

# Encryption at Rest (How-To for AWS and Azure services)

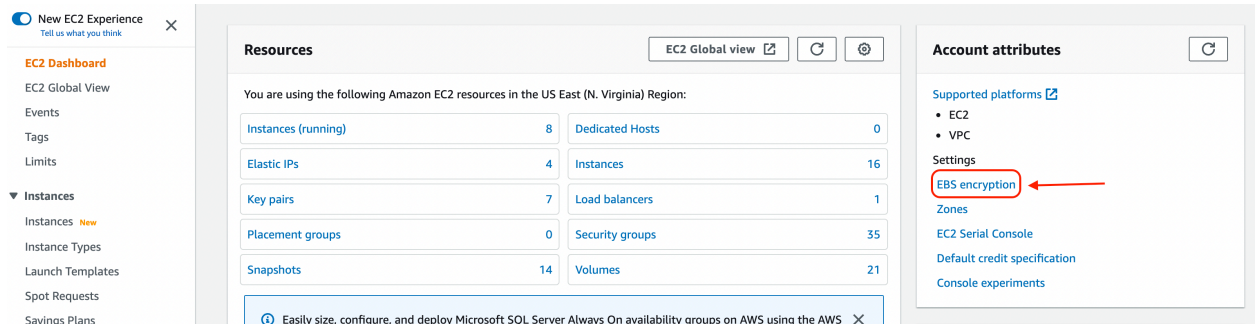
AWS:

1. EC2 EBS volumes (Windows and Linux):

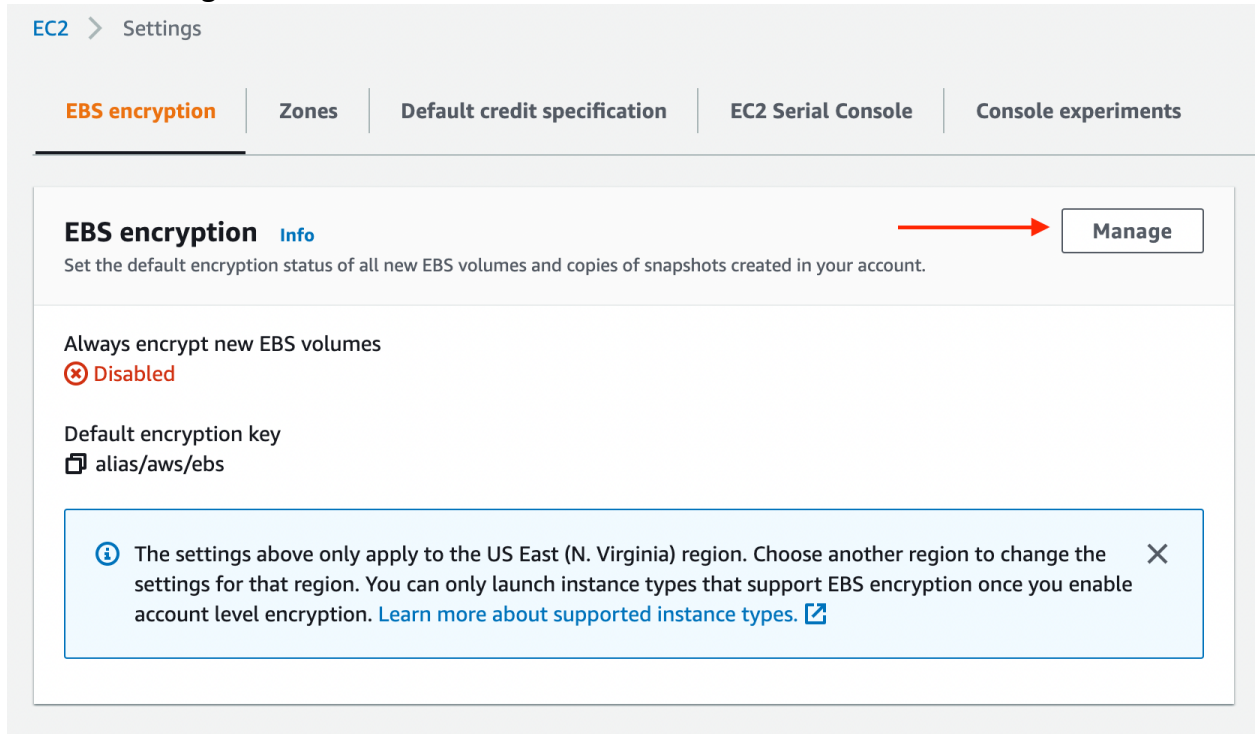
You can enable encryption by default or enable encryption when you create a volume.

