

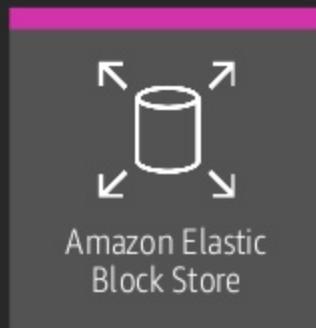
The logo for AWS re:Invent features the word "re:" in a smaller, gray sans-serif font positioned above the word "Invent". The word "Invent" is in a large, bold, white sans-serif font. The "i" in "Invent" has a vertical stroke that extends upwards, connecting it to the "e" in "re:". The background of the logo is a white rectangular area with a thin black border, set against a dark blue gradient background.

AWS
re:Invent

C M P 3 0 1

Backing up Amazon EC2 with Amazon EBS Snapshots

David Green
Enterprise Solutions Architect
Amazon Web Services
@davidmgre



Agenda



Amazon Elastic
Block Store

Agenda

- AWS storage and Amazon Elastic Block Store (EBS) overview
- EBS snapshots overview
- Automation and snapshot management
- Snapshot sharing and cross-region copies
- Encryption

More choice for more applications

Block storage



- General Purpose SSD
- Provisioned IOPS SSD
- Throughput Optimized HDD
- Cold HDD
- Elastic Volumes
- Amazon EC2 instance store

Twice as many block storage offerings as anyone else

Add capacity or change performance



File storage

Amazon Elastic File Service (EFS)

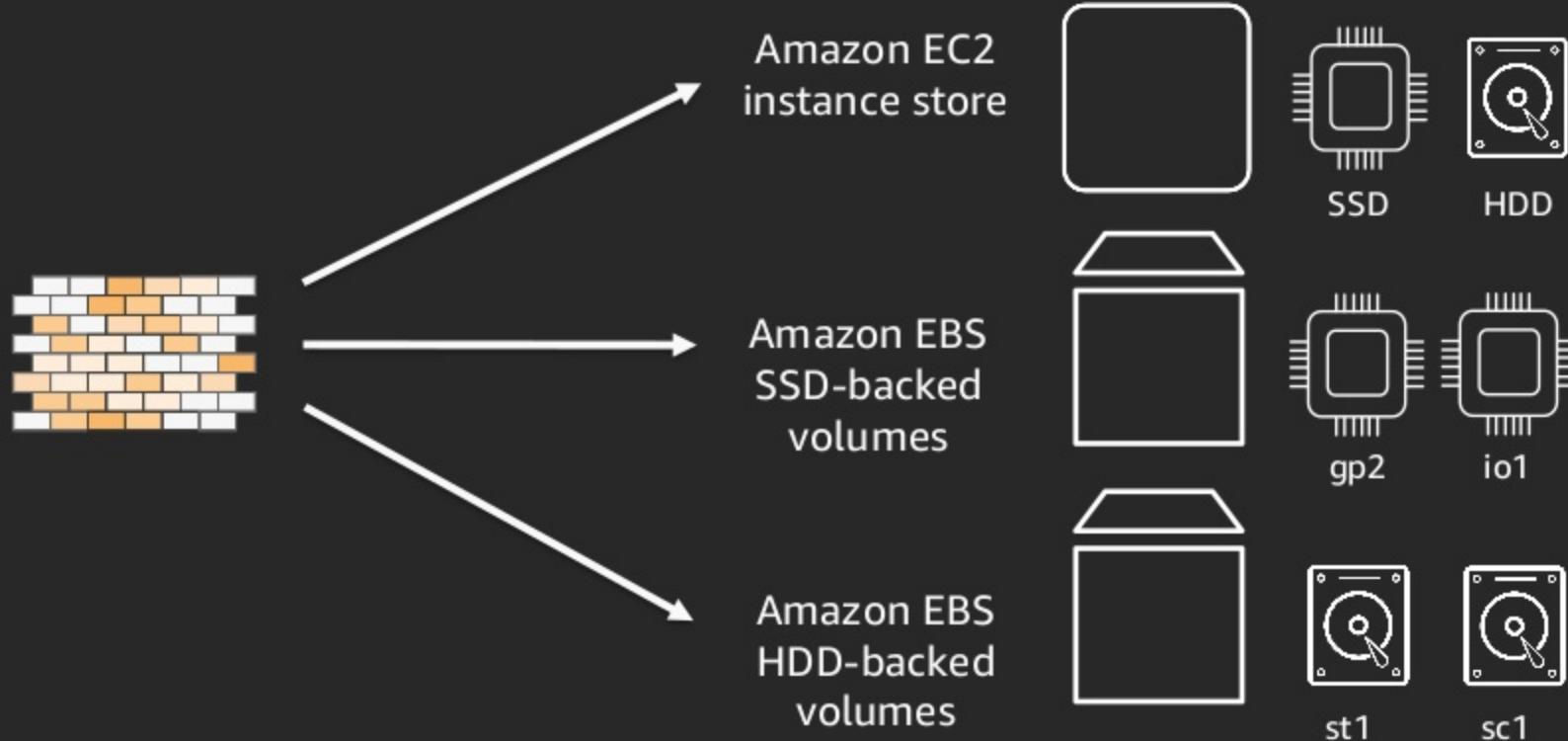


Object storage

Amazon S3 Standard
Amazon S3 Standard-IA
Amazon S3 One Zone-IA
Amazon S3 Glacier



AWS block storage offerings



Hybrid volume backup example

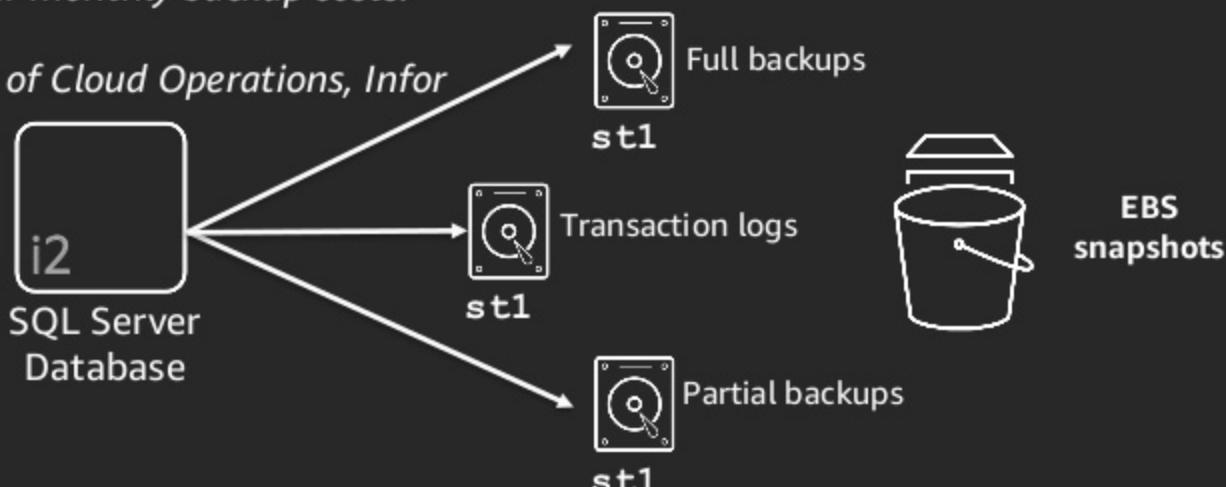


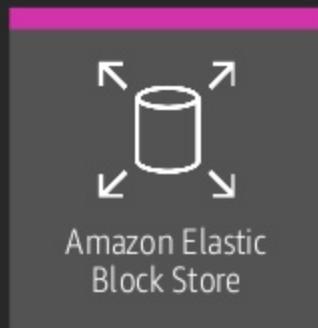
Case study:

<https://aws.amazon.com/solutions/case-studies/infor-ebs/>

*"We've seen much stronger performance for our database backup workloads with the Amazon **EBS ST1** volumes, and we're also saving **75 percent** on our monthly backup costs."*

~Randy Young, Director of Cloud Operations, Infor





What is Amazon Elastic Block Store (EBS)?



Amazon Elastic
Block Store

What is Amazon Elastic Block Store (EBS)?

- Block storage as a service
- Create, attach, manage volumes through an API
- Service accessed over the network
- SSD or HDD
- Encryption support
- Point-in-time snapshot support

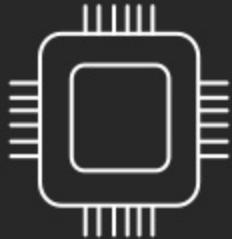


Amazon Elastic
Block Store

What is Amazon Elastic Block Store (EBS)?

- 99.999 availability
- 0.1 – 0.2%
annual failure rate (AFR)

Volume types and performance



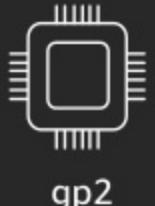
SSD-based



io1

\$0.125/GiB*
\$0.065/IOP*

Highest performance SSD volume
designed for critical and I/O
intensive workloads requiring
99.9% consistent performance



\$0.10/GiB*

General purpose SSD volume that
balances price and performance for
a wide variety of workloads with
predictable baseline and burst

*per GB month of provisioned storage (us-east-1)

Volume types and performance



HDD-based



st1

\$0.045/GiB*

Low cost HDD volume designed for frequently accessed, throughput intensive sequential workloads



sc1

\$0.025/GiB*

Lowest cost HDD volume designed for less frequently accessed sequential workloads

*per GB month of provisioned storage (us-east-1)



Amazon Elastic
Block Store

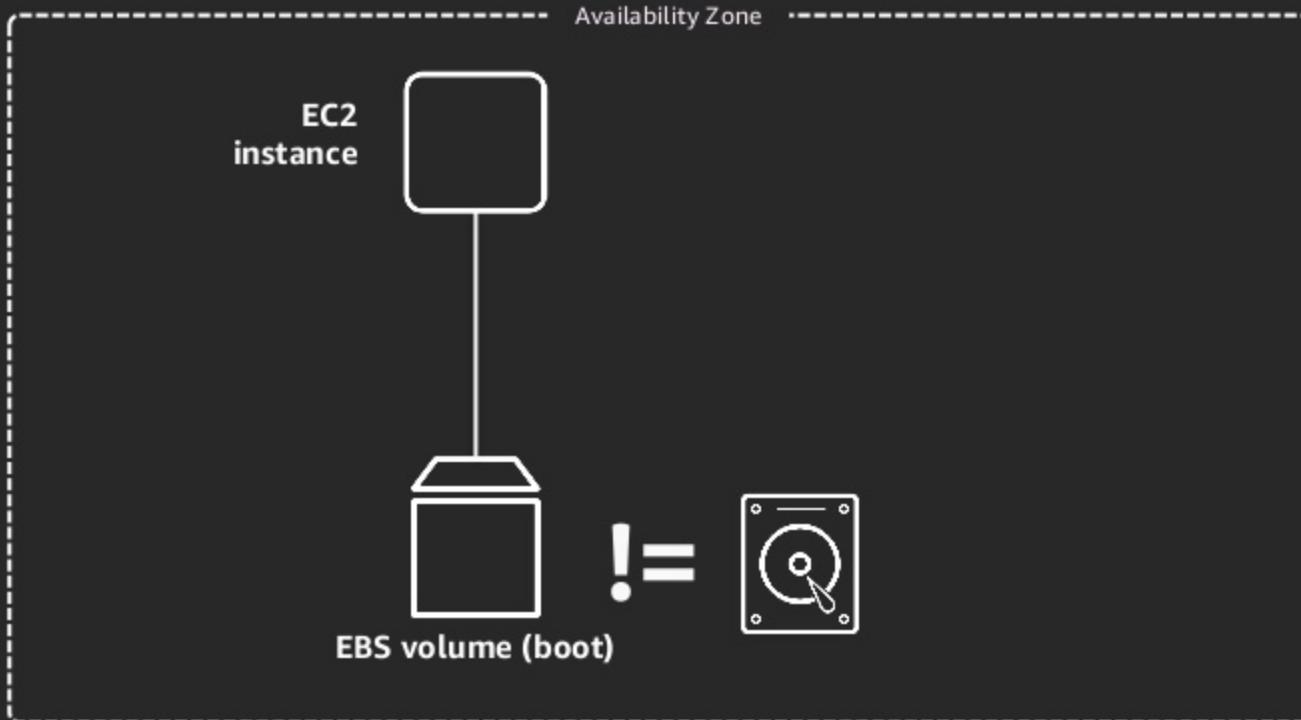
Elastic Volumes

- Increase volume size
- Modify performance
- Change volume type
- Continue using your application without downtime



