Extend On-Premises Windows Server Active Directory to Azure VM

Complete Lab (V24.07)

Ahmed Abdelwahed
ahmed@abdelwahed.me
LinkedIn

Contents

Lab Objective

Our goal in this lab is to extend On-Premise active directory to Microsoft Azure by create additional domain controller for existing On-Premise active directory domain in Microsoft Azure, so we can protect active directory in worst case disaster scenarios, and reduce downtime by redirect internal users to use DC in azure (additional) for authentication and other active directory benefits. Also by this scenario we reduce the active directory recovery time.

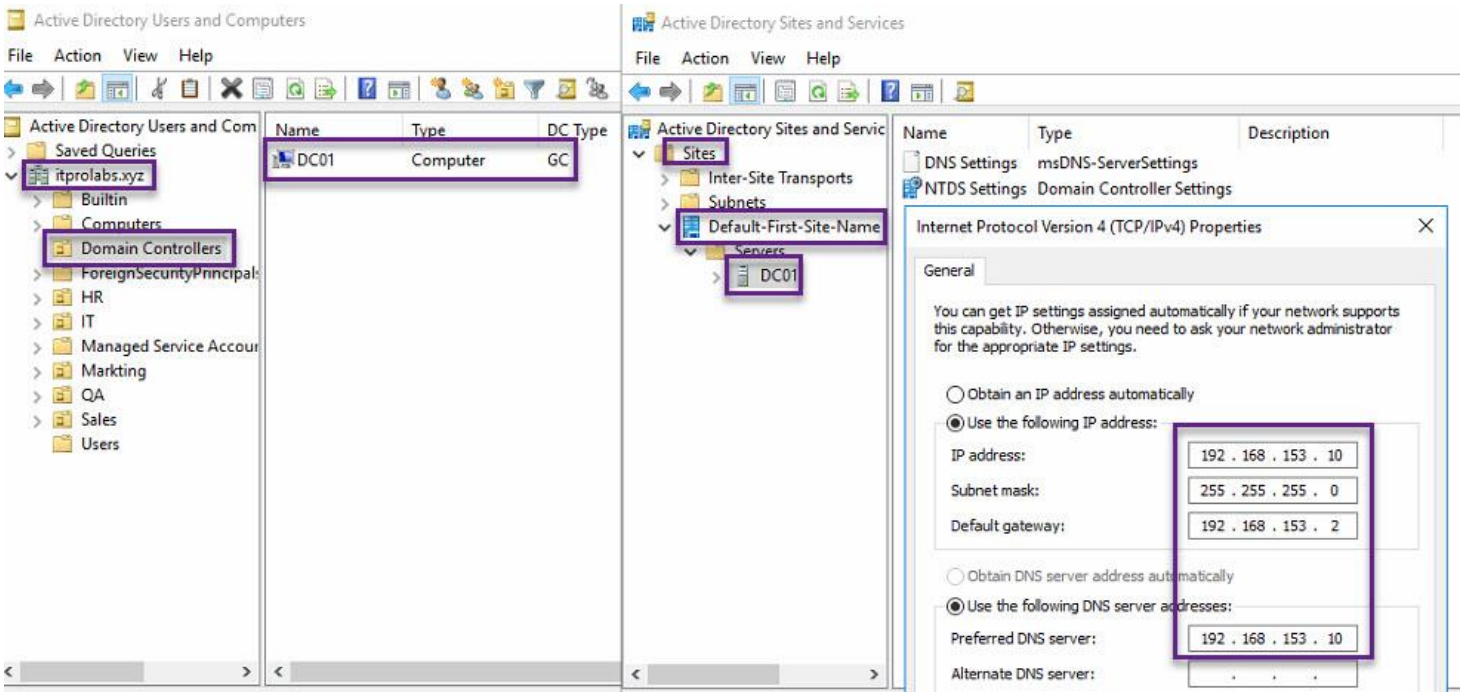
Existing Active directory environment

We have only one On-Premise Domain controller for our ITPROLABS.XYZ domain named DC01, also we have only one active directory site that host our domain controller as explained in the figures below.

- ☒ Server IP: 192.168.153.10
- ☒ DNS: 192.168.153.10
- ☒ DC Name: DC01
- ☒ Domain Name: ITPROLABS.XYZ
- ☒ Site Name: Default- First-Site-Name

Full install windows server 2016 active directory lab explained in the below link:

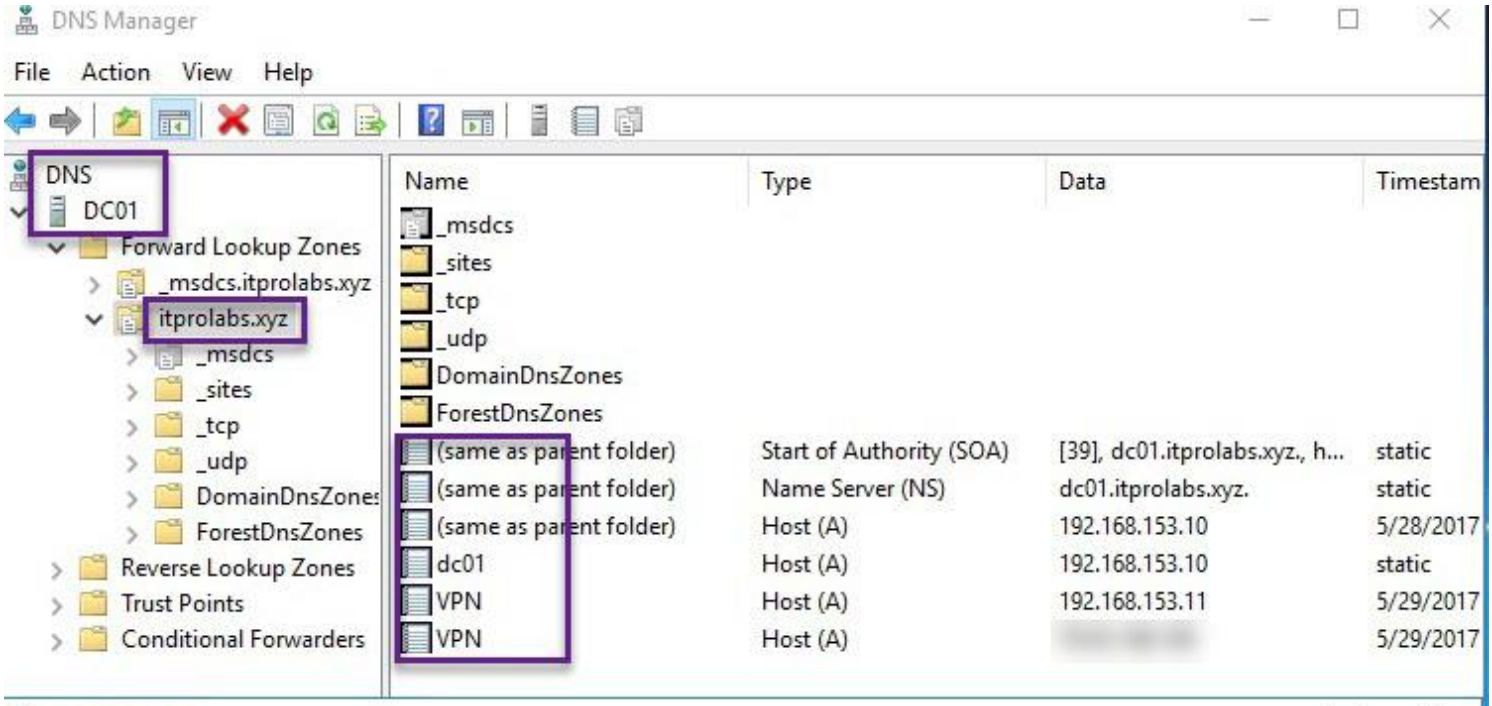
https://gallery.technet.microsoft.com/Install-Windows-Server-f37e3c6d

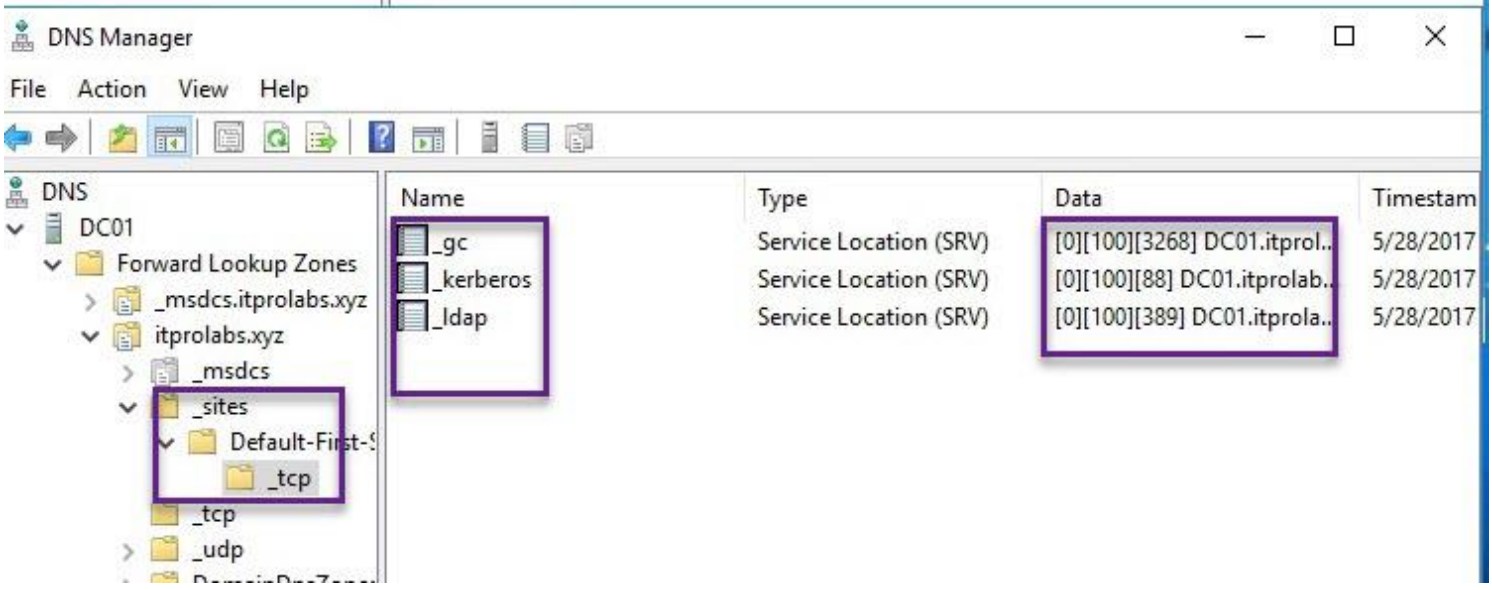


Existing DNS Configuration

We have one DNS server that host active directory integrated zone named ITPROLABS.XYZ domain, also this server (DC01.ITPROLABS.XYZ) working as Global Catalog, Kerberos and LDAP roles.

- ☒ DNS Server: 192.168.153.10
- ☒ DNS Zone: ITPROLABS.XYZ
- ☒ GC, Kerberos, LDAP Server: DC01.itprolabs.xyz



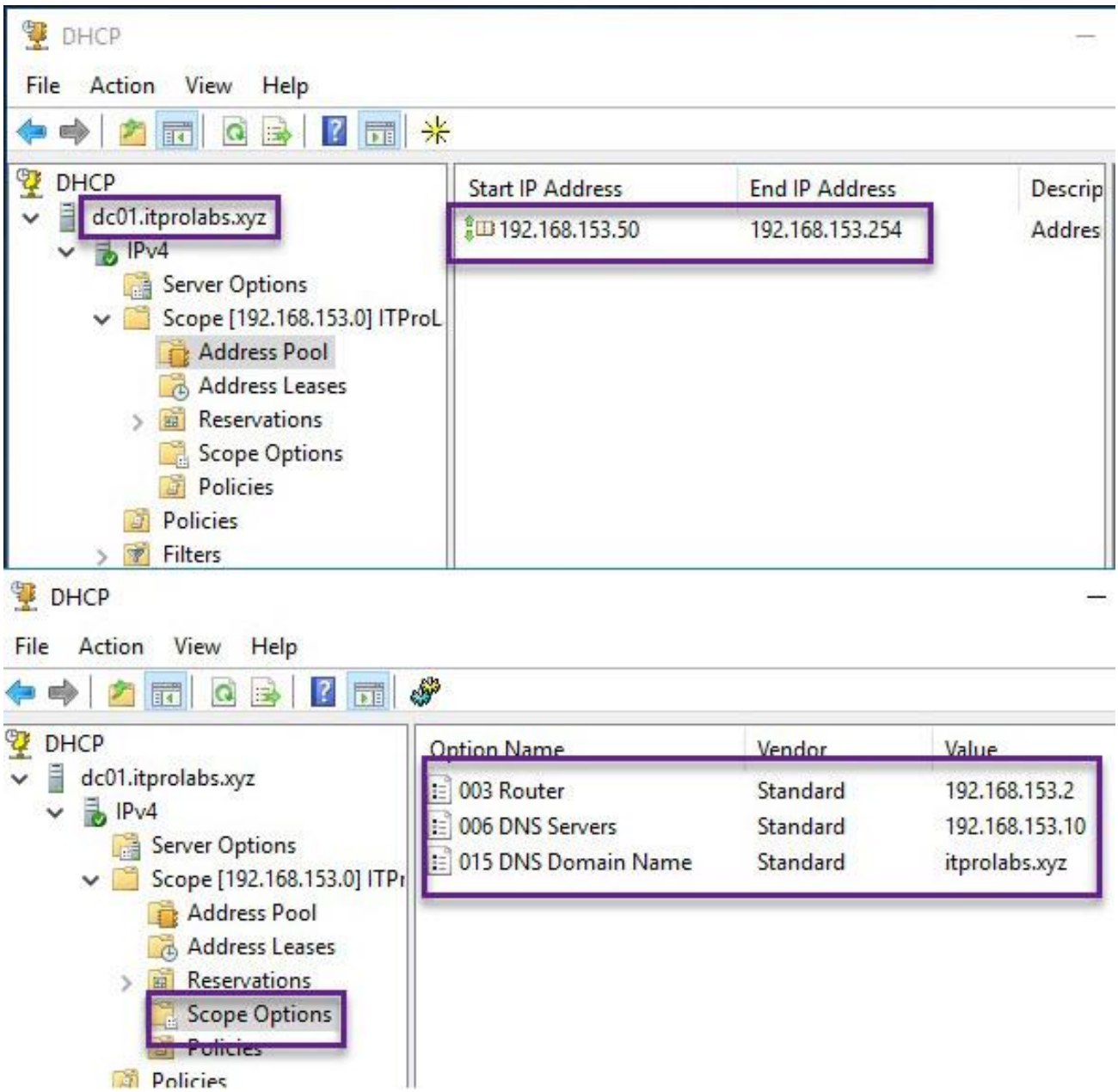


Existing DHCP Configuration

DHCP Server: 192.168.153.10

Full DHCP server on windows server 2016 lab explained in the below link:

https://gallery.technet.microsoft.com/Installing-and-Configuring-bf727a5f

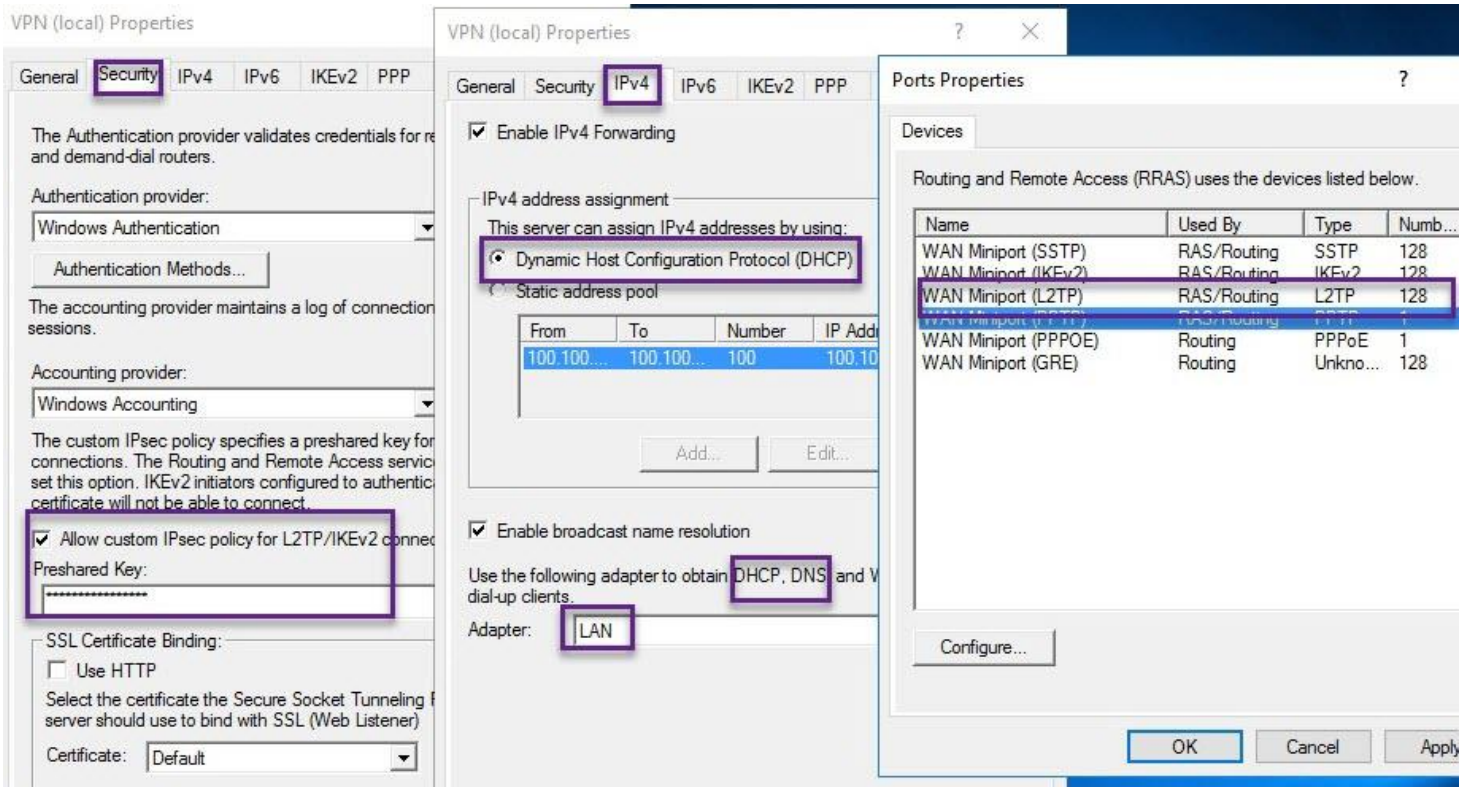


Existing VPN Server Configuration

VPN configuration is important part in our lab because our Windows Server 2016 VM on Azure will contact On-Premise **itprolabs.xyz** domain through L2TP/IPsec VPN. Our VPN configuration fully explained in the following link:

https://gallery.technet.microsoft.com/L2TPIPsec-VPN-On-Windows-5cc2c3ae

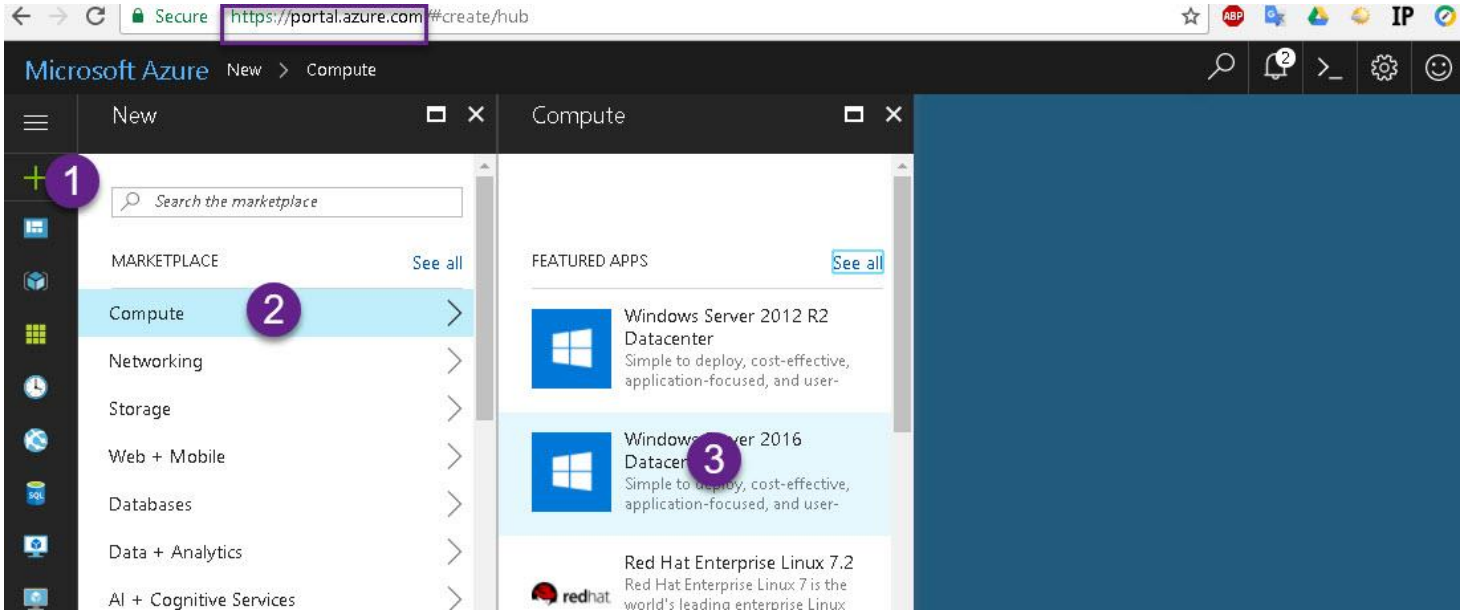
Note: VM on azure doesn't support **PPTP** VPN.



