# ONLINE LAB: Encrypting a VM Data Disk

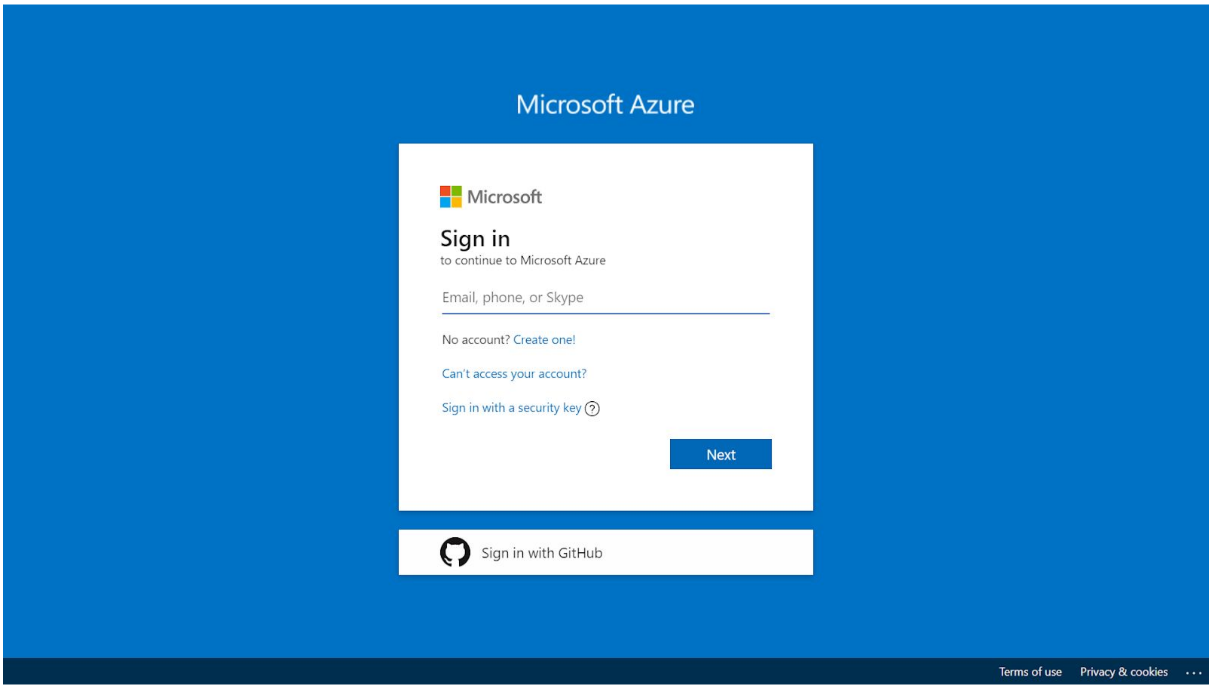
## Your Challenge

- Create a resource group named **vmencryptgrp**
- Create a new virtual machine with **a unique name** in that group
    - Ensure the VM has a data disk attached
- Encrypt the VM data disk using Powershell
- Clean up all of your resources created after you're done

## Solution

### Step 1 Sign Into Azure

Sign into Azure at https://portal.azure.com/



Microsoft Azure

Microsoft

Sign in

to continue to Microsoft Azure

Email, phone, or Skype

No account? Create one!

Can't access your account?

