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 Metesploitable3 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

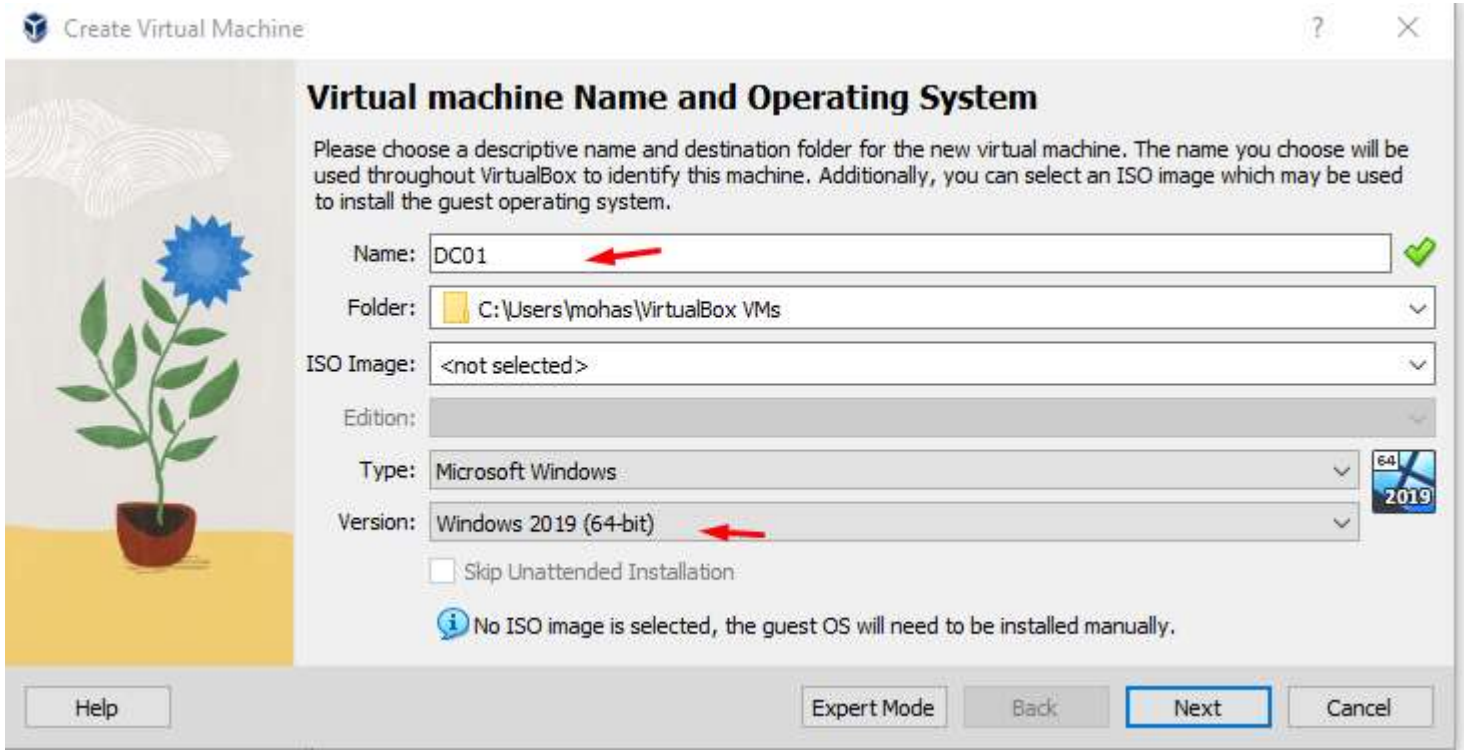
4 MicroSoft SQL Server Express edition from Microsoft Website
https://www.microsoft.com/en-us/download/details.aspx?id=55994

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

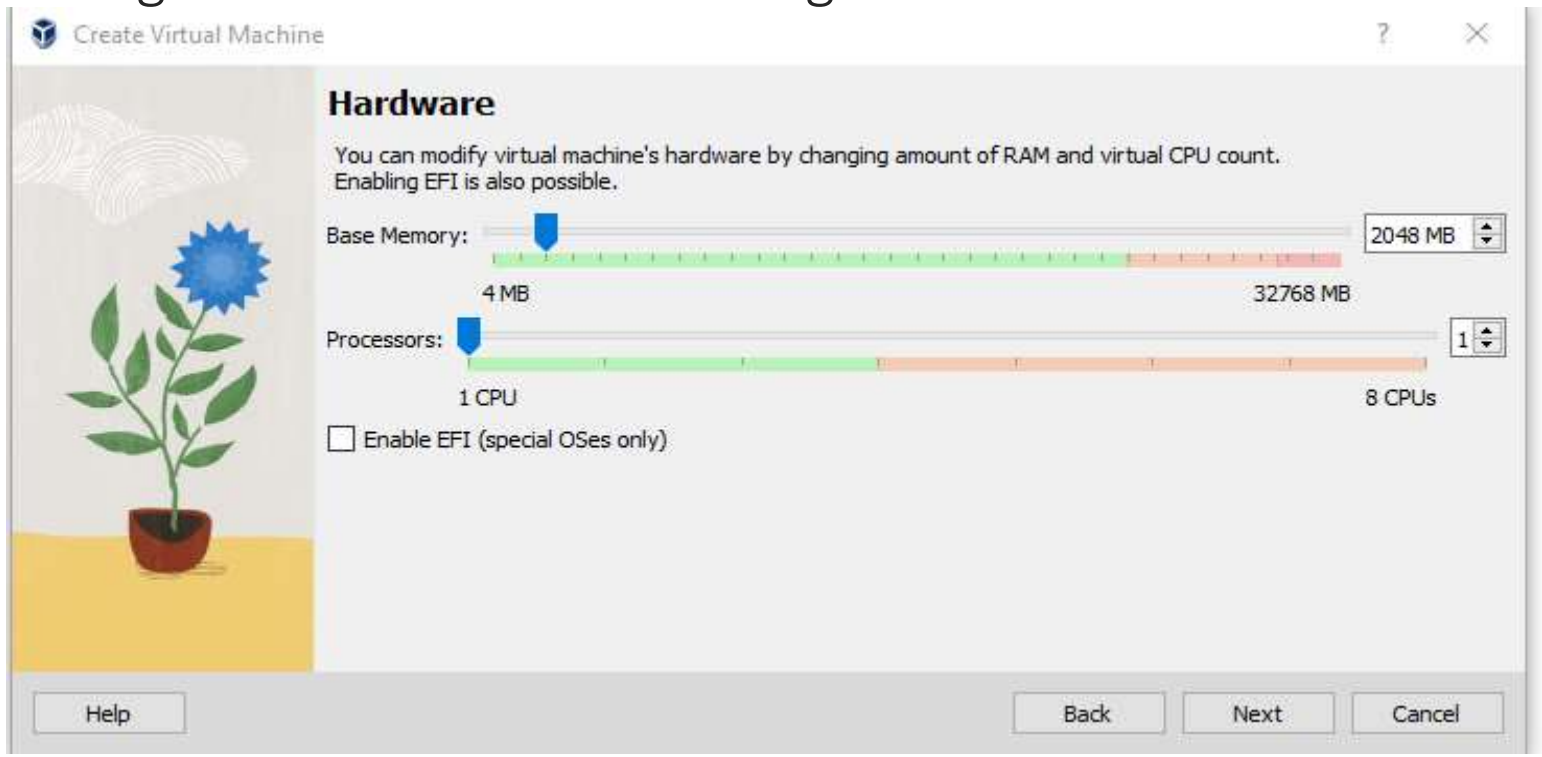
Lab Setup

Installing Windows Server 2019

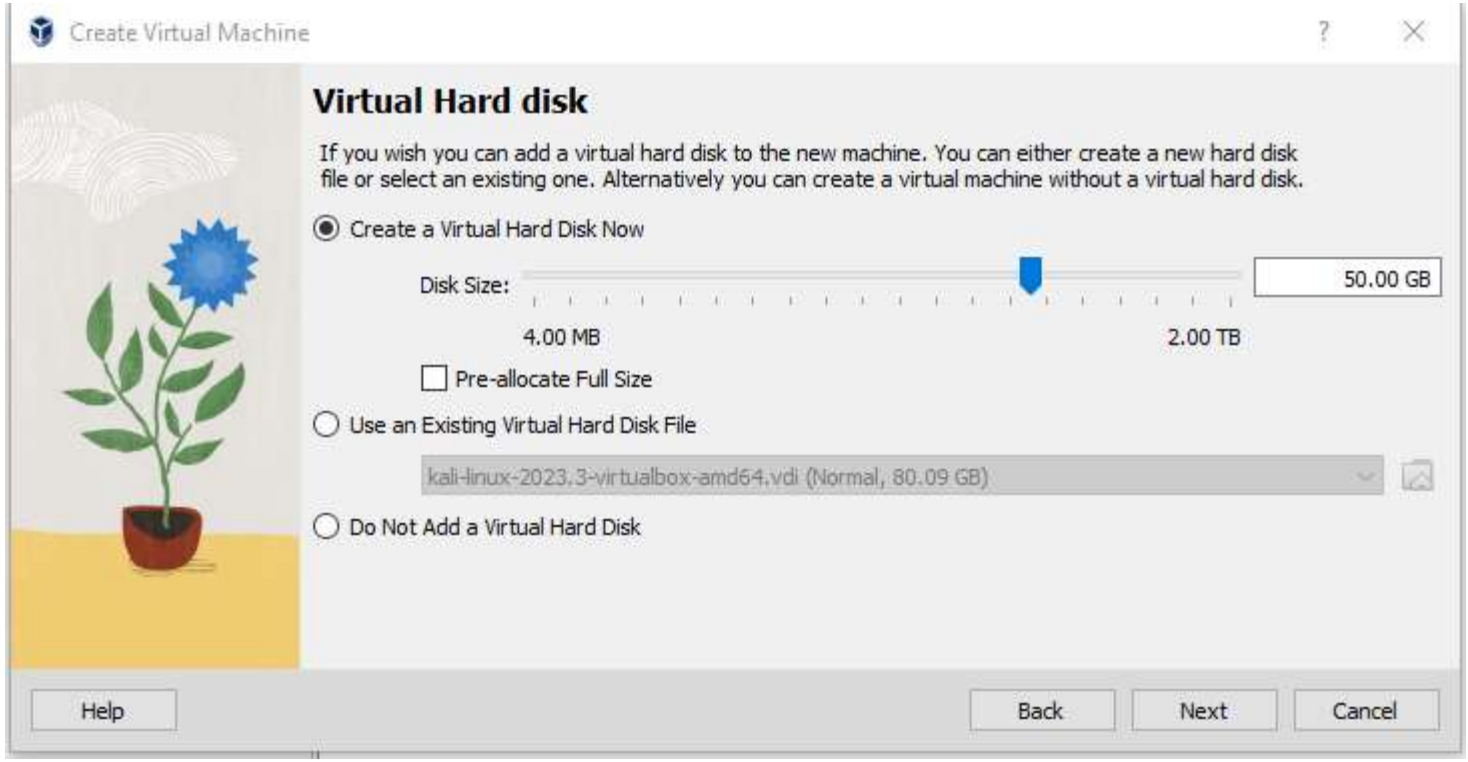


Lab Setup

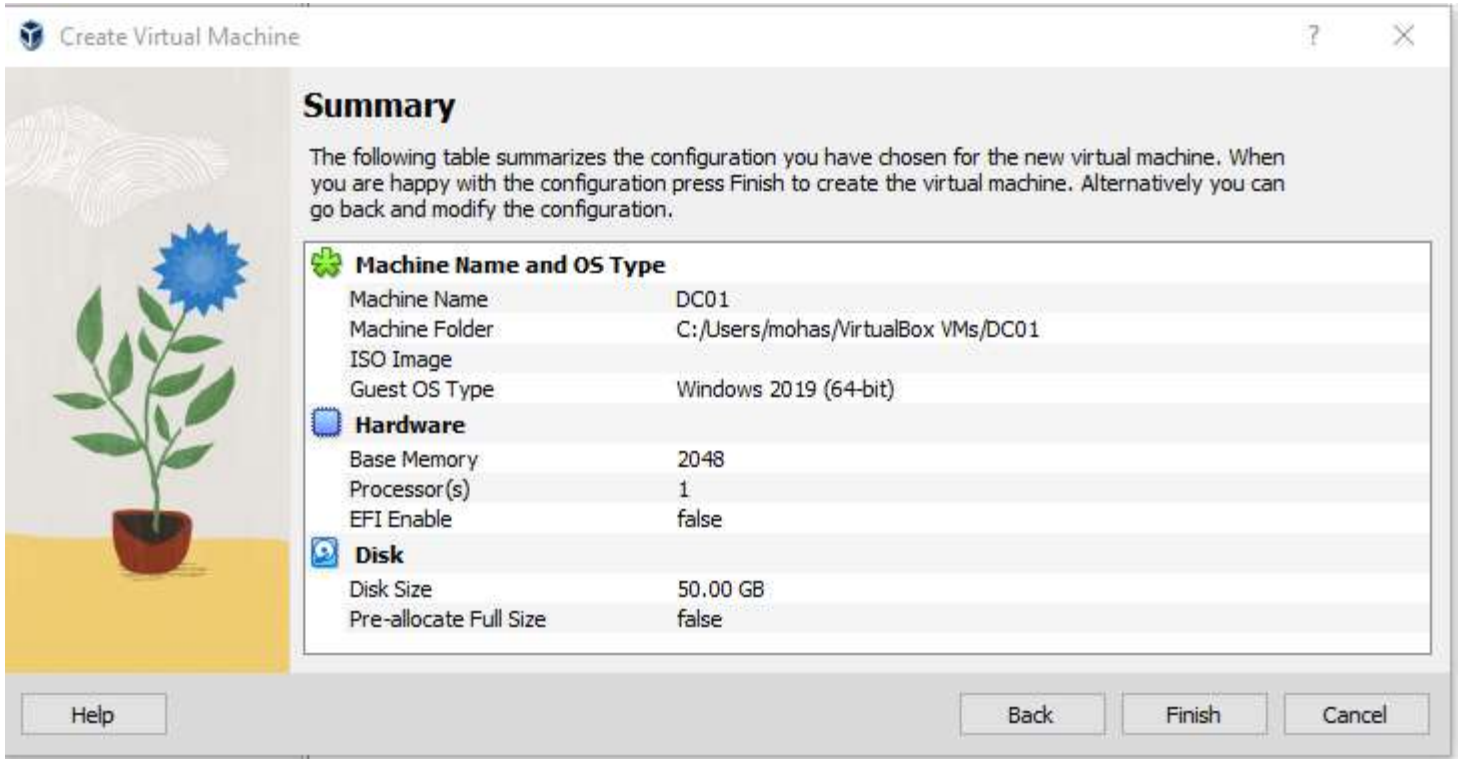
Let’s go with the Default Setting



Lab Setup

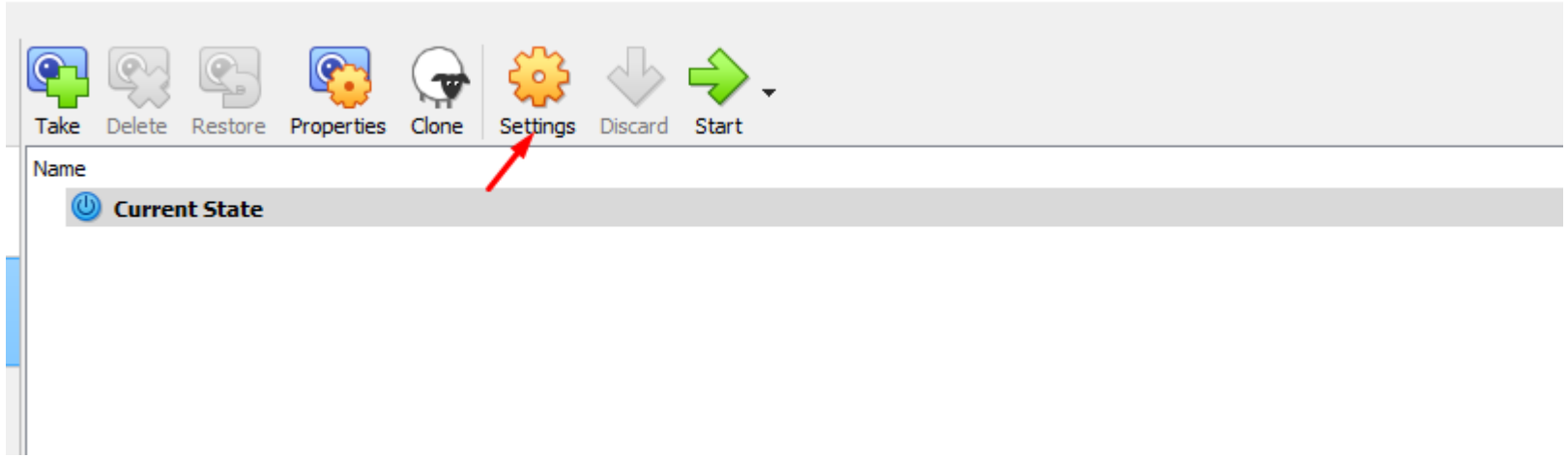

Create Virtual Machine
Virtual Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.
Create a Virtual Hard Disk Now
Disk Size:
50.00 GB
4.00 MB
2.00 TB
Pre-allocate Full Size
Use an Existing Virtual Hard Disk File
kali-linux-2023.3-virtualbox-amd64.vdi (Normal, 80.09 GB)
Do Not Add a Virtual Hard Disk
Help
Back
Next
Cancel

Lab Setup


Create Virtual Machine
Summary
The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.
Machine Name and OS Type
Machine Name DC01
Machine Folder C:/Users/mohas/VirtualBox VMs/DC01
ISO Image
Guest OS Type Windows 2019 (64-bit)
Hardware
Base Memory 2048
Processor(s) 1
EFI Enable false
Disk
Disk Size 50.00 GB
Pre-allocate Full Size false
Help
Back
Finish
Cancel

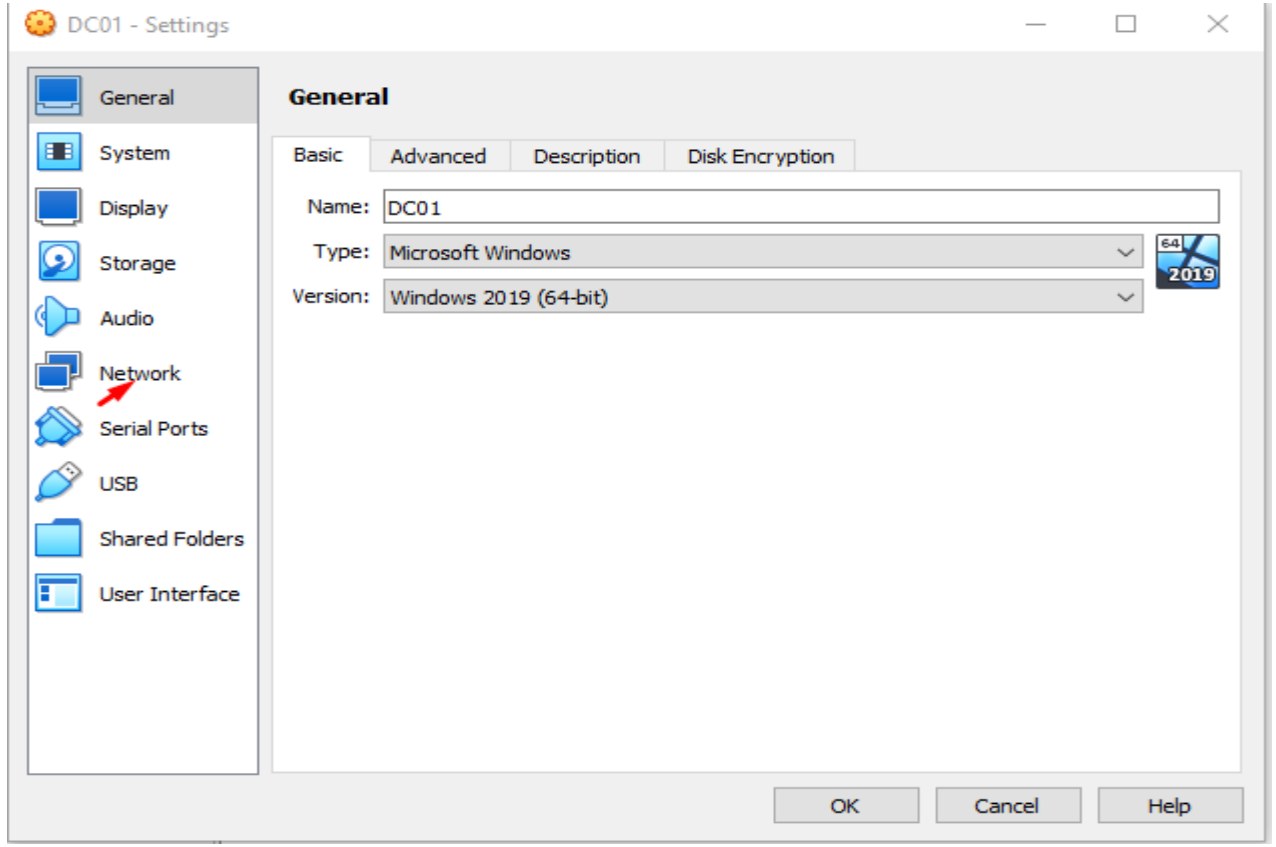
Lab Setup

Let’s Change Some Settings



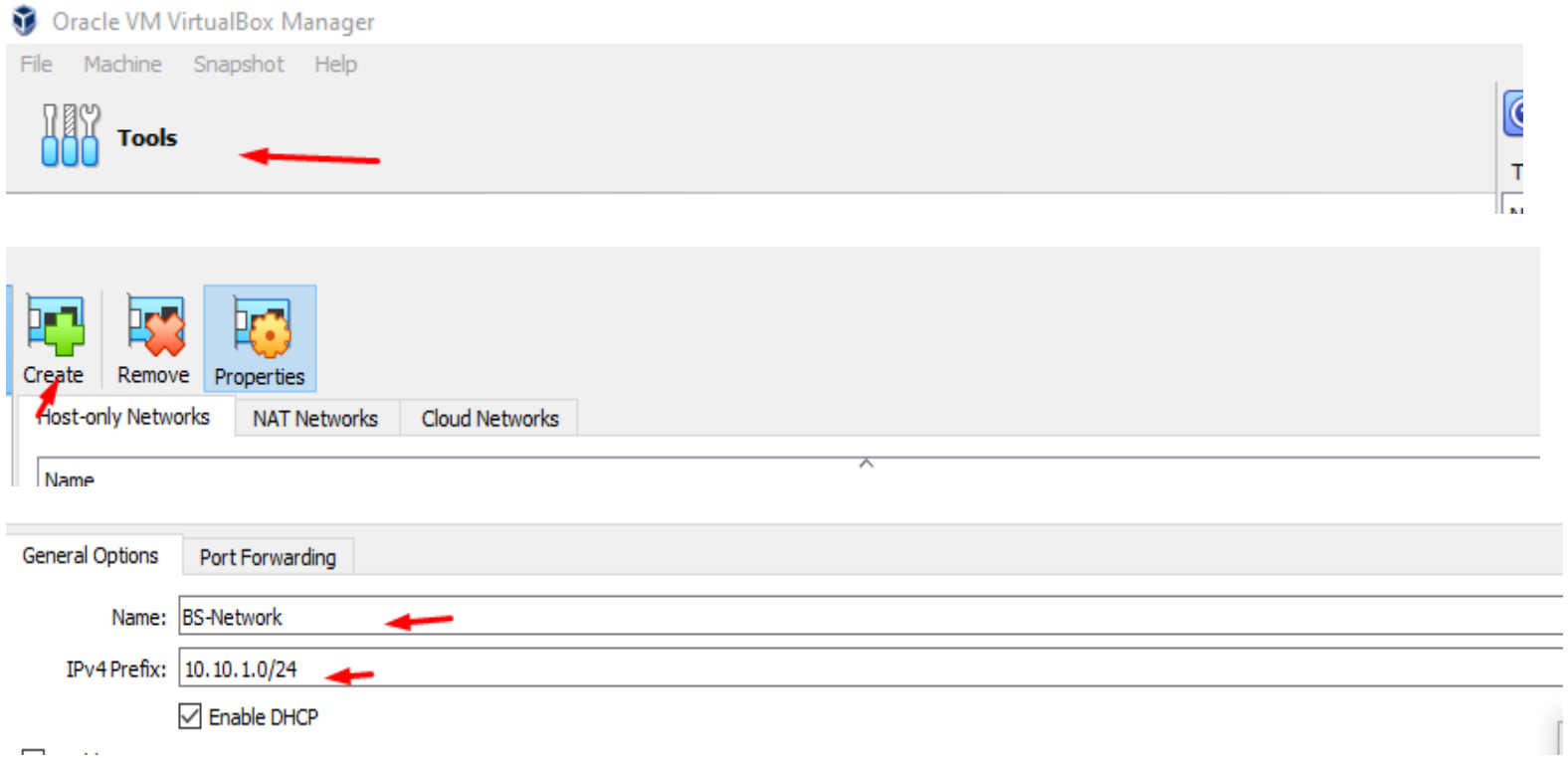
Lab Setup

Network Adapter Settings

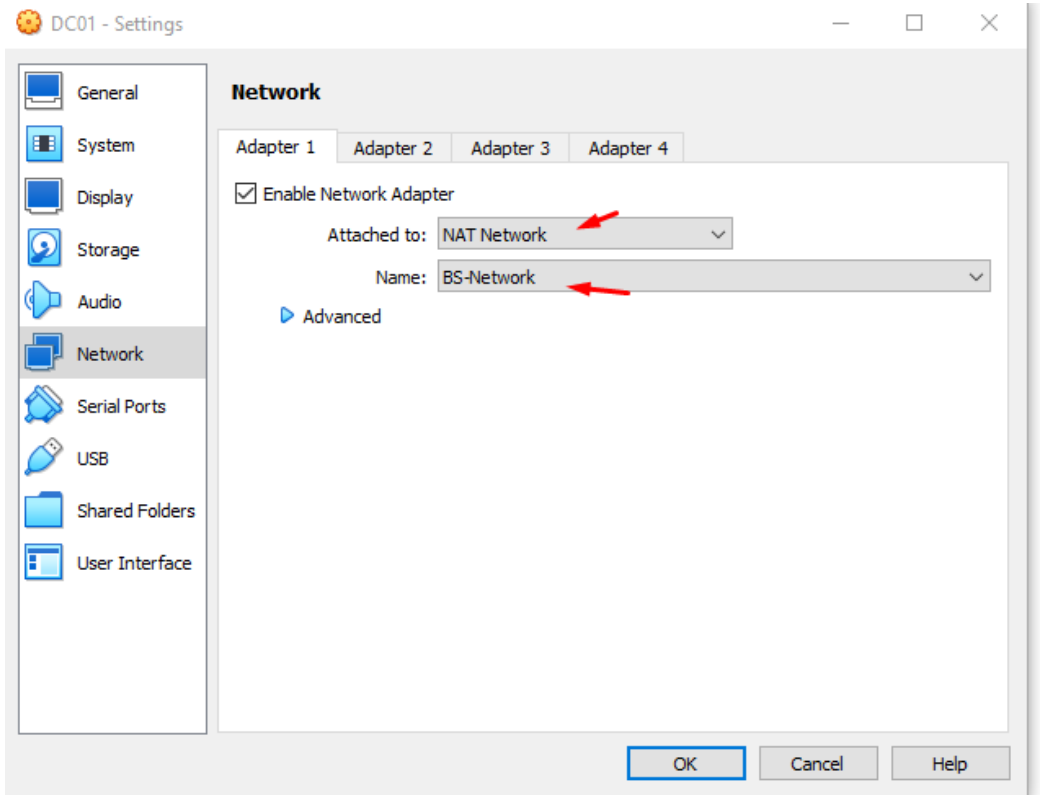


Lab Setup

Creating New Nat Network

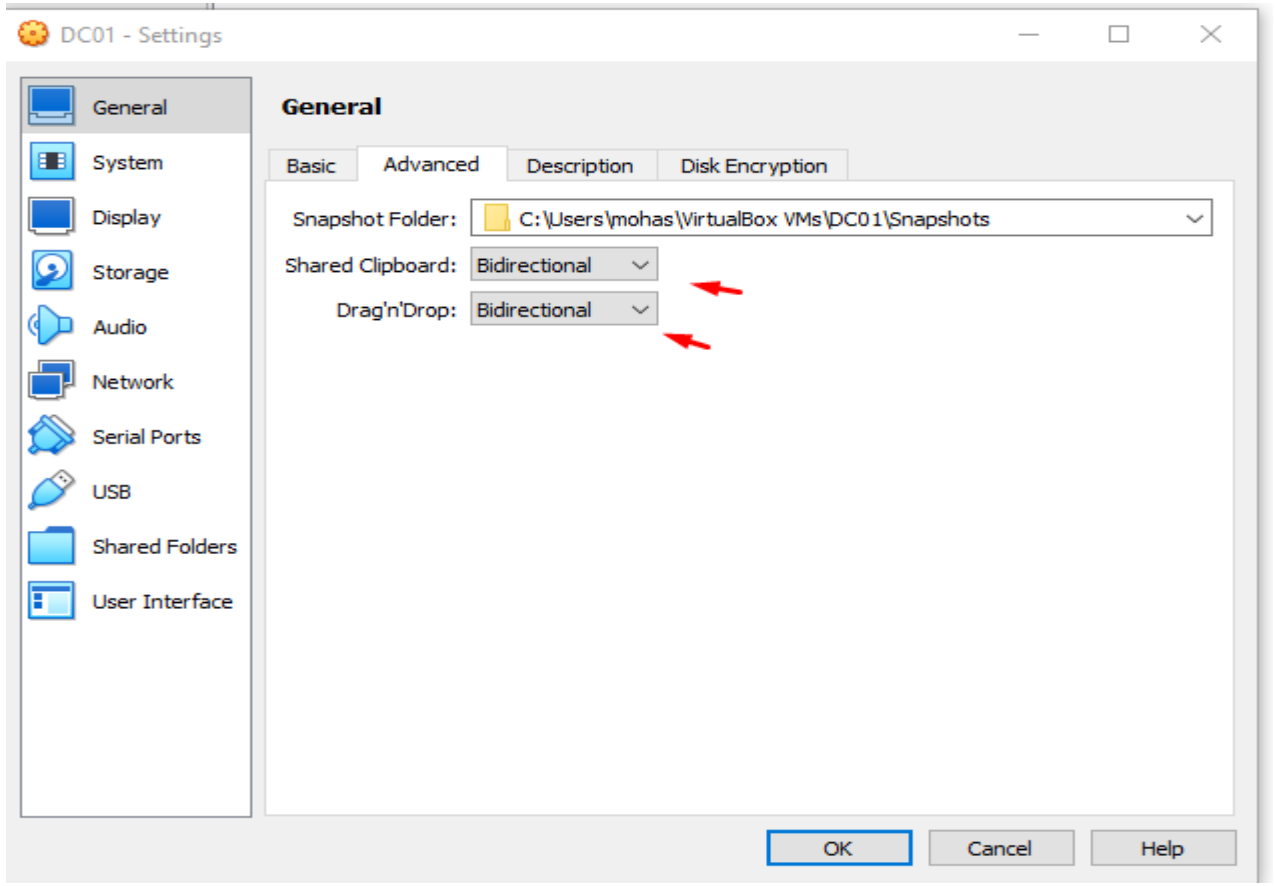


Lab Setup


DC01 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT Network
Name:
BS-Network
Advanced
OK
Cancel
Help

