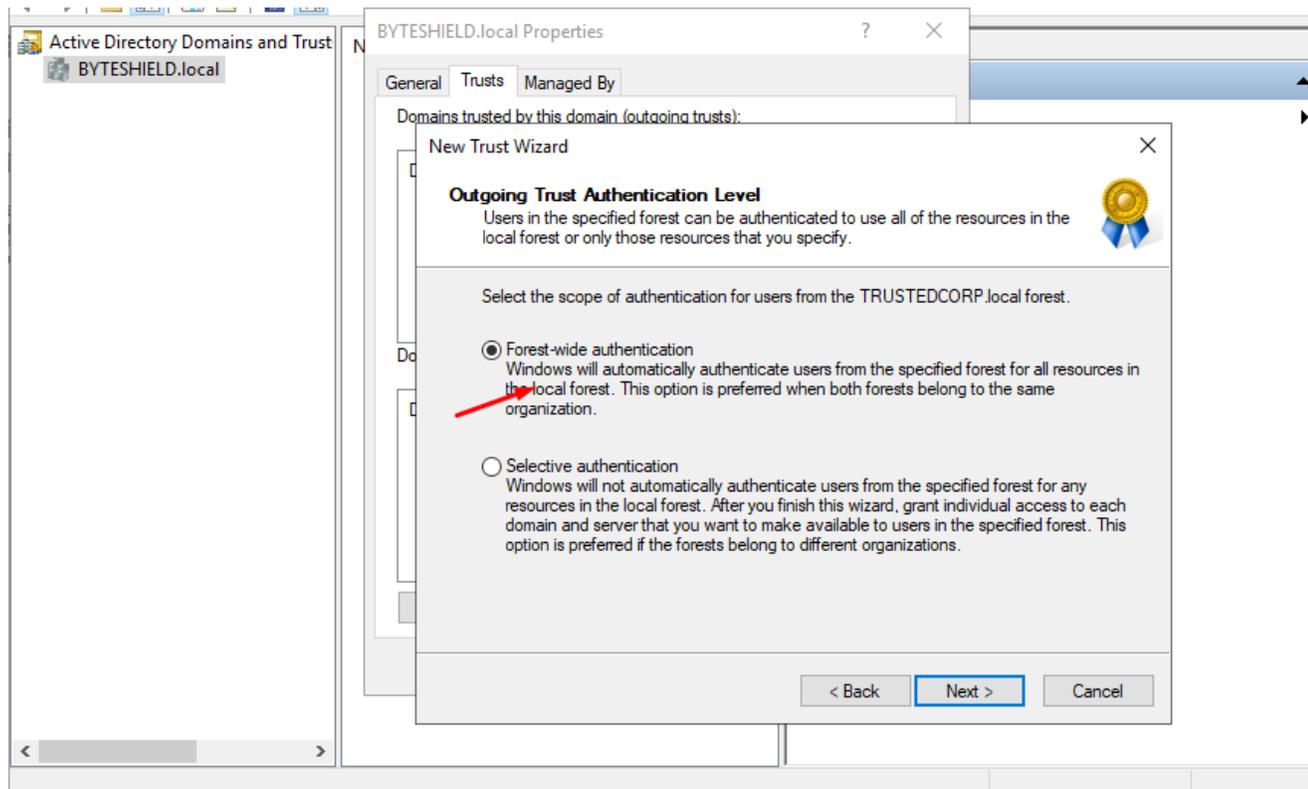
Bidirectional Trust



Lab Setup

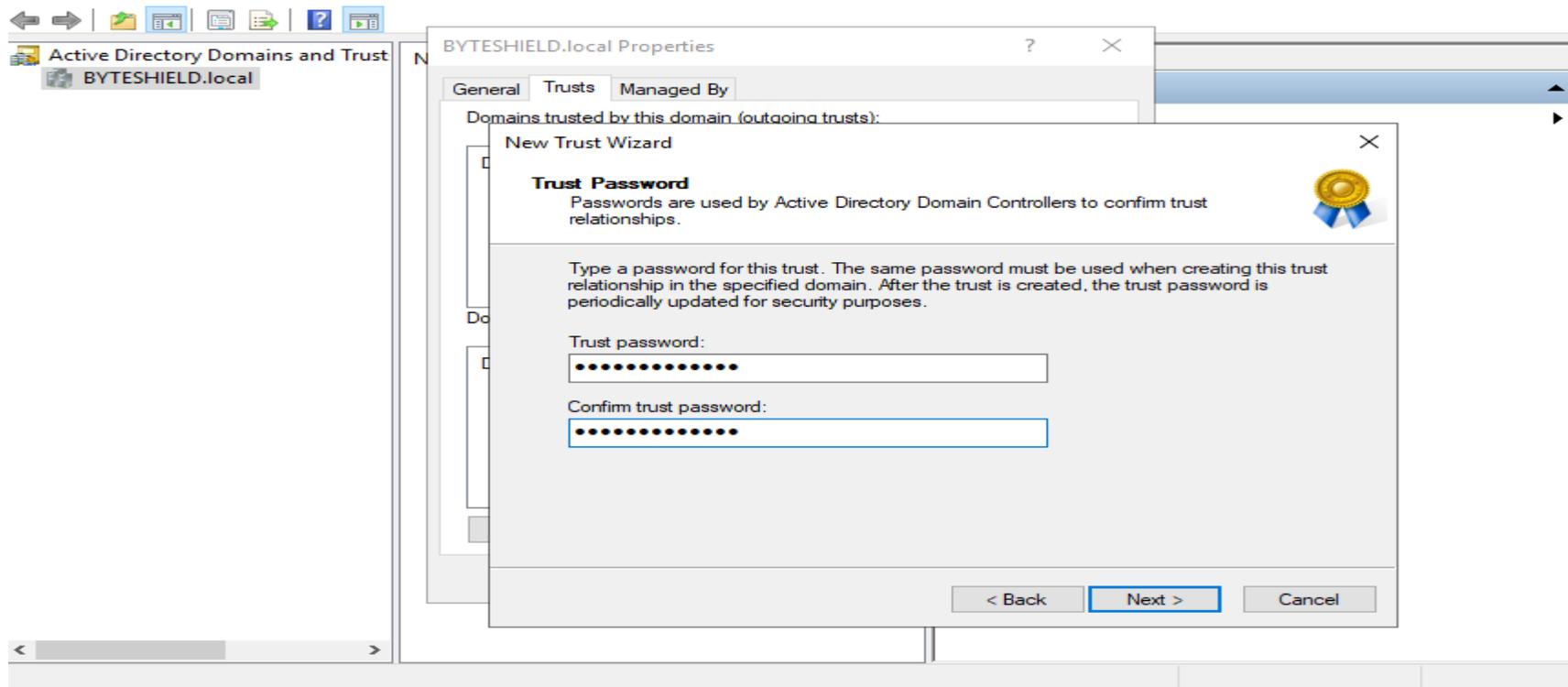


Lab Setup



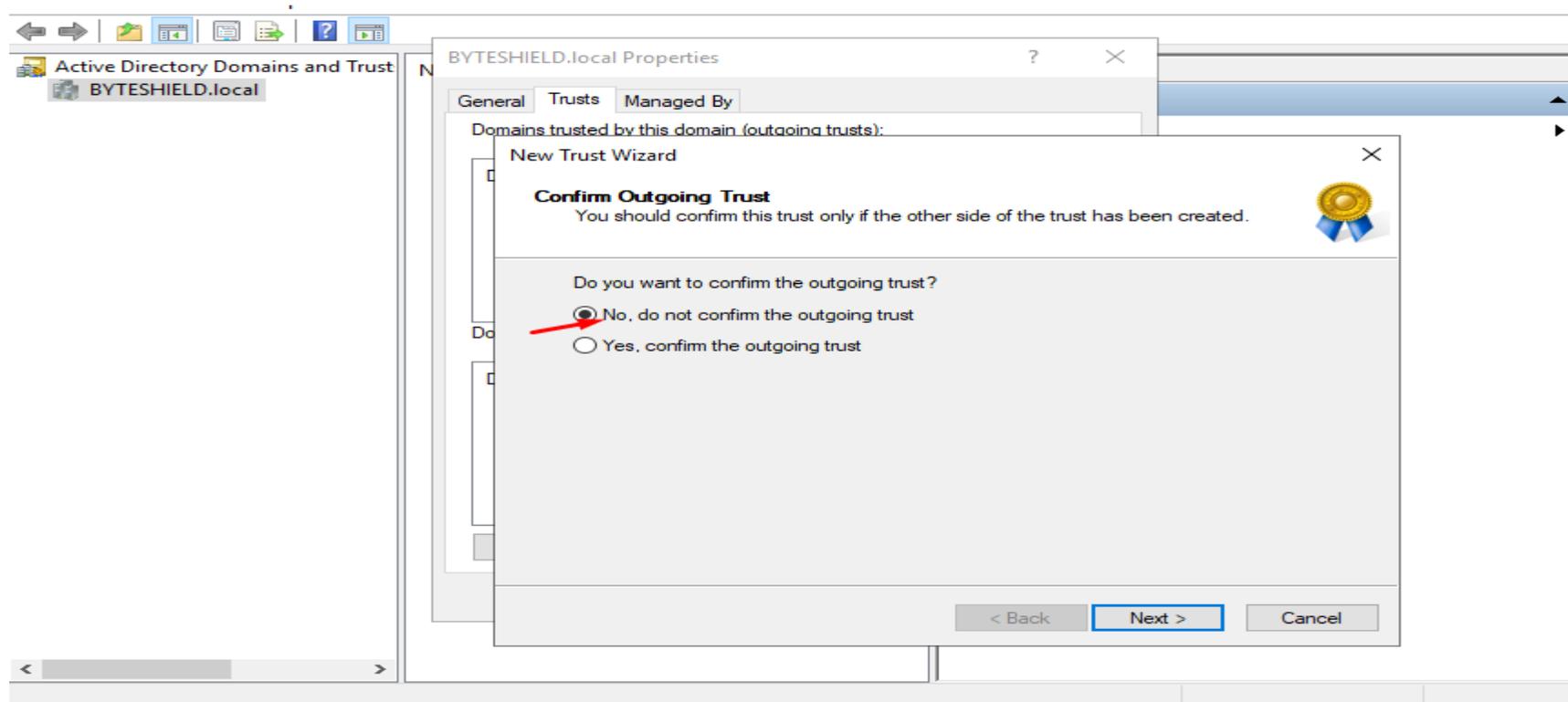
Lab Setup

Create a memorable trust password, it's going to be the same for both side



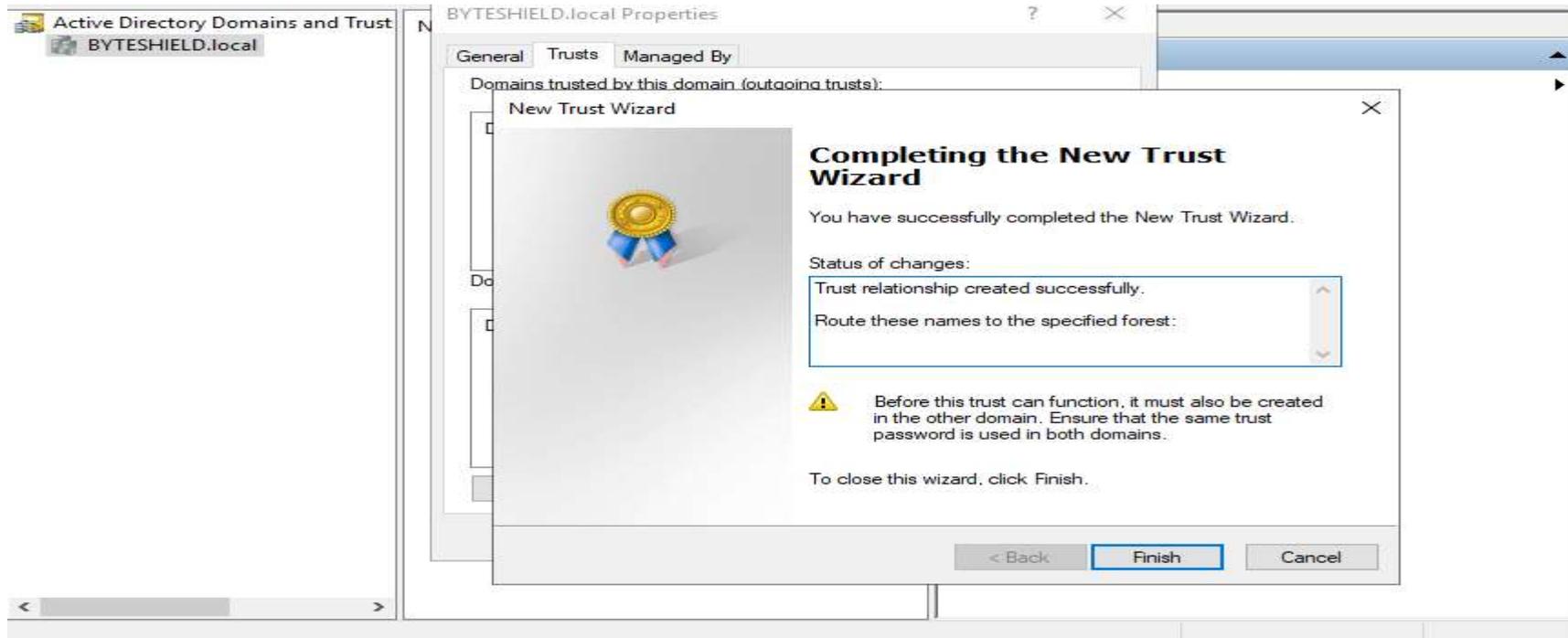
Lab Setup

Next > Next



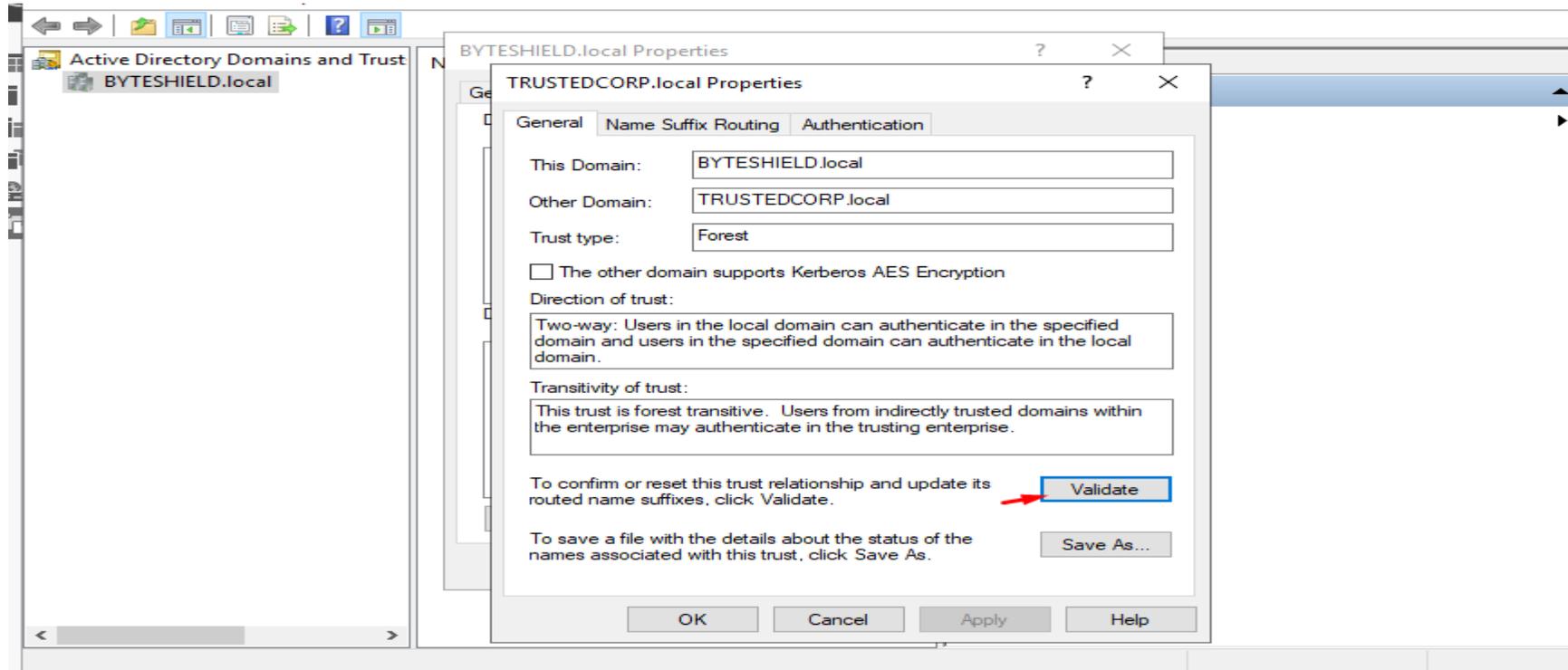
Lab Setup

Do the same on the other side



Lab Setup

Now validate outgoing and incoming trust



Lab Setup

We have Successfully Created a Transitive Trust between BYTESHIELD & TRUSTEDCORP, it is now time to Configure DC02 as a Child Domain to BYTESHIELD

First thing first let's configure network and DNS setting of the Domain

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: 10 . 10 . 1 . 7

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 10 . 1 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 10 . 10 . 1 . 4

Alternate DNS server: 8 . 8 . 8 . 8

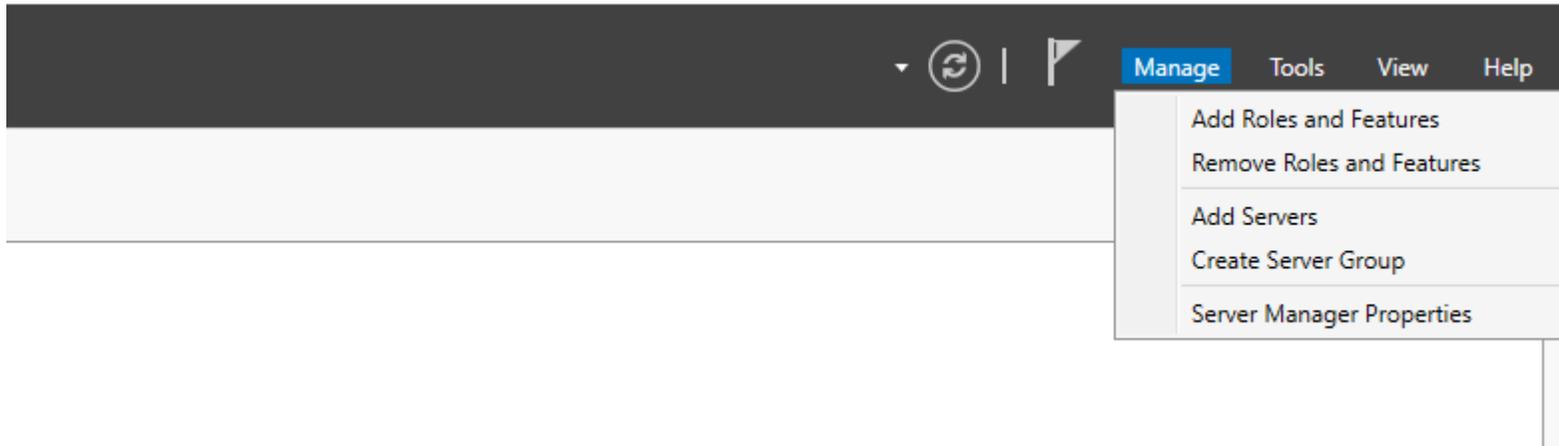
Validate settings upon exit

Advanced...

OK Cancel

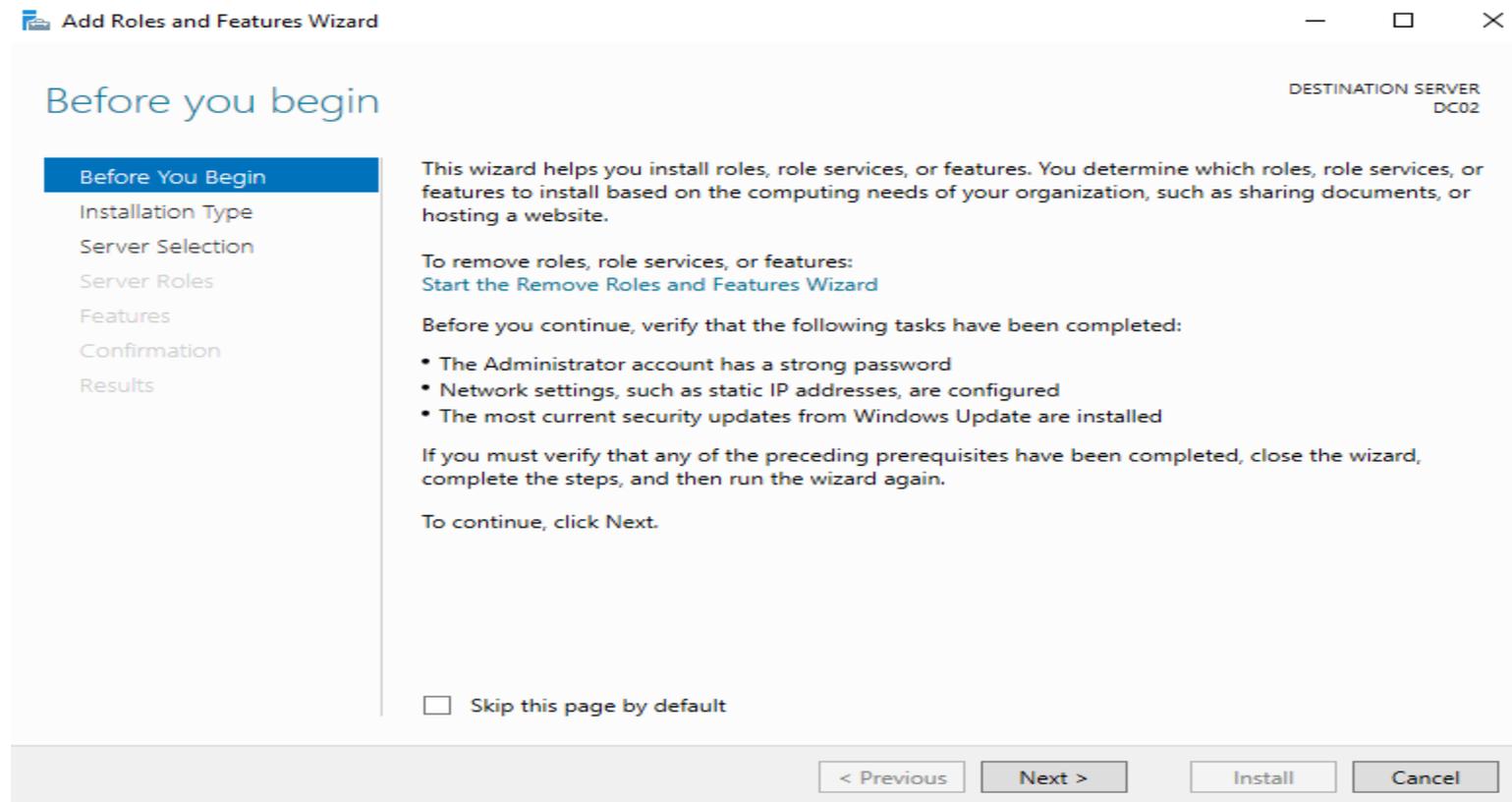
Lab Setup

Here We are going to AD-DS



Lab Setup

The same way we did on the other domain Controllers



Add Roles and Features Wizard DESTINATION SERVER DC02

Before you begin

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

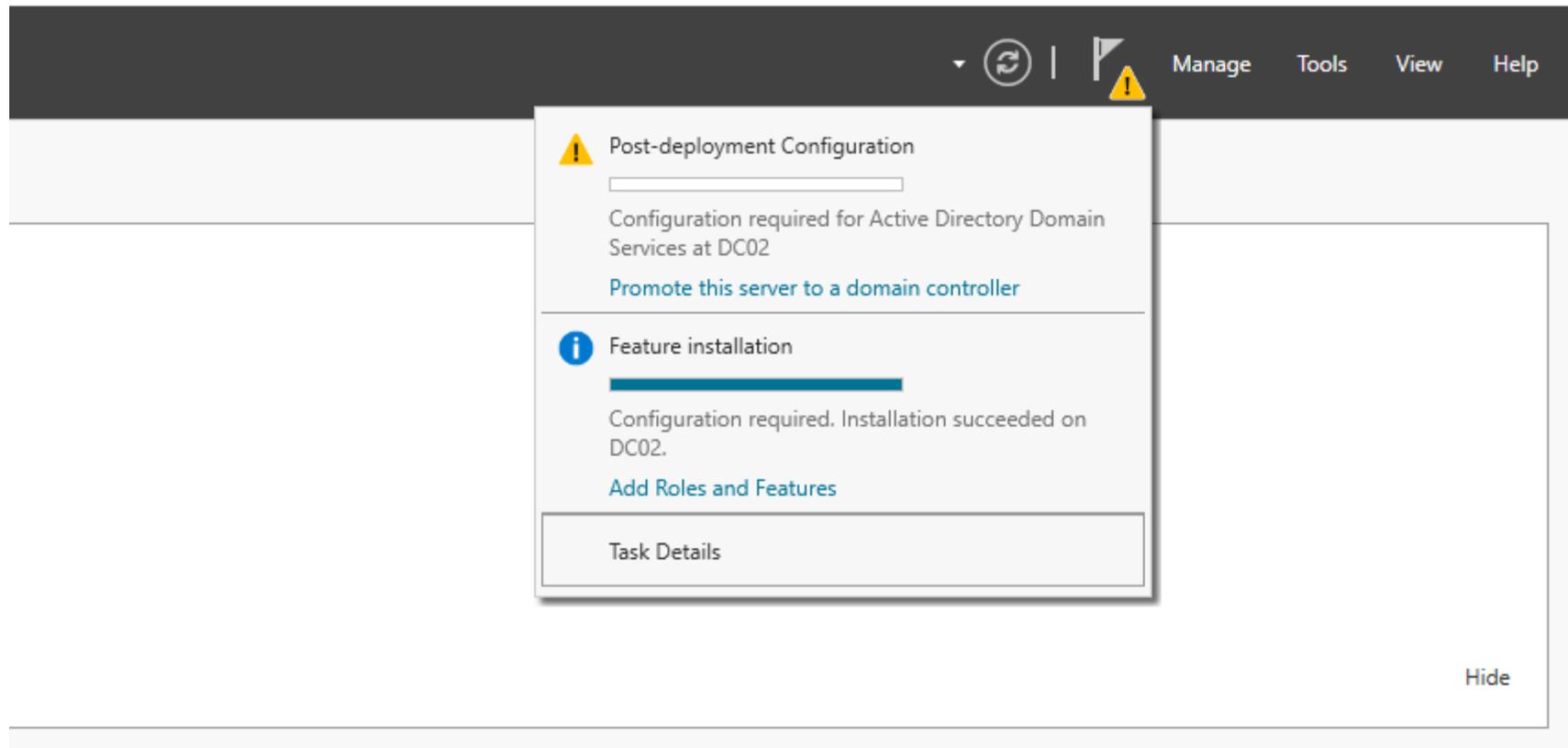
To continue, click Next.

