EBS Snapshots

Data Protection Best Practices

Jeff Bartley, Storage Solutions Architect

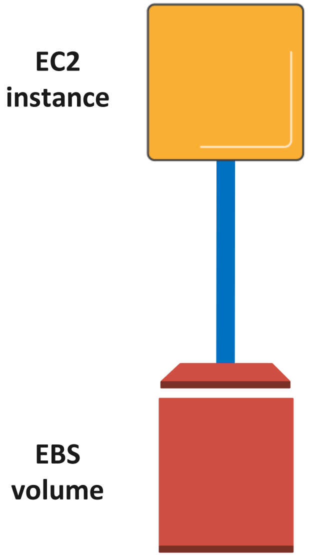
August 27, 2018

Agenda

- EBS Overview
- Snapshot Basics
- Working with Snapshots
    - Amazon Data Lifecycle Manager
    - VSS via EC2 Service Manager
    - Tag on Create, Resource-level permissions
    - Encryption
    - Copying and Sharing
- Cost Monitoring

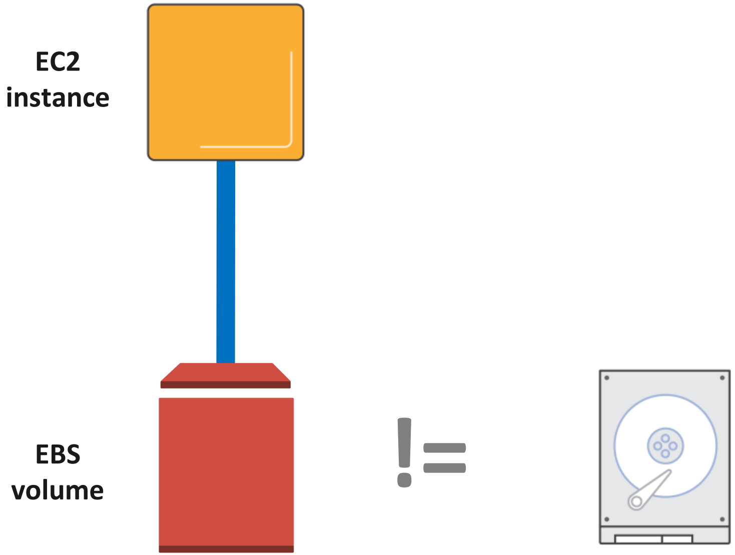
EBS Overview

What is Amazon Elastic Block Store (EBS)?



- Block storage as a service
- Create, attach, manage volumes through an API
- Service accessed over the network

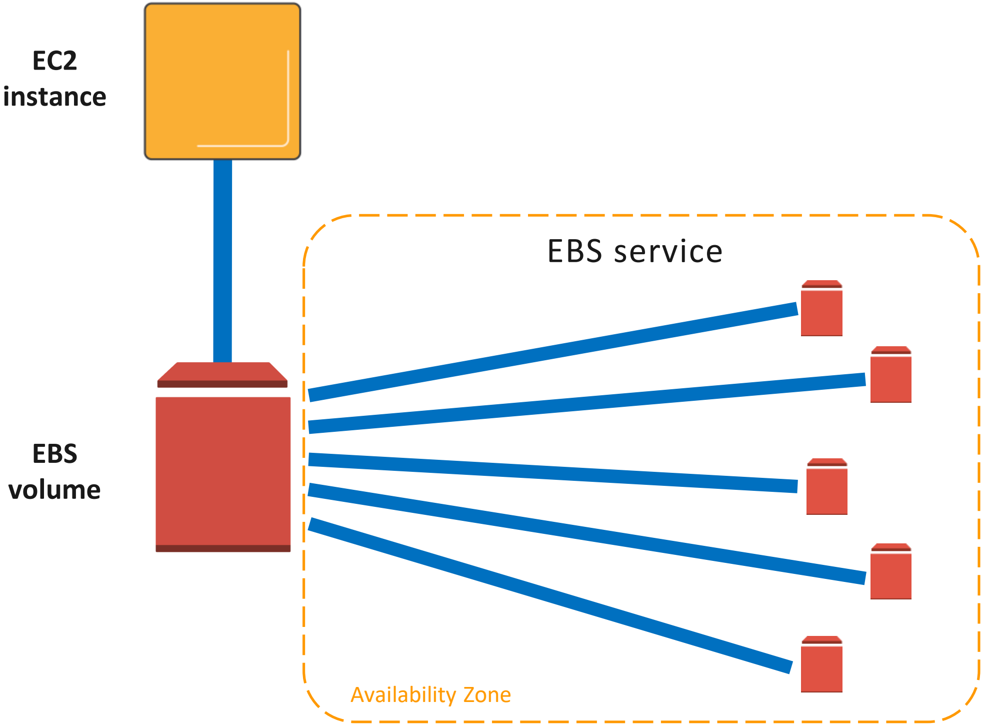
What is Amazon Elastic Block Store (EBS)?



EC2 instance

EBS volume

What is Amazon Elastic Block Store (EBS)?



Current EBS volume types

SSD

HDD

gp2

General Purpose

SSD

io1

Provisioned IOPS

SSD

st1

Throughput Optimized

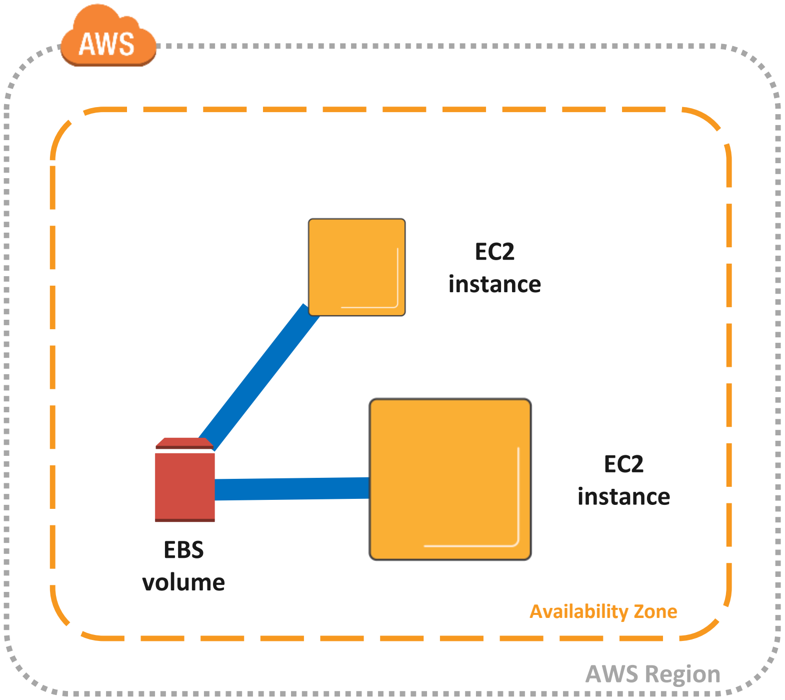
HDD

sc1

Cold

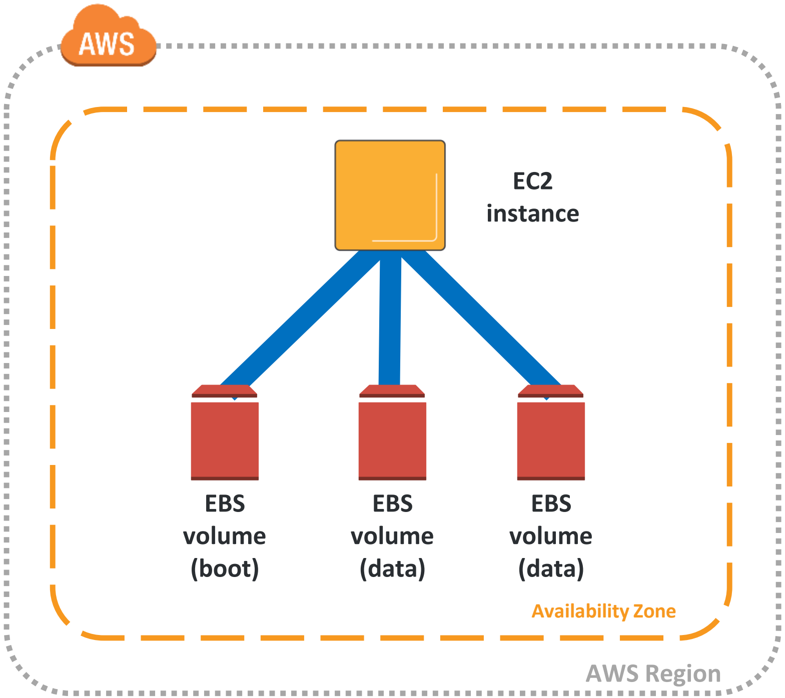
HDD

What is Amazon Elastic Block Store (EBS)?



