mpram / **Azure-Defender-for-IoT** Public

Code Issues Pull requests Actions Projects Wiki Security

main

Azure-Defender-for-IoT / Before HOL / **Azure Defender for IoT BHOL.md**

mpram Azure Defender for IoT/OT HOL **History**

3 contributors

275 lines (143 sloc) 10.7 KB

Before Hands-on Lab

During this time, we will set up the environment that is required for the Hands-on Lab.

Content:

Exercise 1: Azure Passes

Previous to this workshop, after registration, you will receive an Azure Pass to configure with your personal email account, this step will be coordinated with your instructors.

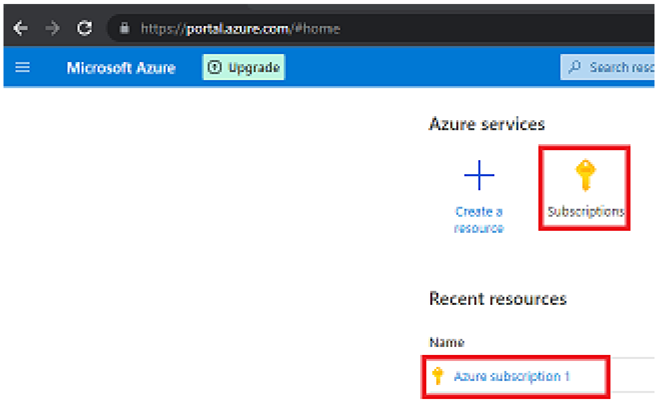
Go to this link: https://www.microsoftazurepass.com/

Click on **START**, make sure you set up this pass with a personal email or just create an outlook email account for this training. After you login and validate the account. You will ask to **Enter the Promo Code**, here you will copy the Azure Pass Code you receive by email and then click on **Claim Promo Code**.

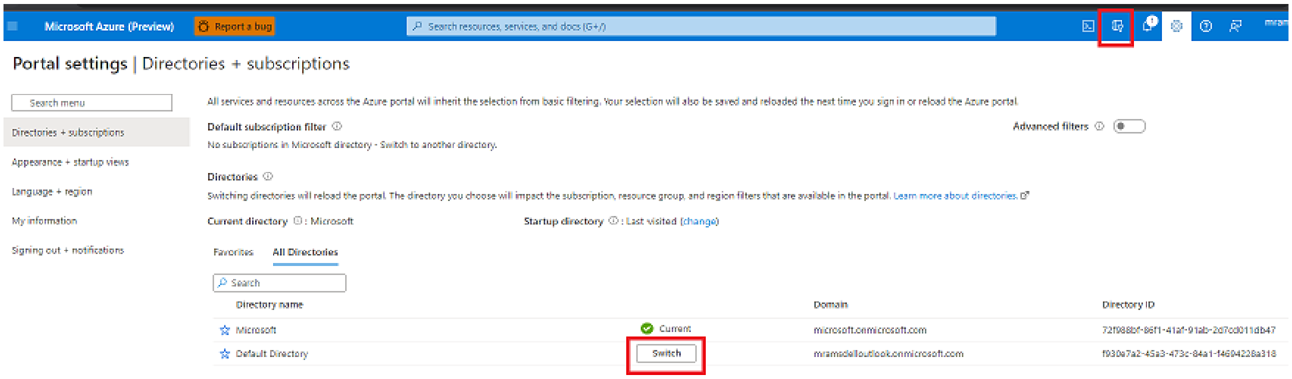
Next, fill the form with your name, after a few minutes you should have a Subscription available to start setting up your servicces in the next exercises.

To validate your subscription is active, go to Azure Portal: https://portal.azure.com/

Right in the home portal you should see the icon for **Subscriptions** click on it you sould see a new Subscription available, also the same subscription could be available in the **Recent Resources** list.



If you don't see your subscription, validate you are accessing the right directory. Go to the top right corner menu, select **Directories+Subscriptions** icon and **Switch** button to change and validate again.


Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
Search menu
Directories + subscriptions
Appearance + startup views
Language + region
My information
Signing out + notifications
Favorites
All Directories
Search
Switch

Portal settings | Directories + subscriptions

All services and resources across the Azure portal will inherit the selection from basic filtering. Your selection will also be saved and reloaded the next time you sign in or reload the Azure portal.

Default subscription filter

No subscriptions in Microsoft directory - Switch to another directory.

Advanced filters

Directories

Switching directories will reload the portal. The directory you choose will impact the subscription, resource group, and region filters that are available in the portal. Learn more about directories.

Current directory : Microsoft

Startup directory : Last visited (change)

Directory name		Domain	Directory ID
☆ Microsoft	✓ Current	microsoft.onmicrosoft.com	72f988bf-86f1-41af-91ab-2d7cd011db47
☆ Default Directory	Switch	mramsdelloutlook.onmicrosoft.com	f930e7a2-45a3-473c-84a1-f4694228a318

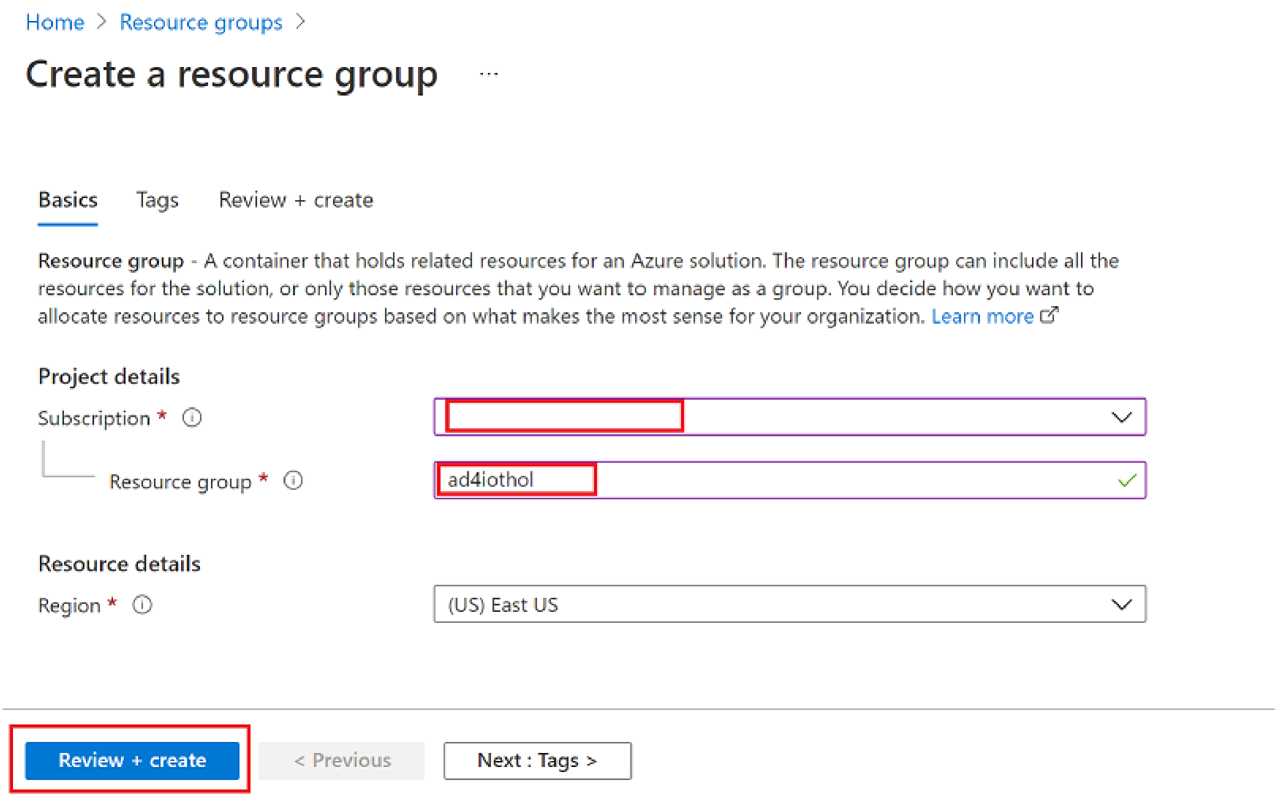
Exercise 2: Set up Environment

Once your Azure Pass is activated and you have a new subscription to work with we will move to this exercise to create a resource group for all the services we will use to build our architecture.

Task 1: Resources

1. In Azure Portal, create a new Resource Group, from the home Page, select **+ Create a Resource** in the search box type **Resource Group**, then select **Create**.

In the next window, select your subscription, assign a name to the resource group **adt4iot+SUFFIX**, select a location and click on **Review + Create**, once you passed the validation, click **create** again



