

Configure Azure Disk Encryption

Understand the scenario

You are an Azure® developer. You need to enable Azure Disk Encryption on an Azure virtual machine. First, you will create a virtual machine. Next, you will add a data disk to the virtual machine. Finally, you will enable Azure Disk Encryption.

Understand your environment

You will be using an Azure resource group named corp-datalod26433909 that initially contains no resources.

# **Create an Azure virtual machine**

* Open **Microsoft Edge**, and then sign in to http://portal.azure.com
* Create an Azure virtual machine by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433909** |
| Virtual machine name | webVM1 |
| Image | **Windows Server 2019 Datacenter - Gen2** |
| Size | **Standard\_B2ms** |
| Username | AzureAdmin |
| Password | Az!26433909! |
| Public inbound ports | **Allow selected ports** |
| Select inbound ports | **RDP (3389)** |
| OS disk type | **Standard HDD** |
| Boot diagnostics | **Disable** |

* Expand this hint for guidance on creating an Azure virtual machine.
  + On the Azure portal home page, select **Create a resource** to display the Azure Marketplace.
  + In Categories, select **Compute**, and then select **Virtual machine**.
  + On the Create a virtual machine blade, on the Basics page, in Resource group, select **corp-datalod26433909**.
  + In Virtual machine name, enter webVM1, and then in Image, select **Windows Server 2019 Datacenter - Gen2**.
  + In Size, select **See all sizes**.
  + On the Select a VM size page, in VM Size, select B2ms, and then select **Select**.
  + On the Basics page, in Username, enter AzureAdmin, and then in Password and Confirm password, enter Az!26433909!.
  + In Public inbound ports, ensure that **Allow selected ports** is selected, and then in Select inbound ports, ensure that **RDP (3389)** is selected.
  + On the Disks page, in OS disk type, select **Standard HDD**.
  + On the Management page, in Boot diagnostics, select **Disable**.
  + Select **Review + create**, review the virtual machine specifications, and then select **Create** to deploy the virtual machine.

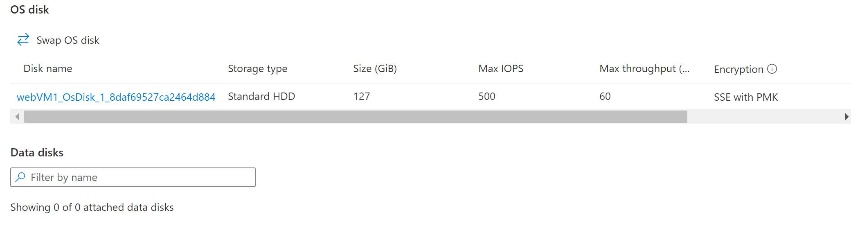
Ignore any warnings about RDP ports as this virtual machine is being used for testing only.

The deployment will take approximately 3–5 minutes. Wait for the deployment to complete before moving on to the next step.

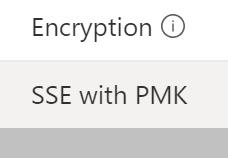
* Verify that **webVM1** contains one OS disk that uses **SSE with PMK** encryption, and that there are no data disks.

Expand this hint for guidance on verifying the current disk specifications in the Azure portal.

* + On the Azure portal home page, select **Virtual machines**, and then select **webVM1**.
  + On the webVM1 resource menu, in Settings, select **Disks**.
  + On the Disks page, in OS disk, verify that there is one disk, and then in the Encryption column, verify that the value is set to **SSE with PMK**.
  + In Data disk, verify that there are no data disks.



You may need to scroll to the right to see the encryption setting.



[Server-side encryption](https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption) (SSE) of Azure Disk Storage is enabled by default and encrypts disks at the storage server level by using a platform-managed key (PMK). The encryption key is managed automatically by the platform, in this case Azure, including protection and regular rotation. You can use server-side encryption with a customer-managed key (SSE with CMK) to manage the encryption key manually for compliance reasons. You can combine SSE with Azure Disk Encryption (ADE), which additionally encrypts the disk at the OS level by using technologies such as BitLocker (Windows) or DM-Crypt (Linux), for what is called double encryption at rest high security requirements.

## Check your work

* Confirm that you created an Azure virtual machine named webVM1.
* Confirm that you verified the current disk specifications.