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

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

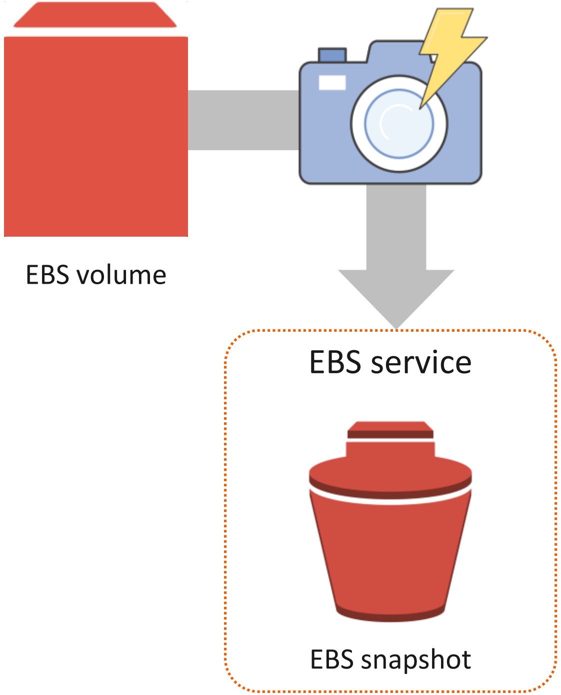
EBS is designed for…

99.999% service availability

0.1% to 0.2% annual failure rate (AFR)

EBS Snapshot Basics

What is an EBS snapshot?



- Point-in-time backup of an EBS volume
- Incremental – only changed blocks are saved
- Stored in S3 (11x 9’s of durability) - accessed via EBS APIs
- Crash consistent
- Contains all information necessary to restore a volume

Why use EBS snapshots?

- Backup data on EBS volumes
- Meet Recovery Point Objectives (RPO)
- Copy volumes within or across Availability Zones
- Copy volumes to another region for Disaster Recovery
- Capture production data for test/dev
- Create Amazon Machine Images (AMIs)

Individual EBS snapshots are crash consistent

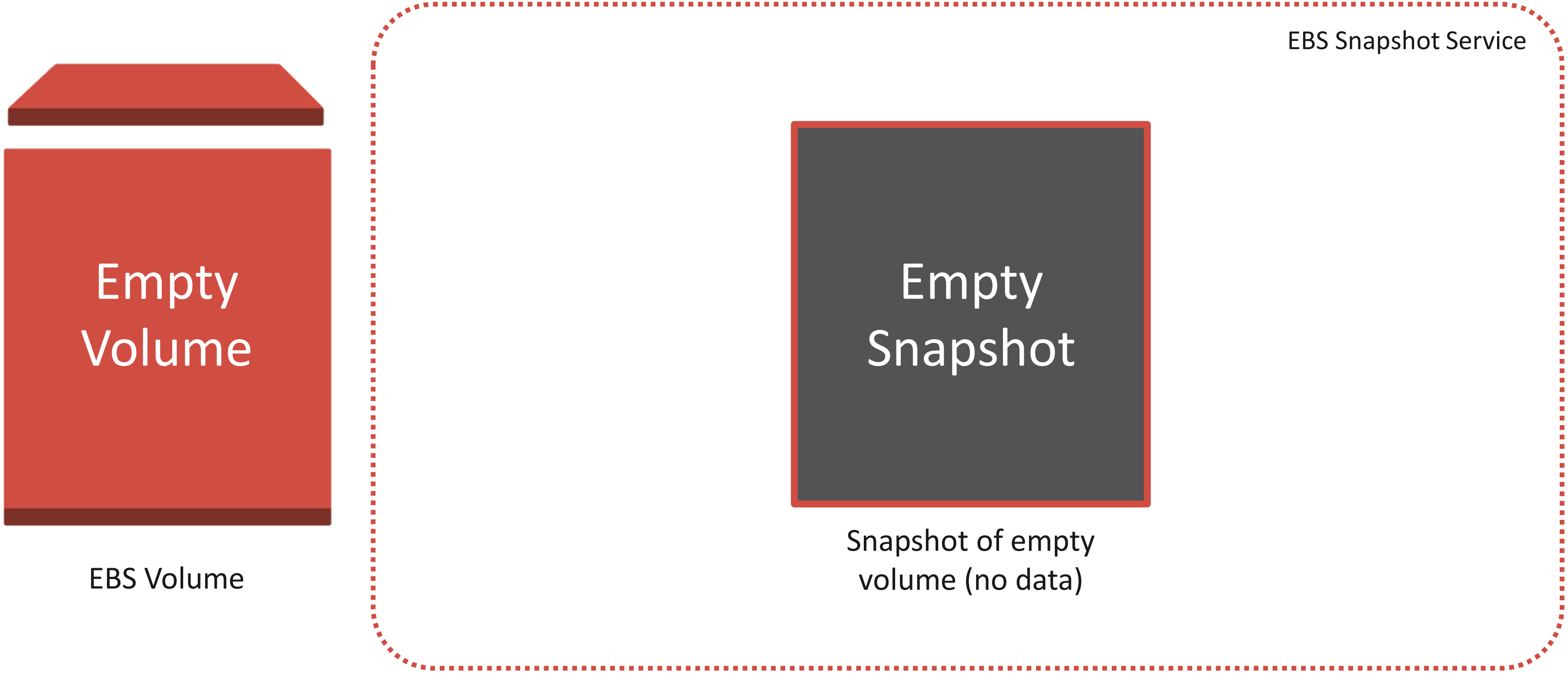
Crash consistency

- Snapshot contains all blocks written to disk at the time of the snapshot
- Data not flushed to disk does not exist in the snapshot
- Similar to pulling the power cord of the server

