

Microsoft Defender for IoT - Before Hands-on Lab

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

Content:

- [Action A: Azure Passes](#)
 - [Task 1: Activating your Azure Pass](#)
 - [Task 2: Validating your Azure Subscription](#)
- [Action B: Set up Environment](#)
 - [Task 1: Resources](#)
 - [Task 2: Virtual Machine](#)
 - [Task 3: Connect to Virtual Machine](#)
 - [Task 4: Enable Hyper-V](#)
 - [Task 5: Create a Storage Account](#)
 - [Task 6: Microsoft Sentinel](#)

Action A: Azure Passes

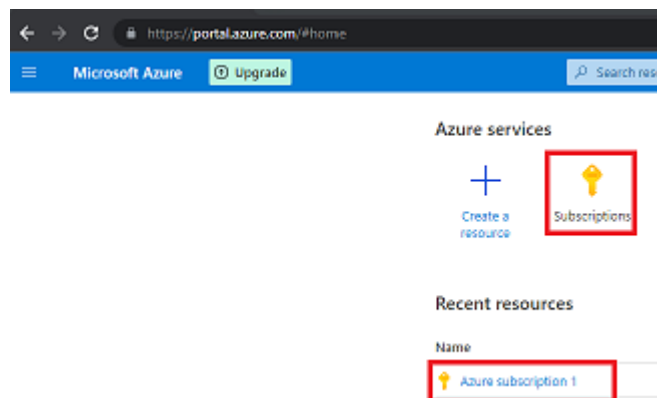
Prior to this workshop, after successful registration, you will receive an Azure Pass. You can activate this Azure Pass with your personal email account. This step will be coordinated with your instructors.

Task 1: Activating your Azure Pass

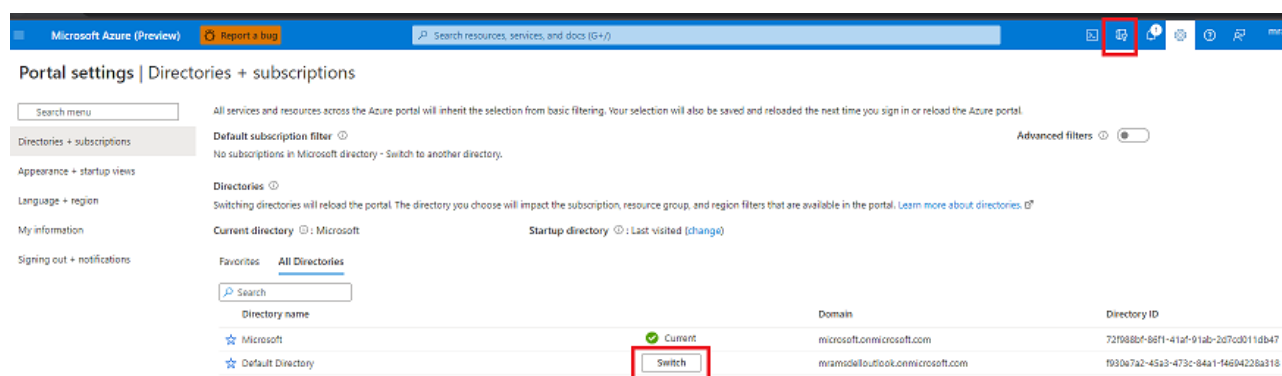
1. Go [here to activate your Azure Pass](#).
2. Click on **START**. Make sure you set up this pass with a personal email or just create an outlook email account for this training.
3. After you login and validate the account, you will be asked to **Enter the Promo Code**. Here you will copy the Azure Pass Code you received by email and then click on **Claim Promo Code**.
4. Next, fill the form with your name. After a few minutes you should have a Subscription available to start setting up your services in the next exercises.

Task 2: Validating your Azure Subscription

1. To validate your subscription is active, go to the [Azure Portal](#).
2. In the Azure Portal, you should see the icon for **Subscriptions**.
3. Click on it. You should see a new Subscription available, also the same subscription could be available in the **Recent Resources** list.



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



Action B: Set up Environment

Once your Azure Pass is activated and you have a new subscription to work with, you are ready to setup the environment you will use during the Microsoft Defender for IoT Hands-on-Lab. For the HOL, you will create one single resource group to host all the services that you will use during the lab.

Task 1: Resources

1. In the 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**.
2. In the next window, select your subscription, assign a name to the resource group: **rg-md4iot+SUFFIX**, select a location near you and click on **Review + Create**.
3. Once you passed the validation, click **create**.

Note: the resource group name needs to be unique within your subscription. That is why we suggest to add a suffix, for instance your initials followed by a number.

Microsoft Azure

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

[Home](#) > [Create a resource](#) > [Resource group](#) >

Create a resource group

Basics

Tags

Review + create

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

Project details

Subscription * ⓘ

Azure Pass - Sponsorship

Resource group * ⓘ

rg-md4iot-mst01

Resource details

Region * ⓘ

(Europe) West Europe

Review + create

< Previous

Next : Tags >

Task 2: Virtual Machine

1. In the upper-left side of the Azure Portal, select: **Create a resource** > **Compute** > **Virtual machine** > > **Create**

Microsoft Azure

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

[Home](#) >

Create a resource

Get started

Recently created

Categories

AI + Machine Learning

Analytics

Blockchain

Compute

Containers

Search services and marketplace

Getting Started? Try our Quickstart center

Popular products [See more in Marketplace](#)

Virtual machine

Create

Learn more

Virtual machine scale set

Create

Learn more

Kubernetes Service

Create

Docs

MS Learn

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 just created Resource Group
Instance details	

Setting	Value
Virtual machine name	Enter vm-md4iot-host
Region	Select (EUROPE) West Europe or a region near your location
Availability Options	Select No infrastructure redundancy required
Security type	Select Standard
Image	Select Windows 10 Pro, Version 20H2 - Gen2
Azure Spot instance	Leave the checkbox unchecked
Size	D4s_v3 - 4 vcpus, 16 GiB memory , see image below
Administrator Account	Use the following Credentials
Username	MDefenderLab
Password	Learningmode123!
Confirm password	Learningmode123!
Inbound port rules	
Public inbound ports	Select Allow selected ports
Select inbound ports	RDP (3389)
Licensing	
I confirm I have an eligible Windows 10 license with multi-tenant hosting rights.	Check the box.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal, specifically the 'Management' tab. The wizard is divided into several sections: 'Project details', 'Instance details', and 'Administrator account'. In the 'Project details' section, the 'Subscription' is set to 'Azure Pass - Sponsorship' and the 'Resource group' is 'rg-md4iot-mst01'. In the 'Instance details' section, the 'Virtual machine name' is 'vm-md4iot-host', the 'Region' is '(Europe) West Europe', the 'Availability options' are 'No infrastructure redundancy required', the 'Security type' is 'Standard', the 'Image' is 'Windows 10 Pro, version 20H2 - Gen2', the 'Azure Spot instance' checkbox is unchecked, and the 'Size' is 'Standard_D4s_v3 - 4 vcpus, 16 GiB memory (€147.75/month)'. In the 'Administrator account' section, the 'Username' is 'MDefenderLab'. At the bottom of the wizard, there are three buttons: 'Review + create' (highlighted with a red box), '< Previous', and 'Next : Disks >'. The 'Management' tab is also highlighted with a red box.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Create a resource >

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. [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 * ⓘ Azure Pass - Sponsorship

Resource group * ⓘ rg-md4iot-mst01 [Create new](#)

Instance details

Virtual machine name * ⓘ vm-md4iot-host ✓

Region * ⓘ (Europe) West Europe

Availability options ⓘ No infrastructure redundancy required

Security type ⓘ Standard

Image * ⓘ Windows 10 Pro, version 20H2 - Gen2 [See all images](#) | [Configure VM generation](#)

Azure Spot instance ⓘ ☐

Size * ⓘ Standard_D4s_v3 - 4 vcpus, 16 GiB memory (€147.75/month) [See all sizes](#)

Administrator account

Username * ⓘ MDefenderLab ✓

Review + create < Previous Next : Disks >

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

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

Home > Create a resource > Create a virtual machine >

Select a VM size

Search by VM size...