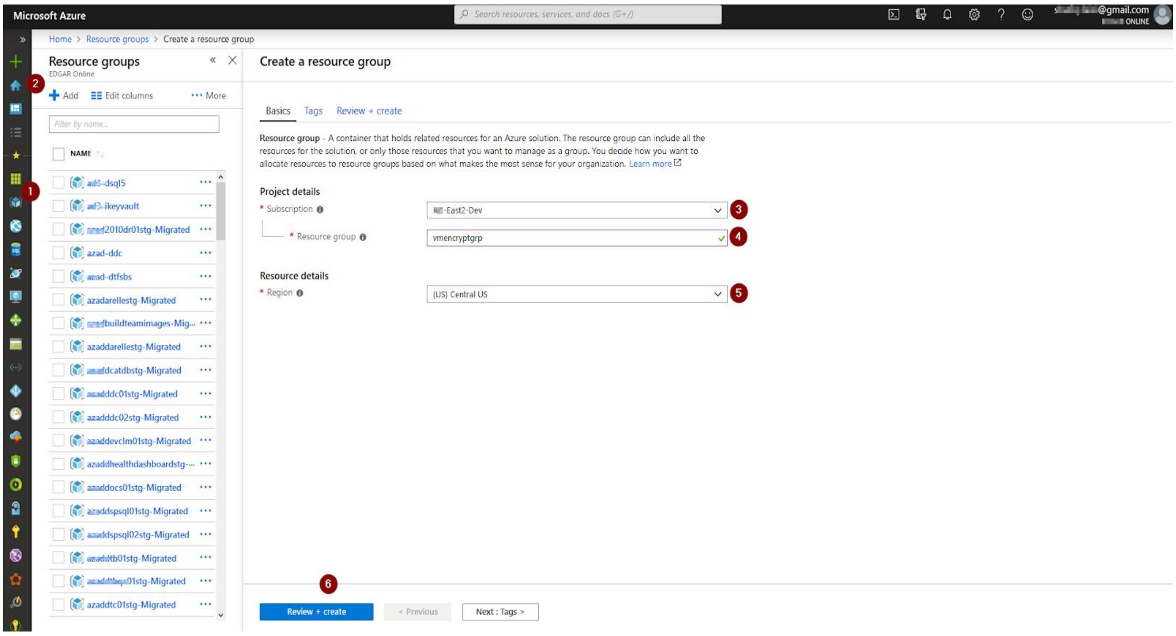
Sign in with a security key

Next

Sign in with GitHub

Terms of use   Privacy & cookies   ...

