

[Open in app](#)[Get started](#)

You have **2** free member-only stories left this month. [Sign up for Medium and get an extra one](#)



Kamran Bilgrami

[Follow](#)

Jan 6, 2020 · 21 min read

[Listen](#)[Save](#)

Ethical Hacking Lessons — Building Free Active Directory Lab in Azure



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.



[Open in app](#)[Get started](#)

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.

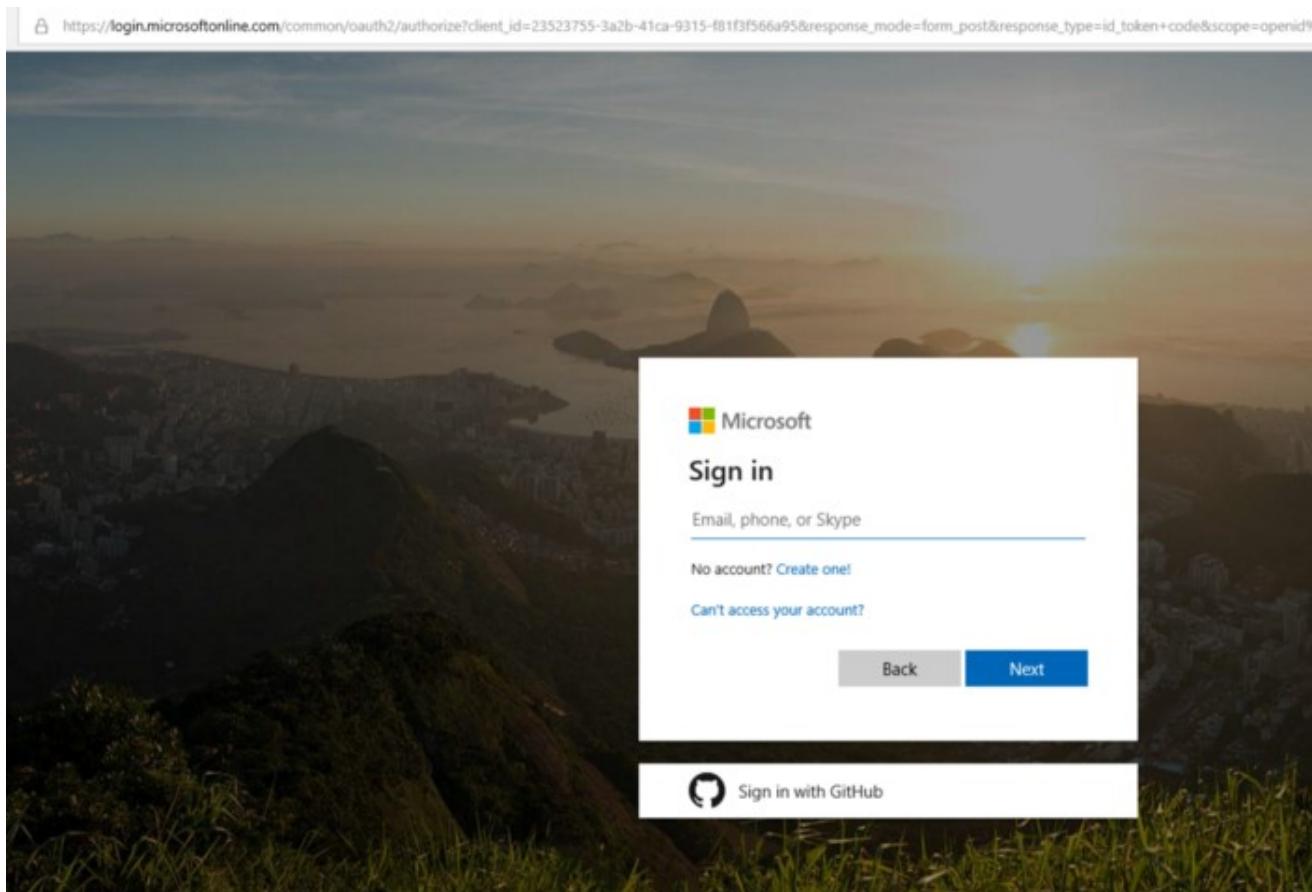
Microsoft offers a [free Azure trial](#) that includes free access to popular Azure products for 12 months, \$200 credit to spend for the first 30 days of sign up, and access to more than 25 products that are always free.

The screenshot shows the Microsoft Azure free trial landing page. At the top, there's a navigation bar with links for Overview, Solutions, Products, Documentation, Pricing, Training, Marketplace, Partners, Support, Blog, and More. A search bar and user account links are also present. The main heading is "Create your Azure free account today" with a subtext "Get started with 12 months of free services". Below this are two prominent buttons: "Start free >" and "Or buy now >". A large image in the center displays a tablet screen showing the Azure portal interface with various service icons and resource lists. At the bottom of the page are icons for Home, Search, and Profile.

[Open in app](#)[Get started](#)

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.



Otherwise, you will have to signup for an account.



[Open in app](#)[Get started](#)

Country/Region

Canada

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

Phone

 Example: (604) 555-0100[Next](#)

2 Identity verification by phone

3 Identity verification by card

4 Agreement



16 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.

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.





Open in app

Get started

The screenshot shows the Azure portal homepage. At the top, there's a navigation bar with links 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. Below the navigation bar is a 'Navigate' section with links for Subscriptions, Resource groups, All resources, and Dashboard. A 'Tools' section follows, featuring Microsoft Learn, Azure Monitor, Security Center, and Cost Management. The 'Useful links' section includes 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 Azure portal with the 'Resource groups' option highlighted in the left navigation menu. The main content area displays the 'Azure services' section 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. Below this is the 'Navigate' section with links for Subscriptions, Resource groups, All resources, and Dashboard. The 'Tools' section is identical to the one in the first screenshot. The 'Useful links' and 'Azure mobile app' sections are also present.

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



[Open in app](#)[Get started](#)

Filter by name... Subscription == all Location == all Add filter

Showing 0 to 0 of 0 records.

Name ↑↓	Subscription ↑↓	Location ↑↓
---------	-----------------	-------------

No resource groups to display
Try changing your filters if you don't see what you're looking for. Learn more of...

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.



[Open in app](#)[Get started](#)

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](#)

< 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.



[Open in app](#)[Get started](#)

Create a resource group

✓ Validation passed.

[Basics](#) [Tags](#) [Review + create](#)

Basics

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

[Create](#)

< Previous

Next >

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



The screenshot shows the Azure portal interface. At the top, there is a navigation bar with icons for Home, All resources, Marketplace, Support, Insights, and Notifications. On the far right of the top bar are 'Open in app' and 'Get started' buttons. Below the top bar, there is a search bar and a filter section with fields for 'Filter by name...', 'Subscription == all', 'Location == all', and an 'Add filter' button. The main content area displays a table with one record. The table has columns for Name, Subscription, and Location. The single row shows 'ADLab' as the Name, 'Free Trial' as the Subscription, and 'Canada Central' as the Location. The table includes sorting arrows for Name, Subscription, and Location. At the bottom of the page are standard navigation icons for Home, Search, and Profile.

[Open in app](#)[Get started](#)

[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](#)

Refresh [Export to CSV](#) | [Assign tags](#) | [+ Add](#)

Subscription == all | Location == all | [+ Add](#)

Azure Active Directory

Monitor

Advisor

Security Center

Cost Management + Billing

Help + support

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



The screenshot shows the Azure portal's 'Virtual Networks' blade. At the top, there are filter options: 'Filter by name...', 'Subscription == all', 'Resource group == all', 'Location == all', and 'Add filter'. Below the filters, it says 'Showing 0 to 0 of 0 records.' There are four columns: 'Name' (sorted by 'Name'), 'Resource group' (sorted by 'Resource group'), 'Location' (sorted by 'Location'), and 'Subscription' (sorted by 'Subscription'). In the center, there is a large 'Create' button with three dots and arrows pointing outwards. Below the button, a message reads: 'No virtual networks to display. 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.' A blue 'Create virtual network' button is at the bottom of this message, with a red box drawn around it.

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.

[Open in app](#)[Get started](#)[HOME](#) / [Virtual networks](#) / Create virtual network

Create virtual network

**Name ***

ADLabNet

Address space * ⓘ

10.0.1.0/24

10.0.1.0 - 10.0.1.255 (256 addresses)

 Add an IPv6 address space ⓘ**Subscription ***

Free Trial

Resource group *

ADLab

[Create new](#)**Location ***

(Canada) Canada Central

Subnet**Name ***

default

Address range * ⓘ

10.0.1.0/24

(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.



[Open in app](#)[Get started](#)

Filter by name...	Subscription == all	Resource group == all	Location == all	Add filter
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.



[Open in app](#)[Get started](#)

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.



[Open in app](#)[Get started](#)

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 or 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.



[Open in app](#)[Get started](#)

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 * ⓘ

HYDRA-DC

Region * ⓘ

(Canada) Canada Central

Availability options ⓘ

No infrastructure redundancy required

Image * ⓘ

Ubuntu Server 18.04 LTS

[Browse all public and private images](#)

Azure Spot instance ⓘ

Yes No

Size * ⓘ

Standard D2s v3

2 vcpus, 8 GiB memory (\$105.71/month)

[Change size](#)

Administrator account

Authentication type ⓘ

Password SSH public key

[Review + create](#)

< Previous

Next : Disks >

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



[Open in app](#)[Get started](#)

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

 Search compute

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 (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.





Open in app

Get started

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	
B1ms	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	
DS1_v2	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.



[Open in app](#)[Get started](#)

Create a virtual machine

Subscription * ⓘ

Free Trial

**Resource group *** ⓘ

ADLab

[Create new](#)**Instance details****Virtual machine name *** ⓘ

HYDRA-DC

**Region *** ⓘ

(Canada) Canada Central

**Availability options** ⓘ

No infrastructure redundancy required

**Image *** ⓘ

Windows Server 2019 Datacenter

[Browse all public and private images](#)**Azure Spot instance** ⓘ Yes No**Size *** ⓘ**Standard B1ms**

1 vcpu, 2 GiB memory (\$21.90/month)

[Change size](#)**Administrator account****Username *** ⓘ

kamran

**Password *** ⓘ

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

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.



[Open in app](#)[Get started](#)

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 >

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.



[Open in app](#)[Get started](#)

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 * [①](#)

ADLabNet

[Create new](#)**Subnet *** [①](#)

default (10.0.1.0/24)

[Manage subnet configuration](#)**Public IP** [①](#)

(new) HYDRA-DC-ip

[Create new](#)**NIC network security group** [①](#) None Basic Advanced**Public inbound ports *** [①](#) 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 [①](#) 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](#)< PreviousNext : Management >

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



[Open in app](#)[Get started](#)

Create a virtual machine

Validation passed

Basics Disks Networking Management Advanced Tags Review + create

PRODUCT DETAILS

Standard B2s

Subscription credits apply ⓘ

by Microsoft

0.0696 CAD/hr

[Terms of use](#) | [Privacy policy](#)

[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

Disk

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.





Open in app

Get started

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsS... Start time: 1/2/2020 6:22:07 PM
Subscription: Free Trial Correlation ID: a635aeef-0610-48fc-9e91-61d1ebe174ef
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

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

Microsoft Azure

HYDRA-DC

Connect

Resource group (changed) : ADLab

Status : Running

Location : Canada Central

Subscription (changed) : Free Trial

Subscription ID : [xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx](#)

Computer name : HYDRA-DC

Operating system : Windows (Windows Server 2019 Datacenter)

Size : Standard B1ms (1 vcpus, 2 GiB memory)

Tags (changed) : Click here to add tags

Azure Spot : N/A

Public IP address : [10.0.2.4 \(IPv4\)](#)

Private IP address : 10.0.1.4

Public IP address (IPv6) : -

Virtual network/subnet : ADLabNet/default

DNS name : Configure

Scale Set : N/A

Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 days

CPU (average)

Network (total)

Disk bytes (total)

Disk operations/sec (average)

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

[Open in app](#)[Get started](#)

To improve security, enable just-in-time access on this VM. [→](#)

[RDP](#) [SSH](#) [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 *

Public IP address ([...:3389](#))

Port number *

3389

[Download RDP File](#)

Having trouble connecting to this VM?

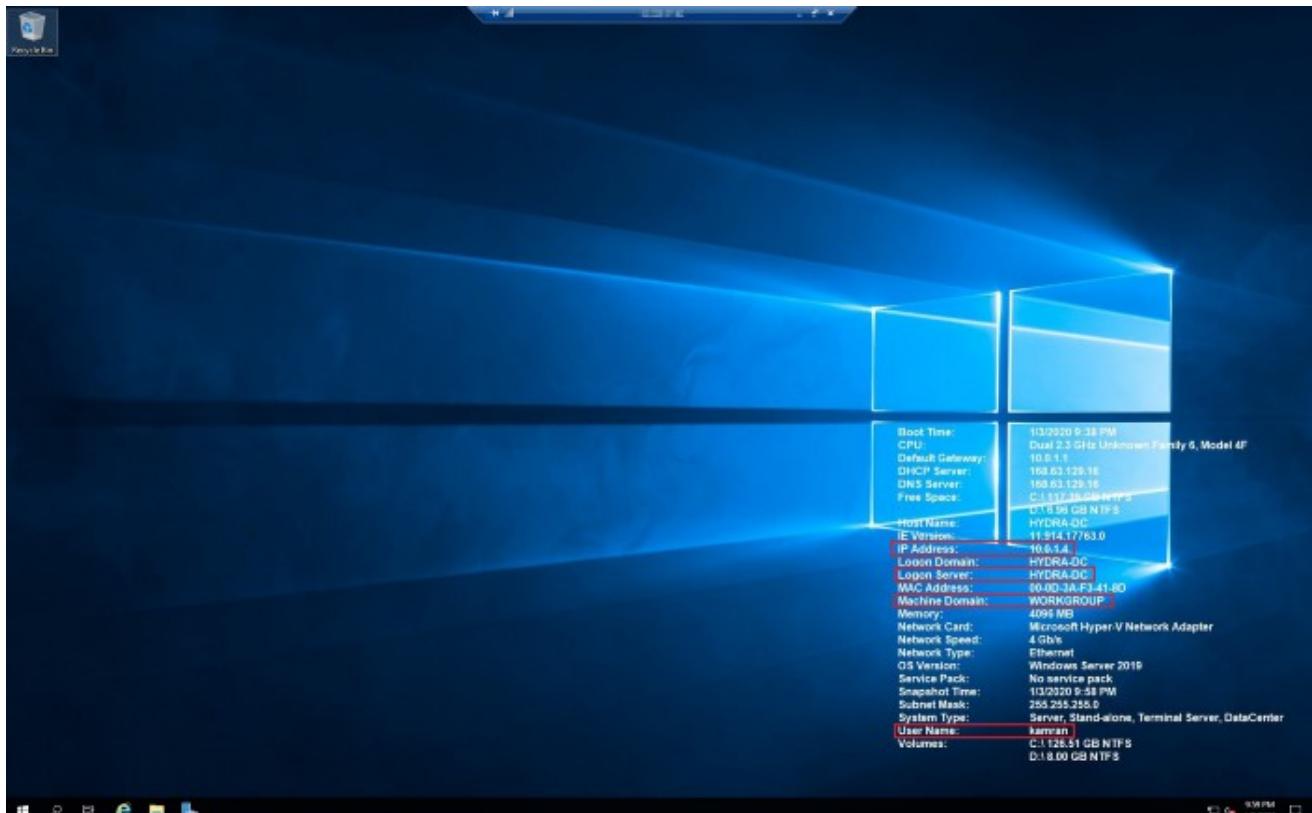
- [Diagnose and solve problems](#)
- [Troubleshoot connection](#)
- [Serial console](#)
- [Reset password](#)

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.