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

Showing 597 VM sizes. Subscription: Azure Pass - Sponsorship Region: West Europe Current size: Standard_D2s_v3 Image: Windows 10 Pro, version 20H2

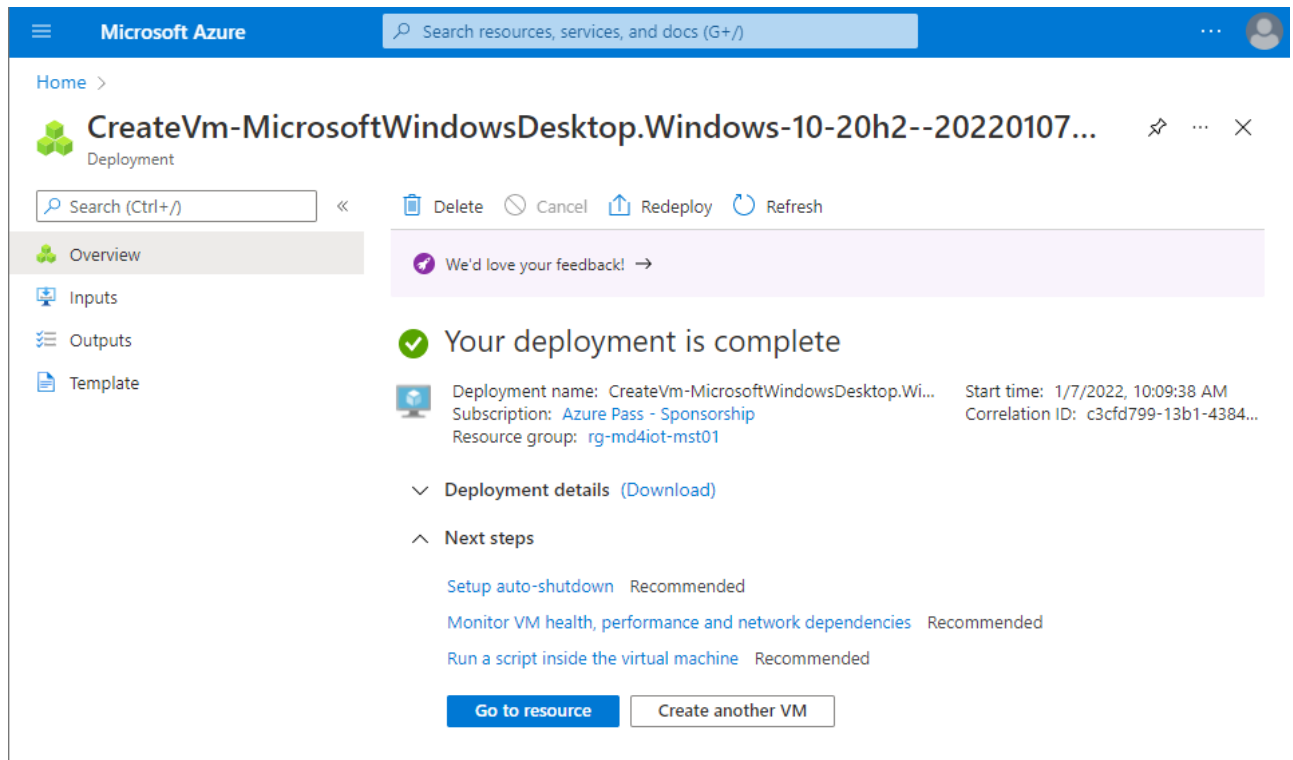
Learn more about VM sizes Guidance choosing a region or VM size Group by series

VM Size ↑↓	Family ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓
Most used by Azure users					
The most used sizes by users in Azure					
D-Series v5					
The latest generation D family sizes recommended for your general purpose needs					
D-Series v4					
The 4th generation D family sizes 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 for general-purpo					
E-Series v5					
The latest generation E family sizes for your high memory needs					
E-Series v4					
The 4th generation E family sizes for your high memory needs					
F-Series v2					
Up to 2X performance boost for vector processing workloads					
FX-Series					
The 1st generation FX family for high CPU and high memory workloads					
H-Series					
High performance compute VMs					
D-Series v3					
The 3rd generation D family sizes for your general purpose needs					
D2s_v3	General purpose	2	8	4	3200
D4s_v3	General purpose	4	16	8	6400
D8s_v3	General purpose	8	32	16	12800
D16s_v3	General purpose	16	64	32	25600
D32s_v3	General purpose	32	128	32	51200

Select

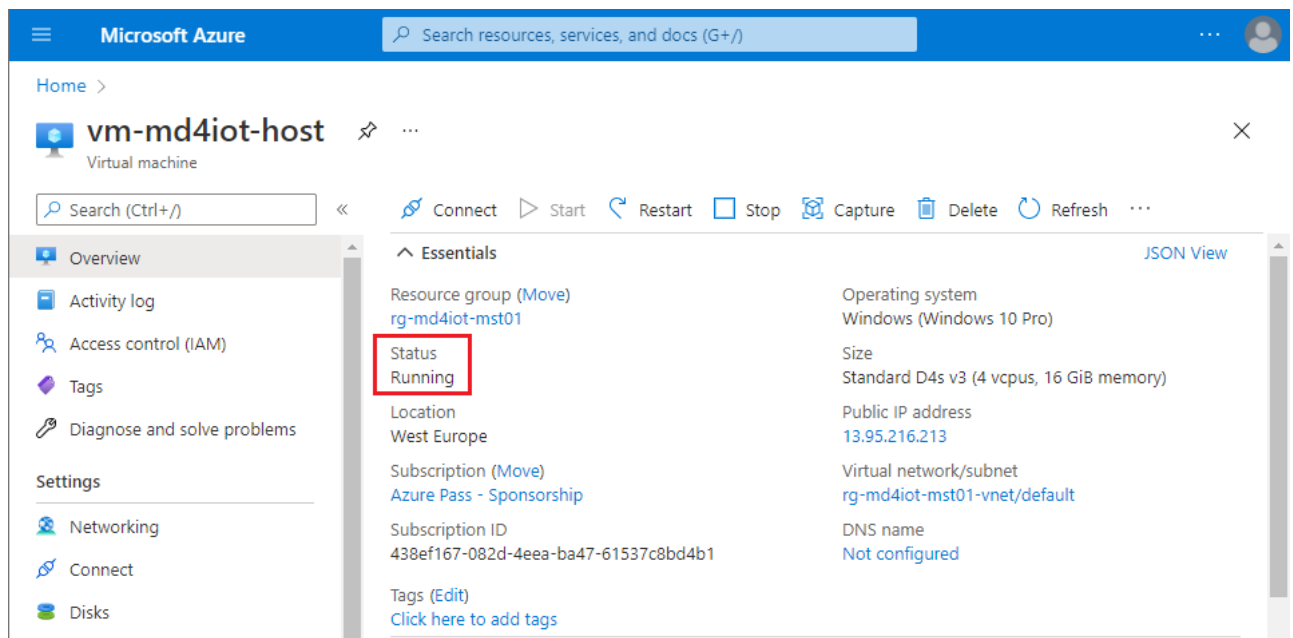
Prices presented are estimates in your local currency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. [View Azure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

- Go to the **Management** tab. In the **Monitoring** section, select **Disable** for **Boot Diagnostics**.
- At the bottom click on **Review + Create**. Once the validation is complete, click **Create**.
- It will take a few minutes to deploy your VM. At the end you should an indication that your deployment is complete.



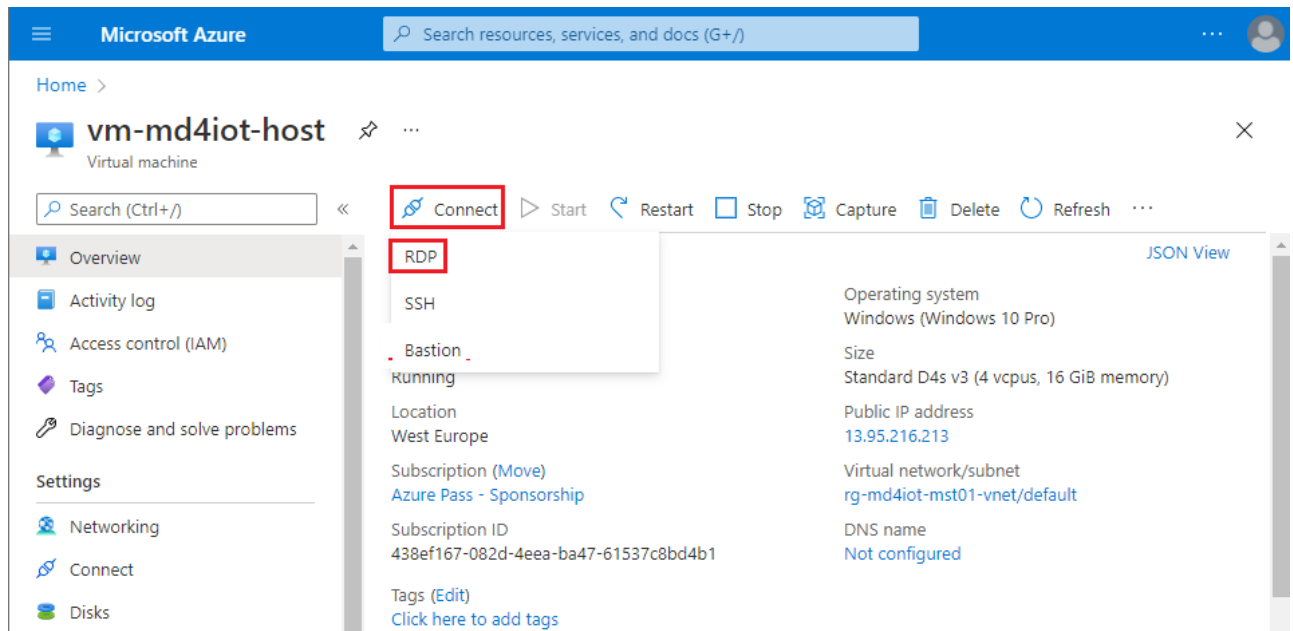
Task 3: Connect to Virtual Machine

1. Navigate to the Azure Portal Home and select your newly created virtual machine.
2. Make sure that the Virtual Machine status is **Running**.