Amazon Elastic
Block Store

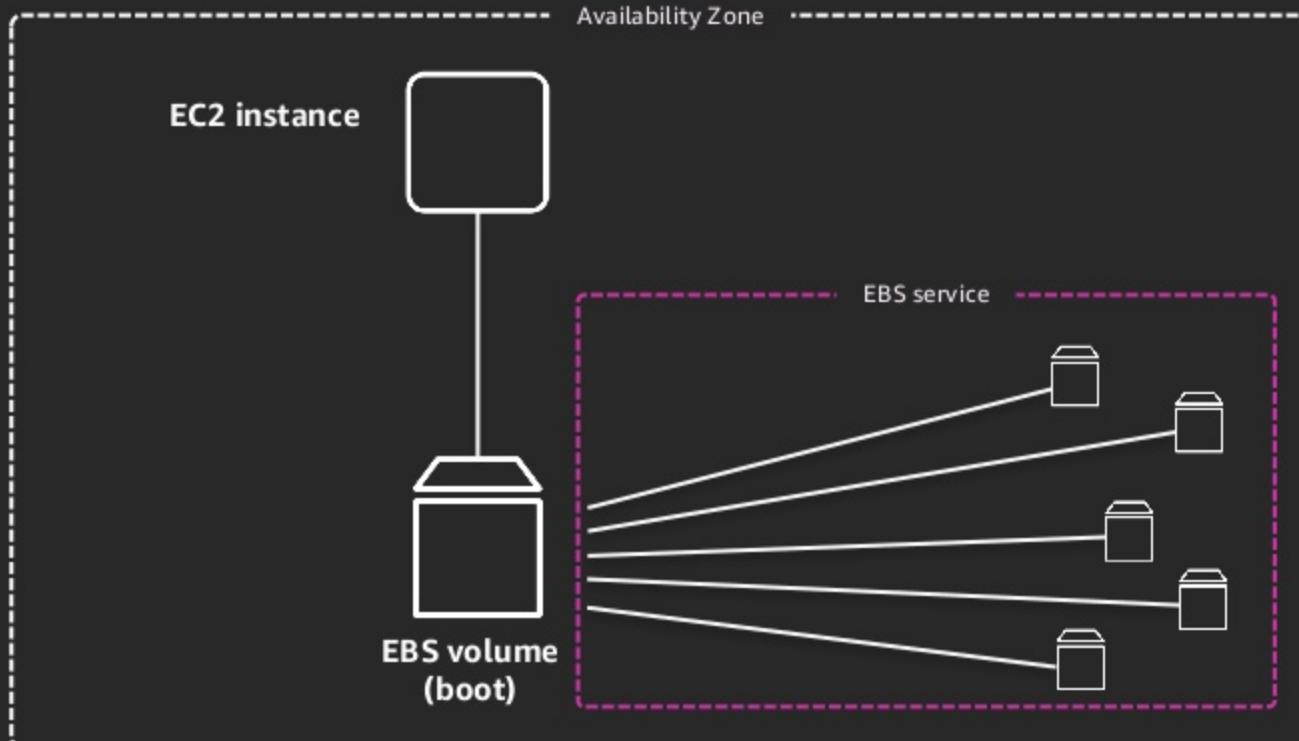
What is Amazon Elastic Block Store (EBS)?





Amazon Elastic
Block Store

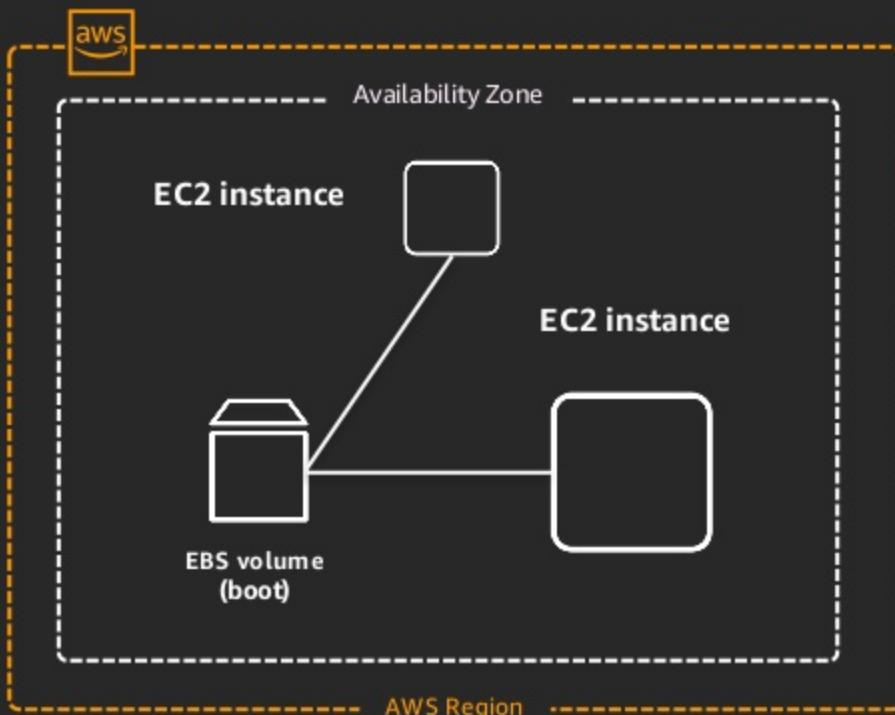
What is Amazon Elastic Block Store (EBS)?





Amazon Elastic
Block Store

What is Amazon Elastic Block Store (EBS)?

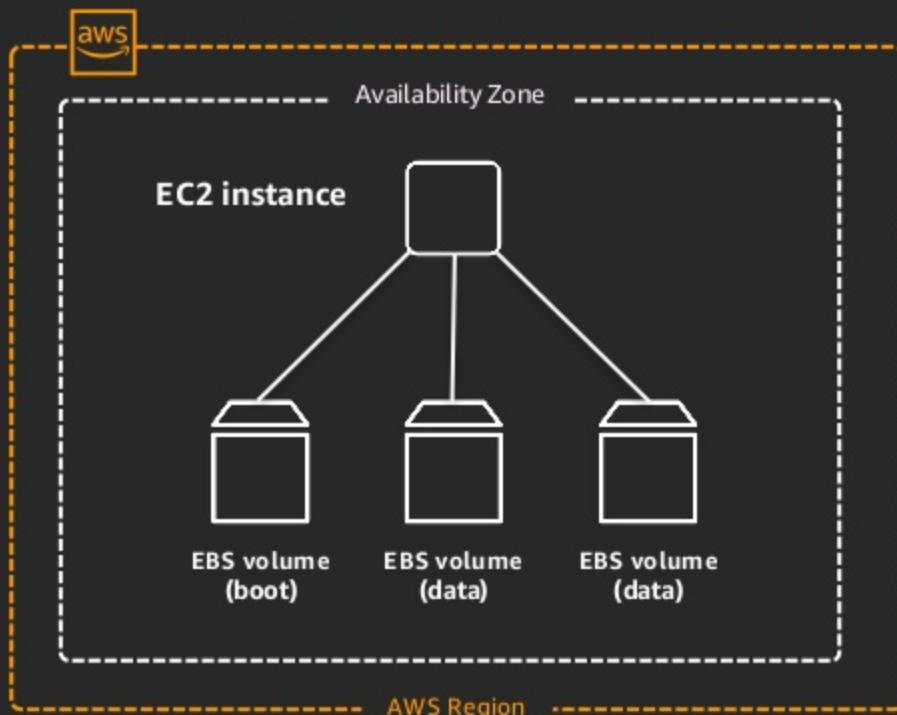


- Volumes persist independent of Amazon EC2
- Select storage and compute based on your workload
- Detach and attach between instances within the same Availability Zone



Amazon Elastic
Block Store

What is Amazon Elastic Block Store (EBS)?



- One instance can have many volumes attached
- Volumes attach to one instance
- **Best Practice:** separate boot and data volumes



EBS Snapshot creation



Creating an EBS snapshot (AWS console)

The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar menu is open, with the 'VOLUMES' option under 'ELASTIC BLOCK STORE' highlighted by a pink oval and a pink arrow pointing from the top-left towards it. At the top center, there's a 'Create Volume' button and an 'Actions' dropdown menu. The 'Actions' menu is open, showing options like 'Modify Volume', 'Delete Volume', 'Attach Volume', 'Detach Volume', 'Force Detach Volume', and 'Create Snapshot'. The 'Create Snapshot' option is highlighted with a pink oval. The main area displays a table of volumes. One volume, 'bees001', is selected, and its details are shown in a modal window at the bottom. The modal includes tabs for 'Description', 'Status Checks', 'Monitoring', and 'Tags'. The 'Description' tab is active, showing the volume's ID, size (80 GiB), creation date (October 17, 2017), state (in-use), attachment information (I-06296579806a2578d), volume type (gp2), and IOPS (240 / 3000). The 'Status Checks' tab indicates no issues. The 'Monitoring' tab shows no data, and the 'Tags' tab shows no tags.

Name	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	All
bees001	gp2	240 / 3000	-	October 17, 2017 at...	us-east-1a	in-use	No
bees002	gp2	240 / 3000	-	October 17, 2017 at...	us-east-1a	in-use	No
bees003	gp2	240 / 3000	-	October 17, 2017 at...	us-east-1a	in-use	No
bees004	gp2	240 / 3000	-	October 17, 2017 at...	us-east-1a	in-use	No
bees005	gp2	240 / 3000	-	October 17, 2017 at...	us-east-1a	in-use	No
bees006	gp2	240 / 3000	-	October 17, 2017 at...	us-east-1a	in-use	No



Creating an EBS snapshot (AWS console)

The screenshot shows the 'Create Snapshot' page in the AWS Lambda service. At the top, the volume ID 'vol-0e66cde28d761063d' is selected. The 'Description' field contains 'EBS Snapshot Example'. The 'Encrypted' option is set to 'Not Encrypted'. Below these fields is a table for adding tags, which currently contains four entries: 'Name' with value 'bees001', 'Cost Center' with value 'IEGB', 'Environment' with value 'Prod', and 'Application Name' with value 'bees'. A button 'Add Tag' is available to add more. At the bottom right are 'Cancel' and 'Create Snapshot' buttons.