[Open in app](#)[Get started](#)

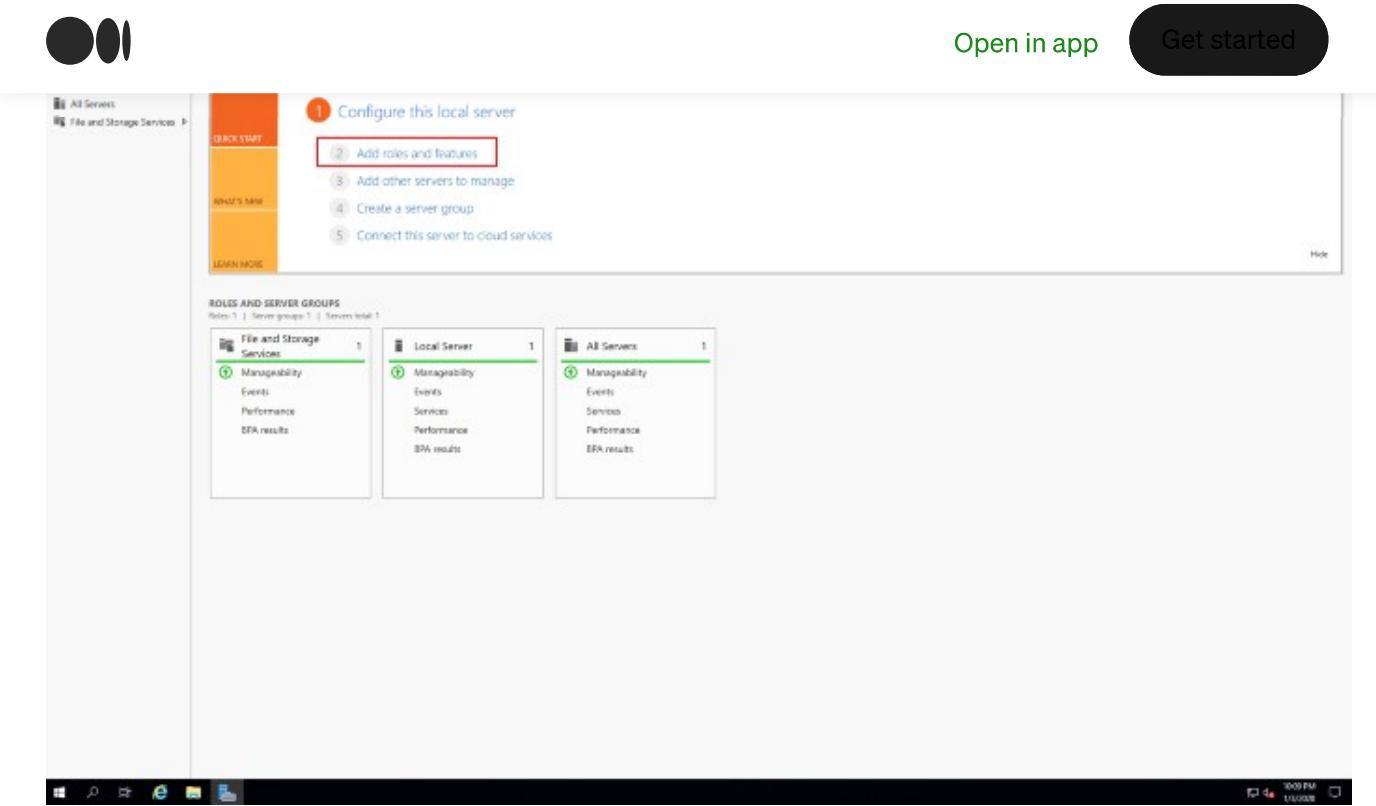
BgInfo utility that setups your desktop background with an image with some useful information such as IP address, machine name/domain, Username, etc. as shown below.



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.



[Open in app](#)[Get started](#)

Before you begin

HYDRA-DC

Before You Begin

[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[Confirmation](#)[Results](#)

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

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

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

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

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

To continue, click Next.

Skip this page by default

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

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



[Open in app](#)[Get started](#)

Select installation type

HYDRA-DC

[Before You Begin](#)**Installation Type**[Server Selection](#)[Server Roles](#)[Features](#)[Confirmation](#)[Results](#)

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

Role-based or feature-based installation

Configure a single server by adding roles, role services, and features.

Remote Desktop Services installation

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

[**< Previous**](#)[**Next >**](#)[Install](#)[Cancel](#)

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

Add Roles and Features Wizard

Select destination server

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

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

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.





Open in app

Get started

Add Roles and Features Wizard



Select server roles

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

Description

- | | |
|---|--|
| <input type="checkbox"/> Active Directory Certificate Services | 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. |
| <input checked="" type="checkbox"/> Active Directory Domain Services | |
| <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 | |
| <input type="checkbox"/> Volume Activation Services | |
| <input type="checkbox"/> Web Server (IIS) | |
| <input type="checkbox"/> Windows Deployment Services | |

Description

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.





Open in app

Get started

Select server role

Add Roles and Features Wizard

Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

- [Tools] Group Policy Management
- ▲ Remote Server Administration Tools
 - ▲ Role Administration Tools
 - ▲ AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell
 - ▲ AD DS Tools
 - [Tools] Active Directory Administrative Center
 - [Tools] AD DS Snap-Ins and Command-Line Tools

Include management tools (if applicable)

Add Features Cancel

< Previous Next > Install Cancel

HYDRA-DC

Click Next.

Add Roles and Features Wizard

DESTINATION SERVER HYDRA-DC

Select server roles

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

Roles	Description
<input type="checkbox"/> Active Directory Certificate Services	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.
<input checked="" type="checkbox"/> Active Directory Domain Services	
<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	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	





Open in app

Get started

Add Roles and Features Wizard

Select features

DESTINATION SERVER
HYDRA-DC

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

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

Features

	Description
<input type="checkbox"/> .NET Framework 3.5 Features	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
<input checked="" type="checkbox"/> .NET Framework 4.7 Features (2 of 7 installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input checked="" type="checkbox"/> BitLocker Drive Encryption (Installed)	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input checked="" type="checkbox"/> Enhanced Storage (Installed)	
<input type="checkbox"/> Failover Clustering	
<input checked="" type="checkbox"/> Group Policy Management	
<input type="checkbox"/> Host Guardian Hyper-V Support	
<input type="checkbox"/> I/O Quality of Service	
<input type="checkbox"/> IIS Hostable Web Core	
<input type="checkbox"/> Internet Printing Client	
<input type="checkbox"/> IP Address Management (IPAM) Server	
<input type="checkbox"/> iSNS Server service	

< Previous Next > Install Cancel

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



[Open in app](#)[Get started](#)

Active Directory Domain Services

HYDRA-DC

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

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.



Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

[Learn more about Azure Active Directory](#)

[Configure Office 365 with Azure Active Directory Connect](#)

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

Click **Install** on the Confirmation tab.

Add Roles and Features Wizard

- □ ×

Confirm installation selections

DESTINATION SERVER
HYDRA-DC

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](#)



[Open in app](#)[Get started](#)

Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
HYDRA-DC

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

View installation progress

i Starting installation**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

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)[< Previous](#)[Next >](#)[Install](#)[Cancel](#)

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





Open in app

Get started

Installation progress

HYDRA-DC

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

View installation progress

i Feature installation

Configuration required. Installation succeeded on HYDRA-DC.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
[Promote this server to a domain controller](#)

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

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

< Previous Next > Close Cancel

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.

The screenshot shows the Windows Server Manager dashboard. On the left, there's a navigation pane with links like 'Dashboard', 'Local Server', 'All Servers', 'AD DS', and 'File and Storage Services'. The main area has a 'WELCOME TO SERVER MANAGER' section with a 'Quick Start' button and a 'WHAT'S NEW' button. Below this, there's a 'ROLES AND SERVER GROUPS' section showing four groups: 'AD DS' (1 item), 'File and Storage Services' (1 item), 'Local Server' (1 item), and 'All Servers' (1 item). Each group has a green status icon and a list of management tools. A prominent yellow warning flag icon is positioned in the top right corner of the dashboard area, pointing to a tooltip. The tooltip contains the following text:
Post-deployment Configuration
Configuration required for Active Directory Domain Services at HYDRA-DC
[Promote this server to a domain controller](#)

Post installation
Configuration required. Installation succeeded on HYDRA-DC.
[Add Roles and Features](#)
[Task Details](#)

Promote VM to Domain Controller

Clicking on the **Promote this server to a domain controller** link will launch Active



[Open in app](#)[Get started](#)

Active Directory Domain Services Configuration Wizard

TARGET SERVER
HYDRA-DC

Deployment Configuration

- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Domain:

*

[Select...](#)

Supply the credentials to perform this operation

<No credentials provided>

[Change...](#)[More about deployment configurations](#)[< Previous](#)[Next >](#)[Install](#)[Cancel](#)

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



[Open in app](#)[Get started](#)

HYDRA-DC

Deployment Configuration

Deployment Configuration

[Domain Controller Options](#)[Additional Options](#)[Paths](#)[Review Options](#)[Prerequisites Check](#)[Installation](#)[Results](#)

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Root domain name:

MARVEL.local

[More about deployment configurations](#)[< Previous](#)[Next >](#)[Install](#)[Cancel](#)

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



[Open in app](#)[Get started](#)

Domain Controller Options

HYDRA-DC

Deployment Configuration
Domain Controller Options

DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

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

Type the Directory Services Restore Mode (DSRM) password

Password: ······

Confirm password: ······|

[More about domain controller options](#)

< Previous **Next >** Install Cancel

Click Next on DNS Options tab.



[Open in app](#)[Get started](#)

DNS Options

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](#) Selected[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.



[Open in app](#)[Get started](#)

Additional Options

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:

[More about additional options](#)[< Previous](#)[Next >](#)[Install](#)[Cancel](#)

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



[Open in app](#)[Get started](#)

HYDRA-DC

Paths

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

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:	C:\windows\NTDS	...
Log files folder:	C:\windows\NTDS	...
SYSVOL folder:	C:\windows\SYSVOL	...

[More about Active Directory paths](#)

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

Review the options and click Next.



[Open in app](#)[Get started](#)

Review Options

HYDRA-DC

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

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "MARVEL.local". This is also the name of the new forest.

The NetBIOS name of the domain: MARVEL

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

[View script](#)

[More about installation options](#)

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

On the final step, click Install button.



[Open in app](#)[Get started](#)

Prerequisites Check

TARGET SERVER
HYDRA-DC

All prerequisite checks passed successfully. Click 'Install' to begin installation.

[Show more](#)[Deployment Configuration](#)[Domain Controller Options](#)[DNS Options](#)[Additional Options](#)[Paths](#)[Review Options](#)[Prerequisites Check](#)[Installation](#)[Results](#)

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

[Rerun prerequisites check](#)[View results](#)

Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System

If you click Install, the server automatically reboots at the end of the promotion operation.

[More about prerequisites](#)[< Previous](#)[Next >](#)[Install](#)[Cancel](#)

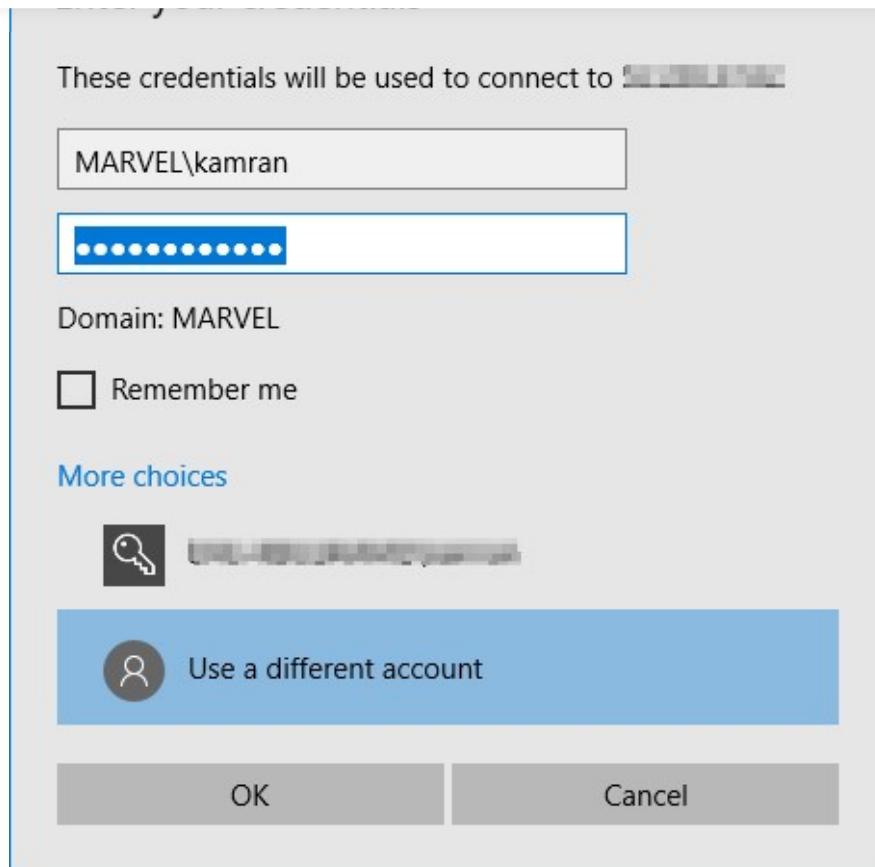
It will take a few minutes for this installation to complete. This will cause a reboot of the machine as well. After that, you can log in with the domain credentials.





