

# Ethical Hacking Lessons — Building Free Active Directory Lab in Azure

Kamran Bilgrami

K

21 min read

Jan 6, 2020



## Motivation

The majority of IT experts concur that Active Directory is the dominant approach for managing the Windows domain networks. This is why adversaries get attracted to discover and exploit vulnerabilities within the Active Directory echo system. In order to defend against those types of attacks, there is a need for practice grounds where Pen Testers, Security Researchers and Ethical hackers can practice offensive and defensive methodologies.

This article is inspired by [TheCyberMentor](#)'s [How to Build an Active Directory Hacking Lab](#) video where he builds a local Active Directory lab for ethical hacking purposes. My personal preference is to use a cloud-based infrastructure wherever possible. I, therefore, decided to look into building a similar low-cost lab (free in this case) in Azure while following his videos. This article basically follows steps from [How to Build an Active Directory Hacking Lab](#) video but in a Windows Azure environment.

# First Things First

It is important to note that some of the practices used during the creation of this lab are intentionally weak to better just to describe the possible attack vectors. You should do the necessary research before using any practices described here into your production or any other network(s).

## Microsoft Azure

Its highly unlikely that you have not heard about the Microsoft Cloud platform — Azure. This article by no means is an intro to Azure. There are plenty of resources available if you want to learn it.

Microsoft offers a [free Azure trial](#) that includes free access to popular Azure products for 12 months, \$200 credit to spend for the first 30 days of sign up, and access to more than 25 products that are always free.

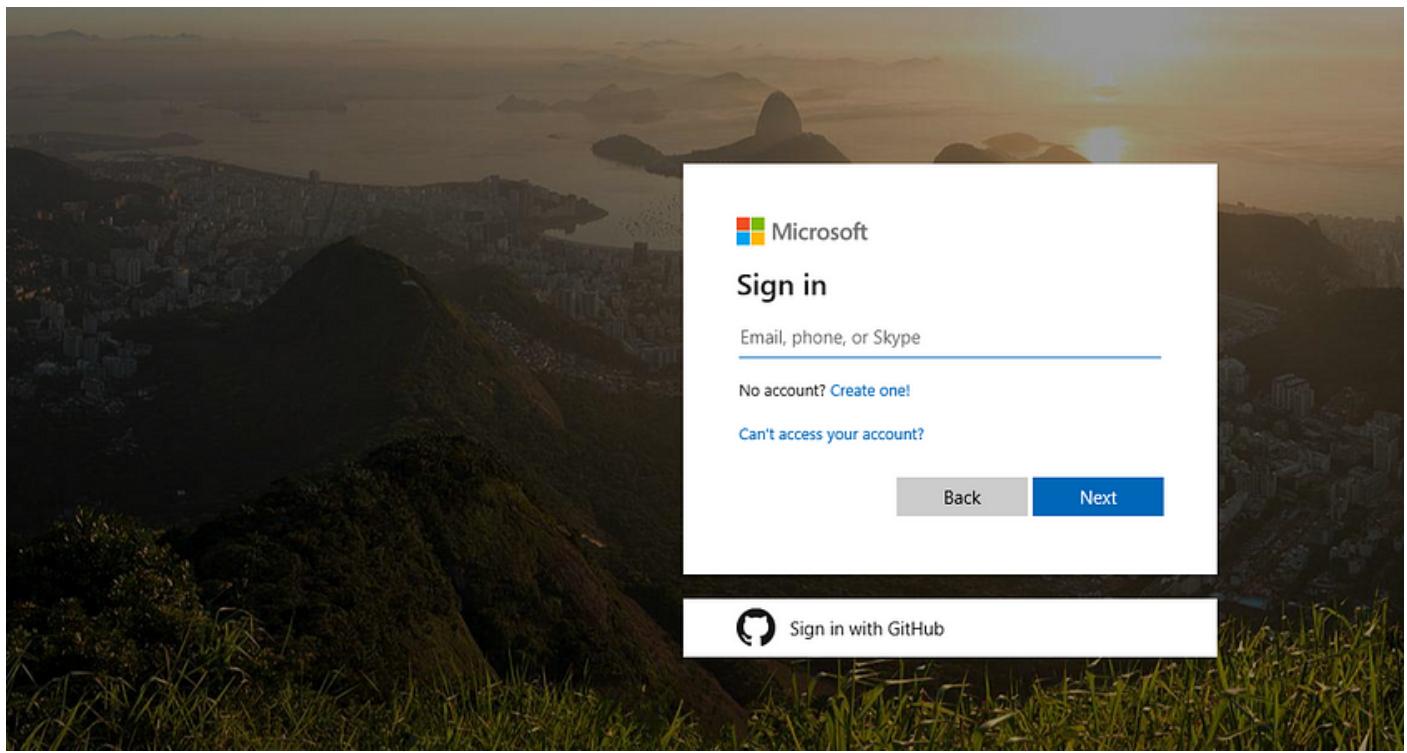
The screenshot shows two parts of the Azure experience. The top part is a landing page with a dark background, featuring a large green button labeled "Start free >" and a smaller blue button labeled "Or buy now >". The text "Create your Azure free account today" and "Get started with 12 months of free services" is displayed. The bottom part is a screenshot of the Microsoft Azure (Preview) portal, showing a list of recent resources including "api", "BuildApp", "AI-DemoBot-Sc1", "adventure-vm-2-ip", and "adventure-vm". It also displays various service icons like "Create a resource", "All resources", "Virtual machines", "App Services", etc., and navigation links for "Subscriptions", "Resource groups", "All resources", and "Dashboard".

Let's set up an account to take advantage of these free services and create this Active Directory lab.

## Account Creation

Let's click on the **Start Free** button. If you have an existing Microsoft account, you can log in through the page shown below.

The screenshot shows a Microsoft login page with a dark background. The URL in the address bar is [https://login.microsoftonline.com/common/oauth2/authorize?client\\_id=23523755-3a2b-41ca-9315-f81f3f566a95&response\\_mode=form\\_post&response\\_type=id\\_token+code&scope=openid9](https://login.microsoftonline.com/common/oauth2/authorize?client_id=23523755-3a2b-41ca-9315-f81f3f566a95&response_mode=form_post&response_type=id_token+code&scope=openid9). The page contains standard Microsoft login fields for email and password, along with "Sign in" and "Forgot password?" buttons.



Otherwise, you will have to signup for an account.

## 1 About you

### Country/Region i

Choose the location that matches your billing address. **You cannot change this selection later.** If your country is not listed, the offer is not available in your region. [Learn More](#)

First name

Last name

Email address i

Phone

[Next](#)

## What's included

- ✓ **12 months of free products**  
Get free access to popular products like *virtual machines*, *storage*, and *databases* in your first 30 days, and for 12 months after you upgrade your account to pay-as-you-go pricing.

- ✓ **\$250 credit**  
Use your \$250 credit to experiment with any Azure service in your first 30 days—beyond the free product amounts.

- ✓ **25+ always-free products**  
Take advantage of more than 25 products, including *serverless*, *containers*, and *artificial intelligence*, that are always free. Get these in your first 30 days, and always—once you choose to upgrade.

- ✓ **No automatic charges**  
You won't be charged unless you choose to upgrade. Before the end of your first 30 days, you'll be notified and have the chance to upgrade and start paying only for the resources you use beyond the free amounts.

## 2 Identity verification by phone

## 3 Identity verification by card

## 4 Agreement

Note that the signup process requires to provide user's phone number and credit card information. The credit

card is not charged unless the user decides to upgrade to a service such as [Pay-As-You-Go](#). I found the [FAQ](#) for the free Azure services quite informative and useful.

Let's assume that we have signed up for the free Azure service. Let's proceed with the Active Directory lab setup. In your favorite browser, go to [Azure portal](#) and login to your account.

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and a navigation bar with icons for Home, Dashboard, All services, and Favorites. Below the search bar is a section titled "Azure services" with icons for Create a resource, Virtual machines, App Services, Storage accounts, SQL databases, Azure Database for PostgreSQL, Azure Cosmos DB, Kubernetes services, Function App, and More services. Under "Navigate", there are links for Subscriptions, Resource groups, All resources, and Dashboard. A "Tools" section includes Microsoft Learn, Azure Monitor, Security Center, and Cost Management. "Useful links" provide links to Technical Documentation, Azure Services, Recent Azure Updates, and Azure mobile app download links for the App Store and Google Play.

## Resource Group Creation

Let's start by creating a dedicated Resource Group for all the lab related resources. A [Resource group](#) acts as a container to hold all the related resources for an Azure solution.

Click on Resource Groups under the Left navigation menu as shown below.

This screenshot shows the Microsoft Azure portal with the "Resource groups" option highlighted in the left navigation menu. The main content area displays the "Azure services" dashboard, which includes sections for Create a resource, Virtual machines, App Services, Storage accounts, SQL databases, Azure Database for PostgreSQL, Azure Cosmos DB, Kubernetes services, Function App, and More services. The "Tools" and "Useful links" sections are also visible.

The resource group list is empty. Let's click on the **Create resource group** button as shown below.

This screenshot shows the Microsoft Azure portal with the "Resource groups" page selected. The top navigation bar shows "Home > Resource groups". The main content area displays a table with no records, indicating that there are no existing resource groups. The table has columns for Name, Type, Location, Status, and Last activity. Buttons at the bottom allow for adding new resource groups, editing, refreshing, exporting to CSV, assigning tags, and providing feedback.

Name ↑↓

Subscription ↑↓

Location ↑↓



No resource groups to display

Try changing your filters if you don't see what you're looking for. [Learn more ↗](#)

[Create resource group](#)

You will be presented with a form like the following. Let's name this Resource group as **ADLab**. I chose **Canada Central** as the Region. You can choose whatever region that makes sense for your geography. Then click on the **Review + create** button.

Microsoft Azure Search resources, services, and

Home > Resource groups > Create a resource group

## Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more ↗](#)

**Project details**

Subscription \* ⓘ Free Trial

Resource group \* ⓘ ADLab

**Resource details**

Region \* ⓘ (Canada) Canada Central

[Review + create](#)

[Review + create](#)

< Previous

Next : Tags >

Necessary validation will be performed and its result will be shown. Its a success in our case. Click on the **Create** button to complete the resource group creation process.

The screenshot shows the 'Create a resource group' page in the Microsoft Azure portal. At the top, there's a blue header bar with the Microsoft Azure logo and a navigation menu. Below it, the breadcrumb navigation shows 'Home > Resource groups > Create a resource group'. The main title 'Create a resource group' is centered above a form. A green success message box contains the text 'Validation passed.' with a checkmark icon. Below the message, there are three tabs: 'Basics' (purple), 'Tags' (blue), and 'Review + create' (underlined black). The 'Review + create' tab is currently selected. Under the 'Basics' section, there are three pairs of labels and values: 'Subscription' (Free Trial), 'Resource group' (ADLab), and 'Region' ((Canada) Canada Central).

Subscription	Free Trial
Resource group	ADLab
Region	(Canada) Canada Central



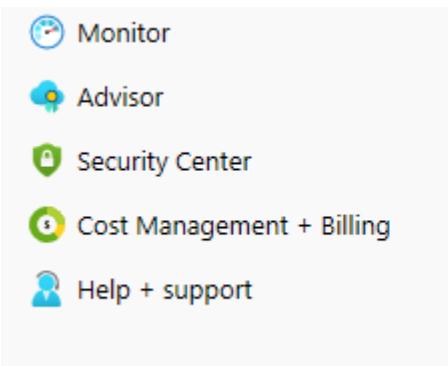
The newly created Resource group now shows up in the list.

Name	Subscription	Location
ADLab	Subscription == all	Canada Central

## Virtual Network Creation

The next step is to create a [Virtual Network](#) that will enable Azure resources (such as Virtual Machines) to securely communicate within the network or outside networks. In order to do that, click on the **Virtual networks** in the navigation menu.

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- Quickstart Center
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks**
- Azure Active Directory



Next, click on the **Create virtual network** button.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar has 'Microsoft Azure' and a search bar. Below it, the breadcrumb navigation shows 'Home > Virtual networks'. The main area is titled 'Virtual networks' with a 'Default Directory' link. There are buttons for '+ Add', 'Edit columns', 'Refresh', 'Export to CSV', 'Assign tags', 'Feedback', and 'Leave preview'. A filter bar allows filtering by 'Filter by name...', 'Subscription', 'Resource group', 'Location', and 'Add filter'. Below the filters, it says 'Showing 0 to 0 of 0 records.' and there are sorting options for 'Name', 'Resource group', 'Location', and 'Subscription'. In the center, there's a large placeholder icon with three dots and arrows. Below the icon, it says 'No virtual networks to display' and provides instructions: 'Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute. [Learn more](#)'. At the bottom right of this section, the 'Create virtual network' button is highlighted with a red box.

Fill in the fields related to Creating that virtual Network. I used **ADLabNet** as the name of the virtual network. Further, I also used **10.0.1.0/24** as the address space and subnet address range. Make sure, you select the resource group **ADLab** that we created earlier. For the rest of the fields, I just used default values. Finally, click on the **Create** button.

The screenshot shows the 'Create virtual network' dialog box. At the top, it says 'Create virtual network' with a close button. The form contains the following fields:

- Name \***: ADLabNet (highlighted with a red box)
- Address space \***: 10.0.1.0/24 (highlighted with a red box)
  - Subtext: 10.0.1.0 - 10.0.1.255 (256 addresses)
- Add an IPv6 address space ⓘ
- Subscription \***: Free Trial
- Resource group \***: ADLab (highlighted with a red box)

**Create new**

**Location \***

**Subnet**  
**Name \***

**Address range \* ⓘ**  
   
(0 addresses)

**DDoS protection ⓘ**  
 Basic  Standard

**Service endpoints ⓘ**  
 Disabled  Enabled

**Firewall ⓘ**  
 Disabled  Enabled

**Create** **Automation options**

That's it with Virtual Network creation. It should show up in the list as shown below.

Virtual networks			
Showing 1 to 1 of 1 records.			
<input type="checkbox"/> Name ↑	Resource group ↑	Location ↑	Subscription ↑
<input type="checkbox"/> ADLabNet	ADLab	Canada Central	Free Trial

## Domain Controller

Creation of Domain Controller (DC) machine consists of few steps including creation of Virtual machine, making necessary configuring changes, promoting machine as DC, etc. Let's go over all these steps one by one.

## Virtual Machine Creation

Let's start with the creation of the first Virtual Machine. This will be our Active Directory Domain Controller. I am going to use a Windows Server 2019 image for it. First of all, click on the **Virtual machines** menu item.

☰

- + Create a resource
- Home
- Dashboard
- All services
- ★ FAVORITES
- All resources
- Resource groups
- Quickstart Center
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines**
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

No virtual machines yet on this list. Just click on the **Create virtual machine** button.

Microsoft Azure

Home > Virtual machines

Virtual machines

Default Directory

+ Add Reservations Edit columns Refresh Assign tags Start Restart Stop Delete Services

Subscriptions: Free Trial

Filter by name... All resource groups All types All locations All tags No grouping

0 items

Name ↑	Type ↑	Status	Resource group ↑	Location ↑	Source	Maintenance status	Subscription
--------	--------	--------	------------------	------------	--------	--------------------	--------------

No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

Learn more about Windows virtual machines | Learn more about Linux virtual machines

Create virtual machine

You will be presented with the following page. Make sure you select the **ADLab** resource group created earlier. Let's name the virtual machine **HYDRA-DC**. Click on the Browse all public and private images link to select the right image for our VM.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The 'Basics' tab is selected. Key fields and their values are:

- Subscription:** Free Trial
- Resource group:** ADLab (selected from a dropdown menu)
- Virtual machine name:** HYDRA-DC
- Region:** (Canada) Canada Central
- Availability options:** No infrastructure redundancy required
- Image:** Ubuntu Server 18.04 LTS (with a red box around the 'Browse all public and private images' link)
- Azure Spot instance:** No (radio button selected)
- Size:** Standard D2s v3 (2 vcpus, 8 GiB memory (\$105.71/month))
- Administrator account:** Authentication type: SSH public key (radio button selected)

At the bottom, there are navigation buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Disks >'.

Click on the **Compute** item under the **Marketplace** tab and choose the **Windows Server 2019 Datacenter** image.

Select an image

Marketplace My Items

Analytics

Blockchain

Compute

Containers

Databases

Developer Tools

DevOps

Identity

Integration

Internet of Things

IT &amp; Management Tools

Media

Mixed Reality

Networking

Security

Software as a Service (SaaS)

Storage

Web



Windows Server 2019 Datacenter with Containers

Microsoft

Windows Server 2019 helps you modernize your applications and infrastructure, adds additional layers of security and bridges on-premises and Azure.



Windows Server 2019 Datacenter with Containers

Microsoft

Windows Server 2019 helps you modernize your applications and infrastructure, adds additional layers of security and bridges on-premises and Azure.



Windows Server 2019 Datacenter Server Core with Containers

Microsoft

Windows Server 2019 helps you modernize your applications and infrastructure, adds additional layers of security and bridges on-premises and Azure.



Windows Server 2019 Datacenter Server Core with Containers

Microsoft

Windows Server 2019 helps you modernize your applications and infrastructure, adds additional layers of security and bridges on-premises and Azure.



Windows Server 2019 Datacenter Server Core

Microsoft

Windows Server 2019 helps you modernize your applications and infrastructure, adds additional layers of security and bridges on-premises and Azure.



Windows Server 2019 Datacenter Server Core

Microsoft

Windows Server 2019 helps you modernize your applications and infrastructure, adds additional layers of security and bridges on-premises and Azure.



Windows Server 2019 Datacenter (zh-cn)

Microsoft

Windows Server 2019 helps you modernize your applications and infrastructure, adds additional layers of security and bridges on-premises and Azure.



Windows Server 2019 Datacenter (zh-cn)

Microsoft

Windows Server 2019 helps you modernize your applications and infrastructure, adds additional layers of security and bridges on-premises and Azure.



Windows Server 2019 Datacenter

Microsoft

Windows Server 2019 helps you modernize your applications and infrastructure, adds additional layers of security and bridges on-premises and Azure.

Now that the appropriate image is selected, from the **Create Virtual Machine** page, click on the **Change size** link. I am going to use the **B1ms** for this machine as shown below.

### Select a VM size

Browse available virtual machine sizes and their features

 Search by VM size...[Clear all filters](#)Size : **Small (0-6)**Generation : **2 selected**Family : **General purpose**Premium disk : **Supported**[+ Add filter](#)

Showing 11 of 167 VM sizes. | Subscription: Visual Studio Enterprise – MPN | Region: Central US | Current size: Standard\_DS1\_v2

VM Si...↑↓	Offering ↑↓	Family	↑↓	vCP...↑↓	RAM (...)↑↓	Data disks↑↓	Max IOPS ↑↓	Temporary stor...↑↓	Premium disk s...↑↓	Cost/month (es...)↑↓
B1ls	Standard	General purpose	1	0.5	2	160	4		Yes	\$5.94
<b>B1ms</b>	Standard	General purpose	1	2	2	640	4		Yes	\$23.81
B1s	Standard	General purpose	1	1	2	320	4		Yes	\$11.90
B2ms	Standard	General purpose	2	8	4	1920	16		Yes	\$95.04
B2s	Standard	General purpose	2	4	4	1280	8		Yes	\$47.52
B4ms	Standard	General purpose	4	16	8	2880	32		Yes	\$190.46
D2s_v3	Standard	General purpose	2	8	4	3200	16		Yes	\$104.76
D4s_v3	Standard	General purpose	4	16	8	6400	32		Yes	\$209.51
<b>DS1_v2</b>	Standard	General purpose	1	3.5	4	3200	7		Yes	\$69.52
DS2_v2	Standard	General purpose	2	7	8	6400	14		Yes	\$139.04

[Select](#)

Prices presented are estimates in your local currency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. [View Azure pricing calculator](#).

Now, we need to create an Administrator account. I used **kamran** as the username and **Password1234** as the password. Definitely not a strong password for an administrator account. Click on **Next: Disks** button.

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure. The 'Subscription' dropdown is set to 'Free Trial'. The 'Resource group' dropdown shows 'ADLab' selected, with 'Create new' as an option. Under 'Instance details', the 'Virtual machine name' is 'HYDRA-DC', 'Region' is '(Canada) Canada Central', 'Availability options' is 'No infrastructure redundancy required', and 'Image' is 'Windows Server 2019 Datacenter'. The 'Azure Spot instance' option is set to 'No'. In the 'Size' section, 'Standard B1ms' is selected, which includes '1 vcpu, 2 GiB memory (\$21.90/month)'. The 'Administrator account' section shows 'Username' as 'kamran' and 'Password' as a masked string. The 'Review + create' and 'Next : Disks >' buttons are at the bottom.

I chose **Standard HDD** OS disk type here. You can certainly go with the Premium SSD also but for the purpose of this lab, the Standard HDD is good enough. Click on **Next: Networking** button.

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure, on the 'Disks' tab. It shows the 'Basics' tab is selected. The 'Disk options' section has 'OS disk type' set to 'Standard HDD'. A note below says: 'The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Standard SSD disks are better for the'. The 'Networking' tab is visible at the top.

High IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Enable Ultra Disk compatibility ⓘ  Yes  No

Ultra Disk compatibility is not available for this VM size and location.

### Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

Create and attach a new disk    Attach an existing disk

Advanced

Review + create    < Previous    Next : Networking >

In the Networking tab, make sure the Virtual network is set to **ADLabNet** that we created earlier. For the rest of the steps, we just accept all the defaults and click on **Review + create** button.

Microsoft Azure    Search resources, services, and docs (G+/)

Home > Virtual machines > Create a virtual machine

## Create a virtual machine

Basics   Disks   **Networking**   Management   Advanced   Tags   Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.  
[Learn more](#)

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ    
[Create new](#)

Subnet \* ⓘ    
[Manage subnet configuration](#)

Public IP ⓘ    
[Create new](#)

NIC network security group ⓘ  None  Basic  Advanced

Public inbound ports \* ⓘ  None  Allow selected ports

Select inbound ports \*

RDP (3389)



**⚠** This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking ⓘ

On  Off

The selected VM size does not support accelerated networking.

#### Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution?

Yes  No

[Review + create](#)

[< Previous](#)

[Next : Management >](#)

Once getting the successful validation, click on the **Create** button to create the Virtual Machine.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Virtual machines > Create a virtual machine

### Create a virtual machine

**Validation passed**

Basics Disks Networking Management Advanced Tags [Review + create](#)

**PRODUCT DETAILS**

Standard B2s by Microsoft **Subscription credits apply ⓘ**  
**0.0696 CAD/hr** [Pricing for other VM sizes](#)

**TERMS**

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

**⚠ You have set RDP port(s) open to the internet.** This is only recommended for testing. If you want to change this setting, go back to Basics tab.

#### Basics

Subscription	Free Trial
Resource group	ADLab
Virtual machine name	HYDRA-DC
Region	(Canada) Canada Central
Availability options	No infrastructure redundancy required
Username	kamran
Public inbound ports	RDP
Already have a Windows Server license?	No
Azure Spot	No

## Disks

OS disk type

Standard HDD

**Create**

< Previous

Next >

Download a template for automation

It will take a few minutes but if everything goes well, you should see a message stating that deployment is completed as shown below. You can click on the **Go to resource** button to navigate to the page for this newly created Virtual machine.

The screenshot shows the Microsoft Azure portal. In the top left, it says "Microsoft Azure". Below that, "Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20200102173317 - Overview". On the left, there's a sidebar with "Overview", "Inputs", "Outputs", and "Template". The main area has a heading "Your deployment is complete" with a green checkmark. It shows deployment details: Deployment name: CreateVm-MicrosoftWindowsServer.WindowsS..., Start time: 1/2/2020 6:22:07 PM, Subscription: Free Trial, Resource group: ADLab. Below that are sections for "Deployment details" (with a "Download" link) and "Next steps" (with links for "Setup auto-shutdown", "Monitor VM health, performance and network dependencies", and "Run a script inside the virtual machine"). At the bottom is a blue "Go to resource" button, which is highlighted with a red box.

You can click on the **Connect** button to see various options for connecting to this machine.

The screenshot shows the Microsoft Azure portal for the HYDRA-DC virtual machine. In the top left, it says "Microsoft Azure". Below that, "Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20200102173317 - Overview > HYDRA-DC". On the left, there's a sidebar with "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Settings" (Networking, Disks, Size, Security, Extensions), "Continuous delivery (Preview)", "Availability + scaling", "Configuration", "Identity", "Properties", "Locks", "Export template", "Operations" (Bastion, Auto-shutdown), and "Auto-shutdown". The main area has a "Connect" button highlighted with a red box. To the right, there are several monitoring charts: "CPU (average)" (showing usage from 5:30 PM to 6:15 PM), "Network (total)" (showing traffic from 5:30 PM to 6:15 PM with values 130.65 MB and 700.37 KB), "Disk bytes (total)" (showing disk usage from 5:30 PM to 6:15 PM), and "Disk operations/sec (average)" (showing disk operations from 5:30 PM to 6:15 PM).

Let's choose **RDP** and download the appropriate file for connecting to the VM.

The screenshot shows a "Connect to virtual machine" dialog for the HYDRA-DC VM. At the top, it says "Connect to virtual machine" and "HYDRA-DC". Below that is a yellow bar with a warning icon and the text "To improve security, enable just-in-time access on this VM. →". At the bottom, there are three buttons: "RDP" (which is highlighted with a red box), "SSH", and "BASTION".

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

IP address \*

Port number \*

[Download RDP File](#)

Having trouble connecting to this VM?

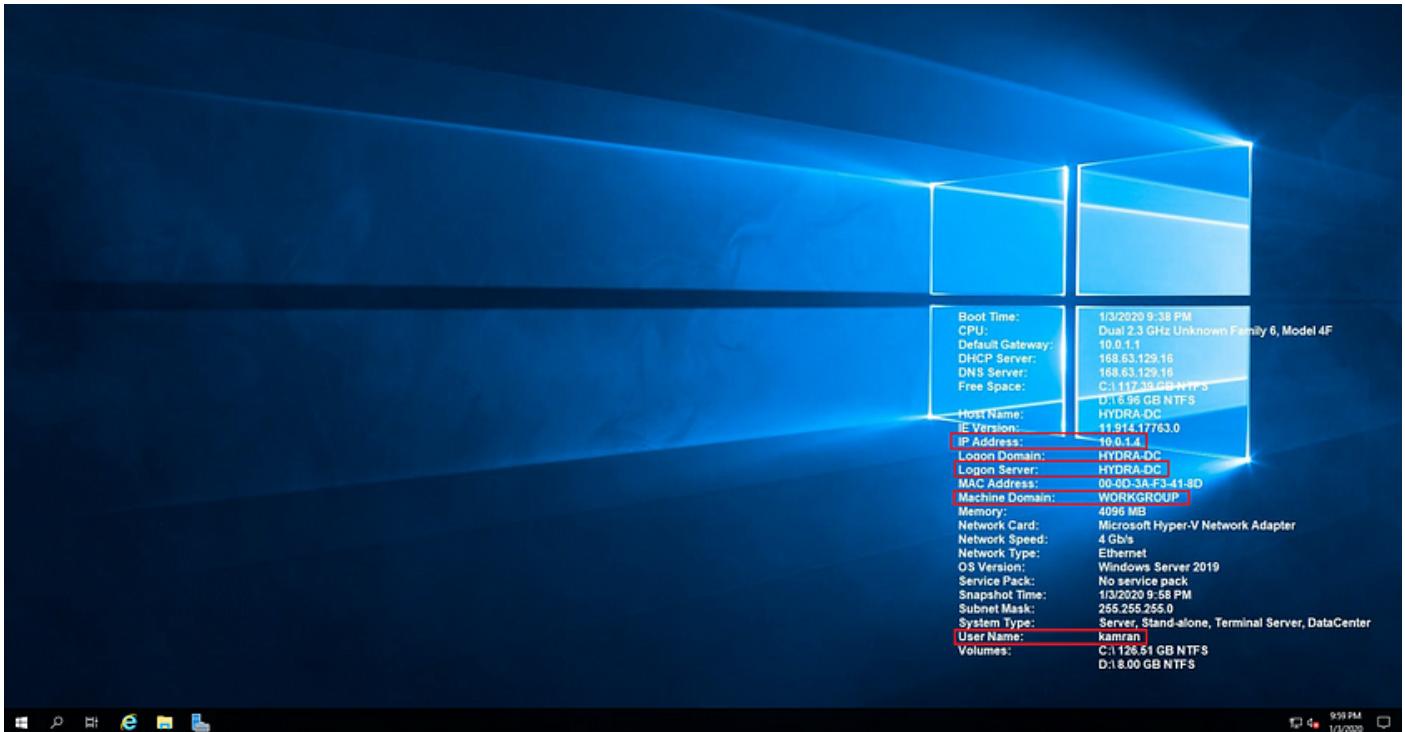
- [Diagnose and solve problems](#)
- [Troubleshoot connection](#)
- [Serial console](#)
- [Reset password](#)

You should be able to login using the username **kamran** and password **Password1234** that we set up earlier in the process. After RDP into this box, you will see a Desktop like the following.



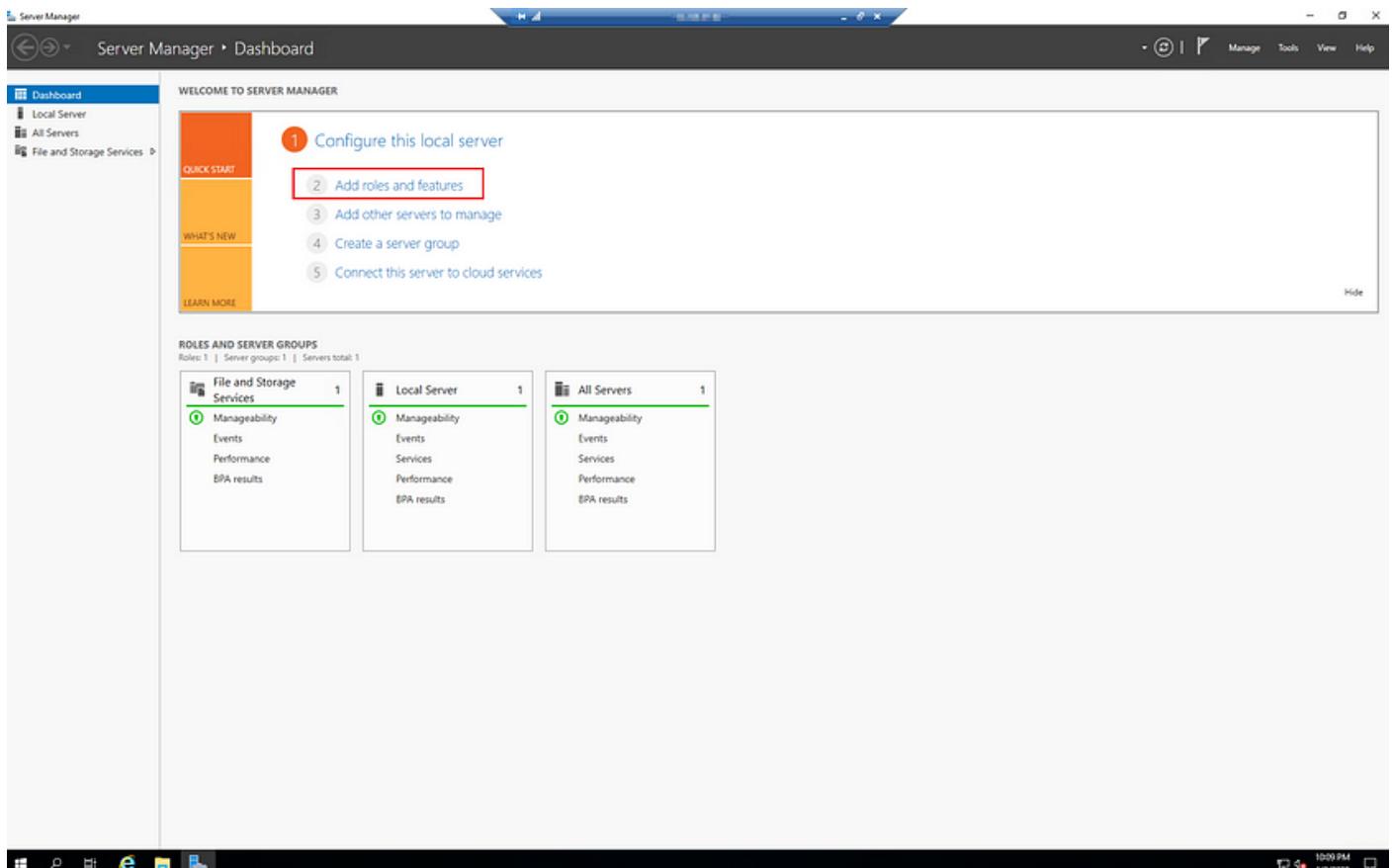
I like to have a little bit more information about the machine on the desktop. This is even more important when you are working against multiple computers. I typically use [BgInfo](#) utility that setups your desktop background with an image with some useful information such as IP address, machine name/domain, Username, etc. as shown below.



