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.

EC2 Dashboard	Resources				
EC2 Global View	You are using the following Amazon E	C2 resources in the US E	ast (N. Virginia) Region:		Supported platforms 🛂
Events	Instances (running)	8	Dedicated Hosts	0	• EC2
Tags					VPC Settings
Linits	Elastic IPs	4	Instances	16	EBS encryption
Instances	Key pairs	7	Load balancers	1	Zones
Instances New	Placement groups	0	Security groups	35	EC2 Serial Console
Launch Templates	Snapshots	14	Volumes	21	Default credit specification
Spot Requests					Console experiments
Savings Plans	Easily size, configure, and depl	oy Microsoft SQL Serve	Always On availability groups on AWS	using the AWS $ imes$	
lick the Mana	ge button.				
EC2 Catting					
EBS encryptio	n Zones Defa	ault credit sp	ecification EC2	Serial Console	e Console experiment
EBS encryption	on Zones Defa	ault credit sp	copies of snapshots crea	Serial Console	e Console experiment Manage nt.
EBS encryption	Zones Defa otion Info ncryption status of all new EBS tnew EBS t new EBS volumes otion key	ault credit sp	copies of snapshots crea	ted in your accour	e Console experiment Manage nt.
EBS encryption	Zones Defa otion Info ncryption status of all new EBS the estimates t new EBS volumes the estimates otion key the estimates	ault credit sp	copies of snapshots crea	ted in your accour	e Console experiment Manage nt.

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

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. alias/aws/ebs The settings above only apply to the US East (N. Virginia) region. Choose another region to change settings for that region. You can only launch instance types that support EBS encryption once you or account level encryption. Learn more about supported instance types.	
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. Q alias/aws/ebs X C The settings above only apply to the US East (N. Virginia) region. Choose another region to change settings for that region. You can only launch instance types that support EBS encryption once you of account level encryption. Learn more about supported instance types.	
Default encryption key Specify the master key to encrypt your volumes. Q alias/aws/ebs X Image: The settings above only apply to the US East (N. Virginia) region. Choose another region to change settings for that region. You can only launch instance types that support EBS encryption once you or account level encryption. Learn more about supported instance types.	
Q alias/aws/ebs X Image: Constraint of the settings above only apply to the US East (N. Virginia) region. Choose another region to change settings for that region. You can only launch instance types that support EBS encryption once you or account level encryption. Learn more about supported instance types.	
 The settings above only apply to the US East (N. Virginia) region. Choose another region to change settings for that region. You can only launch instance types that support EBS encryption once you account level encryption. Learn more about supported instance types. 	🗇 Сору
	ge the 🗙 Su enable

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: Ac Your instance will edit the settings storage options in	dd Storage I be launched with the folk of the root volume. You ca n Amazon EC2.	wing storage device sett n also attach additional E	tings. You can atta BS volumes after	ach additional Ef	3S volumes and instance st stance, but not instance sto	ore volumes to y re volumes. Lear	our instance, o rn more about	r			
Volume Type	i) Device (i)	Snapshot (i)	Siz	ze (GiB) (i)	Volume Type (i)		IOPS (j)	Throughput (MB/s) (i)	Delete on Termination	i Encryption i	
Root	/dev/xvda	snap-046c8ef36d	de8e523 8		General Purpose SSD	gp2) 🗸	100 / 3000	N/A		Not Encrypted	-
Add New Volu	me							Q Filter b	y attributes		
Free tier eligi usage restric	ble customers can get up tions.	to 30 GB of EBS General	Purpose (SSD) o	r Magnetic stora	ge. Learn more about free	usage tier eligibil	ity and	KMS Key Not Encryp (default) av	Aliases KMS Key ID oted vs/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. C Enabled
③ 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 <u>environment variables</u> 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.

Creat	e a vi	rtual mad	chine …				
Basics	Disks	Networking	Management	Advanced	Tags	Review + create	
Azure VN The size Disk opt	As have of of the VM tions	ne operating syste I determines the t	em disk and a tem ype of storage yo	porary disk for s u can use and th	hort-term e number	n storage. You can attach additional data r of data disks allowed. Learn more 🖙	disks.
OS disk t	type * 🕕		Premiun	n SSD (locally-re	dundant s	torage)	\checkmark
Encryptic	on type *		(Default) Encryption at-r	est with a	platform-managed key	\sim
Enable U	lltra Disk o	compatibility ①	Ultra disk Standard	is supported in . B2s.	Availabilit	y Zone(s) 1,2,3 for the selected VM size	

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.

orage policy: VM Encryption Polic		- 1	Configure per disk
Name	Disk Size	Datastore	Datastore Type
🛅 VM home	-	datastore1	VMFS 6
📇 Hard disk 1	2 GB	datastore1	VMFS 6
🏝 Hard disk 2	2 GB	datastore1	VMFS 6
			0
			2

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**.

vm vSphere Client	Menu 🗸 🛛 🔍 Search in i	all environments		C	Administrator@VSPHERE	LOCAL ~
Image: Construction of the state of the	COS-VM-01 Summary Monitor Settings VM SDRS Rules VApp Options More Alarm Definitions Scheduled Tasks VMware EVC Guest User Mappings Policies	Actri Permissions Data Permissions Data Permissions Data Permissions Data Permissions Data Para Para disk 1 Hard disk 1 Hard disk 2	IONS - stores Networks Updates ance Resply VM Storage Policy V VM Storage Policy None None None None	Y Compliance Status	T Lest Checked	GE POLICIES
				No items selected		

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

orage policy: VM Encryption Policy		1	Configure per disk 🔾
Name	Disk Size	Datastore	Datastore Type
T VM home	-	datastore1	VMFS 6
📇 Hard disk 1	2 GB	datastore1	VMFS 6
💩 Hard disk 2	2 GB	datastore1	VMFS 6
			2

- 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.

2 Select a creation type 2 Select a name and folder 3 Select a compute resource	Select storage Select the storage for the con	nfiguration and disk fil	les		
4 Select a compute resource 5 Select compatibility 6 Select a guest OS 7 Customize hardware 8 Ready to complete	Encrypt this virtual maching VM Storage Policy:	ne ① VM Encrypti	on Policy 🗸		
	Name	Cepecity	Provisioned	Free	
	 Storage Compatibility: Con 	mpatible			-
	datastore1	12.5 GB	5.41 GB	7.09 GB	
	< Compatibility				•
	Compatibility Compatibility checks such as a second sec	cceeded.			

3) Continue the wizard to finish the VM creation.