Option 1: Enable encryption by default

1) On EC2 Dashboard. Click **EBS Encryption** under **Account attributes** in the upper-right corner.



2) Click the **Manage** button.



3) Select **Enable** and specify the key that you would like to use for encryption. Then Click **Update EBS encryption**.

EC2 > Settings - EBS encryption > Modify EBS encryption

### EBS encryption [Info](#)

Set the default encryption status of all new EBS volumes and copies of snapshots created in your account.

**Always encrypt new EBS volumes**  
Enables encryption by default for newly created EBS volumes and snapshots.

Enable

**Default encryption key**  
Specify the master key to encrypt your volumes.

ⓘ The settings above only apply to the US East (N. Virginia) region. Choose another region to change the settings for that region. You can only launch instance types that support EBS encryption once you enable account level encryption. [Learn more about supported instance types.](#) [↗](#) ✕

**Note:** Only the new EBS volumes and snapshots that you create after the default encryption is enable will be encrypted by default.

## Option 2: Enable encryption when creating a volume

During the EC2 instance creation, on Step 4 Add Storage, click the dropdown arrow under **Encryption** to select the KMS key that you would like to encryption the volume.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-046c8ef36dde8e523	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Filter by attributes

KMS Key Aliases	KMS Key ID
Not Encrypted (default) aws/ebs	

## 2. Container/serverless on AWS

### ECR:


When creating a new repository, under the **Encryption settings**, check **“Enable”**. You can optionally click the **“Customize encryption settings (advanced)”** to select a key different from the default AWS managed key.

## Encryption settings


### KMS encryption

You can use AWS Key Management Service (KMS) to encrypt images stored in this repository, instead of using the default encryption settings.

Enabled 

 The KMS encryption settings cannot be changed or disabled after the repository is created.

### KMS encryption key settings

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings. [Learn more](#) 

Customize encryption settings (advanced)

Cancel

Create repository

### Fargate:

Make sure it is using version 1.4 and above when creating a Fargate cluster.

EFS volumes (persistent storage) are encrypted by default using AWS managed key (aws/elasticfilesystem).

The ephemeral storage is enabled by default in version 1.4 and above.

### Lambda:

Use [environment variables](#) to store secrets for use with Lambda functions. Lambda always encrypts environment variables at rest.

### Azure:

1. VM (Windows & Linux)

Disk is encrypted by default.

# Create a virtual machine ...

Basics Disks Networking Management Advanced Tags Review + create

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 (locally-redundant storage) ▼

Encryption type \* (Default) Encryption at-rest with a platform-managed key ▼

Enable Ultra Disk compatibility ⓘ   
Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard\_B2s.