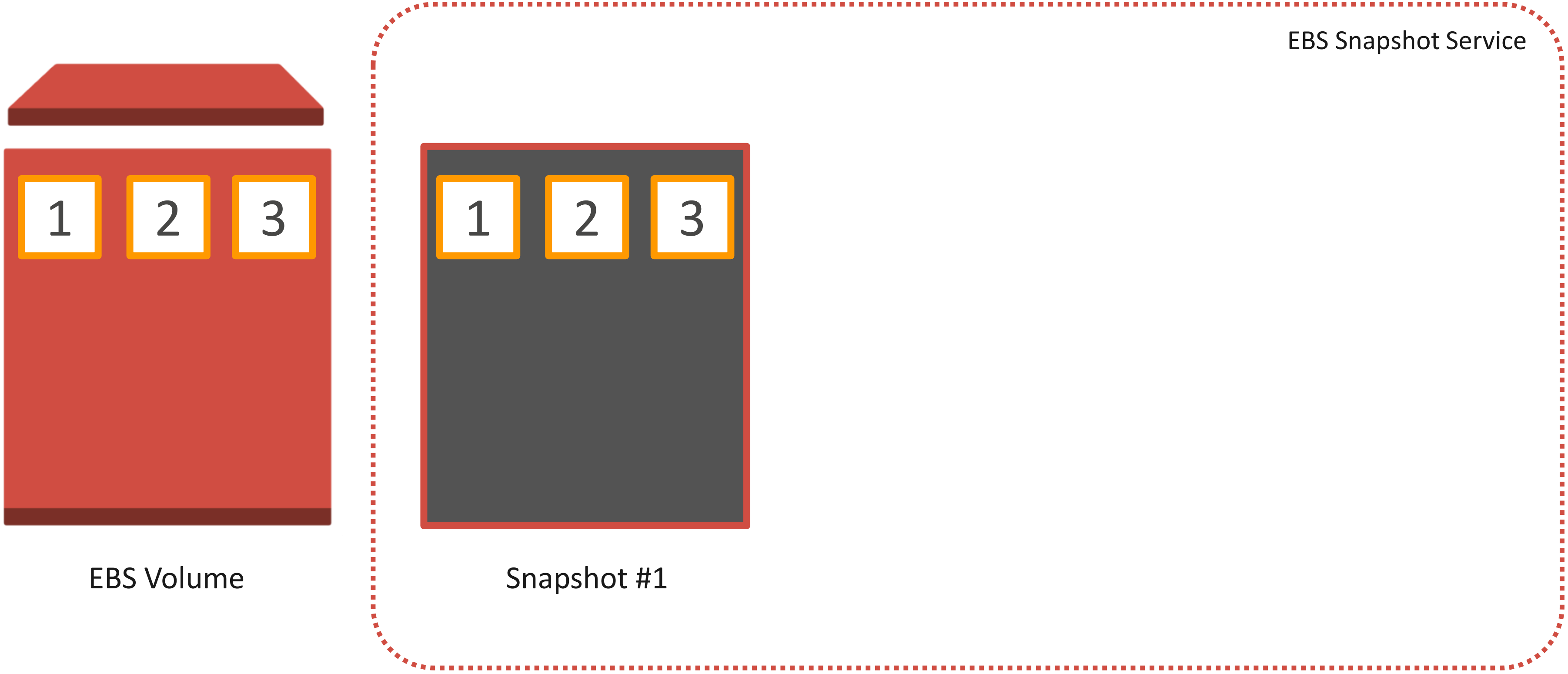
Application consistency

- Writes to application(s) are halted during the snapshot creation process
- Application data is flushed to disk prior to snapshot creation
- Unfreeze/unlock as soon as snapshot creation command is executed.
- Available on Windows instances using Run command and VSS

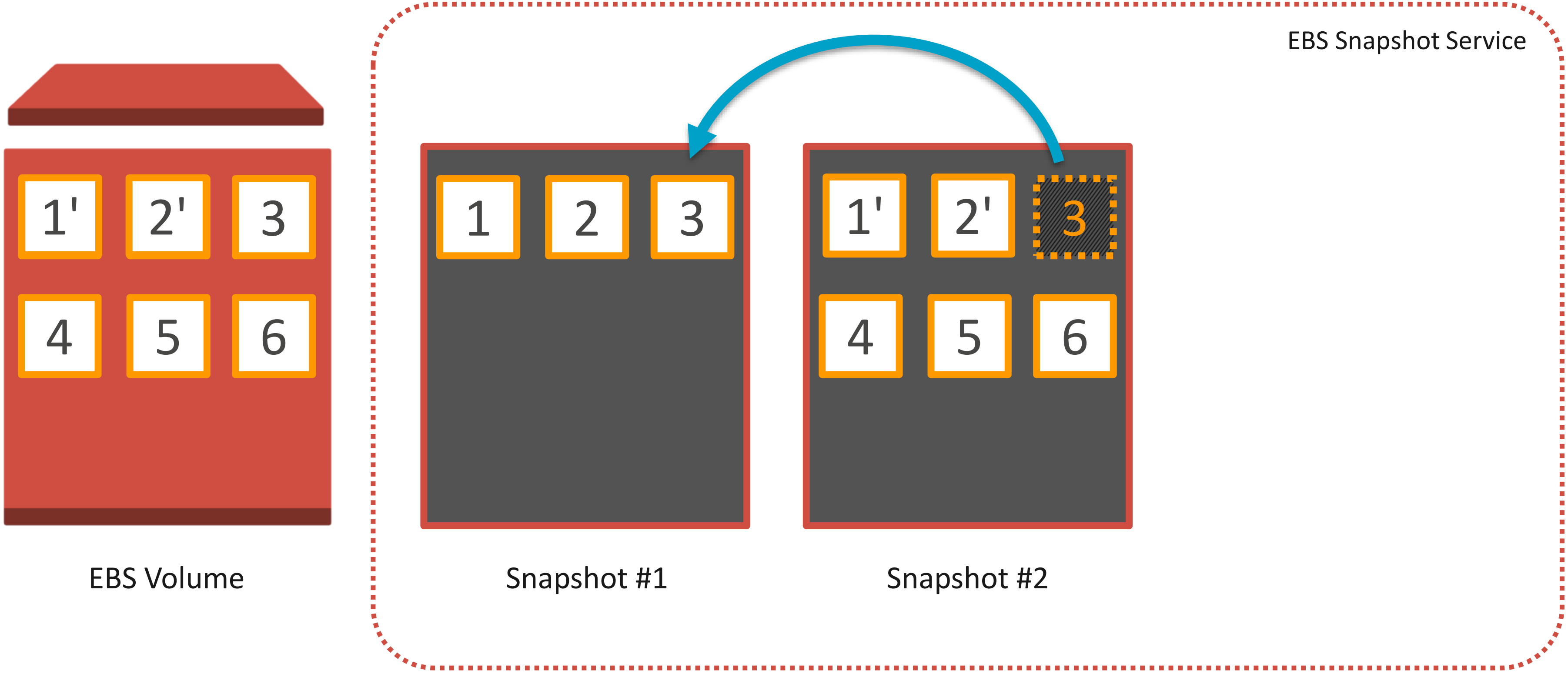
How does an EBS snapshot work?