Create Windows Server 2016 VM in Microsoft Azure

Create Windows Server 2016 Data Center VM step by step

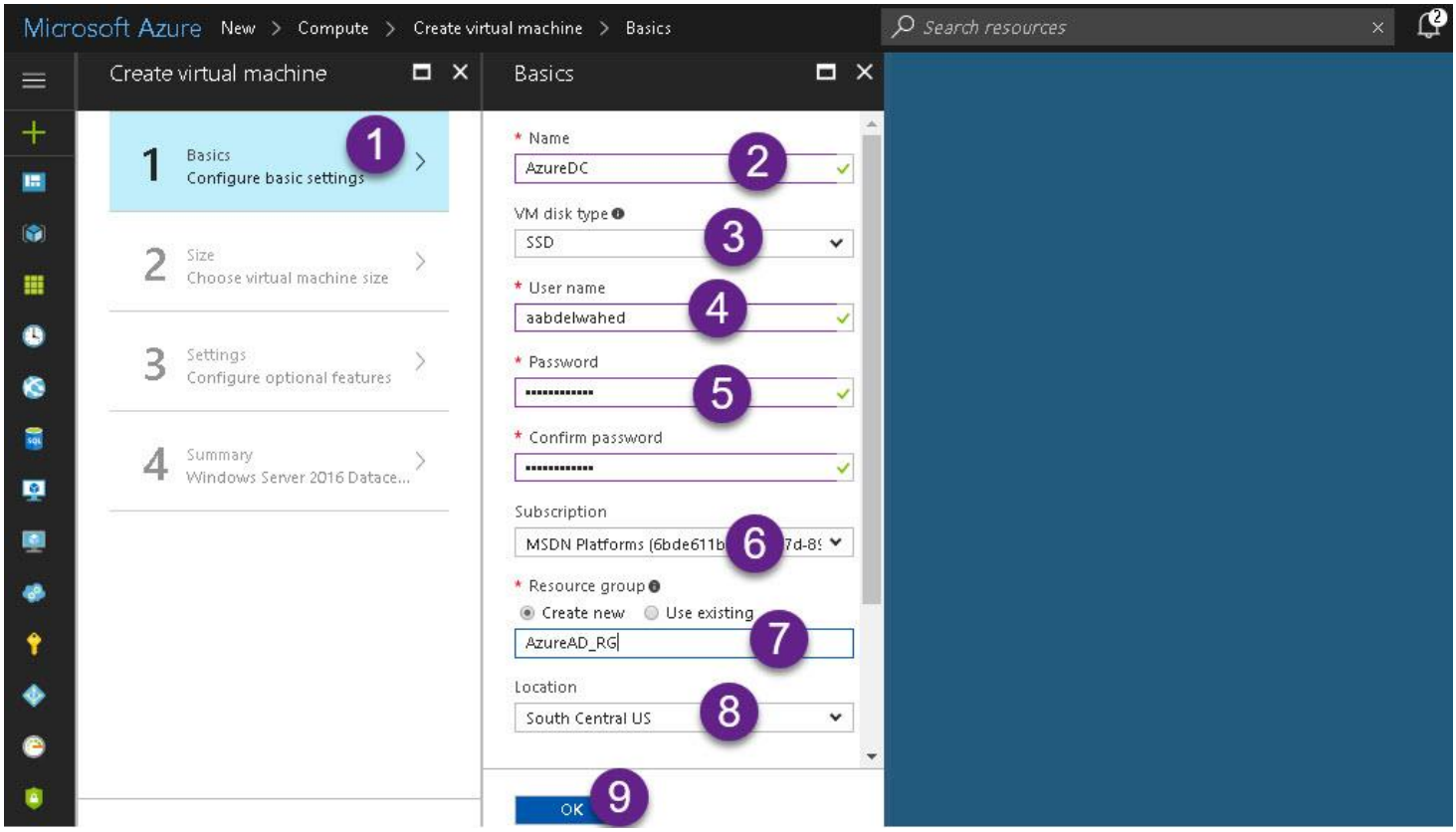
1. **Login to Microsoft Azure Portal** and follow steps as explained in the figures below.



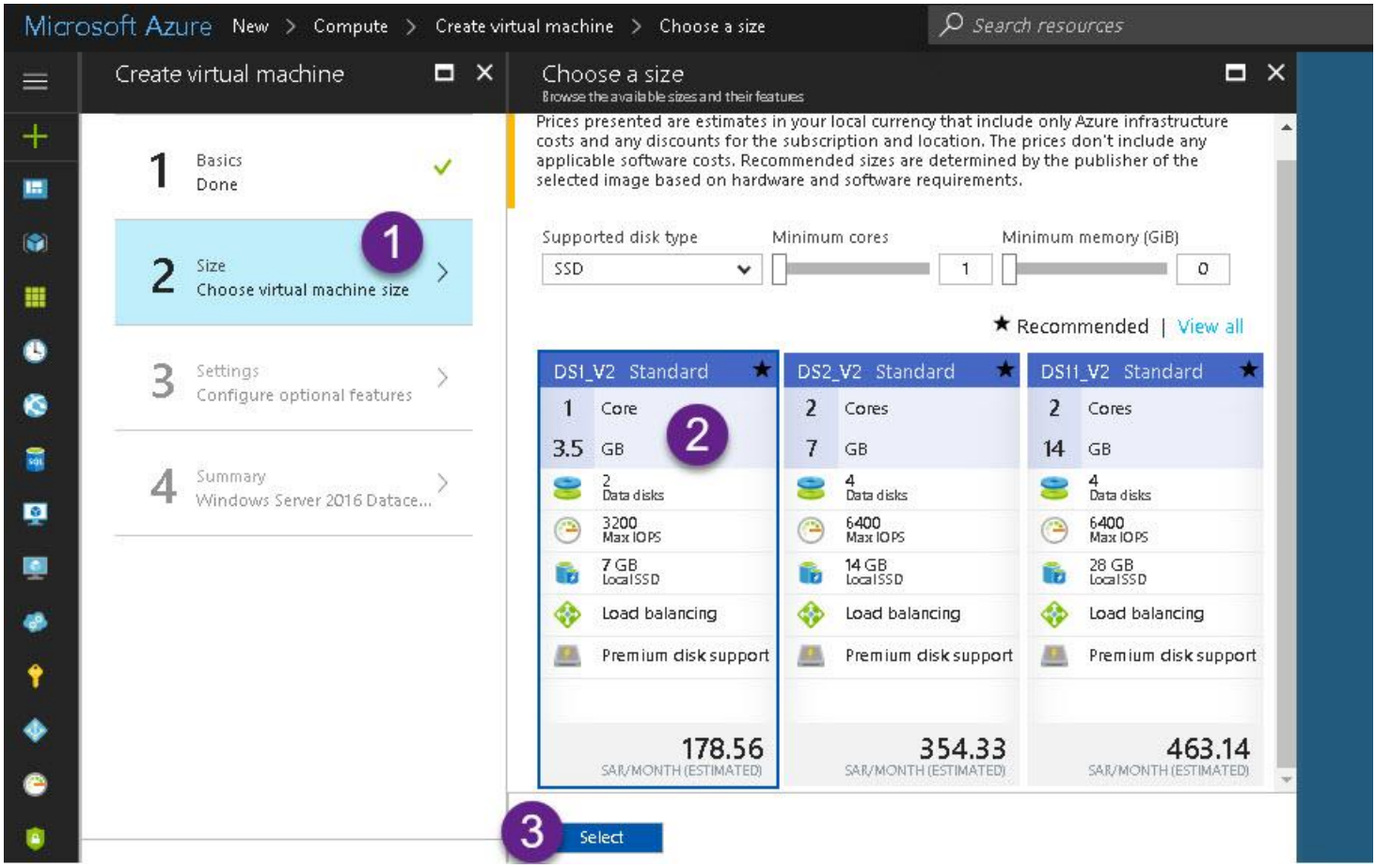
2. Configure VM basic settings including:

1- VM Name (special characters not allowed)
2- Hard Disk type: SSD or HDD
3- Create a local account on the VM with strong password (used for sign in to the VM).
4- Select your subscription.
5- Use exiting resource group or create new one
6- Azure allows you to create resources, such as VMs, in geographic regions, so select region where you want the VM to run (There are 34 geographic regions for Microsoft Azure).

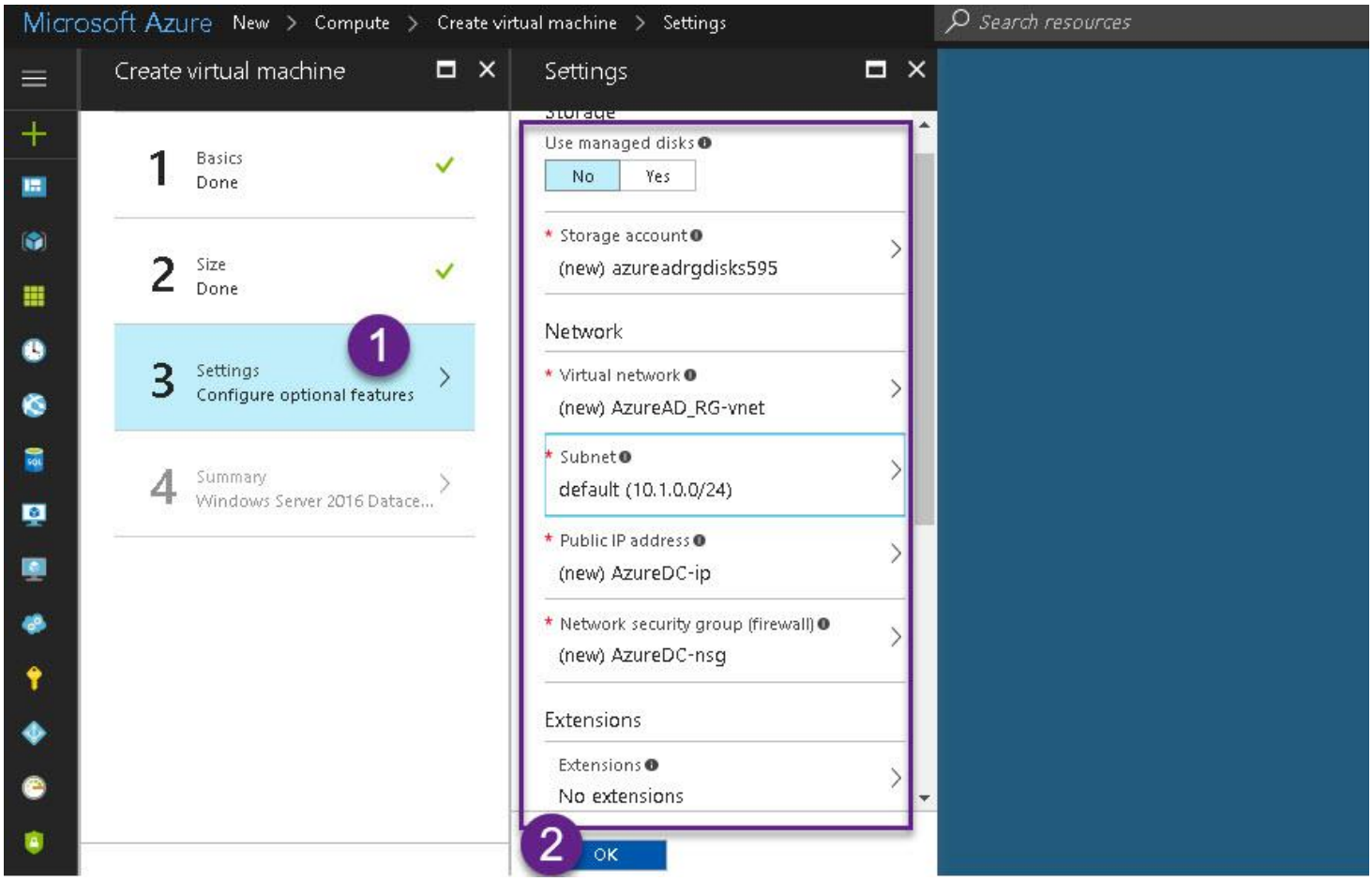
> **Resource group** is logically group related resources such as storage accounts, virtual networks, and virtual machines (VMs) to deploy, manage, and maintain them as a single entity.



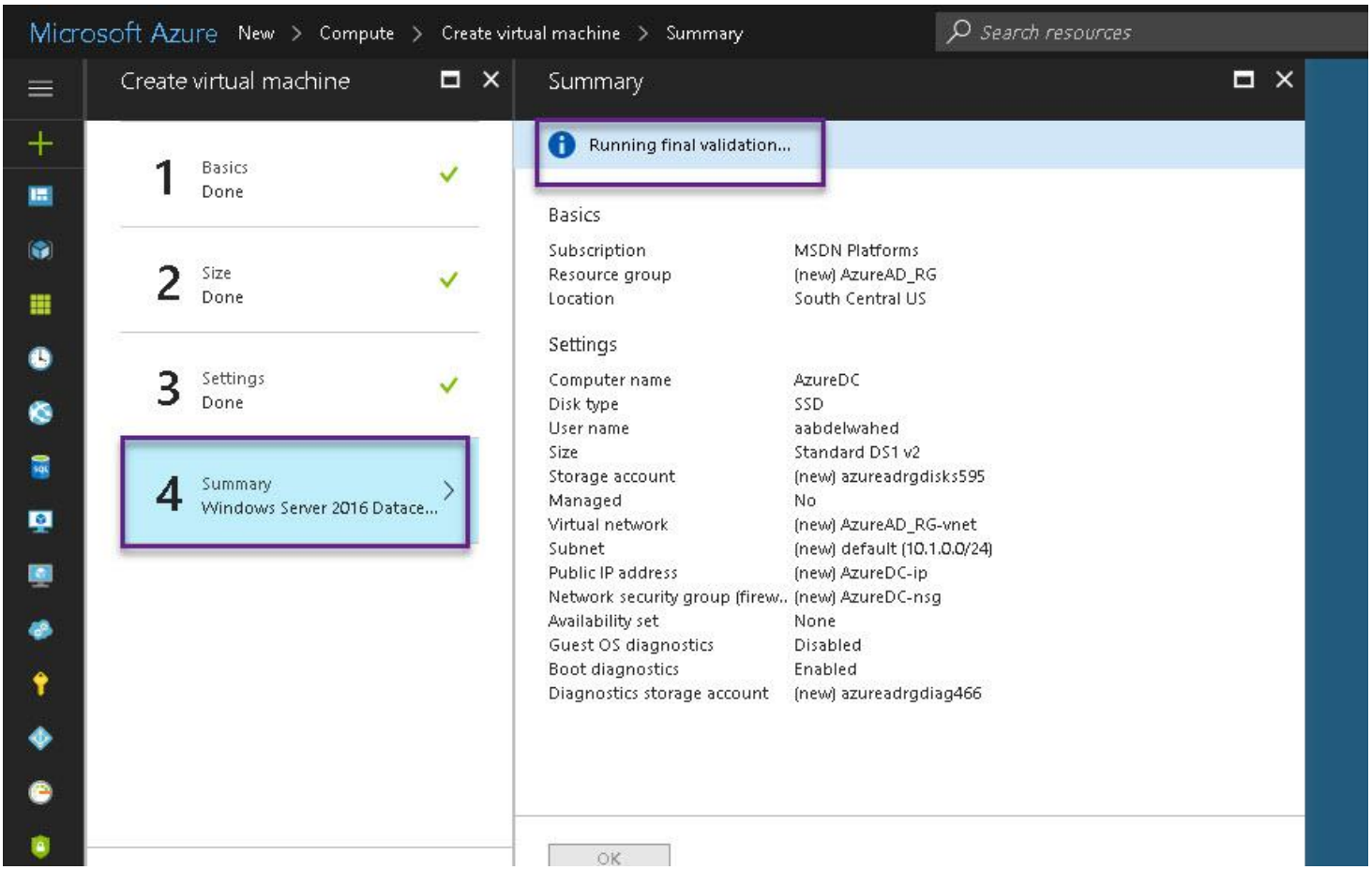
3. **Select VM size** that will determine VM configuration including RAM size, processor cores, storage size which will affect estimated monthly cost. In this lab DS1_V2 Standard is our selected VM size.

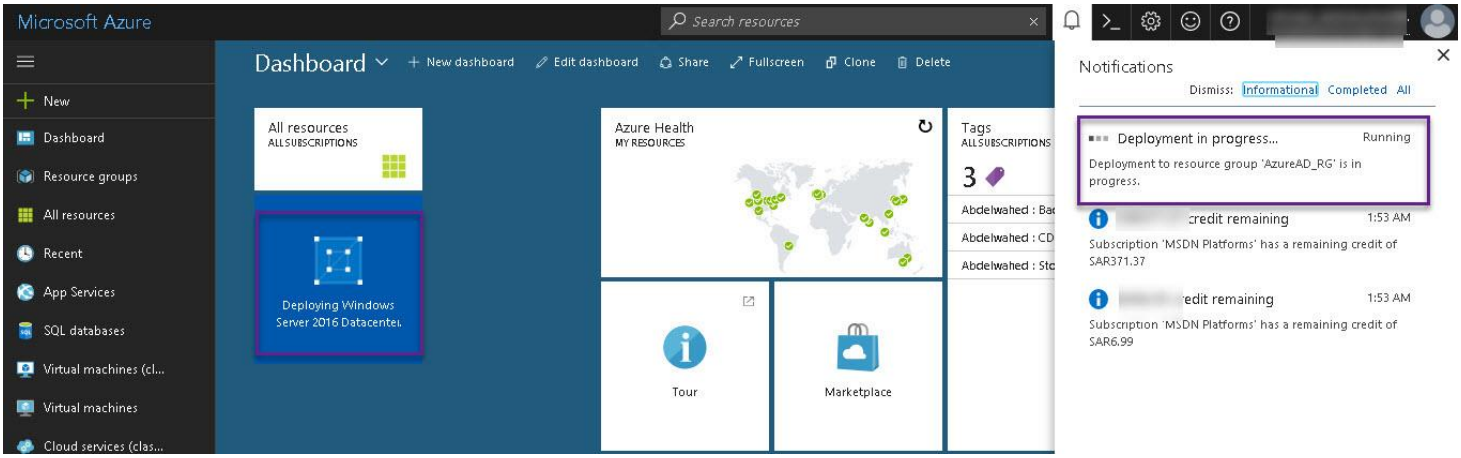


4. Configure **optional features** for example you can create virtual network and assign specific IP addresses to it or you can leave this option by default and azure will configure this options for you.



5. Before start VM creation Azure **validate** your configuration

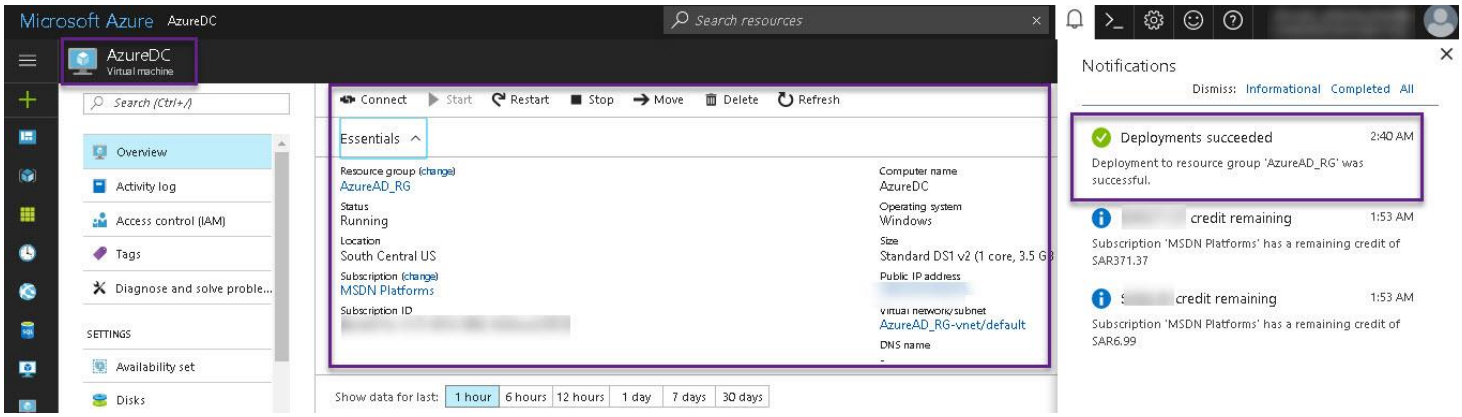




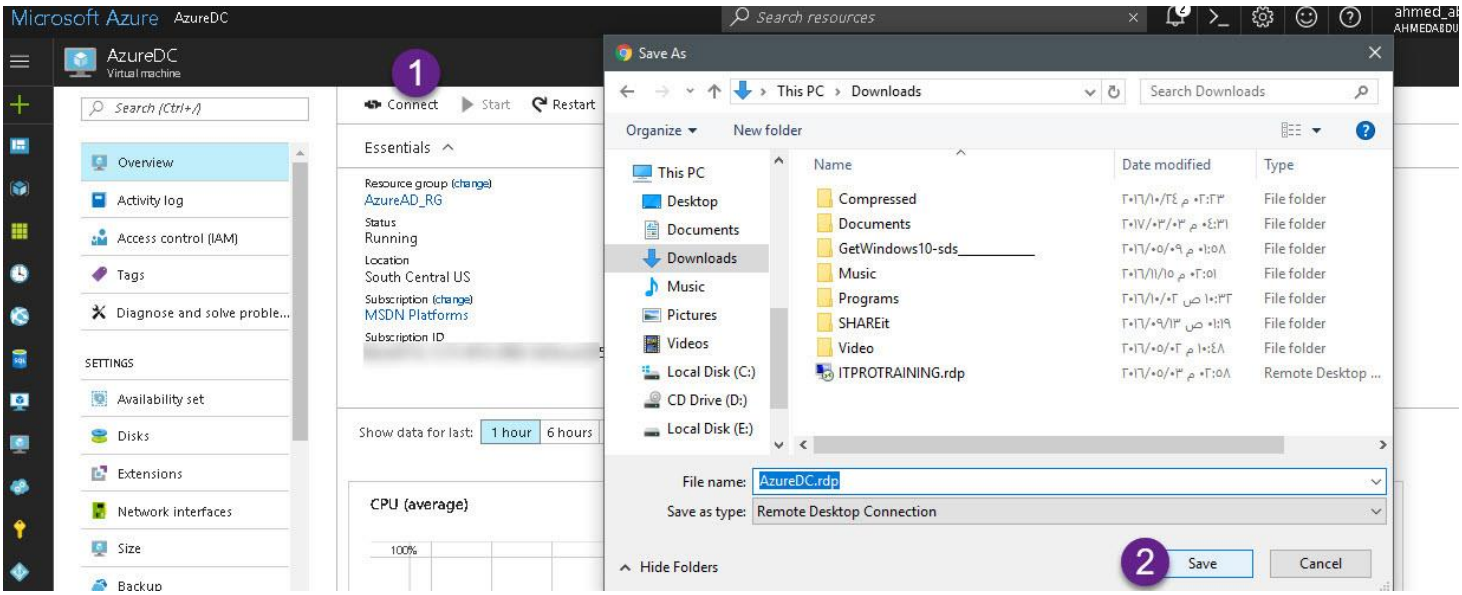
Extend On-Premises Windows Server Active Directory to Azure VM

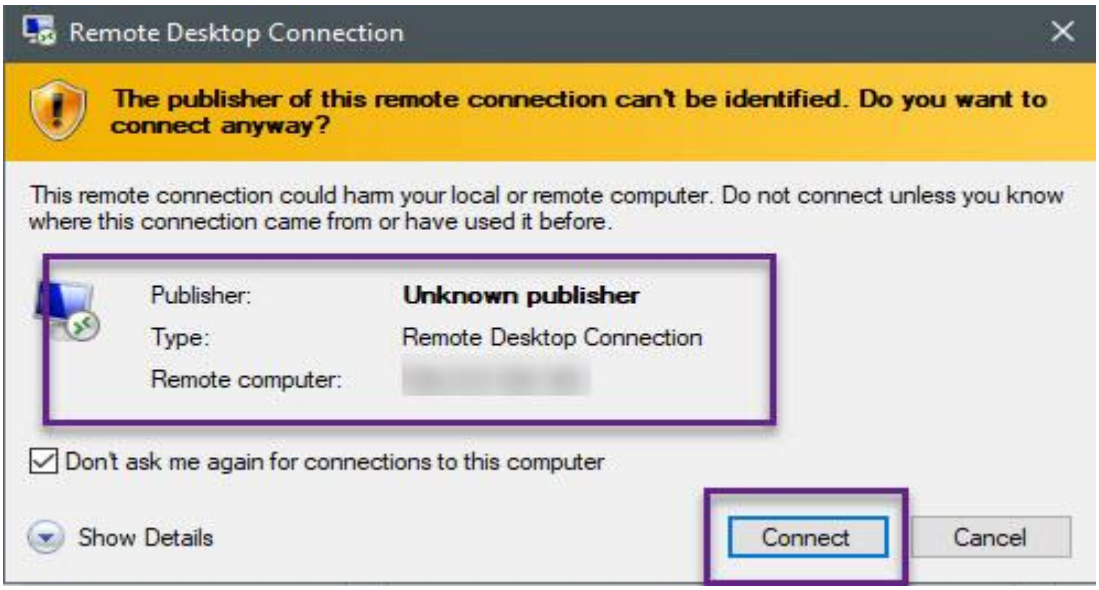
Access Azure VM

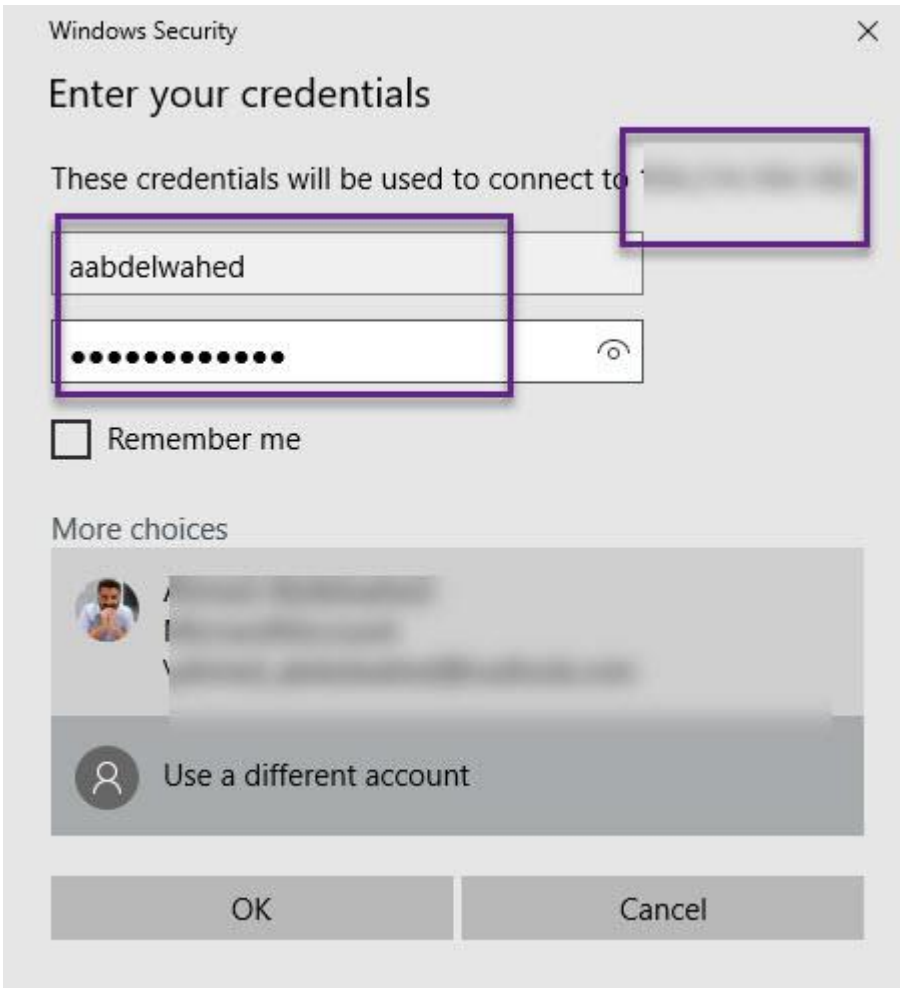
Once your VM is created Microsoft Azure assign public IP address to it so you can access your VM through Remote Desktop with your local account credentials that you are created.



