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

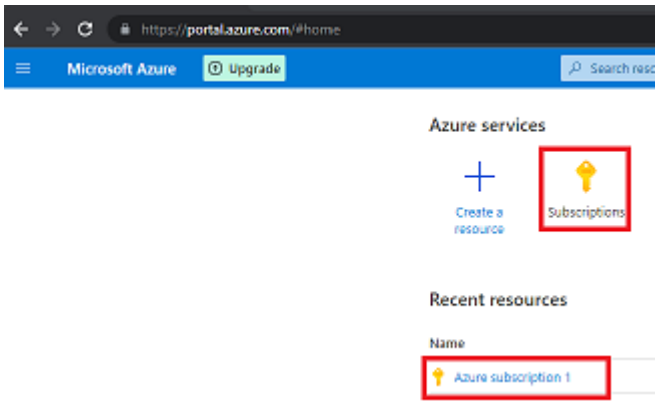
Prior to this workshop, after successful registration, you will receive an Azure Pass. You can activate this Azure Pass with your personal email account. This step will be coordinated with your instructors.

Task 1: Activating your Azure Pass

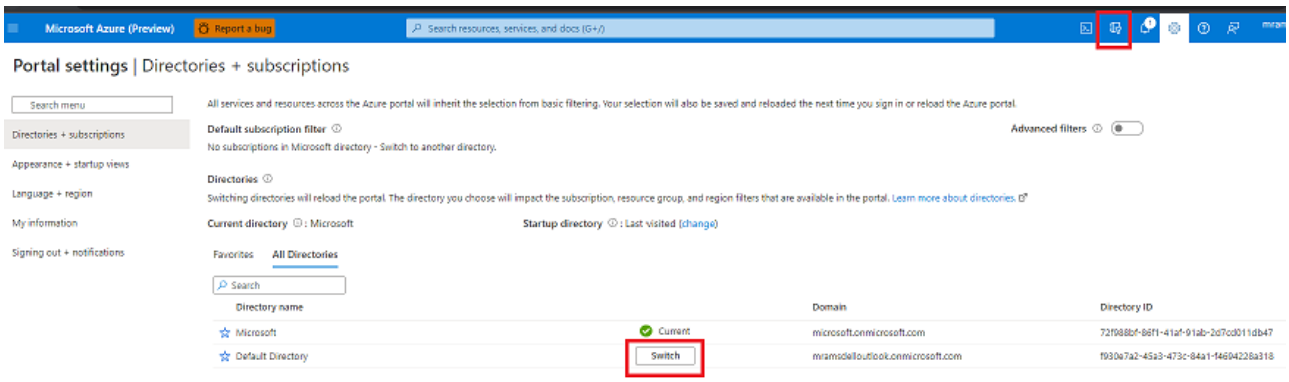
1. Go here to activate your Azure Pass.
2. Click on **START**. Make sure you set up this pass with a personal email or just create an outlook email account for this training.
3. After you login and validate the account, you will be asked to **Enter the Promo Code**. Here you will copy the Azure Pass 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 sould 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.

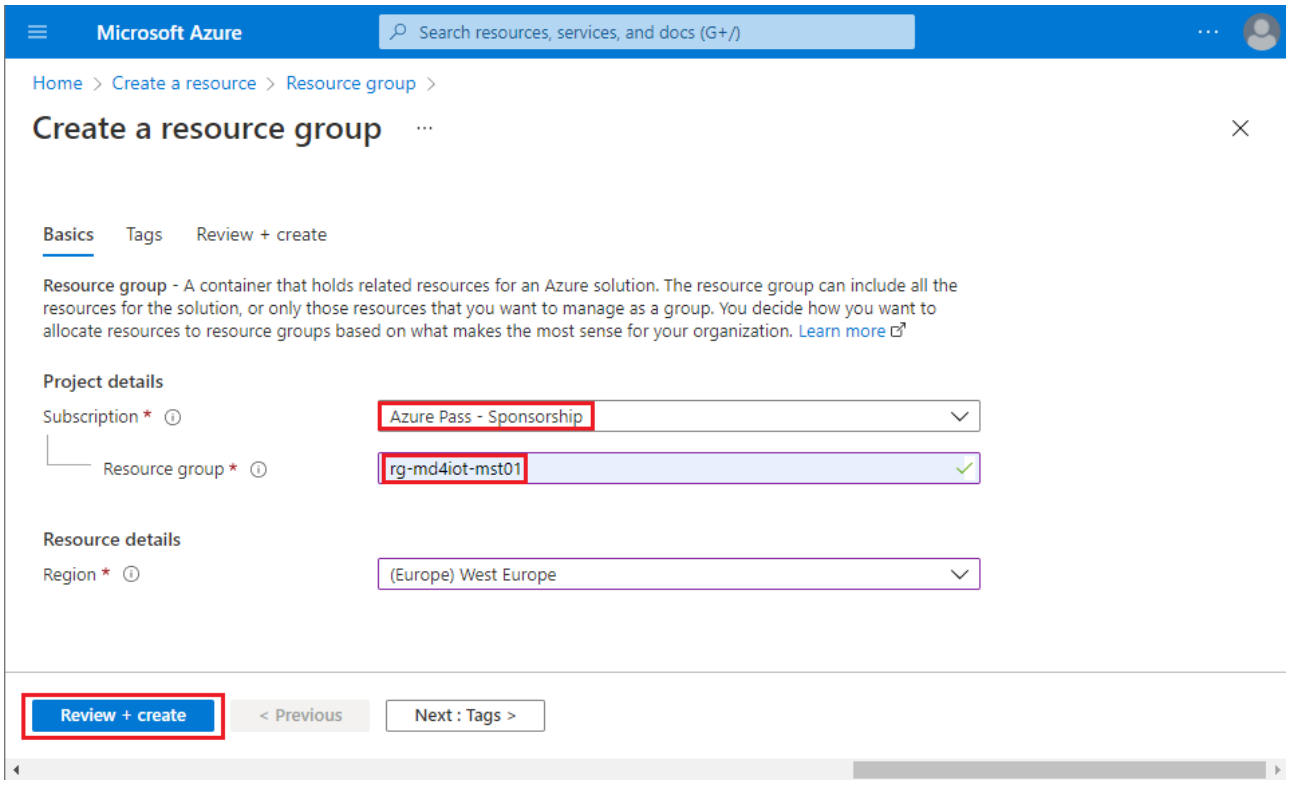
Task 1: Resources

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**.

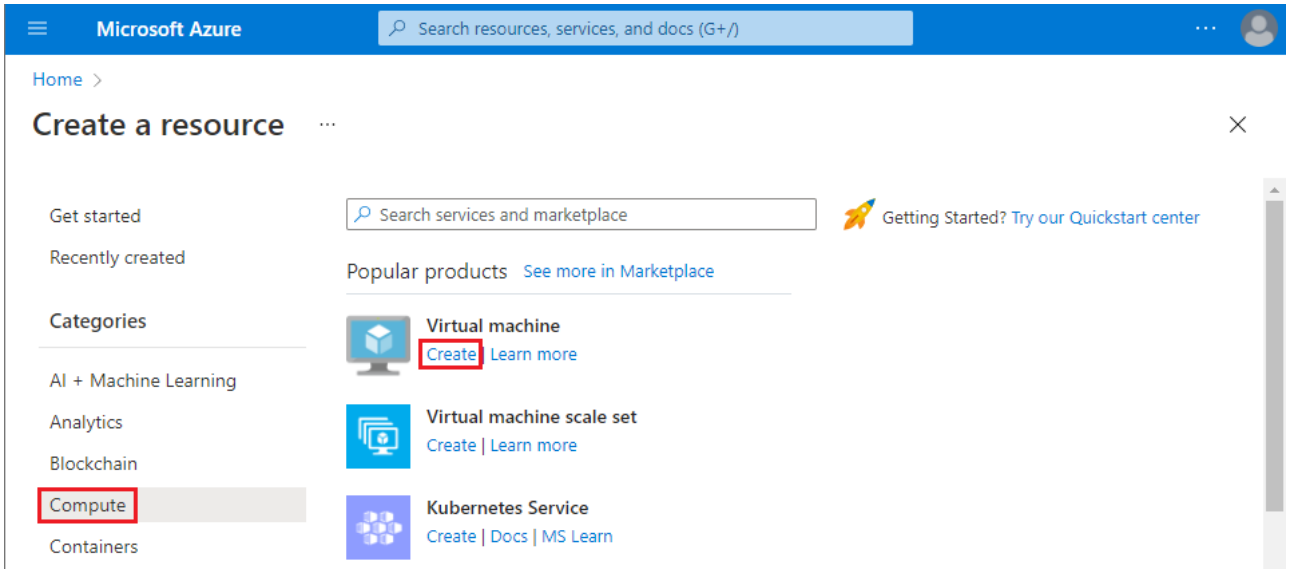
3. Once you passed the validation, click **create**.

> 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.