# Step 2 Create a Resource Group



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: [redacted]-East2-Dev

* Resource group: vmencryptgrp

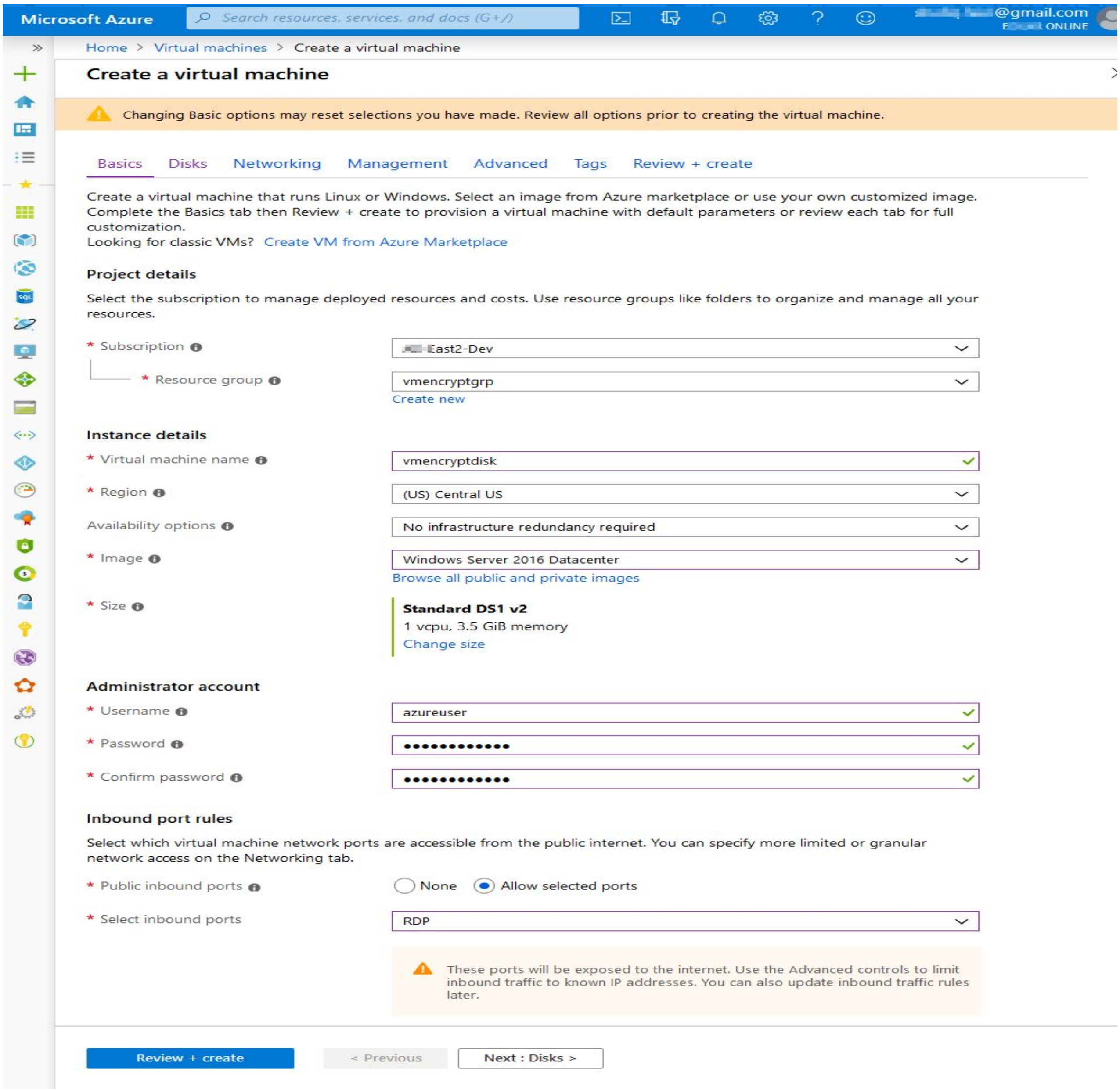
Resource details

* Region: (US) Central US

- [redacted]-dsql5
- [redacted]-ikeyvault
- [redacted]2010dr01stg-Migrated
- azad-ddc
- [redacted]ad-dtfsbs
- azadarellestg-Migrated
- [redacted]buildteamimages-Mig...
- azaddarellestg-Migrated
- [redacted]dcatdbstg-Migrated
- [redacted]ddc01stg-Migrated
- azadddc02stg-Migrated
- [redacted]devclm01stg-Migrated
- azaddhealthdashboardstg-...
- [redacted]docs01stg-Migrated
- [redacted]dspsql01stg-Migrated
- [redacted]dspsql02stg-Migrated
- [redacted]tb01stg-Migrated
- [redacted]01stg-Migrated
- azaddtc01stg-Migrated

1. In the navigation list, click **Resource groups**.
2. Click **Add** to open the **Resource group** blade.
3. For **Resource group** name, enter **vmencryptgrp**.
4. Select a subscription and a location.
5. Click **Review + Create** to proceed to the last step.
6. Click **Create** to create the resource group and follow notification on top right.
7. Click **Refresh** to refresh the list of resource groups.

# Step 3 Create a VM with Data Disk



Microsoft Azure
Search resources, services, and docs (G+/)
[redacted]@gmail.com
[redacted] ONLINE
Home > Virtual machines > Create a virtual machine

Create a virtual machine

⚠ Changing Basic options may reset selections you have made. Review all options prior to creating the 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.