Skip this page by default

< Previous Next > Install Cancel

Lab Setup

Let's Promote it to Domain Controller



Lab Setup

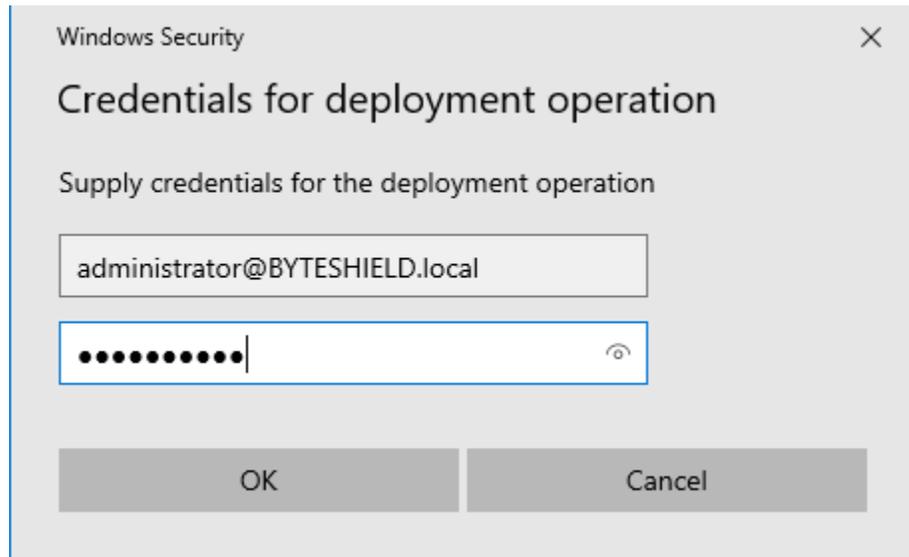
Now instead of selecting forest

domain to an existing

The image shows a composite screenshot of Windows Server configuration steps. On the left, the 'Active Directory Domain Services Configuration Wizard' is open to the 'Deployment Configuration' step. The 'Add a new domain' radio button is selected, and a red arrow points to it. Below this, a 'Windows Security' dialog box titled 'Credentials for deployment operation' is shown, with the username 'administrator@BYTESHIELD.local' entered. A second, smaller 'Windows Security' dialog box is overlaid on the bottom left, showing the username 'Administrator' and a masked password. At the bottom right, a portion of the wizard's 'Next >' button and 'Install' button are visible, along with a taskbar showing 'Events', 'Performance', and 'BPA results'.

Lab Setup

Supplying the Credentials of our Root Domain



Lab Setup

Creating DSRM Passowrd

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
DC02

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new domain

Domain functional level: Windows Server 2016

Specify domain controller capabilities and site information

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

Site name: Default-First-Site-Name

Type the Directory Services Restore Mode (DSRM) password

Password:

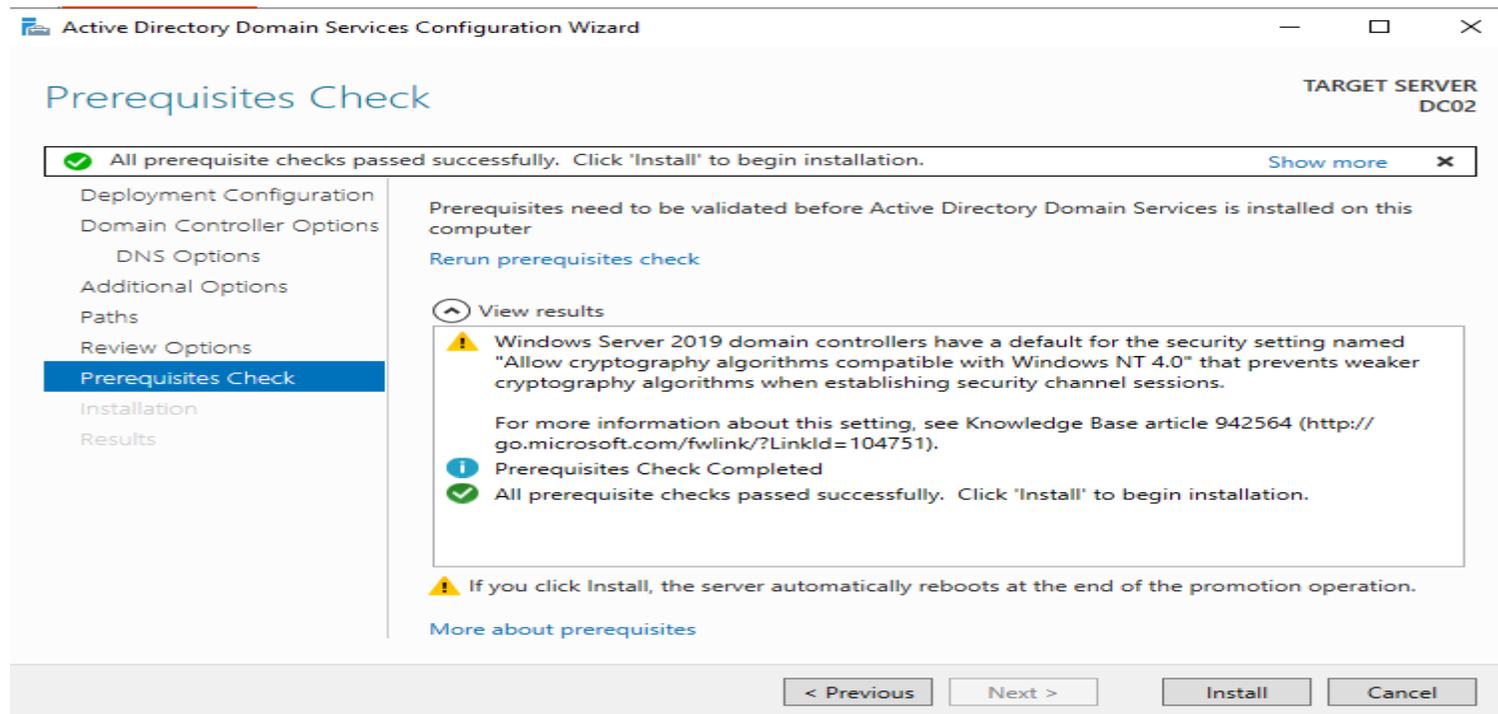
Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

Lab Setup

Follow the Wizard Next > Next and installed the same way you did on the other Domain Controllers



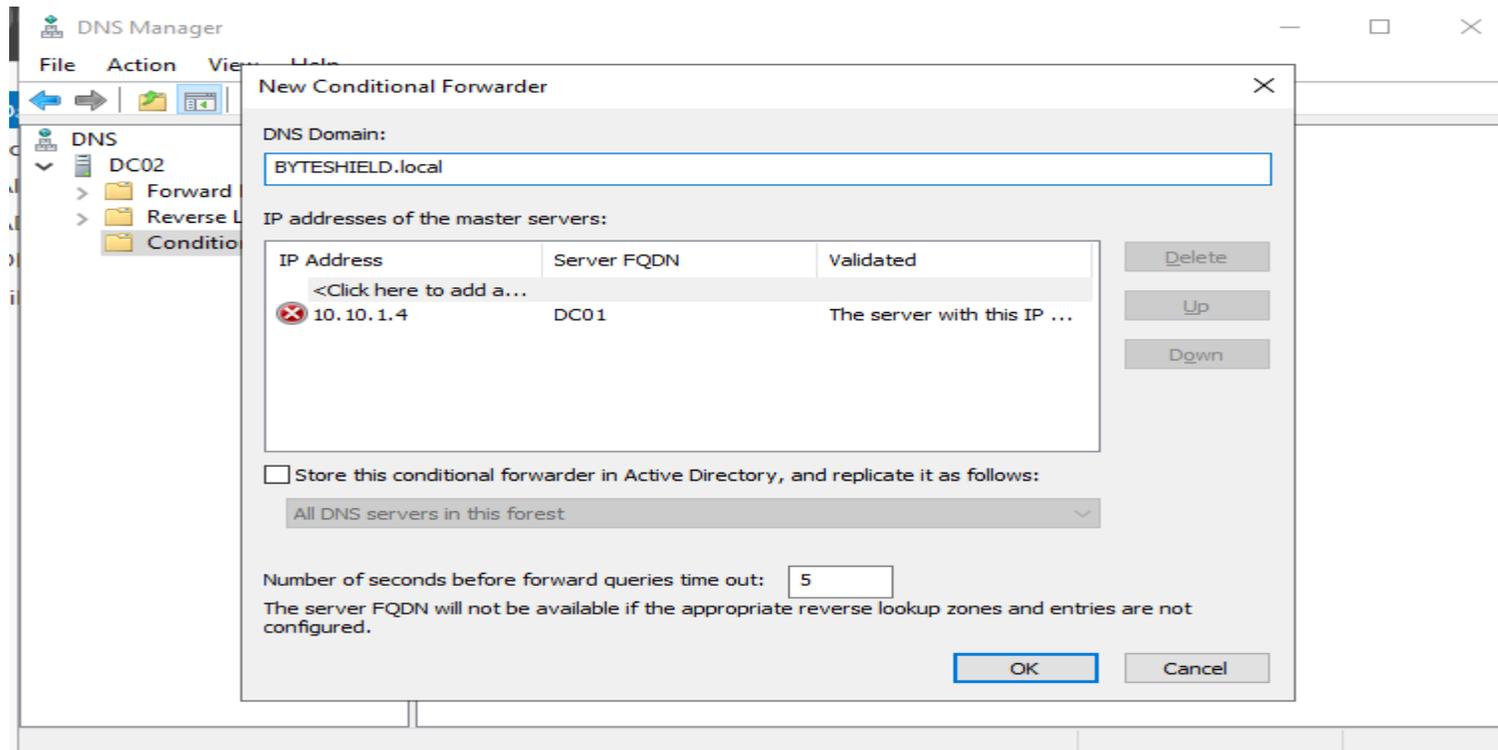
Lab Setup

We have Successfully Create a child domain, now let's create DNS conditional forwarder pointing to the root domain



Lab Setup

Creating Conditional Forwarder pointing to the root domain



Lab Setup

Now we can ping the FQDN of the root domain and vice versa

Create Share on the Child domain as you did on the root domain name it TRI-Share

```
PS C:\Users\Administrator> ping DC01.BYTESHIELD.local

Pinging DC01.BYTESHIELD.local [10.10.1.4] with 32 bytes of data:
Reply from 10.10.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator>
```

Lab Setup

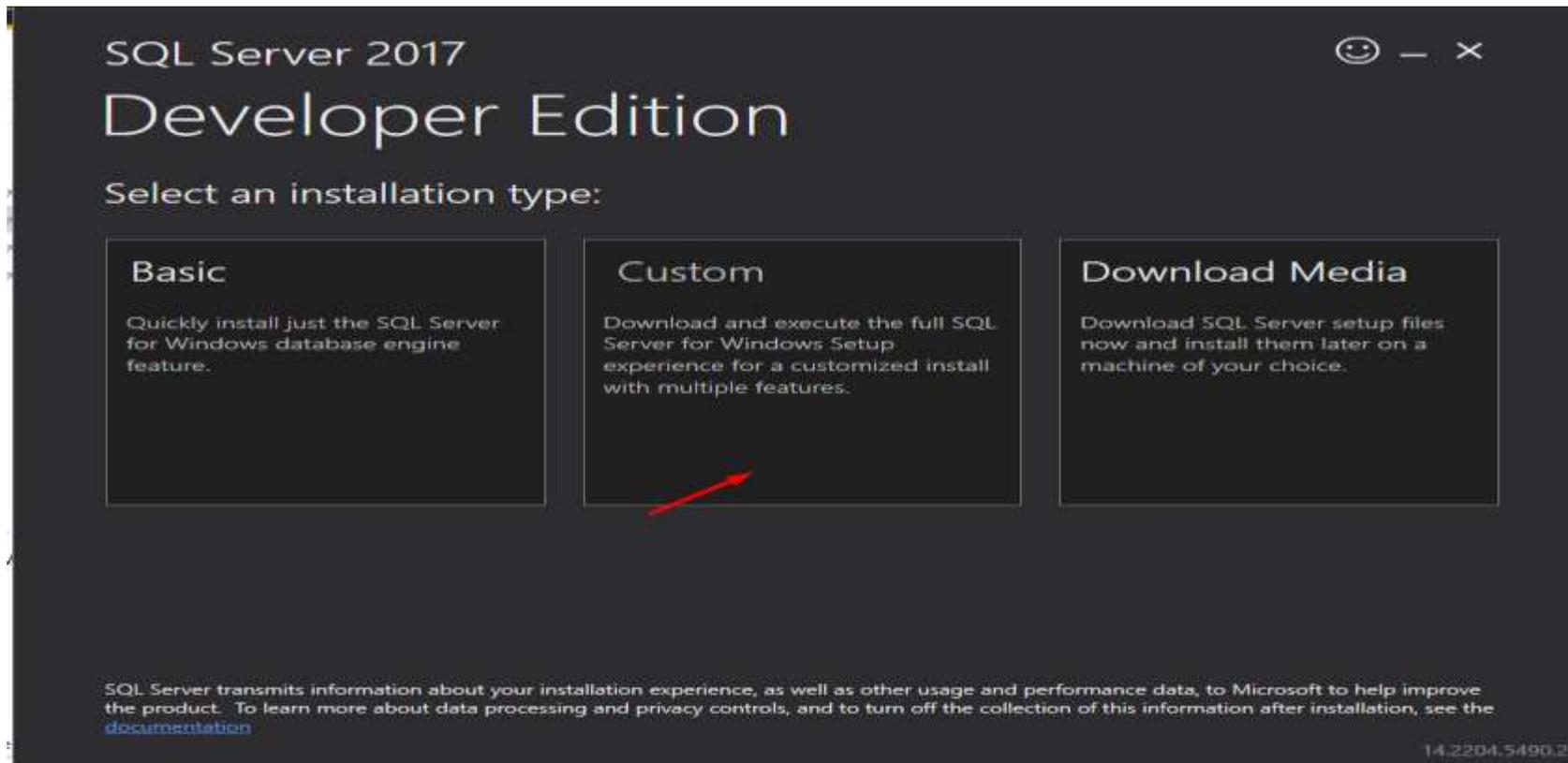
Downloading and Installing SQL Server on DC01, DC02 and Win10-Client-01

You can Download Microsoft Sql Server developer or express edition from MicroSoft website, after downloading it copy it to DC01 IT-DEPT share so that you can access it other machines

<https://download.microsoft.com/download/5/A/7/5A7065A2-C81C-4A31-9972-8A31AC9388C1/SQLServer2017-SSEI-Dev.exe>

Lab Setup

SQL Server installation



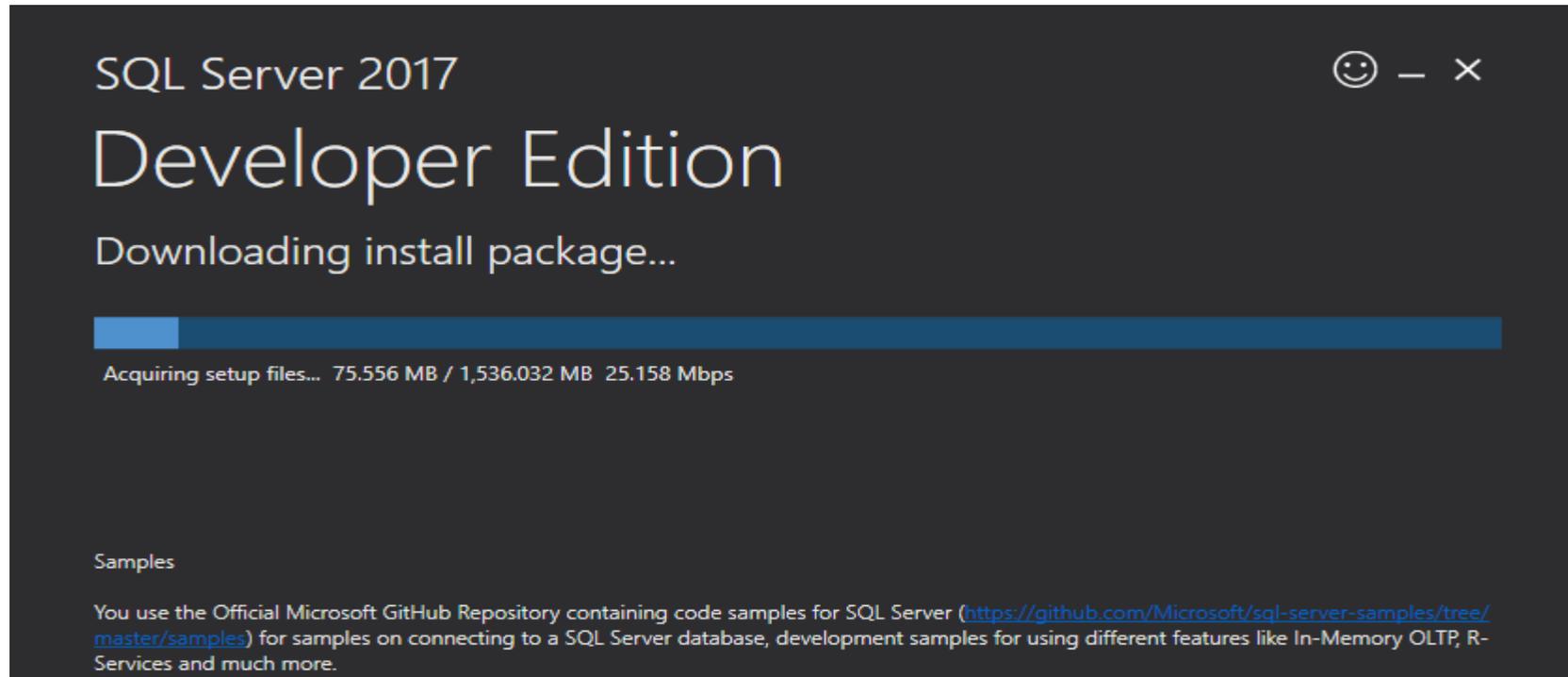
Lab Setup

Install



Lab Setup

This will take sometimes depending on your network speed and Computer performance



Lab Setup

Select New Sql server stand-alone installation and continue



SQL Server Installation Center

- Planning
- Installation**
- Maintenance
- Tools
- Resources
- Advanced
- Options

Microsoft SQL Server 2017

-  [New SQL Server stand-alone installation or add features to an existing installation](#)
Launch a wizard to install SQL Server 2017 in a non-clustered environment or to add features to an existing SQL Server 2017 instance.
-  [Install SQL Server Reporting Services](#)
Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.
-  [Install SQL Server Management Tools](#)
Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.
-  [Install SQL Server Data Tools](#)
Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.
-  [New SQL Server failover cluster installation](#)
Launch a wizard to install a single-node SQL Server 2017 failover cluster.
-  [Add node to a SQL Server failover cluster](#)
Launch a wizard to add a node to an existing SQL Server 2017 failover cluster.
-  [Upgrade from a previous version of SQL Server](#)
Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2017.
-  [New Machine Learning Server \(Standalone\) installation](#)
Launch a wizard to install Machine Learning Server (Standalone) on a Windows machine. This is typically used by data scientists as a standalone analysis server or as a

Lab Setup

Product Key

License Terms

Global Rules

Microsoft Update

Product Updates

Install Setup Files

Install Rules

Feature Selection

Feature Rules

Feature Configuration Rules

Ready to Install

Installation Progress

Complete

Validate this instance of SQL Server 2017 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server: Developer, Evaluation, or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. Developer edition does not have an expiration, has the same set of features found in Evaluation, but is licensed for non-production database application development only. To upgrade from one installed edition to another, run the Edition Upgrade Wizard.

Specify a free edition:

Developer

Enter the product key:

_____ - _____ - _____ - _____ - _____

Lab Setup

Accept and Next



Lab Setup

Next > Next

Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

Looking for Reporting Services? [Download it from the web](#)

Features:

- Instance Features
 - Database Engine Services
 - SQL Server Replication
 - Machine Learning Services (In-Database)
 - R
 - Python
 - Full-Text and Semantic Extractions for Search
 - Data Quality Services
 - PolyBase Query Service for External Data
 - Analysis Services

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL

Prerequisites for selected features:

Already installed:

- Windows PowerShell 3.0 or higher
- Microsoft .NET Framework 4.6

Disk Space Requirements

Drive C: 1001 MB required, 36710 MB available

Select All Unselect All

Instance root directory: C:\Program Files\Microsoft SQL Server\ ...

Shared feature directory: C:\Program Files\Microsoft SQL Server\ ...

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\ ...

< Back Next > Cancel

Lab Setup

Choose named instance and change its name from the default

Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

Default instance
 Named instance:

Instance ID:

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version
---------------	-------------	----------	---------	---------

< Back Next > Cancel

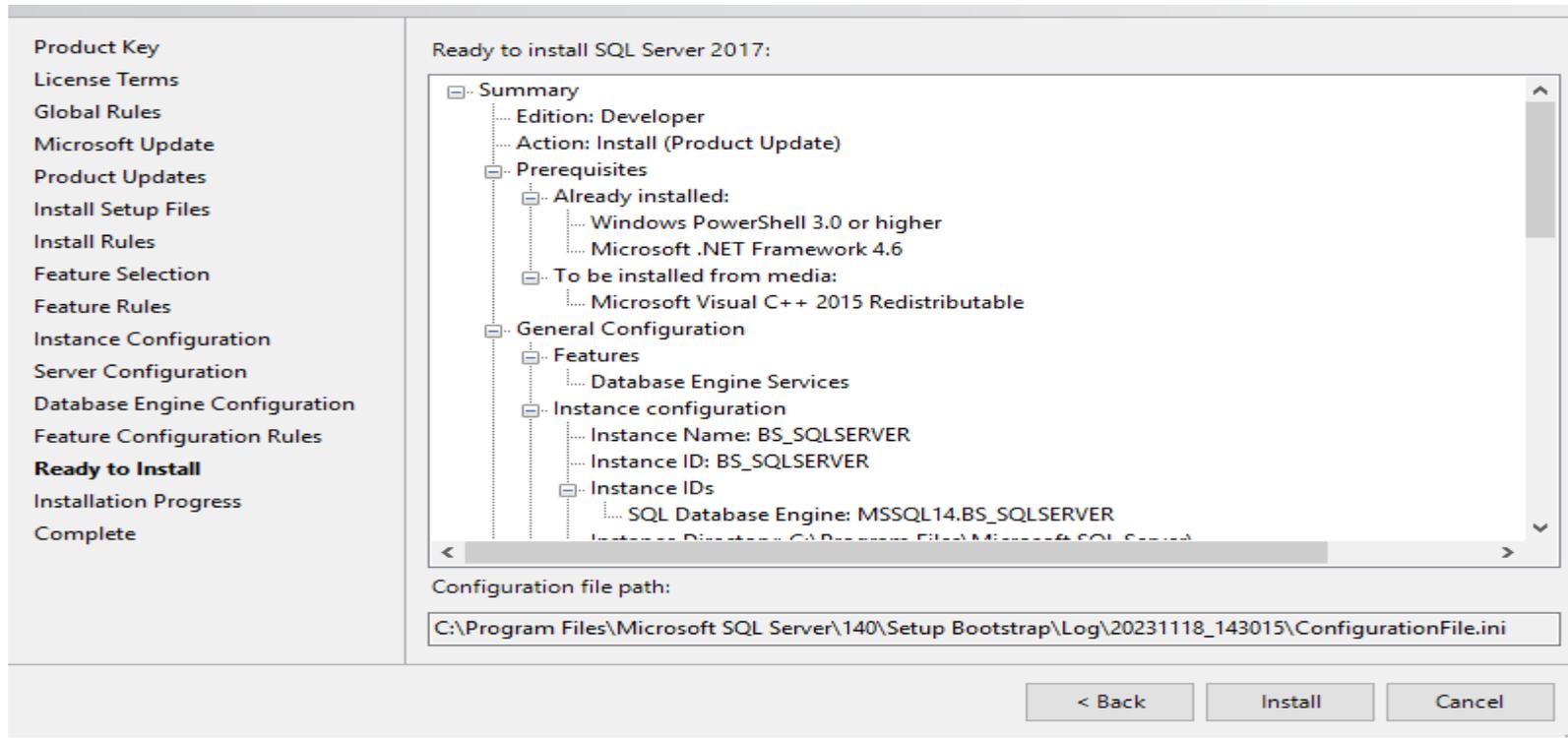
Lab Setup

Next > Next and choose mixed mode authentication, click add current user or add to select another user

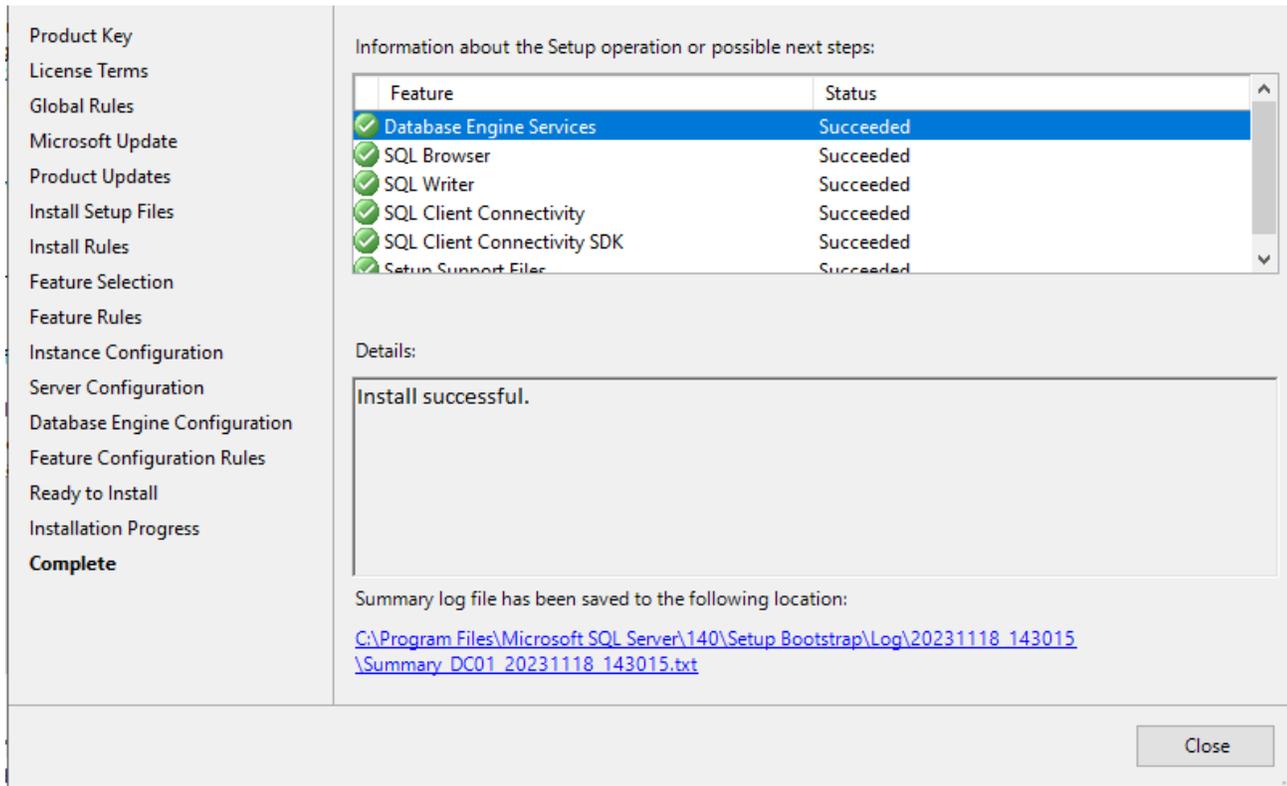
The screenshot shows the 'Server Configuration' step of the SQL Server Enterprise Setup Wizard. The left-hand navigation pane lists various installation options, with 'Database Engine Configuration' currently selected. The main window has tabs for 'Server Configuration', 'Data Directories', 'TempDB', and 'FILESTREAM'. The 'Server Configuration' tab is active, displaying instructions to specify authentication mode and administrators. The 'Authentication Mode' section has three radio buttons: 'Windows authentication mode', 'Mixed Mode (SQL Server authentication and Windows authentication)', and 'Mixed Mode (SQL Server authentication and Windows authentication)'. The 'Mixed Mode' option is selected, and a red arrow points to it. Below this, there are two password fields: 'Enter password:' and 'Confirm password:', both containing masked characters. The 'Specify SQL Server administrators' section contains a list box with one entry, 'BYTESHIELD\Administrator (Administrator)', which is highlighted in blue. A red arrow points to this entry. To the right of the list box is a text box stating 'SQL Server administrators have unrestricted access to the Database Engine.' Below the list box are three buttons: 'Add Current User', 'Add...', and 'Remove'. A red arrow points to the 'Add Current User' button. At the bottom of the wizard are three buttons: '< Back', 'Next >', and 'Cancel'.