Open in app

Get started

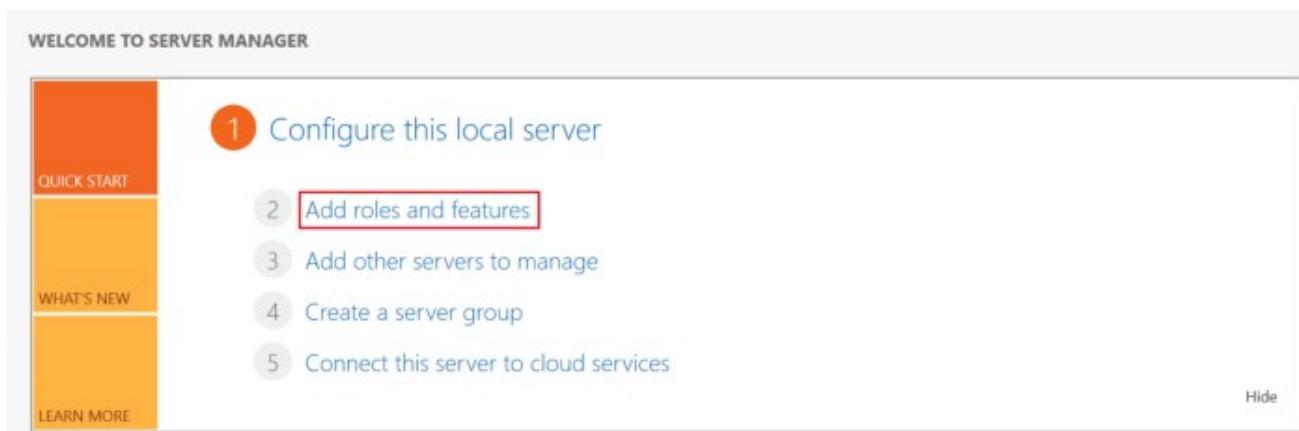


The desktop background image showing that we log in to the newly created MARVEL domain.

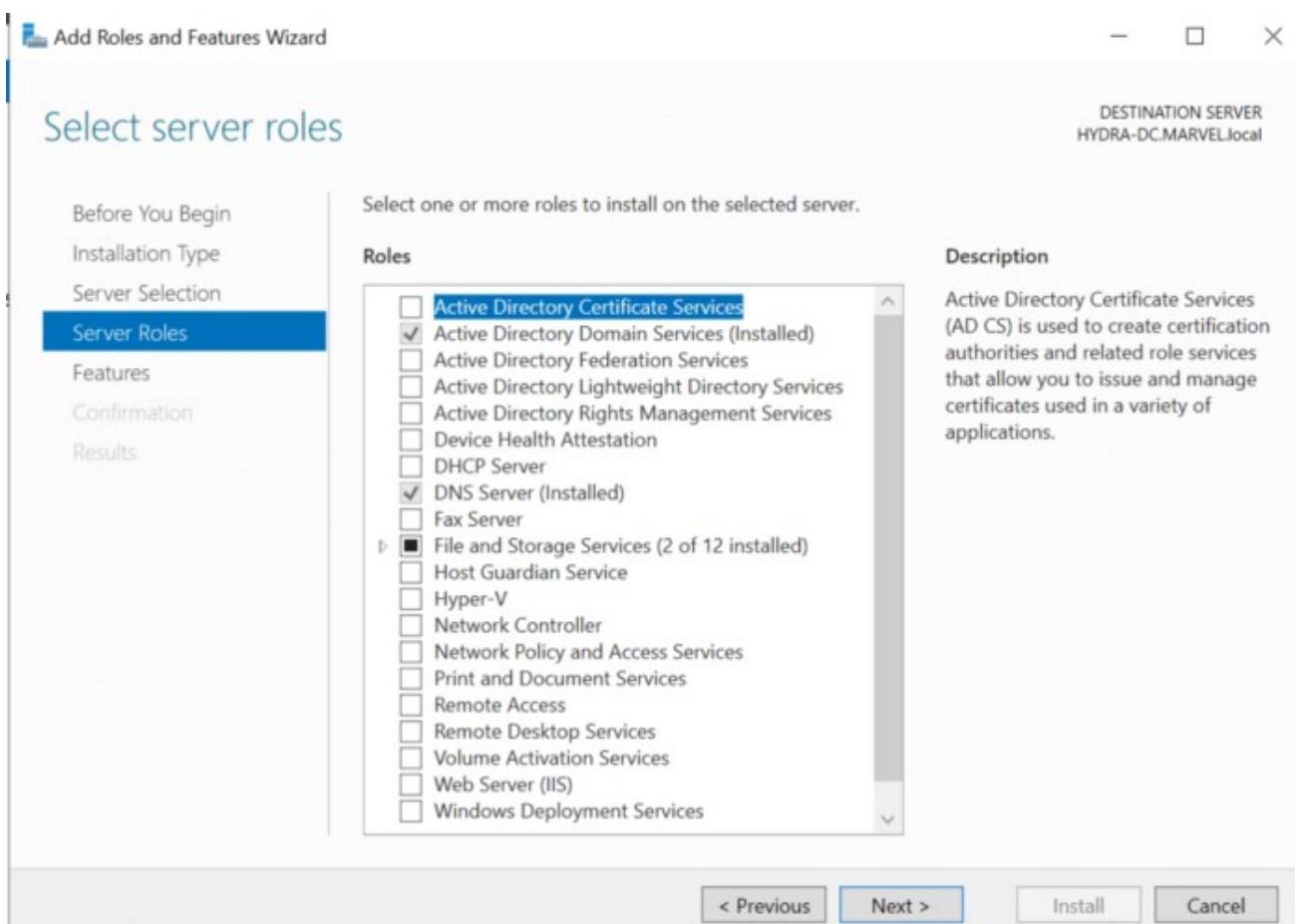


[Open in app](#)[Get started](#)

click on the **Add roles and features**.

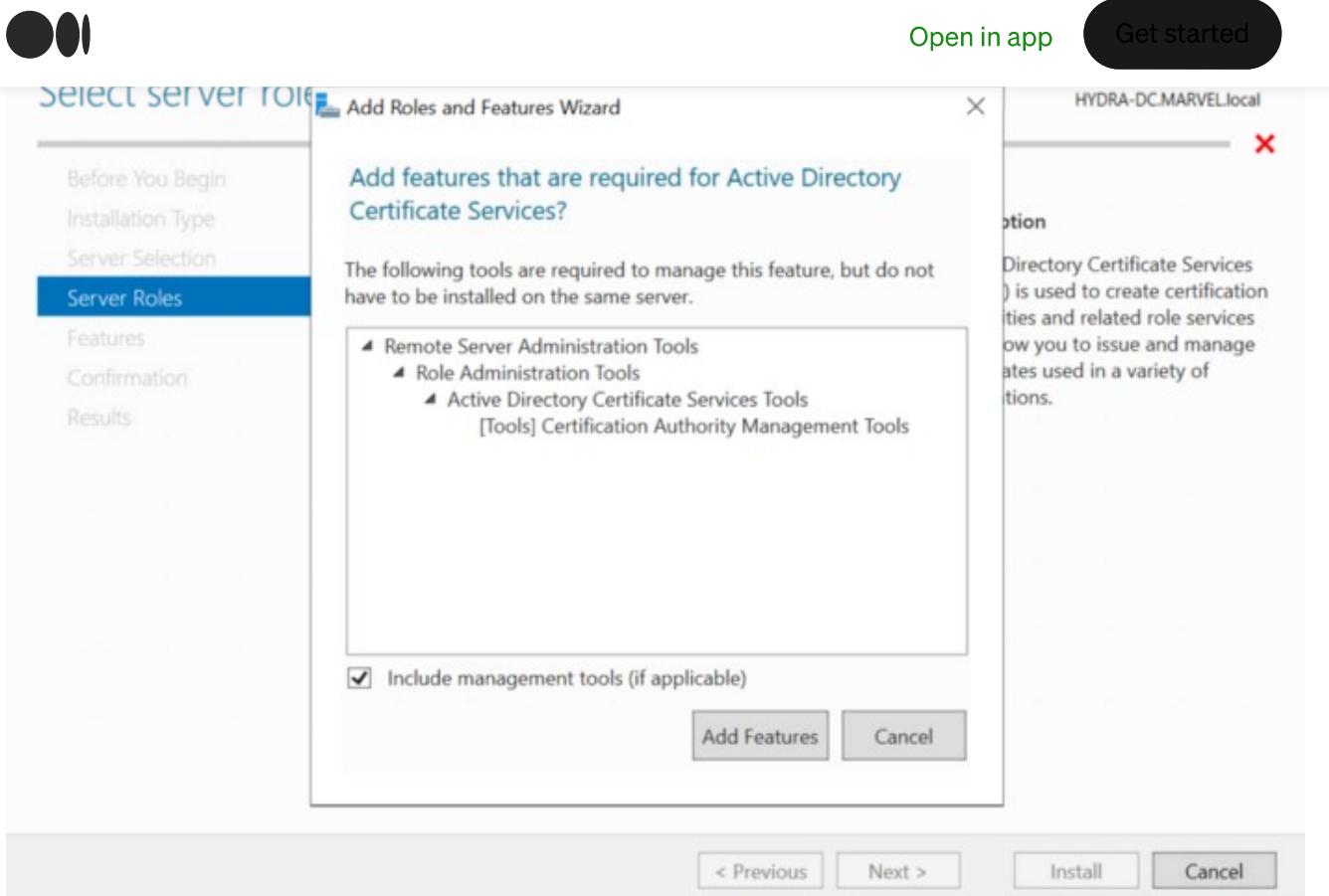


This will launch the **Add Roles and Features Wizard** that we used before too. Just keep clicking Next until you are on the Server Roles tab. Check the **Active Directory Certificate Services (ADCS)** here.

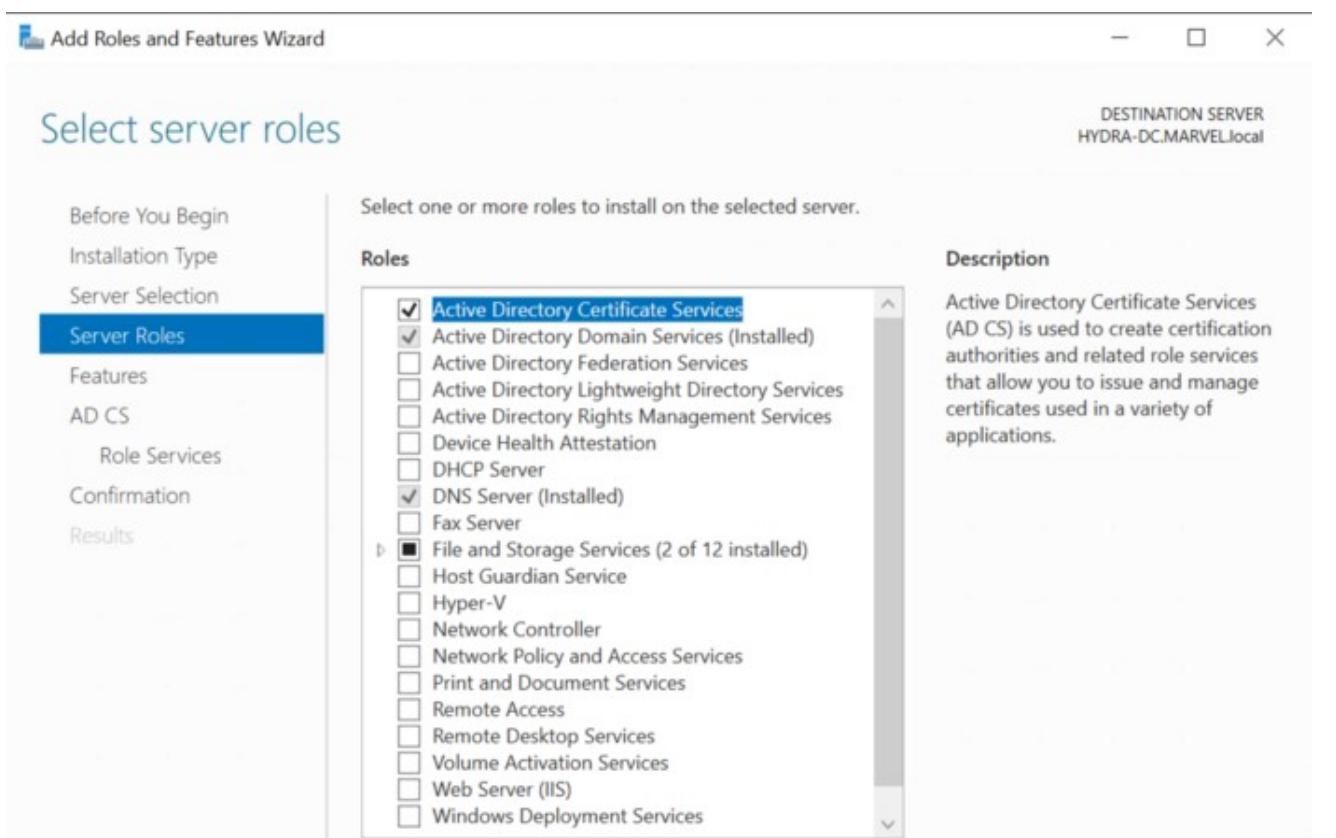


That will pop-up the following dialog with the information about the required features





Click on the Next button.



[Open in app](#)[Get started](#)

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.