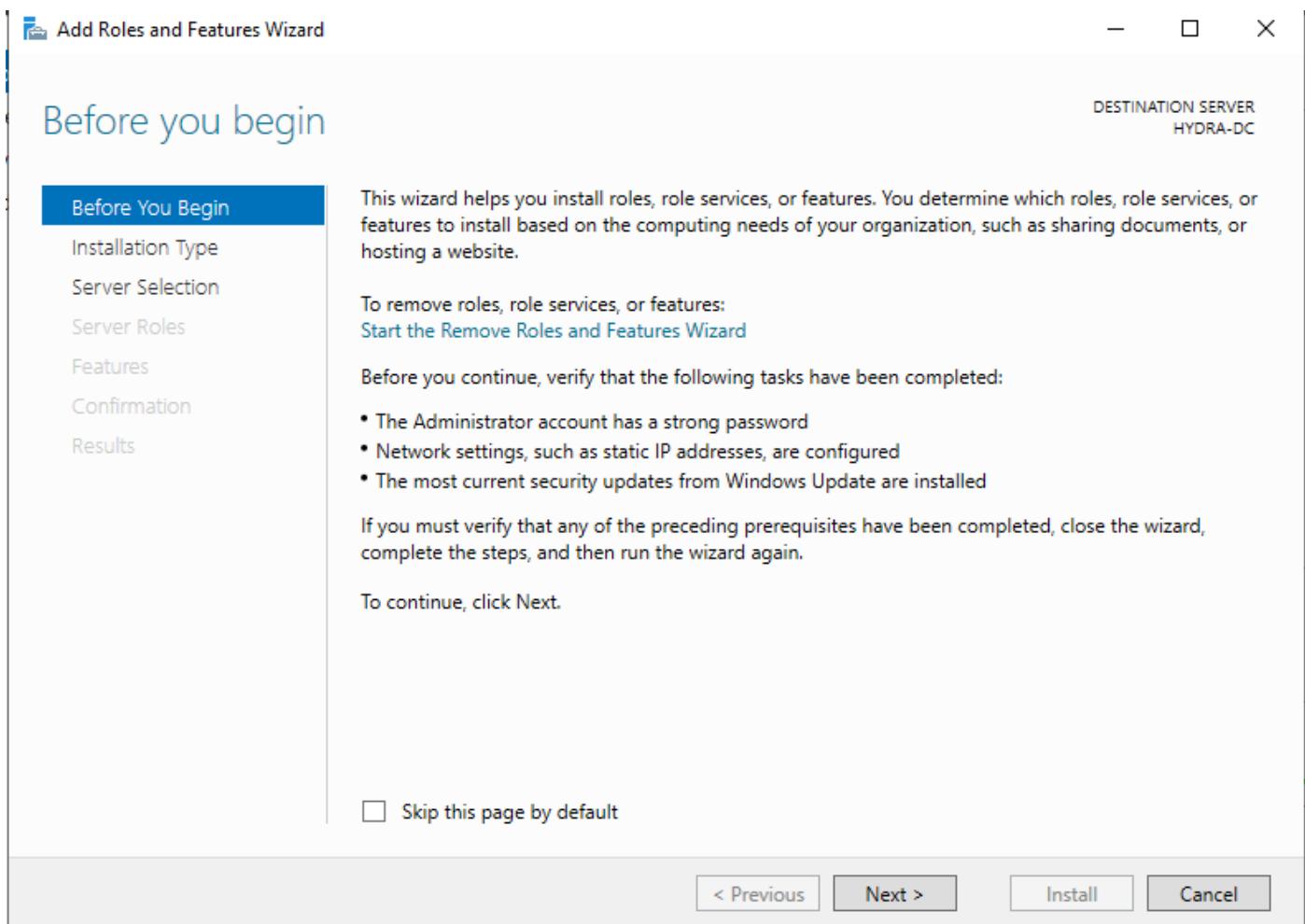


## Configuring Services

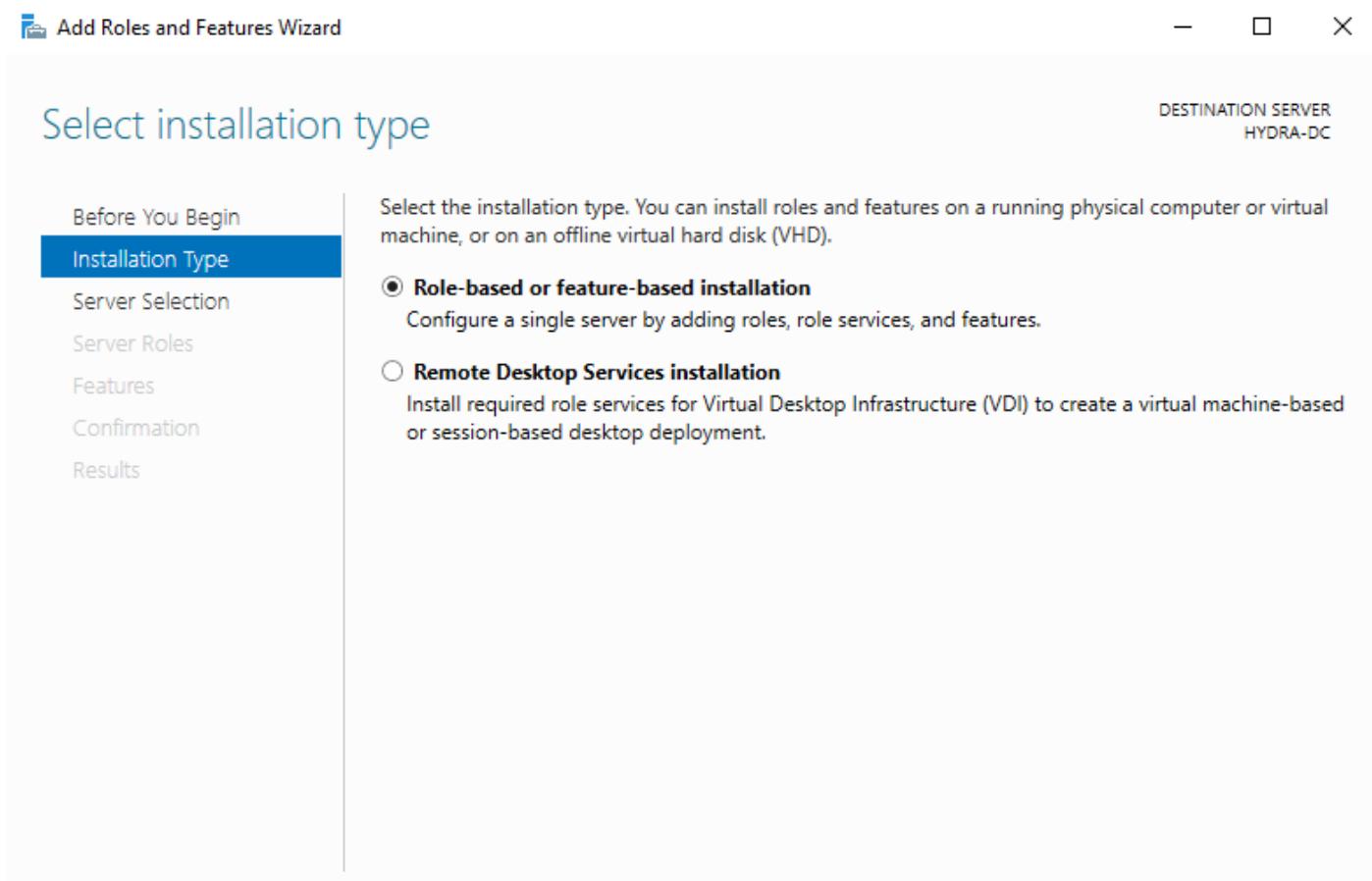
Now that we are connected to the machine, its time to configure it as a Domain Controller. Let's launch the Server Manager and click on **Add roles and features** option.



This will start the **Add Roles and Features Wizard**. The first tab **Before you begin** simply provides some information about the wizard and a few suggestions about tasks that should be completed before continuing with this wizard. Make sure you read and understand it and then click Next.



On the next tab **Installation Type**, we just choose **Role-based or feature-based installation** option and click Next.



On the next tab **Server Selection**, we can just choose **Next**.

Add Roles and Features Wizard

DESTINATION SERVER  
HYDRA-DC

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

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

(●) Select a server from the server pool  
(○) Select a virtual hard disk

**Server Pool**

Name	IP Address	Operating System
HYDRA-DC	10.0.1.4	Microsoft Windows Server 2019 Datacenter

Filter: [ ]

1 Computer(s) found

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

< Previous Next > Install Cancel

On the **Server Roles** tab, check the “Active Directory Domain Service” checkbox.

Add Roles and Features Wizard

DESTINATION SERVER  
HYDRA-DC

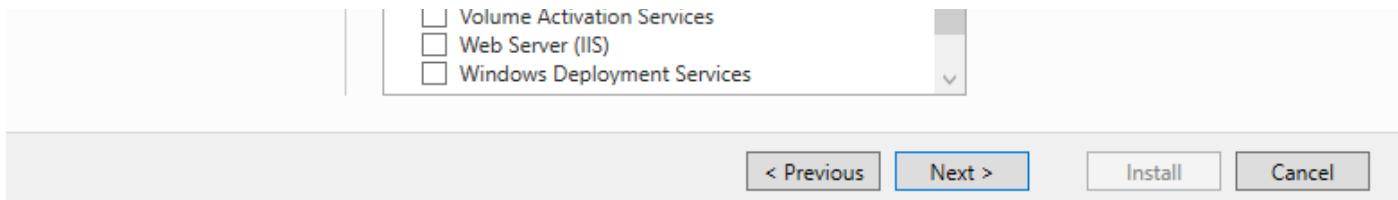
Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
Confirmation  
Results

Select one or more roles to install on the selected server.

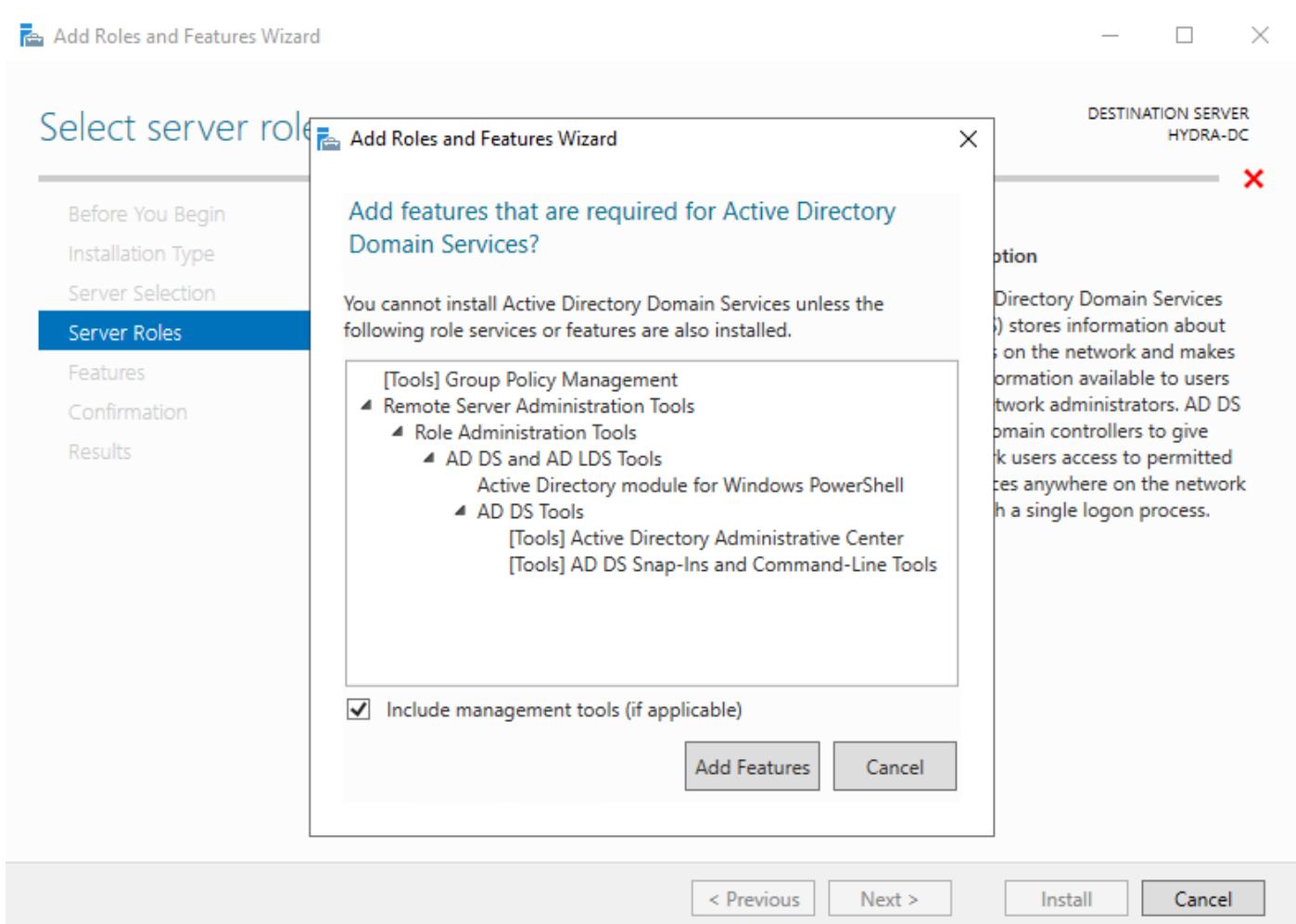
**Roles**

<input type="checkbox"/> Active Directory Certificate Services	<b>Active Directory Domain Services</b> <input checked="" type="checkbox"/> <input type="checkbox"/> Active Directory Federation Services <input type="checkbox"/> Active Directory Lightweight Directory Services <input type="checkbox"/> Active Directory Rights Management Services <input type="checkbox"/> Device Health Attestation <input type="checkbox"/> DHCP Server <input type="checkbox"/> DNS Server <input type="checkbox"/> Fax Server <input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed) <input type="checkbox"/> Host Guardian Service <input type="checkbox"/> Hyper-V <input type="checkbox"/> Network Controller <input type="checkbox"/> Network Policy and Access Services <input type="checkbox"/> Print and Document Services <input type="checkbox"/> Remote Access <input type="checkbox"/> Remote Desktop Services	<b>Description</b> Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
--	--	--

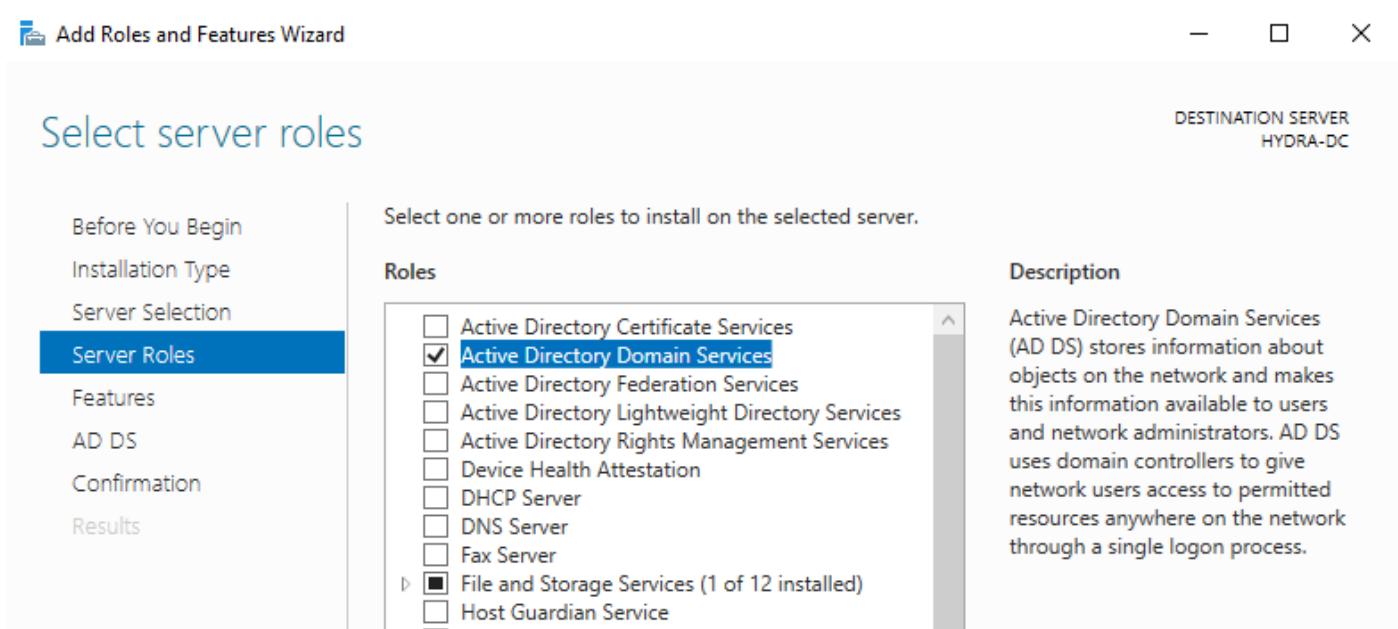
< Previous Next > Install Cancel

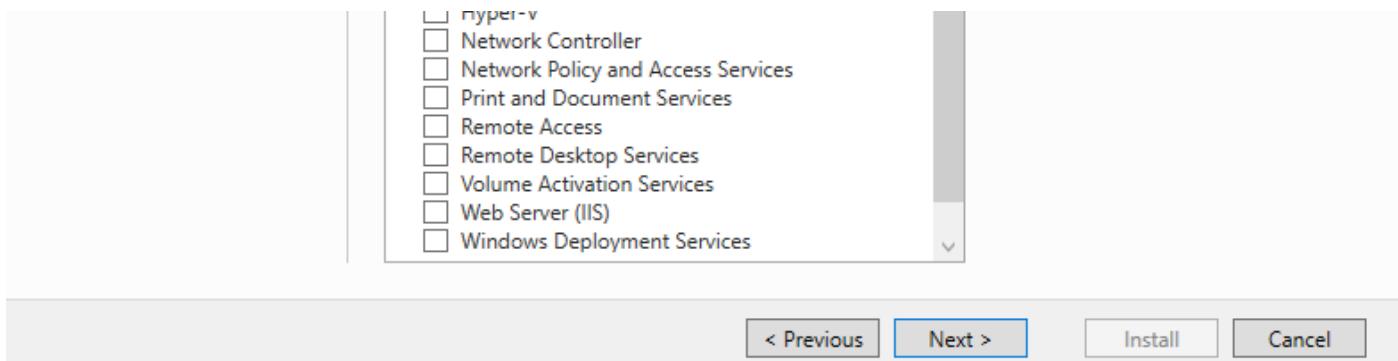


This will bring up following dialog where you simply confirm that you are ok installing other features that Active Directory Domain Services (ADDS) will have to install as well. Click on **Add Features** button.

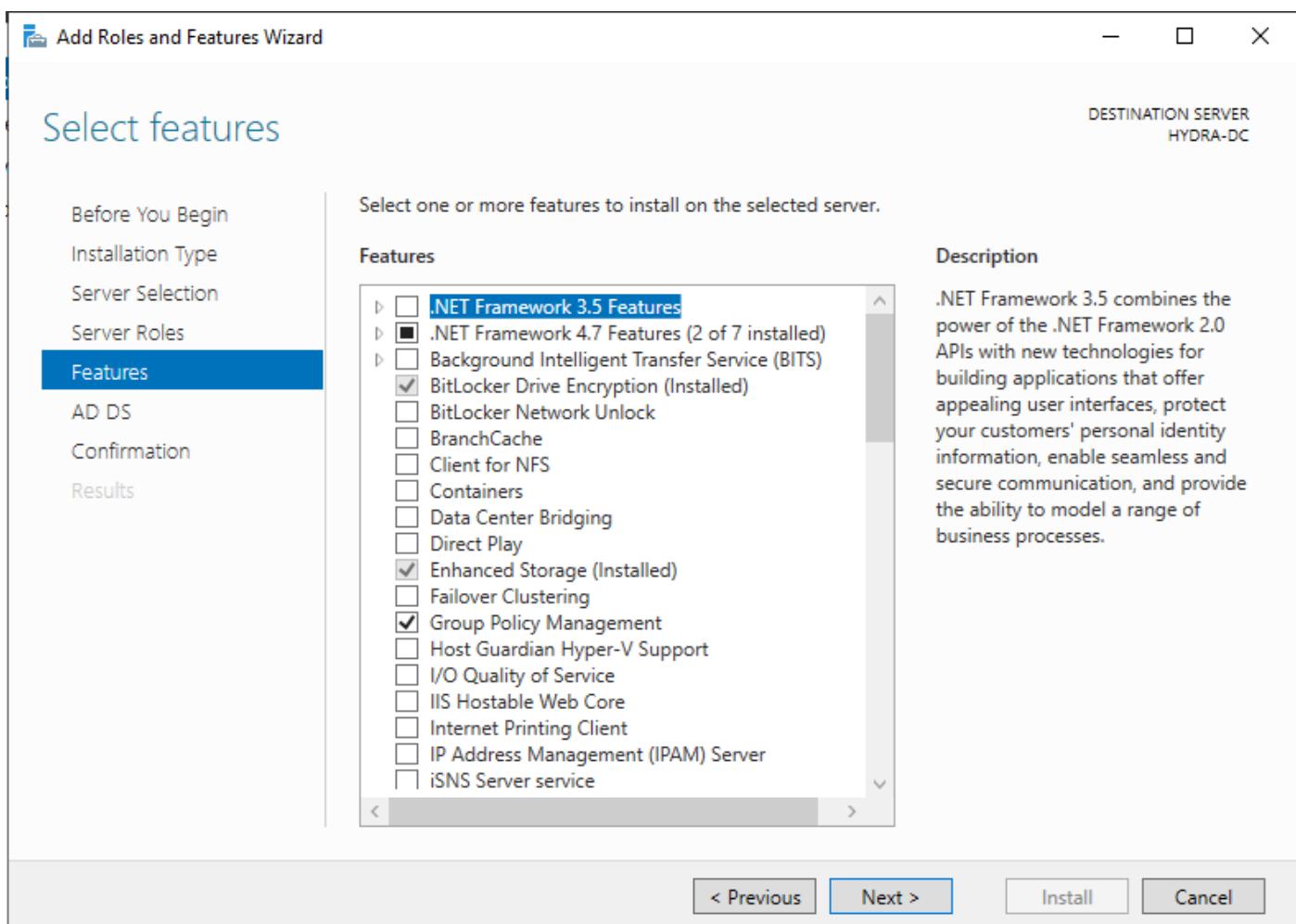


Click Next.

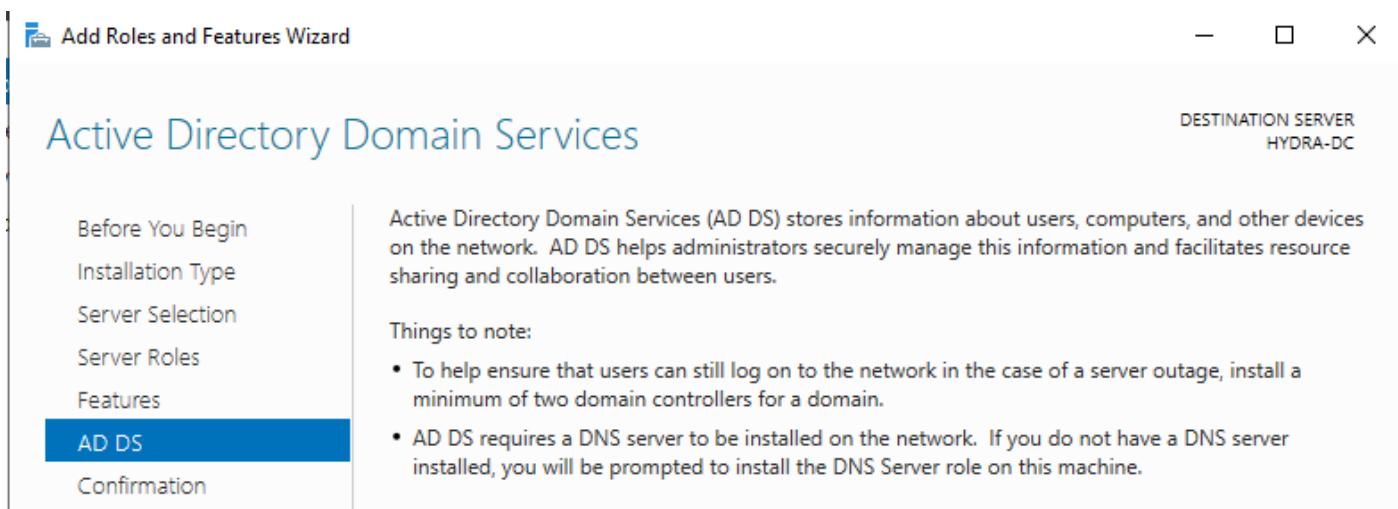




You can click Next on the **Features** tab.



You can click Next on the **AD DS** tab.



RESULTS



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](#)

< Previous Next > Install Cancel

Click **Install** on the **Confirmation** tab.

Add Roles and Features Wizard

DESTINATION SERVER  
HYDRA-DC

## Confirm installation selections

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

< Previous Next > Install Cancel

This will start the installation and show you the progress.

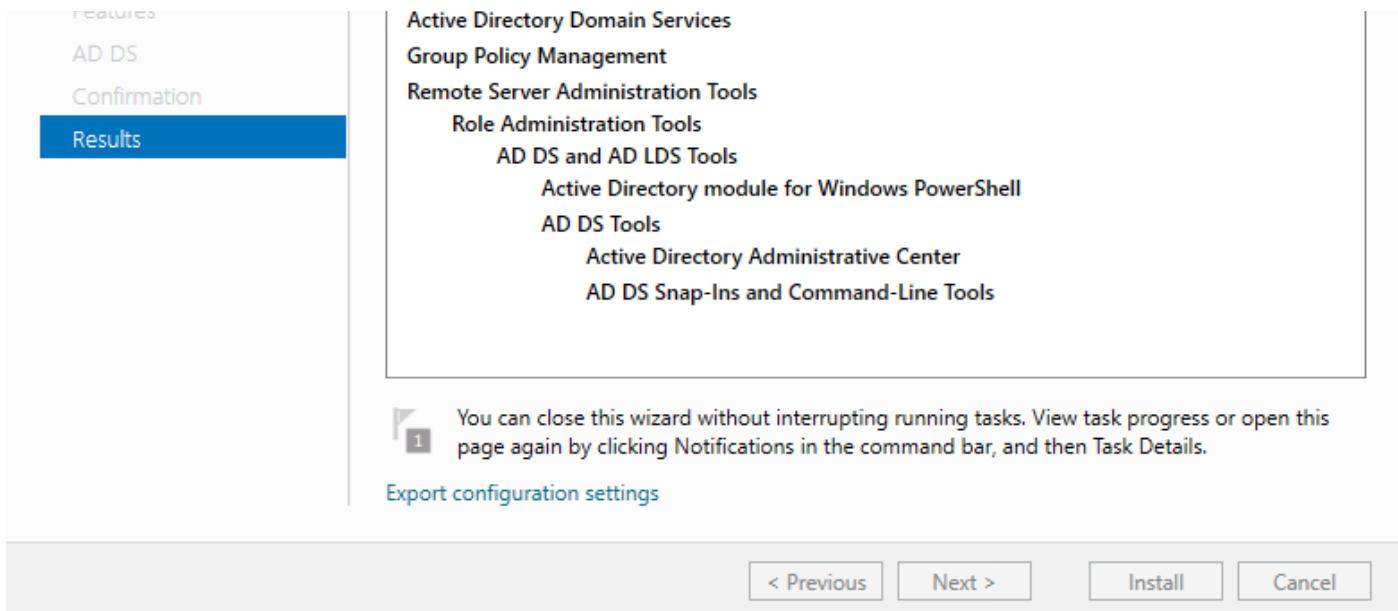
Add Roles and Features Wizard

DESTINATION SERVER  
HYDRA-DC

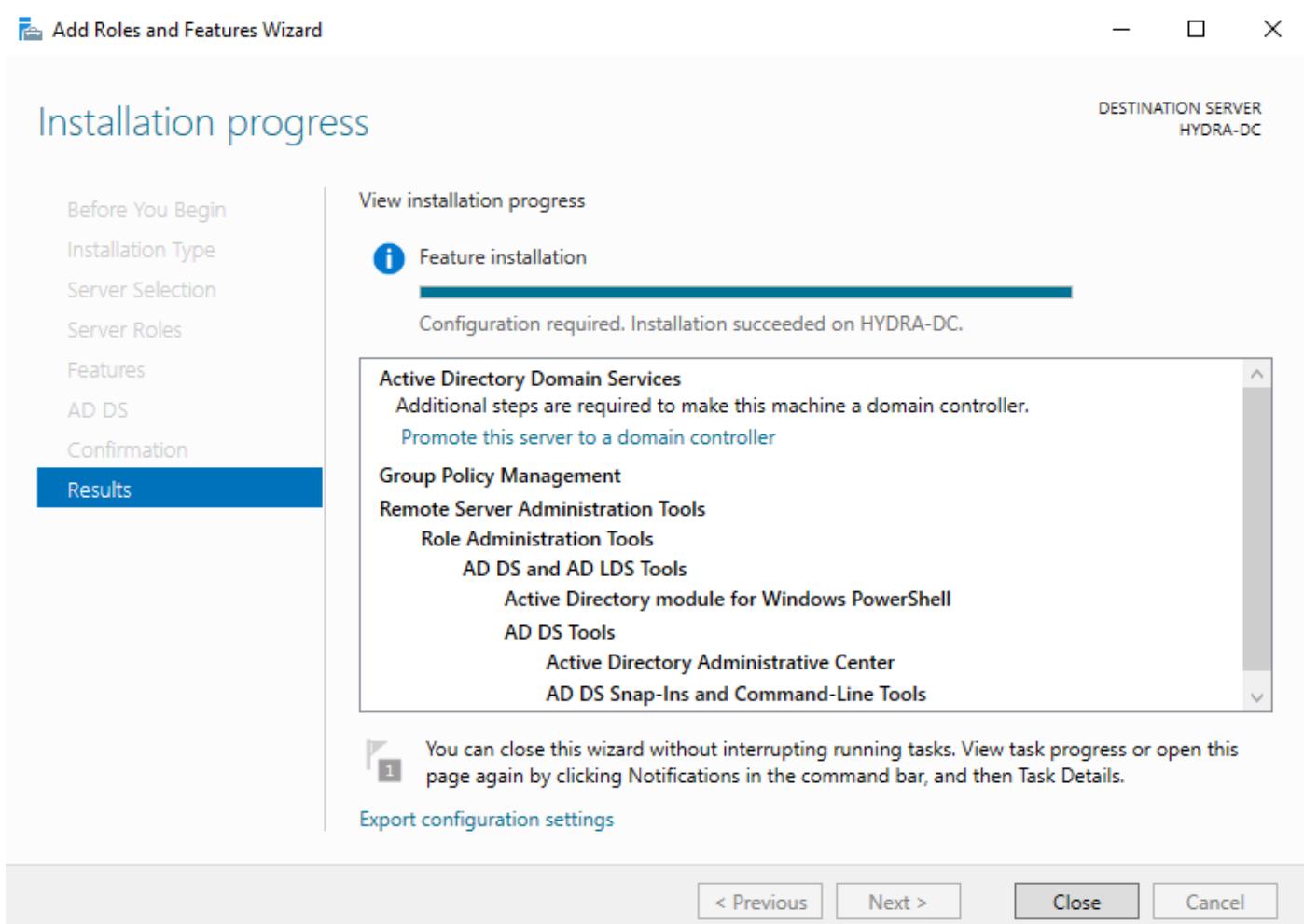
## Installation progress

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Continue

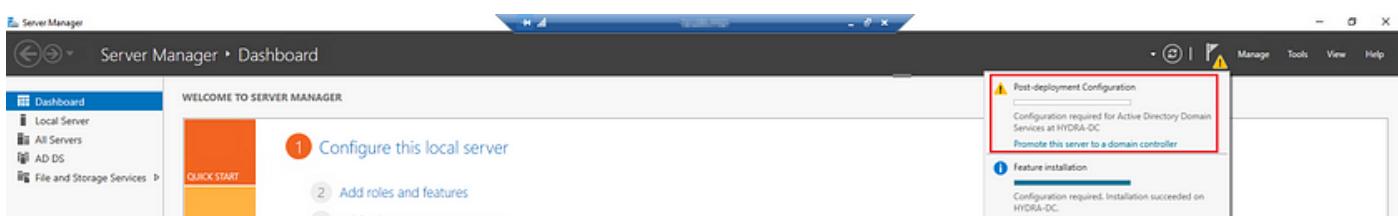
View installation progress  
 Starting installation

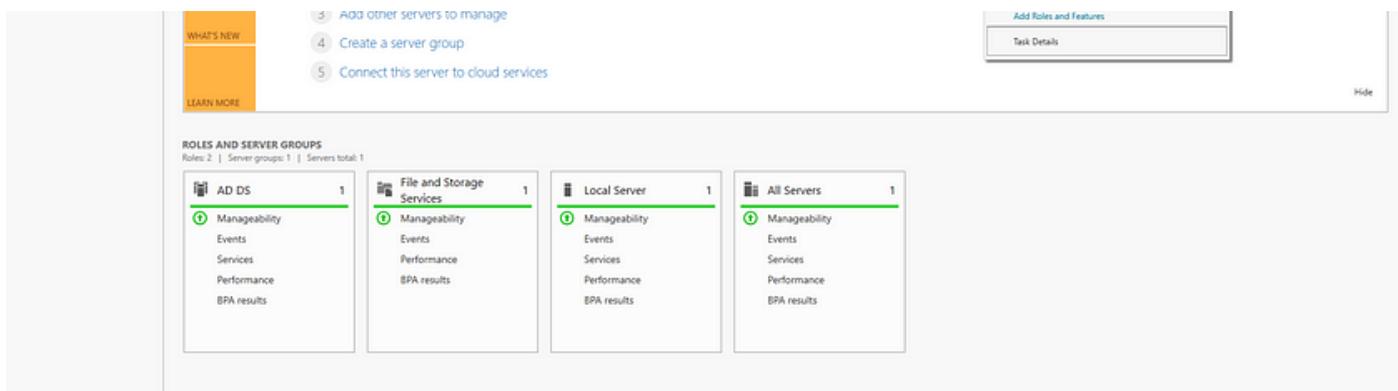


Once the installation is complete, you can just click the Close button.