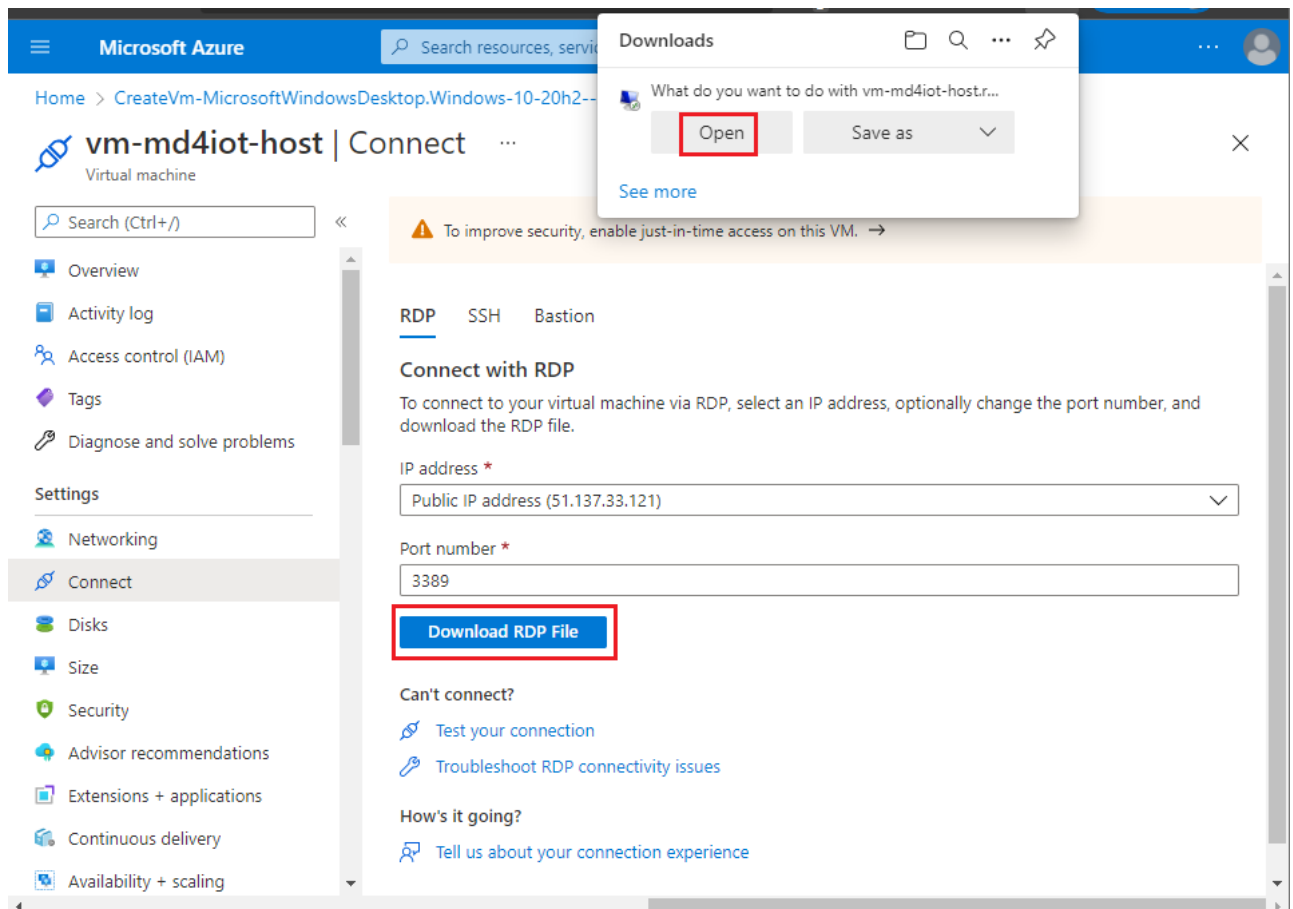
TIP: You will not be able to connect if your Virtual Machines is not in **Running** status. So give it a minute or two to finish updating.

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



NOTE: In this HOL you are using RDP to connect to your virtual machine. A more secure option is to use Bastion, however, there are subscription costs we have to take into account. Because your Azure pass only has a limited amount of credit, we want to make sure that you get the most out of it working with Microsoft Defender for IoT.

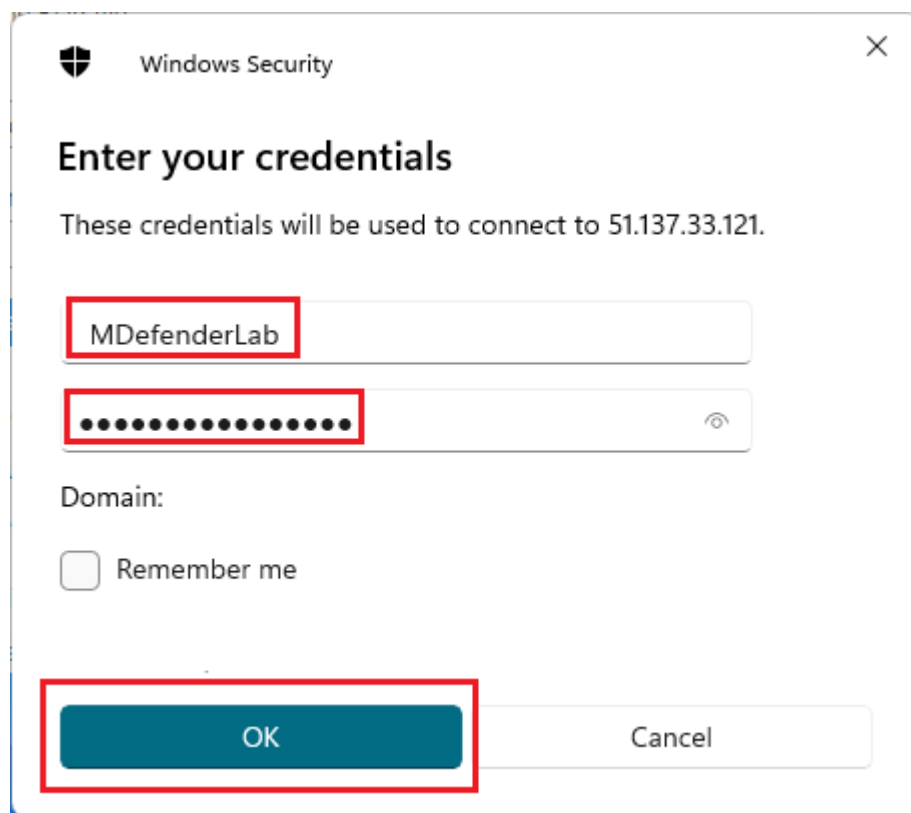
4. In the **Connect** page, click on **Download RDP File** and click on **Open**.