# **Add a new data disk to the Azure virtual machine**

* Create a new disk named DataFiles that is attached to **webVM1**, and then configure the disk by using the **Standard HDD** OS disk type and a size of 128 GiB.

Expand this hint for guidance on creating and attaching a new data disk.

* + On the webVM1 Disks page, in Data disks, select **Create and attach a new disk**.



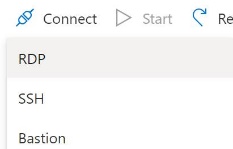
* + In Disk name, enter DataFiles, in Storage type, select **Standard HDD**, in Size (GiB), enter 128, and then on the command bar, select **Save**.

The update will take approximately 1–2 minutes. Wait for the update to complete before moving on to the next step.

* Connect to **webVM1** by using **RDP**, and then when prompted, sign in as AzureAdmin using Az!26433909! as the password.

Expand this hint for guidance on connecting to a virtual machine by using RDP.

* + On the webVM1 Overview page, on the command bar, select **Connect**, and then select **RDP**.



* + On the Connect page, select **Download RDP File**.
  + Open the RDP file, and then in the Remote Desktop Connection window, select **Connect**.
  + When prompted for credentials, select **More choices**, and then select **Use a different account**.
  + In User name, enter AzureAdmin, in Password, enter Az!26433909!, and then select **OK**.
  + In the Remote Desktop Connection warning message box, select **Yes**, and then wait for the RDP session to initialize.
  + In the RDP session, if prompted to allow your PC to be discoverable by other PCs and devices on this network, select **No**.



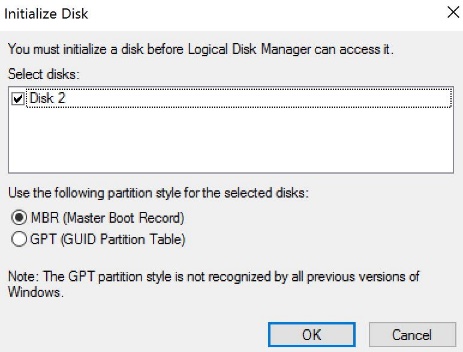
* + Wait for Server Manager to load, and then minimize **Server Manager**.

Resize the RDP session window so that you can view the instructions for the challenge at the same time.

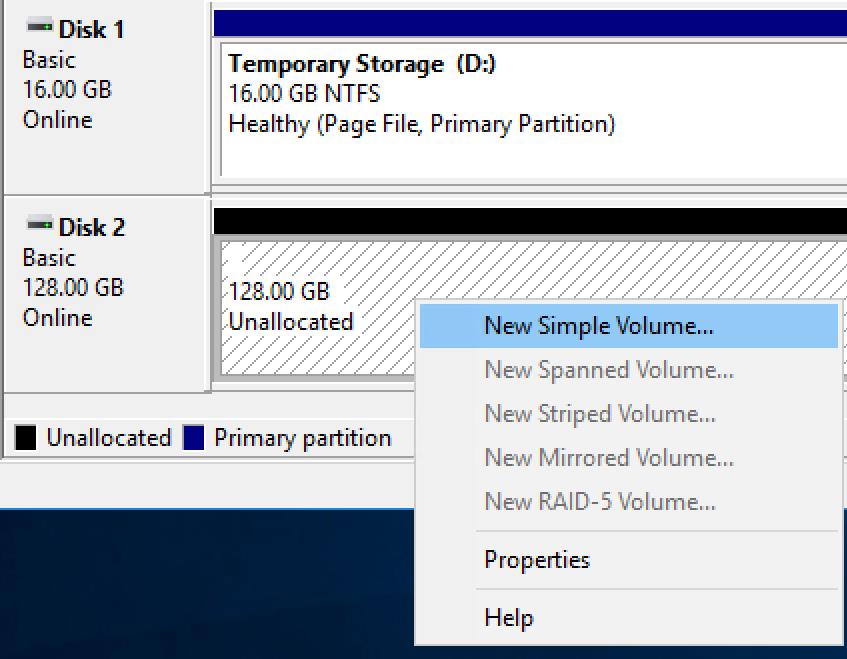
* Initialize the new disk as a simple volume by using the drive letter **F**, the **NTFS** file system, and a volume label of DataFiles.

Expand this hint for guidance on initializing and formatting a new data disk.