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 *

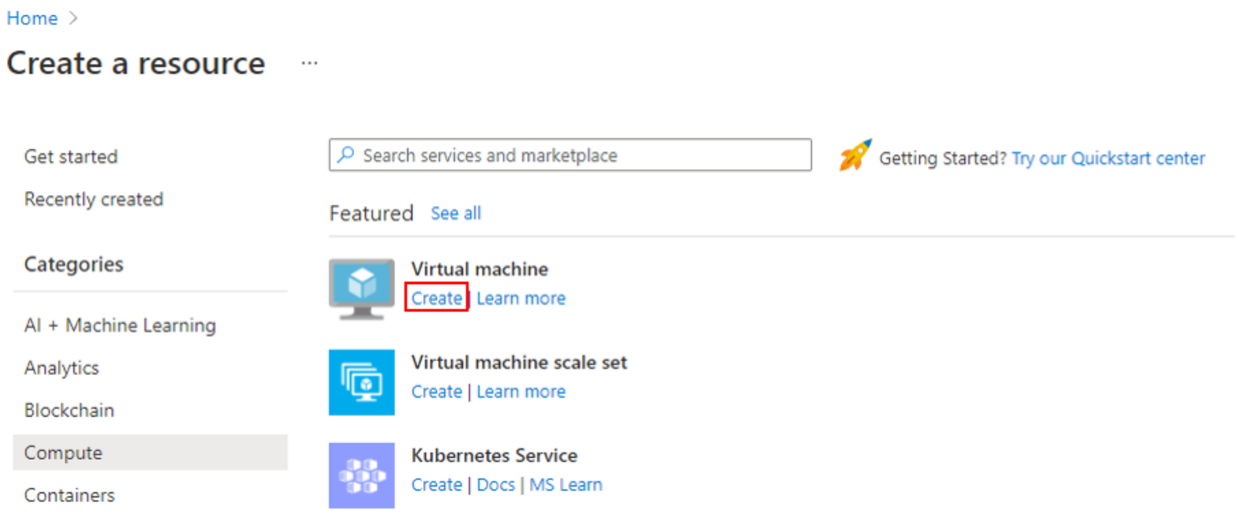
Resource group * ad4iothol

Resource details

Region * (US) East US

Task 2: Virtual Machine

1. On the upper-left side of the portal, select: **Create a resource** > **Compute** > **Virtual machine** >> **Create**

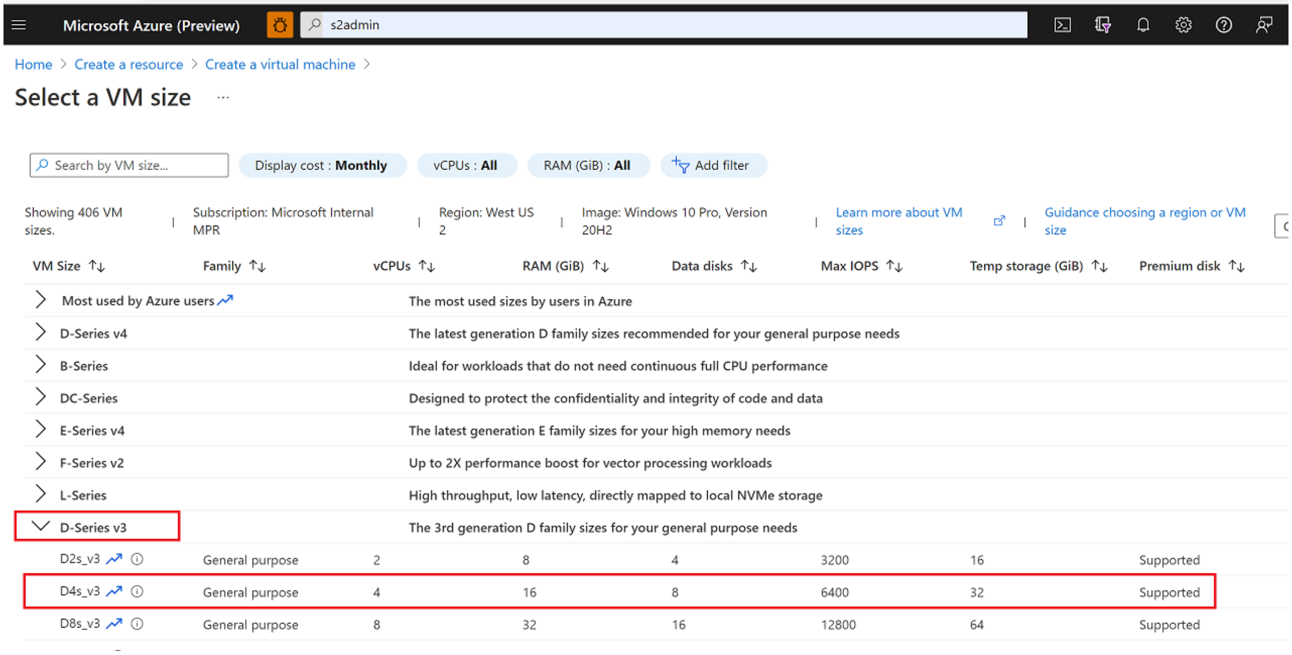


2. In **Create a virtual machine**, type or select the values in the **Basics** tab:

Setting	**Value**
Project Details	
Subscription	Select your Azure subscription
Resource Group	Select Your Resource Group
Instance details	
Virtual machine name	Enter **myofflinesensor**
Region	Select **(US) East US**
Availability Options	Select **No infrastructure redundancy required**
Image	Select **Windows 10 Pro, Version 20H2 - Gen2**
Azure Spot instance	Select **No**
Size	**D4s_v3 - 4 vcpus, 16 GiB memory**, see image below
Administrator Account	**Use the following Credentials**
Username	**ADefenderlab**
Password	**Learningmode123!**

Setting	Value
Confirm password	**Learningmode123!**
Inbound port rules	
Public inbound ports	Select **3389**.
Licensing	
I confirm I have an eligible Windows 10 license with multi-tenant hosting rights.	**Check the box.**

3. In the Size section, select **See all Images**, look for the **D-Series v3** open that section, then you will find the right VM.


Microsoft Azure (Preview)
s2admin
Home > Create a resource > Create a virtual machine >
Select a VM size ···
Search by VM size...
Add filter
Learn more about VM sizes
Guidance choosing a region or VM size

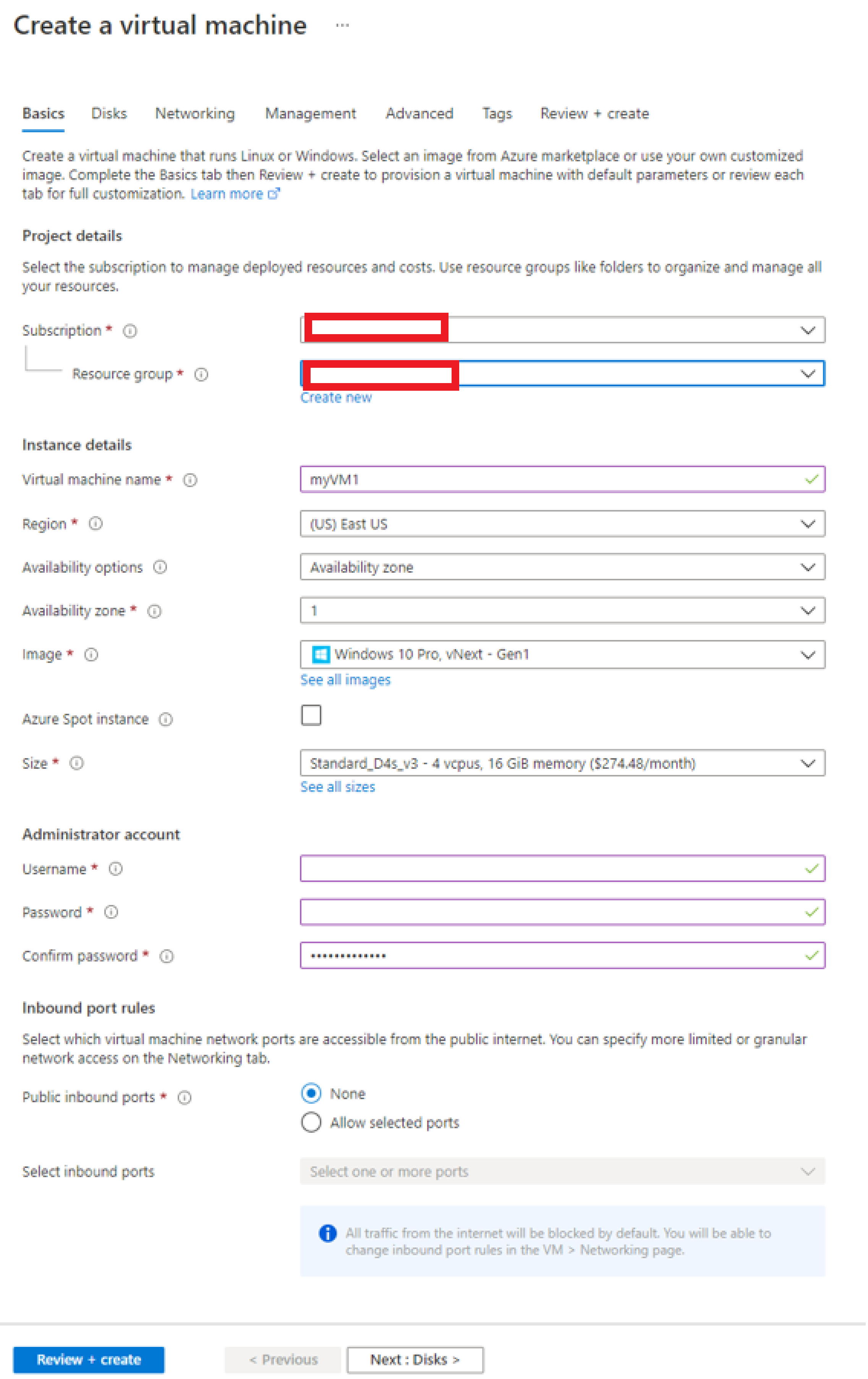
Display cost : **Monthly** vCPUs : **All** RAM (GiB) : **All**

Showing 406 VM sizes. | Subscription: Microsoft Internal MPR | Region: West US 2 | Image: Windows 10 Pro, Version 20H2

VM Size ↑↓	Family ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓	Temp storage (GiB) ↑↓	Premium disk ↑↓
> Most used by Azure users	The most used sizes by users in Azure						
> D-Series v4	The latest generation D family sizes recommended for your general purpose needs						
> B-Series	Ideal for workloads that do not need continuous full CPU performance						
> DC-Series	Designed to protect the confidentiality and integrity of code and data						
> E-Series v4	The latest generation E family sizes for your high memory needs						
> F-Series v2	Up to 2X performance boost for vector processing workloads						
> L-Series	High throughput, low latency, directly mapped to local NVMe storage						
∨ D-Series v3	The 3rd generation D family sizes for your general purpose needs						
D2s_v3	General purpose	2	8	4	3200	16	Supported
D4s_v3	General purpose	4	16	8	6400	32	Supported
D8s_v3	General purpose	8	32	16	12800	64	Supported

4. Go to the **Management**, in the **Monitoring** section, select **Disable** for **Boot Diagnostics**

5. At the bottom click on **Review + Create**. Once the validation is complete, select **Create**



Create a virtual machine ...