2. Azure Container Registry/Instances  
Encryption is enabled by default.

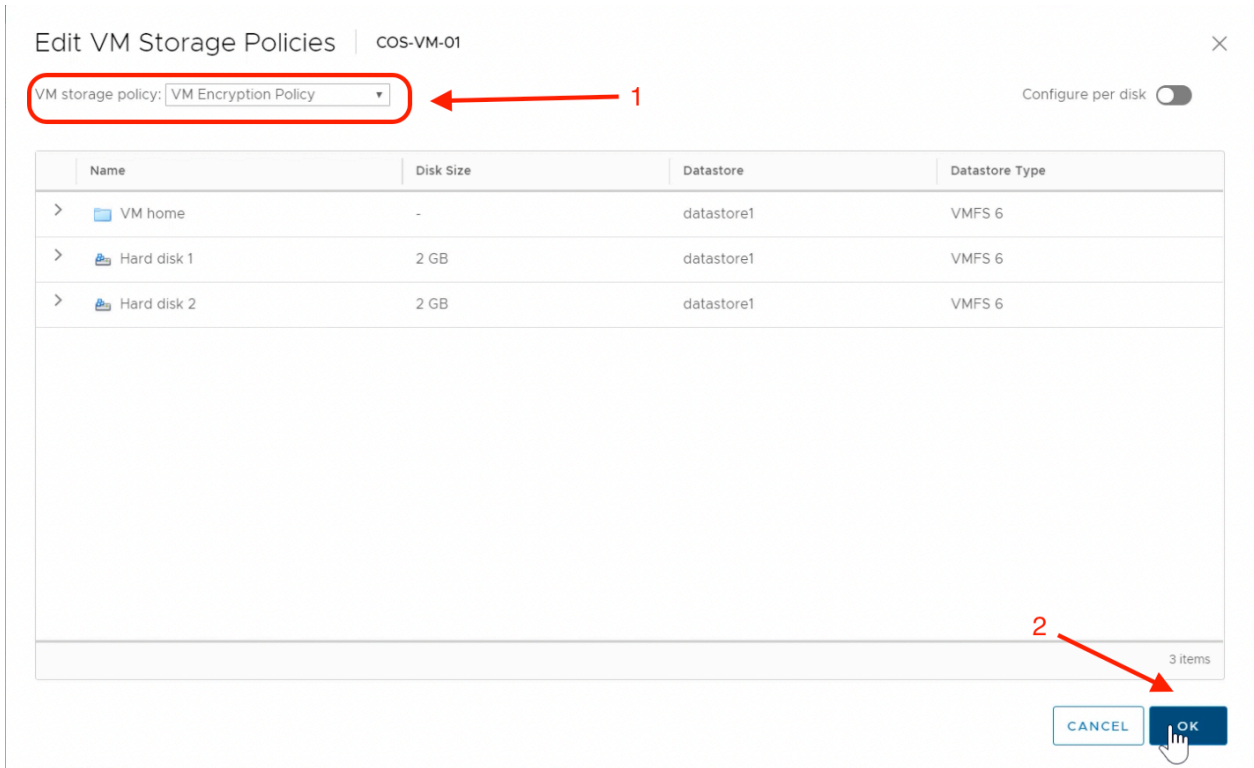
3. Azure Function  
Use Azure Storage Account for storage and SA is encrypted by default.

## VMware:

1. Encrypt existing VM or Virtual Disk

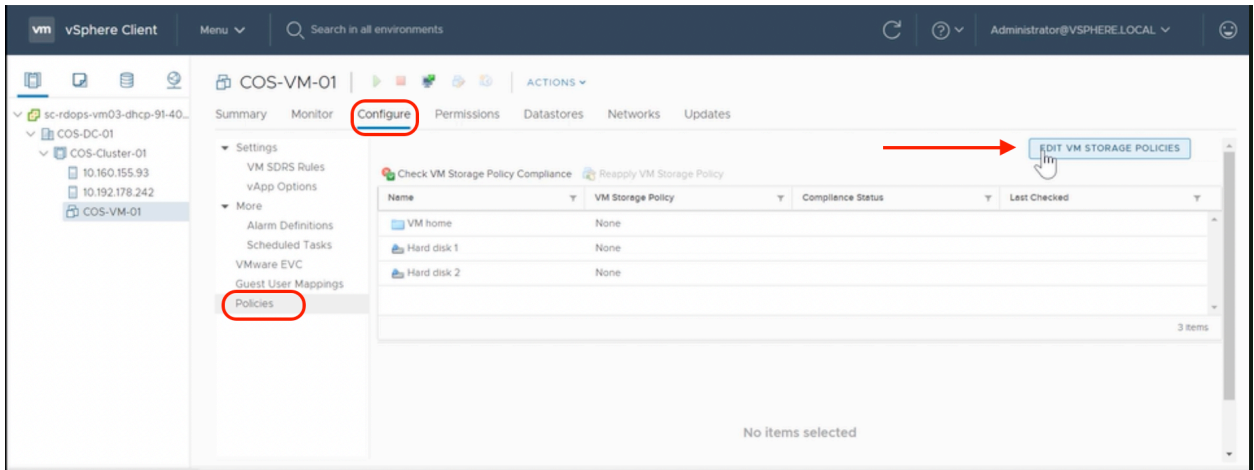
Option 1:

- 1) Connect to vCenter with vSphere Client.
- 2) Power off the virtual machine.
- 3) Right-click the VM and select **VM Policies > Edit VM Storage Policies**.
- 4) Select an encryption storage policy and click **OK**. You can use the default "VM Encryption Policy" or use a custom storage encryption policy.