* + In the Remote Desktop Connection window, right-click **Start**, and then select **Disk Management**.
  + In the Initialize Disk dialog box, review the default values, and then select **OK** to initialize the new disk.

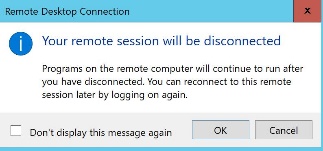


* + In Disk Management, right-click the new, unallocated disk, and then select **New Simple Volume**.



* + In the New Simple Volume Wizard, select **Next** twice to advance to the Assign Drive Letter or Path page.
  + In Assign the following drive letter, ensure that **F** is selected, and then select **Next**.
  + In File System, ensure that **NTFS** is selected, and then in Volume label, enter DataFiles,
  + Select **Next**, and then select **Finish** to format the new disk.
  + Close the **Disk Management** window.
* Close the **Remote Desktop Connection** window

If prompted by a Your remote session will be disconnected message, select **OK**.



## Check your work

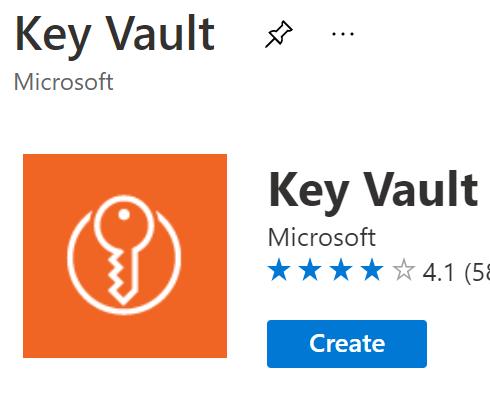
* Confirm that you added a new data disk named DataFiles to the virtual machine.
* Confirm that you connected to webVM1 by using RDP.
* Confirm that you created a new simple volume named DataFiles that uses NTFS and the drive letter F.

# **Enable Azure Disk Encryption**

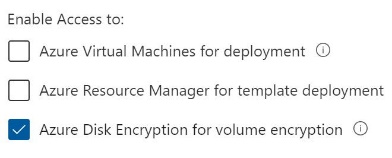
* Create an Azure key vault by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433909** |
| Key vault name | KV26433909 |
| Pricing tier | **Standard** |
| Azure Disk Encryption for volume encryption | **Selected** |

* Expand this hint for guidance on creating a key vault.
  + On the Azure portal menu, select **Create a resource** to display the Azure Marketplace.
  + In Search services and marketplace, search for and select Key Vault, and then select **Create**.



* + On the Create key vault blade, in Resource group, select **corp-datalod26433909**, in Key vault name, enter KV26433909, in Pricing tier, ensure that **Standard** is selected, and then select **Next : Access policy**.
  + On the Access policy page, select the **Azure Disk Encryption for volume encryption** check box.



* + Select **Review + create**, review the specifications for the key vault, and then select **Create**.

The deployment will take approximately 1–2 minutes.

* Launch an Azure **Cloud Shell** **PowerShell** session by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433909** |
| Storage account | cs26433909 |
| File share | cloudshell |

* Expand this hint for guidance on launching Azure Cloud Shell.
  + On the Azure portal page header, in the global controls section, select the **Cloud Shell** icon.



* + On the Welcome to Azure Cloud Shell page, select **PowerShell**.



* + On the You have no storage mounted page, select **Show advanced settings**.

The Show advanced settings option

* + In Resource group, ensure that **Use existing** is selected, and then ensure that **corp-datalod26433909** is selected.
  + In Storage account, ensure that **Create new** is selected, and then enter cs26433909.
  + In File share, ensure that **Create new** is selected, and then enter cloudshell.
  + Select **Create storage**, and then wait for the Cloud Shell session to initialize.
* Retrieve the properties of the KV26433909 key vault in the corp-datalod26433909 resource group by using the [Get-AzKeyVault](https://docs.microsoft.com/en-us/powershell/module/az.keyvault/get-azkeyvault) cmdlet, and then store the results in a local variable named $KeyVault.

Expand this hint for guidance on retrieving the properties of a key vault.

* + In Azure Cloud Shell, run the following command to retrieve the properties of the key vault:

$KeyVault = Get-AzKeyVault -VaultName KV26433909 -ResourceGroupName corp-datalod26433909

Cloud Shell does not support the keyboard shortcut Ctrl+V for paste. Instead, select the command prompt, and then use **Ctrl+Shift+V** to paste.