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. Learn more

Project details

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

Subscription * : [redacted]

Resource group * : [redacted]

Create new

Instance details

Virtual machine name * : myVM1 ✓

Region * : (US) East US

Availability options : Availability zone

Availability zone * : 1

Image * : Windows 10 Pro, vNext - Gen1

See all images

Azure Spot instance : □

Size * : Standard_D4s_v3 - 4 vcpus, 16 GiB memory ($274.48/month)

See all sizes

Administrator account

Username * : ✓

Password * : ✓

Confirm password * : •••••••••••••• ✓

Inbound port rules

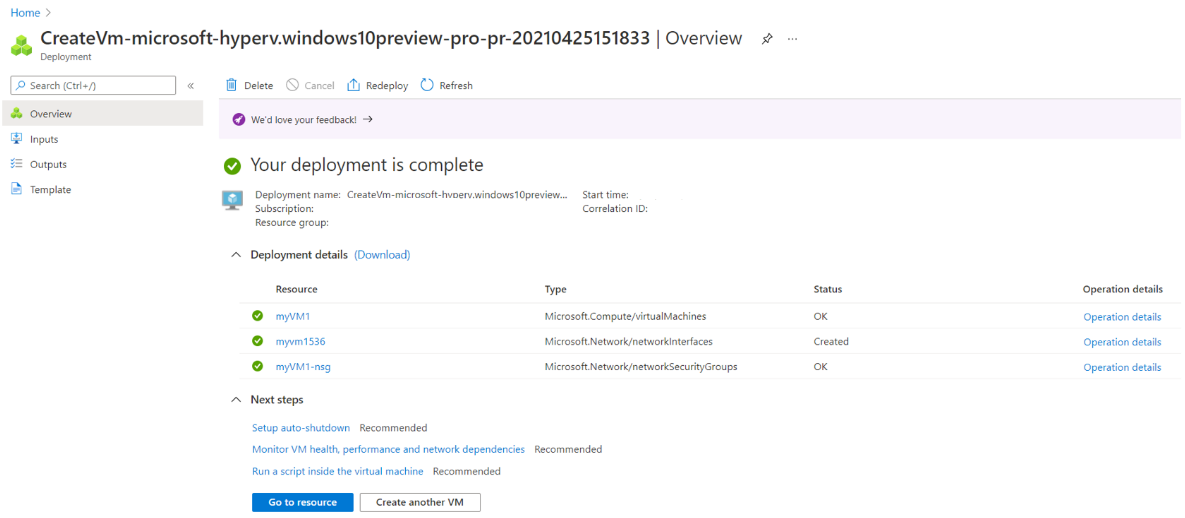
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * : ● None ○ Allow selected ports

Select inbound ports : Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

6. It will take a few minutes to deploy. At the end you should see your resources deployed.



CreateVm-microsoft-hyperv.windows10preview-pro-pr-20210425151833 | Overview

Deployment

Your deployment is complete

Deployment name: CreateVm-microsoft-hyperv.windows10preview...
Subscription:
Resource group:
Start time:
Correlation ID:

Deployment details (Download)

Resource	Type	Status	Operation details
myVM1	Microsoft.Compute/virtualMachines	OK	Operation details
myvm1536	Microsoft.Network/networkInterfaces	Created	Operation details
myVM1-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details

Next steps

Setup auto-shutdown Recommended

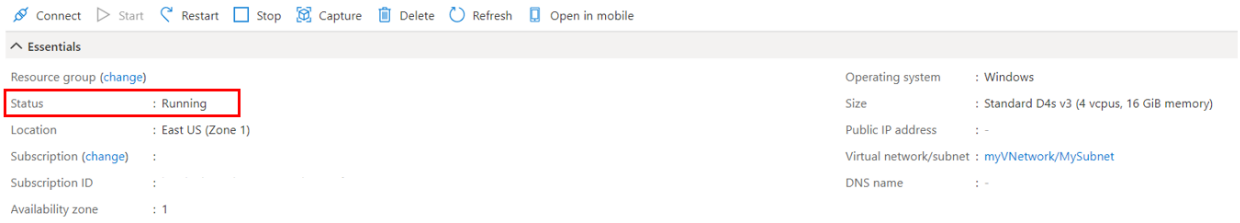
Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

Task 3: Connect to Virtual Machine

1. Navigate to the Azure Portal Home and select your newly created virtual machine.

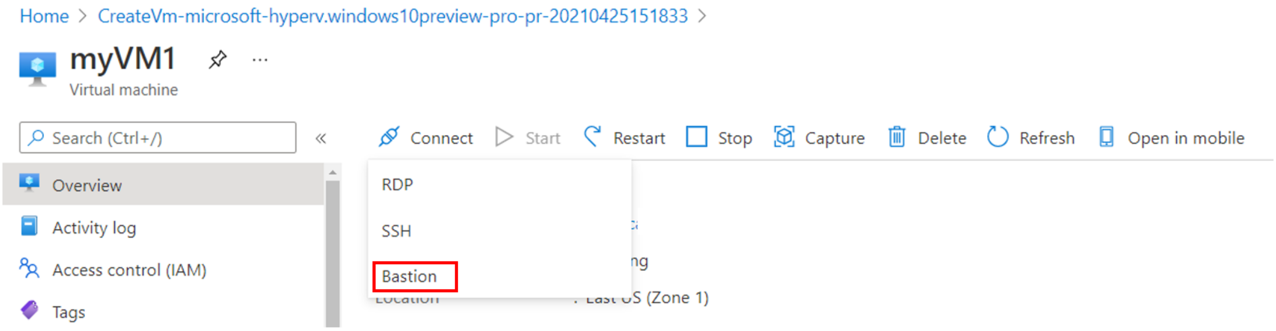
2. Make sure that the Virtual Machine status is **Running**.



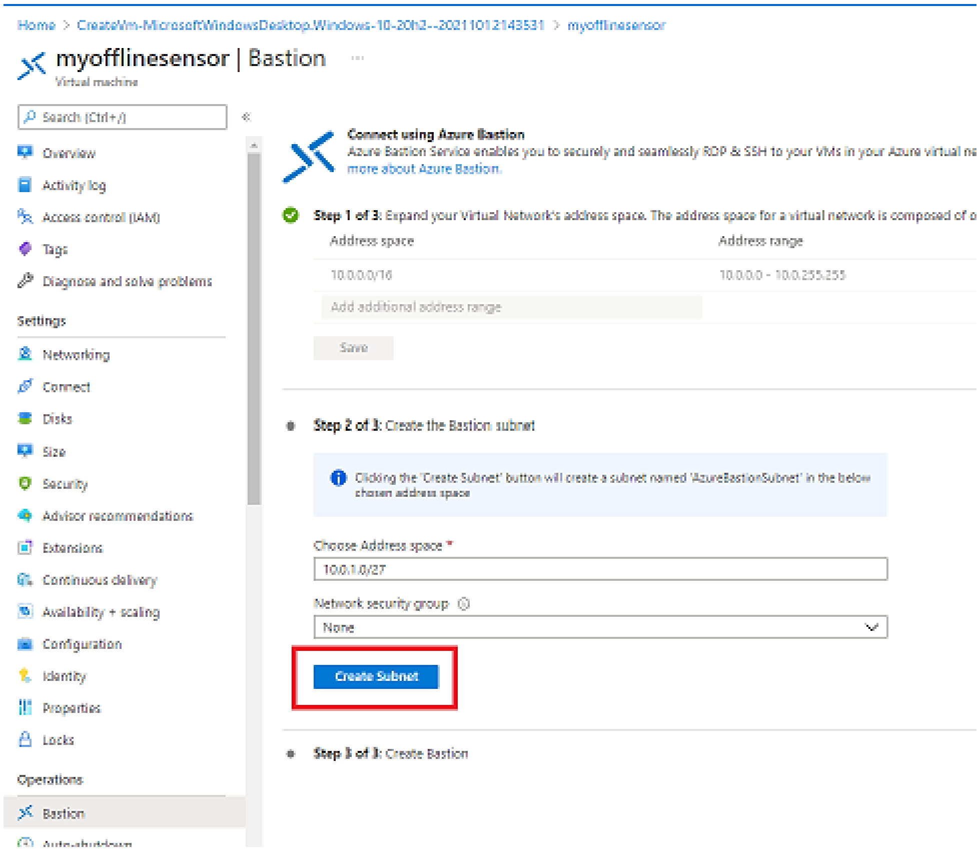
Resource group (change)	
Status	: Running
Location	: East US (Zone 1)
Subscription (change)	:
Subscription ID	:
Availability zone	: 1
Operating system	: Windows
Size	: Standard D4s v3 (4 vcpus, 16 GiB memory)
Public IP address	: -
Virtual network/subnet	: myVNetwork/MySubnet
DNS name	: -

> [!TIP] You will not be able to connect if your Virtual Machines is not in **Running** status. So give it a minute or two to finish updating.

3. In the VM menu, select **Connect**, then select **Bastion** or **RDP**.



4. If you select **Bastion** you will be ask to set it up in 3 steps, **Step 1** it is completed, for **Step 2**, click on **Create Subnet**, after step 2 is completed, **Step 3** will set up a public ip, scroll down and click on **Create Azure Bastion using defaults**



Connect using Azure Bastion
Azure Bastion Service enables you to securely and seamlessly RDP & SSH to your VMs in your Azure virtual ne
more about Azure Bastion.

Step 1 of 3: Expand your Virtual Network's address space. The address space for a virtual network is composed of o

Address space	Address range
10.0.0.0/16	10.0.0.0 - 10.0.255.255
Add additional address range	

Step 2 of 3: Create the Bastion subnet

Clicking the 'Create Subnet' button will create a subnet named 'AzureBastionSubnet' in the below chosen address space

Choose Address space * 10.0.1.0/27

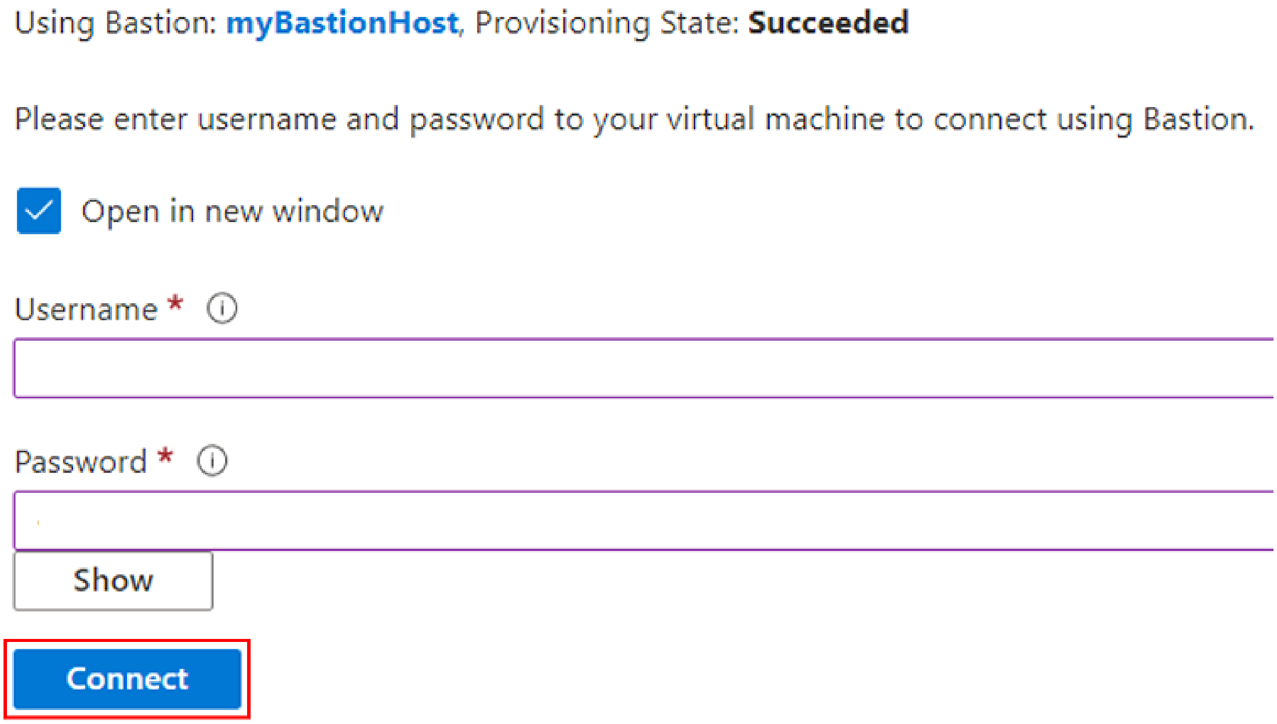
Network security group: None

Step 3 of 3: Create Bastion

After a few minutes you will be able to login

In the **Bastion** page, click on **Use Bastion** then enter the username and password for the virtual machine.