Volumes > Create Snapshot

Create Snapshot

Volume vol-0e66cde28d761063d i

Description i

Encrypted Not Encrypted i

Key	(127 characters maximum)	Value	(255 characters maximum)
Name	bees001	x	
Cost Center	IEGB	x	
Environment	Prod	x	
Application Name	bees	x	

Add Tag 46 remaining (Up to 50 tags maximum)

Cancel Create Snapshot



Creating an EBS snapshot (AWS console)

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Ava...
bees001	vol-05d3346f...	80 GiB	gp2	240 / 3000		October 17, 2017 at...	us-e...
bees002	vol-0c76ed03...	80 GiB	gp2	240 / 3000		October 17, 2017 at...	us-e...
bees003	vol-0d66241f...					October 17, 2017 at...	us-e...
bees004	vol-05673501...					October 17, 2017 at...	us-e...
bees005	vol-0b449fc3...					October 17, 2017 at...	us-e...
bees006	vol-07d544a5...					October 17, 2017 at...	us-e...
bees: vol-05d3346fa44fc9cab							

Description Status Checks

Volume ID Size Created State Attachment information Volume type

Volume ID: i-06296579806a2578d (bees) :/dev/sdf
State: in-use
Attachment information: (attached)
Volume type: gp2

Alarm status: None
Snapshot: -
Availability Zone: us-east-1a
Encrypted: Encrypted
KMS Key ID: bae63fd5-612
KMS Key Aliases: aws/ebs

Create Snapshot

Snapshot Creation Started
View snapshot [snap-074af3a6274e03950](#)

Close



Viewing an EBS snapshot (AWS console)

The screenshot shows the AWS EC2 Dashboard with the "Schemas" tab selected. On the left, a sidebar lists various EC2 services: EC2 Dashboard, Events, Tags, Reports, Limits, Instances (Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), Images (AMIs, Bundle Tasks), and Elastic Block Store (Volumes, Snapshots). The "Snapshots" item is highlighted with a red oval. The main content area displays a table of snapshots owned by the user, with one row selected. The selected row shows the following details:

Name	Snapshot ID	Size	Description	Status	Started	Progress
My Snapshot Name	snap-074af3a6274e03950	80 GiB	Snapshot Description	completed	October 17, 2017 at 3:49:13 ...	available (100%)

Below the table, a detailed view of the selected snapshot is shown:

Snapshot: snap-074af3a6274e03950 (My Snapshot Name)

Description	Permissions	Tags
Snapshot ID: snap-074af3a6274e03950	Progress: 100%	
Status: completed	Capacity: 80 GiB	
Volume: vol-05d3346fa44fc9cab	Encrypted: Encrypted	
Started: October 17, 2017 at 3:49:13 PM UTC-7	KMS Key ID: bae63fd5-6121-411b-84d1-fd93f8d8b6a4	
Owner: 517977164187	KMS Key Aliases: aws:ebs	
Product codes: Loading...	KMS Key ARN: arn:aws:kms:us-east-1:bae63fd5-6121-411b-84d1-fd93f8d8b6a4	



Creating an EBS snapshot (AWS CLI)

```
[ec2-user@ebs ~]$ aws ec2 create-snapshot --volume-id vol-05d3346fa44fc9cab --description "Snapshot Description"
```

```
{  
    "Description": "Snapshot Description",  
    "Tags": [],  
    "Encrypted": true,  
    "VolumeId": "vol-07c96678d6d69ffd7",  
    "State": "pending",  
    "VolumeSize": 100,  
    "StartTime": "2018-11-26T06:14:16+00:00",  
    "Progress": "",  
    "OwnerId": "██████████",  
    "SnapshotId": "snap-09befcd5c06219b47"  
}
```

```
[ec2-user@ebs ~]$
```

<https://docs.aws.amazon.com/cli/latest/reference/ec2/create-snapshot.html>



Viewing an EBS snapshot (AWS CLI)

```
[ec2-user@ebs ~]$ aws ec2 describe-snapshots --snapshot-id snap-063f15dea2d87d3aa
{
    "Snapshots": [
        {
            "Description": "Snapshot Description",
            "VolumeSize": 100,
            "Encrypted": true, (highlighted)
            "VolumeId": "vol-07c96678d6d69ffd7",
            "State": "completed",
            "KmsKeyId": "arn:aws:kms:us-west-2::key/19fc8073-ef5e-4de2-84c0-6a0af43a22e97",
            "StartTime": "2018-11-26T06:14:16.687000+00:00",
            "Progress": "100%",
            "OwnerId": "XXXXXXXXXX",
            "SnapshotId": "snap-09befcd5c06219b47"
        }
    ]
}
```

<https://docs.aws.amazon.com/cli/latest/reference/ec2/create-snapshot.html>

EBS snapshots are crash consistent



Crash
consistency

- Snapshots will contain the blocks of completed I/O operations
- Data not flushed to disk does not exist in the snapshot
- Similar to pulling the power cord of a server

Application
consistency

- Application data is flushed to disk prior to snapshot creation
- New writes to application(s) are halted during the snapshot creation process
- Unfreeze/unlock as soon as snapshot creation command is successfully executed



Application-consistent,
VSS-enabled
S

VSS support with AWS Systems Manager (SSM)



SSM + VSS

- VSS manages disk operations, such as file writes, when a backup is in progress
- VSS-enabled snapshots of Amazon EBS volumes are available through Amazon EC2 Systems Manager Run Command.
- With VSS, you don't need to use application-specific backup solutions, such as native SQL Backup, or develop and maintain custom scripts.

VSS support with AWS Systems Manager (SSM)

- Call the Run Command:

*AWSEC2-
CreateVssSnapshot*

Commands > Run a command

Run a command

A command document includes the information about the command you want to run. Select a command document from the following list and then specify parameters for the command.

Command document* 

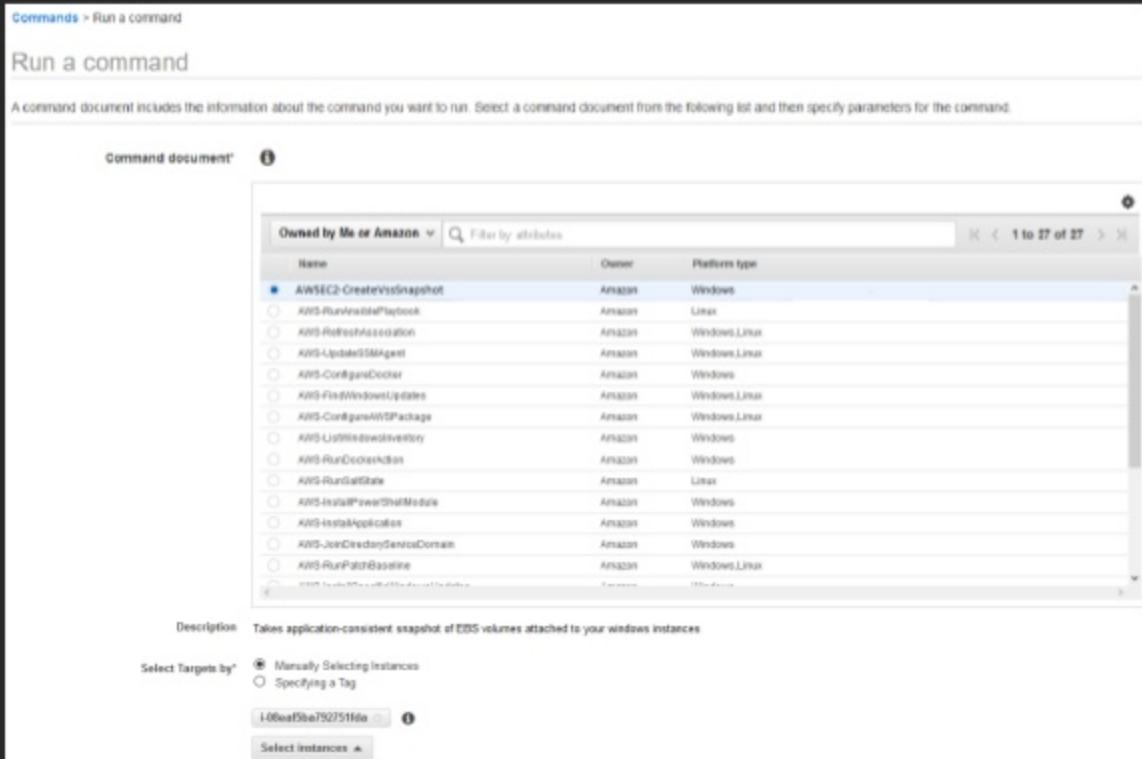
Owned by Me or Amazon			 Filter by attributes
Name	Owner	Platform type	
AWSEC2-CreateVssSnapshot	Amazon	Windows	
AWSS-RunAWSLambda	Amazon	Linux	
AWSS-RefreshAssociation	Amazon	Windows,Linux	
AWSS-UpdateSSMagent	Amazon	Windows,Linux	
AWSS-ConfigureConnector	Amazon	Windows	
AWSS-FindWindowsUpdates	Amazon	Windows,Linux	
AWSS-ConfigureAWSPackage	Amazon	Windows,Linux	
AWSS-UtilizedDeviceInventory	Amazon	Windows	
AWSS-RunDeployment	Amazon	Windows	
AWSS-RunGuardState	Amazon	Linux	
AWSS-InstallPowerShellModule	Amazon	Windows	
AWSS-InstallApplications	Amazon	Windows	
AWSS-JoinDirectoryServiceDomain	Amazon	Windows	
AWSS-RunPatchBaseline	Amazon	Windows,Linux	
AWSS-RunAWSLambdaFunction	Amazon	Windows,Linux	

Description  Takes application-consistent snapshot of EBS volumes attached to your windows instances

Select Targets by* 
 Manually Selecting Instances
 Specifying a Tag



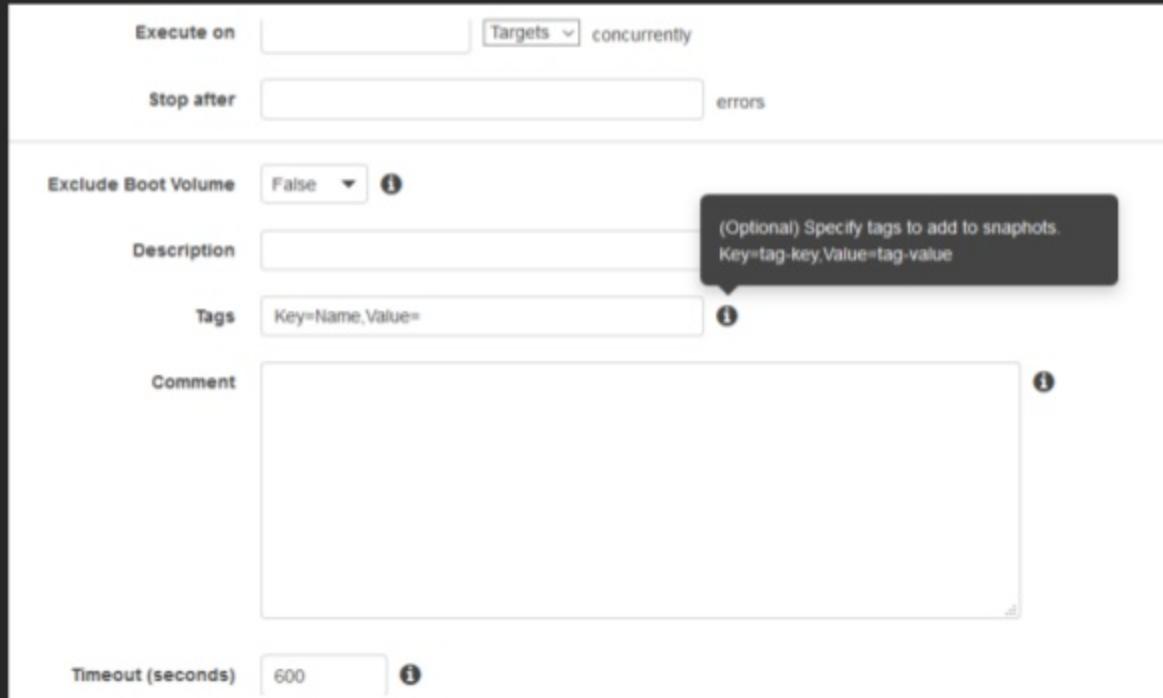




<https://docs.aws.amazon.com/systems-manager/latest/userguide/integration-vss.html>

VSS support with AWS Systems Manager (SSM)

- Select the instance
- Add description, tags
- Can exclude boot volume
- Run Command makes the VSS agent flush I/O, freeze



- SSM VSS included in Microsoft Windows Server AMI version 2017.11.21 and up

VSS support with AWS Systems Manager (SSM)

The screenshot shows the 'Create policy' interface in the AWS Management Console. It's a two-step process: 'Editor' (step 1) and 'Review' (step 2). Step 1 is currently active, showing a visual editor for creating AWS permissions. A policy definition is being built for the EC2 service, granting 'List', 'Write', and 'Tagging' actions on all resources. The JSON editor tab is also visible.