Lab Setup

Next and Install

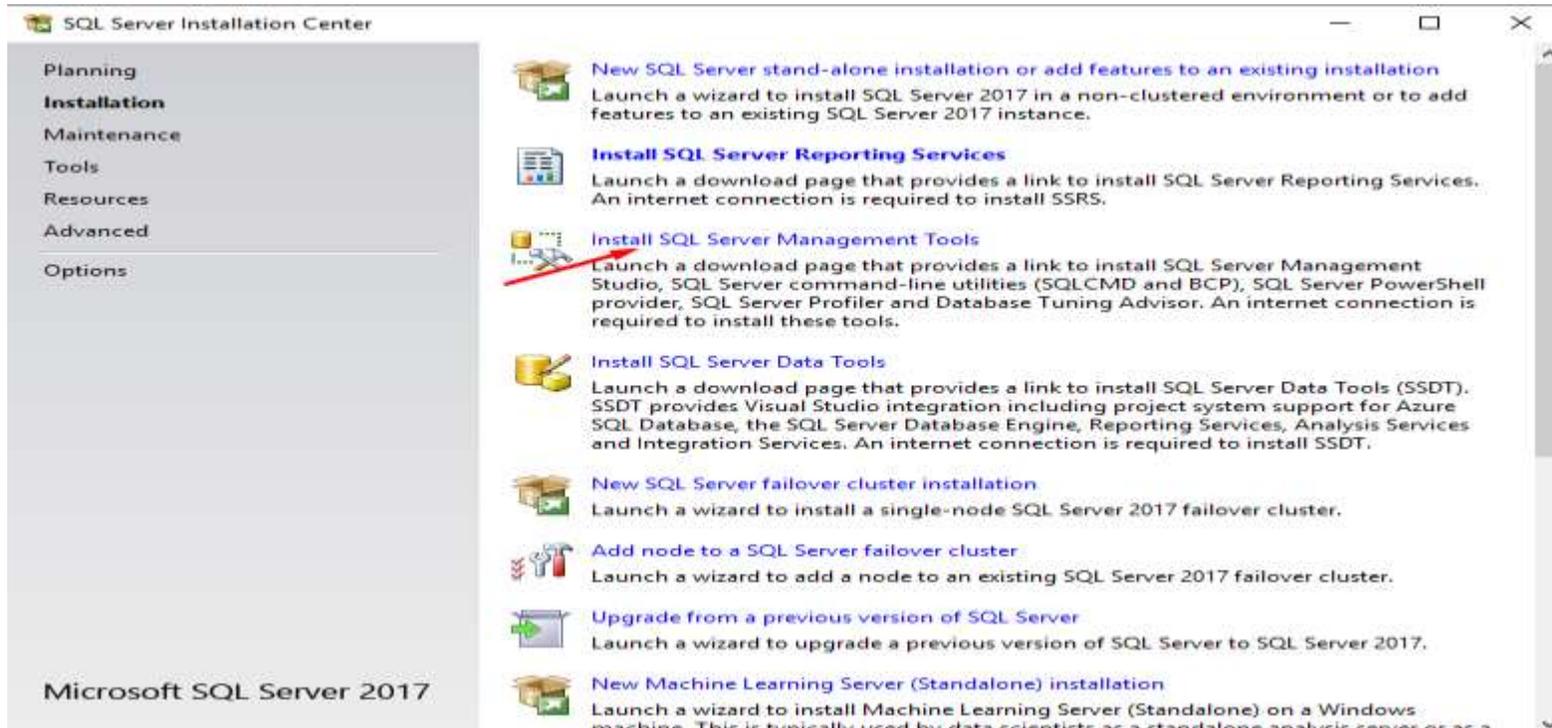


Lab Setup



Lab Setup

Since we installed the Server let's install Sql server management studio SSMS, clicking install sql server management tools, we will get redirected to Microsoft website



Lab Setup

Scroll Down and Click the link to Download this Version

Download SSMS

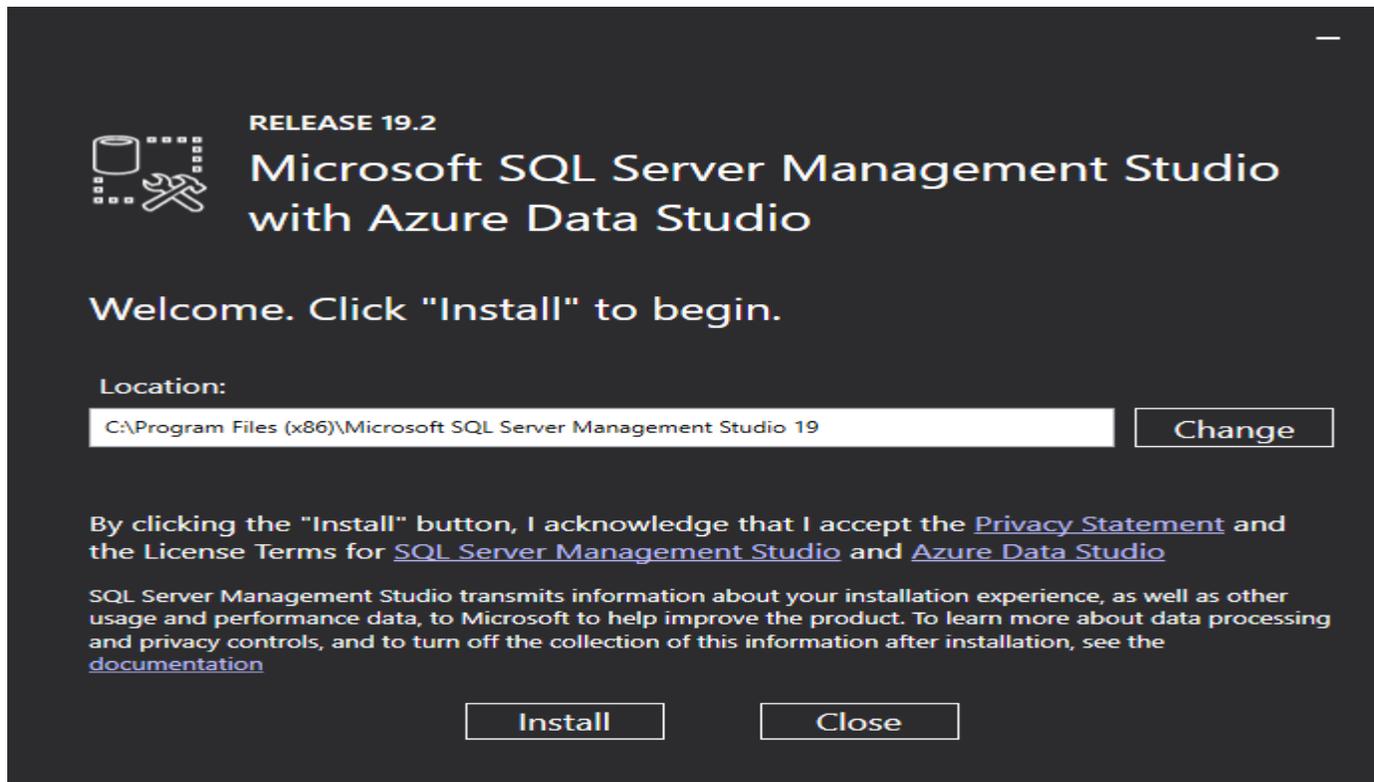
↓ [Free Download for SQL Server Management Studio \(SSMS\) 19.2](#)

SSMS 19.2 is the latest general availability (GA) version. If you have a *preview* version of SSMS 19 installed, uninstall it before installing SSMS 19.2. If you have SSMS 19.x installed, installing SSMS 19.2 upgrades it to 19.2.

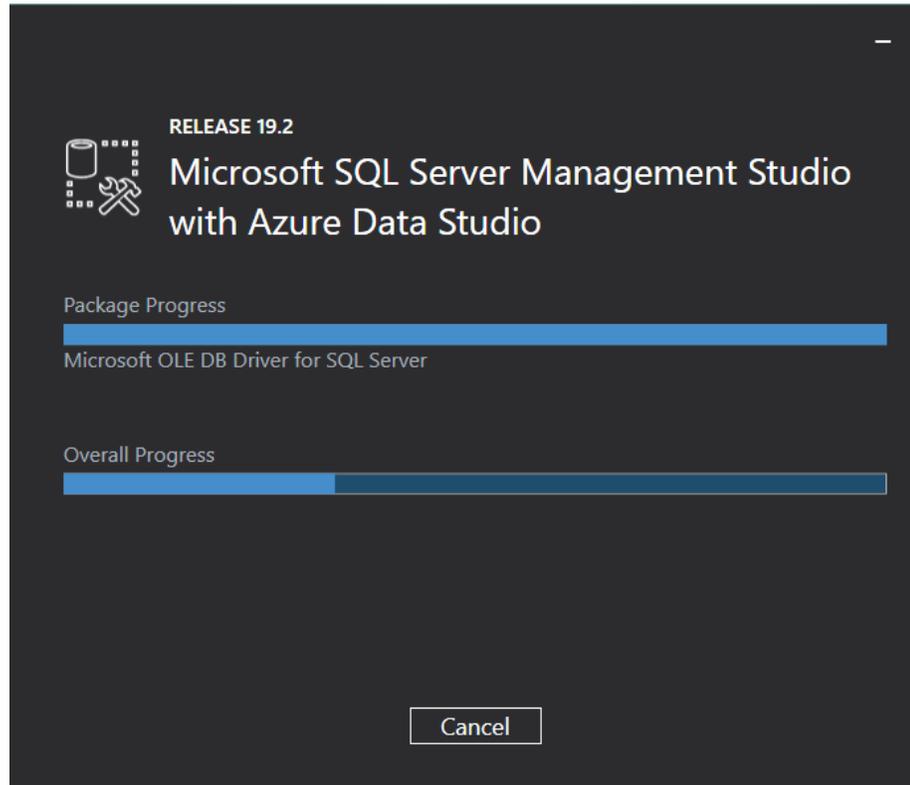
- Release number: 19.2
- Build number: 19.2.56.2
- Release date: November 13, 2023

Lab Setup

Installing SSMS



Lab Setup



RELEASE 19.2

 Microsoft SQL Server Management Studio
with Azure Data Studio

Package Progress

Microsoft OLE DB Driver for SQL Server

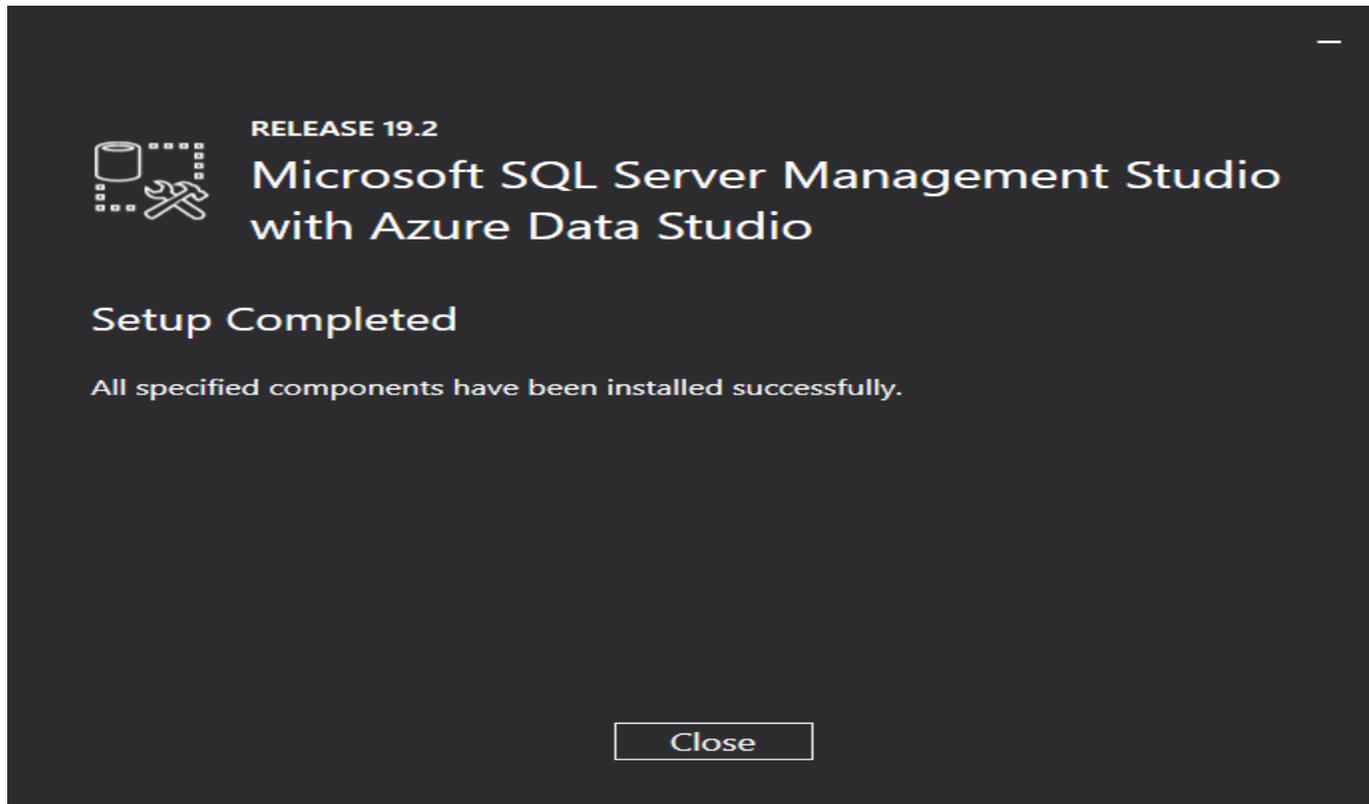
Overall Progress

Cancel

The screenshot shows a dark-themed installation progress dialog. At the top left is the Microsoft SQL Server logo. To its right, the text 'RELEASE 19.2' is displayed. Below this, the main title 'Microsoft SQL Server Management Studio with Azure Data Studio' is shown. Underneath the title, there are two progress bars. The first is labeled 'Package Progress' and shows a blue bar that is nearly full. Below it, the text 'Microsoft OLE DB Driver for SQL Server' is visible. The second progress bar is labeled 'Overall Progress' and shows a blue bar that is approximately one-third full. At the bottom center of the dialog is a 'Cancel' button.

Lab Setup

Successfully Installed



Lab Setup

The next thing is to make it accessible remote, let's use a windows command line utility to check Connection status

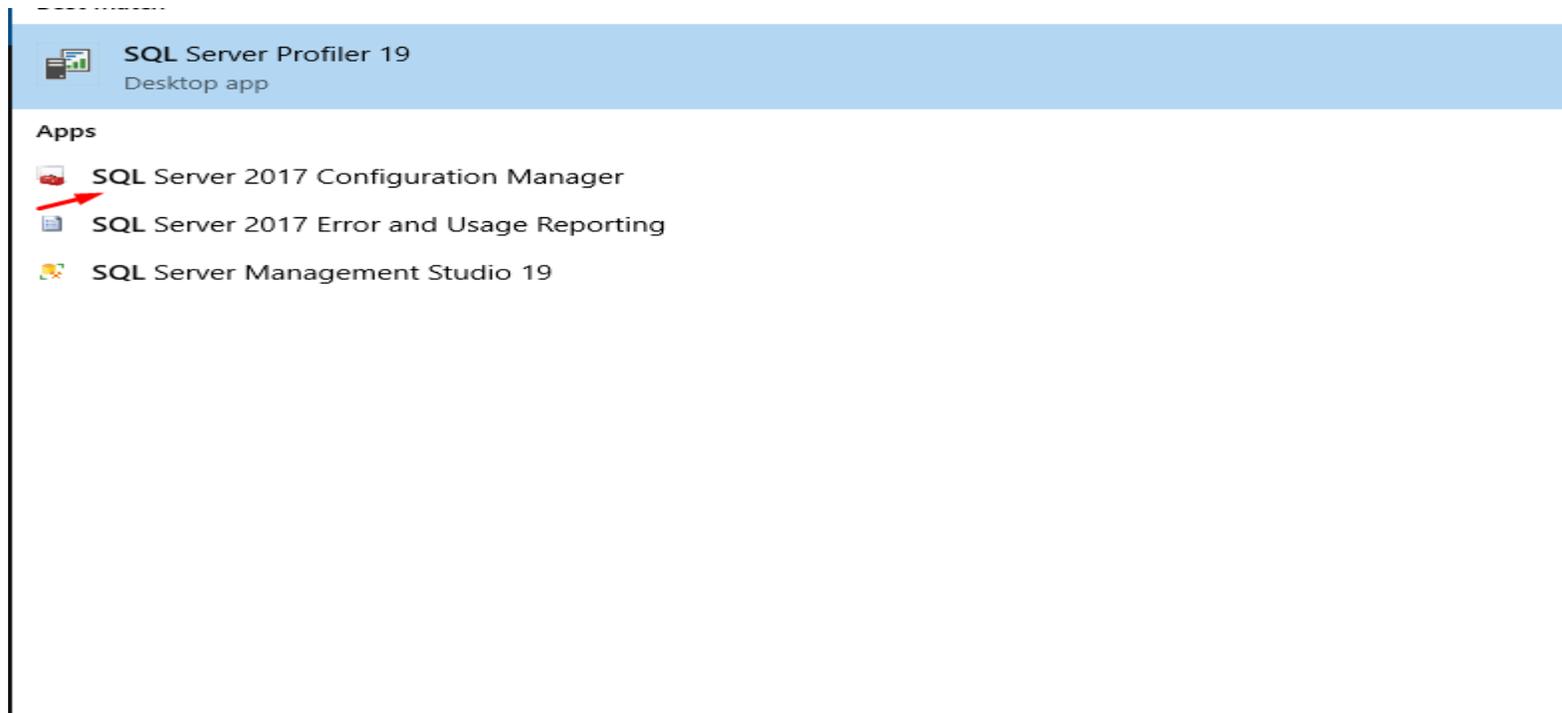
```
PS C:\Users\Administrator> netstat -an | more
Active Connections

```

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3269	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49678	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49698	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49749	0.0.0.0:0	LISTENING
TCP	10.10.1.4:53	0.0.0.0:0	LISTENING
TCP	10.10.1.4:139	0.0.0.0:0	LISTENING
TCP	10.10.1.4:389	10.10.1.4:49697	ESTABLISHED
TCP	10.10.1.4:389	10.10.1.4:49742	ESTABLISHED
TCP	10.10.1.4:389	10.10.1.4:49746	ESTABLISHED
TCP	10.10.1.4:389	10.10.1.7:57947	ESTABLISHED
TCP	10.10.1.4:49667	10.10.1.7:51897	ESTABLISHED
TCP	10.10.1.4:49697	10.10.1.4:389	ESTABLISHED
TCP	10.10.1.4:49742	10.10.1.4:389	ESTABLISHED
TCP	10.10.1.4:49746	10.10.1.4:389	ESTABLISHED
TCP	10.10.1.4:51144	10.10.1.7:49667	TIME_WAIT

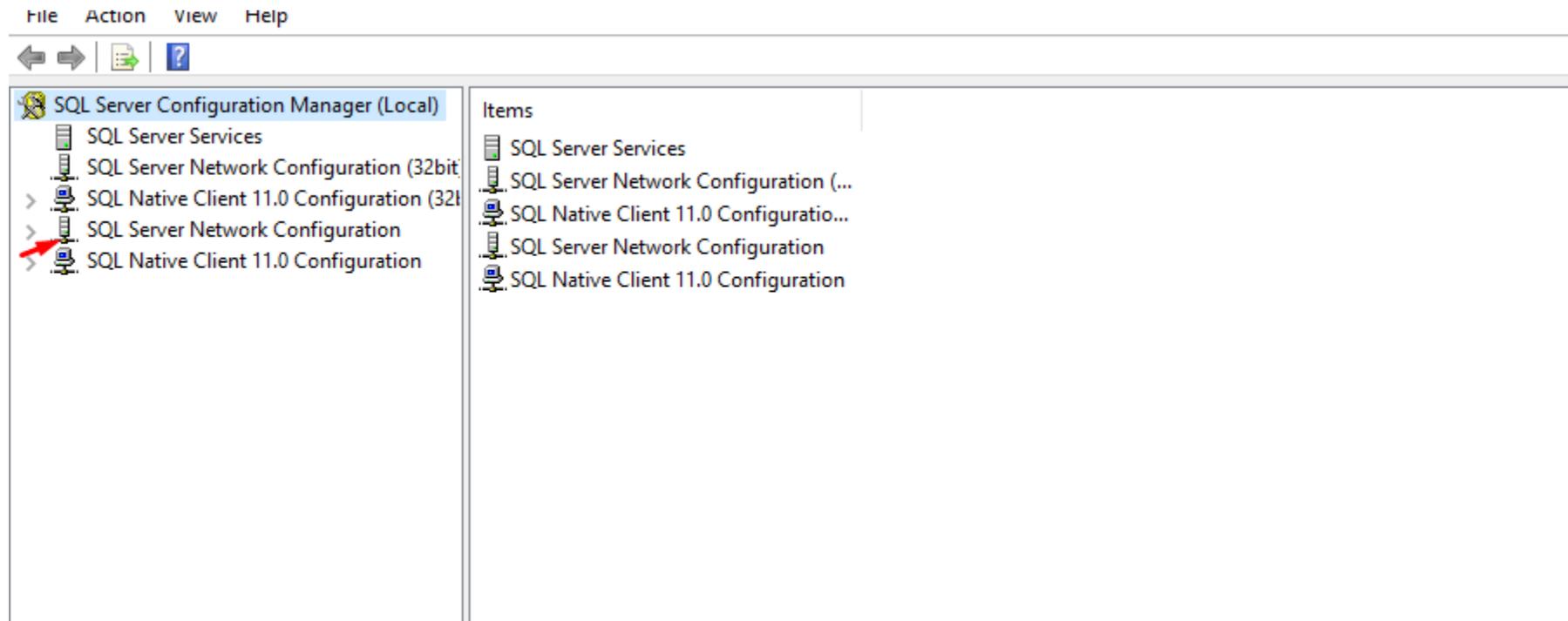
Lab Setup

Mssql server by default listens on port 1433, previous command shows that port 1344 is not in listening state, Let's configure it so that we can access it remotely