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

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



The screenshot shows the 'Select Role Services' step of an Active Directory Certificate Services (AD CS) installation. On the left, a vertical navigation bar lists steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services' (which is highlighted in blue), 'Confirmation', and 'Results'. The main area is titled 'Select the role services to install for Active Directory Certificate Services'. It contains two columns: 'Role services' and 'Description'. Under 'Role services', there is a list of checkboxes. The first checkbox, 'Certification Authority', is checked and highlighted in blue. Other options include 'Certificate Enrollment Policy Web Service', 'Certificate Enrollment Web Service', 'Certification Authority Web Enrollment', 'Network Device Enrollment Service', and 'Online Responder'. To the right of the list is a detailed description: 'Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.' At the bottom of the screen are navigation buttons: '< Previous' (disabled), 'Next >', 'Install' (disabled), and '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.



[Open in app](#)[Get started](#)

Confirm installation selections

HYDRA-DC.MARVEL.local

[Before You Begin](#)[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[AD CS](#)[Role Services](#)[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 checkmarks.

Add Roles and Features Wizard



If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

[Yes](#)[No](#)[Export configuration settings](#)[Specify an alternate source path](#)[< Previous](#)[Next >](#)[Install](#)[Cancel](#)

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

Add Roles and Features Wizard

DESTINATION SERVER
HYDRA-DC.MARVEL.local

Installation progress

[Before You Begin](#)
[View installation progress](#)

Starting installation

Active Directory Certificate Services

- Certification Authority

Remote Server Administration Tools

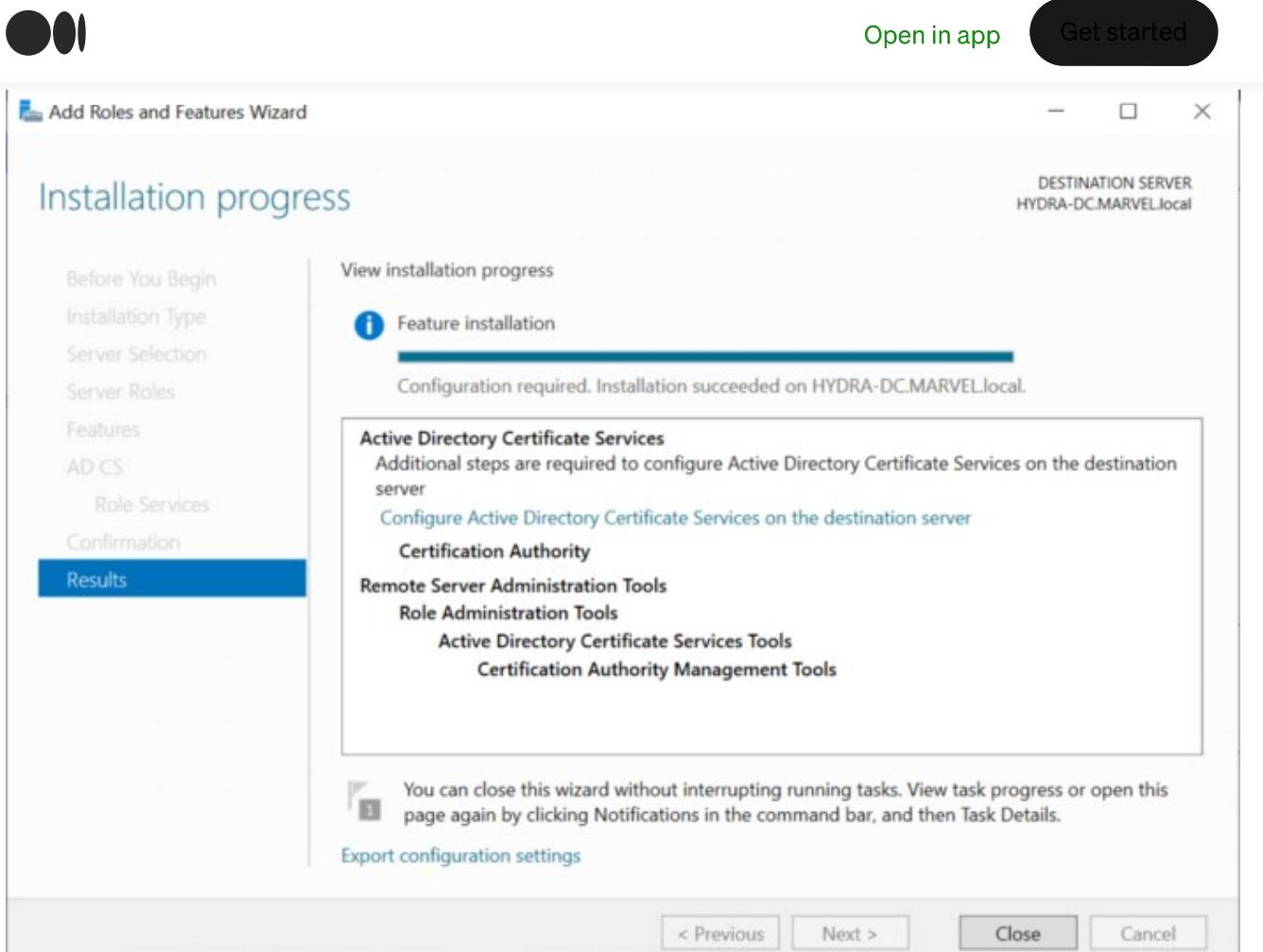
- Role Administration Tools

Active Directory Certificate Services Tools

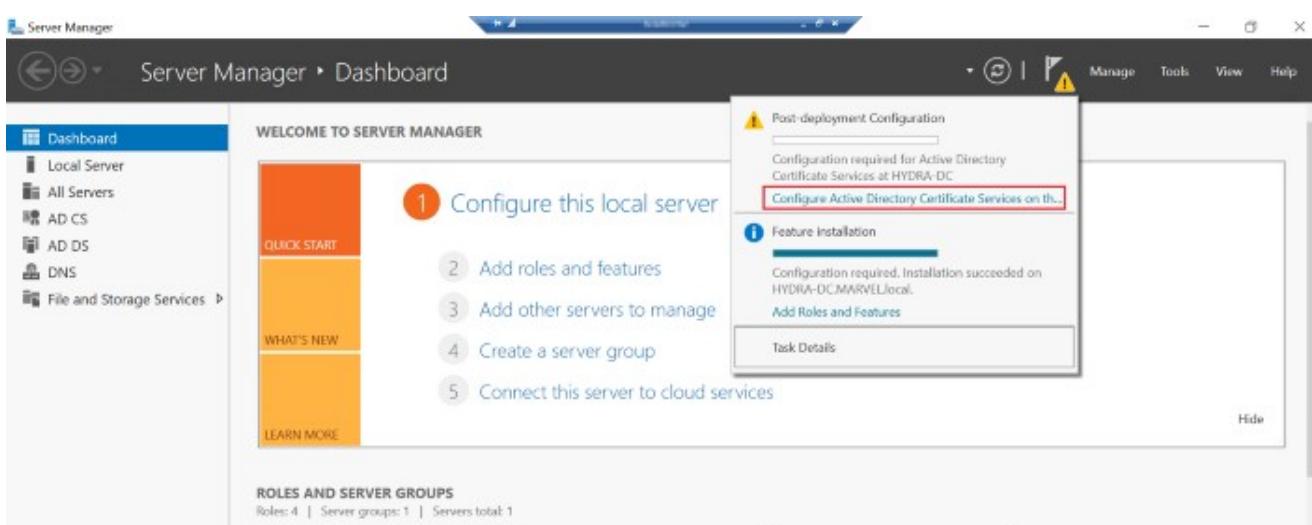
- Certification Authority Management Tools

[Export configuration settings](#)





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.

[Open in app](#)[Get started](#)

Credentials

HYDRA-DC.MARVEL.local

Credentials

[Role Services](#)[Confirmation](#)[Progress](#)[Results](#)

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials:

[Change...](#)[More about AD CS Server Roles](#)[< Previous](#)[Next >](#)[Configure](#)[Cancel](#)

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



[Open in app](#)[Get started](#)

Role Services

HYDRA-DC.MARVEL.local

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.



[Open in app](#)[Get started](#)

Setup type

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 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.

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**.



[Open in app](#)[Get started](#)

CA type

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 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.



[Open in app](#)[Get started](#)

Private Key

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 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.



[Open in app](#)[Get started](#)

Cryptography for CA

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 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.



[Open in app](#)[Get started](#)

CA Name

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:

Distinguished name suffix:

Preview of distinguished name:

[More about CA Name](#)

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

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



[Open in app](#)[Get started](#)

Validity Period

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):

 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](#)

[Open in app](#)[Get started](#)

CA Database

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:

C:\windows\system32\CertLog

Certificate database log location:

C:\windows\system32\CertLog

[More about CA Database](#)[< Previous](#)[Next >](#)[Configure](#)[Cancel](#)

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



[Open in app](#)[Get started](#)

Confirmation

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.



[Open in app](#)[Get started](#)

Results

HYDRA-DC.MARVEL.local

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

The following roles, role services, or features were configured:

Active Directory Certificate Services

Certification Authority
[More about CA Configuration](#)

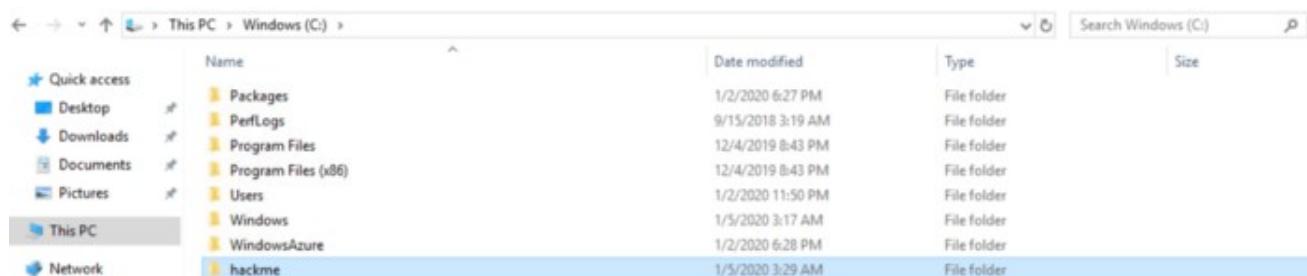
✓ Configuration succeeded

< Previous Next > Close Cancel

Restart the VM now so the changes take effect.

Setting up a Share

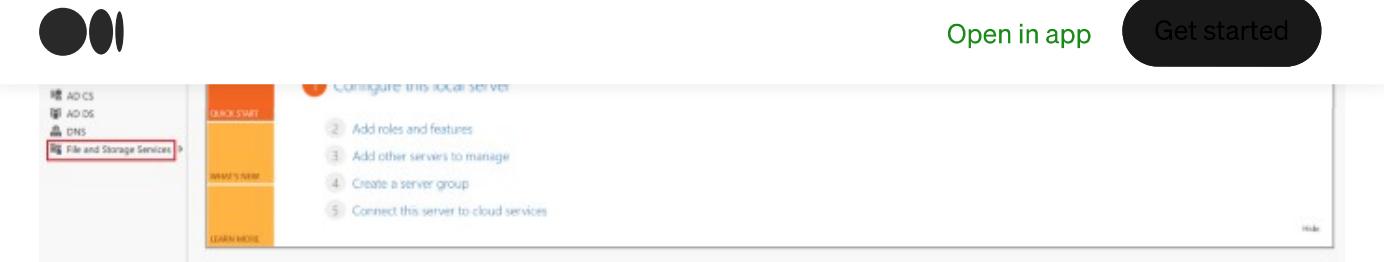
Create a folder **hackme** on the C drive.



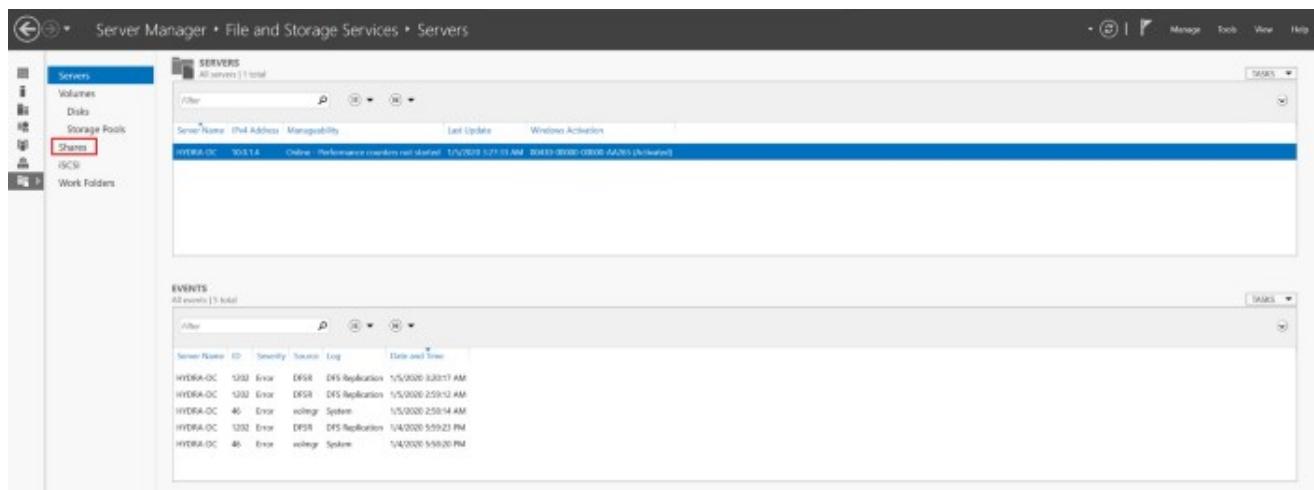
Name	Date modified	Type	Size
Packages	1/2/2020 6:27 PM	File folder	
PerfLogs	9/15/2018 3:19 AM	File folder	
Program Files	12/4/2019 8:43 PM	File folder	
Program Files (x86)	12/4/2019 8:43 PM	File folder	
Users	1/2/2020 11:50 PM	File folder	
Windows	1/5/2020 3:17 AM	File folder	
WindowsAzure	1/2/2020 6:28 PM	File folder	
hackme	1/5/2020 3:29 AM	File folder	

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

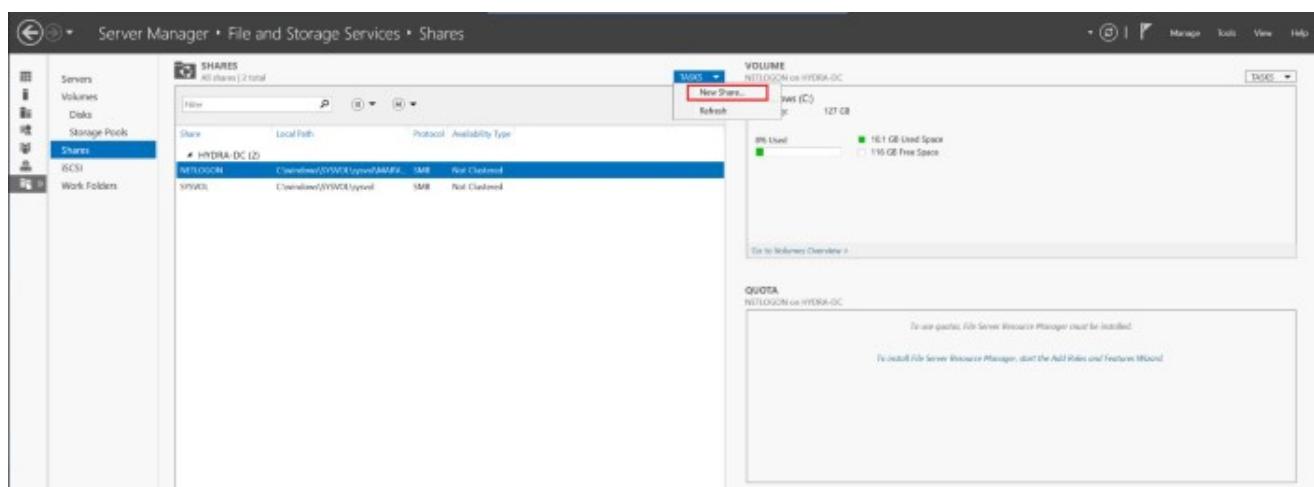




Click on the **Shares** as shown below.