A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor.

Visual editor JSON Import managed policy

Use the visual editor to create and edit a policy by choosing services, actions, resources, and request conditions to add permissions to your policy. You can add multiple permission blocks to define complex permissions or to grant access to more than one service. [Learn more](#)

Expand all | Collapse all

EC2 (3 actions)

Service * EC2

Actions * List

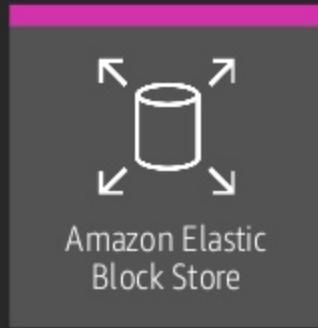
- DescribeInstances
- Write
- CreateSnapshot
- Tagging
- CreateTags

Resources * All resources

Request Conditions [Specify request conditions \(optional\)](#)

Clone Remove

<https://docs.aws.amazon.com/systems-manager/latest/userguide/integration-vss.html#integration-vss-restore>



EBS snapshot scheduling

The old way...



Snapshot scheduling – the old way...



Tagging



AWS Lambda



Amazon EC2
Run command



EBS Snapshot scheduling with Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager (DLM)



Amazon Data Lifecycle Manager (DLM) automates the creation, retention, and deletion of Amazon EBS volume snapshots.

Amazon Data Lifecycle Manager (DLM)



- Use policies to enforce **regular snapshot schedules**
- Policies identify volumes to backup using **tags**
- Retain backups for compliance / audit requirements
- Control snapshot costs by **optional automatic deletion** of old snapshots
- Use **IAM** to control DLM policy access
- **No cost to use** – pay only for data stored in snapshots

Amazon Data Lifecycle Manager (DLM)

Use policies to set backup and retention schedules

Customer requirement

*"All EC2 instance **root volumes** will be backed up once per day, saved for 7 days."*

*"All **Finance** or **Accounting** data volumes are backed up every 12 hours and retained for 10 days."*

Data lifecycle policy

Tags: **voltype:root**
Create: **every 24 hours**
Start Time: **0700 UTC**
Retention: **most recent 7**

Tags: **dept:finance, dept:accounting**
Create: **every 12 hours**
Start Time: **0900 UTC**
Retention: **most recent 20**

Amazon Data Lifecycle Manager (DLM)

The screenshot shows the AWS EC2 Dashboard with the 'Volumes' section selected. A modal overlay is displayed, showing the details for a selected volume named 'bees'. The modal includes a table of volumes, a search bar, and tabs for Description, Status Checks, Monitoring, and Tags. The 'Tags' tab is active, showing three tags: Name (bees), accounting (finance), and voltype (root).

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Available
bees	vol-0922181f...	16 GiB	gp2	100	snap-0ed126e...	November 19, 2018...	us-east
bees	vol-07ccff889e407af8 (bees)	16 GiB	gp2	100	snap-0ed126e...	November 19, 2018...	us-east
bees	vol-0977b78...	16 GiB	gp2	100	snap-0ed126e...	November 19, 2018...	us-east

Volumes: vol-07ccff889e407af8 (bees)

Add/Edit Tags

Key	Value	Actions
Name	bees	Hide Column
accounting	finance	Show Column
voltype	root	Show Column

Amazon Data Lifecycle Manager (DLM)

The screenshot shows the AWS Management Console interface for creating a snapshot lifecycle policy. The top navigation bar includes the AWS logo, Services dropdown, Resource Groups dropdown, a row of orange icons, a user profile (dg @ pandas), and region (N. Virginia). The main title is "Create Snapshot Lifecycle Policy". A sub-header states: "Data Lifecycle Manager for EBS Snapshots will help you automate the creation and deletion of EBS snapshots based on a schedule. Volumes are targeted by tags".

Description*: snapshot root every 24 hours

Target volumes with tags: This policy will be applied to volumes with **any** of the following tags.

You cannot use tags that are in use by another enabled or disabled lifecycle policy.

Tags: * voltype : root

Schedule name*: Daily Snapshot

Create snapshots every: 24 Hours

Snapshot creation start time: 07 : 00 UTC

Amazon Data Lifecycle Manager (DLM)

The screenshot shows the AWS Data Lifecycle Manager (DLM) configuration page. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, a toolbar with several icons, a user profile 'dg @ pandas', a region 'N. Virginia' dropdown, and a 'Support' dropdown.

Snapshot creation start time: 07 : 00 UTC

Snapshots start being created within one hour of the specified start time.

Retention rule: Number of snapshots that will be retained. i

* 7

Rule summary: Every 24 hours a snapshot will be created starting at 07:00 UTC.
A maximum of 7 snapshots will be retained of a target volume.
The oldest snapshot retained will be <= 7 days old.

Copy tags: Copy Tags from Volume

Tag created snapshots: Any snapshot created with this policy will automatically be tagged with the policy ID and schedule name. You can add additional tags below.

Key	(127 characters maximum)	Value	(255 characters maximum)

Amazon Data Lifecycle Manager (DLM)

The screenshot shows the AWS Data Lifecycle Manager (DLM) policy creation interface. At the top, there is a navigation bar with the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, a toolbar with several icons, a user profile 'dg @ pandas', a region 'N. Virginia' dropdown, and a 'Support' dropdown.

The main content area displays a message: 'This resource currently has no tags' and 'Choose the Add tag button or click to add a Name tag'. Below this is a button labeled 'Add Tag' and the text '50 remaining (Up to 50 tags maximum)'.

A section titled 'IAM role' contains the text: 'This policy needs to be associated with an IAM role that has snapshot create and delete permissions, if you are unsure what IAM role to use, select the AWS Default role.' There are two radio button options: 'Default role' (selected) and 'Choose another role'. A note in a callout box states: 'If EBS default role is not present, one will be automatically created with all needed permissions. [View Default role](#)'.

Below this is a section for 'Policy status after creation*' with two radio button options: 'Enable policy' (selected) and 'Disable policy'.

At the bottom right are 'Cancel' and 'Create Policy' buttons.

Amazon Data Lifecycle Manager (DLM)

The screenshot shows the AWS Amazon Data Lifecycle Manager (DLM) console. At the top, there's a navigation bar with the AWS logo, Services dropdown, Resource Groups dropdown, and various icons. On the right, there are notifications, user info (dg @ pandas), region (N. Virginia), and support links.

In the main area, there's a search bar with the query "policyId : policy-09959bf4562f95fb9" and an "Add filter" button. Below the search is a table with one row:

Policy ID	Description	State
policy-09959bf4562f95fb9	snapshot root every 24 hours	ENABLED

Below the table, the policy details are shown:

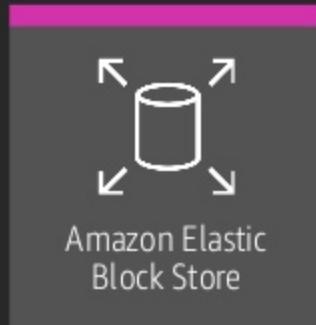
Policy: policy-09959bf4562f95fb9

Details

Policy ID	policy-09959bf4562f95fb9	Description	snapshot root every 24 hours
Date created	Mon Nov 26 14:17:32 GMT-800 2018	Policy state	ENABLED
Date modified	Mon Nov 26 14:17:32 GMT-800 2018	Schedule name	Daily Snapshot
Target volumes with these tags	voltype:root	Tags added to snapshots	
Rule summary	Every 24 hours a snapshot will be created starting at 07:00 UTC. A maximum of 7 snapshots will be retained of a target volume. The oldest snapshot retained will be <= 7 days old.	Execution Role Arn	arn:aws:iam::role/service-role/AWSDataLifecycleManagerDefaultRole

Every EBS snapshot functions as a full point-in-time backup.

To minimize costs, EBS snapshots are incremental – You are billed only for unique blocks.