At this point, it will show you a warning flag as shown in the image below. Clicking on the flag will show you the link for **Promote this server to a domain controller**. Click on that link.





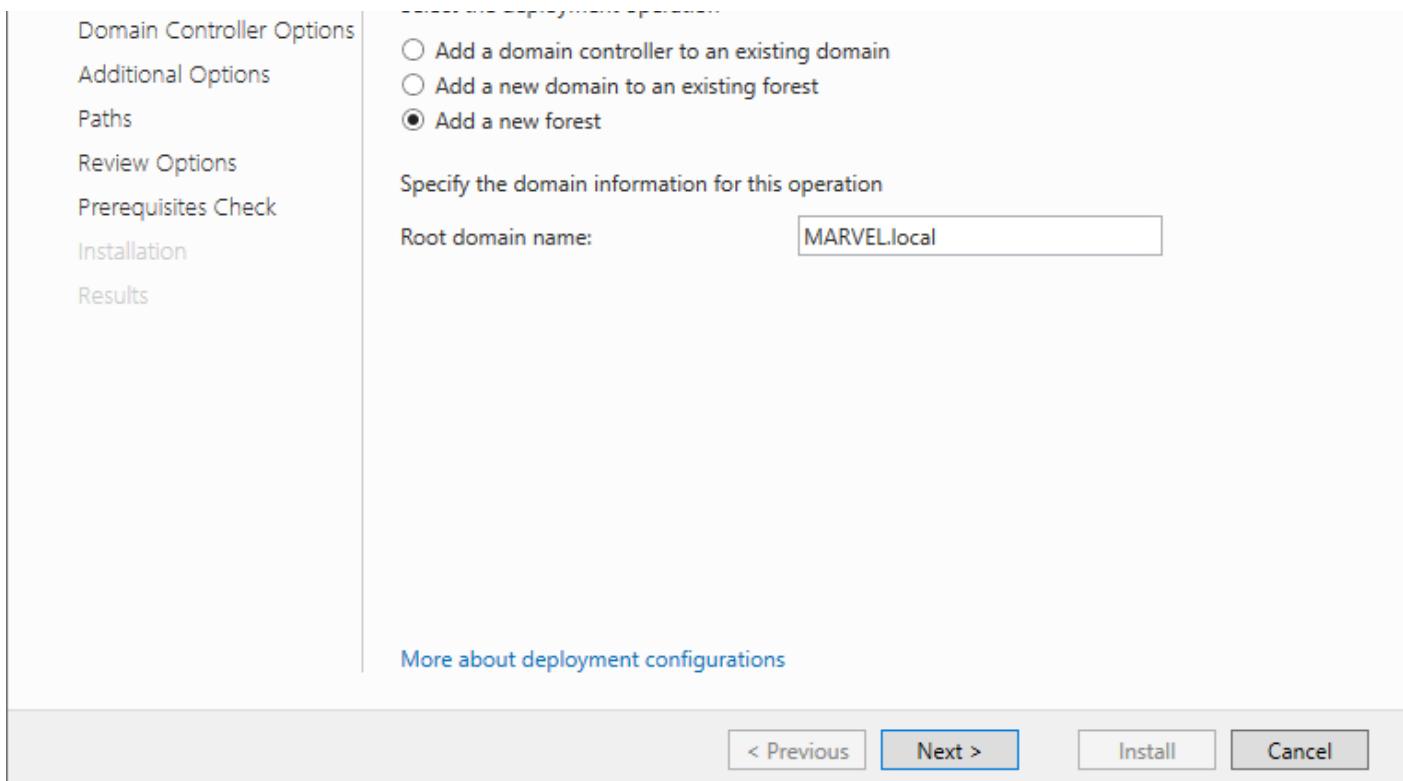
## Promote VM to Domain Controller

Clicking on the **Promote this server to a domain controller** link will launch **Active Directory Domain Service Configuration Wizard**. The first tab Deployment Configuration shows various deployment operations. Let's Choose **Add a new forest** option here.

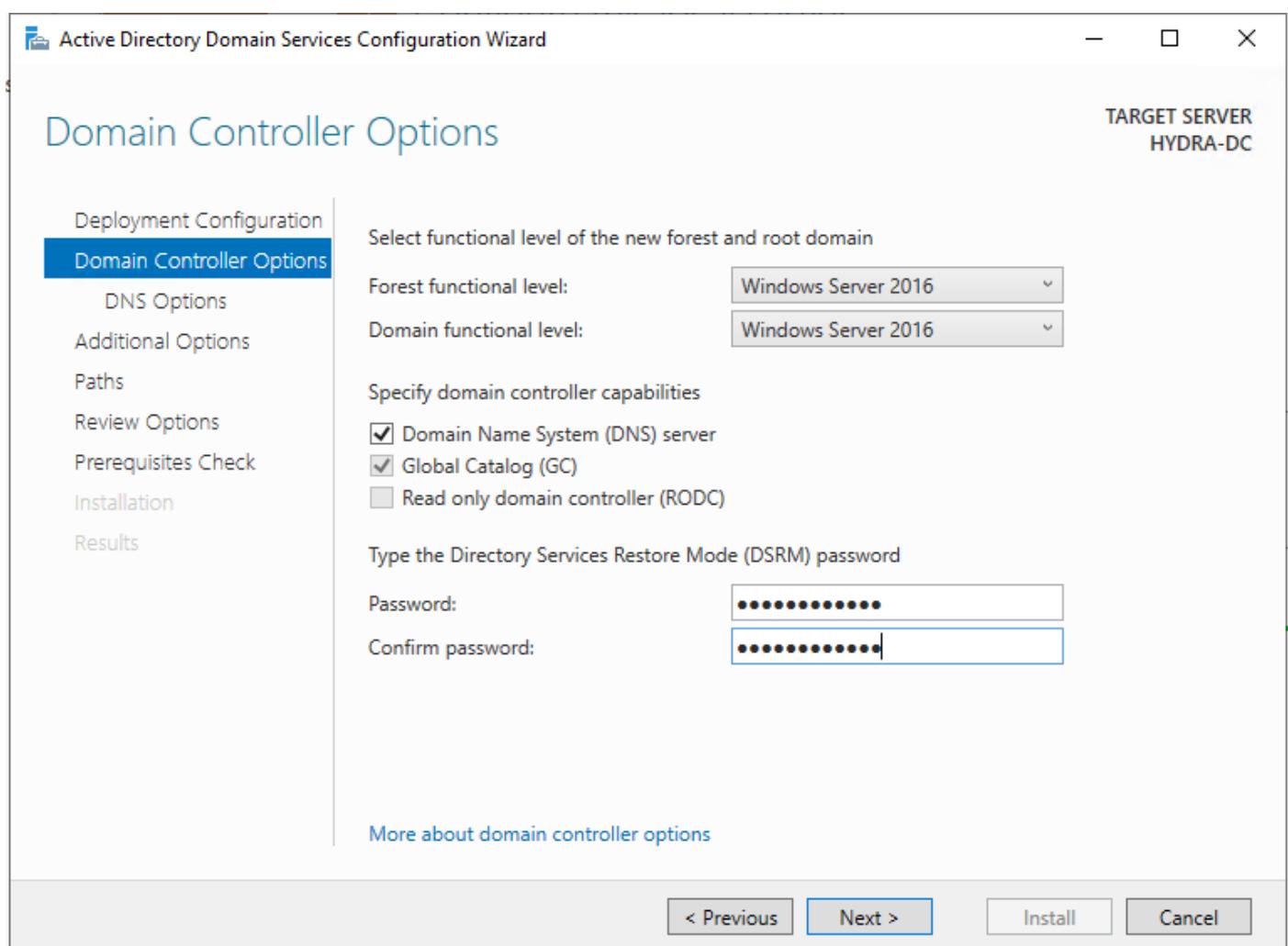
The screenshot shows the 'Deployment Configuration' page of the Active Directory Domain Services Configuration Wizard. The target server is 'HYDRA-DC'. The left sidebar lists navigation options: Deployment Configuration (selected), Domain Controller Options, Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. The main area has three sections: 'Select the deployment operation' (radio buttons for 'Add a domain controller to an existing domain' (selected), 'Add a new domain to an existing forest', and 'Add a new forest'), 'Specify the domain information for this operation' (a 'Domain:' field with a red asterisk and a 'Select...' button), and 'Supply the credentials to perform this operation' (a field showing '<No credentials provided>' and a 'Change...' button). A link 'More about deployment configurations' is at the bottom. Navigation buttons at the bottom are '< Previous', 'Next >', 'Install', and 'Cancel'.

Enter **MARVEL.local** as the domain name and click Next.

The screenshot shows the 'Deployment Configuration' page of the Active Directory Domain Services Configuration Wizard. The target server is 'HYDRA-DC'. The left sidebar lists navigation options: Deployment Configuration (selected), Domain Controller Options, Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. The main area has three sections: 'Select the deployment operation' (radio buttons for 'Add a domain controller to an existing domain' (selected), 'Add a new domain to an existing forest', and 'Add a new forest'), 'Specify the domain information for this operation' (a 'Domain:' field with a red asterisk and a 'Select...' button), and 'Supply the credentials to perform this operation' (a field showing '<No credentials provided>' and a 'Change...' button). A link 'More about deployment configurations' is at the bottom. Navigation buttons at the bottom are '< Previous', 'Next >', 'Install', and 'Cancel'.



On the **Domain Controller Options** tab, enter a password for DSRM and click Next.



Click Next on **DNS Options** tab.



# DNS Options

TARGET SERVER  
HYDRA-DC

! A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... [Show more](#) X

Deployment Configuration

Domain Controller Options

**DNS Options**

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify DNS delegation options

Create DNS delegation

[More about DNS delegation](#)

< Previous

Next >

Install

Cancel

The NetBIOS domain name should populate automatically, Click Next.

## Active Directory Domain Services Configuration Wizard

— □ X

# Additional Options

TARGET SERVER  
HYDRA-DC

Deployment Configuration

Domain Controller Options

DNS Options

**Additional Options**

Paths

Review Options

Prerequisites Check

Installation

Results

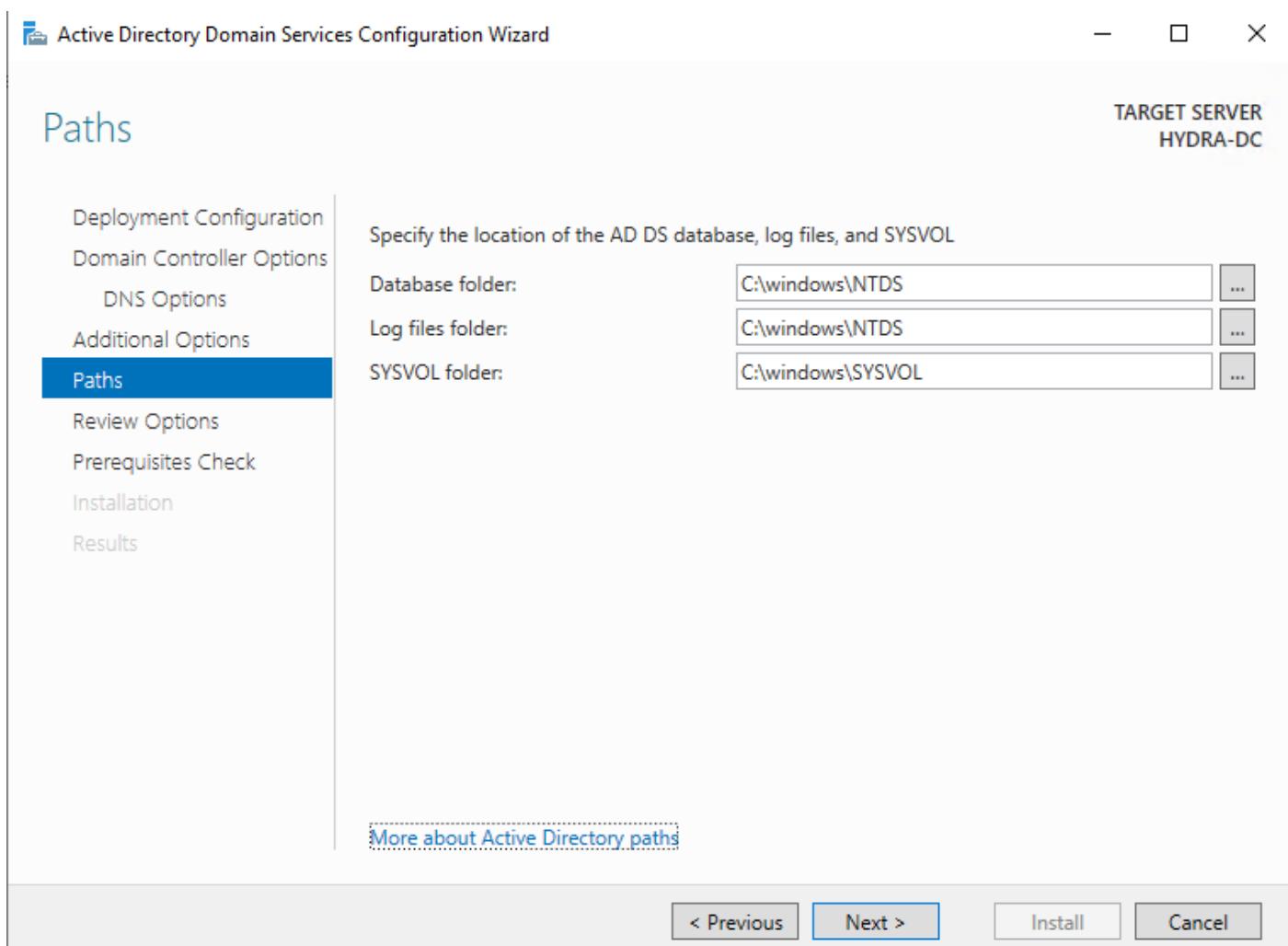
Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

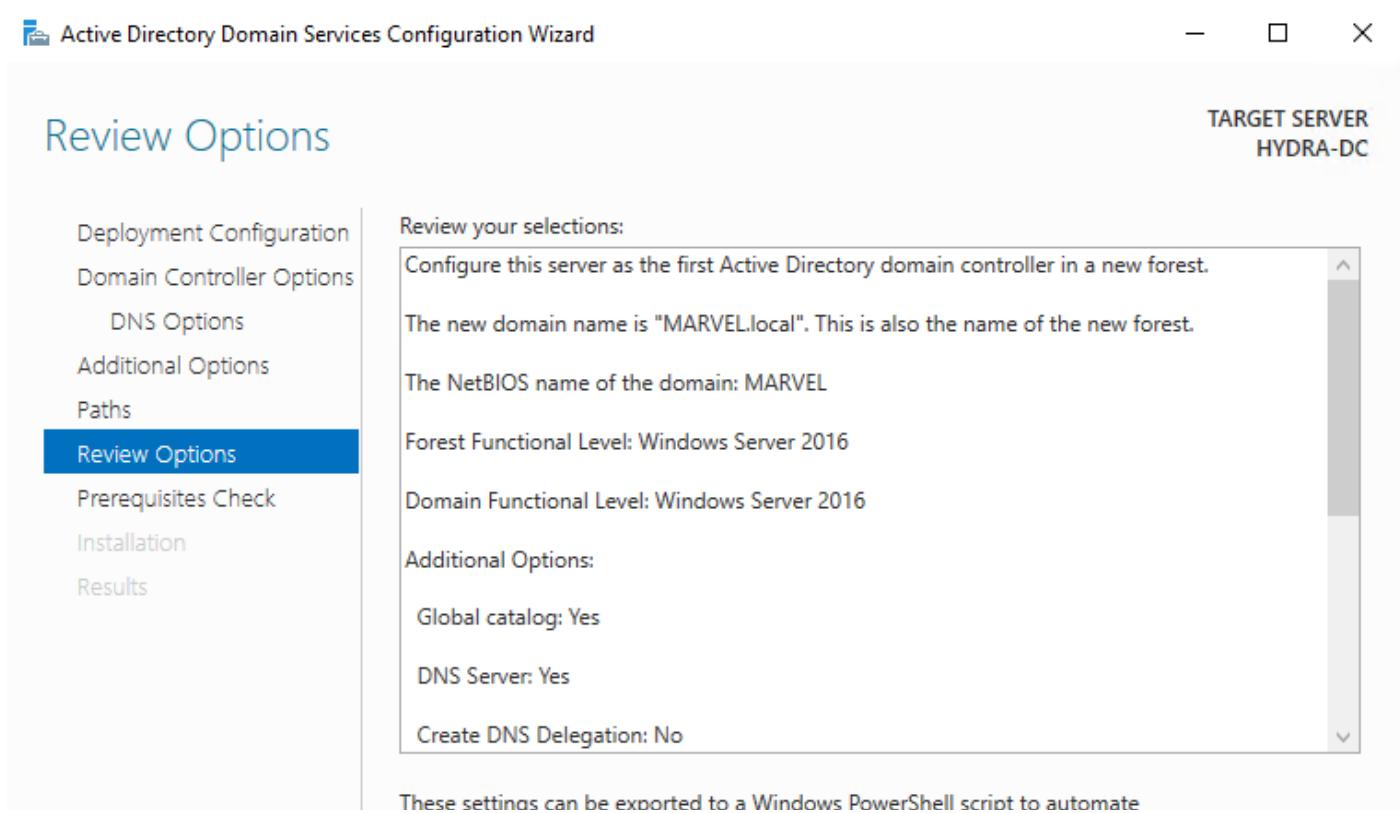
MARVEL

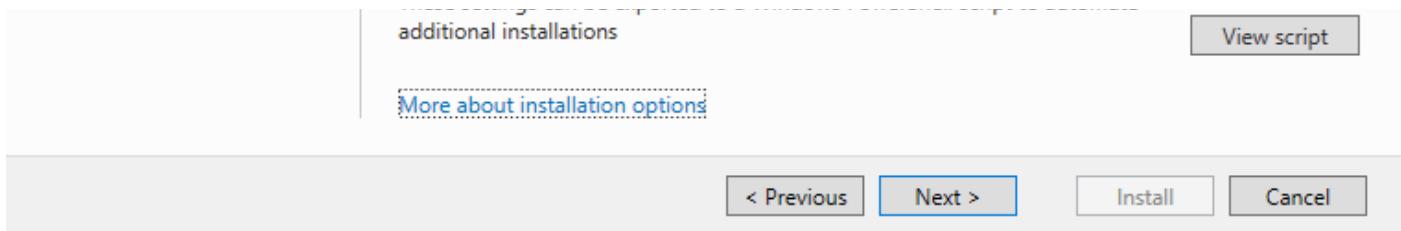
[More about additional options](#)

Accept all the defaults on the **Paths** tab and just click Next.



Review the options and click Next.

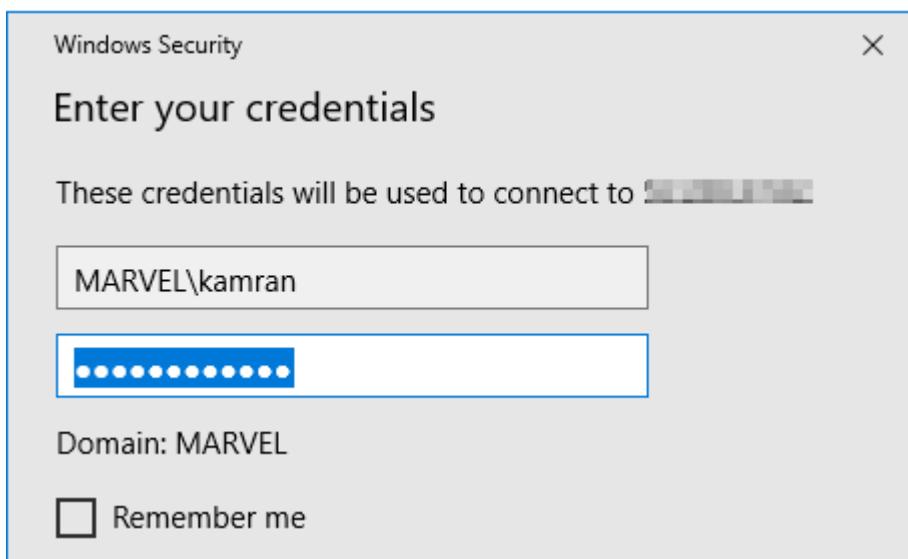


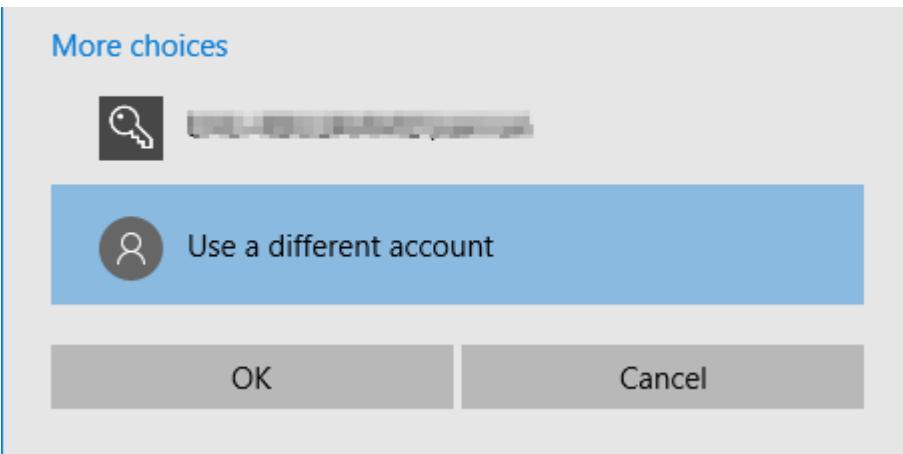


On the final step, click Install button.

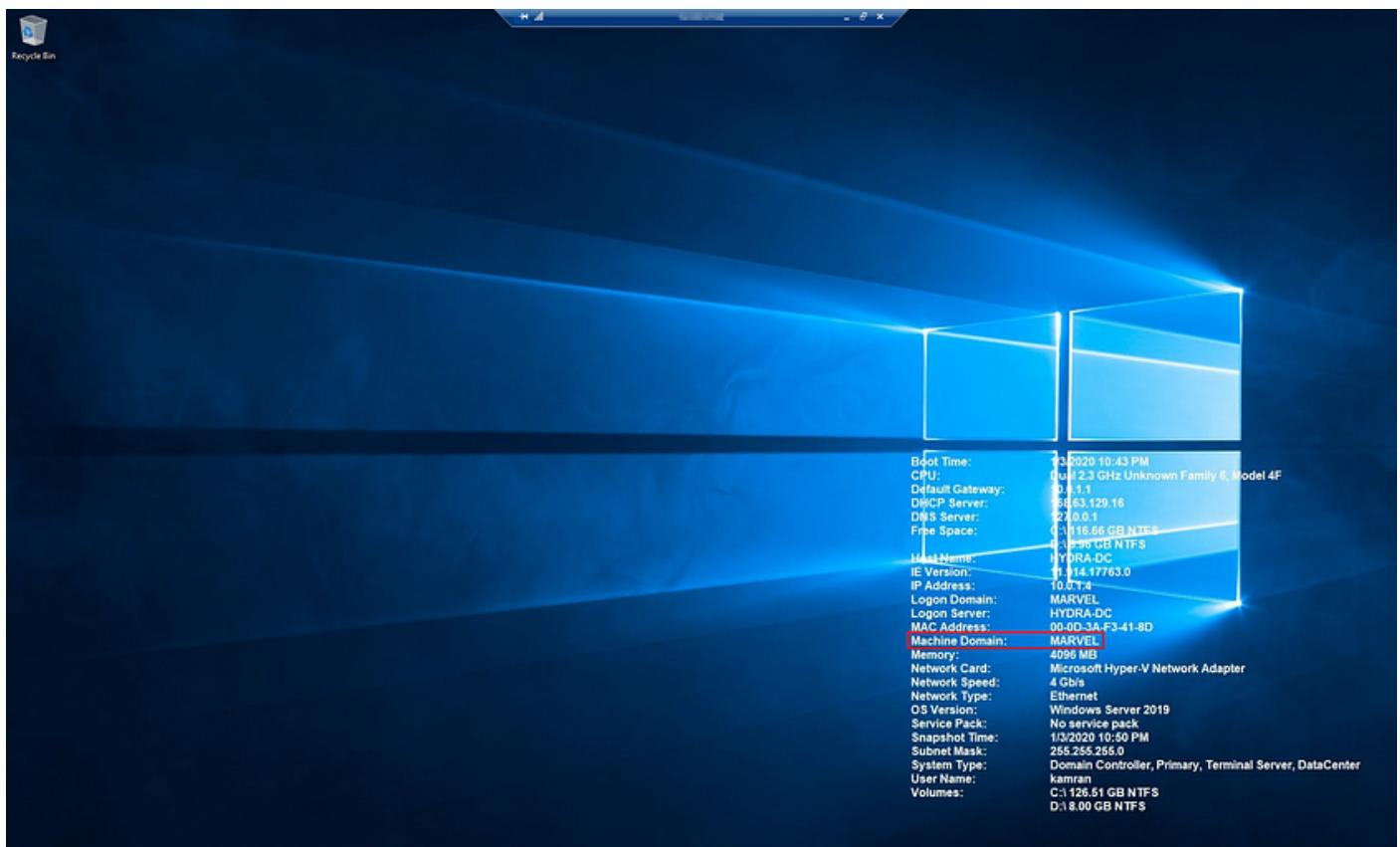
This screenshot shows the 'Prerequisites Check' step of the Active Directory Domain Services Configuration Wizard. The title bar indicates the target server is 'HYDRA-DC'. The main message at the top says 'All prerequisite checks passed successfully. Click 'Install' to begin installation.' Below this, a sidebar lists options: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options, Paths, Review Options, and Prerequisites Check (which is selected and highlighted in blue). The main pane displays a warning message: 'Prerequisites need to be validated before Active Directory Domain Services is installed on this computer' and a link 'Rerun prerequisites check'. A 'View results' section is expanded, showing three items: 1) A warning about Windows Server 2019 domain controllers having a default security setting named 'Allow cryptography algorithms compatible with Windows NT 4.0' that prevents weaker cryptography algorithms. It includes a link to Microsoft Knowledge Base article 942564. 2) A warning about network adapters not having static IP addresses assigned. It states that both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. 3) A warning that if the 'Install' button is clicked, the server will automatically reboot at the end of the promotion operation. At the bottom, there are navigation buttons: '< Previous' and 'Next >' on the left, and 'Install' and 'Cancel' on the right.

It will take a few minutes for this installation to complete. This will cause a reboot of the machine as well. After that, you can log in with the domain credentials.



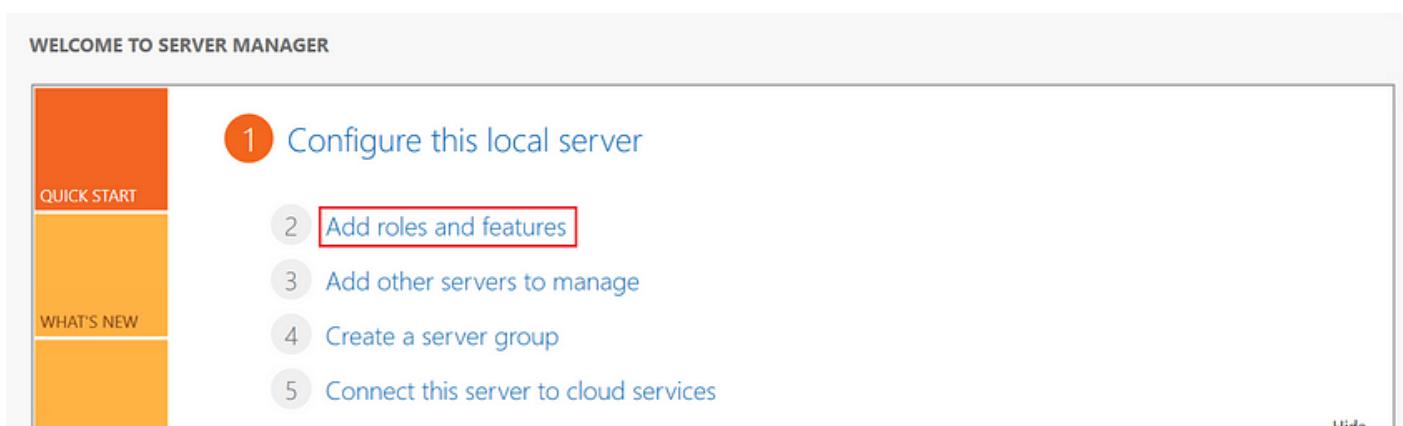


The desktop background image showing that we log in to the newly created MARVEL domain.