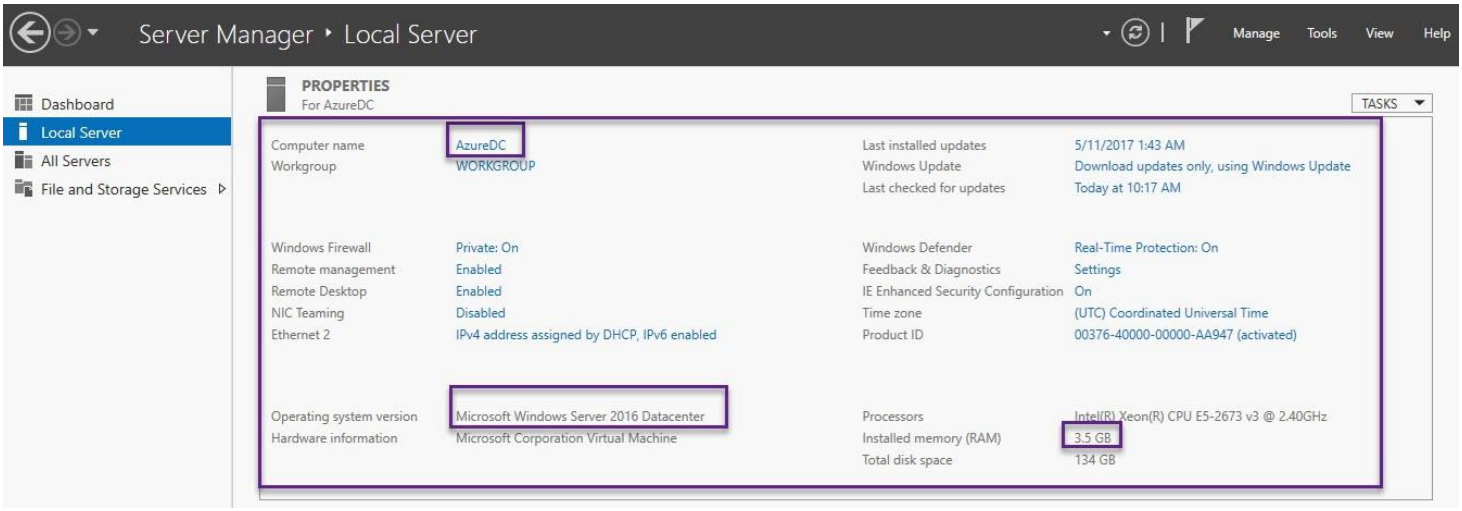
Now you can **connect** through remote desktop by click Connect tab as explained in the figures below




Remote Desktop Connection
The publisher of this remote connection can't be identified. Do you want to connect anyway?
This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.
Publisher:
Unknown publisher
Type:
Remote Desktop Connection
Remote computer:
Don't ask me again for connections to this computer
Show Details
Connect
Cancel


Windows Security
Enter your credentials
These credentials will be used to connect to
aabdelwahed
Remember me
More choices
Use a different account
OK
Cancel

Finally, we sign in Windows Server 2016 VM which we created.

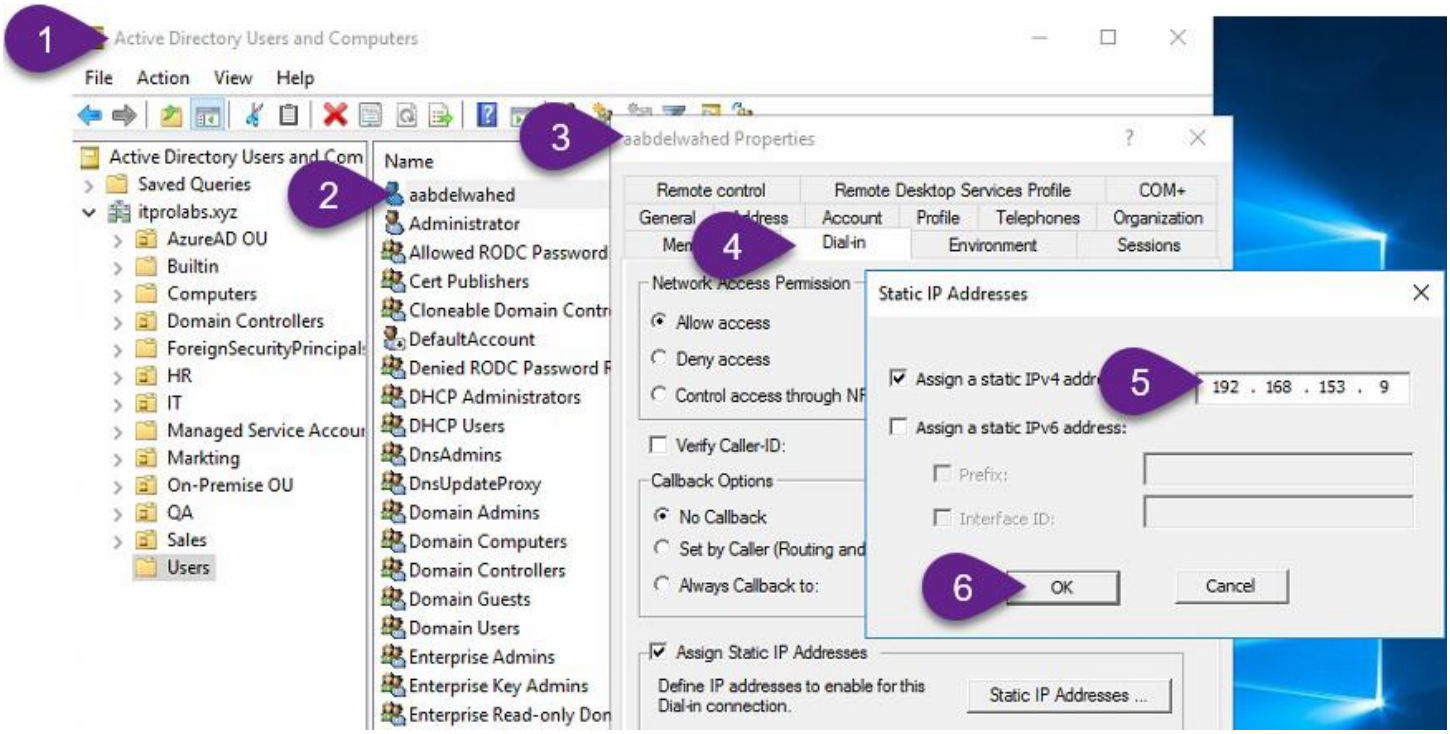


For more information about create and configure windows server 2016 VM on azure, check the following link:
https://gallery.technet.microsoft.com/Create-and-Configure-65fecd55

Connect Azure VM Server to On-Premise network using L2TP/IPsec VPN

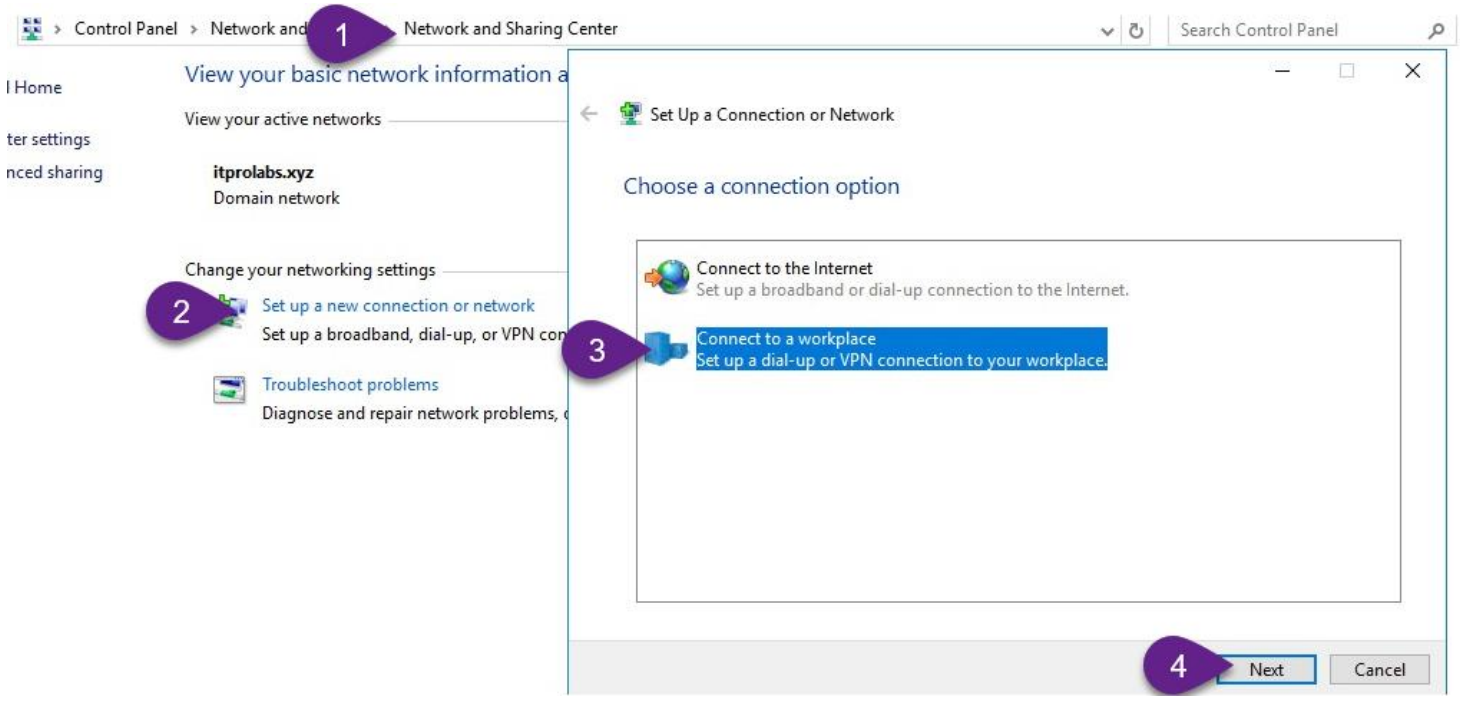
Assign static IP address for Azure VM VPN connection

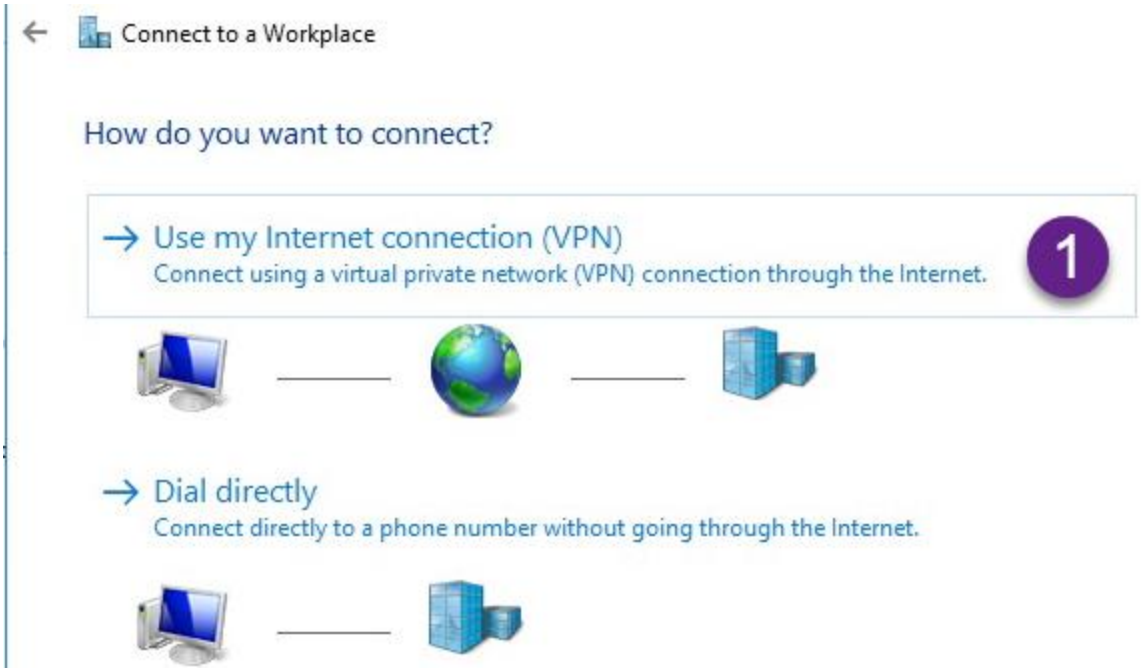
Its preferable to assign static IP address for additional DC when connect to On-Premise network, so PCs in On-Premise can contact additional DC easily, to do this we will assign static IP address for user that we will use it in VPN connection from Azure to On-Premise, in this example we will assign this option to **aabdelwahed** user.

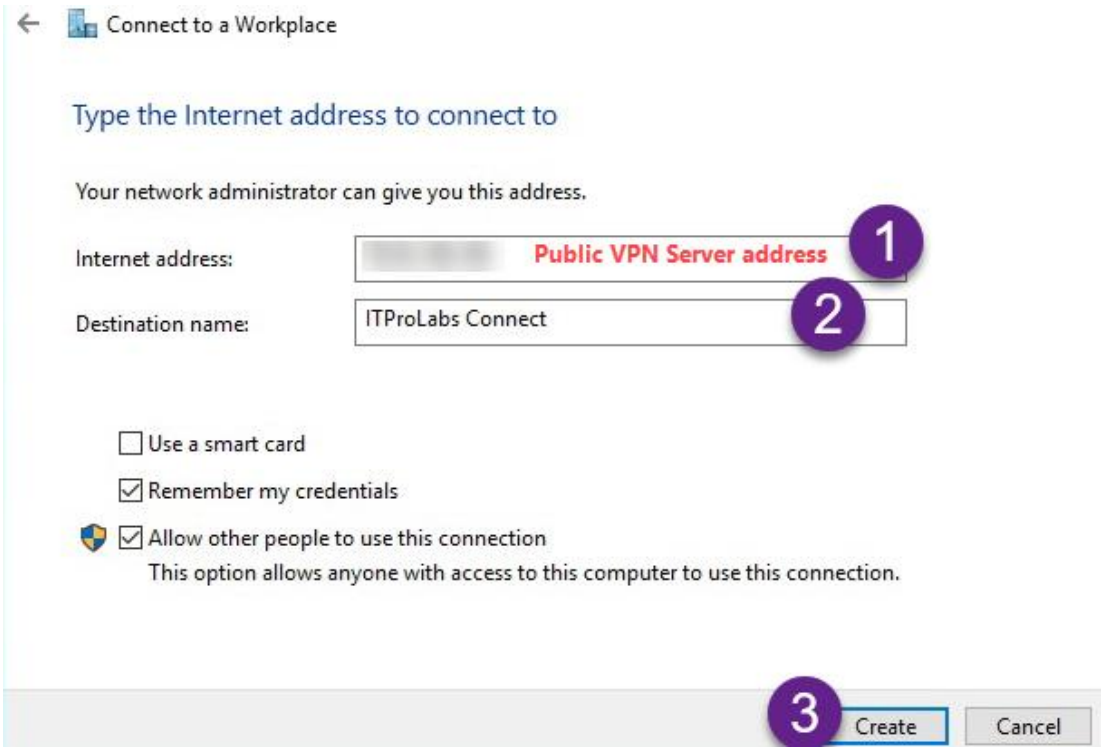


Create VPN connection from Windows Server 2016 VM on Microsoft Azure

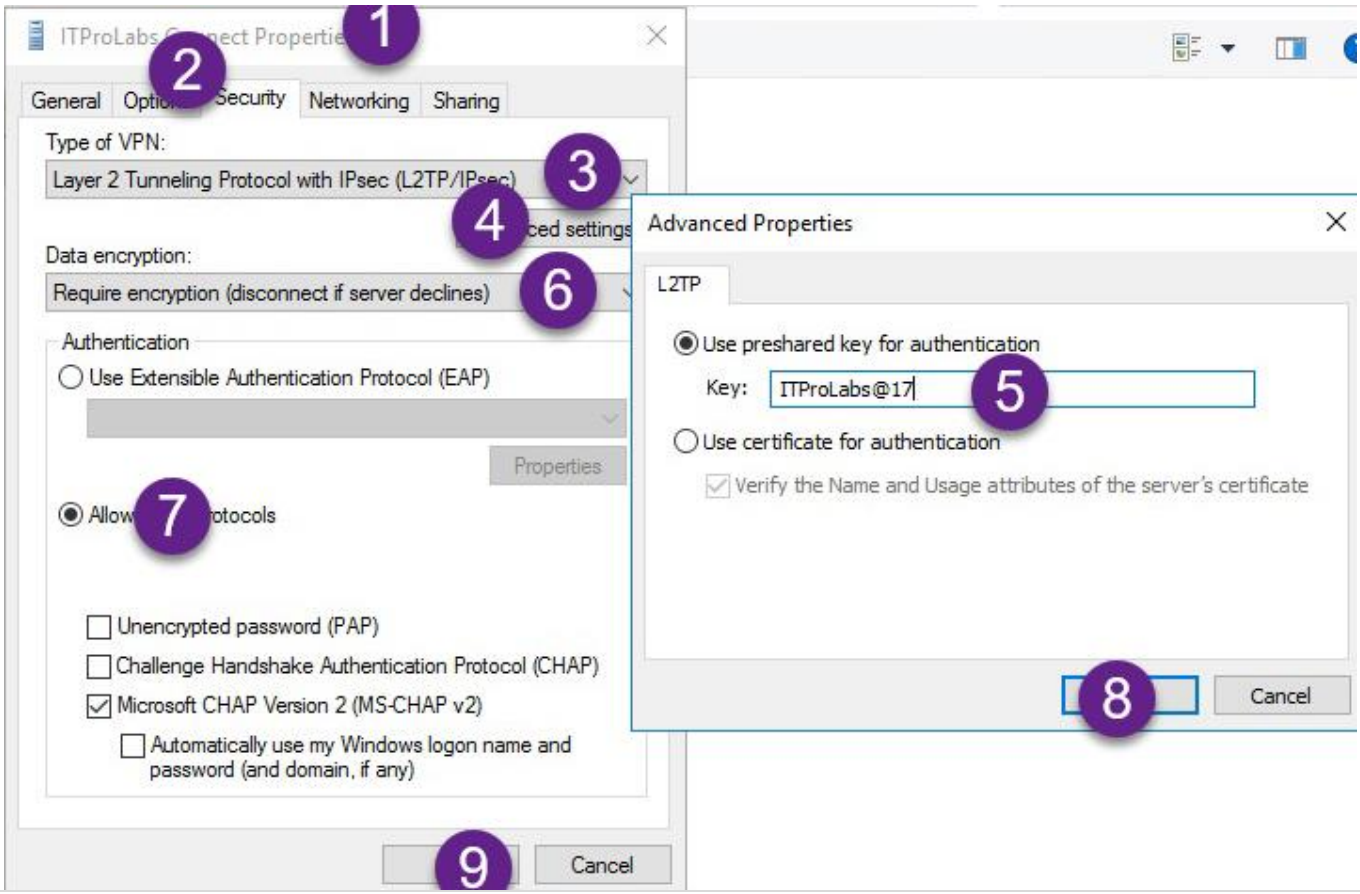
Connect to Windows Server 2016 on Azure and create VPN connect, as explained in the figures below