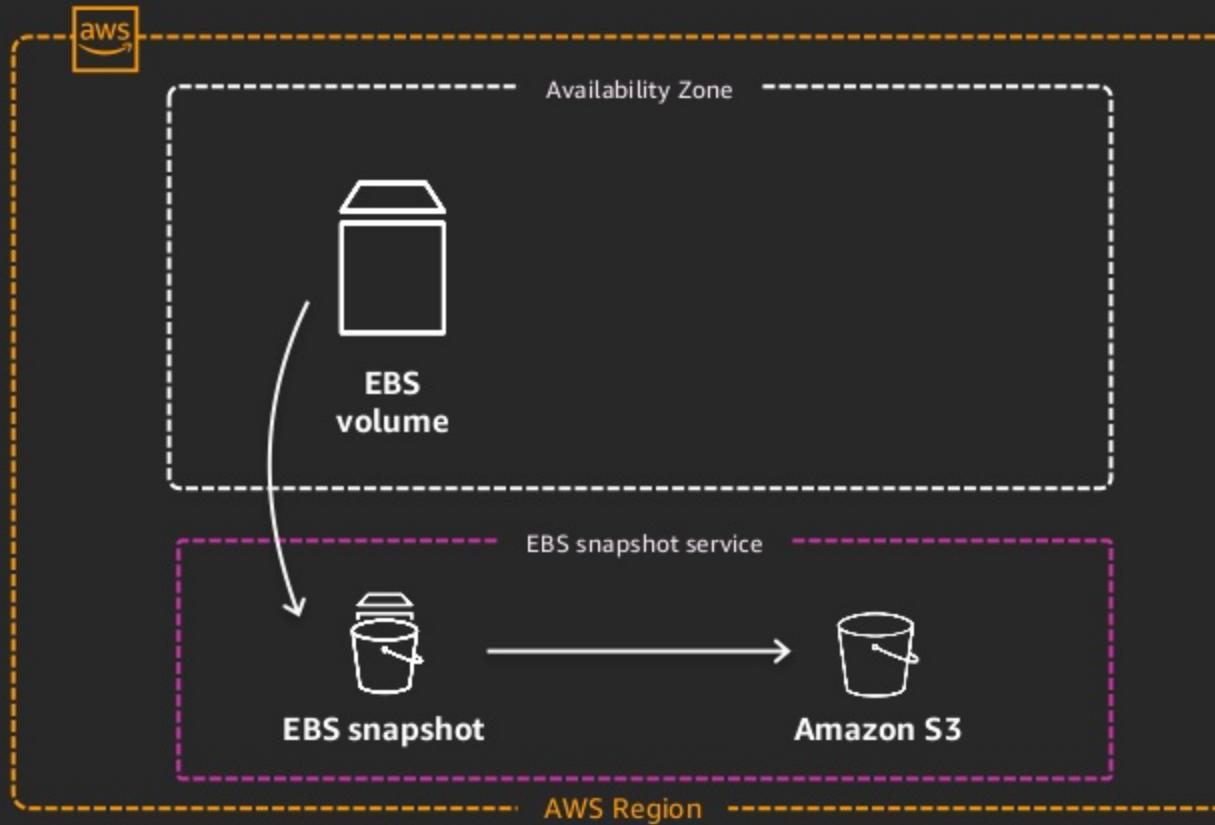


How EBS snapshots work



Amazon EBS
snapshot

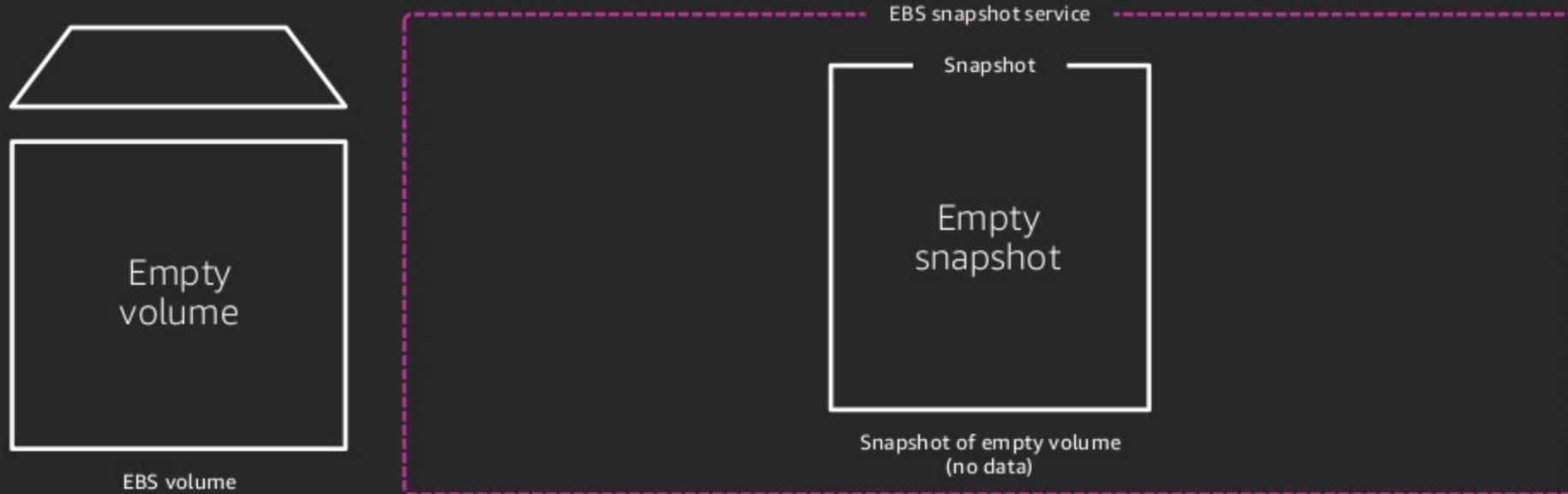
How does an EBS snapshot work?





Amazon EBS
snapshot

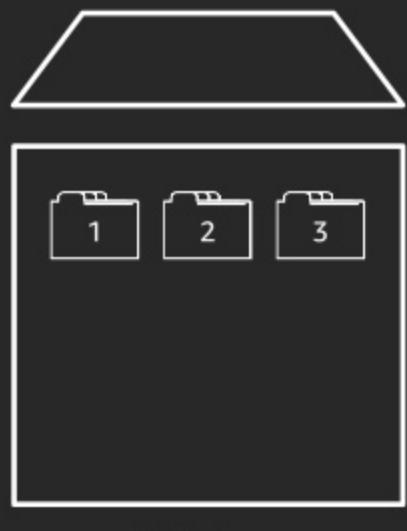
How does an EBS snapshot work?





Amazon EBS
snapshot

How does an EBS snapshot work?



EBS volume

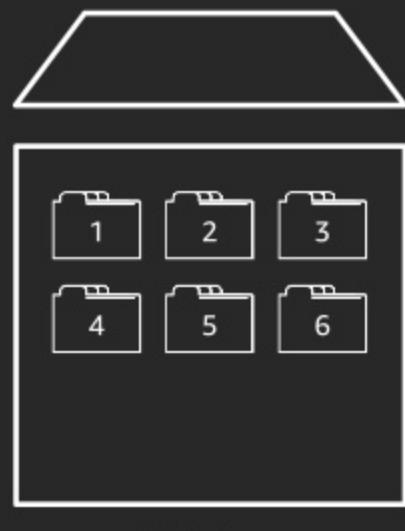


EBS snapshot service

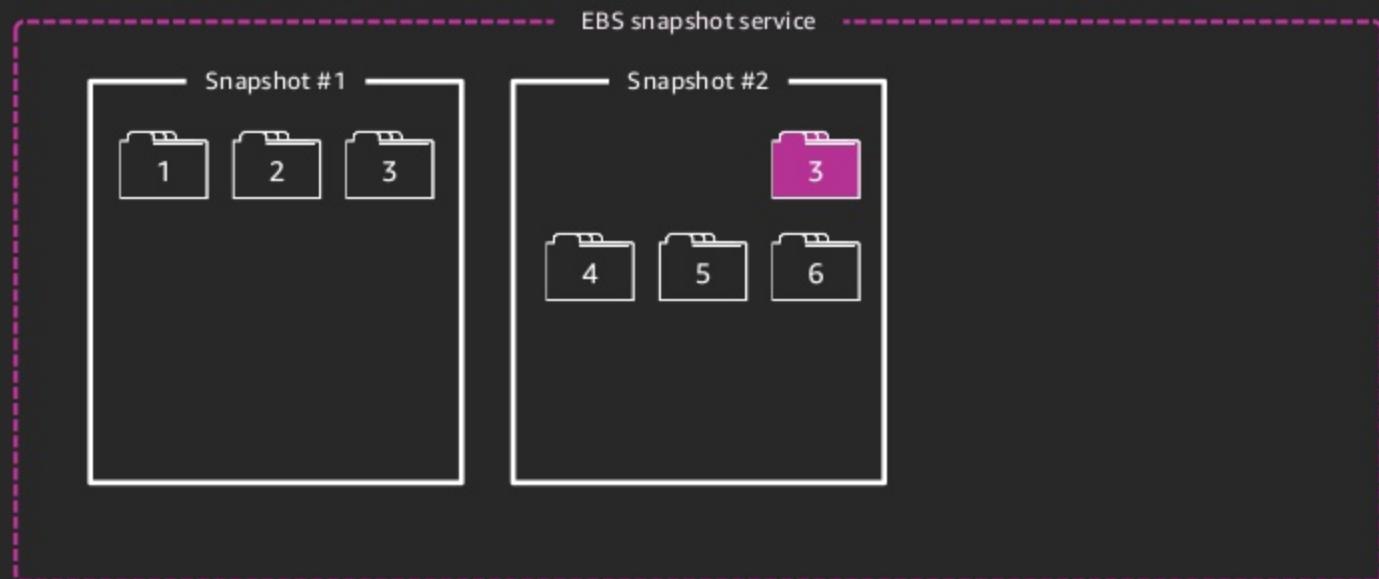


Amazon EBS
snapshot

How does an EBS snapshot work?



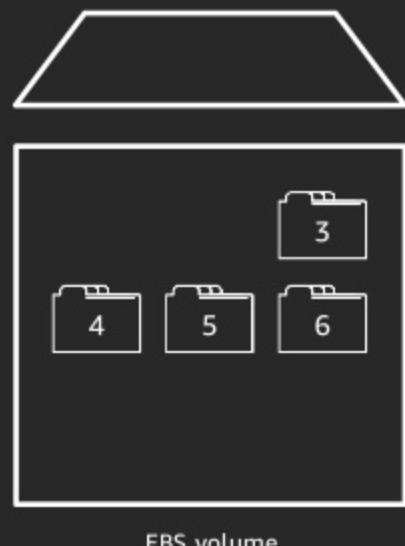
EBS volume





Amazon EBS
snapshot

How does an EBS snapshot work?



Snapshot #1



EBS snapshot service

Snapshot #2



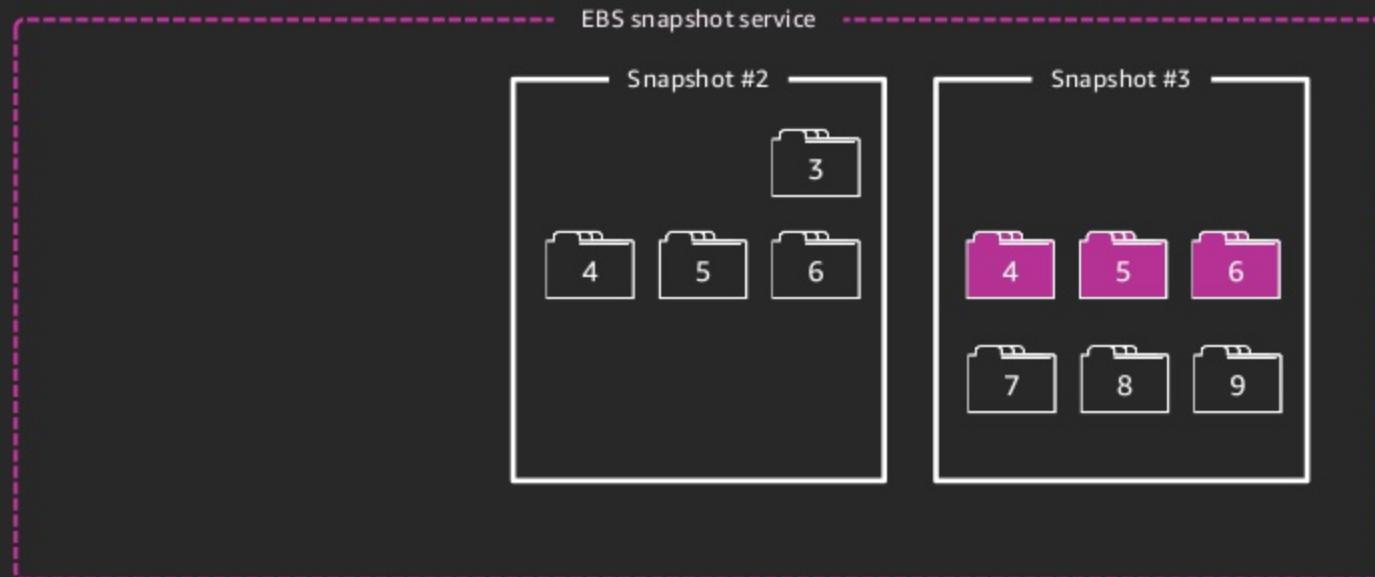


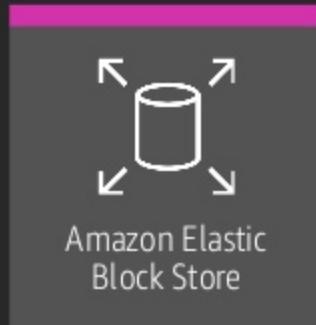
Amazon EBS
snapshot

How does an EBS snapshot work?