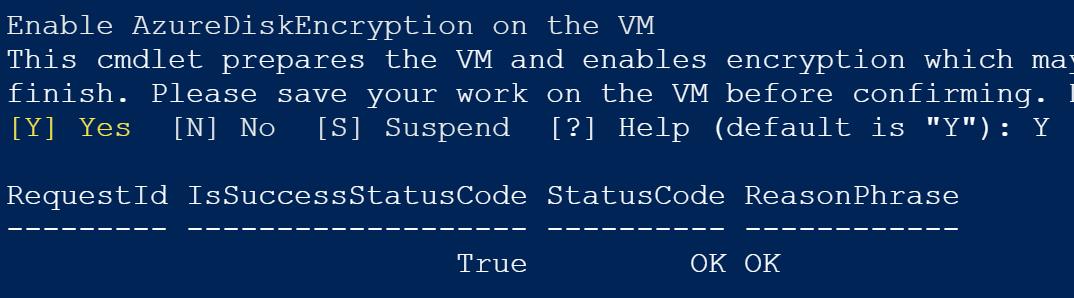
* Enable Azure Disk Encryption for webVM1 by using the [Set-AzVMDiskEncryptionExtension](https://docs.microsoft.com/en-us/powershell/module/az.compute/set-azvmdiskencryptionextension) cmdlet and the corp-datalod26433909 resource group.

Expand this hint for guidance on enabling Azure Disk Encryption.

* + Run the following command to retrieve the properties of the key vault:

Set-AzVMDiskEncryptionExtension -ResourceGroupName corp-datalod26433909 -VMName webVM1 -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -DiskEncryptionKeyVaultId $KeyVault.ResourceId

* + If prompted to continue, enter Y.



The command will take approximately 2–3 minutes to complete.

* Verify that the encryption for webVM1 succeeded by using the [Get-AzVmDiskEncryptionStatus](https://docs.microsoft.com/en-us/powershell/module/az.compute/get-azvmdiskencryptionstatus) cmdlet and the corp-datalod26433909 resource group.

Expand this hint for guidance on verifying that the encryption succeeded.

* + Run the following command to verify that the encryption succeeded:

Get-AzVmDiskEncryptionStatus -VMName webVM1 -ResourceGroupName corp-datalod26433909

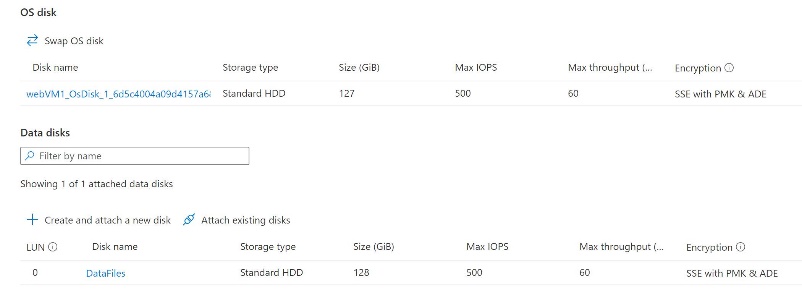
The encryption for both the OS and data disks should be verified.



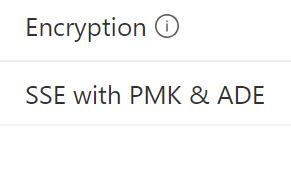
* Close the **Cloud Shell** window.
* In the Azure portal, verify that the updated disk specifications use Azure Disk Encryption.

Expand this hint for guidance on verifying the updated disk specifications in the Azure portal.

* + On the Azure portal home page, select **Virtual machines**, and then select **webVM1**.
  + On the webVM1 resource menu, in Settings, select **Disks**.
  + On the Disks page, verify that there is now an OS disk and a data disk that both use **SSE with PMK & ADE** encryption.



The updated disk specifications should show there is now an OS disk and a data disk that both use **SSE with PMK & ADE**.



## Check your work

* Confirm that you created a key vault by using the Azure portal.
* Confirm that you enabled Azure Disk Encryption.
* Confirm that you verified Azure Disk Encryption.

# **Summary**

Congratulations, you have completed the **Configure Azure Disk Encryption** challenge.

You have accomplished the following:

* Created an Azure virtual machine.
* Added a new data disk to the Azure virtual machine.
* Enabled Azure Disk Encryption.