Field	Enter
Username	*ADefenderlab*
Password	*Learningmode123!*



Using Bastion: **myBastionHost**, Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

☑ Open in new window

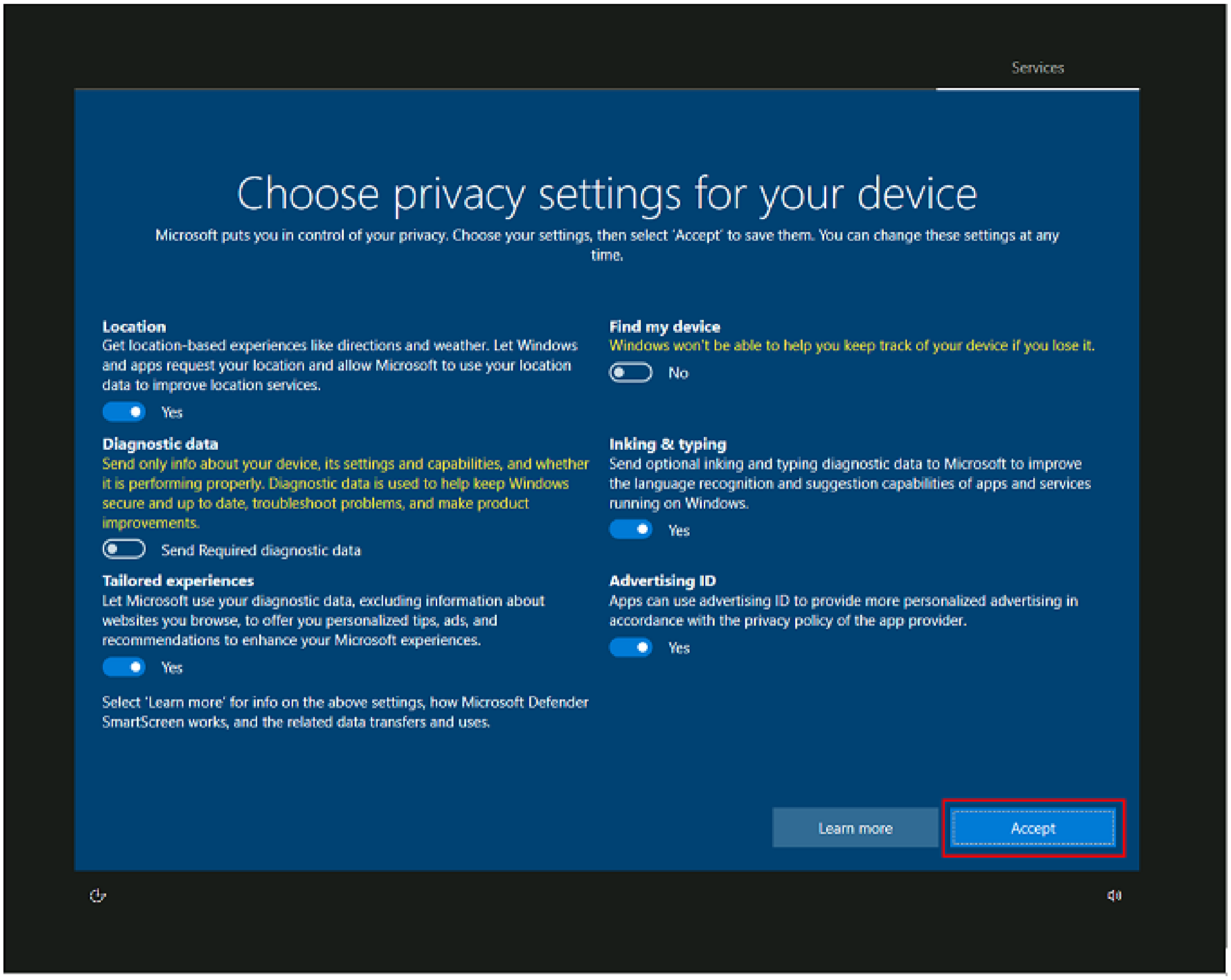
Username *

Password *

5. Select **Connect**.

6. A new tab should open, and you should be connected to your virtual machine.

7. **Accept** the default settings.



Choose privacy settings for your device

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

Location
Get location-based experiences like directions and weather. Let Windows and apps request your location and allow Microsoft to use your location data to improve location services.
Yes

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

Tailored experiences
Let Microsoft use your diagnostic data, excluding information about websites you browse, to offer you personalized tips, ads, and recommendations to enhance your Microsoft experiences.
Yes

Select 'Learn more' for info on the above settings, how Microsoft Defender SmartScreen works, and the related data transfers and uses.

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

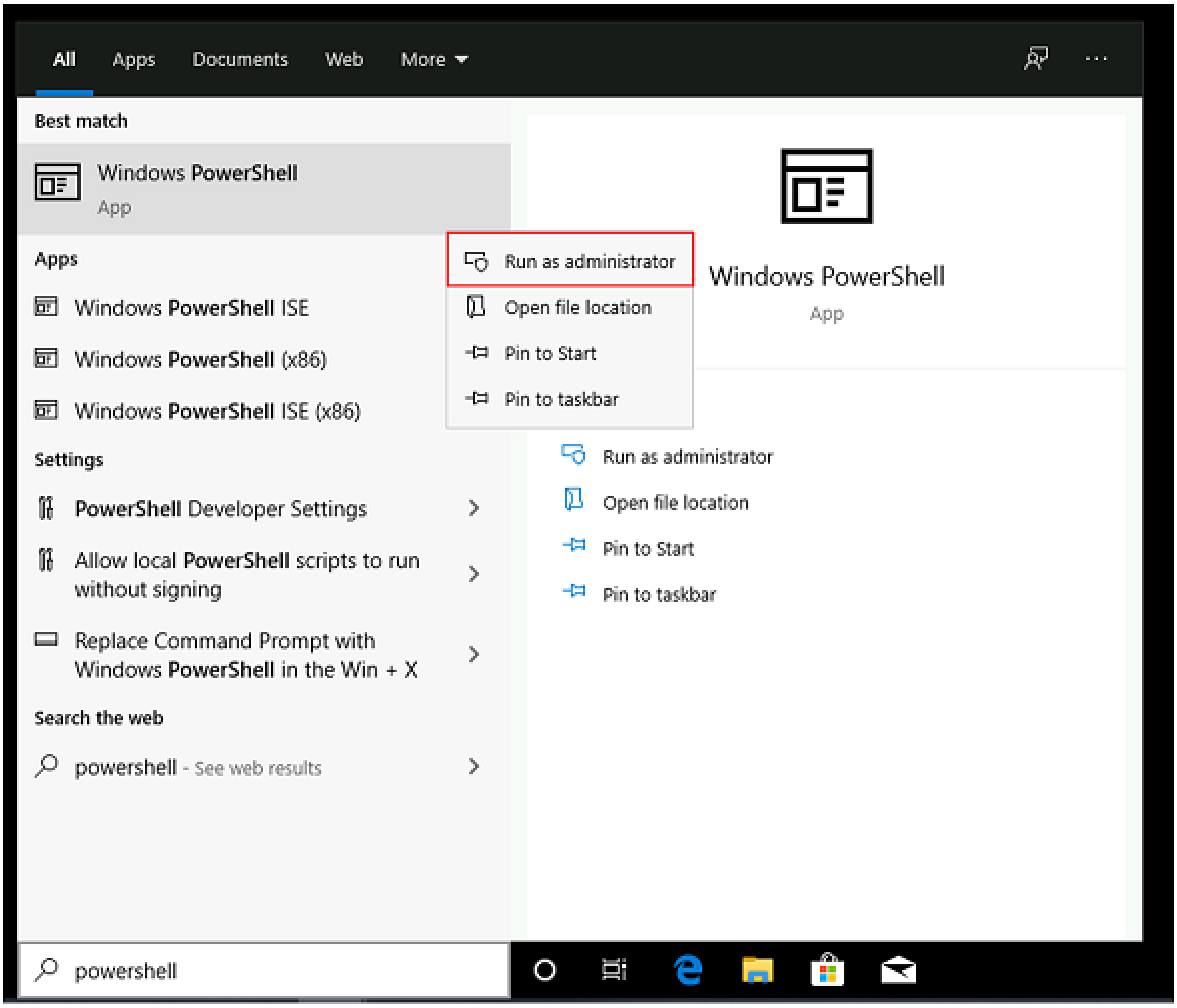
Inking & typing
Send optional inking and typing diagnostic data to Microsoft to improve the language recognition and suggestion capabilities of apps and services running on Windows.
Yes

Advertising ID
Apps can use advertising ID to provide more personalized advertising in accordance with the privacy policy of the app provider.
Yes

Task 4: Enable Hyper-V

We are going to enable Hyper-V via PowerShell in the newly created VM.