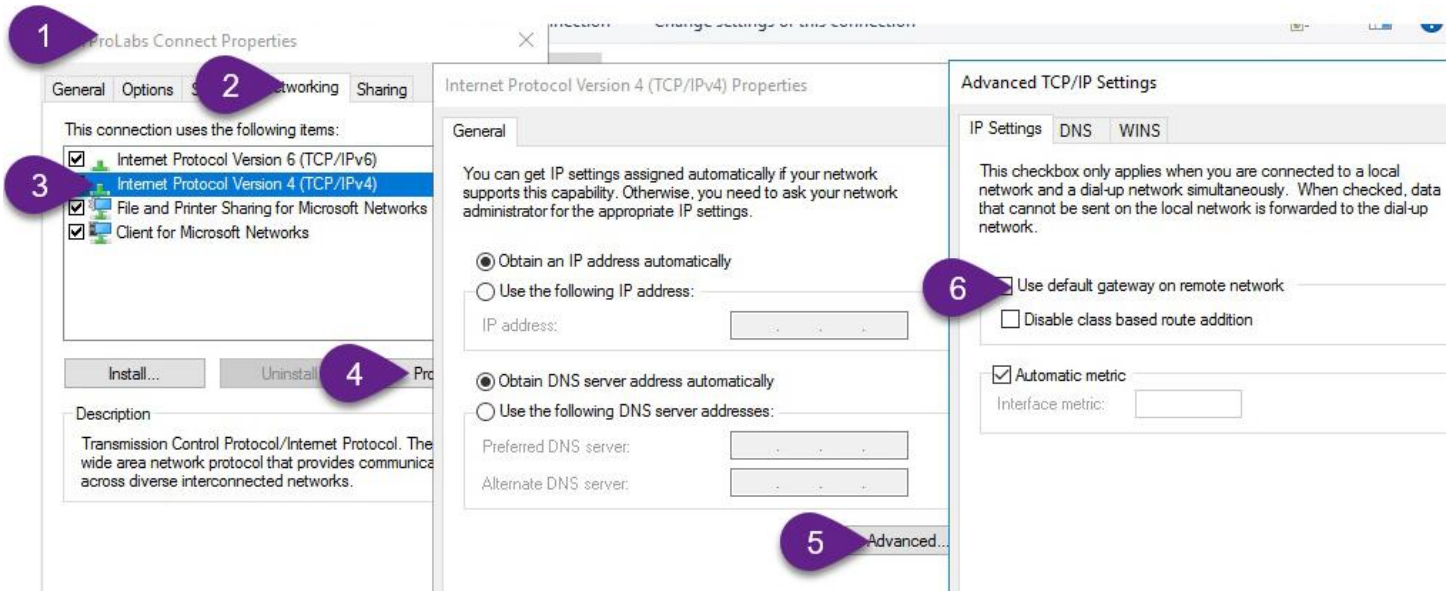


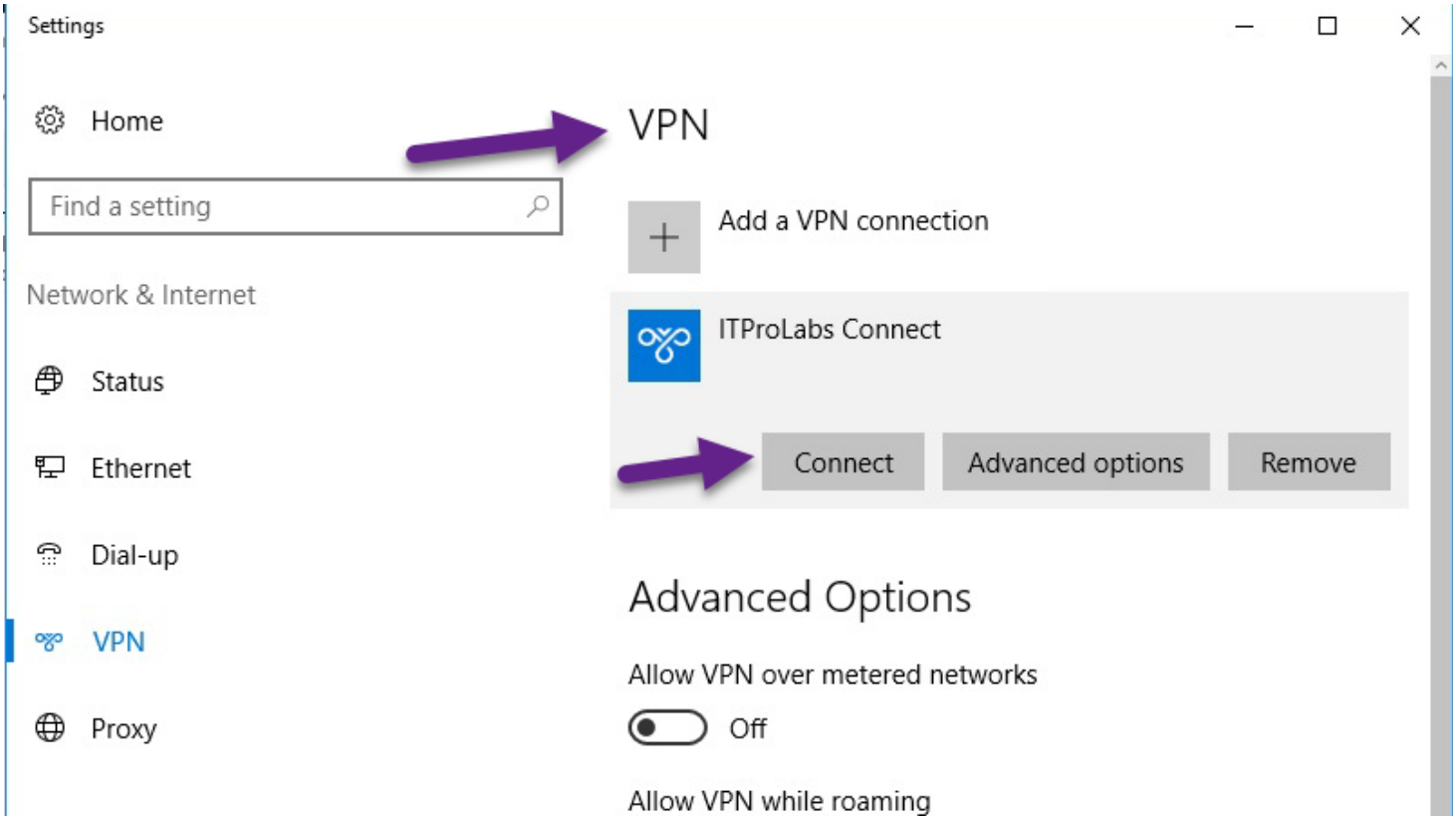


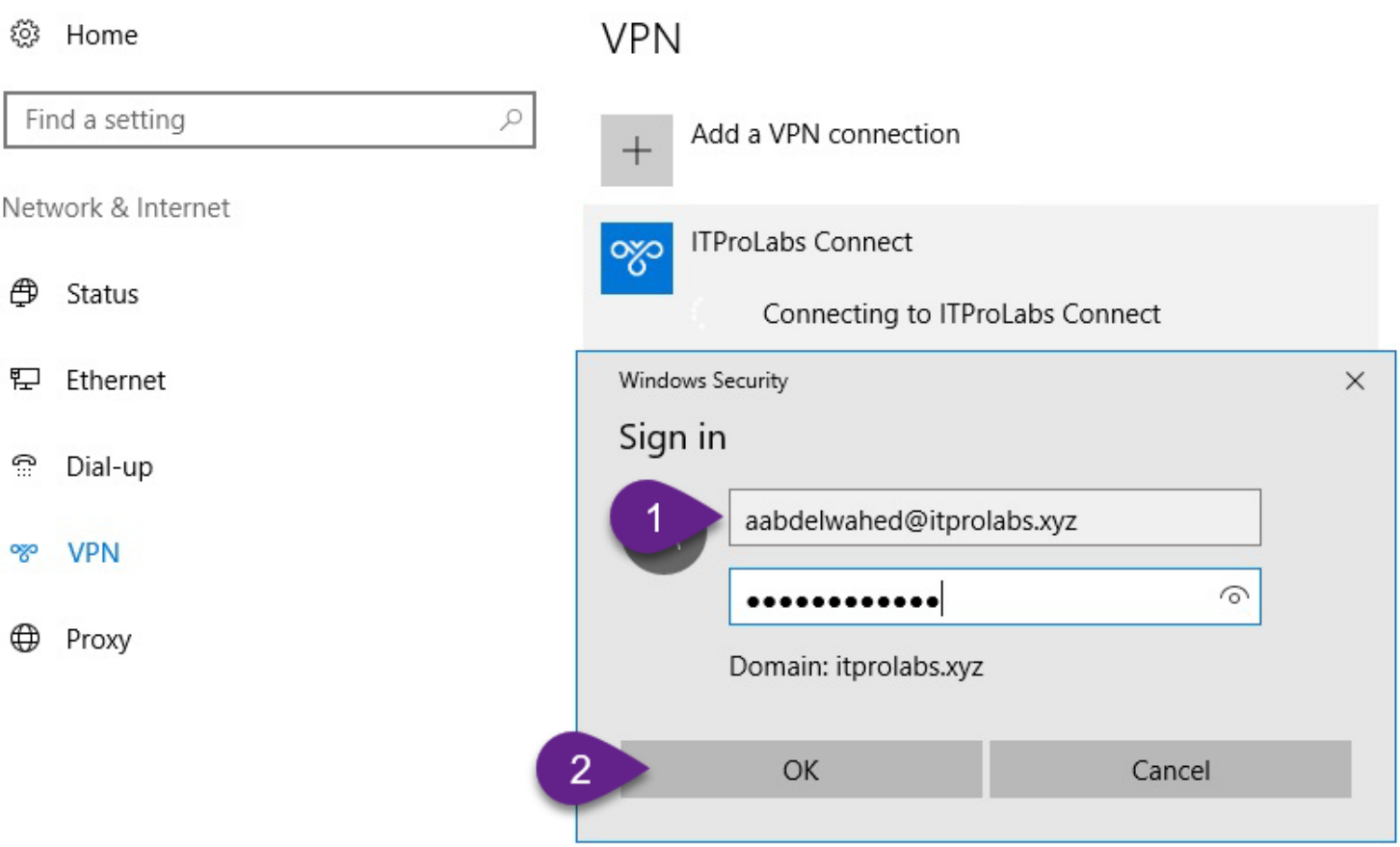
- Configure L2TP/IPsec

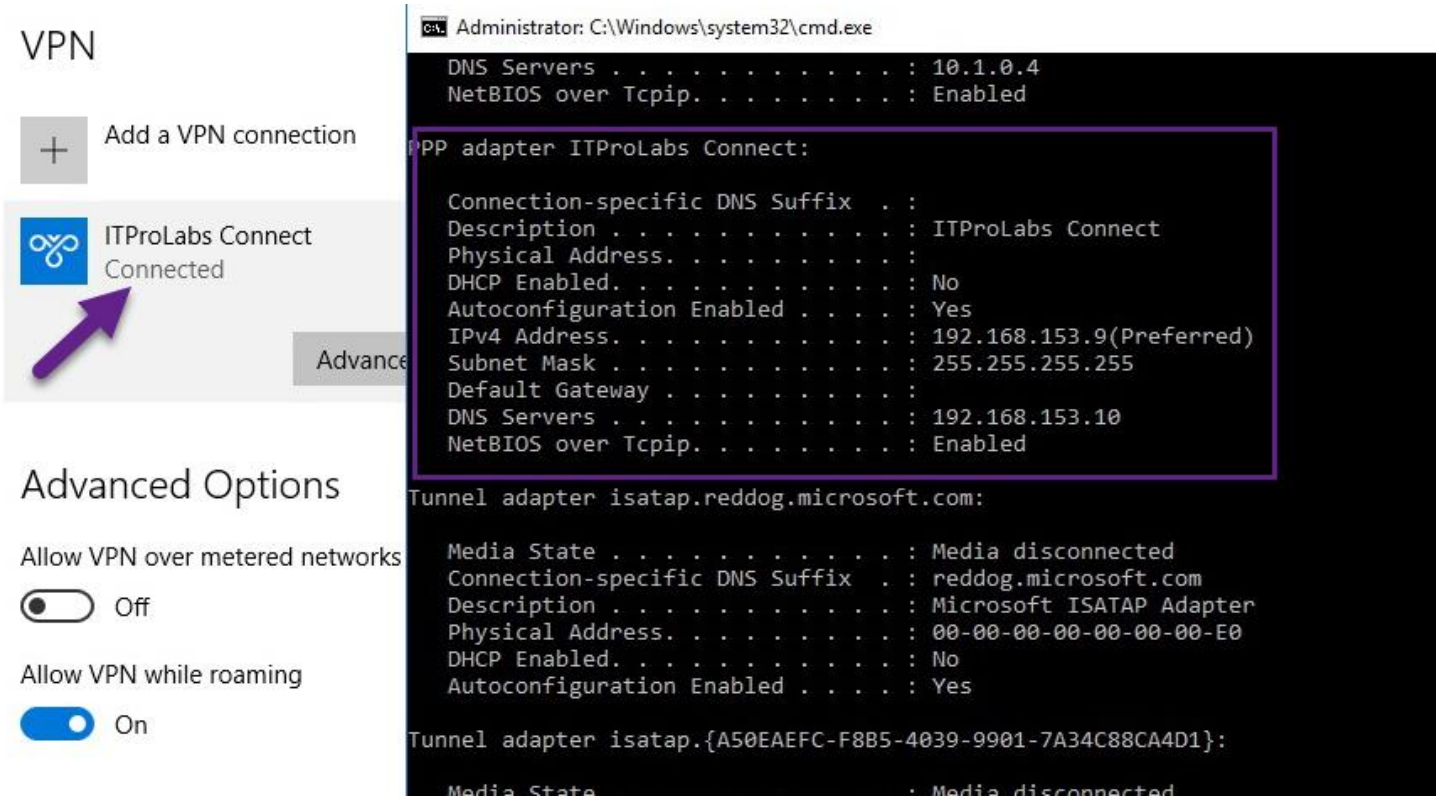


- Enable internet connectivity with VPN and start connection






Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
VPN
Add a VPN connection
ITProLabs Connect
Connecting to ITProLabs Connect
Windows Security
Sign in
1
aabdelwahed@itprolabs.xyz
Domain: itprolabs.xyz
2
OK
Cancel

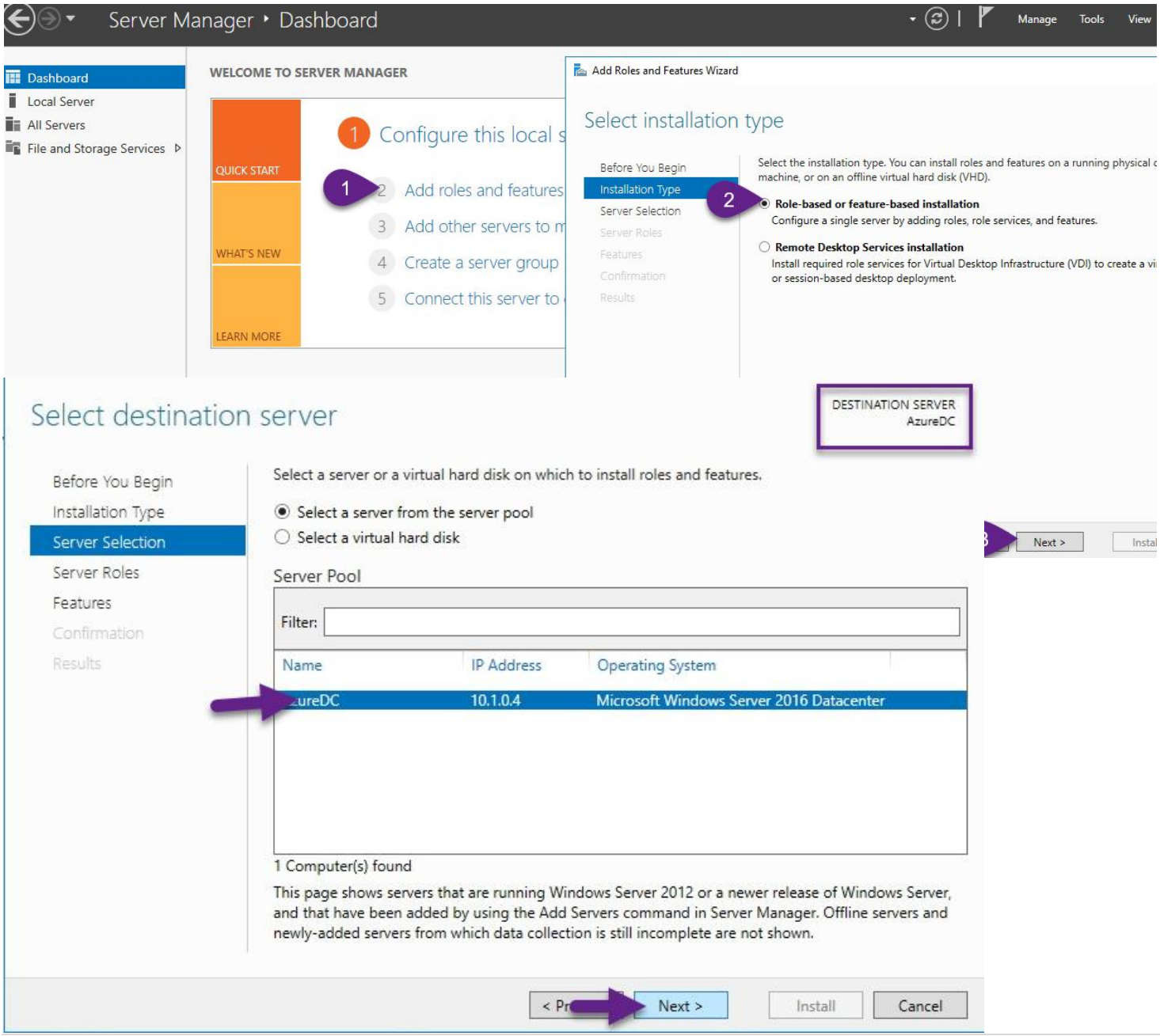

VPN
Add a VPN connection
ITProLabs Connect
Connected
Advance
Advanced Options
Allow VPN over metered networks
Off
Allow VPN while roaming
On
Administrator: C:\Windows\system32\cmd.exe
DNS Servers . . . . . : 10.1.0.4
NetBIOS over Tcpip. . . . . : Enabled
PPP adapter ITProLabs Connect:
Connection-specific DNS Suffix . :
Description . . . . . : ITProLabs Connect
Physical Address. . . . . :
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.153.9(Preferred)
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . :
DNS Servers . . . . . : 192.168.153.10
NetBIOS over Tcpip. . . . . : Enabled
Tunnel adapter isatap.reddog.microsoft.com:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : reddog.microsoft.com
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Tunnel adapter isatap.{A50EAEFC-F8B5-4039-9901-7A34C88CA4D1}:
Media State . . . . . : Media disconnected

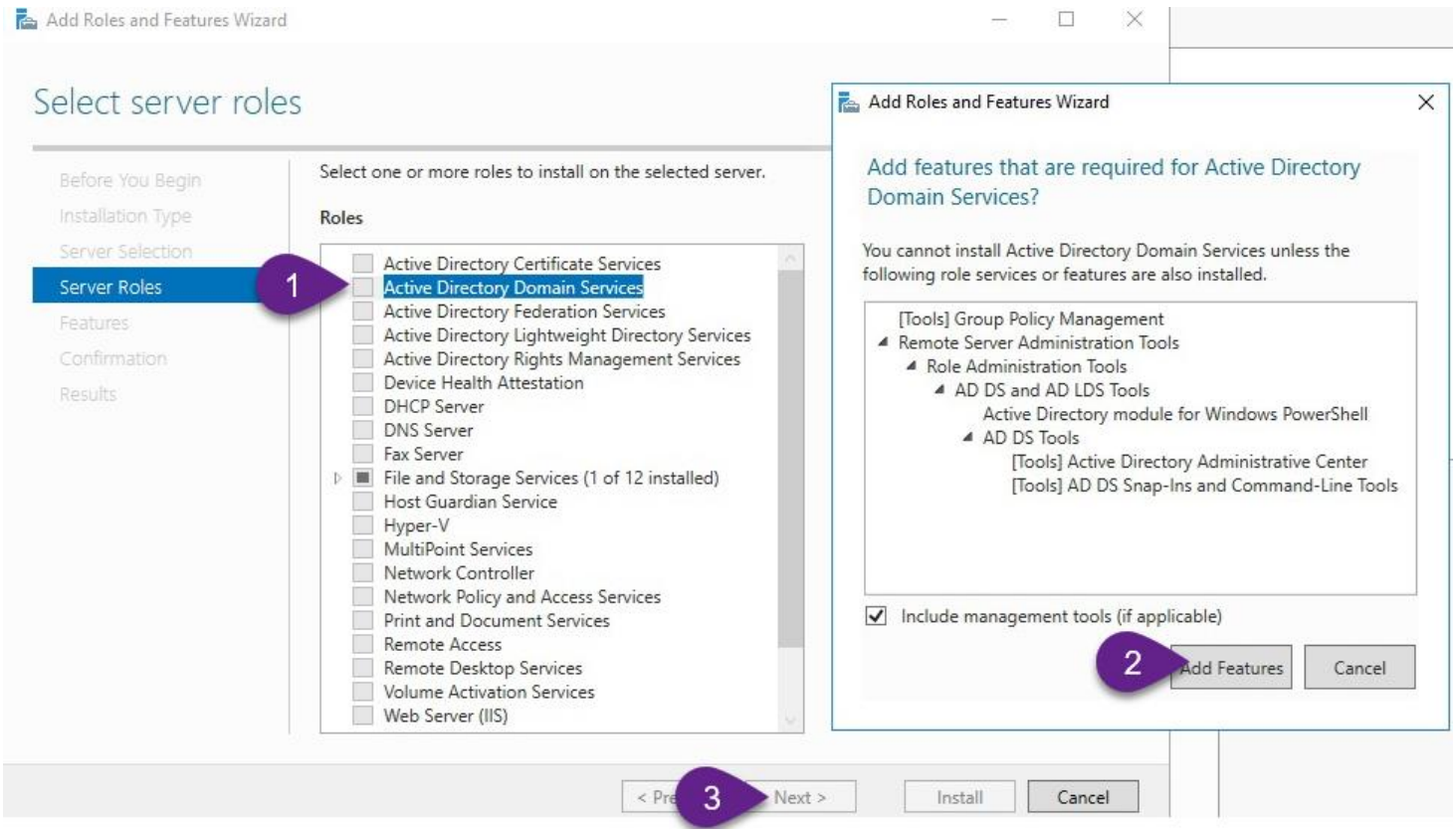
Now Windows Server 2016 VM on Microsoft Azure is ready to be additional DC for ITPROLABS.XYZ

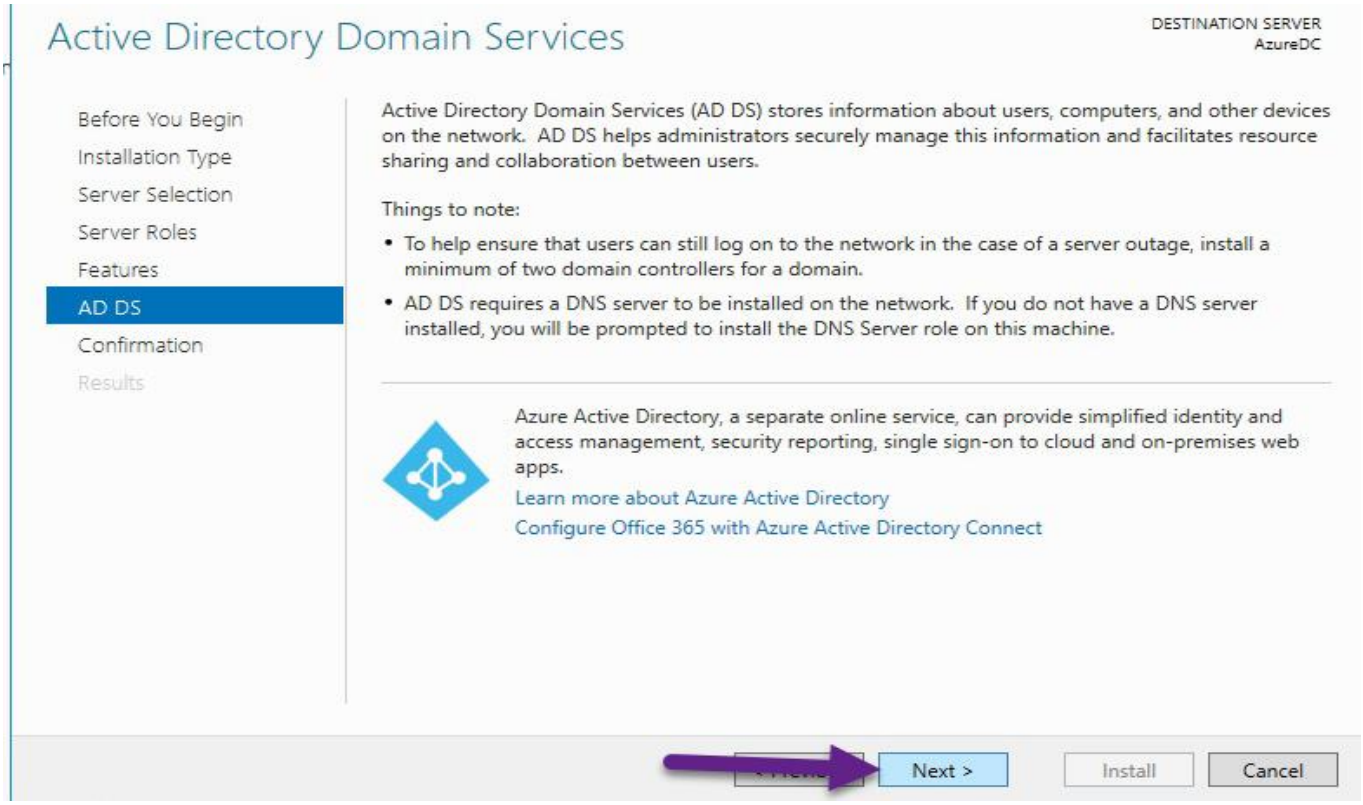
Install additional DC in Azure Windows Server 2016 VM