Task 2: Virtual Machine

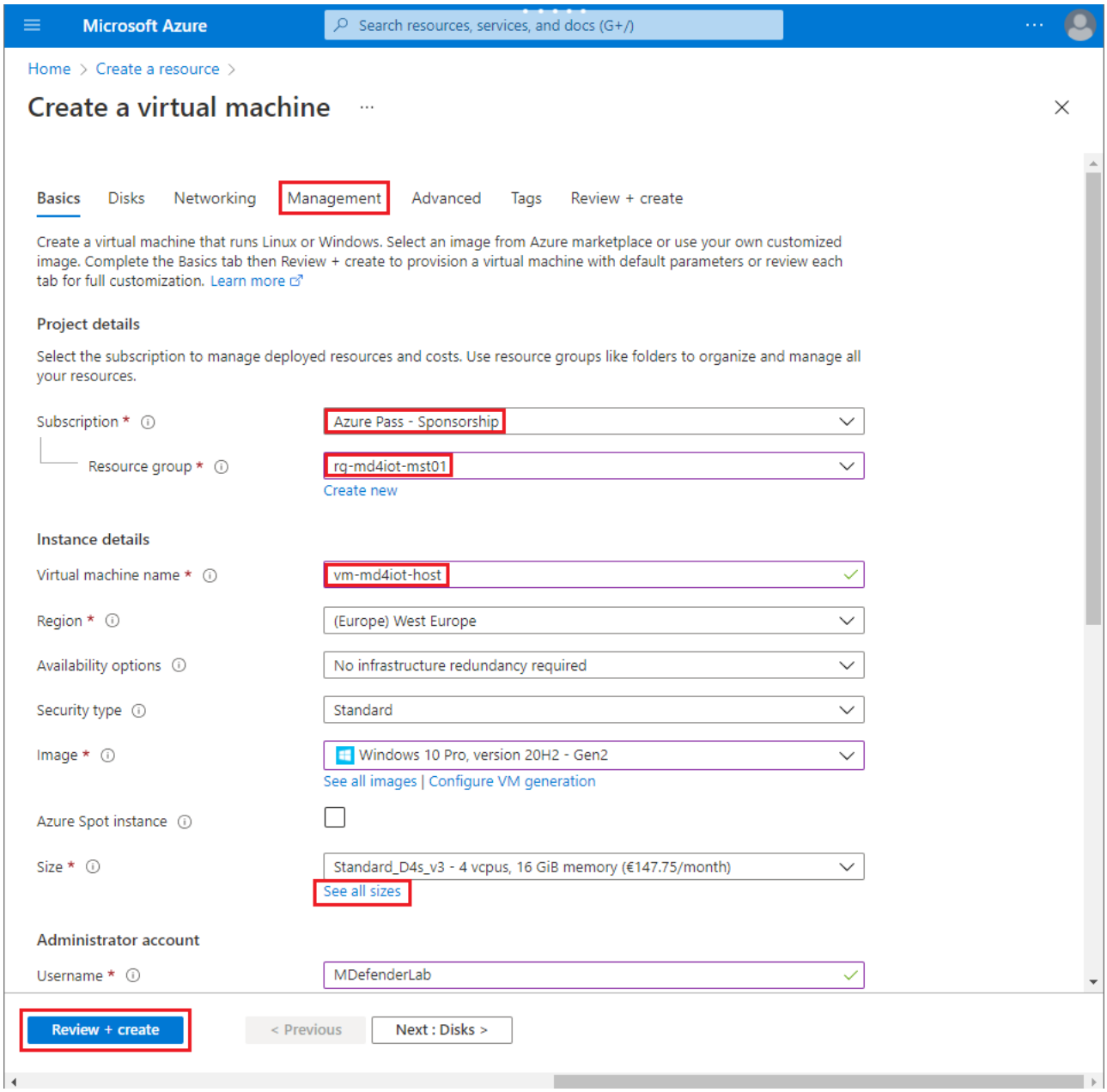
1. In the upper-left side of the Azure Portal, select: **Create a resource** > **Compute** > **Virtual machine** >> **Create**



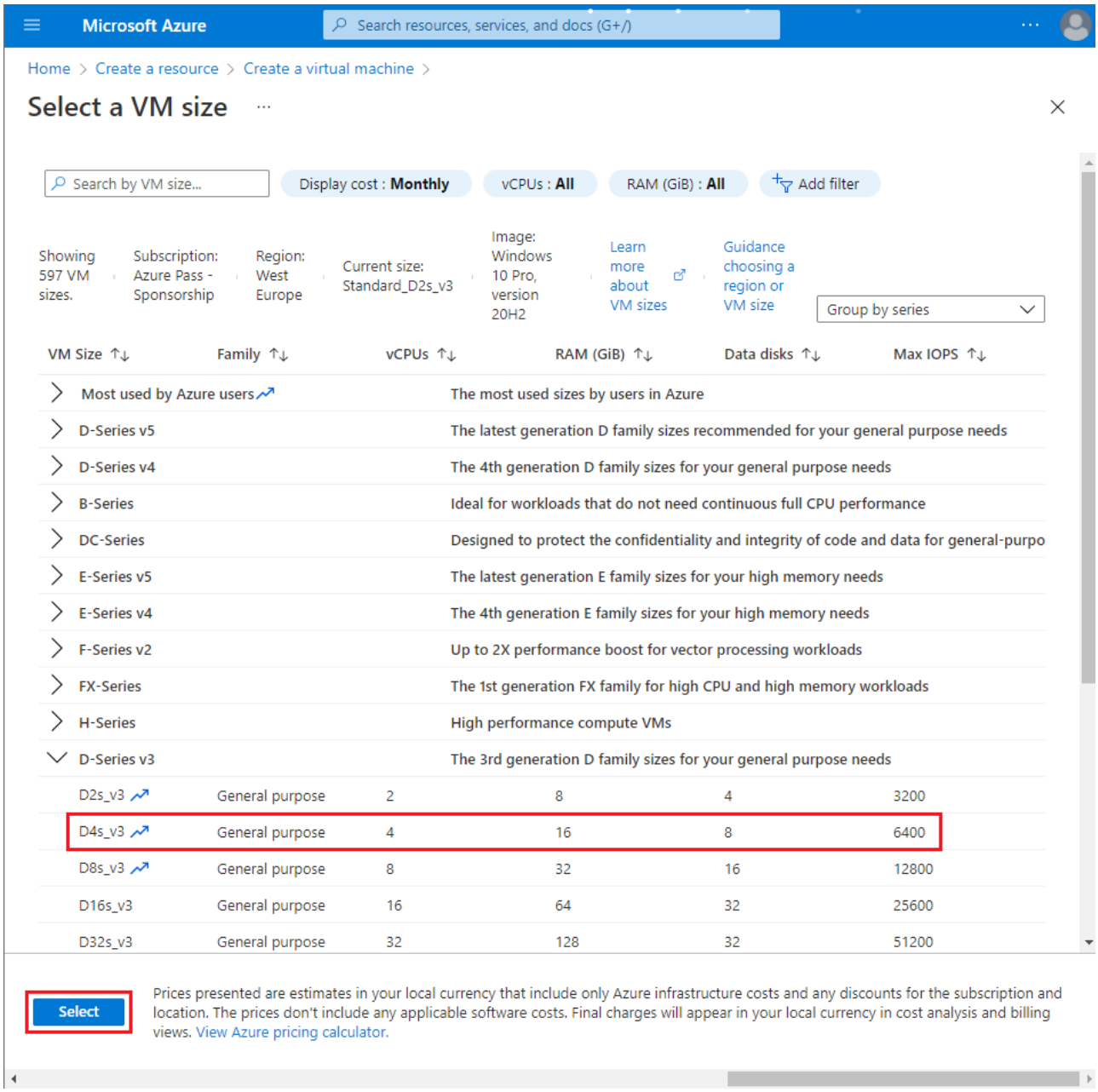
2. In **Create a virtual machine**, type or select the values in the **Basics** tab:

Setting	Value
Project Details	
Subscription	Select your Azure subscription
Resource Group	Select your 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**.



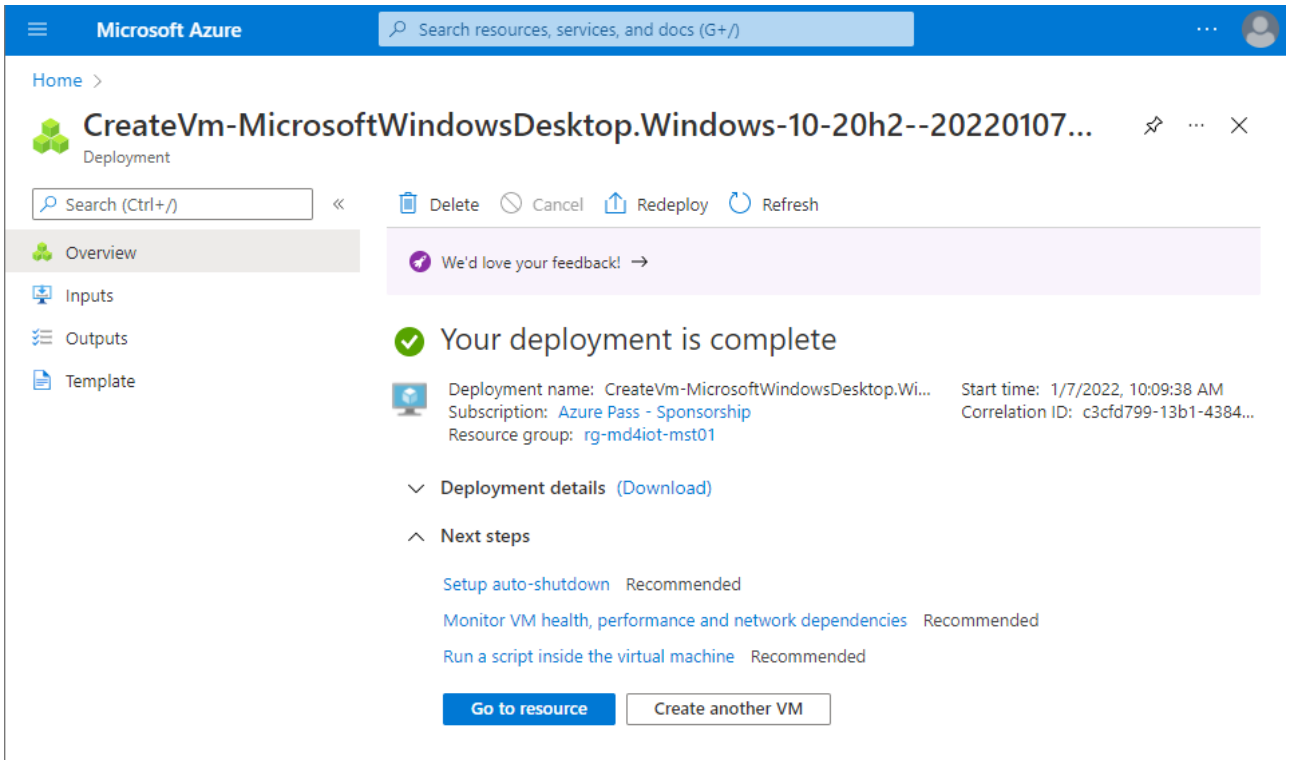
3. In the Size section, select **See all Images**, look for the **D-Series v3** open that section, then you will find the right VM.