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: [redacted]East2-Dev

* Resource group: vmencryptgrp

Create new

**Instance details**

* Virtual machine name: vmencryptdisk ✓

* Region: (US) Central US

Availability options: No infrastructure redundancy required

* Image: Windows Server 2016 Datacenter

Browse all public and private images

* Size: **Standard DS1 v2**
1 vcpu, 3.5 GiB memory
Change size

**Administrator account**

* Username: azureuser ✓

* Password: ●●●●●●●●●●●● ✓

* Confirm password: ●●●●●●●●●●●● ✓

**Inbound port rules**

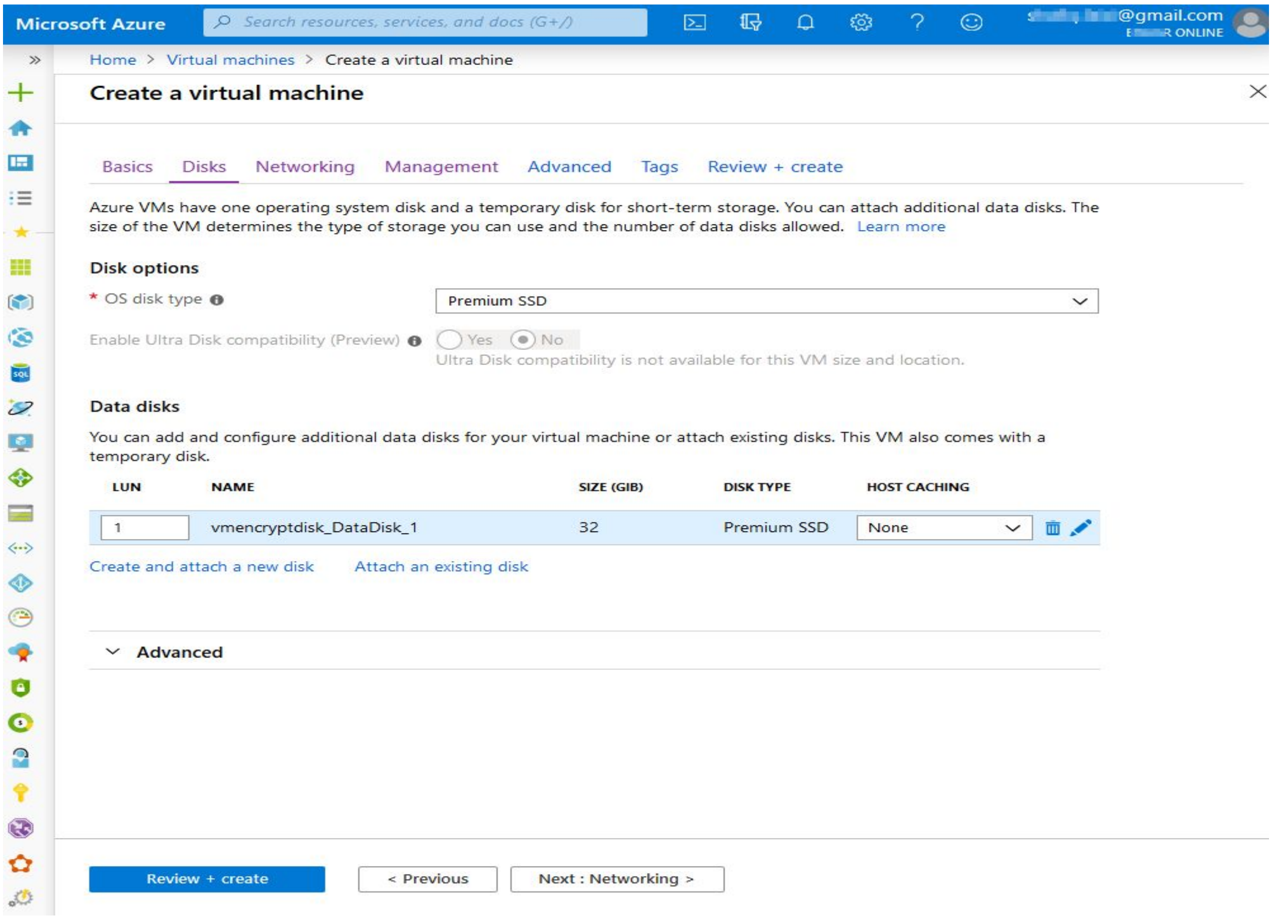
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports: ○ None ● Allow selected ports

* Select inbound ports: RDP

⚠ These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

1. Click on the list again, and click on **Virtual Machines.**
2. Click on **Add** to open **Virtual Machine** blade.
3. Choose your **Subscription** and also the **Resource Group** we created earlier named **vmencryptgrp**.
4. Provide a desired name in **Virtual machine name.** Here we name it **vmencryptdisk**
5. Choose your desired **Region,** leave **Availability Option** as is.
6. Choose your desired **Image** from the list
7. Choose VM **size** by clicking **Change Size** if other than default.
8. Enter **Username** and **Password** for VM login
9. For **Inbound port rules,** click on **allow selected port** and choose **RDP(3389)**
10. Leave the rest as default and click on **Next:Disks >**


Microsoft Azure
Search resources, services, and docs (G+/)
[redacted]@gmail.com
[redacted] ONLINE
Home > Virtual machines > Create a virtual machine