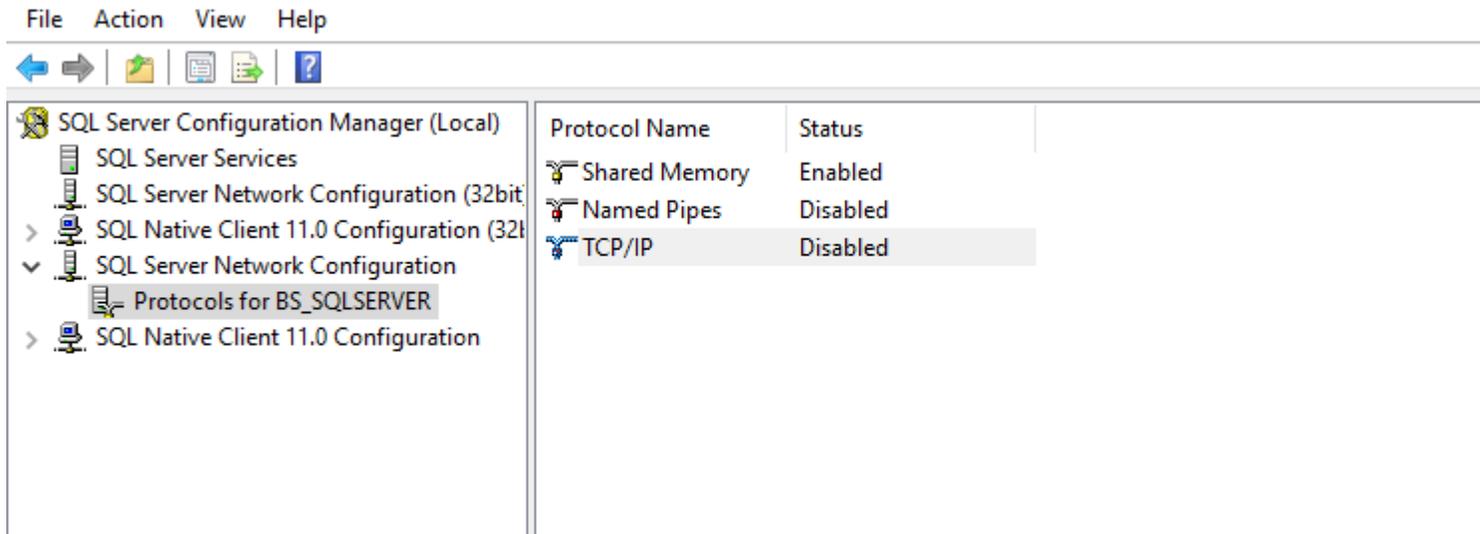
Lab Setup

After searching and clicking Configuration manager, select network configuration



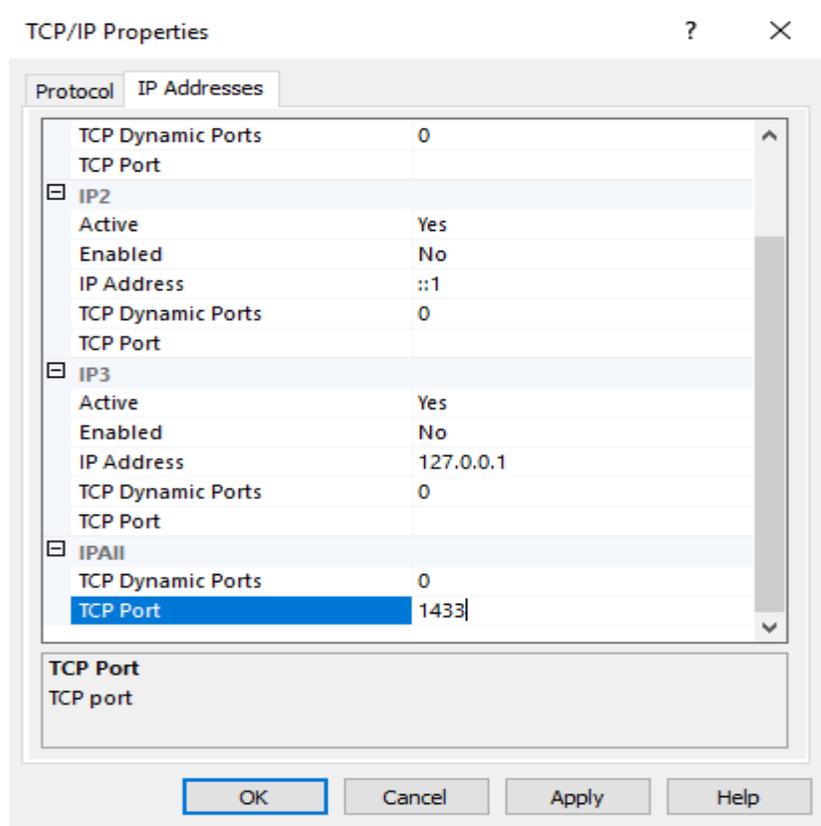
Lab Setup

Double click or right click to go to TCP/IP properties



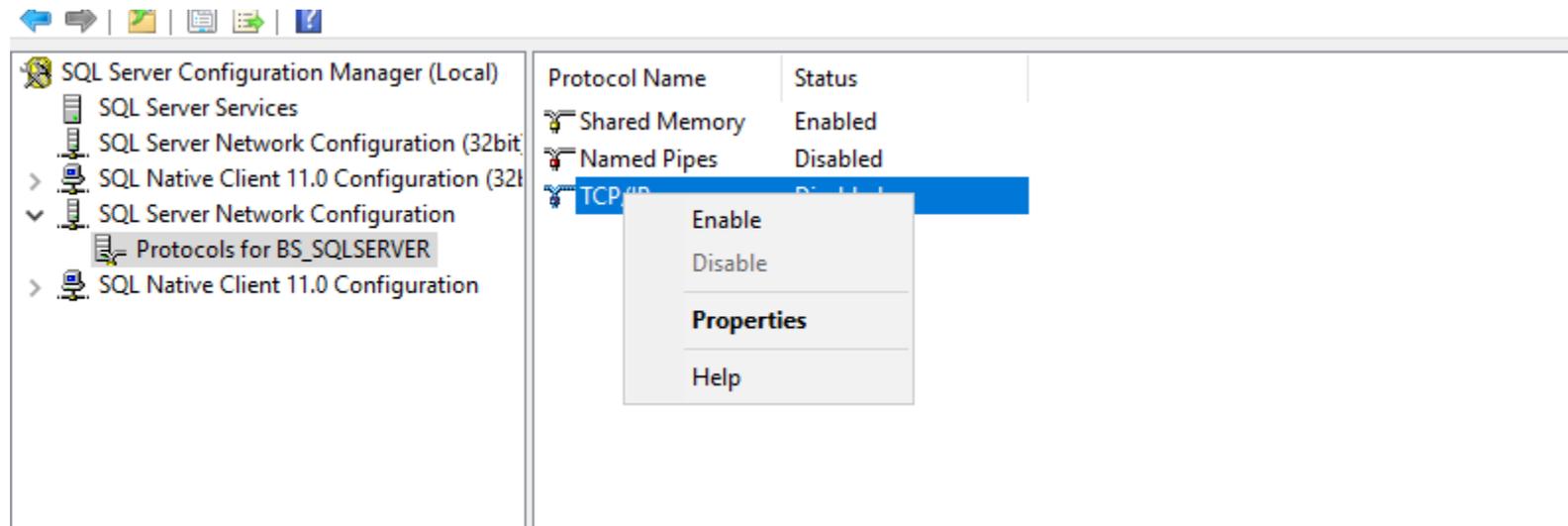
Lab Setup

Select Ip address Tab scroll down and set the port 1344 apply and Ok



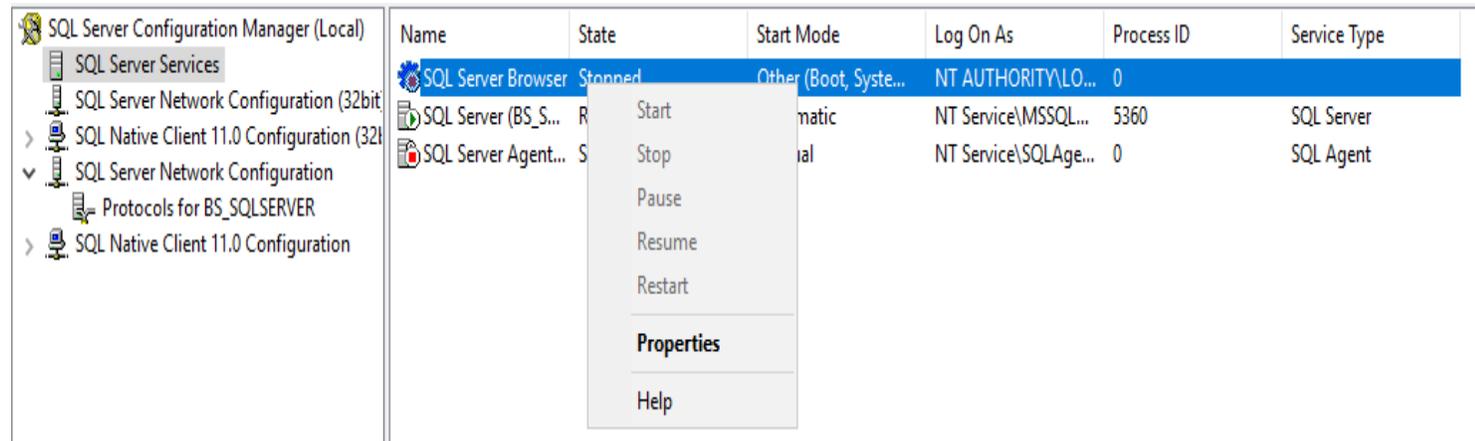
Lab Setup

The TCP/IP protocol is in disable state, let's right click on it and enable it



Lab Setup

Now Let's go sql server services and start the services, right click go to the properties

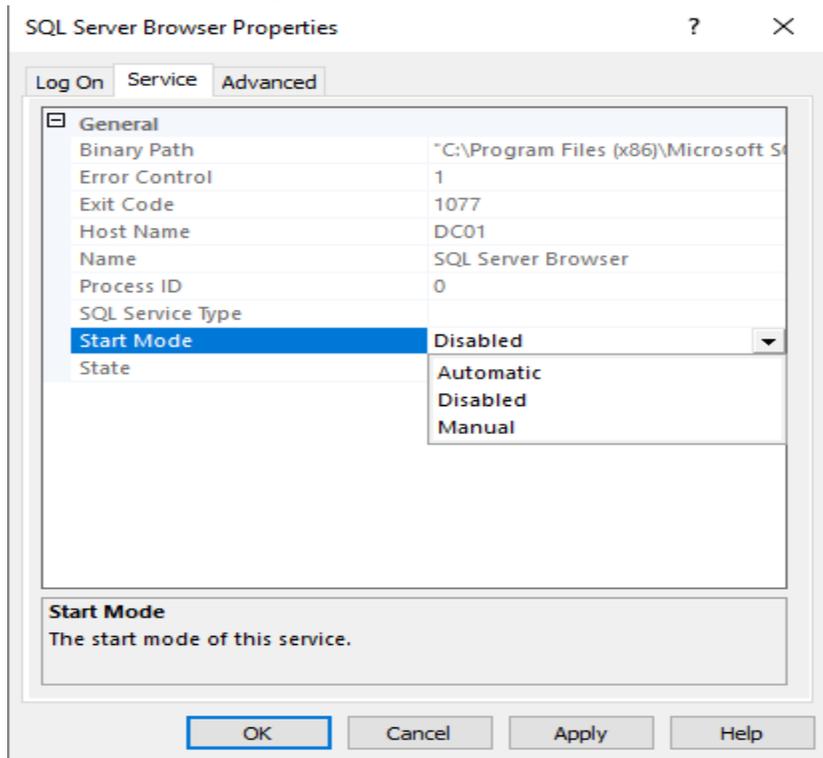


The screenshot shows the SQL Server Configuration Manager interface. The left pane displays a tree view with 'SQL Server Services' selected. The main pane shows a table of services. A right-click context menu is open over the 'SQL Server Browser' service, with 'Properties' highlighted.

Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server Browser	Stopped	Other (Boot, System, Manual or Disabled)	NT AUTHORITY\LOCAL SERVICE	0	SQL Server
SQL Server (BS_S...	Running	Automatic	NT Service\MSSQLSERVER	5360	SQL Server
SQL Server Agent...	Stopped	Manual	NT Service\SQLAgent	0	SQL Agent

Lab Setup

On the Service tab make it start automatically, Apply and Ok, Do the same to the other services



Lab Setup

Now Let's bring up SSMS and connect to it to restart the service

Best match



SQL Server 2017 Configuration Manager

Desktop app

Apps



SQL Server 2017 Error and Usage Reporting



SQL Server Profiler 19



SQL Server Management Studio 19



Lab Setup

Click Connect

Connect to Server

SQL Server

Server type: Database Engine

Server name: DC01\BS_SQLSERVER

Authentication: Windows Authentication

User name: BYTESHIELD\Administrator

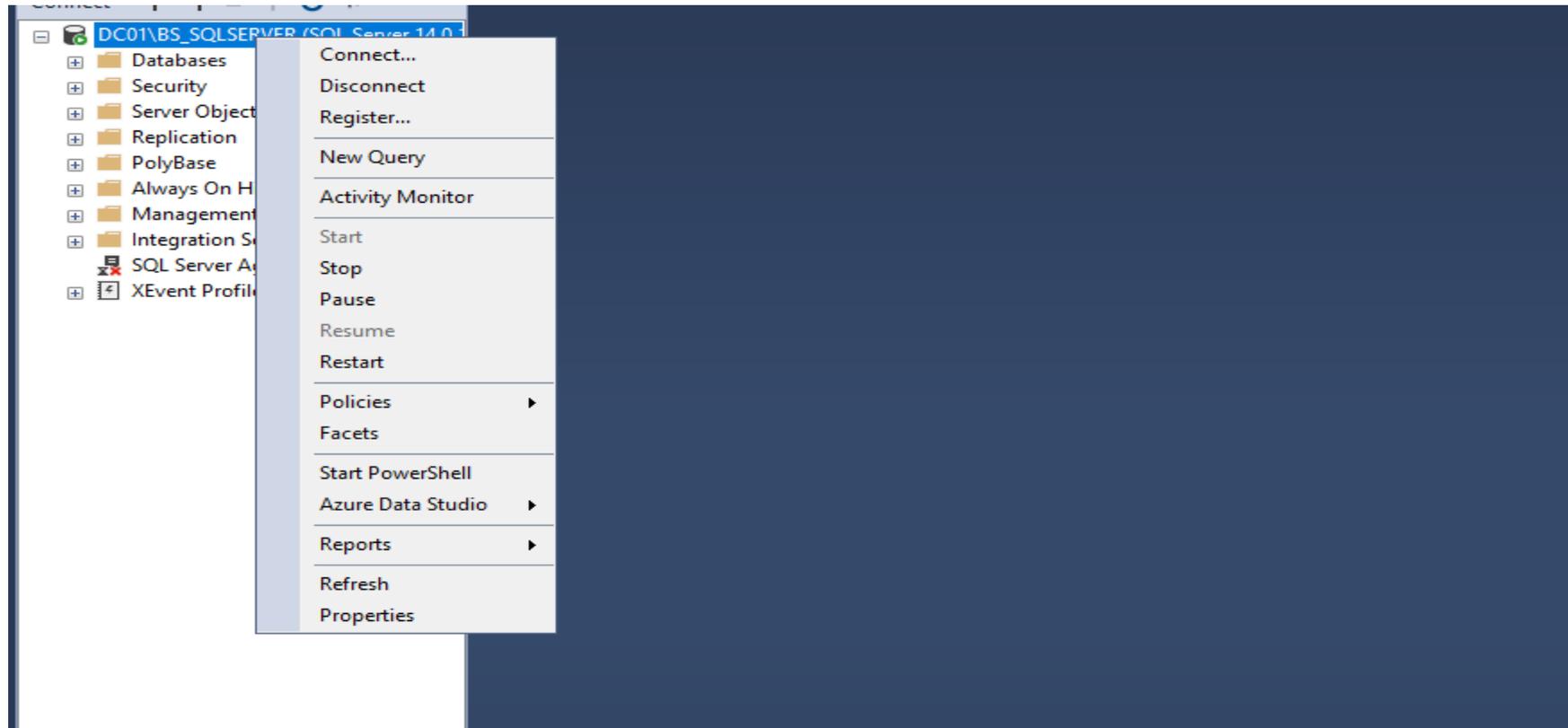
Password:

Remember password

Connect Cancel Help Options >>

Lab Setup

Right Click on the server instance and select restart



Lab Setup

Going back to Powershell console and Check we discovered that the port is in listening state

```
PS C:\Users\Administrator> netstat -an | more
Active Connections

```

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3269	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49678	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49698	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49749	0.0.0.0:0	LISTENING
TCP	0.0.0.0:52061	0.0.0.0:0	LISTENING
TCP	10.10.1.4:53	0.0.0.0:0	LISTENING
TCP	10.10.1.4:139	0.0.0.0:0	LISTENING
TCP	10.10.1.4:389	10.10.1.4:49697	ESTABLISHED
TCP	10.10.1.4:389	10.10.1.4:49742	ESTABLISHED
TCP	10.10.1.4:389	10.10.1.4:49746	ESTABLISHED

Lab Setup

We have Successfully installed Microsoft sql server developer edition and basic Configuration needed for our purpose.

Instruction

Follow the same steps and install Sql server on DC03 and Windows 10 Client Machine

Lab Setup

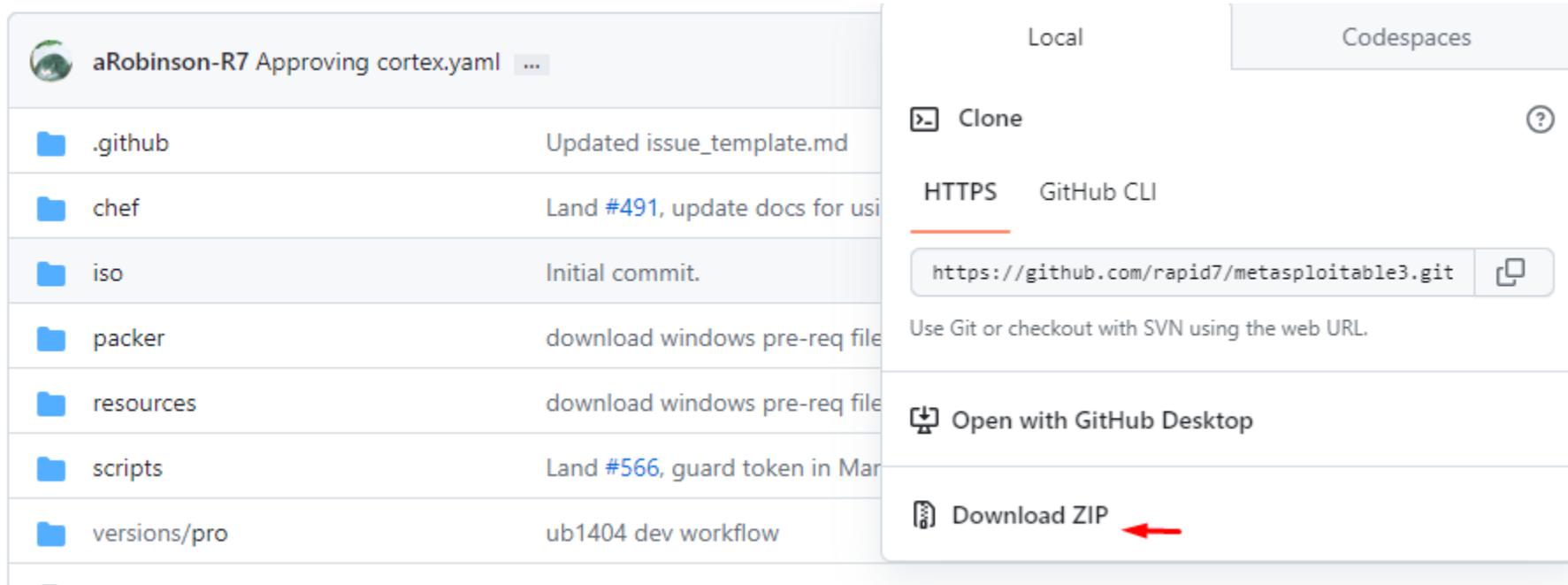
Installing Metasploitable3 on windows server 2008, Let's follow the Installation guide on rapid7 github page

<https://github.com/rapid7/metasploitable3>

```
PS C:\Users\mohas> cd .\Desktop\  
PS C:\Users\mohas\Desktop> mkdir metasploitable3-workspace  
  
Directory: C:\Users\mohas\Desktop  
  
Mode                LastWriteTime         Length Name  
----                -  
d-----           11/19/2023   1:14 AM          metasploitable3-workspace  
  
PS C:\Users\mohas\Desktop>
```

Lab Setup

Download Metasploitable zip file to the folder you created and unzip it there



The screenshot shows a GitHub repository page for 'aRobinson-R7 Approving cortex.yaml'. The repository contains several folders: .github, chef, iso, packer, resources, scripts, and versions/pro. The 'iso' folder is selected, and the context menu is open, showing options: Clone, HTTPS (GitHub CLI), Open with GitHub Desktop, and Download ZIP. A red arrow points to the 'Download ZIP' option.

Folder	Commit Message
.github	Updated issue_template.md
chef	Land #491, update docs for usi
iso	Initial commit.
packer	download windows pre-req file
resources	download windows pre-req file
scripts	Land #566, guard token in Mar
versions/pro	ub1404 dev workflow

Local Codespaces

Clone ?

HTTPS GitHub CLI

<https://github.com/rapid7/metasploitable3.git>

Use Git or checkout with SVN using the web URL.

Open with GitHub Desktop

Download ZIP ←

Lab Setup

Downloading requirement

Building Metasploitable 3

System Requirements:

- OS capable of running all of the required applications listed below
- VT-x/AMD-V Supported Processor recommended
- 65 GB Available space on drive
- 4.5 GB RAM

Requirements:

- [Packer](#)
- [Vagrant](#)
- [Vagrant Reload Plugin](#)
- [VirtualBox](#), libvirt/qemu-kvm, or vmware (paid license required), or parallels (paid license required)
- Internet connection

Lab Setup

Downloading and Installing Packer

Operating System

macOS

Windows

Linux

FreeBSD

NetBSD

OpenBSD

Solaris

Binary download for Windows

386

Version: 1.9.4

Download 

AMD64

Version: 1.9.4

Download 

Lab Setup

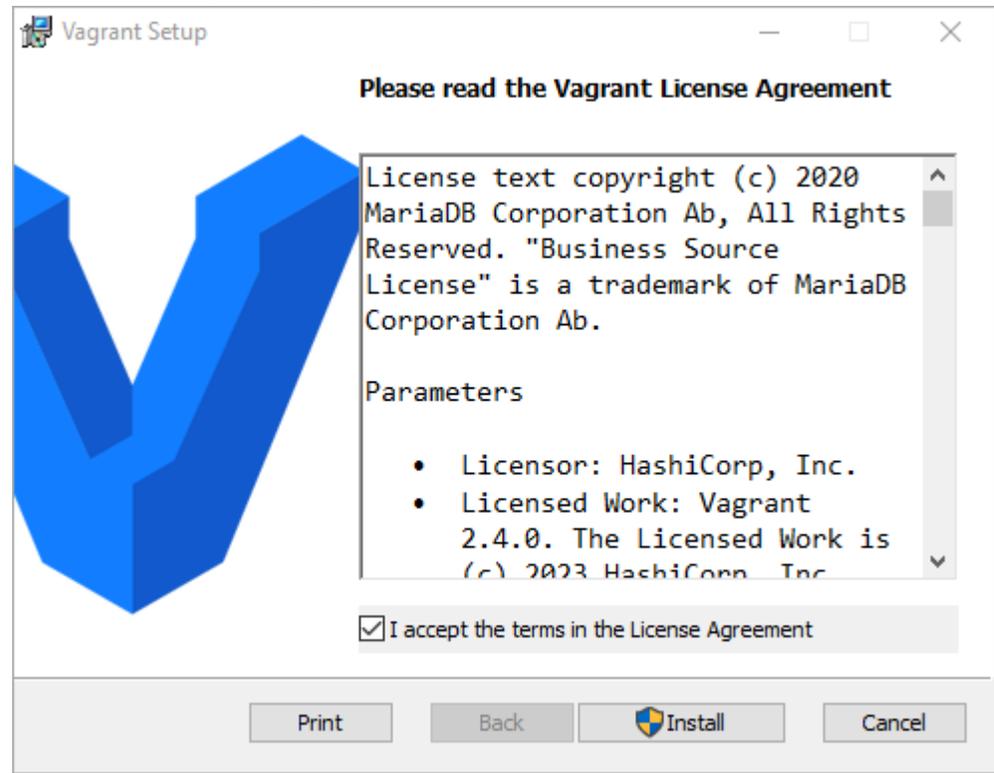
I have Downloaded all the requirement, do the same and save and unzip them all in one folder

Name	Date modified	Type	Size
 metasploitable3-master	11/19/2023 1:19 AM	WinRAR ZIP archive	151,903 KB
 packer_1.9.4_windows_amd64	8/18/2023 8:12 PM	WinRAR ZIP archive	22,188 KB
 vagrant_2.4.0_windows_i686	10/16/2023 8:20 PM	Windows Installer ...	281,460 KB
 vagrant-reload-master	11/19/2023 1:29 AM	WinRAR ZIP archive	6 KB

idi

Lab Setup

Installing Vagrant



Lab Setup

Now we have all the files available it is time to build the Virtual machine

```
PS C:\Users\mohas\Desktop\metasploitable3-workspace> ls

Directory: C:\Users\mohas\Desktop\metasploitable3-workspace

Mode                LastWriteTime         Length Name
----                -
d-----            10/4/2023   2:20 PM          metasploitable3-master
d-----            11/19/2023   1:32 AM          packer_1.9.4_windows_amd64
d-----            11/19/2023   1:32 AM          vagrant-reload-master
-a----            10/16/2023   8:20 PM      288215040 vagrant_2.4.0_windows_i686.msi

PS C:\Users\mohas\Desktop\metasploitable3-workspace> Set-ExecutionPolicy -Scope CurrentUser Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Yes
PS C:\Users\mohas\Desktop\metasploitable3-workspace>
```

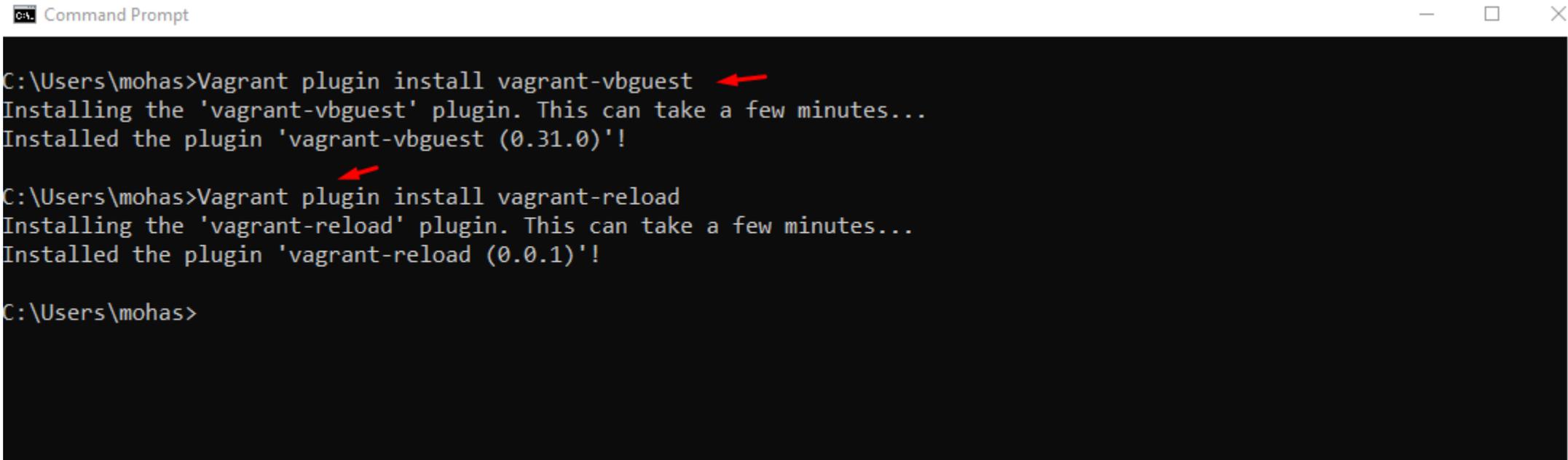
Lab Setup

Vagrant file Download, all the files should be saved in one folder

```
PS C:\Users\mohas\Desktop\metasploitable3-workspace> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"  
PS C:\Users\mohas\Desktop\metasploitable3-workspace>
```

Lab Setup

Now open your command prompt and install some dependencies with vagrant



```
C:\Users\moahas>Vagrant plugin install vagrant-vbguest
Installing the 'vagrant-vbguest' plugin. This can take a few minutes...
Installed the plugin 'vagrant-vbguest (0.31.0)!'

C:\Users\moahas>Vagrant plugin install vagrant-reload
Installing the 'vagrant-reload' plugin. This can take a few minutes...
Installed the plugin 'vagrant-reload (0.0.1)!'

C:\Users\moahas>
```

Lab Setup

It is now time to build the VM using a powershell script called build.ps1 inside metasploitable3 folder we downloaded, running the script without any argument will prompt us for confirmation, if we y the script will build 2 VMs for us linux and windows version of the VM, but typing n will make the script to exit show us the arguments to choose from.

```
PS C:\Users\mohas\Desktop\metasploitable3-workspace\metasploitable3-master> .\build.ps1
```

```
Compatible version of VirtualBox found.
```

```
Compatible version of Packer found.
```

```
Compatible version of Vagrant found.
```

```
Compatible version of vagrant-reload plugin found.
```

```
All requirements found. Proceeding...
```

```
No box name passed as input. Build both the boxes ? (y/n): n
```

```
To build metasploitable boxes separately, use the following commands:
```

```
- .\build.ps1 windows2008
```

```
- .\build.ps1 ubuntu1404
```

Lab Setup

We interested in building windows server 2008 so we will choose it

```
PS C:\Users\mohas\Desktop\metasploitable3-workspace\metasploitable3-master> .\build.ps1 windows2008

Compatible version of VirtualBox found.
Compatible version of Packer found.
Compatible version of Vagrant found.
Compatible version of vagrant-reload plugin found.
All requirements found. Proceeding...
Building metasploitable3-win2k8 Vagrant box...
Warning: Bundled plugins used

This template relies on the use of plugins bundled into the Packer binary.
The practice of bundling external plugins into Packer will be removed in an
upcoming version.

To remove this warning and ensure builds keep working you can install these
external plugins with the 'packer plugins install' command

* packer plugins install github.com/hashicorp/virtualbox
* packer plugins install github.com/hashicorp/qemu
* packer plugins install github.com/hashicorp/vagrant
* packer plugins install github.com/hashicorp/vmware

Alternatively, if you upgrade your templates to HCL2, you can use 'packer init'
with a 'required_plugins' block to automatically install external plugins.

You can try HCL2 by running 'packer hcl2_upgrade
C:\Users\mohas\Desktop\metasploitable3-workspace\metasploitable3-master\packer\templates\windows_2008_r2.json'

virtualbox-iso: output will be in this color.

==> virtualbox-iso: Retrieving Guest additions
==> virtualbox-iso: Trying C:\Program Files\Oracle\VirtualBox\VBBoxGuestAdditions.iso
==> virtualbox-iso: Trying file://C:/Program%20Files/Oracle/VirtualBox/VBoxGuestAdditions.iso
==> virtualbox-iso: file://C:/Program%20Files/Oracle/VirtualBox/VBoxGuestAdditions.iso => C:/Program Files/Oracle/Virtua
lBox/VBoxGuestAdditions.iso
==> virtualbox-iso: Retrieving ISO
==> virtualbox-iso: Trying https://download.microsoft.com/download/4/1/D/41DEA7E0-B30D-4012-A1E3-F24DC03BA1BB/7601.17514
.101119-1850_x64fre_server_eval_en-us-GRMSXEVAL_EN_DVD.iso
```