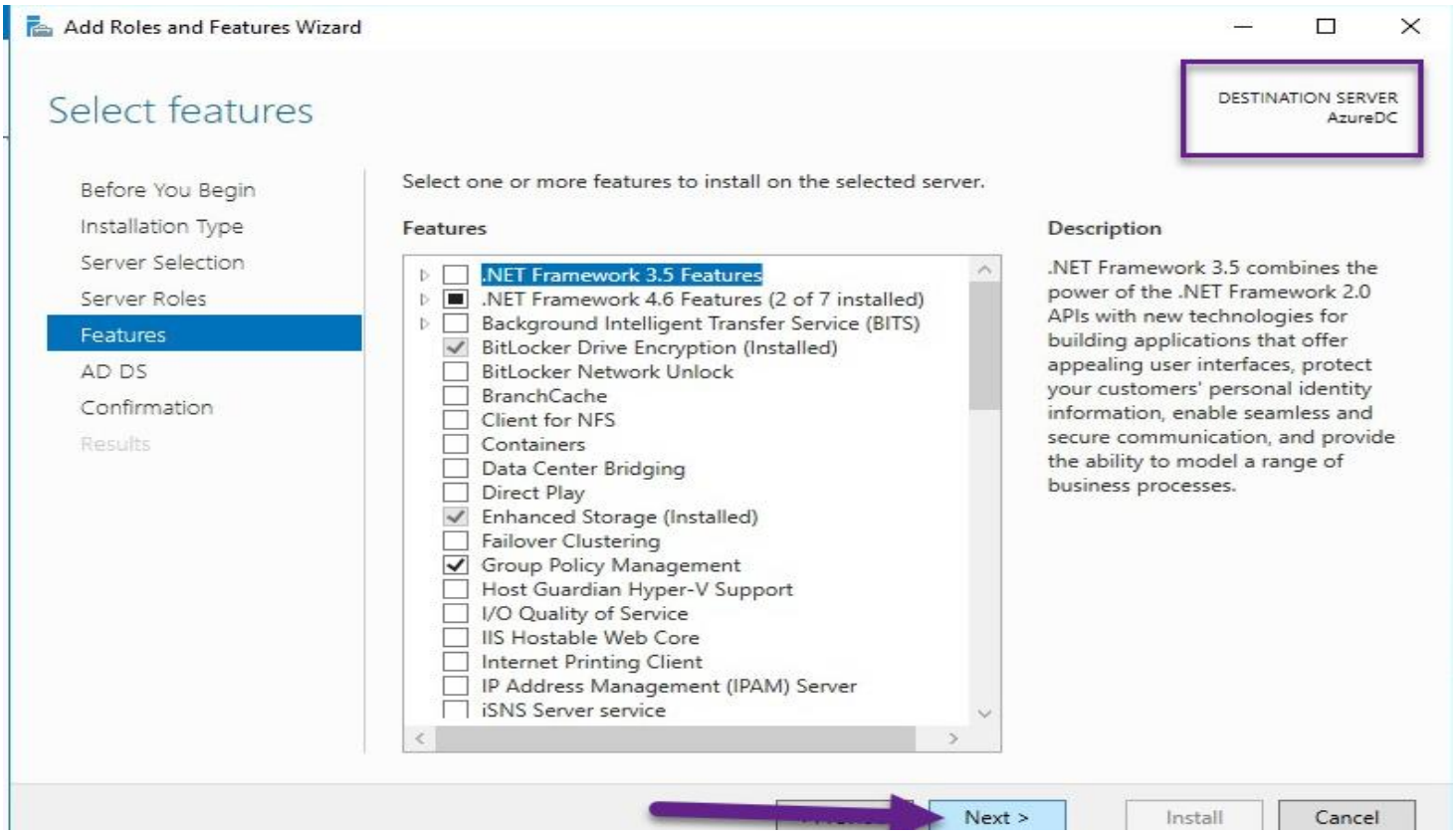
Now windows server 2016 VM on Microsoft Azure connected to our private network through L2TP/IPsec, so now we can create additional DC for our domain On-Perm (itprolabs.xyz)

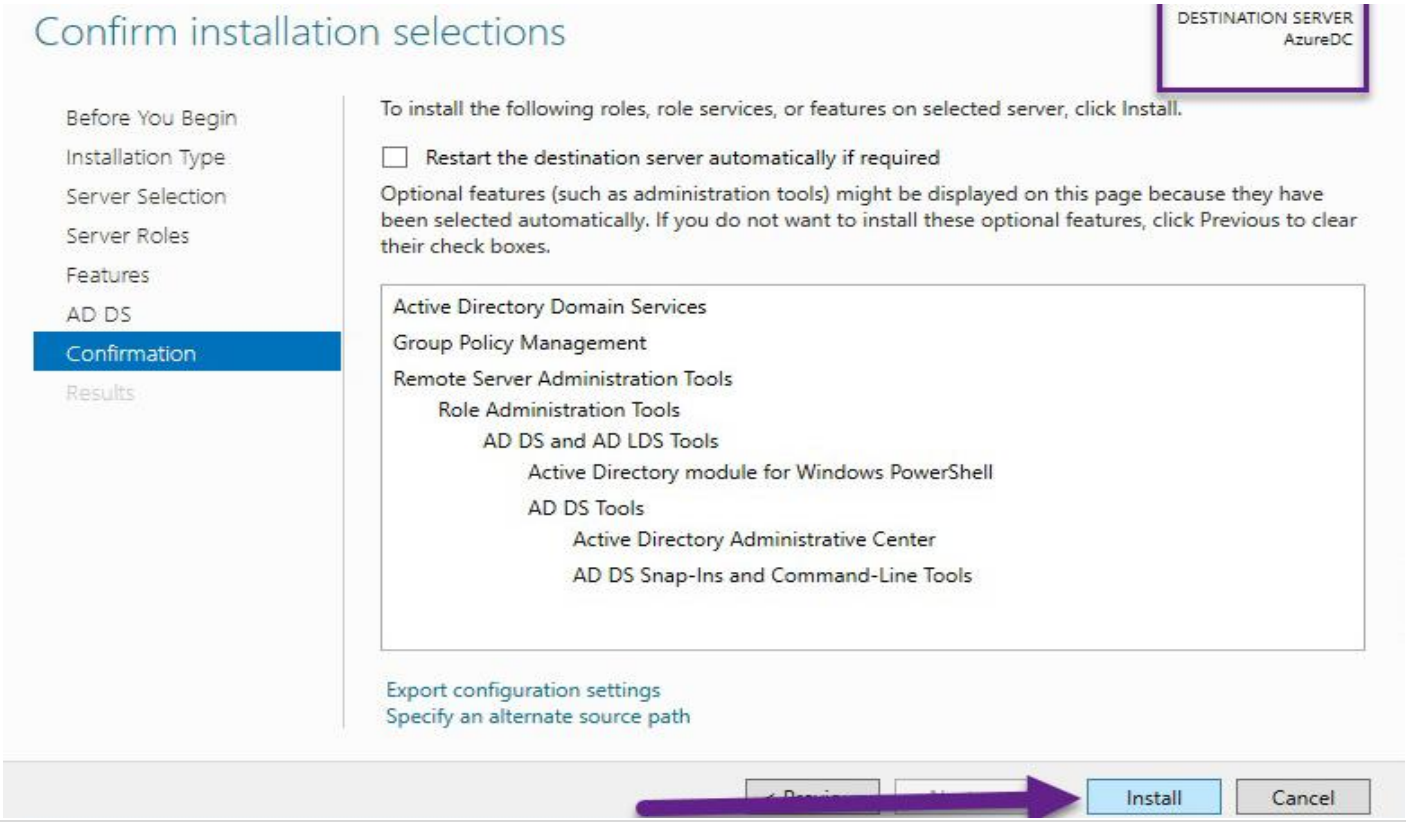
install Active Directory Domain services



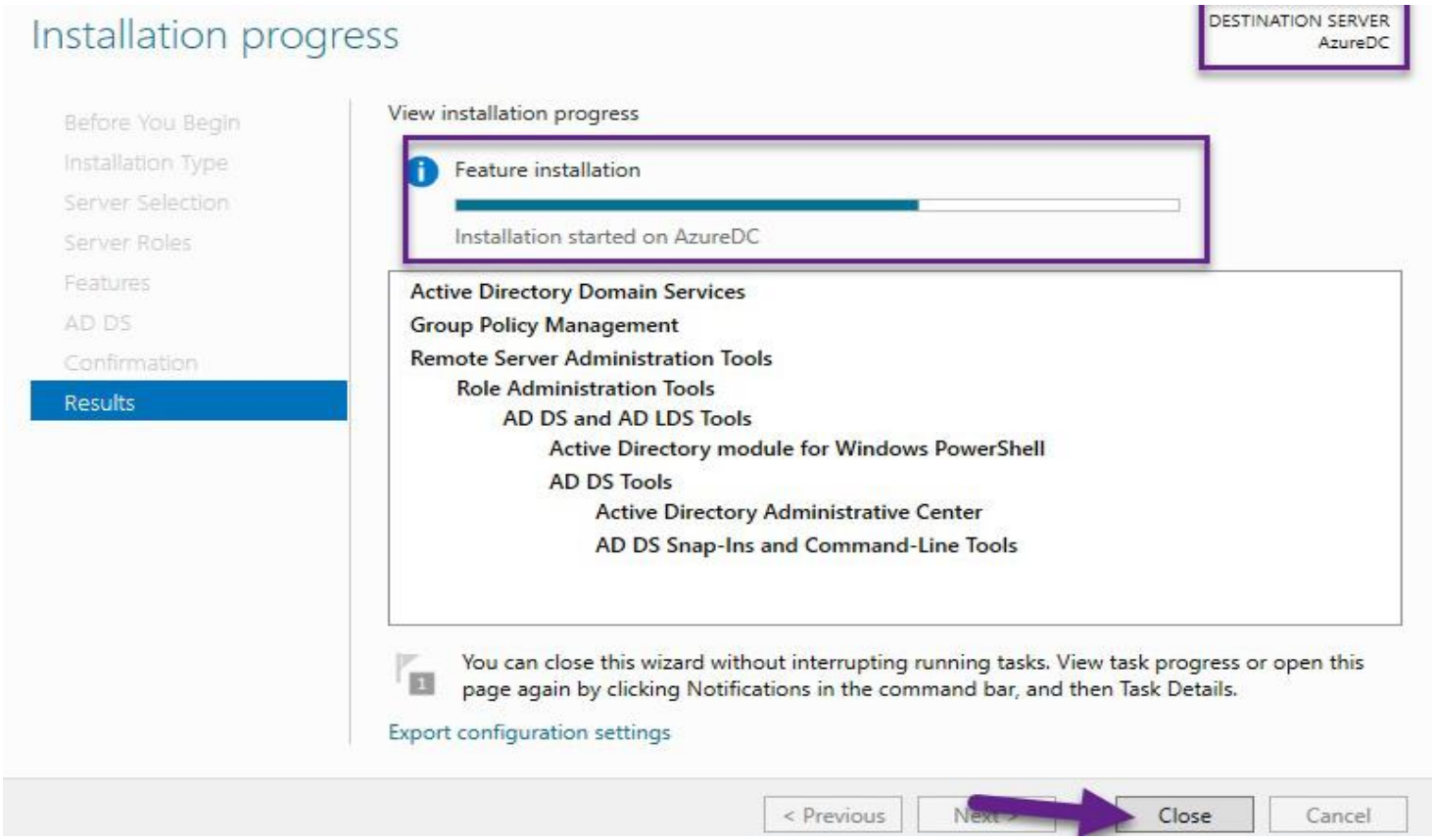

Add Roles and Features Wizard
Select server roles
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
1
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)
2
Add Features
Cancel
3
Next >
Install
Cancel


Active Directory Domain Services
DESTINATION SERVER
AzureDC
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.
Things to note:
• To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
• AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect
Next >
Install
Cancel

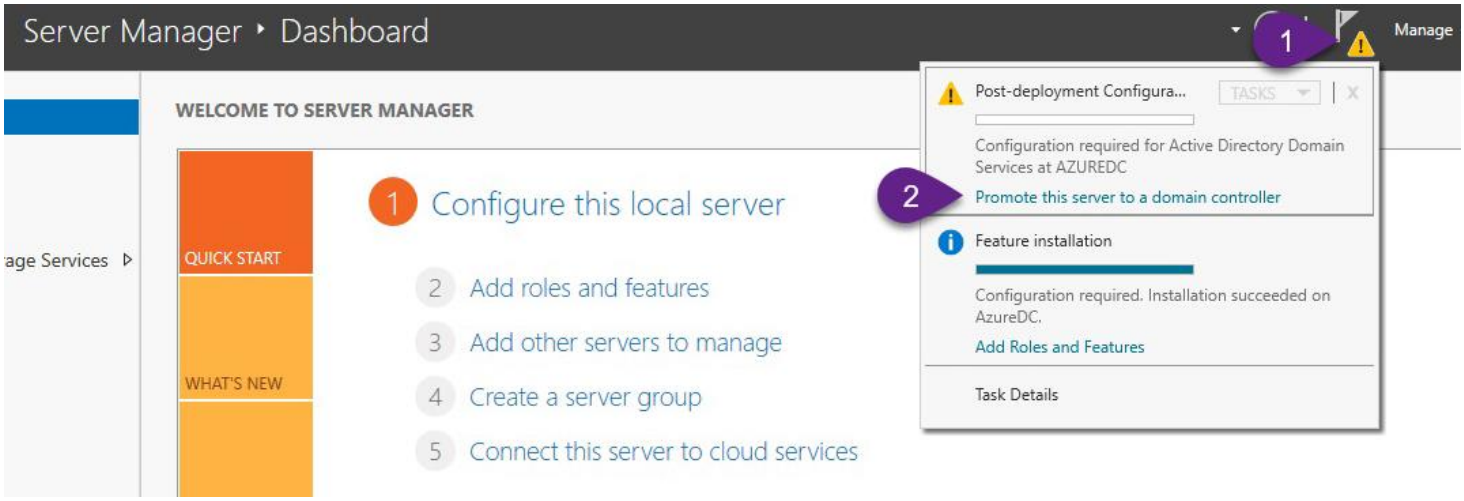

Add Roles and Features Wizard
Select features
DESTINATION SERVER
AzureDC
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.6 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption (Installed)
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage (Installed)
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
Next >
Install
Cancel


Confirm installation selections
DESTINATION SERVER
AzureDC
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
Install
Cancel

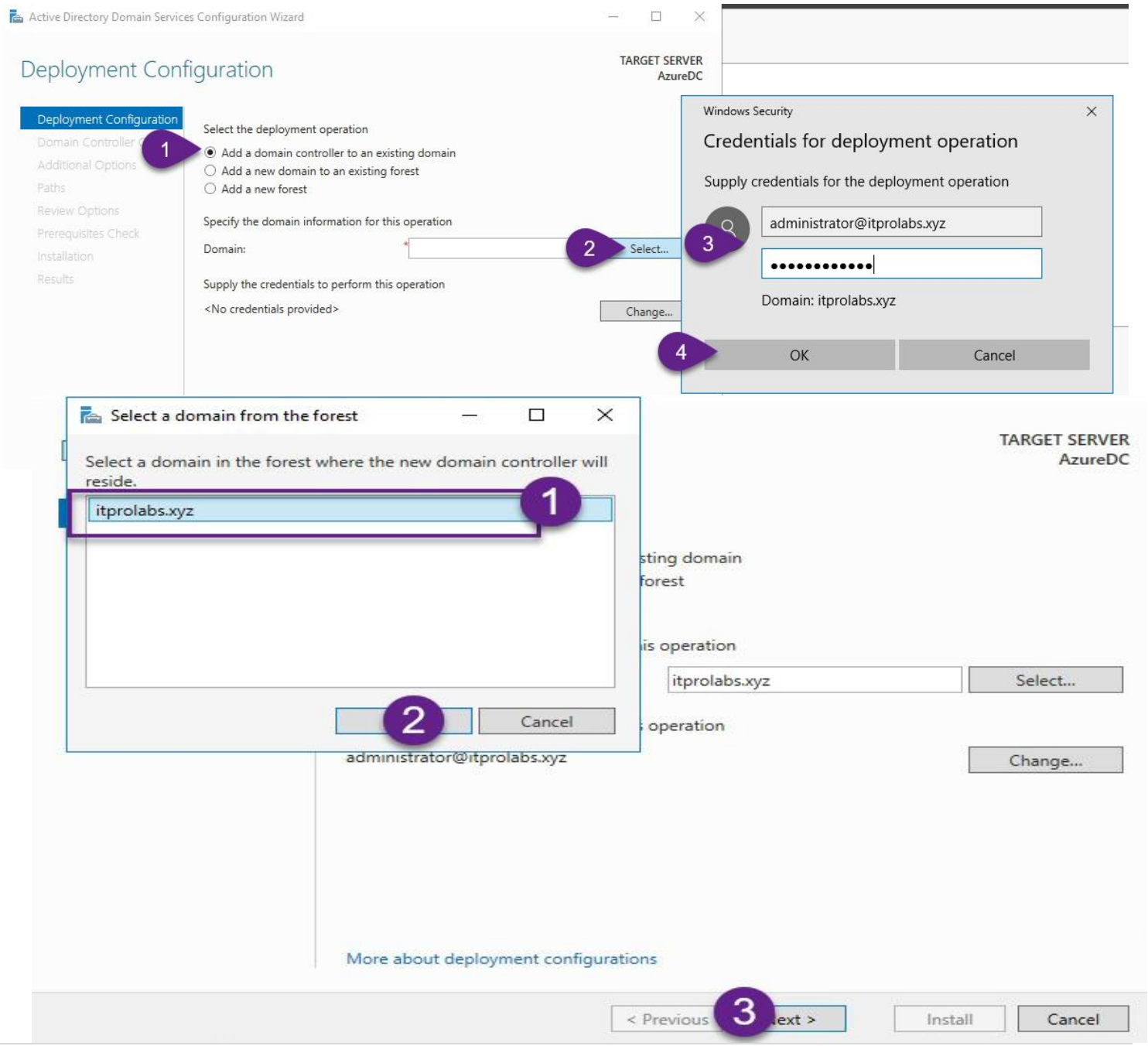
Extend On-Premises Windows Server Active Directory to Azure VM



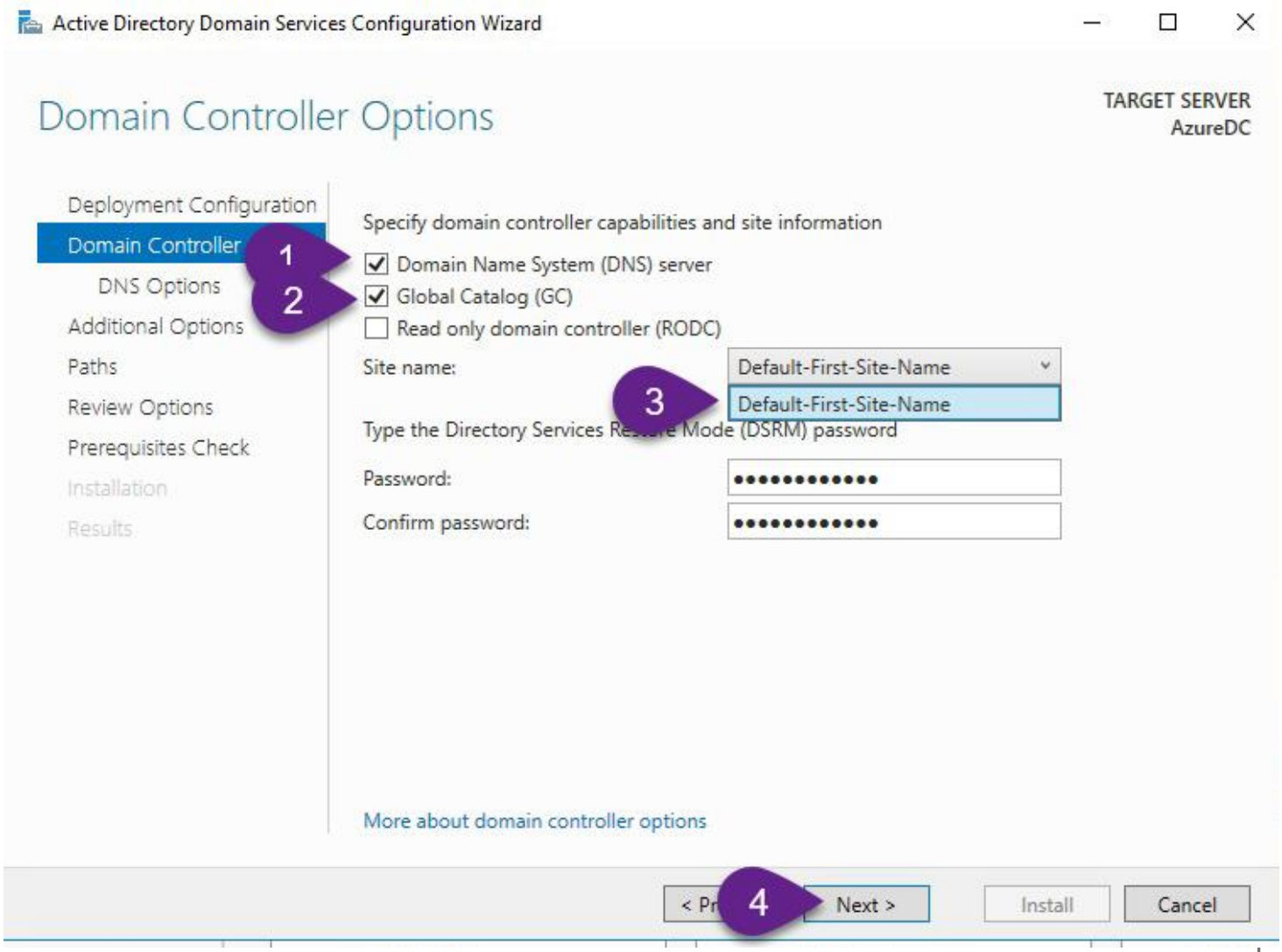
Promote Windows Server 2016 Data Center VM in Azure to be additional DC

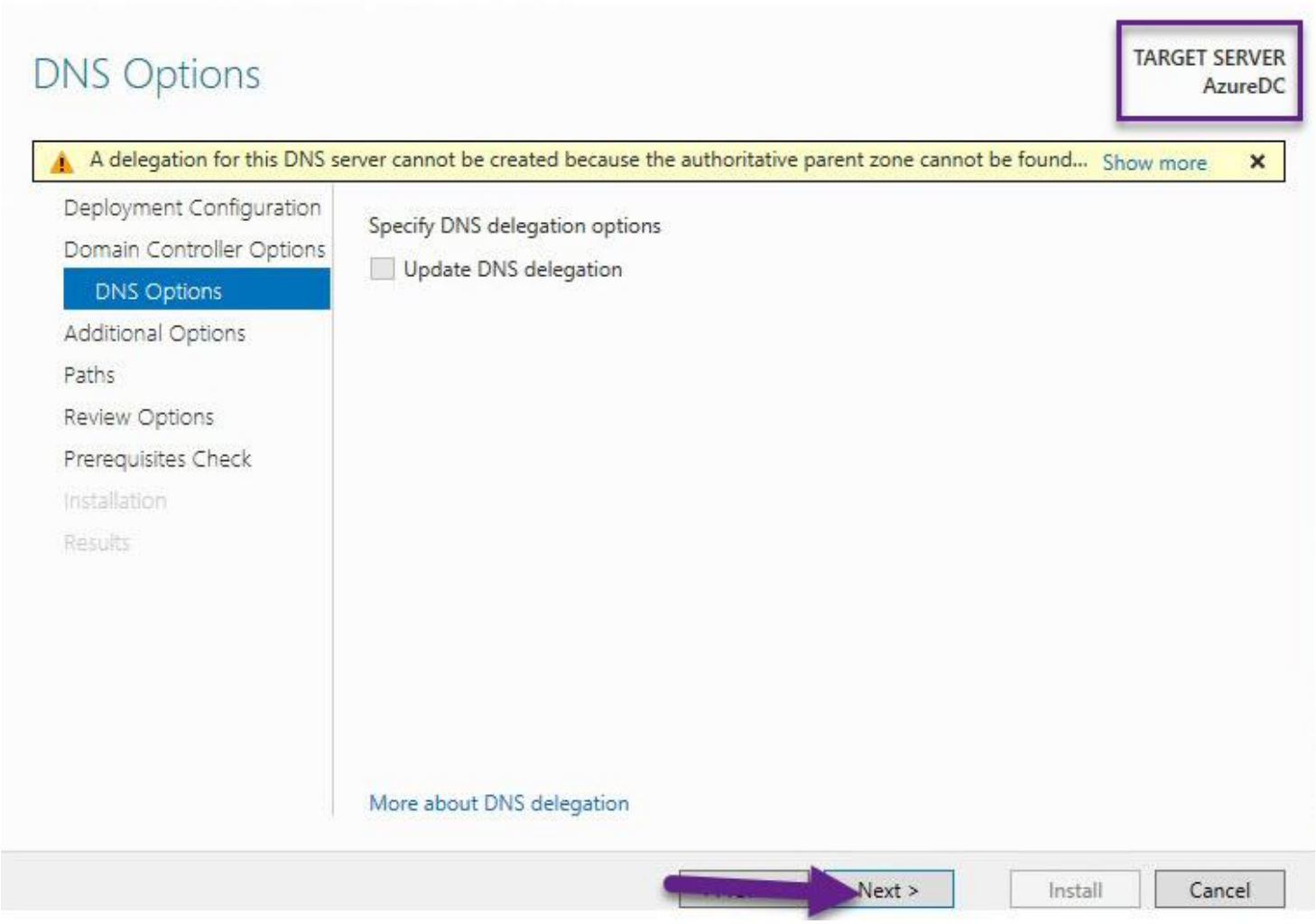


1. There is three options when you try to promoote your server to active dirctory:
   - Promote your server to be additional DC in existing domain (selected for our scienario)
   - Promote your server to child domain in existing forest
   - Promote your server to new forst
2. Select your domain that you want to create additional for (select itprolabs.xyz for our scienario).