Create a virtual machine

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: Premium SSD

Enable Ultra Disk compatibility (Preview): ○ Yes ● No

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

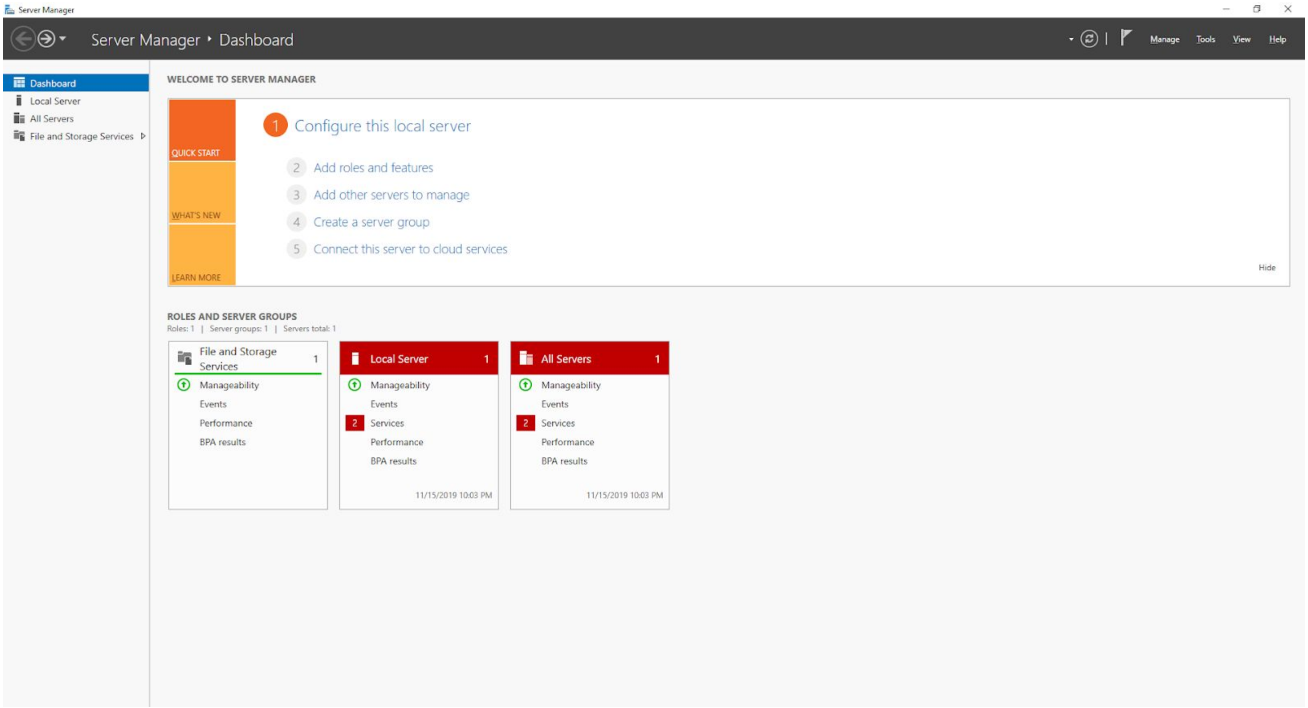
Data disks

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 |
|---|---|---|---|---|
| 1 | vmencryptdisk_DataDisk_1 | 32 | Premium SSD | None |

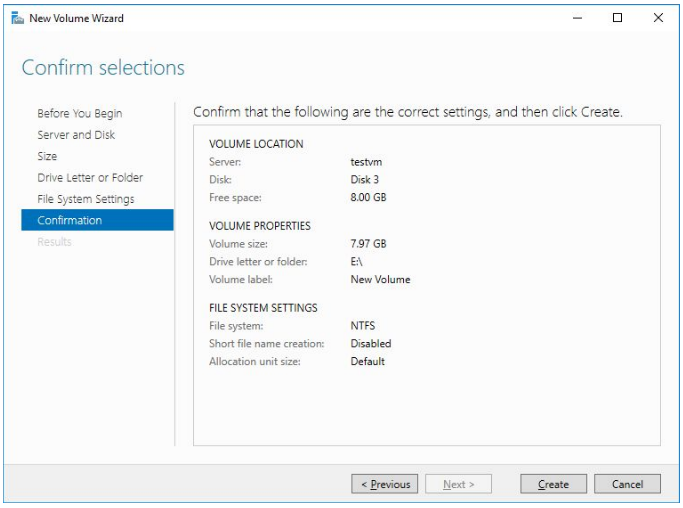
11. Choose OS disk type of your choice from drop down. Here we choose **Premium SSD**
12. In **Data disks** section, click on *Create and attach a new disk* and and provide *Name* and select *None (empty disk)* from drop down
13. Select disk **Size** by clicking on *Change size* - Here we choose 32 GB
14. Click *Next* and leave all the rest as default until *Review + create*
15. Click on **Create** and the deployment will initialize - wait until the VM is created
16. Navigate to **vmencryptgrp** and hit *Refresh* - The VM will show up once deployment succeeds.

# Step 4 - Initialize the Disk



In order to encrypt the data disk, you first must initialize the disk inside the VM.

1. Use RDP to connect to the virtual machine
2. On the server manager dashboard, which starts when you log in, select “File and Storage Services”
3. On the left, select “Disks”
4. There should be one disk that is “Unknown” partition and “Msft Virtual Disk” as its Name.
5. Right click on it, and select “New Volume”
6. Proceed through the Wizard by selecting Next, Next, OK, Next, Next, and then Create.
7. Close the Server Manager when done.
8. Verify that a data disk “New Volume” has been added as drive letter E:\



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

VOLUME LOCATION
Server: testvm
Disk: Disk 3
Free space: 8.00 GB

VOLUME PROPERTIES
Volume size: 7.97 GB
Drive letter or folder: E:\
Volume label: New Volume