Lab Setup

The Downloading and Building the VM takes longer time to complete, it depends on your system performance and network speed, after building the VM type `vagrant up win2k8` to import it to Virtualbox

```
PS C:\Users\moahas\Desktop\metasploitable3-workspace\metasploitable3-master> vagrant up win2k8
Bringing machine 'win2k8' up with 'virtualbox' provider...
==> win2k8: Importing base box 'rapid7/metasploitable3-win2k8'...
==> win2k8: Matching MAC address for NAT networking...
==> win2k8: Checking if box 'rapid7/metasploitable3-win2k8' version '0.1.0-weekly' is up to date...
==> win2k8: Setting the name of the VM: metasploitable3-master_win2k8_1700418129117_8961
==> win2k8: Clearing any previously set network interfaces...
A host only network interface you're attempting to configure via DHCP
already has a conflicting host only adapter with DHCP enabled. The
DHCP on this adapter is incompatible with the DHCP settings. Two
host only network interfaces are not allowed to overlap, and each
host only network interface can have only one DHCP server. Please
reconfigure your host only network or remove the virtual machine
using the other host only network.
PS C:\Users\moahas\Desktop\metasploitable3-workspace\metasploitable3-master>
```

Lab Setup

Here we go, we logon with username vagrant and password vagrant



Lab Setup

Now before renaming and joining the Vm to the Domain, let's change the network configuration

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

Loading personal and system profiles took 11145ms.
PS C:\Users\vagrant> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

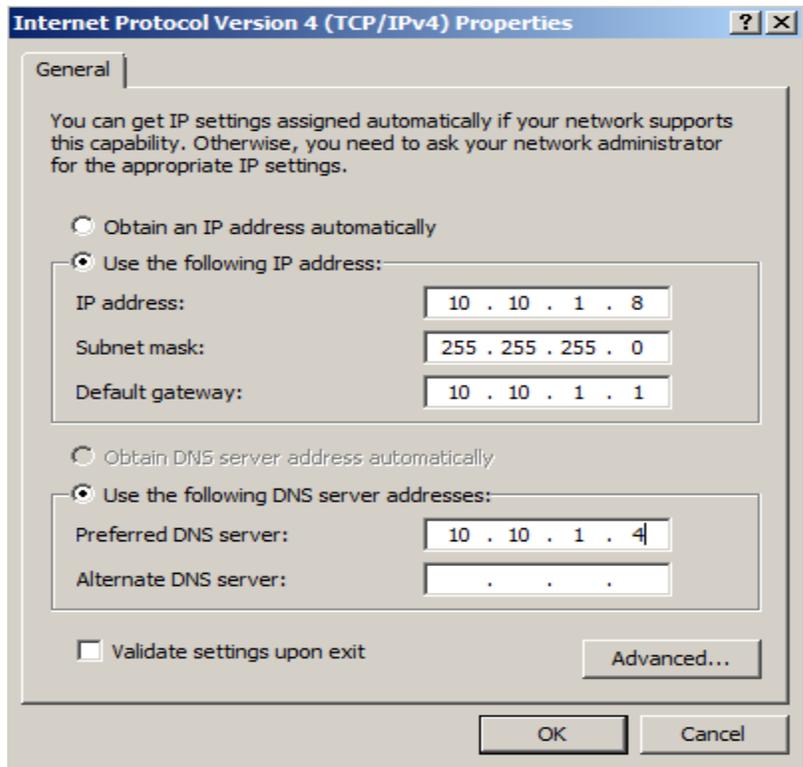
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::fd63:83a2:85e3:4729%11
    IPv4 Address. . . . . : 10.10.1.8
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.1.1

Tunnel adapter isatap.<6FEEDED4-FC1E-4857-BEB8-72167D5BDAA6>:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
PS C:\Users\vagrant> _
```

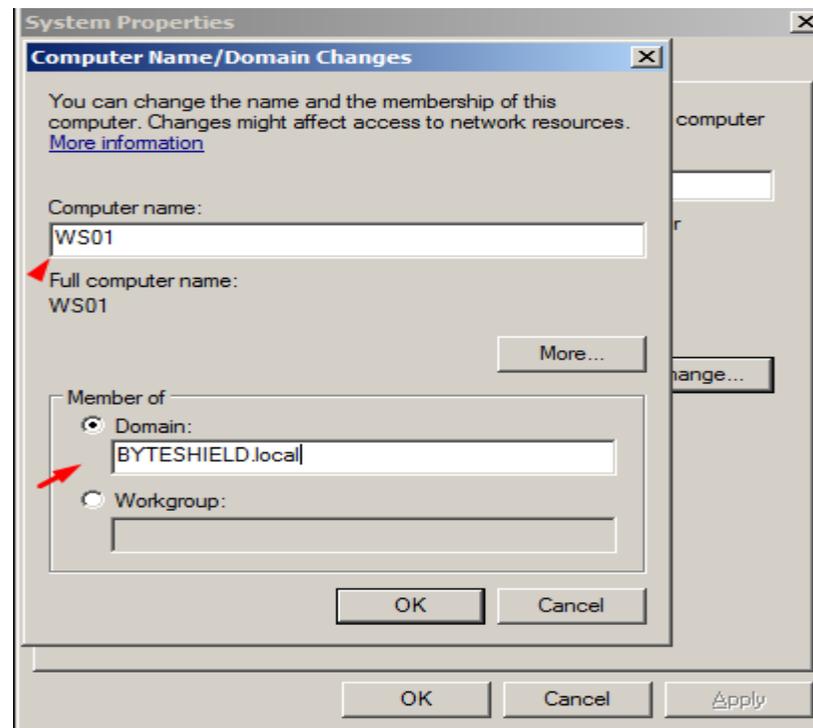
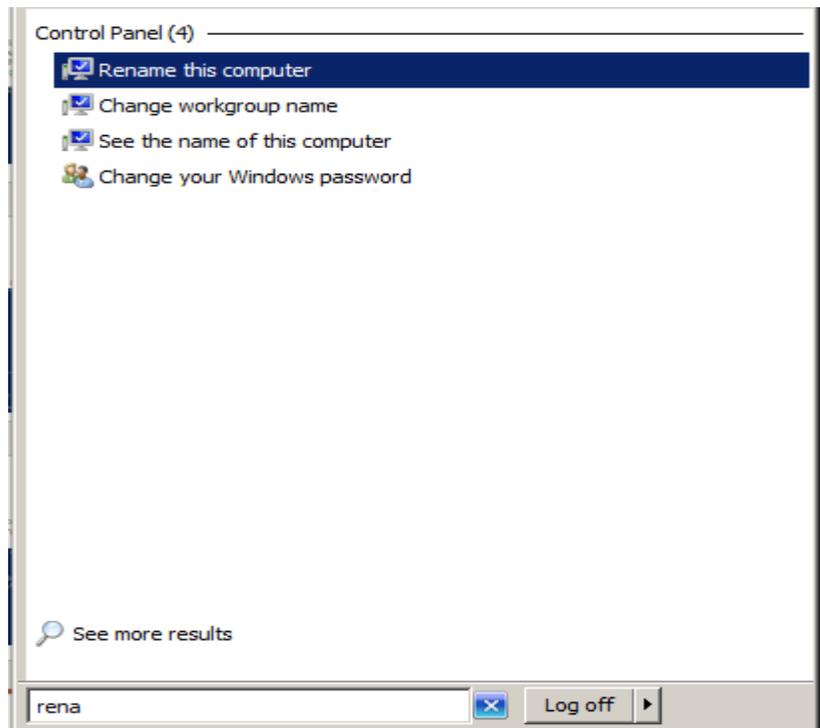
Lab Setup

Here is the IPv4 Static Configuration



Lab Setup

Search for rename this Computer to change the name of the computer to WS01 and join it to Byteshield Domain



Lab Setup

Now We can Verify our setup

```
Administrator: Windows PowerShell
PS C:\Users\vagrant> ping dc01

Pinging DC01.BYTESHIELD.local [10.10.1.4] with 32 bytes of data:
Reply from 10.10.1.4: bytes=32 time=1ms TTL=128
Reply from 10.10.1.4: bytes=32 time<1ms TTL=128
Reply from 10.10.1.4: bytes=32 time<1ms TTL=128
Reply from 10.10.1.4: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\vagrant> ping win10-client-01

Pinging win10-client-01.BYTESHIELD.local [10.10.1.5] with 32 bytes of data:
Reply from 10.10.1.5: bytes=32 time=1ms TTL=128
Reply from 10.10.1.5: bytes=32 time<1ms TTL=128
Reply from 10.10.1.5: bytes=32 time<1ms TTL=128
Reply from 10.10.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\vagrant> ping win10-client-02