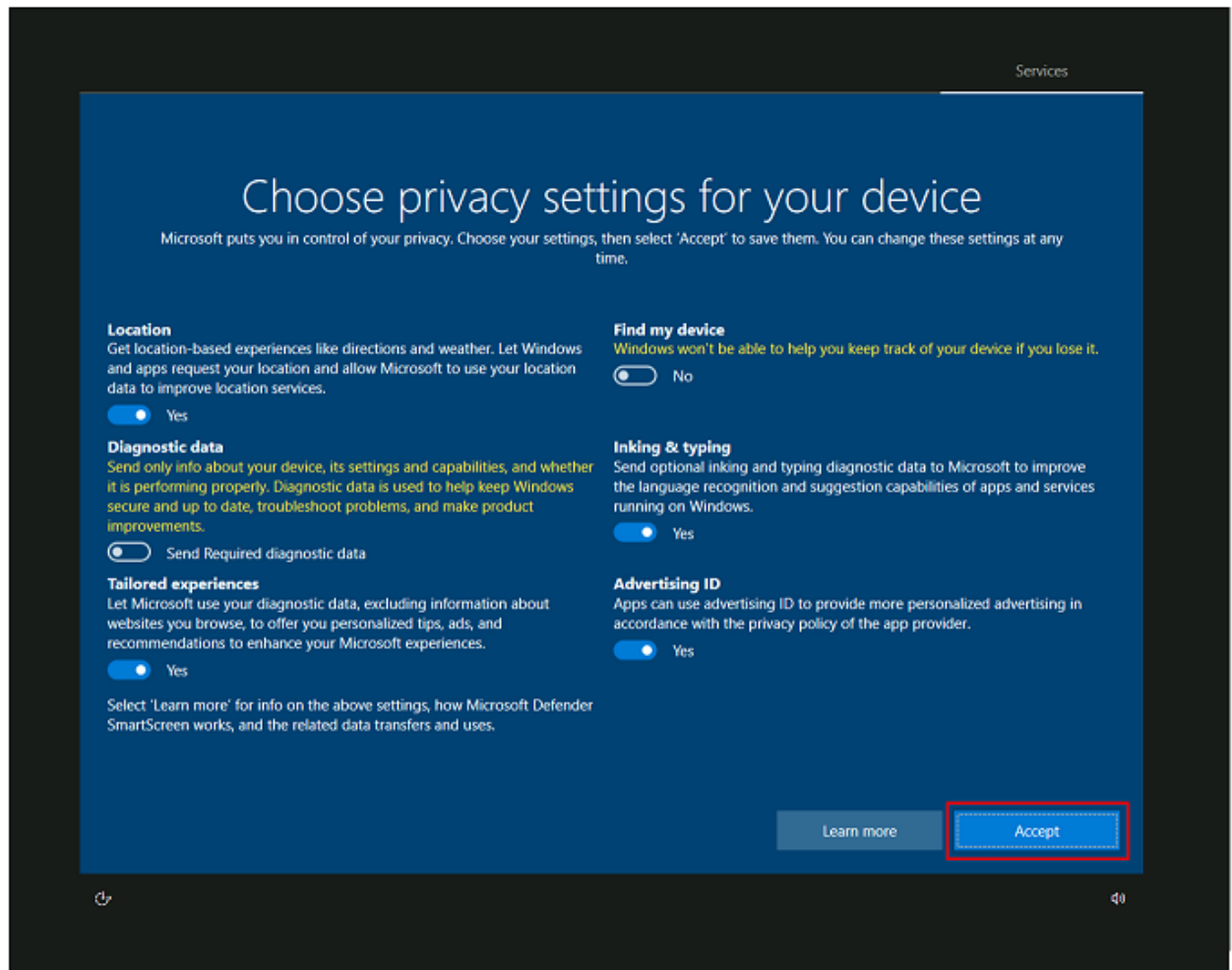
5. In the RDP login screen, enter the username and password for the virtual machine.

Field	Enter
-------	-------

Field	Enter
Username	<i>MDefenderLab</i>
Password	<i>Learningmode123!</i>



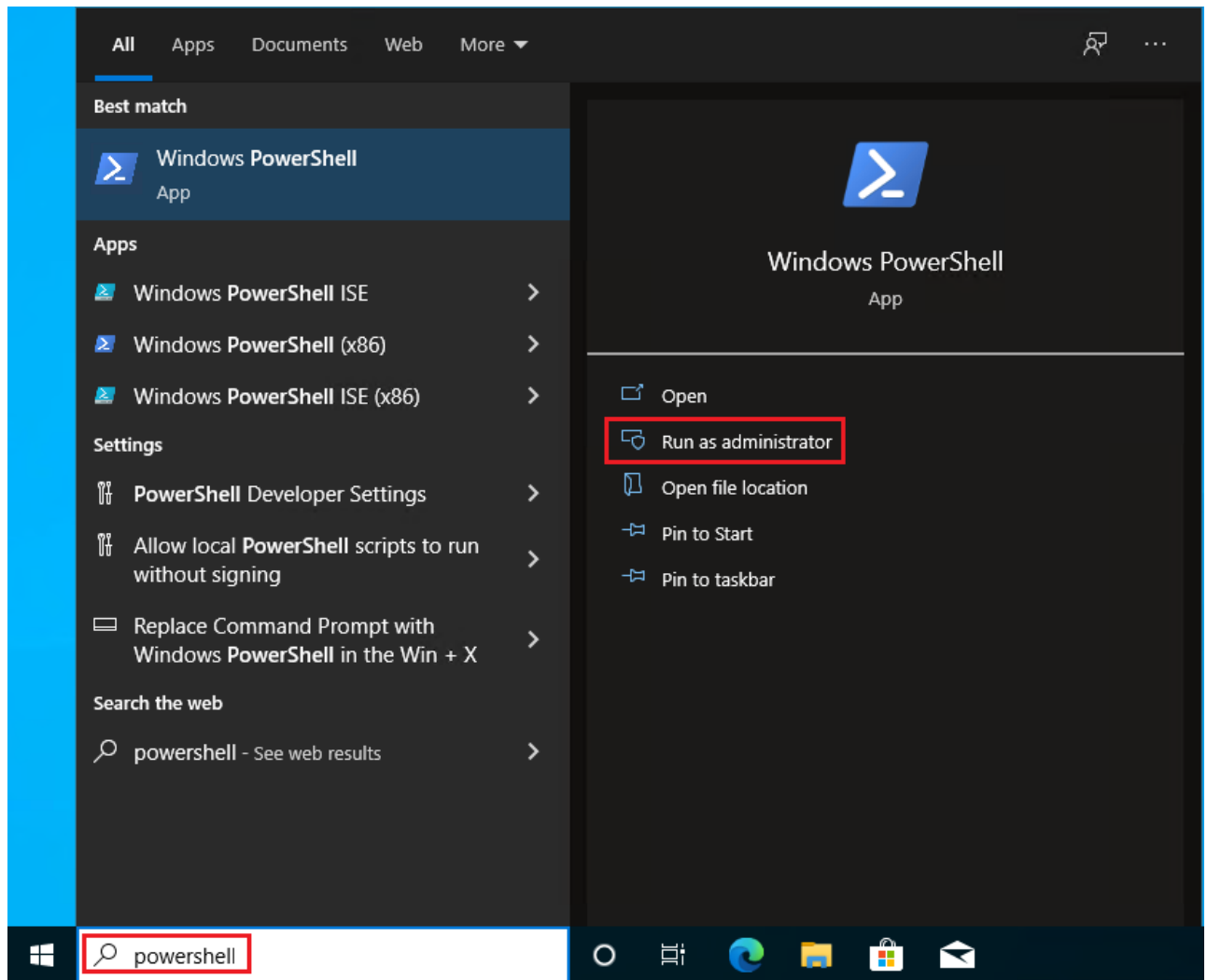
6. Click **OK** to login to the virtual machine.
7. A new window should open which is the connection to your Virtual Machine.
8. **Accept** the default settings.



Task 4: Enable Hyper-V

We are going to enable Hyper-V via PowerShell in the newly created VM. This allows us to create additional virtual machines inside this virtual machine (a.k.a nested Hyper-v). This is one of the reasons why the VM we created is a relatively large one.