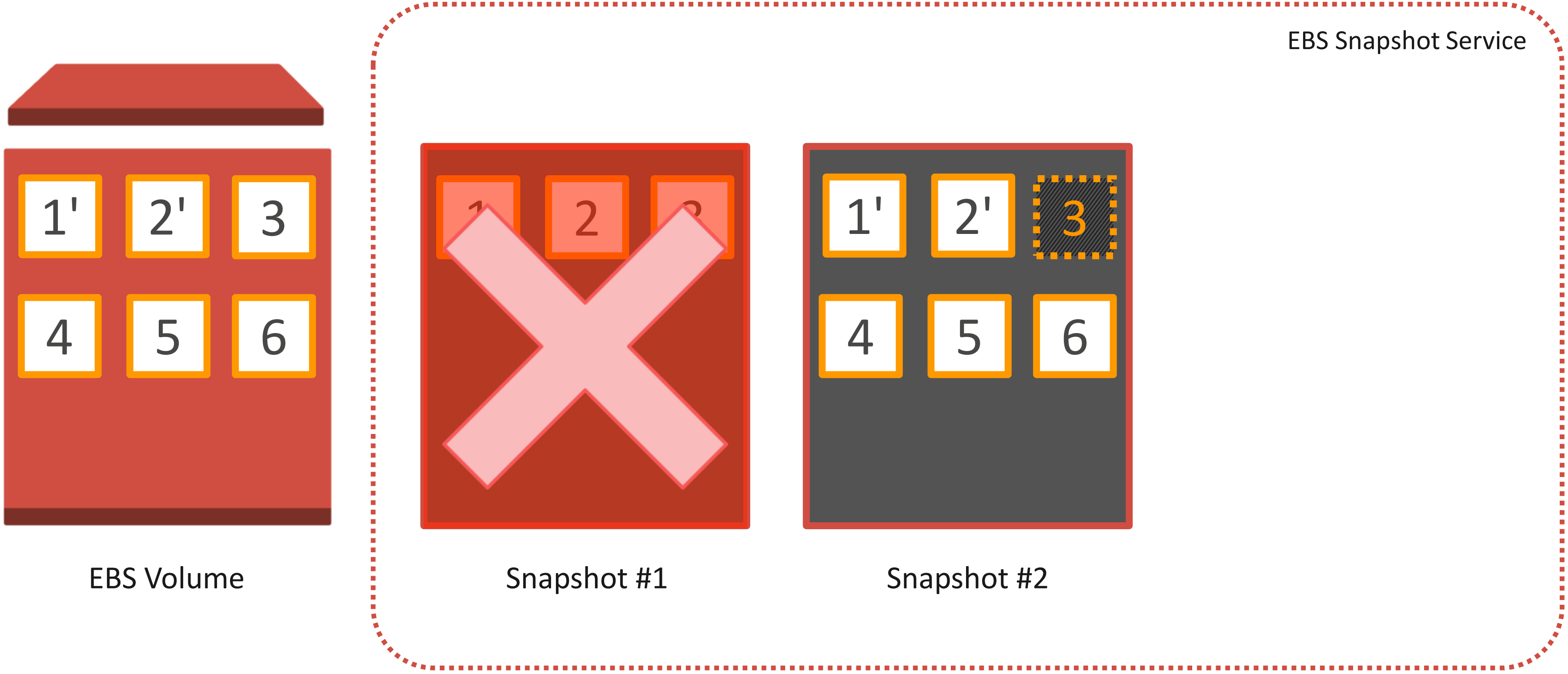
How does an EBS snapshot work?



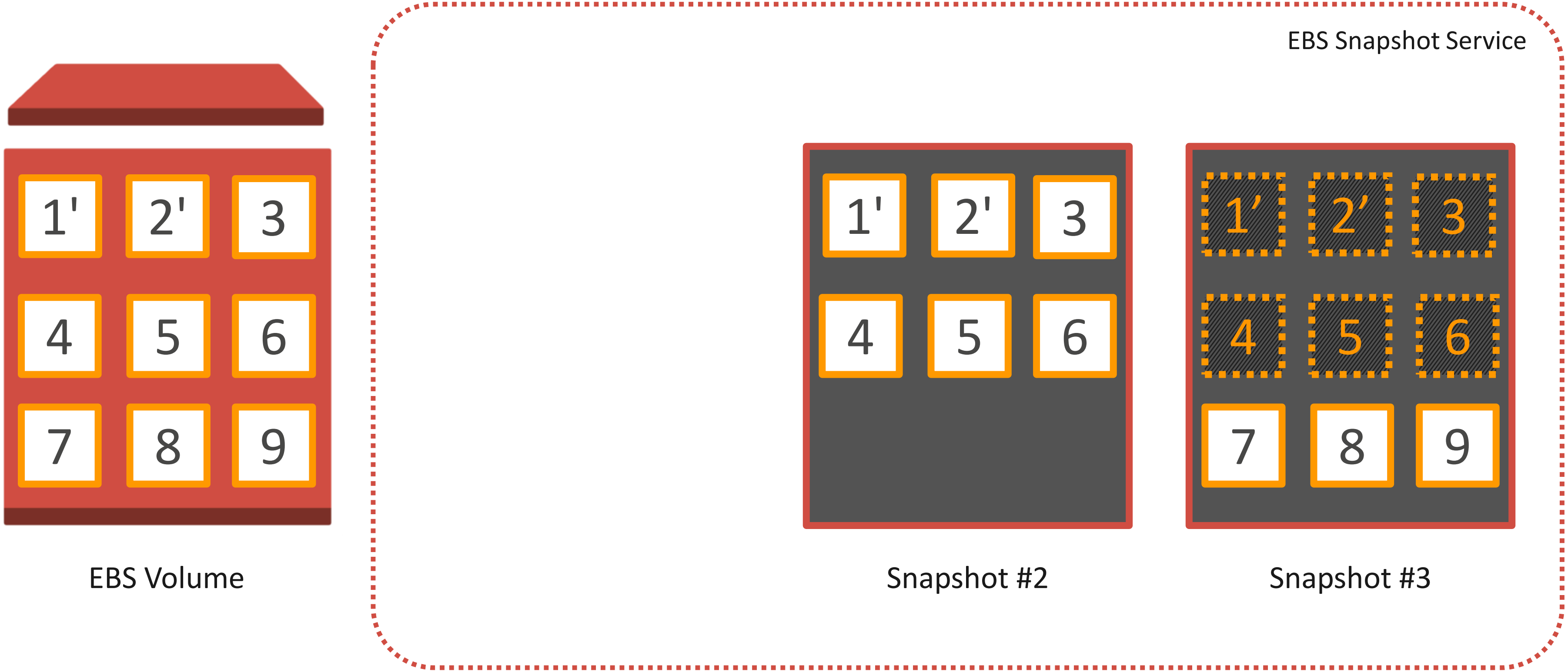
How does an EBS snapshot work?



How does an EBS snapshot work?



How does an EBS snapshot work?



EBS Snapshot Service

EBS Volume

Snapshot #2

Snapshot #3

Working with Snapshots

How to create EBS snapshots

Manually

Create EBS snapshots manually using the AWS Management Console, CLI or API

Amazon Data Lifecycle Manager (DLM)

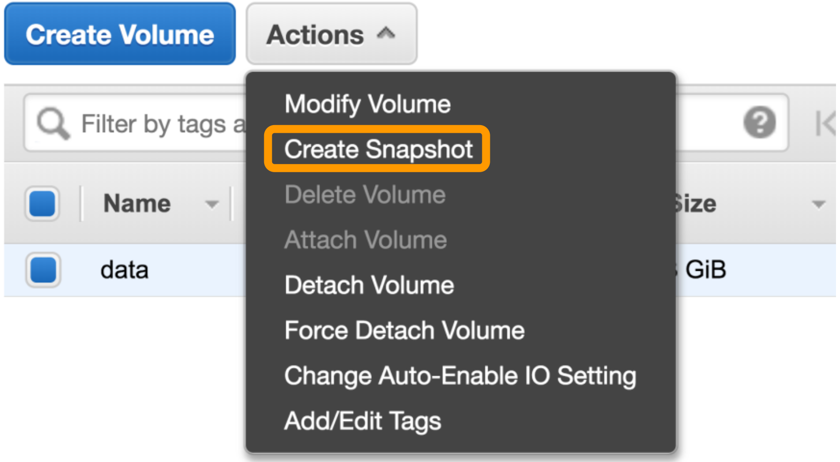
Automatically create and retain EBS snapshots using DLM policies

VSS on Windows

Use Service Manager Run command to take EBS snapshots using Windows VSS

Manually create a snapshot

```
aws ec2 create-snapshot
  --volume-id vol-00077cd243d4af642
  --description ”data before resize”
  --tag-specifications
    'ResourceType=snapshot,
     Tags=[{Key=CostCenter,Value=115},
           {Key=IsProd,Value=Yes}]'
```

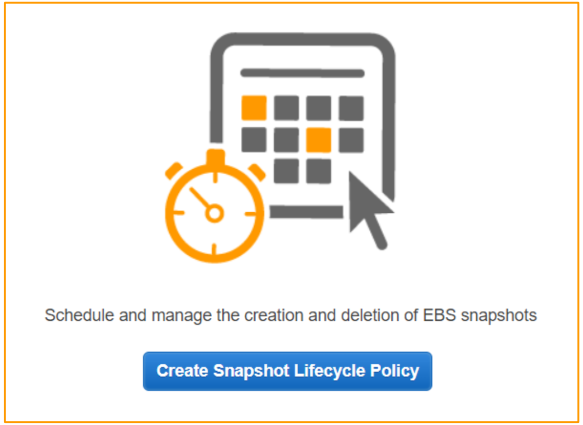


New: Amazon Data Lifecycle Manager

New!