EBS volume





EBS snapshot encryption

EBS snapshot encryption

When enabled, following types of data are encrypted:

- Data in flight between the volume and the instance
- Data at rest inside the volume
- Snapshots created from the volume



<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

EBS snapshot encryption



- Snapshots of **encrypted volumes** are **automatically encrypted**
- Volumes that are created from encrypted snapshots are automatically encrypted
- When you copy an unencrypted snapshot that you own, you can encrypt it during the copy process
- When you copy an encrypted snapshot that you own, you can re-encrypt it with a different key during the copy process

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

Best practices – EBS snapshot encryption



EBS encryption:
data volumes

Volumes > Create Volume

Create Volume

Volume Type: General Purpose SSD (gp2) ⓘ

Size (GiB): 100 (Min: 1 GiB, Max: 16384 GiB)

IOPS: 300 / 3000 (Baseline of 3 IOPS per GB with a minimum of 100 IOPS, tunable to 3000 IOPS) ⓘ

Availability Zone*: us-east-1a ⓘ

Throughput (Mbps): Not applicable ⓘ

Snapshot ID: Select a snapshot ⓘ

Encryption: Encrypt this volume ⓘ

Master Key: (Default) aws/ebs ⓘ

KMS Key Description: Default master key that protects my EBS volumes when no other key is defined

KMS Key Account: This account ⓘ

KMS Key ID: bae60f05-6121-411b-84d1-f800fb0bb6ef

KMS Key ARN: arn:aws:kms:us-east-1:111111111111:key/bae60f05-6121-411b-84d1-f800fb0bb6ef

Key	(127 characters maximum)	Value	(255 characters maximum)
Name	Encrypted Volume	 ⓘ	 ⓘ
Application Name	AppD1	 ⓘ	 ⓘ

Add Tag: 48 remaining (Up to 50 tags maximum)

Cancel Create Volume

Best practices – EBS snapshot encryption



EBS encryption:
data volumes

Master Key (default) aws/ebs C

KMS Key Description Default master key that protects my EBS volumes when no other key is defined

KMS Key Account This account

KMS Key ID bae63fd5-6121-411b-84d1-fd93fb8b6a4

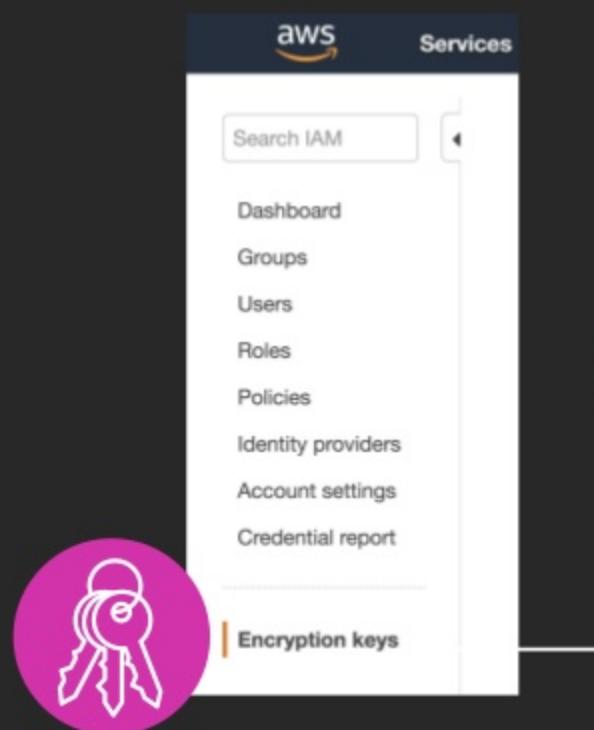
KMS Key ARN arn:aws:kms:us-east-1:...:key/bae63fd5-6121-411b-B4d1-fd93fb8b6a4

Key	(127 characters maximum)	Value	(255 characters maximum)
Name	Encrypted Volume	X	
Application Name	App01	X	

Add Tag 48 remaining (Up to 50 tags maximum)

Cancel Create Volume

Best practices – EBS snapshot encryption



The screenshot shows the AWS IAM service interface. On the left, there's a sidebar with options like 'Dashboard', 'Groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Credential report'. At the bottom of this sidebar, 'Encryption keys' is highlighted with a pink border. The main area is titled 'Create a new AWS KMS master key for EBS' and contains a form for creating an alias ('ebs-master') and a description ('Master EBS Encryption Key'). A large pink circle with a white key icon is overlaid on the left side of the main form area. An arrow points from the 'Encryption keys' link in the sidebar up towards the 'Create Alias and Description' form.

Create a new AWS KMS master key for EBS

Create Alias and Description

Provide an alias and a description for this key. These properties of the key can be changed later. [Learn more](#).

 Alias (required)

Description

- Define **key rotation** policy
- Enable AWS CloudTrail **auditing**
- Control who can **use** key
- Control who can **administer** key

Best practices – EBS snapshot encryption



EBS encryption:
data volumes

Encryption Encrypt this volume (i)

Master Key C

KMS Key Description Master EBS Encryption Key

KMS Key Account This account (██████████)

KMS Key ID 9b117d93-c37a-495c-baef-404515f2ed7f

KMS Key ARN arn:aws:kms:us-east-1:██████████:key/9b117d93-c37a-495c-baef-404515f2ed7f

Key	(127 characters maximum)	Value	(255 characters maximum)
Name		Encrypted Volume	<small>x</small>
Application Name		App01	<small>x</small>

Add Tag 48 remaining (Up to 50 tags maximum)

Cancel Create Volume

RunInstances with custom CMKs



EBS encryption:
data volumes

Screenshot of the AWS EC2 "RunInstances" wizard, Step 4: Add Storage. The screenshot shows the configuration of storage volumes for a new instance. Two volumes are listed: the root volume and an EBS volume.

Volume type	Device	Snapshot	Size (GiB)	Volume type	IOPS	Throughput (MB/s)	Delete on termination	Encrypted
Root	/dev/hda1	snap-01234123412...	8	General purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not encrypted
EBS	/dev/sdb	Search (case-insensitive)	8	General purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not encrypted

[Add new volume](#)

Cancel Previous Review and Launch Next: Add Storage

RunInstances with custom CMKs



EBS encryption:
data volumes

AWS Step 4: Add Storage interface showing EBS volume configuration and a modal for selecting a KMS Key.

The main table shows:

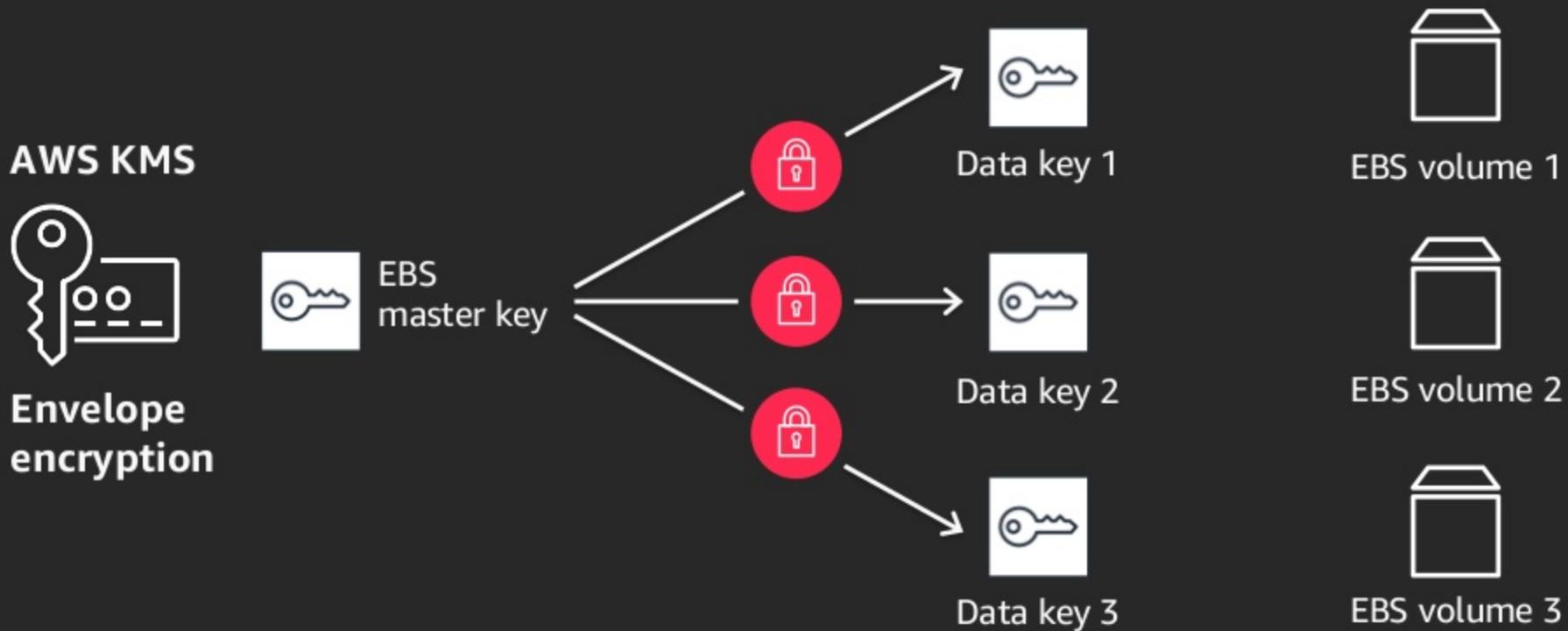
Volume type	Device	Snapshot	Size (GiB)	Volume type	IOPS	Throughput (MB/s)	Delete on termination	Encrypted
Root	/dev/xvda	snap-01234123412...	8	General purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not encrypted
EBS	/dev/sdb	Search (case insensitive)	8	General purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	1111aa11-012...

An open modal lists KMS Key Aliases and KMS Key ID:

KMS Key Aliases	KMS Key ID
Not encrypted	
MyKey	1111aa11-0129-4e01-b45c-f200a021448f
ExampleKey	2222bb23-0230-4g1g-b346-fedecae421d7qj
AnotherKey	123cf12e1-1420-45f9-b226-g2d6ef025ewf
NewKey	12dqw12e-2220-5df23-b416-n23gsfdg44

Buttons at the bottom: Cancel, Previous, Review and Launch (highlighted), Next: Add Storage.