1. Search for **PowerShell** and right click to select **Run as Administrator**.

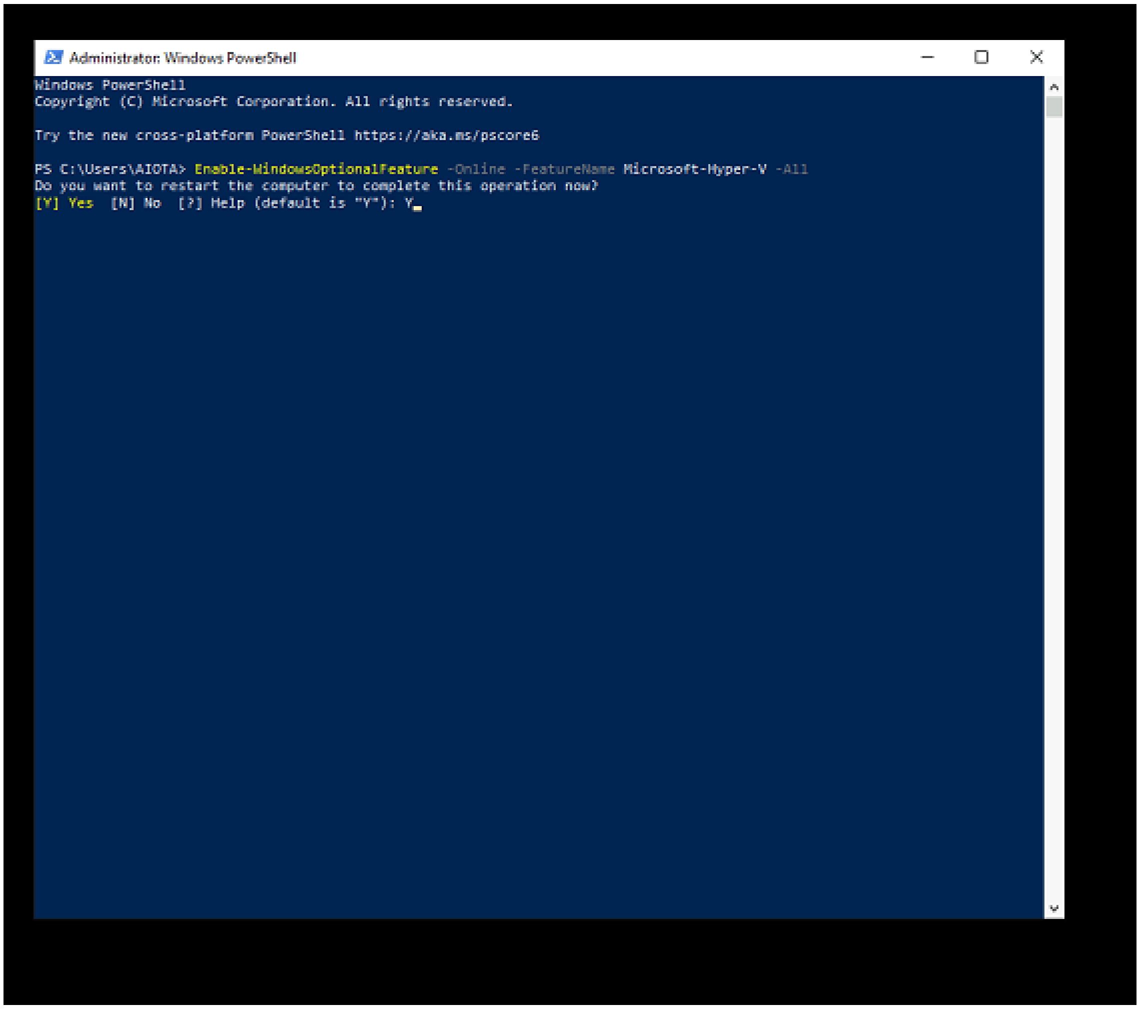


2. Run the following command:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All
```

If the command couldn't be found, make sure you're running PowerShell as an **Administrator**.

3. When the installation has completed, reboot the VM by typing in **Y**.



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\AIOTA> Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All
Do you want to restart the computer to complete this operation now?
[Y] Yes  [N] No  [?] Help (default is "Y"): Y
```

4. Reconnect to the VM.

> [!NOTE] If you are not promoted to restart the VM within PowerShell. Please close the Bastion Host tab, and return to the Azure Portal, and select your VM. At this point you can either "restart your VM" and reconnect via Bastion. OR you can *STOP* the VM and *Start* the VM again.

5. Login back to the Virtual Machine, using RDP or Bastion, open **Microsoft Edge** and download the 'Storage Explorer' click **Download**.

6. Once the download is completed run the installation selecting **Install for me only (recommended)** option. Next, click on **I accept the agreement**, and **Install**, you will ask a few additional questions, select **Next** each time, the installation will run for a few seconds.

Task 5: Create a Storage Account

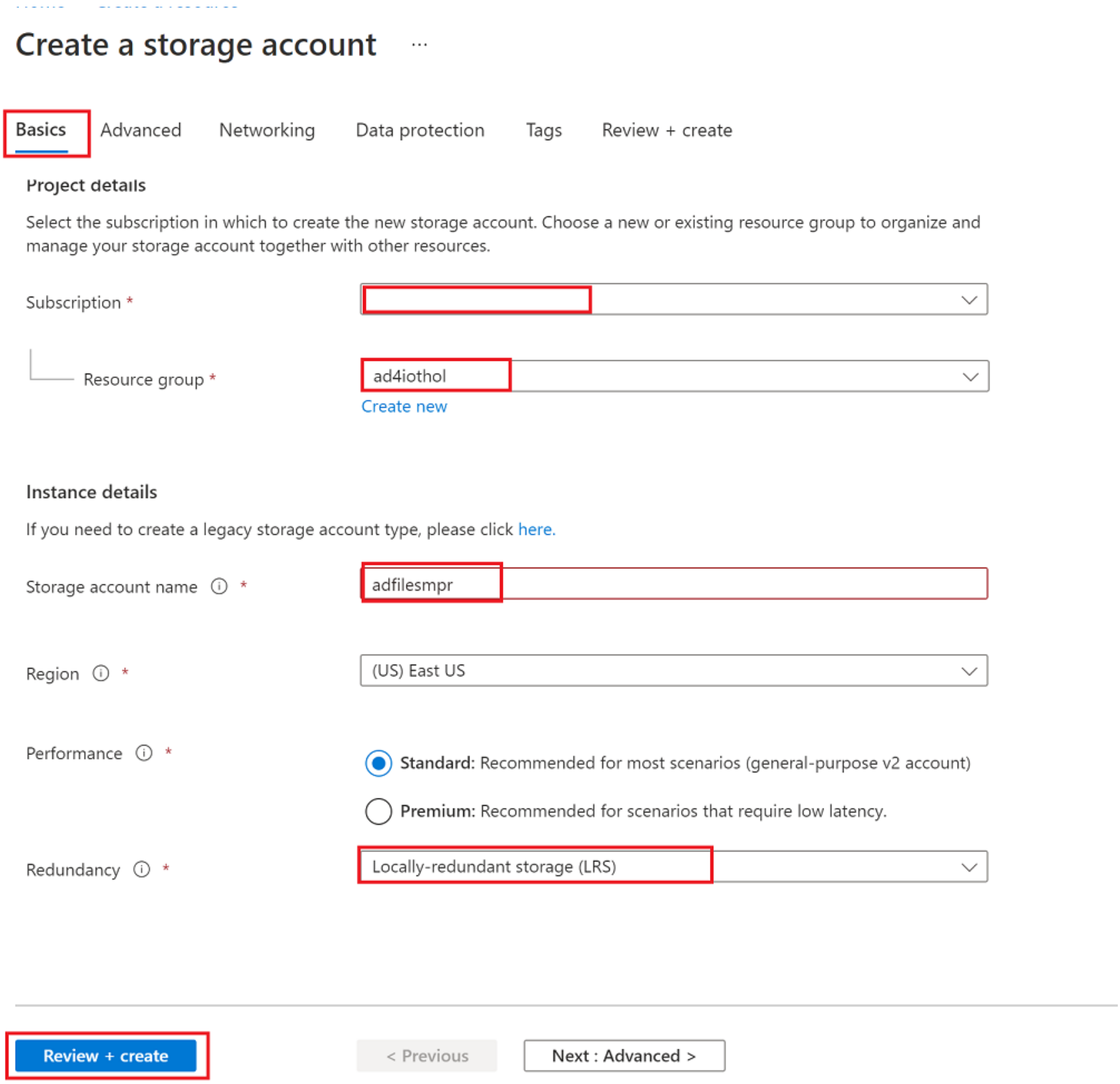
1. In Azure Portal, click on + **Create a Resource**. In the marketplace look for **Storage Account**, then click create.

2. Fill the form:

   Basics Tab:

   - **Subscriptions**: Select the subscription you are using for this workshop.
   - **Resource Group**: Select the resource group created for this workshop in previous step.
   - **Storage Account Name**: adfiles+Suffix.
   - **Region**: East US
   - **Redundancy**: Locally-redundant storage(LRS)

Then **Review + Create** after the validation is complete, click **Create**



Create a storage account ···

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *:

Resource group *: ad4iothol

Instance details

If you need to create a legacy storage account type, please click here.