Simple, automated way to back up data stored on EBS volumes by ensuring that EBS snapshots are created and deleted on a custom schedule.

- Define policies for regular backup schedules
- Retain backups for compliance/audit purposes
- Control snapshot costs by automatically deleting old backups
- Identify volumes to backup using tags
- Use IAM to control DLM policy access
- No cost to use



Schedule and manage the creation and deletion of EBS snapshots

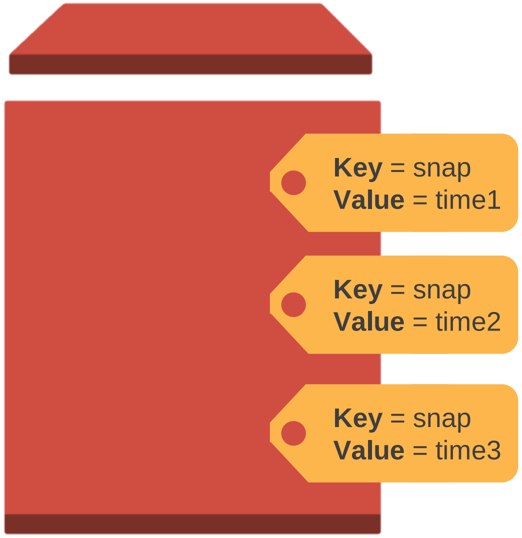
New: Amazon Data Lifecycle Manager

Use policies to set backup and retention schedules

Customer Requirement	Data Lifecycle Policy	
"All EC2 instance root volumes will be backed up once per day, saved for 7 days."	**Tags:**	voltype:root
	Create:	every 24 hours
	Start Time:	0700 UTC
	Retention:	most recent 7
"All Finance and Accounting data volumes are backed up every 12 hours and retained for 10 days."	**Tags:**	dept:finance, dept:accounting
	Create:	every 12 hours
	Start Time:	0900 UTC
	Retention:	most recent 20

New: Amazon Data Lifecycle Manager

Use multiple policies to snapshot more often than 12 or 24 hours



EBS Volume

Policy #1

Tags:	snap:time1
Create:	every 24 hours
Start Time:	0000 UTC
Retention:	most recent 7

Policy #2

Tags:	snap:time2
Create:	every 24 hours
Start Time:	0800 UTC
Retention:	most recent 7

Policy #3

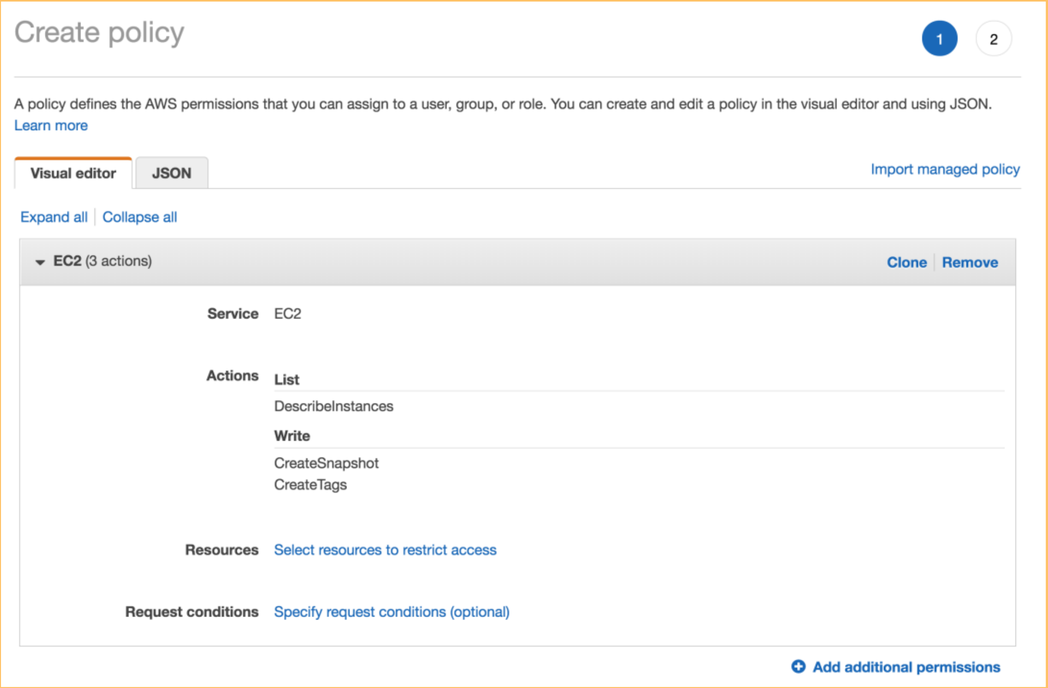
Tags:	snap:time3
Create:	every 24 hours
Start Time:	01600 UTC
Retention:	most recent 7

Amazon Data Lifecycle Manager - Things to know

- A lifecycle policy applies to any of the tags specified
- A tag cannot be used with multiple policies
- Snapshots will be taken within one hour of the configured start time
- Backup periods currently every 12 or 24 hours
- DLM will apply AWS tags on snapshot creation for easier management

VSS support via EC2 SSM

- Use Policy Generator to create IAM policy for AWS service, AWS Systems Manager
- *Actions: DescribeInstances, CreateTags, and CreateSnapshot*
- *Create Amazon EC2 type IAM role and attach to Windows instances*



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

EC2 (3 actions)

Service EC2

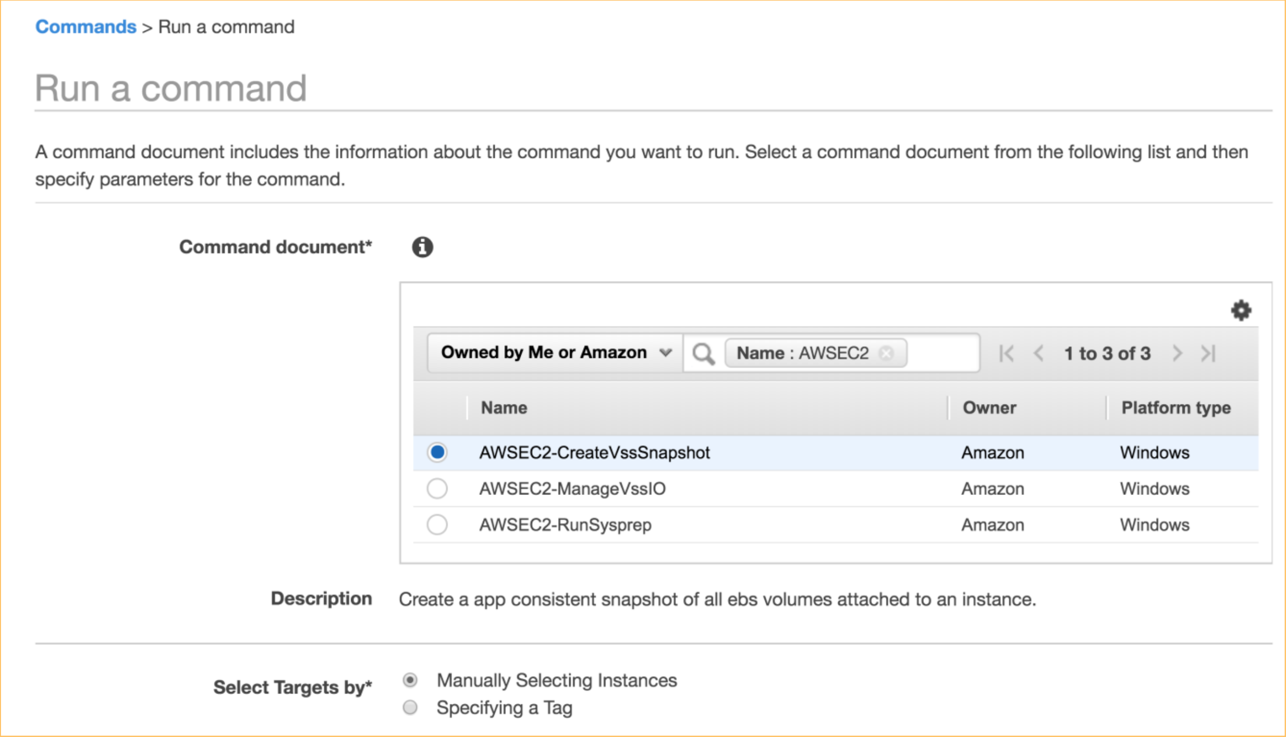
Actions
List
DescribeInstances
Write
CreateSnapshot
CreateTags