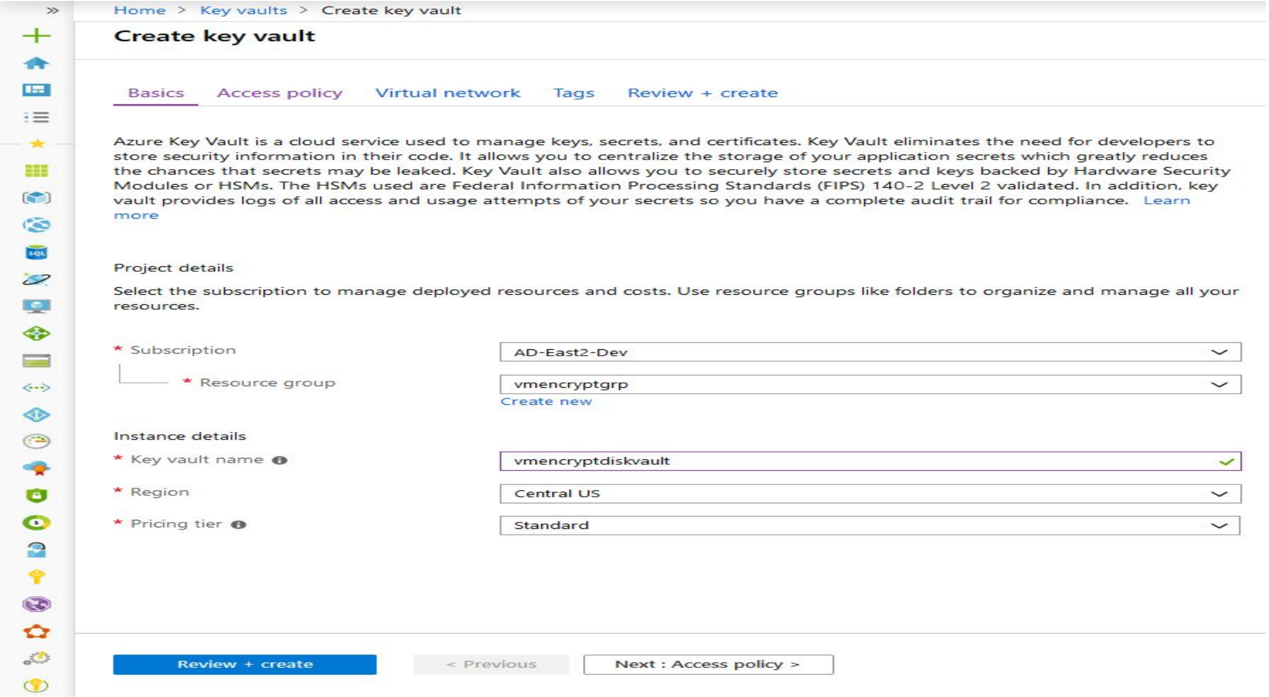
FILE SYSTEM SETTINGS
File system: NTFS
Short file name creation: Disabled
Allocation unit size: Default

# Step 5 - Disk Encryption

Pre-requisites:

- Azure powershell Module ‘Az’ installed
- Create Key vault
- Set key vault advanced access policy

Create Key vault:



Create key vault

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance. 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: AD-East2-Dev