Storage account name ⓘ *: adfilesmpr

Region ⓘ *: (US) East US

Performance ⓘ *:

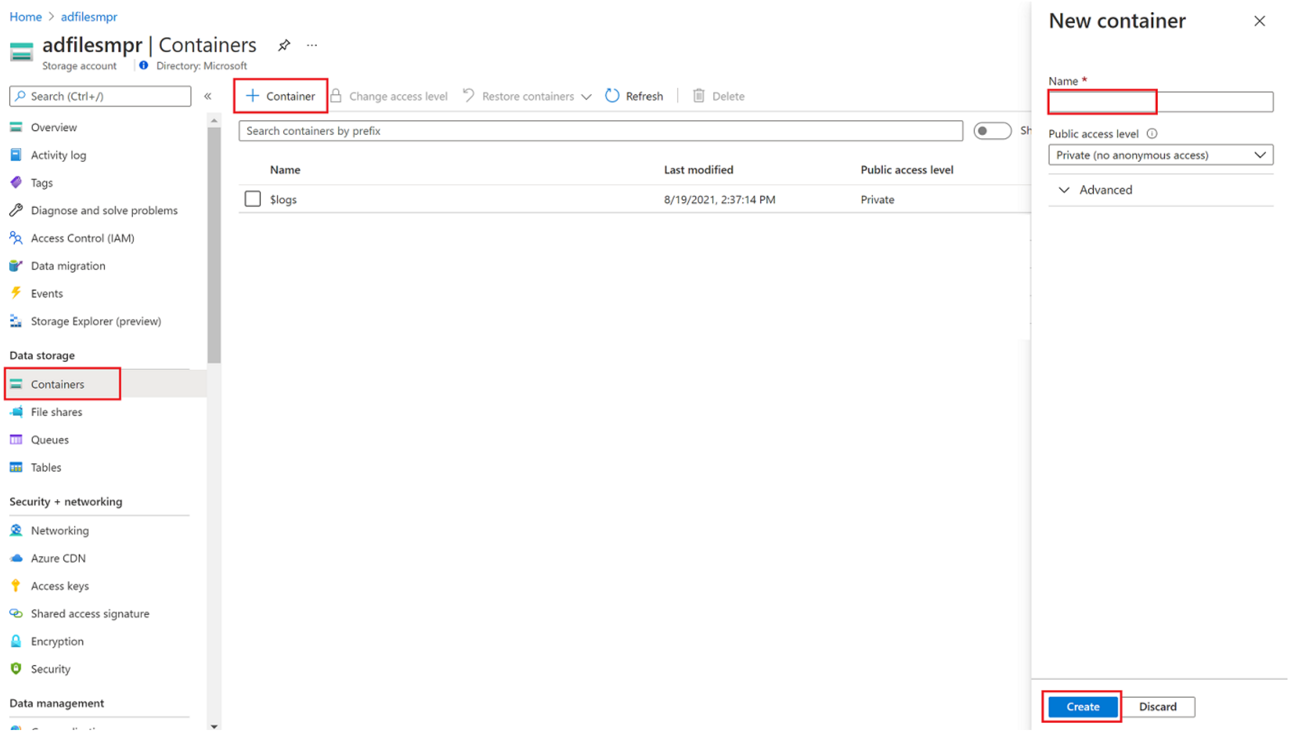
● **Standard:** Recommended for most scenarios (general-purpose v2 account)

○ **Premium:** Recommended for scenarios that require low latency.

Redundancy ⓘ *: Locally-redundant storage (LRS)

3. Once the Storage account is created, click on it. Under **Data Storage** select **Containers**, then on the right side select + **Container**.

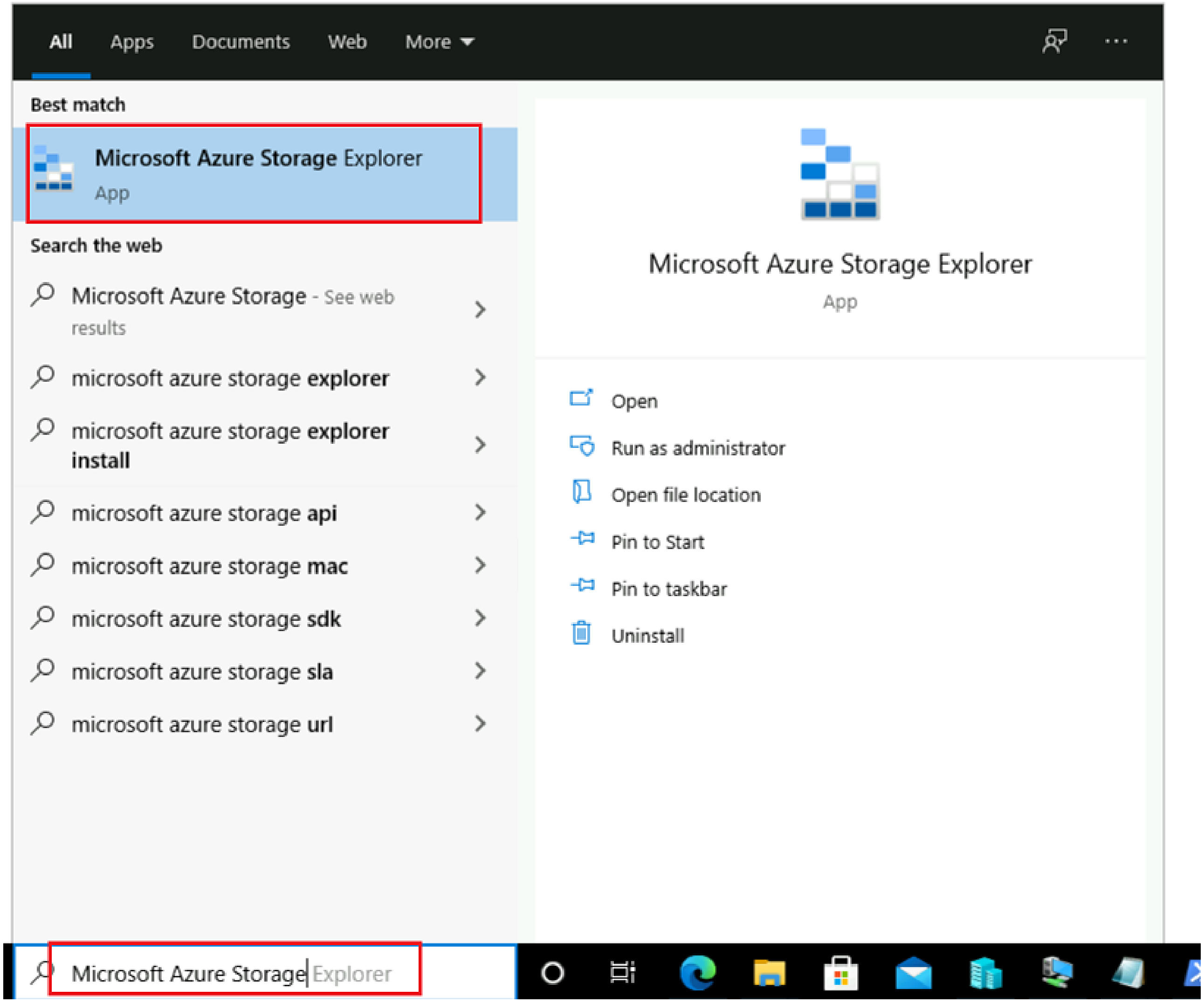
4. A new window will open on the right, assign a name **acitvationfiles** and then click **Create**.



Name	Last modified	Public access level
$logs	8/19/2021, 2:37:14 PM	Private

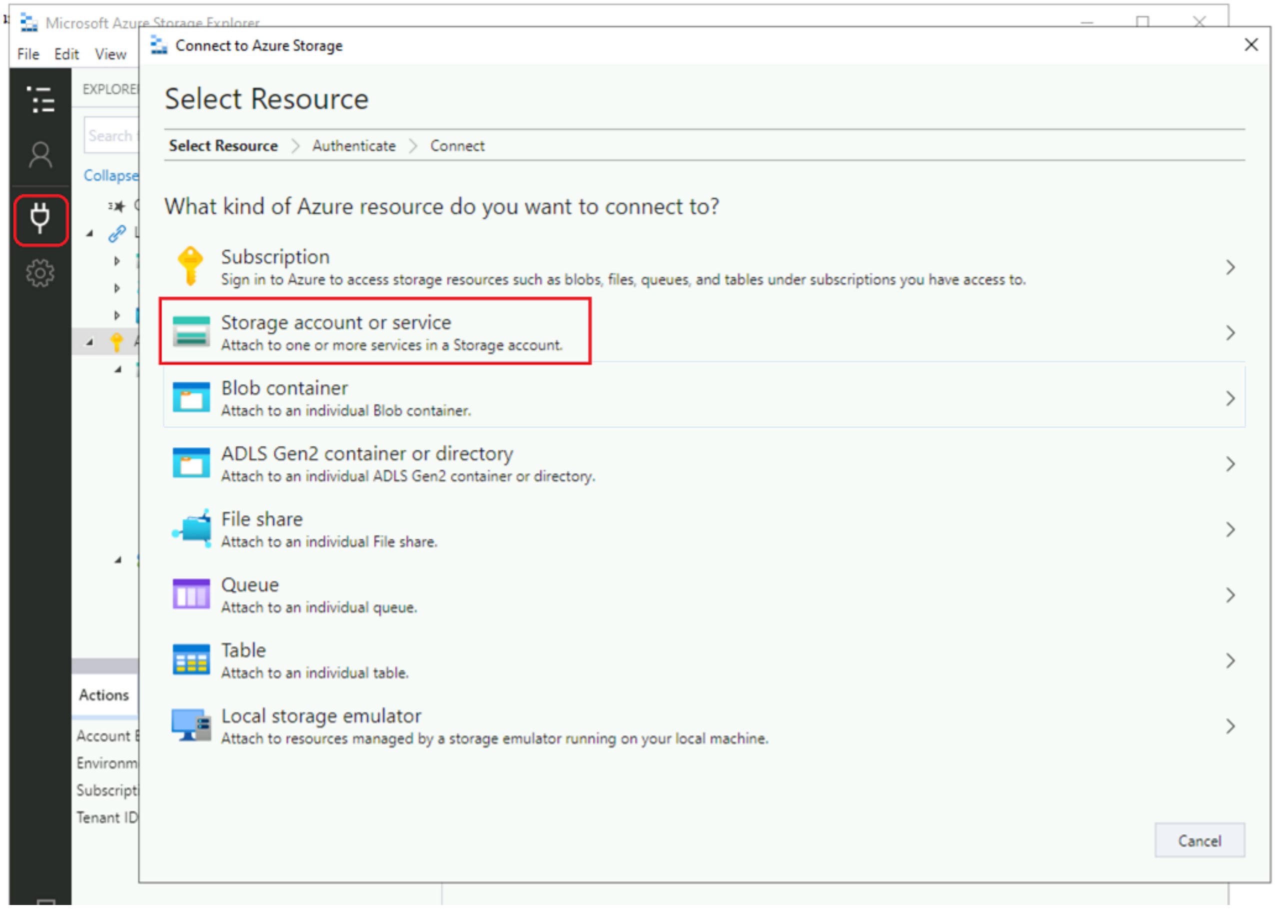
Public access level: Private (no anonymous access)

5. Login to the Windows virtual machine, in the search box enter Microsoft Storage Explorer


All
Apps
Documents
Web
More
Best match
Microsoft Azure Storage Explorer
App
Search the web
Microsoft Azure Storage - See web results
microsoft azure storage explorer
microsoft azure storage explorer install
microsoft azure storage api
microsoft azure storage mac
microsoft azure storage sdk
microsoft azure storage sla
microsoft azure storage url
Microsoft Azure Storage Explorer
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall
Microsoft Azure Storage Explorer

6. You will be prompt to login, use the personal email you are using to set up your Azure Pass for this training.

7. Once you are login, go to the connect icon on the left bar, then select **Storage account or service**.



Select Resource

Select Resource > Authenticate > Connect

What kind of Azure resource do you want to connect to?