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.



[Open in app](#)[Get started](#)

Select the profile for this share

Select Profile

- Share Location
- Share Name
- Other Settings
- Permissions
- Confirmation
- Results

File share profile:

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

Description:

This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.

- Suitable for general file sharing
- Advanced options can be configured later by using the Properties dialog

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

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



[Open in app](#)[Get started](#)

Select the server and path for this share

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:[Browse...](#)[< Previous](#)[Next >](#)[Create](#)[Cancel](#)

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



[Open in app](#)[Get started](#)

Specify share name

[Select Profile](#)[Share Location](#)[Share Name](#)[Other Settings](#)[Permissions](#)[Confirmation](#)[Results](#)

Share name:

Share description:

Local path to share:

Remote path to share:

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

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



[Open in app](#)[Get started](#)

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.



[Open in app](#)[Get started](#)

Specify permissions to control access

Select Profile
Share Location
Share Name
Other Settings

Permissions

Confirmation

Results

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.



[Open in app](#)[Get started](#)

Confirm selections

[Select Profile](#)[Share Location](#)[Share Name](#)[Other Settings](#)[Permissions](#)**Confirmation**[Results](#)

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

SHARE LOCATION

Server: HYDRA-DC
Cluster role: Not Clustered
Local path: C:\hackme

SHARE PROPERTIES

Share name: hackme
Protocol: SMB
Access-based enumeration: Disabled
Caching: Enabled
BranchCache: Disabled
Encrypt data: Disabled

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

Shortly after you will see the message about share created successfully. You can close this dialog now.



[Open in app](#)[Get started](#)

View results

- Select Profile
- Share Location
- Share Name
- Other Settings
- Permissions
- Confirmation
- Results**

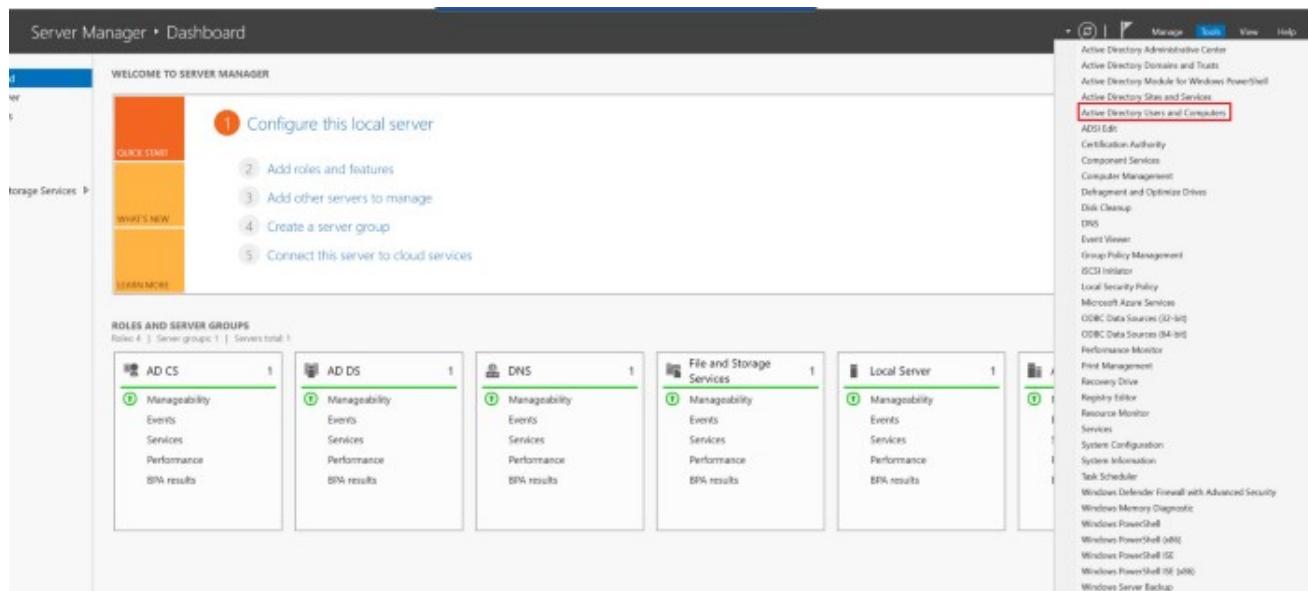
The share was successfully created.

Task	Progress	Status
Create SMB share	<div style="width: 100%;">Completed</div>	Completed
Set SMB permissions	<div style="width: 100%;">Completed</div>	Completed

[< Previous](#)[Next >](#)[Close](#)[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.



This will launch the **Active Directory Users and Computer** application as shown





Open in app

Get started

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a navigation pane displays the domain structure under 'Active Directory Users and Computers'. The 'Computers' node under the 'MARVEL.local' domain is currently selected. The main pane is titled 'Name' and 'Type' and contains the message 'There are no items to show in this view.' A horizontal scrollbar is visible at the bottom of the main pane.

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

The screenshot shows the same Active Directory Users and Computers interface after clicking on the 'Users' node. The 'Users' node is now expanded, revealing a list of security groups and individual users. The columns in the main pane are 'Name', 'Type', and 'Description'. The list includes standard security groups like 'Domain Admins', 'Domain Computers', and 'Guest', as well as individual users like 'kamran'. The 'Computers' node is still selected in the navigation pane.

Name	Type	Description
Allowed RODC Password Replication Group	Security Group...	Members in this group c...
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
Denied RODC Password Replication Group	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domain Controllers	Security Group...	Members of this group ...
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
kamran	User	Built-in account for ad...
Key Admins	Security Group...	Members of this group ...
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group ca...
Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...



The screenshot shows the Windows Start menu with the 'Active Directory Users and Computers' icon selected. The application window is open, displaying a list of security groups under the 'MARVEL' domain. A context menu is open at the bottom-left of the window, with 'New' highlighted. A secondary context menu is displayed, listing various object types: Computer, Contact, Group, InetOrgPerson, msDS-ShadowPrincipalContainer, msImaging-PSPs, MSMQ Queue Alias, and Organizational Unit. The 'Organizational Unit' option is highlighted with a red box.

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

The screenshot shows the 'New Object - Organizational Unit' dialog box. The 'Name' field contains 'Group'. The 'Create in' dropdown is set to 'MARVEL\local/'. A checkbox labeled 'Protect container from accidental deletion' is checked. To the right of the dialog, a preview pane displays a table of object types and their descriptions, with the 'Organizational Unit' row highlighted.

Type	Description
builtinDomain	Default container for up...
Container	Default container for do...
Organizational...	Default container for do...
Container	Default container for sec...
Container	Default container for ma...
Container	Default container for up...



[Open in app](#)[Get started](#)

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a navigation pane displays the domain structure under 'Active Directory Users and Computers' (MARVEL.local). The 'Users' folder is selected. On the right, a table lists users with their names, types, and descriptions.

Name	Type	Description
Guest	User	Built-in account for guest logins.
kamran	User	Built-in account for administrator access.

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



[Open in app](#)[Get started](#)

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a tree view shows the structure: Active Directory Users and Computers > Saved Queries > MARVEL.local > Builtin > Computers > Domain Controllers > ForeignSecurityPrincipal > Managed Service Account > Users > Groups. The 'Users' folder is selected. On the right, a table lists two users: Guest (User, Built-in account for guest...) and kamran (User, Built-in account for administrator...). A context menu is open over the 'New' option in the main menu, which includes options like 'Computer', 'Contact', 'Group', etc. The 'User' option is highlighted with a red box.

Creates a new item in this container.

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

The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: MARVEL.local/Users'. Below that, there are fields for 'First name:' (Frank), 'Last name:' (Castle), and 'Full name:' (Frank Castle). Under 'User logon name:', the 'User logon name' field contains 'fcastle' and the 'Domain' dropdown shows '@MARVEL.local'. Under 'User logon name (pre-Windows 2000):', the 'Domain' field contains 'MARVEL\)' and the 'Logon name' field contains 'fcastle'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

I used a kind of weak password **Password1**. Uncheck **User must change password at next logon** and check the option for **Do not password expire**. Click **Next**.





Open in app

Get started

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 Next > Cancel

Click Finish here.

New Object - User X

Create in: MARVEL.local/Users

When you click Finish, the following object will be created:

Full name: Frank Castle
User logon name: fcastle@MARVEL.local
The password never expires.

< Back Finish Cancel

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.





Open in app

Get started

Create in: MARVEL.local/Users

First name:	Peter	Initials:	<input type="text"/>
Last name:	Parker		
Full name:	Peter Parker		
User logon name:	pparker	@MARVEL.local	<input type="button" value="▼"/>
User logon name (pre-Windows 2000):	MARVEL\	pparker	

[< Back](#) [Next >](#) [Cancel](#)

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.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

Name	Type	Description
Guest	User	Built-in account for guest access to the computer/domain
kamran	User	Built-in account for administering the computer/domain
Frank	User	
Petre F	User	

Right-click context menu for the **kamran** user is open, with the **Copy...** option highlighted with a red box.

Disables the account for the current selection.

Let's give this user first name **S01**, last name **Service** and logon name of **S01 Service**.





Open in app

Get started

Create in: MARVEL.local/Users

First name: SQL Initials:

Last name: Service

Full name: SQL Service

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

Create in: MARVEL.local/Users

Password:

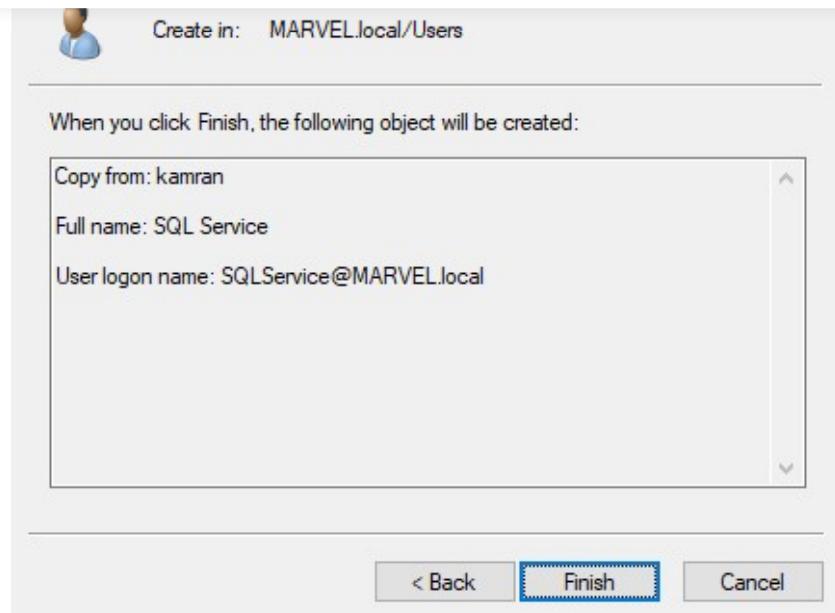
Confirm password:

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

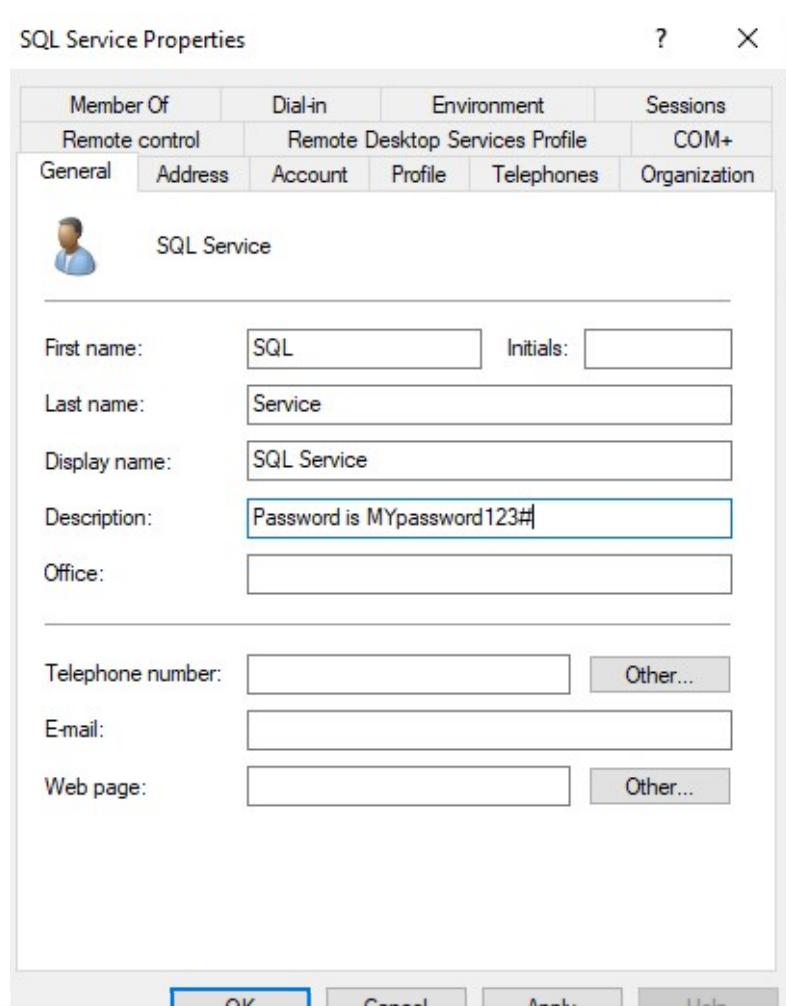
< Back Next > Cancel

Click Finish here.