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

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

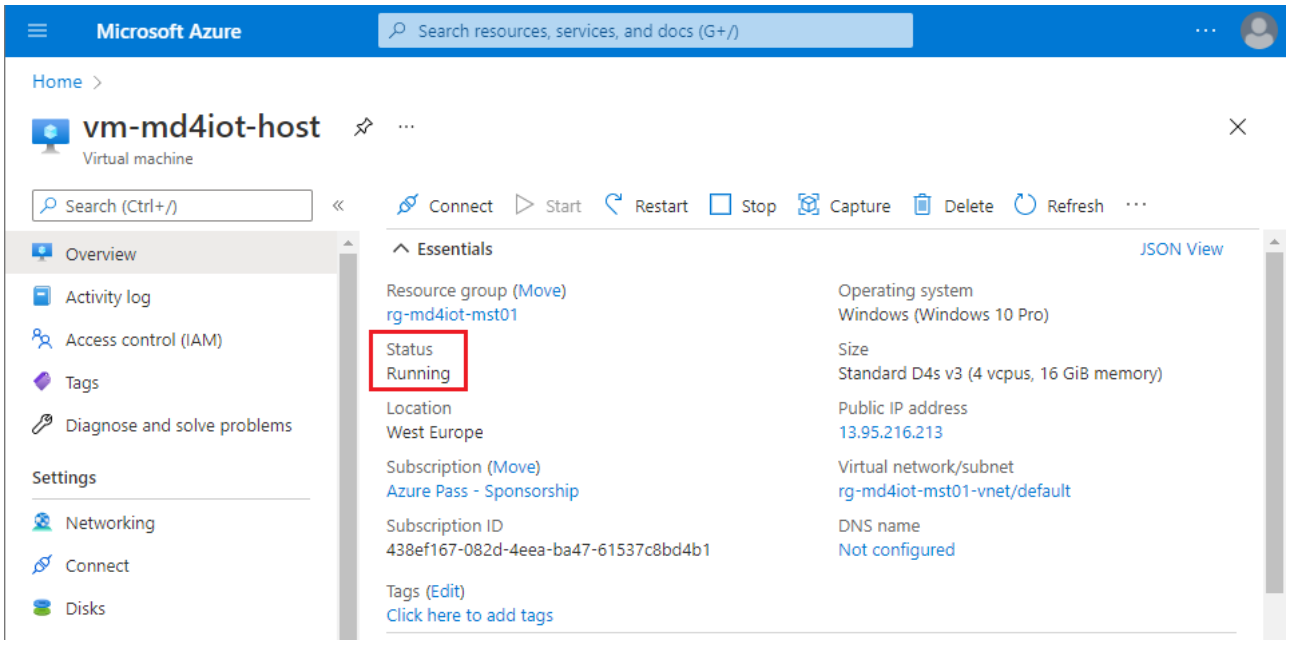
6. It will take a few minutes to deploy your VM. At the end you should an indication that your deployment is complete.



Task 3: Connect to Virtual Machine

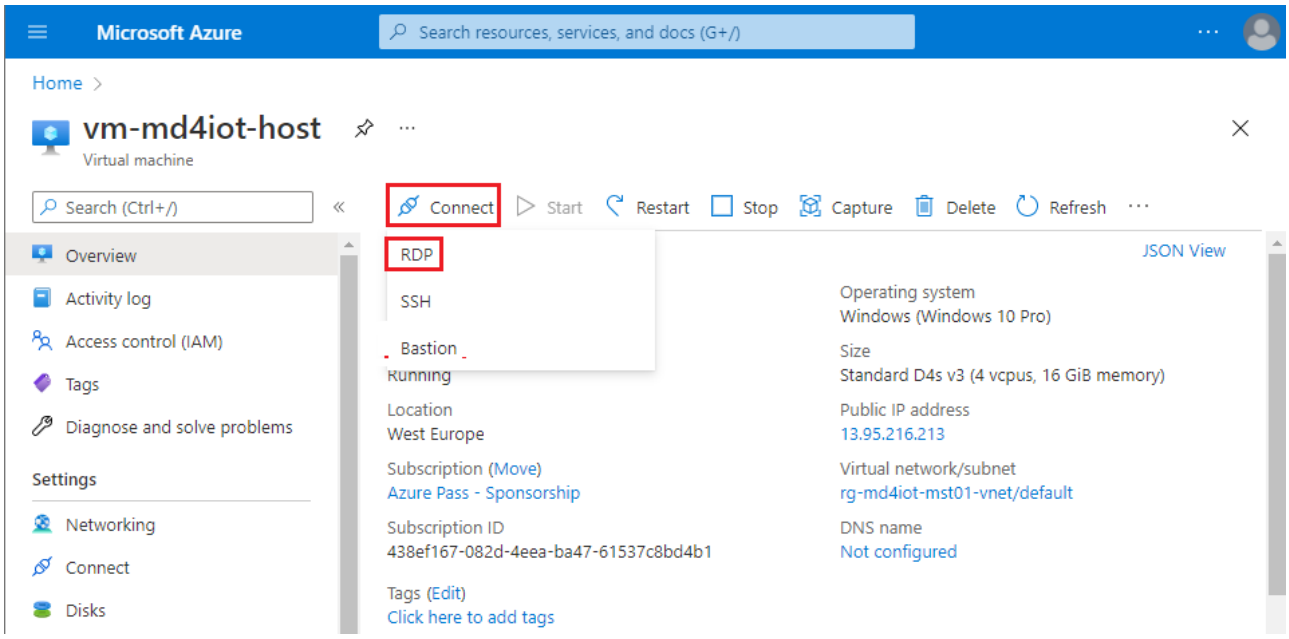
1. Navigate to the Azure Portal Home and select your newly created virtual machine.

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



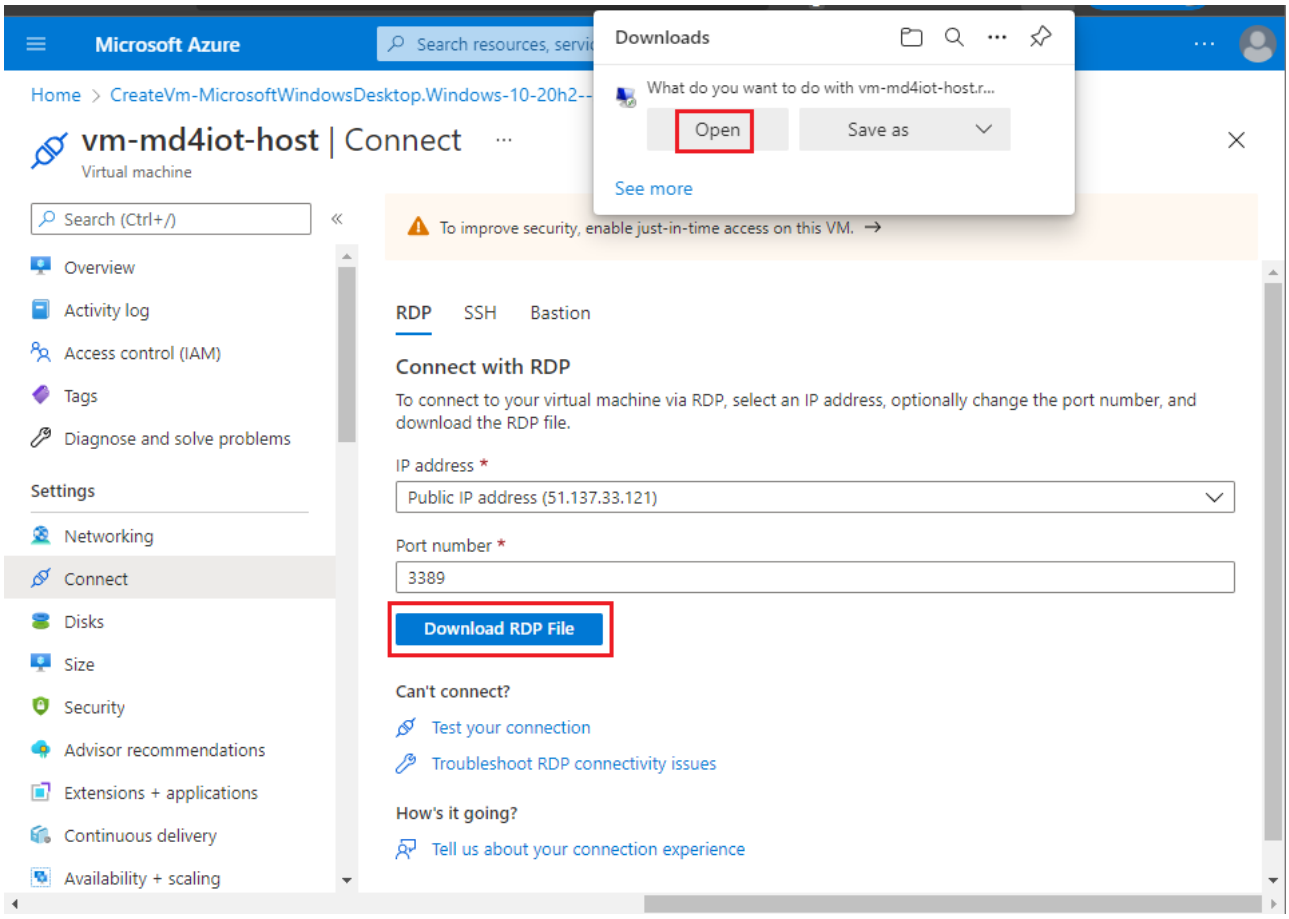
> **TIP:** You will not be able to connect if your Virtual Machines is not in **Running** status. So give it a minute or two to finish updating.