Subscription
Sign in to Azure to access storage resources such as blobs, files, queues, and tables under subscriptions you have access to.

Storage account or service
Attach to one or more services in a Storage account.

Blob container
Attach to an individual Blob container.

ADLS Gen2 container or directory
Attach to an individual ADLS Gen2 container or directory.

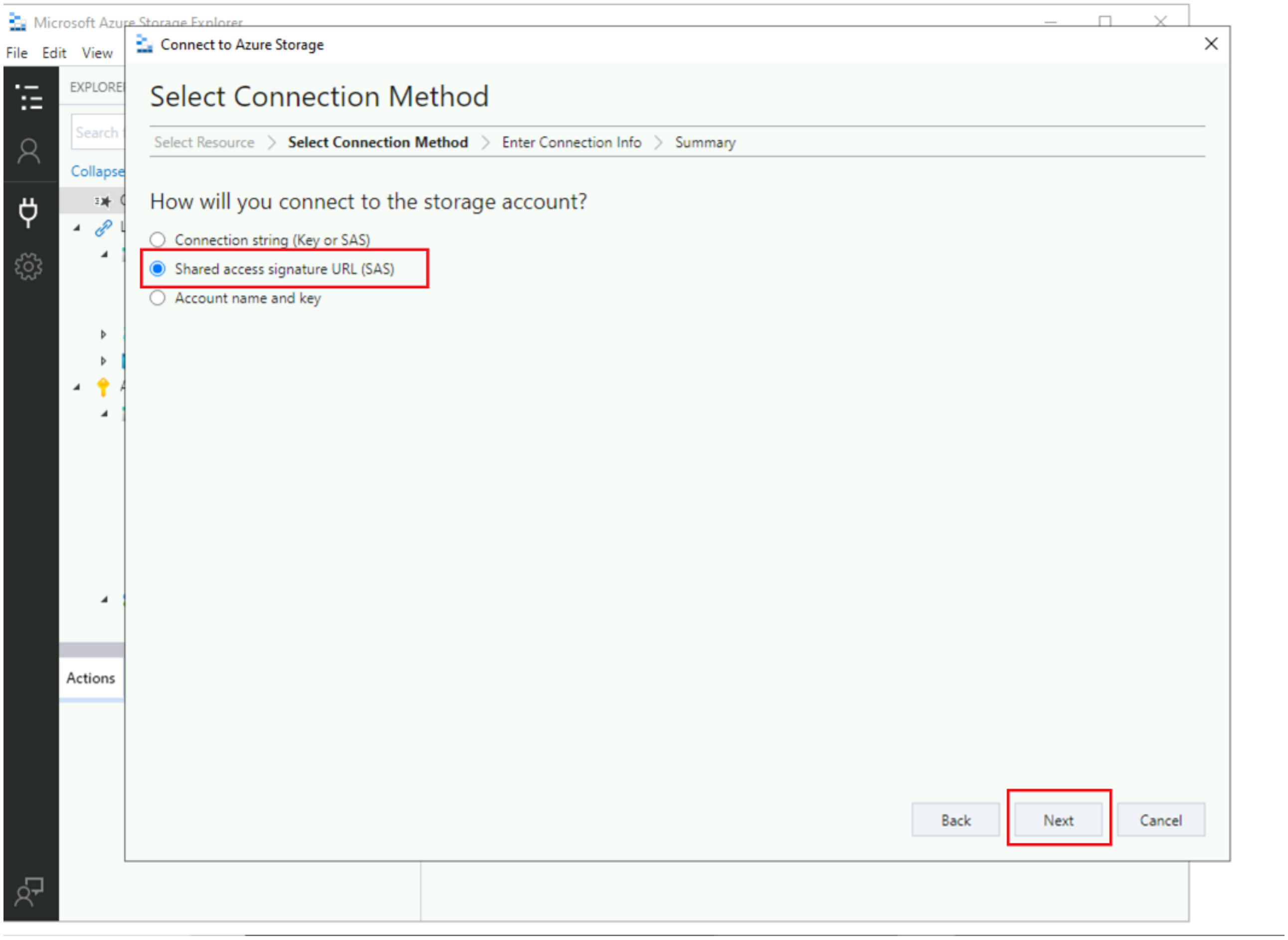
File share
Attach to an individual File share.

Queue
Attach to an individual queue.

Table
Attach to an individual table.

Local storage emulator
Attach to resources managed by a storage emulator running on your local machine.

9. In the next step select **Shared Access Signature URL(SAS)** and then **Next**


Microsoft Azure Storage Explorer
File Edit View
EXPLORER
Search
Collapse
Actions
Connect to Azure Storage

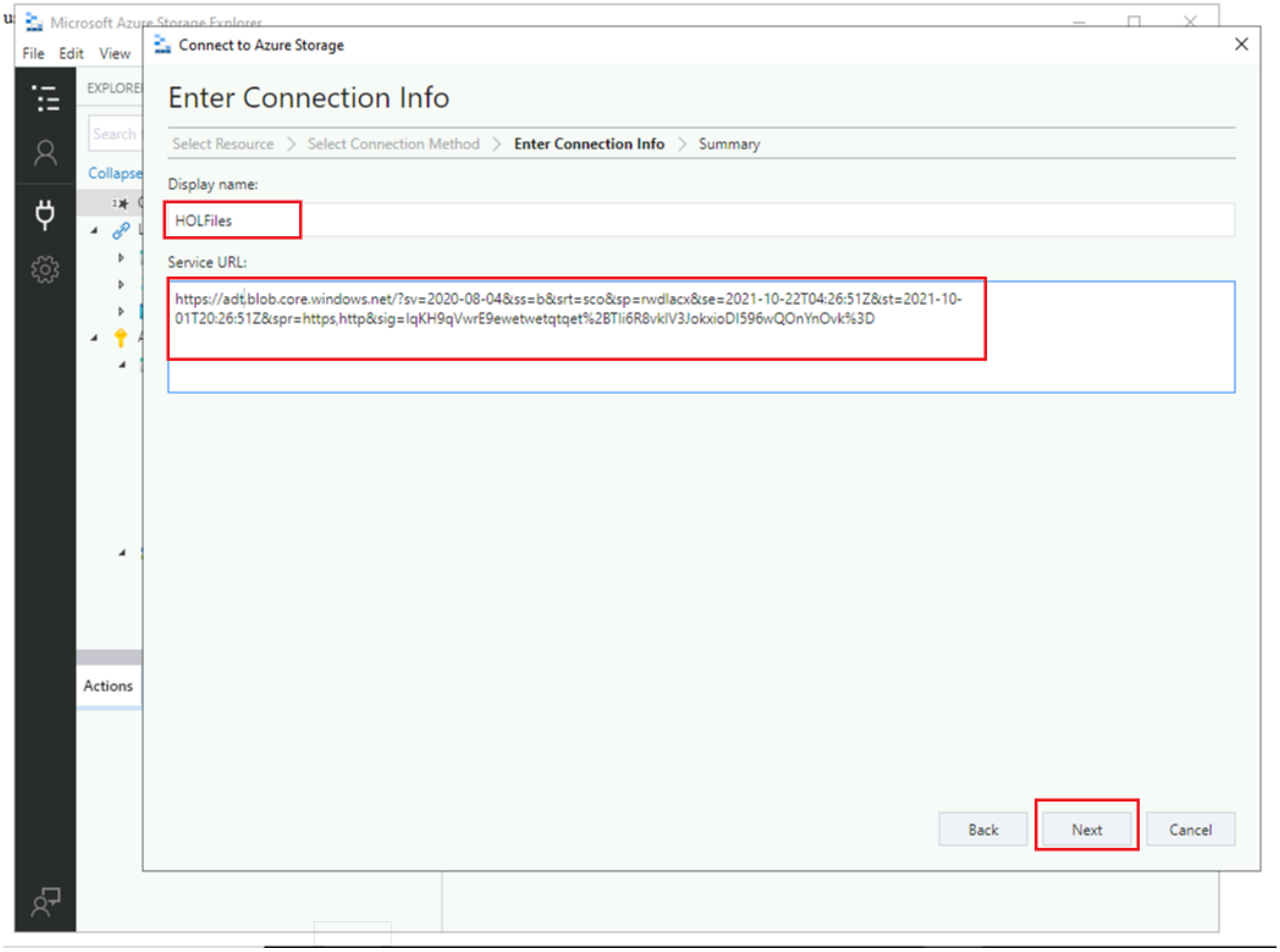
Select Connection Method

Select Resource > Select Connection Method > Enter Connection Info > Summary

How will you connect to the storage account?

○ Connection string (Key or SAS)
● Shared access signature URL (SAS)
○ Account name and key

10. In the Enter Connection Info window, you wil assign a name to the connection **HOLFiles** and you will paste below the Blob SAS URL (service URL) you received by email previous to this training.