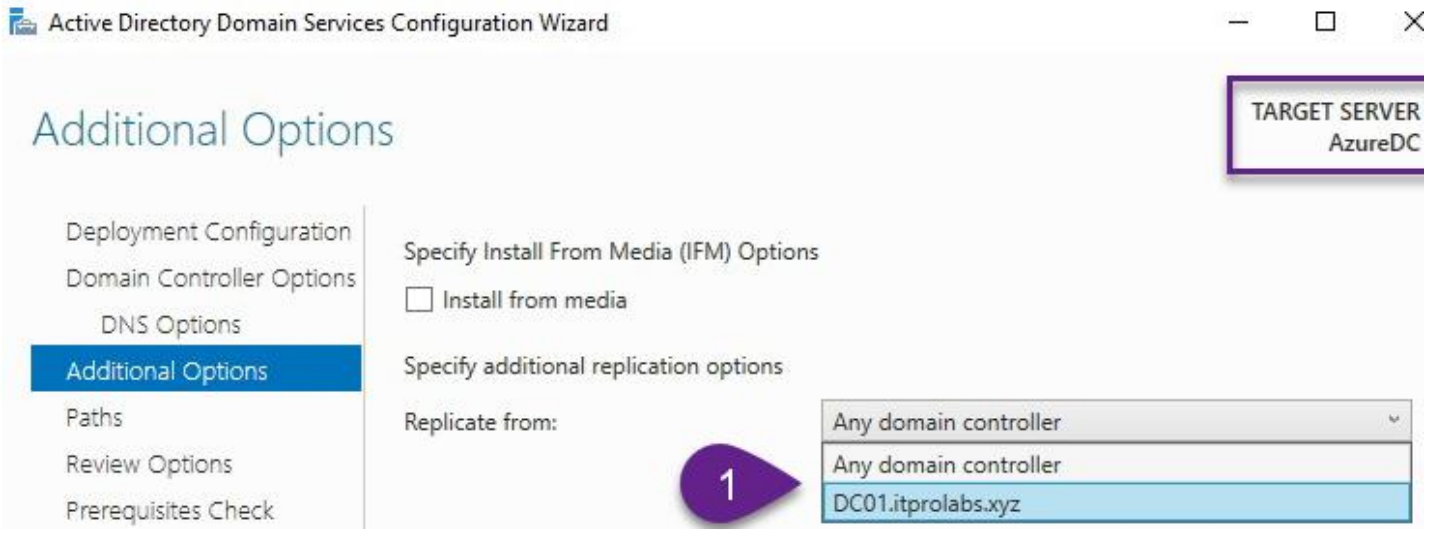


3. Its recommend to allow this server to also work as **GC** and **DNS** according to your requirements, also select site that will host your server, if you select the same site with parent domain your replication between two servers will be at the same time by default.

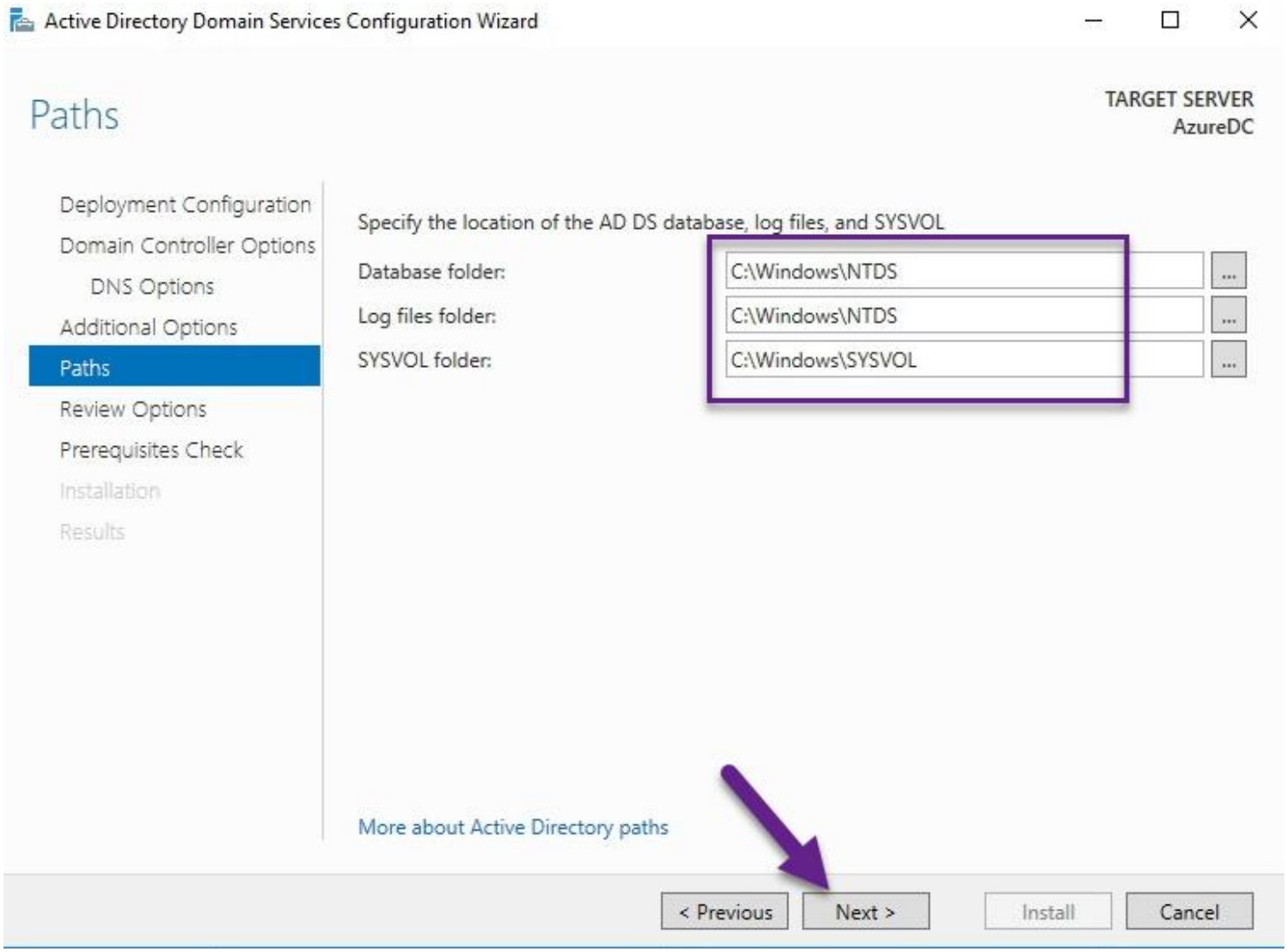




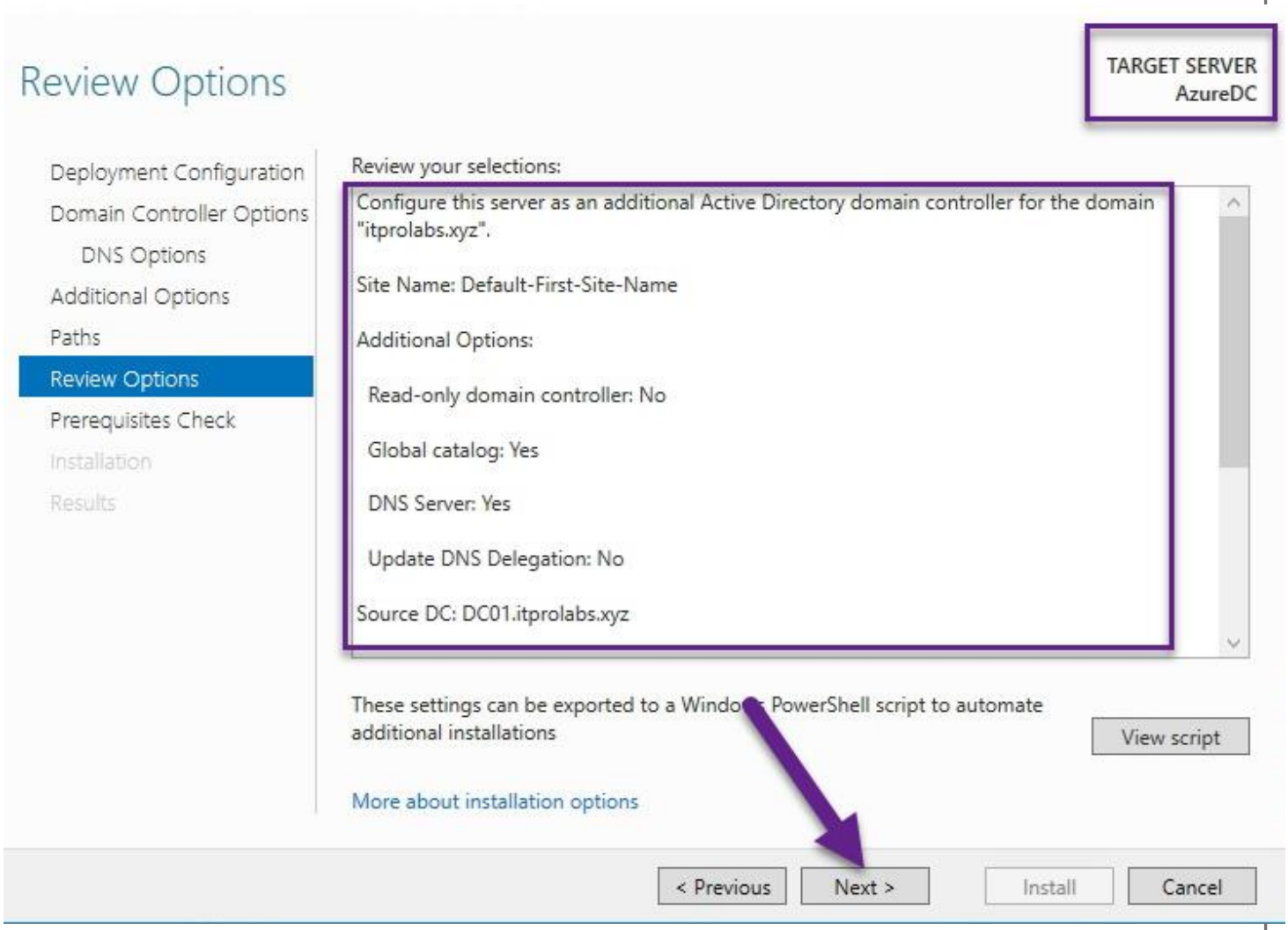
4. Select which DC that you want to replicate from



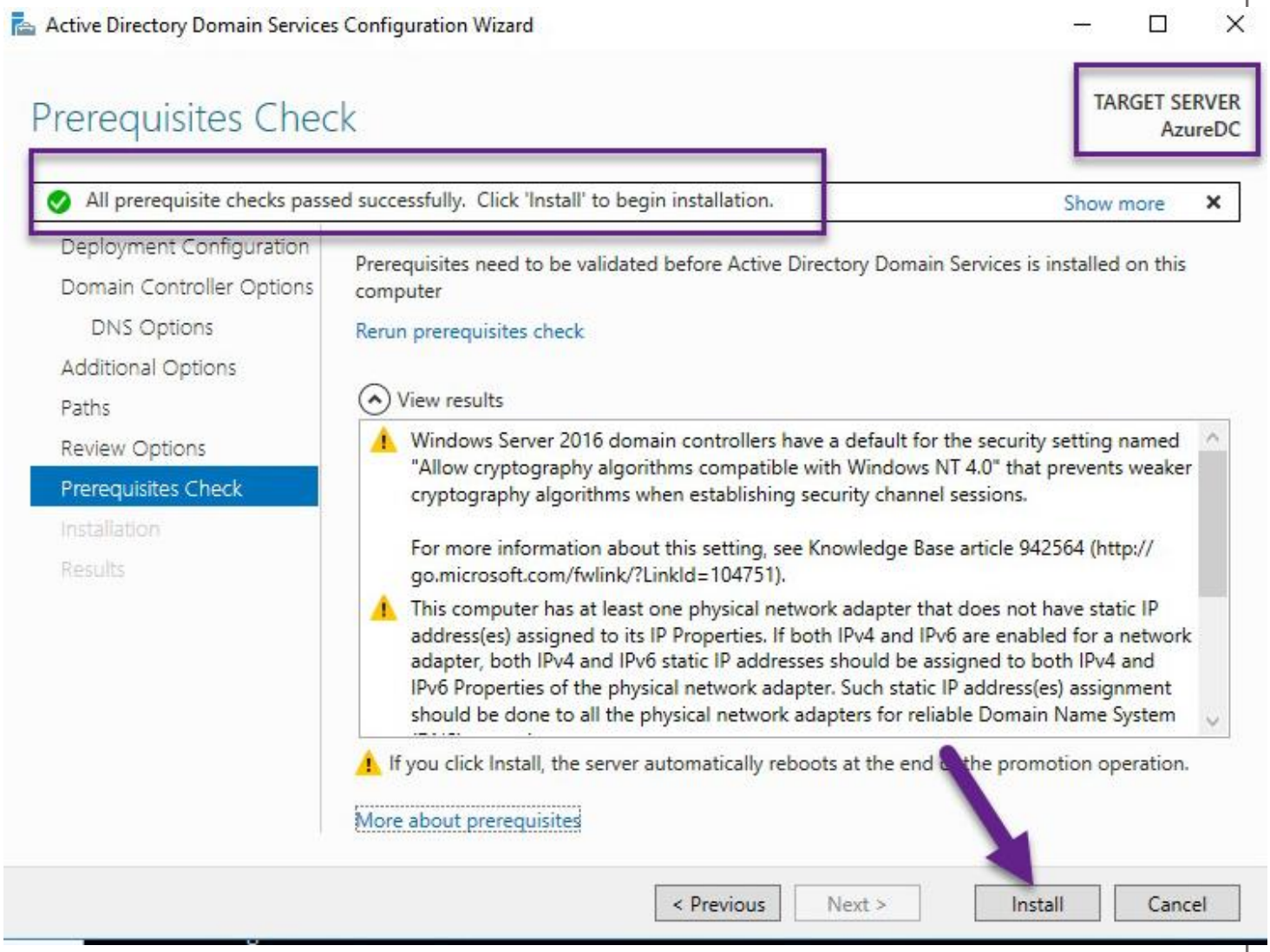
5. Select active directory database and log files store location