Pinging win10-client-02.BYTESHIELD.local [10.10.1.9] with 32 bytes of data:
Reply from 10.10.1.9: bytes=32 time<1ms TTL=128
Reply from 10.10.1.9: bytes=32 time=1ms TTL=128
Reply from 10.10.1.9: bytes=32 time<1ms TTL=128
Reply from 10.10.1.9: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\vagrant> _
```

Lab Setup

We have done a lot of Installation setup, now we will focus on Domain and Sql server users and groups creation and their respective access rights

DC01 Users

joe.smith	david.williams	jessica.williams
lisa.jones	james.brown	mike.johnson
p.brown	justin.smith	Richard.White
enox	michelle.smith	
S.Service	Sql_Service	

Lab Setup

Users & Groups

DC02 Users

anthony.smith christopher.smith

jessica.williams Jessy_adm

tom.smith TRSql_Service

Lab Setup

DC03 Users

amanda.jones

paul.jones

michelle.Moore

jason.johnson

jennifer.williams

Clement.Kevin

michelle.johnson

mike.davis

Brown.lee

Ruth.David

TCSql_Service

Lab Setup

Win10-Client-01 Users

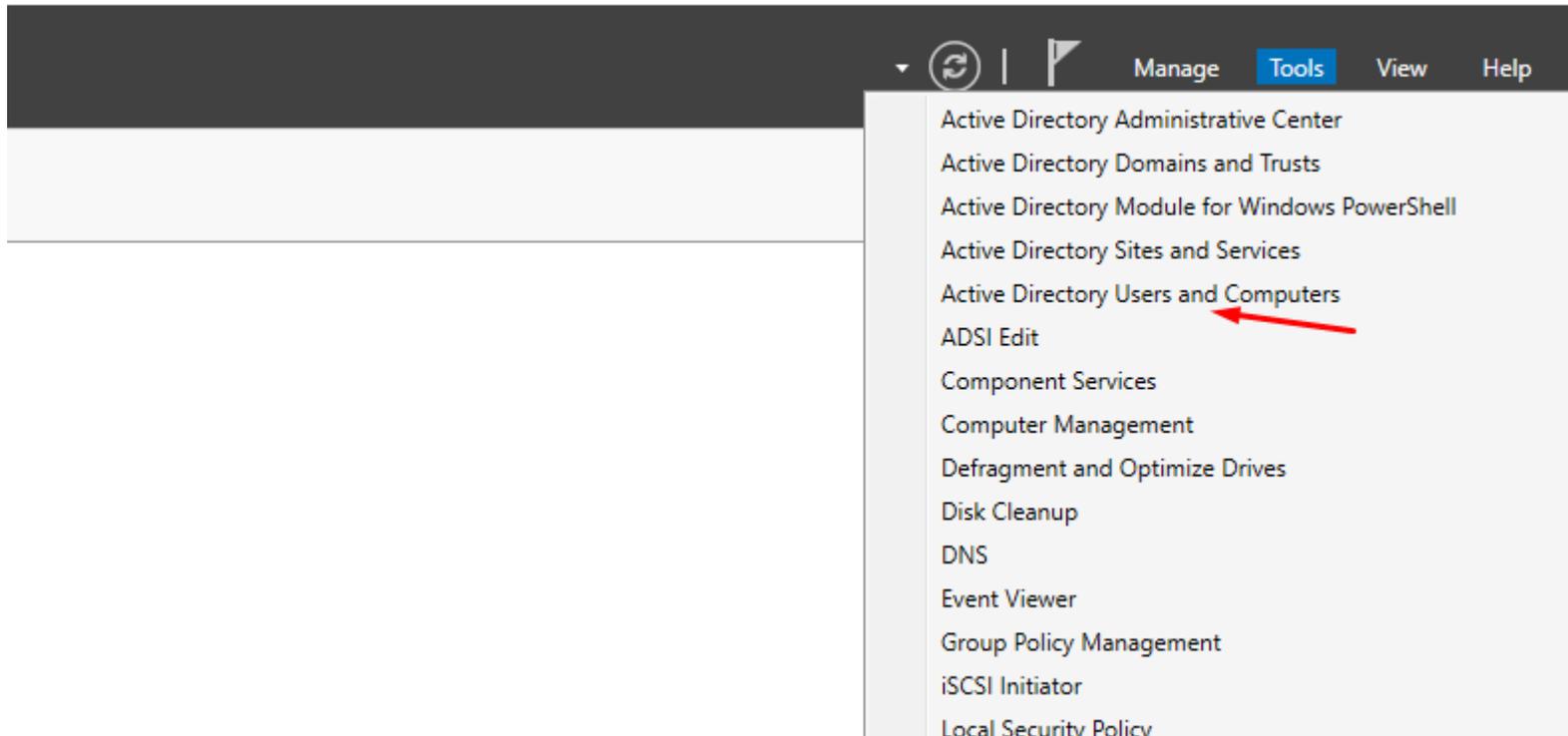
jessica.williams joe.smith justin.smith
local_adm p.brown

Win10-Client-02 Users

Ruth.David Brown.lee Richard.White
Clement.Kevin michelle.Moore

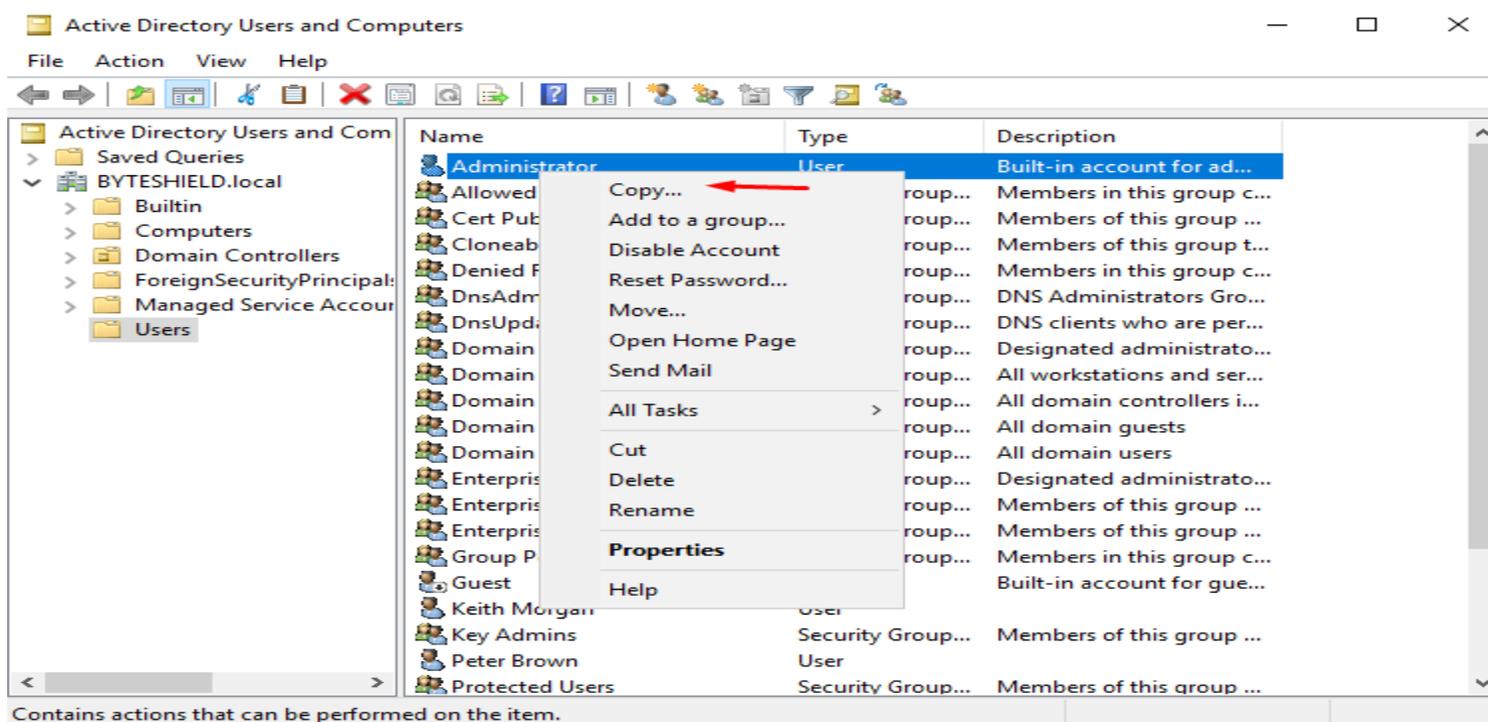
Lab Setup

Now it is to start Creating users and groups, starting with DC01, logon and open sever manager



Lab Setup

Right click on the administrator and click copy to Create an Admin user



Lab Setup

David Williams as Admin User

The image displays two sequential screenshots of the 'Copy Object - User' dialog box in Windows, showing the configuration for a new user named David Williams.

Left Screenshot: User Information

- Create in:** BYTESHIELD.local/Users
- First name:** David
- Last name:** Williams
- Full name:** David Williams
- User logon name:** David.Williams (with a dropdown menu showing @BYTESHIELD.local)
- User logon name (pre-Windows 2000):** BYTESHIELD\David.Williams

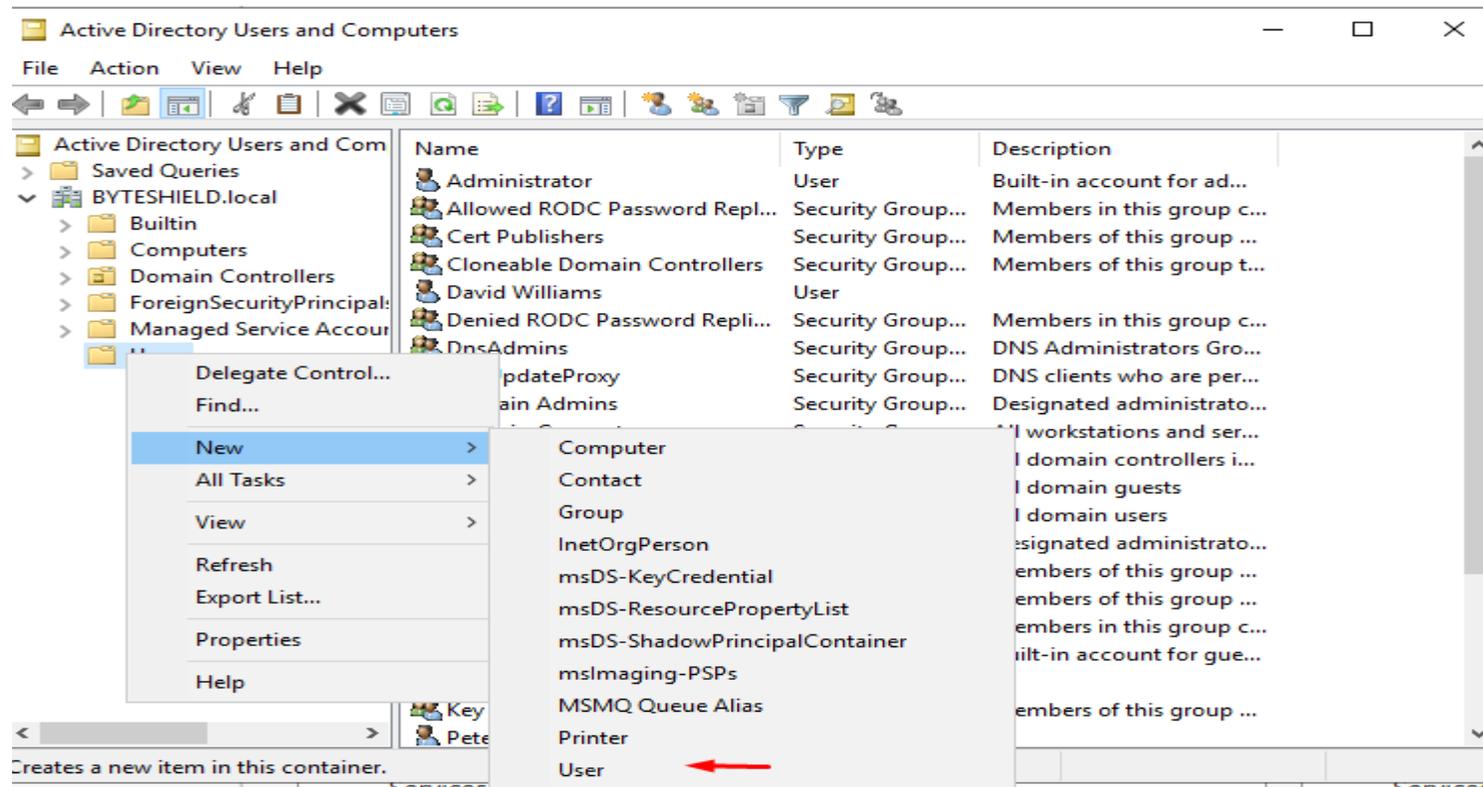
Right Screenshot: Password and Account Settings

- Password:** [Masked]
- Confirm password:** [Masked]
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

Both screenshots show navigation buttons at the bottom: < Back, Next >, and Cancel.

Lab Setup

Right click on the users container > new to Create a Regular user



Lab Setup

Joe Smith as a regular user

The image displays two side-by-side screenshots of the 'New Object - User' dialog box in Windows, illustrating the steps to create a regular user named Joe Smith.

Left Screenshot (Name Tab):

- Create in:** BYTESHIELD.local/Users
- First name:** joe
- Last name:** smith
- Full name:** joe smith
- User logon name:** joe.smith (with a dropdown menu showing @BYTESHIELD.local)
- User logon name (pre-Windows 2000):** BYTESHIELD\ (with a dropdown menu showing joe.smith)

Right Screenshot (Password Tab):

- Password:** [Redacted]
- Confirm password:** [Redacted]
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

Lab Setup

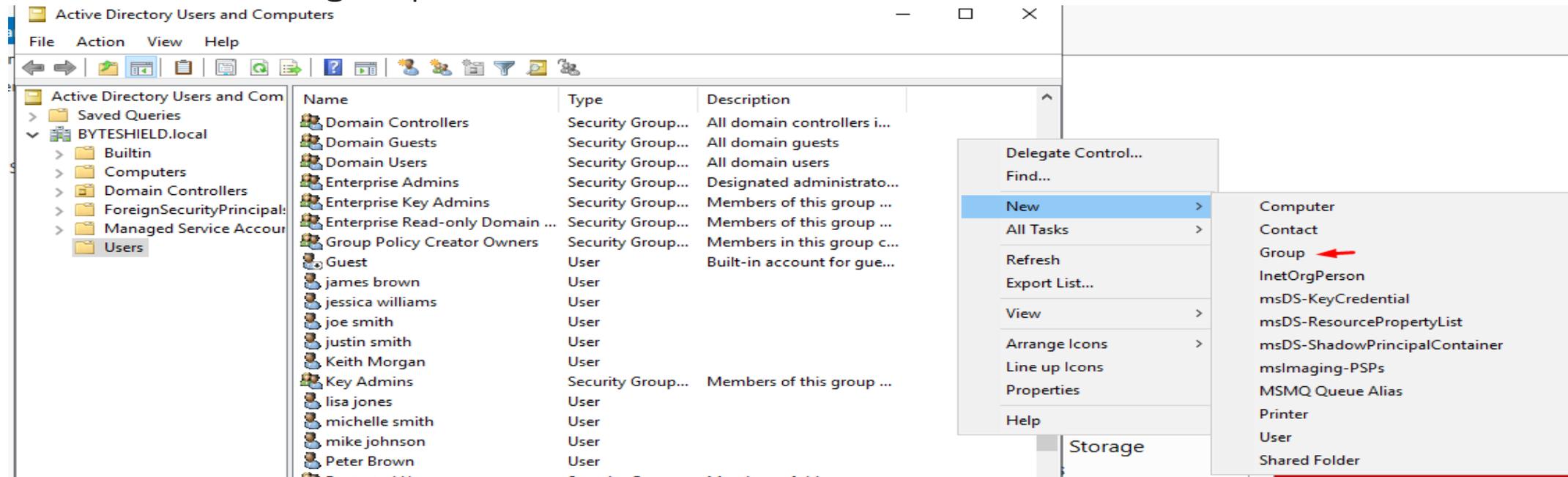
We have Created two domain users, admin and a regular user

Instruction

- On DC01 Create the rest of the users with Sql_Service as Domain admin
- On DC02 Create the Users with TRSql_Service and Jessy_admin as Domain Admins
- On DC03 Create the Users with TCSql_Service and Paul.jones as Domain Admins
- On the two Windows Clients logon with the respective Domain users
- On WS01 make justin.smith a local admin, logon with p.brown Credentials also

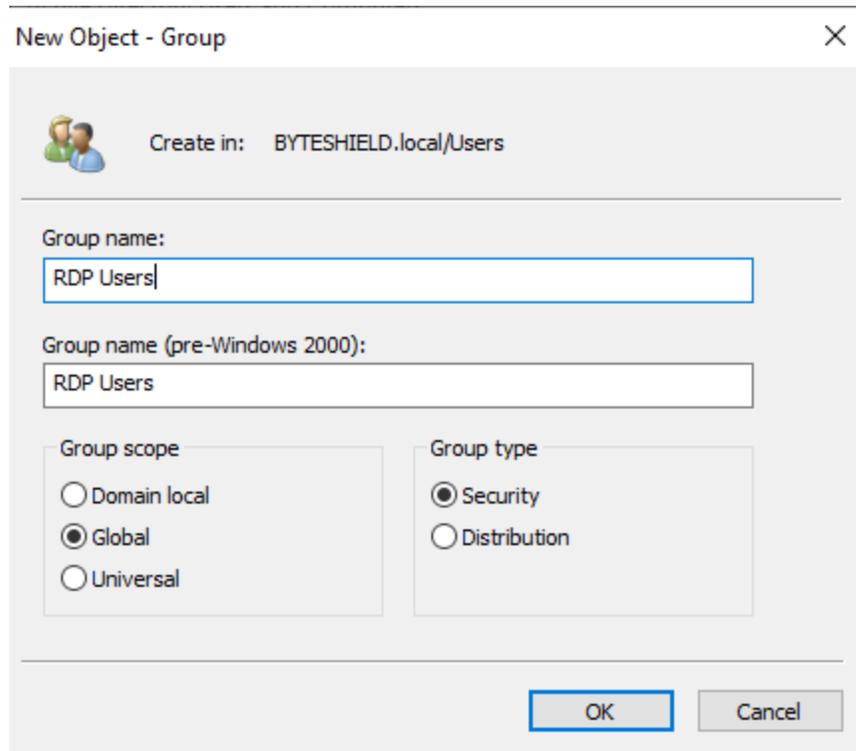
Lab Setup

After Users Creation, the next thing is to create user's groups, right anywhere within and select new > group



Lab Setup

Remote Desktop Users Group Creation



New Object - Group

Create in: BYTESHIELD.local/Users

Group name:
RDP Users

Group name (pre-Windows 2000):
RDP Users

Group scope

- Domain local
- Global
- Universal

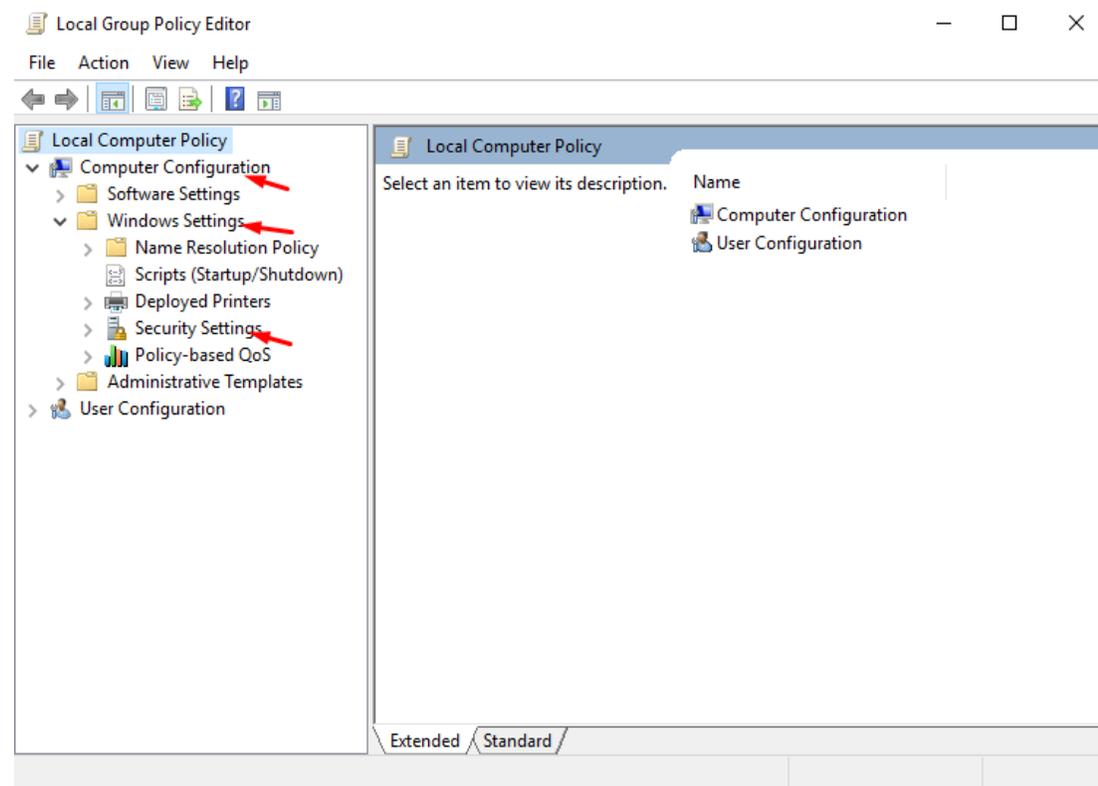