[Open in app](#)[Get started](#)

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



[Open in app](#)[Get started](#)

```
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-A804-00C04FC2DCD2/4845b522-46e3-49d9-8dc6-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.



The screenshot shows the Windows Active Directory Users and Computers console. On the left, a tree view displays the domain structure under 'MARVEL.local': Active Directory Users and Computers, Saved Queries, MARVEL.local (with sub-nodes: Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Account, Users, Groups). The 'Computers' node is selected. The main pane on the right is titled 'Name' and lists 'Type' and 'Description'. It contains the message: '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 . : vx10vxmt3duuhciftc1cahbrsa.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's 'Virtual machines' page. The top navigation bar includes 'Microsoft Azure', a search bar, and a user profile. Below the navigation, the page title is 'Virtual machines' with a 'Default Directory' link. A red box highlights the '+ Add' button. Other buttons include 'Reservations', 'Edit columns', 'Refresh', 'Assign tags', 'Start', 'Restart', 'Stop', 'Delete', and 'Services'. A 'Subscriptions: Free Trial' section is present. At the bottom, there are filters for 'Name', 'Type', 'Status', 'Resource group', 'Location', 'Source', 'Maintenance status', and 'Subscription', along with a 'No grouping' dropdown. A table lists one item: 'HYDRA-DC' (Type: Virtual machine, Status: Running, Resource group: ADLab, Location: Canada Central, Source: Marketplace, Maintenance status: -, Subscription: Free Trial).



Open in app

Get started

- 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**

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The 'Basics' tab is selected. Key configuration details are highlighted:

- Virtual machine name:** ThePunisher (highlighted with a red box)
- Region:** (Canada) Canada Central
- Image:** Windows 10 Enterprise, Version 1909 (highlighted with a red box)
- Size:** Standard B1s (highlighted with a red box)
Description: 1 vcpu, 1 GiB memory (\$11.05/month)
- Administrator account:**
 - Username:** fcastle (highlighted with a red box)
 - Password:** myPassword01 (highlighted with a red box)

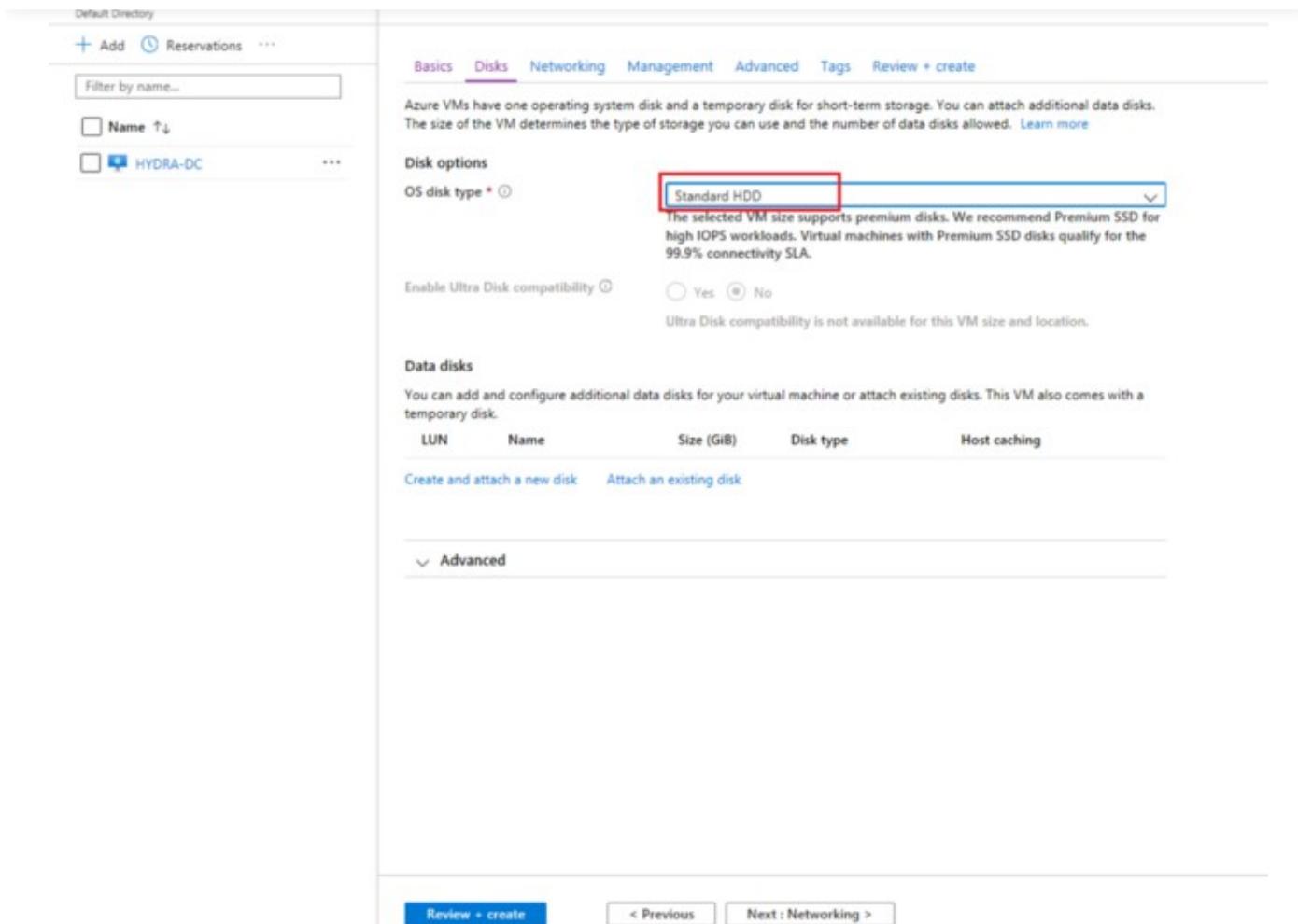
At the bottom, there are 'Review + create' and 'Next : Disks >' buttons.

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



 Open in app

Get started



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 *

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

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.



Default Directory

+ Add Reservations ...

Filter by name...

Name ↑↓

HYDRA-DC ...

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) ThePunisher-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 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 >](#)

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



The screenshot shows the Azure Marketplace interface for creating a new virtual machine. A green banner at the top indicates "Validation passed". The "Review + create" tab is selected. The "PRODUCT DATA" section shows a Standard B1s VM by Microsoft with a price of 0.0148 CAD/hr. The "TERMS" section contains legal text about agreeing to Microsoft's terms and privacy statement. A warning message in a yellow box states: "⚠ 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." Below this, the "Basics" section lists configuration details: 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). The "Disks" section shows OS disk type (Standard HDD) and Use managed disks (Yes). At the bottom are "Create", "Previous", "Next >", and "Download a template for automation" buttons.

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.

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named "CreateVm-MicrosoftWindowsDesktop.Windows-10-19h2--20200105001945". A green banner at the top says "Your deployment is complete". The "Deployment details" section shows the deployment name, subscription (Free Trial), resource group (ADLab), start time (1/5/2020 12:26:04 AM), and correlation ID (c6947723-ad52-4900-b72a-eb7c040f3a8d). Below this are sections for "Deployment details" (with a "Download" link) and "Next steps" (including "Setup auto-shutdown Recommended", "Monitor VM health, performance and network dependencies Recommended", and "Run a script inside the virtual machine Recommended"). At the bottom is a "Go to resource" button.





Open in app

Get started

Resource group (changed): ADLab

Status: Running

Location: Canada Central

Subscription ID: 10d0f9e0-0000-4079-9000-000000000000

Computer name: (Not available)

Operating system: Windows

Size: Standard B1s (1 vCore, 1.0 GB memory)

Tags (change): Click here to add tags

Azure Spot: N/A

Public IP address: 10.0.1.5

Private IP address (IPv4): -

Public IP address (IPv6): -

Private IP address (IPv6): -

Virtual network/subnet: ADLabNet/Default

DNS name: Configure

Scale Set: N/A

Show data for last: 1 hour, 6 hours, 12 hours, 1 day, 7 days, 30 days

CPU (average)

Network (total)

Disk bytes (total)

Disk operations/sec (average)

Monitoring Insights (preview)

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.

File Network View

Network

Quick access

This PC

Network

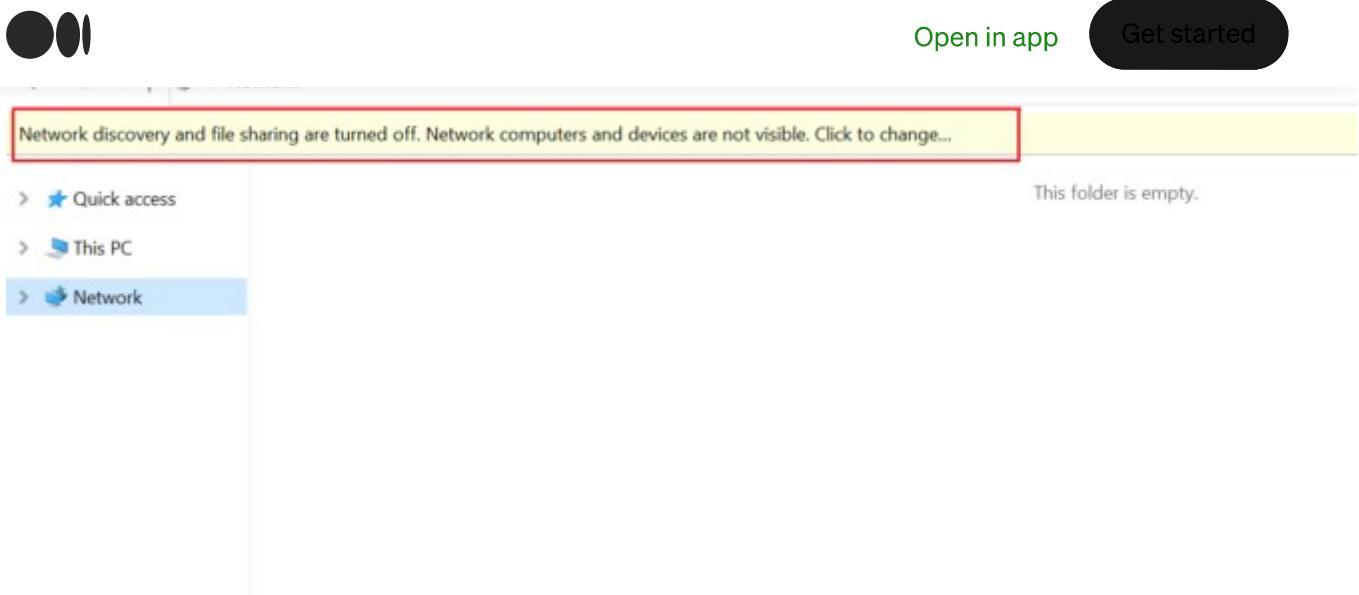
Network

Network discovery is turned off. Network computers and devices are not visible. Please turn on network discovery in Network and Sharing Center.

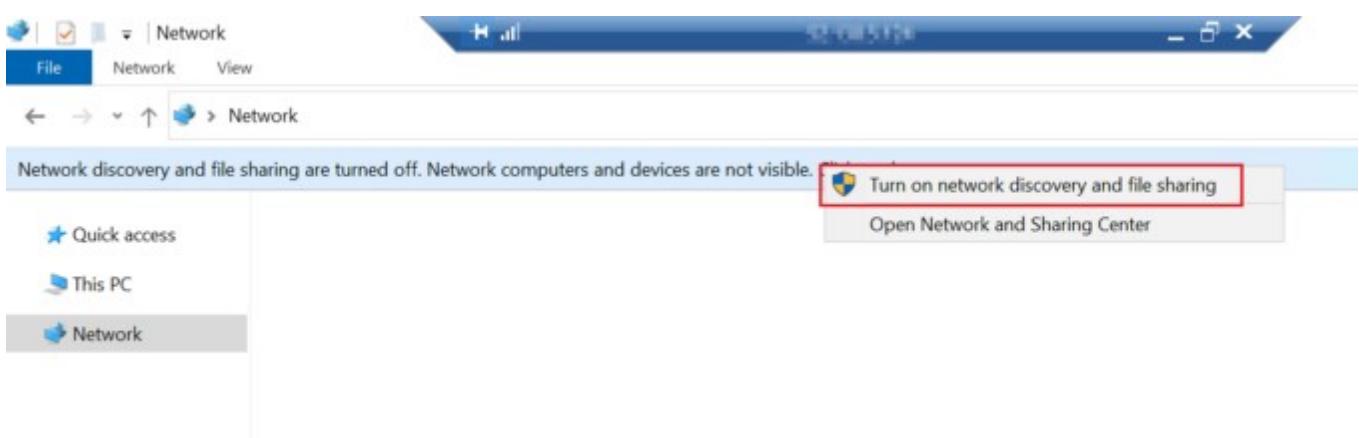
OK

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.