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.

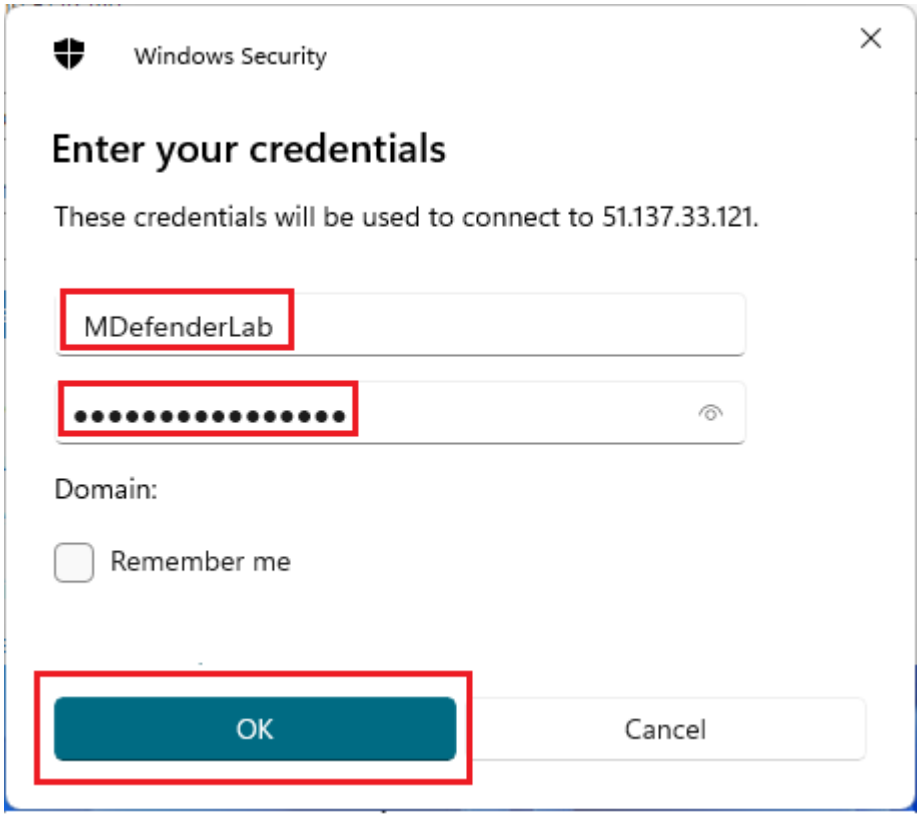
4. In the **Connect** page, click on **Download RDP File** and click on **Open**.



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

Field	Enter

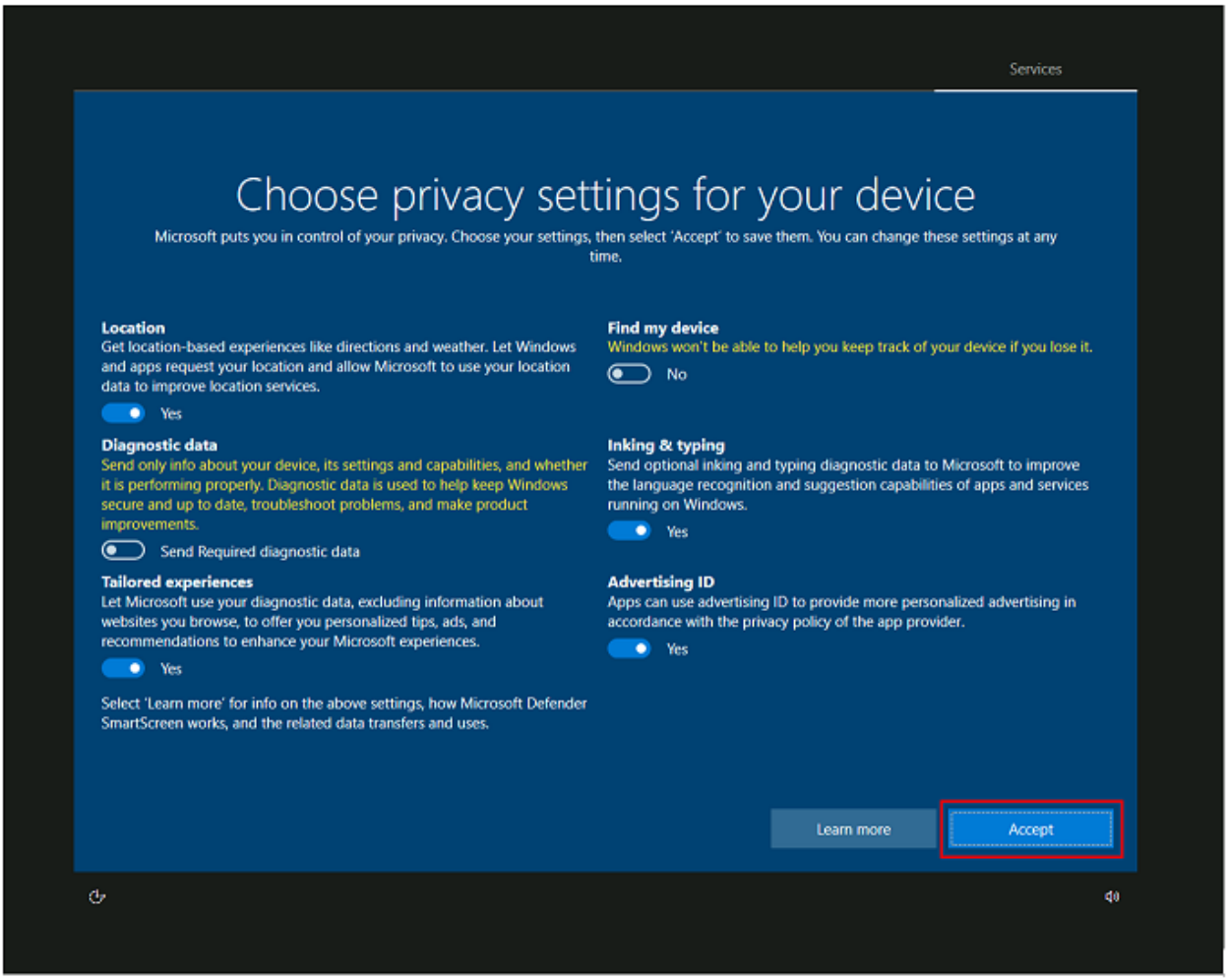
Field	Enter
Username	*MDefenderLab*
Password	*Learningmode123!*



6. Click **OK** to login to the virtual machine.

7. A new window should open which is the connection to your Virtual Machine.

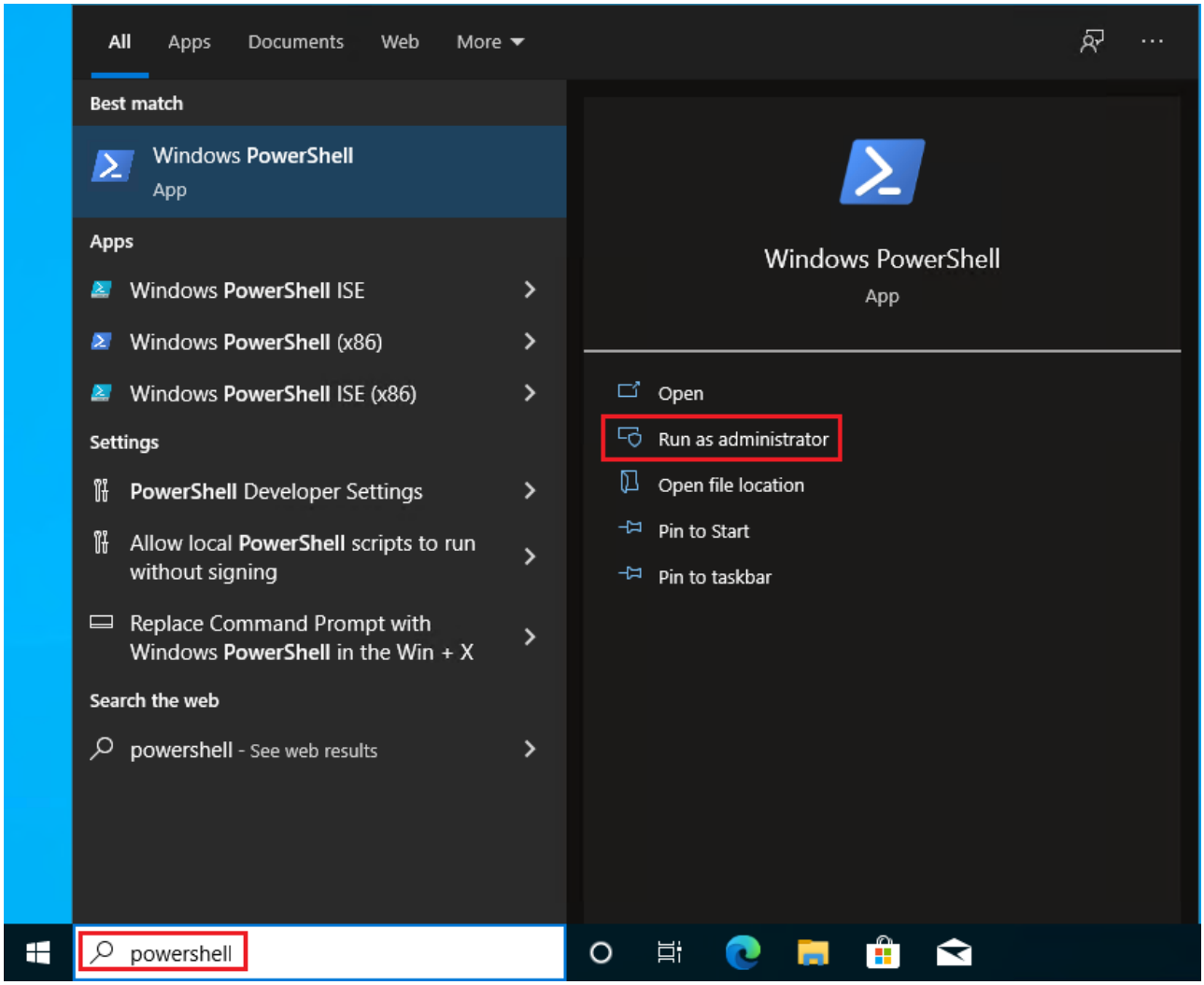
8. **Accept** the default settings.