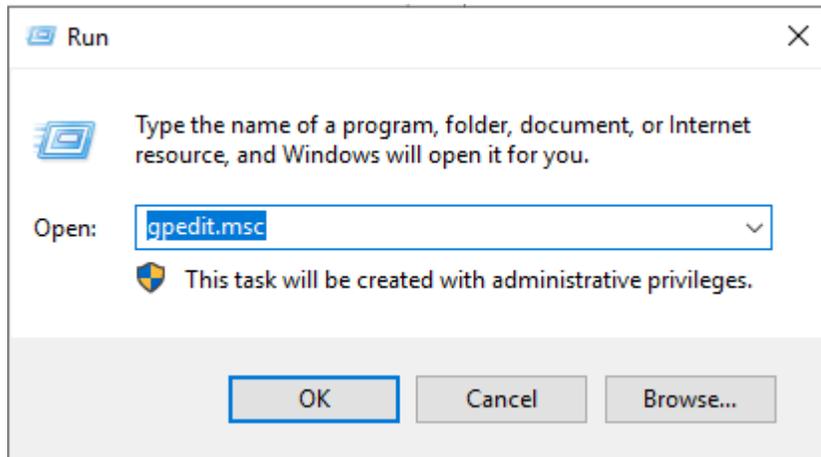
Group type

- Security
- Distribution

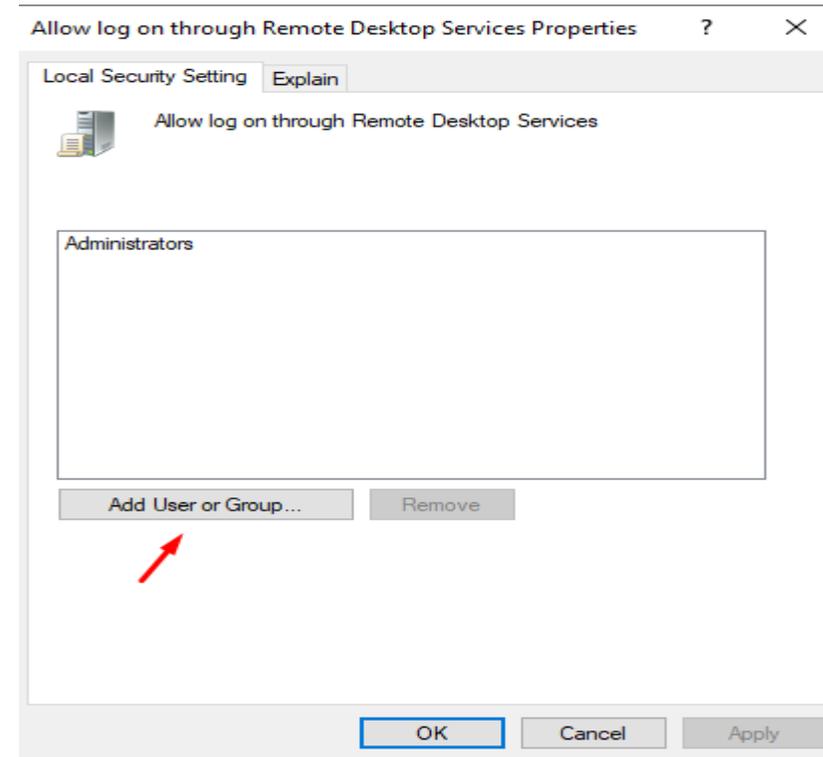
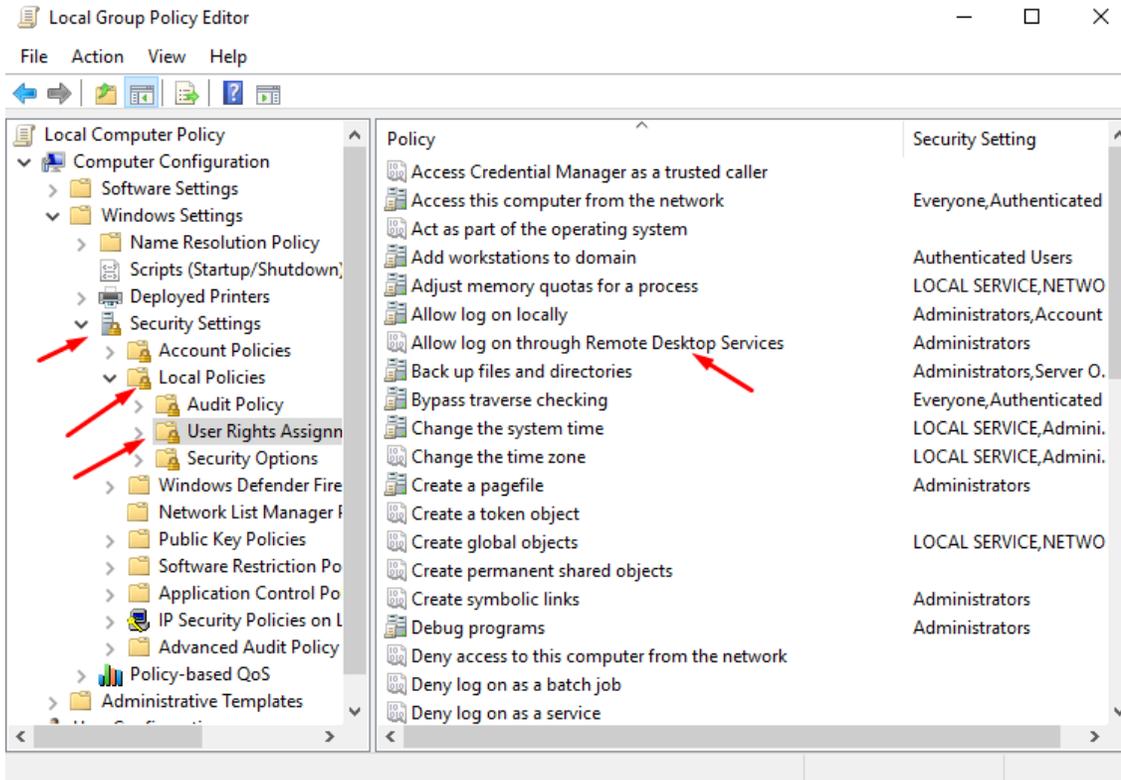
OK Cancel

Lab Setup

Now let's Create localuser group Policy for remote desktop access

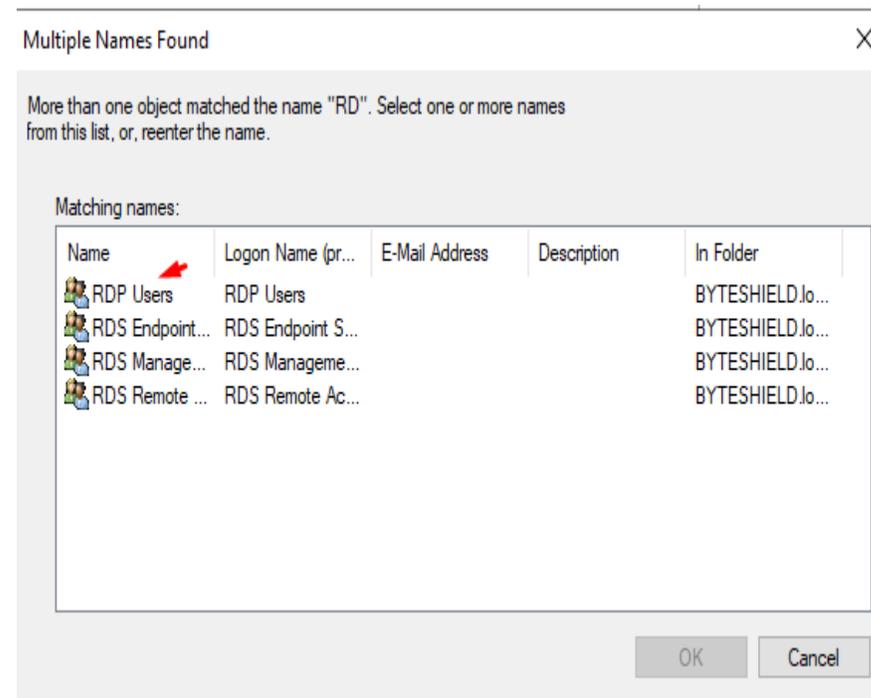
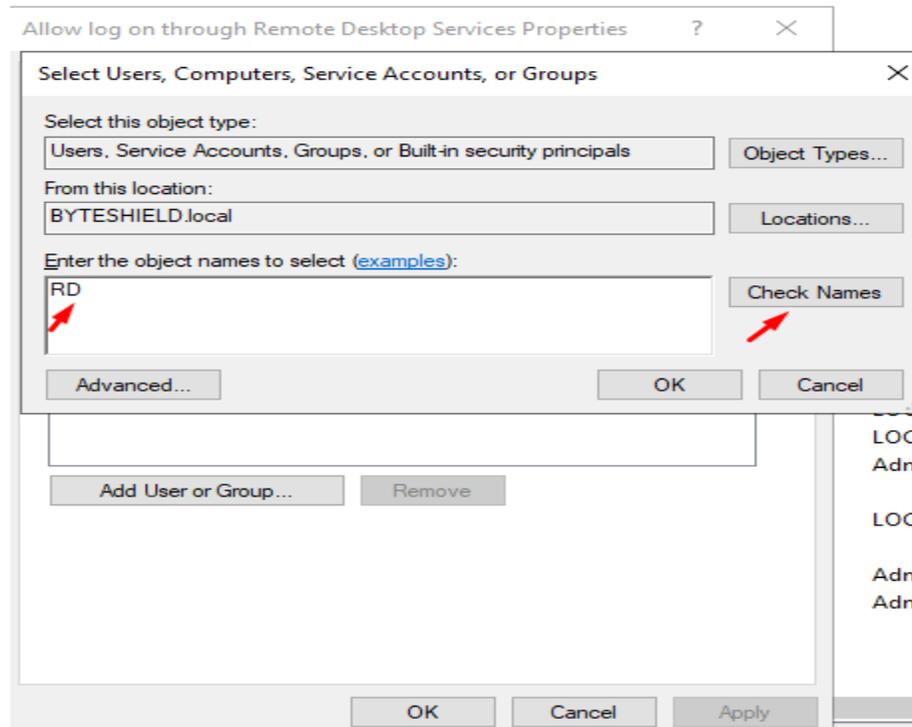


Lab Setup



Lab Setup

Now Let's Search for the RDP users Group we just Created



Lab Setup

Remote Desktop Service is disabled by default, we can enable it

The image shows two screenshots from a Windows Server 2012 R2 environment. The left screenshot displays the 'PROPERTIES For DC01' window, where the 'Remote Desktop' status is 'Disabled', indicated by a red arrow. The right screenshot shows the 'System Properties' dialog box, 'Remote' tab, where the 'Allow remote connections to this computer' radio button is selected, also indicated by a red arrow.

PROPERTIES For DC01

Computer name	DC01
Domain	BYTESHIELD.local
Windows Defender Firewall	Private: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet	10.10.1.4

System Properties

Computer Name | Hardware | Advanced | Remote

Remote Assistance

Allow Remote Assistance connections to this computer

Advanced...

Remote Desktop

Choose an option, and then specify who can connect.

Don't allow remote connections to this computer

Allow remote connections to this computer

Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

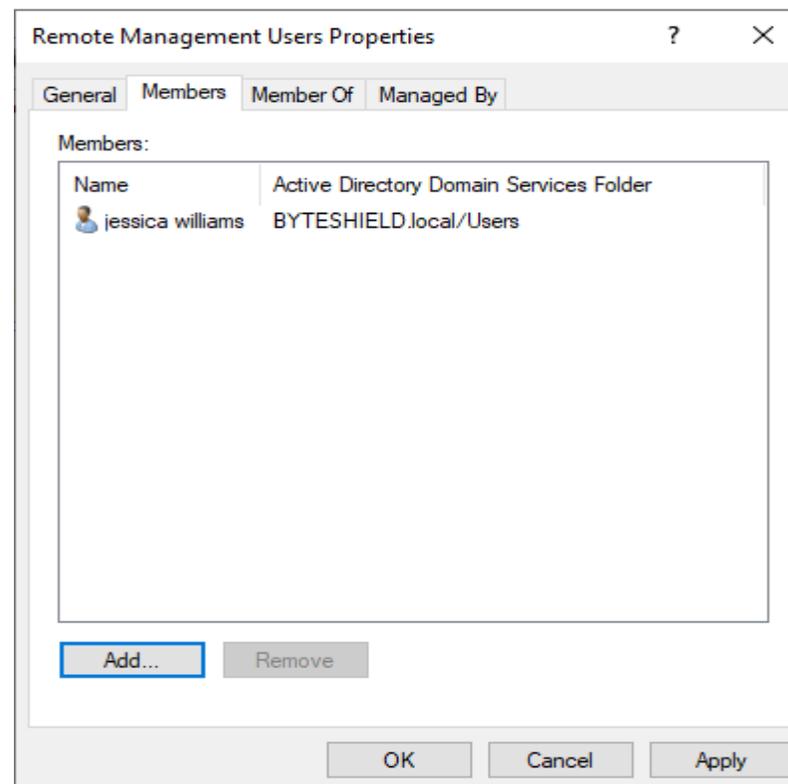
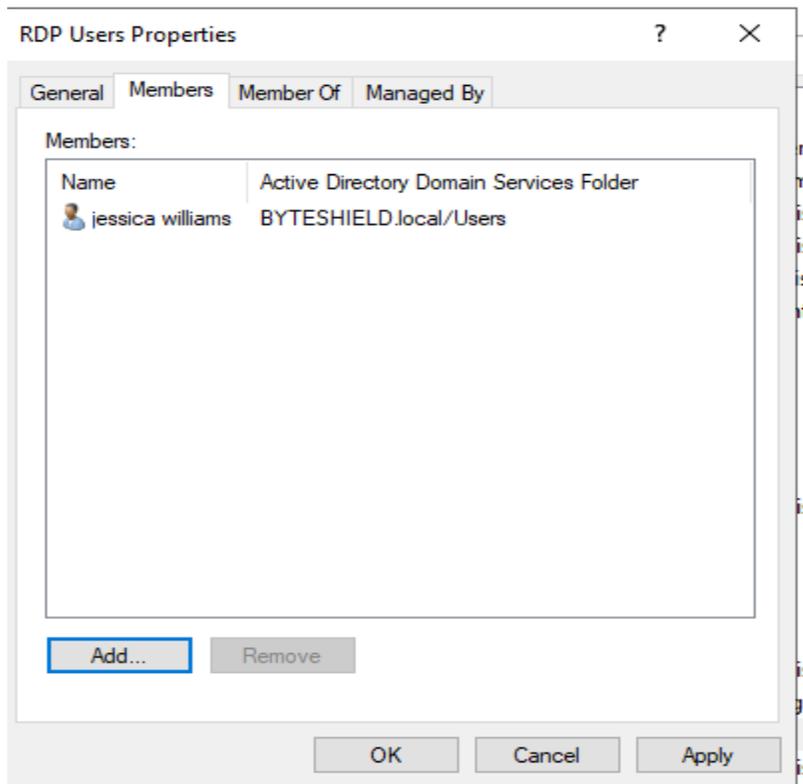
Help me choose

Select Users...

OK Cancel Apply

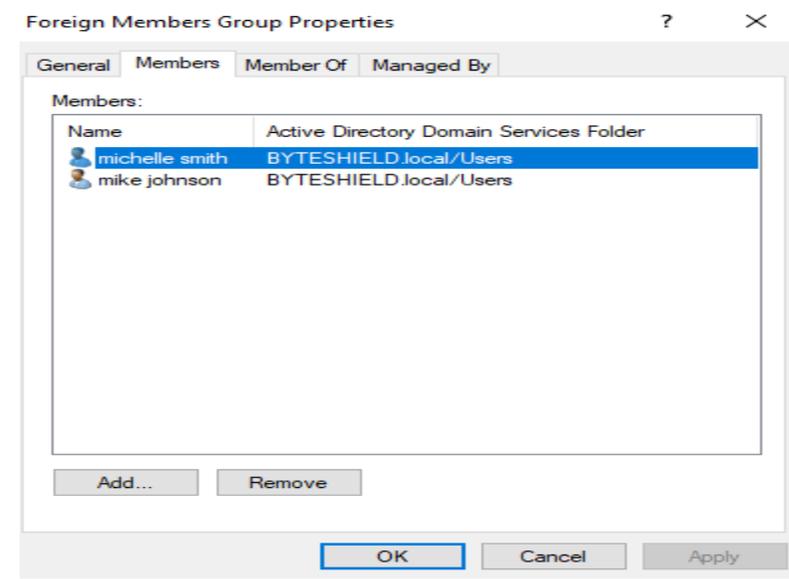
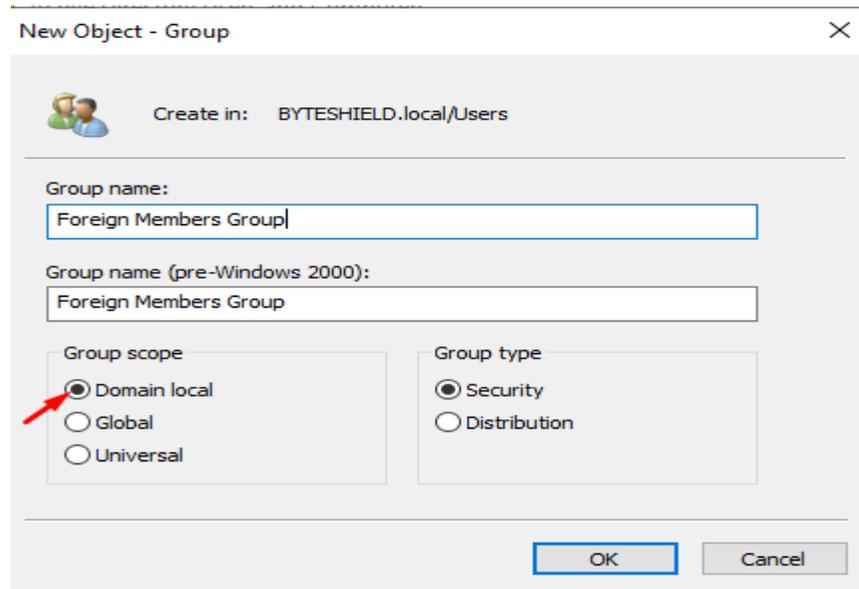
Lab Setup

Let's add Jessica Williams to the RDP users and Remote management service Groups



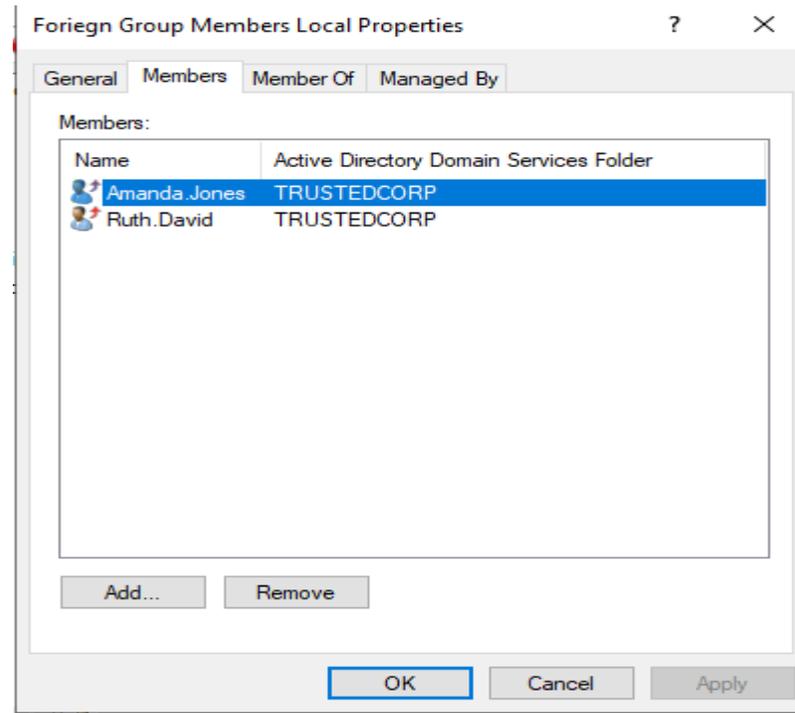
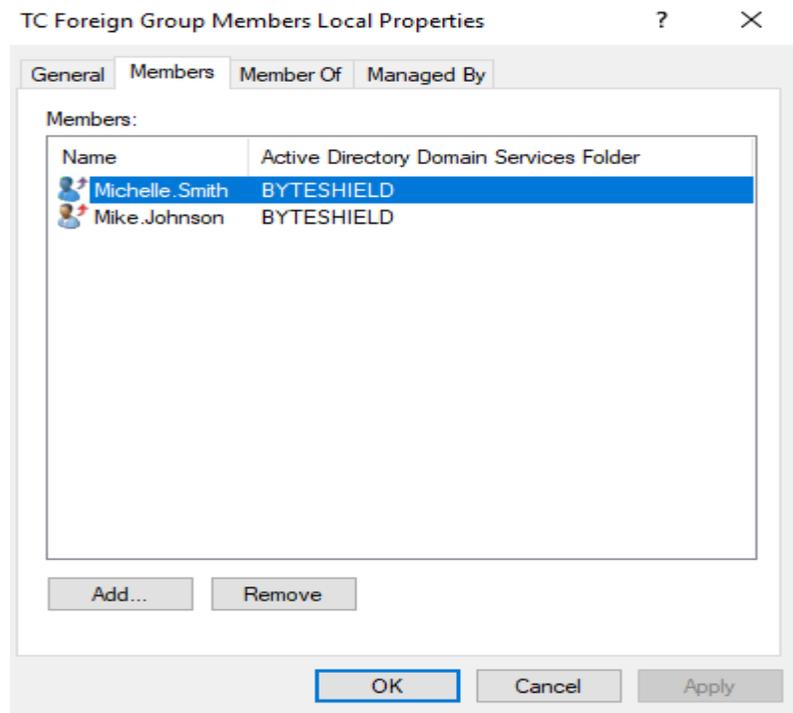
Lab Setup

Foreign Group membership, we are Create a local and Universal BYTESHIELD Domain Group and map them to TRUSTEDCORP as Foreign Members and and vise versa, By default Domain groups are created as global groups, we will change that to domain local group, we have michelle and mike as member of the domain local group



Lab Setup

We will Create Domain localgroup in BYTESHIELD and add some TRUSTEDCORP domain Users as foreign group members and vice versa.



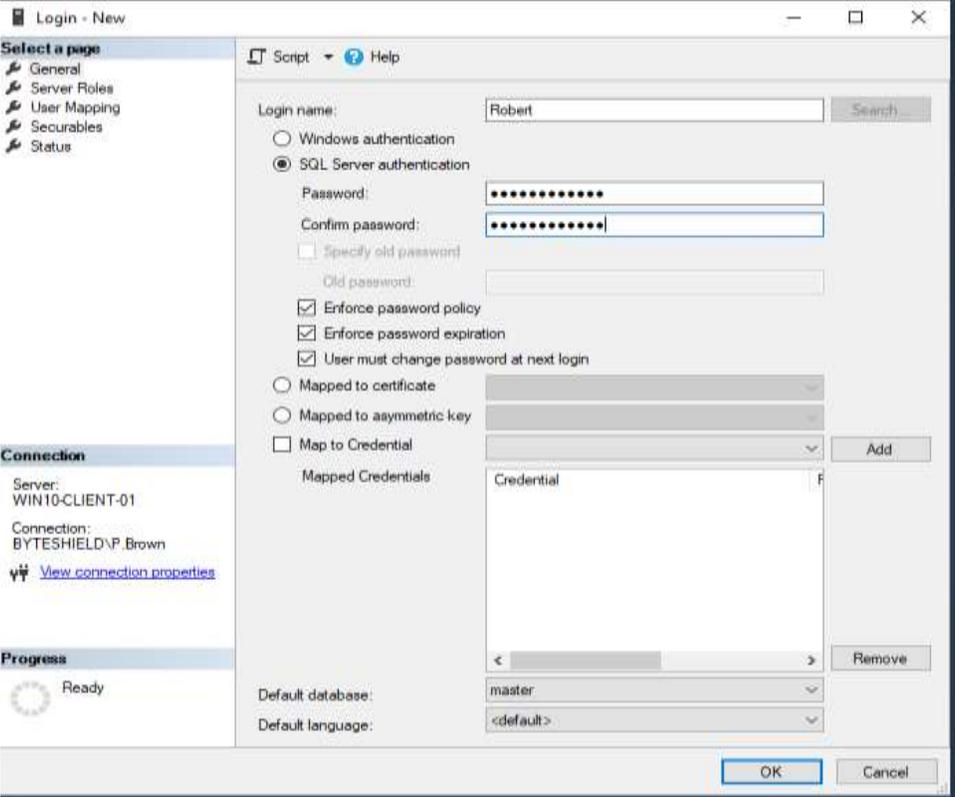
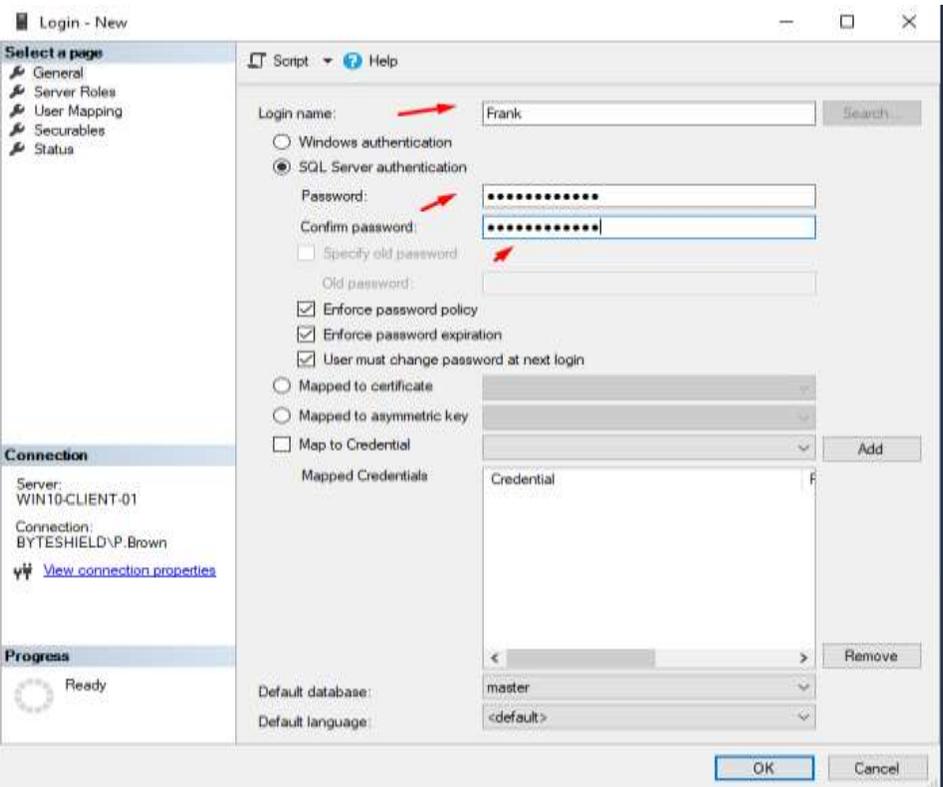
Lab Setup

Creating SQL Server Users Frank and Robert, Win10-Client-01 we Create 3 Users, 2 with Sql Authentication while 1 Windows authentication

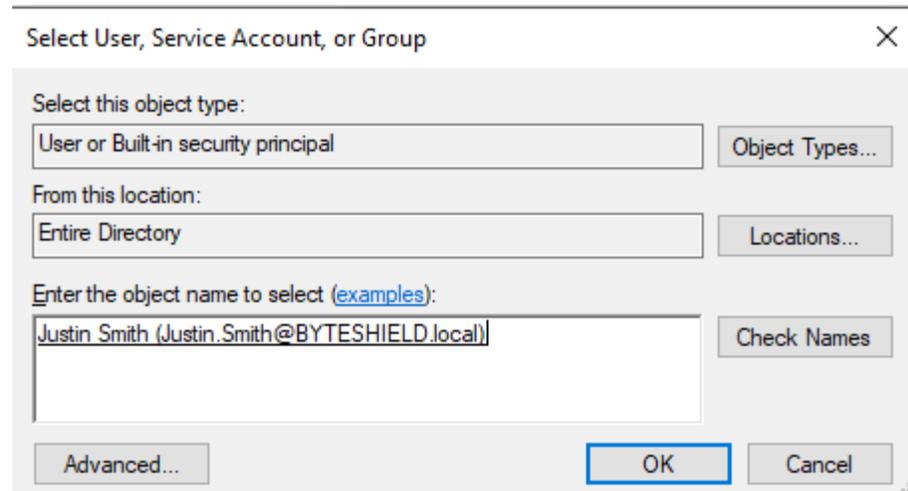
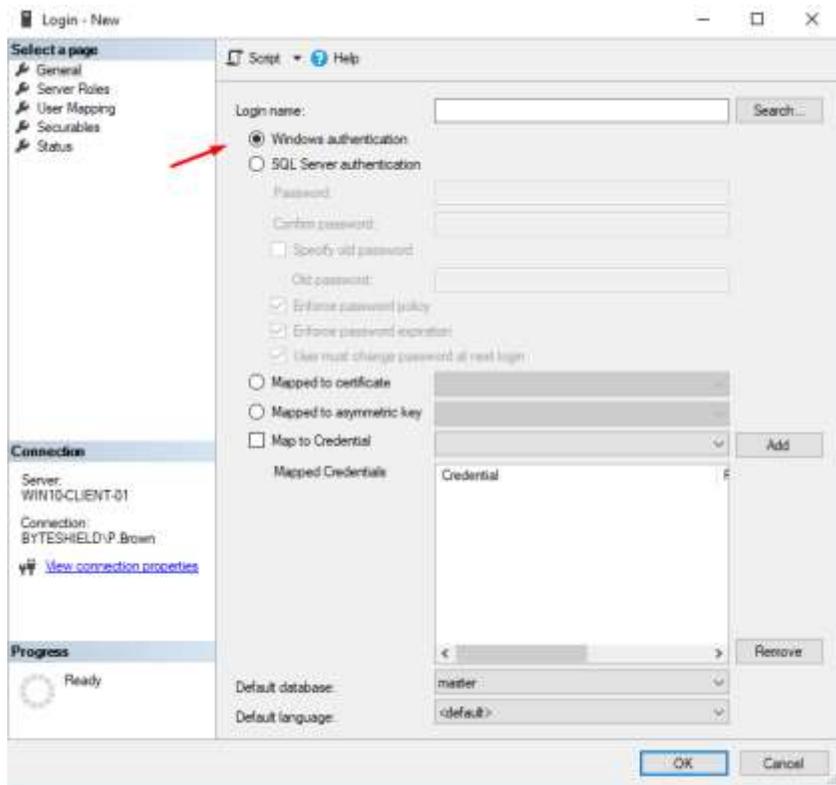


Lab Setup

Creating SQL User

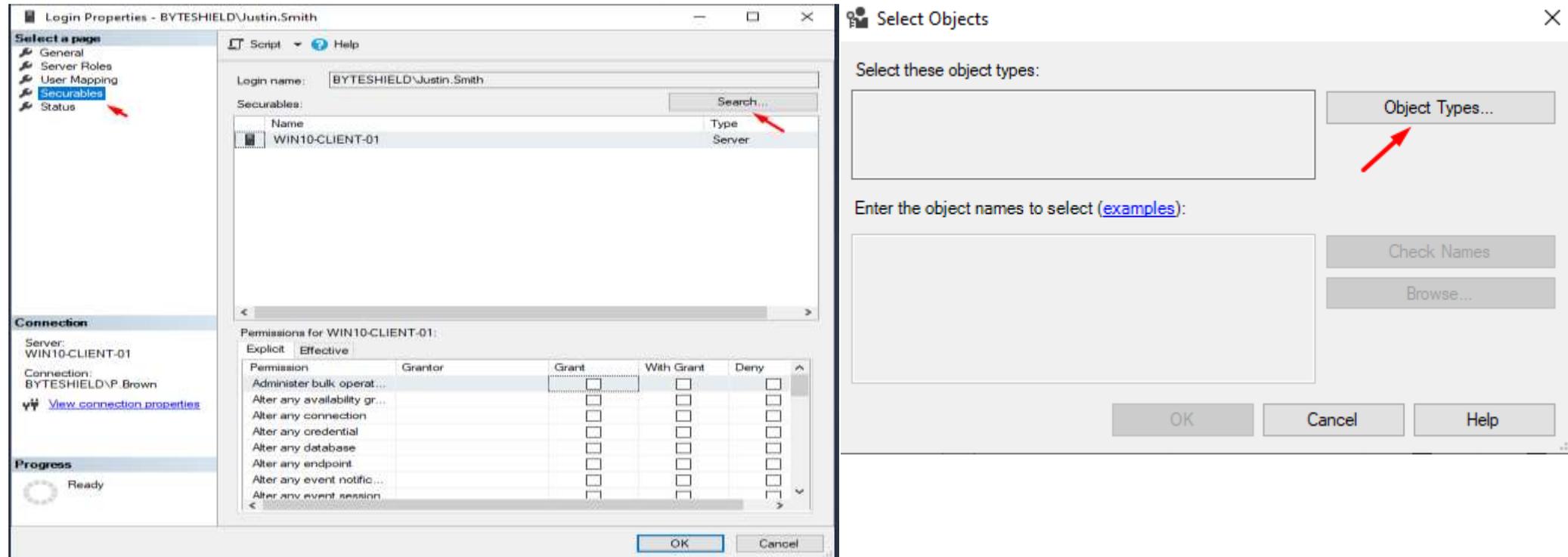


Lab Setup



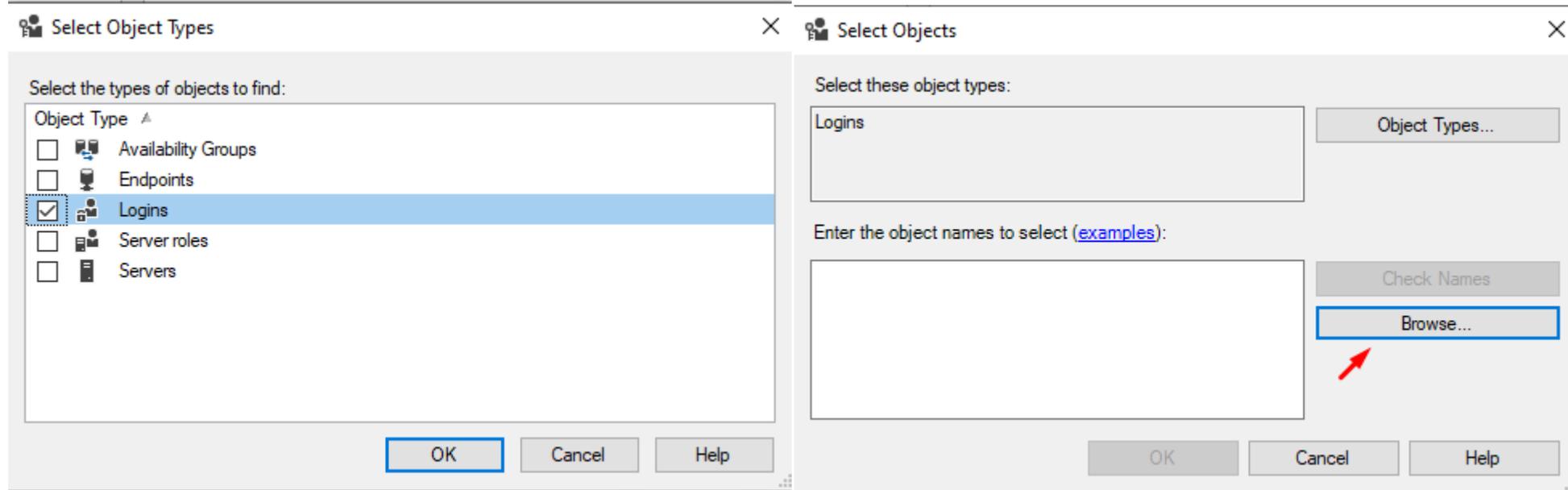
Lab Setup

We have made justin.smith as SQL server user with public role, we are going to make the user to impersonate the the systemadmin



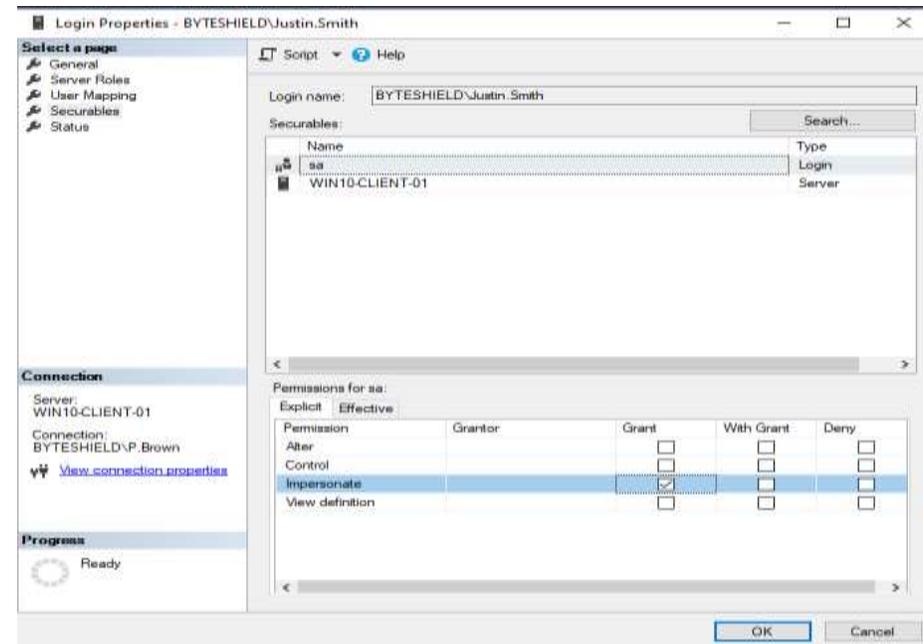
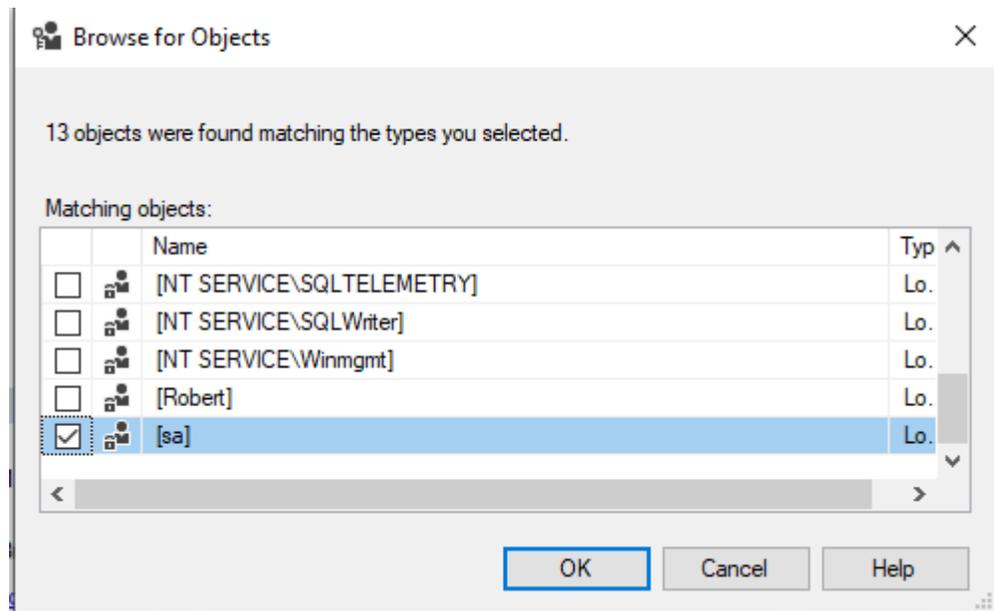
Lab Setup

Impersonating sa



Lab Setup

Impersonating sa



Lab Setup

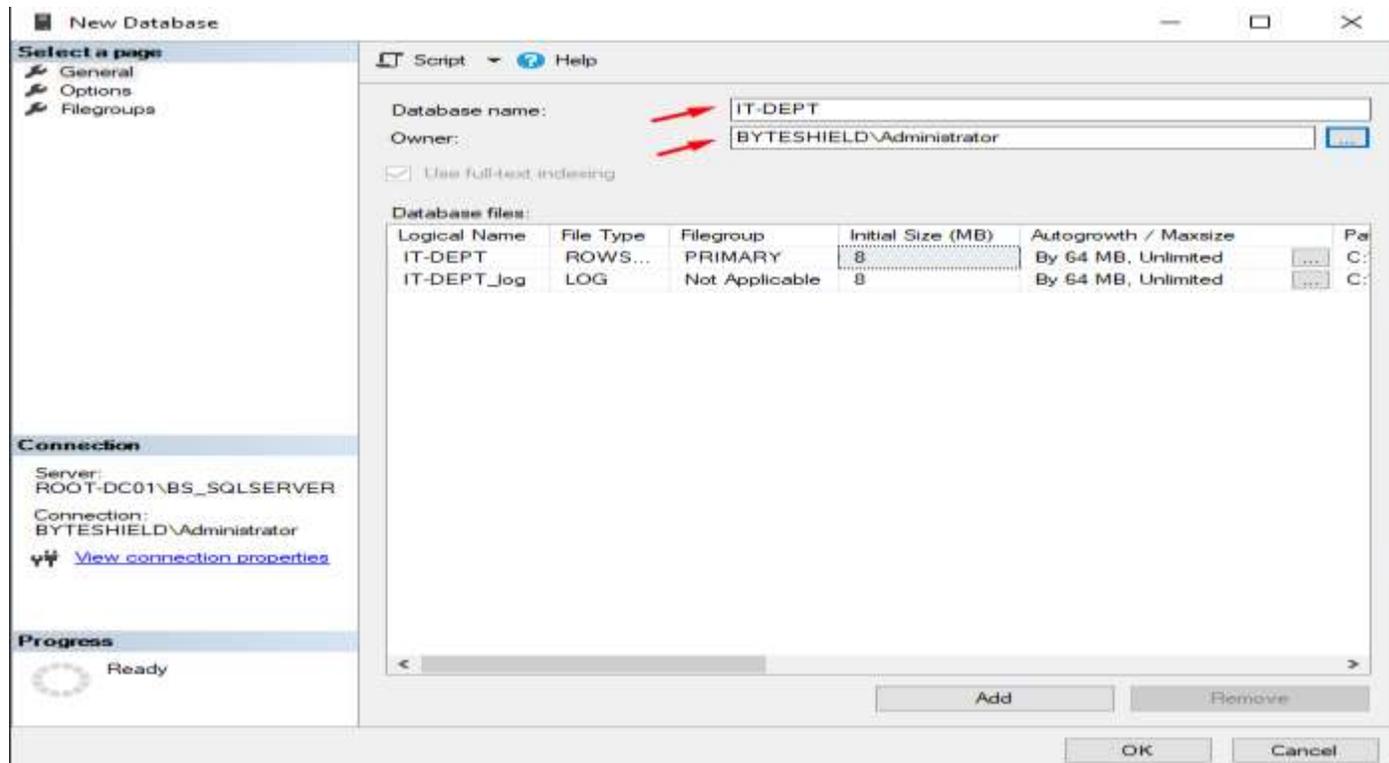
On ROOT-DC01 we are also going to Create 2 SQL users David and Kevin, David with have public role on database with Kevin will have db_owner role on the same database, we are going to make David to Impersonate Kevin

Creating the Database



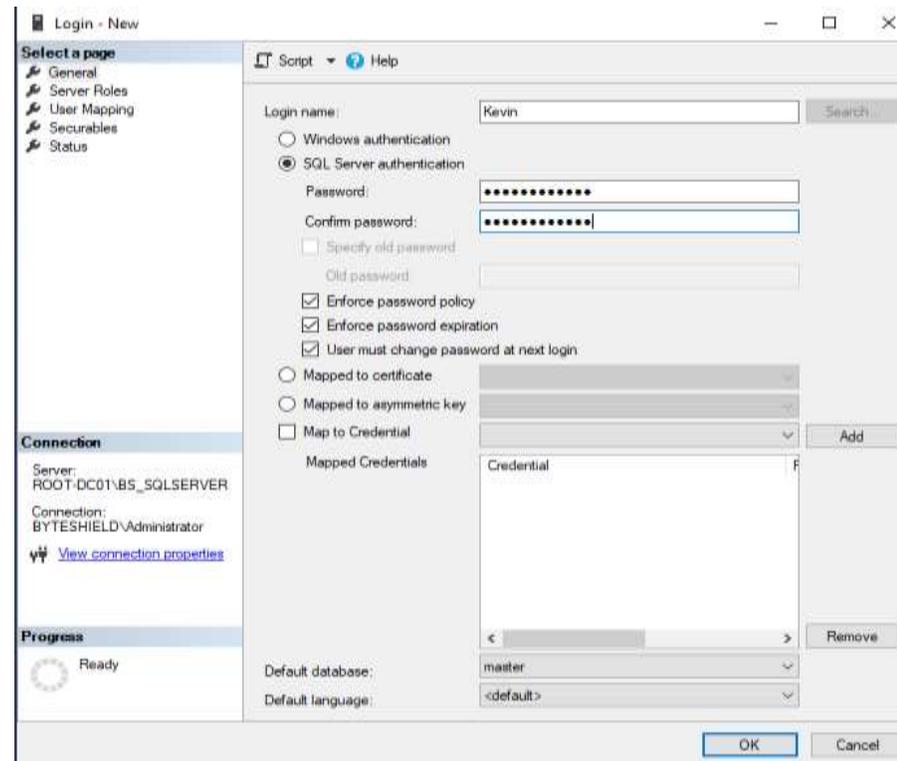
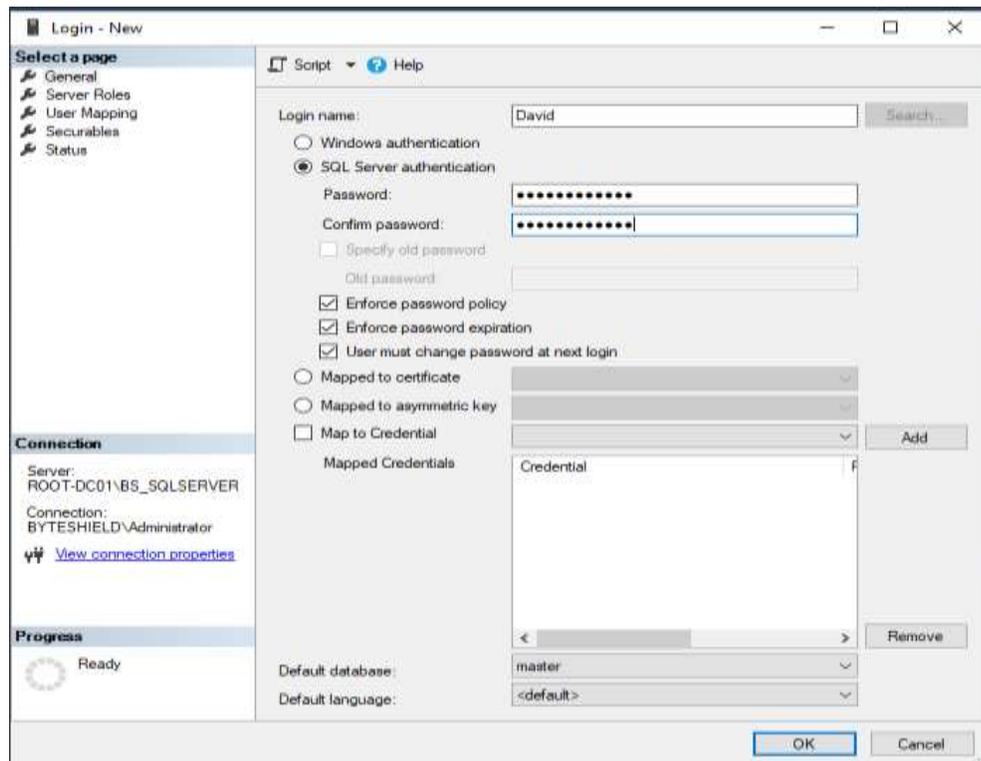
Lab Setup

Here we create the database owned by Administrator



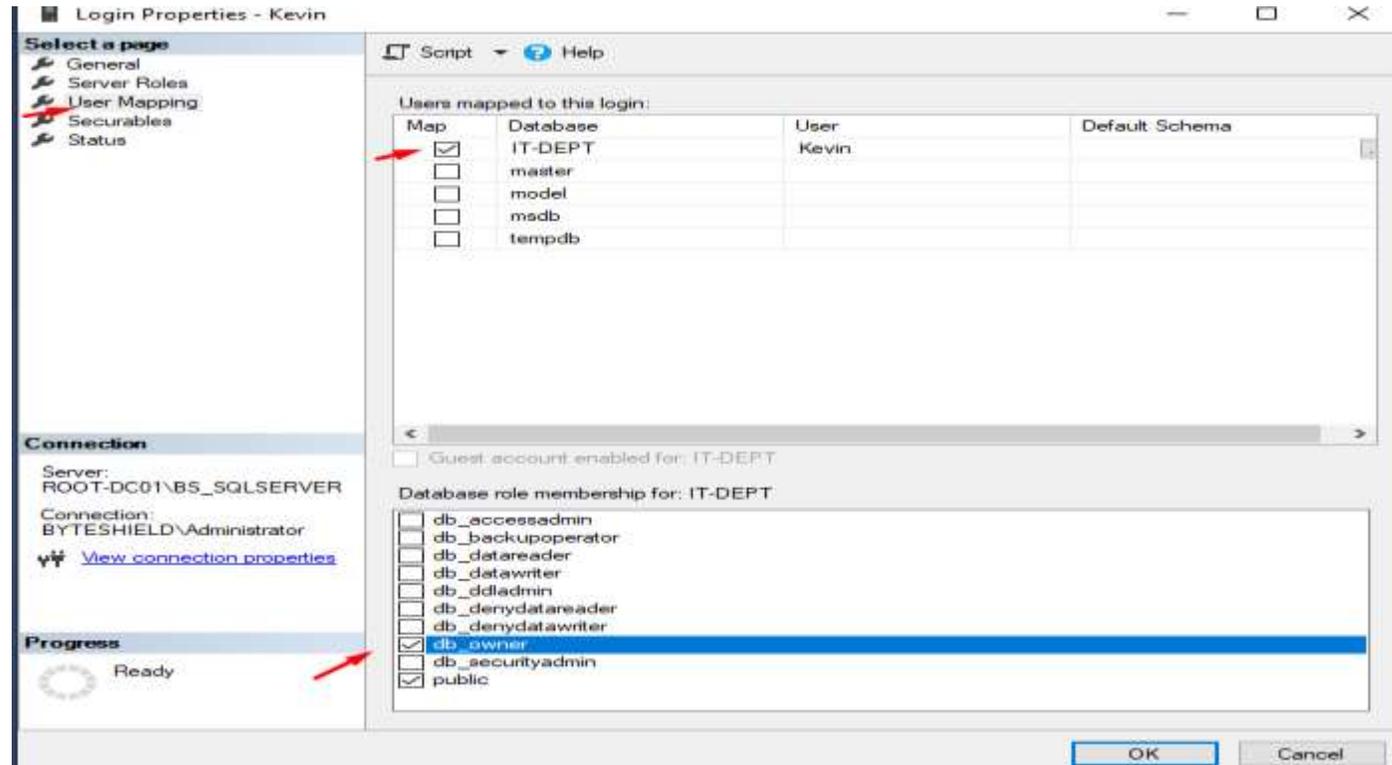
Lab Setup

Creating the users the same way Created for Win10-Client-01



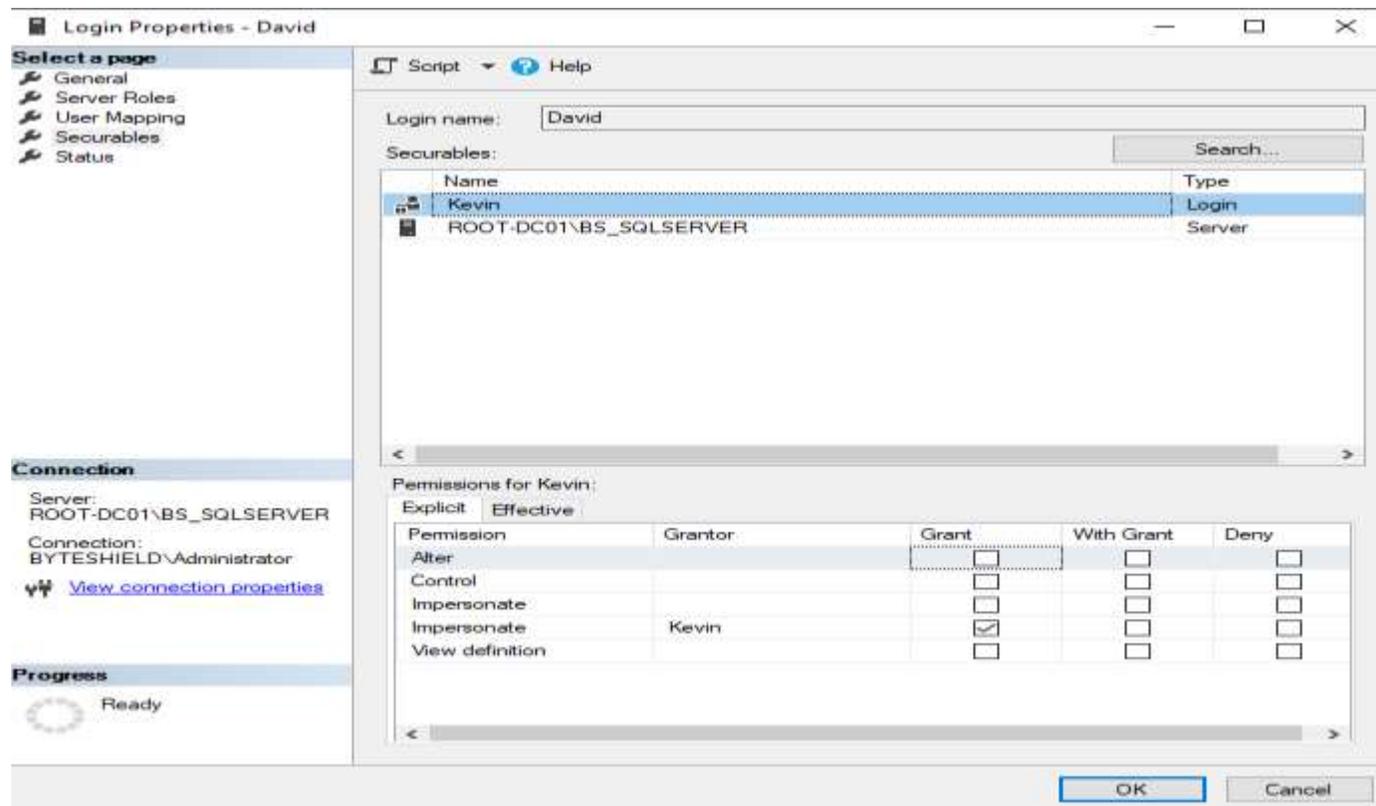
Lab Setup

Now Let's Give Kevin the db_owner role on the database we created, that give Kevin the ability to elevate his role sa, while David can impersonate Kevin



Lab Setup

Now we will let David Impersonate Kevin



Lab Setup

Creating SPN for SQL Server on ROOT-DC01