Resources Select resources to restrict access

Request conditions Specify request conditions (optional)

VSS support via EC2 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*

	Name	Owner	Platform type
●	AWSEC2-CreateVssSnapshot	Amazon	Windows
○	AWSEC2-ManageVssIO	Amazon	Windows
○	AWSEC2-RunSysprep	Amazon	Windows

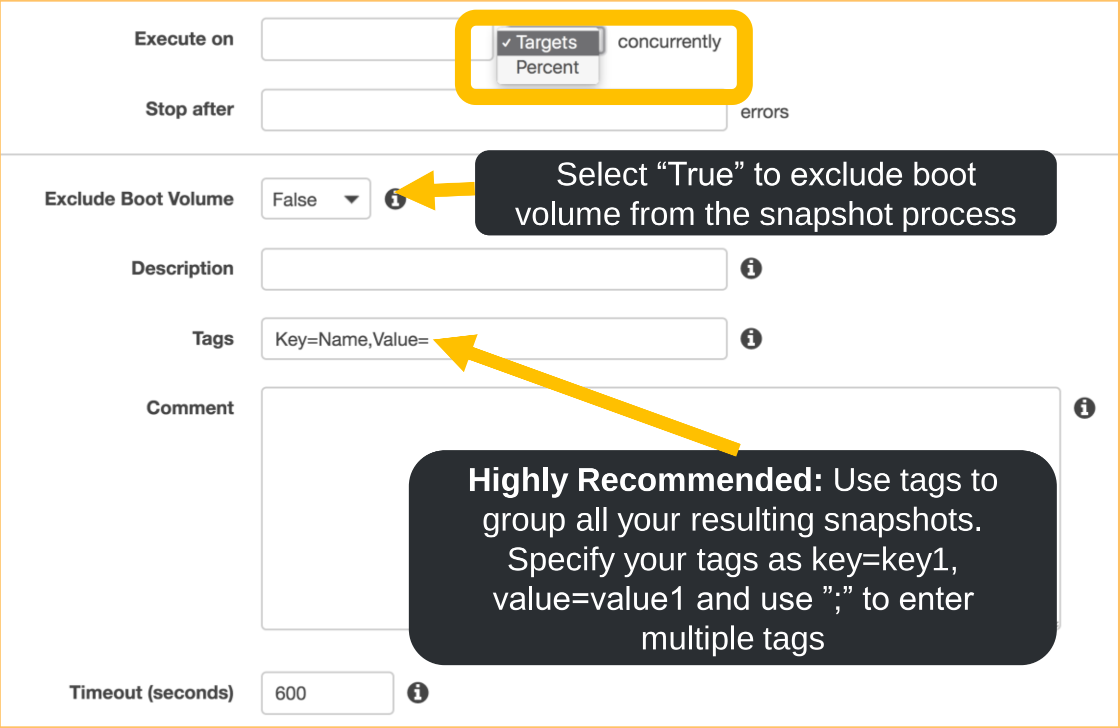
Description Create a app consistent snapshot of all ebs volumes attached to an instance.

Select Targets by*

● Manually Selecting Instances
○ Specifying a Tag

VSS support via EC2 SSM

1. Select the instance
2. Add description, tags
3. Can exclude boot volume
4. Run Command makes the VSS agent freeze and flush I/O



Execute on ✓ Targets / Percent concurrently

Stop after errors

Exclude Boot Volume: False

Description:

Tags: Key=Name,Value=

Comment:

Timeout (seconds): 600

Select “True” to exclude boot volume from the snapshot process

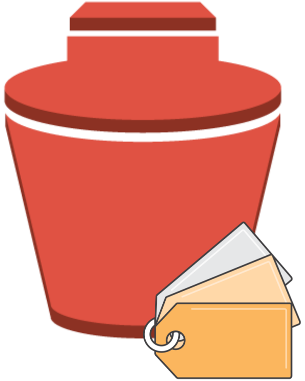
Highly Recommended: Use tags to group all your resulting snapshots. Specify your tags as key=key1, value=value1 and use ”;” to enter multiple tags