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**.

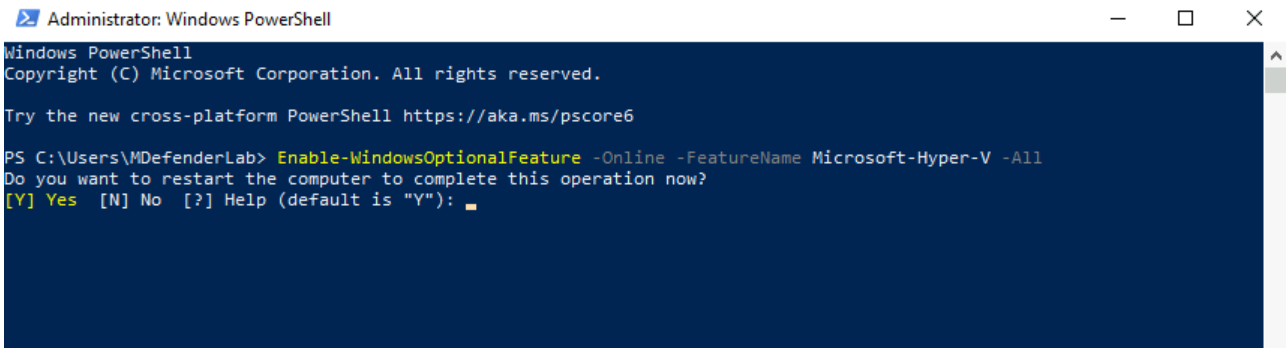


2. Run the following command in the PowerShell Window:

```
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**.

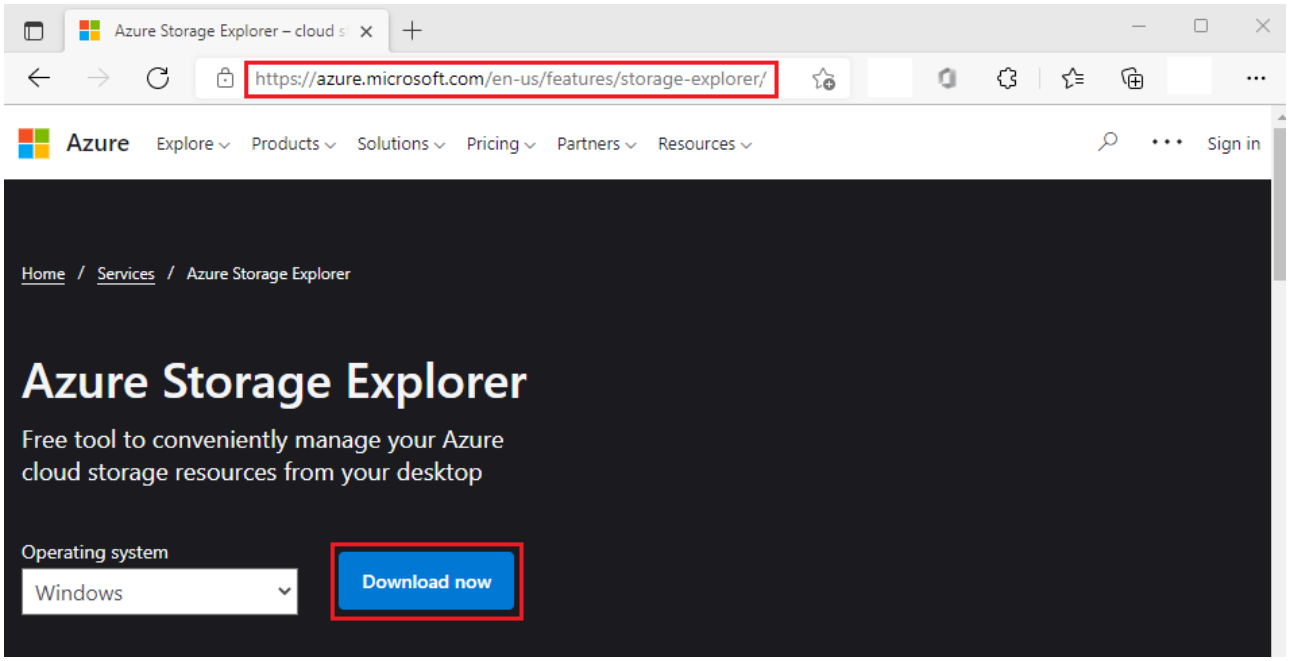


4. Reconnect to the VM.

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

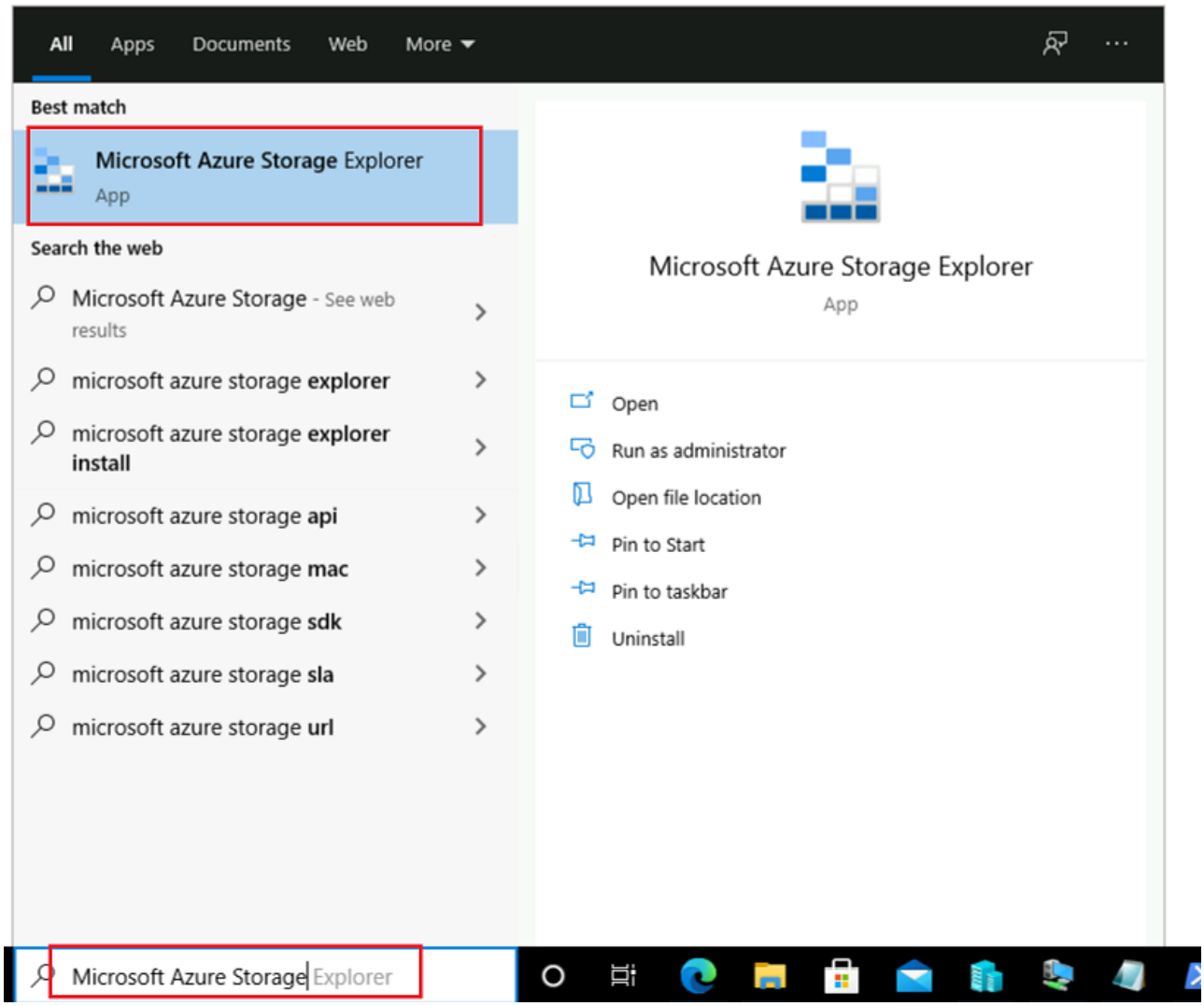
> your VM" and reconnect via RDP or you can *STOP* the VM and *Start* the VM again.

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

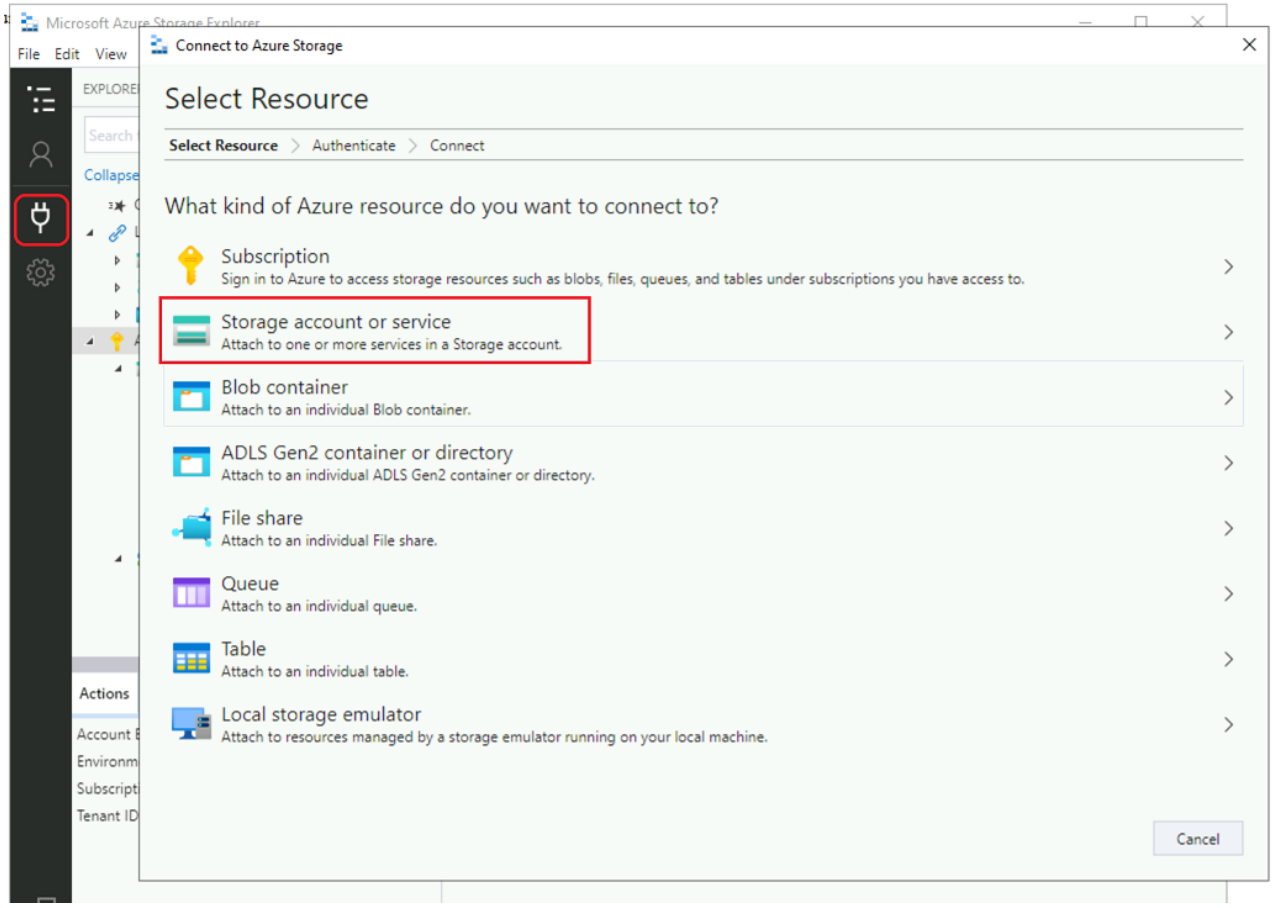