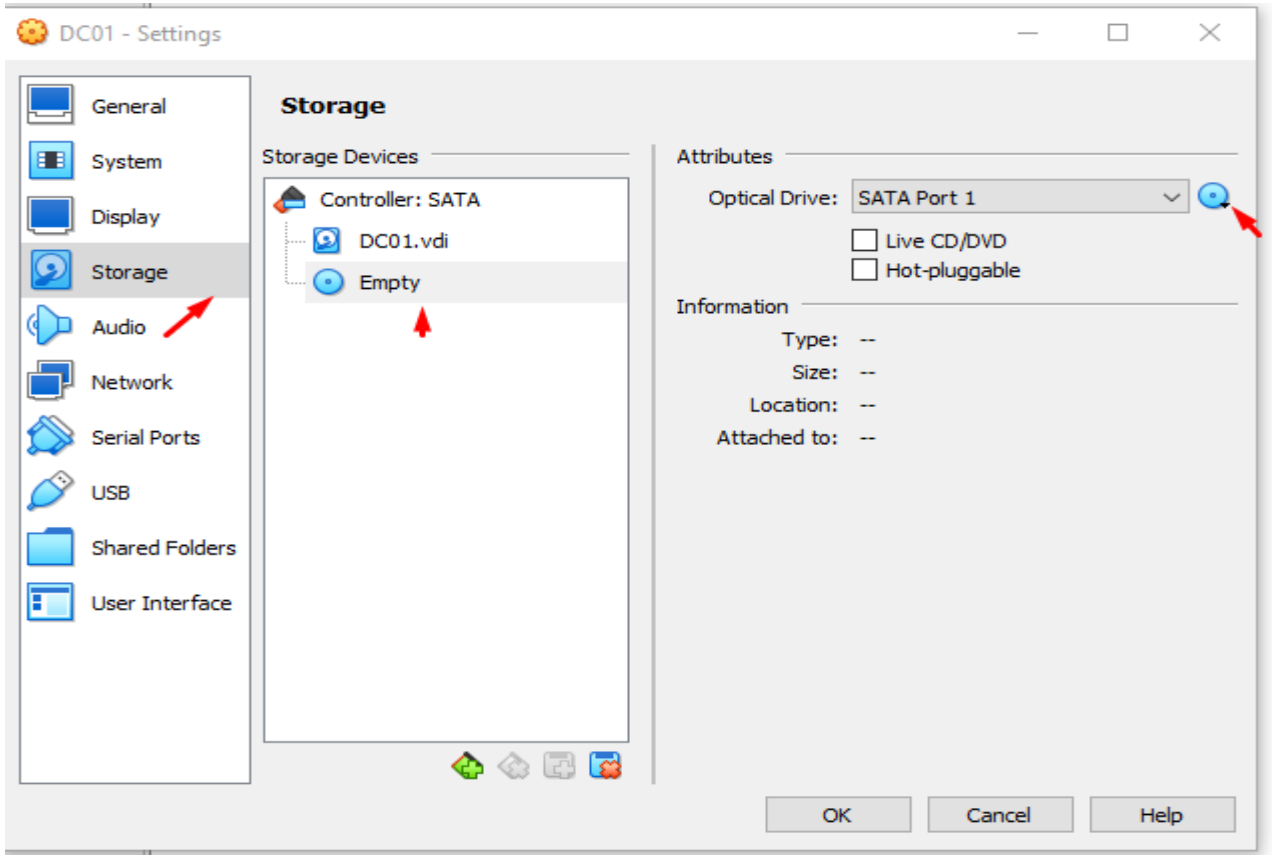
Lab Setup

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



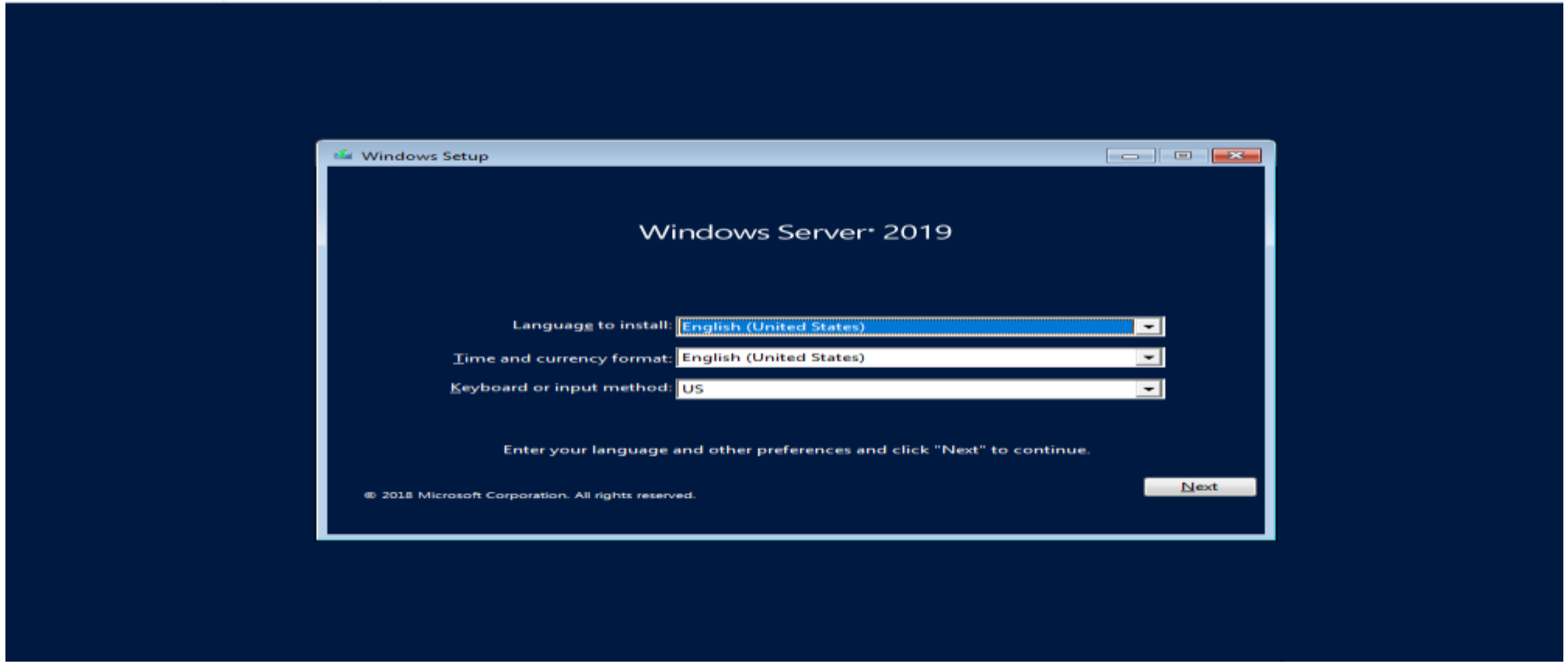
Lab Setup

Installing the OS



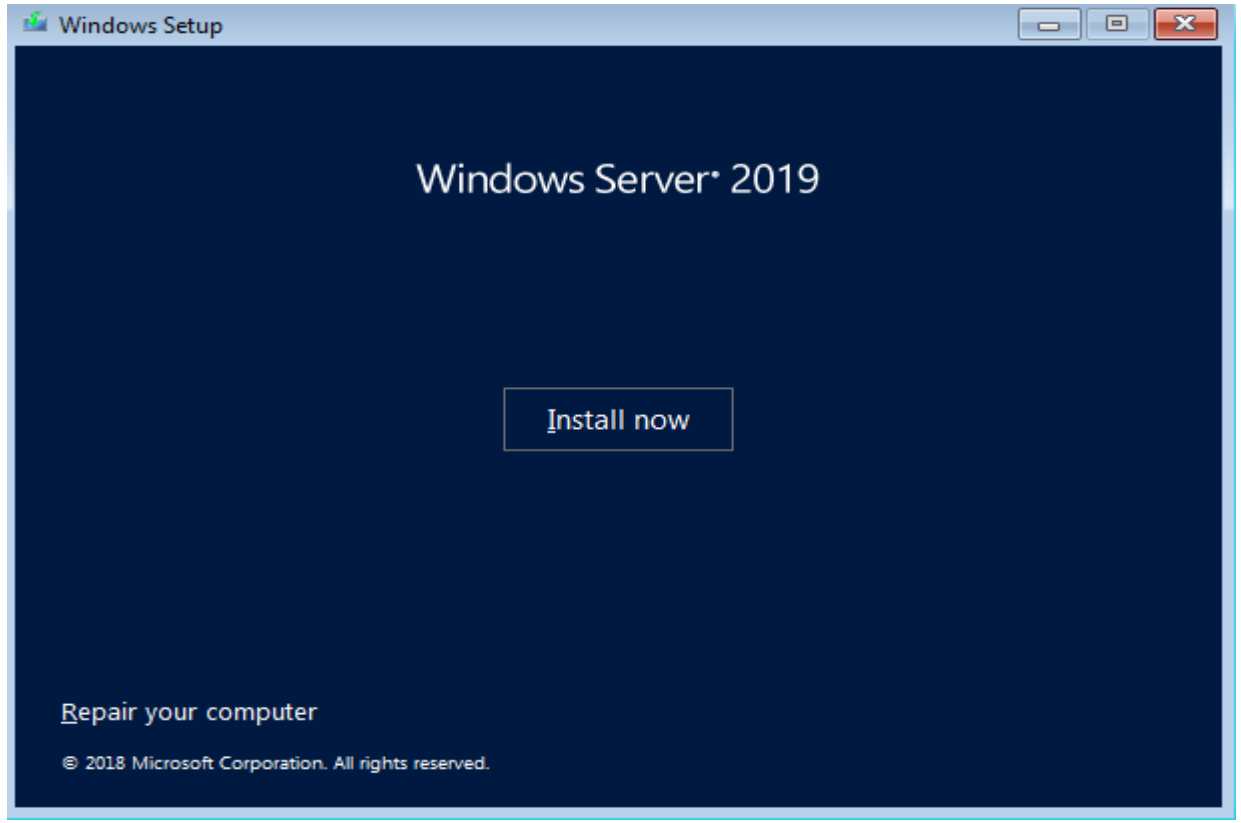
Lab Setup

Installing the OS



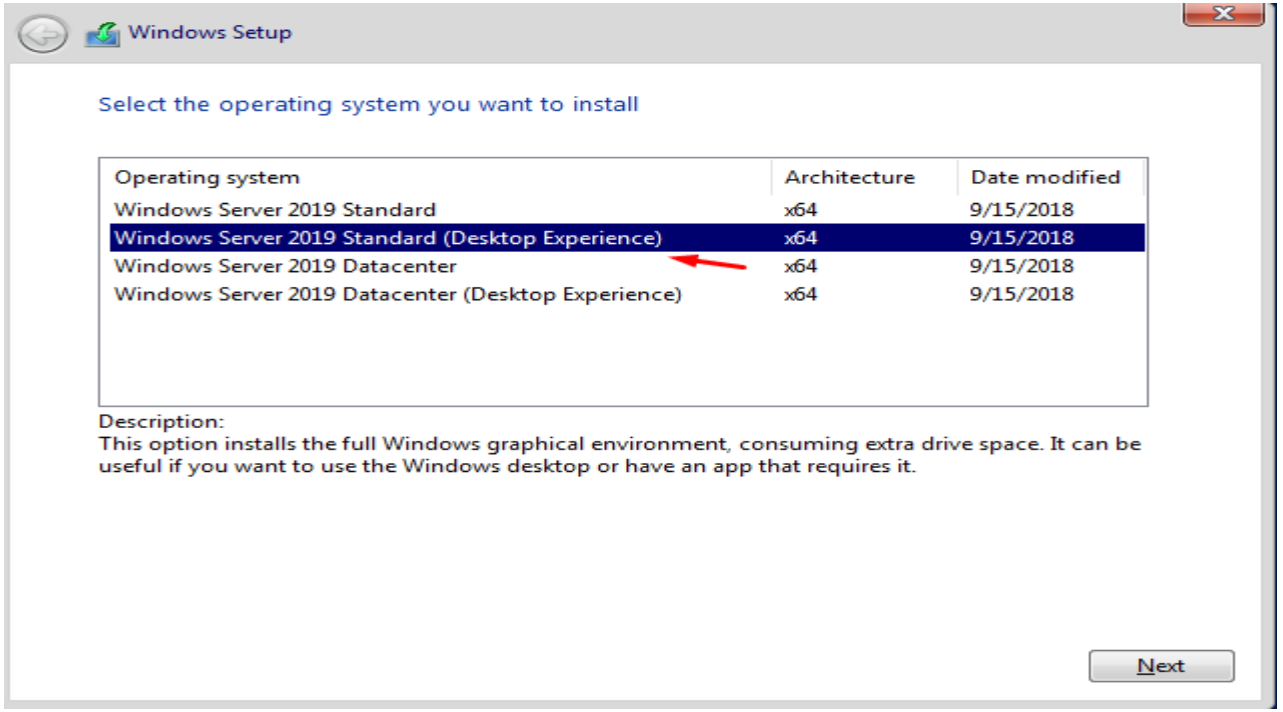
Lab Setup

Install now



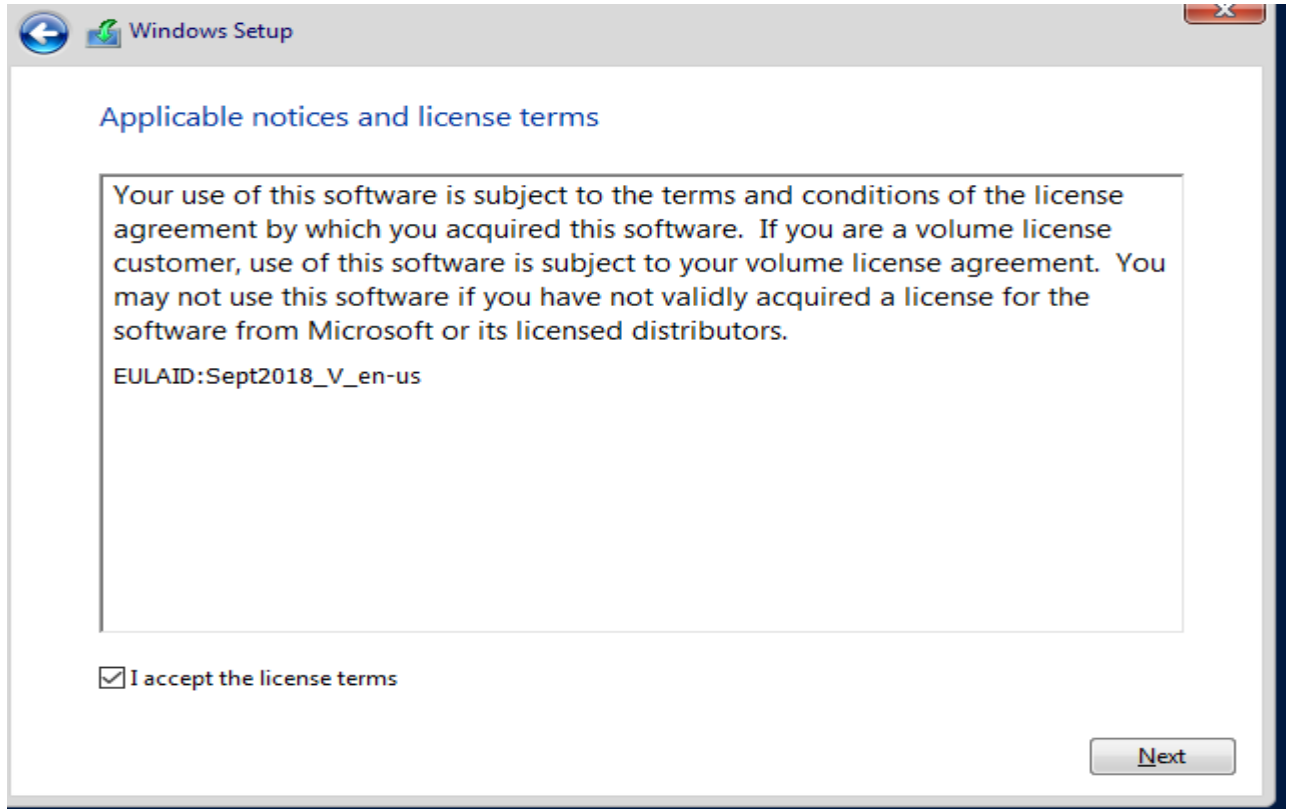
Lab Setup

Choose windows server with Desktop Experience



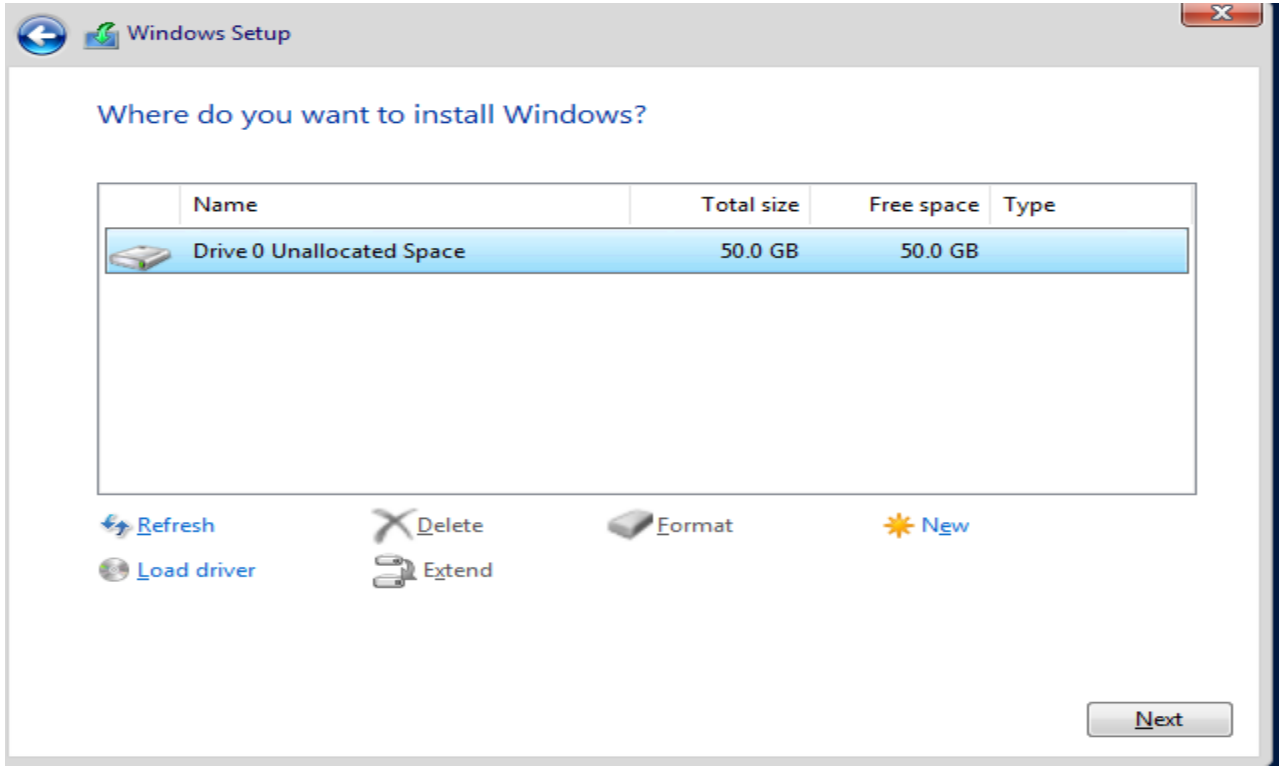
Lab Setup

Accept and Click Next



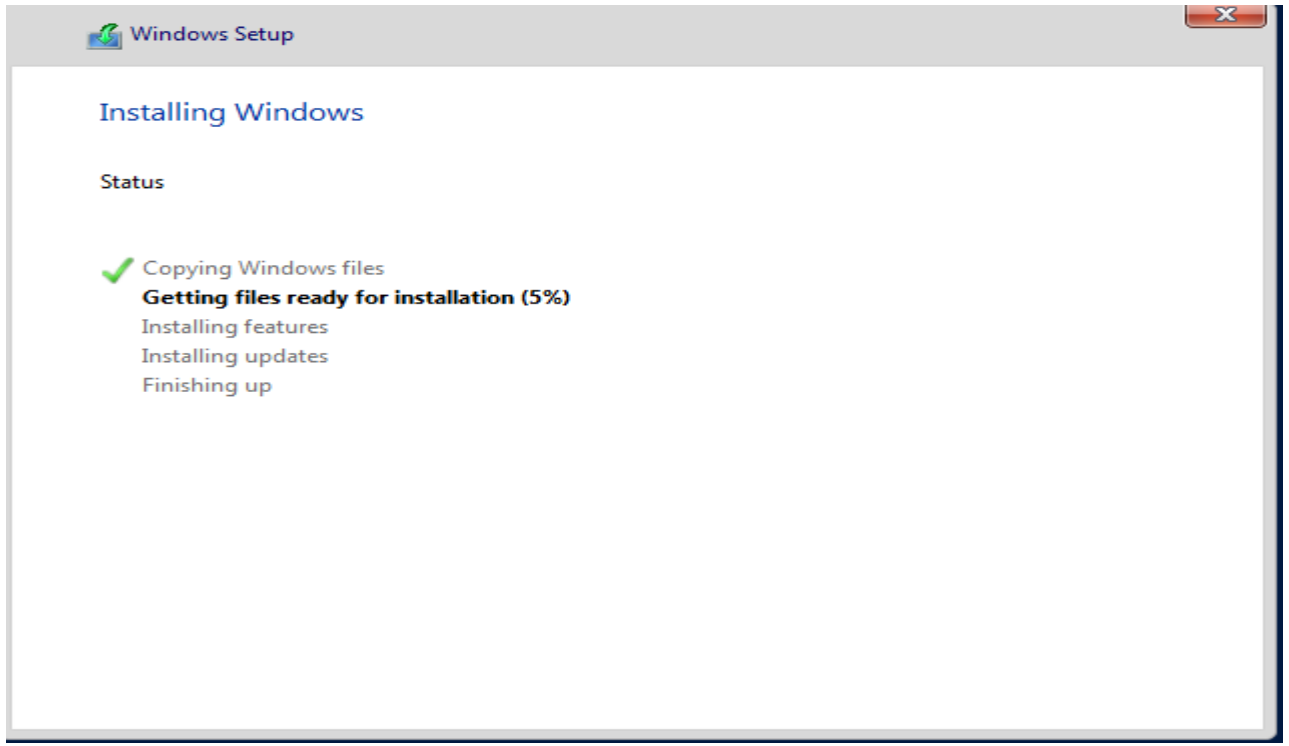
Lab Setup

Choose Custom install and Click Next



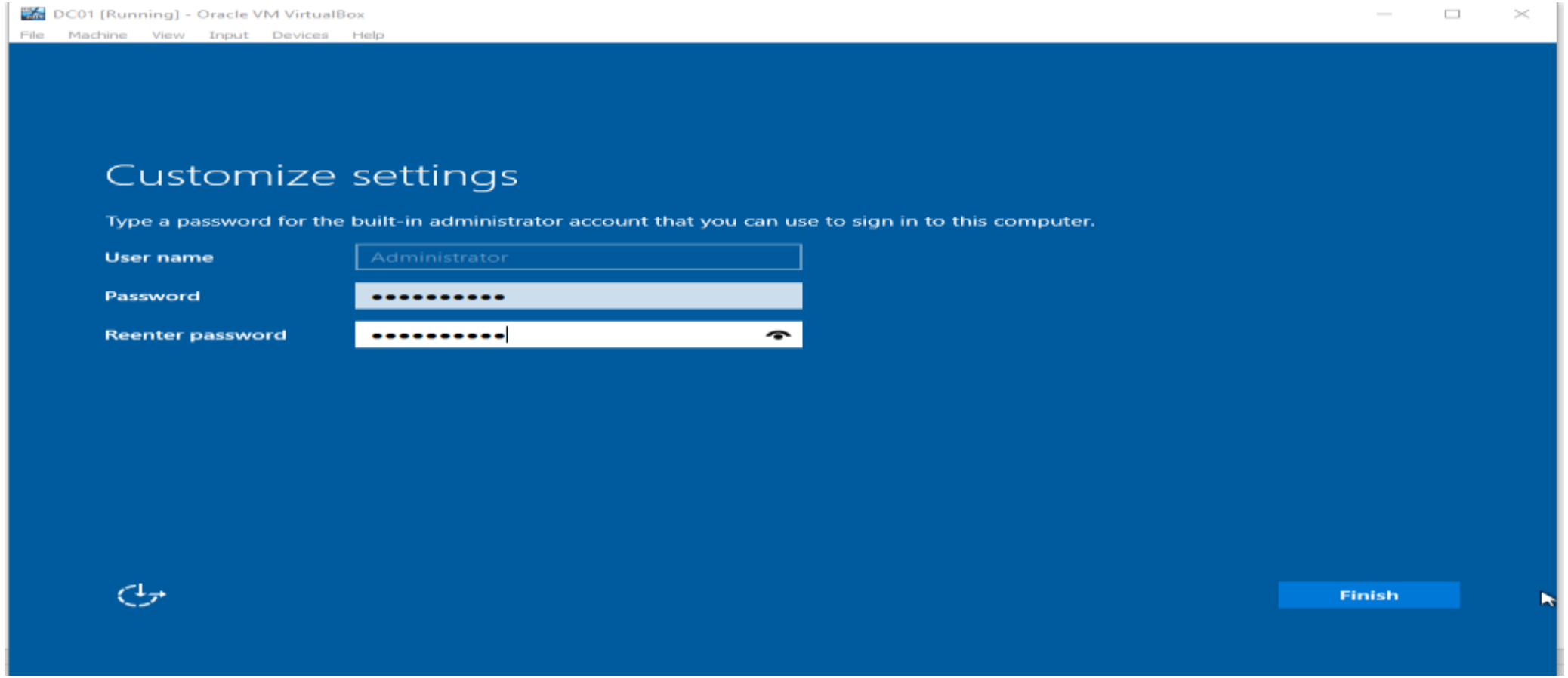
Lab Setup

Now allow the OS to be copied the VM we created



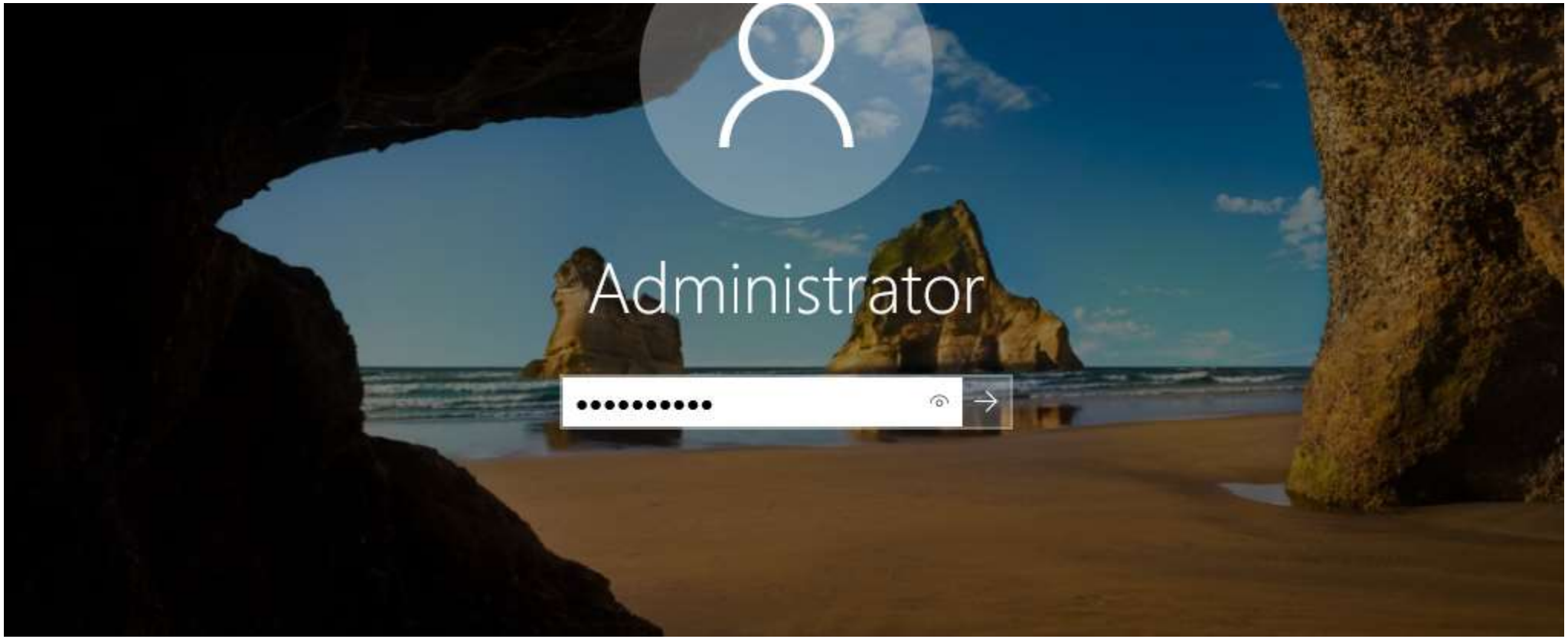
Lab Setup

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



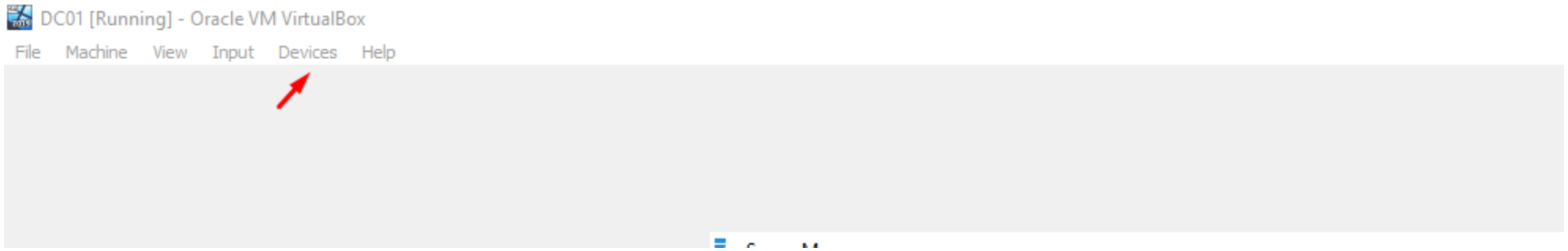
Lab Setup

Successfully Installed the OS



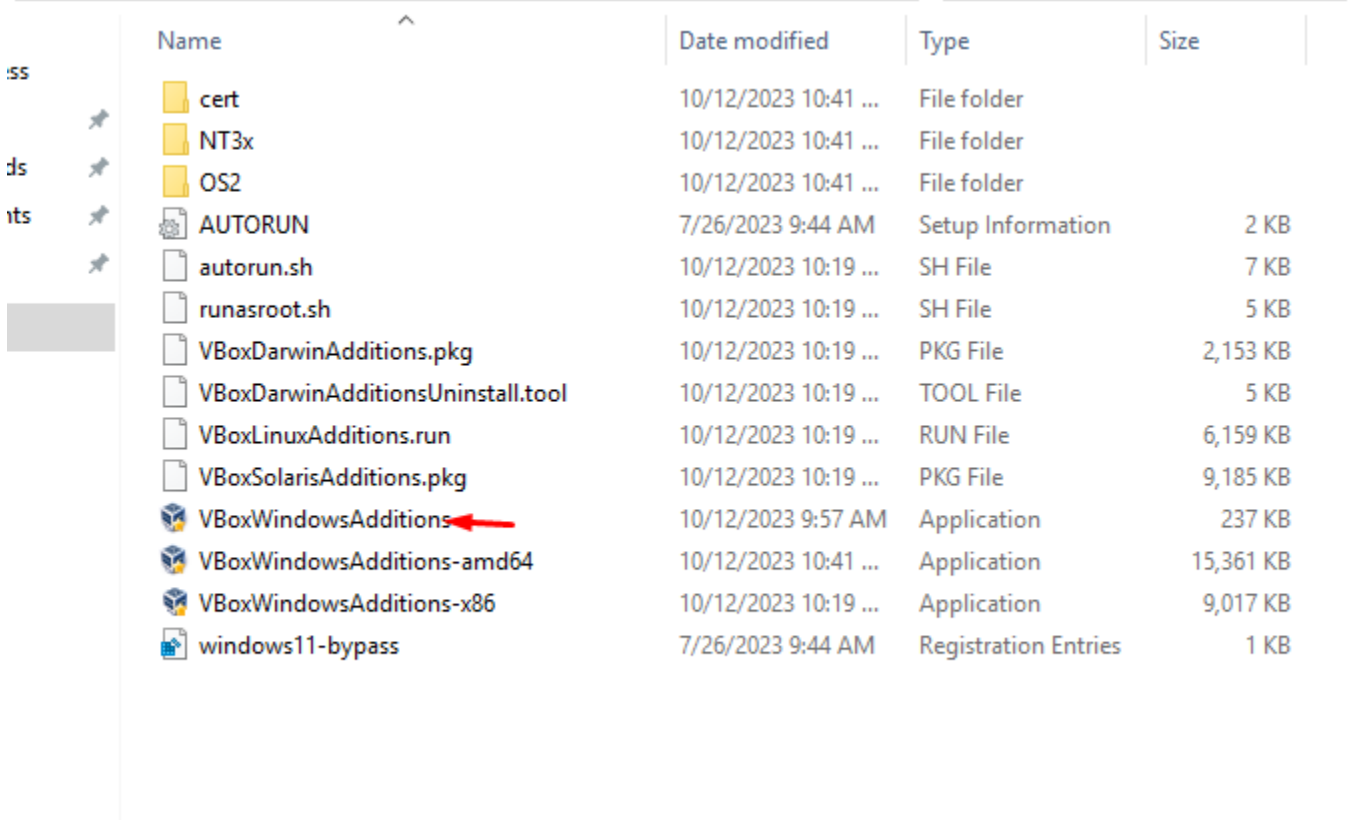
Lab Setup

Go Devices and Click insert guest edition CD image



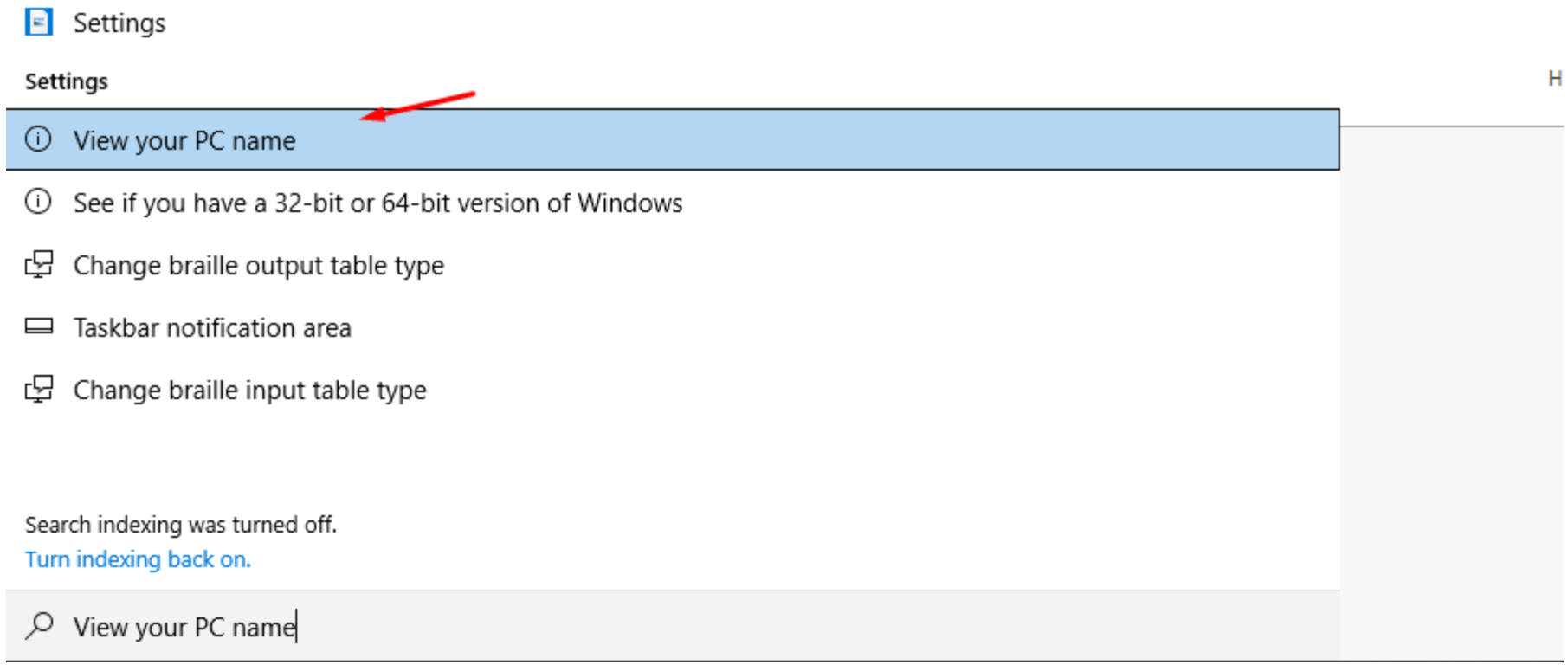
Lab Setup

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



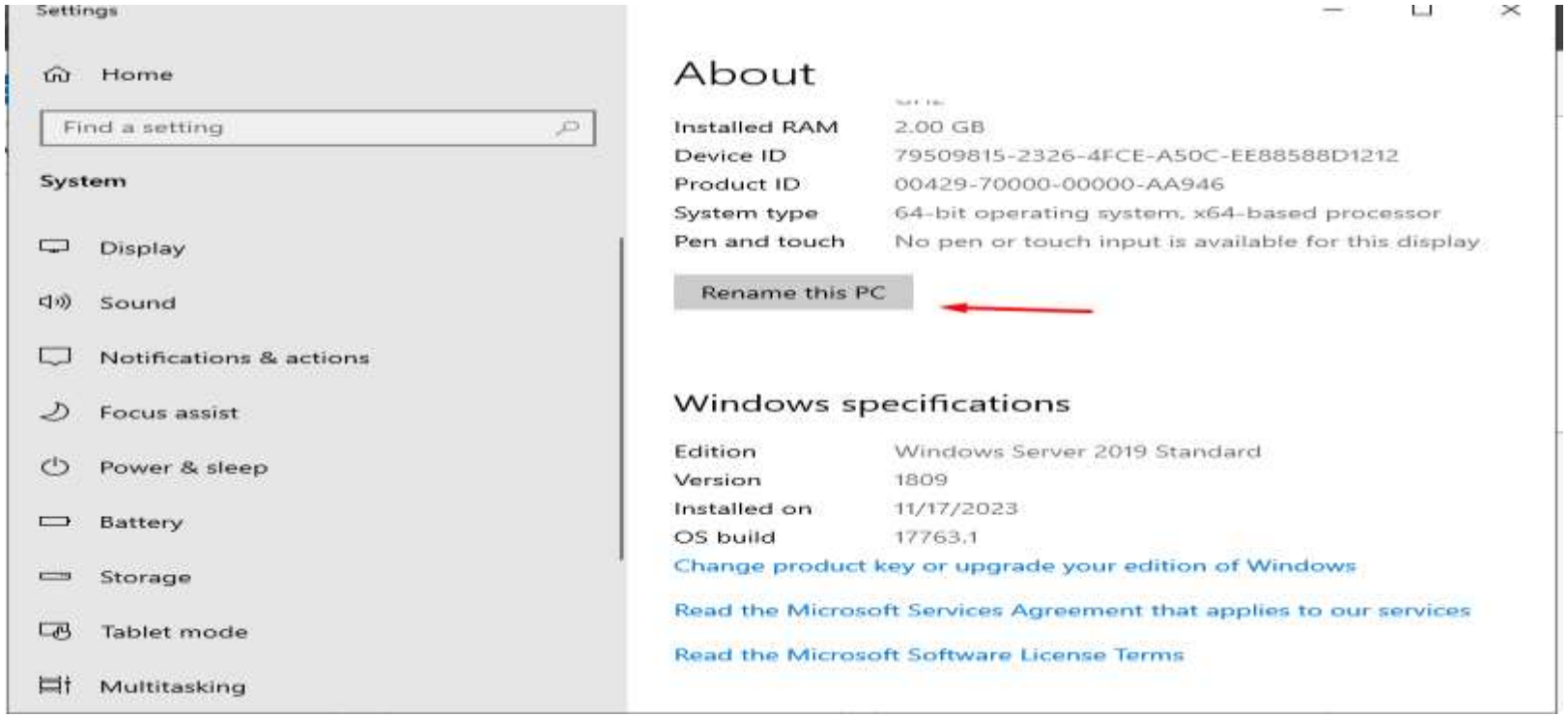
Lab Setup

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



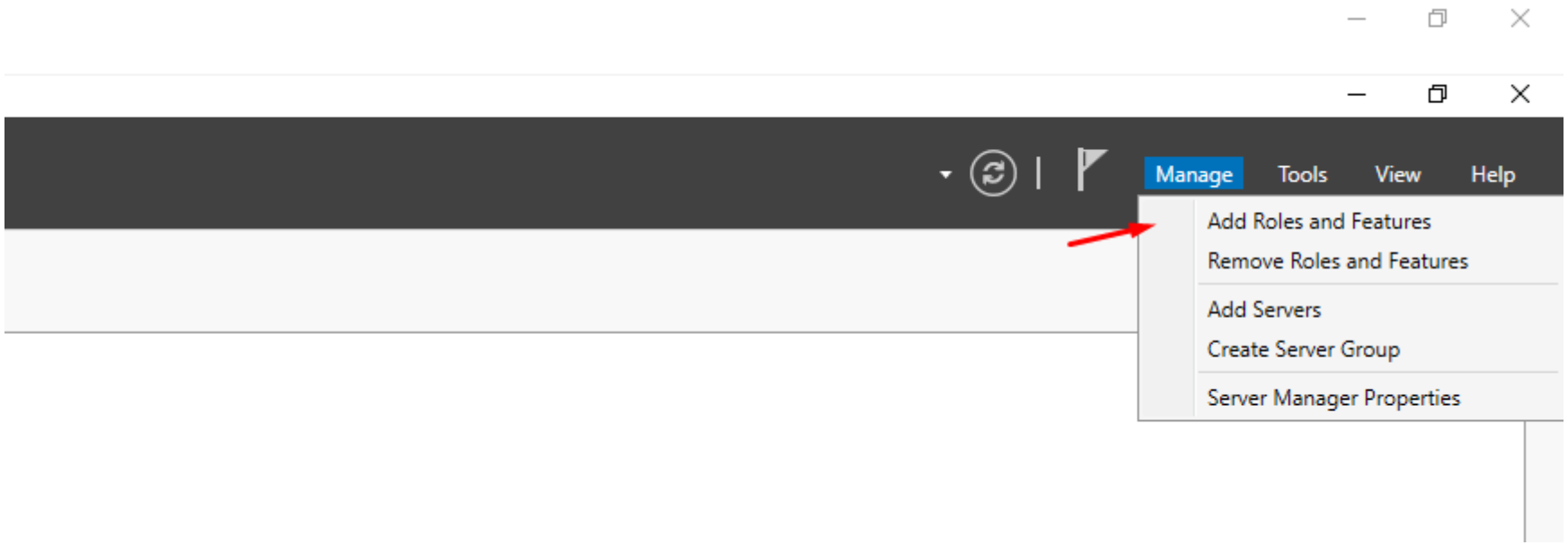
Lab Setup

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



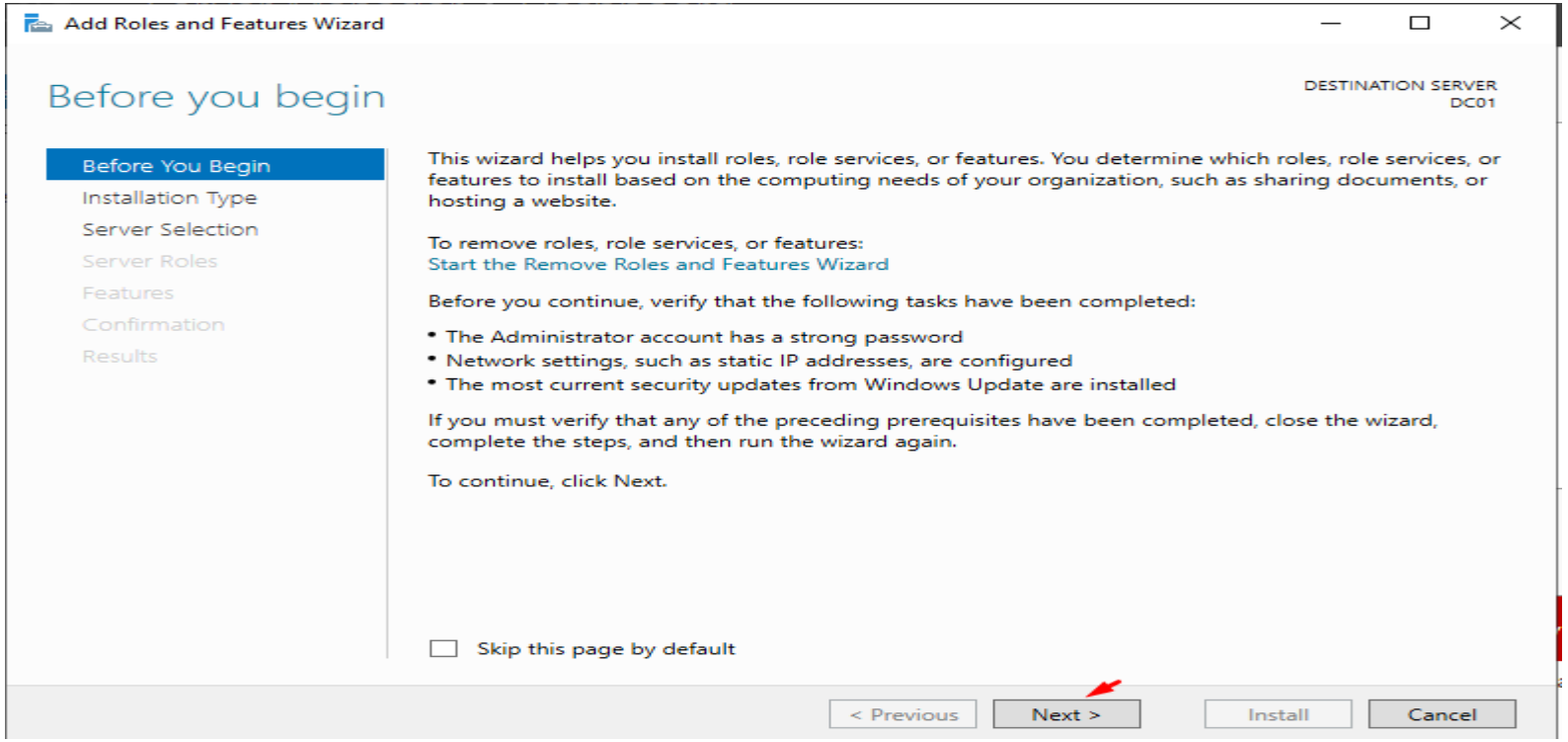
Lab Setup

Installing AD-DS and Domain Controller on the Server



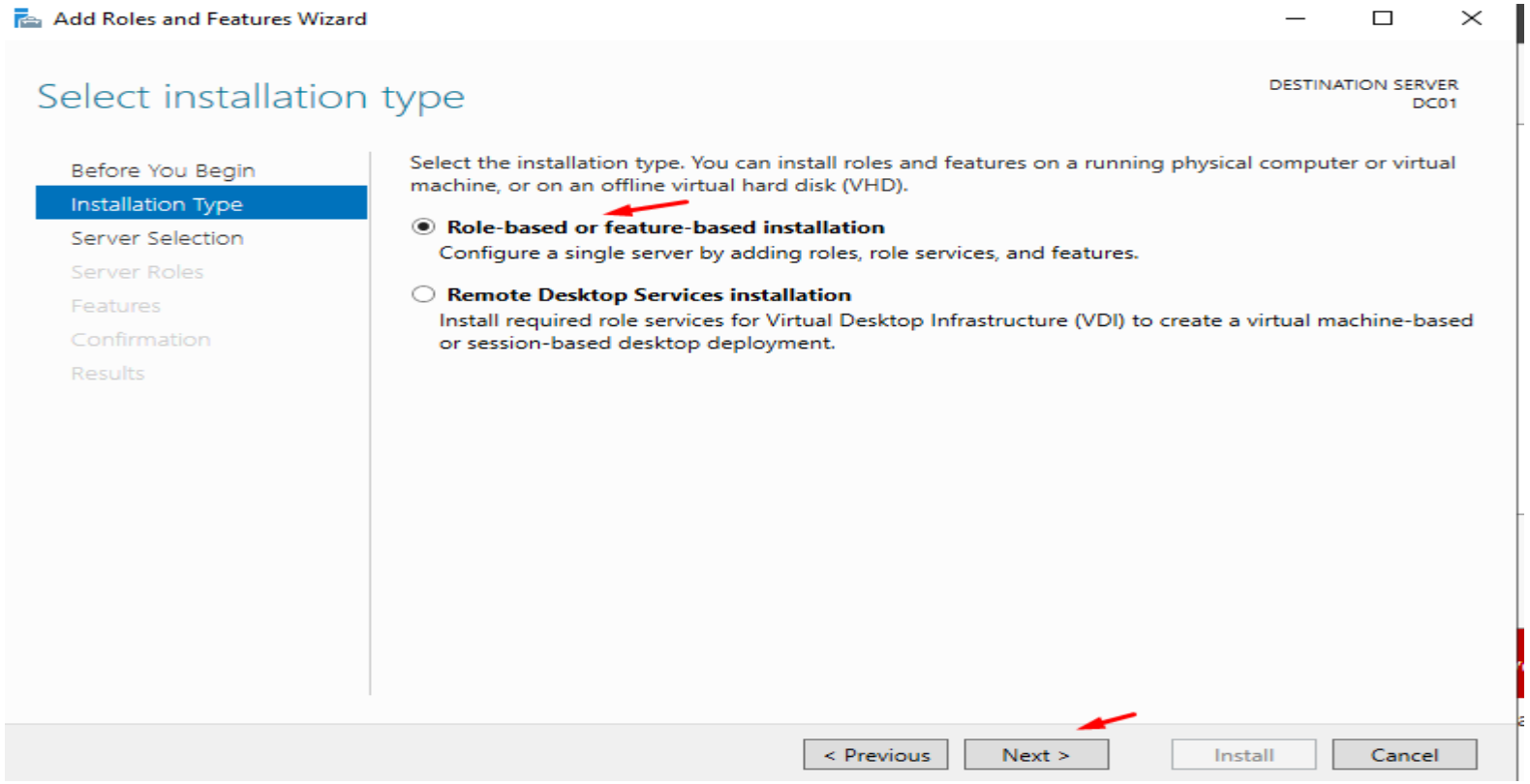
Lab Setup

Next



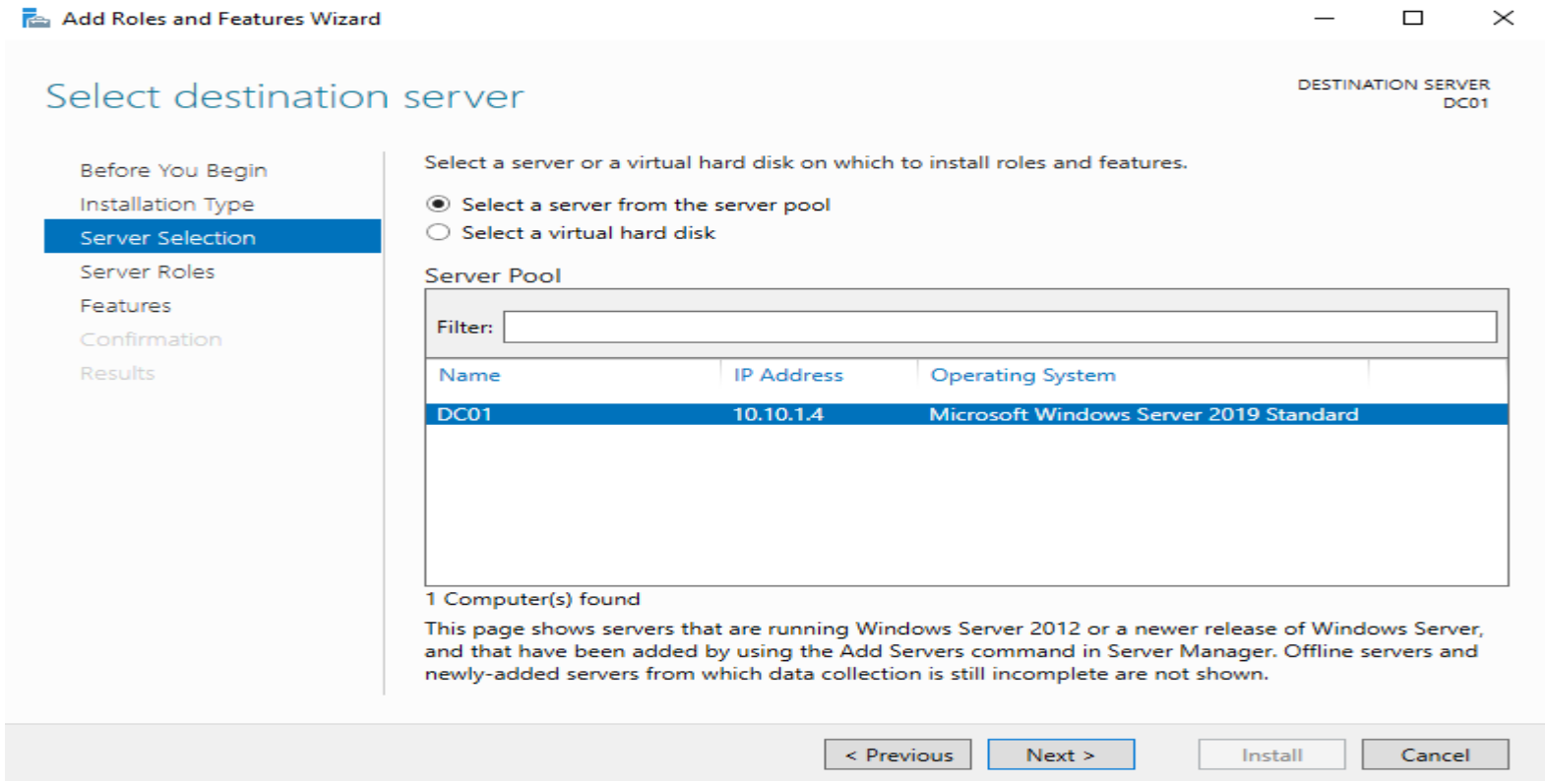
Lab Setup

Next



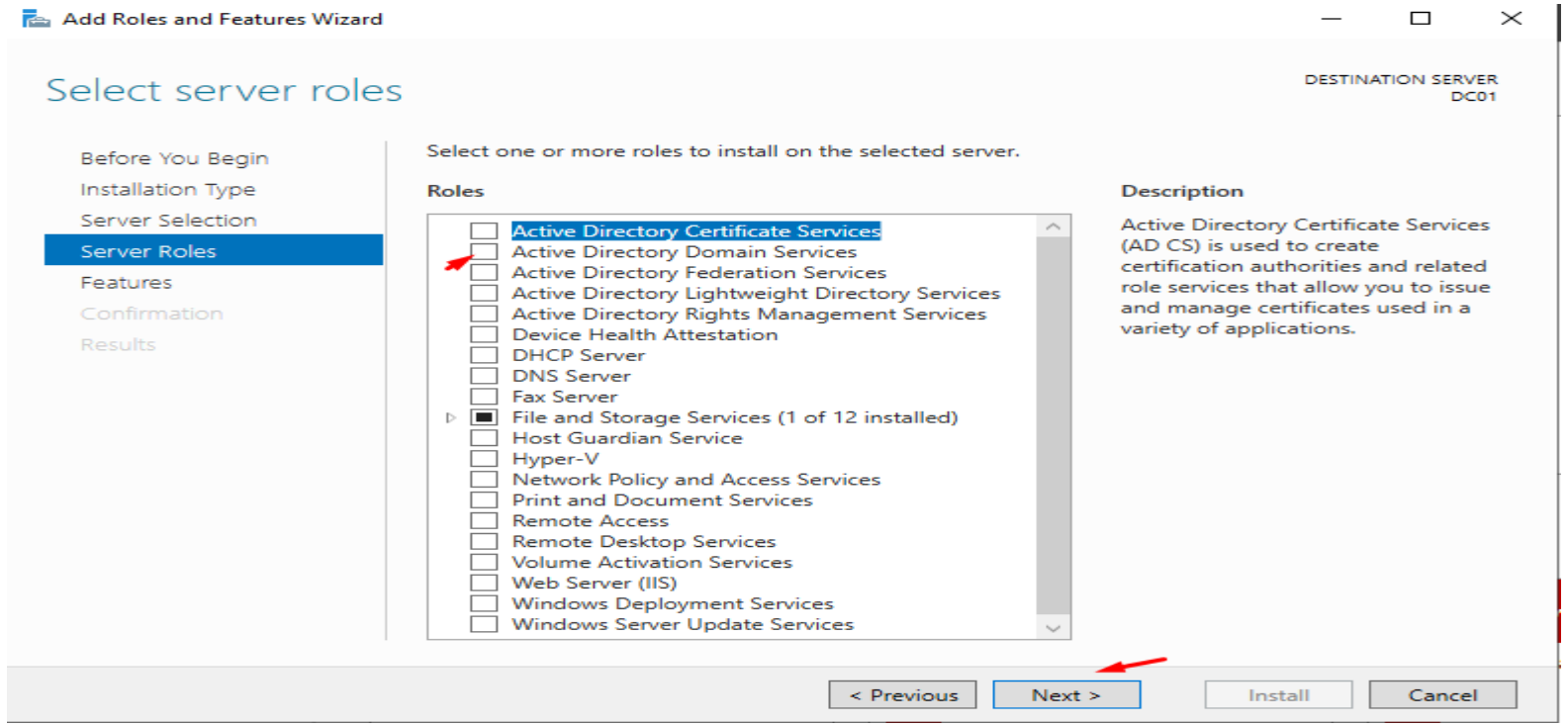
Lab Setup

Next

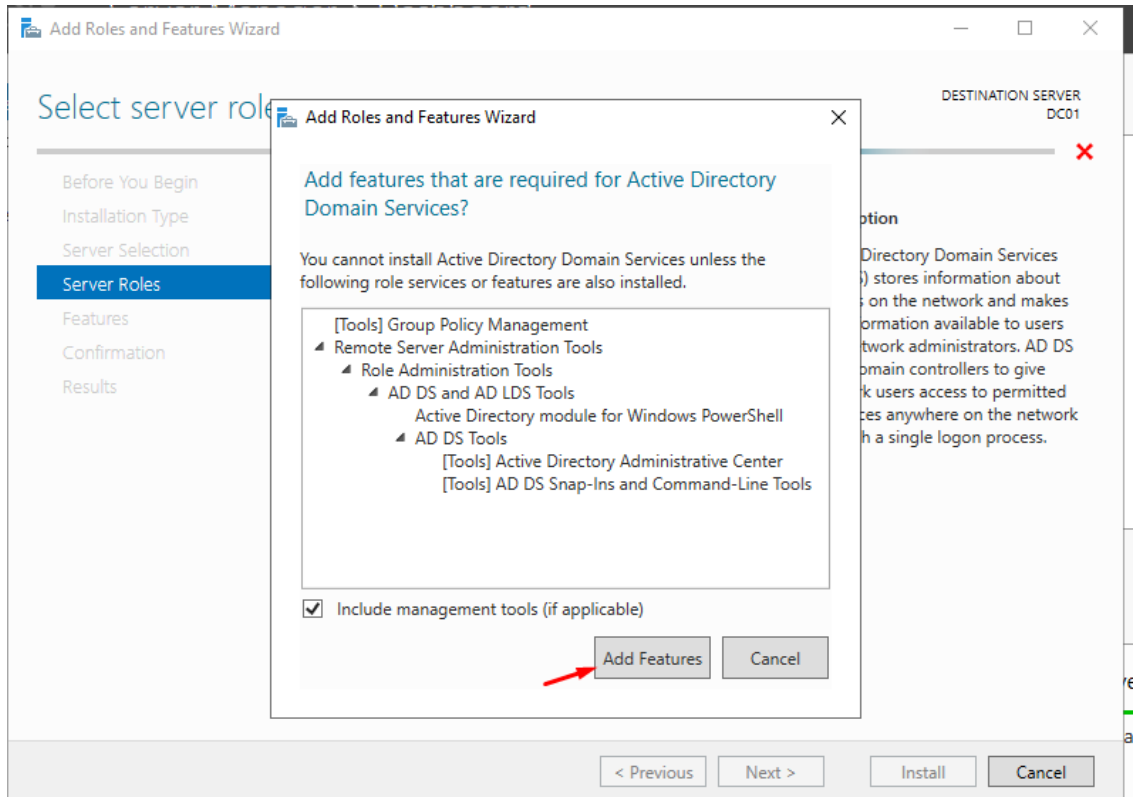


Lab Setup

Select Active Directory DomainService and Click add features

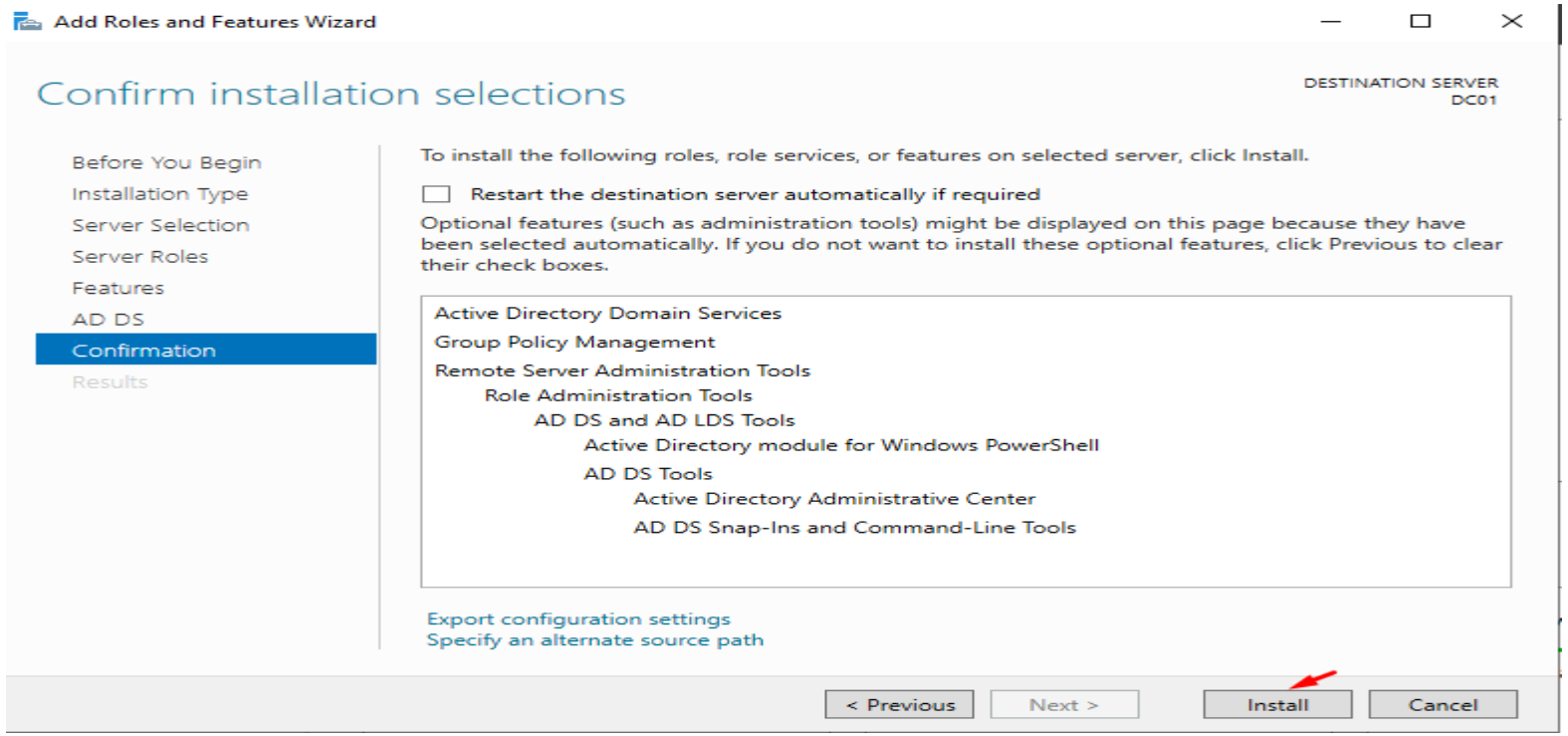


Lab Setup


Add Roles and Features Wizard
Select server role
DESTINATION SERVER
DC01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel

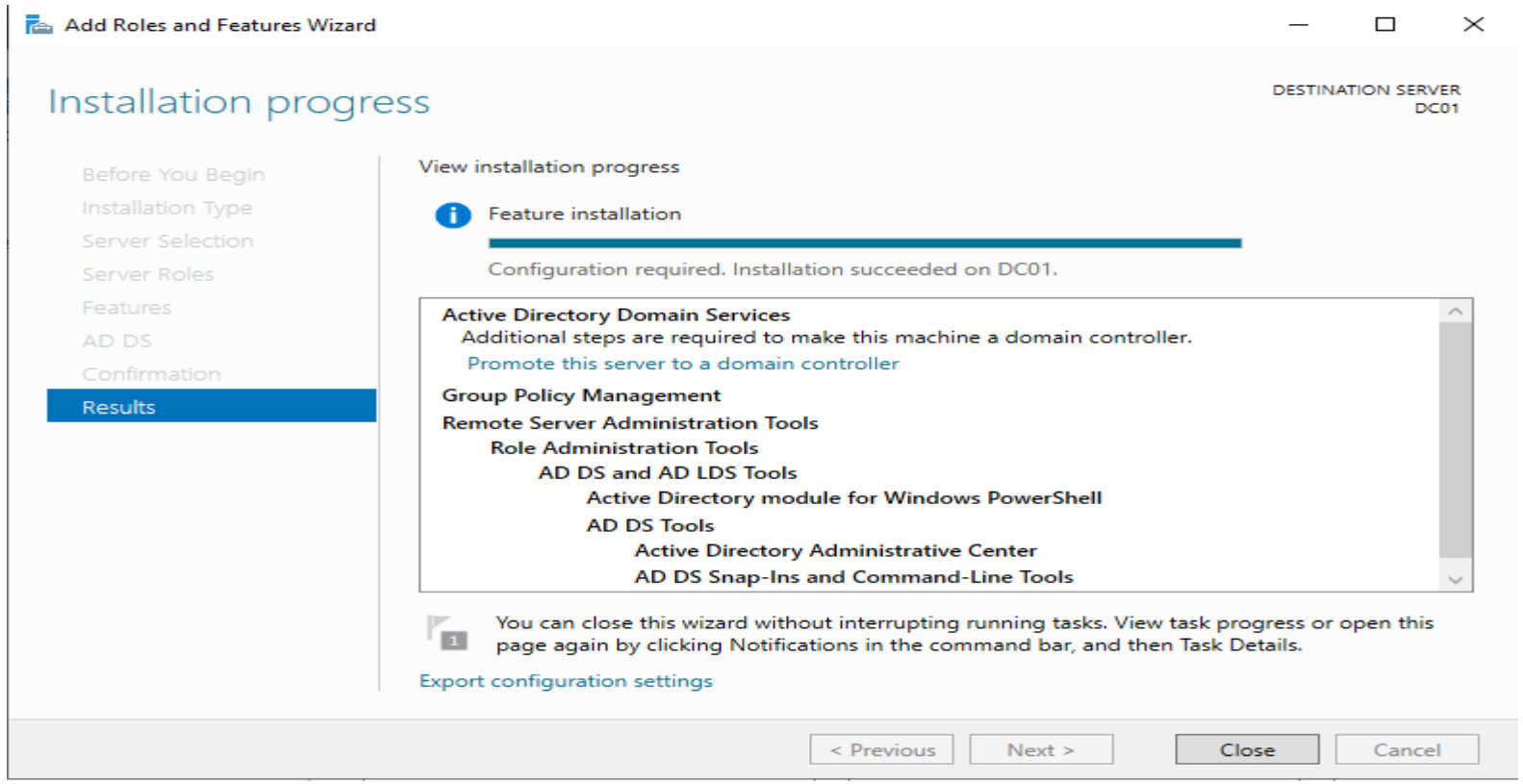
Lab Setup

Next to Install



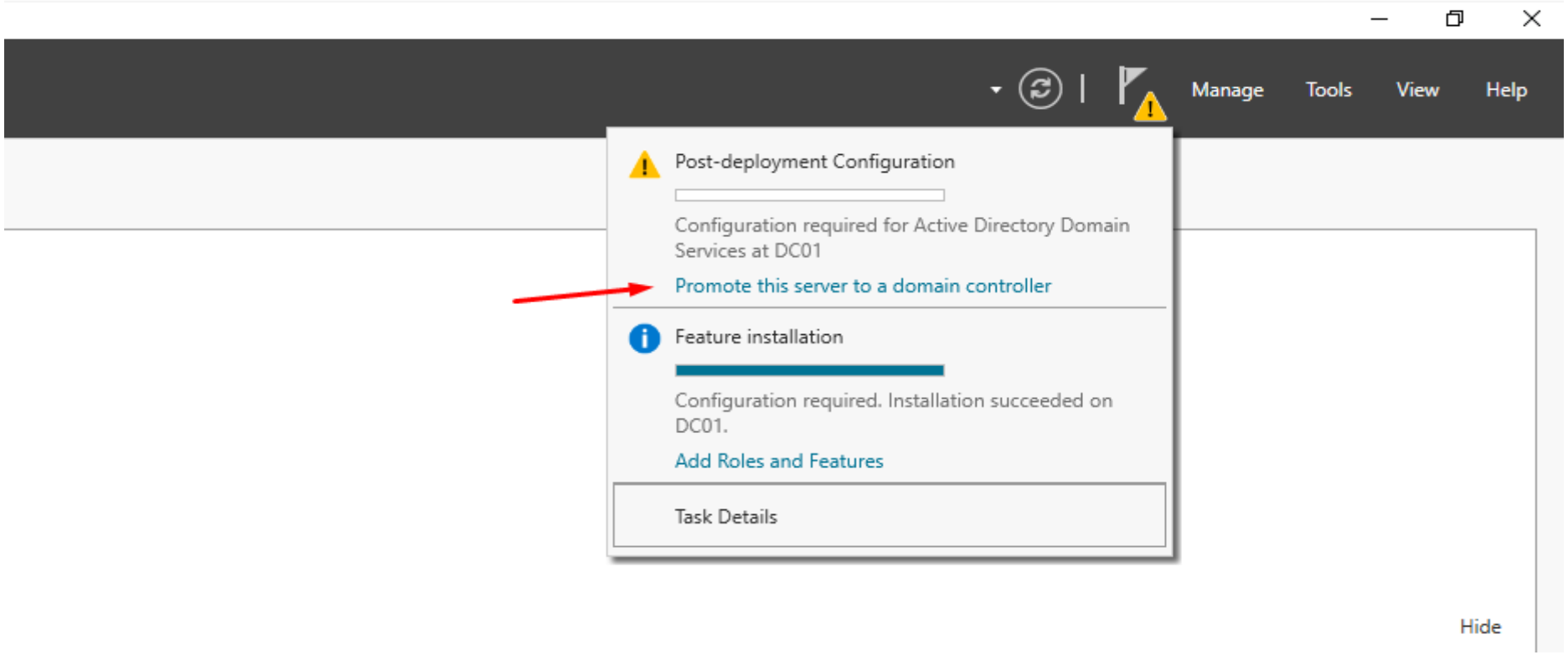
Lab Setup

After the installation click close



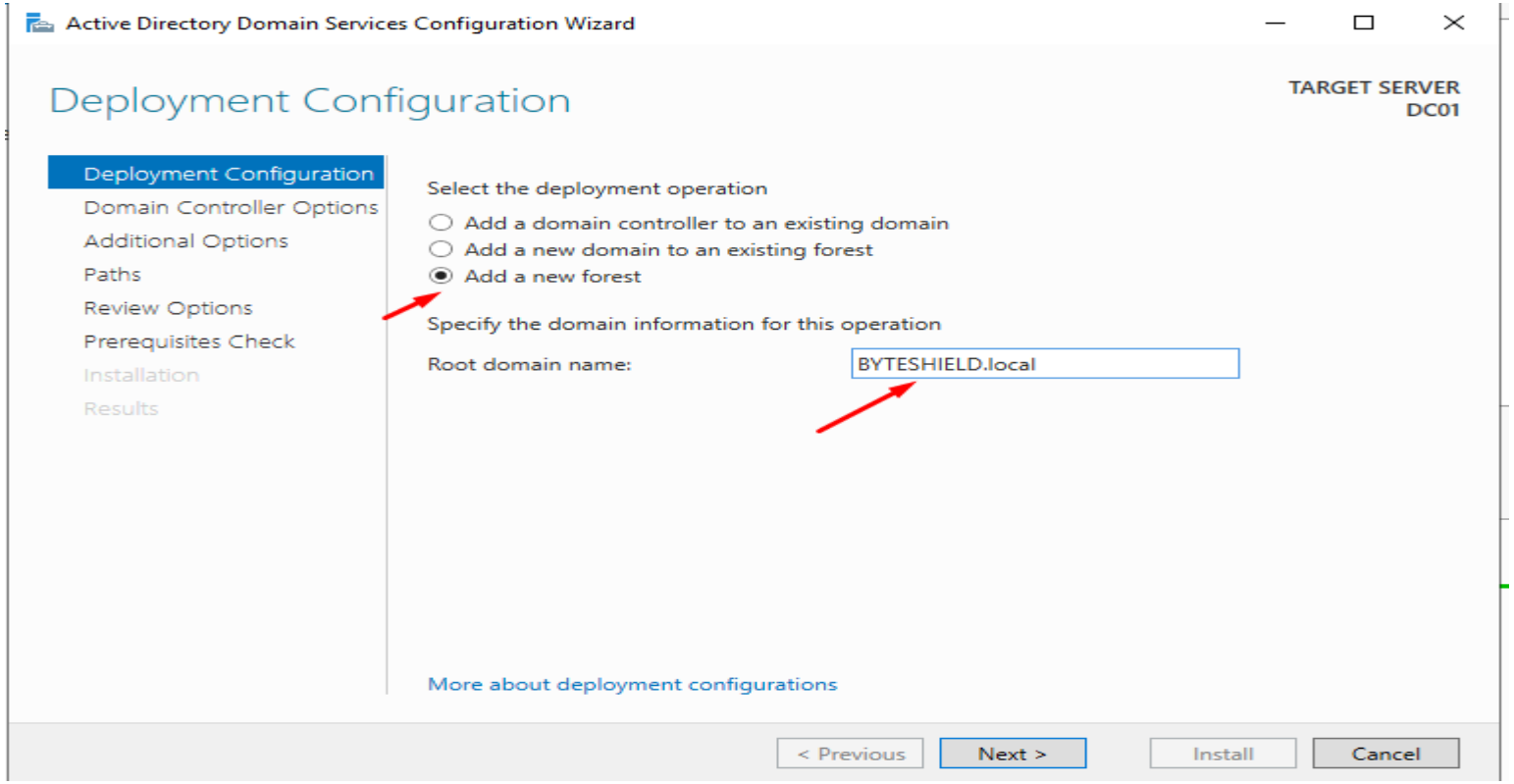
Lab Setup

Installing Domain Controller



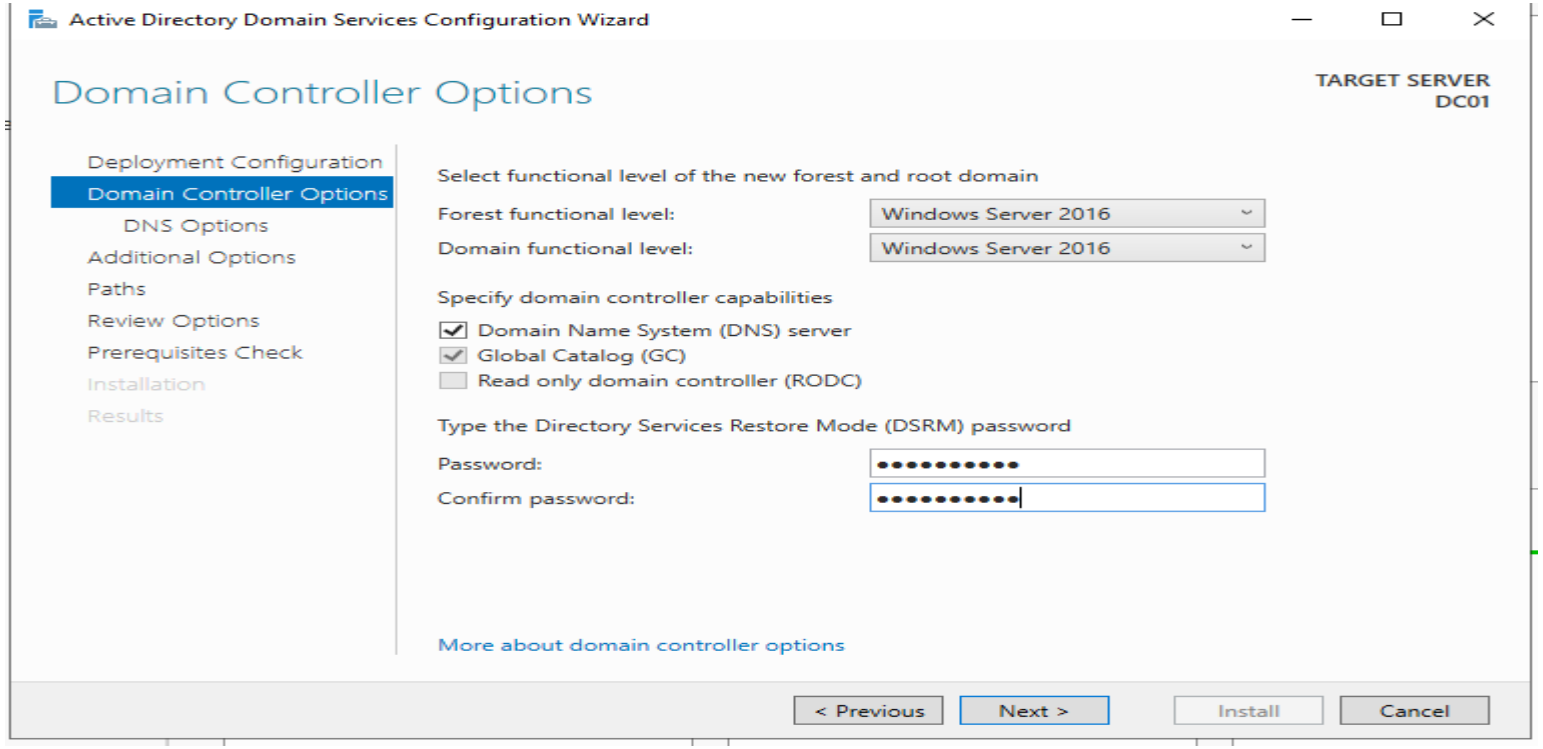
Lab Setup

Adding new forest and FQDN



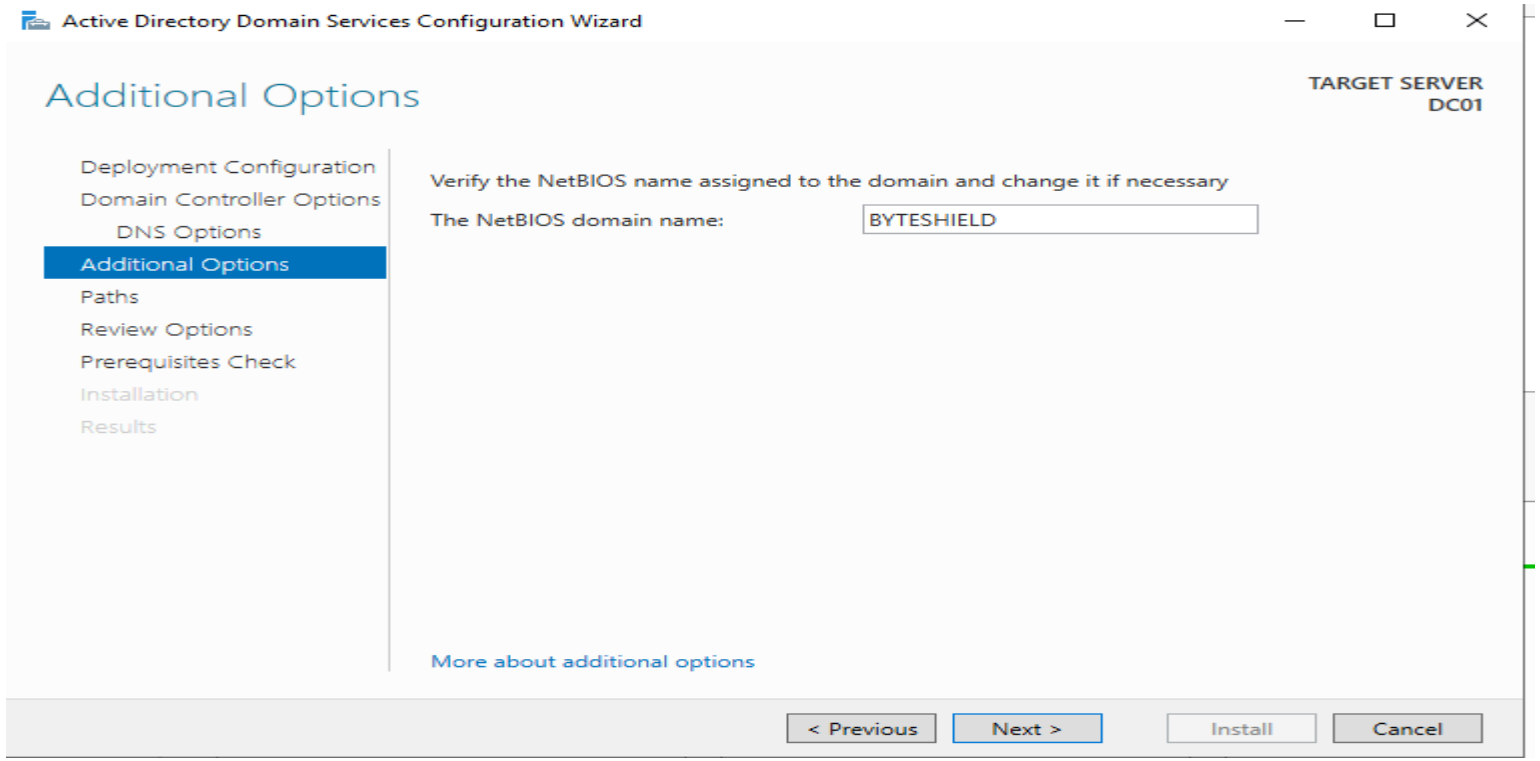
Lab Setup

Creating a memorable Domain Services Recovery mode password (DSRM)



Lab Setup

Next > Next > Install to Finish

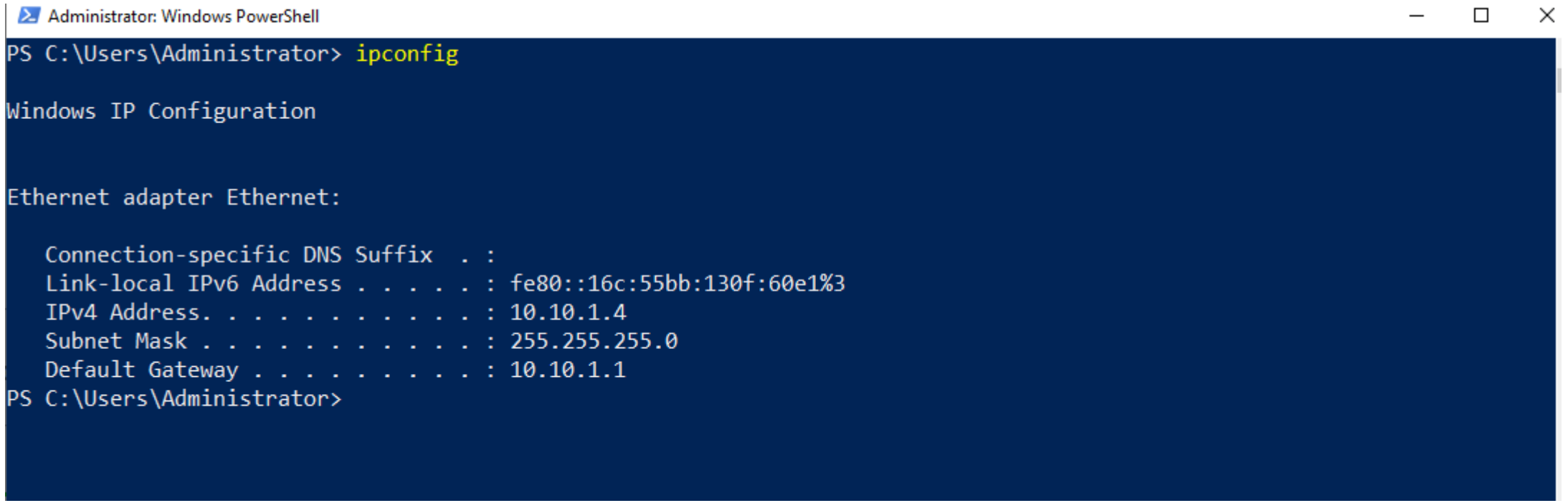


Lab Setup

AD-DS and Domain Controller has been Successfully installed

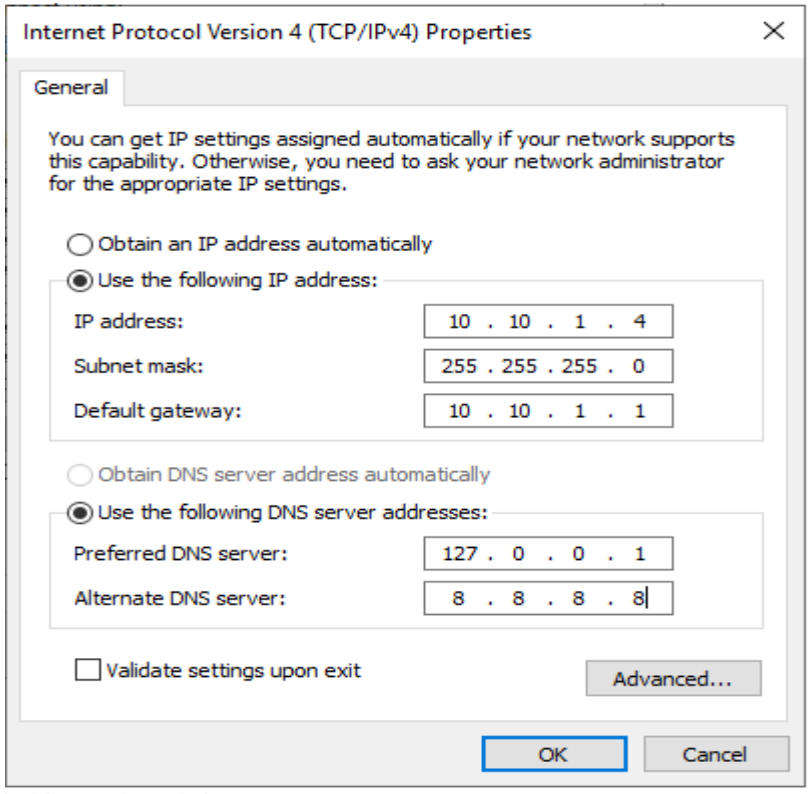
Lab Setup

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



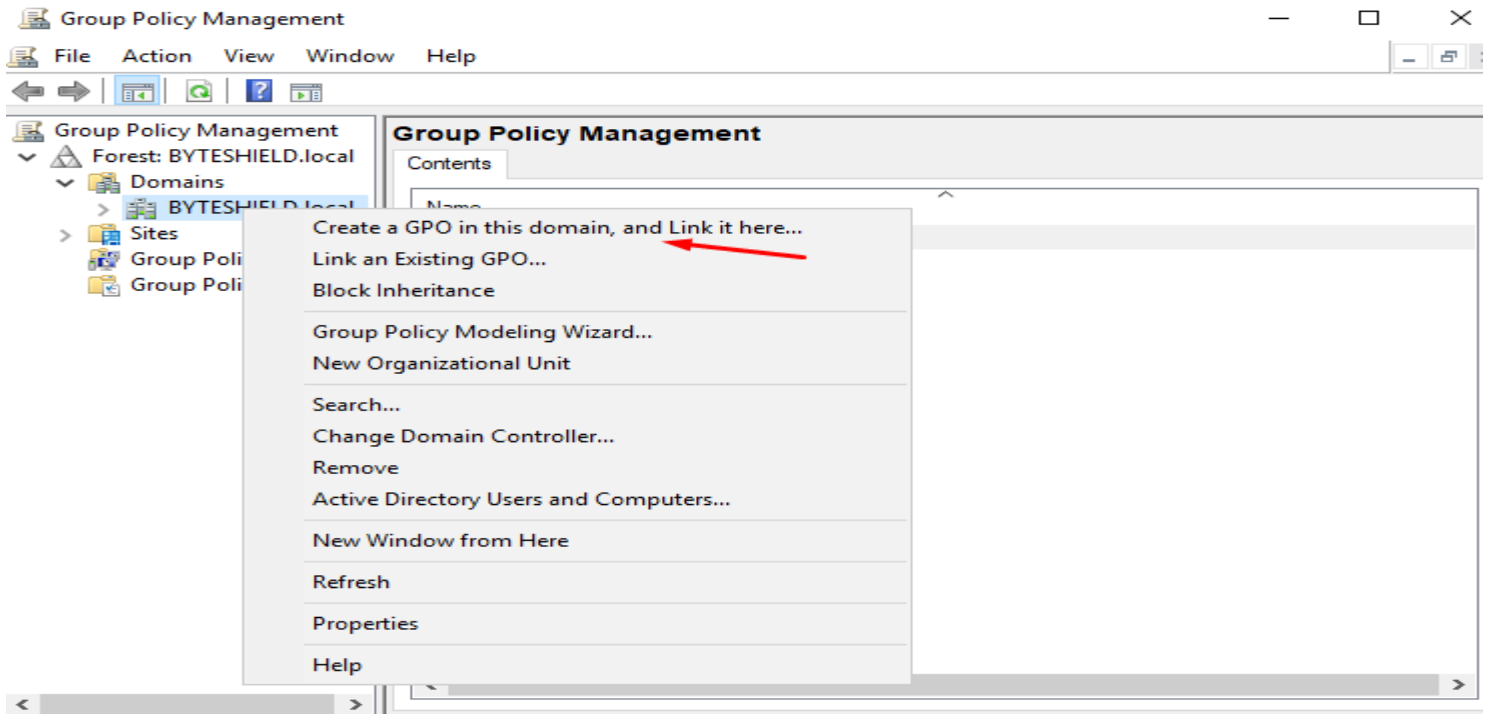
Lab Setup

Network Settings



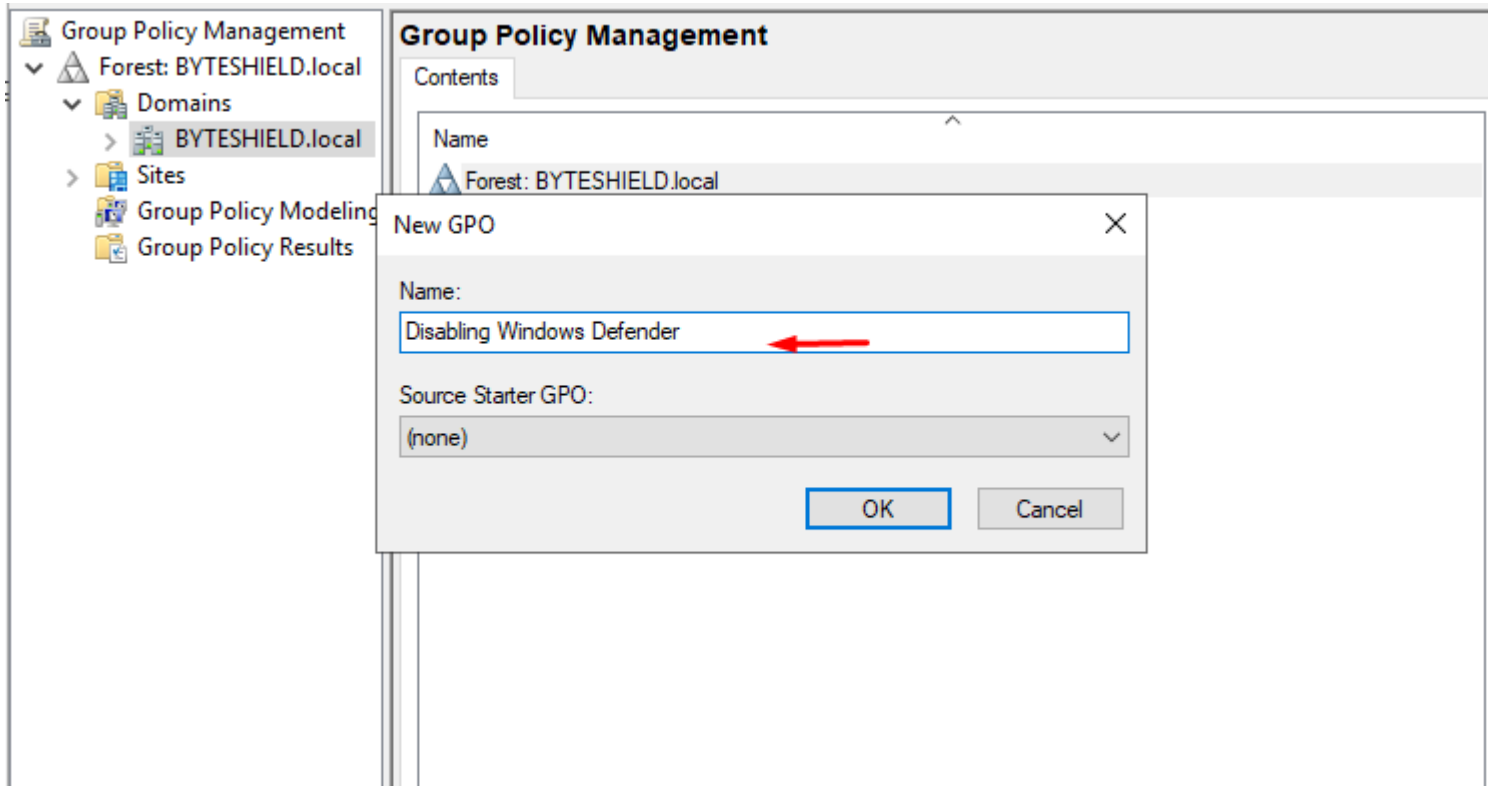
Lab Setup

Creating Policy to Disable Windows Defender



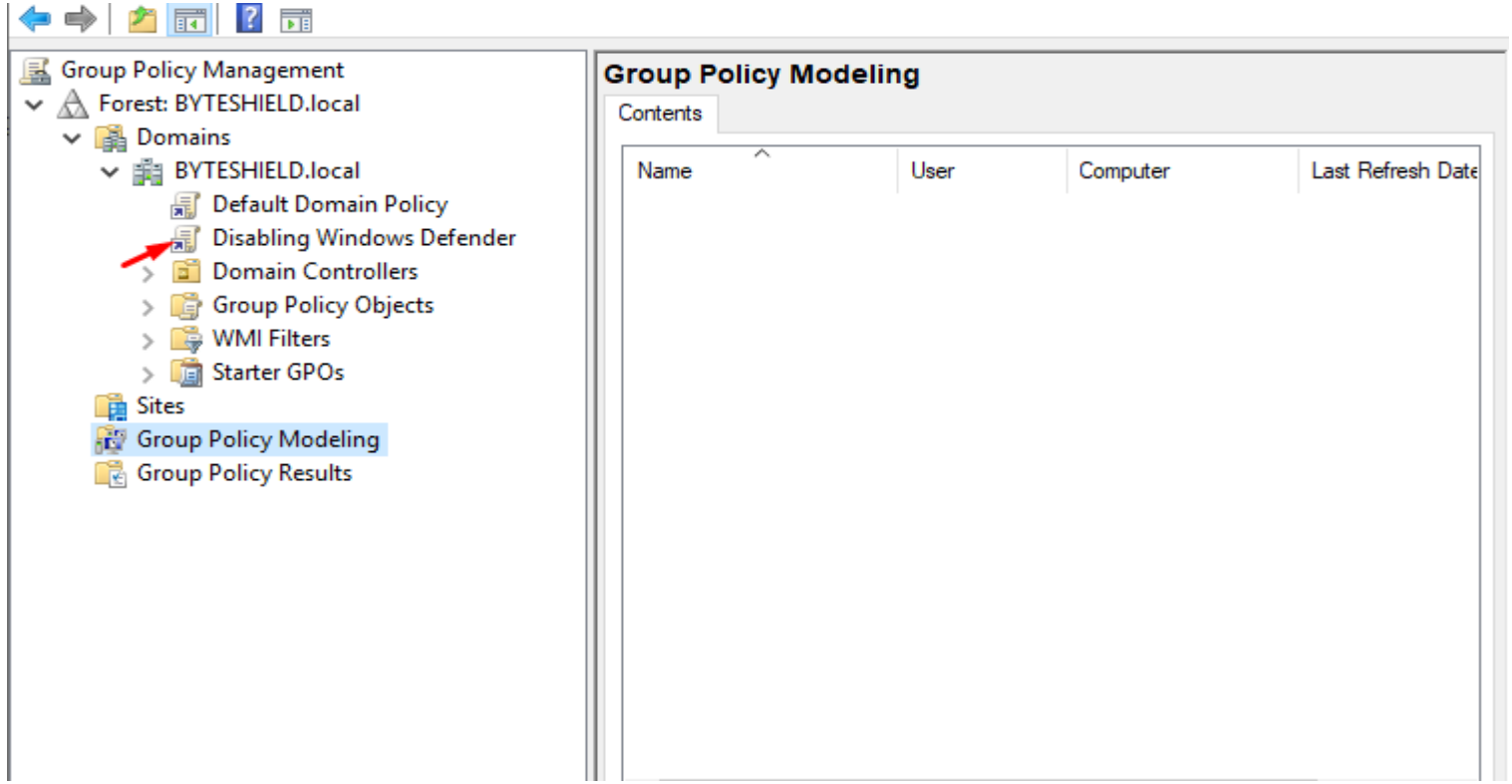
Lab Setup

Naming the Policy

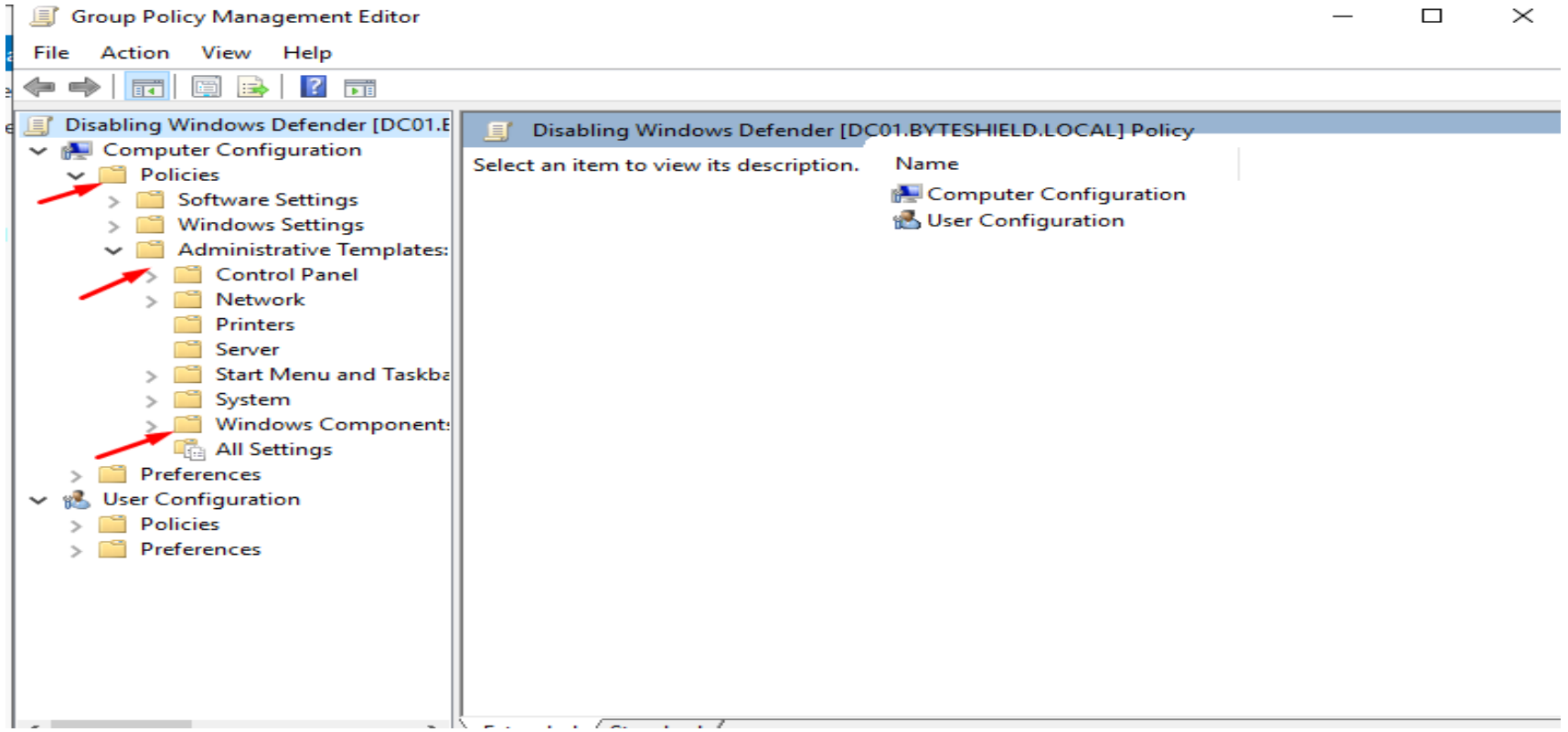


Lab Setup

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

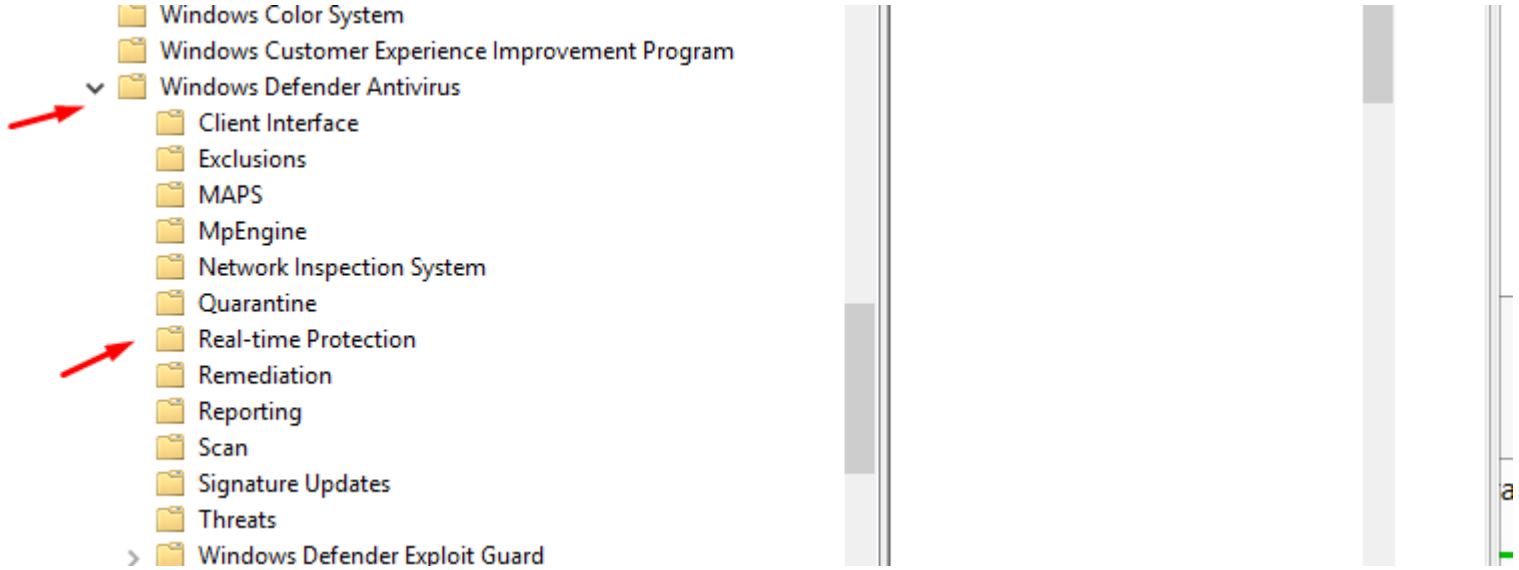


Lab Setup


Group Policy Management Editor
File
Action
View
Help
Disabling Windows Defender [DC01.E
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates:
Control Panel
Network
Printers
Server
Start Menu and Taskba
System
Windows Component
All Settings
Preferences
User Configuration
Policies
Preferences
Disabling Windows Defender [DC01.BYTESHIELD.LOCAL] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration