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

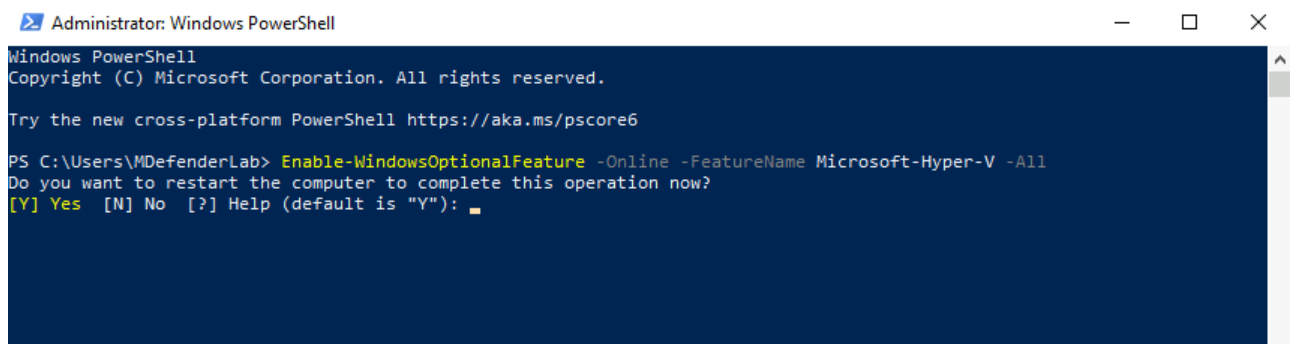


2. Run the following command in the PowerShell Window:

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

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

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

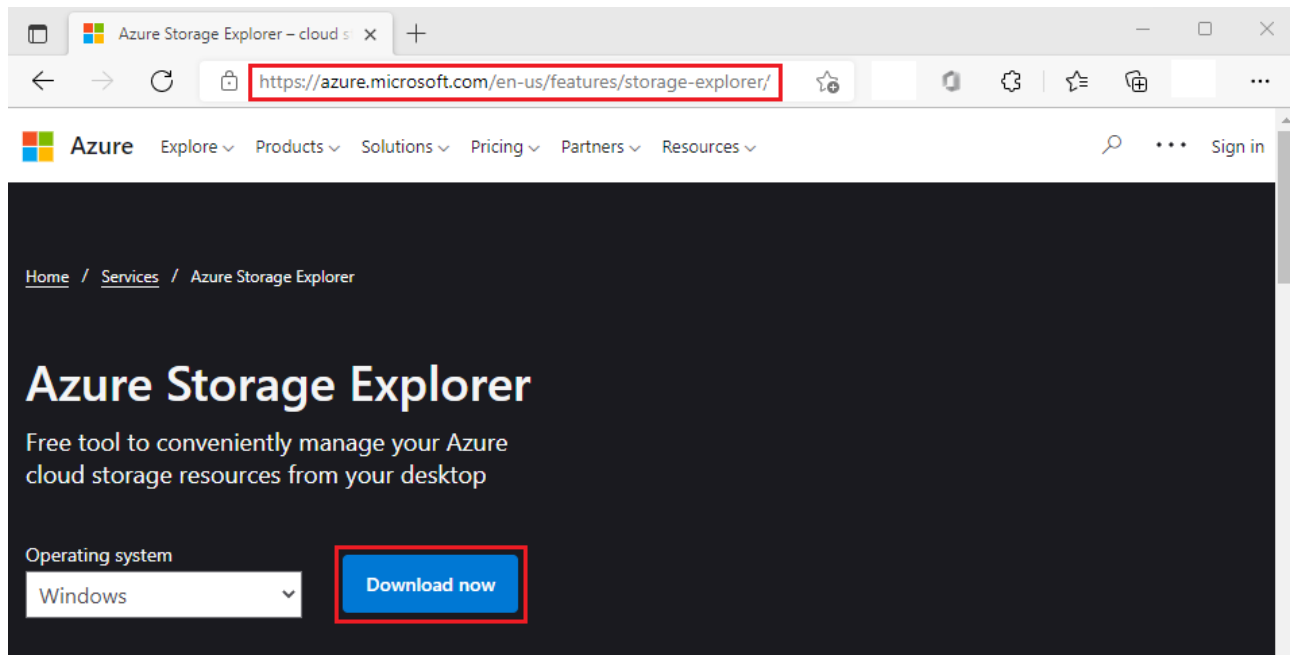


4. Reconnect to the VM.

NOTE: If you are not prompted to restart the VM within PowerShell, please close the RDP Connection, return to the Azure Portal and select your VM. At this point you can either "restart

your VM" and reconnect via RDP or you can *STOP* the VM and *Start* the VM again.

5. Login back to the Virtual Machine, using RDP, open **Microsoft Edge** and download the '[Storage Explorer](#)' click **Download now**.



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

You will execute this task on your physical machine, not in the Virtual Machine you created in the previous steps.

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 one of the previous steps.
- **Storage Account Name:** mdfiles+Suffix.
- **Region:** (*EUROPE*) *West Europe* or a region near your location
- **Performance:** Standard
- **Redundancy:** Locally-redundant storage(LRS)

3. Click **Review + Create**. After validation is complete, click **Create**

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

Home > Create a resource > Storage account >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

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 * Azure Pass - Sponsorship

Resource group * rg-md4iot-mst01 [Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ * mdfilesmst01

Region ⓘ * (Europe) West Europe

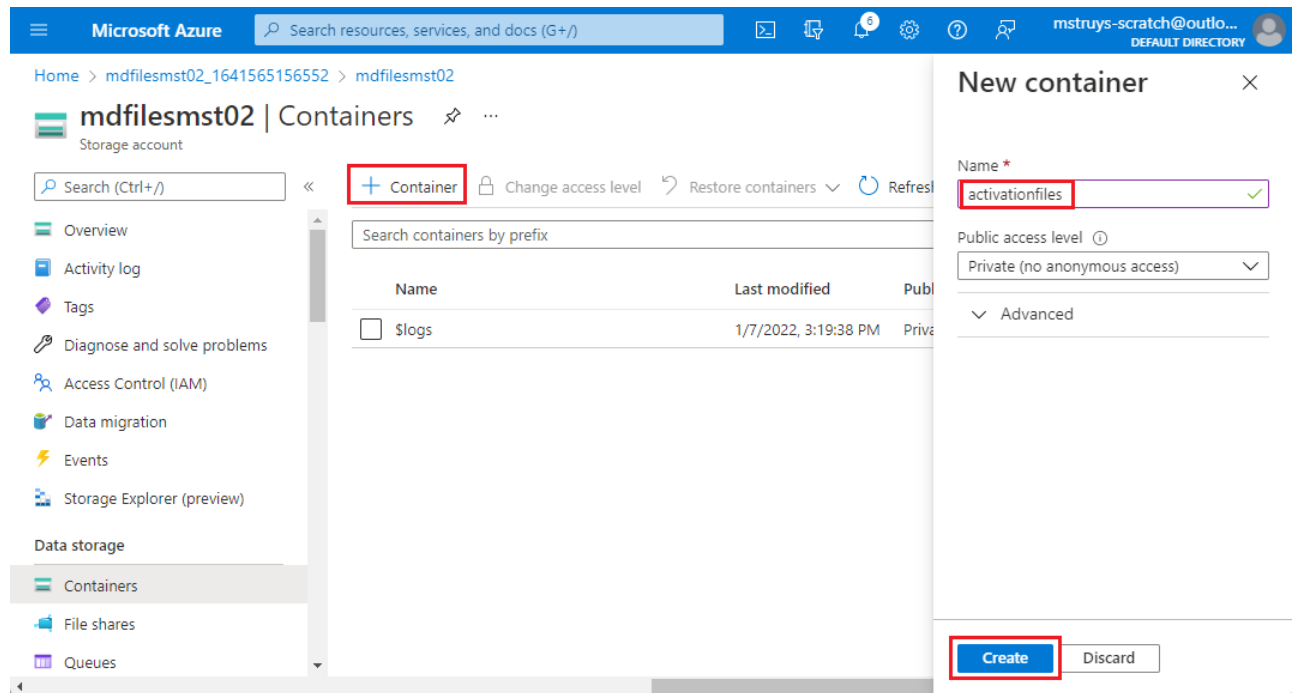
Performance ⓘ *

- ☒ Standard: Recommended for most scenarios (general-purpose v2 account)
- ☐ Premium: Recommended for scenarios that require low latency.

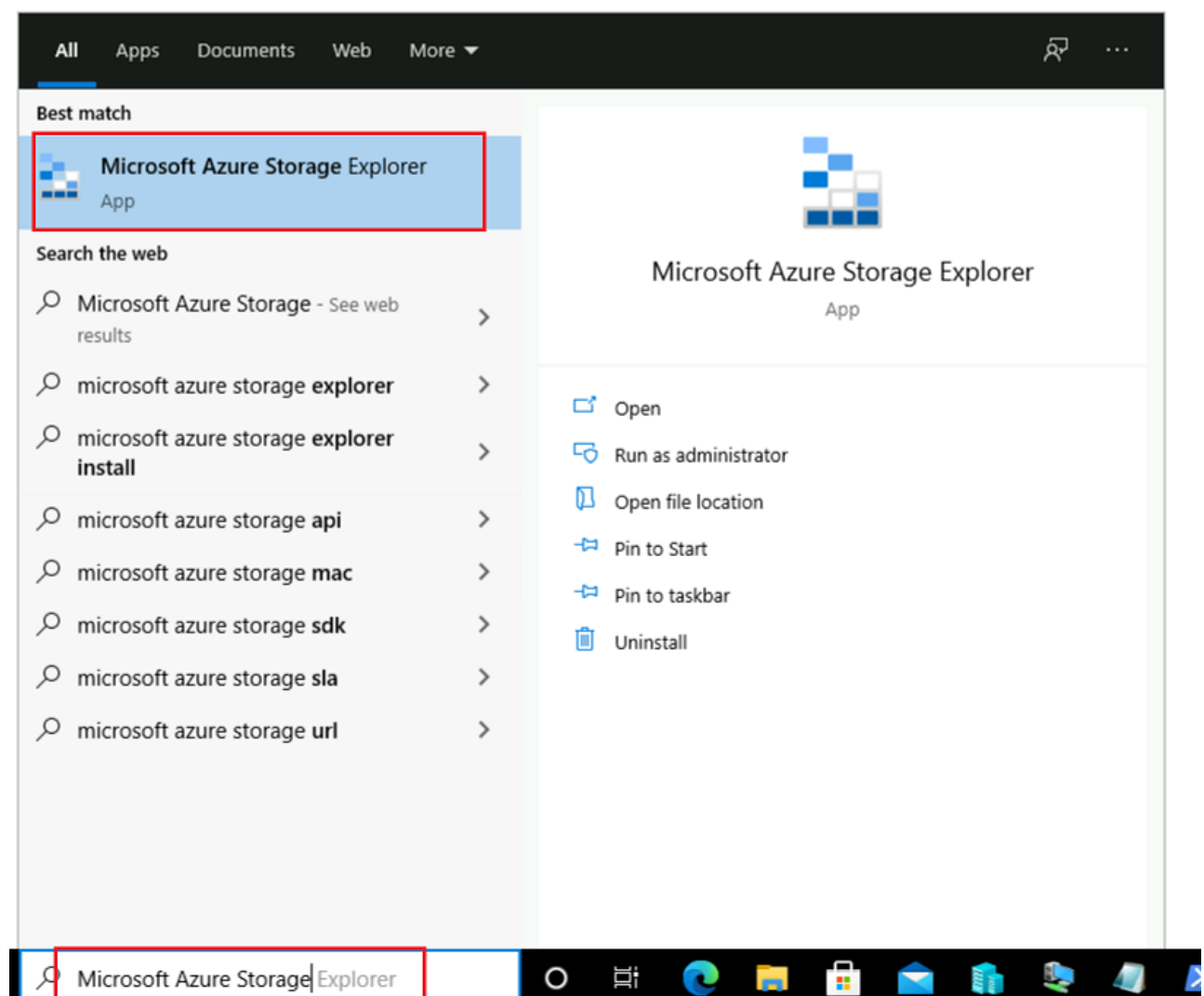
Redundancy ⓘ * Locally-redundant storage (LRS)