SSM VSS included in Microsoft Windows Server AMI version 2017.11.21 & up

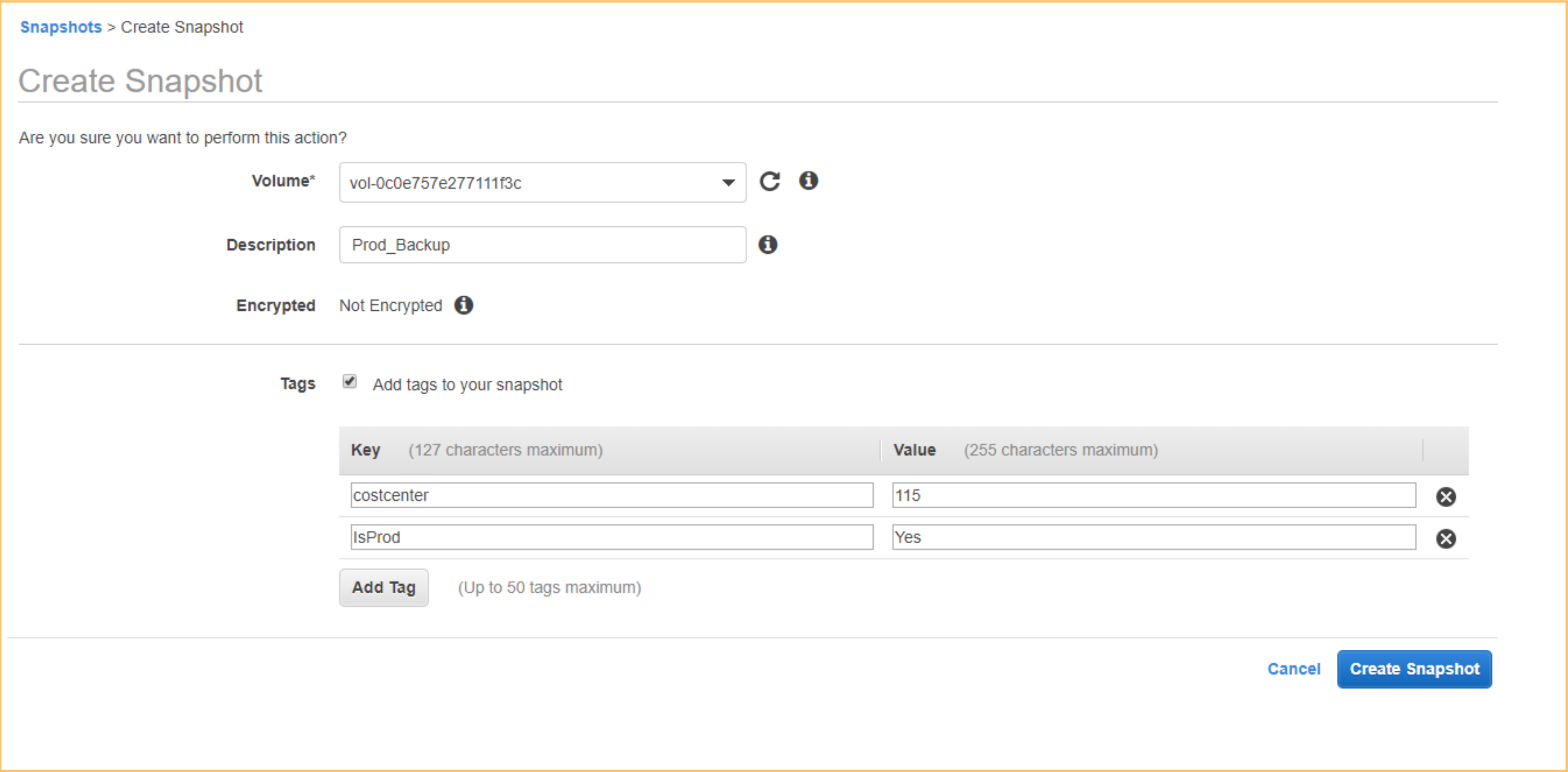
New: Tag EBS snapshots on creation

New!

- EBS volumes and snapshots support tagging on creation
- Resource tagging is an atomic operation
- Tag on resource creation ensures that resources are properly tracked, monitored and enforced from the moment of creation
- No longer need to build tagging scripts that run after EBS snapshots have been created



New: Tag EBS snapshots on creation



Snapshots > Create Snapshot

Create Snapshot

Are you sure you want to perform this action?

Volume* vol-0c0e757e277111f3c

Description Prod_Backup

Encrypted Not Encrypted

Tags ☑ Add tags to your snapshot

Key (127 characters maximum)	**Value** (255 characters maximum)
costcenter	115
IsProd	Yes

New: Resource-level permissions

IAM policies can mandate the use of specific tags when taking actions on EBS snapshots

New!

Supported on the following APIs:

- `CreateSnapshot`
- `DeleteSnapshot`
- `ModifySnapshotAttribute`

Use Cases

- Require use of specific tags
- Specify which users can take snapshots for a given set of volumes
- Restrict access to delete snapshots

New: Resource-level permissions

Example: allow the deletion of a snapshot only if the snapshot is tagged with User:*username*