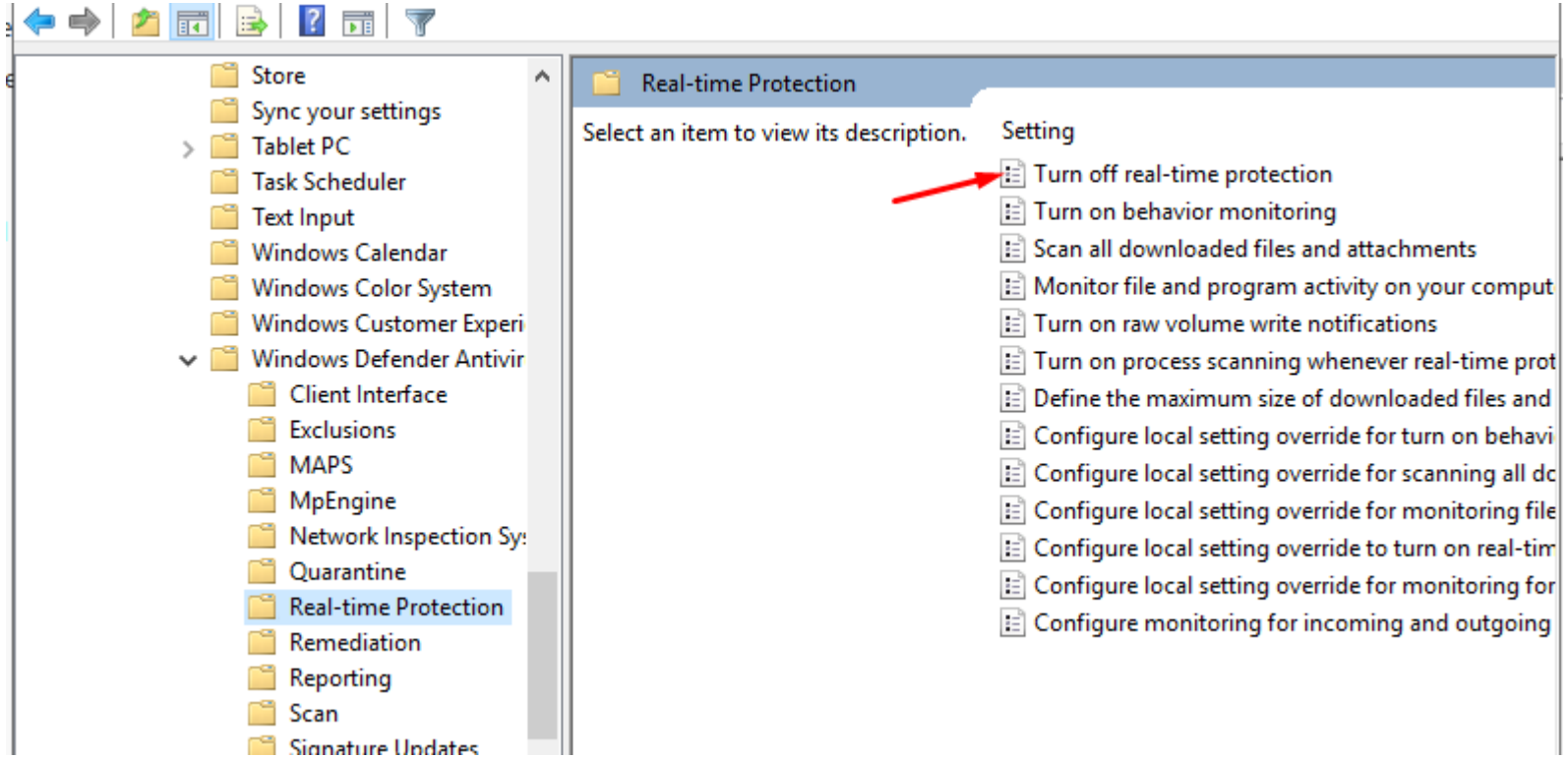
Lab Setup

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



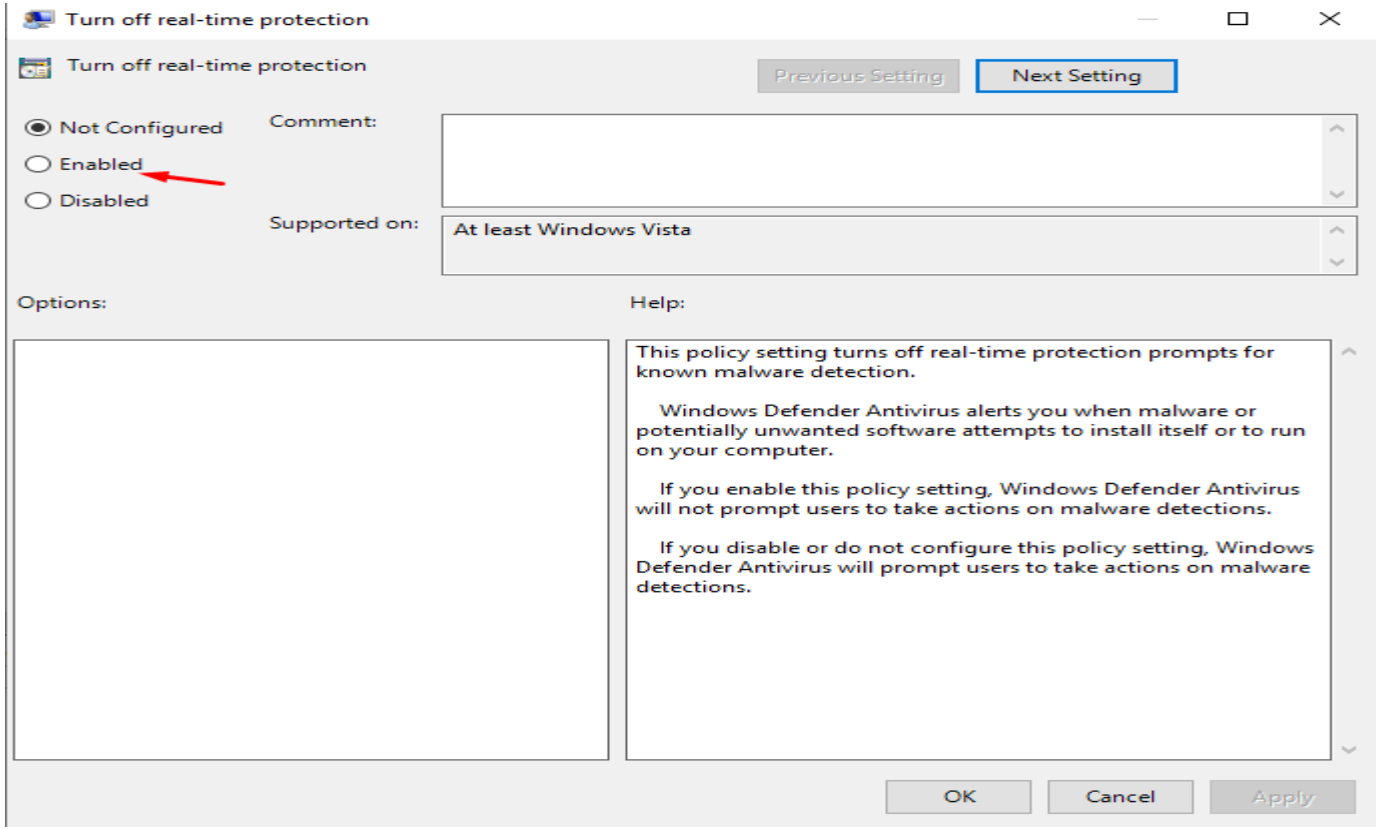
Lab Setup

Double Click on turn off real-time Protection



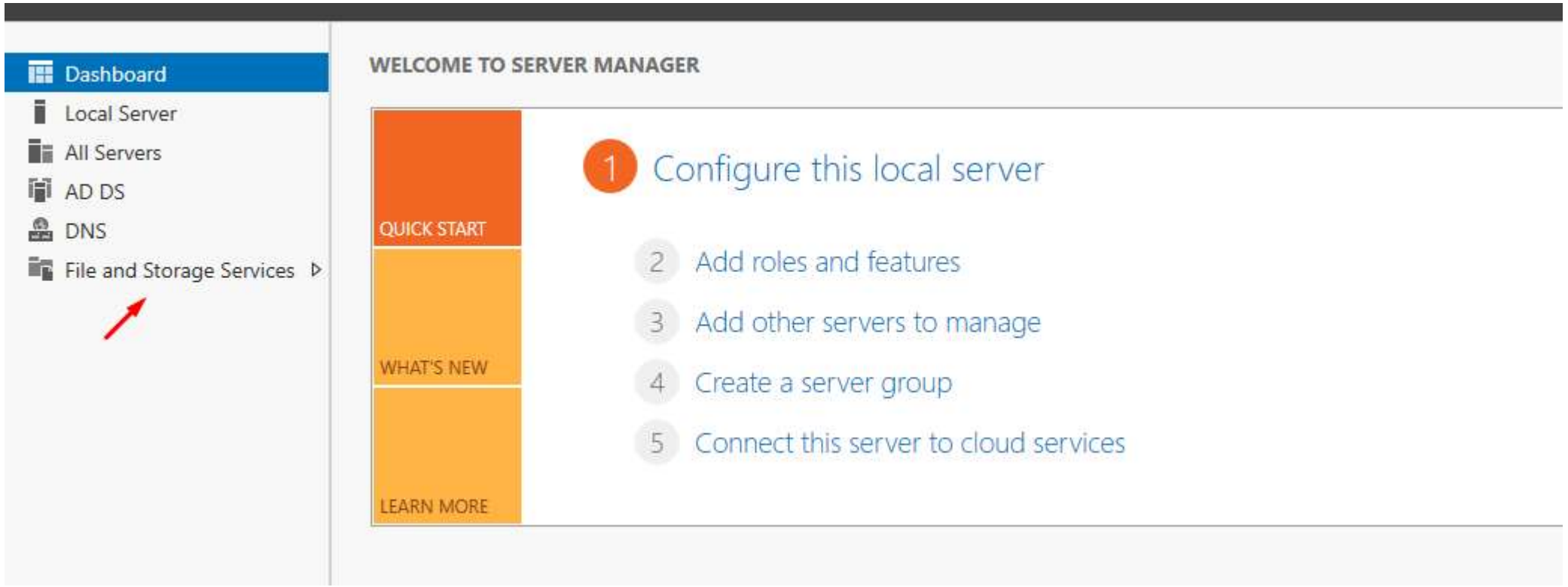
Lab Setup

Select enable and Ok

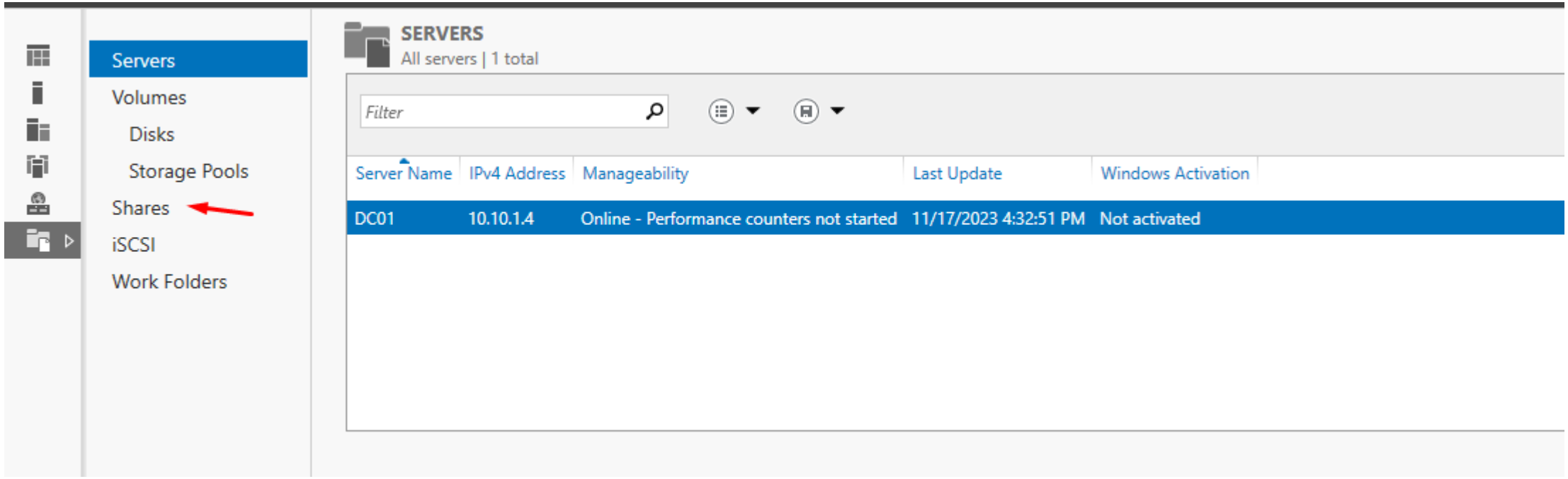


Lab Setup

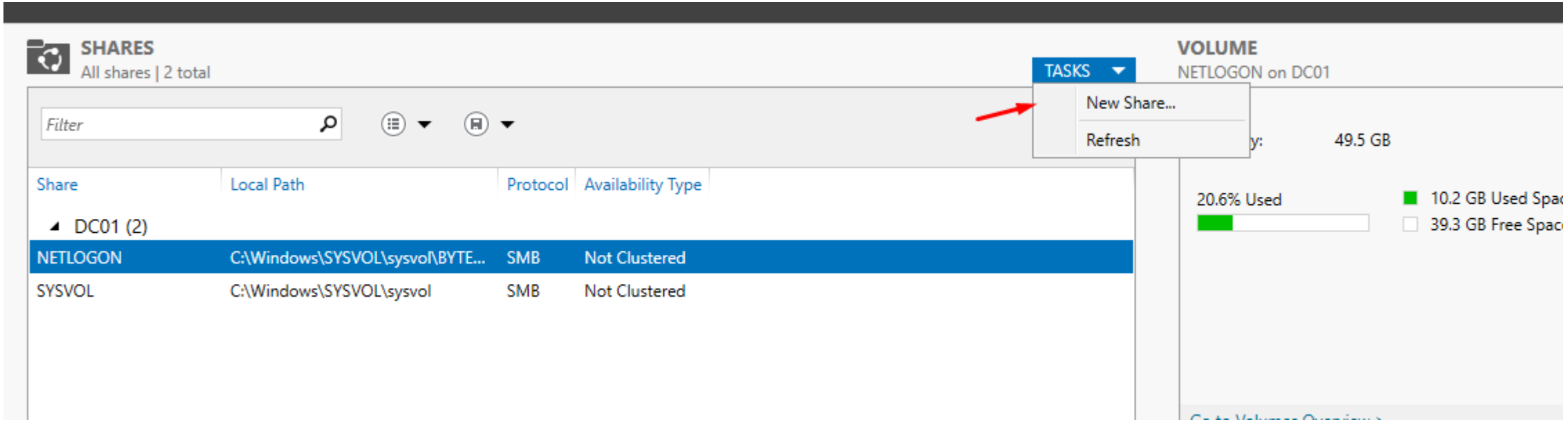
Creating Smb Share



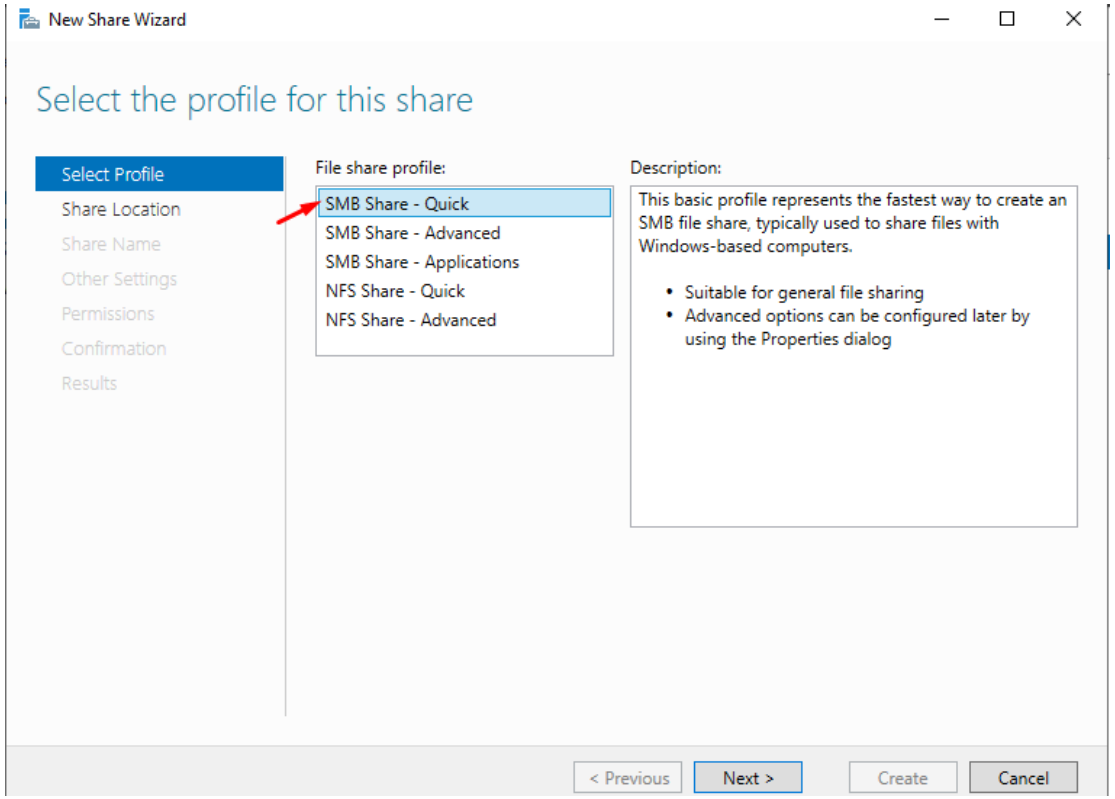
Lab Setup


Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
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

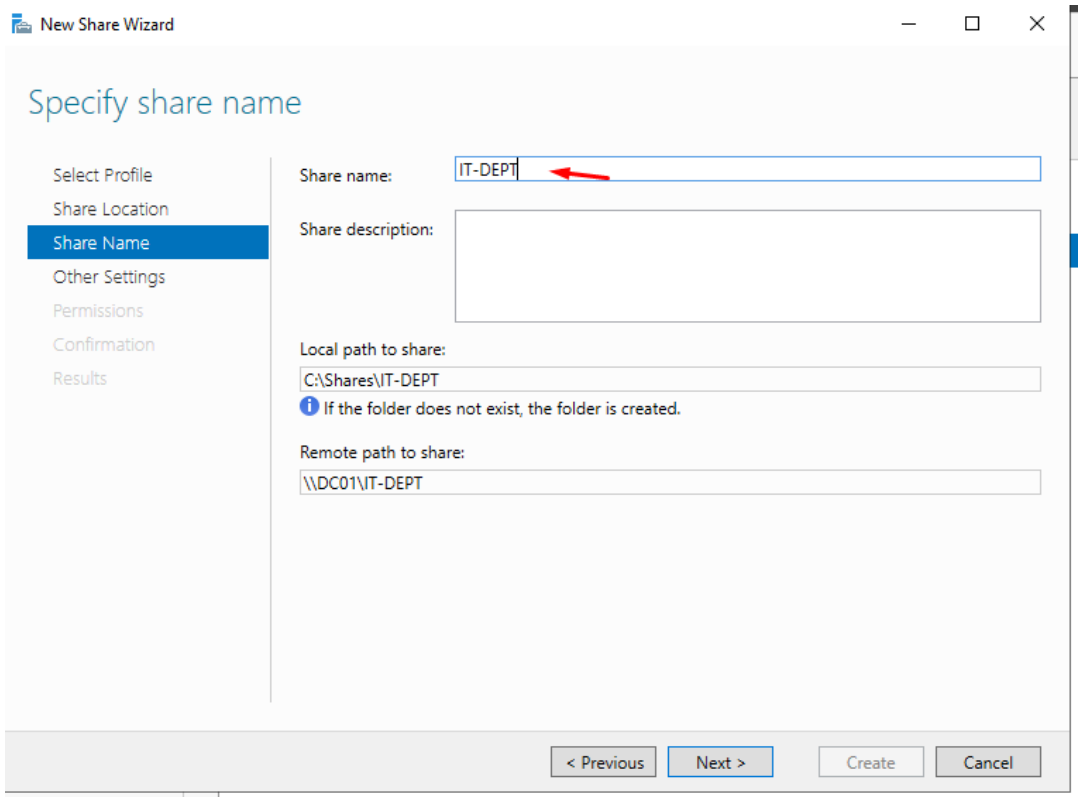
Lab Setup


SHARES
All shares | 2 total
TASKS
New Share...
Refresh
VOLUME
NETLOGON on DC01
Filter
Share
Local Path
Protocol
Availability Type
DC01 (2)
NETLOGON
C:\Windows\SYSVOL\sysvol\BYTE...
SMB
Not Clustered
SYSVOL
C:\Windows\SYSVOL\sysvol
SMB
Not Clustered
49.5 GB
20.6% Used
10.2 GB Used Spac
39.3 GB Free Spac

Lab Setup

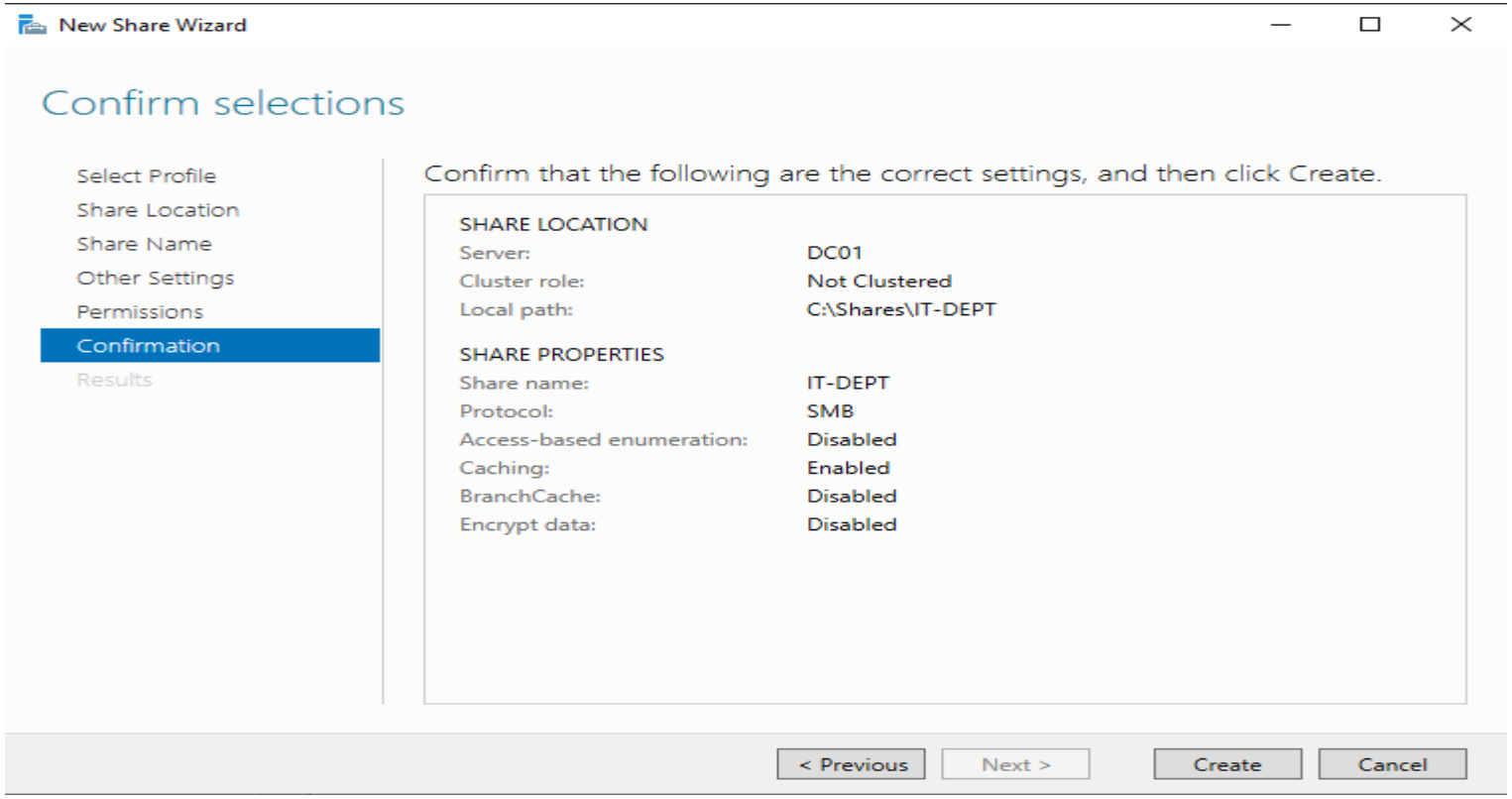

New Share Wizard
Select the profile for this share
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
File share profile:
SMB Share - Quick
SMB Share - Advanced
SMB Share - Applications
NFS Share - Quick
NFS Share - Advanced
Description:
This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.
Suitable for general file sharing
Advanced options can be configured later by using the Properties dialog
< Previous
Next >
Create
Cancel

Lab Setup


New Share Wizard
Specify share name
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
Share name:
IT-DEPT
Share description:
Local path to share:
C:\Shares\IT-DEPT
If the folder does not exist, the folder is created.
Remote path to share:
\\DC01\IT-DEPT
< Previous
Next >
Create
Cancel

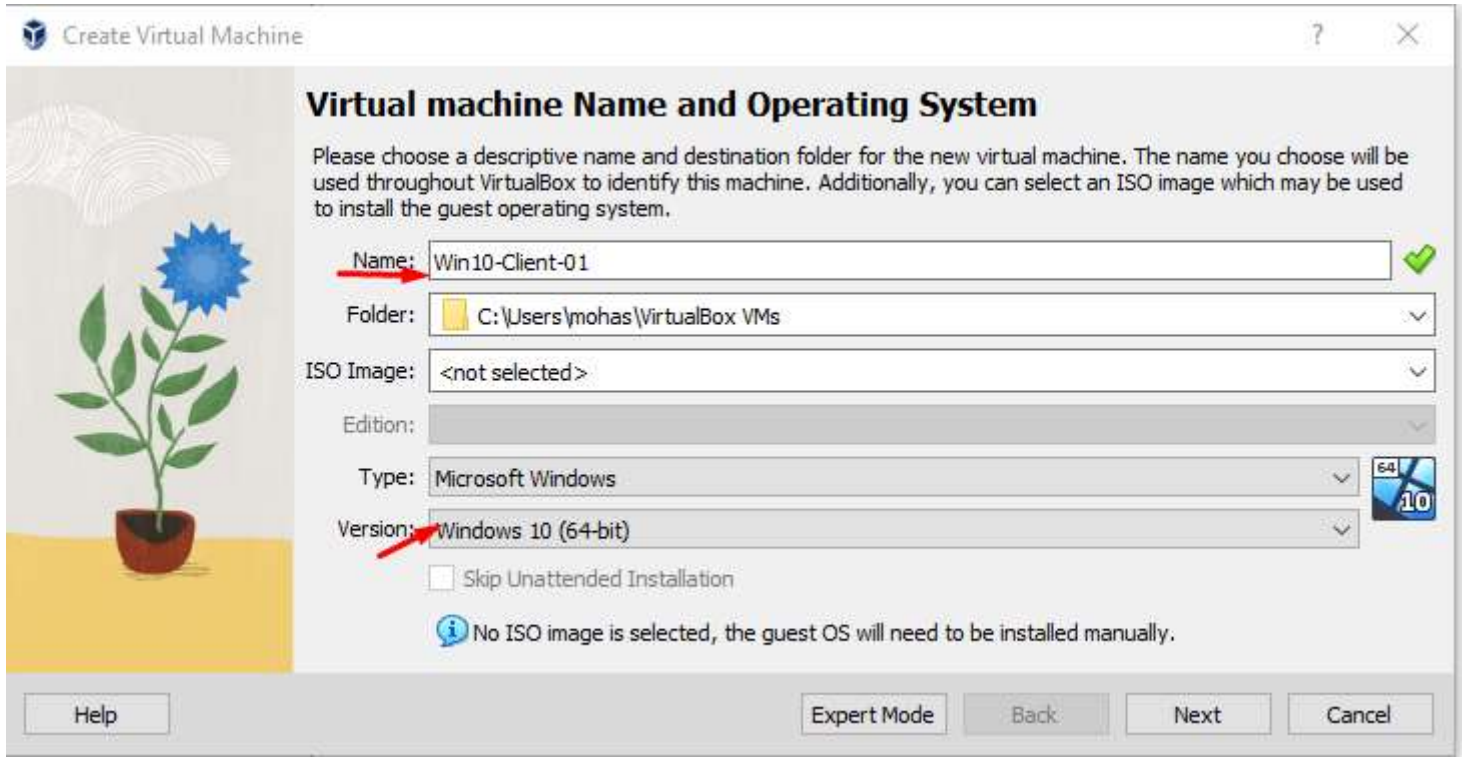
Lab Setup

Next > Next > Create



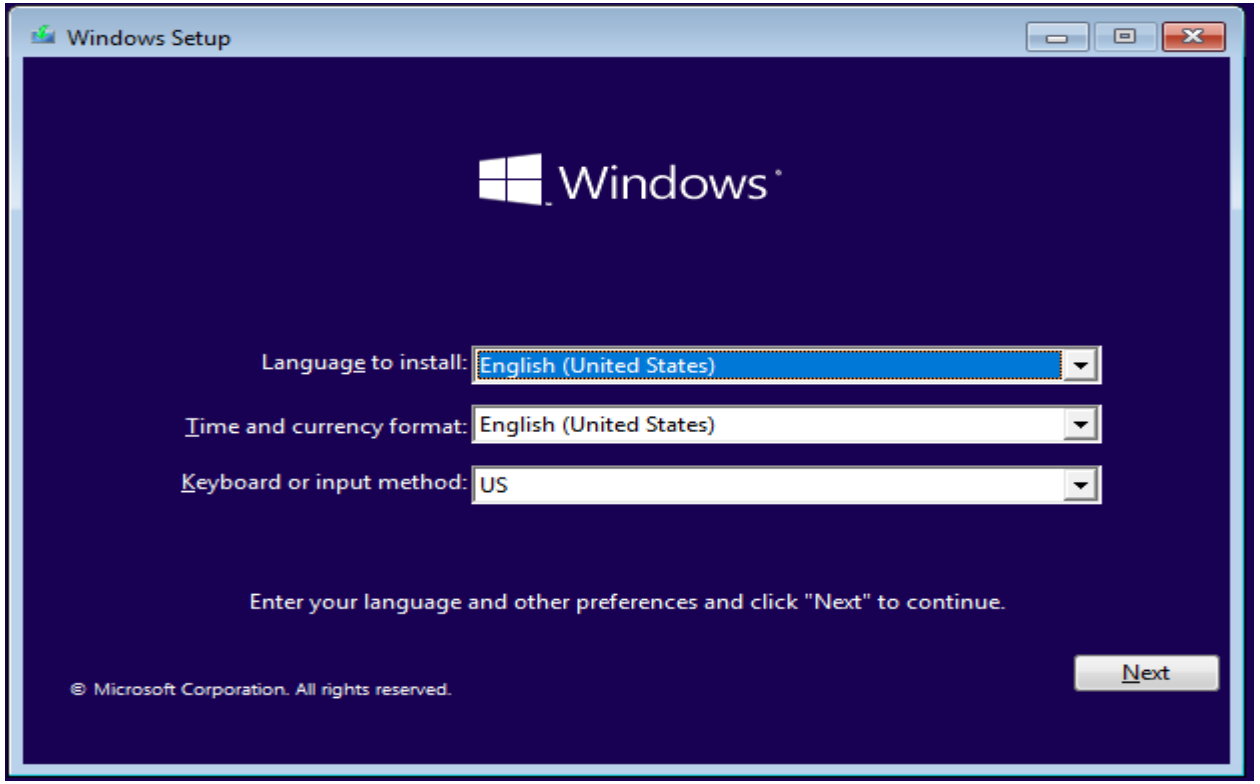
Lab Setup

Installing Windows 10 Enterprise edition



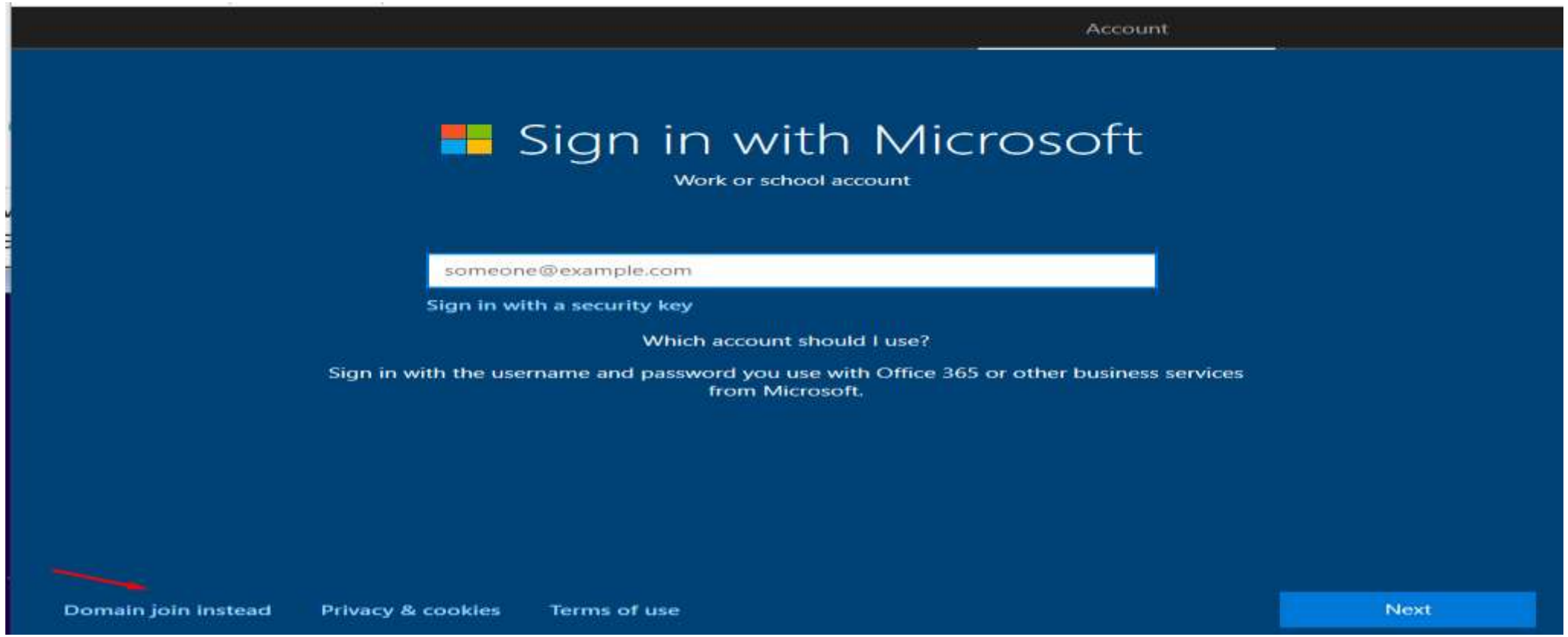
Lab Setup

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



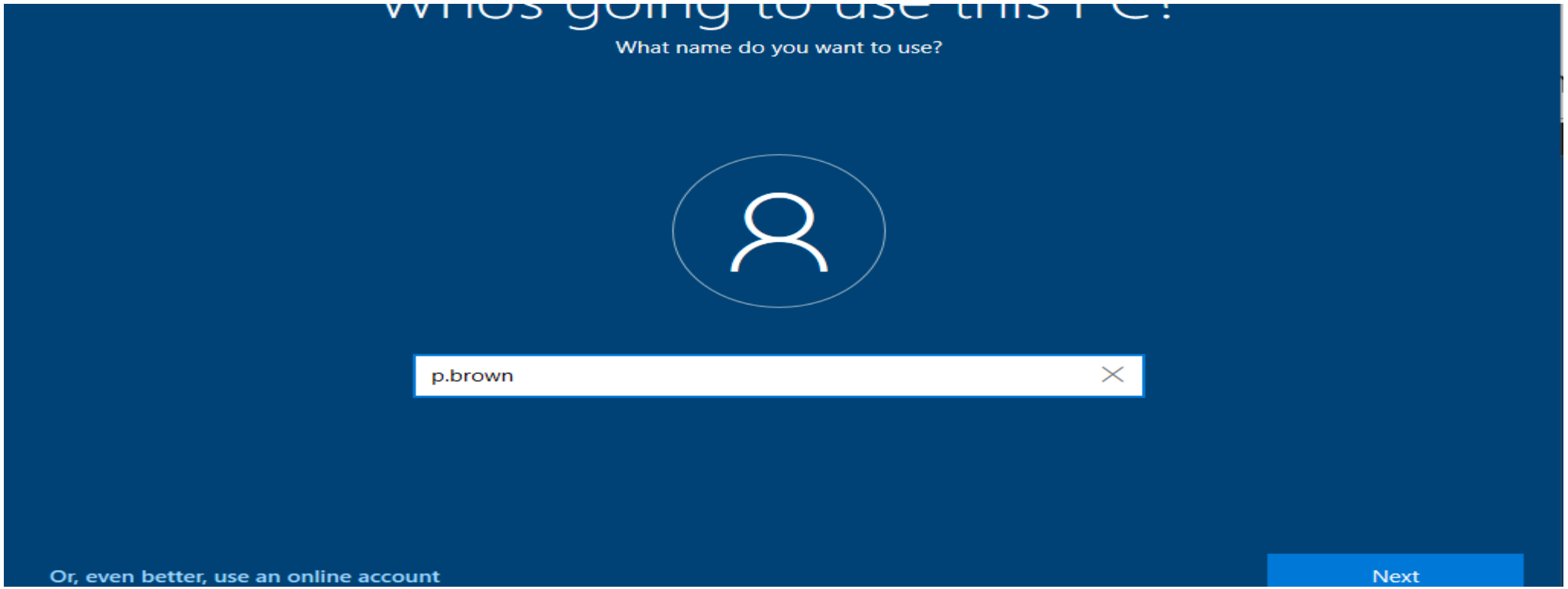
Lab Setup

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



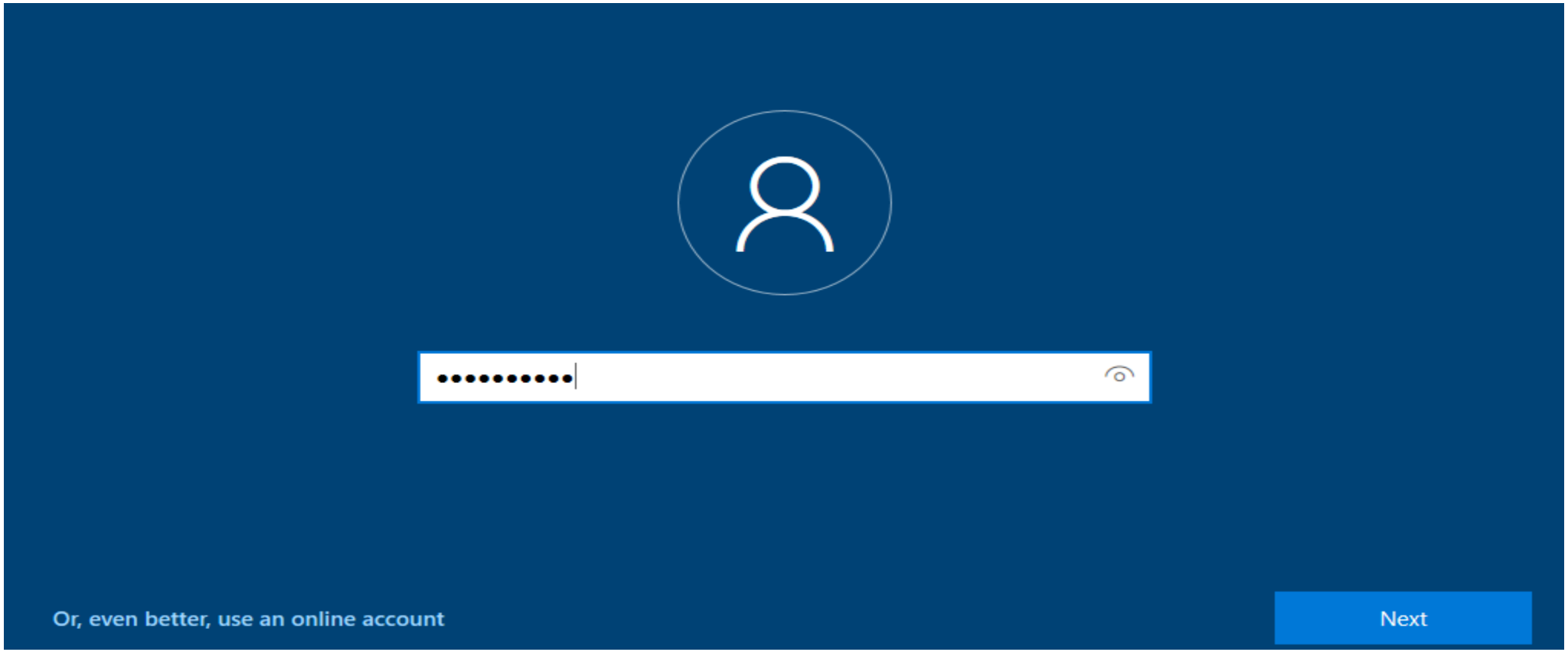
Lab Setup

Creating User



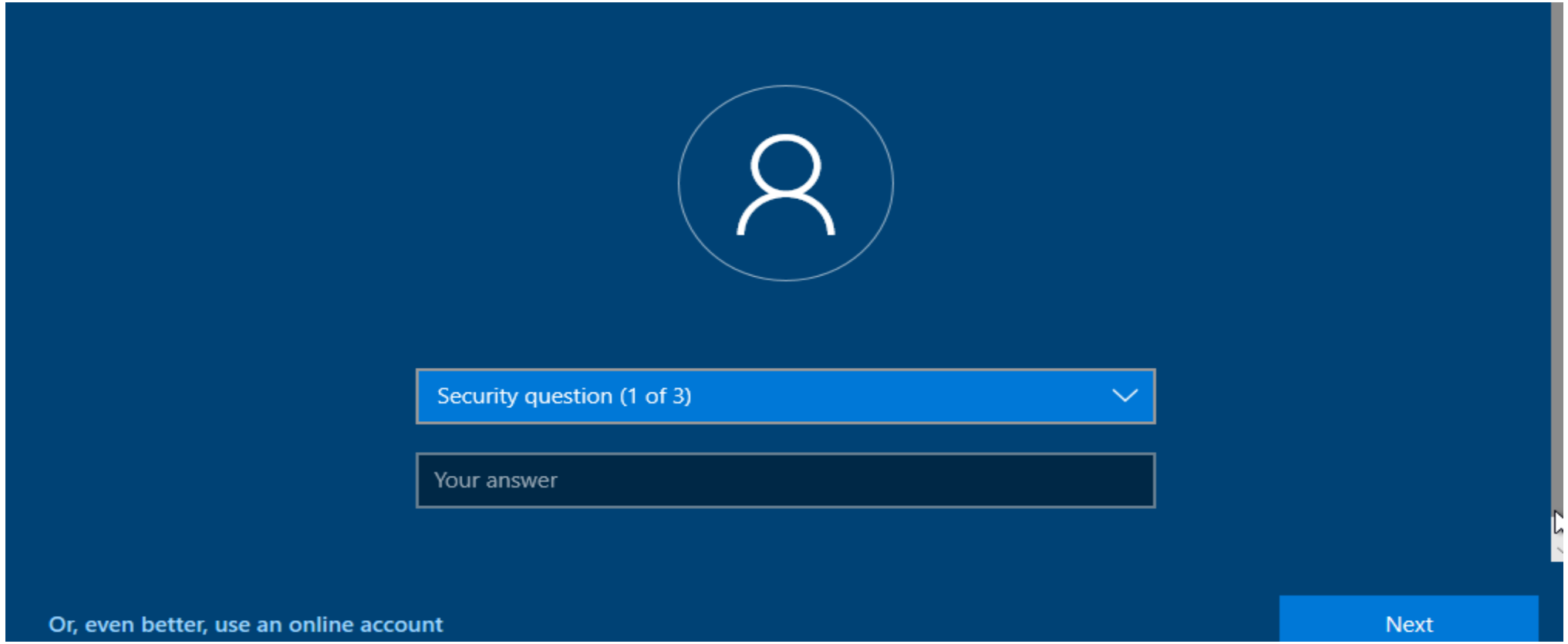
Lab Setup

Create a memorable Password and Confirm it



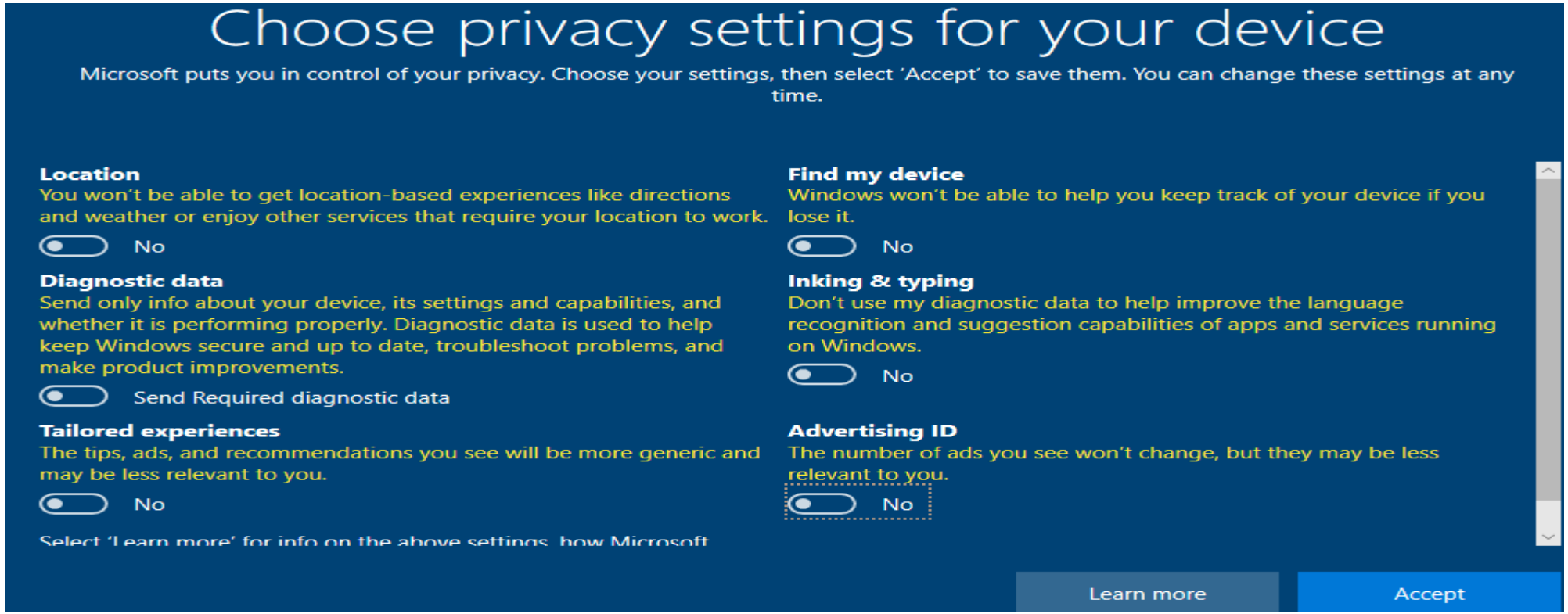
Lab Setup

Select 3 memorable Security question and move on



Lab Setup

Accept

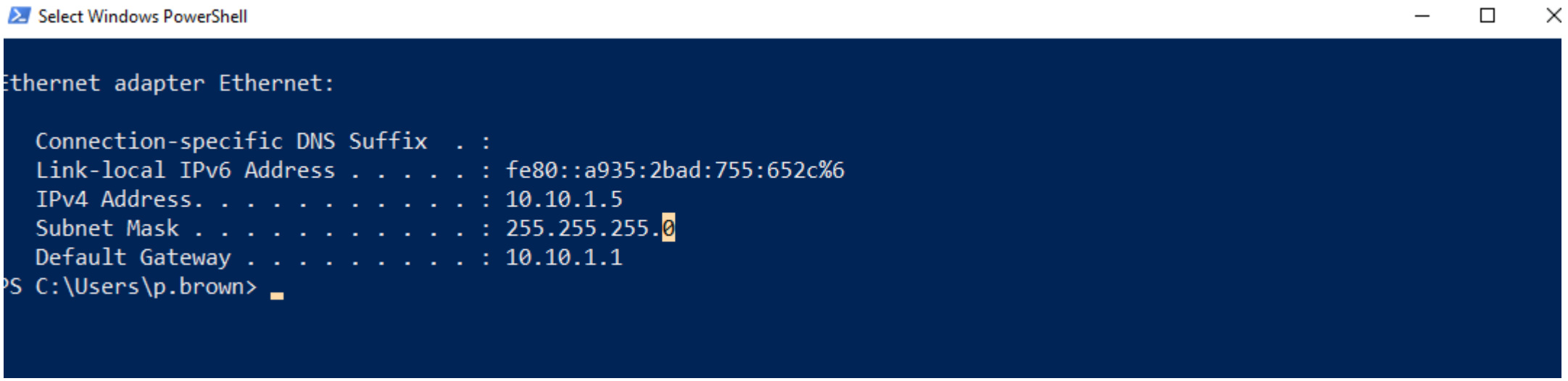


Lab Setup

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

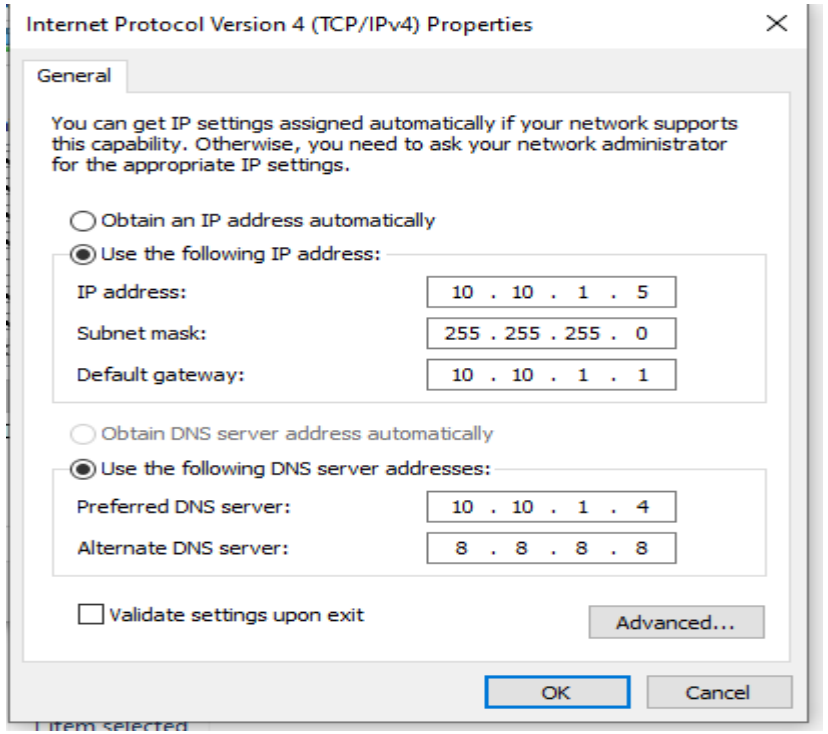
Lab Setup

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



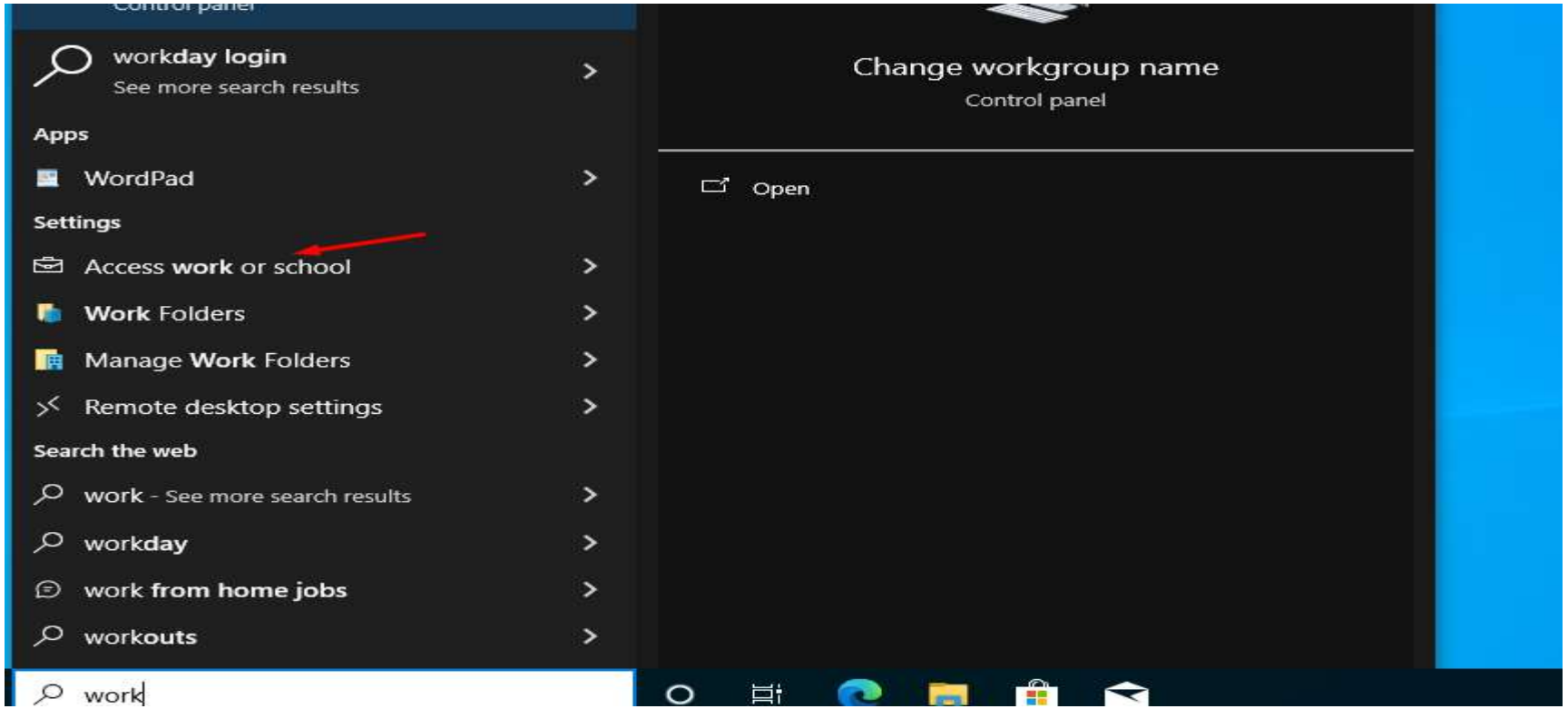
Lab Setup

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



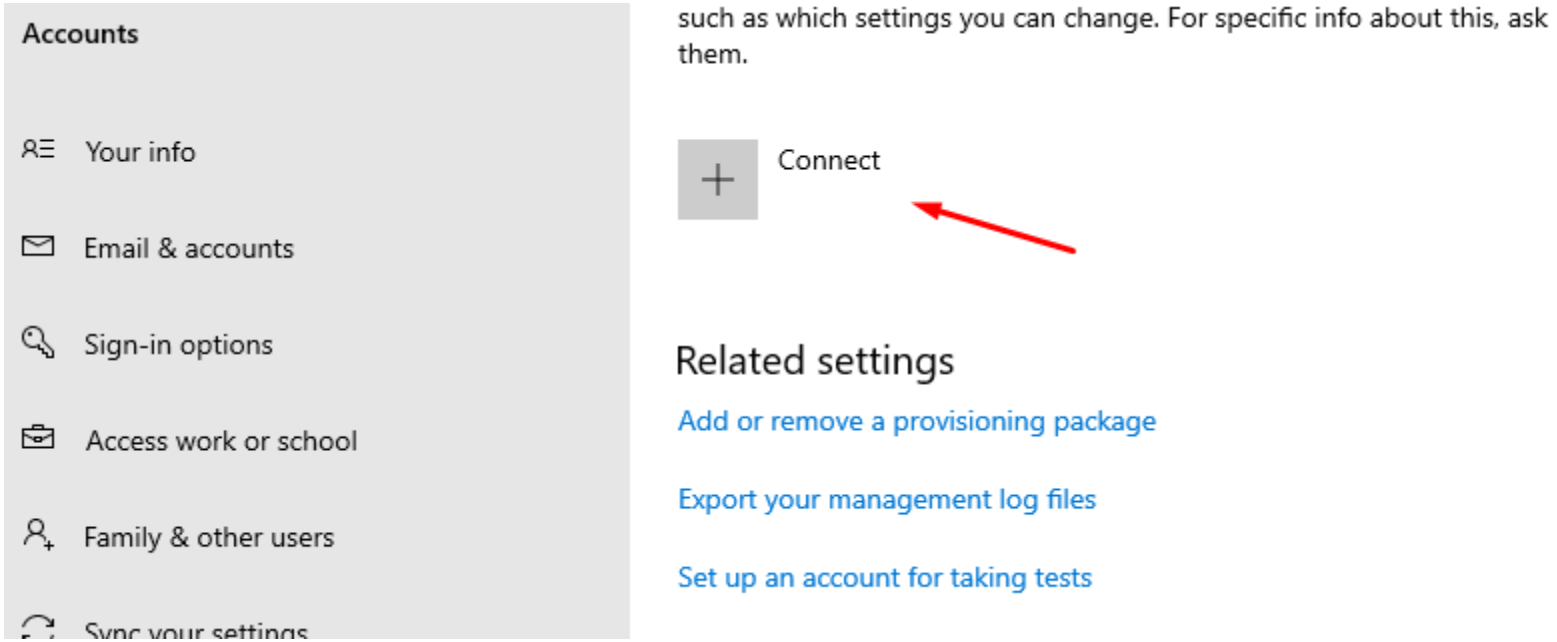
Lab Setup

Joining the Client, search for work or school

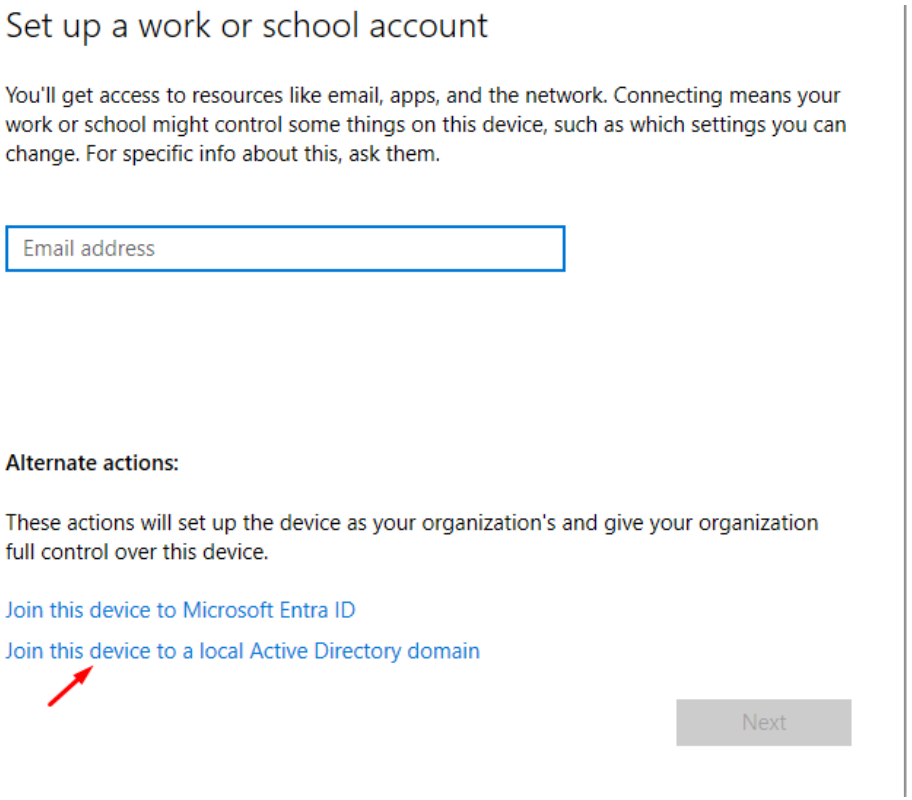


Lab Setup

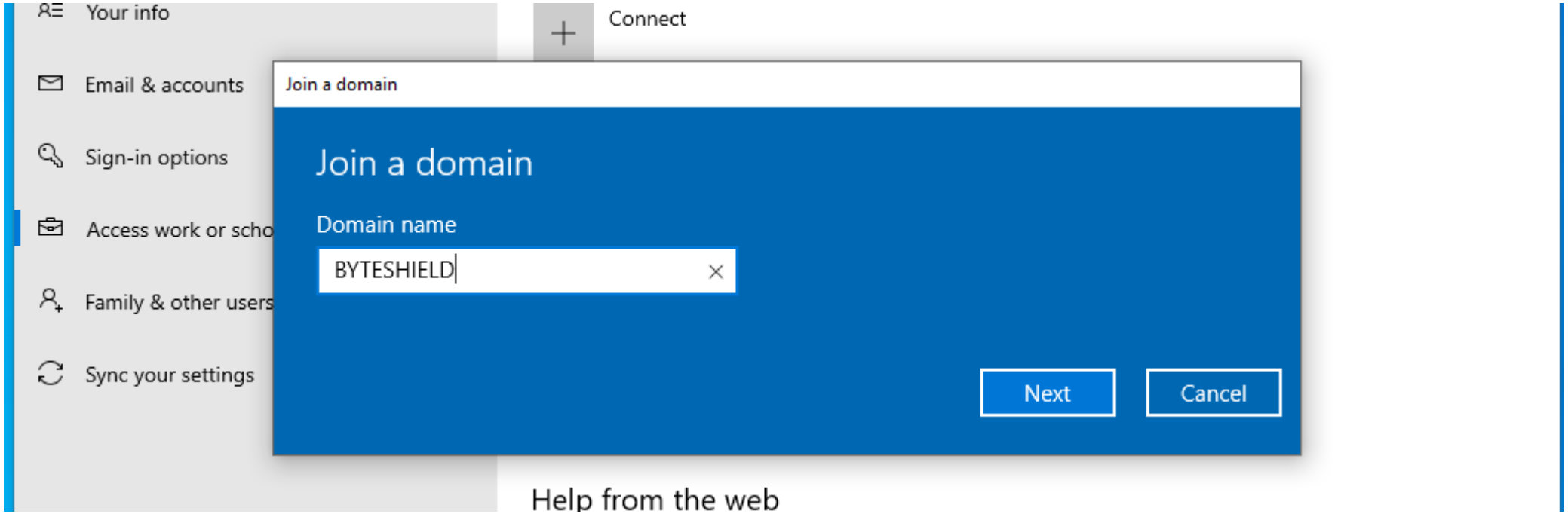
Connect



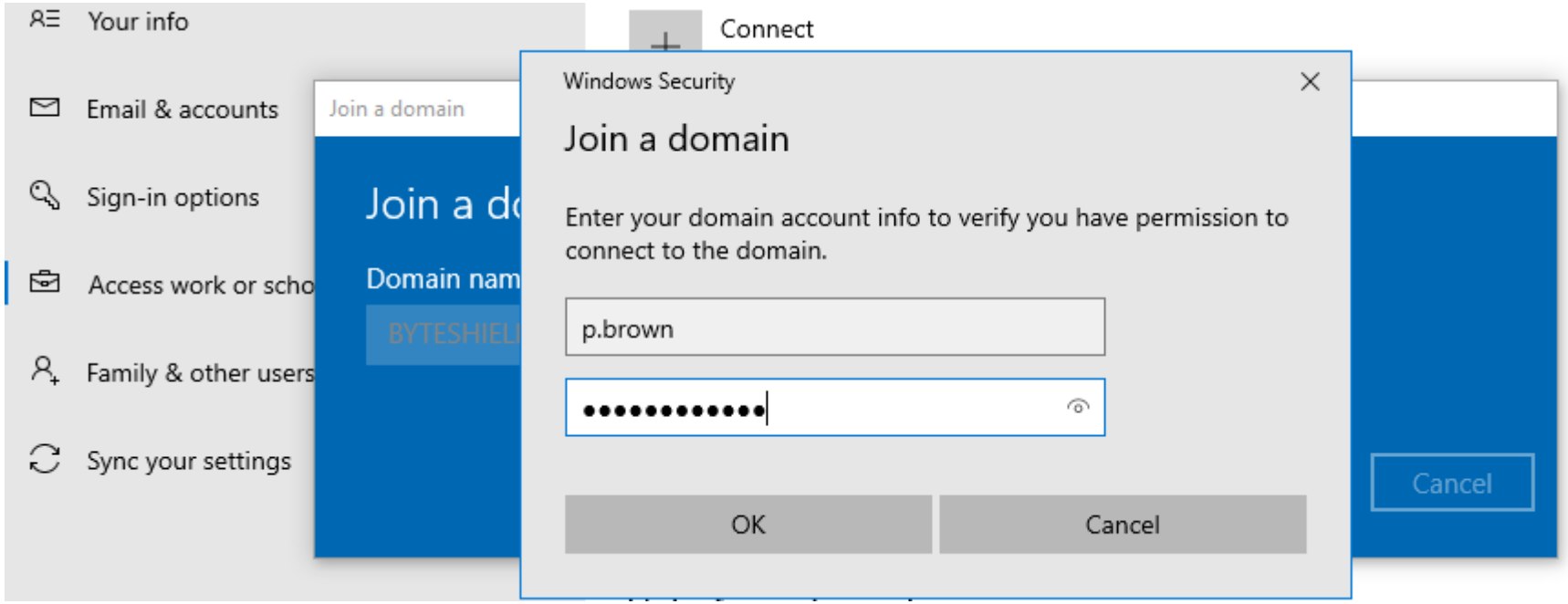
Lab Setup


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.
Email address
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