EBS snapshot encryption



EBS snapshot encryption

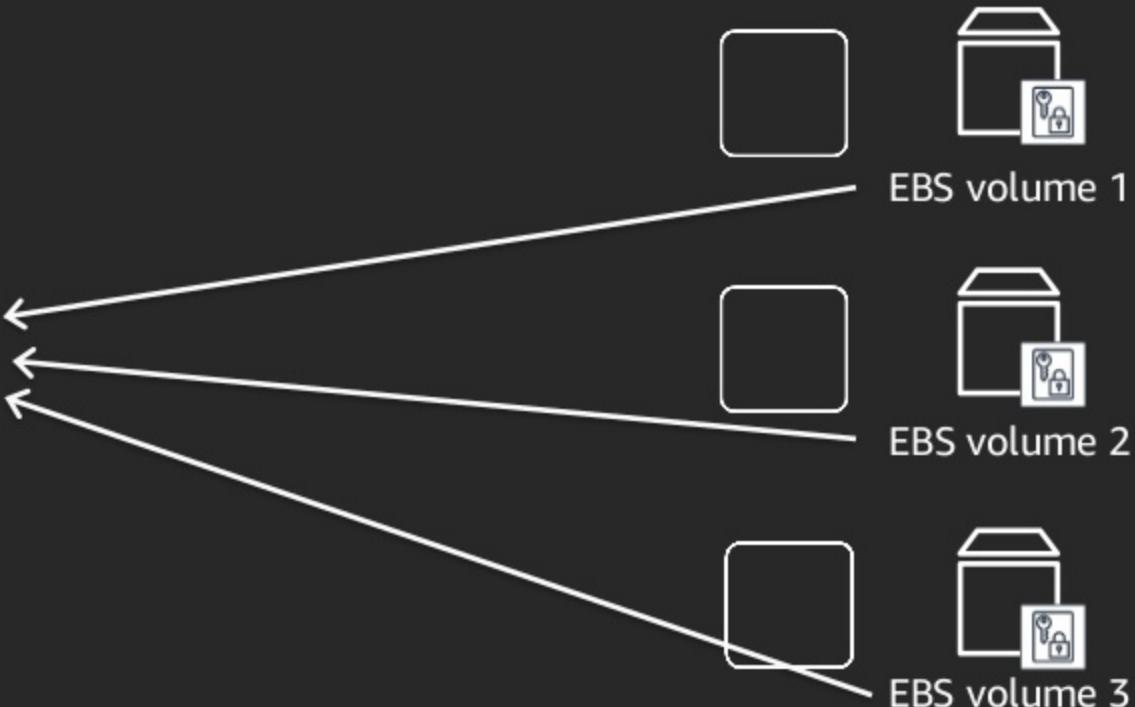
AWS KMS



Envelope
encryption



EBS
master key



EBS snapshot encryption

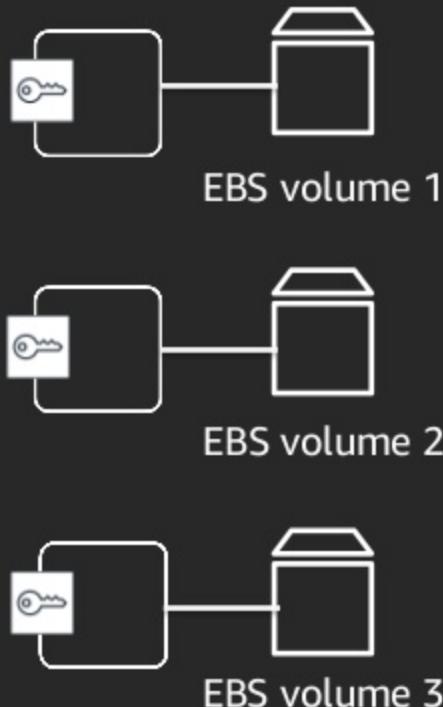
AWS KMS



EBS
master key

Envelope encryption

- Limits exposure risk
- Performance
- Simplifies key management





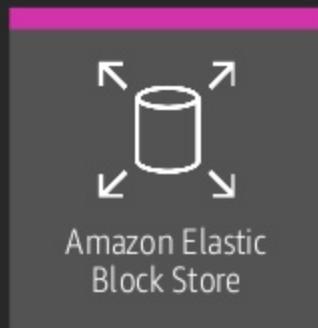
Preview: EBS encryption enhancements

Preview: EBS encryption enhancements



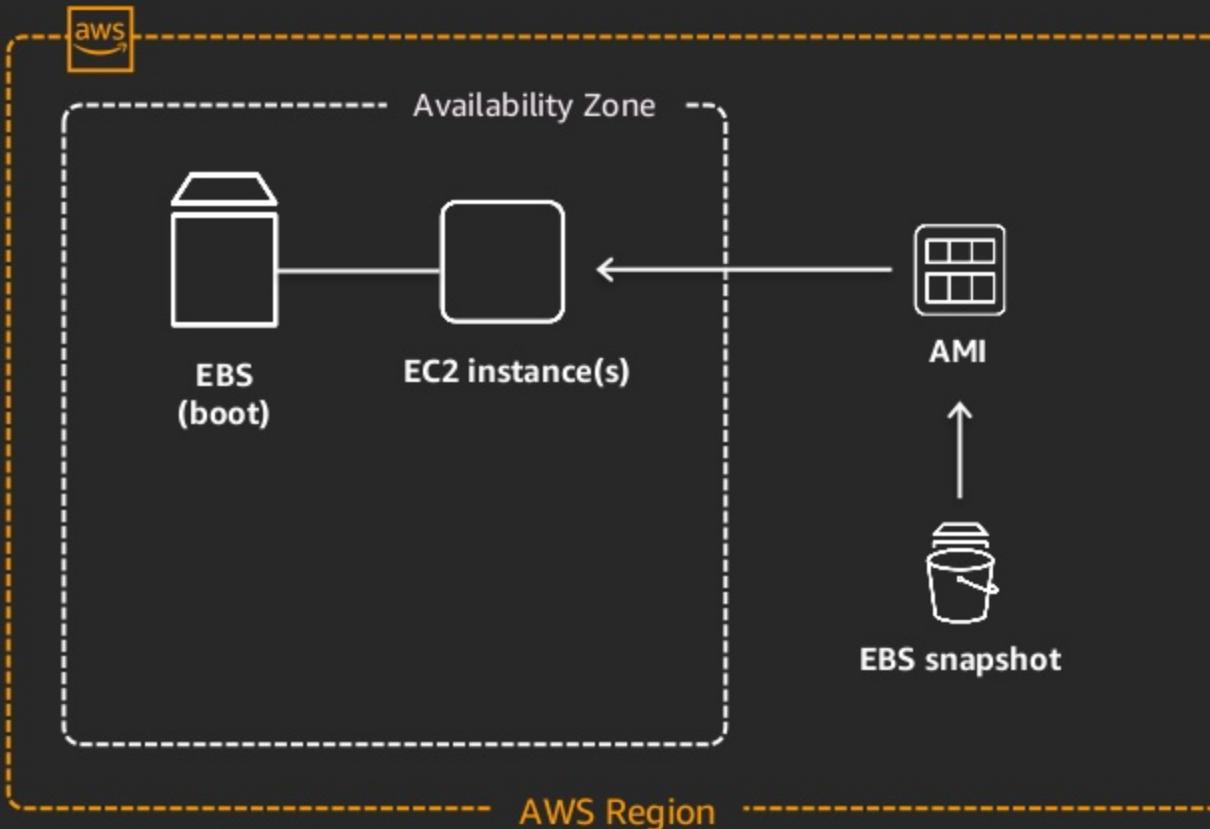
- Launch **encrypted EBS backed Amazon EC2 Instances** from **unencrypted AMIs**
- Share custom CMK encrypted AMIs between accounts
- Launch **encrypted EBS backed Amazon EC2 Instances** from **shared AMIs**

Contact us at: ebs-encryption-preview@amazon.com

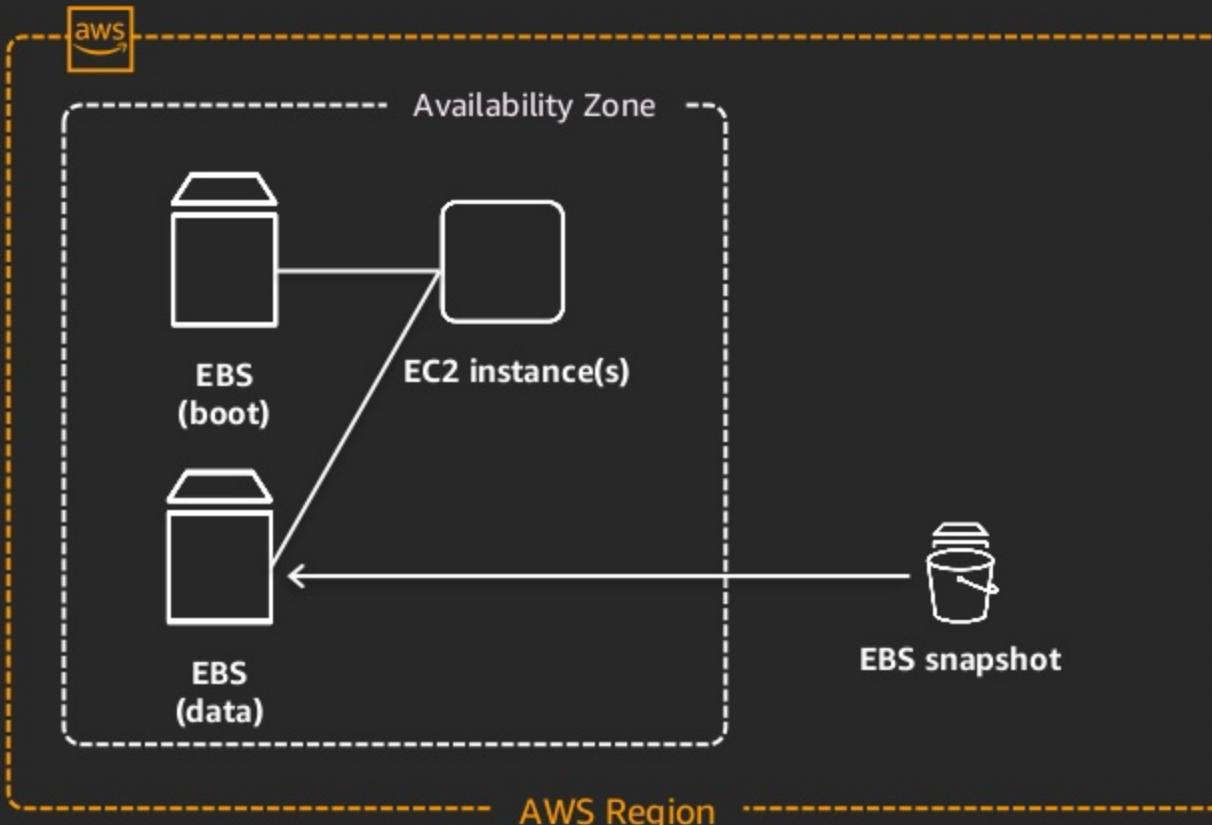


What can you do with EBS snapshots?

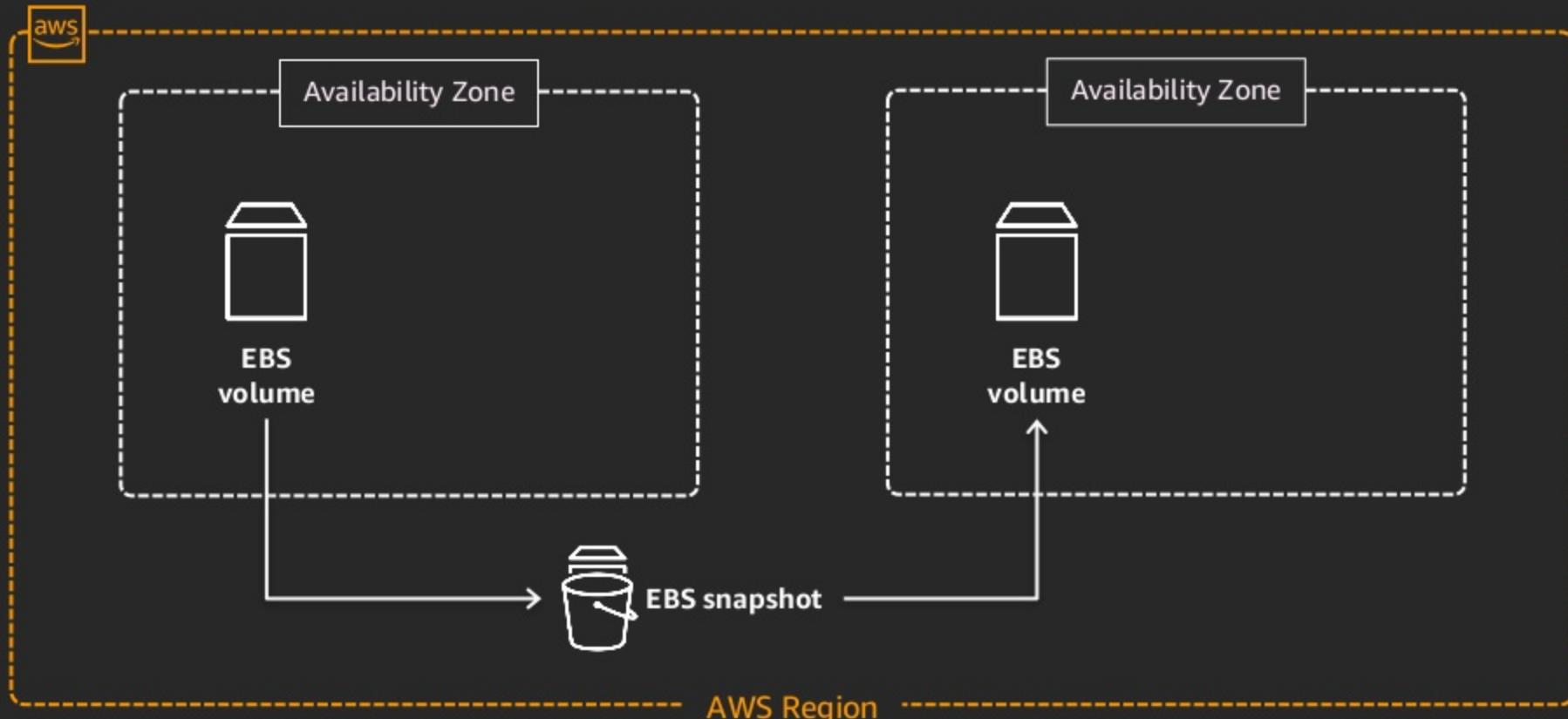
What can you do with a snapshot?