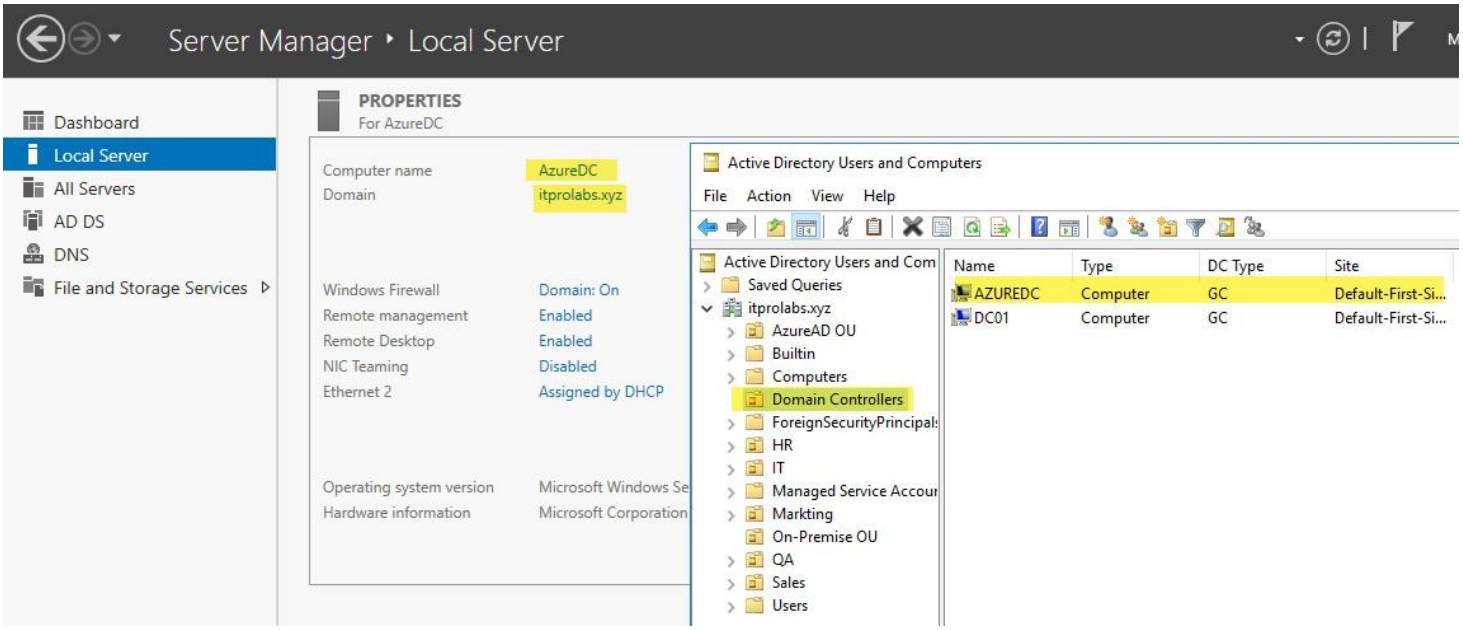
6. Review your selected configuration



7. Prerequisites checked passed, now your VM is ready to promote.

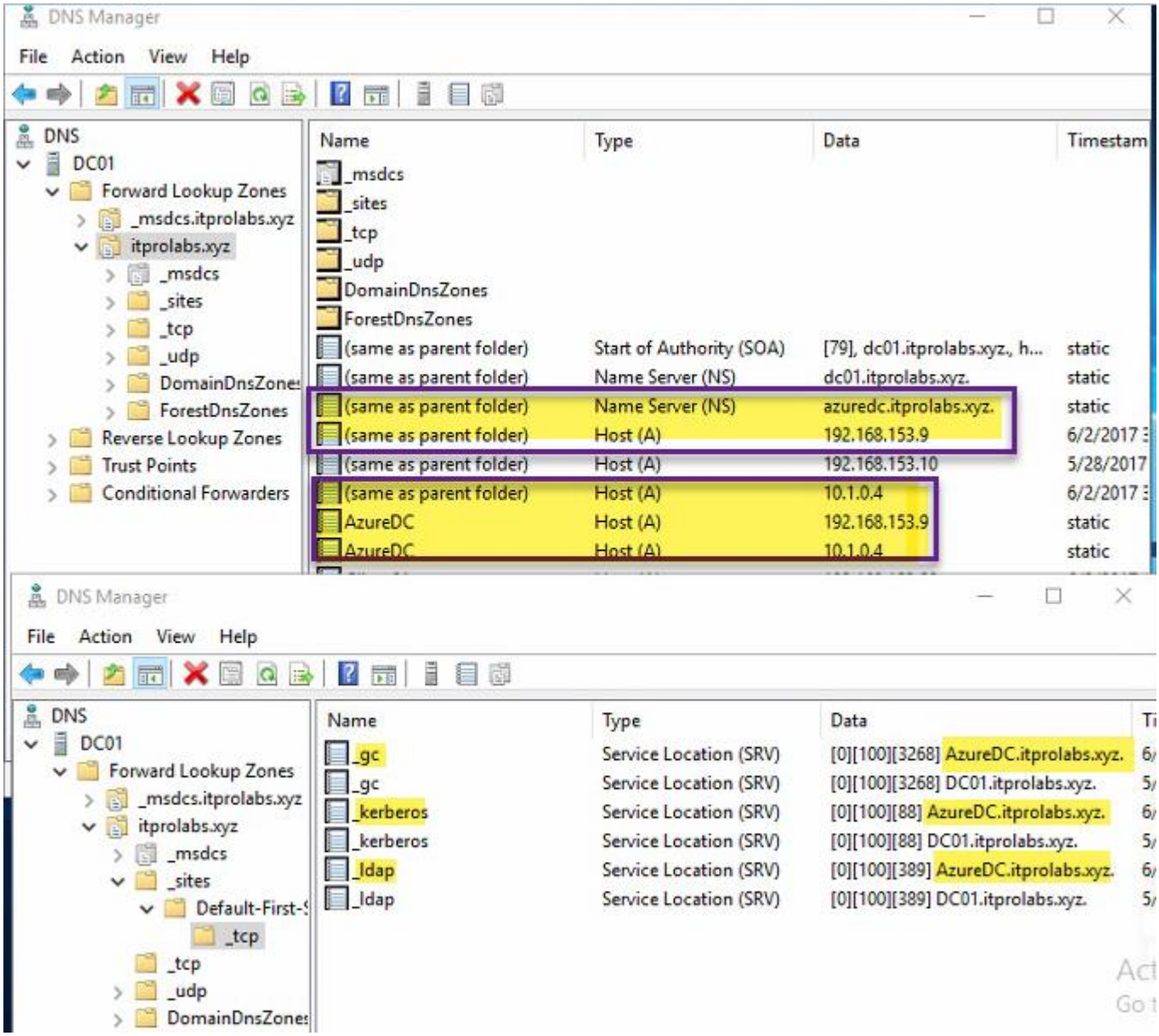


8. Now Windows Server 2016 is working as additional DC.

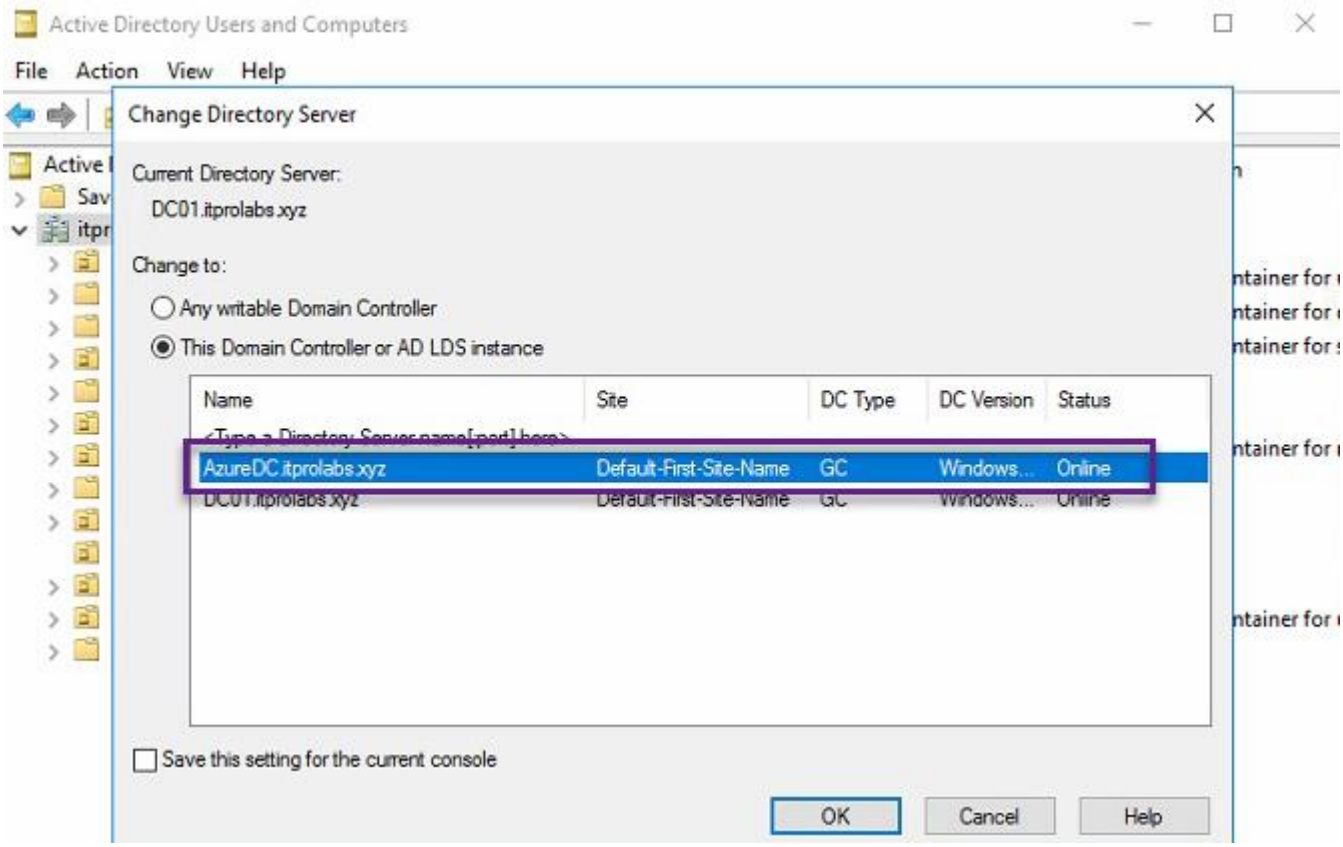


Check Active Directory & DNS changes

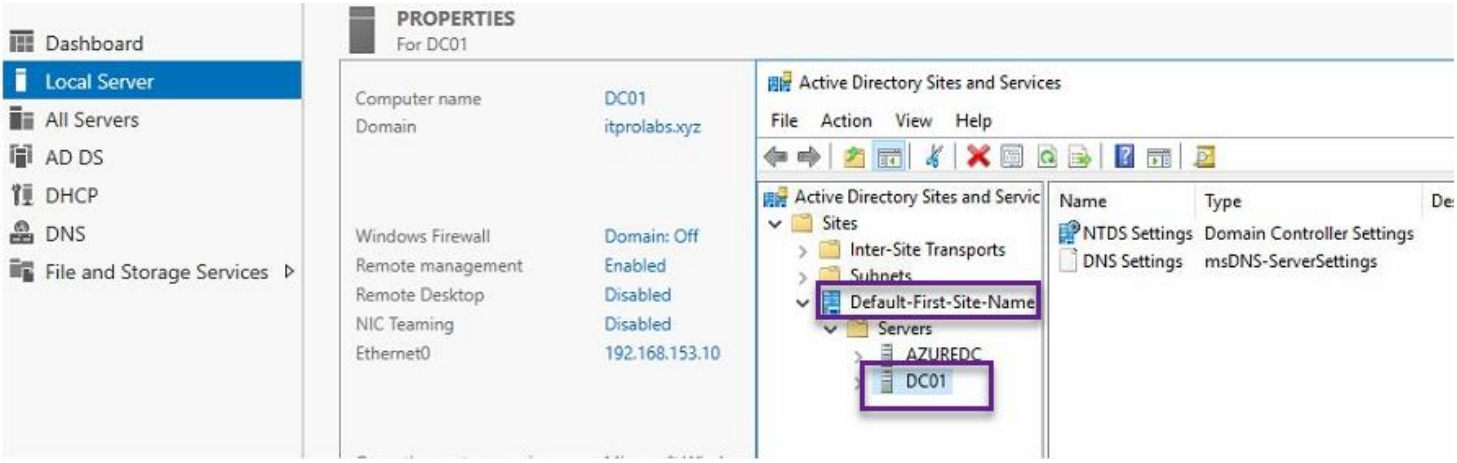
1. From **DNS**, our new DC on azure is added as name server, GC, Kerberos and LDAP.



2. Our VM Server on Azure is added as a DC

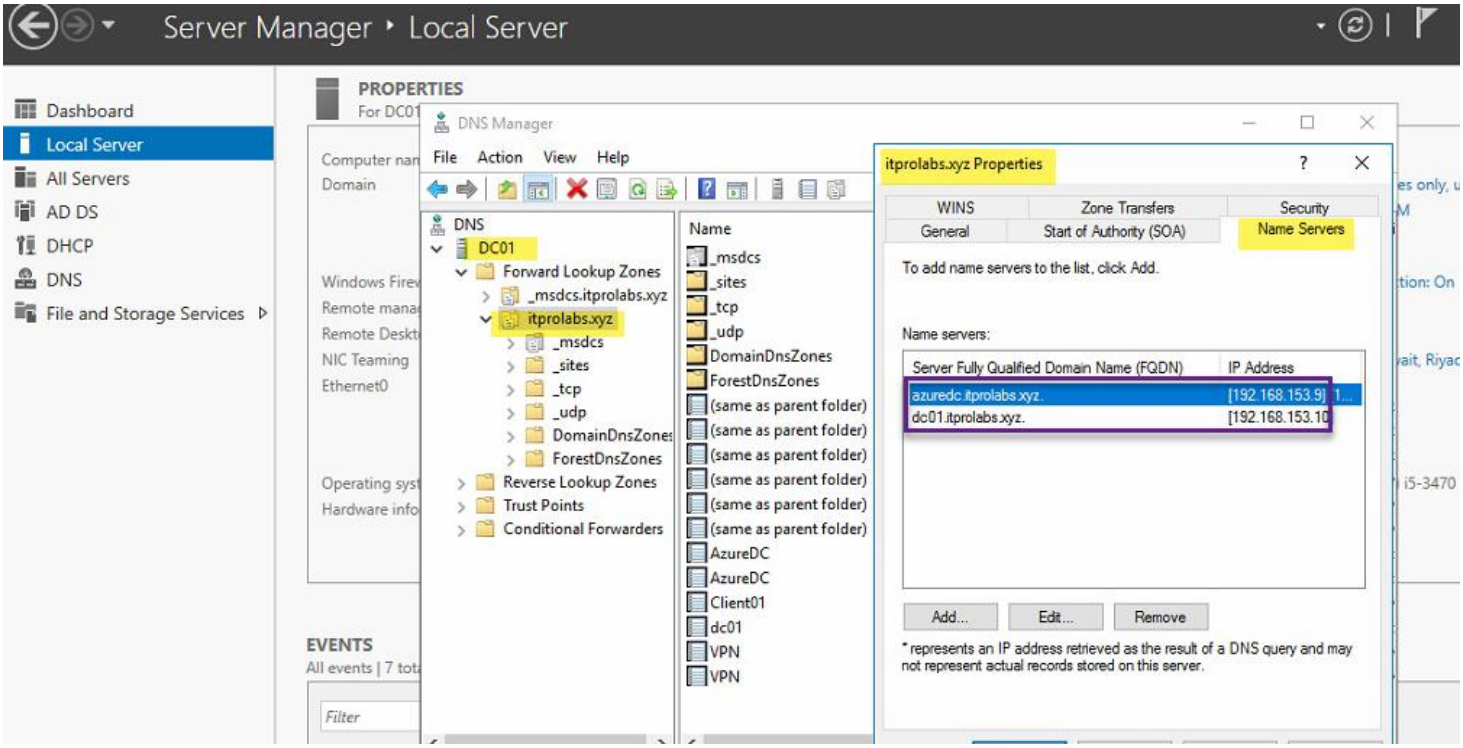


3. Also, is added as second server in default **active directory site**

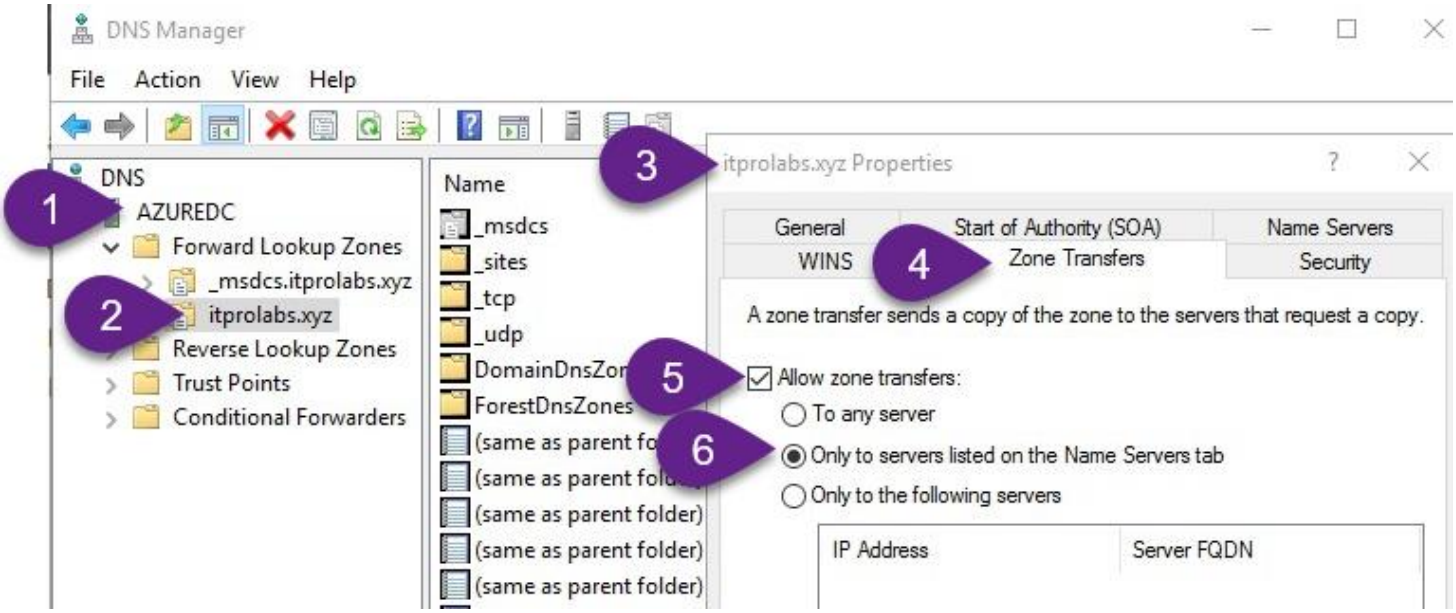


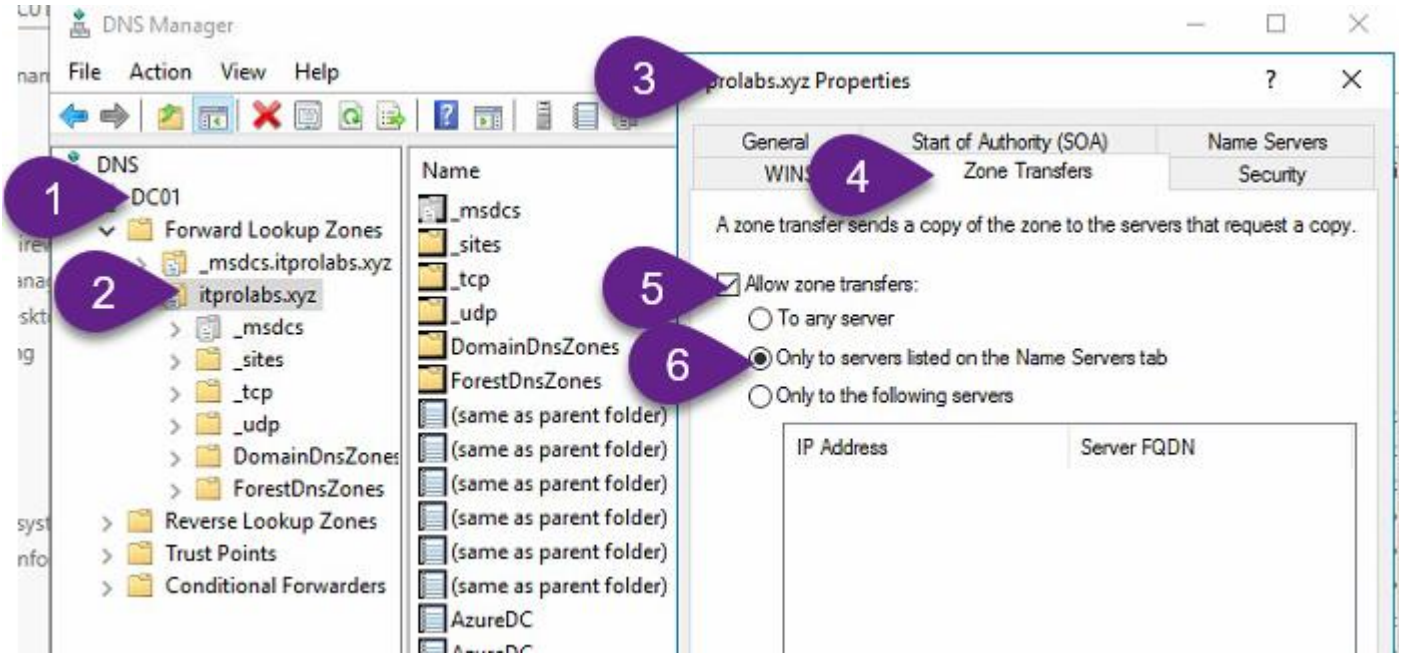
Allow DNS zone transfer between two servers

through additional DC installation and configuration process we allow additional DC to work as DNS server, so when we access DNS wizard as figured below we will find in **name servers** tab our two DNS servers.

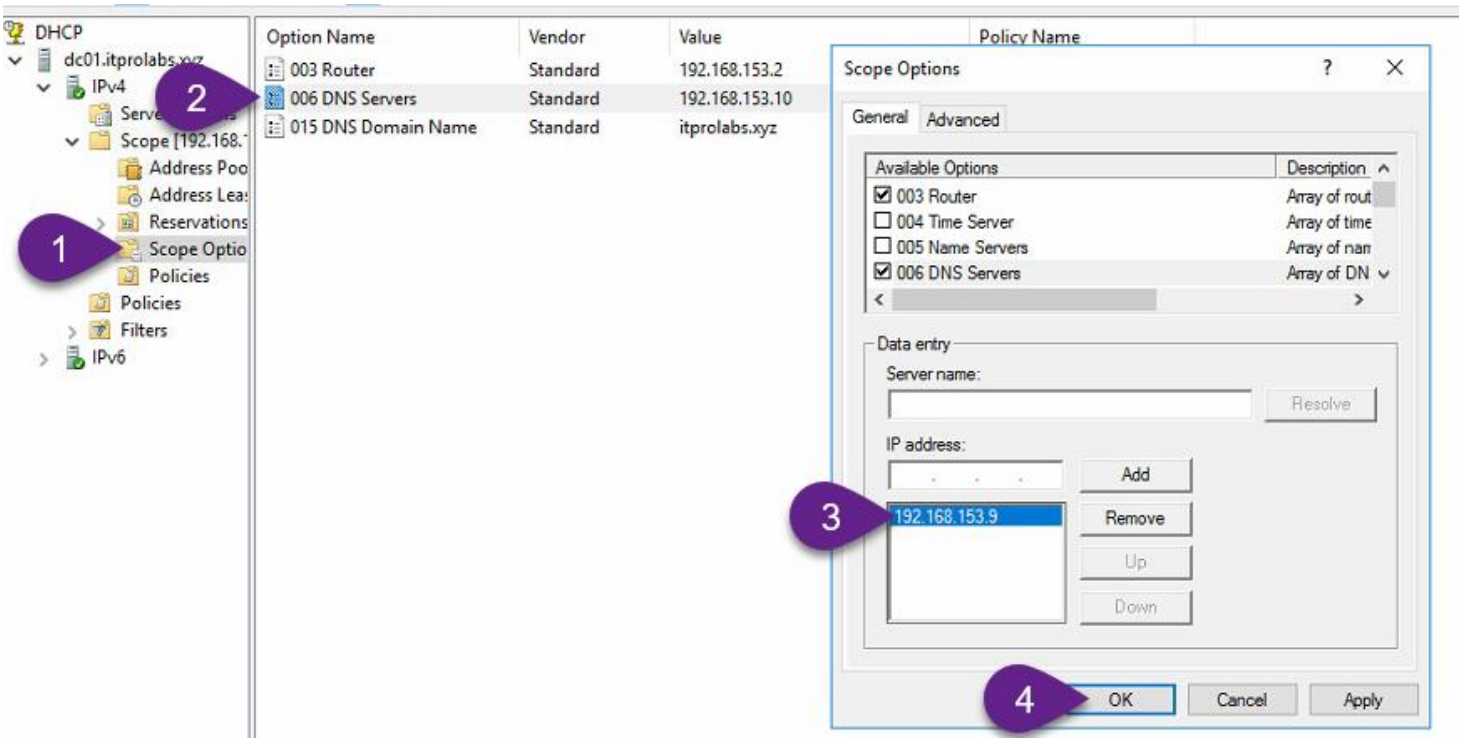


Finally, we will configure DNS zone transfer between the two servers. As explained in the figures below



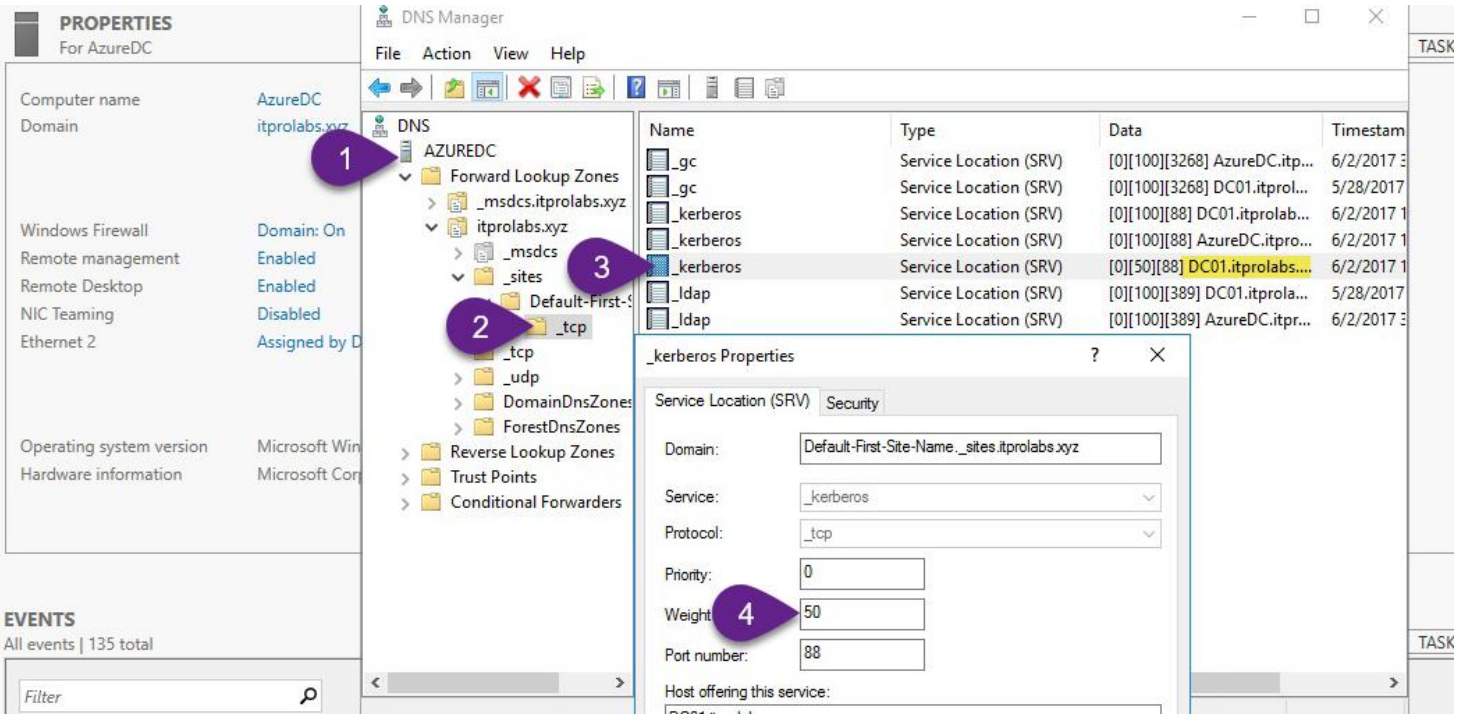


Configure DHCP to force internal users to use a new DC on Azure as DNS



Configure DNS to force internal users to use a new DC on Azure for authentication

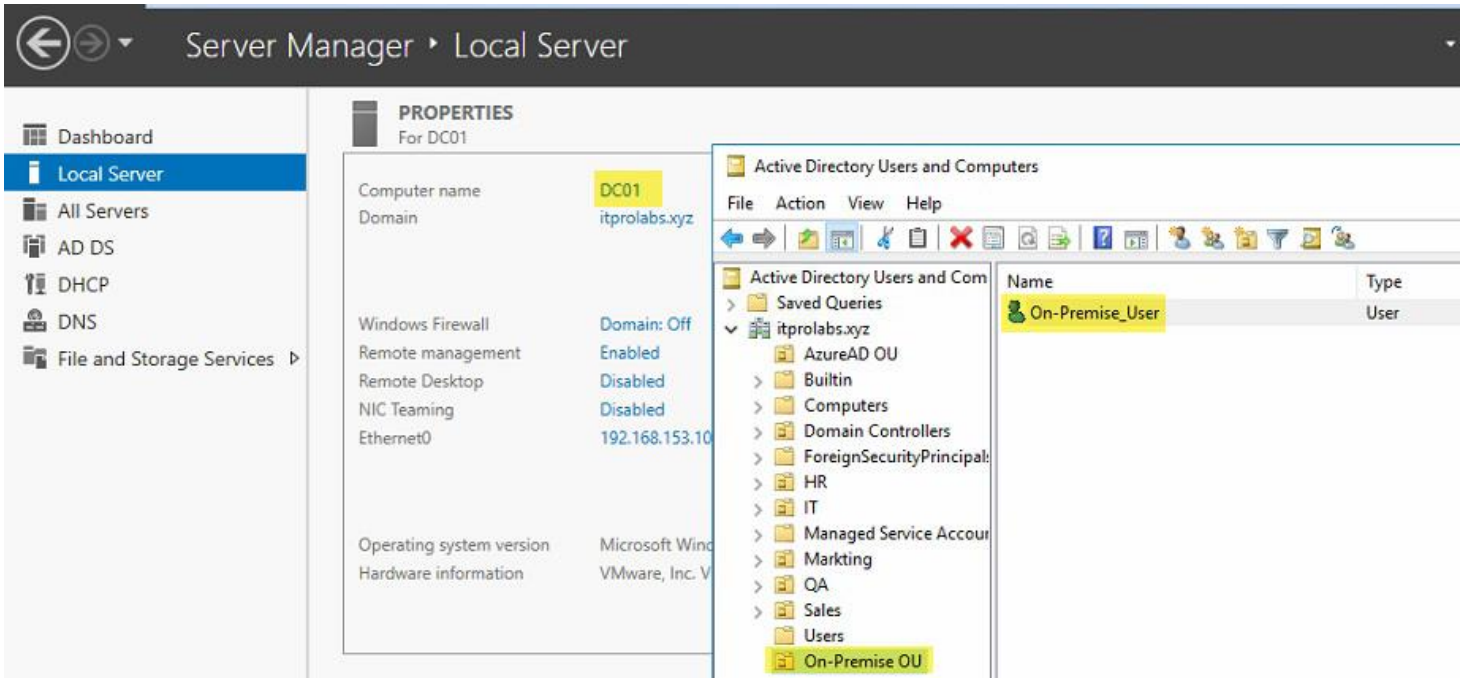
To force clients to authenticate or use your new server as GC or LDAP, just increase Azure VM weight or decrease weight for On-Perm server as explained below.