* Resource group: vmencryptgrp

Create new

Instance details

* Key vault name: vmencryptdiskvault

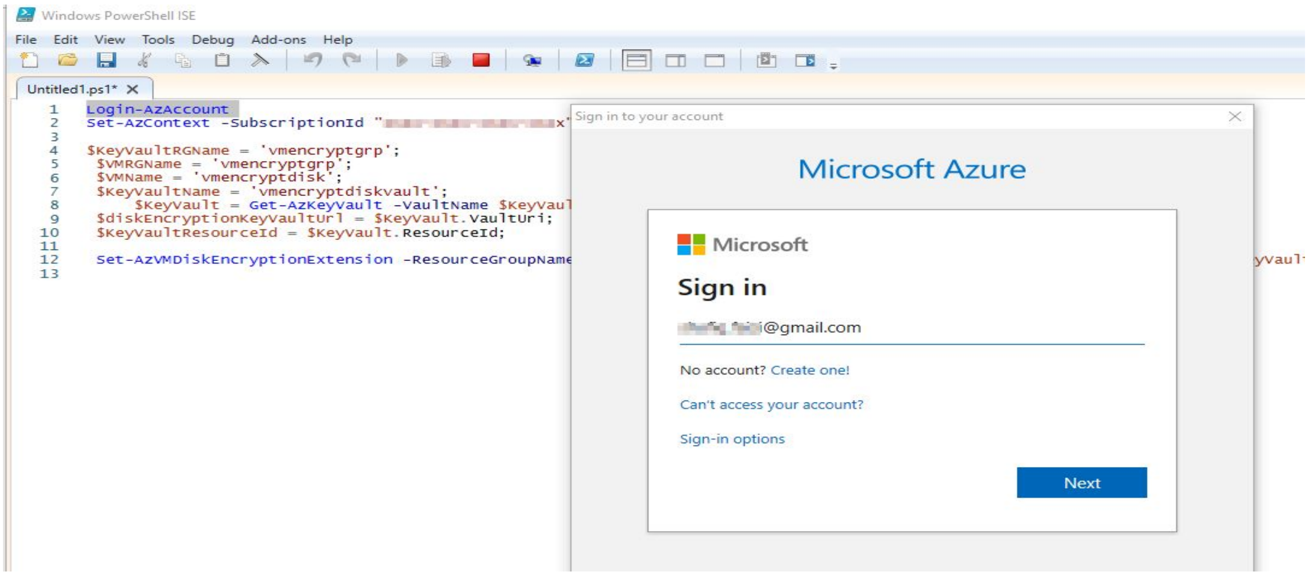
* Region: Central US

* Pricing tier: Standard

1. Click on **Key vault** from the Navigation list on the left
2. Click **Add** and select your subscription and Resource Group we created
3. Provide a unique name for key vault, select region and pricing tier
4. Click on the *Next: Access policy* and from the options check ‘*Azure Disk Encryption for volume encryption’*
5. Click on *Next* and leave everything else as default and hit **Create**.
6. Check **vmencryptgrp** once the Key vault is created

Encrypt VM Data disk

- In order to encrypt the data disk, we need to first login to the azure portal through the following commands and select our subscription, and provide values to the following parameters
- *Note that the command “Login-AzAccount” should be “Connect-AzAccount” and has been corrected below. Login-AzAccount was an alias to Connect-AzAccount and is no longer supported in recent PowerShell released*.



```
Login-AzAccount
Set-AzContext -SubscriptionId "[redacted]x"

$KeyVaultRGName = 'vmencryptgrp';
 $VMRGName = 'vmencryptgrp';
 $VMName = 'vmencryptdisk';
 $KeyVaultName = 'vmencryptdiskvault';
     $KeyVault = Get-AzKeyVault -VaultName $KeyVaul
 $diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
 $KeyVaultResourceId = $KeyVault.ResourceId;

 Set-AzVMDiskEncryptionExtension -ResourceGroupName                yVaul
```