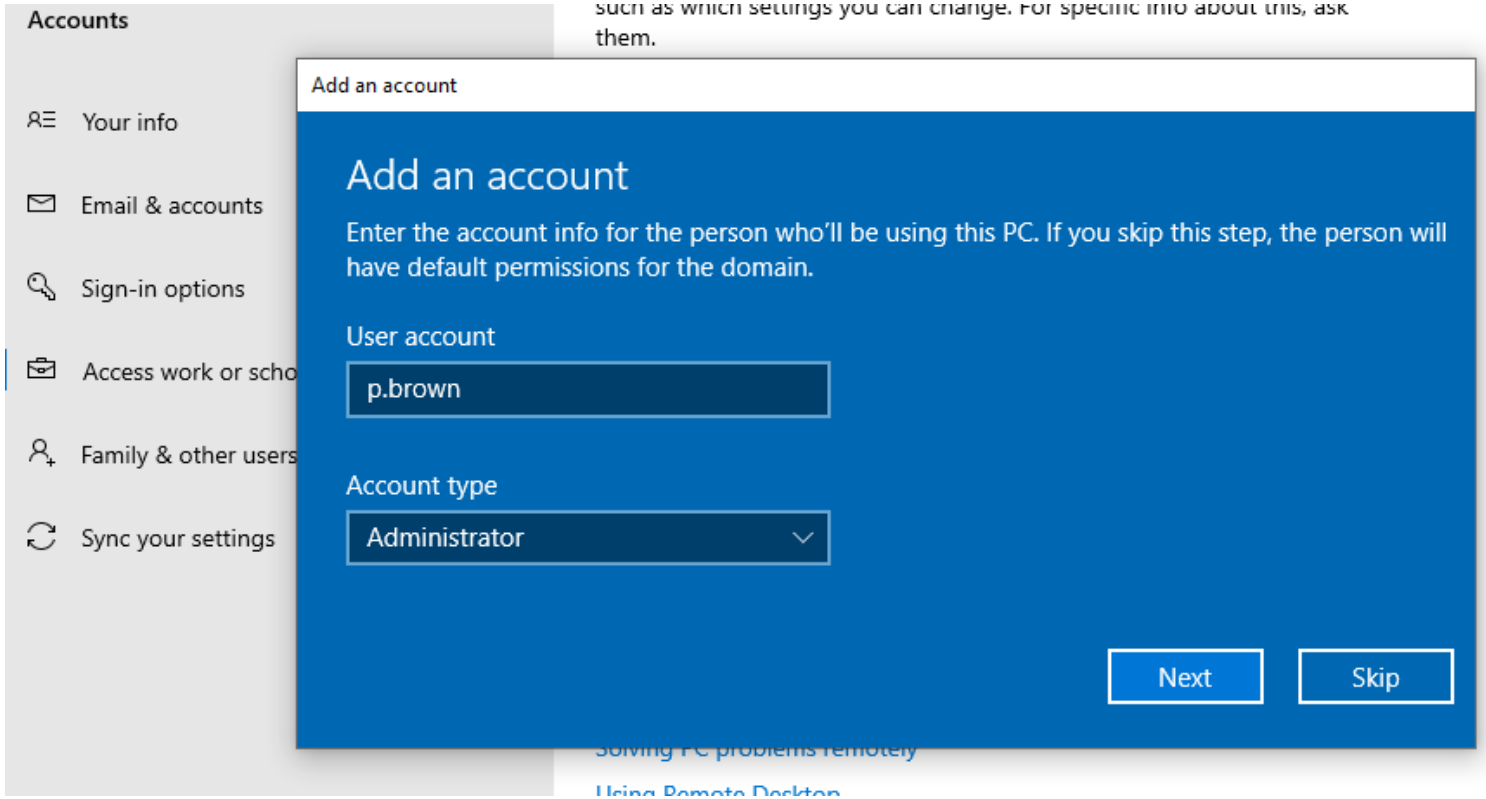
Lab Setup


Your info
Email & accounts
Sign-in options
Access work or scho
Family & other users
Sync your settings
Connect
Join a domain
Join a domain
Domain name
BYTESHIELD
Next
Cancel
Help from the web

Lab Setup

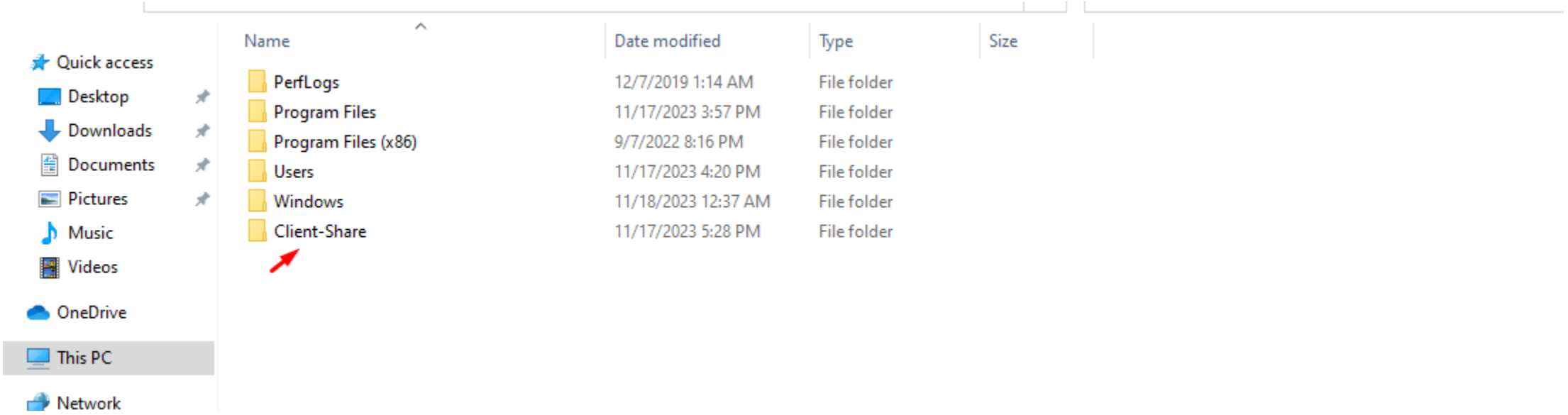

Your info
Email & accounts
Sign-in options
Access work or scho
Family & other users
Sync your settings
Connect
Join a domain
Join a d
Domain nam
Cancel
Windows Security
Join a domain
Enter your domain account info to verify you have permission to connect to the domain.
p.brown
OK
Cancel

Lab Setup


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

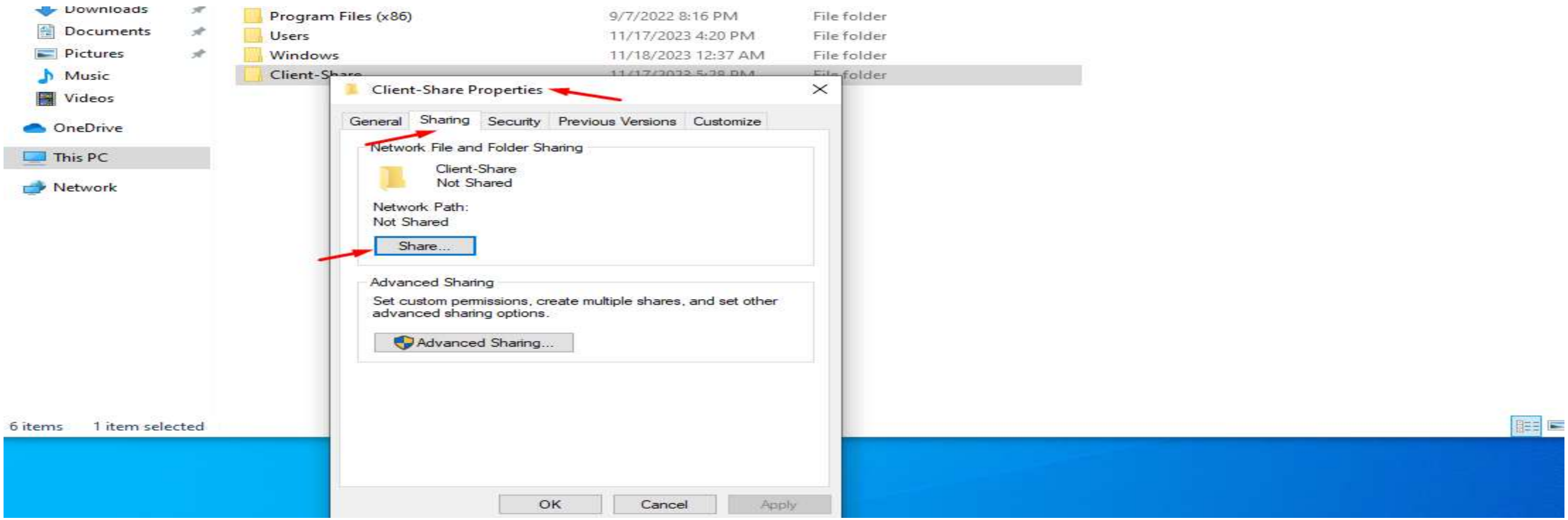
Lab Setup

Creating Smb Share on Windows Client



Lab Setup

Right Click and go the Properties and share it



Lab Setup

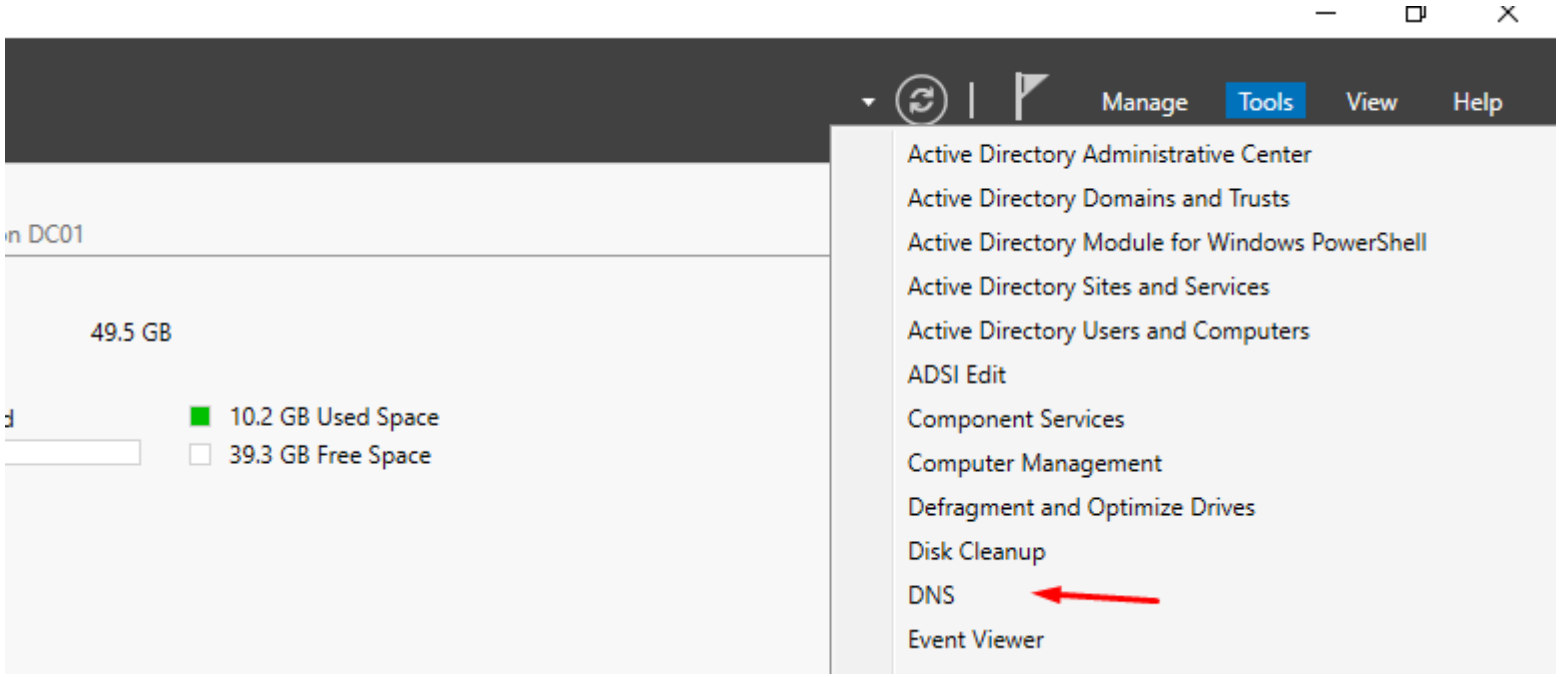
Now we are done setting up Win10-Client-01 Machine