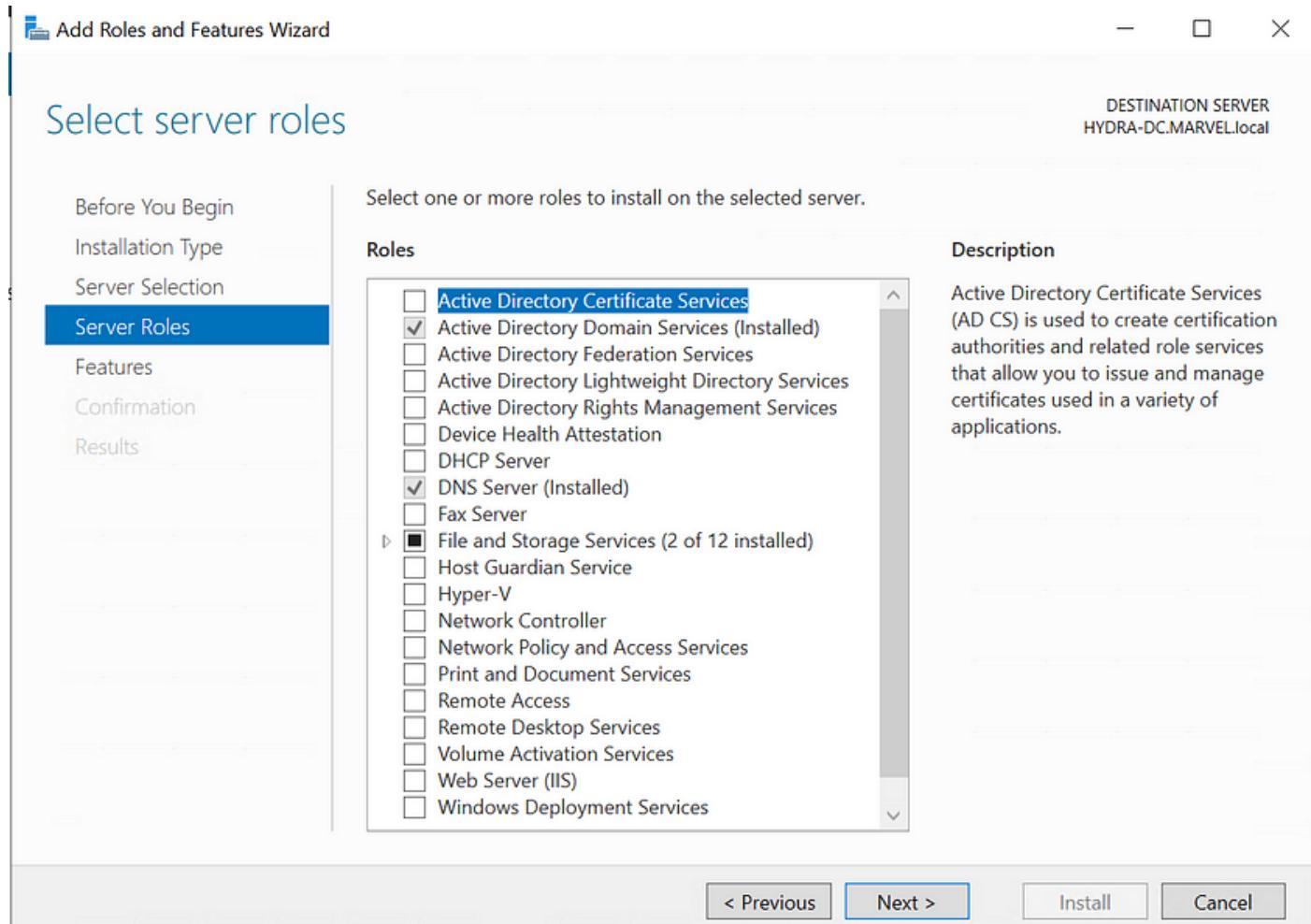
## Configuring Certificate Services

The next step is to setup Certificate Services. Let's launch the Server Manager again and click on the **Add roles and features**.

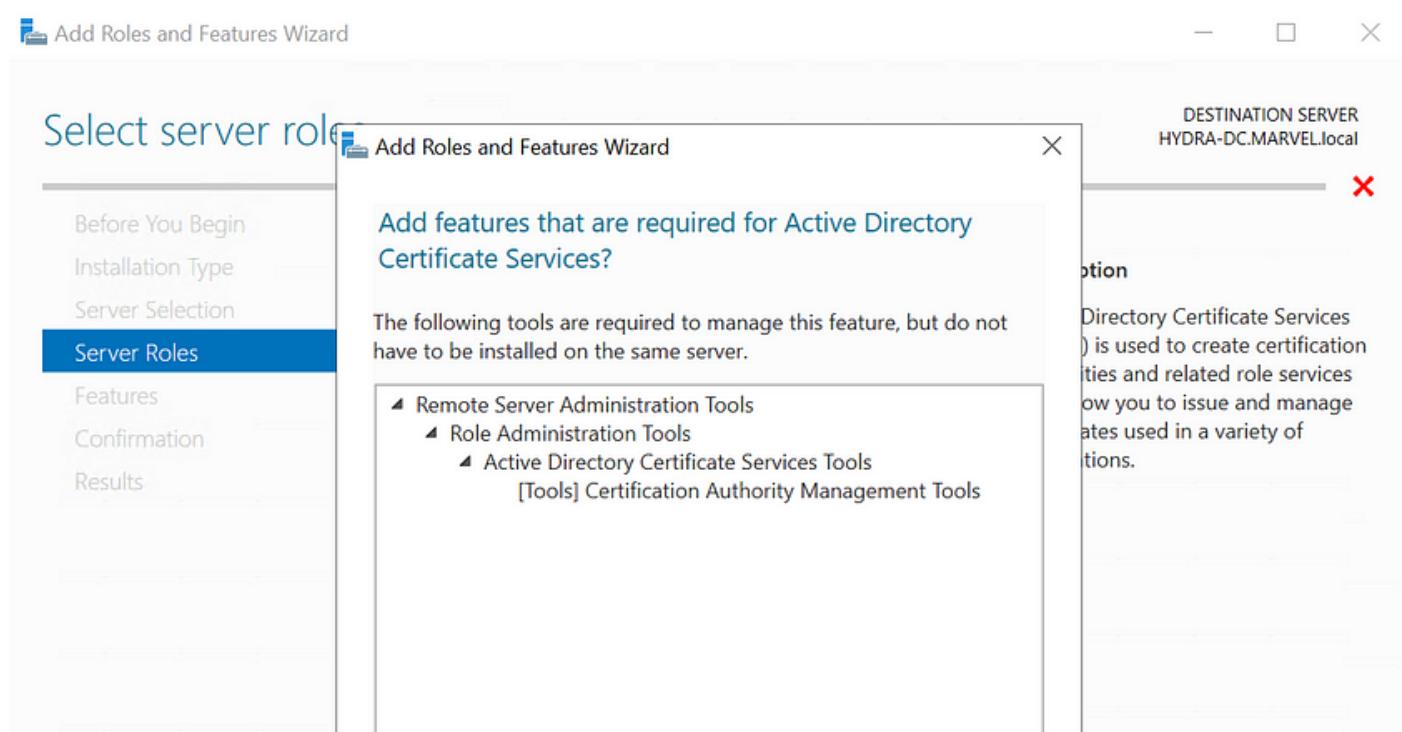


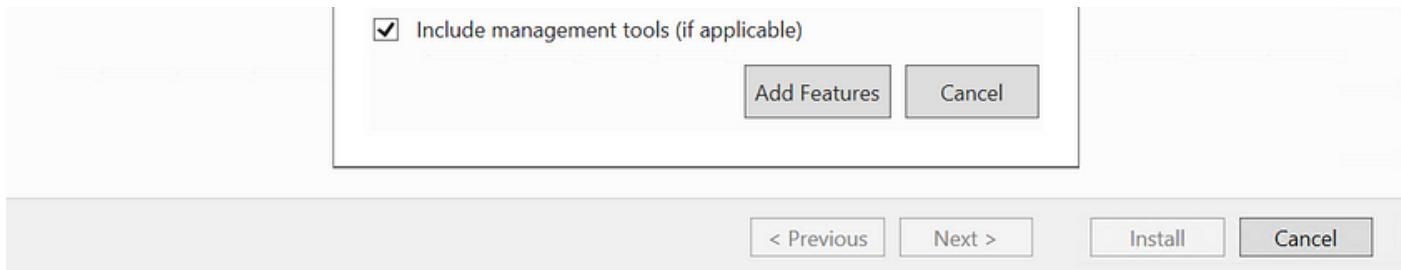
[LEARN MORE](#)

This will launch the **Add Roles and Features Wizard** that we used before too. Just keep clicking Next until you are on the Server Roles tab. Check the **Active Directory Certificate Services (ADCS)** here.



That will pop-up the following dialog with the information about the required features for ADCS. Click on **Add Features** button.





Click on the Next button.

Add Roles and Features Wizard

## Select server roles

DESTINATION SERVER  
HYDRA-DC.MARVEL.local

Before You Begin

Installation Type

Server Selection

**Server Roles**

Features

AD CS

Role Services

Confirmation

Results

Select one or more roles to install on the selected server.

**Roles**

<input checked="" type="checkbox"/> Active Directory Certificate Services	Description
<input checked="" type="checkbox"/> Active Directory Domain Services (Installed)	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input type="checkbox"/> DHCP Server	
<input checked="" type="checkbox"/> DNS Server (Installed)	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (2 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Controller	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	

< Previous    Next >    Install    Cancel

Click on the **AD CS** tab.

Add Roles and Features Wizard

## Active Directory Certificate Services

DESTINATION SERVER  
HYDRA-DC.MARVEL.local

Before You Begin

Installation Type

Server Selection

**Server Roles**

Features

**AD CS**

Role Services

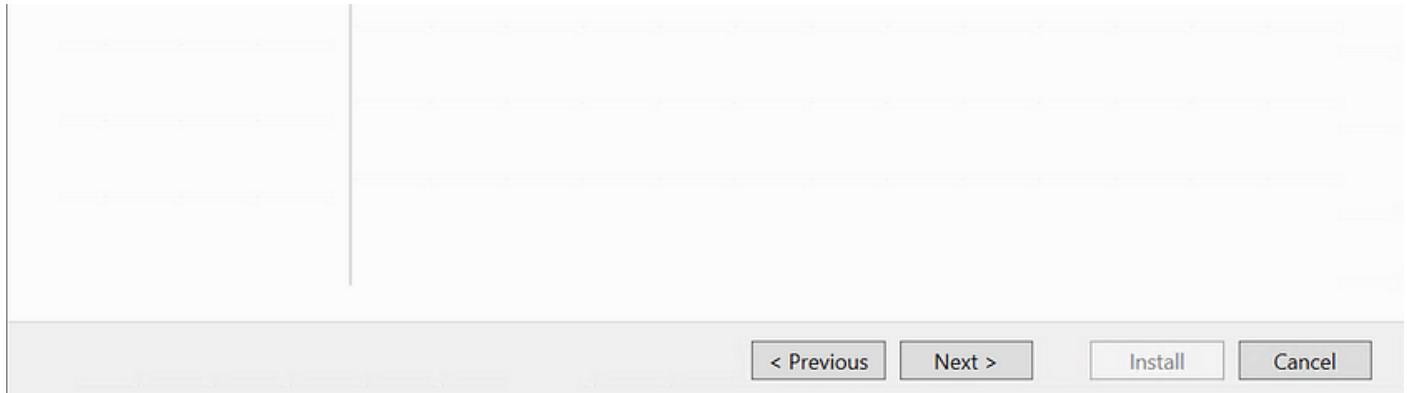
Confirmation

Results

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.



Check the **Certification Authority** checkbox and click Next.

Select the role services to install for Active Directory Certificate Services	
Role services	Description
<input checked="" type="checkbox"/> Certification Authority	Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
<input type="checkbox"/> Certificate Enrollment Policy Web Service	
<input type="checkbox"/> Certificate Enrollment Web Service	
<input type="checkbox"/> Certification Authority Web Enrollment	
<input type="checkbox"/> Network Device Enrollment Service	
<input type="checkbox"/> Online Responder	

< Previous    Next >    Install    Cancel

On the **Confirmation** tab, check the **Restart the destination server automatically if required** checkbox. This will prompt a confirmation dialog. Select Yes and then click on Next.

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

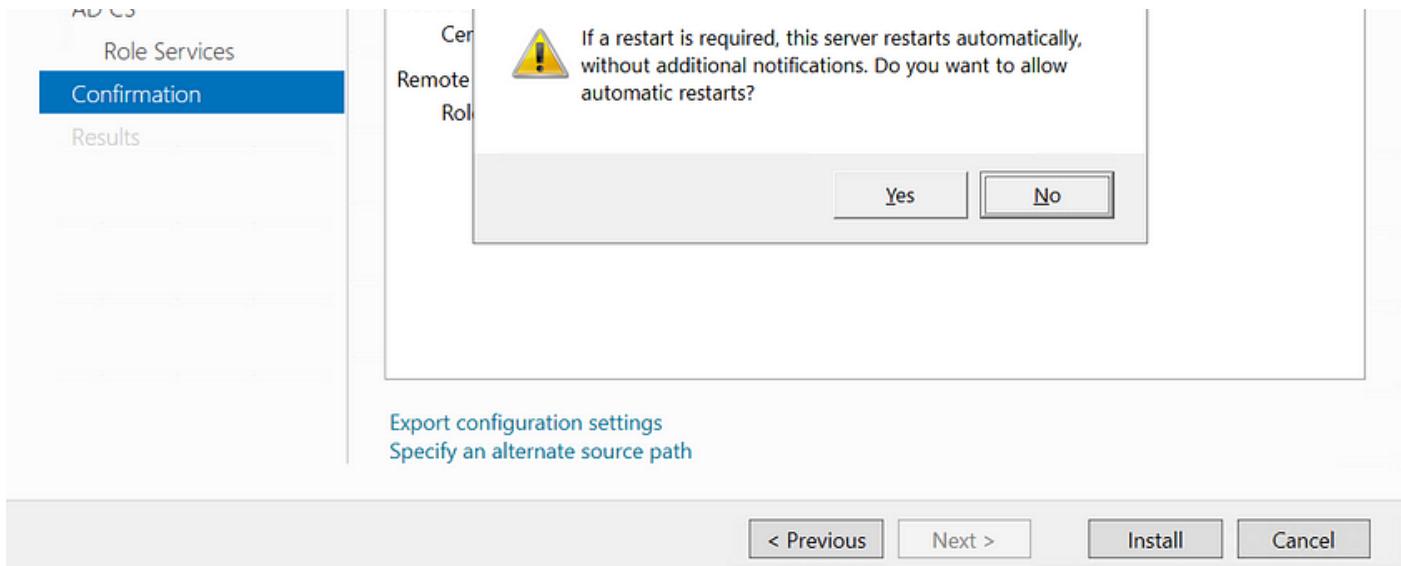
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their checkboxes.

Add Roles and Features Wizard

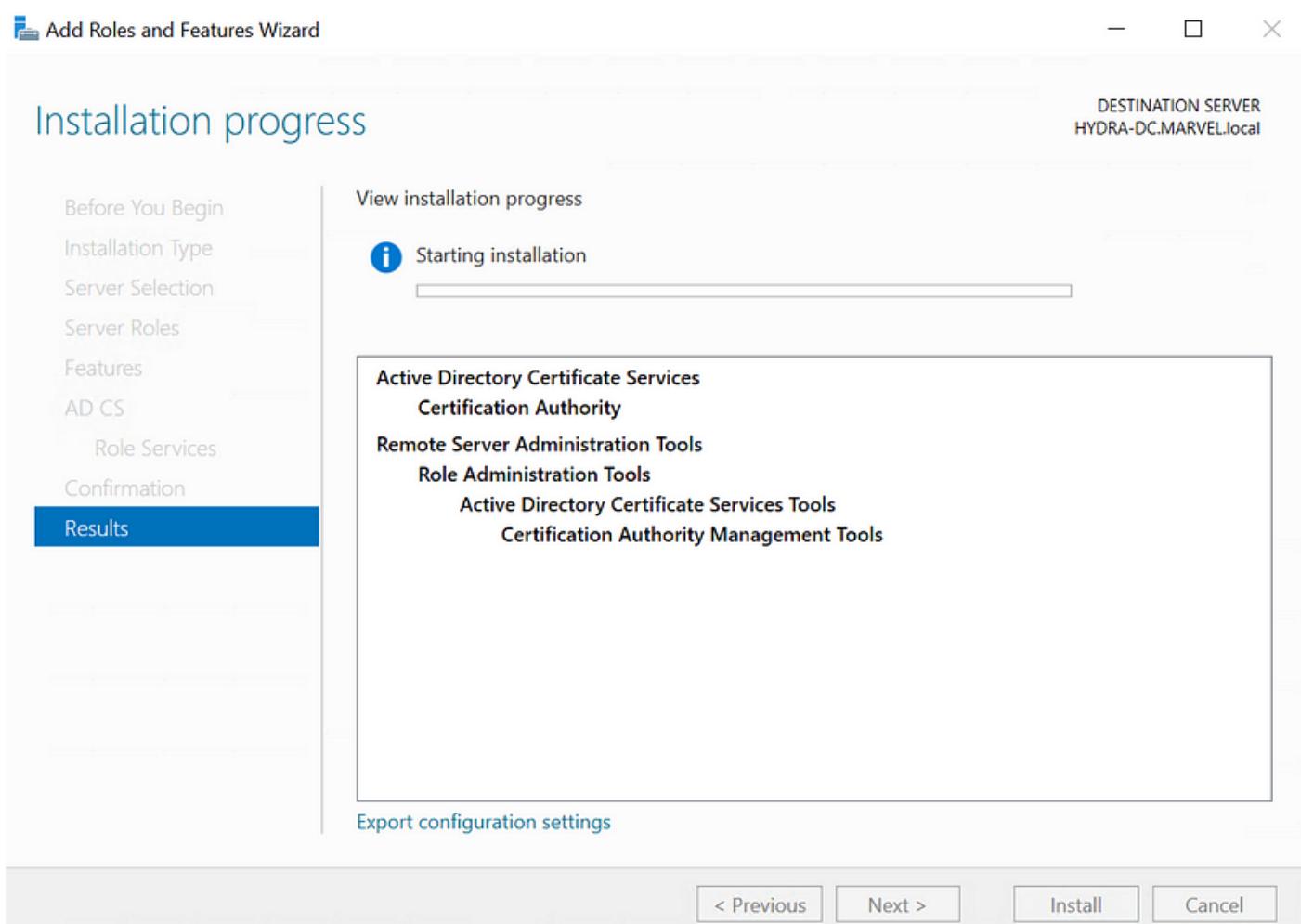
DESTINATION SERVER  
HYDRA-DC.MARVEL.local

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
AD CS  
Role Services  
Confirmation  
Results

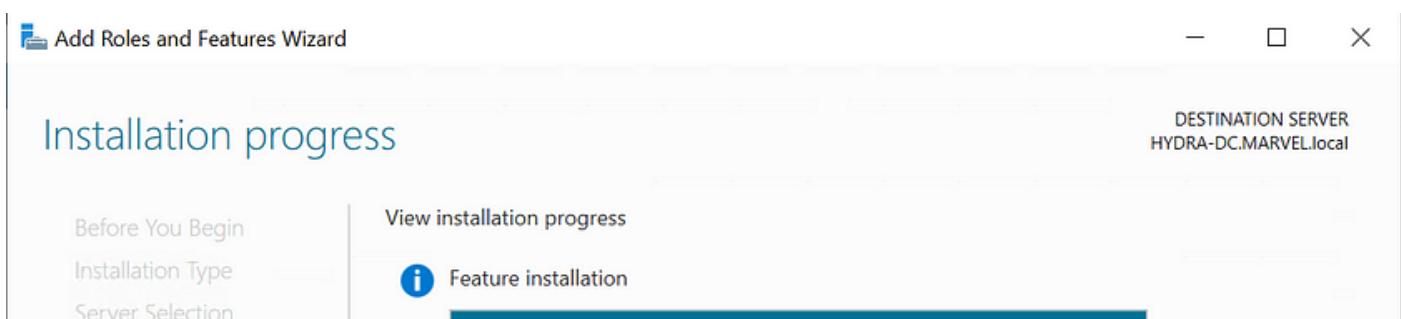
Active D

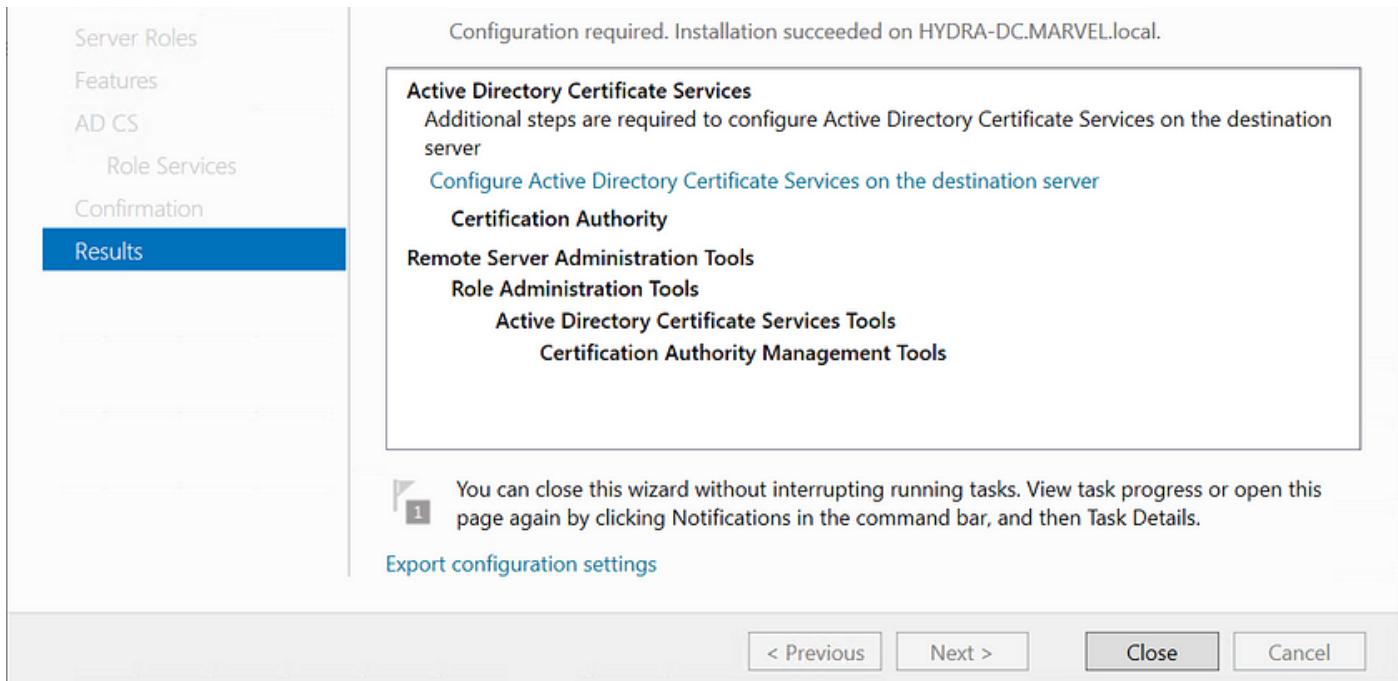


This will start the installation process for ADCS and the required components.

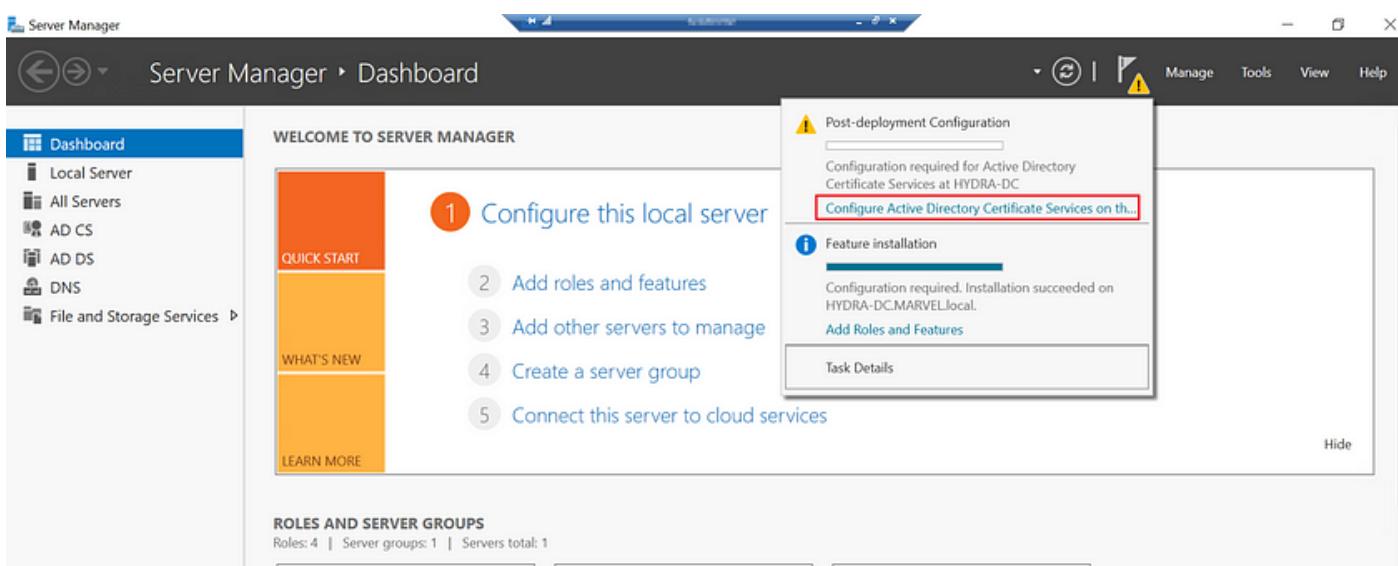


asdfffd

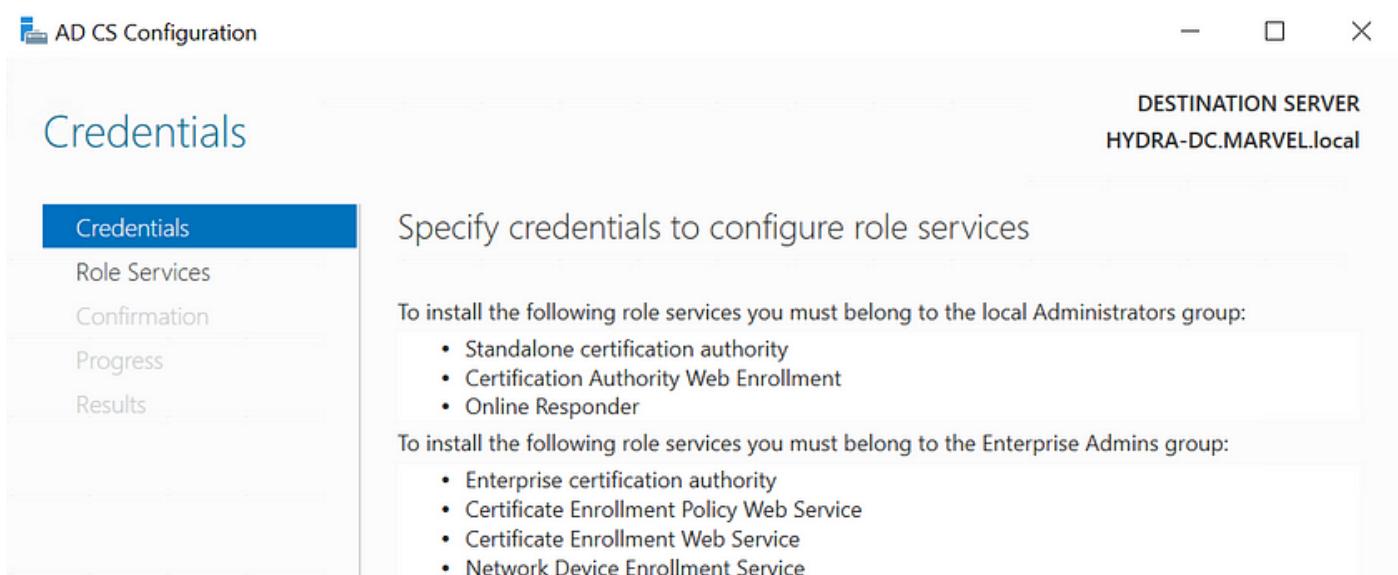


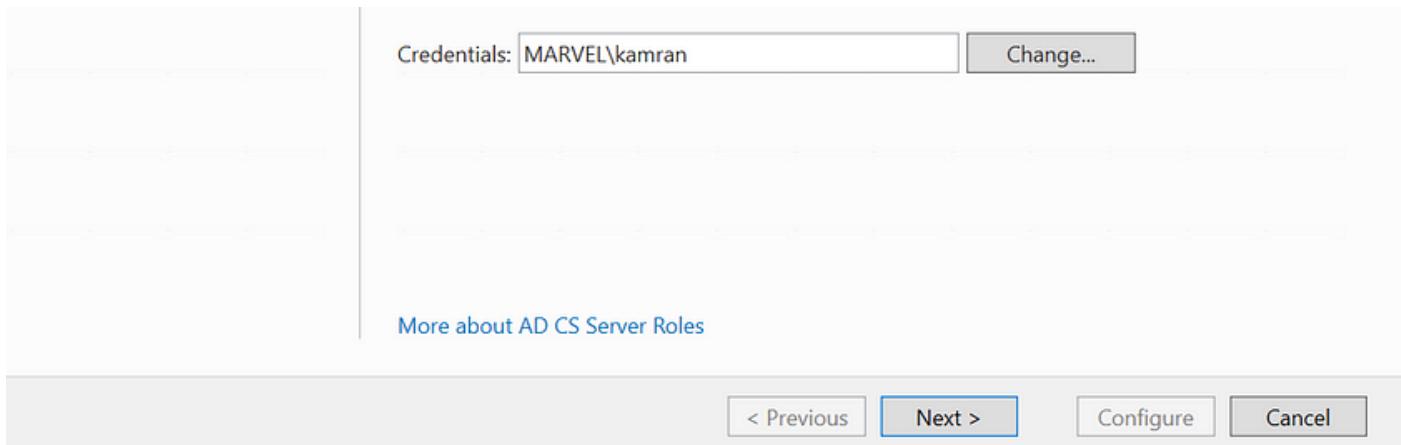


At this point, you will see a warning flag. Click on that flag and then click on the link for **Configure Active Directory Certificate Services on the destination server**.



This will launch the **AD CS Configuration** wizard. Click next on the **Credentials** tab.





On the **Role Services** tab, check the **Certification Authority** check box and click Next.

AD CS Configuration DESTINATION SERVER HYDRA-DC.MARVEL.local

## Role Services

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Select Role Services to configure

- Certification Authority
- Certification Authority Web Enrollment
- Online Responder
- Network Device Enrollment Service
- Certificate Enrollment Web Service
- Certificate Enrollment Policy Web Service

More about AD CS Server Roles

< Previous Next > Configure Cancel

Make sure to select **Enterprise CA** on the **Setup Type** tab and click Next.

AD CS Configuration DESTINATION SERVER HYDRA-DC.MARVEL.local

## Setup Type

Credentials  
Role Services  
Setup Type  
CA Type

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

Private Key  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Enterprise CA  
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

Standalone CA  
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

[More about Setup Type](#)

< Previous Next > Configure Cancel

Make sure to select **Root CA** on the **CA Type** tab and click Next.