Microsoft Azure Storage Explorer
File Edit View
EXPLORER
Search
Collapse
Actions
Connect to Azure Storage
Enter Connection Info
Select Resource > Select Connection Method > Enter Connection Info > Summary
Back
Next
Cancel

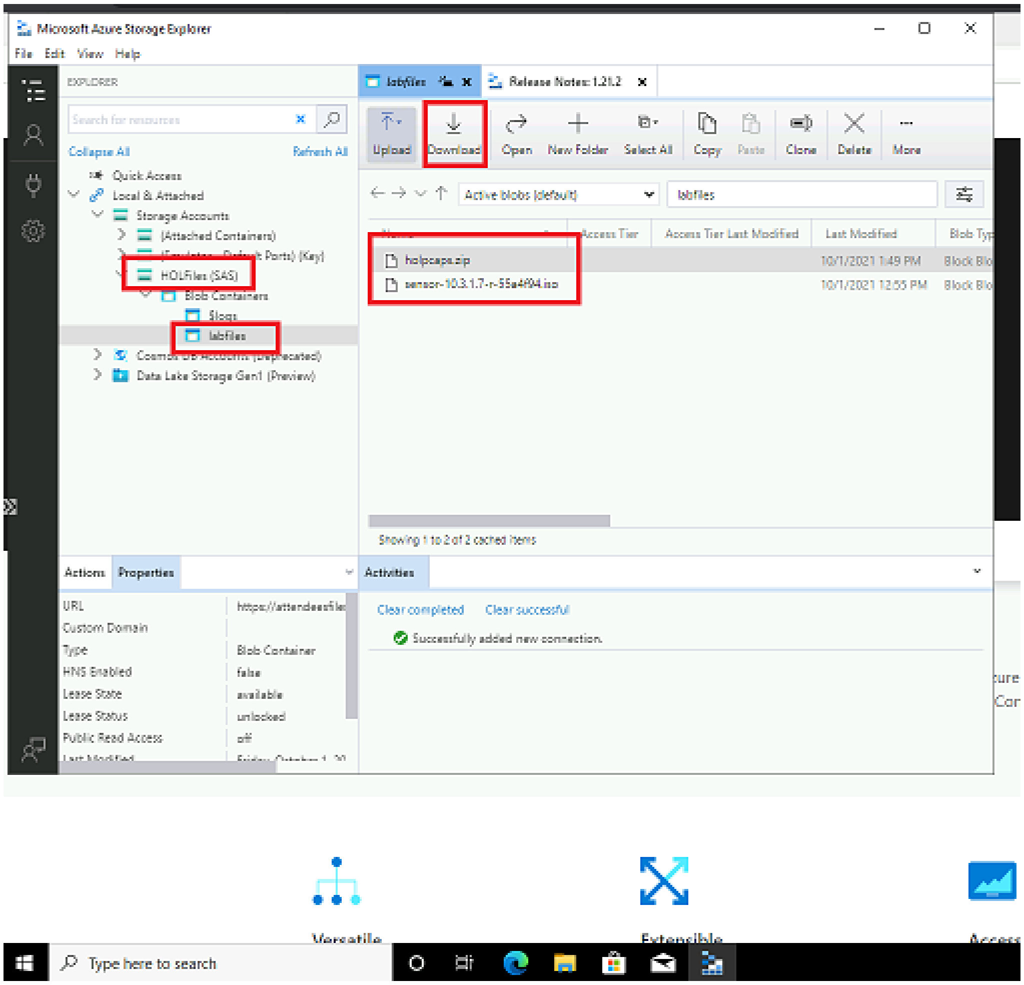
Display name:

HOLFiles

Service URL:

https://adt.blob.core.windows.net/?sv=2020-08-04&ss=b&srt=sco&sp=rwdlacx&se=2021-10-22T04:26:51Z&st=2021-10-01T20:26:51Z&spr=https,http&sig=lqKH9qVwrE9ewetwetqtqet%2BTIi6R8vkIV3JokxioDI596wQOnYnOvk%3D

11. Once the storage account is connected you should select the container on the left side **attendeefiles** then **Labfiles** now in the right side you will see the two files you need to download locally. Select the files and click **Download**



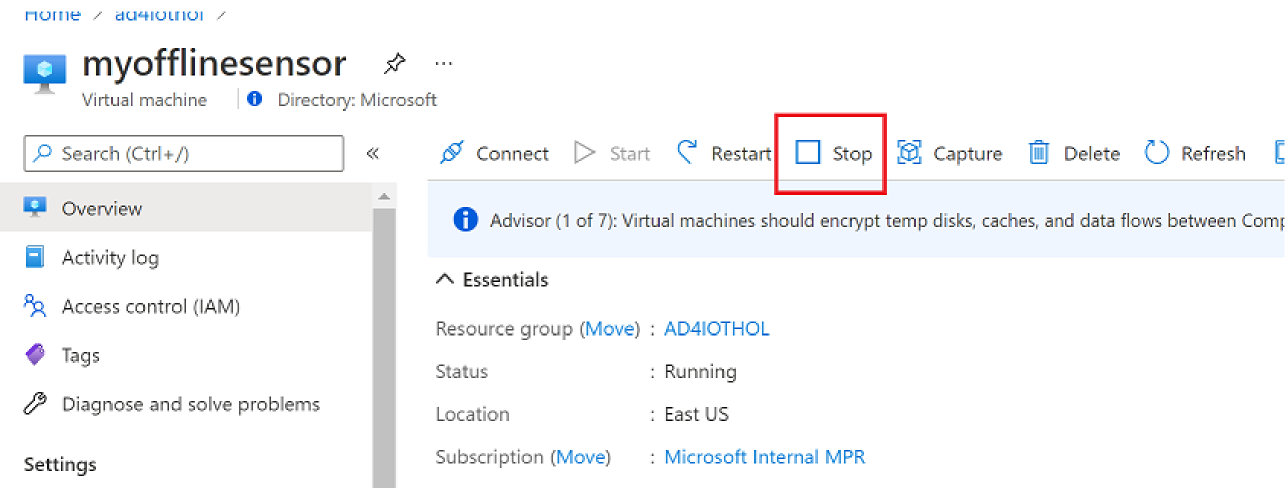
Name	Last Modified	Blob Type
holpcaps.zip	10/1/2021 1:49 PM	Block Blob
sensor-10.3.1.7-r-55a4f94.iso	10/1/2021 12:55 PM	Block Blob

Showing 1 to 2 of 2 cached items

URL	https://attendeesfile
Custom Domain	
Type	Blob Container
HNS Enabled	false
Lease State	available
Lease Status	unlocked
Public Read Access	off

Successfully added new connection.

12. Once this download is complete, go to the Azure Portal select your Virtual Machine and click **Stop**. Now you are all set for your training session.



Advisor (1 of 7): Virtual machines should encrypt temp disks, caches, and data flows between Comp

Resource group (Move) : AD4IOTHOL

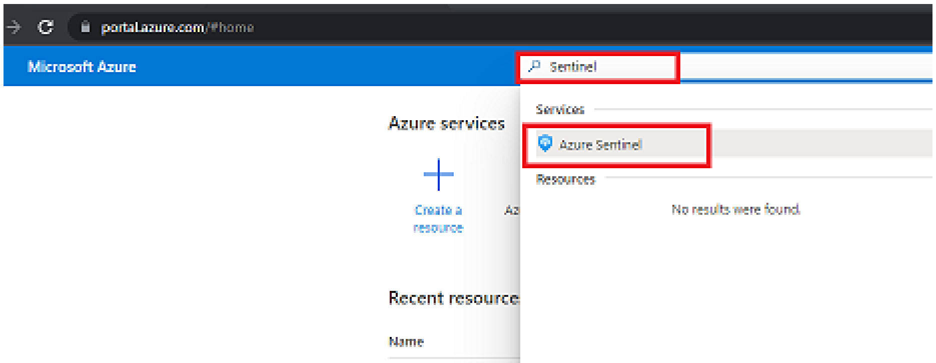
Status : Running

Location : East US

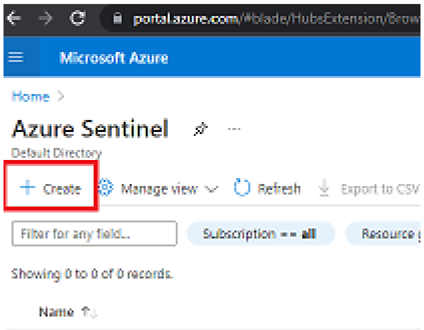
Subscription (Move) : Microsoft Internal MPR

Task 6: Azure Sentinel

1. Go to Azure Portal, in the top search box, type **Azure Sentinel**, then select it from the list.

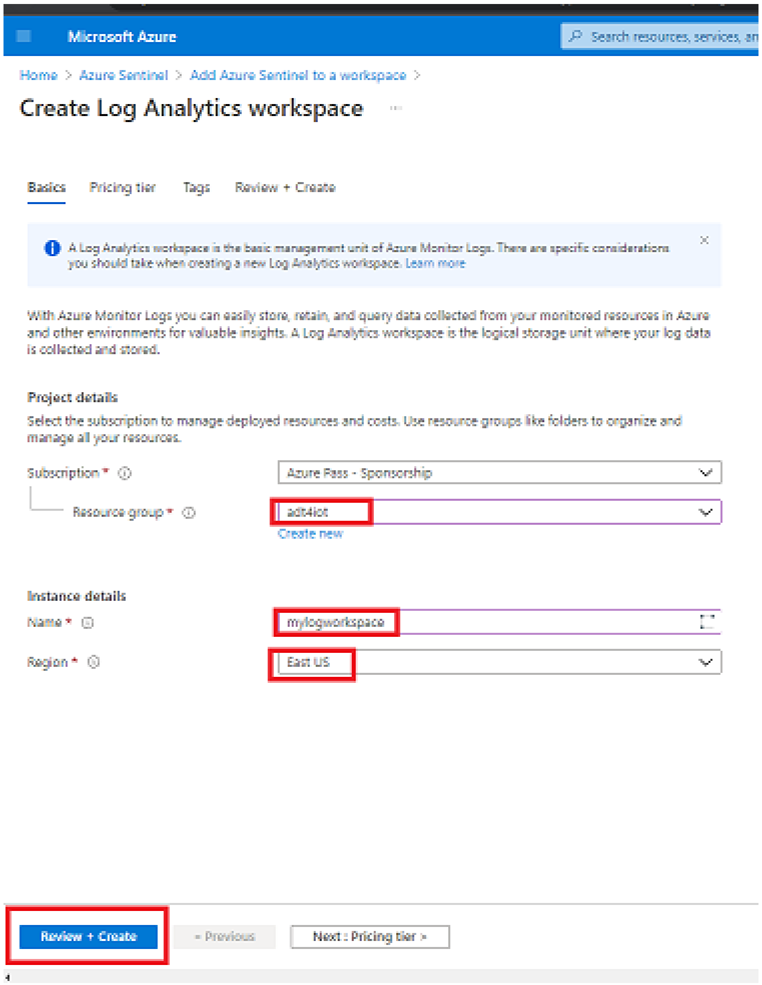


2. Then, click **Create**, a new pop up window appears, select **+ Create a new workspace**



3. In the new window, fill the form with the following data:
   - **Subscription**: Select the subscription you are using for this training.

- **Resource Group**: select the resource group you created previously.
- **Name**: Mylogworkspace+SUFFIX
- **Regions**: East US



Create Log Analytics workspace

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription * : Azure Pass - Sponsorship

Resource group * : adt4iot

Instance details

Name * : mylogworkspace

Region * : East US

4. Click **Review and create**, after validation is completed, click **create**

You have completed all your pre-work tasks before attending the Hands-on Lab! Please make sure your Virtual Machine is **STOP** until the training date, otherwise you will consume your Azure Credit before the training.