[Open in app](#)[Get started](#)

Do you want to turn on network discovery and file sharing for all public networks?

→ No, make the network that I am connected to a private network

Network discovery and file sharing will be turned on for private networks, such as those in homes and workplaces.

→ Yes, turn on network discovery and file sharing for all public networks

[Cancel](#)

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



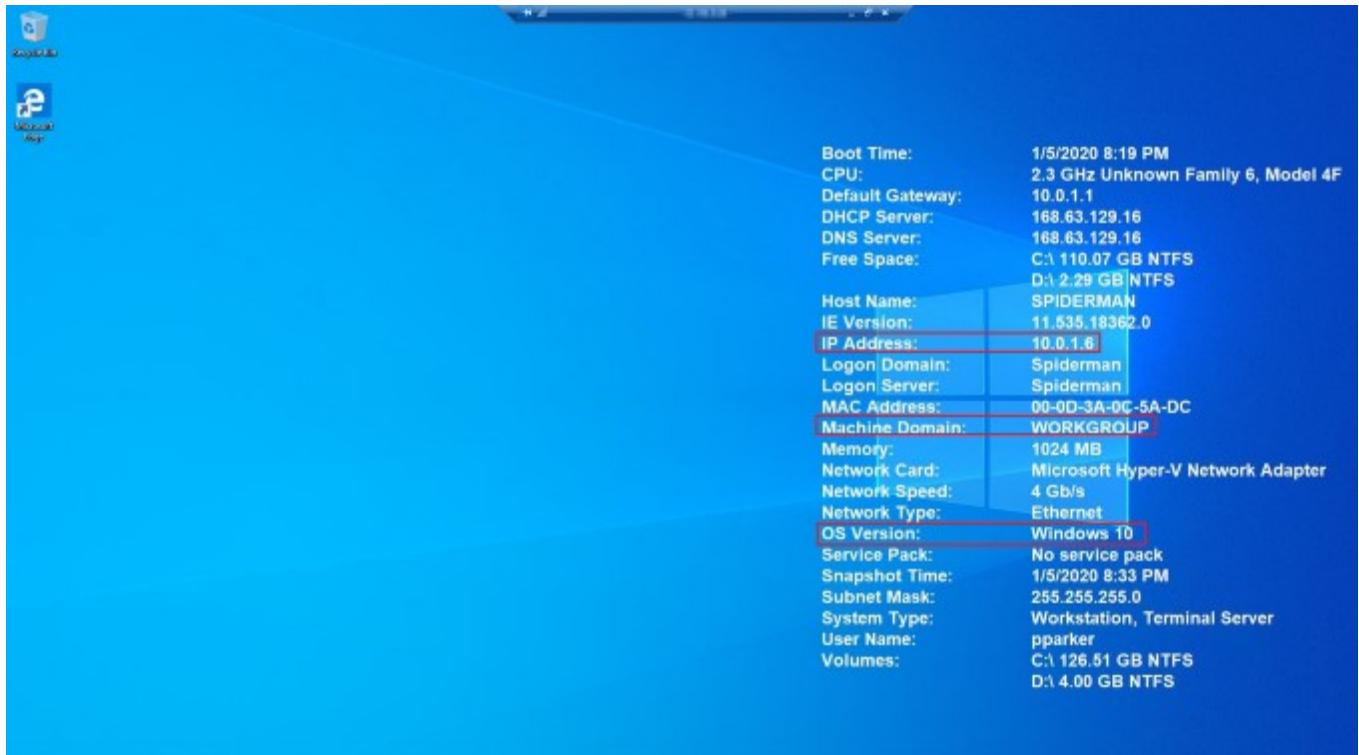
Setting up the second User Machine

The steps for creating the second User machine are exactly the same as for the first user



[Open in app](#)[Get started](#)

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.

The screenshot shows the Microsoft Azure Virtual Machines page. It lists three virtual machines:

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

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.



[Open in app](#)[Get started](#)

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.



[Open in app](#)[Get started](#)

Home

Find a setting

Network & Internet

Status

Ethernet

Dial-up

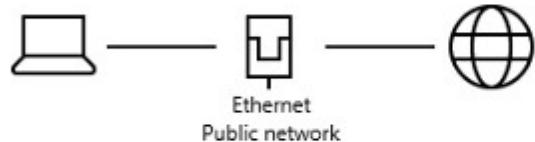
VPN

Data usage

Proxy

Status

Network status



You're connected to the Internet

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

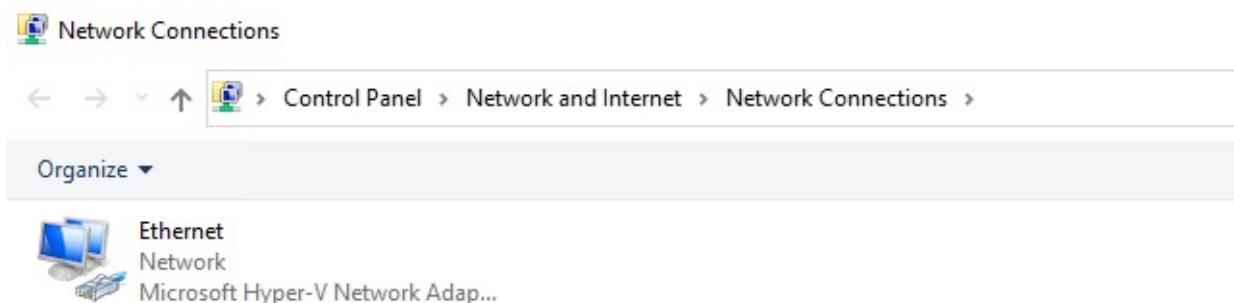
[Change adapter options](#)
View network adapters and change connection settings.

Click on the **Change adapter options**.



The screenshot shows the Windows Control Panel under 'Network & Internet'. On the left, a sidebar lists options: Status, Ethernet (which is selected and highlighted in blue), Dial-up, VPN, Data usage, and Proxy. The main pane is titled 'Ethernet' and shows a status icon with 'Connected'. Below the title, there's a section titled 'Related settings' with a red box around the link 'Change adapter options'. Other links in this section include 'Change advanced sharing options', 'Network and Sharing Center', and 'Windows Firewall'. At the bottom, there's a 'Have a question?' section with links to 'Troubleshooting network connection issues' and 'Get help'.

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

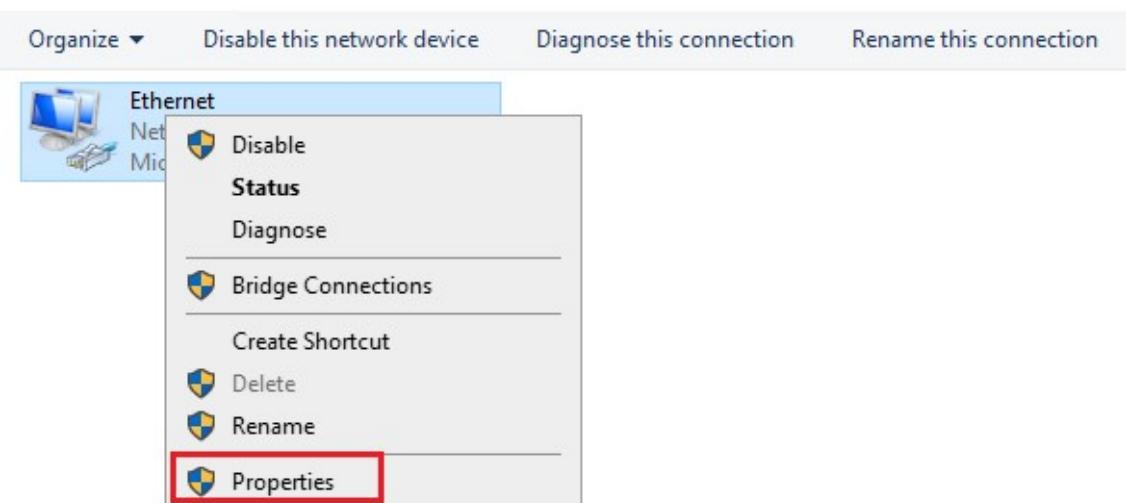


Right-click on the Ethernet and click on the properties menu item.

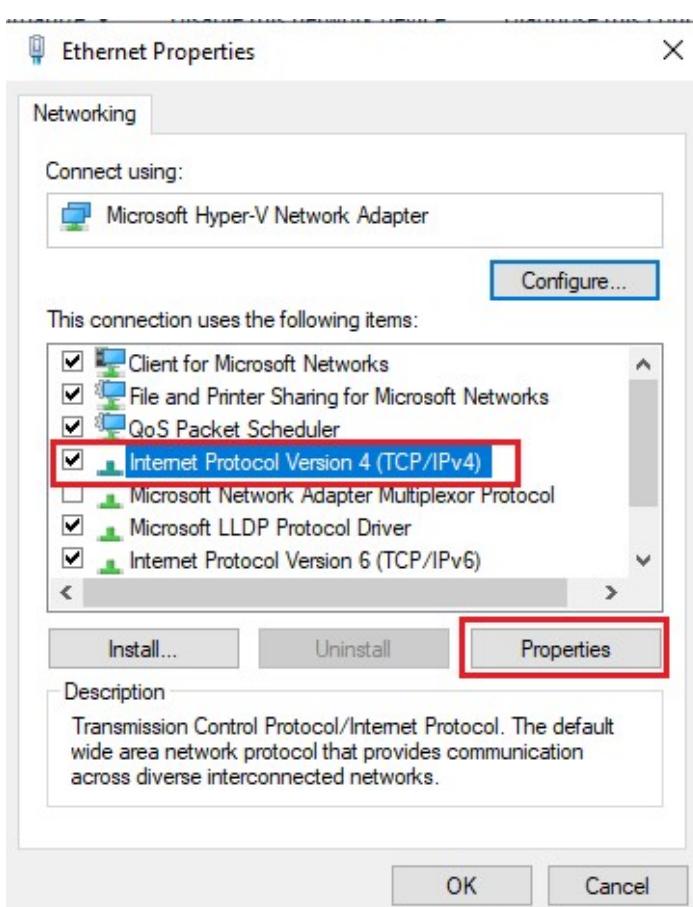


Open in app

Get started



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 D^L address for this machine.



[Open in app](#)[Get started](#)

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

Subnet mask:

Default gateway:

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Validate settings upon exit [Advanced...](#)

[OK](#) [Cancel](#)

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.





Open in app

Get started

Best match



Access work or school

System settings

Apps



Control Panel



Search the web



access - See web results



Settings (8+)



access|work or school



The screenshot shows the Microsoft Settings app interface. On the left, a sidebar lists various settings categories: Home, Find a setting (search bar), Accounts, Your info, Email & accounts, Sign-in options, Access work or school (which is selected and highlighted in blue), Other users, and Sync your settings. On the right, the main content area has a title 'Access work or school'. It explains that connecting to work or school resources might control some device settings. A large 'Connect' button with a plus sign is prominently displayed, with a red box highlighting it. Below the button, under 'Related settings', are links to 'Add or remove a provisioning package', 'Export your management log files', 'Set up an account for taking tests', and 'Enroll only in device management'. At the bottom, there's a 'Have a question?' section with a link to a help page.

Open in app Get started

Settings

Home

Find a setting

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Other users

Sync your settings

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

Add or remove a provisioning package

Export your management log files

Set up an account for taking tests

Enroll only in device management

Have a question?

[Open in app](#)[Get started](#)

Set up a work or school account

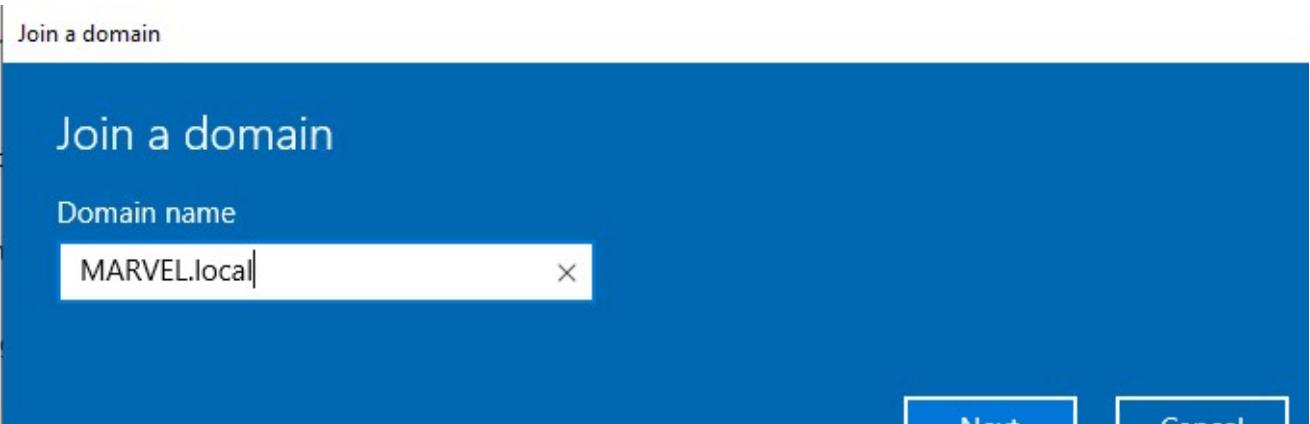
You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

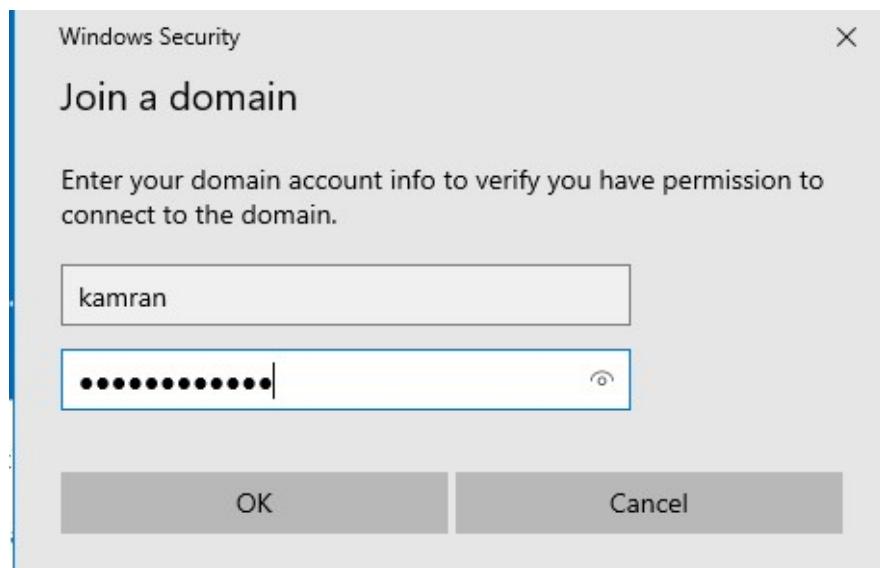
Alternate actions:

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

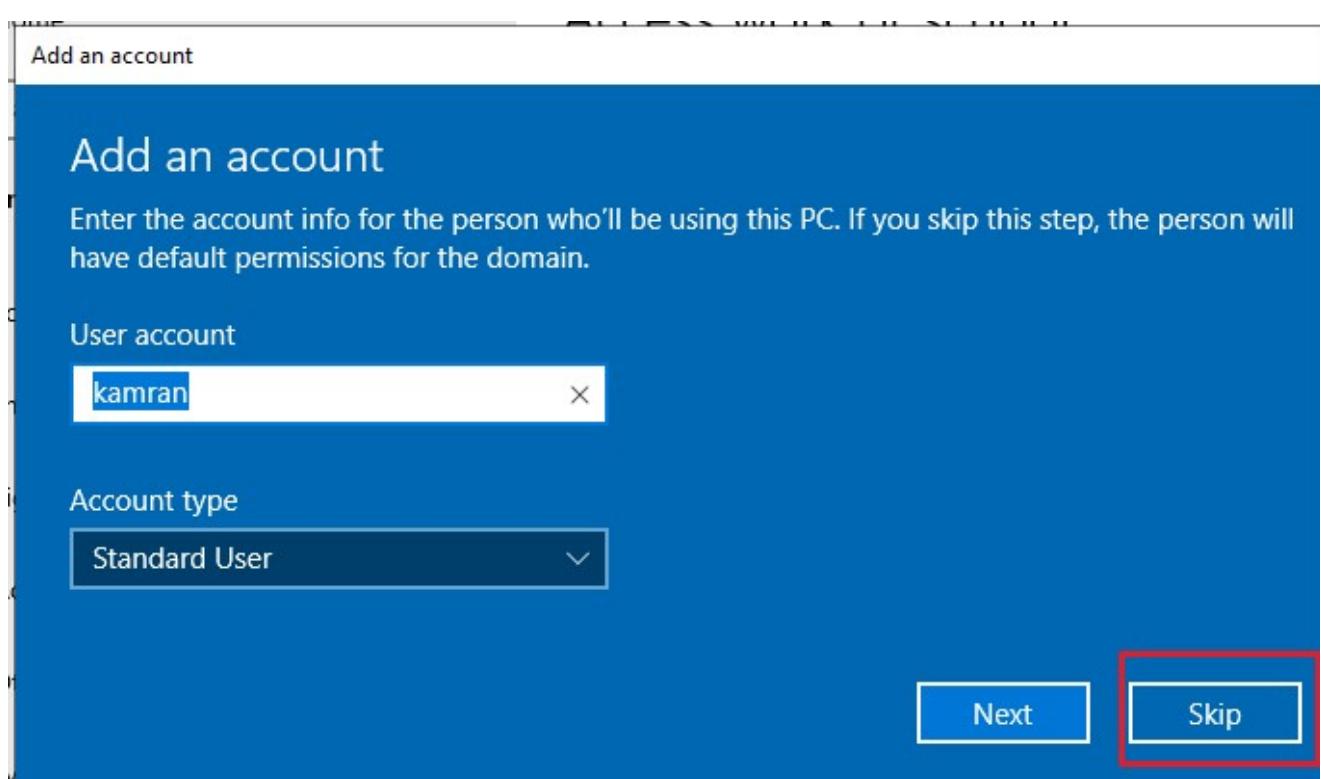
[Join this device to Azure Active Directory](#)[Join this device to a local Active Directory domain](#)[Next](#)

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



[Open in app](#)[Get started](#)

Click on the Skip on the next dialog.



Finally choose to **Restart now**.



[Open in app](#)[Get started](#)

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. On the left, the navigation pane displays the tree structure of the domain: Active Directory Users and Computers, Saved Queries, MARVEL.local (which is expanded to show Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Accounts, Users, and Groups). In the main pane, there is a table listing two computer objects:

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.



[Open in app](#)[Get started](#)

Enter your credentials

These credentials will be used to connect to **192.168.1.100**.

Domain: MARVEL

Remember me

More choices



192.168.1.100\kamran



Use a different account

OK

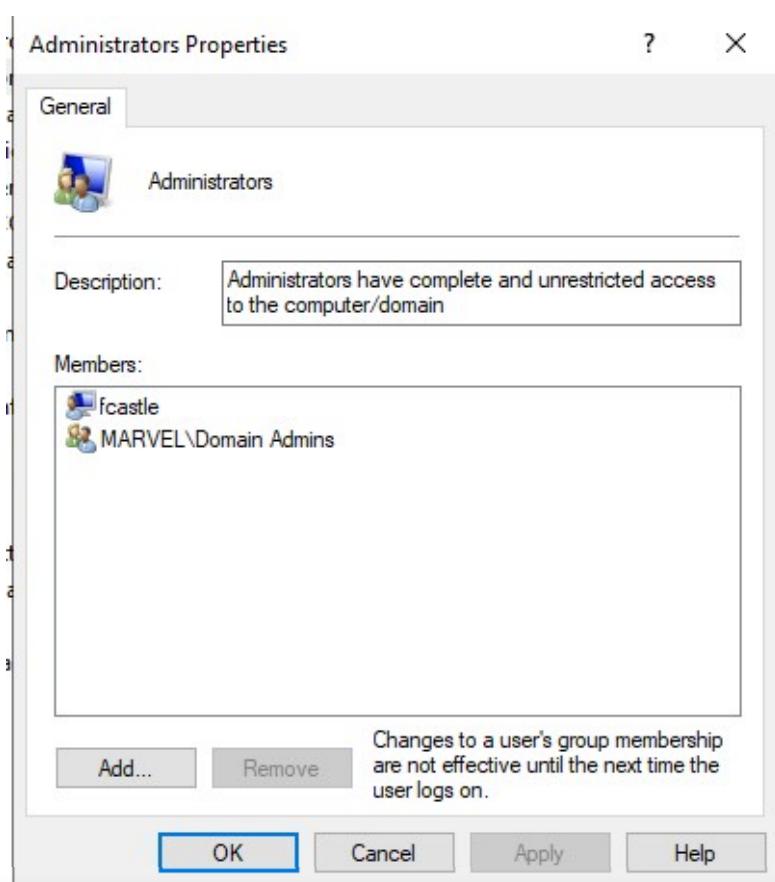
Cancel

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



Name	Description
Access Control Assistance Operators	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operators	Members are authorized to perfor...