6. Once the download is completed run the installation selecting **Install for me only (recommended)** option. Next, click on **I accept the agreement**, and **Install**, you will ask a few additional questions, select **Next** each time, the installation will run for a few seconds.

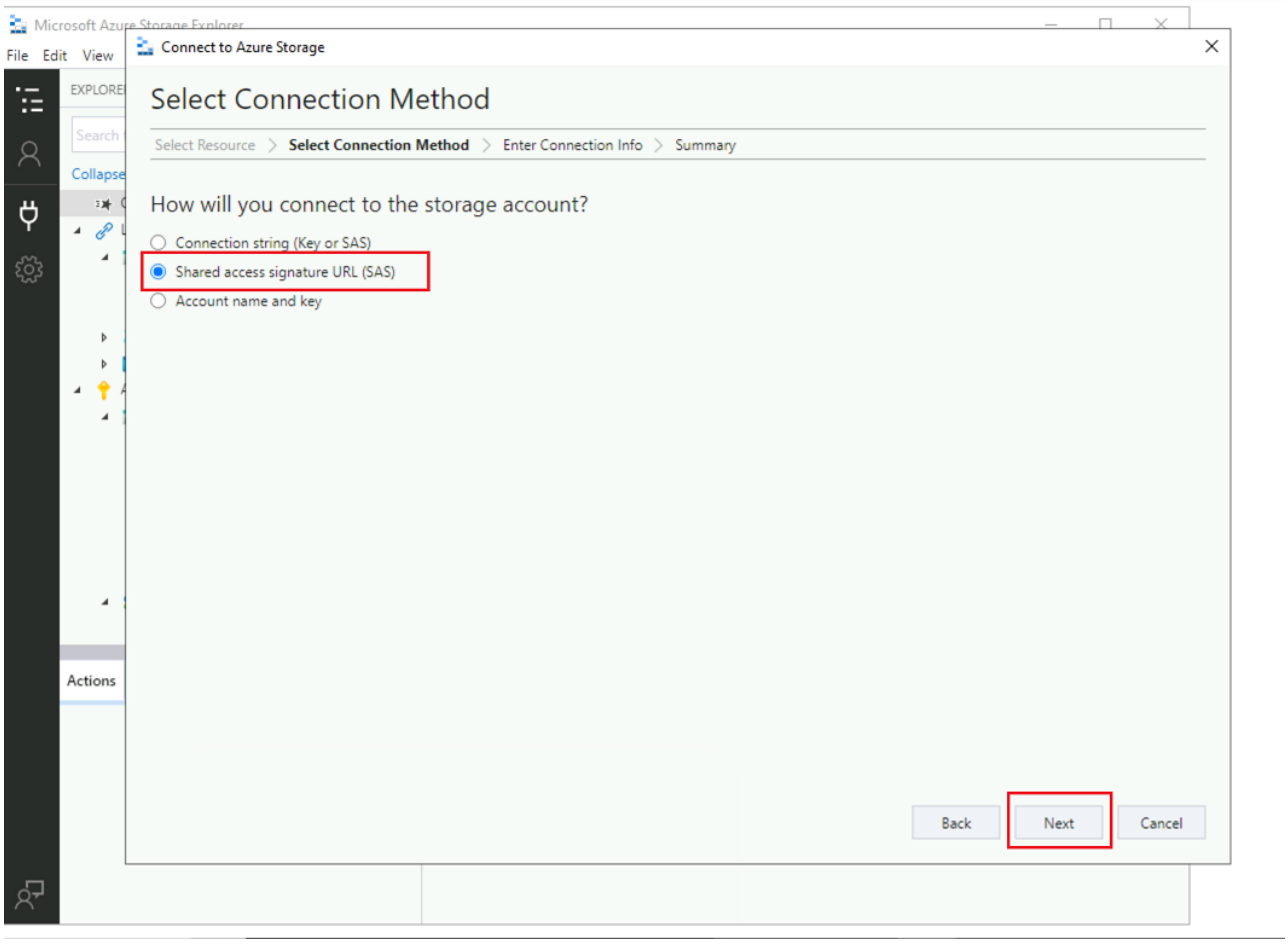
1. On the Windows Virtual Machine you created earlier, in the search box on the desktop enter **Microsoft Azure Storage Explorer** if you don't have the Azure Storage Explorer already open.



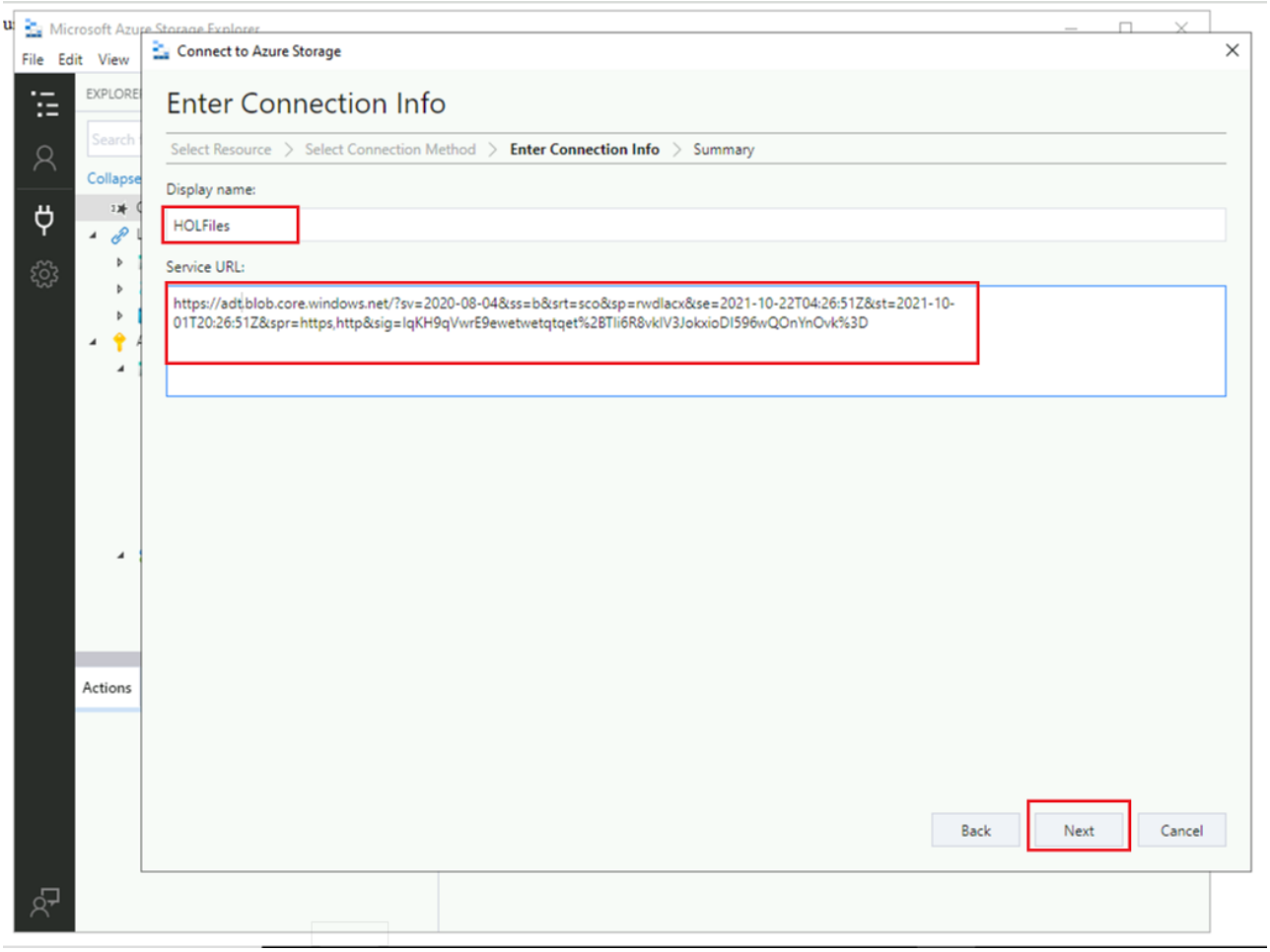
2. Go to the connect icon on the left bar, and select **Storage account or service**.