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

- Once the Storage account is created, click on it. Under **Data Storage** select **Containers**, then on the right side select **+ Container**.
- A new window will open on the right, assign a name **activationfiles** and then click **Create**.

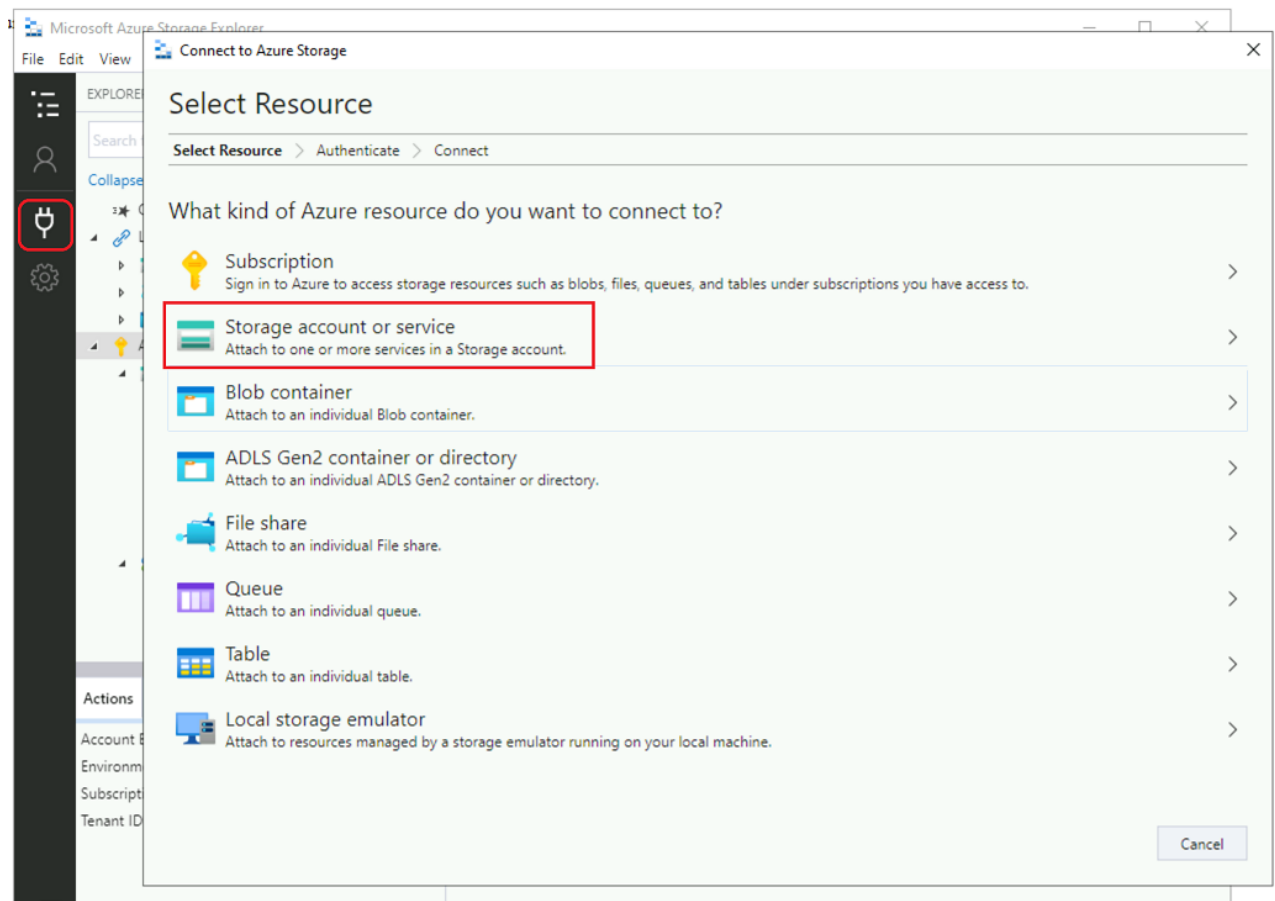


6. Login to the Windows Virtual Machine you created earlier with RDP. In the search box on the desktop enter **Microsoft Storage Explorer**.