Instruction

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

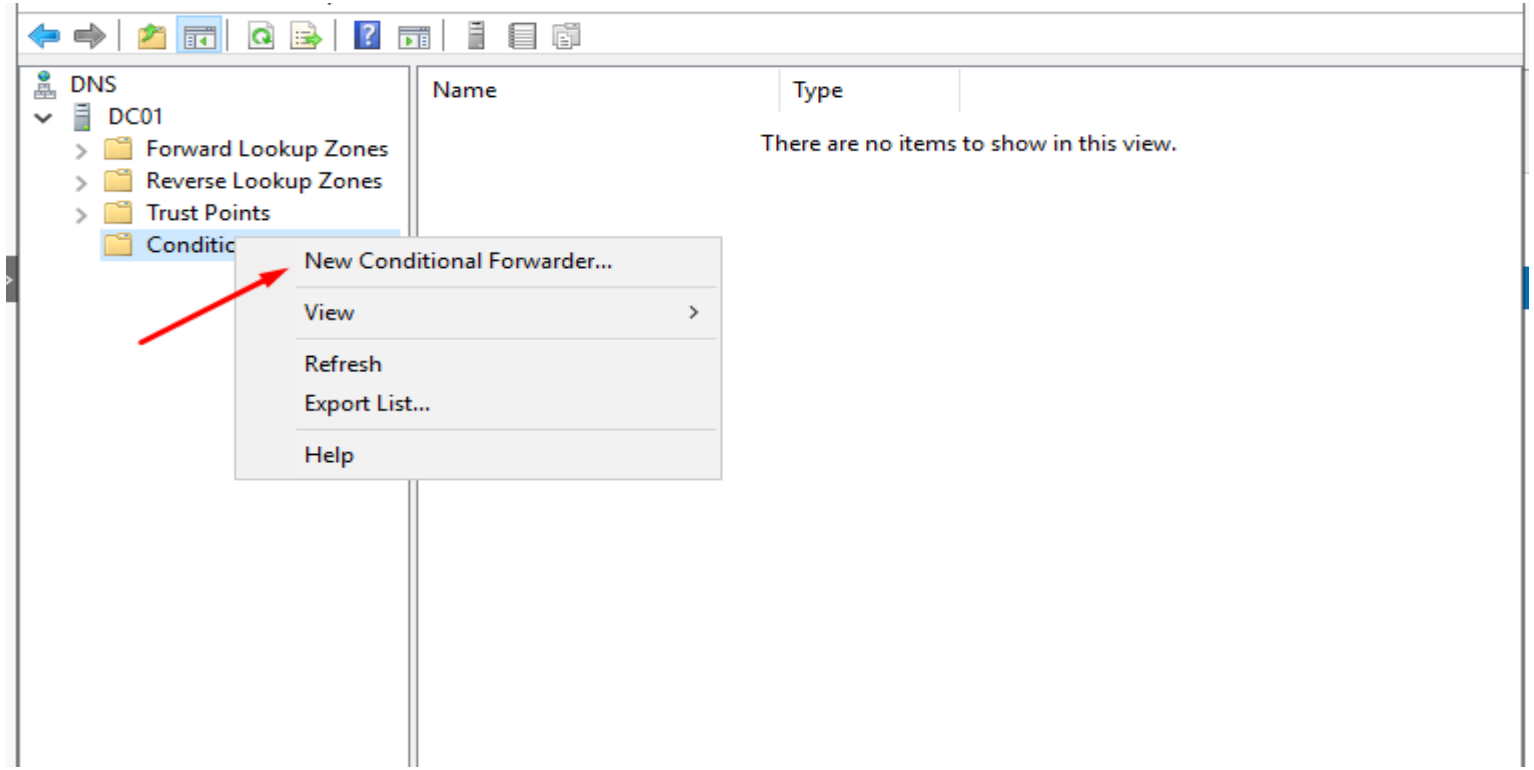
Lab Setup

Setting up DNS conditional forwarders for both side



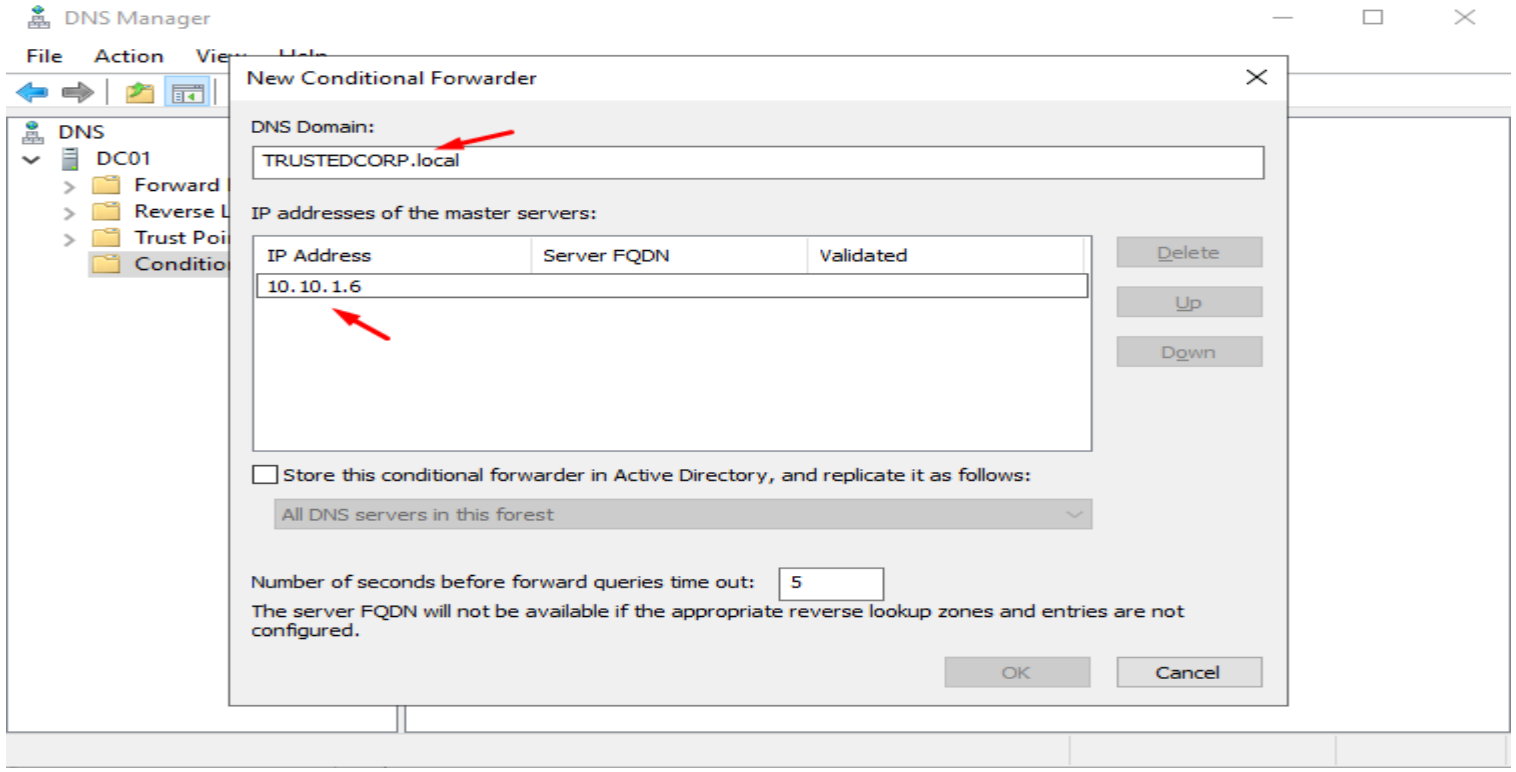
Lab Setup

Adding Forwarder



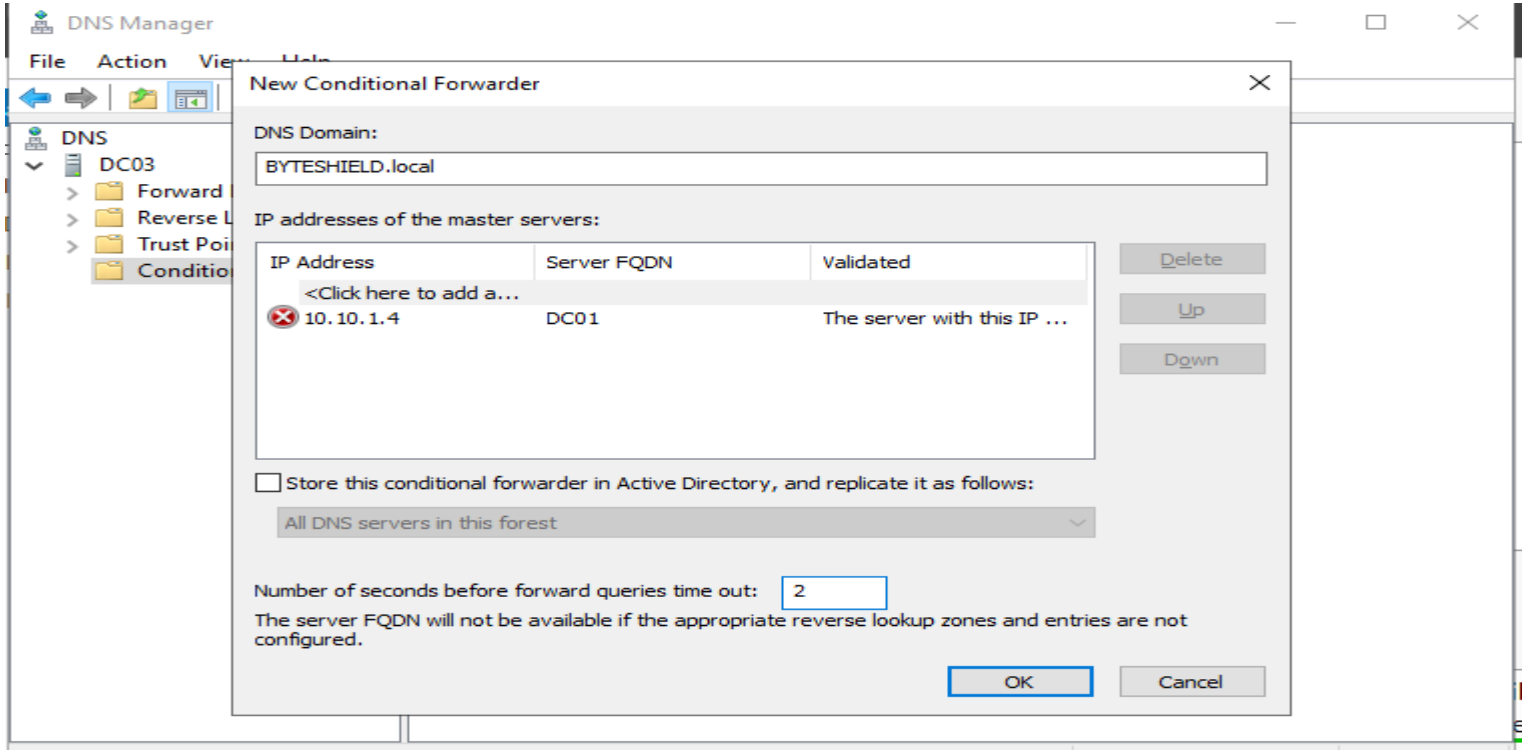
Lab Setup

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
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 = 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:
```

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,

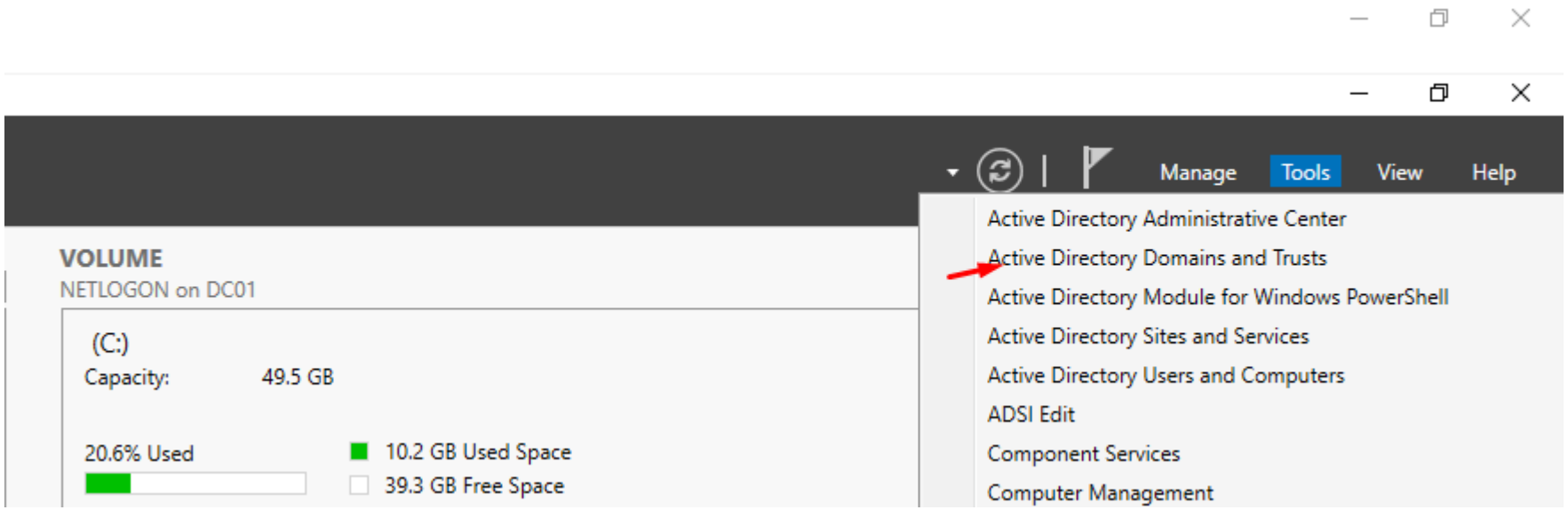
INSTRUCTION

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

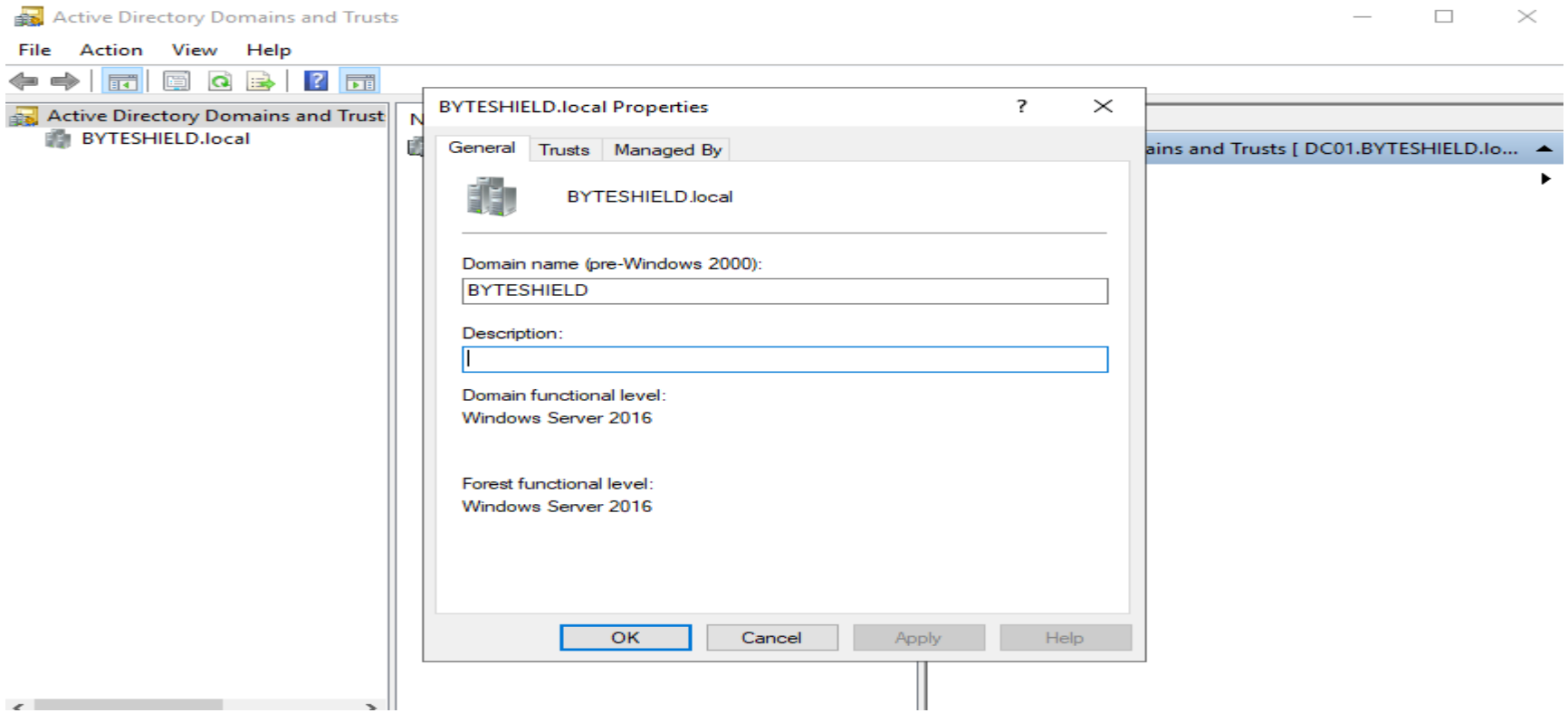
Lab Setup

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



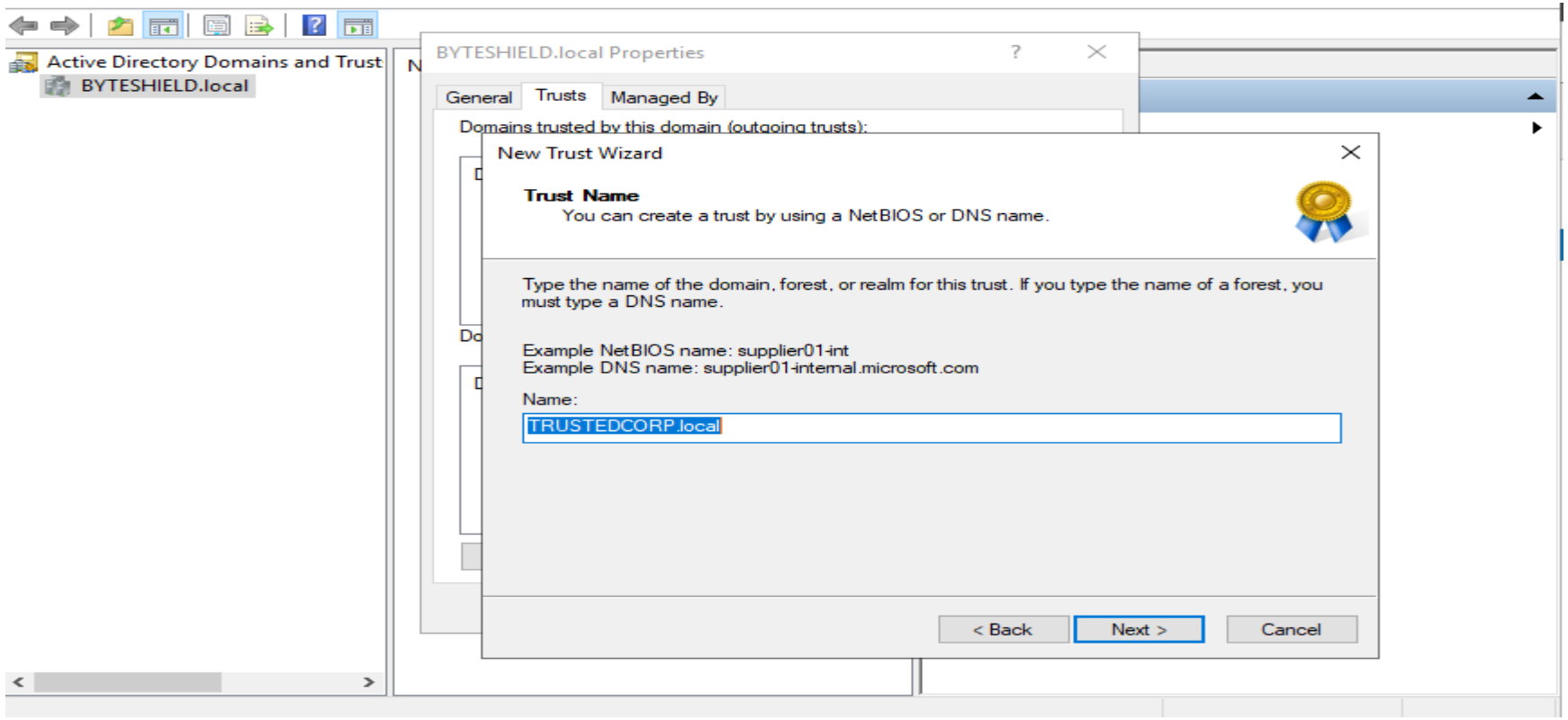
La Setup

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



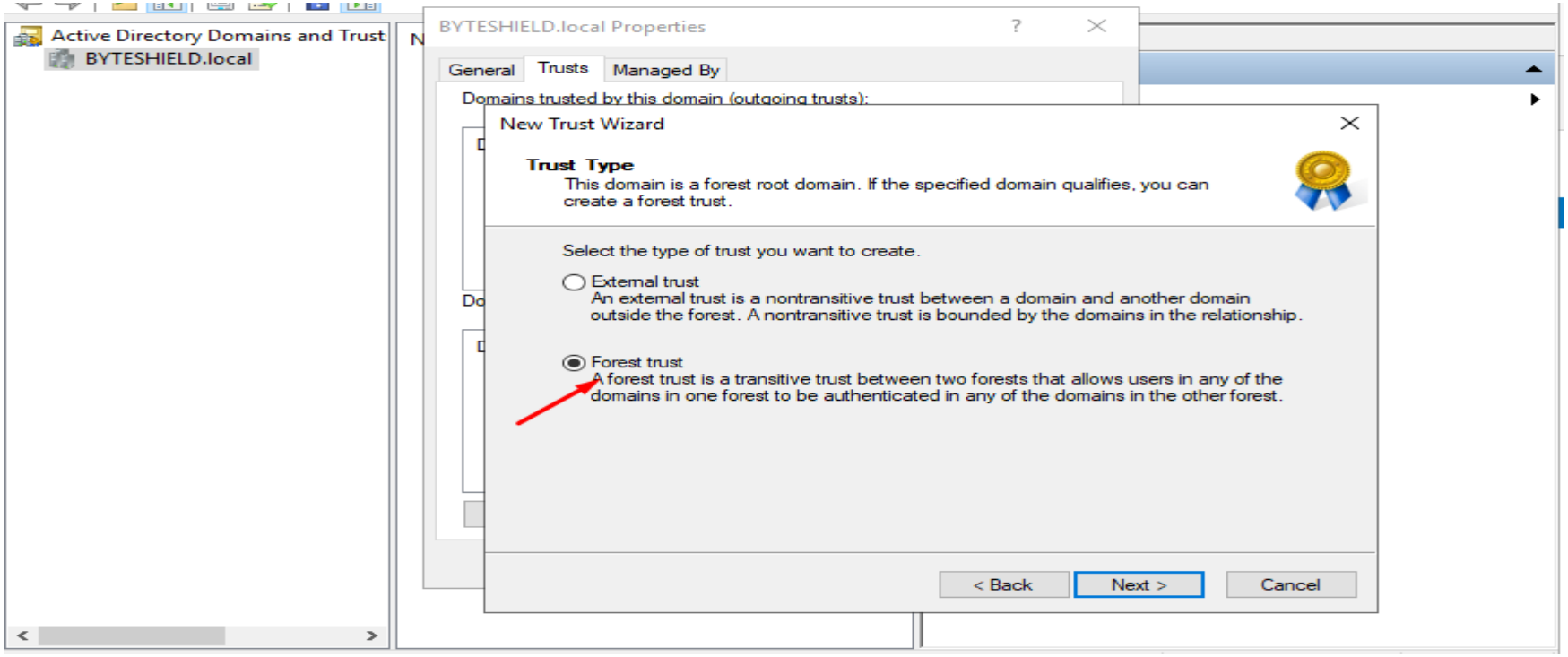
Lab Setup

Enter the Domain



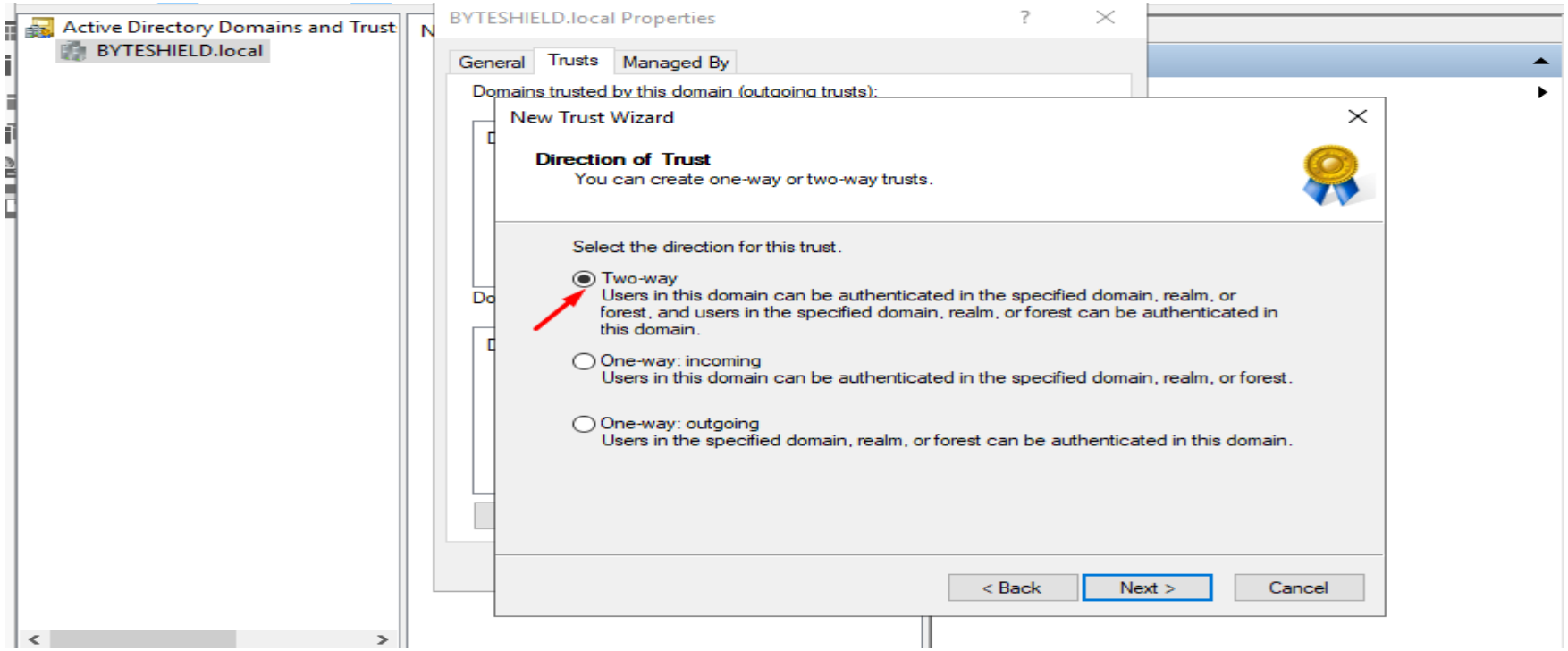
Lab Setup

Forest trust

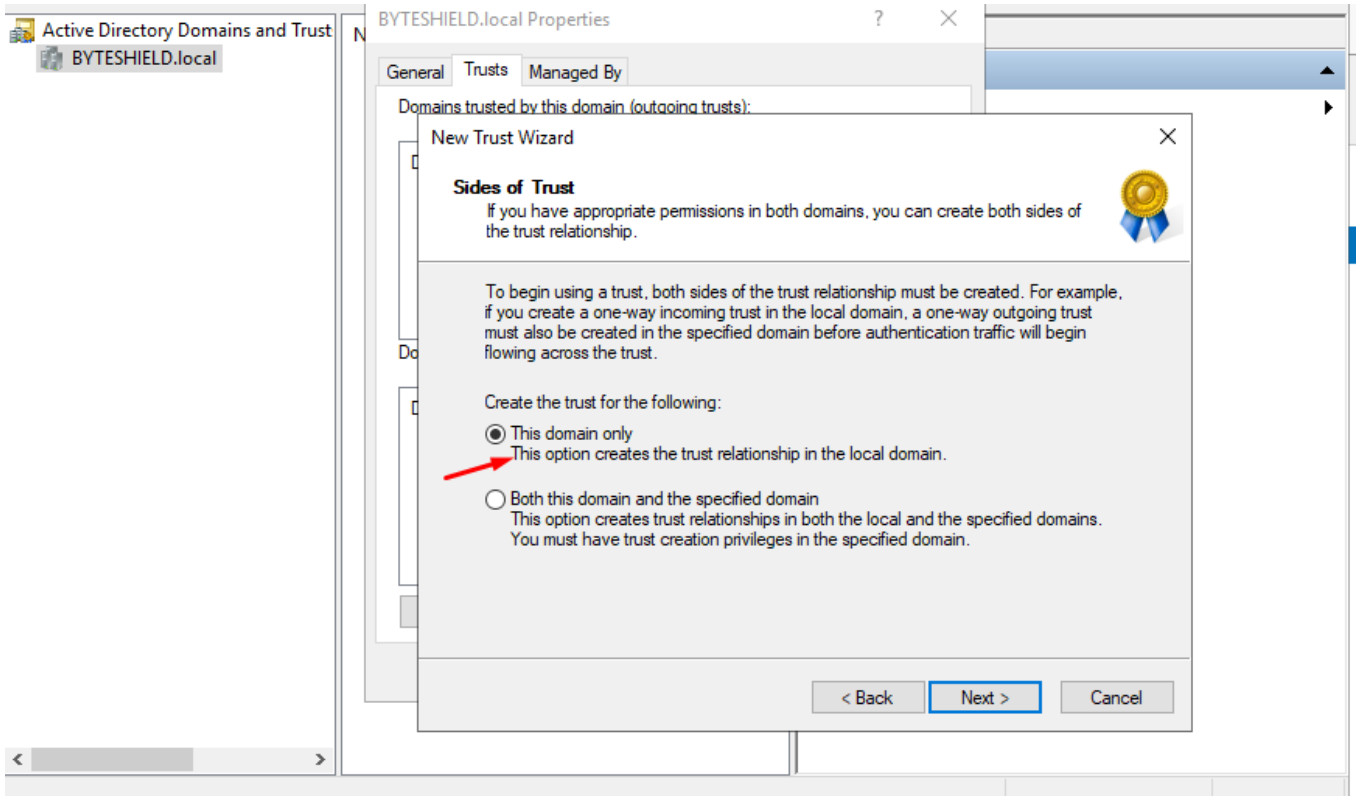


Lab Setup

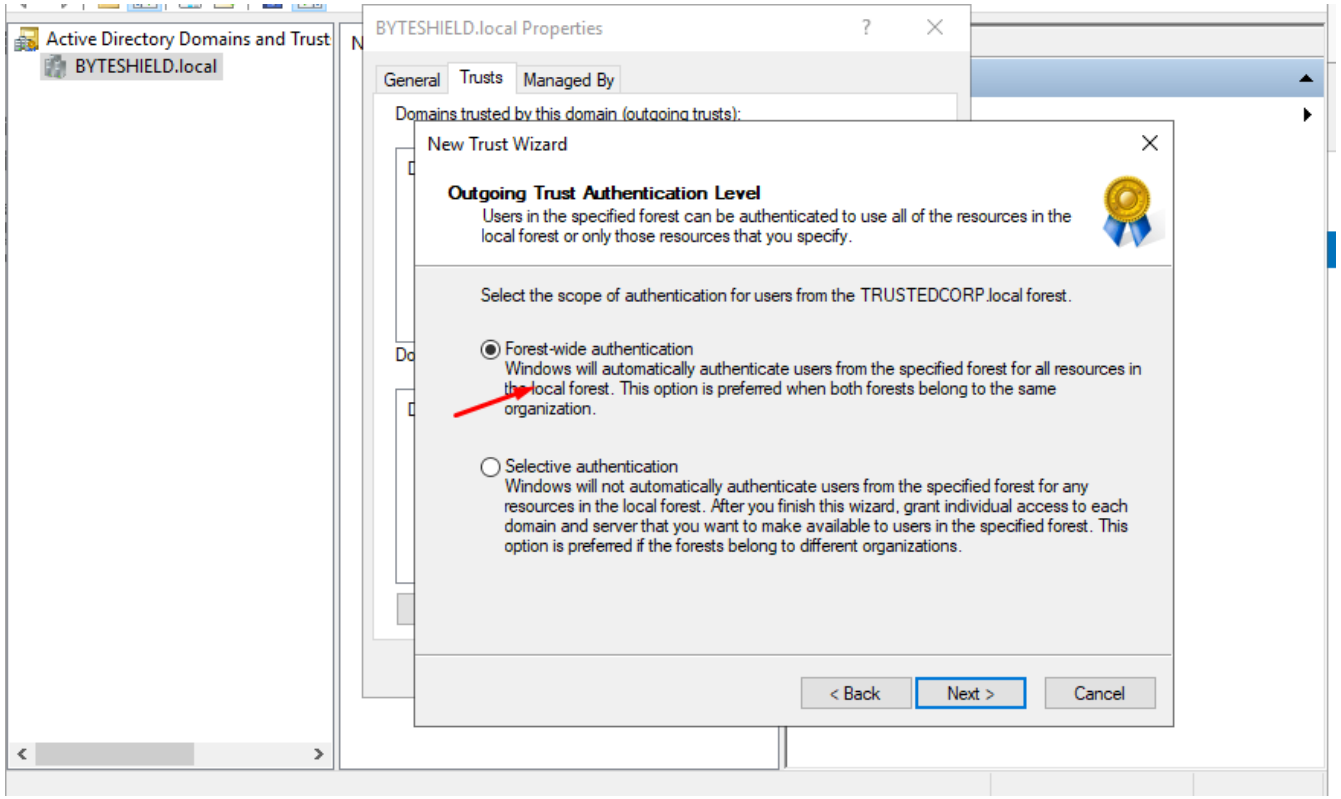
Bidirectional Trust



Lab Setup

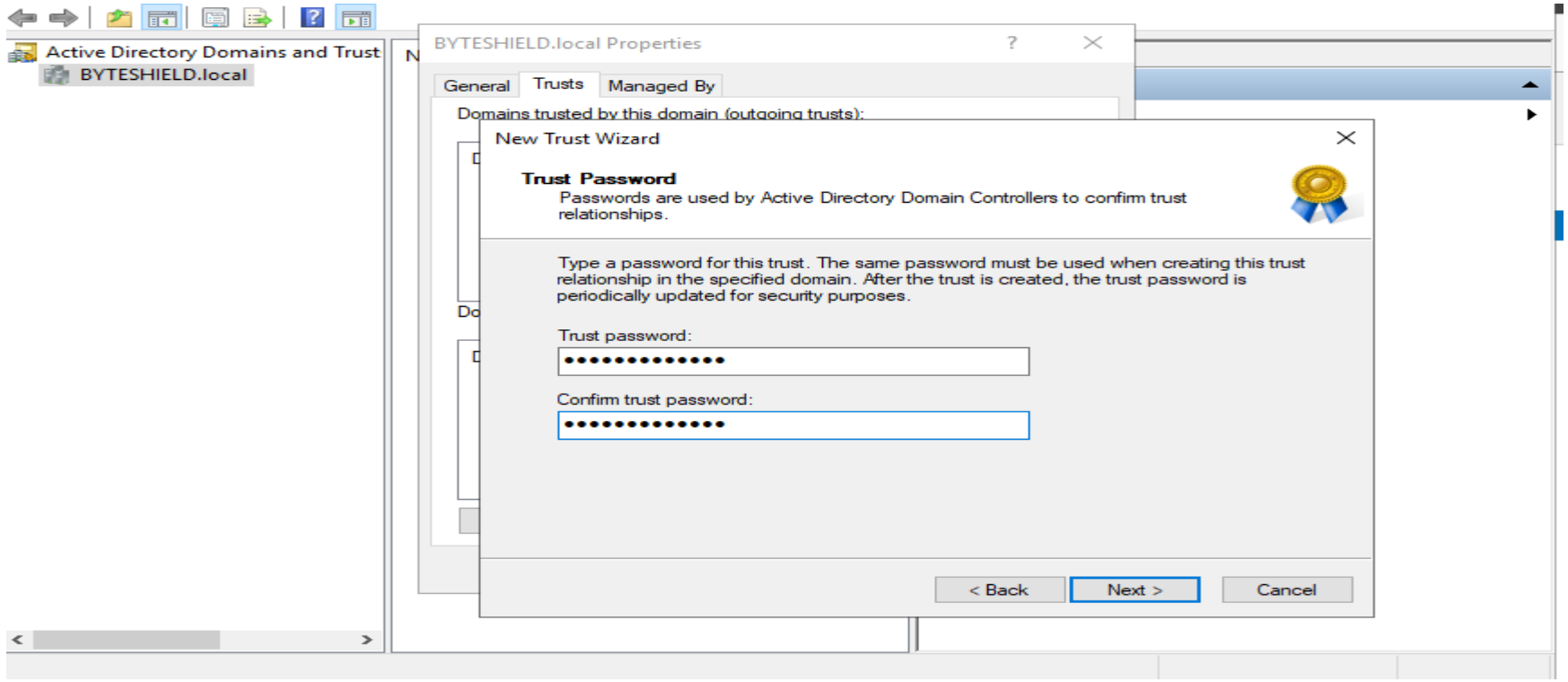

Active Directory Domains and Trust
BYTESHIELD.local
BYTESHIELD.local Properties
General
Trusts
Managed By
Domains trusted by this domain (outgoing trusts):
New Trust Wizard
Sides of Trust
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.
To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.
Create the trust for the following:
This domain only
This option creates the trust relationship in the local domain.
Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains.
You must have trust creation privileges in the specified domain.
< Back
Next >
Cancel

Lab Setup


Active Directory Domains and Trust
BYTESHIELD.local
BYTESHIELD.local Properties
General
Trusts
Managed By
Domains trusted by this domain (outgoing trusts):
New Trust Wizard
Outgoing Trust Authentication Level
Users in the specified forest can be authenticated to use all of the resources in the local forest or only those resources that you specify.
Select the scope of authentication for users from the TRUSTEDCORP.local forest.
Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.
Selective authentication
Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you finish this wizard, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.
< Back
Next >
Cancel

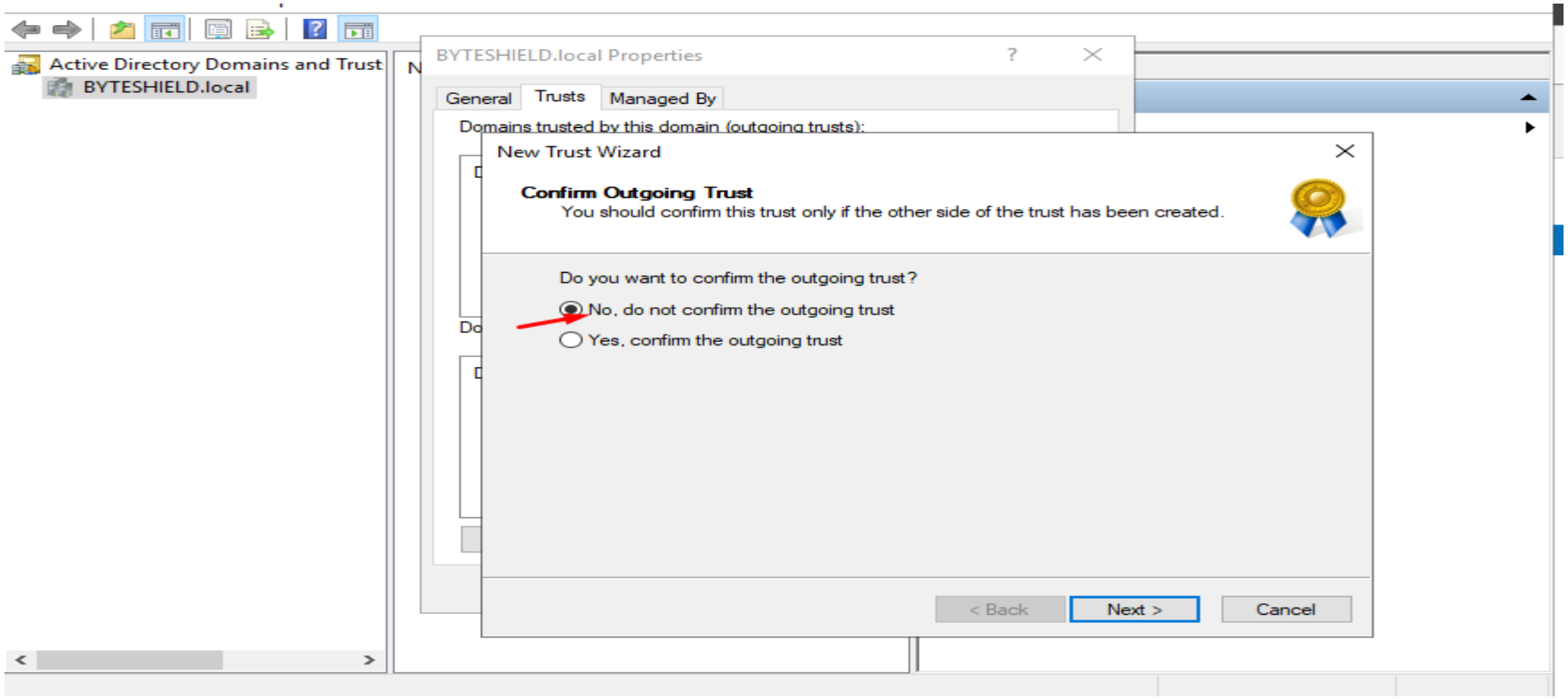
Lab Setup

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



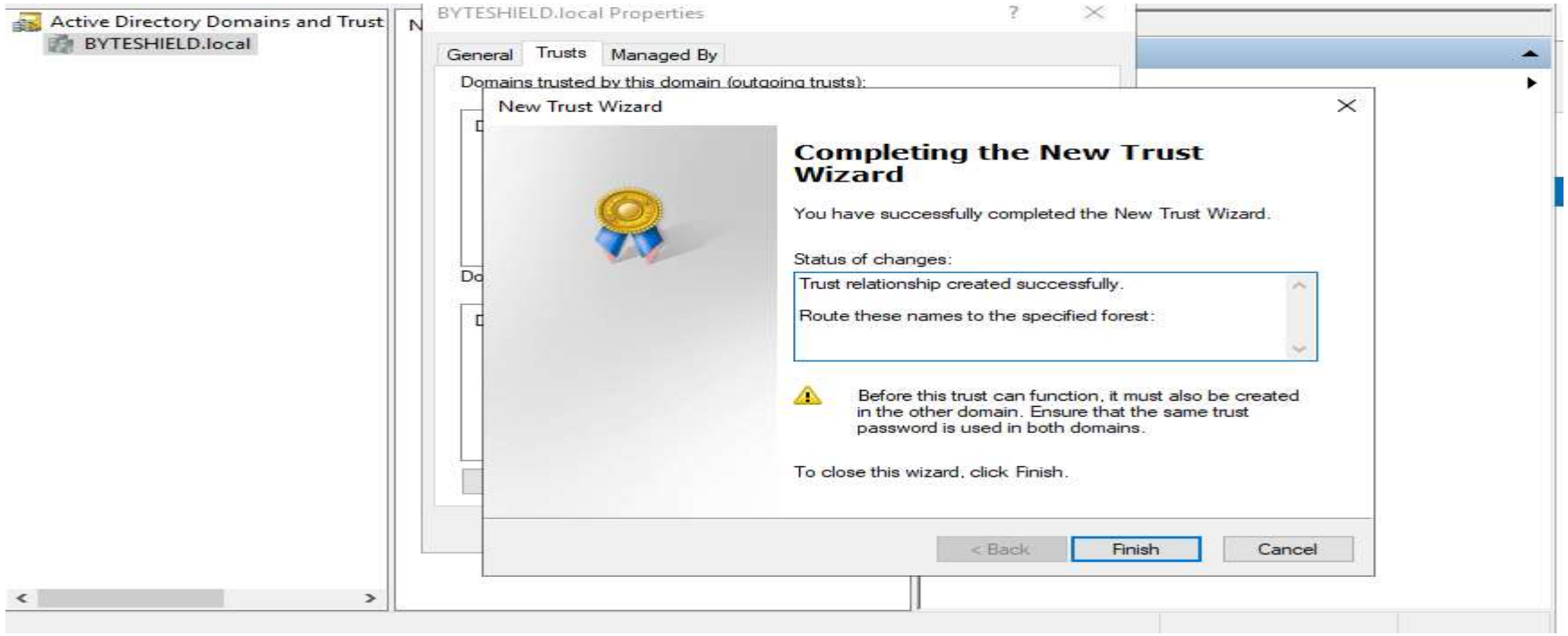
Lab Setup

Next > Next



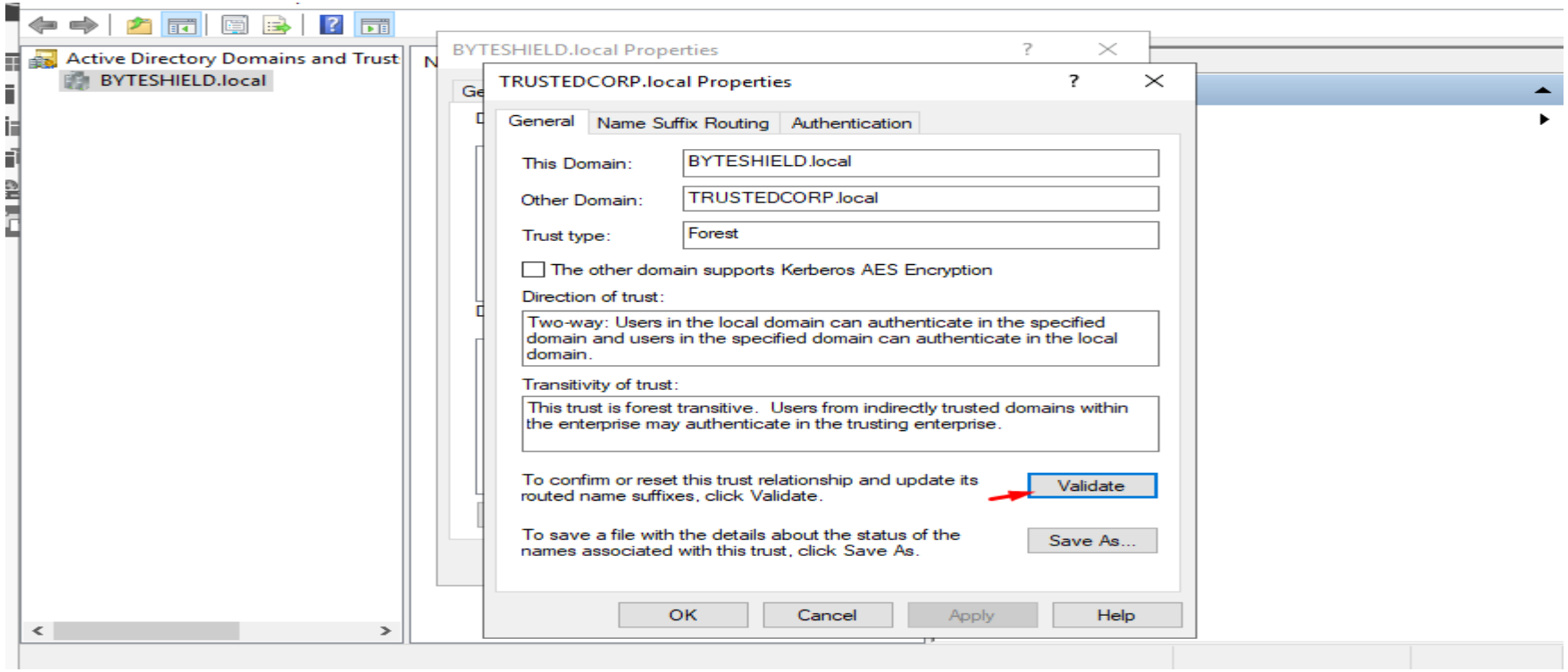
Lab Setup

Do the same on the other side



Lab Setup

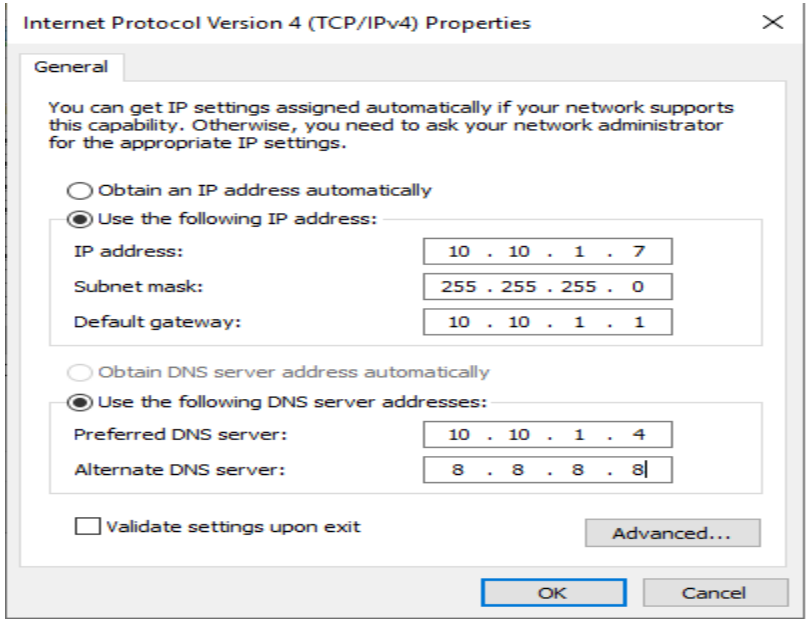
Now validate outgoing and incoming trust



Lab Setup

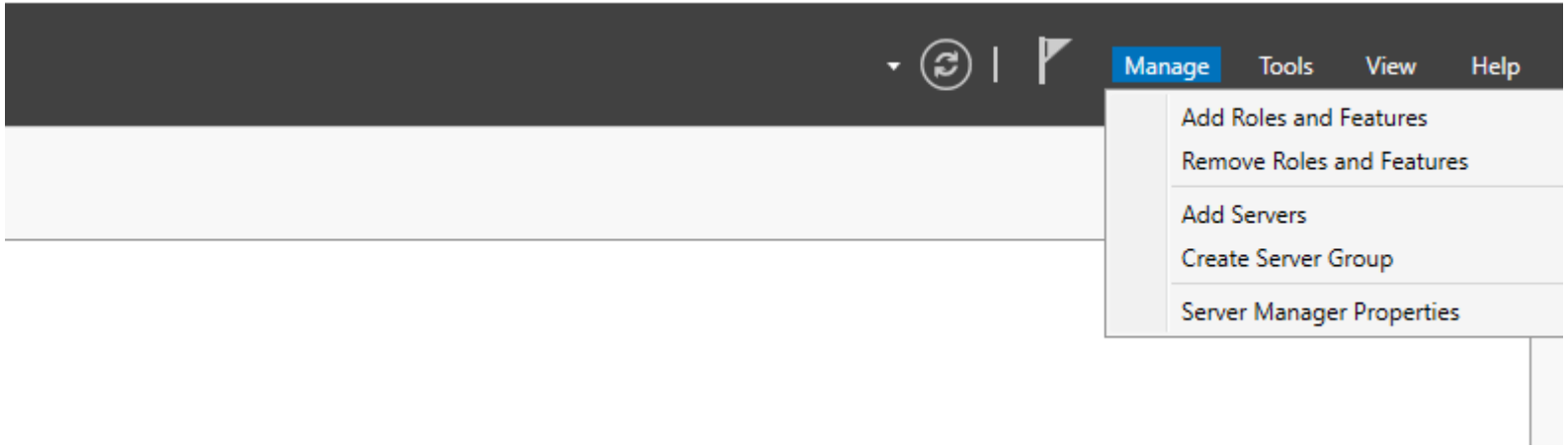
We have Successfully Created a Transitive Trust between BYTESHIELD & TRUSTEDCORP, it is now time to Configure DC02 as a Child Domain to BYTESHIELD

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



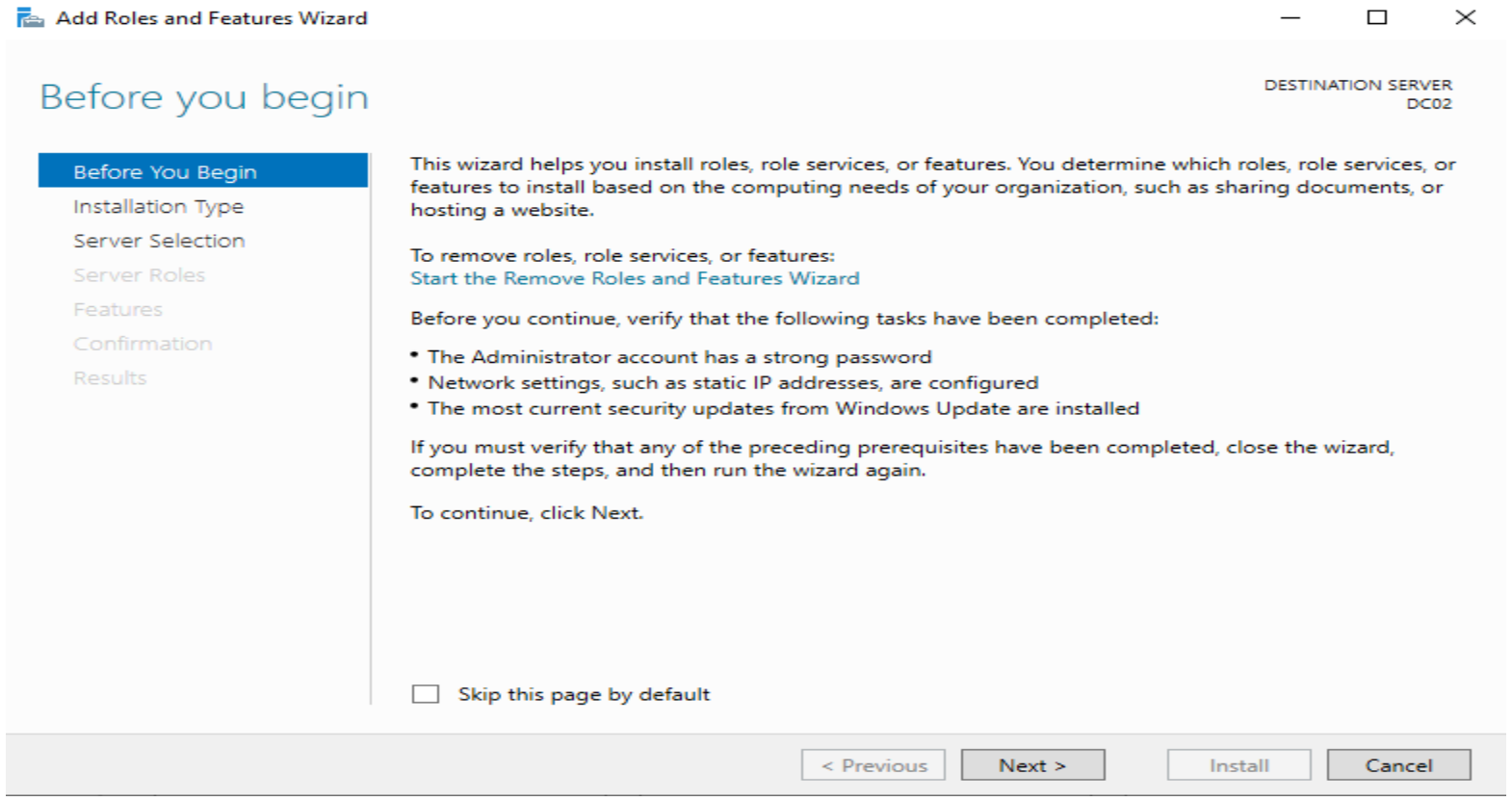
Lab Setup

Here We are going to AD-DS



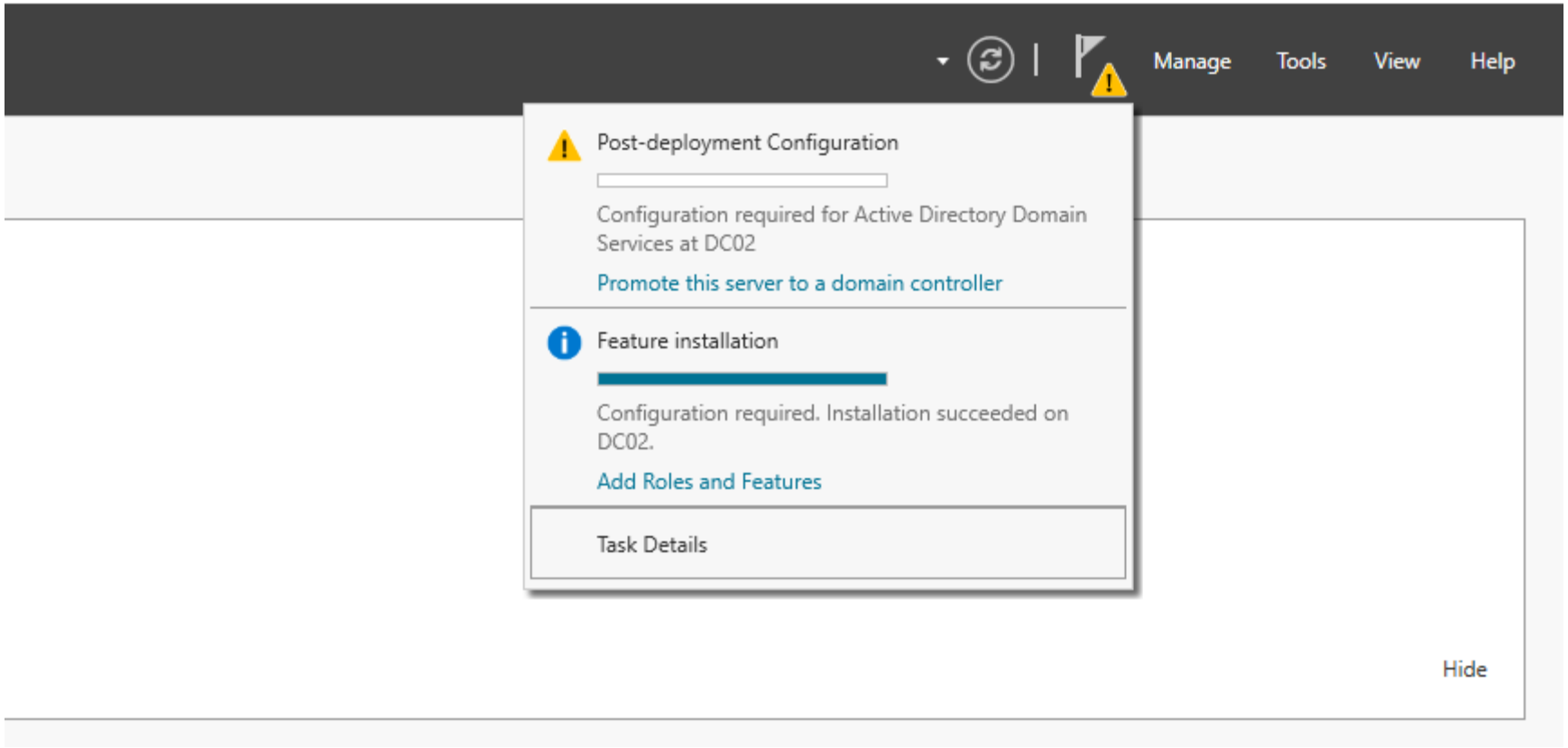
Lab Setup

The same way we did on the other domain Controllers



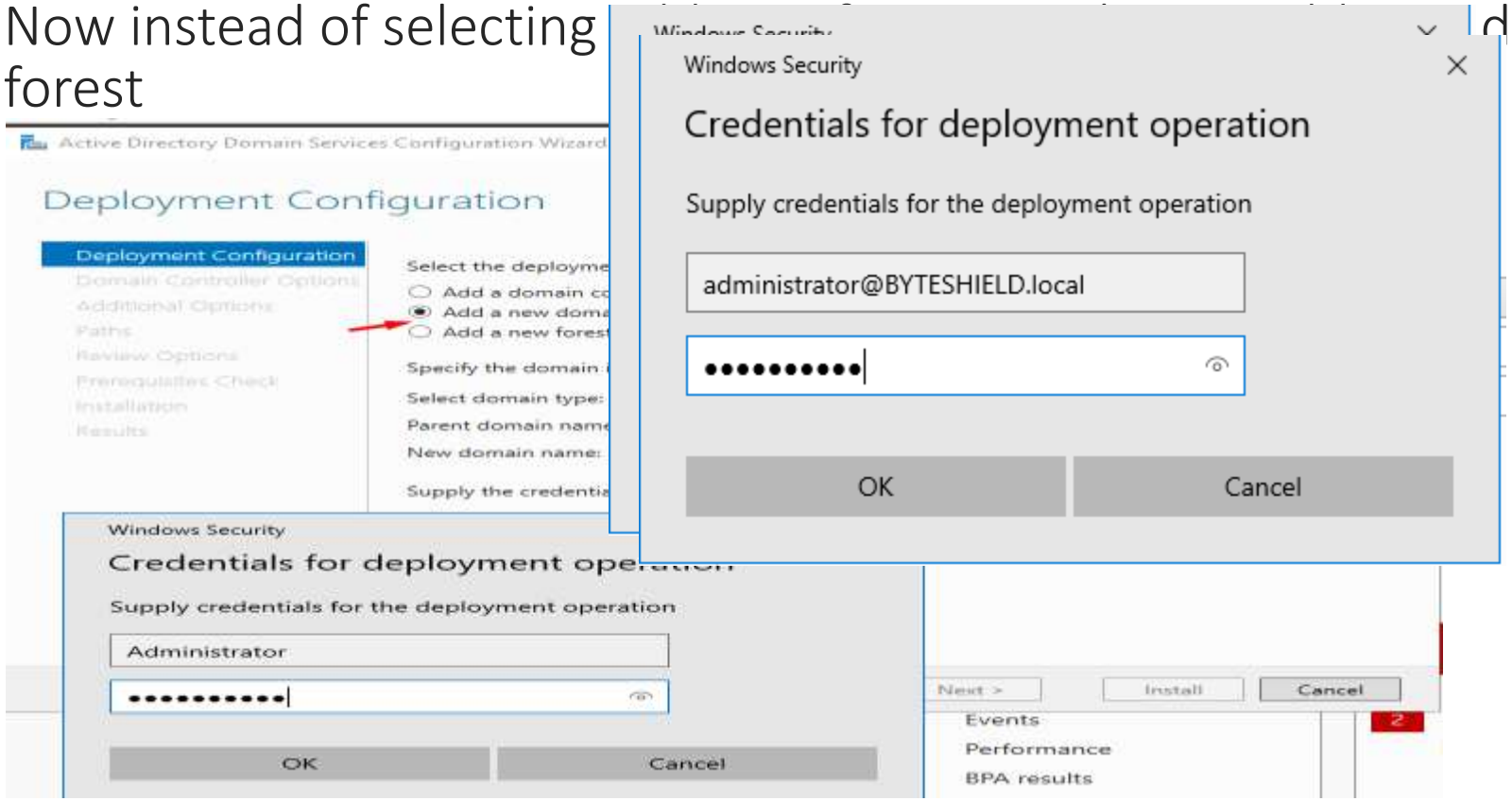
Lab Setup

Let’s Promote it to Domain Controller



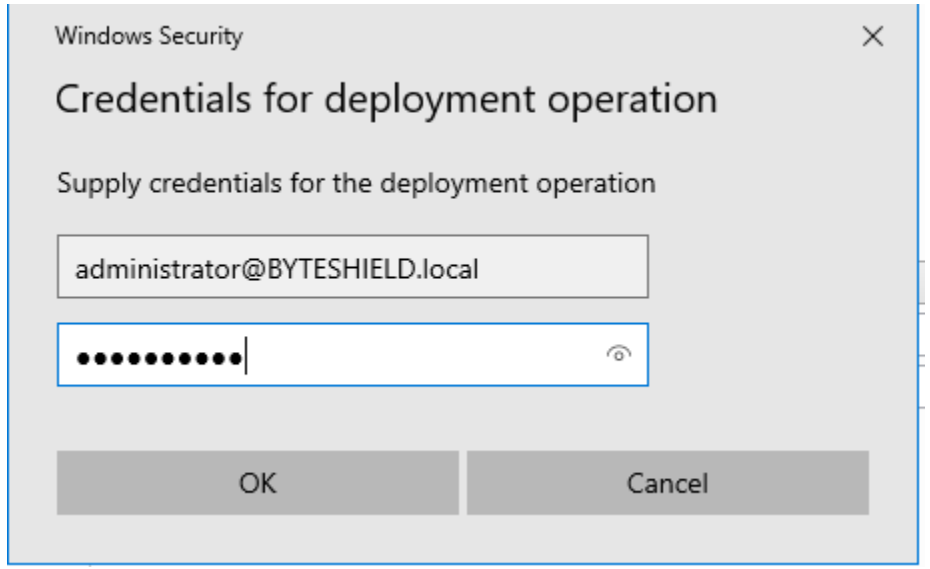
Lab Setup

Now instead of selecting domain to an existing forest



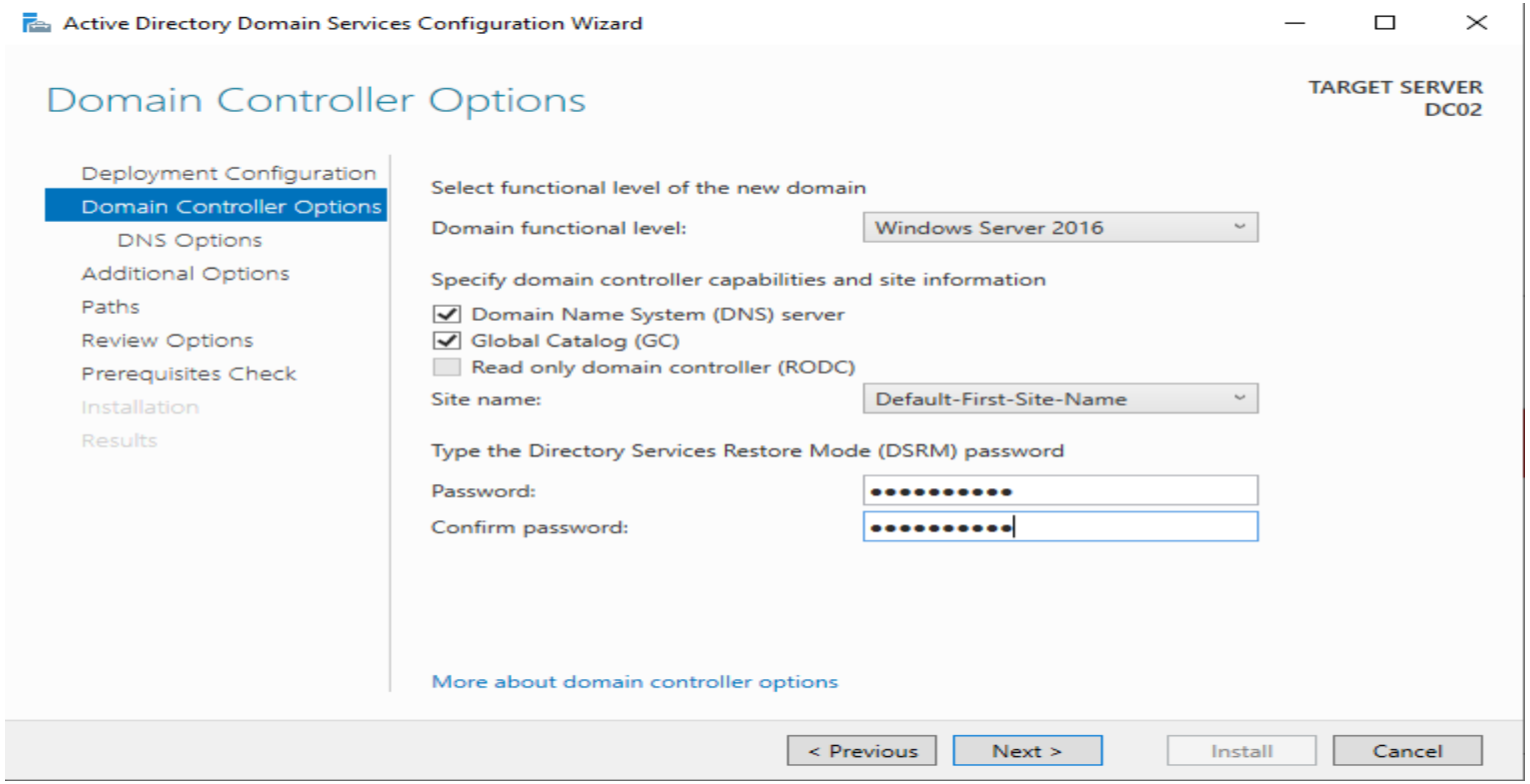
Lab Setup

Supplying the Credentials of our Root Domain



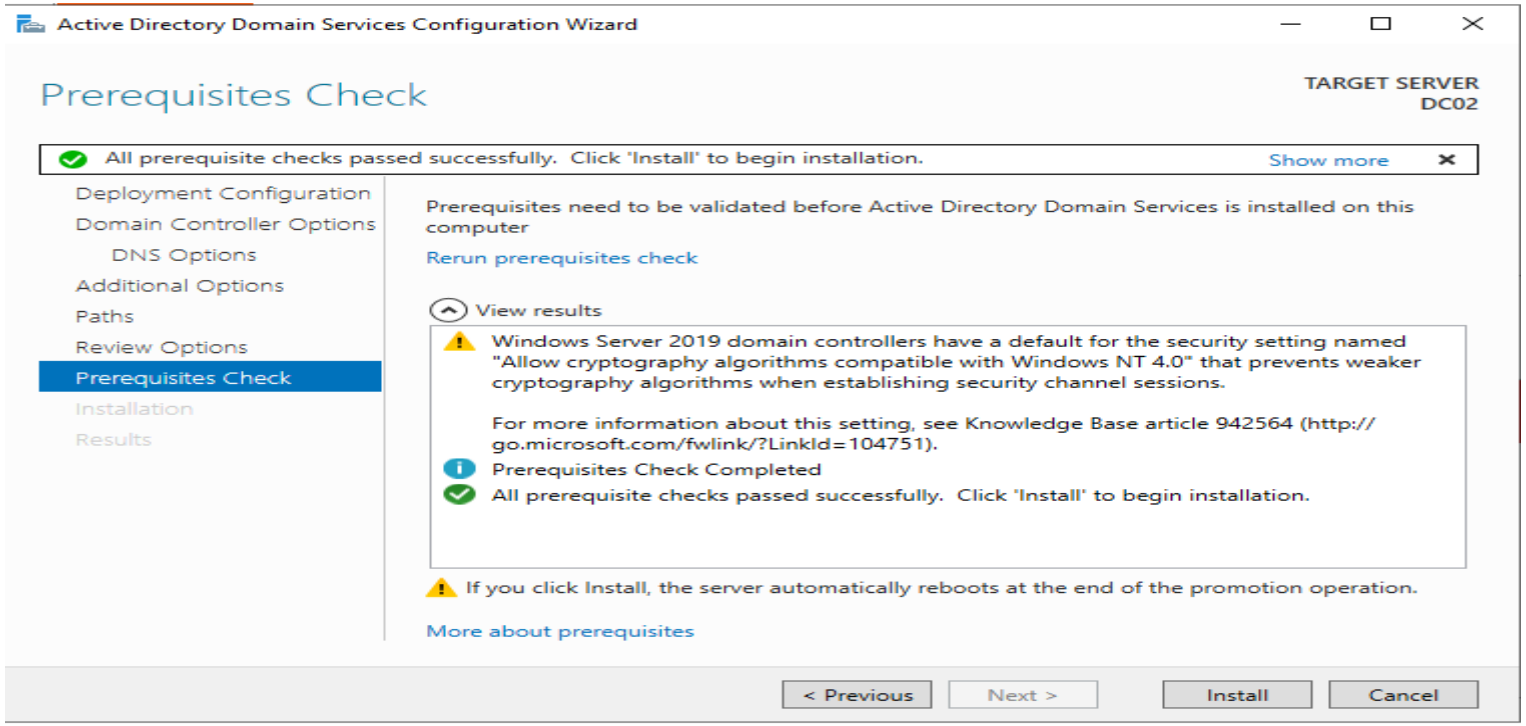
Lab Setup

Creating DSRM Passowrd



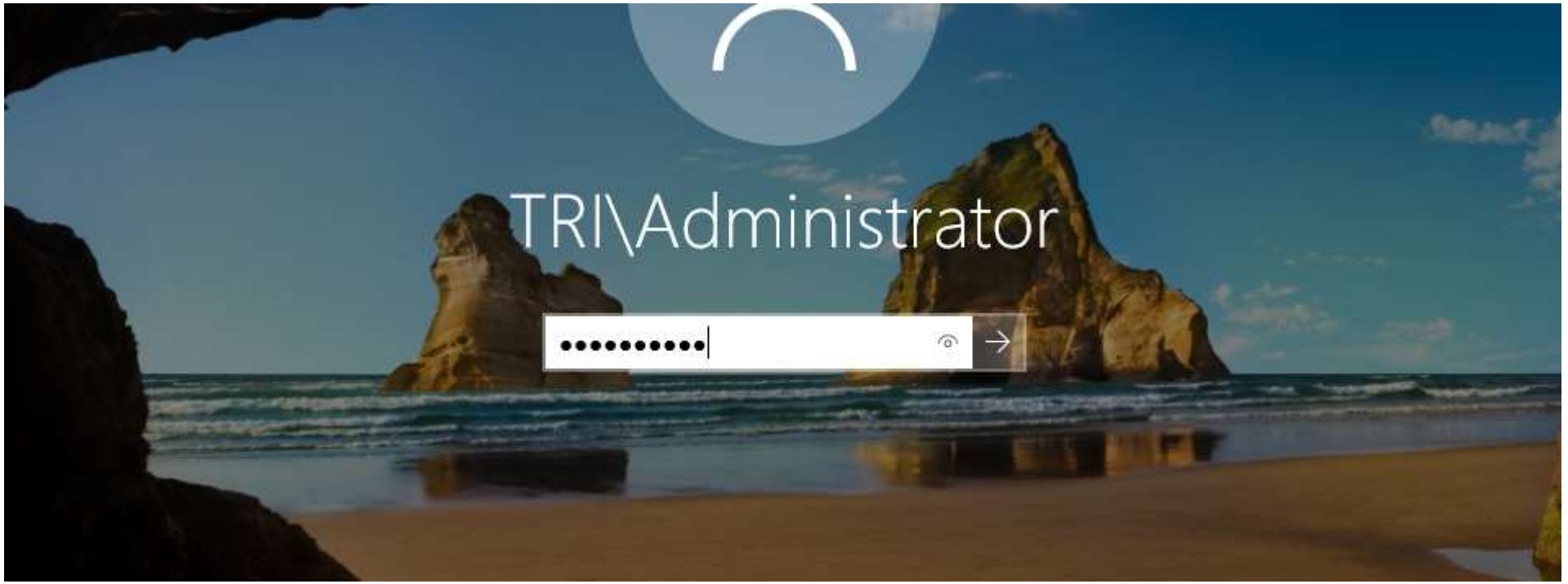
Lab Setup

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



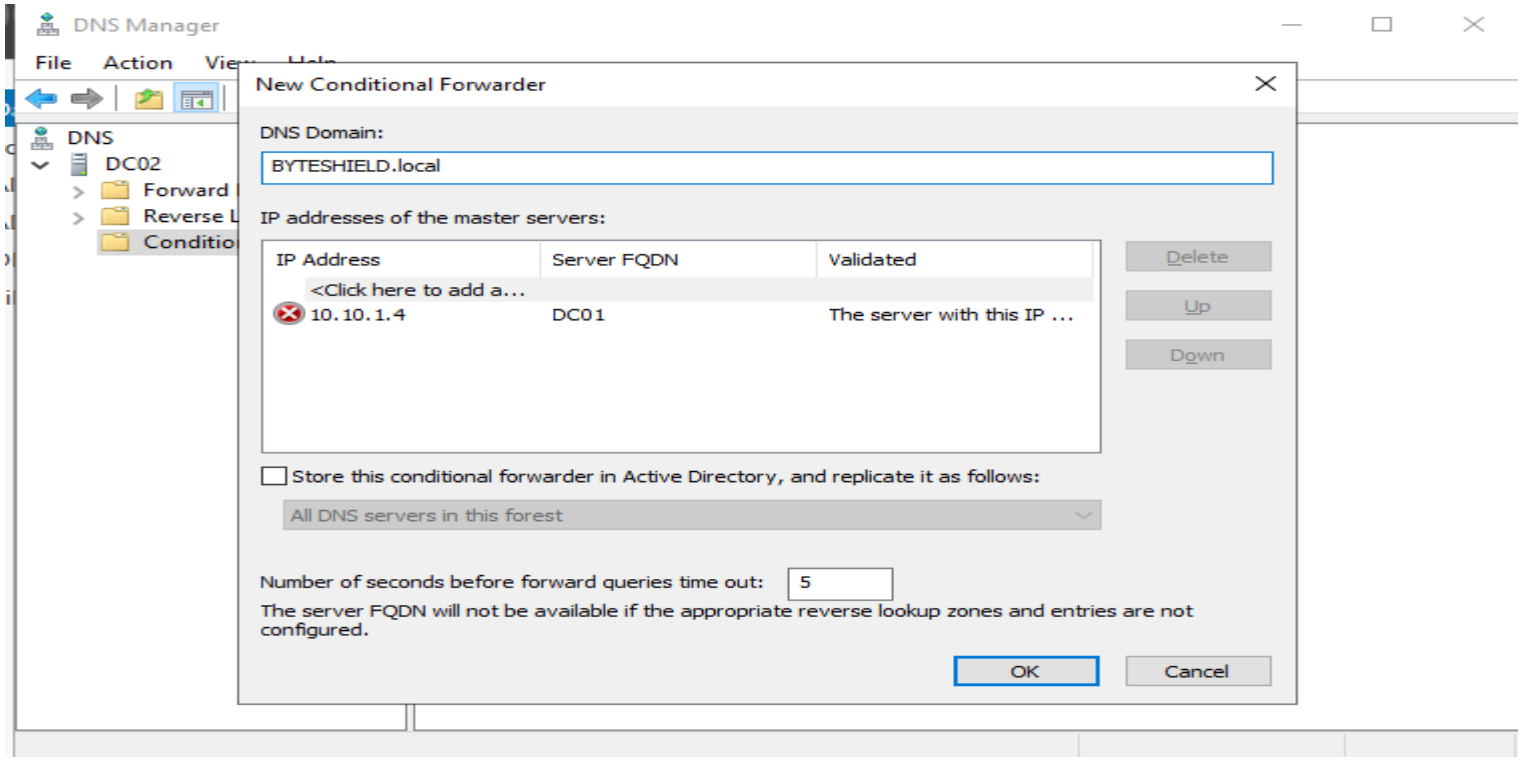
Lab Setup

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
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 = 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

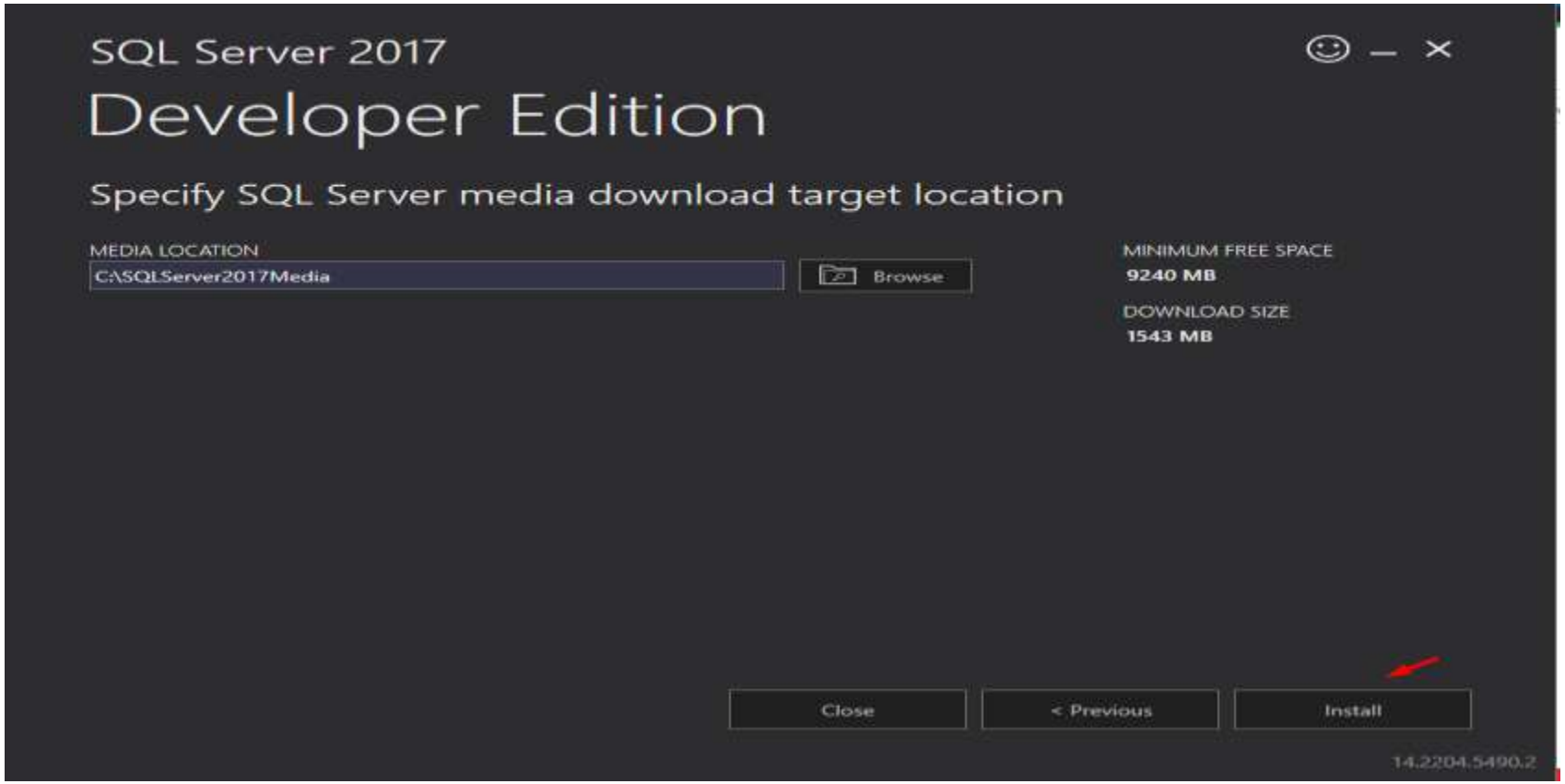
https://download.microsoft.com/download/5/A/7/5A7065A2-C81C-4A31-9972-8A31AC9388C1/SQLServer2017-SSEI-Dev.exe

Lab Setup

SQL Server installation

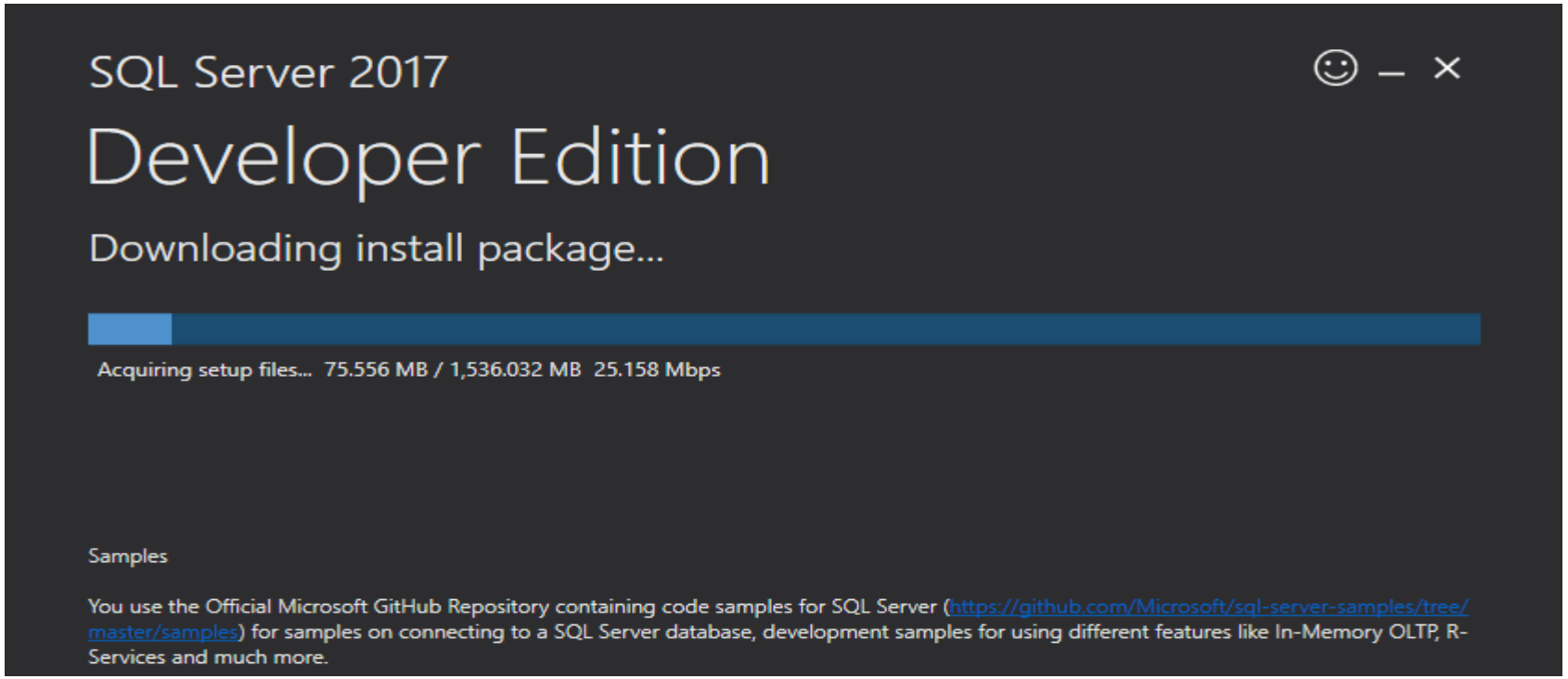
Lab Setup

Install



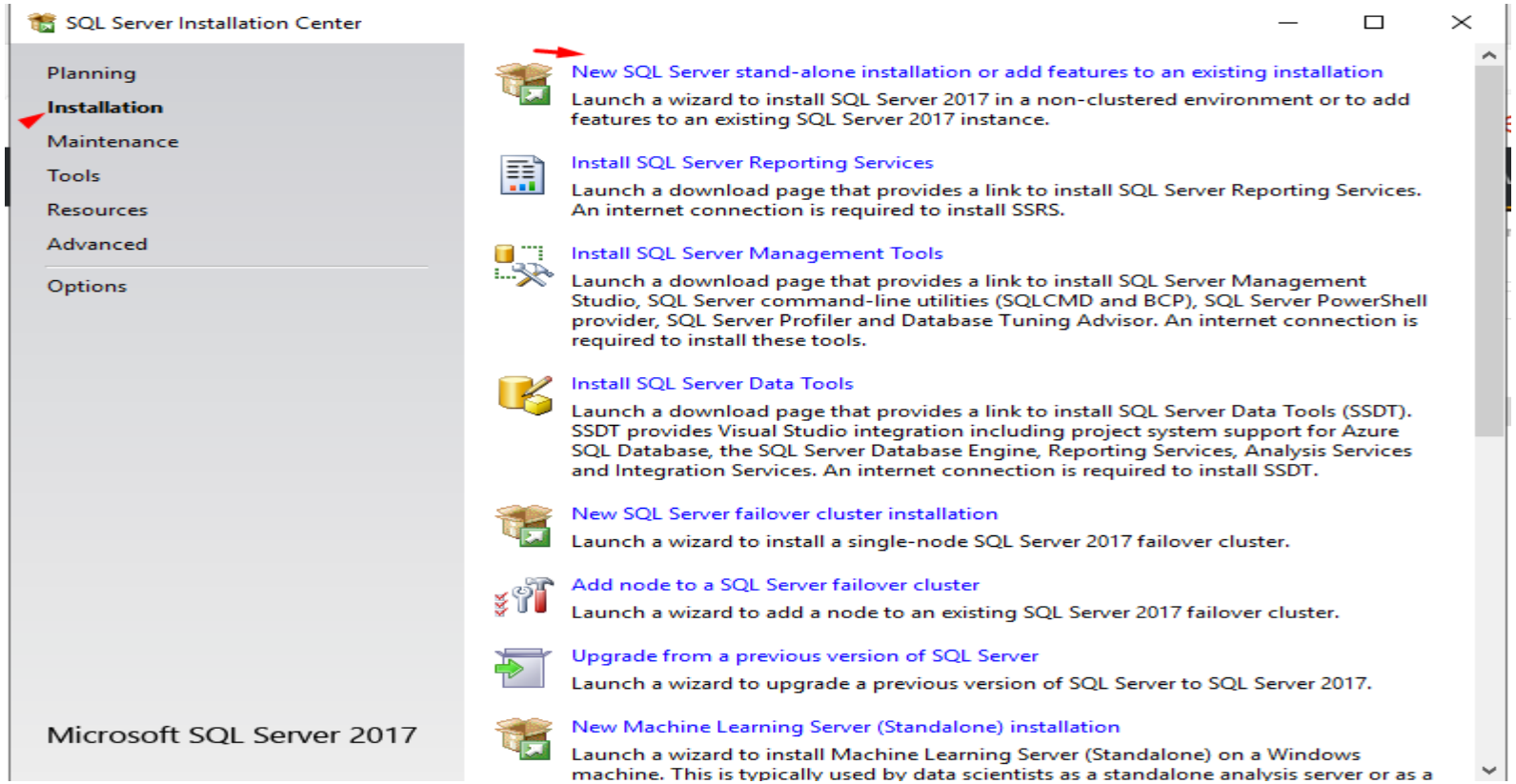
Lab Setup

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

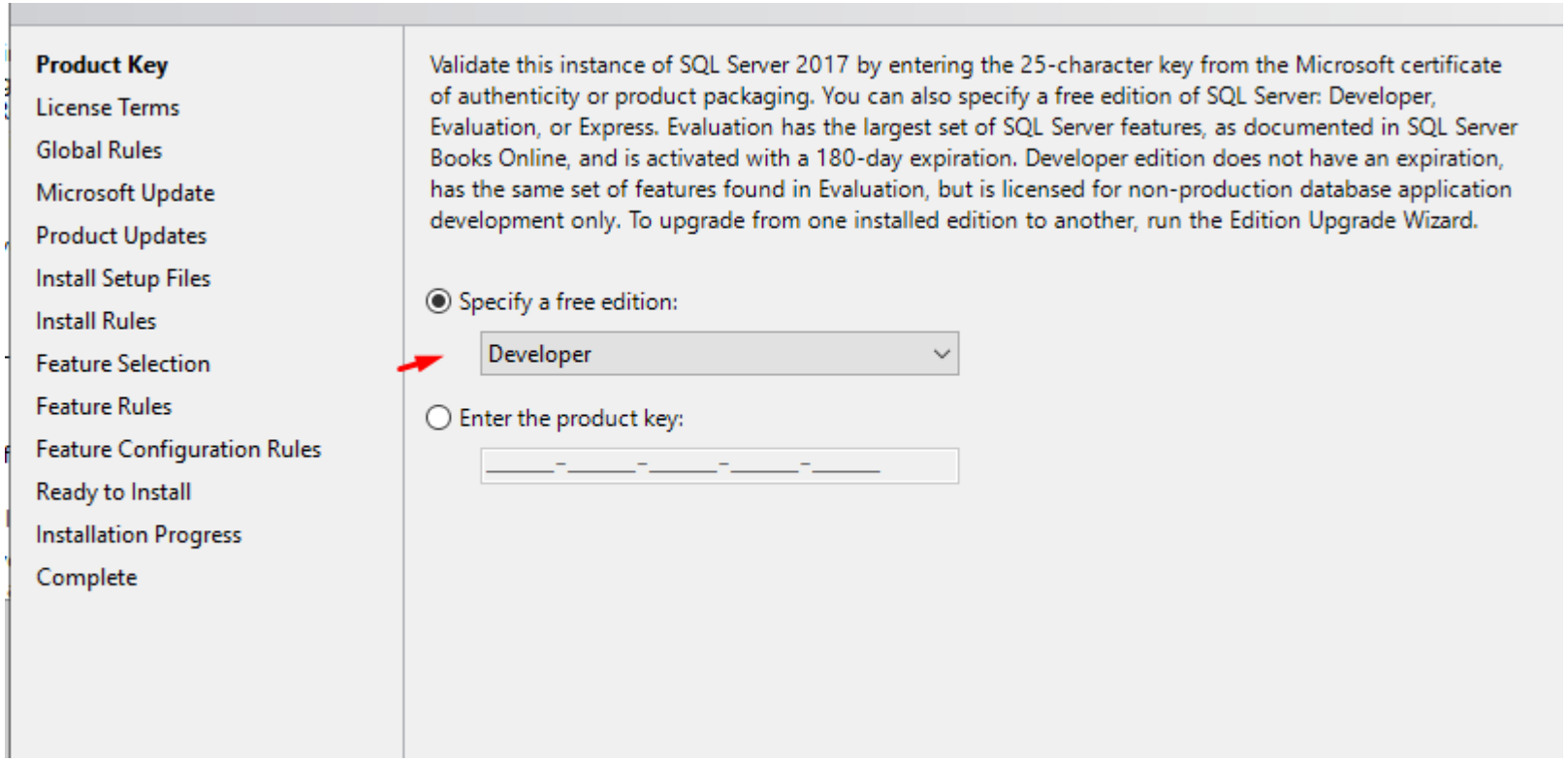


Lab Setup

Select New Sql server stand-alone installation and continue



Lab Setup

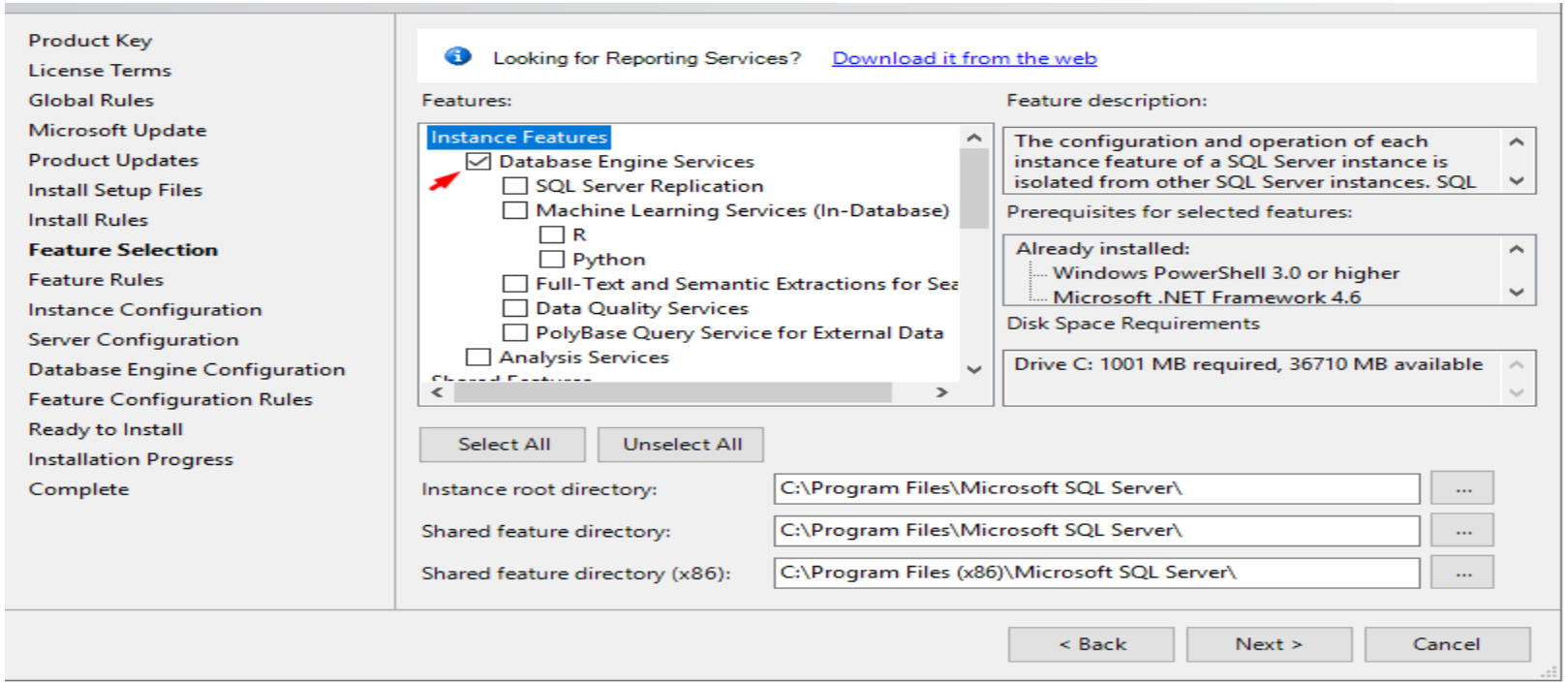

Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Validate this instance of SQL Server 2017 by entering the 25-character key from the Microsoft 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

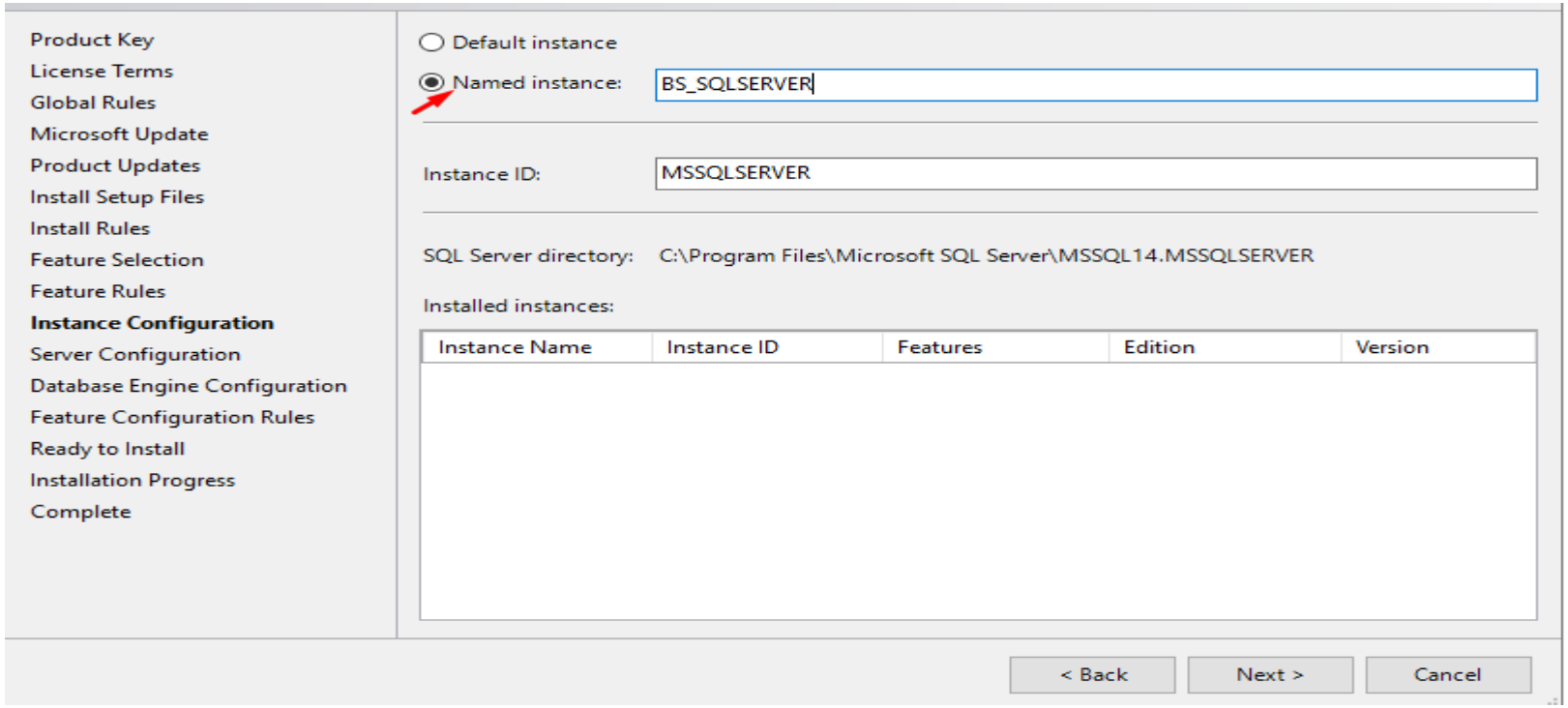
Lab Setup

Next > Next



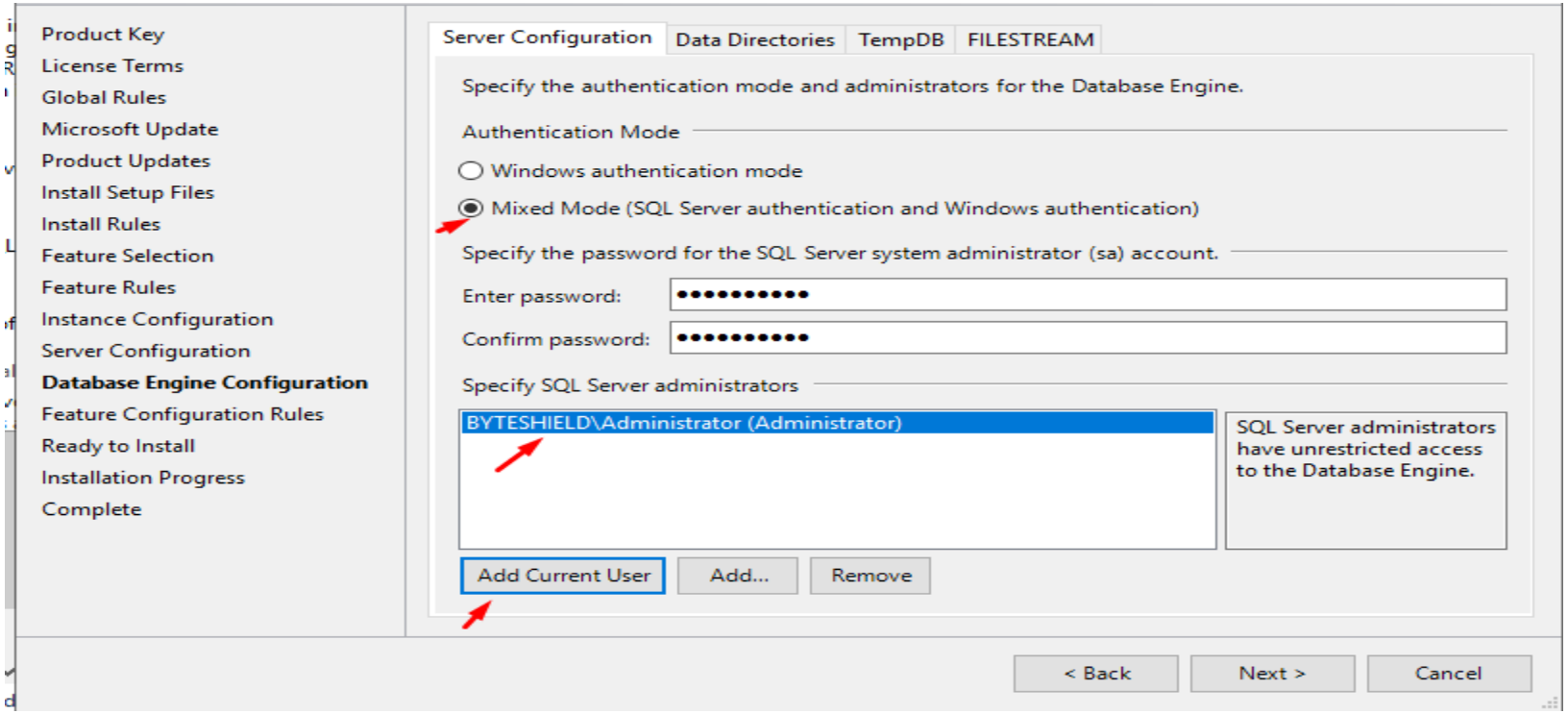
Lab Setup

Choose named instance and change its name from the default



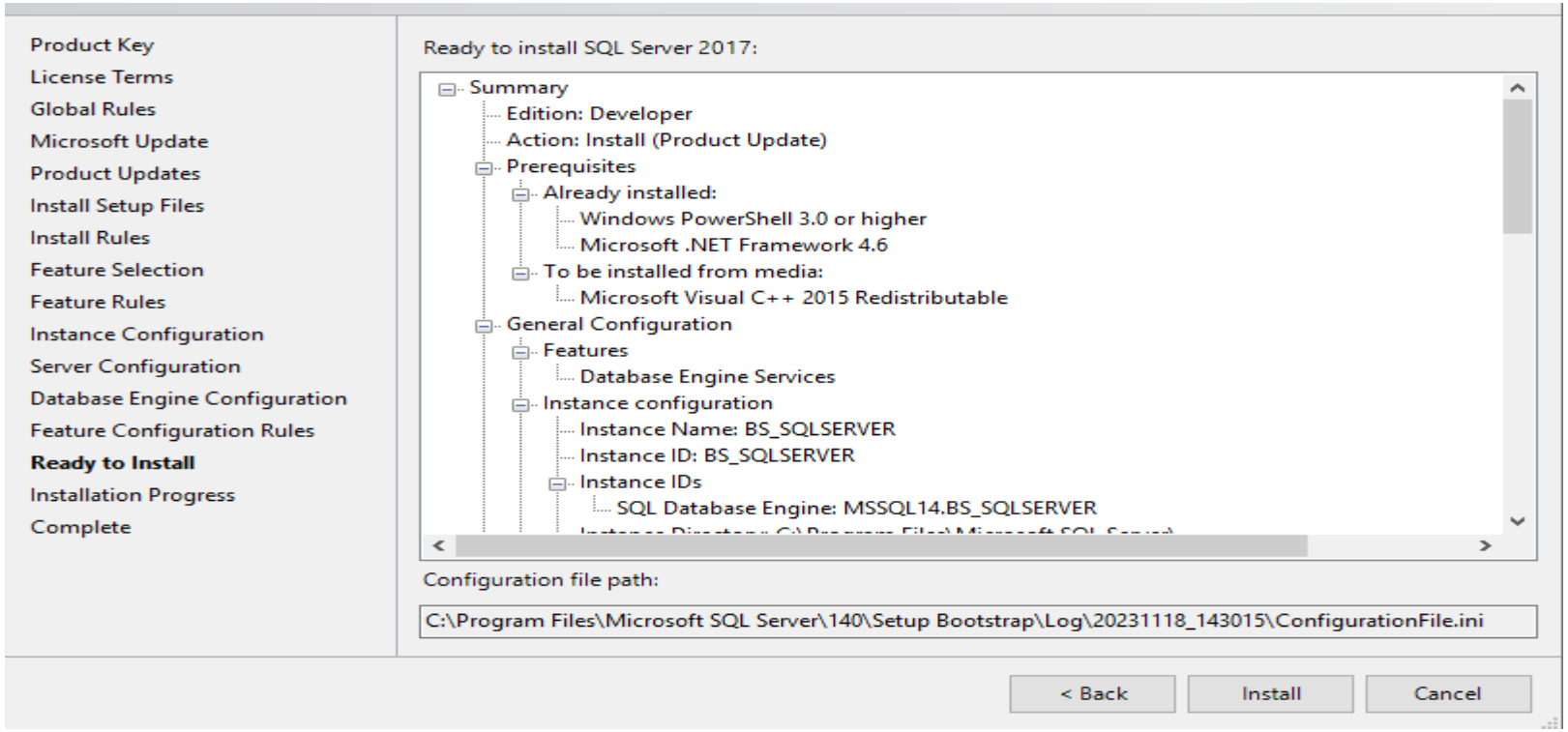
Lab Setup

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

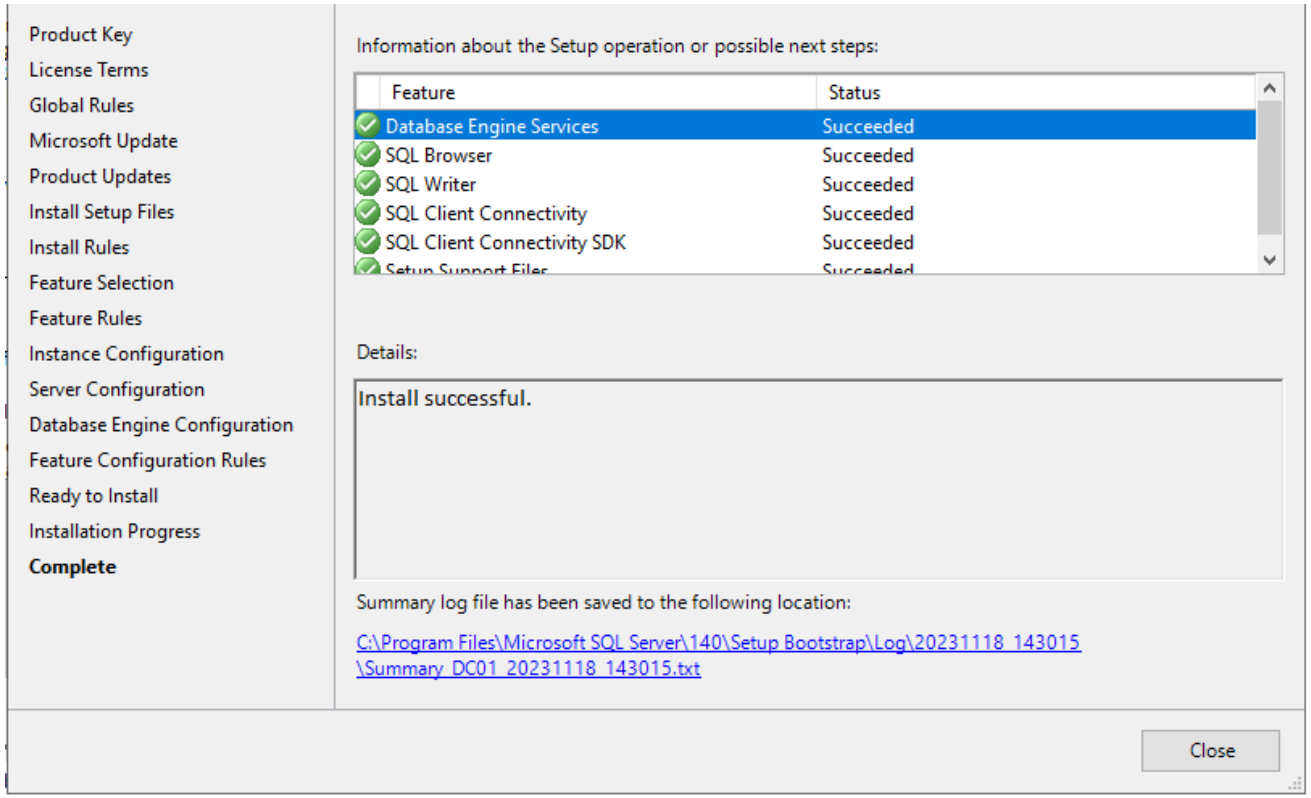


Lab Setup

Next and Install

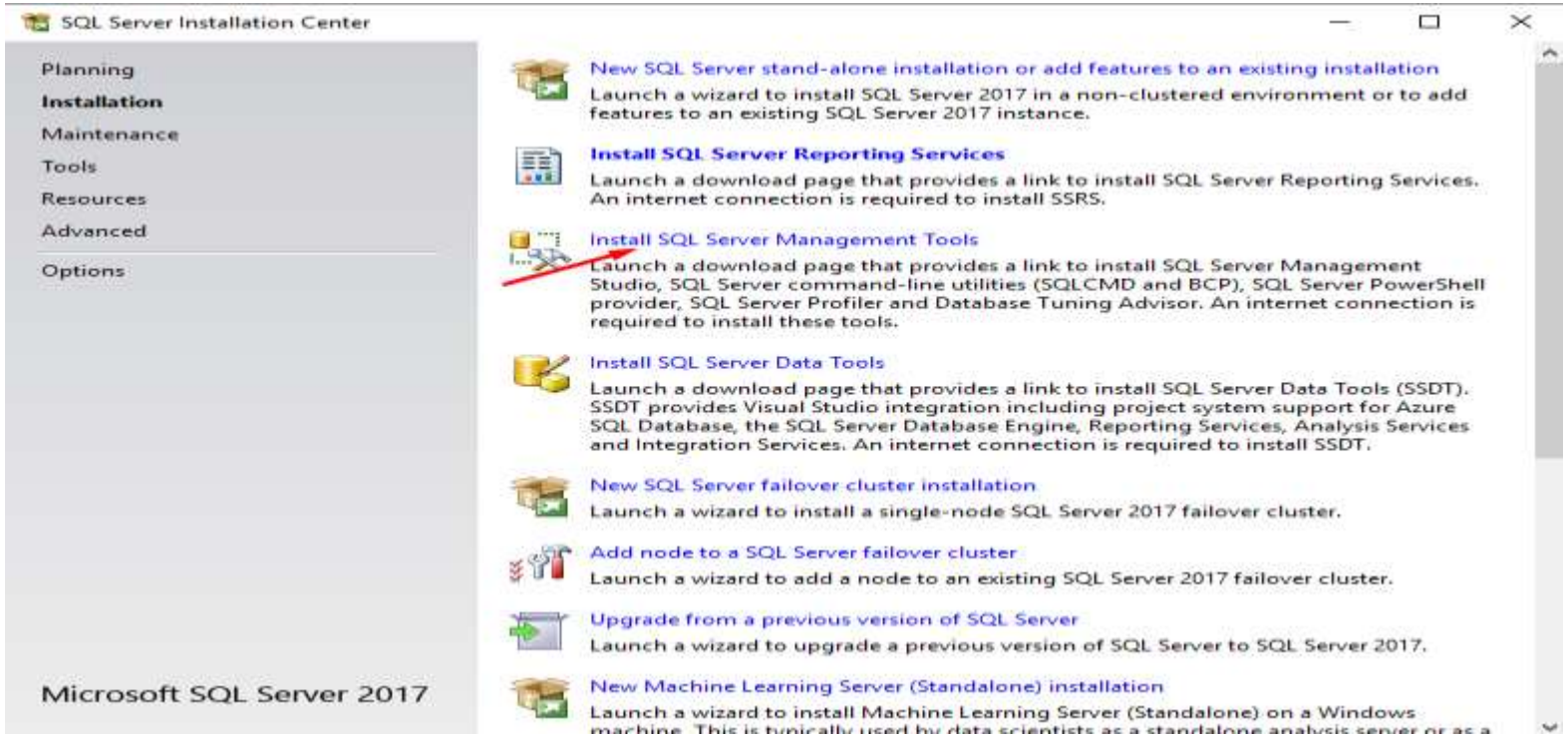


Lab Setup


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
Information about the Setup operation or possible next steps:
Feature
Status
Database Engine Services
Succeeded
SQL Browser
Succeeded
SQL Writer
Succeeded
SQL Client Connectivity
Succeeded
SQL Client Connectivity SDK
Succeeded
Details:
Install successful.
Summary log file has been saved to the following location:
C:\Program Files\Microsoft SQL Server\140\Setup Bootstrap\Log\20231118_143015
\Summary_DC01_20231118_143015.txt
Close

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

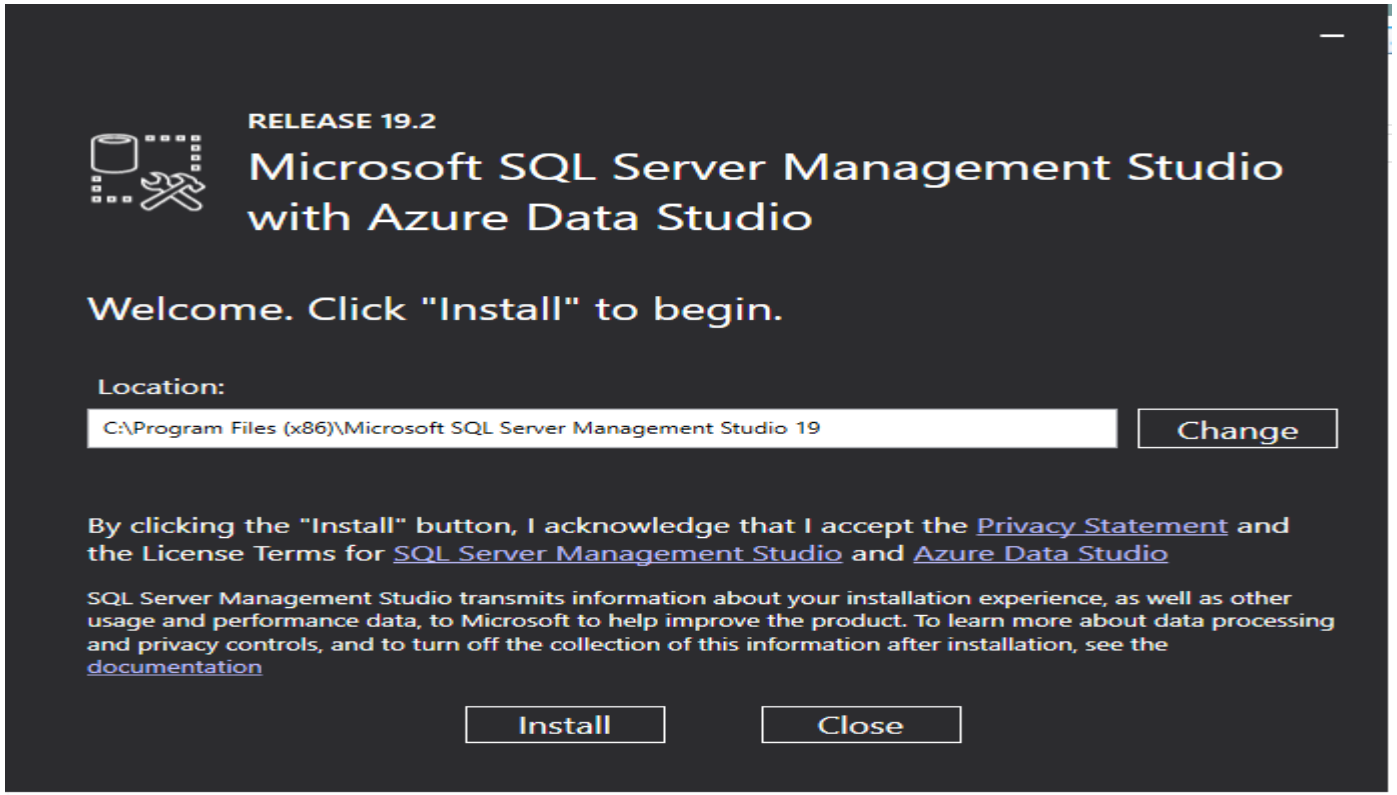
↓ **Free Download for SQL Server Management Studio (SSMS) 19.2**

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.

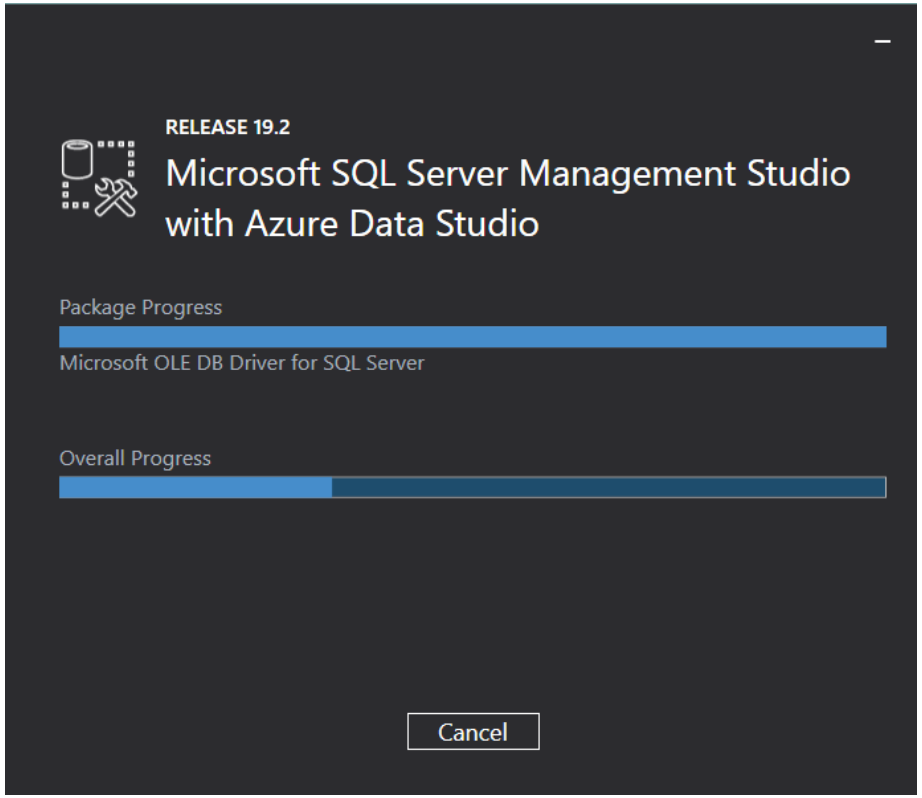
- Release number: 19.2
- Build number: 19.2.56.2
- Release date: November 13, 2023

Lab Setup

Installing SSMS

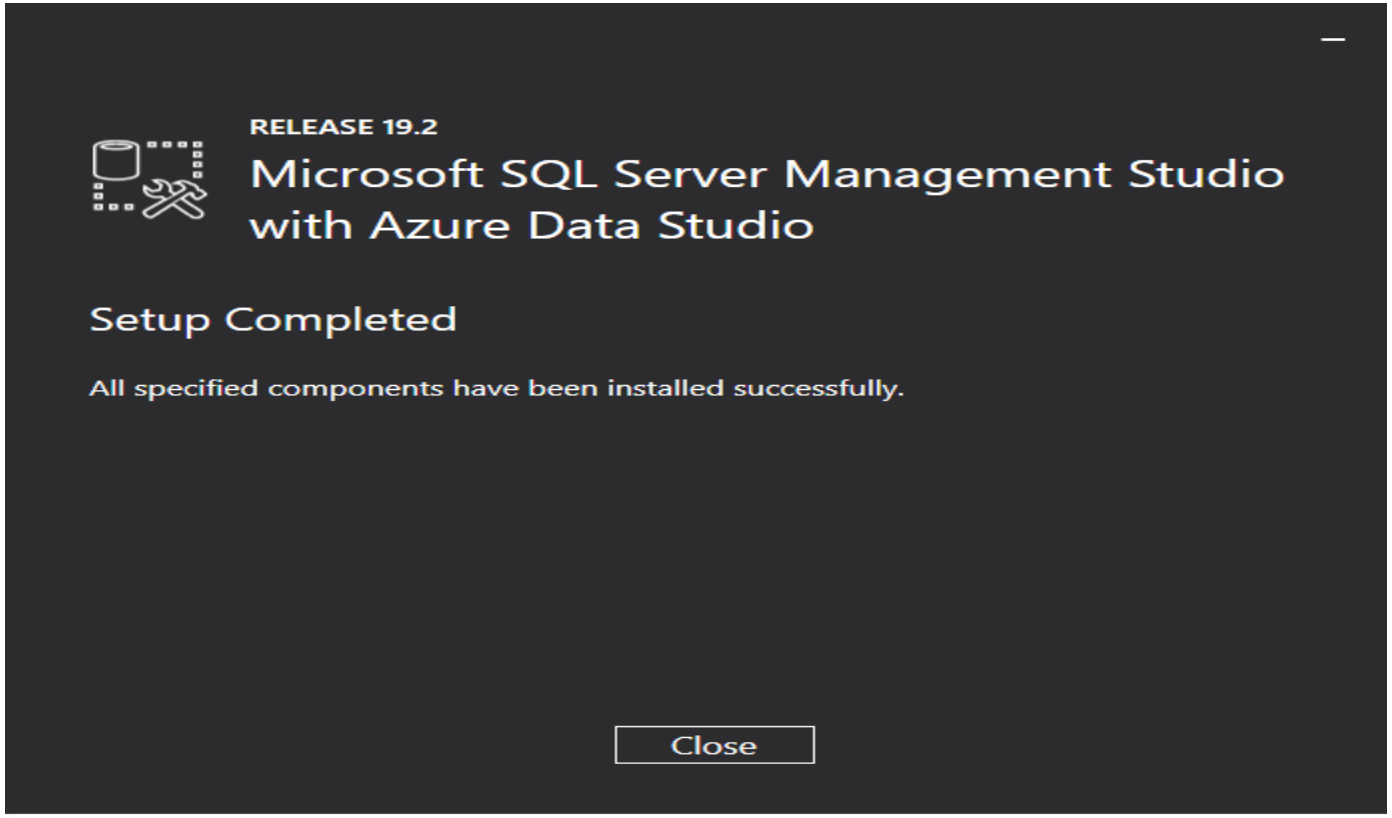


Lab Setup


RELEASE 19.2
Microsoft SQL Server Management Studio
with Azure Data Studio
Package Progress
Microsoft OLE DB Driver for SQL Server
Overall Progress
Cancel

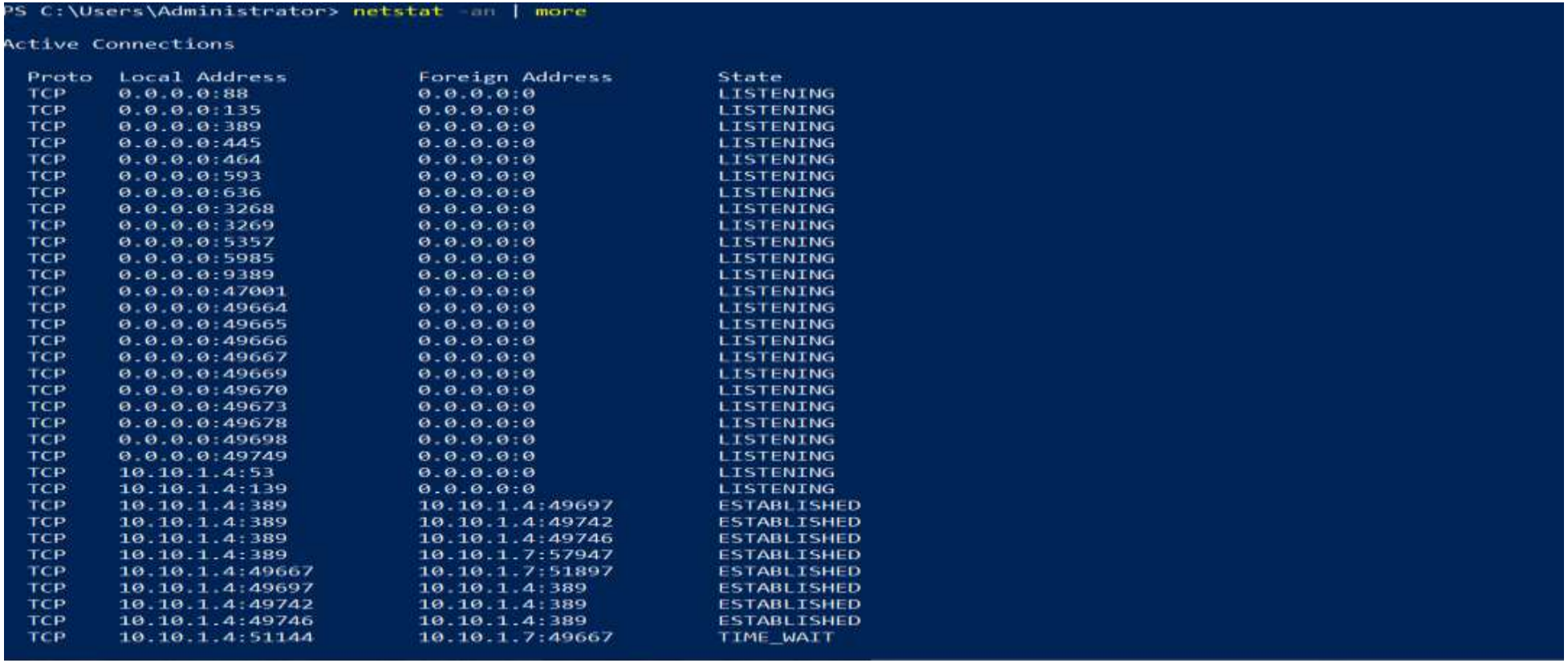
Lab Setup

Successfully Installed



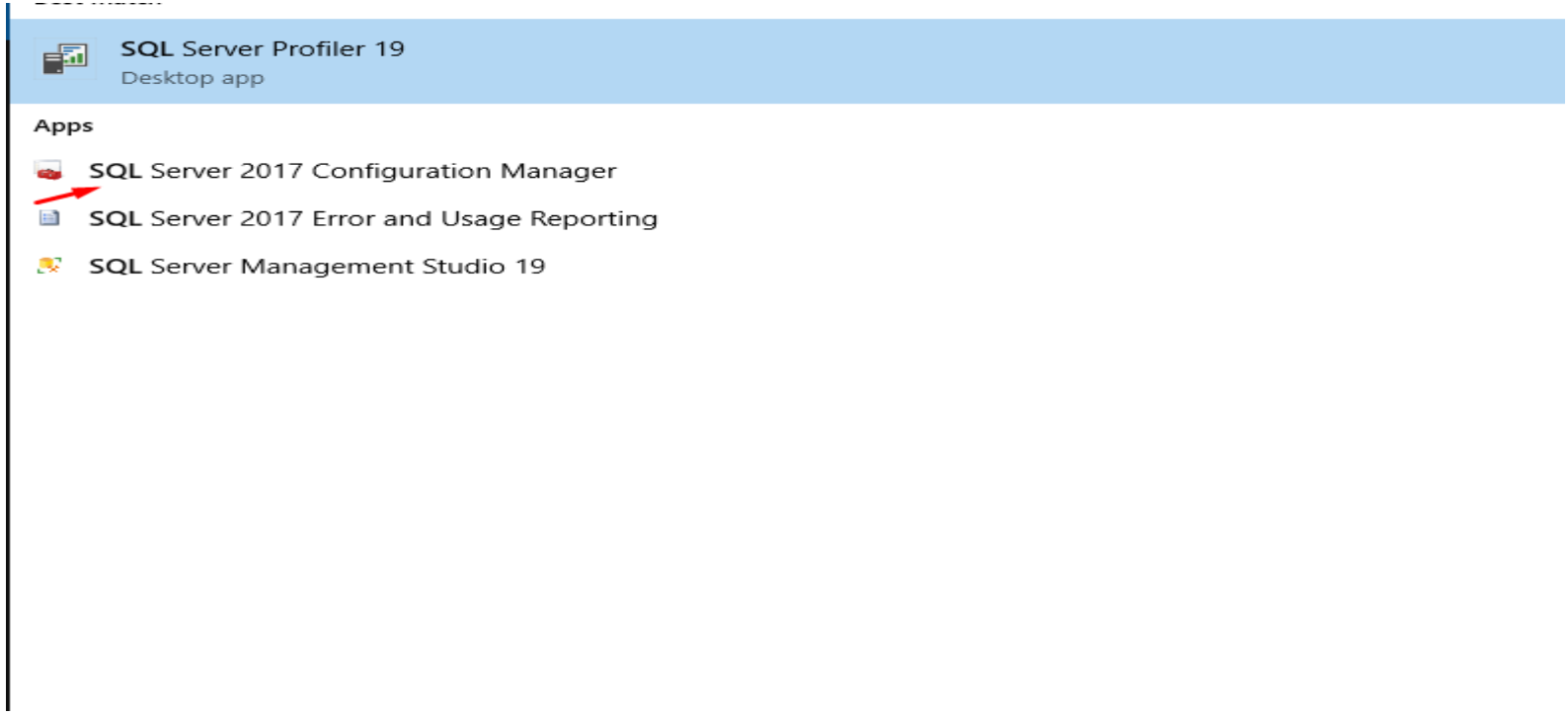
Lab Setup

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



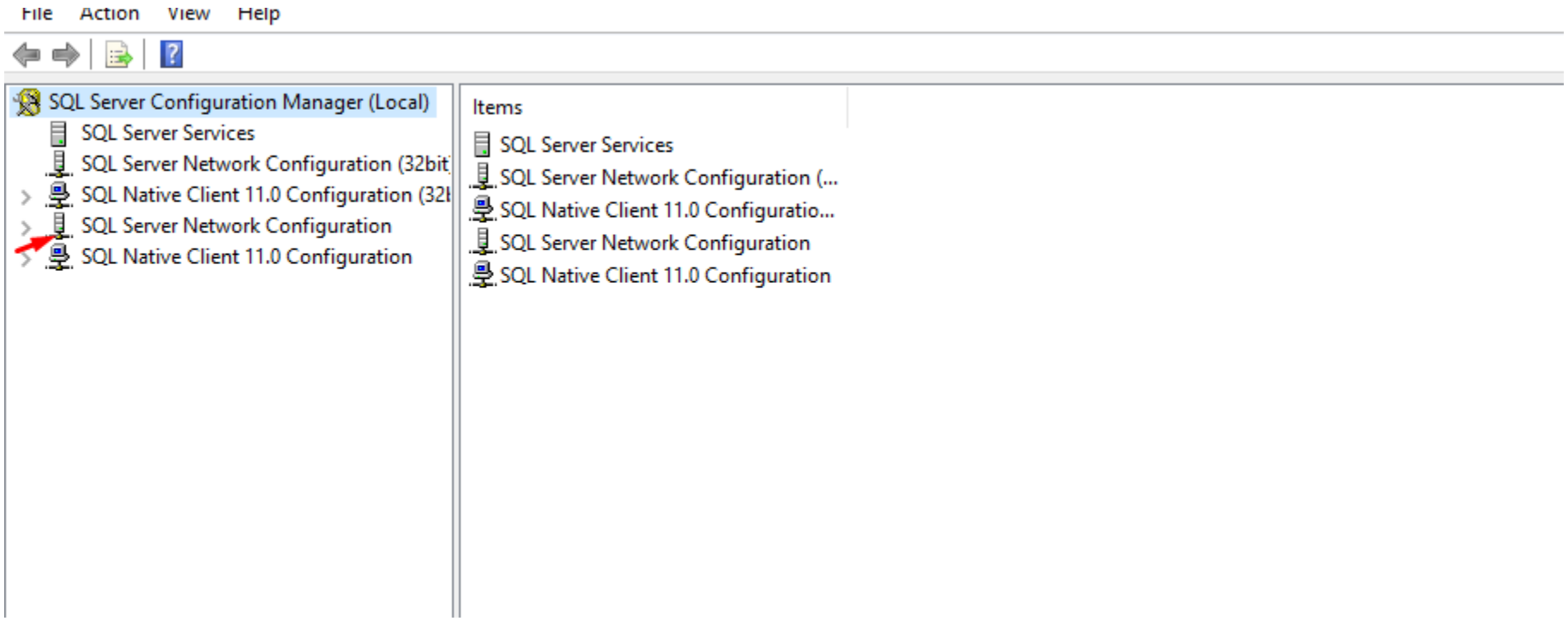
Lab Setup

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



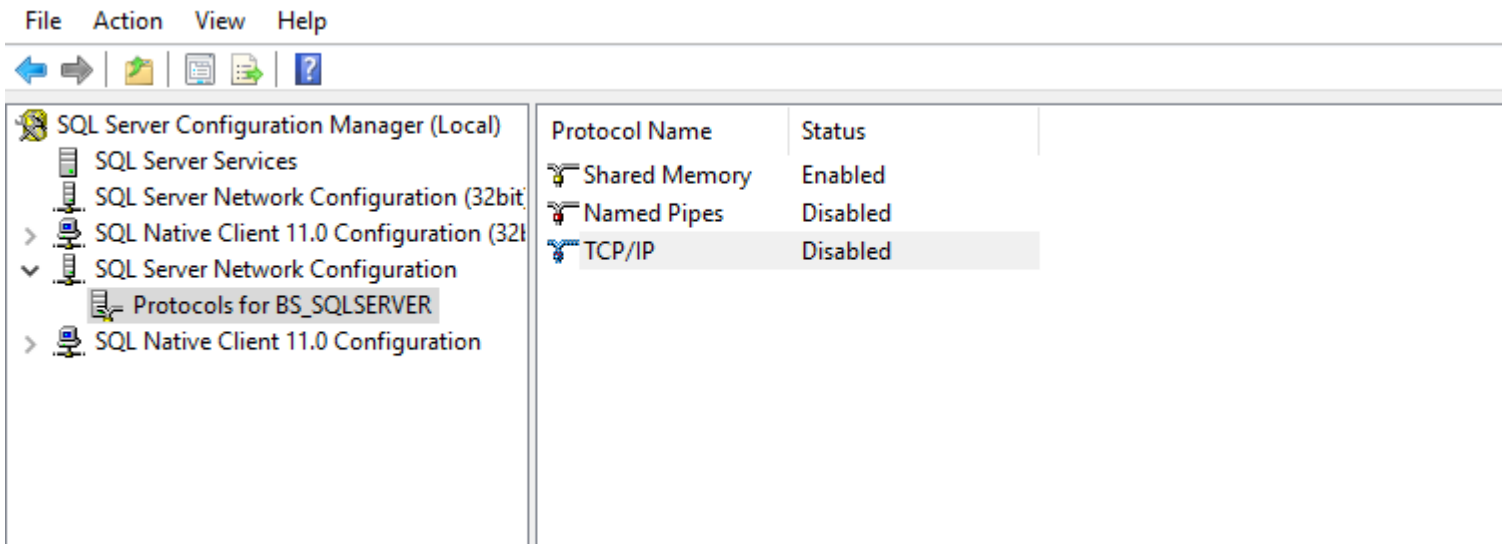
Lab Setup

After searching and clicking Configuration manager, select network configuration



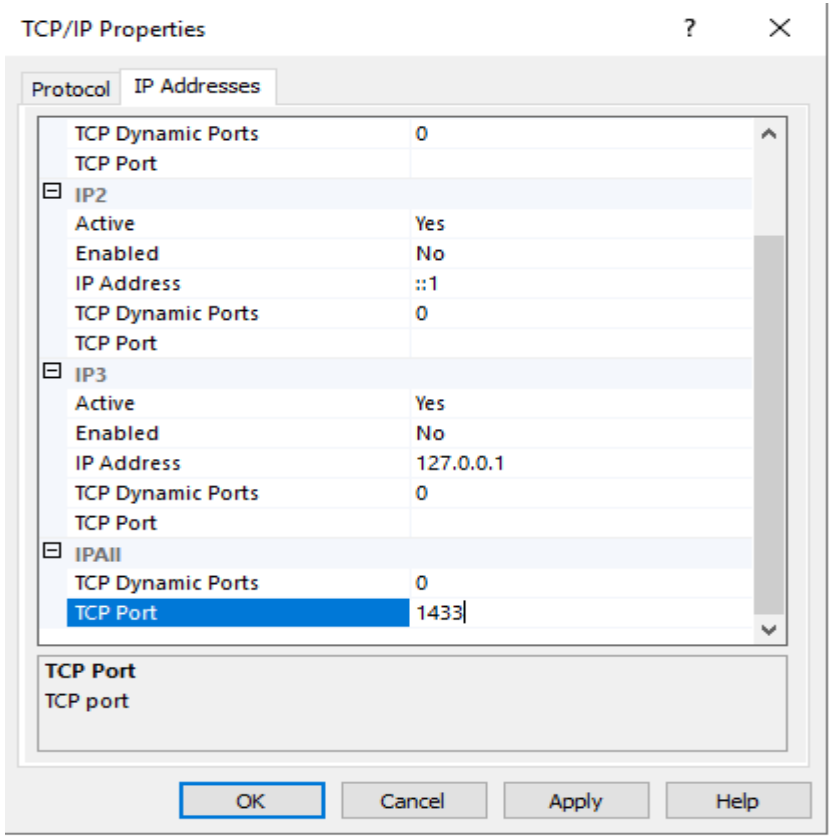
Lab Setup

Double click or right click to go toTCP/IP properties



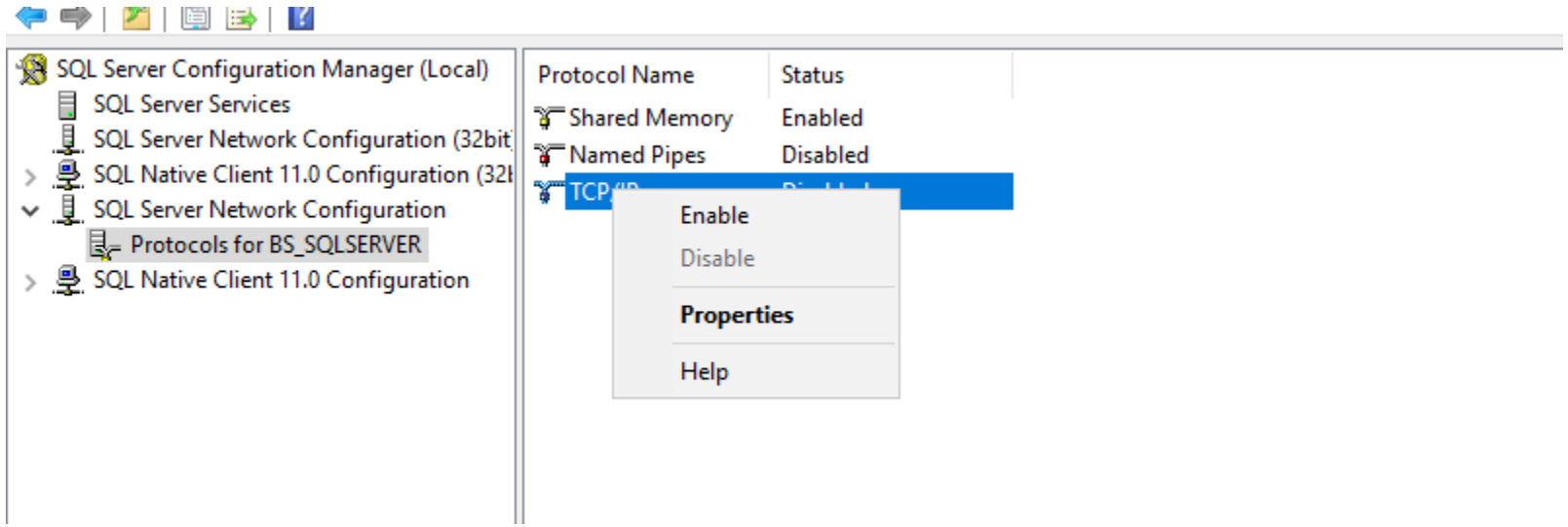
Lab Setup

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



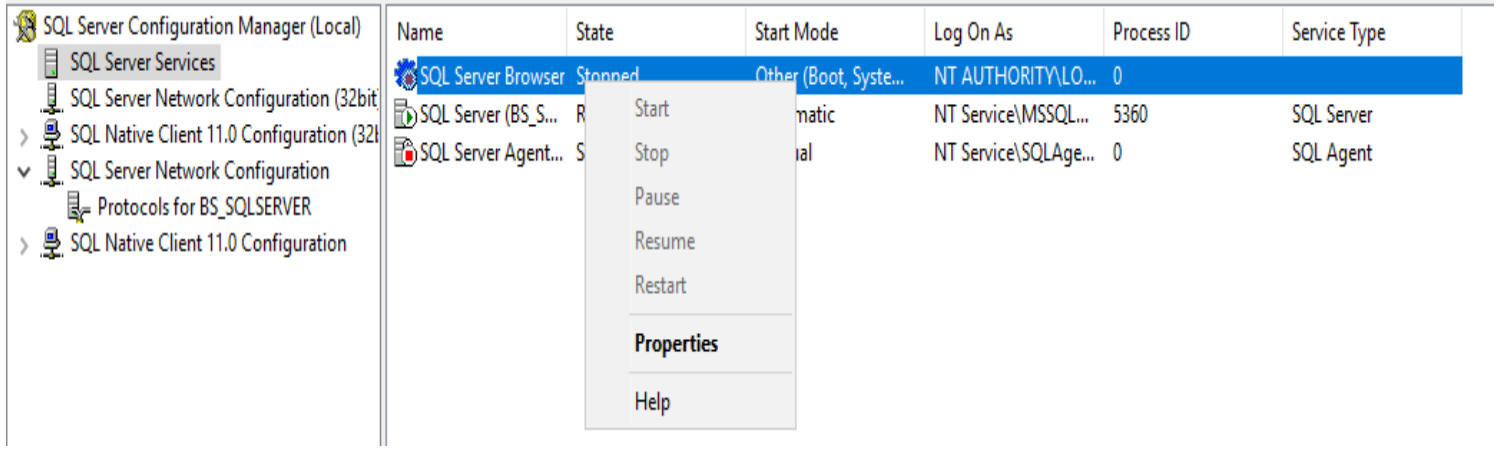
Lab Setup

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



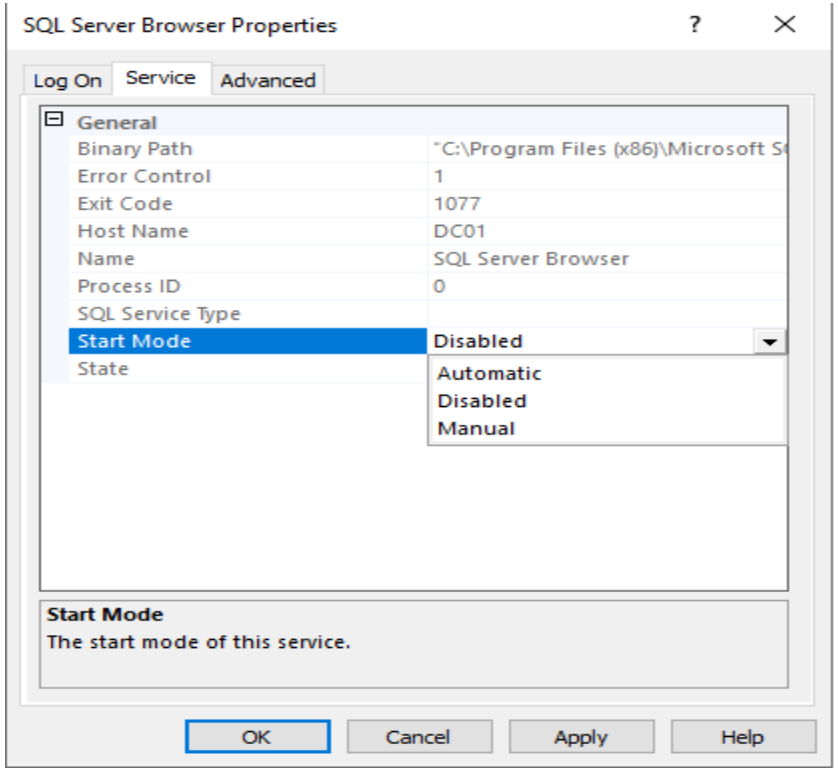
Lab Setup

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



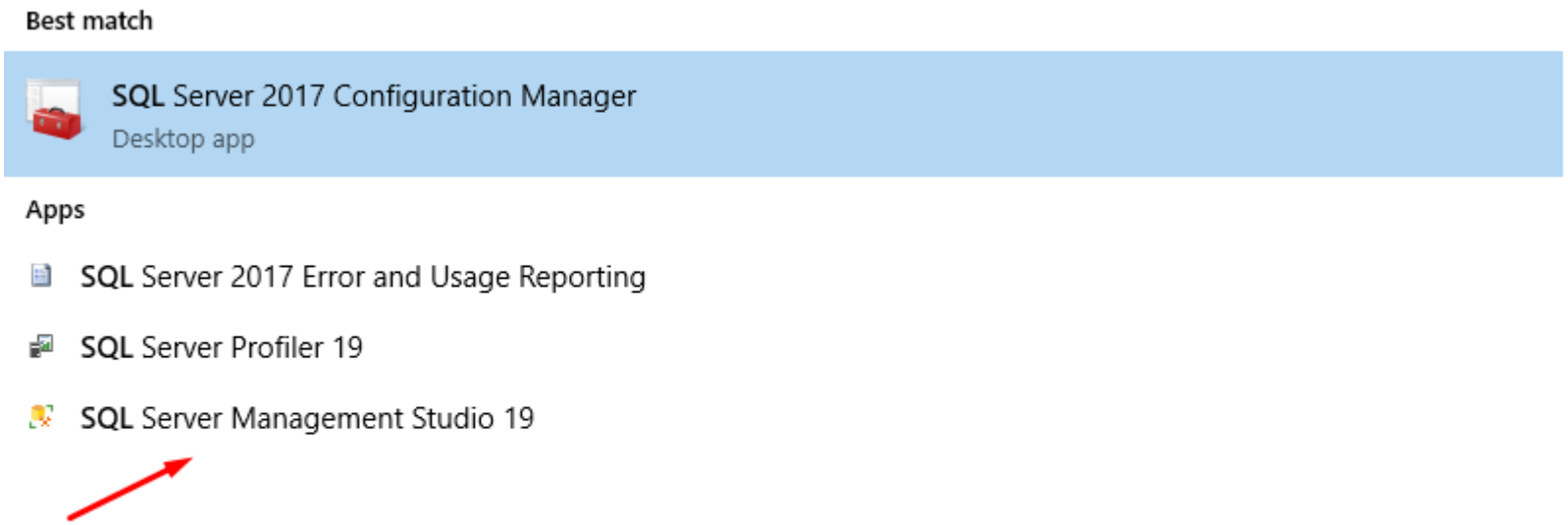
Lab Setup

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



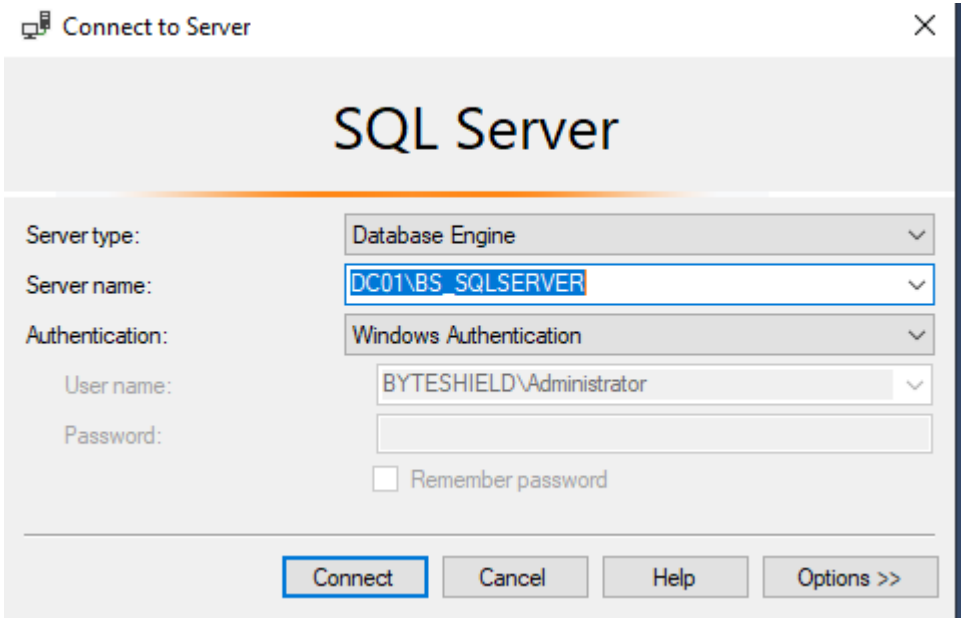
Lab Setup

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



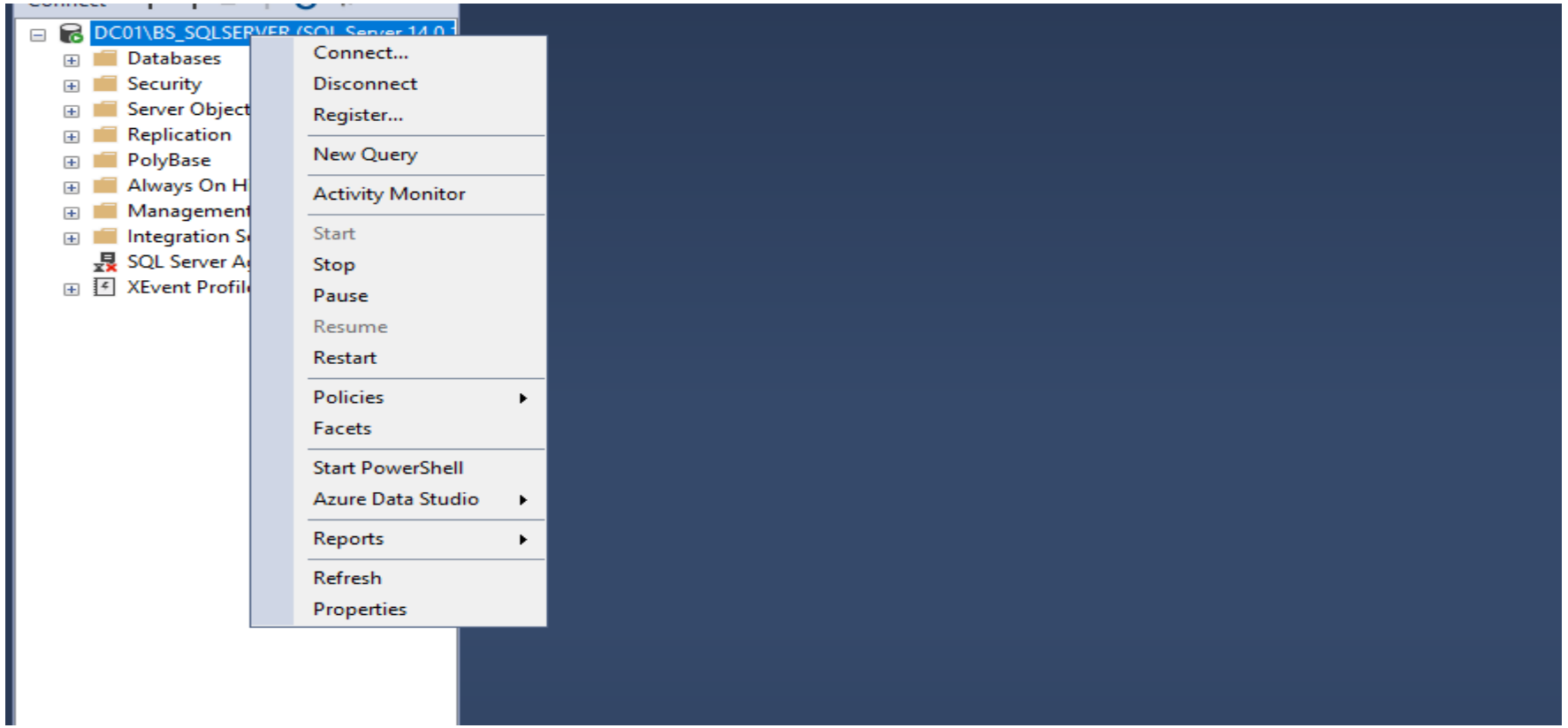
Lab Setup

Click Connect



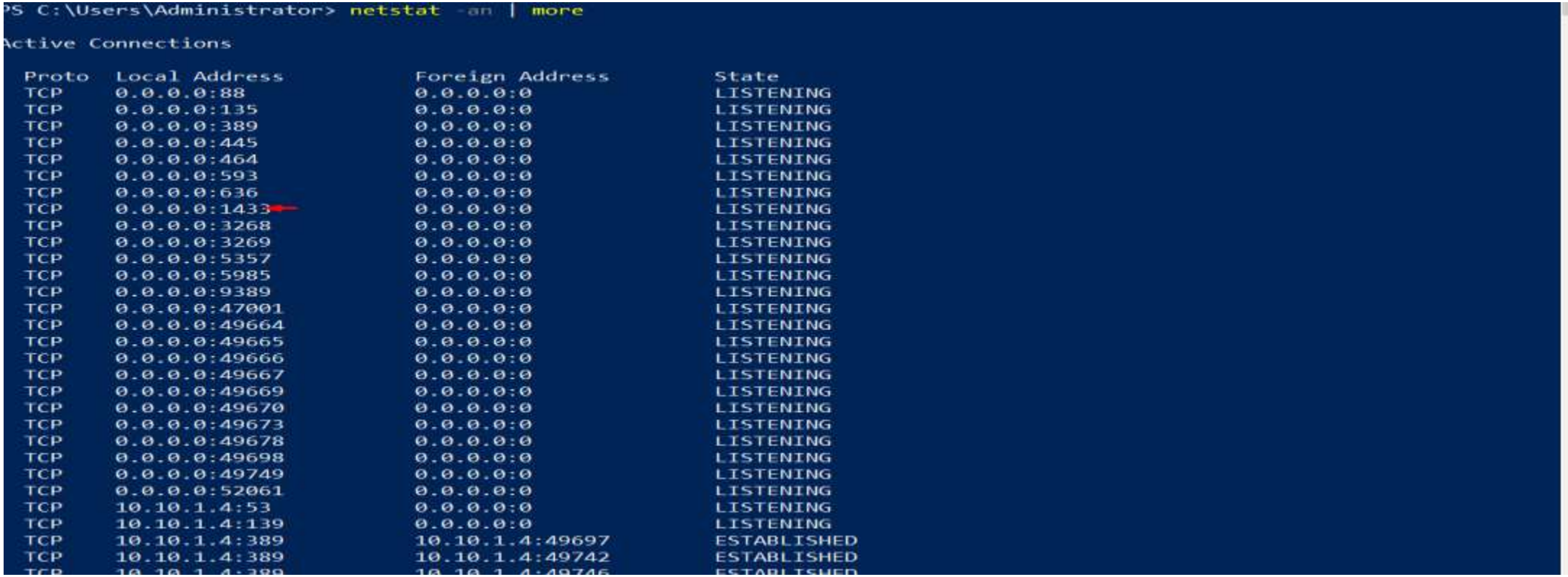
Lab Setup

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



Lab Setup

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

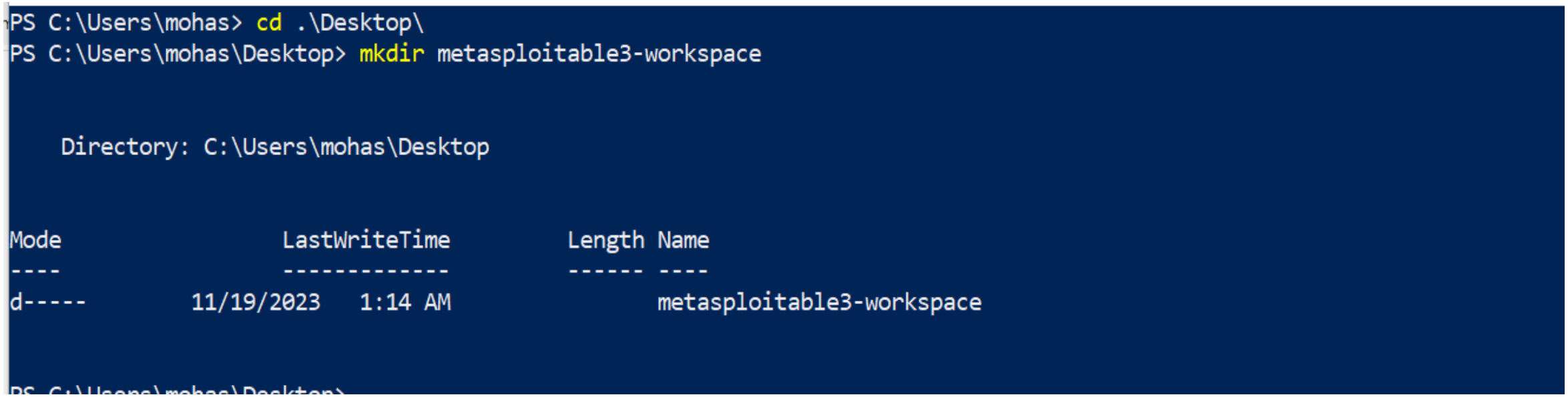
Instruction

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

Lab Setup

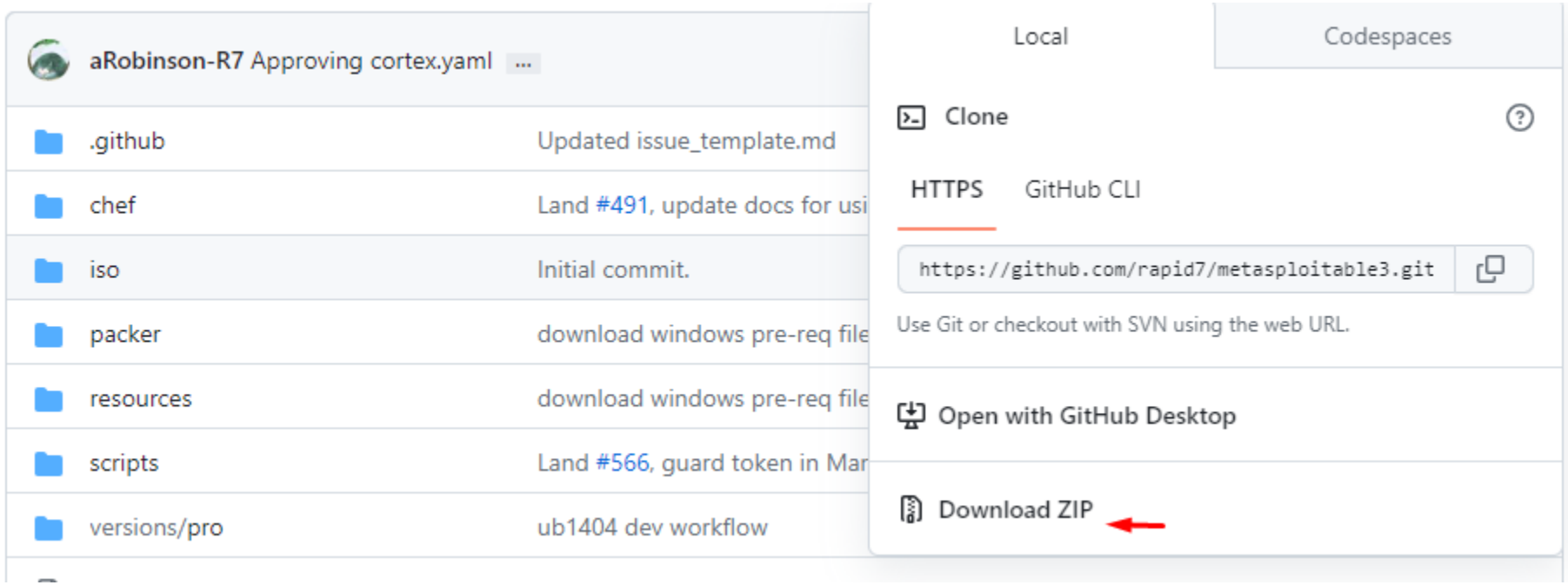
Installing Metasploitable3 on windows server 2008, Let's follow the Installation guide on rapid7 github page

https://github.com/rapid7/metasploitable3



Lab Setup

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



Lab Setup

Downloading requirement

Building Metasploitable 3

System Requirements:

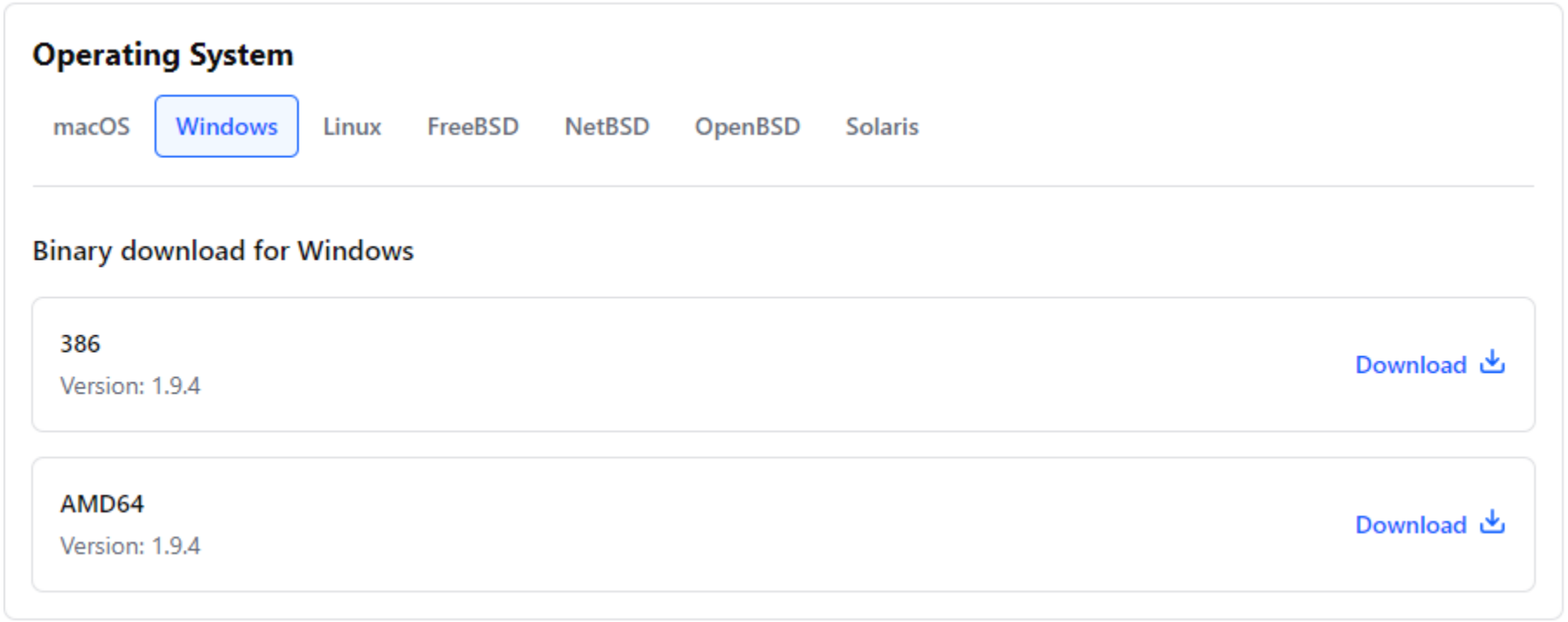
- OS capable of running all of the required applications listed below
- VT-x/AMD-V Supported Processor recommended
- 65 GB Available space on drive
- 4.5 GB RAM

Requirements:

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

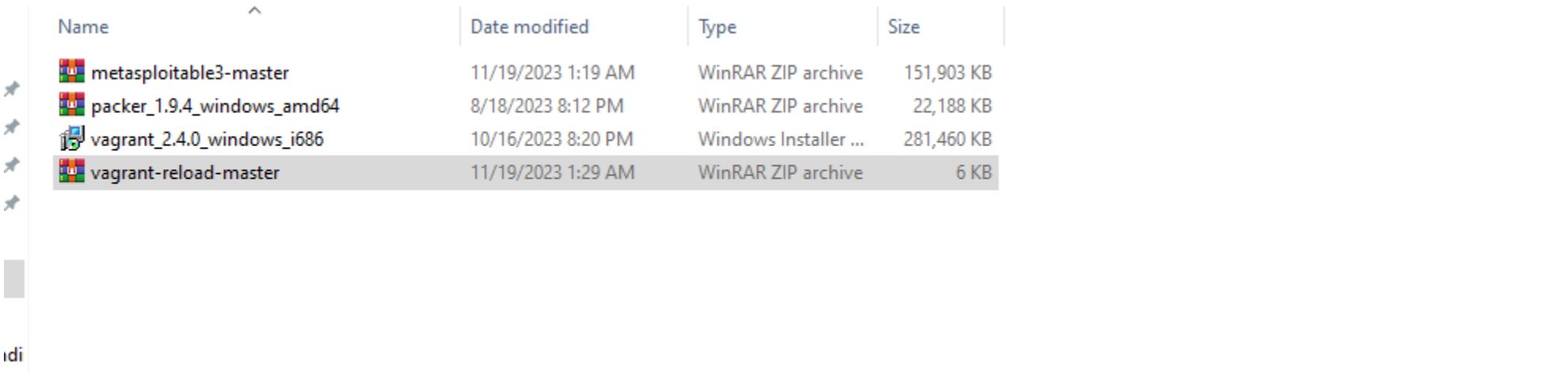
Lab Setup

Downloading and Installing Packer



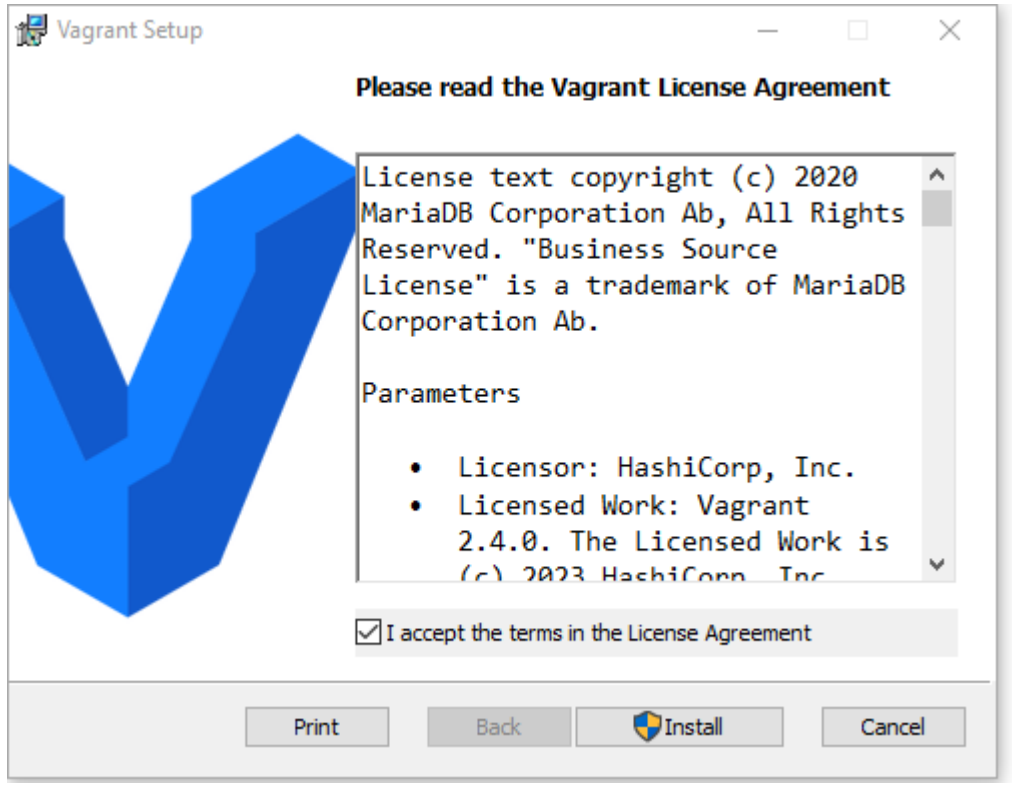
Lab Setup

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



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
```