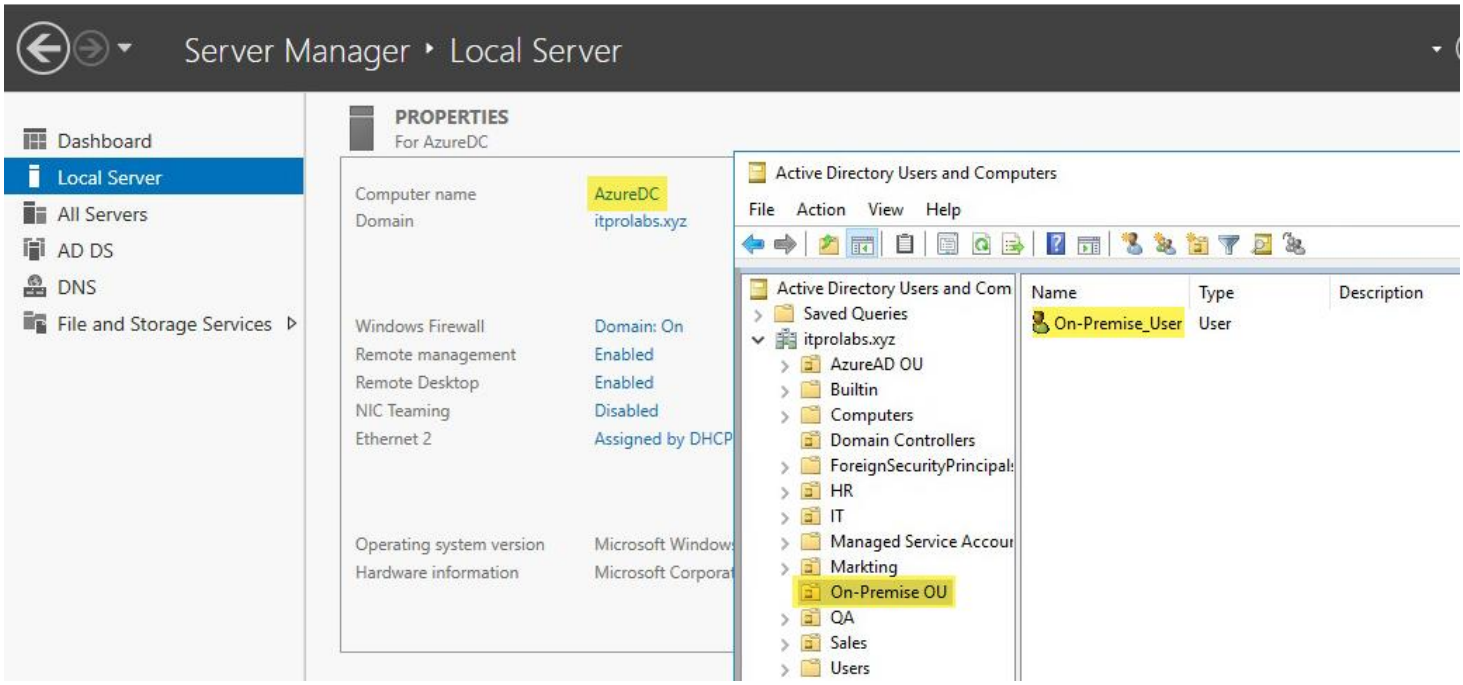
Testing

Test two side active directory replications

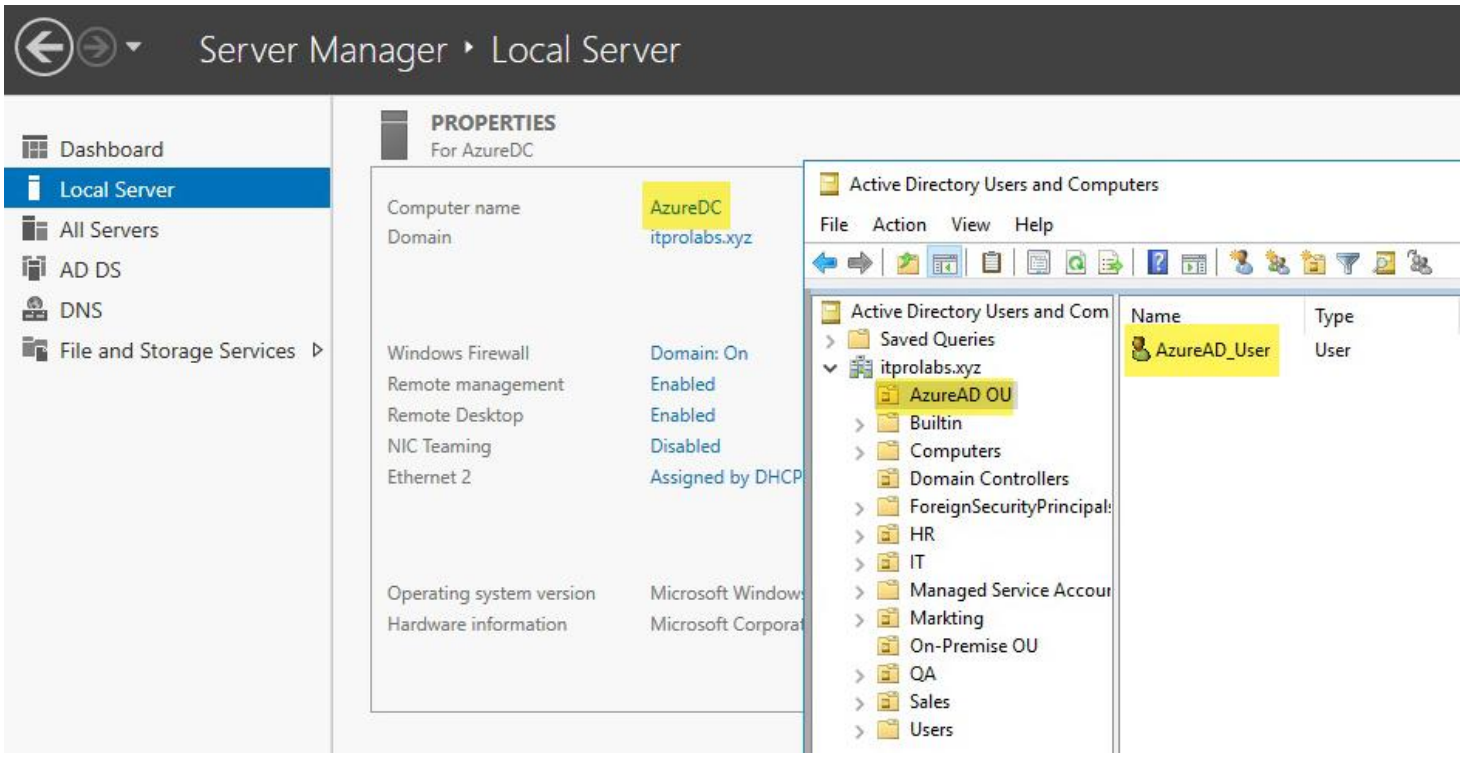
1. Create OU On-Perm and create test user with in and check replication on VM on Azure



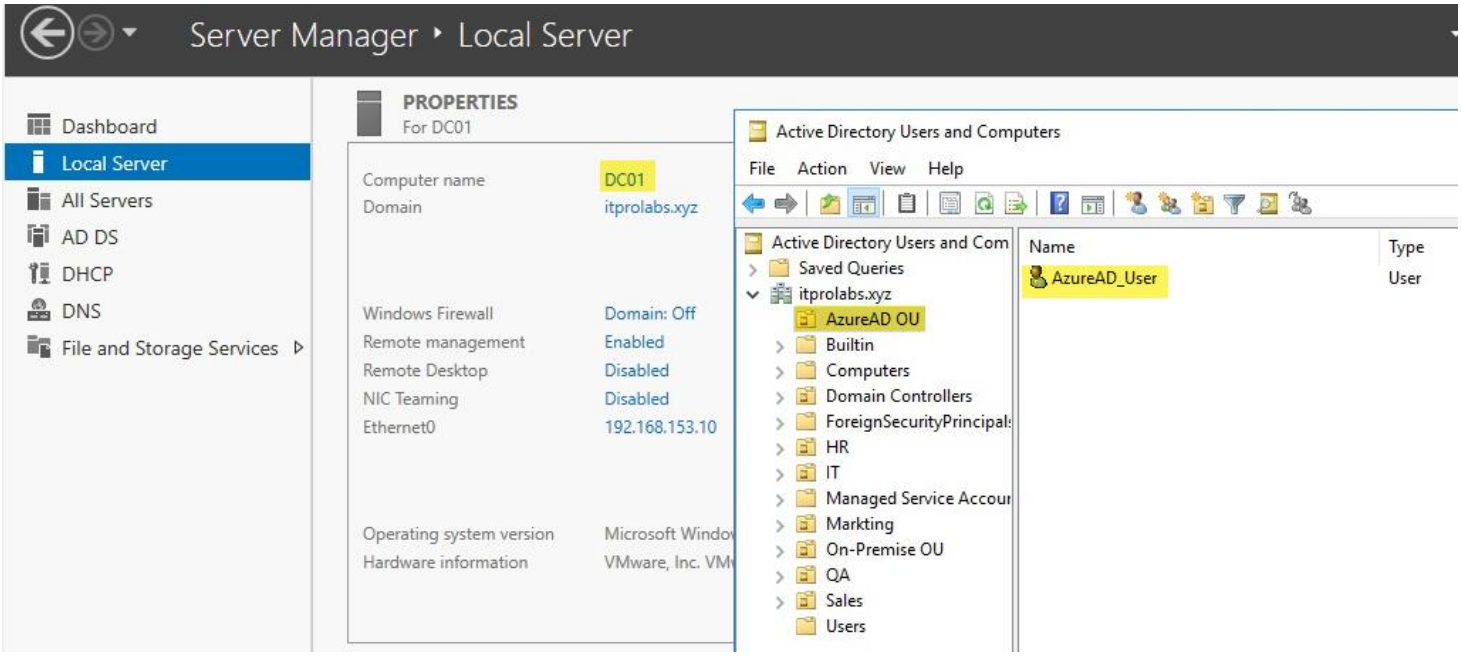
In the figure below the created OU with user replicated to VM on Azure



2. Create OU on Azure and create test user within and check replication On-Perm

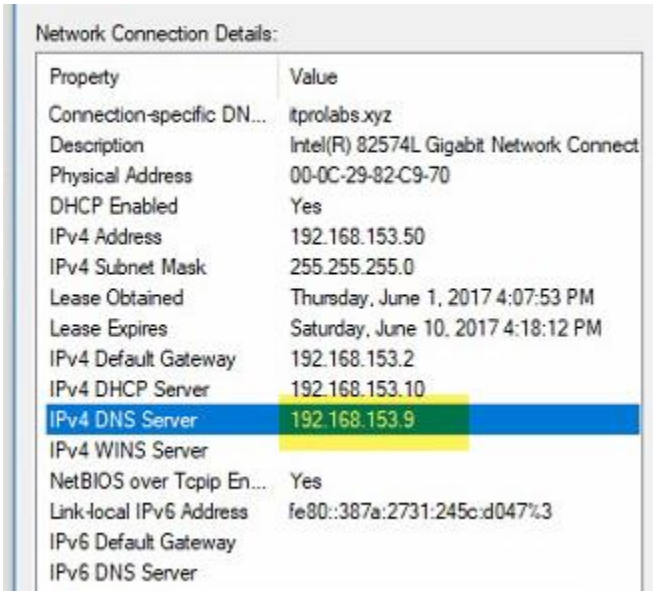


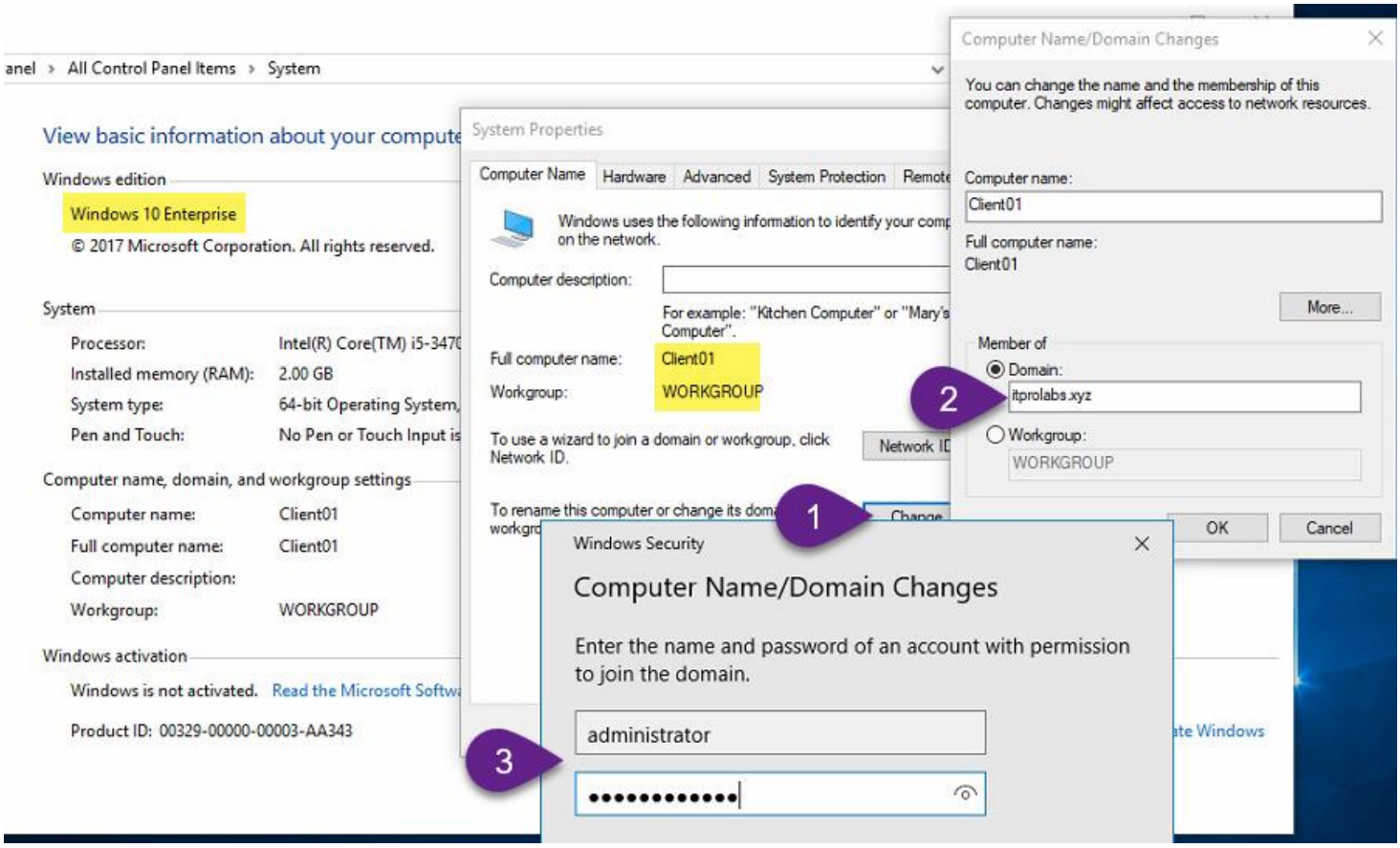
In the figure below the created OU with user replicated to On-Perm server

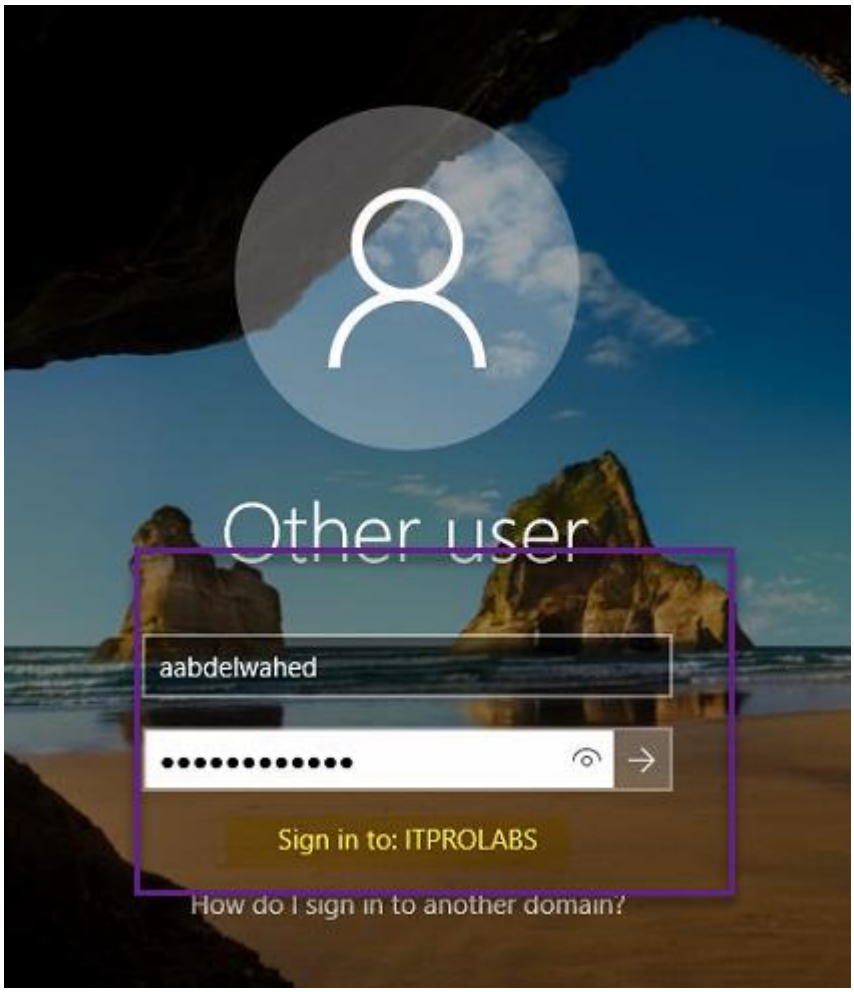


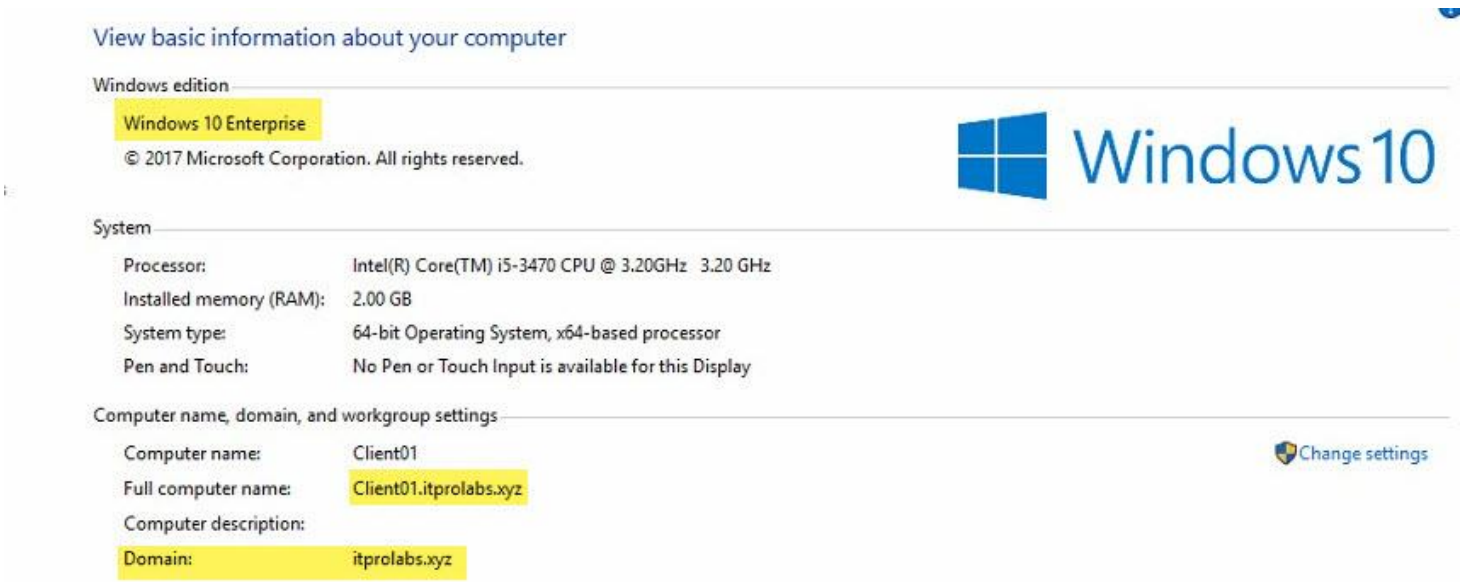
Join On-Premise Windows 10 Client to domain through DC on Azure

Configure windows 10 Client to obtain IP address automatic from DHCP server which distribute Windows Server 2016 VM on Azure as DNS server (192.168.153.9), also we force users early in this lab to authenticate from VM on Azure.






Other user
aabdelwahed
Sign in to: ITPROLABS
How do I sign in to another domain?


View basic information about your computer
Windows edition
Windows 10 Enterprise
© 2017 Microsoft Corporation. All rights reserved.
Windows 10
System
Processor: Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz 3.20 GHz
Installed memory (RAM): 2.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings
Computer name: Client01
Full computer name: Client01.itprolabs.xyz
Computer description:
Domain: itprolabs.xyz
Change settings

Extend On-Premises Windows Server Active Directory to Azure VM

Testing internet connectivity with ITPROLABS.XYZ DNS on Azure

From VM on Azure we use local DNS Server that related to our itprolabs.xyz domain