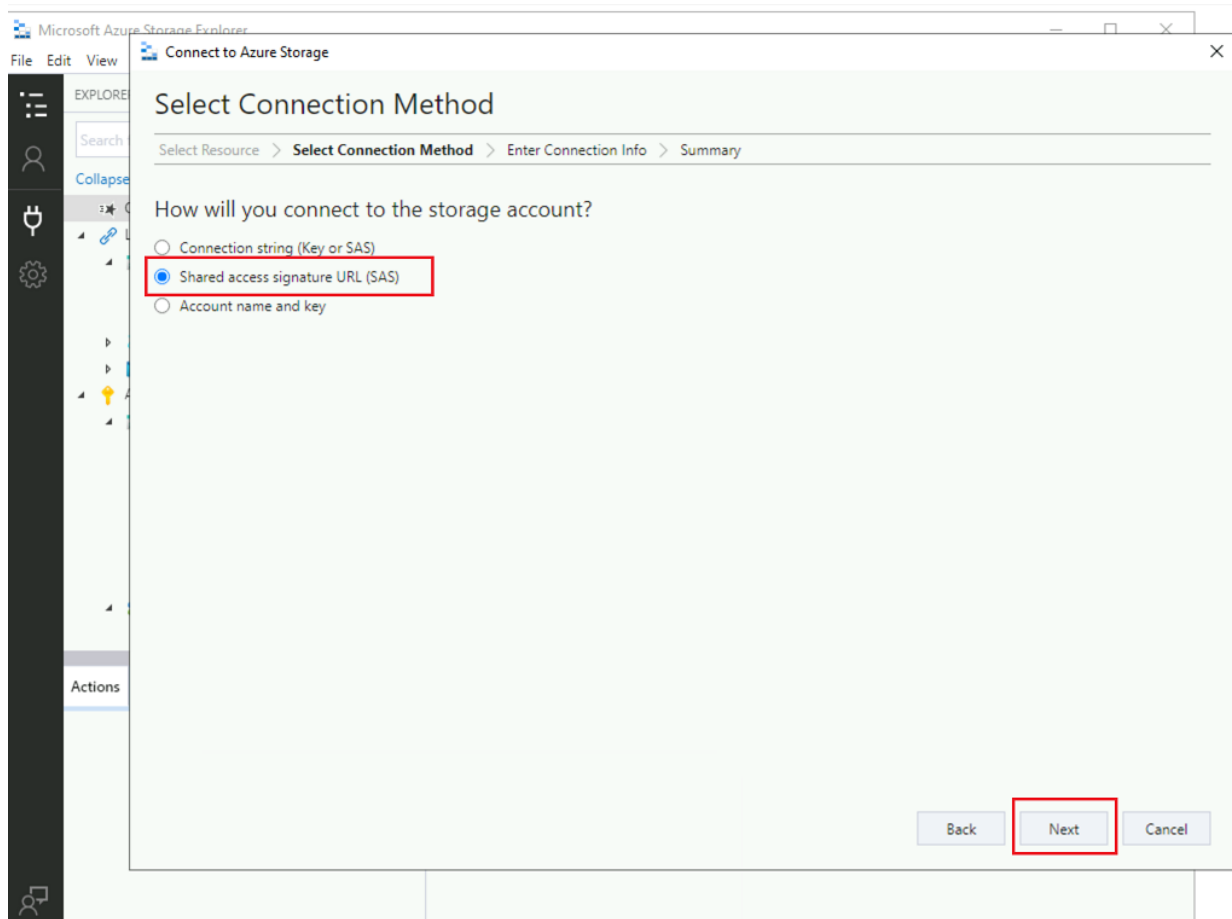


7. You will be prompt to login, use the personal email you are using to set up your Azure Pass for this training.

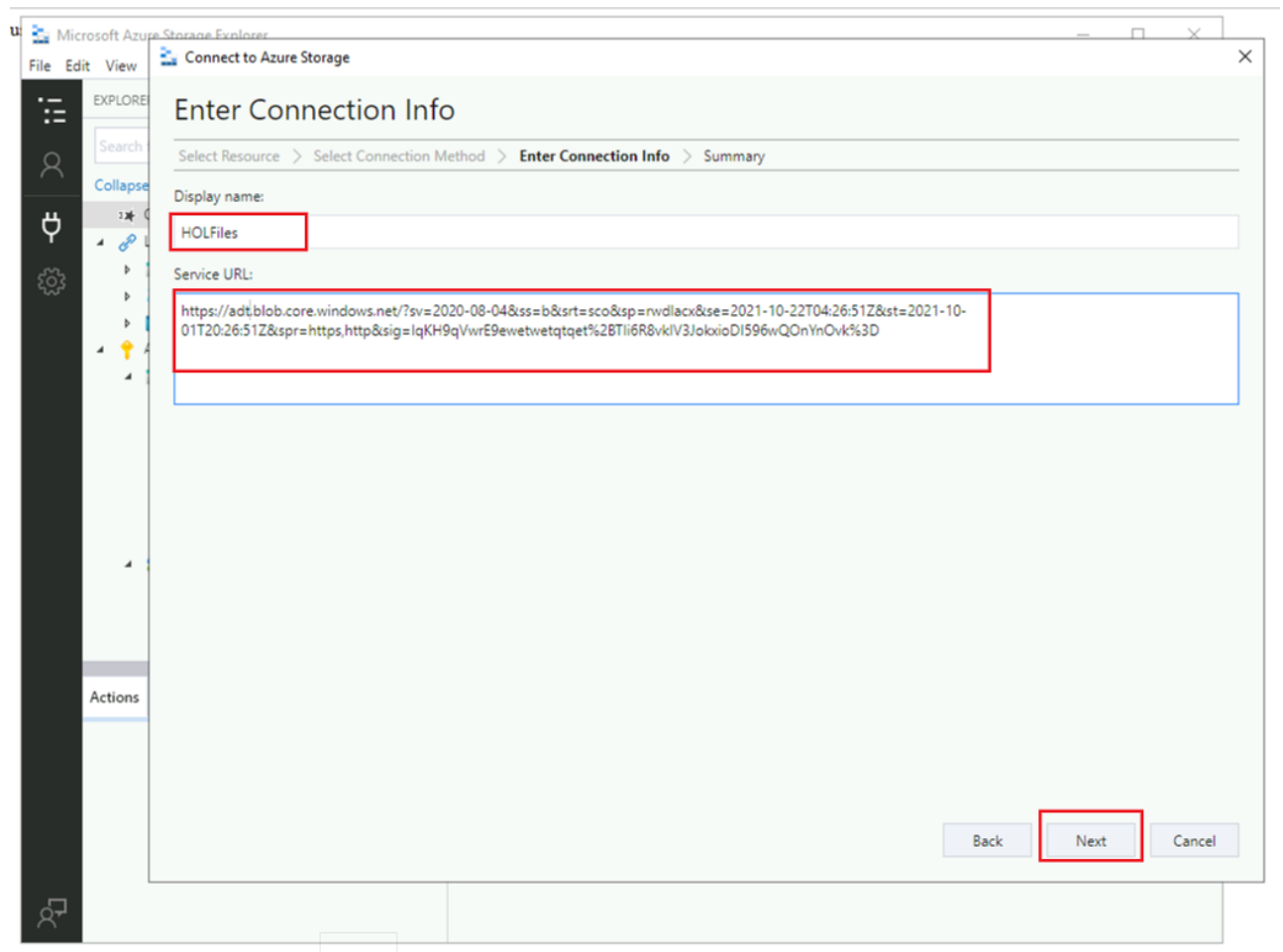
8. Once you are login, go to the connect icon on the left bar, then select **Storage account or service**.



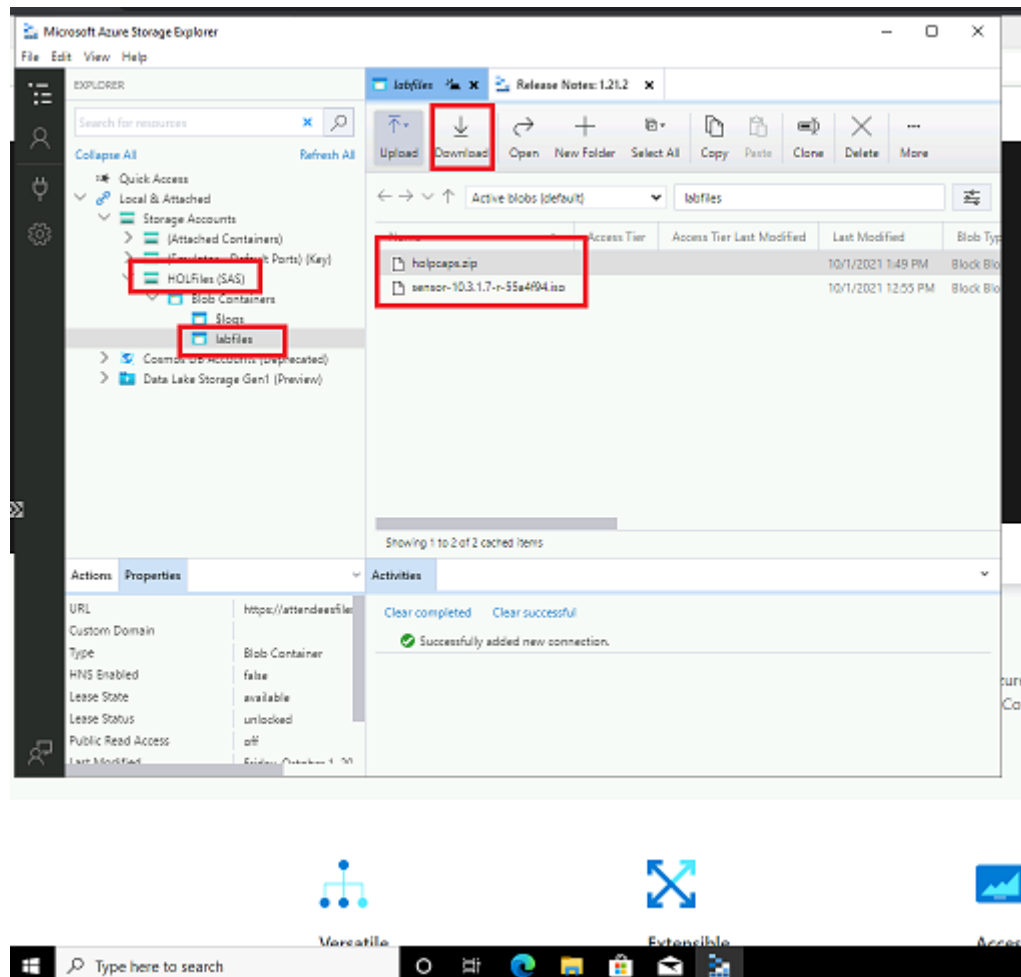
9. In the next step select **Shared Access Signature URL(SAS)** and then **Next**