AD CS Configuration DESTINATION SERVER HYDRA-DC.MARVEL.local

## CA Type

Credentials  
Role Services  
Setup Type  
**CA Type**  
Private Key  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

Root CA  
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

Subordinate CA  
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous Next > Configure Cancel

Select **Create a new private key** on the **Private Key** tab and click Next.

AD CS Configuration DESTINATION SERVER HYDRA-DC.MARVEL.local

## Private Key

Credentials  
Role Services  
Setup Type  
CA Type  
**Private Key**  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

Create a new private key  
Use this option if you do not have a private key or want to create a new private key.

Use existing private key  
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.  
 Select a certificate and use its associated private key  
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.  
 Select an existing private key on this computer  
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous **Next >** Configure Cancel

Stick with the default options on the **Cryptography** tab and click Next.

AD CS Configuration DESTINATION SERVER HYDRA-DC.MARVEL.local

Cryptography for CA

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
**Cryptography**  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256  
SHA384  
SHA512  
SHA1  
MD5

Allow administrator interaction when the private key is accessed by the CA.

[More about Cryptography](#)

< Previous **Next >** Configure Cancel

Stick with all the default names of **CA Name** tab and click Next.

AD CS Configuration

## CA Name

DESTINATION SERVER  
HYDRA-DC.MARVEL.local

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name**
- Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:  
**MARVEL-HYDRA-DC-CA**

Distinguished name suffix:  
**DC=MARVEL,DC=local**

Preview of distinguished name:  
**CN=MARVEL-HYDRA-DC-CA,DC=MARVEL,DC=local**

[More about CA Name](#)

< Previous    Next >    [Configure](#)    [Cancel](#)

On the **Validity Period**, change it **99** years and click **Next**.

AD CS Configuration

## Validity Period

DESTINATION SERVER  
HYDRA-DC.MARVEL.local

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name**
- Validity Period**
- Certificate Database
- Confirmation
- Progress
- Results

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):  
**99** **Years**

CA expiration Date: 1/5/2119 8:17:00 AM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

[< Previous](#)[Next >](#)[Configure](#)[Cancel](#)

Stick with the default database and log location and click Next.

AD CS Configuration

## CA Database

DESTINATION SERVER  
HYDRA-DC.MARVEL.local

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Validity Period  
**Certificate Database**  
Confirmation  
Progress  
Results

Specify the database locations

Certificate database location:

Certificate database log location:

More about CA Database

< Previous [Next >](#) Configure Cancel

Click the Configure button on the **Confirmation** tab.

AD CS Configuration

## Confirmation

DESTINATION SERVER  
HYDRA-DC.MARVEL.local

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
**Confirmation**  
Progress  
Results

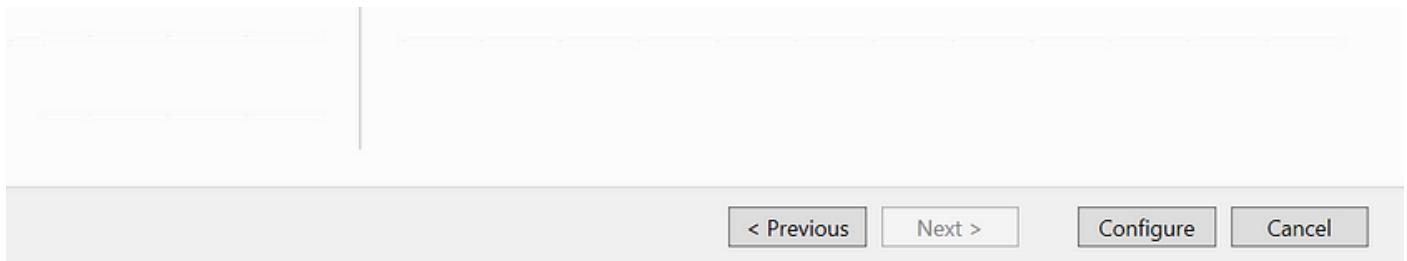
To configure the following roles, role services, or features, click Configure.

**Active Directory Certificate Services**

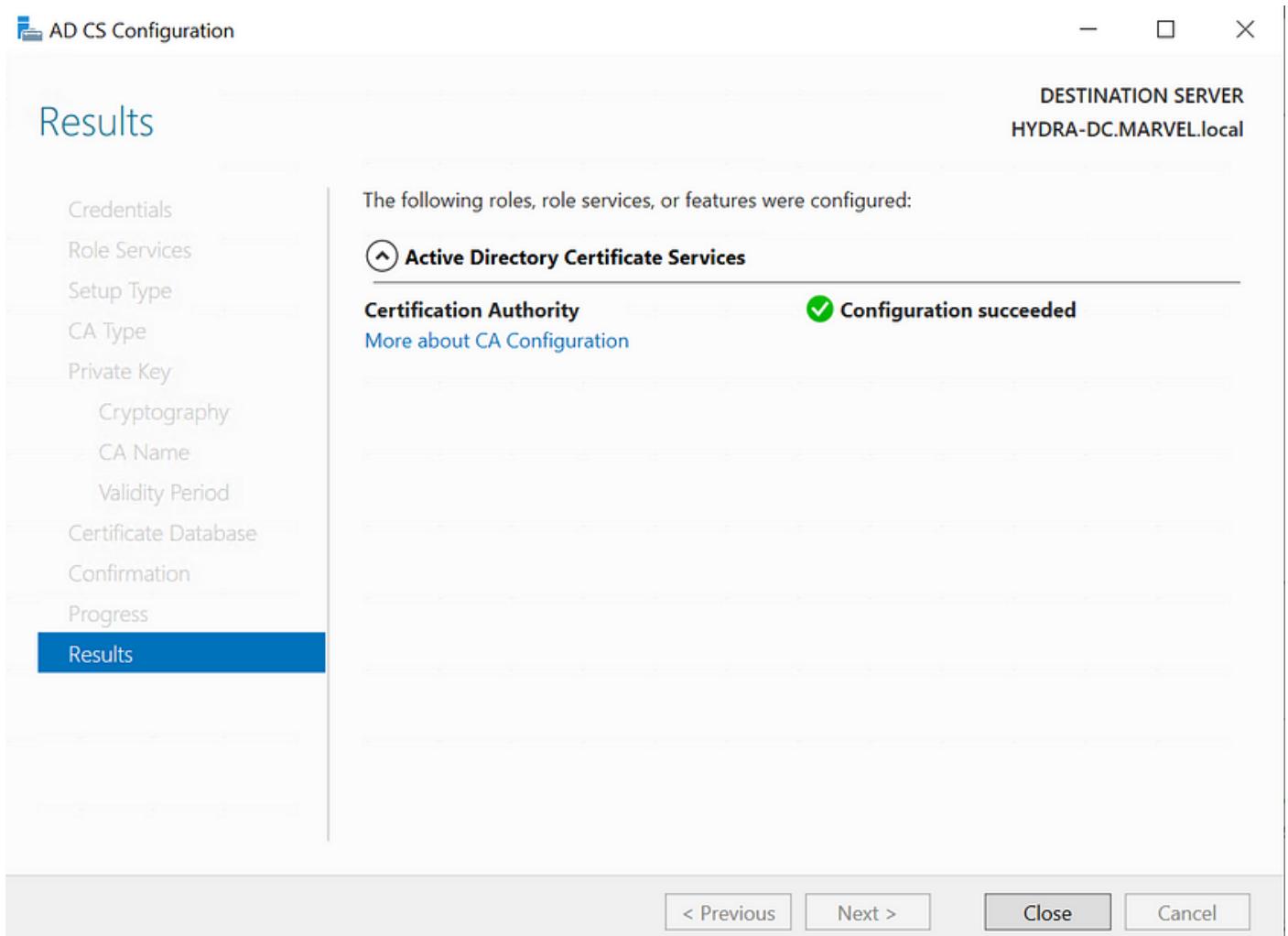
**Certification Authority**

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	1/5/2119 8:17:00 AM
Distinguished Name:	CN=MARVEL-HYDRA-DC-CA,DC=MARVEL,DC=local
Certificate Database Location:	C:\windows\system32\CertLog
Certificate Database Log Location:	C:\windows\system32\CertLog

< Previous [Next >](#) Configure Cancel



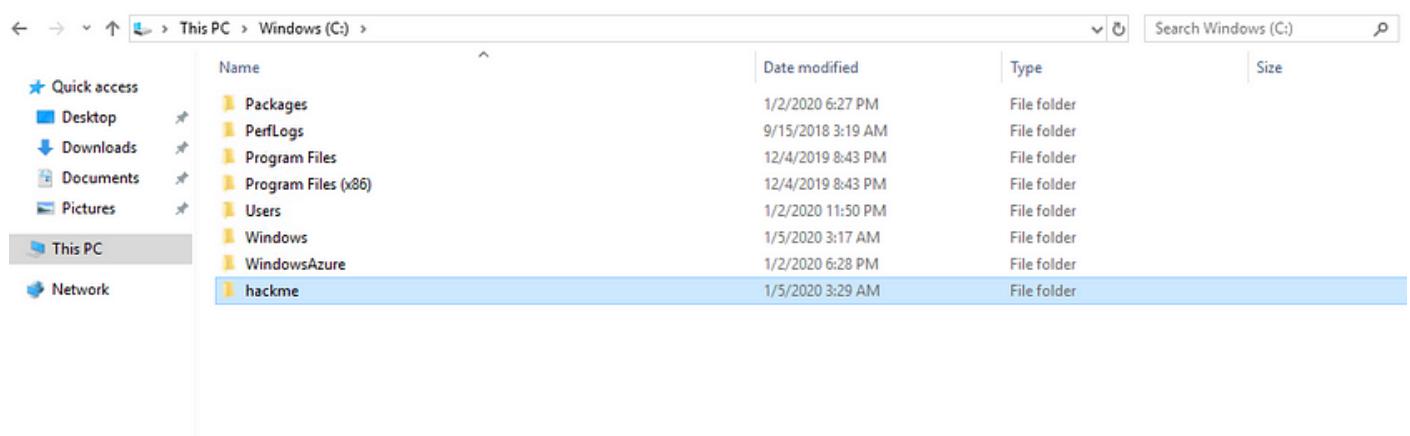
Shortly after you will see the message about Configuration succeeded. You can close this dialog now.



Restart the VM now so the changes take effect.

## Setting up a Share

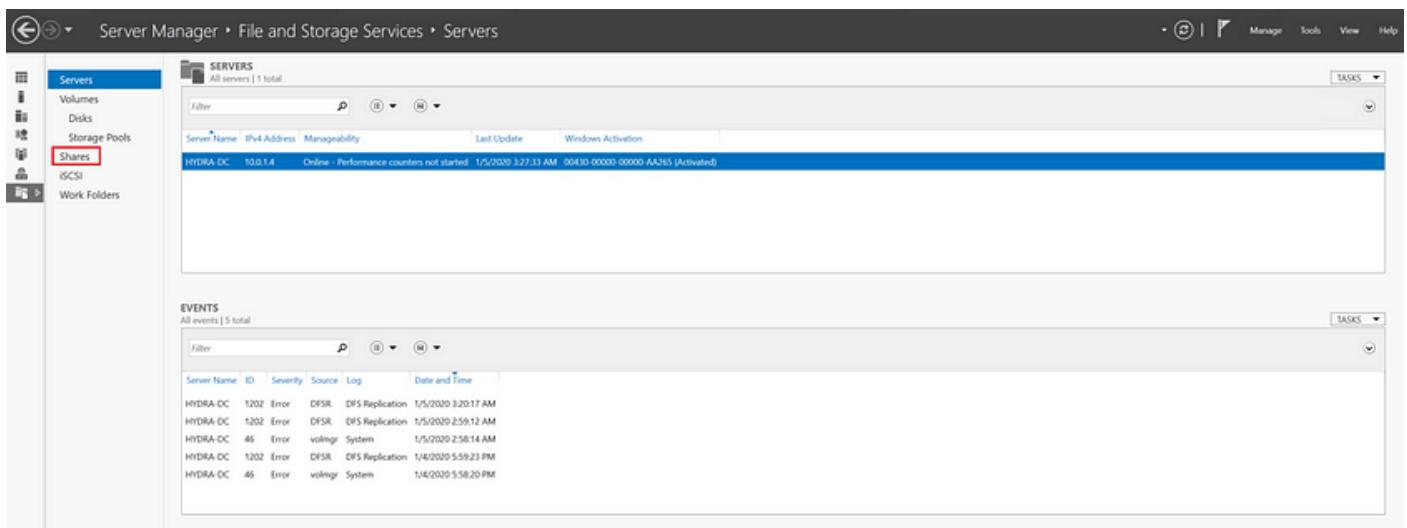
Create a folder **hackme** on the C drive.



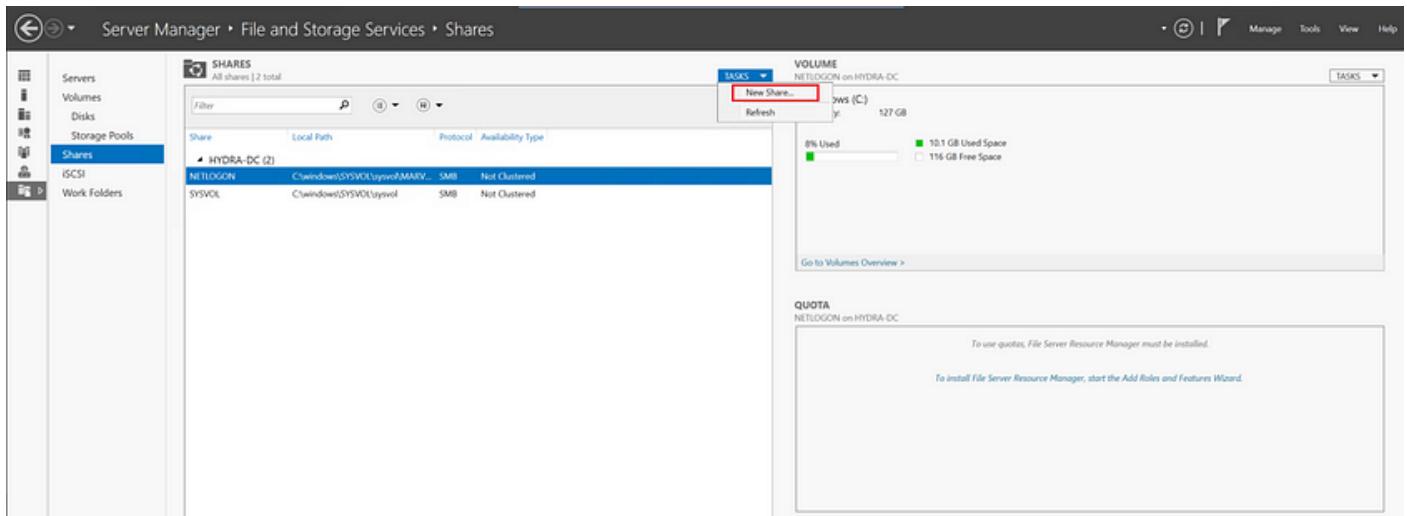
Launch the Server Manager and click on the **File and Storage Services** tab.



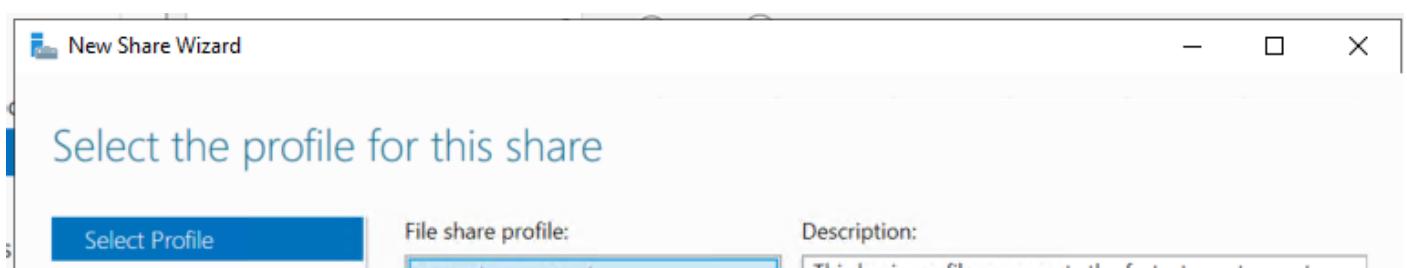
Click on the **Shares** as shown below.



Click on the **New Share** menu item under **Tasks** as shown below.



This will launch the **New Share Wizard**. Make sure **SMB Share — Quick** File share profile is selected and click Next.



Share Location  
Share Name  
Other Settings  
Permissions  
Confirmation  
Results

SMB Share - Quick  
SMB Share - Advanced  
SMB Share - Applications  
NFS Share - Quick  
NFS Share - Advanced

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

Select **Type a Custom path** option and enter **c:\hackme** folder path and click Next.

New Share Wizard

Select Profile  
Share Location  
Share Name  
Other Settings  
Permissions  
Confirmation  
Results

Server:

Server Name	Status	Cluster Role	Owner Node
HYDRA-DC	Online	Not Clustered	

Share location:

Select by volume:

Volume	Free Space	Capacity	File System
C:	116 GB	127 GB	NTFS
D:	6.96 GB	8.00 GB	NTFS

The location of the file share will be a new folder in the \Shares directory on the selected volume.

Type a custom path:  
C:\hackme

< Previous Next > Create Cancel

Stick with **hackme** as the Share name and click Next.

New Share Wizard

Share Name: hackme

Description:

Comments:

Create Cancel

## Specify share name

Select Profile

Share Location

**Share Name**

Other Settings

Permissions

Confirmation

Results

Share name:

hackme

Share description:

Local path to share:

C:\hackme

Remote path to share:

\\\\HYDRA-DC\\hackme

< Previous

Next >

Create

Cancel

Stick with the defaults on the **Other Settings** tab and click Next.

New Share Wizard



## Configure share settings

Select Profile

Share Location

Share Name

**Other Settings**

Permissions

Confirmation

Results

Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

< Previous

Next >

Create

Cancel

Stick with the defaults on the **Permissions** tab and click Next.

The screenshot shows the 'New Share Wizard' window with the title 'Specify permissions to control access'. On the left, a sidebar lists tabs: 'Select Profile', 'Share Location', 'Share Name', 'Other Settings', 'Permissions' (which is selected and highlighted in blue), 'Confirmation', and 'Results'. The main content area contains a descriptive text about share permissions and a table showing current permissions. A 'Customize permissions...' button is at the bottom of the table. At the bottom right are buttons for '< Previous', 'Next >', 'Create', and 'Cancel'.

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and fil...
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

Customize permissions...

< Previous    Next >    Create    Cancel

Click on the **Create** button on the **Confirmation** tab.

The screenshot shows the 'New Share Wizard' window with the title 'Confirm selections'. The sidebar shows tabs: 'Select Profile', 'Share Location', 'Share Name', 'Other Settings', 'Permissions', 'Confirmation' (selected and highlighted in blue), and 'Results'. The main content area displays a summary of share settings. A large button at the bottom right says 'Create'.

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

<b>SHARE LOCATION</b>	
Server:	HYDRA-DC
Cluster role:	Not Clustered
Local path:	C:\hackme
<b>SHARE PROPERTIES</b>	
Share name:	hackme
Protocol:	SMB
Access-based enumeration:	Disabled
Caching:	Enabled
BranchCache:	Disabled
Encrypt data:	Disabled

Create

The screenshot shows the "New Share Wizard" dialog box. At the top right are buttons for "< Previous", "Next >", "Create", and "Cancel". On the left, a vertical navigation bar lists steps: "Select Profile", "Share Location", "Share Name", "Other Settings", "Permissions", "Confirmation", and "Results". The "Results" step is highlighted with a blue background. In the main area, the message "The share was successfully created." is displayed above a table. The table has columns "Task", "Progress", and "Status". It contains two rows: "Create SMB share" (Completed) and "Set SMB permissions" (Completed). At the bottom right of the dialog are buttons for "< Previous", "Next >", "Close", and "Cancel".

## Creating Domain Users

Let's create a few domain users now. Launch the Server Manager and click on the **Active Directory Users and Computers** menu option as shown below.

The screenshot shows the "Server Manager" dashboard. The top navigation bar includes "Manage", "Tools", "View", and "Help". A sidebar on the left lists "Storage Services" and "QUICK START" options like "Configure this local server", "Add roles and features", "Add other servers to manage", "Create a server group", and "Connect this server to cloud services". Below this is a section titled "ROLES AND SERVER GROUPS" showing roles: AD CS (1), AD DS (1), DNS (1), File and Storage Services (1), Local Server (1), and others. On the right, a vertical menu under "Tools" has "Active Directory Users and Computers" highlighted with a red box. Other options include "Active Directory Administrative Center", "Active Directory Domains and Trusts", "Active Directory Module for Windows PowerShell", "Active Directory Sites and Services", "ADSI Edit", "Certification Authority", "Component Services", "Computer Management", "Defragment and Optimize Drives", "Disk Cleanup", "DNS", "Event Viewer", "Group Policy Management", "iSCSI Initiator", "Local Security Policy", "Microsoft Azure Services", "ODBC Data Sources (32-bit)", "ODBC Data Sources (64-bit)", "Performance Monitor", "Print Management", "Recovery Drive", "Registry Editor", "Resource Monitor", "Services", "System Configuration", and "System Information".

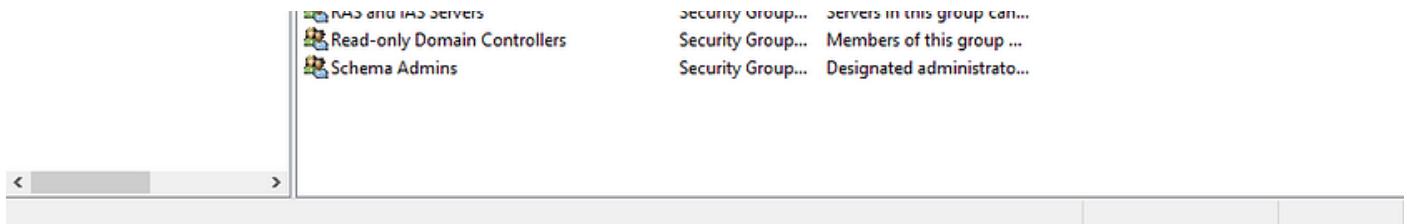


This will launch the **Active Directory Users and Computer** application as shown below. Its shown the **MARVEL.local** domain.

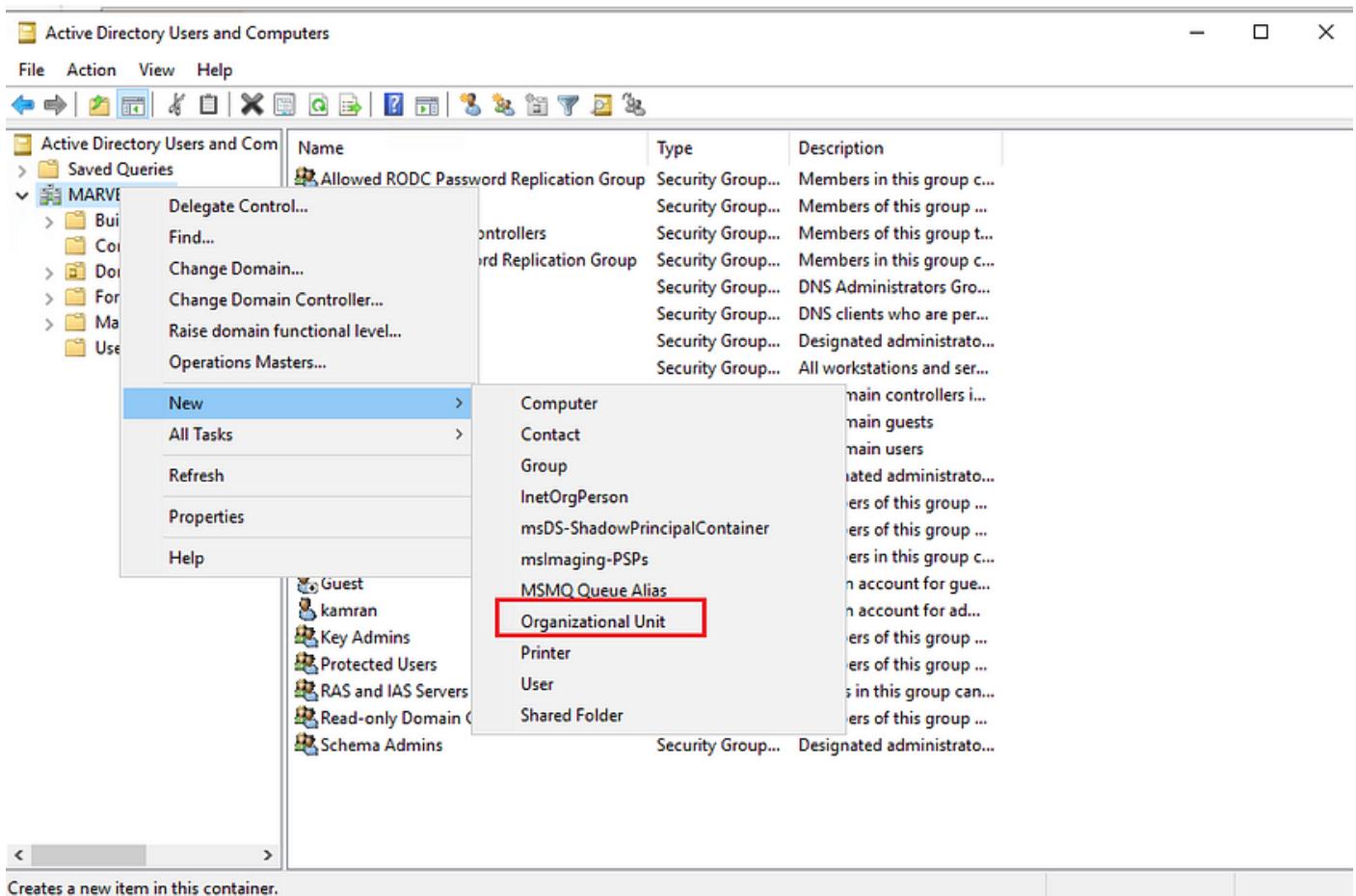
A screenshot of the Active Directory Users and Computers application window. The title bar says "Active Directory Users and Computers". The menu bar includes File, Action, View, Help. The toolbar has various icons for navigation and management. The left pane shows the navigation tree: Active Directory Users and Com, Saved Queries, MARVEL.local (expanded), Builtin, Computers, Domain Controllers, ForeignSecurityPrincipal, Managed Service Account, and Users. The main pane has three columns: Name, Type, and Description. The description column displays the message "There are no items to show in this view." A status bar at the bottom shows navigation controls and the path "D:\Windows\system32\dsa.msc".

Click on the **Users** node. Let's clean up the entries here a little for ease of management.

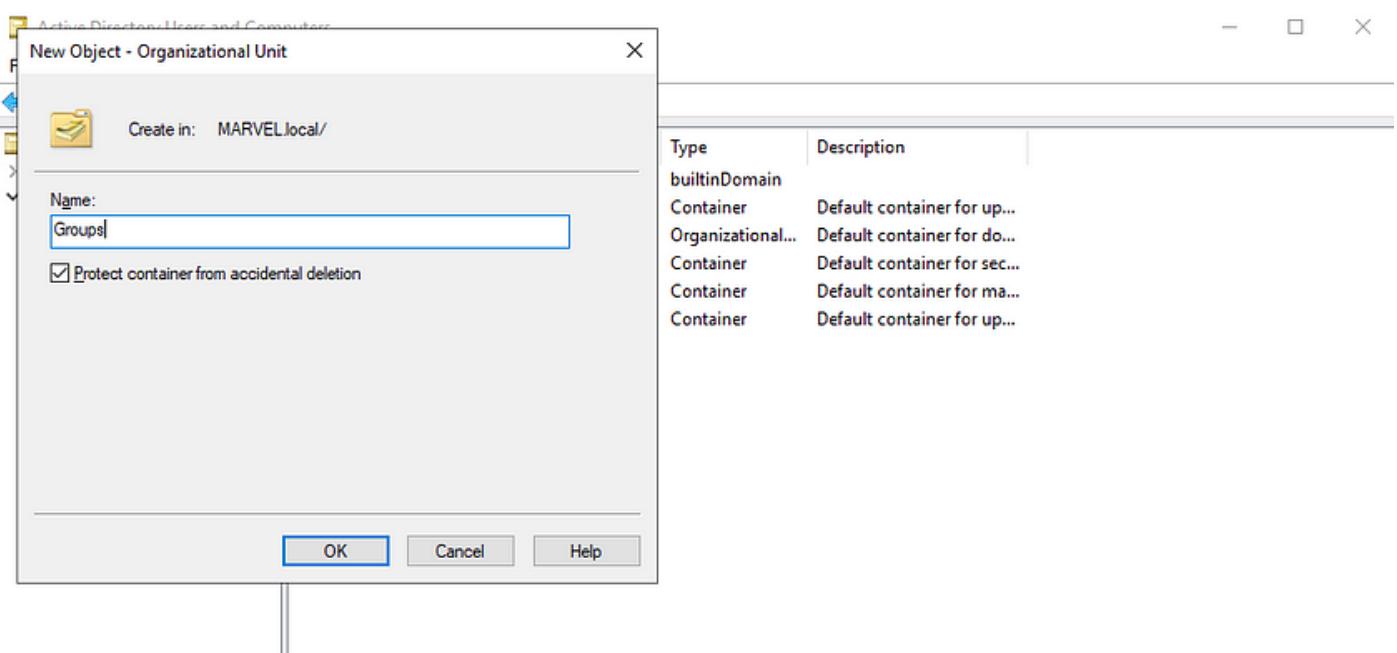
A screenshot of the Active Directory Users and Computers application window, similar to the previous one but with the "Users" node selected in the navigation tree. The main pane now displays a list of objects under the "Users" node. The columns are Name, Type, and Description. The list includes: Allowed RODC Password Replication Group (Security Group...), Cert Publishers (Security Group...), Cloneable Domain Controllers (Security Group...), Denied RODC Password Replication Group (Security Group...), DnsAdmins (Security Group...), DnsUpdateProxy (Security Group...), Domain Admins (Security Group...), Domain Computers (Security Group...), Domain Controllers (Security Group...), Domain Guests (Security Group...), Domain Users (Security Group...), Enterprise Admins (Security Group...), Enterprise Key Admins (Security Group...), Enterprise Read-only Domain Controllers (Security Group...), Group Policy Creator Owners (Security Group...), Guest (User), kamran (User), Key Admins (Security Group...), Protected Users (Security Group...), and DAC LUIDs Cache (Security Group...). The status bar at the bottom shows the path "D:\Windows\system32\dsa.msc".



Right-click on MARVEL.local node and select menu option for creating a new Organization Unit (OU) as shown below.



Following dialog will be prompted. Let's name this OU as **Groups**.

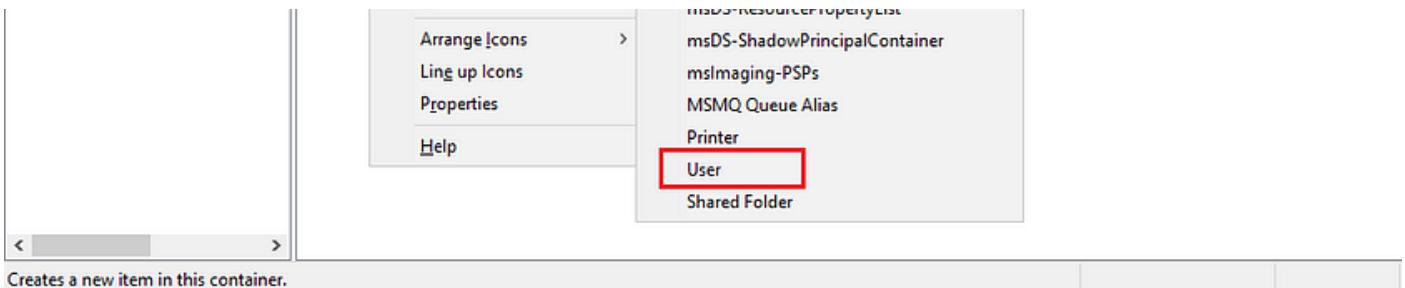


With the exception of **Guest** and **kamran** users, let's move all others into the newly created **Groups** OU by drag & drop. The Users node should look as follows after that.