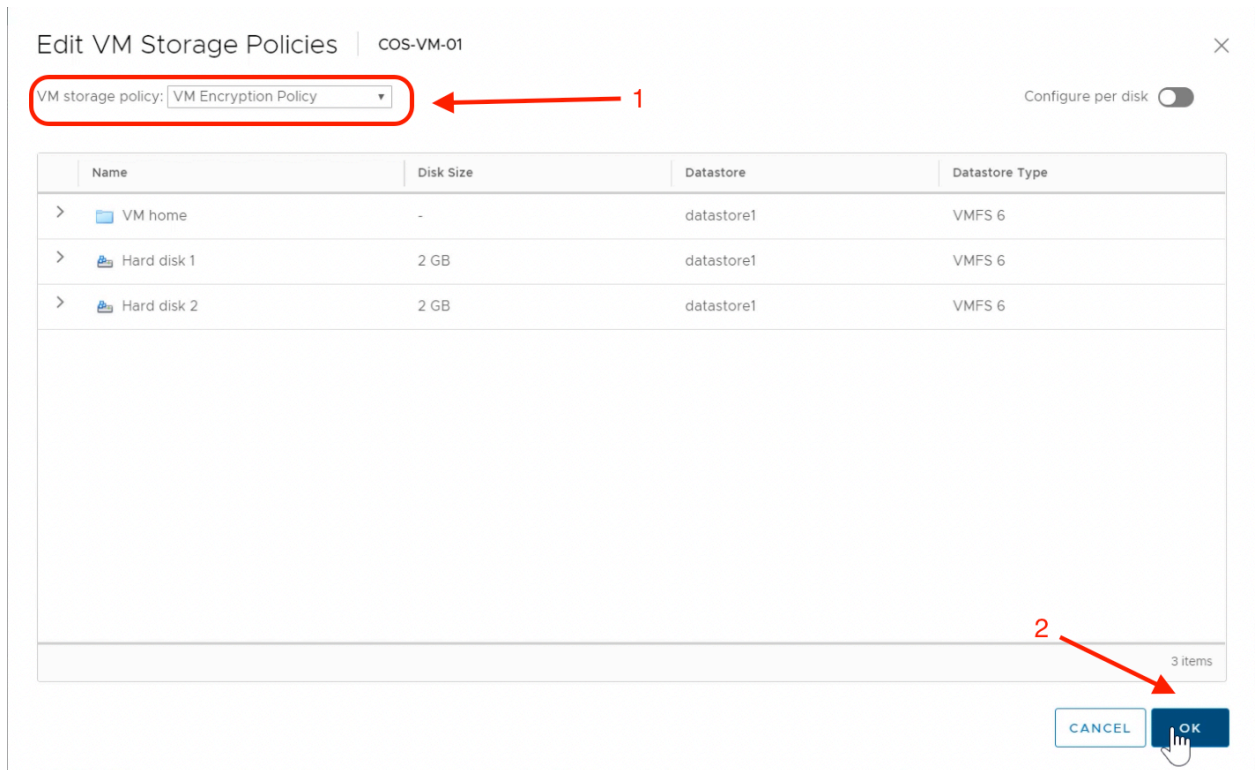


Option 2:

- 1) Connect to vCenter with vSphere Client.
- 2) Power off the virtual machine.
- 3) Select the VM that you want to encrypt on the left panel and navigate to the **Configure** tab on the right panel.
- 4) Select **Policies** and click **EDIT VM STORAGE POLICIES**.



- 5) Select an encryption storage policy and click **OK**. You can use the default “VM Encryption Policy” or use a custom storage encryption policy.



2. Encrypt a VM when it is created

- 1) Launch the New Virtual Machine wizard.
- 2) When selecting storage, check **“Encrypt this virtual machine”** and select the encryption policy. Then click **Next**.

## New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

### Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

VM Storage Policy: VM Encryption Policy ▾

Name	Capacity	Provisioned	Free
Storage Compatibility: Compatible			
datastore1	12.5 GB	5.41 GB	7.09 GB

### Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

3) Continue the wizard to finish the VM creation.