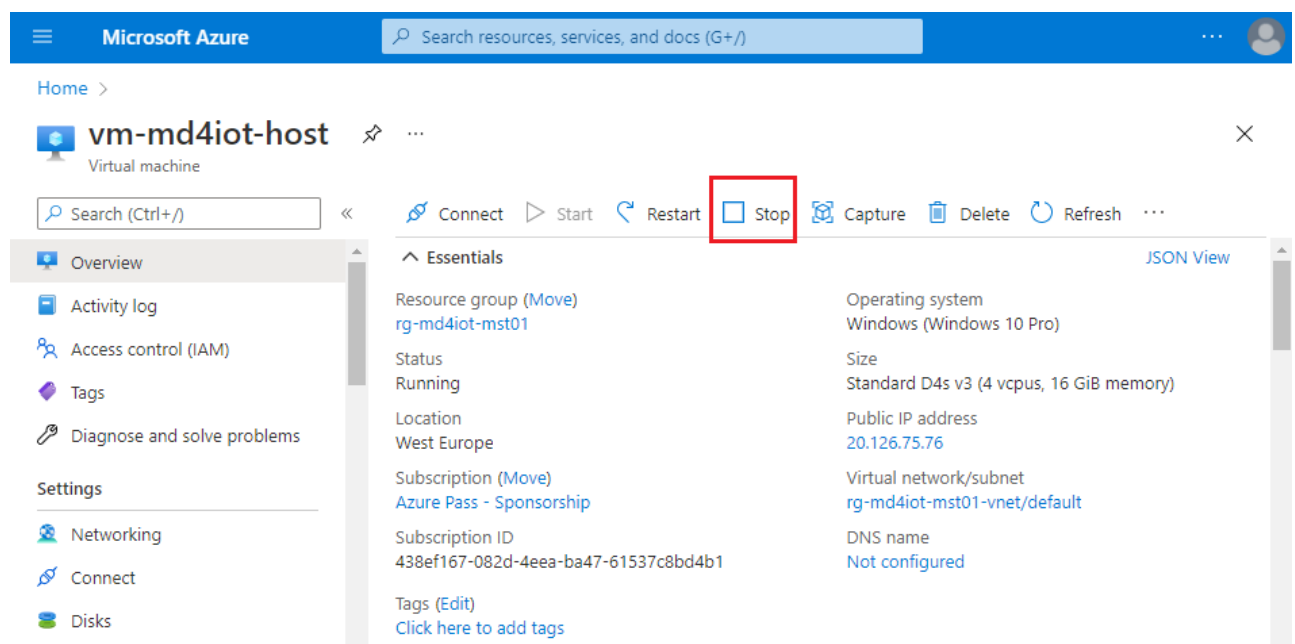
10. In the Enter Connection Info window, you will assign a name to the connection **HOLFiles** and you will paste below the Blob SAS URL (service URL) you received by email in the confirmation email that you received after registering for this HOL. If you didn't receive any confirmation mail (with subject *Microsoft Defender for IoT/OT Hands-on Lab: you are registered!*), please check your spam folder or send us an email at iotacademy@microsoft.com.



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**



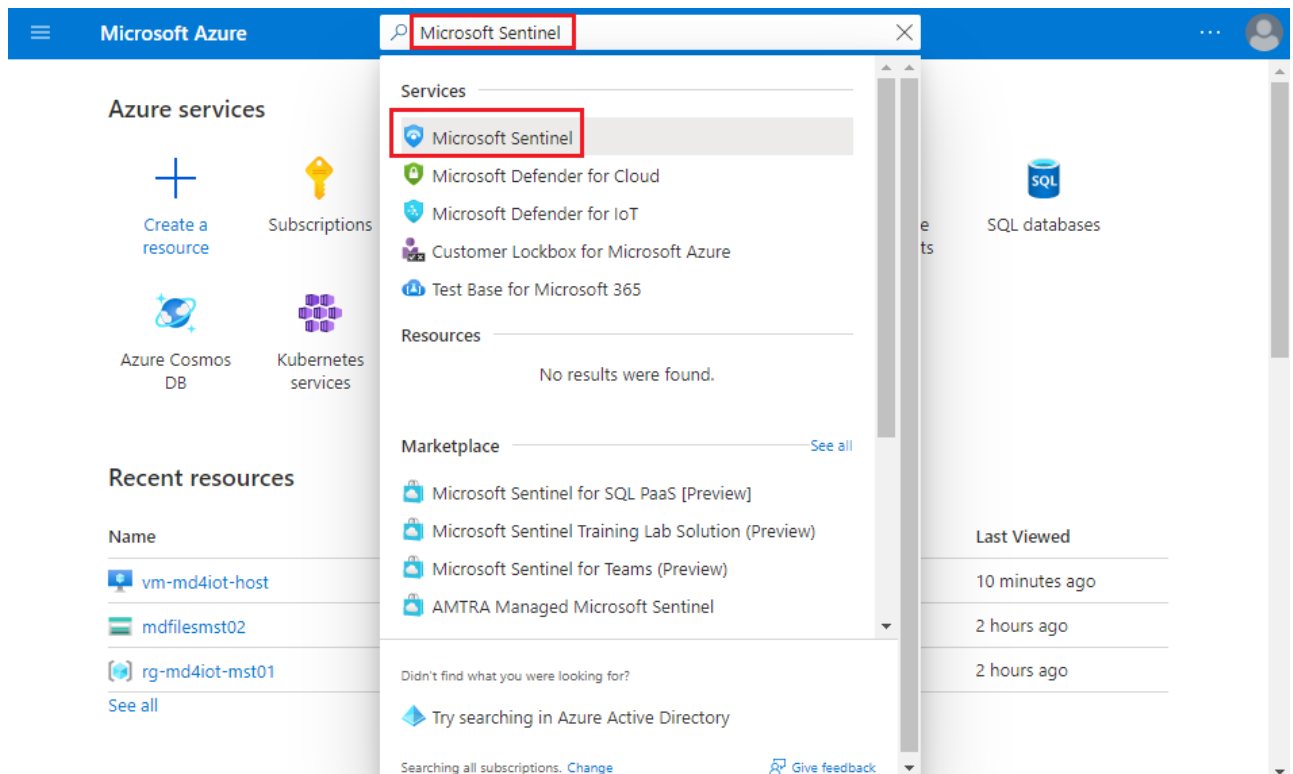
12. When this download is complete, close your RDP connection.
13. On your physical machine, go to the Azure Portal, select your Virtual Machine and click **Stop**. Now you are all set for your training session.



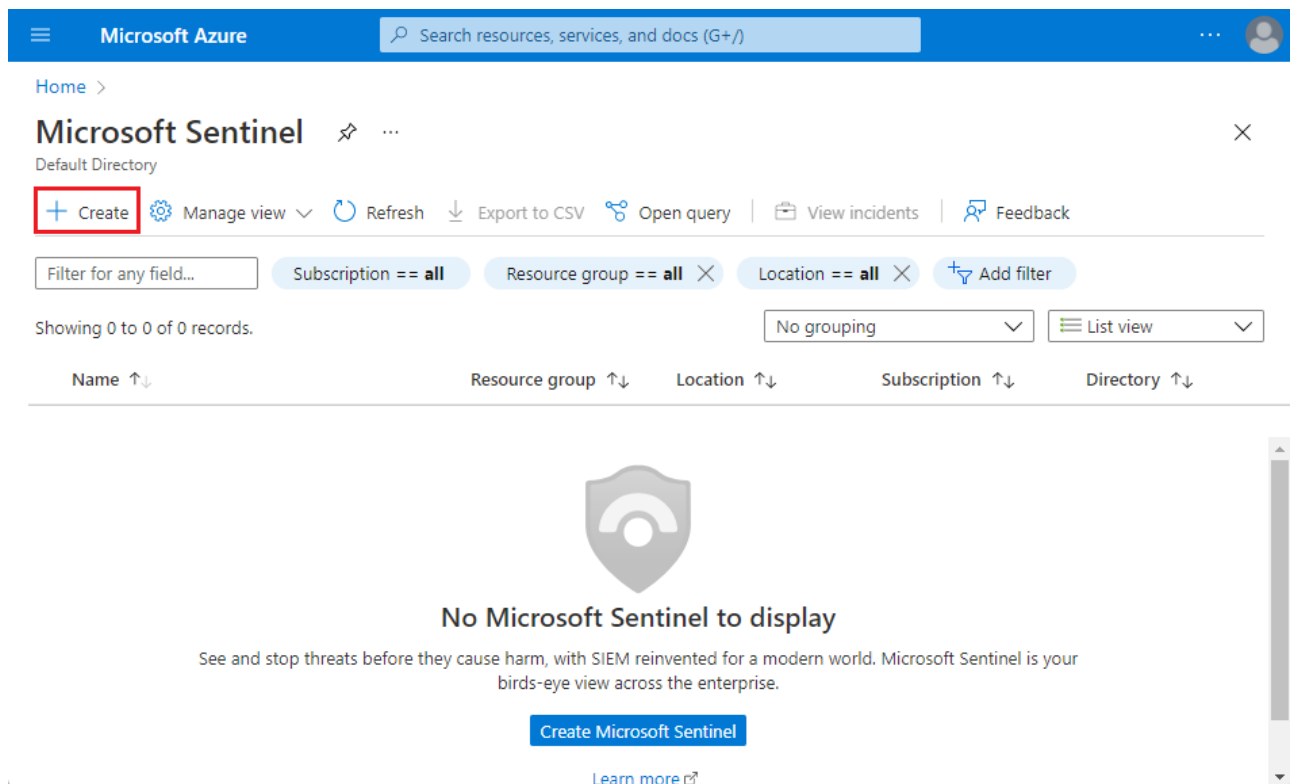
Task 6: Microsoft Sentinel

You will execute this task on your physical machine, not in the Virtual Machine you should have stopped in the previous step.

1. Go to Azure Portal, in the top search box, type **Microsoft 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:** West Europe (or another region close to you).

Microsoft Azure

Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace >

Create Log Analytics workspace

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 * ⓘ rg-md4iot-mst01
[Create new](#)

Instance details

Name * ⓘ MyLogWorkspace-mst01 ✓

Region * ⓘ West Europe

Review + Create << Previous Next: Tags >

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.