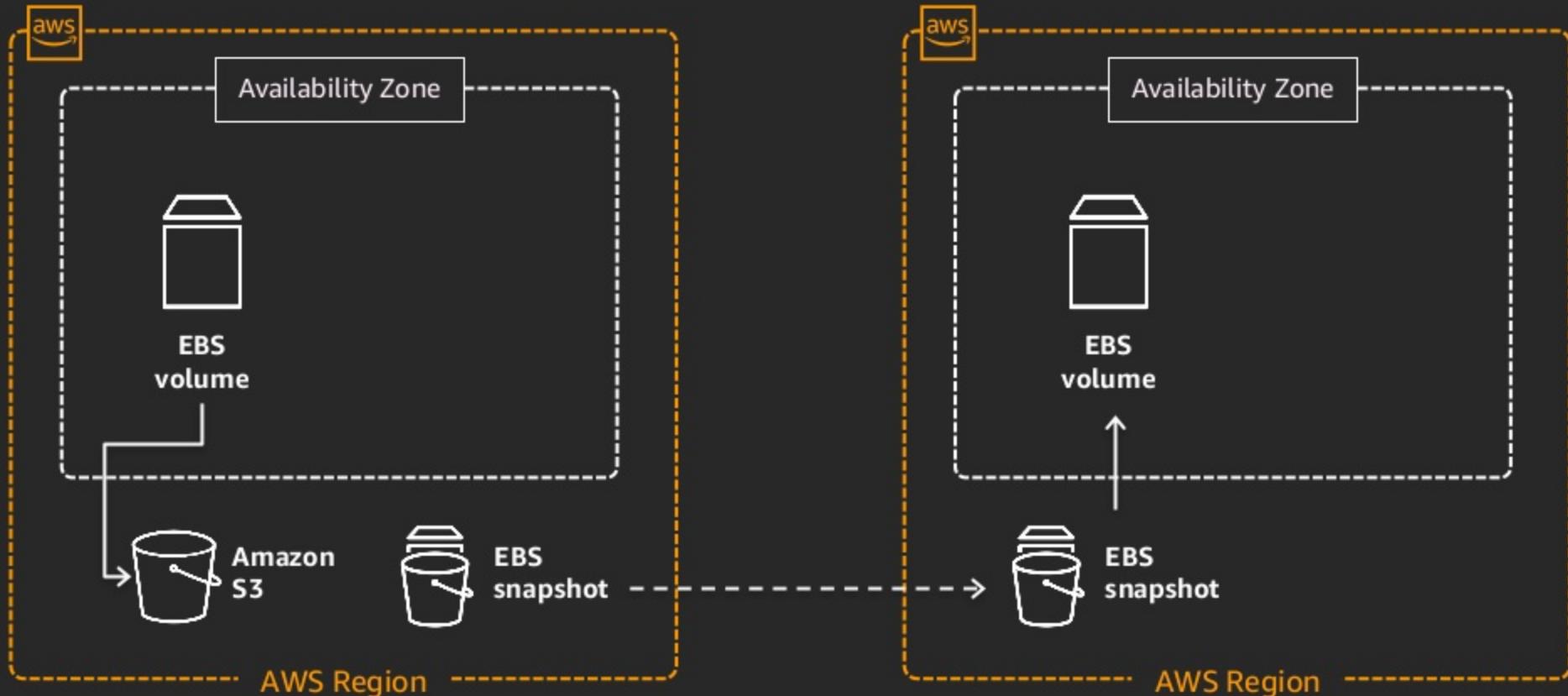
What can you do with a snapshot?

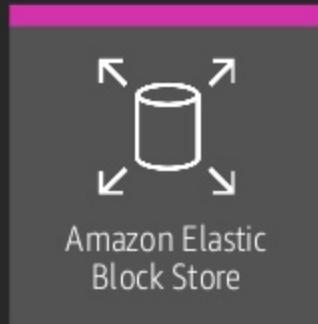


What can you do with a snapshot?



What can you do with a snapshot?





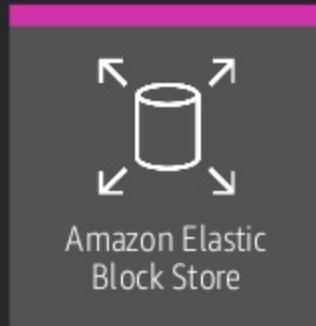
EBS snapshot copying

EBS Snapshot copying



- Amazon S3 encryption protects the snapshot in-transit during the copy operation
- The first copy to another region is always a full copy
- Snapshots are incremental after the first copy*

*The same CMK must be used on both ends to support subsequent incremental copies



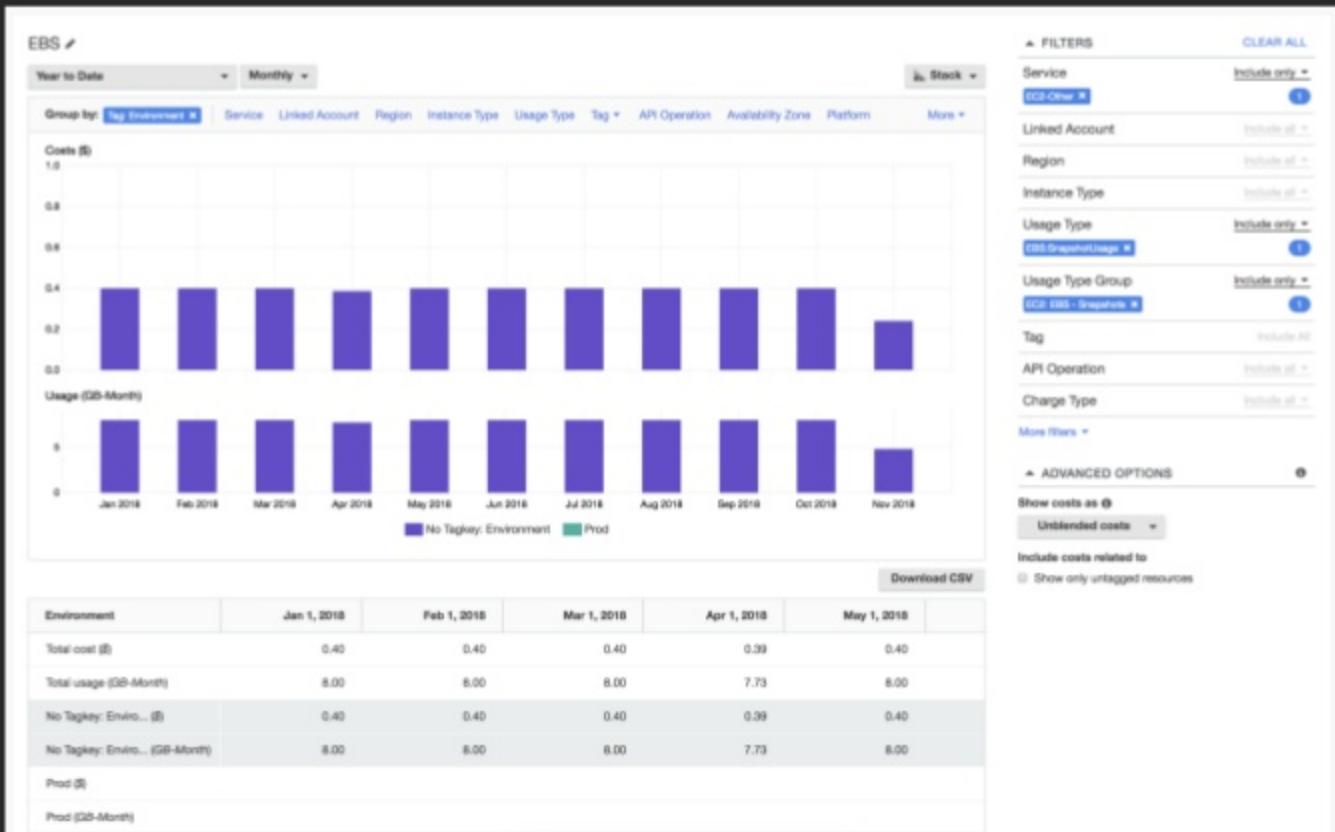
EBS snapshot cost monitoring

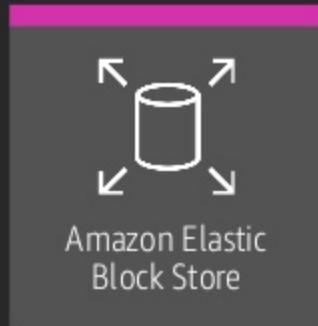
EBS Snapshot cost monitoring



- Custom tags support **key/value** pairs
- Use tags for identification and management
- Activate tags for **cost allocation tags** to provide greater visibility into snapshot storage costs

EBS Snapshot cost monitoring





In closing...

In closing...



Tag, tag, tag!

Tag your environments to be easily identified and associated with the cost explorer



Automate!

Leverage Amazon Data Lifecycle Management (DLM) to automatically create and (optionally) delete snapshots



Encrypt

Encryption of Amazon EBS volumes is literally a checkbox. Use it!

In closing...



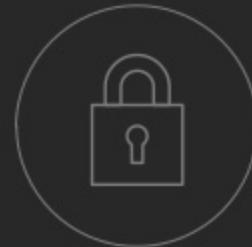
Tag, tag, tag!

Tag your environments to be easily identified and associated with the cost explorer



Automate!

Leverage Amazon Data Lifecycle Management (DLM) to automatically create and (optionally) delete snapshots



Encrypt

Encryption of Amazon EBS volumes is literally a checkbox. Use it!

In closing...



Tag, tag, tag!

Tag your environments to be easily identified and associated with the cost explorer



Automate!

Leverage Amazon Data Lifecycle Management (DLM) to automatically create and (optionally) delete snapshots



Encrypt

Encryption of Amazon EBS volumes is literally a checkbox. Use it!

Thank you!

David Green
Enterprise Solutions Architect
Amazon Web Services
@davidmgre



Please complete the session
survey in the mobile app.