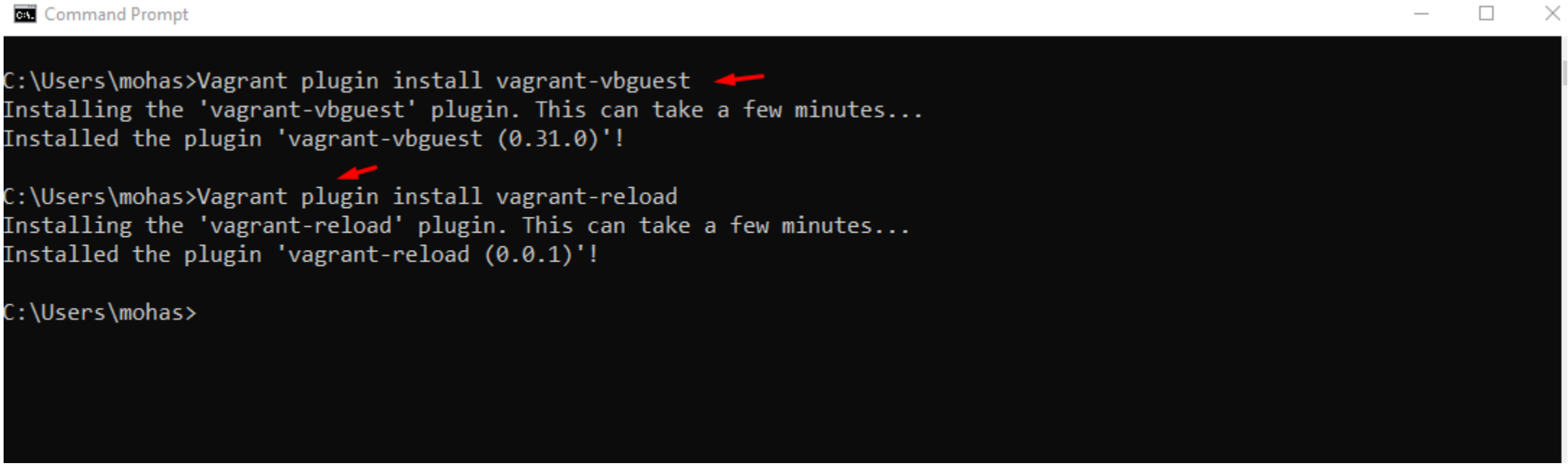
Lab Setup

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/me
tasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"
PS C:\Users\mohas\Desktop\metasploitable3-workspace>
```

Lab Setup

Now open your command prompt and install some dependencies with vagrant



Lab Setup

It is now time to build the VM using a powershell script called build.ps1 inside metasplitable3 folder we downloaded, running the script without any argument with 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
```