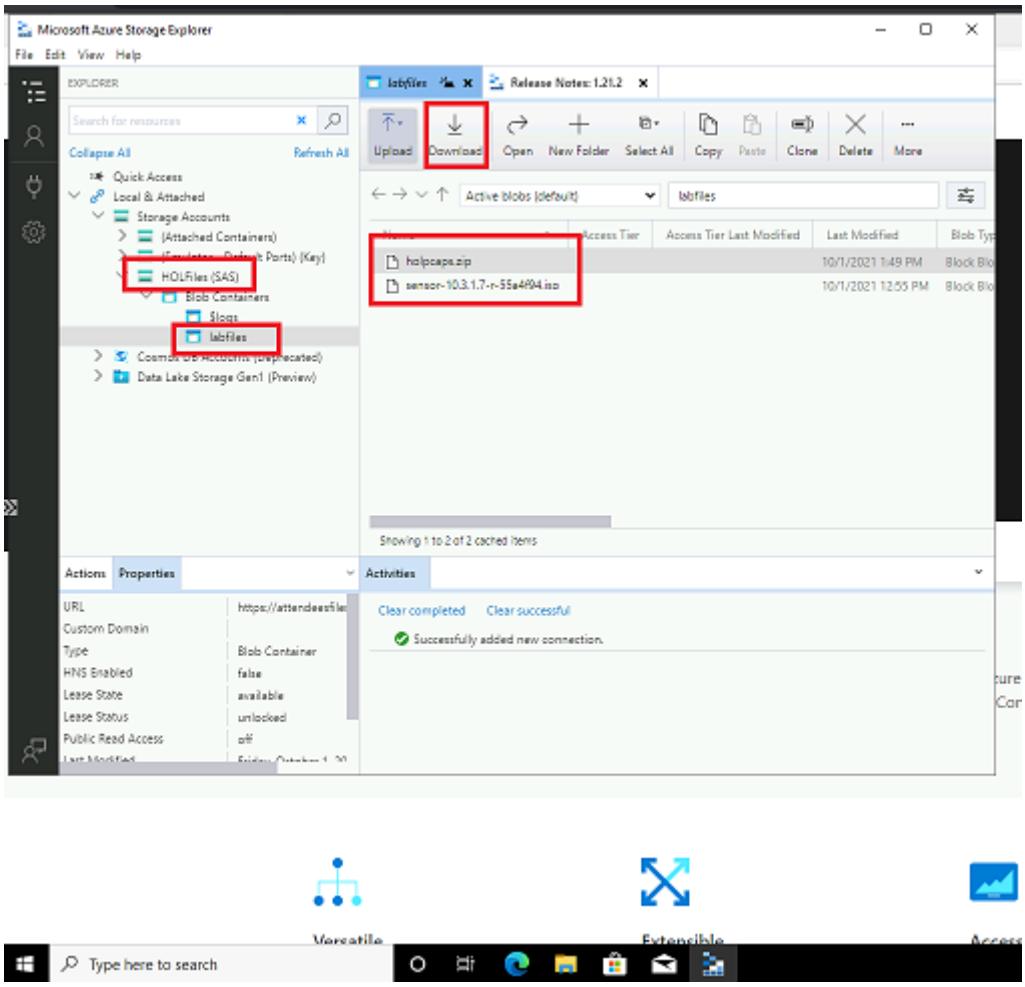
3. In the next step select **Shared Access Signature URL(SAS)** and then **Next**



4. 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 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.

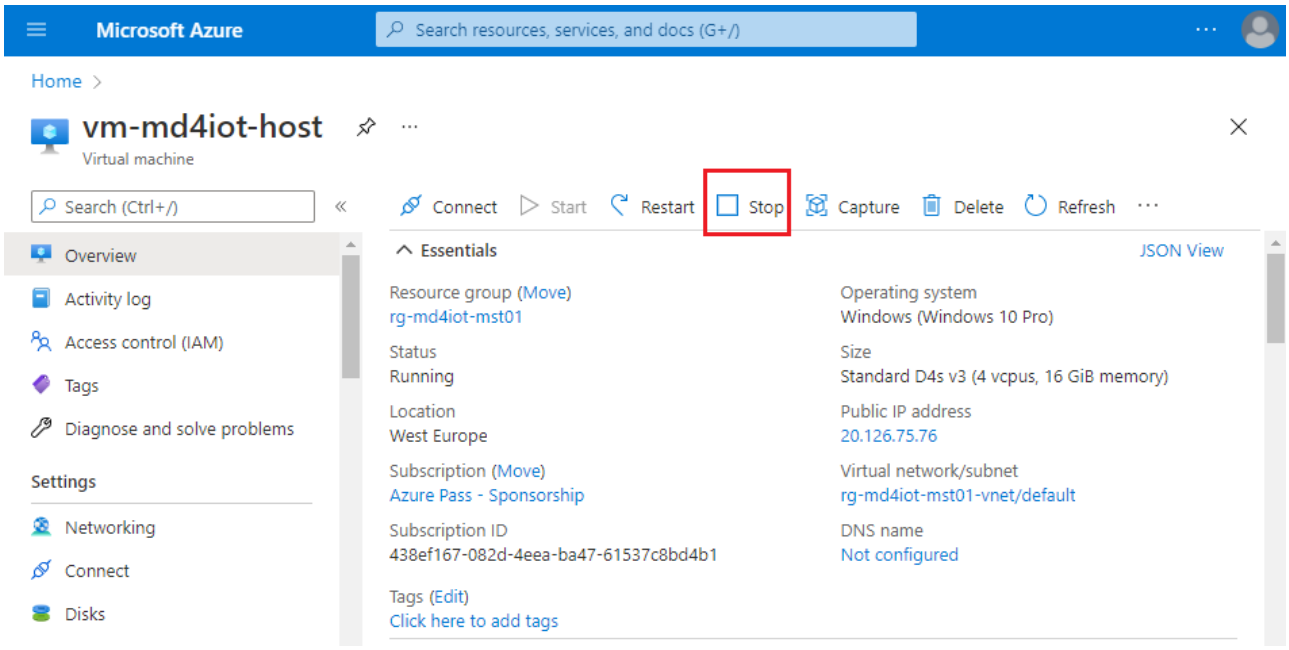


5. Once the storage account is connected you should select the container on the left side **attendeefiles** then **Labfiles** now in the right side you will see the two files you need to download locally. Select the files and click **Download**



6. When this download is complete, close your RDP connection.