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 ...

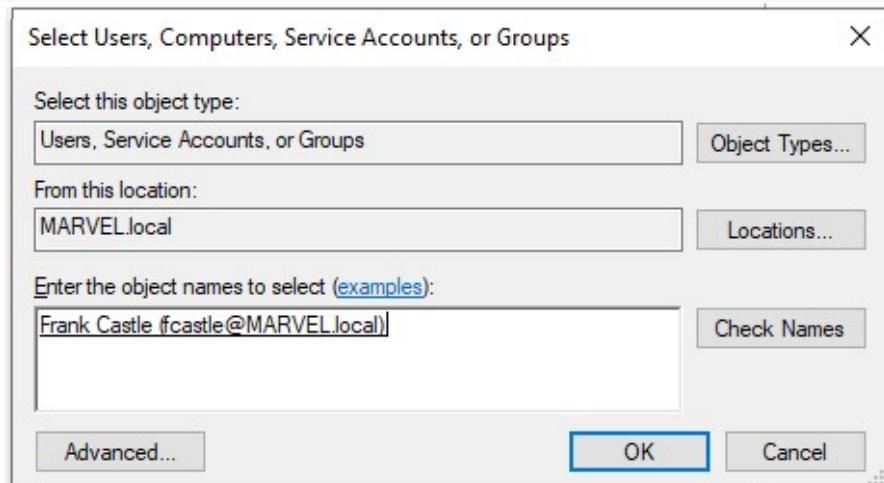
It will show existing users in this group. Click **Add** here.



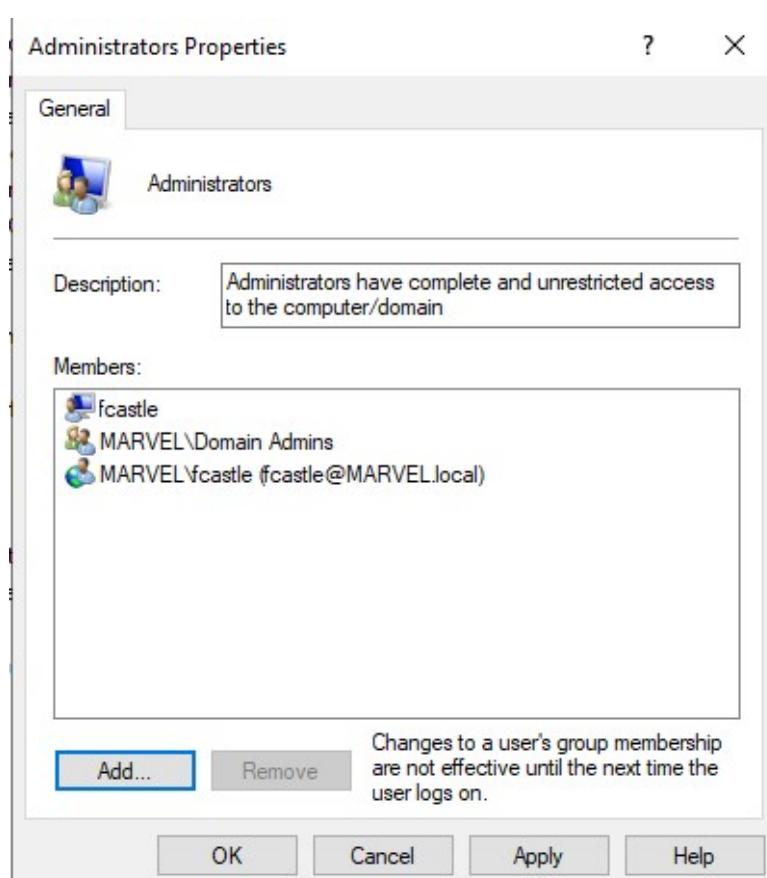


Open in app

Get started



This will add that user as local Administrator.



Repeat the same steps for domain user Petre Parker.



[Open in app](#)[Get started](#)

The screenshot shows the 'Administrators' group properties window. At the top, there's a thumbnail icon of three people. Below it, the title 'Administrators' is displayed. A description box contains the text: 'Administrators have complete and unrestricted access to the computer/domain'. The 'Members:' section lists four entries: 'fcastle', 'MARVEL\Domain Admins', 'MARVEL\fcastle (fcastle@MARVEL.local)', and 'MARVEL\pparker (pparker@MARVEL.local)'. Below the members list are two buttons: 'Add...' (highlighted with a blue border) and 'Remove'. A note below the buttons states: 'Changes to a user's group membership are not effective until the next time the user logs on.' At the bottom of the window are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

Let's login to the **spiderman** machine as a domain administrator and add the **Marvel\ppar1** as the local admin.





Open in app

Get started

The screenshot shows the Windows Computer Management interface. On the left, under 'Local Users and Groups', the 'Groups' folder is selected. On the right, a list of groups is shown, with 'Administrators' highlighted. A properties dialog box for 'Administrators Properties' is open, showing the 'General' tab. The group name is 'Administrators' and its description is 'Administrators have complete and unrestricted access to the computer/domain'. The 'Members:' section lists several users: 'MARVEL\Domain Admins', 'MARVEL\pparker (pparker@MARVEL.local)', and 'pparker'. At the bottom of the dialog box, a note states: 'Changes to a user's group membership are not effective until the next time the user logs on.' Below the dialog are standard Windows buttons: 'Add...', 'Remove', 'OK', 'Cancel', 'Apply', and 'Help'.

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.

The screenshot shows the Microsoft Azure Virtual machines dashboard. The top navigation bar includes 'Home > Virtual machines' and a search bar. Below the navigation, there are buttons for 'Add', 'Reservations', 'Edit columns', 'Refresh', 'Assign tags', 'Start', 'Restart', 'Stop', 'Delete', and 'Services'. A 'Subscriptions: Free Trial' section is present, along with filters for 'Filter by name...', 'All resource groups', 'All types', 'All locations', and a checkbox for '1 of 3 items selected'. The main table lists three virtual machines: 'HYDRA-DC' (Virtual machine, Running, ADLab, Canada Central, Marketplace), 'Spiderman' (Virtual machine, Running, ADLab, Canada Central, Marketplace), and 'ThePunisher' (Virtual machine, Running, ADLab, Canada Central, Marketplace). At the bottom of the page are icons for 'Home', 'Search', and 'Profile'.

[Open in app](#)[Get started](#)

Create a virtual machine

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 * ⓘ

kali



Region * ⓘ

(Canada) Canada Central



Availability options ⓘ

No infrastructure redundancy required



Image * ⓘ

Kali Linux



[Browse all public and private images](#)

Azure Spot instance ⓘ

Yes No

Size * ⓘ

Standard B1ms

1 vcpu, 2 GiB memory (\$21.90/month)

[Change size](#)

Administrator account

Authentication type ⓘ

Password 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 can use.



[Open in app](#)[Get started](#)[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

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 Collecto



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.



[Open in app](#)[Get started](#)

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		
<hr/>				

⌄ Advanced

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

Use the existing Virtual network ADLabNet.



[Open in app](#)[Get started](#)

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.



Open in app **Get started**

Resource group (changed) : ADLab

Status : Running
Location : Canada Central
Subscription ID : 6d03f8e0-4762-4080-86a3-200a07ae1bb0
Computer name : kali
Operating system : Linux (Kali-kali-rolling)
Size : Standard E1s (1 vcores, 2 GiB memory)
Tags (change) : Click here to add tags

Power Spot : N/A
Public IP address : 10.0.0.100 (192.168.1.100)
Private IP address : 10.0.1.7
Public IP address (IPv6) : -
Private IP address (IPv6) : -
Virtual network/Subnet : ADLabNet/default
DNS name : Configure
Scale Set : N/A

Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 days

CPU (average)

Network (total)

Disk bytes (total)

Disk operations/sec (average)

I use putty to connect to the Kali machine using SSH.

Home Search User profile

[Open in app](#)[Get started](#)

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Translation
- Selection
 - Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH
 - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

hacker@5.10.1.10 22

Connection type:

 Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

[Load](#)[Save](#)[Delete](#)

Close window on exit:

 Always Never Only on clean exit[About](#)[Help](#)[Open](#)[Cancel](#)

Once I logged in, I ran netdiscover utility to find the machines.

```
hacker@kali: ~
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.





Open in app

Get started

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
```

Nmap scan for the two user machines is shown below.



[Open in app](#)[Get started](#)

```
Nmap scan report for 10.0.1.6
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!!!