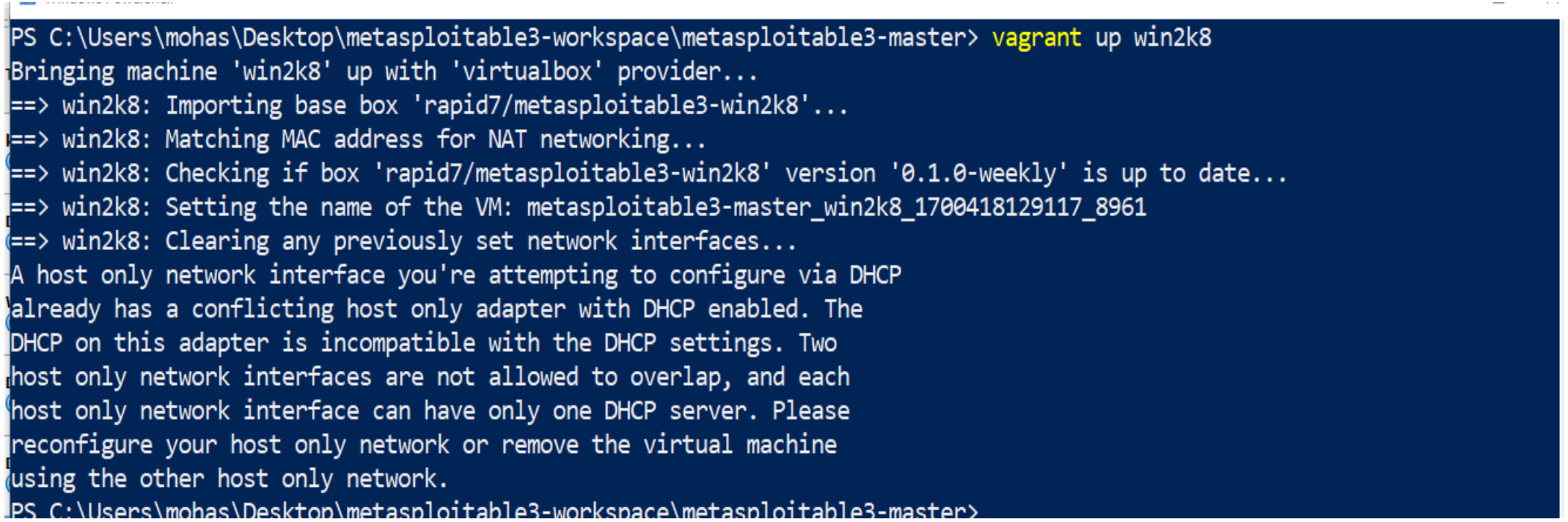
Lab Setup

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/VBoxGuestAdditions.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

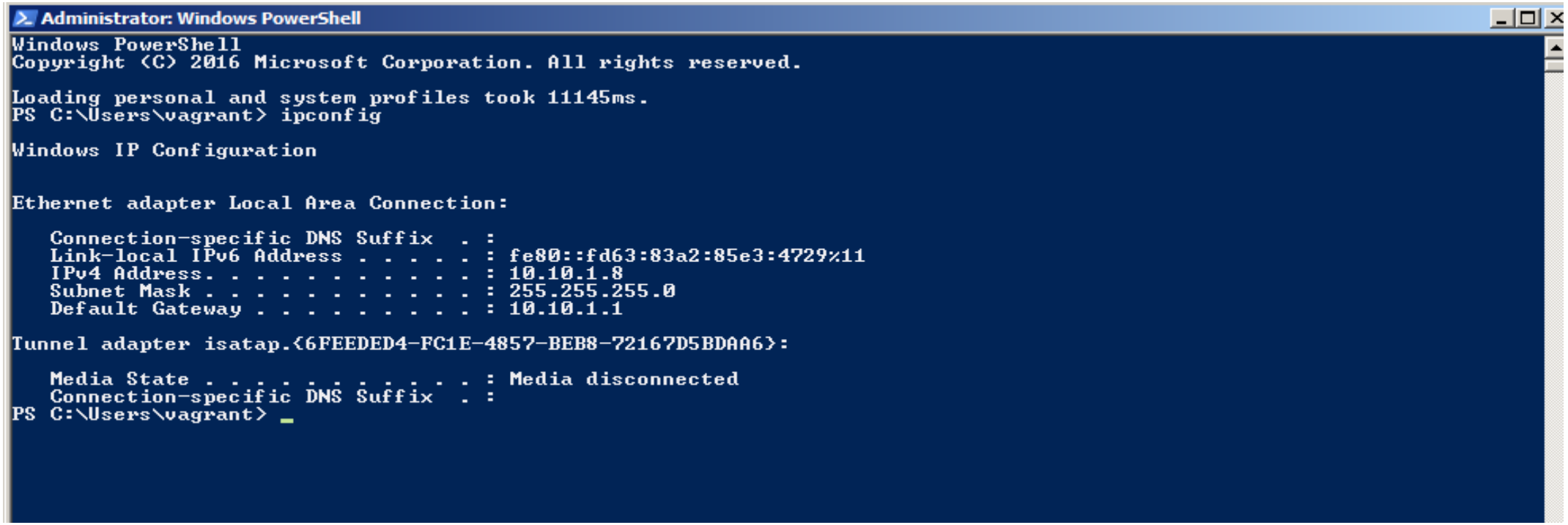


Lab Setup

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

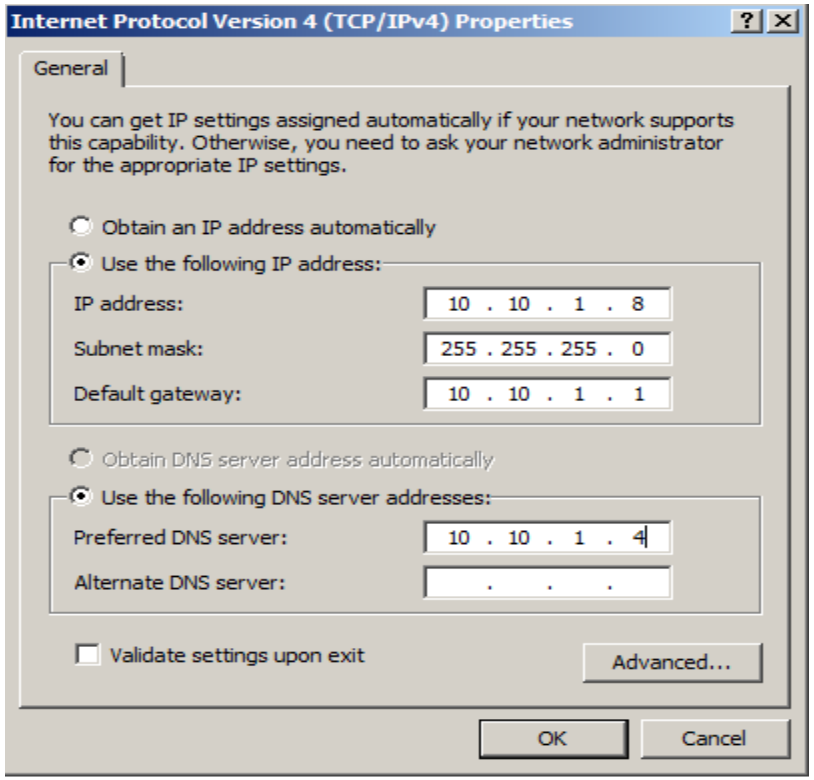
Lab Setup

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



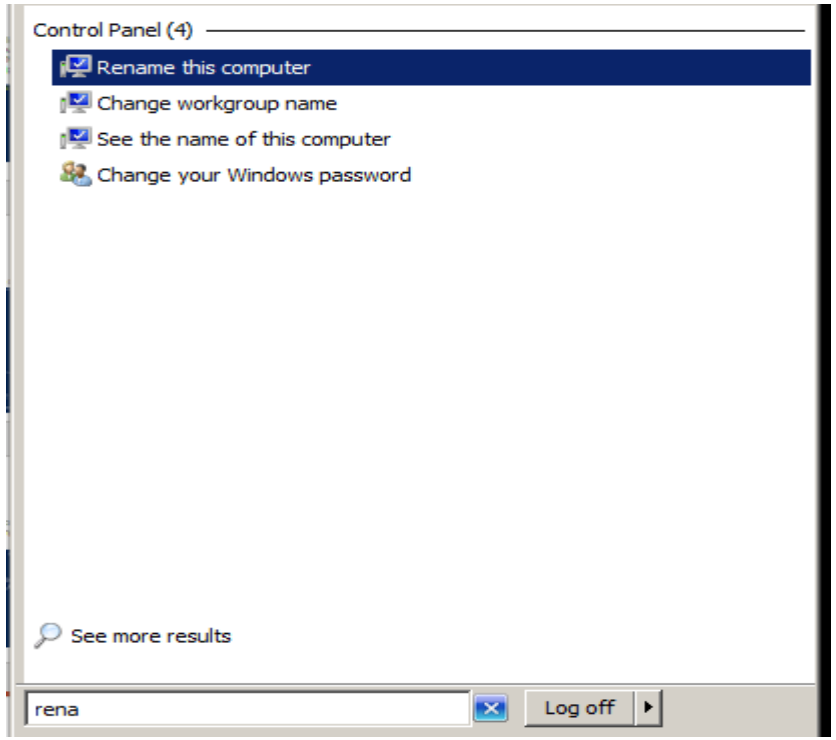
Lab Setup

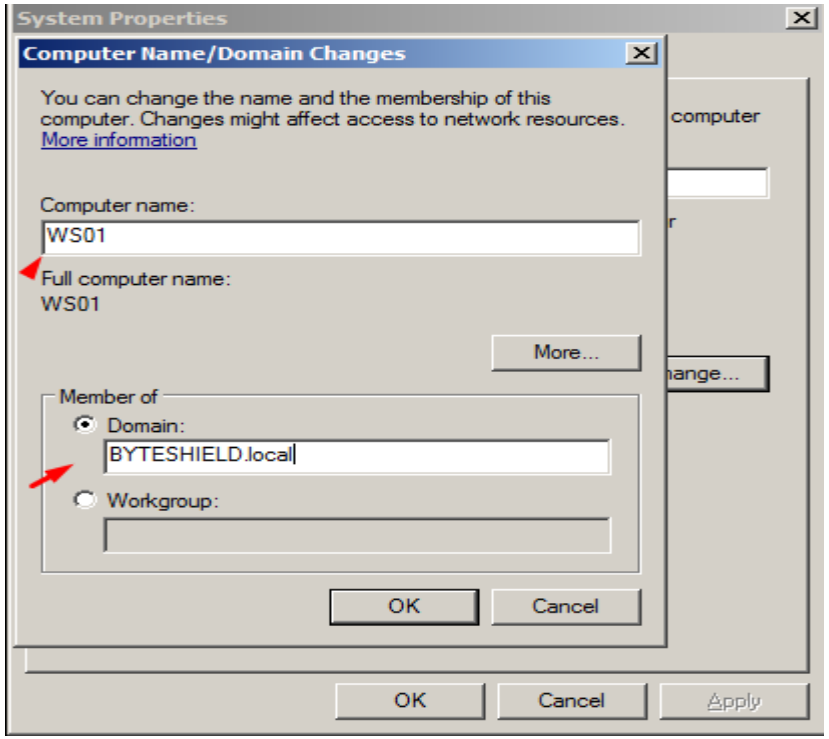
Here is the IPv4 Static Configuration



Lab Setup

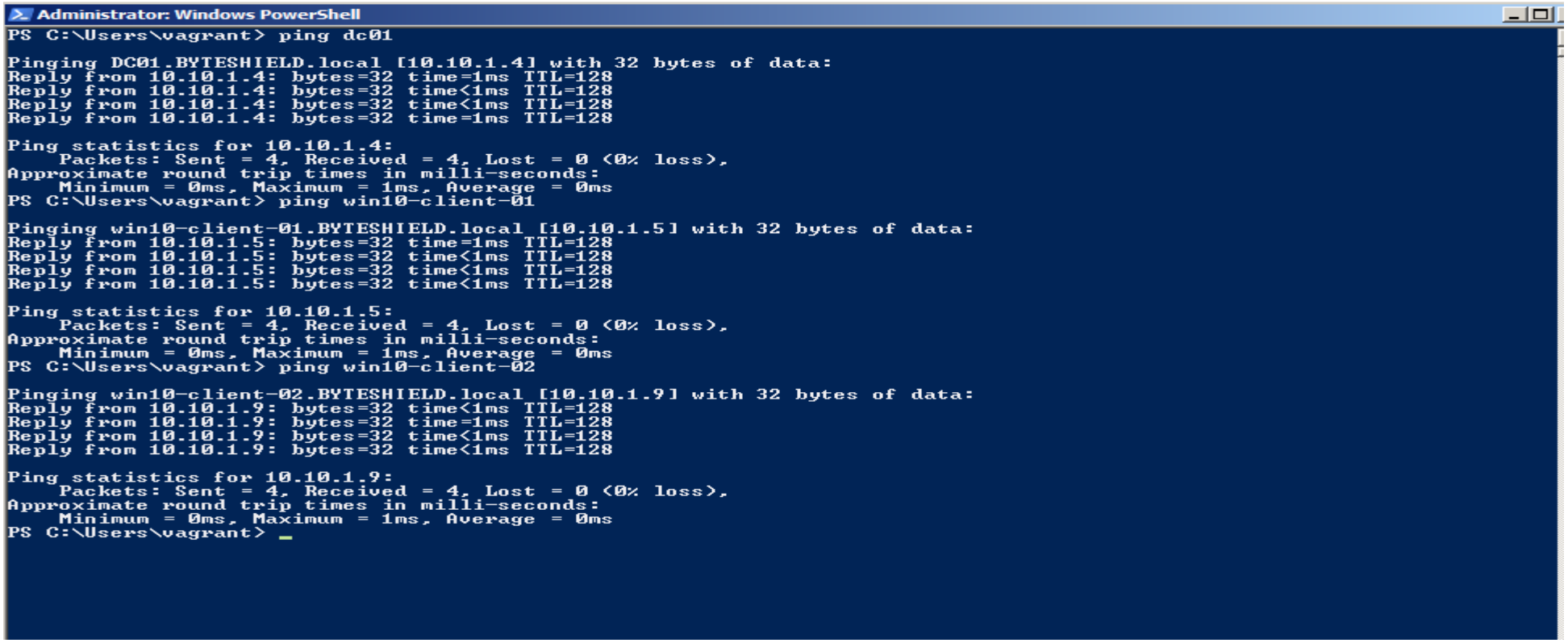
Search for rename this Computer to change the name of the computer to WS01 and join it to Byteshield Domain





Lab Setup

Now We can Verify our setup



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

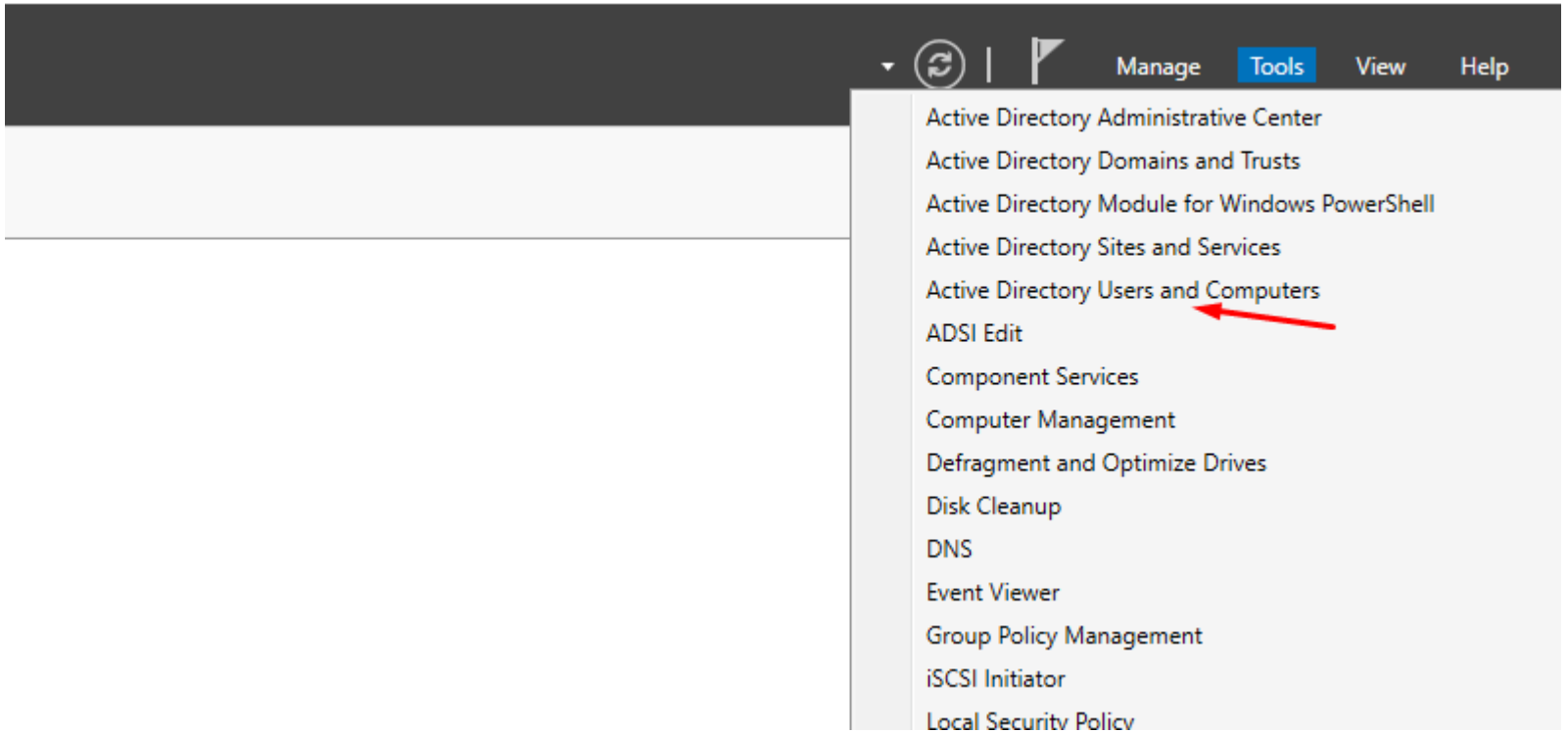
Win10-Client-02 Users

Ruth.David Brown.lee Richard.White

Clement.Kevin michelle.Moore

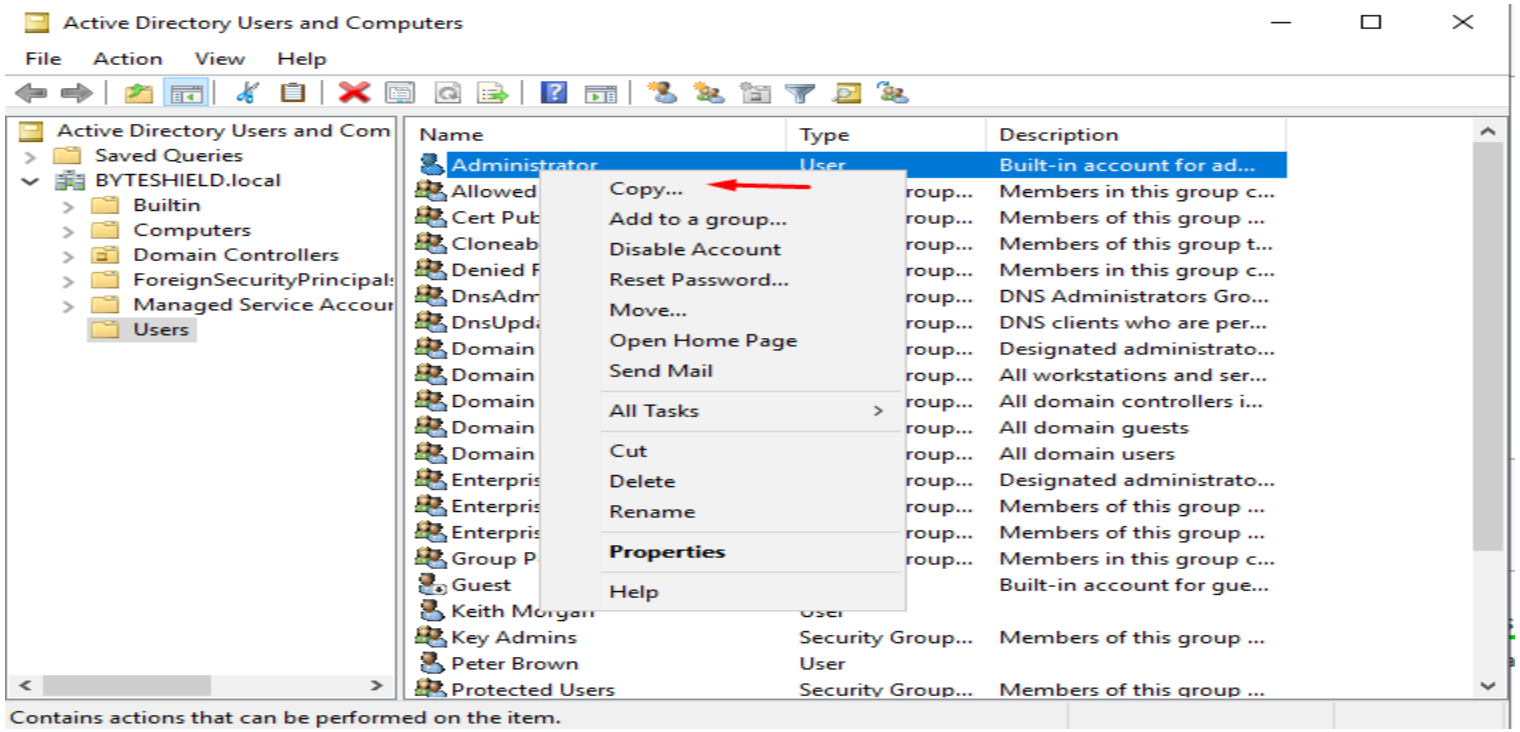
Lab Setup

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



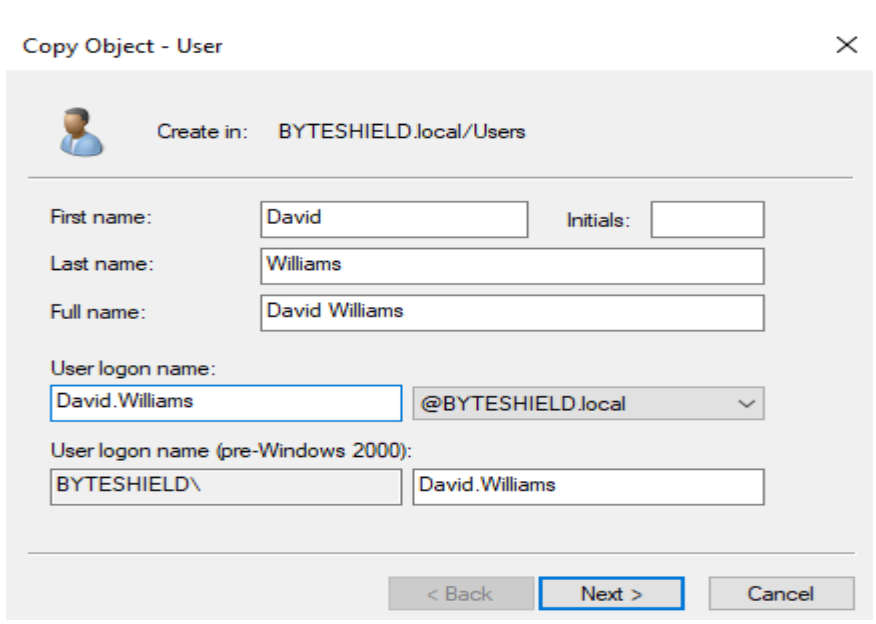
Lab Setup

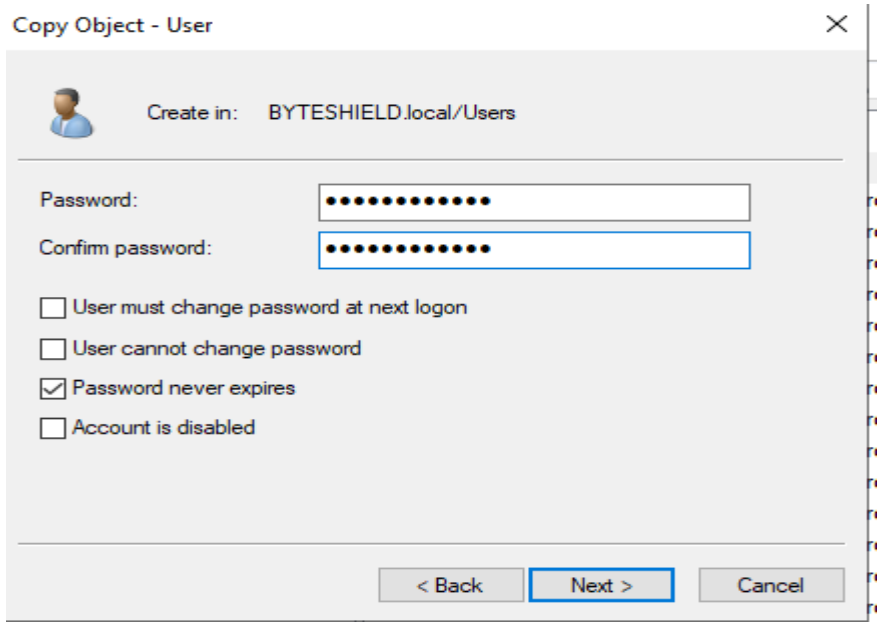
Right click on the administrator and click copy to Create an Admin user



Lab Setup

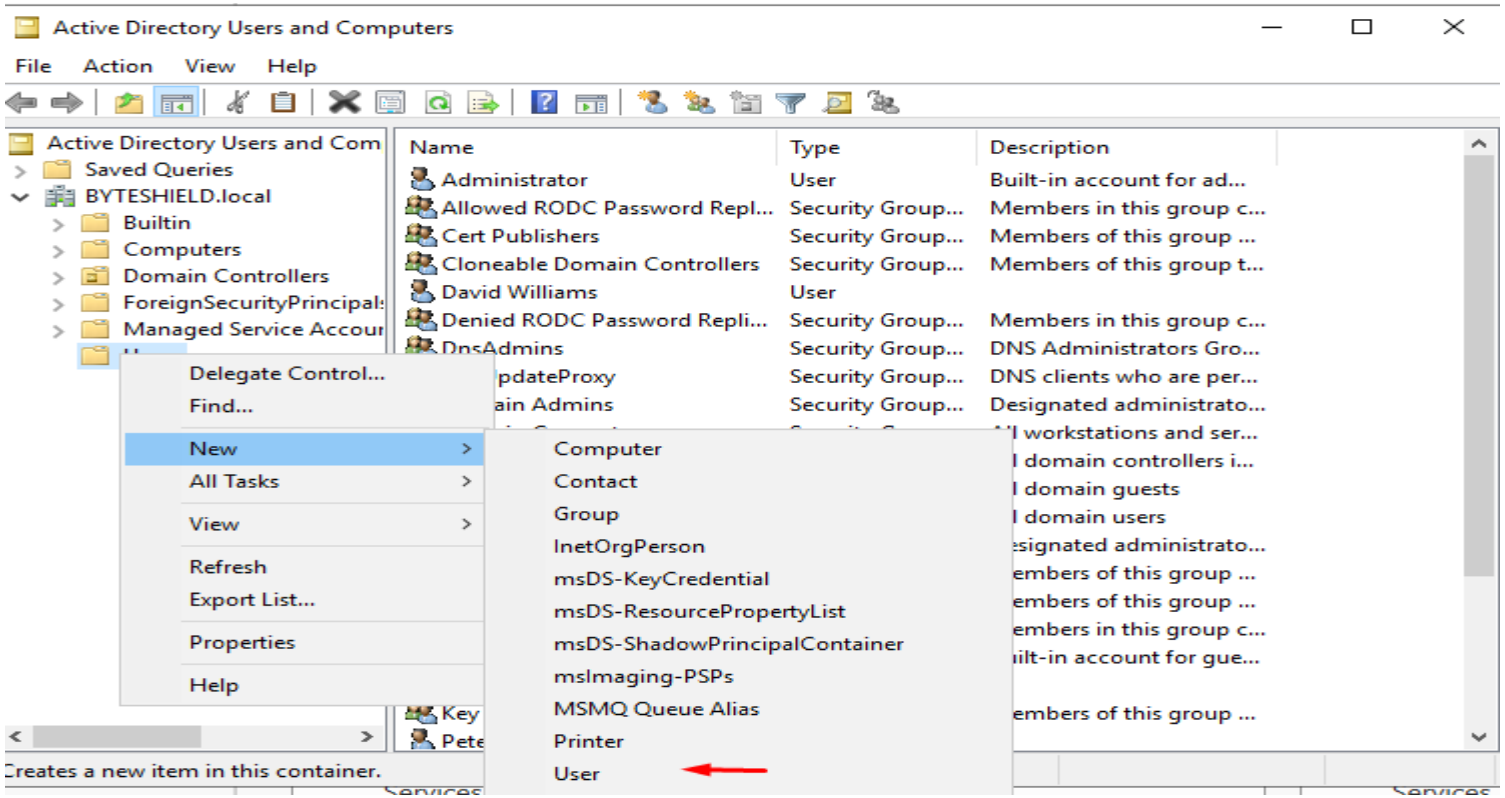
David Williams as Admin User





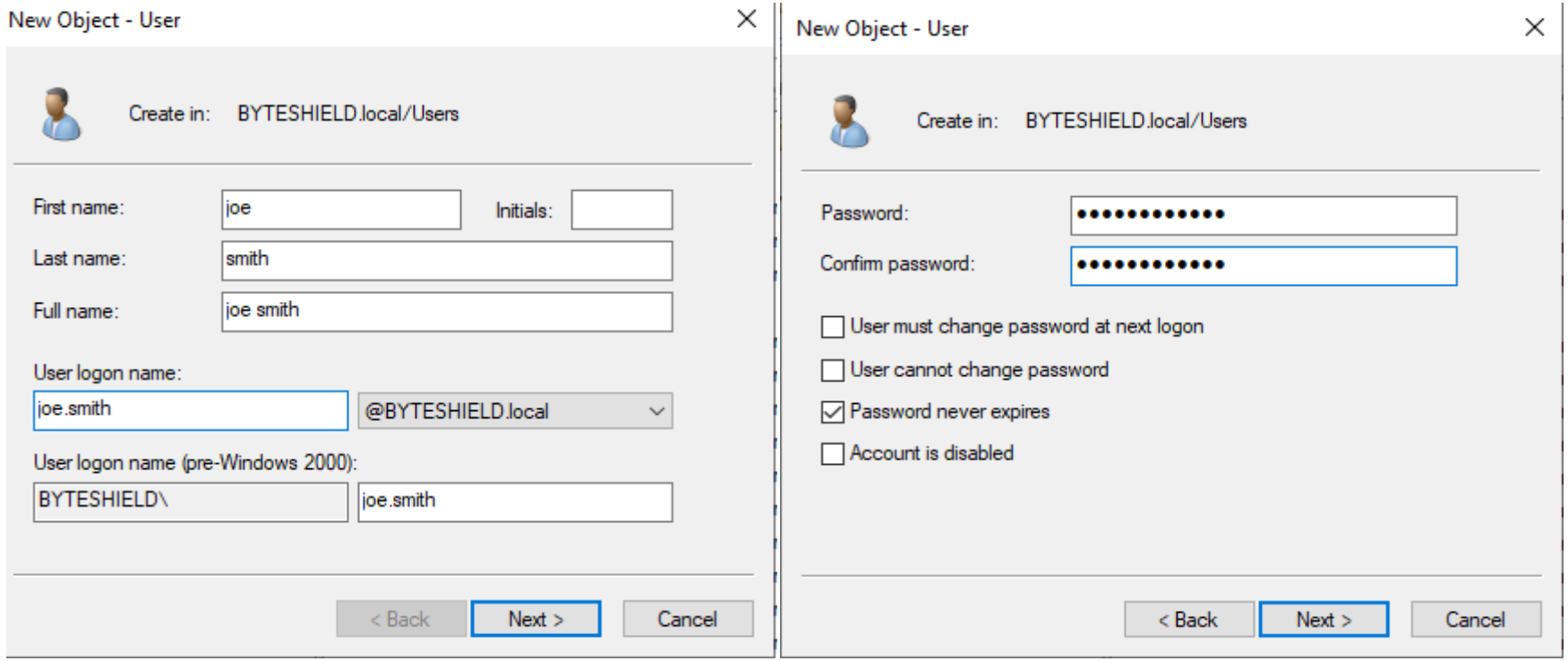
Lab Setup

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



Lab Setup

Joe Smith as a regular user



Lab Setup

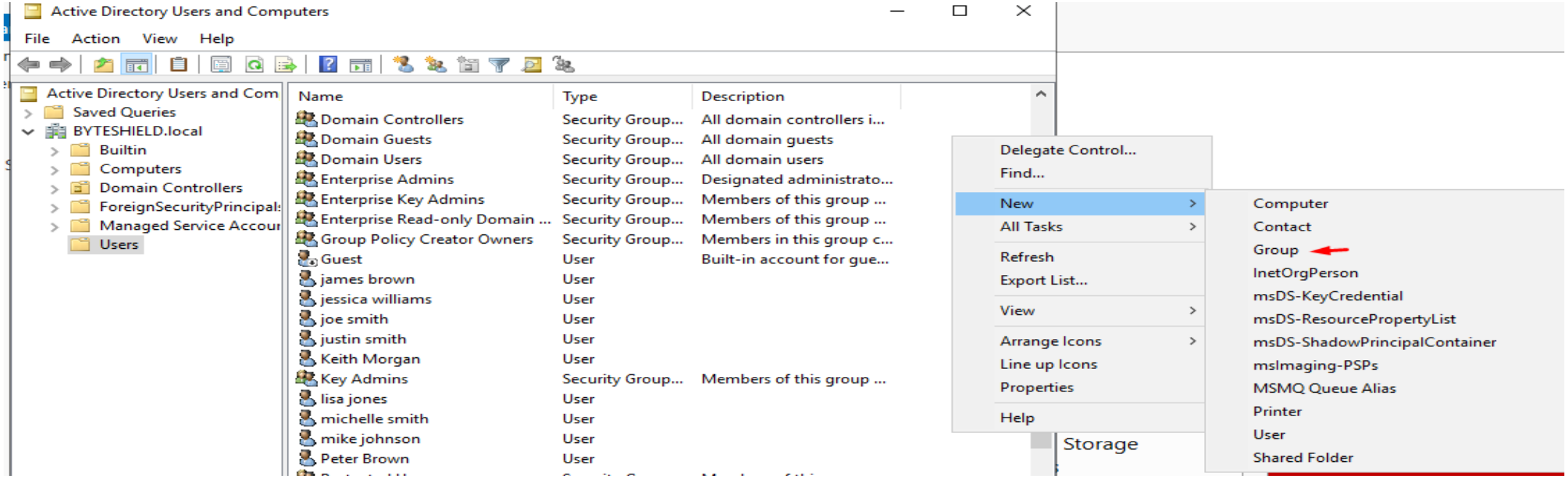
We have Created two domain users, admin and a regular user

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

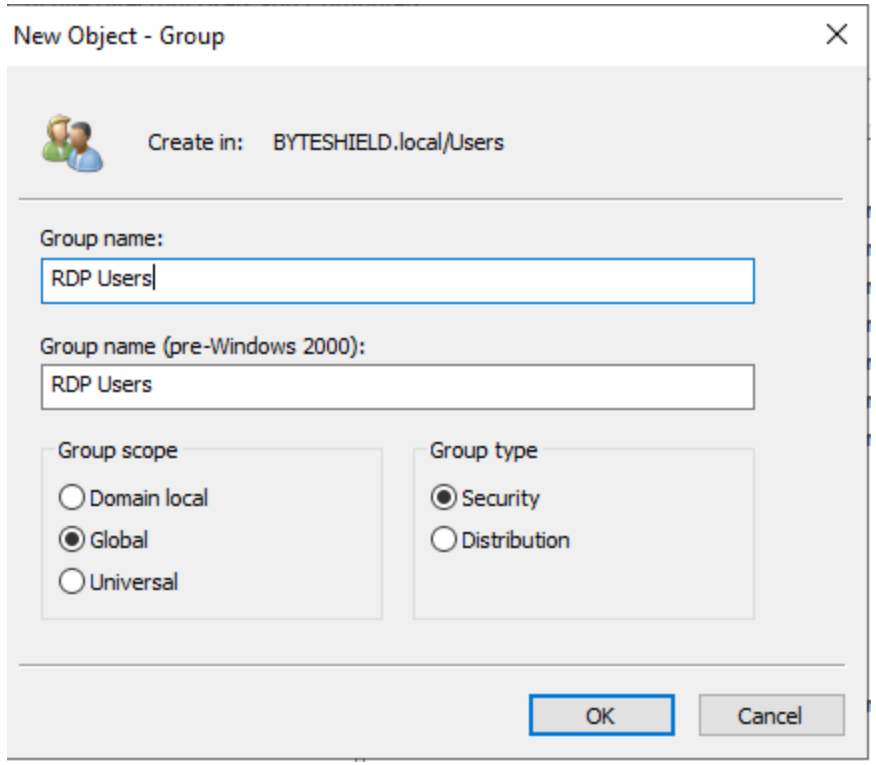
Lab Setup

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



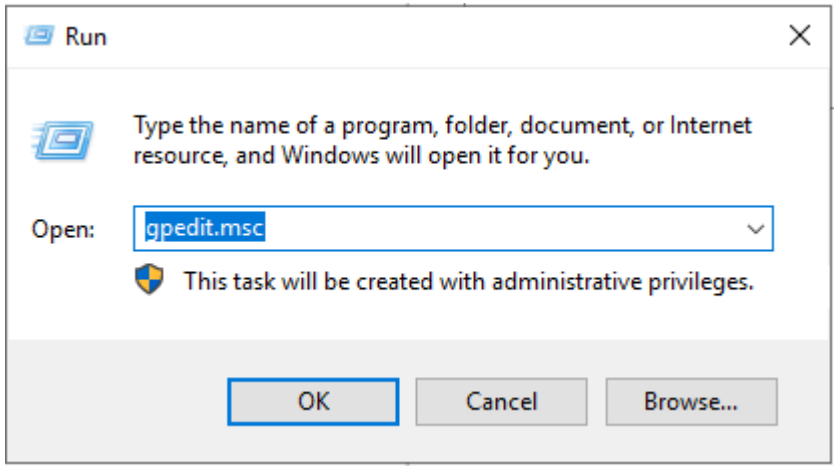
Lab Setup

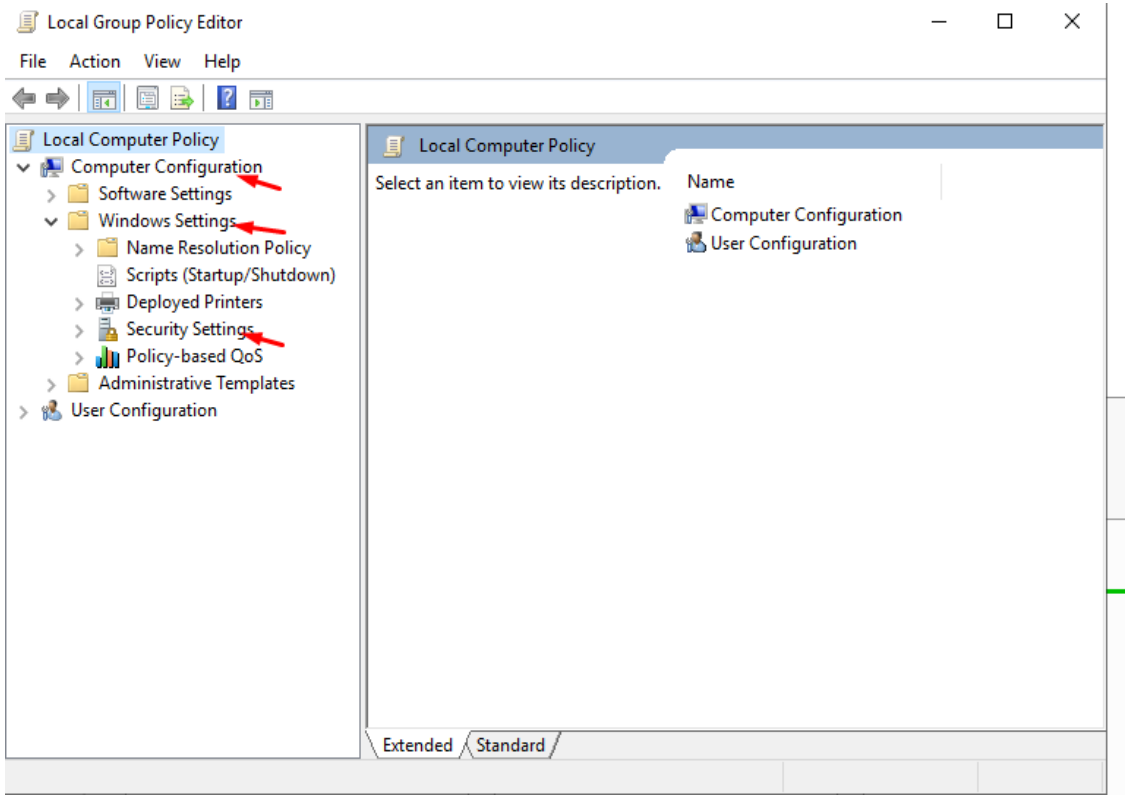
Remote Desktop Users Group Creattion



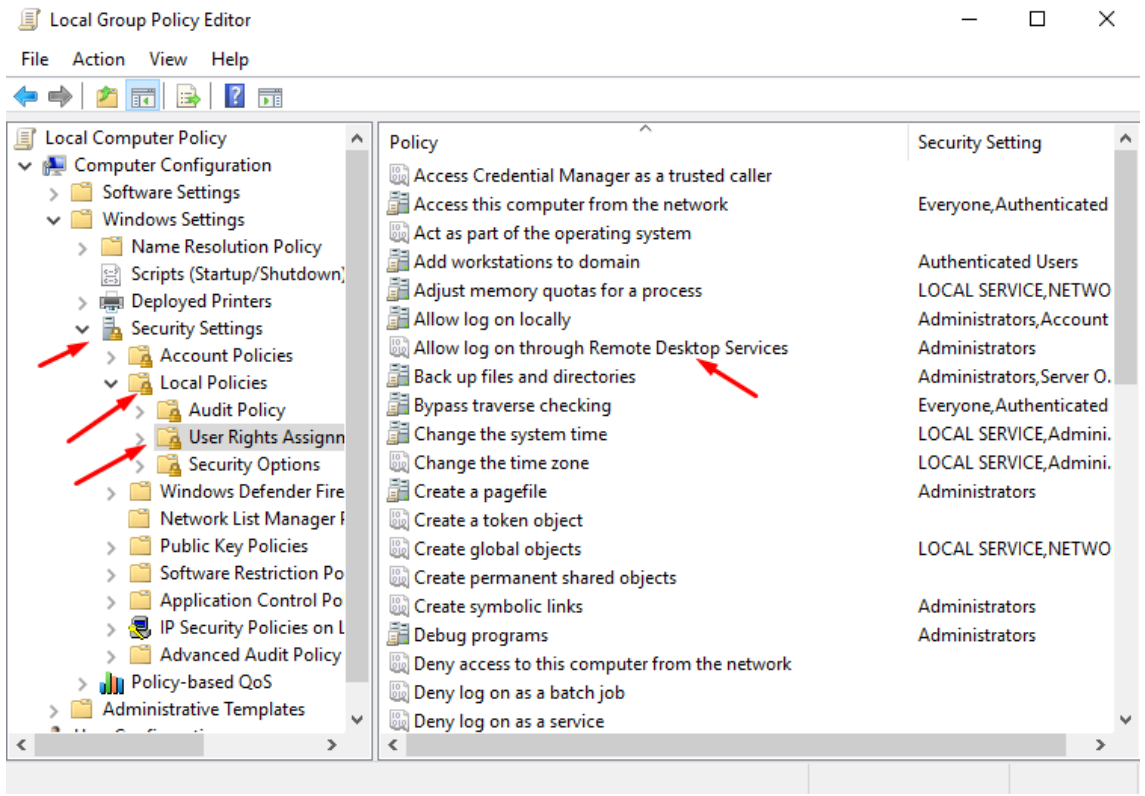
Lab Setup

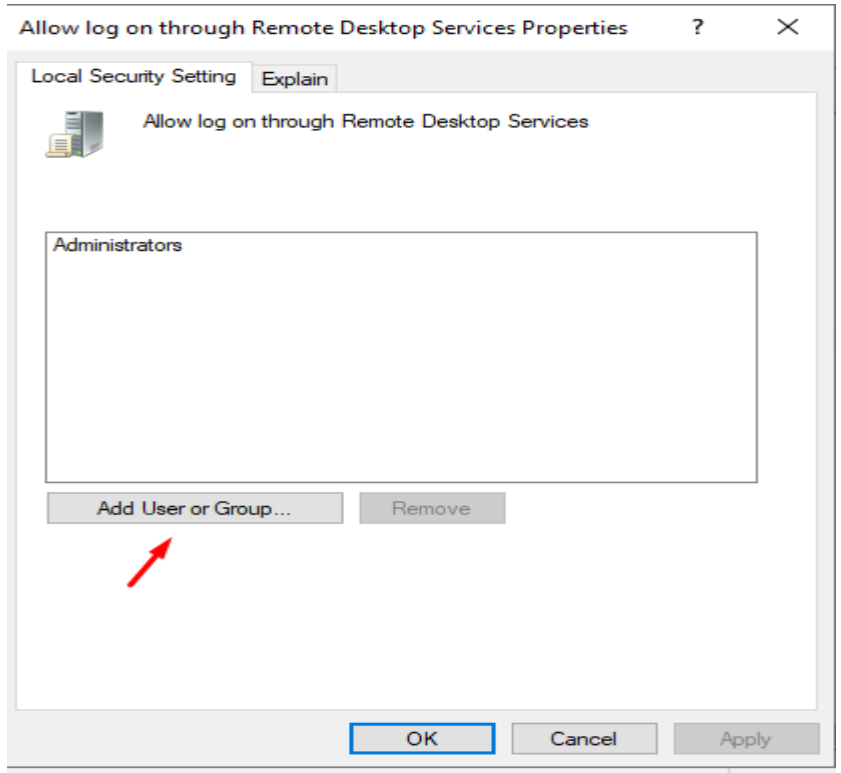
Now let’s Create localuser group Policy for remote desktop access





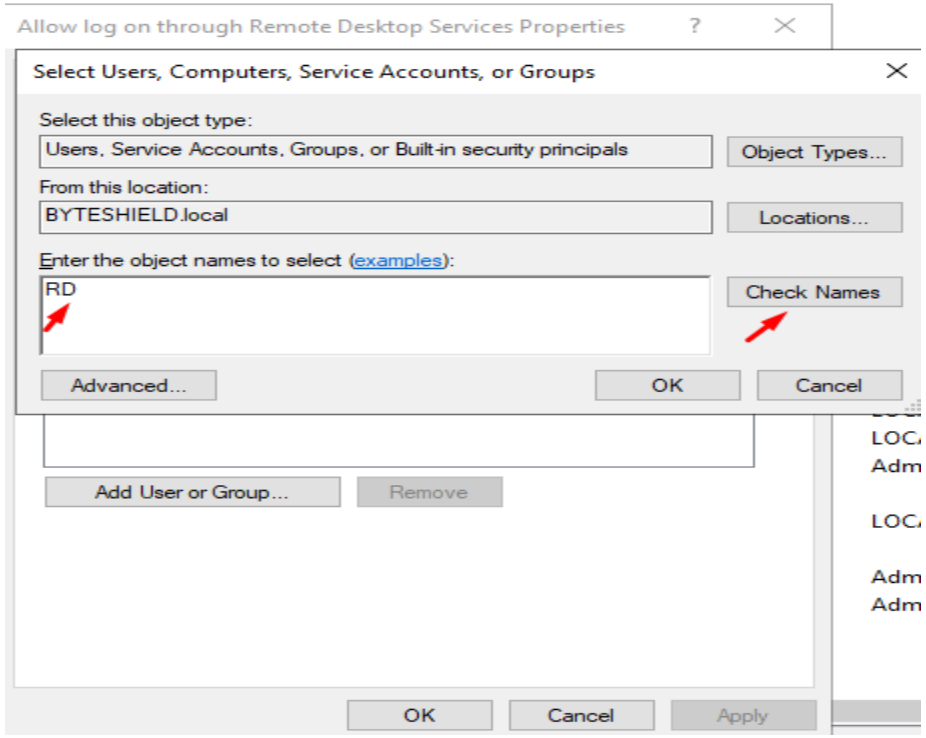
Lab Setup

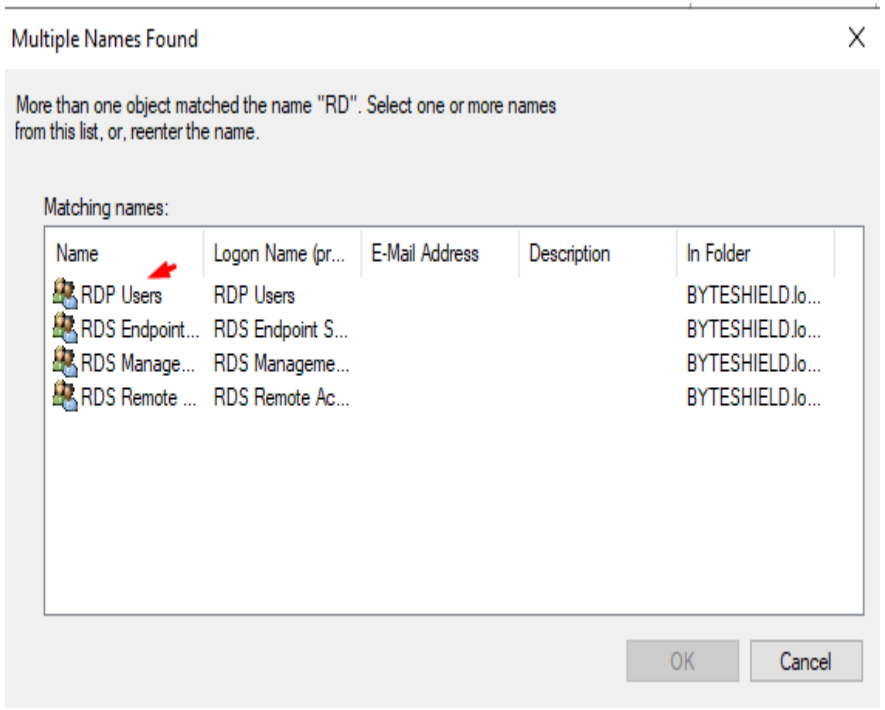

Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignn
Security Options
Windows Defender Fire
Network List Manager P
Public Key Policies
Software Restriction Po
Application Control Po
IP Security Policies on L
Advanced Audit Policy
Policy-based QoS
Administrative Templates
Policy
Security Setting
Access Credential Manager as a trusted caller
Access this computer from the network
Everyone,Authenticated
Act as part of the operating system
Add workstations to domain
Authenticated Users
Adjust memory quotas for a process
LOCAL SERVICE,NETWO
Allow log on locally
Administrators,Account
Allow log on through Remote Desktop Services
Administrators
Back up files and directories
Administrators,Server O.
Bypass traverse checking
Everyone,Authenticated
Change the system time
LOCAL SERVICE,Admini.
Change the time zone
LOCAL SERVICE,Admini.
Create a pagefile
Administrators
Create a token object
Create global objects
LOCAL SERVICE,NETWO
Create permanent shared objects
Create symbolic links
Administrators
Debug programs
Administrators
Deny access to this computer from the network
Deny log on as a batch job
Deny log on as a service


Allow log on through Remote Desktop Services Properties
Local Security Setting
Explain
Allow log on through Remote Desktop Services
Administrators
Add User or Group...
Remove
OK
Cancel
Apply

Lab Setup

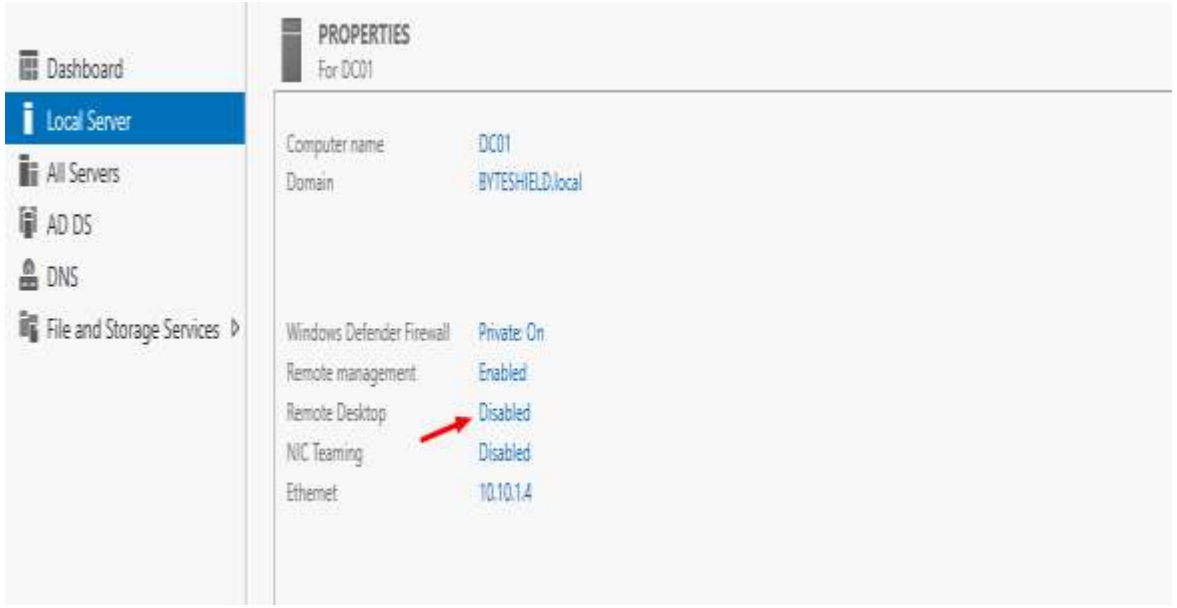
Now Let’s Search for the RDP users Group we just Created

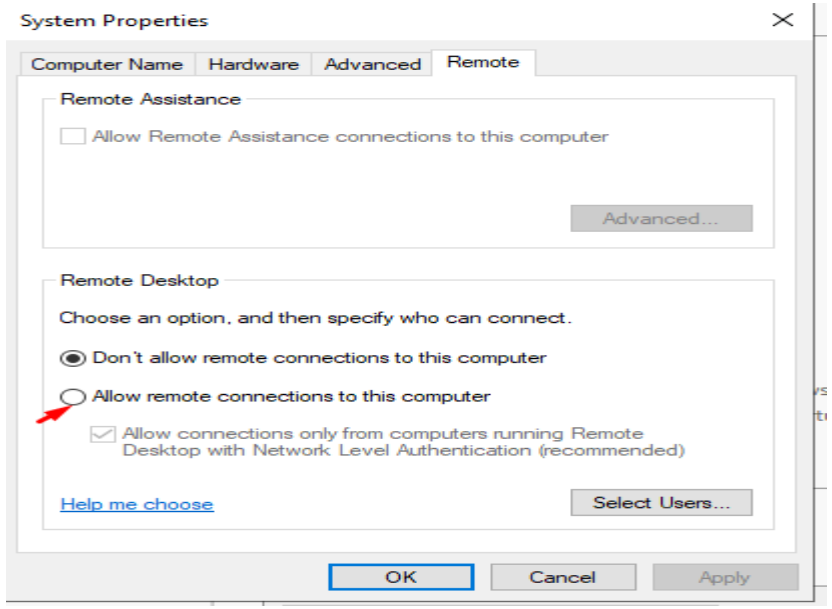




Lab Setup

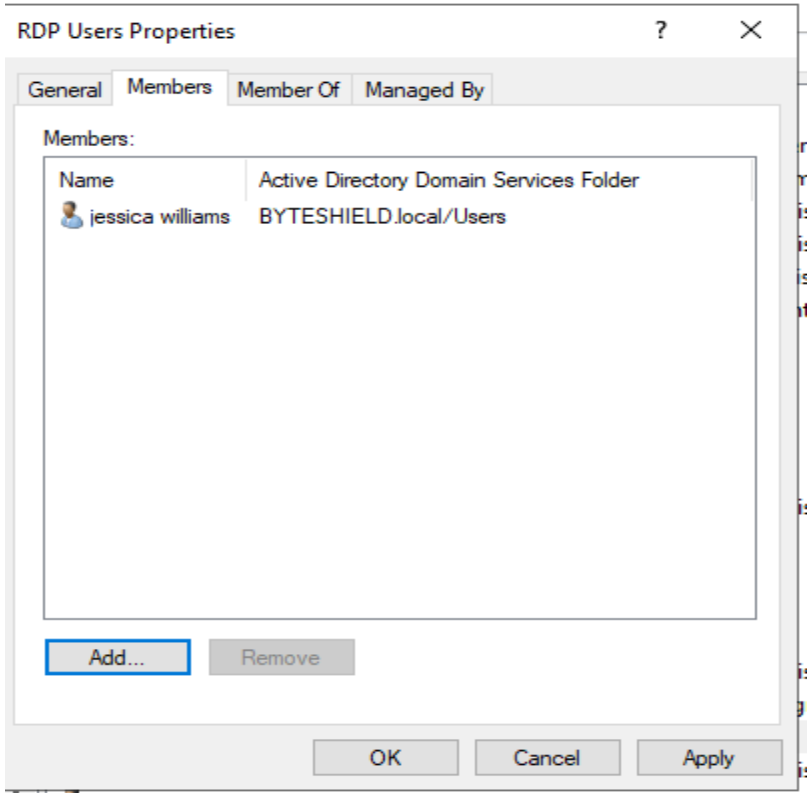
Remote Desktop Service is disabled by default, we can enable it

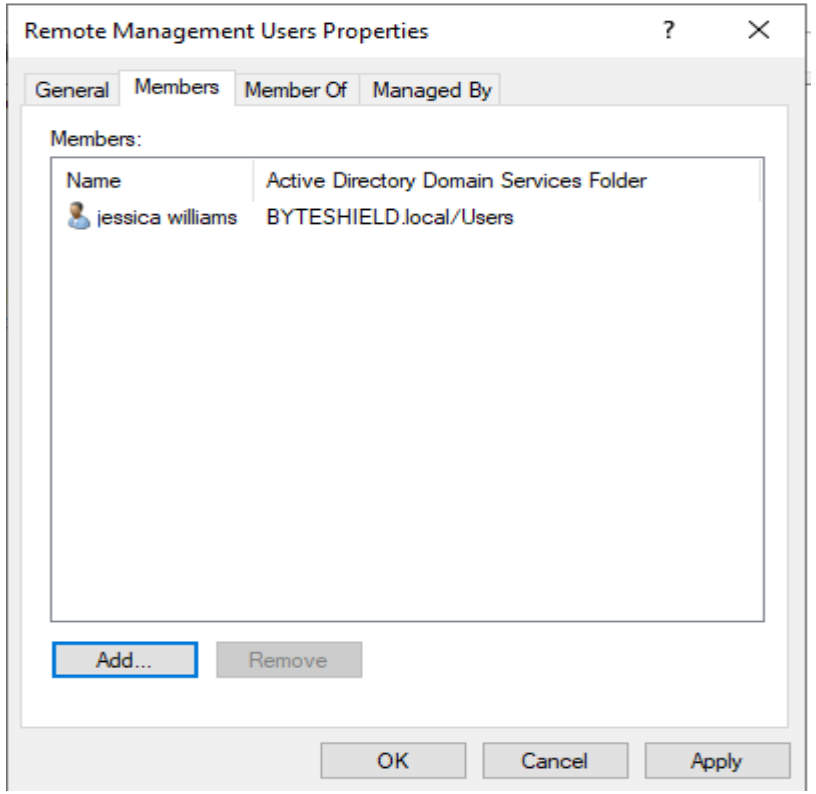




Lab Setup

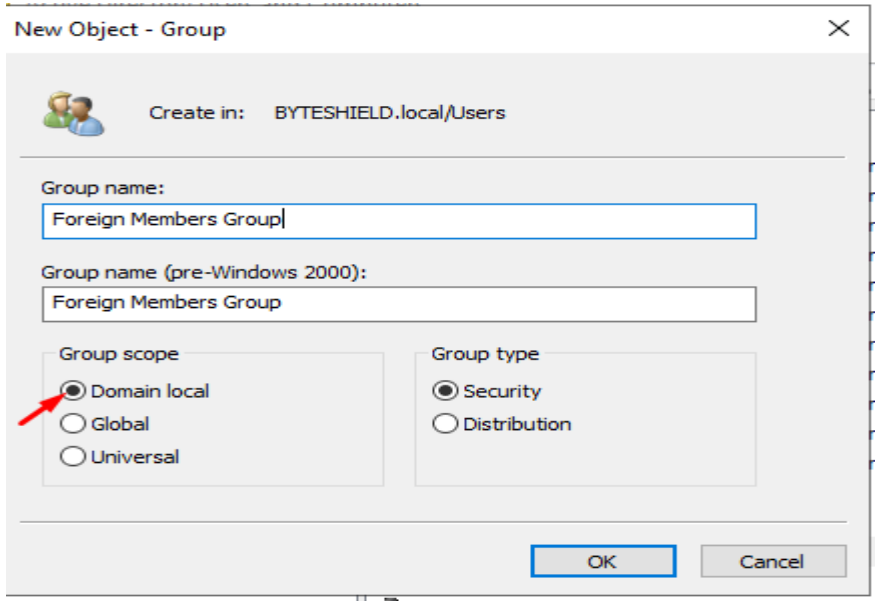
Let’s Jessica Williams to the RDP users and Remote management service Groups

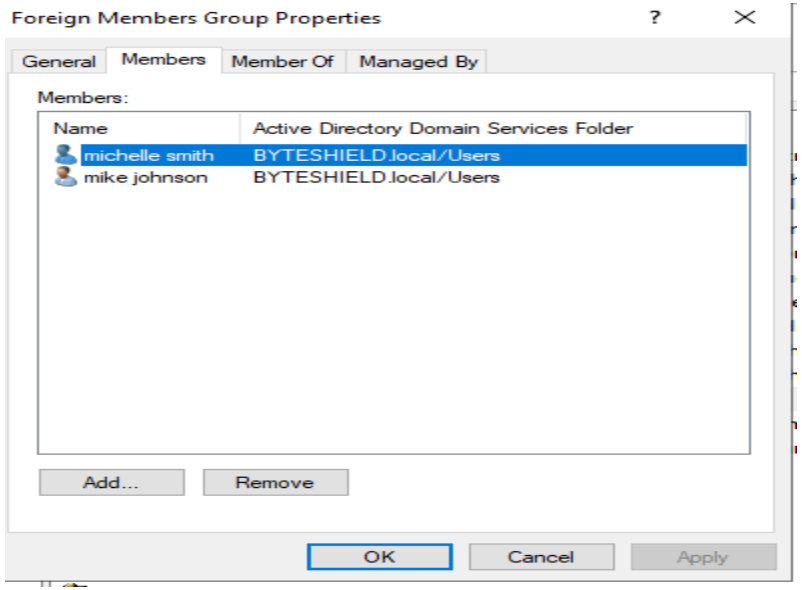




Lab Setup

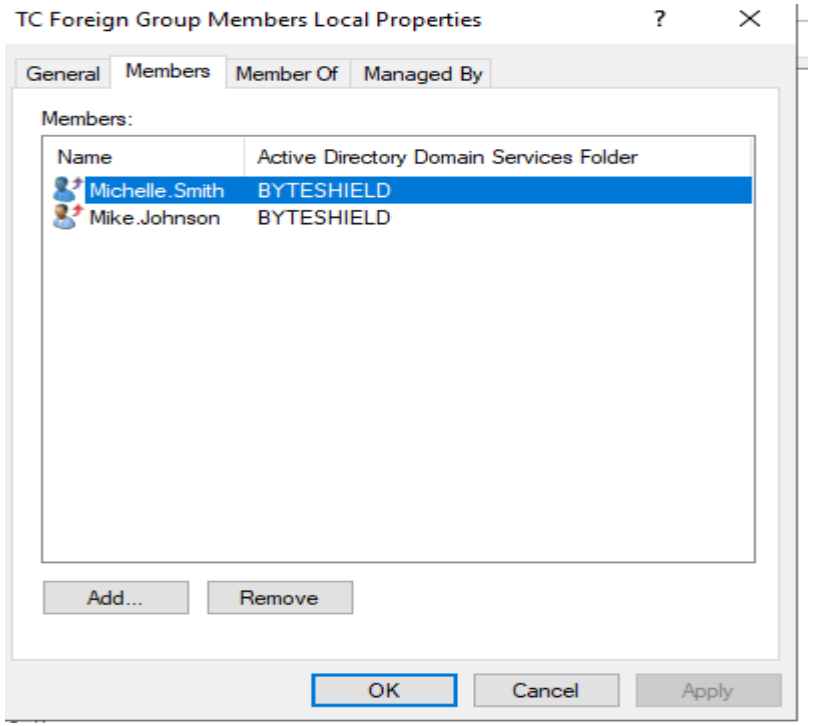
Foreign Group membership, we are Create a local and Universal BYTESHIELD Domain Group and map them to TRUSTEDCORP as Foreign Members and and vise versa, By default Domain groups are created as global groups, we will change that to domain local group, we have michelle and mike as member of the domain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