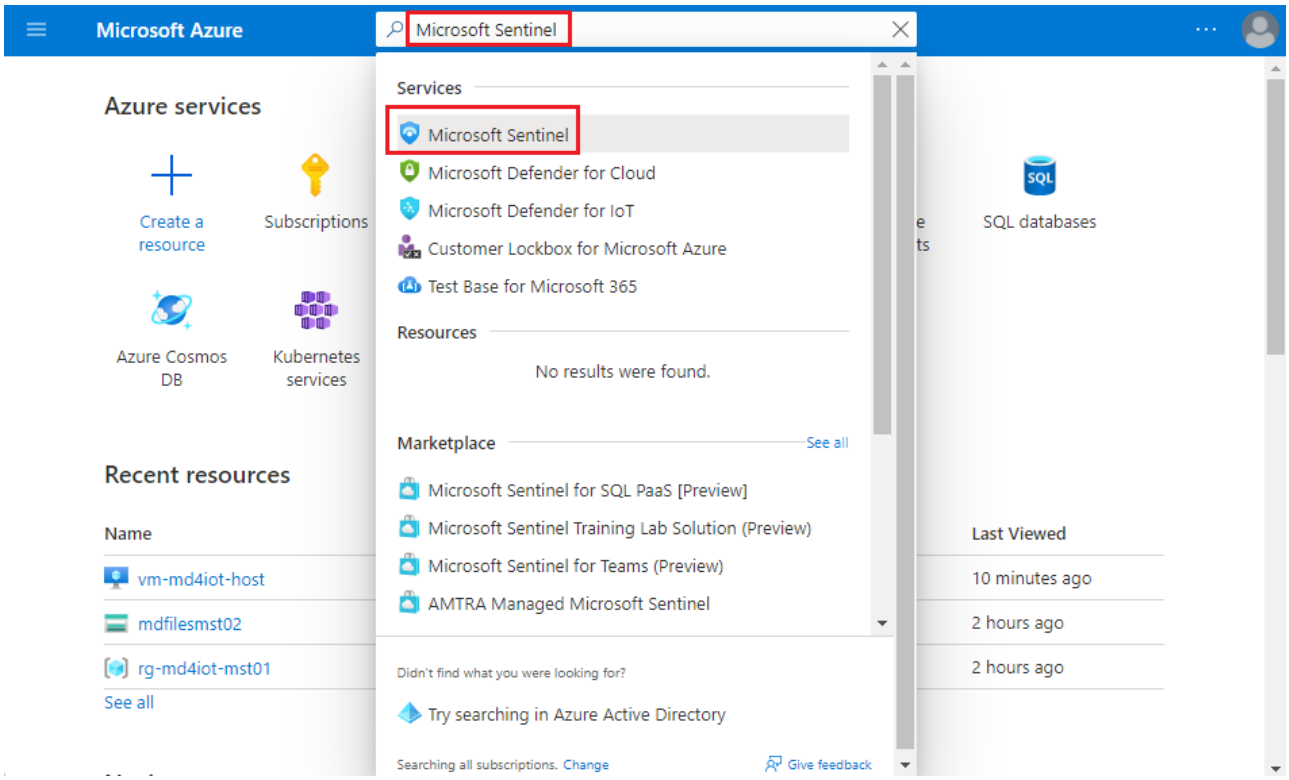
7. On your physical machine, go to the Azure Portal, select your Virtual Machine and click **Stop**. Now you are all set for your training session.



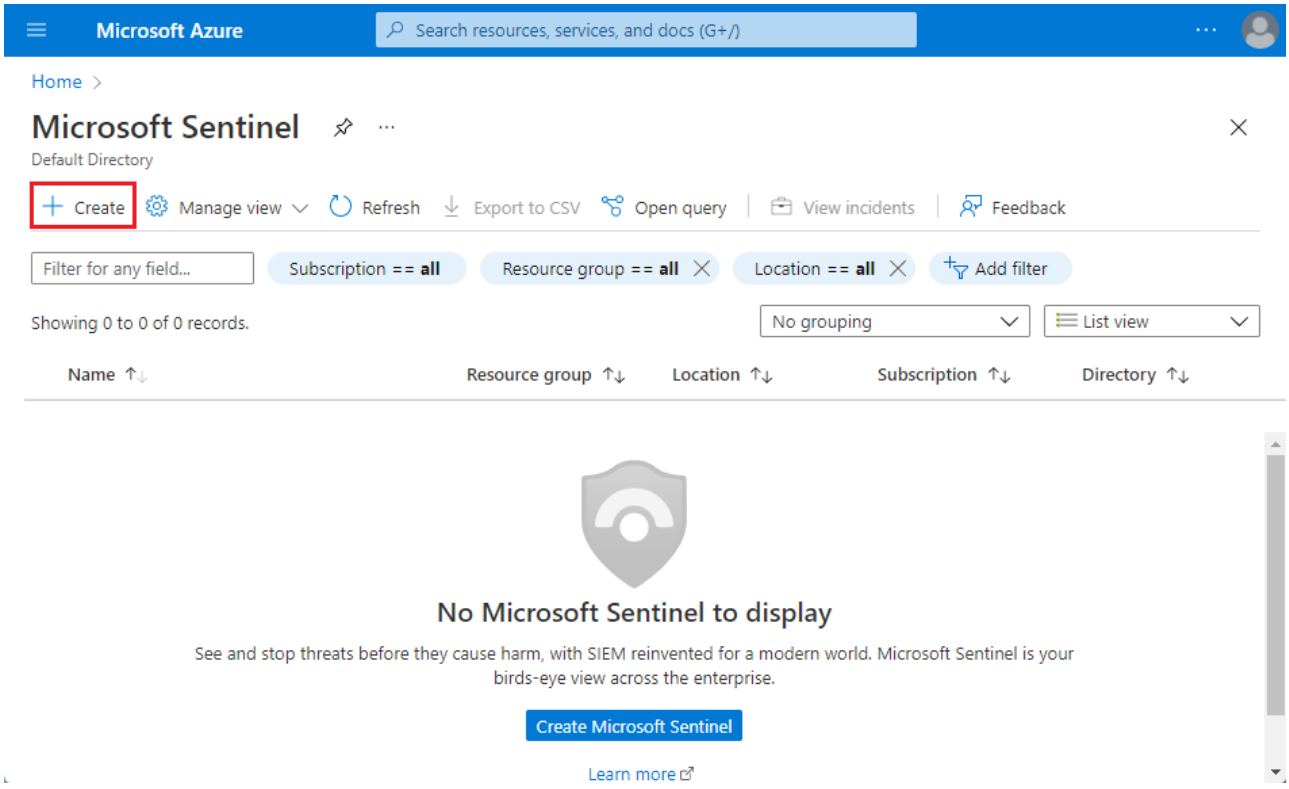
Task 6: Microsoft Sentinel

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.

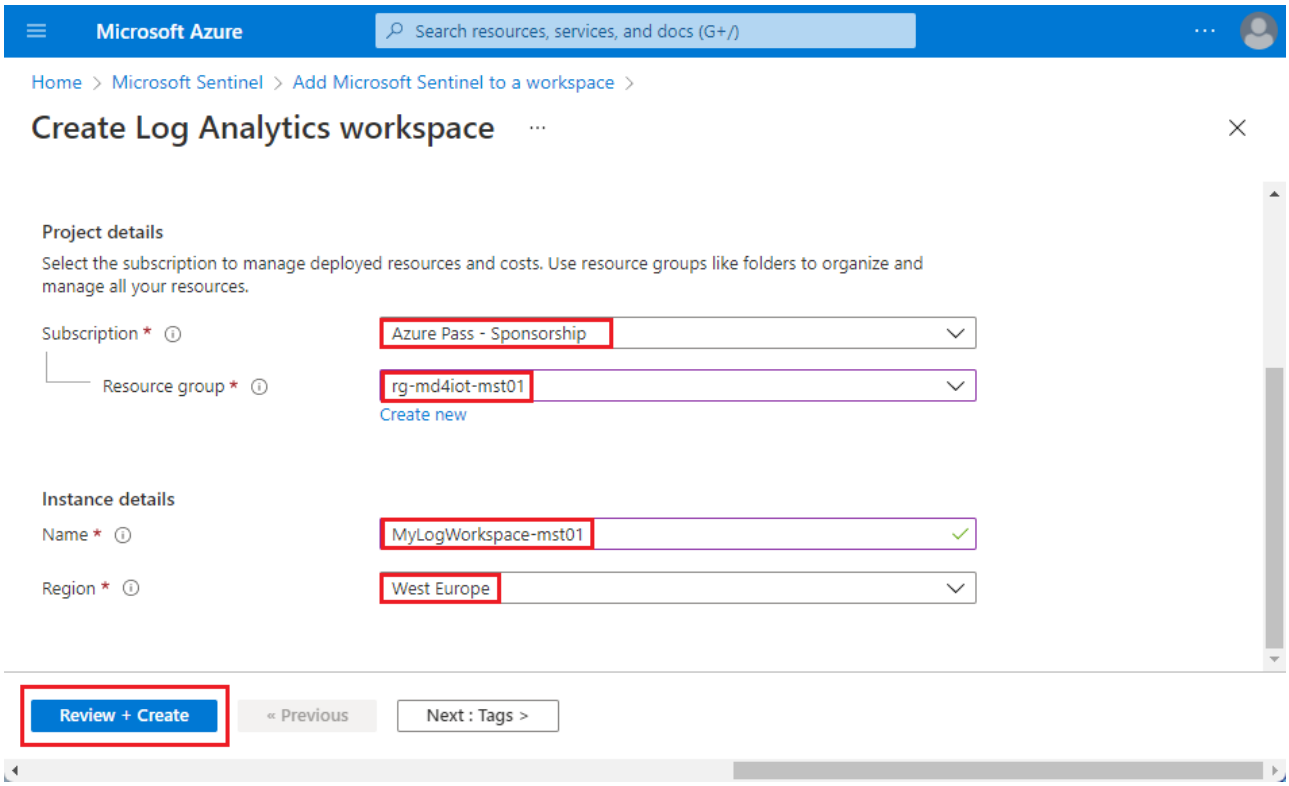


2. Then, click **Create**, a new pop up window appears, select **+ Create a new workspace**



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).



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.