The screenshot shows the Active Directory Users and Computers console. The left pane displays the navigation tree under 'MARVEL.local' with 'Users' selected. The right pane lists two users: 'Guest' (User, Description: 'Built-in account for gue...') and 'kamran' (User, Description: 'Built-in account for ad...').

Right-click and select the option for creating a new user.

The screenshot shows the Active Directory Users and Computers console with the 'Users' folder selected in the navigation tree. A context menu is open, and the 'New' option is highlighted with a red box. A secondary submenu is displayed, listing 'Computer', 'Contact', 'Group', 'InetOrgPerson', 'msDS-KeyCredential', and 'msDNCR-ResourceDescriptorList'.



Let's create the first user with First name **Frank**, Last name **Castle** and logon name as **fcastle** as shown below. Click on Next.

New Object - User

Create in: MARVEL.local/Users

First name:  Initials:   
Last name:   
Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back  Cancel

I used a kind of weak password **Password1**. Uncheck **User must change password at next logon** and check the option for **Password never expires**. Click Next.

New Object - User

Create in: MARVEL.local/Users

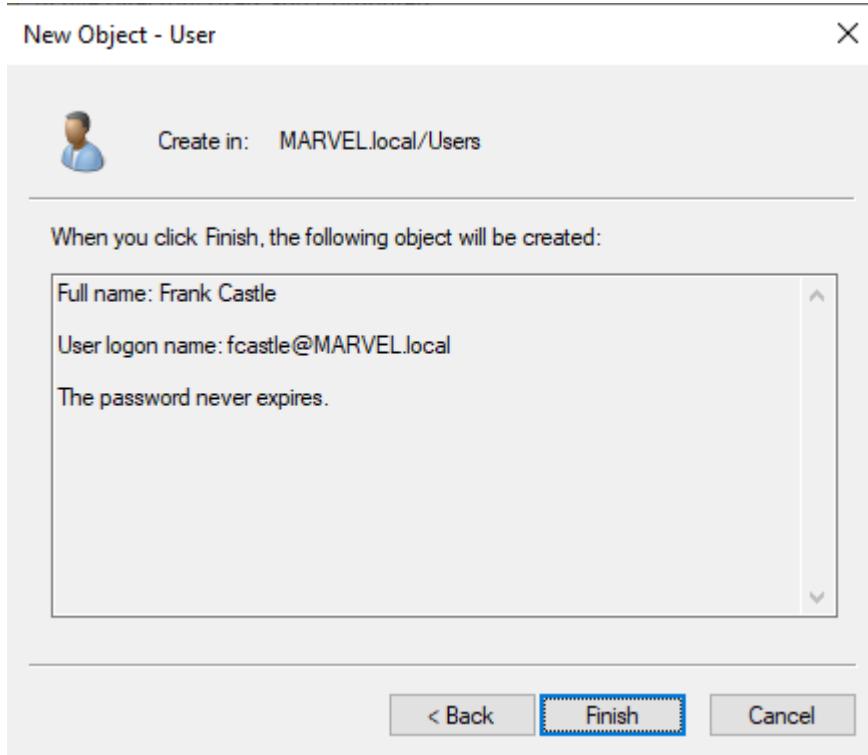
Password:

Confirm password:

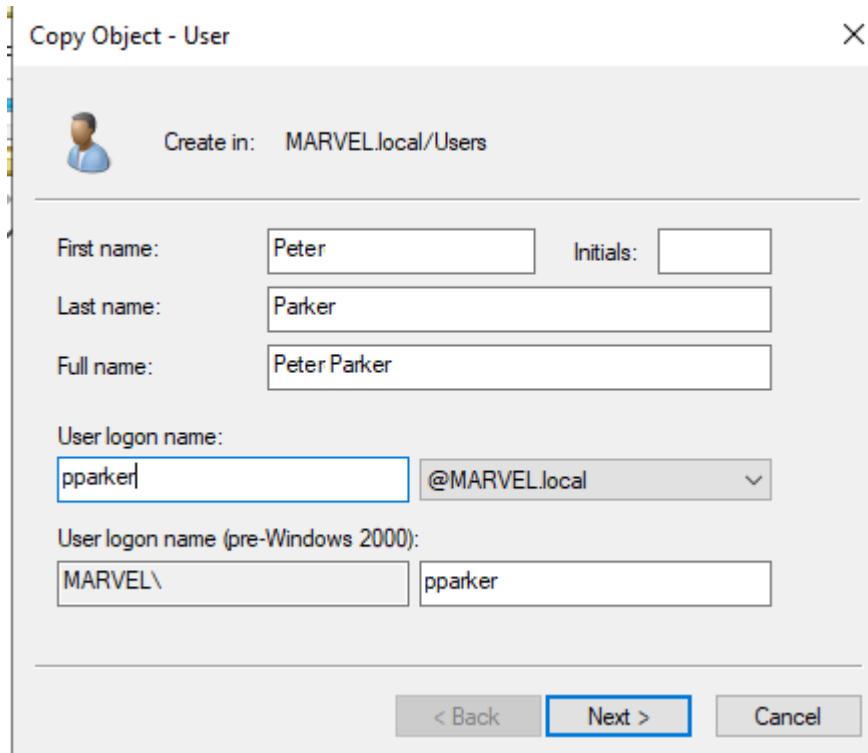
User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

< Back  Cancel

Click Finish here.



Repeat same steps to create another user with First name **Peter**, Last name **Parker** and logon name as **pparker** as shown below. I used the same password **Password1** for this user as well.



Finally, create a domain-admin type user. For that, we just copy the existing admin user **kamran** by right-clicking on its username and click on the **Copy...** menu option as shown below.



The screenshot shows the Windows Active Directory Users and Computers interface. On the left, a tree view shows 'Active Directory Users and Computers', 'Saved Queries', and a 'MARVEL.local' container with subfolders like 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', 'Users', and 'Groups'. The 'Users' folder is selected. On the right, a list of users is displayed with columns for 'Name', 'Type', and 'Description'. The 'kamran' user is selected and highlighted with a red box around the 'Copy...' option in the context menu. Other options in the menu include 'Add to a group...', 'Disable Account', 'Reset Password...', 'Move...', 'Open Home Page', 'Send Mail', 'All Tasks', 'Cut', 'Delete', 'Rename', 'Properties', and 'Help'. A status bar at the bottom says 'Disables the account for the current selection.'

Let's give this user first name **SQL**, last name **Service** and logon name of **SQLService**. Click Next then.

Copy Object - User X

Create in: MARVEL.local/Users

First name:  Initials:

Last name:

Full name:

User logon name:  @MARVEL.local

User logon name (pre-Windows 2000):

< Back Next > Cancel

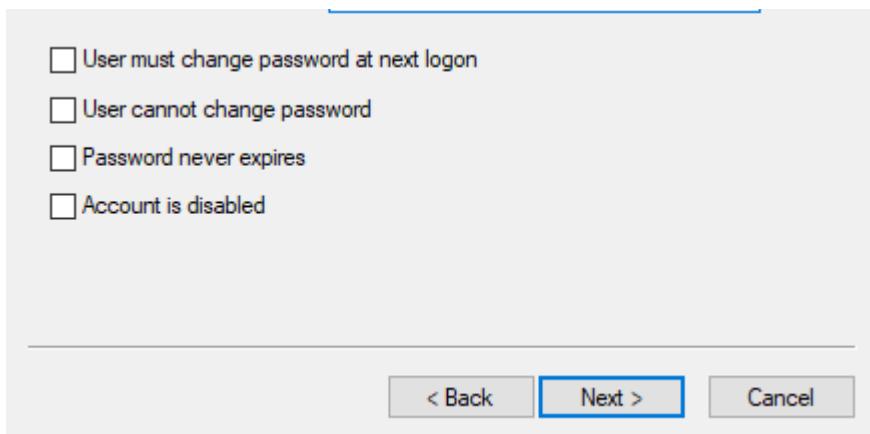
Let's set the password for this user as **MYpassword123#** with settings as shown below. Click Next then.

Copy Object - User X

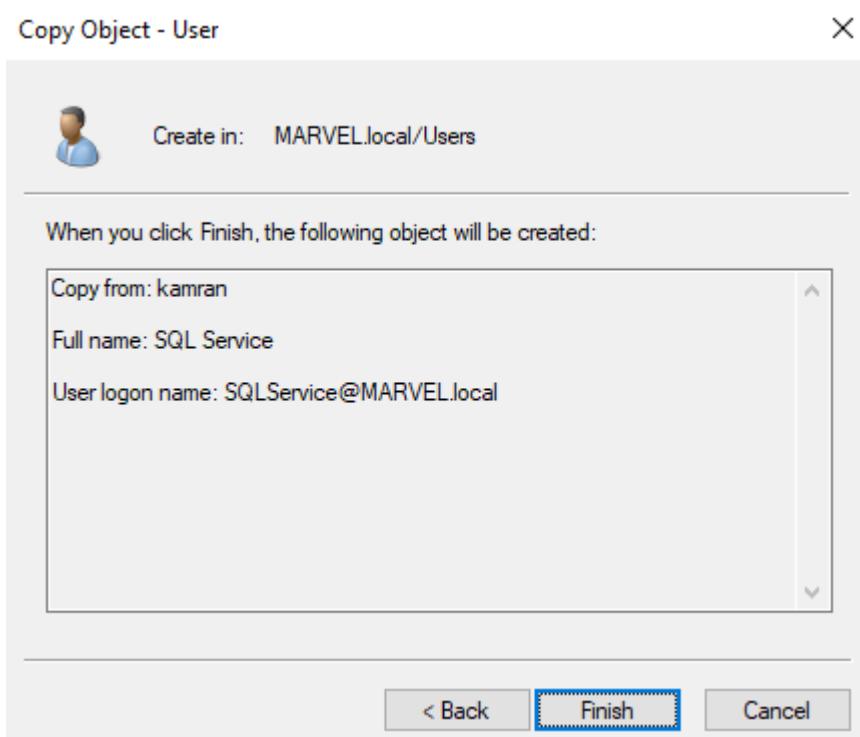
Create in: MARVEL.local/Users

Password:

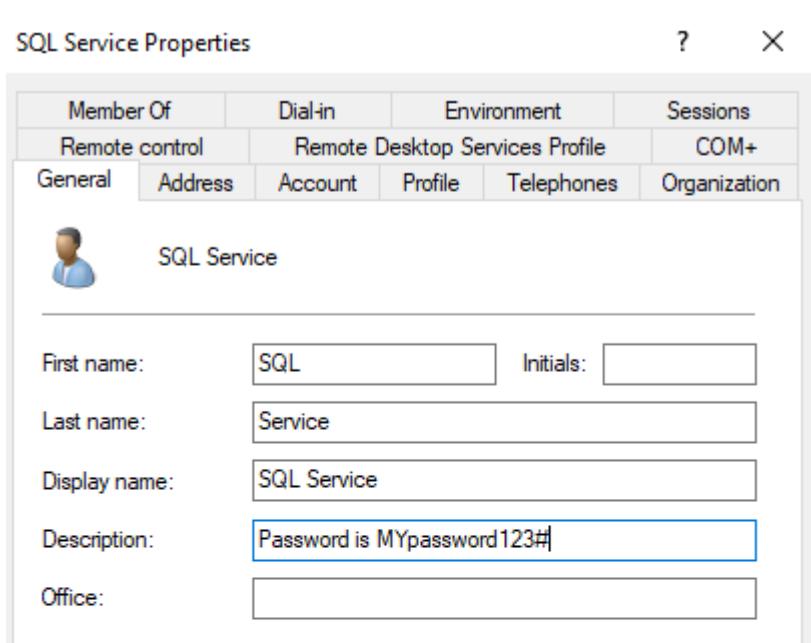
Confirm password:

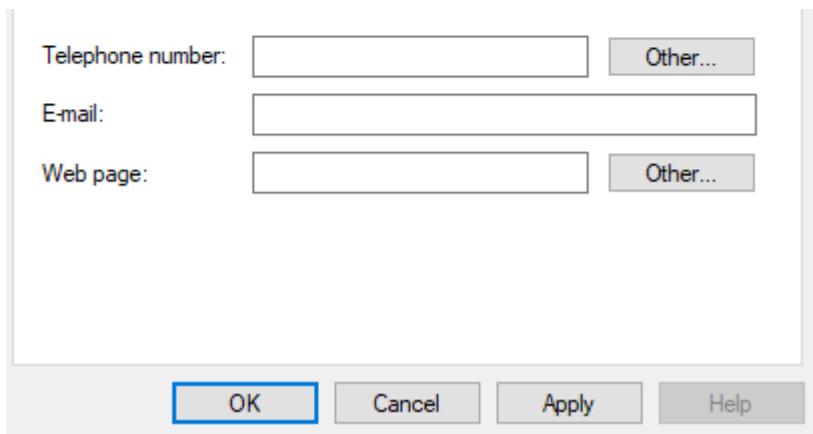


Click Finish here.



Go back on the properties for SQLService user and set Description as Password is **MYpassword123#** as shown below.





Let's set up the [Service Principal Names](#) (SPN) for the SQLService account using `setspn` utility.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.914]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\kamran>setspn -a HYDRA-DC/SQLService.MARVEL.local:60111 MARVEL\SQLService
Checking domain DC=MARVEL,DC=local

Registering ServicePrincipalNames for CN=SQL Service,CN=Users,DC=MARVEL,DC=local
    HYDRA-DC/SQLService.MARVEL.local:60111
Updated object
```

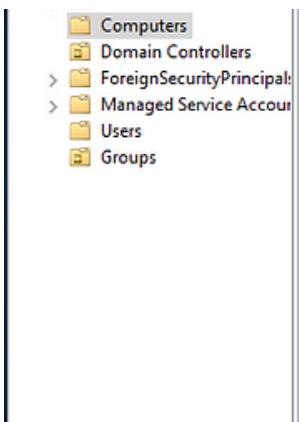
We can run `setspn` again to confirm the domain for existing SPN as shown below.

```
Administrator: Command Prompt
C:\Users\kamran>setspn -T MARVEL.local -Q */
Checking domain DC=MARVEL,DC=local
CN=HYDRA-DC,OU=Domain Controllers,DC=MARVEL,DC=local
  Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/HYDRA-DC.MARVEL.local
  ldap/HYDRA-DC.MARVEL.local/ForestDnsZones.MARVEL.local
  ldap/HYDRA-DC.MARVEL.local/DomainDnsZones.MARVEL.local
  TERMSRV/HYDRA-DC
  TERMSRV/HYDRA-DC.MARVEL.local
  DNS/HYDRA-DC.MARVEL.local
  GC/HYDRA-DC.MARVEL.local/MARVEL.local
  RestrictedKrbHost/HYDRA-DC.MARVEL.local
  RestrictedKrbHost/HYDRA-DC
  RPC/4845b522-46e3-49d9-8dc6-a40dd174f60e._msdcs.MARVEL.local
  HOST/HYDRA-DC/MARVEL
  HOST/HYDRA-DC.MARVEL.local/MARVEL
  HOST/HYDRA-DC
  HOST/HYDRA-DC.MARVEL.local
  HOST/HYDRA-DC.MARVEL.local/MARVEL.local
  E3514235-4B06-11D1-AB04-00C04FC2DCD2/4845b522-46e3-49d9-8dc6-a40dd174f60e/MARVEL.local
  ldap/HYDRA-DC/MARVEL
  ldap/4845b522-46e3-49d9-8dc6-a40dd174f60e._msdcs.MARVEL.local
  ldap/HYDRA-DC.MARVEL.local/MARVEL
  ldap/HYDRA-DC
  ldap/HYDRA-DC.MARVEL.local
  ldap/HYDRA-DC.MARVEL.local/MARVEL.local
CN=krbtgt,CN=Users,DC=MARVEL,DC=local
  kadmin/changepw
CN=SQL Service,CN=Users,DC=MARVEL,DC=local
  HYDRA-DC/SQLService.MARVEL.local:60111

Existing SPN found!
```

This basically completes the creation of domain users and required configuration. As of now, no computers have joined the domain.

Name	Type	Description
There are no items to show in this view.		



Important to note the IP address of the domain machine as this will be used when joining user computers to the domain.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.914]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\kamran>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : vxl0vxmt3duuheiftc1cahbrsa.ux.internal.cloudapp.net
  Link-local IPv6 Address . . . . . : fe80::d024:c02a:7aa1:3a2a%6
  IPv4 Address. . . . . : 10.0.1.4
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.1.1
```

## Setting up first User Machine

Let's start setting up our first user machine. Under the Virtual machines page, click on the **Add** button.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and a user profile. Below it, the 'Virtual machines' section is active. A red box highlights the '+ Add' button. The page displays a table of existing virtual machines, with one entry for 'HYDRA-DC' shown. The table columns include Name, Type, Status, Resource group, Location, Source, Maintenance status, and Subscription.

Name	Type	Status	Resource group	Location	Source	Maintenance status	Subscription
HYDRA-DC	Virtual machine	Running	ADLab	Canada Central	Marketplace	-	Free Trial

Enter all the information about this virtual machine. Here are the key points.

Select **ADLab** as Resource Group

Set machine name as **ThePunisher**

Choose **Windows 10 Enterprise Version 1909** image.

Choose **Standard B1s** machine size

Name username as **fcastle**. Give it a weak password. I use **myPassword01**

Microsoft Azure

Home > Virtual machines > Create a virtual machine

**Virtual machines** Default Directory

+ Add Reservations ...

Filter by name... Name ↑ HYDRA-DC ...

**Create a virtual machine**

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for classic VMs? [Create VM from Azure Marketplace](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Free Trial

Resource group \* ADLab [Create new](#)

**Instance details**

Virtual machine name \* ThePunisher

Region \* (Canada) Canada Central

Availability options No infrastructure redundancy required

Image \* Windows 10 Enterprise, Version 1909 [Browse all public and private images](#)

Azure Spot instance No

Size \* Standard B1s  
1 vcpu, 1 GiB memory (\$11.05/month) [Change size](#)

**Administrator account**

Username \* fcastle

Password \* \*\*\*\*\*

[Review + create](#) < Previous Next : Disks >

The screenshot shows the 'Create a virtual machine' wizard on the 'Basics' tab. The 'Virtual machine name' field is highlighted with a red box and contains 'ThePunisher'. The 'Region' dropdown shows '(Canada) Canada Central'. The 'Image' dropdown shows 'Windows 10 Enterprise, Version 1909'. The 'Size' dropdown shows 'Standard B1s' with a note about 1 vcpu, 1 GiB memory, and a monthly price of \$11.05. The 'Administrator account' section shows 'fcastle' in the 'Username' field and a masked password. Navigation buttons at the bottom include 'Review + create', '< Previous', and 'Next : Disks >'.

Choose **Standard HDD** for this VM as well.

Microsoft Azure

Home > Virtual machines > Create a virtual machine

**Virtual machines** Default Directory

+ Add Reservations ...

Filter by name... Name ↑ HYDRA-DC ...

**Create a virtual machine**

Basics Disks Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

**Disk options**

OS disk type \* Standard HDD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Enable Ultra Disk compatibility No

Ultra Disk compatibility is not available for this VM size and location.

**Data disks**

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

[Create and attach a new disk](#) [Attach an existing disk](#)

**Advanced**

The screenshot shows the 'Create a virtual machine' wizard on the 'Disks' tab. The 'OS disk type' dropdown is highlighted with a red box and shows 'Standard HDD'. A note below explains that the selected VM size supports premium disks and recommends Premium SSD for high IOPS workloads. The 'Enable Ultra Disk compatibility' radio button is set to 'No'. Navigation buttons at the bottom include '< Previous', 'Next : Advanced >', and 'Review + create'.

[Review + create](#)

[< Previous](#)

[Next : Networking >](#)

Make sure this VM is also using the **ADLabNet** Virtual network. For the rest of the options, just use defaults and click on the **Review + create** button.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal, specifically the 'Networking' tab. On the left, there's a sidebar for 'Virtual machines' with a list of existing VMs including 'HYDRA-DC'. The main area has tabs for Basics, Disks, Networking (which is selected), Management, Advanced, Tags, and Review + create. Under the Networking tab, it says: 'Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.' A note below says: 'Learn more'. The 'Virtual network' dropdown is set to 'ADLabNet' (highlighted with a red box). The 'Subnet' dropdown is set to 'default (10.0.1.0/24)'. The 'Public IP' dropdown is set to '(new) ThePunisher-ip'. Under 'NIC network security group', the 'Basic' radio button is selected. Under 'Public inbound ports', the 'Allow selected ports' radio button is selected, and 'RDP (3389)' is listed. A warning message in an orange box says: '⚠️ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.' Below this, under 'Accelerated networking', the 'Off' radio button is selected. A note says: 'The selected image does not support accelerated networking.' Under 'Load balancing', it says: 'You can place this virtual machine in the backend pool of an existing Azure load balancing solution.' A note below says: 'Learn more'. Under 'Place this virtual machine behind an existing load balancing solution?', the 'No' radio button is selected. At the bottom, there are buttons for 'Review + create', '< Previous', and 'Next : Management >'.

You should see a message about validations succeeded. Click on **Create** button here.

The screenshot shows the 'Create a virtual machine' wizard again, but now the validation has passed. A green bar at the bottom displays a green checkmark icon and the text 'Validation passed'. The rest of the interface is identical to the previous screenshot, showing the 'Networking' tab with the 'ADLabNet' virtual network selected.

Filter by name...

Basics	Disks	Networking	Management	Advanced	Tags	Review + create																						
<b>PRODUCT DETAILS</b>																												
Standard B1s	Subscription credits apply ⓘ																											
by Microsoft	0.0148 CAD/hr																											
<a href="#">Terms of use</a>   <a href="#">Privacy policy</a>	<a href="#">Pricing for other VM sizes</a>																											
<b>TERMS</b>																												
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the <a href="#">Azure Marketplace Terms</a> for additional details.																												
<b>⚠ You have set RDP port(s) open to the internet.</b> This is only recommended for testing. If you want to change this setting, go back to Basics tab.																												
<b>Basics</b> <table border="1"> <tr> <td>Subscription</td> <td>Free Trial</td> </tr> <tr> <td>Resource group</td> <td>ADLab</td> </tr> <tr> <td>Virtual machine name</td> <td>ThePunisher</td> </tr> <tr> <td>Region</td> <td>(Canada) Canada Central</td> </tr> <tr> <td>Availability options</td> <td>No infrastructure redundancy required</td> </tr> <tr> <td>Username</td> <td>fcastle</td> </tr> <tr> <td>Public inbound ports</td> <td>RDP</td> </tr> <tr> <td>Azure Spot</td> <td>No</td> </tr> <tr> <td colspan="2"><b>Disks</b></td> </tr> <tr> <td>OS disk type</td> <td>Standard HDD</td> </tr> <tr> <td>Use managed disks</td> <td>Yes</td> </tr> </table>							Subscription	Free Trial	Resource group	ADLab	Virtual machine name	ThePunisher	Region	(Canada) Canada Central	Availability options	No infrastructure redundancy required	Username	fcastle	Public inbound ports	RDP	Azure Spot	No	<b>Disks</b>		OS disk type	Standard HDD	Use managed disks	Yes
Subscription	Free Trial																											
Resource group	ADLab																											
Virtual machine name	ThePunisher																											
Region	(Canada) Canada Central																											
Availability options	No infrastructure redundancy required																											
Username	fcastle																											
Public inbound ports	RDP																											
Azure Spot	No																											
<b>Disks</b>																												
OS disk type	Standard HDD																											
Use managed disks	Yes																											
<a href="#">Create</a> < Previous    Next > <a href="#">Download a template for automation</a>																												

Shortly after you see the message that deployment is complete. You can just click on the Go to resource button to view the newly created VM.

Microsoft Azure

Home > CreateVm-MicrosoftWindowsDesktop.Windows-10-19h2--20200105001945 - Overview

CreateVm-MicrosoftWindowsDesktop.Windows-10-19h2--20200105001945 - Overview

Deployment

Search (Ctrl+ /)

Delete Cancel Redeploy Refresh

Overview

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsDesktop.Window... Start time: 1/5/2020 12:26:04 AM

Subscription: Free Trial Correlation ID: c6947723-ad52-4900-b72a-eb7c040f3a8d

Resource group: ADLab

Deployment details (Download)

Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

Go to resource

Microsoft Azure

Home > CreateVm-MicrosoftWindowsDesktop.Windows-10-19h2--20200105001945 - Overview > ThePunisher

ThePunisher Virtual machine

Search (Ctrl+ /)

Connect Start Stop Capture Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource group (change) : ADLab

Status : Running

Location : Canada Central

Subscription (change) : Free Trial

Subscription ID : 80127484-4700-4C00-BE00-000000000000

Computer name : (not available)

Azure Spot : N/A

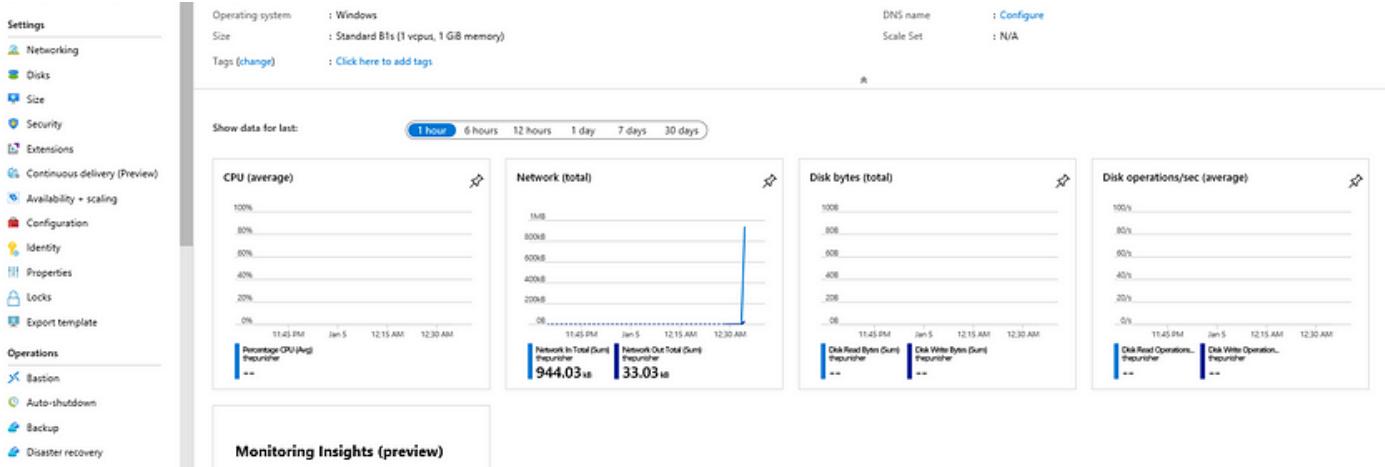
Public IP address : XXXXXXXXXX

Private IP address : 10.0.1.5

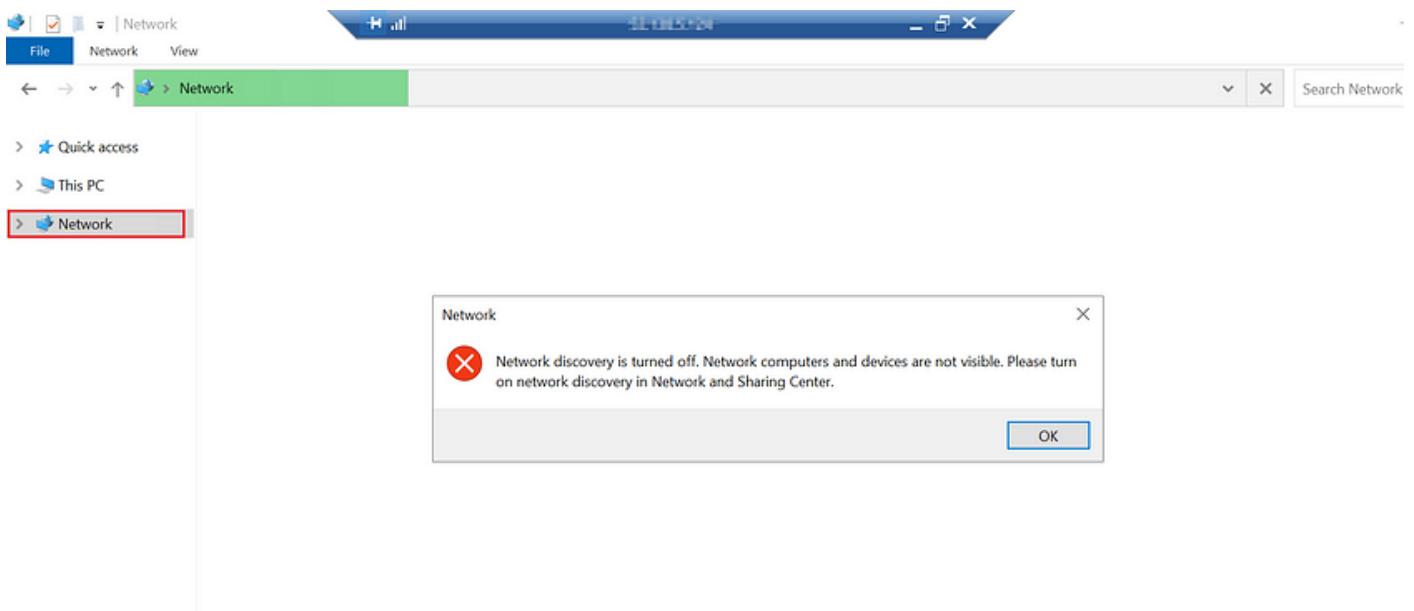
Public IP address (IPv6) : -

Private IP address (IPv6) : -

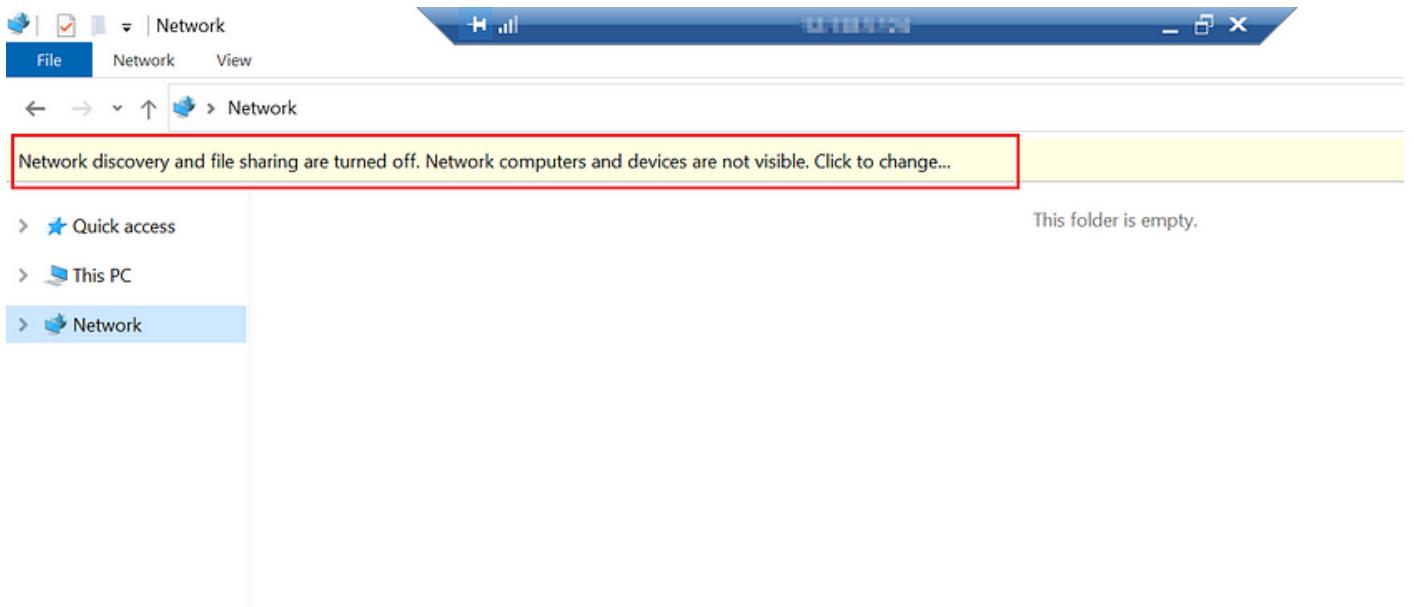
Virtual network/subnet : ADLabNet/default



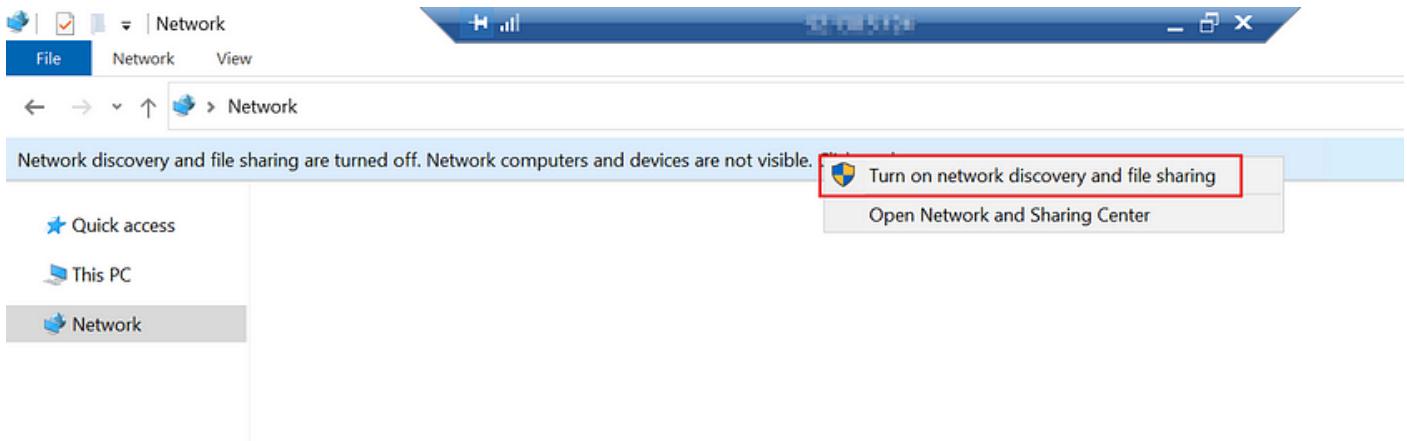
Remote Desktop into this box using the local user account we just setup **fcastle** (password **myPassword01**). Launch File Explorer and click on the **Network** node. You will be prompted with a message box stating Network Discovery is turned off. Click OK here.