```
PS C:\Users\Administrator> setspn.exe -S "BS_SQLSERVER/ROOT-DC01.BYTESHIELD.local:1433" "BYTESHIELD\SqL_Service"  
Checking domain DC=BYTESHIELD,DC=local  
  
Registering ServicePrincipalNames for CN=Sql_Service,CN=Users,DC=BYTESHIELD,DC=local  
    BS_SQLSERVER/ROOT-DC01.BYTESHIELD.local:1433  
Updated object
```

```
CN=Sql_Service,CN=Users,DC=BYTESHIELD,DC=local  
    BS_SQLSERVER/ROOT-DC01.BYTESHIELD.local:1433  
CN=WIN10-CLIENT-02,CN=Computers,DC=BYTESHIELD,DC=local  
    RestrictedKrbHost/WIN10-CLIENT-02  
    HOST/WIN10-CLIENT-02  
    RestrictedKrbHost/Win10-Client-02.BYTESHIELD.local  
    HOST/Win10-Client-02.BYTESHIELD.local  
CN=WIN10-CLIENT-01,CN=Computers,DC=BYTESHIELD,DC=local  
    MSSQLSvc/Win10-Client-01.BYTESHIELD.local:1433  
    MSSQLSvc/Win10-Client-01.BYTESHIELD.local  
    RestrictedKrbHost/WIN10-CLIENT-01  
    HOST/WIN10-CLIENT-01  
    RestrictedKrbHost/Win10-Client-01.BYTESHIELD.local  
    HOST/Win10-Client-01.BYTESHIELD.local  
CN=WS01,CN=Computers,DC=BYTESHIELD,DC=local  
    TERMSRV/WS01  
    TERMSRV/WS01.BYTESHIELD.local  
    WSMAN/WS01  
    WSMAN/WS01.BYTESHIELD.local  
    RestrictedKrbHost/WS01  
    HOST/WS01  
    RestrictedKrbHost/WS01.BYTESHIELD.local  
    HOST/WS01.BYTESHIELD.local
```

```
Existing SPN found!
```

Lab Setup

On TRUSTED-DC03 Let's give justin.smith Sysadmin role for cross forest authentication on the SQL server



Lab Setup

Sql Cross forest Authentication

Select User, Service Account, or Group

Select this object type:
User or Built-in security principal

From this location:
BYTESHIELD.local

Enter the object name to select (examples):
Justin Smith (Justin.Smith@BYTESHIELD.local)

Advanced... OK Cancel

Login - New

Select a page
General
Server Roles
User Mapping
Securables
Status

Script Help

Login name: BYTESHIELD\Justin.Smith

Windows authentication
 SQL Server authentication

Password:
Confirm password:

Specify old password
Old password:

Enforce password policy
 Enforce password expiration
 User must change password at next login

Mapped to certificate
 Mapped to asymmetric key

Map to Credential

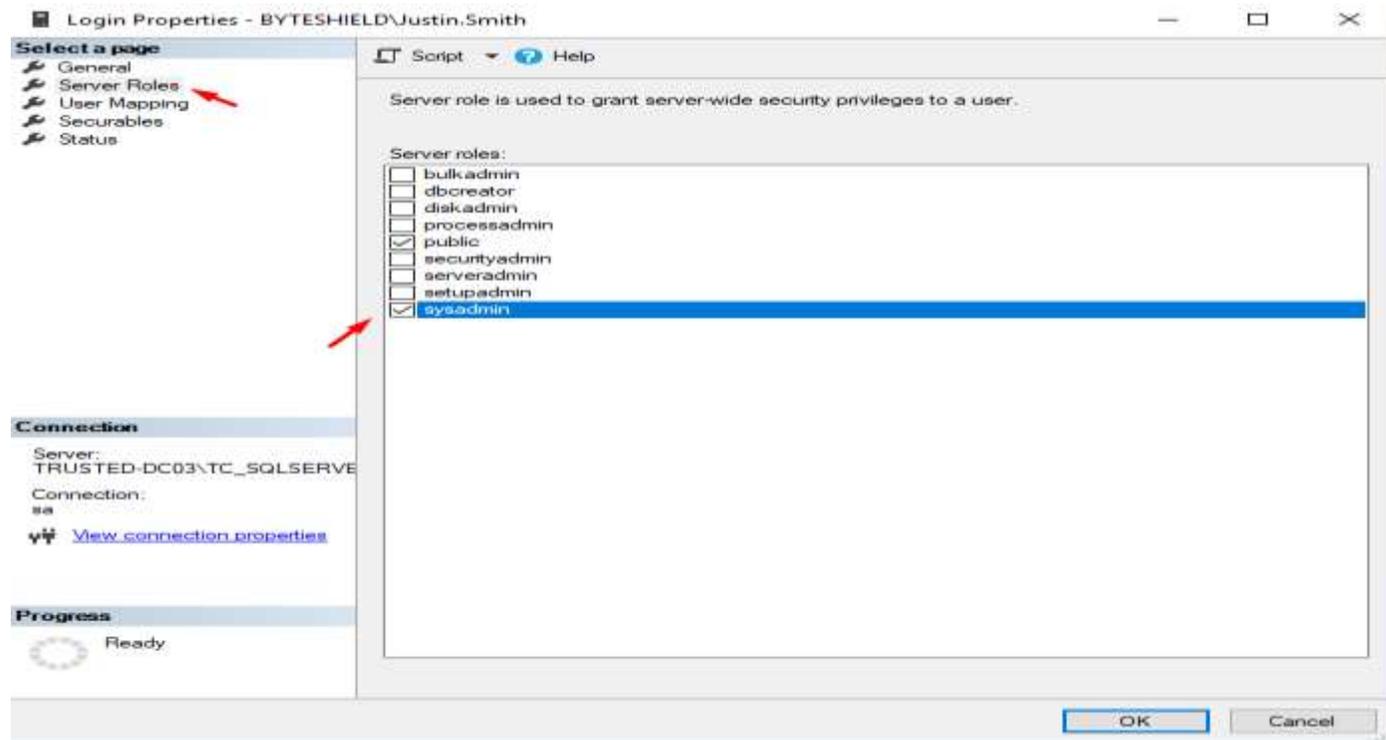
Mapped Credentials

Default database: master
Default language: <default>

OK Cancel

Lab Setup

Giving Justin.smith sysadmin on the Server



Lab Setup

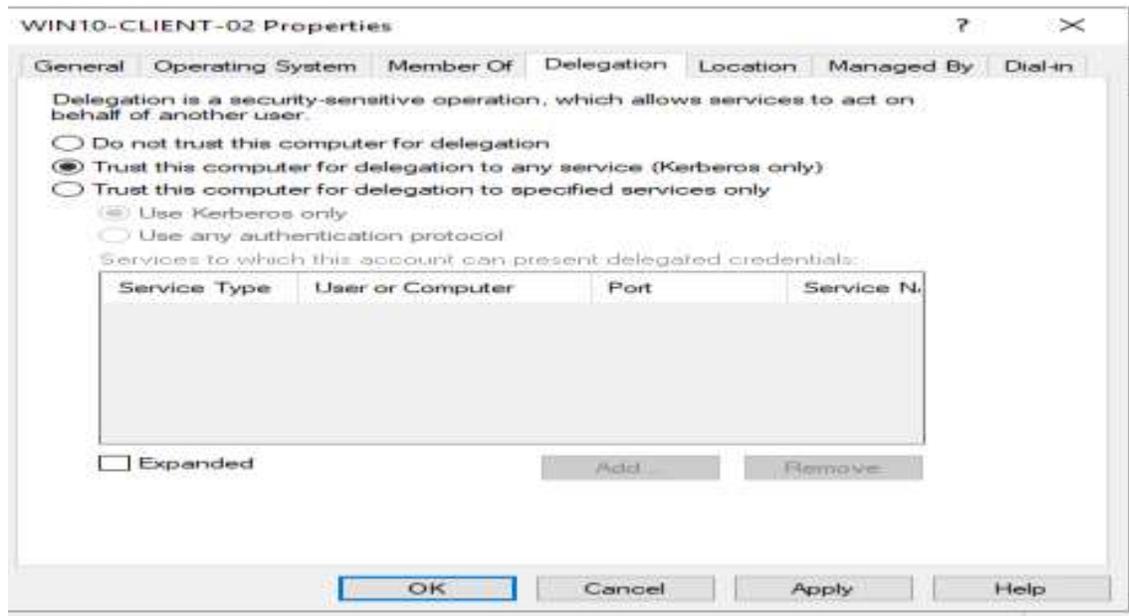
Creating SPN for SQL Server on TRUSTED-DC03

```
PS C:\Users\Administrator> setspn.exe -S "TC_SQLSERVER/TRUSTED-DC03.TRUSTEDCORP.local:1433" "TRUSTEDCORP\TCSql_Service"  
Checking domain DC=TRUSTEDCORP,DC=local  
  
Registering ServicePrincipalNames for CN=TCSql_Service,CN=Users,DC=TRUSTEDCORP,DC=local  
    TC_SQLSERVER/TRUSTED-DC03.TRUSTEDCORP.local:1433  
Updated object
```

```
CN=TCSql_Service,CN=Users,DC=TRUSTEDCORP,DC=local  
    TC_SQLSERVER/TRUSTED-DC03.TRUSTEDCORP.local:1433  
CN=WS01,CN=Computers,DC=TRUSTEDCORP,DC=local  
    TERMSRV/WS01  
    TERMSRV/WS01.TRUSTEDCORP.local  
    WSMAN/WS01  
    WSMAN/WS01.TRUSTEDCORP.local  
    RestrictedKrbHost/WS01  
    HOST/WS01  
    RestrictedKrbHost/WS01.TRUSTEDCORP.local  
    HOST/WS01.TRUSTEDCORP.local
```

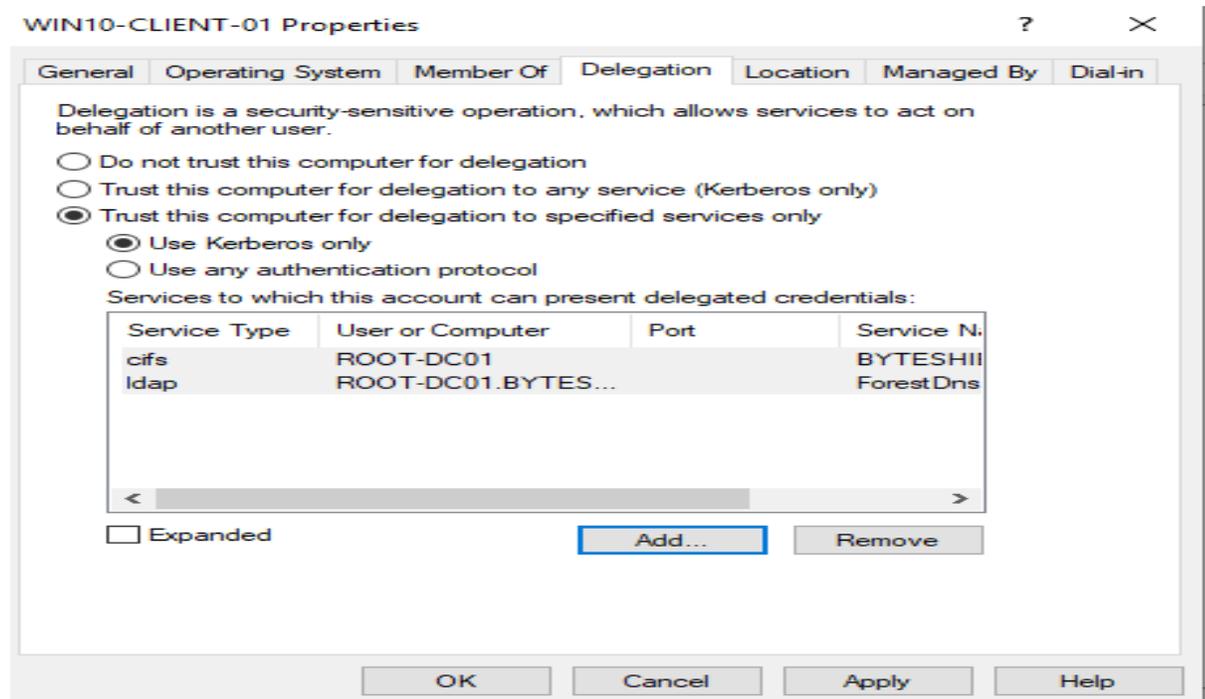
Lab Setup

Unconstrained Delegation Setup, we are going to use Win10-Client-02 for unconstrained delegation and also make it a member of domain admins group because it is going to be admin Workstation



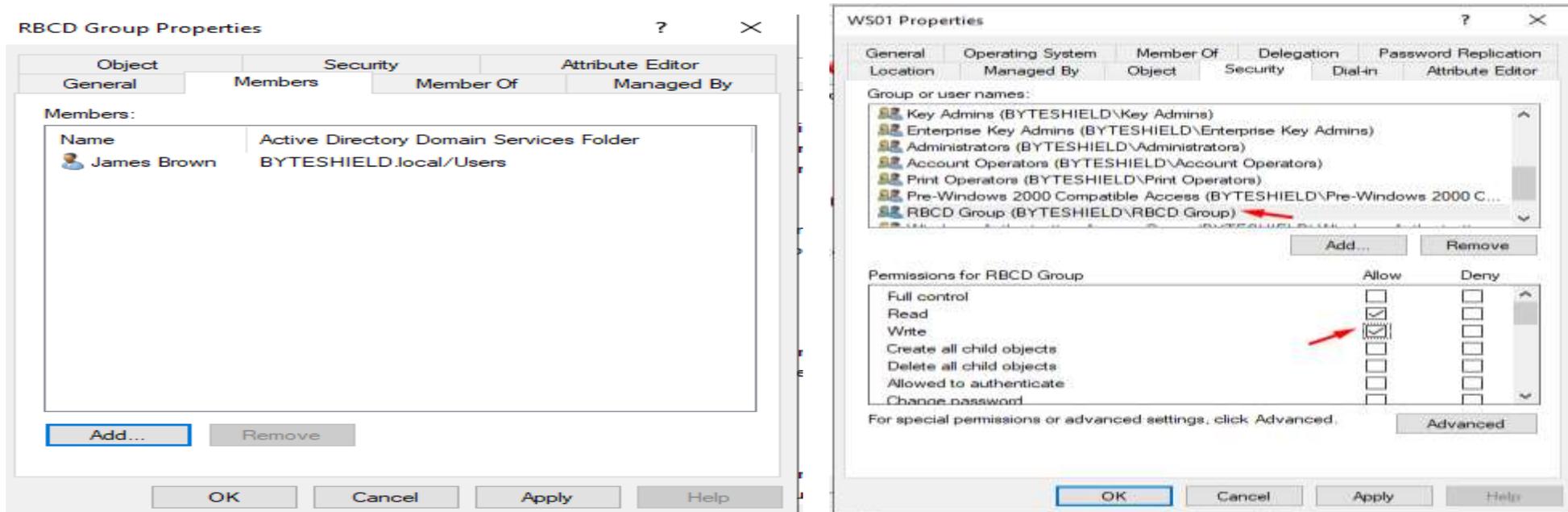
Lab Setup

Constrained Delegation Setup, we are going to use Win10-Client-01 for constrained delegation



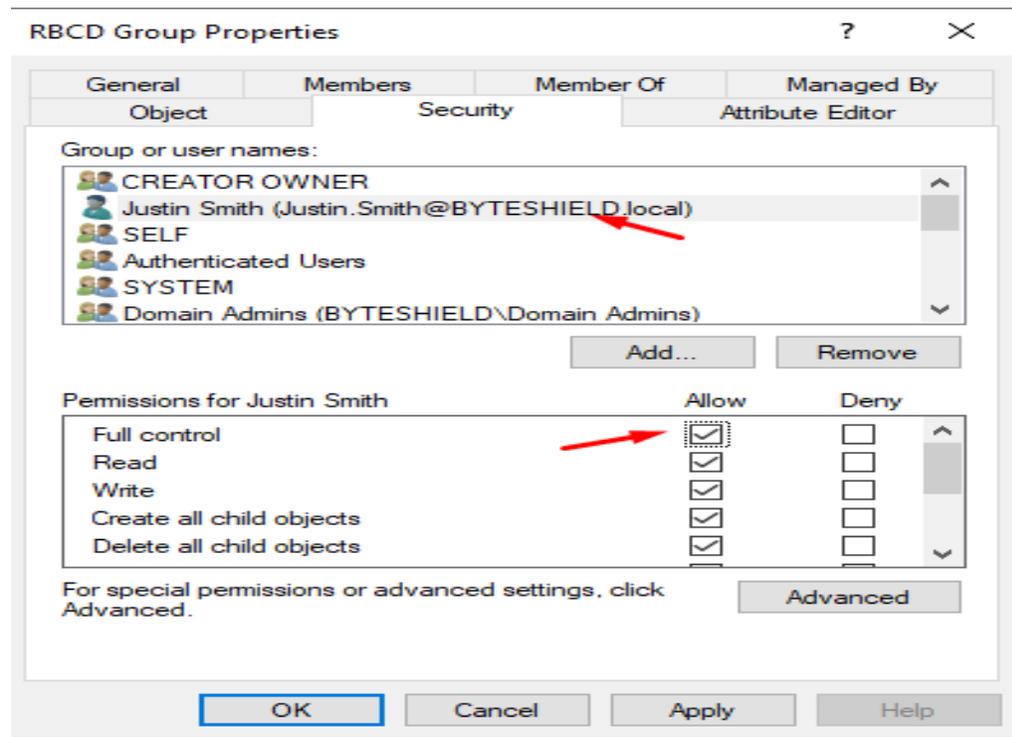
Lab Setup

Resource-based constrained delegation RBDC setup, we are going to create a group and name it RBDC group, this group will have write permission over WS01 and justin.smith with have full permission over the group, that will give our user ability to add himself to the group, james.brown is a member to the group



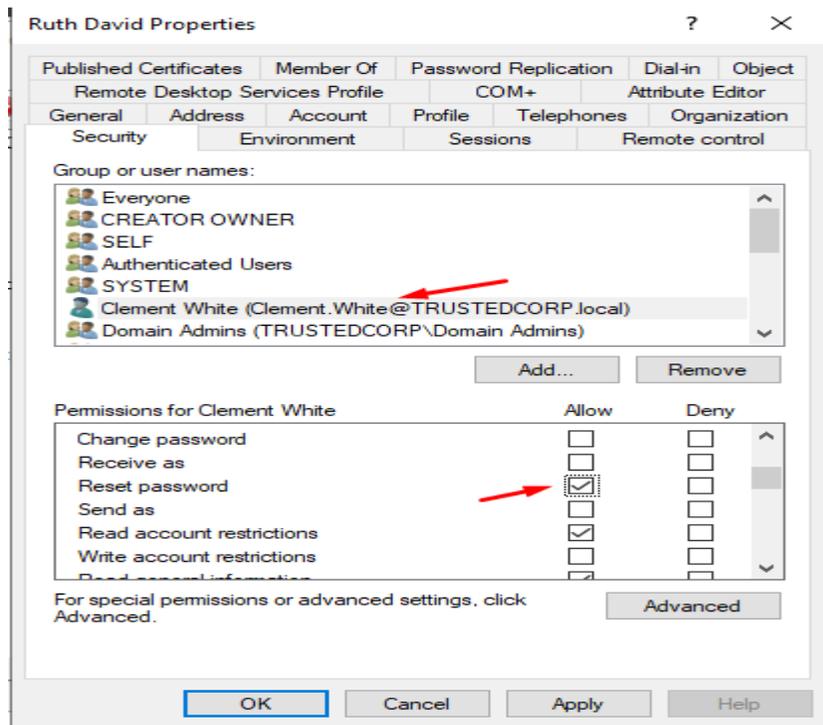
Lab Setup

Now Our user has full control over the Group, the user can add himself to the group



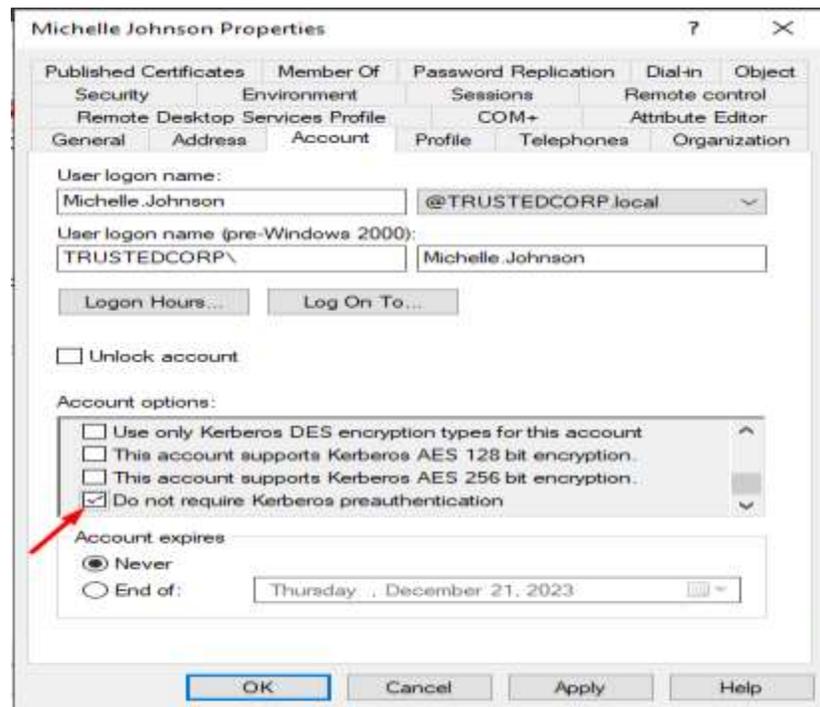
Lab Setup

On TRUSTED-DC03 we going to make Clement to have ExtendedRight over Ruth.David



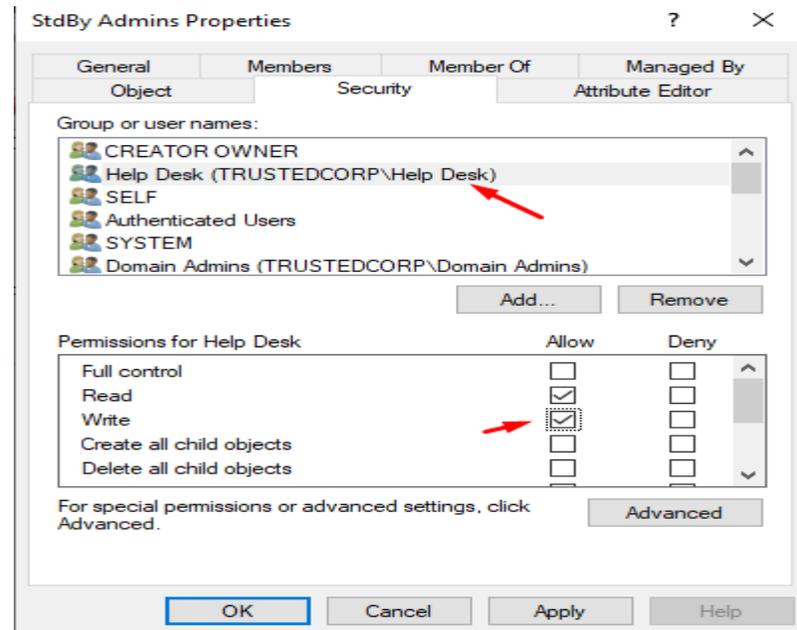
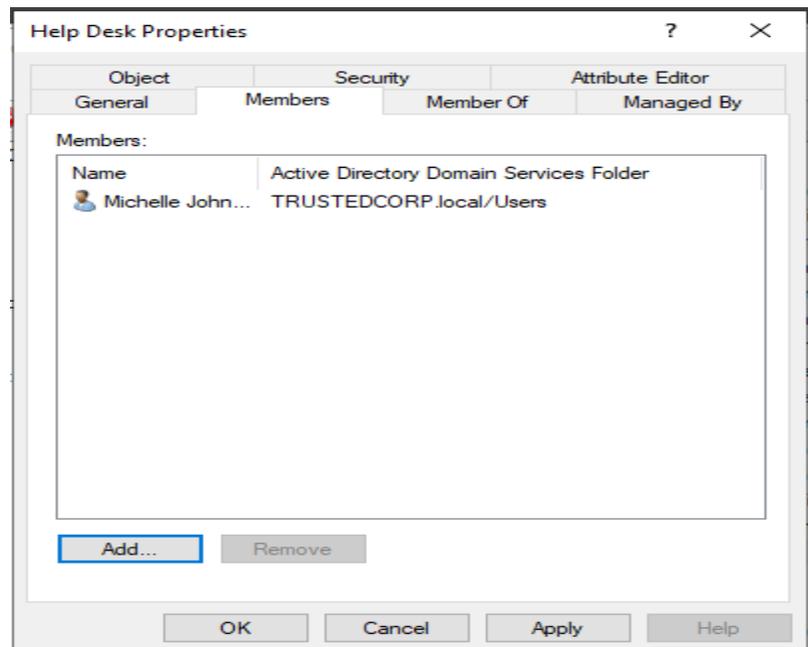
Lab Setup

While Michelle.Johnson will have Don not Require Kerberos preauthentication selected



Lab Setup

Michelle.johnson is a member of help desk user group while help desk user group has write privilege over StdBy Admins



Lab Setup

BYTESHIELD Domain User James Brown should be a member of Backup Operators of TRUSTEDCORP