Sign in

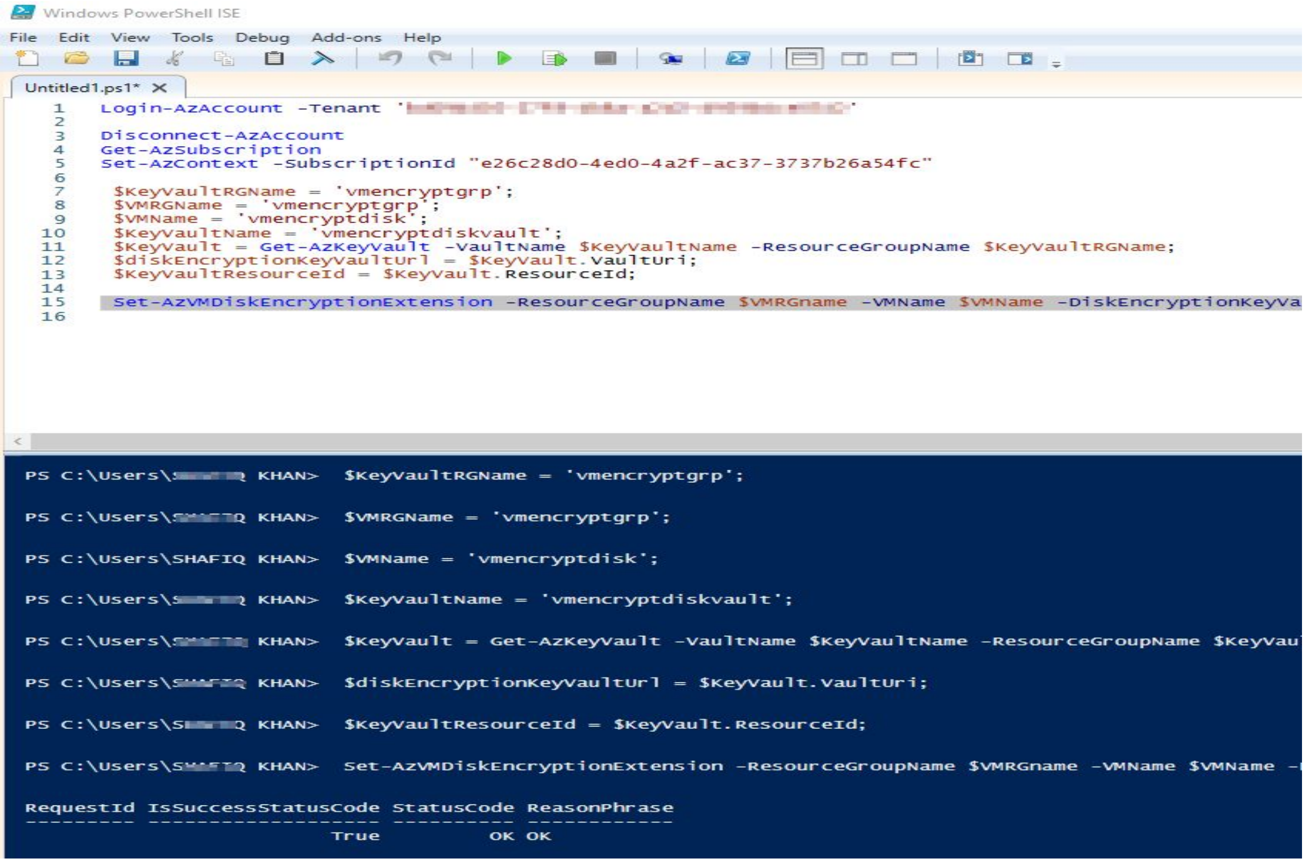
[redacted]@gmail.com

```
## If you do not use Cloud Shell, you need to log in
Connect-AzAccount
Set-AzContext -SubscriptionId "xxxx-xxxx-xxxx-xxxx"

## If you use Cloud Shell, you can start here
$KeyVaultRGName = 'vmencryptgrp';
$VMRGName = 'vmencryptgrp';
$VMName = 'vmencryptdisk';
$KeyVaultName = 'vmencryptdiskvault';
$KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KeyVaultRGName;
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
$KeyVaultResourceId = $KeyVault.ResourceId;

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $VMName
-DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyVaultId $KeyVaultResourceId;
```

Once you run all the scripts one by one, The last step which is *Set-AzVMDiskEncryptionExtension* will start the encryption process on the VM. It will take around 5-10 minutes and during this time the VM will be rebooted. Once this process is completed, you will get status code of ‘ok’ in powershell as shown below:



```
Login-AzAccount -Tenant '[redacted]'

Disconnect-AzAccount
Get-AzSubscription
Set-AzContext -SubscriptionId "e26c28d0-4ed0-4a2f-ac37-3737b26a54fc"

 $KeyVaultRGName = 'vmencryptgrp';
 $VMRGName = 'vmencryptgrp';
 $VMName = 'vmencryptdisk';
 $KeyVaultName = 'vmencryptdiskvault';
 $KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KeyVaultRGName;
 $diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
 $KeyVaultResourceId = $KeyVault.ResourceId;

 Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $VMName -DiskEncryptionKeyVa
```

```
PS C:\Users\[redacted] KHAN>  $KeyVaultRGName = 'vmencryptgrp';

PS C:\Users\[redacted] KHAN>  $VMRGName = 'vmencryptgrp';

PS C:\Users\SHAFIQ KHAN>  $VMName = 'vmencryptdisk';

PS C:\Users\[redacted] KHAN>  $KeyVaultName = 'vmencryptdiskvault';

PS C:\Users\[redacted] KHAN>  $KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KeyVau

PS C:\Users\[redacted] KHAN>  $diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;

PS C:\Users\[redacted] KHAN>  $KeyVaultResourceId = $KeyVault.ResourceId;

PS C:\Users\[redacted] KHAN>  Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $VMName -

RequestId IsSuccessStatusCode StatusCode ReasonPhrase
--------- ------------------- ---------- ------------
                         True         OK OK
```

In order to confirm the encryption, run the following command :

*Get-AzVmDiskEncryptionStatus  -ResourceGroupName $VMRGName  -VMName $VMName*

Take a screenshot of the result of this.

# Step 6 Clean up

1. In the navigation list, click **Resource groups**.
2. Click **vmencryptgrp** to open the resource group.
3. Click **Delete resource group** to delete the resource group.
4. On the **Are you sure you want to delete** blade, type the resource group name: **vmencryptgrp**.
5. Click **Delete** to delete the resource group.