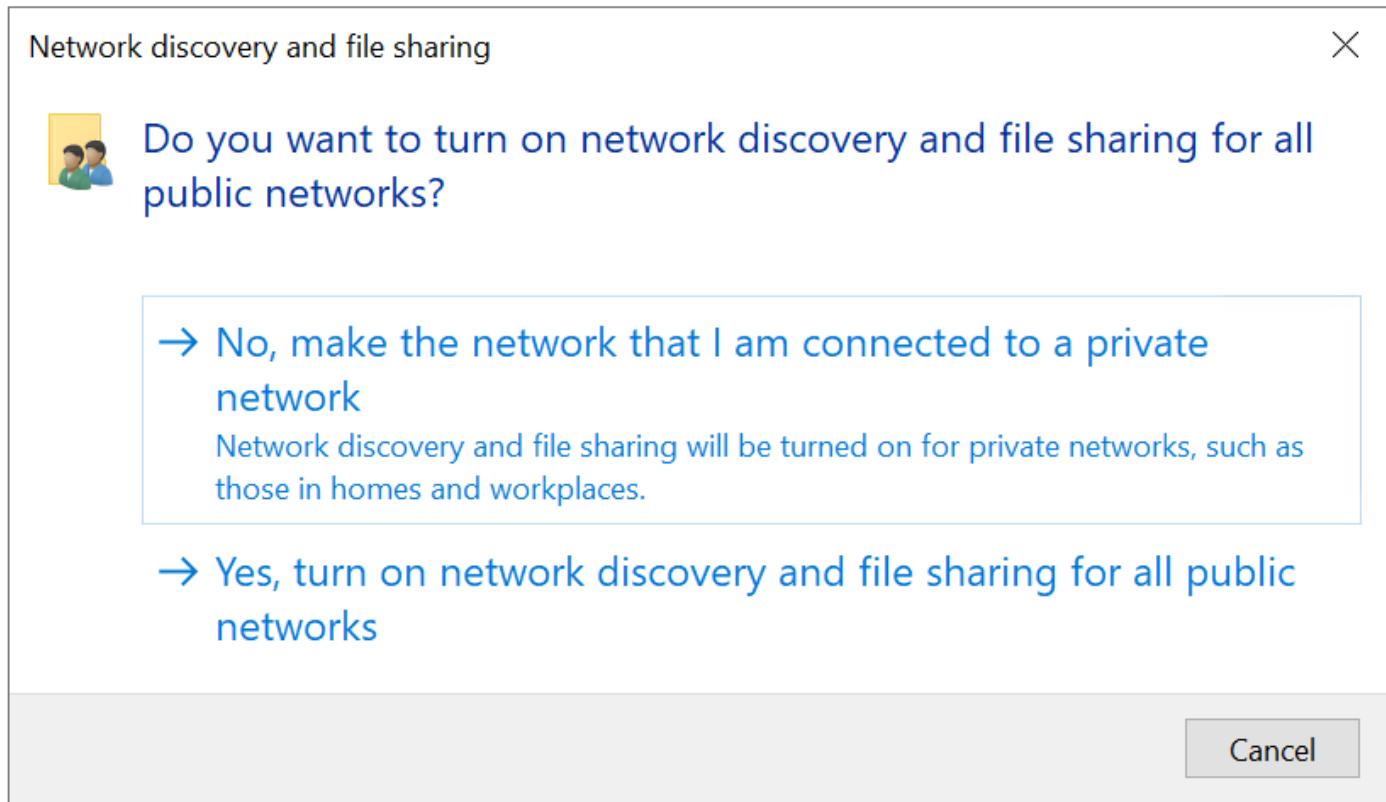
Click on the message below to change the Network discovery and file sharing settings.



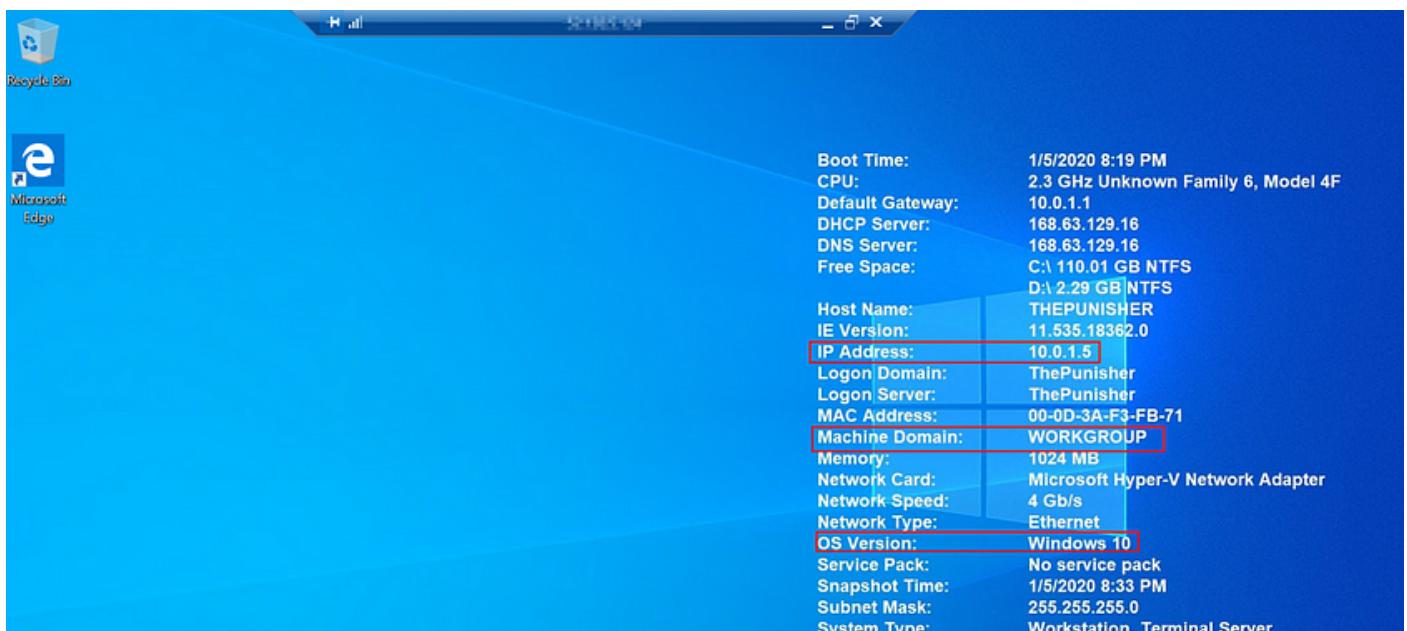
Click on **Turn on network discovery and file sharing** option.



You will be prompted with the following options. Click on the first one.



Use the Sysinternals's [BgInfo](#) utility on this box as well just like we did for the domain controller earlier.



User Name: castle  
Volumes: C:\ 126.51 GB NTFS  
D:\ 4.00 GB NTFS

## Setting up the second User Machine

The steps for creating the second User-machine are exactly the same as for the first user machine. This is also a Windows 10 Enterprise version 1909 image. I created this VM with the name **Spiderman**. For this machine, the username is **pparker** with another weak password of **myPassword02**. Repeat all the steps including those for turning on Network discovery and setting up BgInfo utility. This machine should look as follows. Some info may be different (such as IP address depending upon the setting you used etc.).



At this point, if we browse to the Virtual Machines page in the Azure portal, it should look as follows.

Name	Type	Status	Resource group	Location	Source	Maintenance status	Subscription
HYDRA-DC	Virtual machine	Running	ADLab	Canada Central	Marketplace	-	Free Trial
Spiderman	Virtual machine	Running	ADLab	Canada Central	Marketplace	-	Free Trial
ThePunisher	Virtual machine	Running	ADLab	Canada Central	Marketplace	-	Free Trial

## User Machines Join Domain

Now its time to have these machines join the domain. I will show the steps for **ThePunisher**. The same steps will have to be done on the other user machine **Spiderman**.

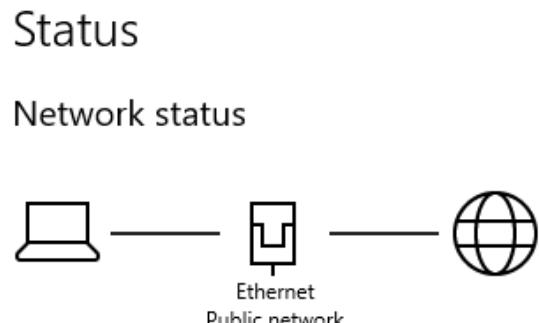
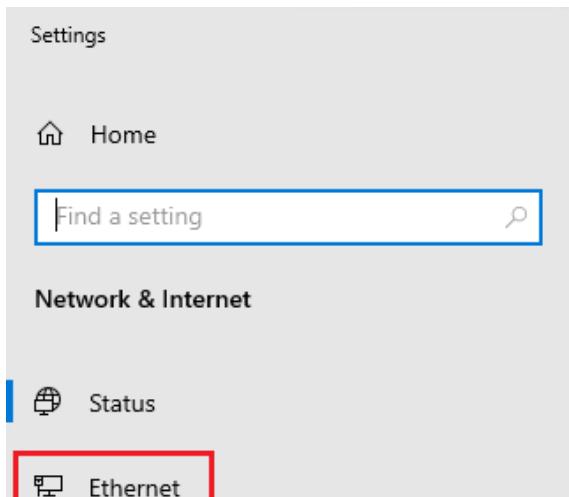
While in **ThePunisher** machine, right-click on the Network icon in the system tray. You will see two options here. Click on the **Open Network & Internet Settings** as shown below.

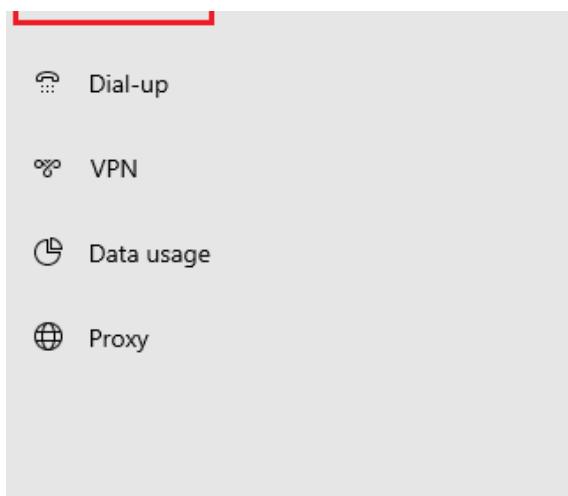
Boot Time:	1/5/2020 8:19 PM
CPU:	2.3 GHz Unknown Family 6, Model 4F
Default Gateway:	10.0.1.1
DHCP Server:	168.63.129.16
DNS Server:	168.63.129.16
Free Space:	C:\ 110.01 GB NTFS D:\ 2.29 GB NTFS
Host Name:	THEPUNISHER
IE Version:	11.535.18362.0
IP Address:	10.0.1.5
Logon Domain:	ThePunisher
Logon Server:	ThePunisher
MAC Address:	00-0D-3A-F3-FB-71
Machine Domain:	WORKGROUP
Memory:	1024 MB
Network Card:	Microsoft Hyper-V Network Adapter
Network Speed:	4 Gb/s
Network Type:	Ethernet
OS Version:	Windows 10
Service Pack:	No service pack
Snapshot Time:	1/5/2020 8:33 PM
Subnet Mask:	255.255.255.0
System Type:	Workstation, Terminal Server
User Name:	fcastle
Volumes:	C:\ 126.51 GB NTFS D:\ 4.00 GB NTFS

Troubleshoot problems

[Open Network & Internet settings](#)

This will open the **Settings** dialog. Click on the **Ethernet** item in left navigation as shown below.





If you have a limited data plan, you can make this network a metered connection or change other properties.

[Change connection properties](#)

[Show available networks](#)

## Change your network settings

[Change adapter options](#)

View network adapters and change connection settings.

Click on the **Change adapter options**.

A screenshot of the Windows Settings interface under Network &amp; Internet. The 'Ethernet' option is highlighted with a blue bar. Other options include 'Status', 'Dial-up', 'VPN', 'Data usage', and 'Proxy'. A 'Find a setting' search bar is at the top.

## Ethernet

[Network](#)  
Connected

### Related settings

[Change adapter options](#)

[Change advanced sharing options](#)

[Network and Sharing Center](#)

[Windows Firewall](#)

### Have a question?

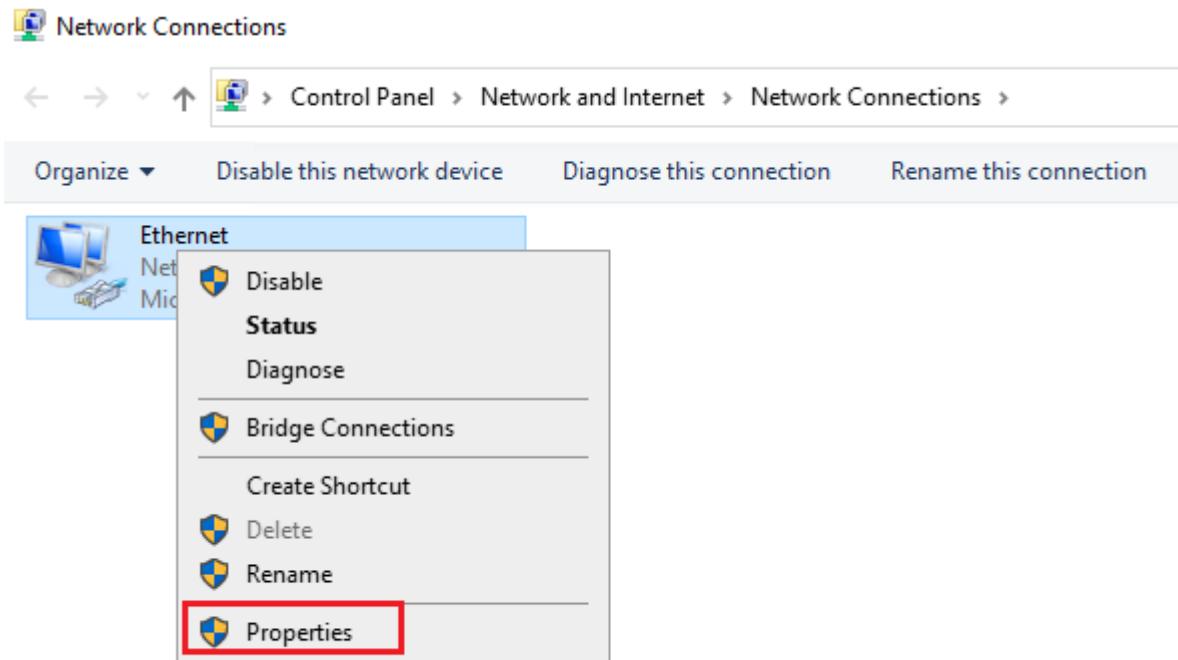
[Troubleshooting network connection issues](#)

[Get help](#)

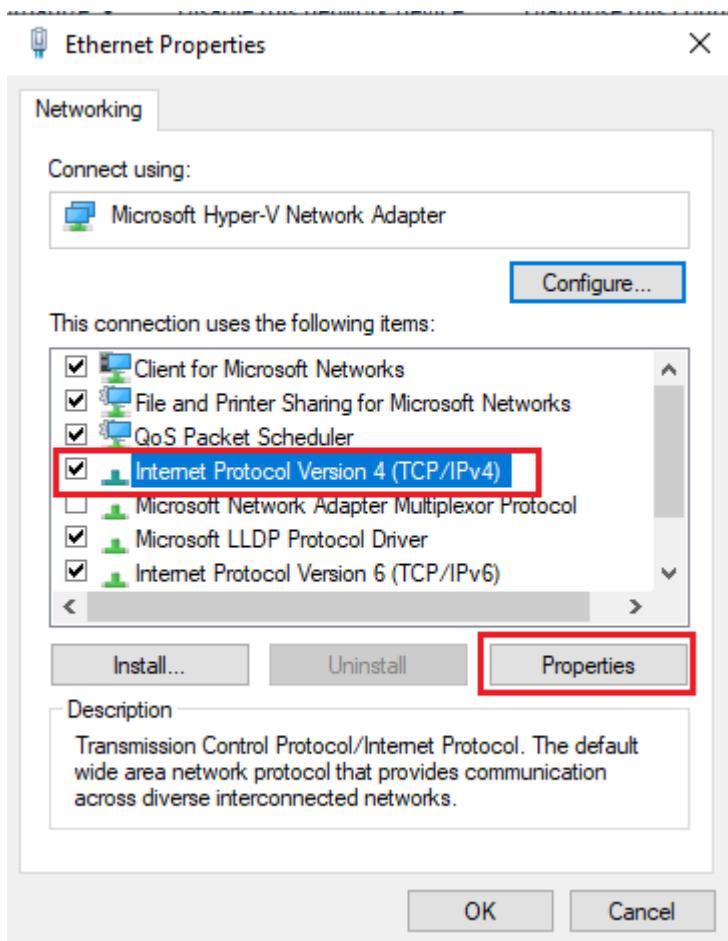
This will bring up the Network Connection dialog showing the Ethernet connection.

A screenshot of the Windows Control Panel's Network Connections window. It shows three connections: 'Ethernet' (Network icon), 'Microsoft Hyper-V Network Adapter' (Network icon), and 'Microsoft Virtual PC Host Adapter' (Network icon). The 'Ethernet' connection is listed first. The window includes a breadcrumb navigation bar and an 'Organize' dropdown menu.

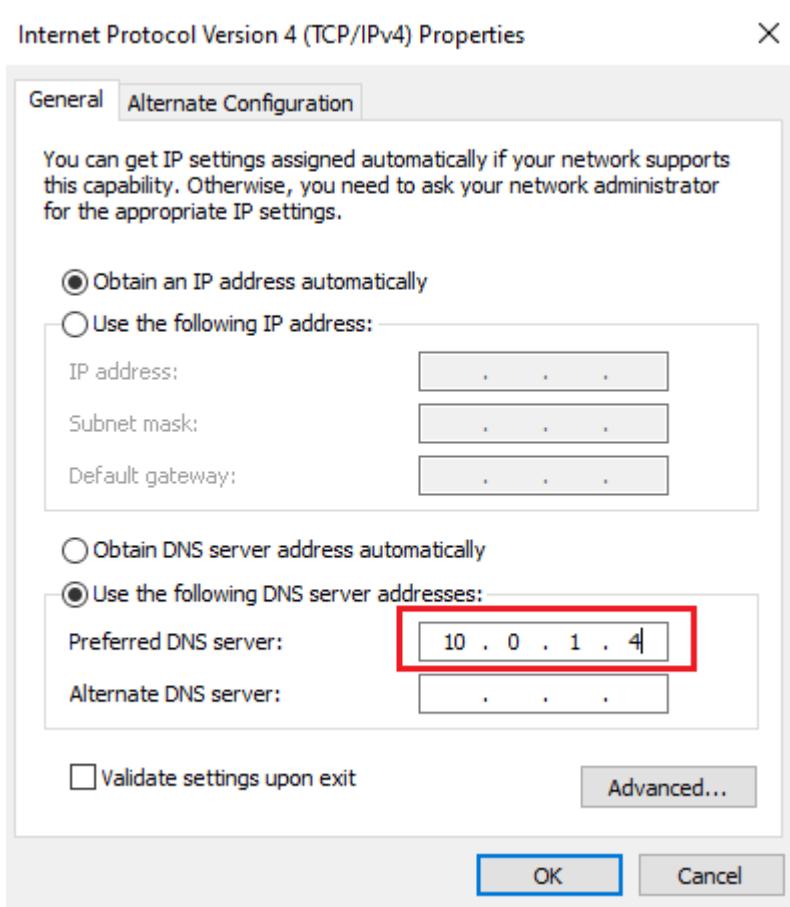
Right-click on the Ethernet and click on the properties menu item.



Select the IP4 from the list and click properties.

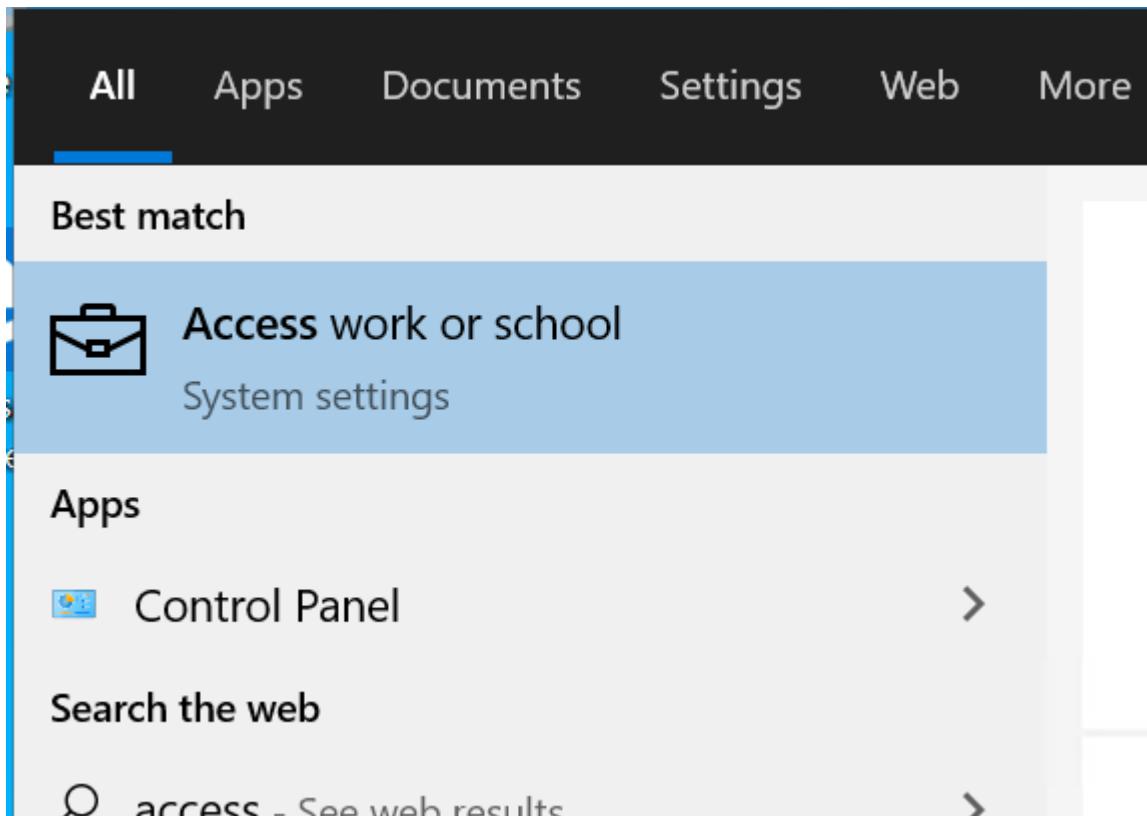


This is where we use the IP address of the domain controller (10.0.1.4 in my case) as the DNS address for this machine.



Click OK and close this dialog. At this point, my RDP connection to the VM was lost. I had to restart the VM from Azure portal and log back into the VM using the same local user account.

Find the **Access work or school** system setting and launch it.



## Settings (8+)

access|work or school

Click Connect here.

Settings

- □ ×

Home

Find a setting



Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Other users

## Access work or school

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.

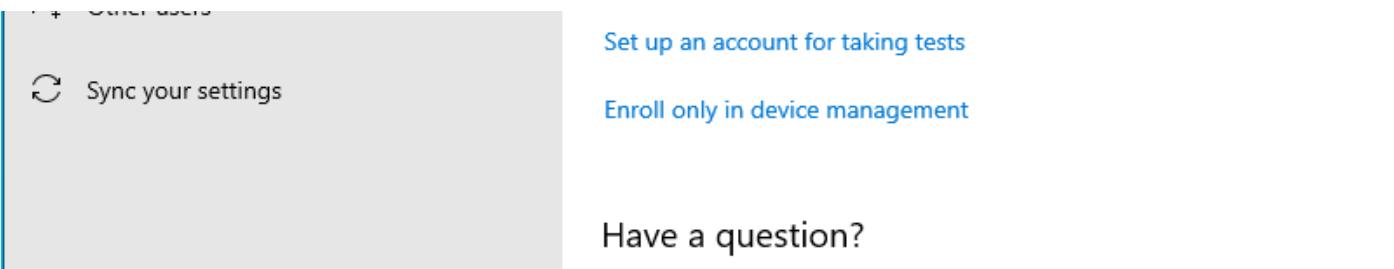


Connect

## Related settings

Add or remove a provisioning package

Export your management log files



## Have a question?

From the next dialog, click the link for **Join this device to a local Active Directory domain**.

This screenshot shows a 'Set up a work or school account' dialog. It includes a Microsoft account sign-in button, a 'Set up a work or school account' section, a note about connecting to resources, and an 'Email address' input field.

**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 Azure Active Directory](#)

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

[Next](#)

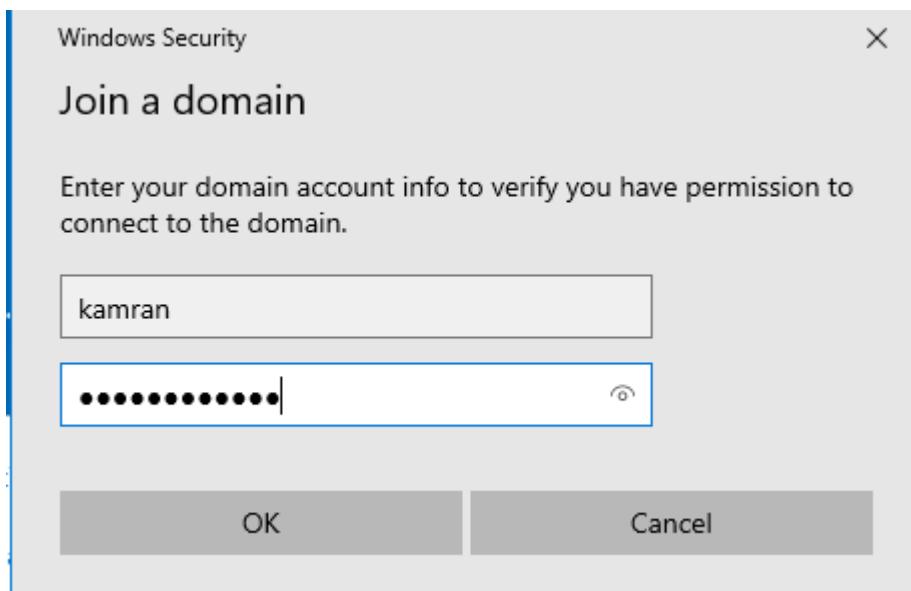
Following dialog will be prompted. Enter **MARVEL.local** as the domain name and click on Next.

This screenshot shows a 'Join a domain' dialog. It includes a 'Join a domain' button, a 'Domain name' label, and an input field containing 'MARVEL.local'.

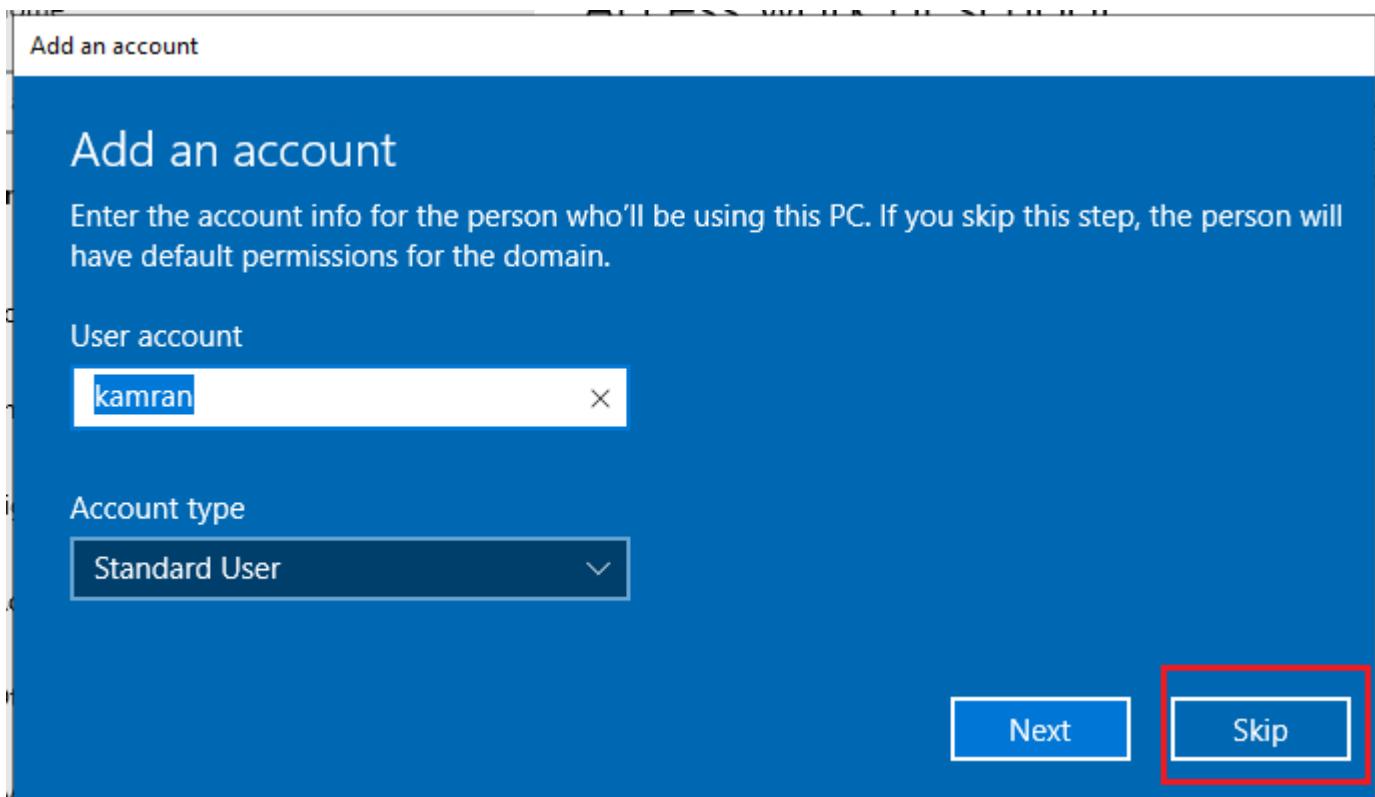
Next

Cancel

You will be prompted to enter the credentials for domain admin. In my case its **kamran** with password **Password1234**.