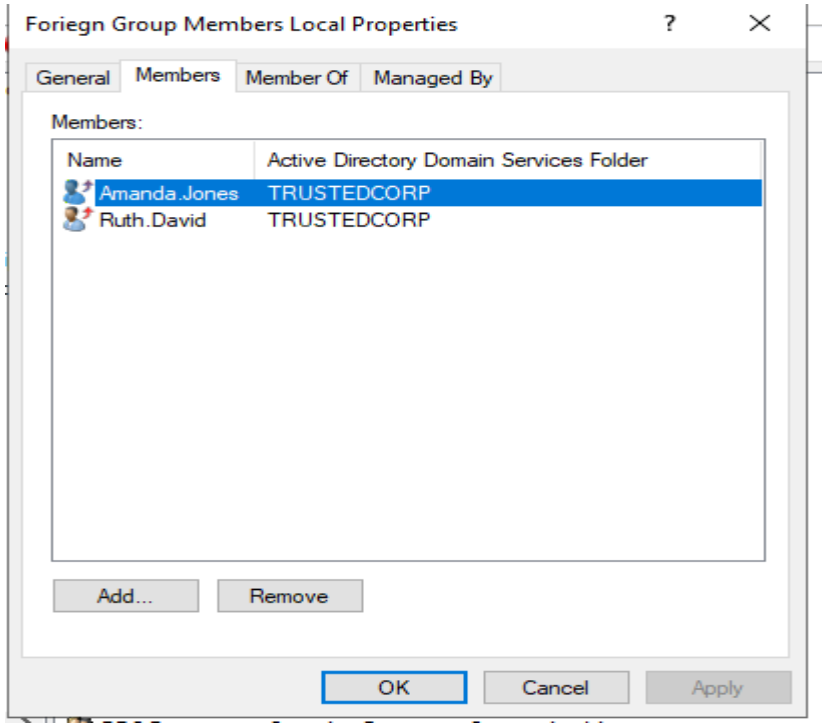




Lab Setup

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



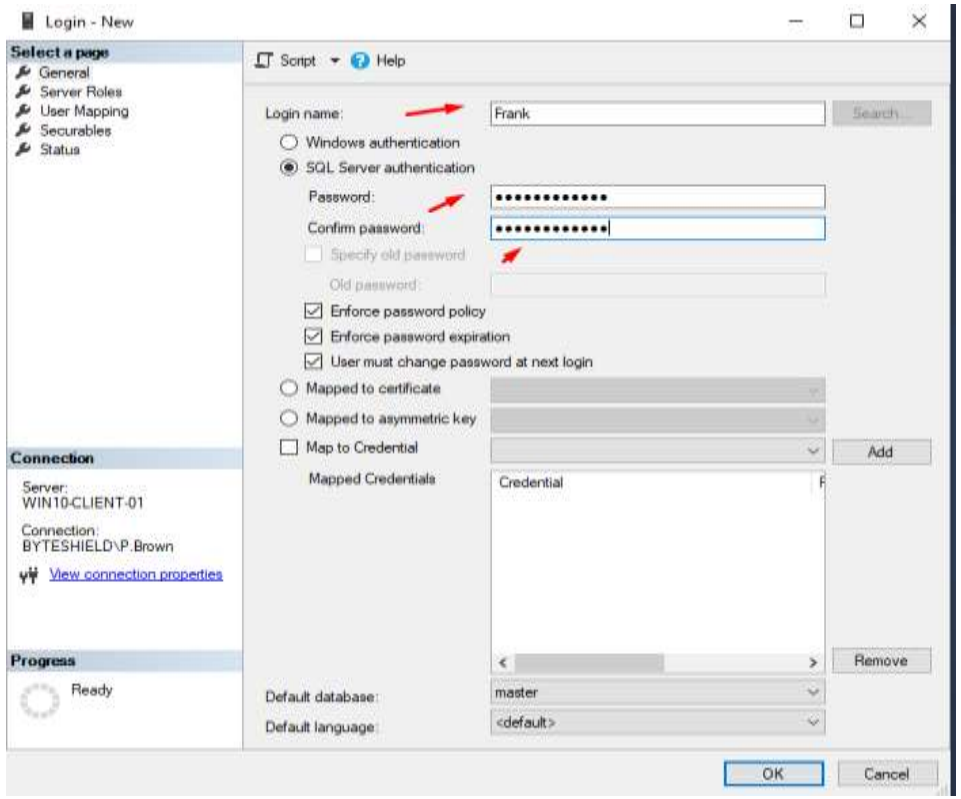


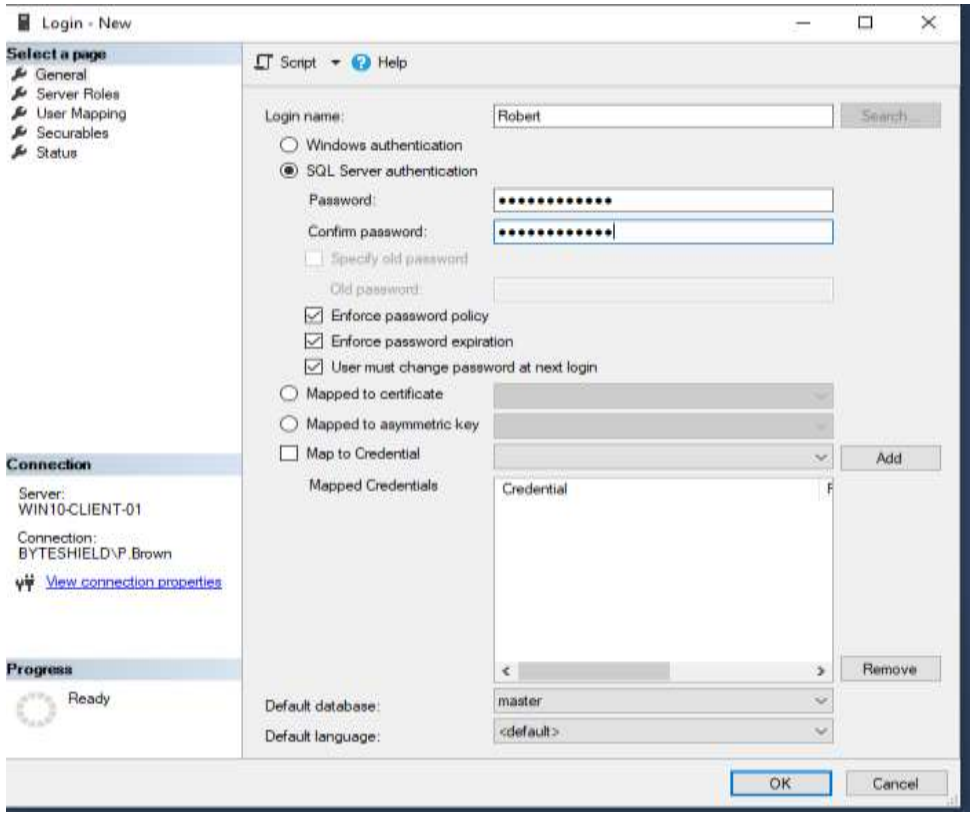
Lab Setup

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

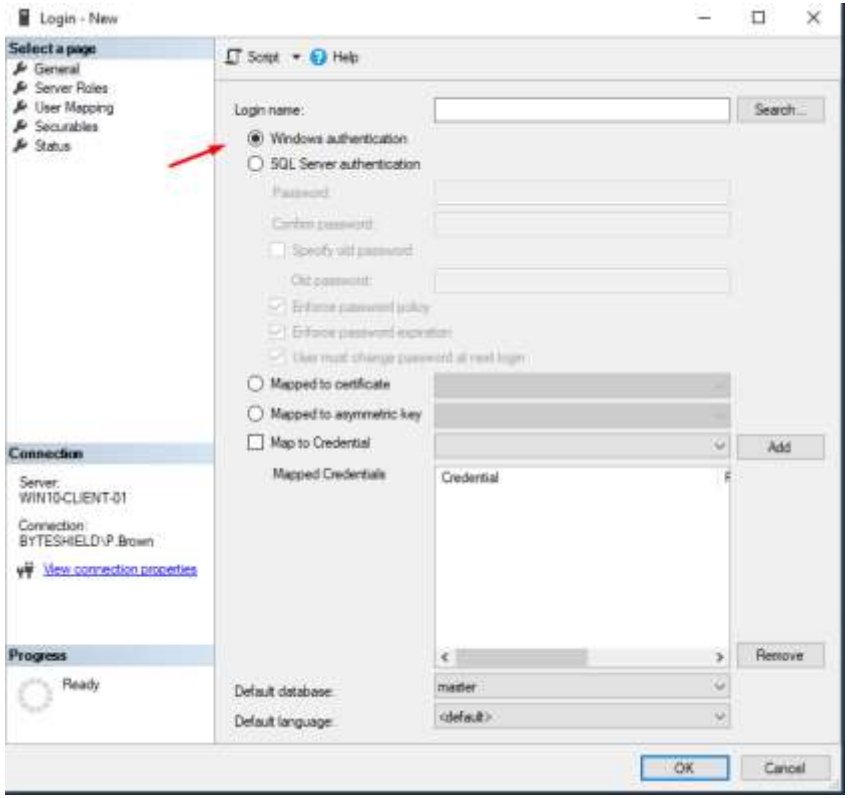
Lab Setup

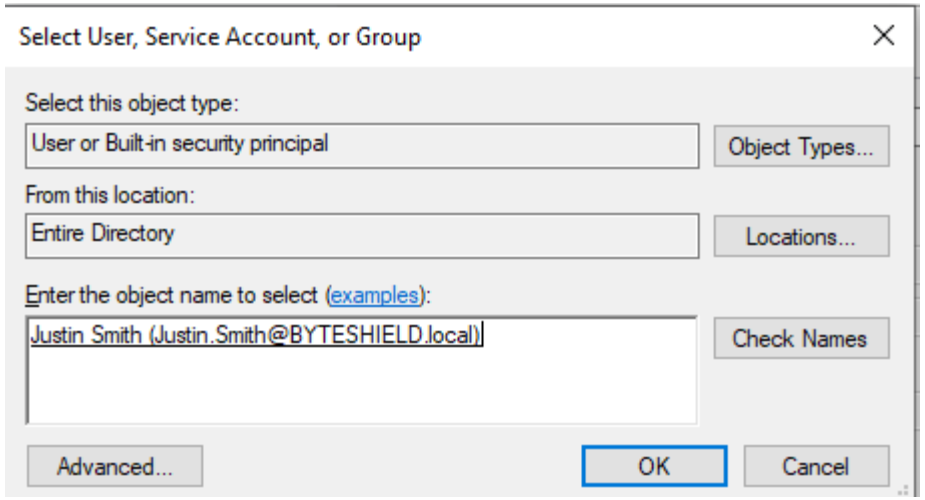
Creating SQL User





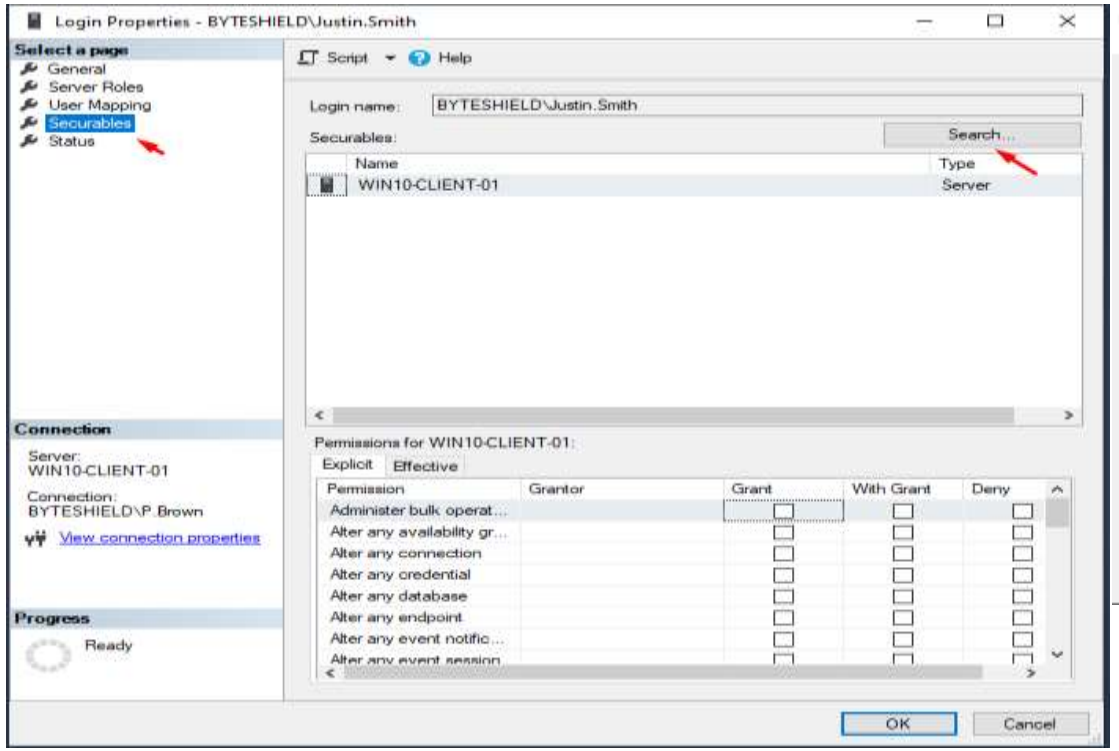
Lab Setup

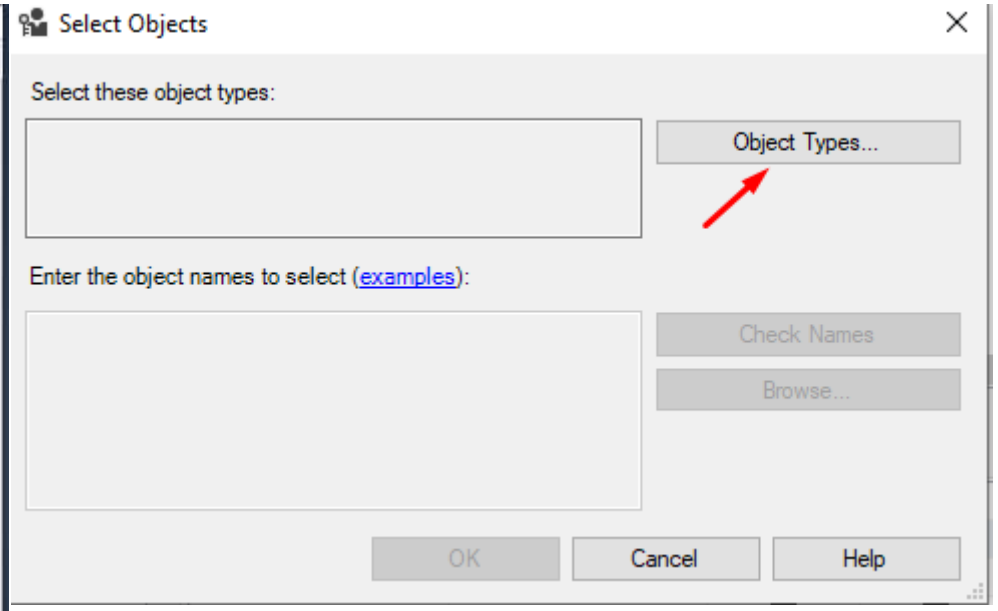

Login - New
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Login name:
Search...
Windows authentication
SQL Server authentication
Password:
Confirm password:
Specify old password
Old password:
Enforce password policy
Enforce password expiration
User must change password at next login
Mapped to certificate
Mapped to asymmetric key
Map to Credential
Add
Mapped Credentials
Credential
Remove
Connection
Server:
WIN10-CLIENT-01
Connection:
BYTESHIELD\P.Brown
View connection properties
Progress
Ready
Default database:
master
Default language:
<default>
OK
Cancel


Select User, Service Account, or Group
Select this object type:
User or Built-in security principal
Object Types...
From this location:
Entire Directory
Locations...
Enter the object name to select (examples):
Justin Smith (Justin.Smith@BYTESHIELD.local)
Check Names
Advanced...
OK
Cancel

Lab Setup

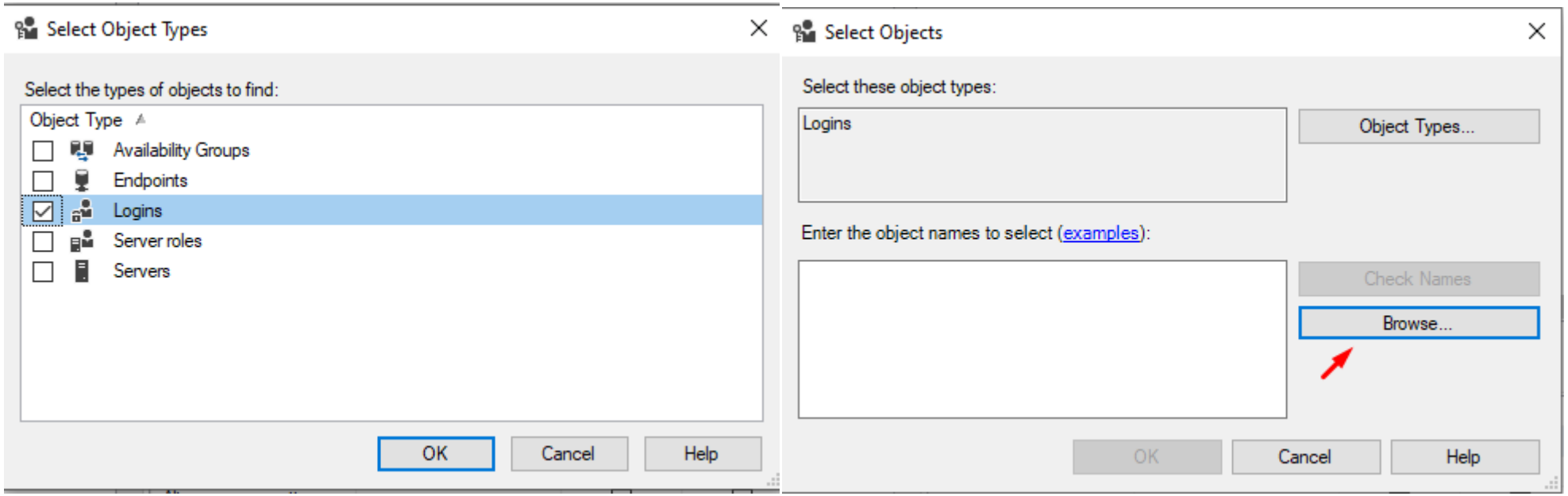
We have made justin.smith as SQL server user with public role, we are going to make the user to impersonate the the systemadmin





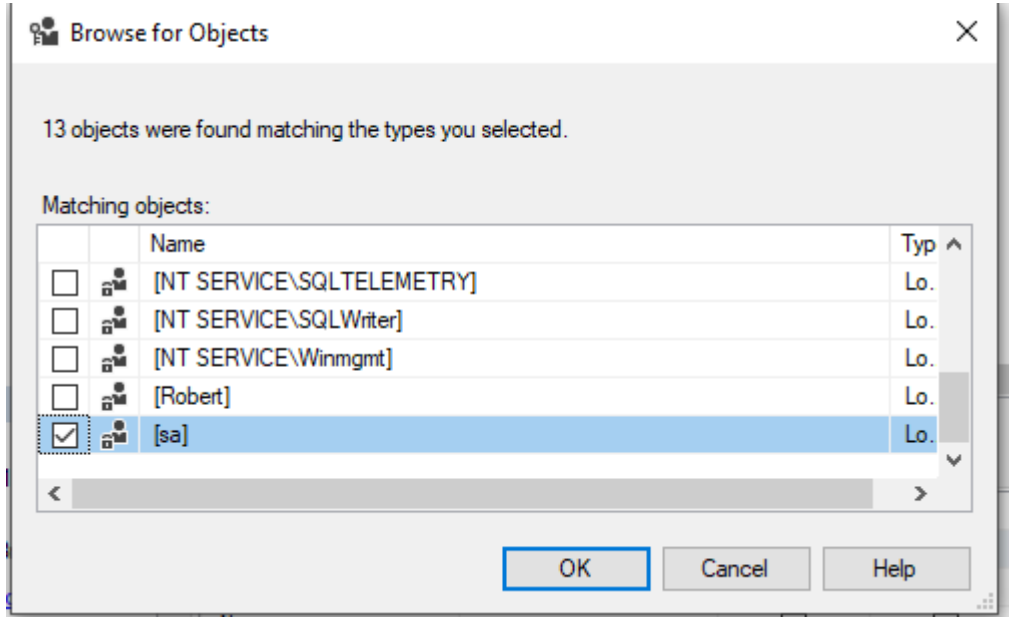
Lab Setup

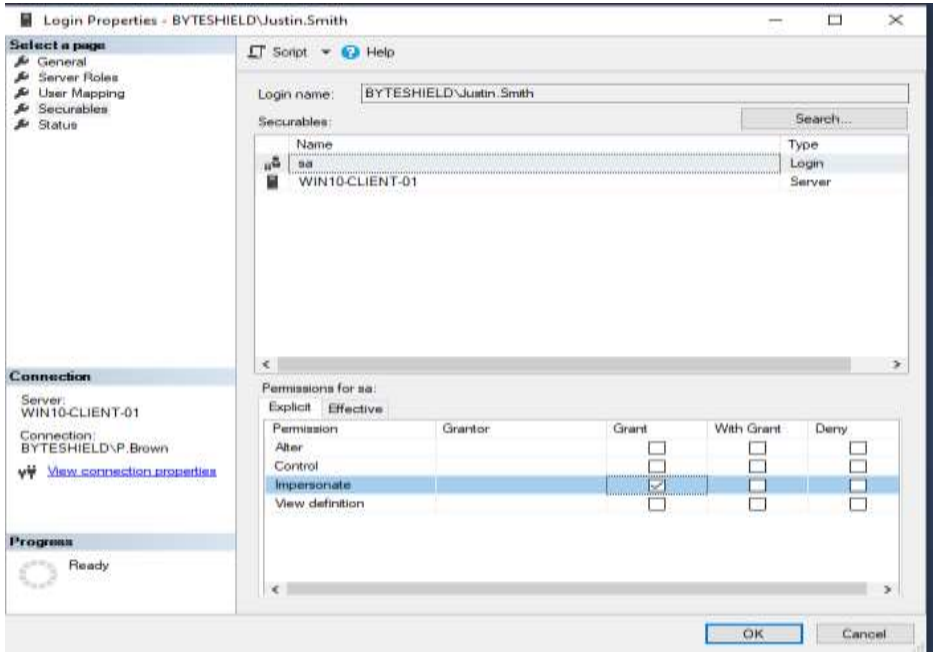
Impersonating sa



Lab Setup

Impersonating sa





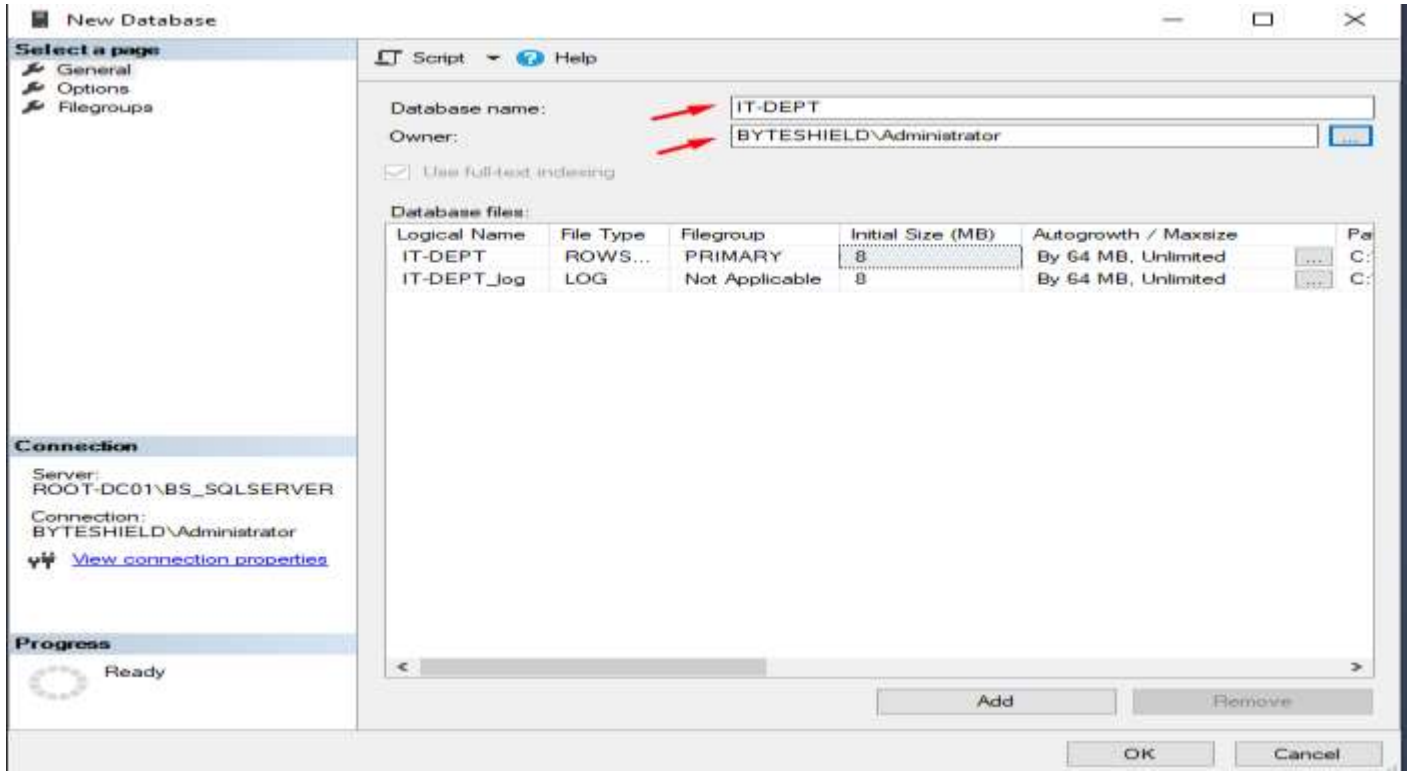
Lab Setup

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

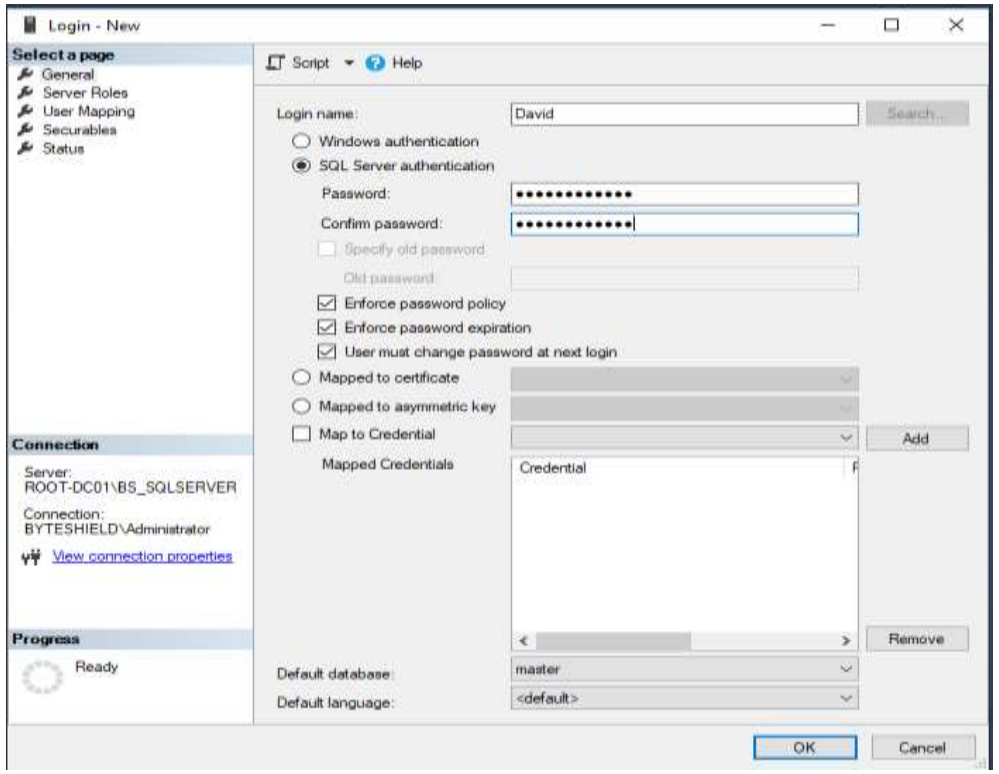
Lab Setup

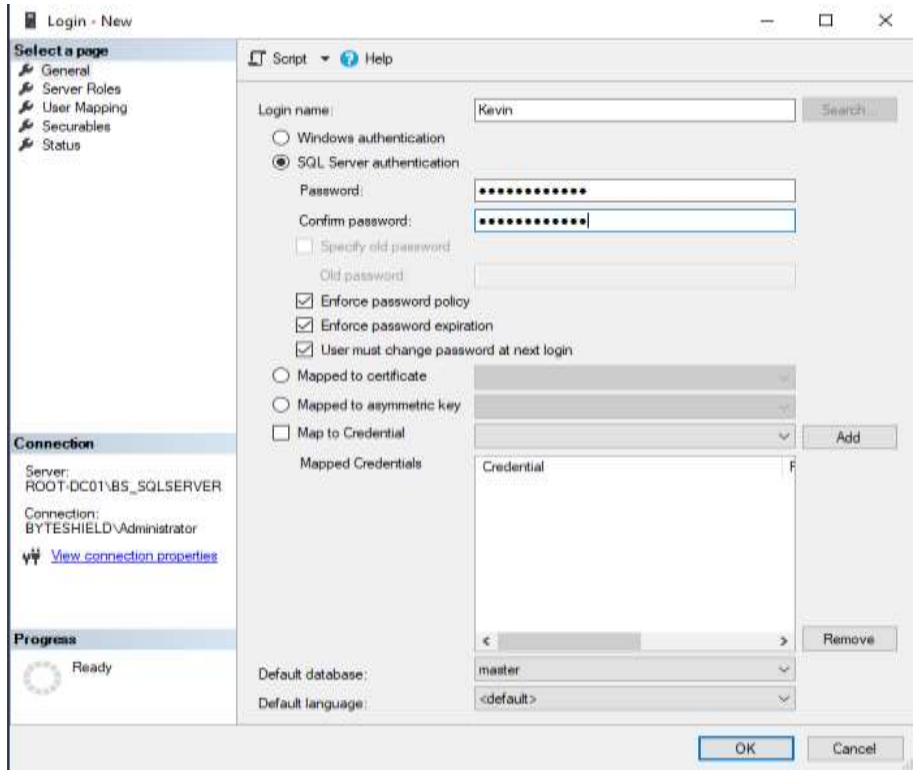
Here we create the database owned by Administrator



Lab Setup

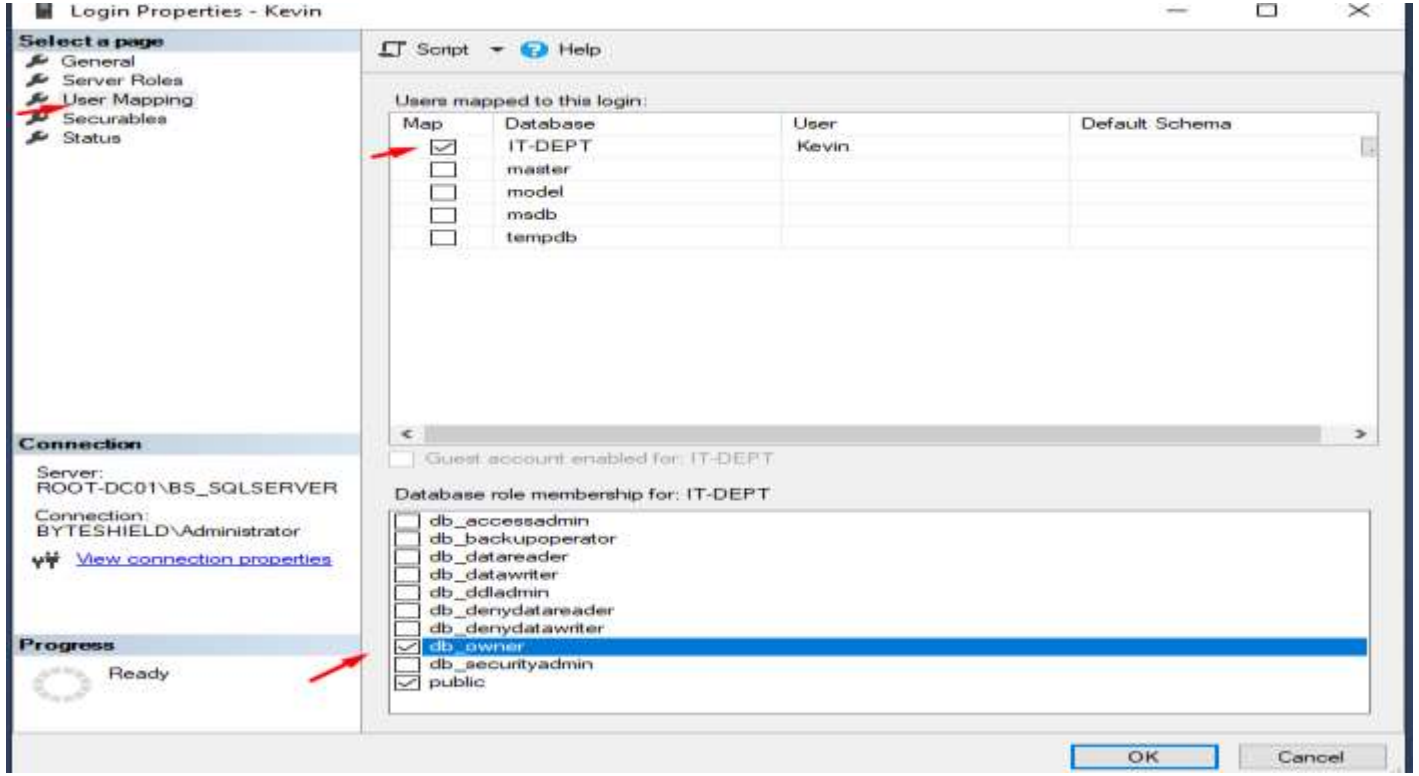
Creating the users the same way Created for Win10-Client-01





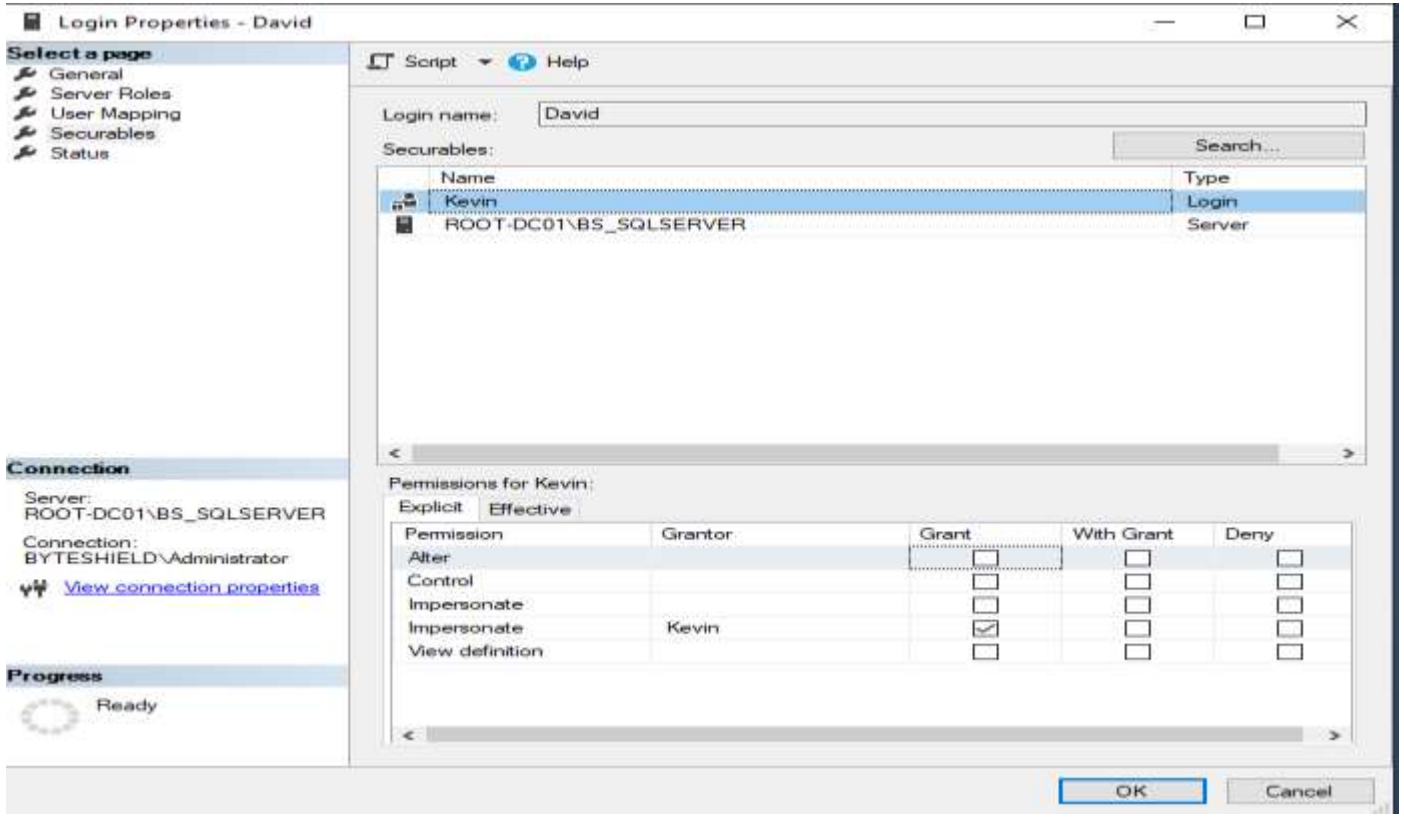
Lab Setup

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
```

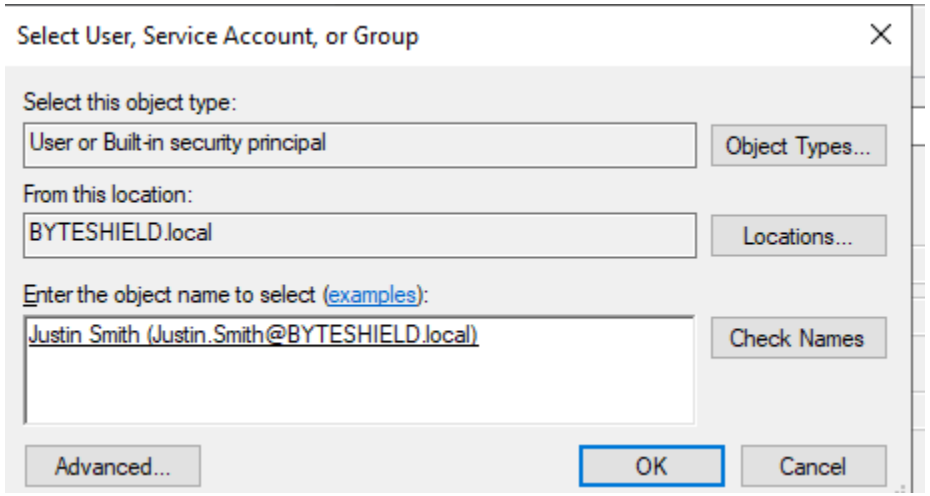
```
N=Sql_Service,CN=Users,DC=BYTESHIELD,DC=local
        BS_SQLSERVER/ROOT-DC01.BYTESHIELD.local:1433
N=WIN10-CLIENT-02,CN=Computers,DC=BYTESHIELD,DC=local
        RestrictedKrbHost/WIN10-CLIENT-02
        HOST/WIN10-CLIENT-02
        RestrictedKrbHost/Win10-Client-02.BYTESHIELD.local
        HOST/Win10-Client-02.BYTESHIELD.local
N=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
N=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!
```

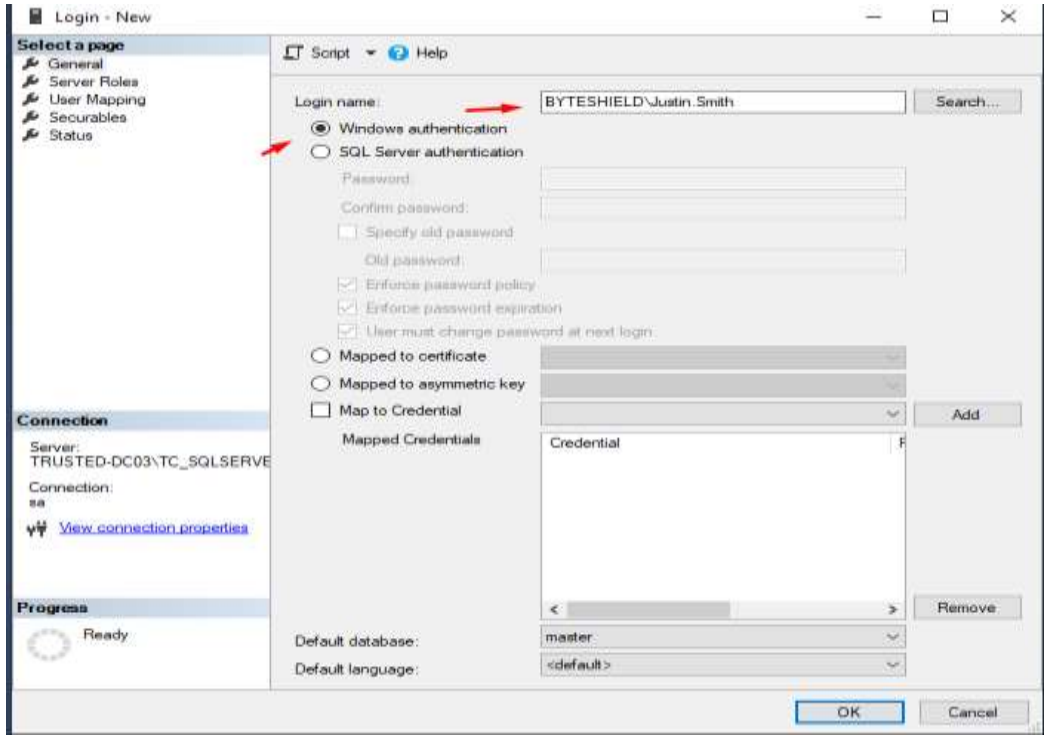
Lab Setup

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

Lab Setup

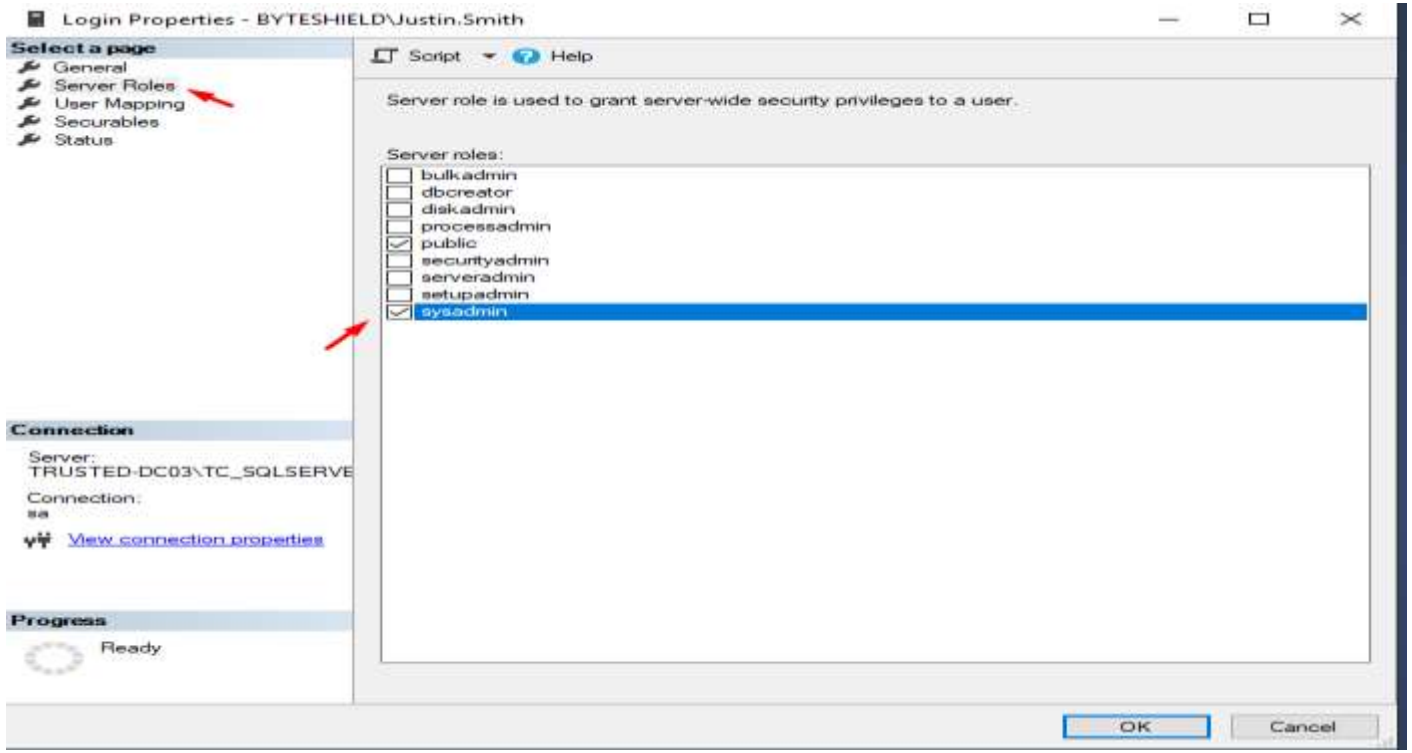
Sql Cross forest Authentication





Lab Setup

Giving Justin.smith sysadmin on the Server



Lab Setup

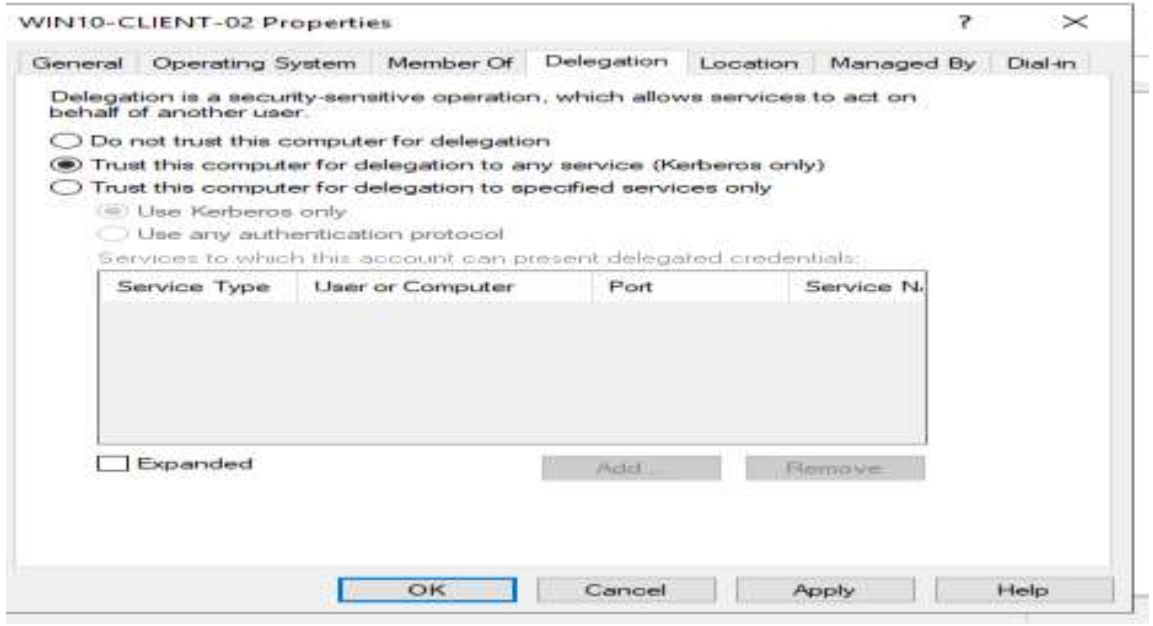
Creating SPN for SQL Server on TRUSTED-DC03

```
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
```

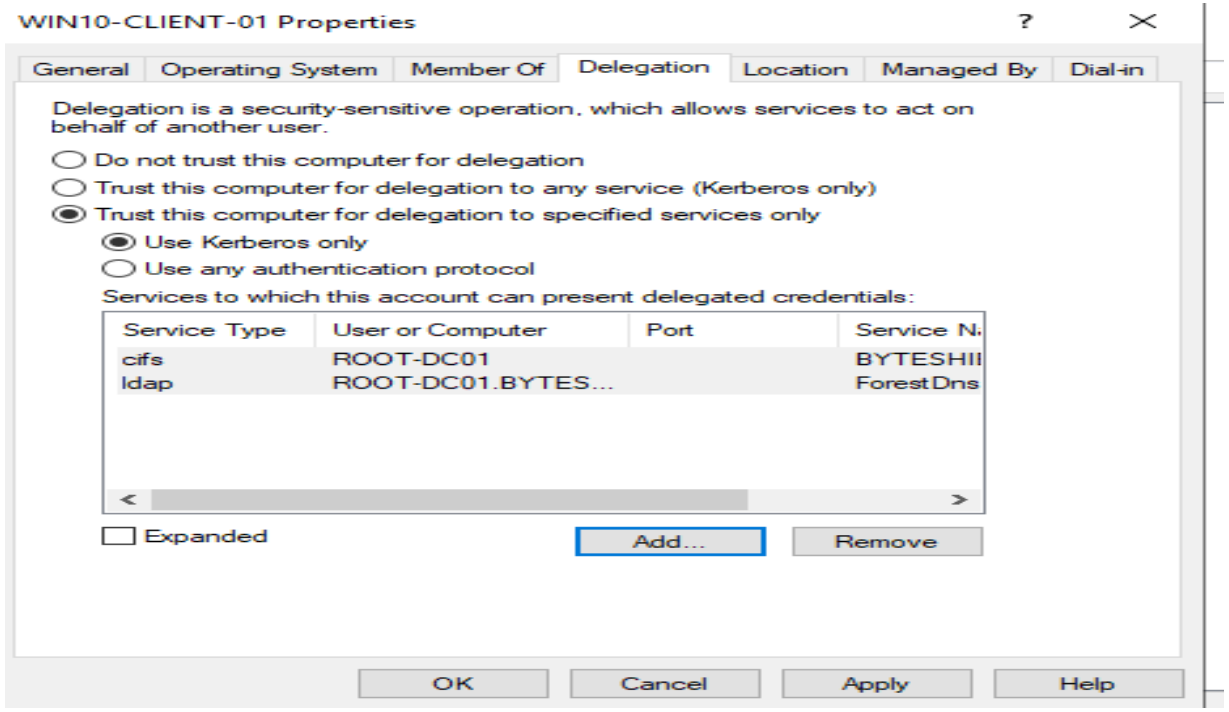
Lab Setup

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



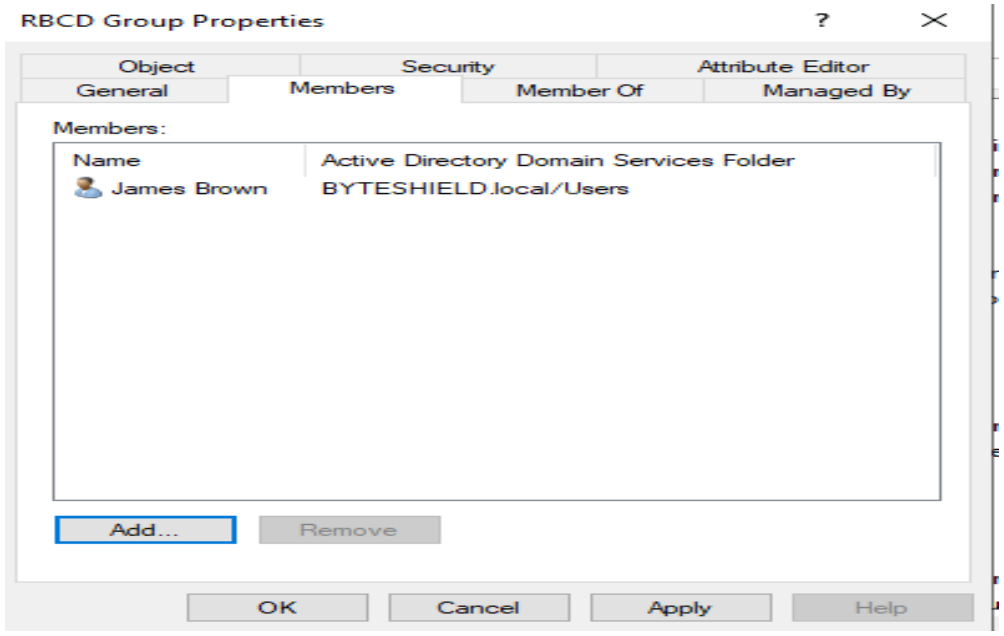
Lab Setup

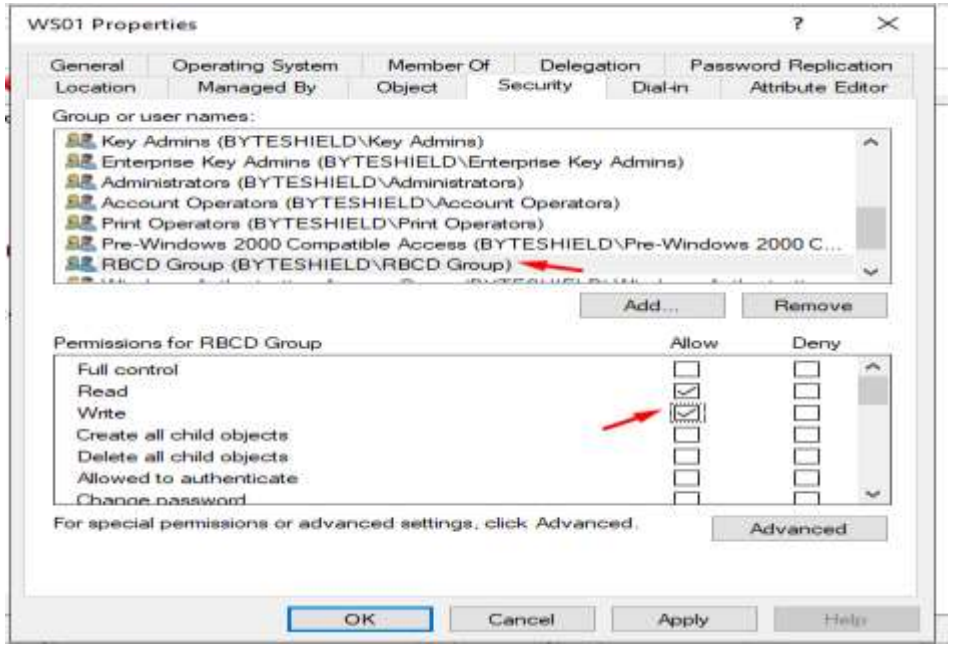
Constrained Delegation Setup, we are going to use Win10-Client-01 for constrained delegation



Lab Setup

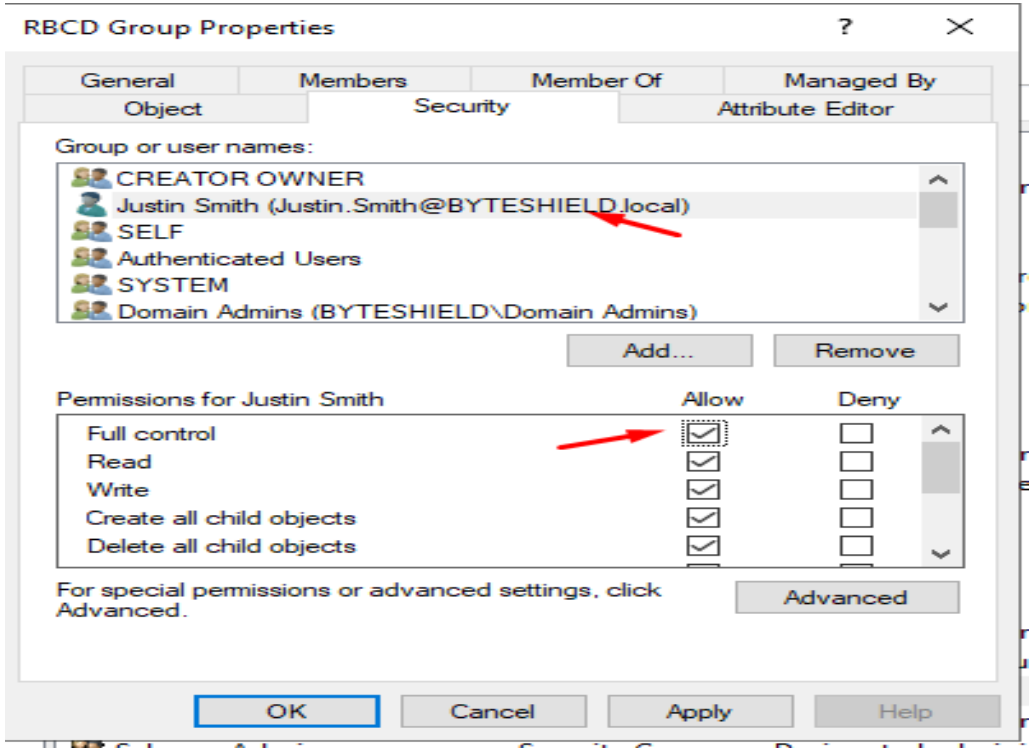
Resource-based constrained delegation RBDC setup, we are going to create a group and name it RBDC group, this group will have write permission over WS01 and justin.smith with have full permission over the group, that will give our user ability to add himself to the group, james.brown is a member to the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





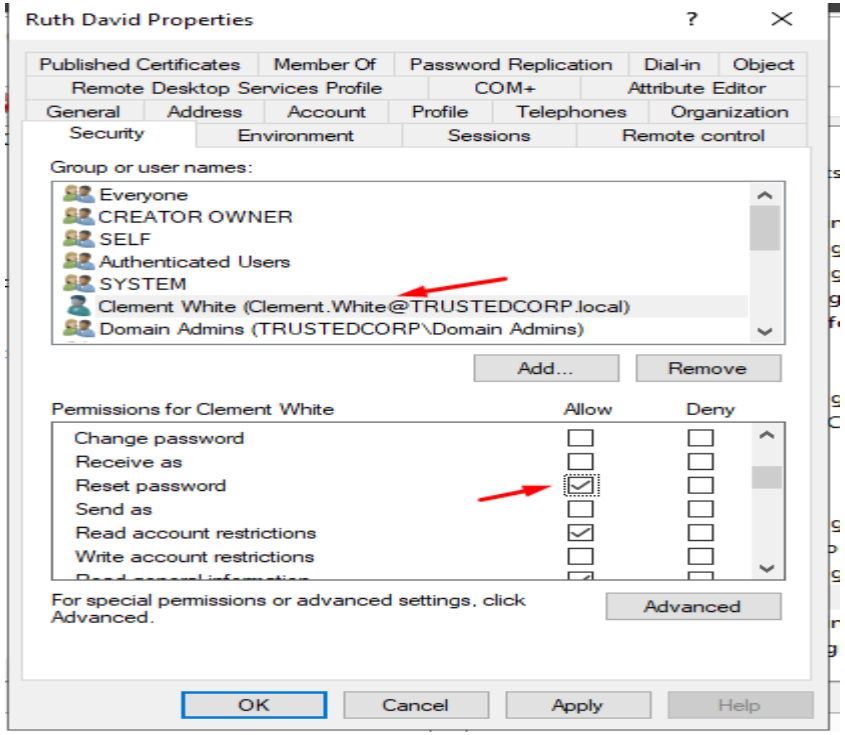
Lab Setup

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



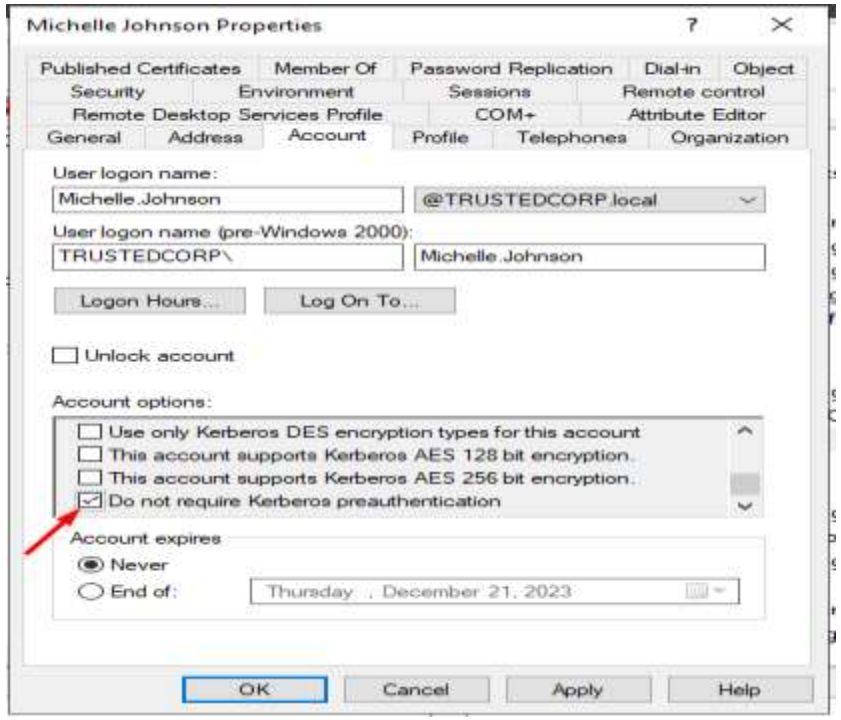
Lab Setup

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



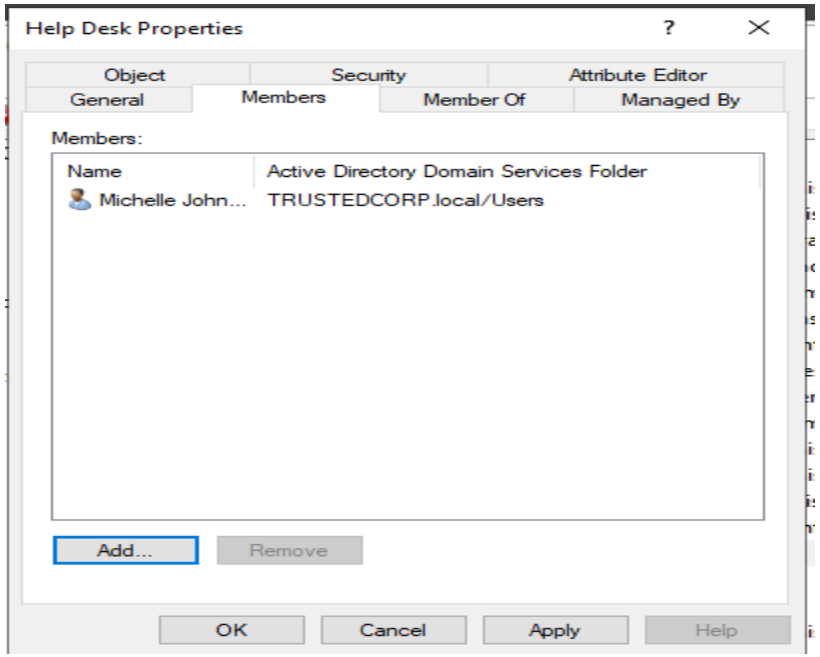
Lab Setup

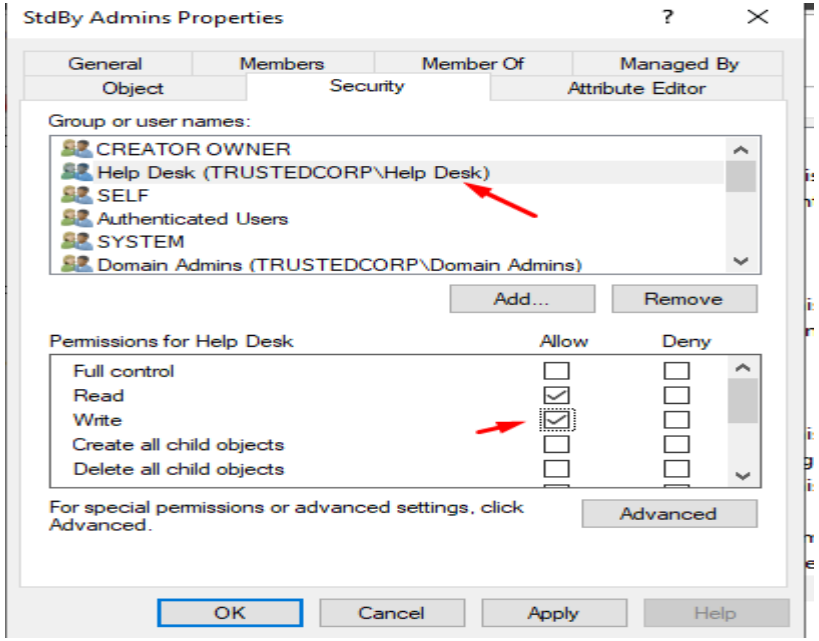
While Michelle.Johnson will have Don not Require Kerberos preauthentication selected



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