Click on the Skip on the next dialog.



Finally choose to **Restart now**.



## Restart your PC

After you restart, your PC will be joined to this domain: MARVEL.local

**Restart now**

**Restart later**

Now repeat the same steps for the other user machine Spiderman to have it join the domain.

At this point, if we login to the Domain Controller, we should see both the user computers listed under the **MARVEL.local** domain as shown below.

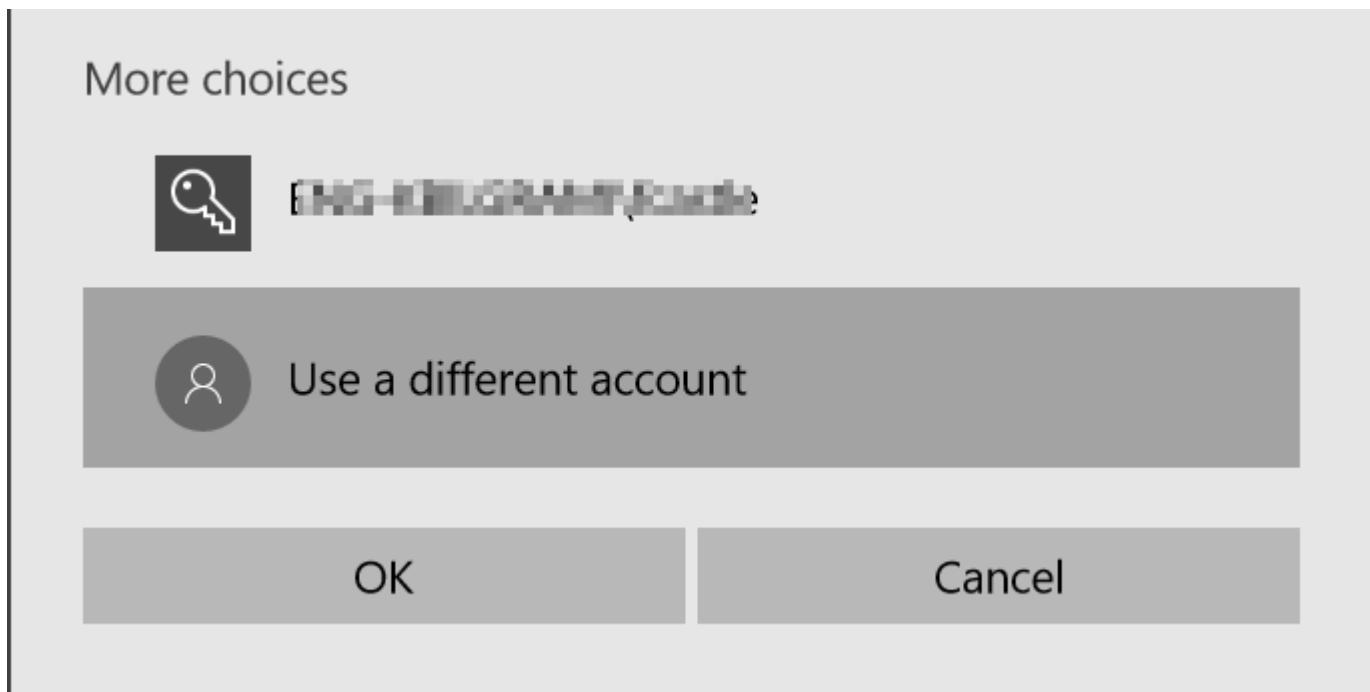
The screenshot shows the Windows Active Directory Users and Computers management console. The left navigation pane shows the tree structure: Active Directory Users and Computers > MARVEL.local > Computers. Under Computers, there are two entries: Spiderman and ThePunisher. Both are listed as Computer type. The right pane displays a table with columns: Name, Type, and Description. The Name column lists Spiderman and ThePunisher. The Type column shows Computer for both. There is no Description column present.

Name	Type	Description
Spiderman	Computer	
ThePunisher	Computer	

## Configuring Domain Users to User-Machines

We have created domain users but not yet set up these against any user machines yet. Let's login to the **ThePunisher** first as a domain administrator to do that.

The screenshot shows a Windows Security dialog box titled "Windows Security". The main instruction is "Enter your credentials". It states that these credentials will be used to connect to **192.168.0.107**. The username field contains "MARVEL\kamran" and the password field shows a redacted password. Below the fields, it says "Domain: MARVEL". At the bottom, there is a checkbox labeled "Remember me".



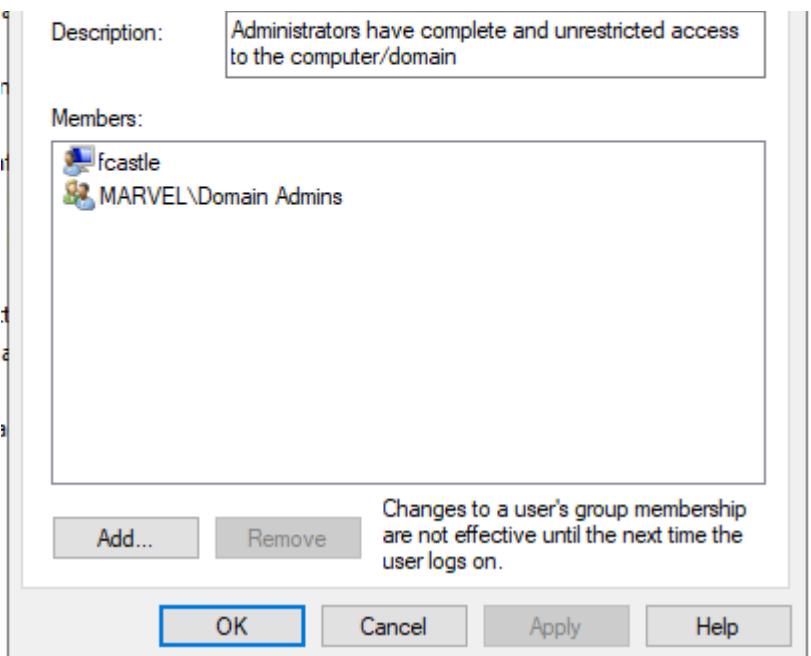
Go to Computer Management -> Groups -> Administrators and double click.

A screenshot of the Windows Computer Management snap-in. The left pane shows a tree view with "Computer Management (Local)" selected, expanded to show "System Tools", "Local Users and Groups" (which has "Users" and "Groups" children), and "Services and Applications". The "Groups" node under Local Users and Groups is selected and highlighted with a red box. The right pane displays a table of groups with columns "Name" and "Description". The "Administrators" group is selected and highlighted with a red box. Other groups listed include "Access Control Assistance Operators", "Backup Operators", "Cryptographic Operators", "Device Owners", "Distributed COM Users", "Event Log Readers", "Guests", "Hyper-V Administrators", "IIS\_IUSRS", "Network Configuration Operators", "Performance Log Users", "Performance Monitor Users", "Power Users", "Remote Desktop Users", "Remote Management Users", "Replicator", "System Managed Accounts Group", and "Users".

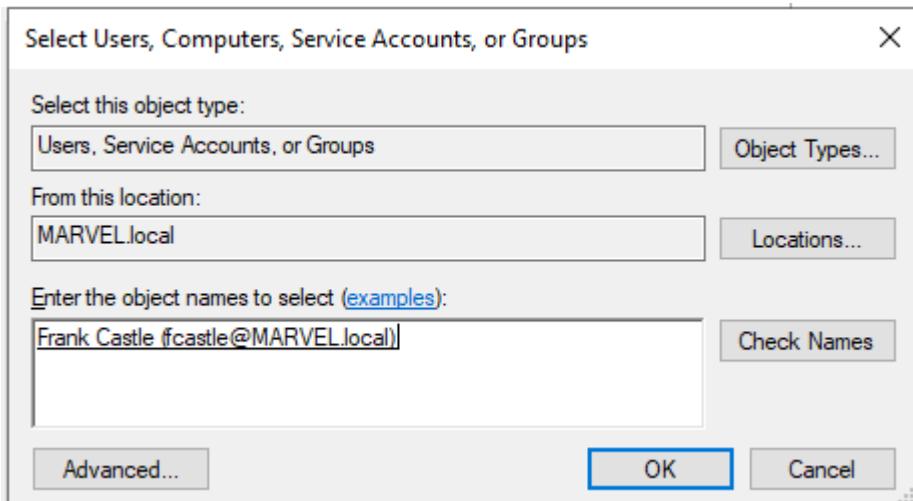
Name	Description
Access Control Assistance Operators	Members of this group can remot...
<b>Administrators</b>	<b>Administrators have complete an...</b>
Backup Operators	Backup Operators can override se...
Cryptographic Operators	Members are authorized to perform...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuration Operators	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor Users	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management Users	Members of this group can acces...
Replicator	Supports file replication in a dom...
System Managed Accounts Group	Members of this group are mana...
Users	Users are prevented from making ...

It will show existing users in this group. Click **Add** here.

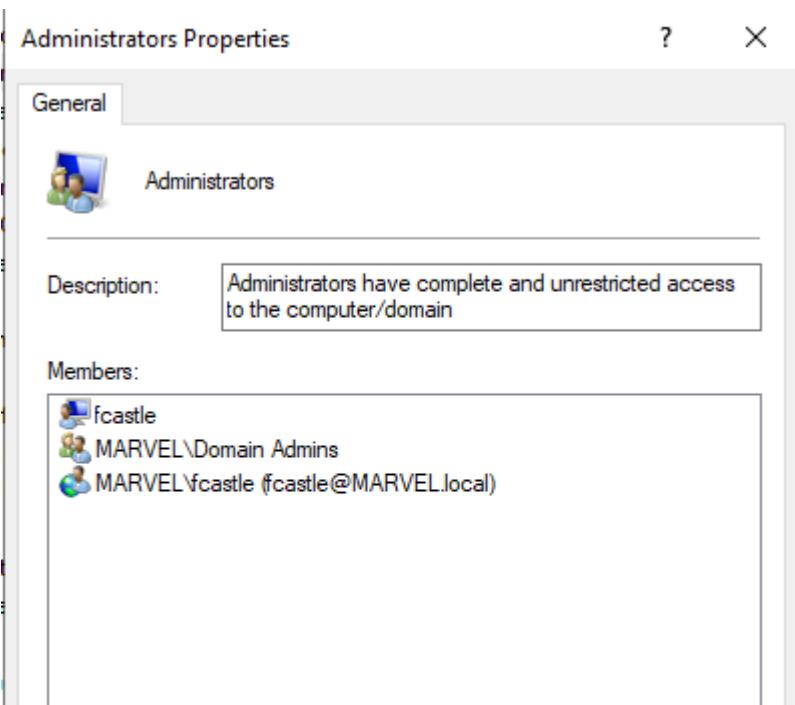
A screenshot of the "Administrators Properties" dialog box. The title bar says "Administrators Properties". Below it is a toolbar with a question mark icon and a close button. The main area is titled "General". It shows a thumbnail of a user icon and the text "Administrators".

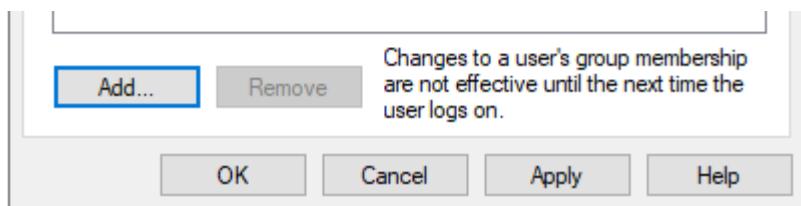


Find **Frank Castle** domain user and click on OK button.

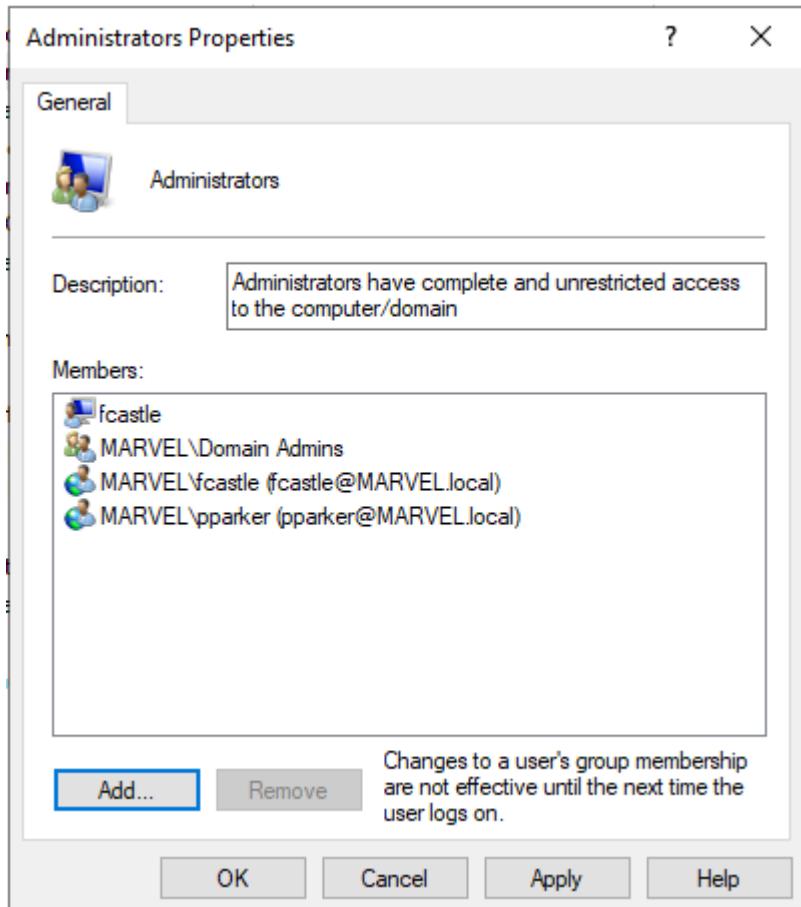


This will add that user as local Administrator.





Repeat the same steps for domain user Petre Parker.



Let's login to the **spiderman** machine as a domain administrator and add the **MARVEL\pparker** as the local admin.

Computer Management

File Action View Help

System Tools

- Task Scheduler
- Event Viewer
- Shared Folders
- Local Users and Groups
  - Users
  - Groups
- Performance
- Device Manager

Storage

- Disk Management

Services and Applications

Administrators Properties

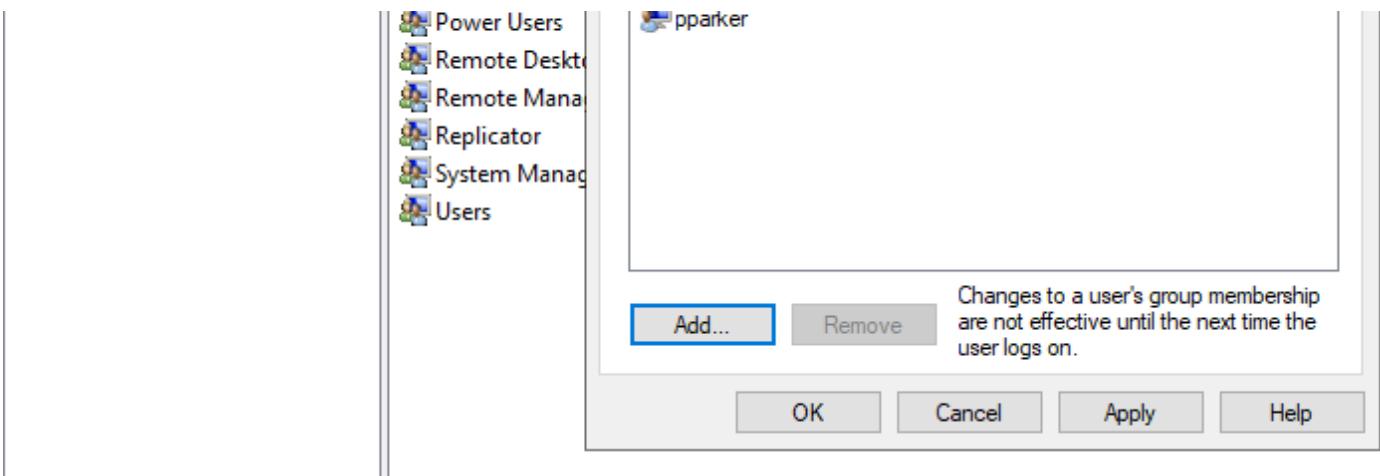
General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

- MARVEL\Domain Admins
- MARVEL\pparker (pparker@MARVEL.local)



Our Domain setup is all complete now. Last thing to do it add a Kali Linux machine here too.

## Setting up Kali Linux

Log in to the Azure Portal, browse to Virtual machines section and click on Add button.

A screenshot of the Microsoft Azure portal's Virtual machines list. The top navigation bar shows 'Microsoft Azure' and the current location 'Home &gt; Virtual machines'. The main area displays a table of three virtual machines: HYDRA-DC, Spiderman, and ThePunisher. Each row includes a checkbox, name, type, status, resource group, location, and source information. The table has columns for Name, Type, Status, Resource group, Location, and Source.

Setup the virtual machine with the setting shown below.

A screenshot of the Microsoft Azure 'Create a virtual machine' wizard. The top navigation bar shows 'Microsoft Azure' and the current location 'Home &gt; Virtual machines &gt; Create a virtual machine'. The main area is titled 'Create a virtual machine'. It contains two sections: 'Project details' and 'Instance details'. In 'Project details', 'Subscription' is set to 'Free Trial' and 'Resource group' is set to 'ADLab'. In 'Instance details', 'Virtual machine name' is 'kali', 'Region' is '(Canada) Canada Central', 'Availability options' is 'No infrastructure redundancy required', and 'Image' is 'Kali Linux'. All fields have a green checkmark indicating they are valid.

[Browse all public and private images](#)

Azure Spot instance [?](#)  Yes  No

Size [\\*](#) [?](#)

<b>Standard B1ms</b>
1 vcpu, 2 GiB memory (\$21.90/month)
<a href="#">Change size</a>

Administrator account

Authentication type [?](#)

<input checked="" type="radio"/> Password	<input type="radio"/> SSH public key
---	--------------------------------------

Username [\\*](#) [?](#)

hacker	
--------	--

Password [\\*](#) [?](#)

*****	
-------	--

Confirm password [\\*](#) [?](#)

*****	
-------	--

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

[Review + create](#) [< Previous](#) [Next : Disks >](#)

Important thing to note is that there is a Kali Linux image available in the market place that we can use.

Select an image

Marketplace [My Items](#)

AI + Machine Learning

Analytics

Blockchain

Compute

Containers

Databases

Developer Tools

DevOps

Identity

Integration

Internet of Things

IT & Management Tools

Media

Mixed Reality

Networking

**Security**

Software as a Service (SaaS)

Storage

Web

**Kali Linux**

 Kali Linux  
Kali Linux  
Deploy a professional grade penetration testing platform.

**Panorama (BYOL)**

 Palo Alto Networks, Inc.  
Central management system for Palo Alto Networks Firewalls, WildFire Appliances and Log Collectors

**Avi Controller Version 18.2.x - BYOL and PAYG**

 Avi Networks  
BYOL Controller and BYOL/PAYG Service Engines

**Avi Controller Version 18.1.x - BYOL and PAYG**

 Avi Networks  
BYOL Controller and BYOL/PAYG Service Engines

**Avi Controller Version 17.2.x - BYOL**

 Avi Networks  
BYOL Controller and Service Engines

**Kaspersky Secure Mail Gateway**

 Kaspersky Lab  
KSMG provides anti-malware, anti-spam, anti-phishing and content filtering.

**IKAN ALM 5.8 demo**

 IKAN Development  
IKAN ALM evaluation version (with a 30-day license)

**SEPPmail™ E-Mail Encryption Appliance - Version 11**

 SEPPmail AG  
Deploys a single SEPPmail Appliance VM in your Azure Subscription

Use the Standard HDD disk.

Microsoft Azure

Home > Virtual machines > Create a virtual machine

## Create a virtual machine

[Basics](#) **Disks** [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

### Disk options

OS disk type \* ⓘ

Standard HDD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Enable Ultra Disk compatibility ⓘ

Yes  No

Ultra Disk compatibility is not available for this VM size and location.

### Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

[Create and attach a new disk](#)   [Attach an existing disk](#)

✓ Advanced

---

[Review + create](#)   [< Previous](#)   [Next : Networking >](#)

Use the existing Virtual network ADLabNet.

[Home](#) > [Virtual machines](#) > Create a virtual machine

## Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ

ADLabNet



[Create new](#)

Subnet \* ⓘ

default (10.0.1.0/24)



[Manage subnet configuration](#)

Public IP ⓘ

(new) kali-ip



[Create new](#)

NIC network security group ⓘ

None  Basic  Advanced

Public inbound ports \* ⓘ

None  Allow selected ports

Select inbound ports \*

SSH (22)



**⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.**

Accelerated networking ⓘ

On  Off

The selected image does not support accelerated networking.

### Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution?

Yes  No

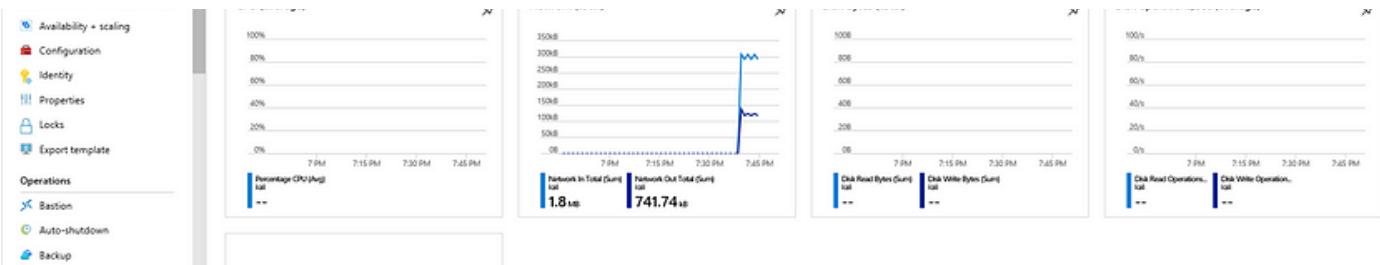
[Review + create](#)

[< Previous](#)

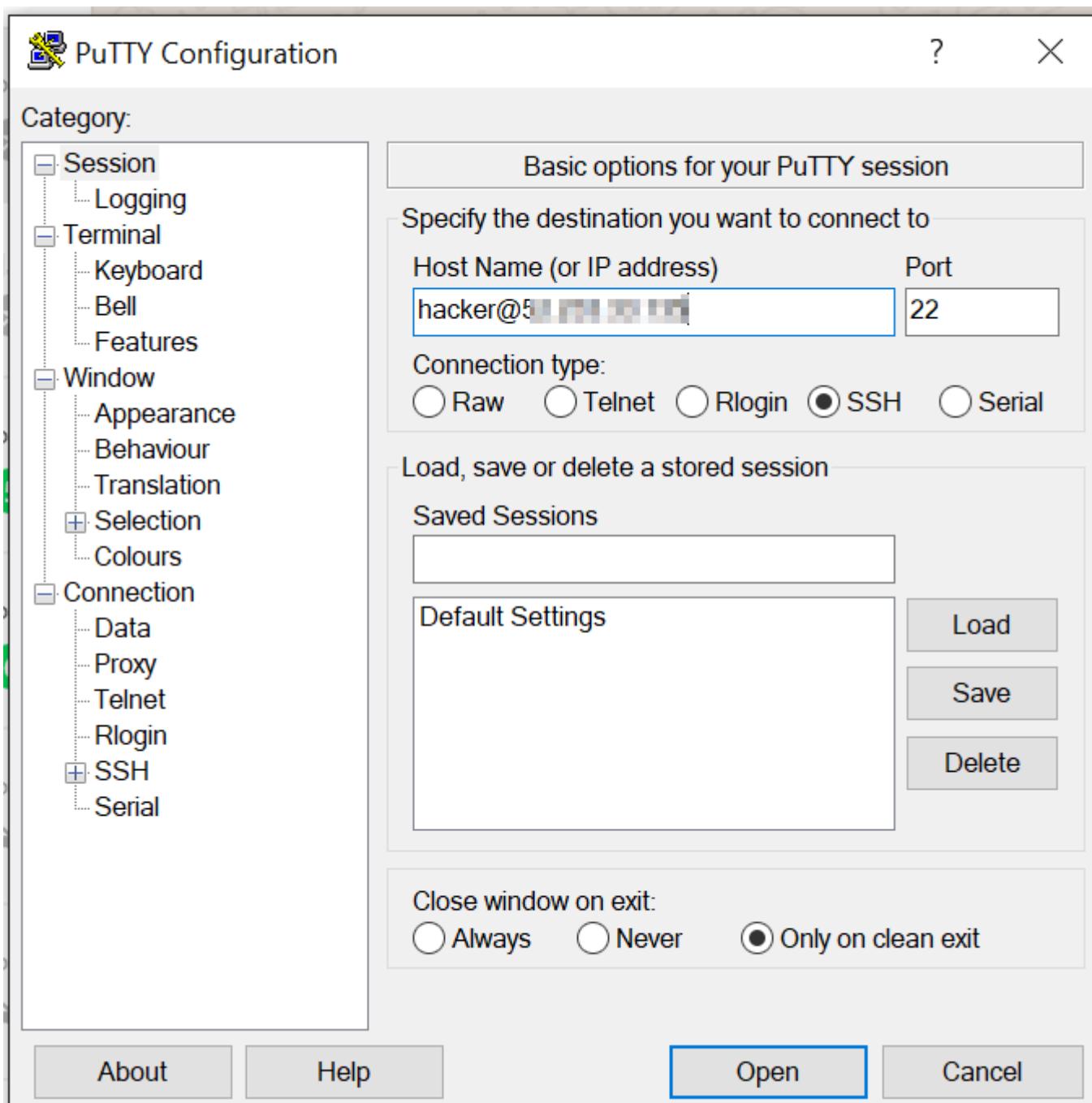
[Next : Management >](#)

Following the rest of the steps we should have a Kali Linux virtual machine.

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'kali'. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', and various account icons. The main content area has a title 'Home > CreateVM-kali-linux.kali-linux-kali-20200105193134 - Overview > kali'. On the left, there's a sidebar with 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (Networking, Disks, Size, Security, Extensions), and 'Continuous delivery (Preview)'. The main panel displays the VM details: Status: Running, Location: Canada Central, Subscription: Free Trial, Computer name: kali, Operating system: Linux (kali-kali-rolling), Size: Standard B1ms (1 vCore, 2 GB memory). It also shows network information: Virtual network/subnet: ADLabNet/default, DNS name: Configure, and other details like Public IP address (10.0.1.7) and Private IP address (IPv6). At the bottom, there are performance monitoring charts for CPU (average), Network (total), Disk bytes (total), and Disk operations/sec (average).



I use [putty](#) to connect to the Kali machine using SSH.



Once I logged in, I ran [netdiscover](#) utility to find the machines.

```
hacker@kali:~$ sudo netdiscover -r 10.0.1.0/24
```

Its results, as expected, came back with the IP addresses of the domain controller and two user machines.

```
hacker@kali: ~
Currently scanning: Finished!      |      Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts.  Total size: 168
-----

| IP       | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|----------|-------------------|-------|-----|-----------------------|
| 10.0.1.1 | 12:34:56:78:9a:bc | 1     | 42  | Unknown vendor        |
| 10.0.1.4 | 12:34:56:78:9a:bc | 1     | 42  | Unknown vendor        |
| 10.0.1.5 | 12:34:56:78:9a:bc | 1     | 42  | Unknown vendor        |
| 10.0.1.6 | 12:34:56:78:9a:bc | 1     | 42  | Unknown vendor        |


```

Nmap scan against the domain controller is shown below.

```
hacker@kali: ~
hacker@kali:~$ nmap -A -T4 10.0.1.4 -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-05 19:51 EST
Nmap scan report for 10.0.1.4
Host is up (0.0020s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| fingerprint-strings:
|_ DNSVersionBindReqTCP:
|   version
|_ bind
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-01-06 00:52:10Z)
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap       Microsoft Windows Active Directory LDAP (Domain: MARVEL.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Subject Alternative Name: othername:<unsupported>, DNS:HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-05T08:10:30
| Not valid after:  2021-01-04T08:10:30
|_ssl-date: 2020-01-06T00:54:22+00:00; 0s from scanner time.
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap   Microsoft Windows Active Directory LDAP (Domain: MARVEL.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Subject Alternative Name: othername:<unsupported>, DNS:HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-05T08:10:30
| Not valid after:  2021-01-04T08:10:30
|_ssl-date: 2020-01-06T00:54:21+00:00; 0s from scanner time.
3268/tcp  open  ldap       Microsoft Windows Active Directory LDAP (Domain: MARVEL.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Subject Alternative Name: othername:<unsupported>, DNS:HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-05T08:10:30
| Not valid after:  2021-01-04T08:10:30
|_ssl-date: 2020-01-06T00:54:21+00:00; 0s from scanner time.
3269/tcp  open  ssl/ldap   Microsoft Windows Active Directory LDAP (Domain: MARVEL.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Subject Alternative Name: othername:<unsupported>, DNS:HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-05T08:10:30
| Not valid after:  2021-01-04T08:10:30
|_ssl-date: 2020-01-06T00:54:21+00:00; 0s from scanner time.
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-02T22:43:42
| Not valid after:  2020-07-03T22:43:42
|_ssl-date: 2020-01-06T00:56:54+00:00; 0s from scanner time.
```

Nmap scan for the two user machines is shown below.

```
hacker@kali: ~
hacker@kali:~$ nmap -A -T4 10.0.1.5 -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-05 19:56 EST
Nmap scan report for 10.0.1.5
Host is up (0.0029s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc      Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=ThePunisher.MARVEL.local
| Not valid before: 2020-01-04T21:28:52
| Not valid after:  2020-07-05T21:28:52
|_ssl-date: 2020-01-06T00:56:54+00:00; 0s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.33 seconds
```

```
hacker@kali:~$ nmap -A -T4 10.0.1.6 -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-05 19:57 EST
Nmap scan report for 10.0.1.6
Host is up (0.0022s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
3389/tcp   open  ms-wbt-server  Microsoft Terminal Services
| ssl-cert: Subject: commonName=Spiderman.MARVEL.local
| Not valid before: 2020-01-04T21:25:15
|_Not valid after:  2020-07-05T21:25:15
|_ssl-date: 2020-01-06T00:57:38+00:00; 0s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.84 seconds
```

Until next, happy ethical hacking!!!