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":"ec2:DeleteSnapshot",
            "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
            "Condition":{
                "StringEquals":{
                    "ec2:ResourceTag/User":"${aws:username}"
                }
            }
        }
    ]
}
```

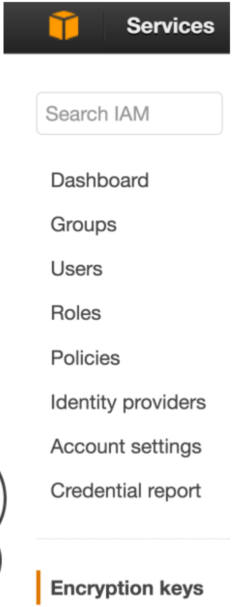
Creating snapshots - Things to know

- Snapshots live in the region in which they were created
- Snapshot creation does not impact EBS volume performance
- Avoid simultaneous snapshots on a single volume
- Use Amazon Data Lifecycle Manager to automate creation and retention of snapshots
- Use tags to manage, organize and secure snapshots

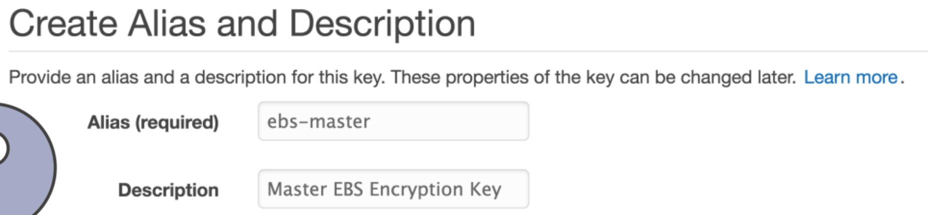
EBS snapshot encryption

- Snapshots of encrypted volumes are automatically encrypted.
- Volumes that are created from encrypted snapshots are automatically encrypted.
- EBS creates a default CMK for encrypting volumes and snapshots or use a custom CMK.
- 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.

EBS snapshot encryption – Best practices



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) ebs-master

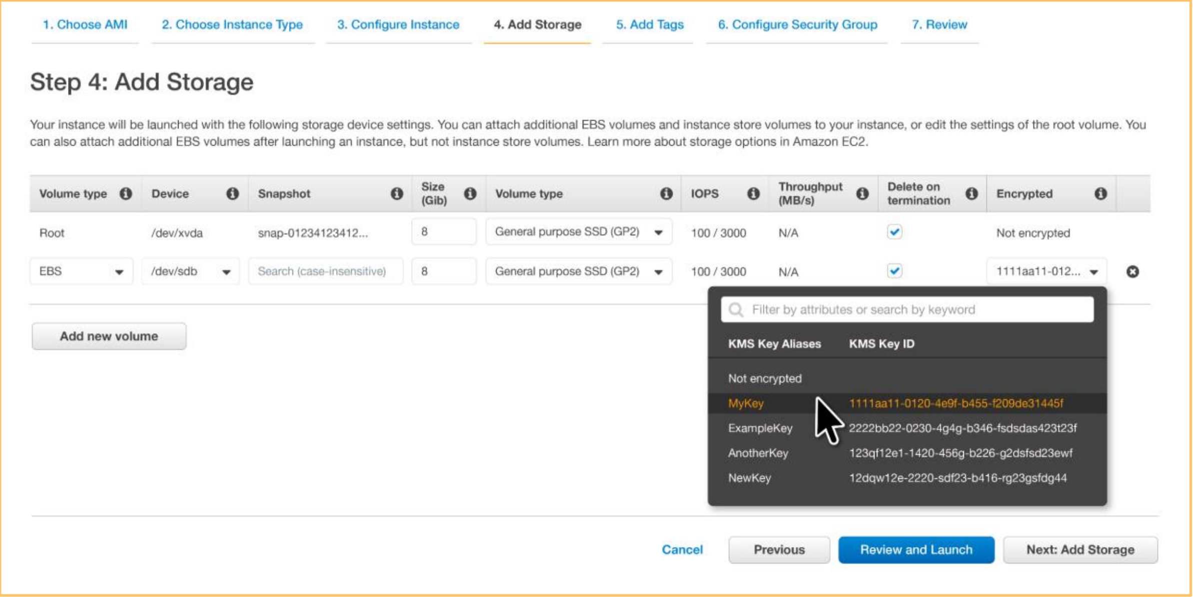
Description Master EBS Encryption Key

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

New: RunInstances with custom CMK

New!

EBS encryption: data volumes



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	Encrypted
Root	/dev/xvda	snap-01234123412...	8	General purpose SSD (GP2)	100 / 3000	N/A	☑	Not encrypted
EBS	/dev/sdb	Search (case-insensitive)	8	General purpose SSD (GP2)	100 / 3000	N/A	☑	1111aa11-012...

Filter by attributes or search by keyword

KMS Key Aliases	KMS Key ID
Not encrypted	
MyKey	1111aa11-0120-4e9f-b455-f209de31445f
ExampleKey	2222bb22-0230-4g4g-b346-fsdsdas423t23f
AnotherKey	123qf12e1-1420-456g-b226-g2dsfsd23ewf
NewKey	12dqw12e-2220-sdf23-b416-rg23gsfdg44

Copying snapshots - Things to know

- Snapshots must be in Complete state before they can be copied
- Snapshots copied within a region are free as long as the encryption state doesn't change and both copies use the same CMK.
- The first copy to another region is always a full copy
- Snapshots are incremental after the first copy
  - For encrypted snapshots the same CMK must be used on both ends in order to get incremental copies.
- Tags on snapshots are not copied

Sharing EBS snapshots

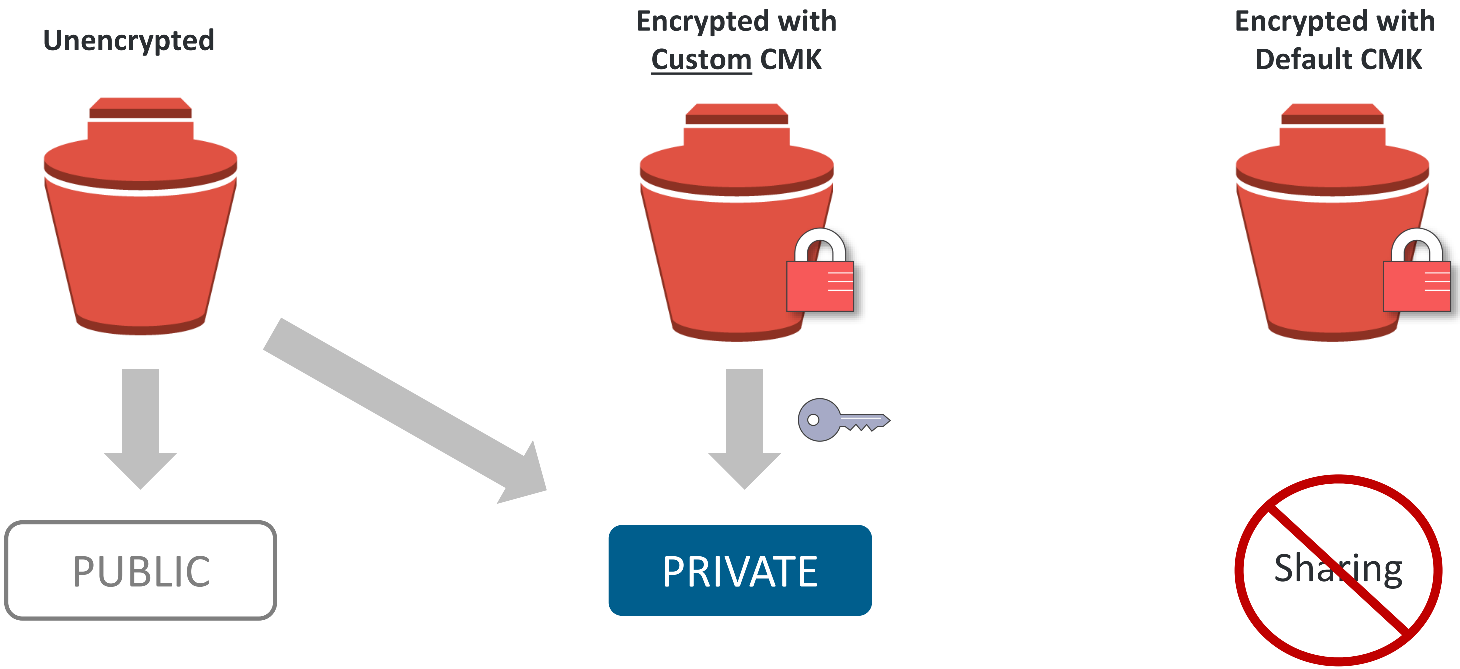
Sharing a snapshot means giving other accounts permission to do **two** things:

- Make a copy of the snapshot
- Create a volume from the snapshot

Use Cases

- Share custom AMIs
- Share snapshots with test/dev accounts for testing
- Share with restricted accounts for long-term archive

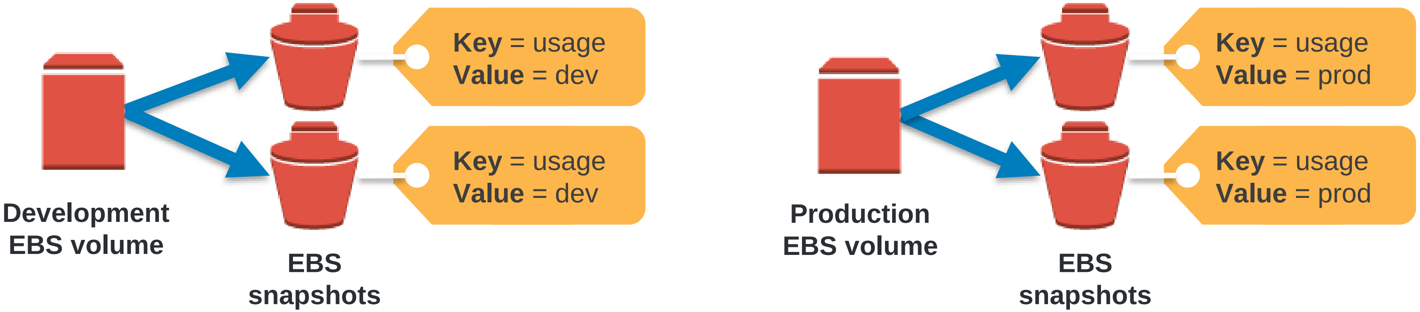
Sharing EBS snapshots



Cost Monitoring

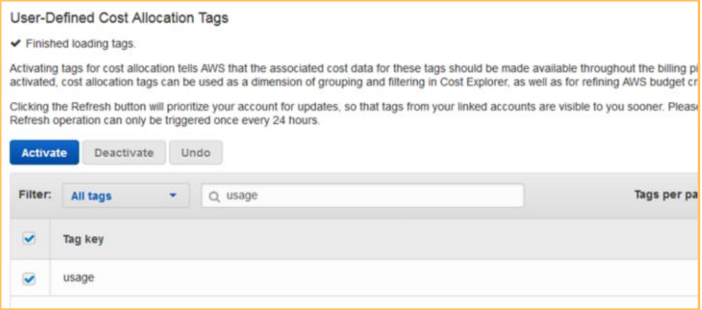
Tracking snapshot costs - Tagging

- Custom tags provide the ability to assign key/value pairs to AWS resources
- Amazon EBS snapshots support custom tags for identification and management
- Amazon EBS snapshot tags can be activated as “cost allocation” tags allowing for greater visibility into snapshot storage costs



Tracking snapshot costs – Cost Explorer

First, activate custom tags for cost allocation



User-Defined Cost Allocation Tags

✓ Finished loading tags.

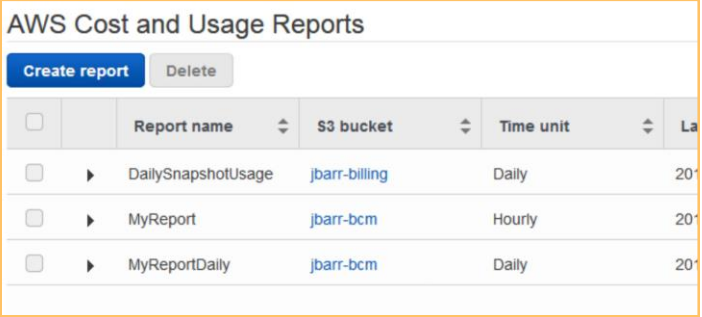
Activating tags for cost allocation tells AWS that the associated cost data for these tags should be made available throughout the billing pi activated, cost allocation tags can be used as a dimension of grouping and filtering in Cost Explorer, as well as for refining AWS budget cr

Clicking the Refresh button will prioritize your account for updates, so that tags from your linked accounts are visible to you sooner. Pleas Refresh operation can only be triggered once every 24 hours.

Filter: All tags | usage | Tags per pa

☑	Tag key
☑	usage

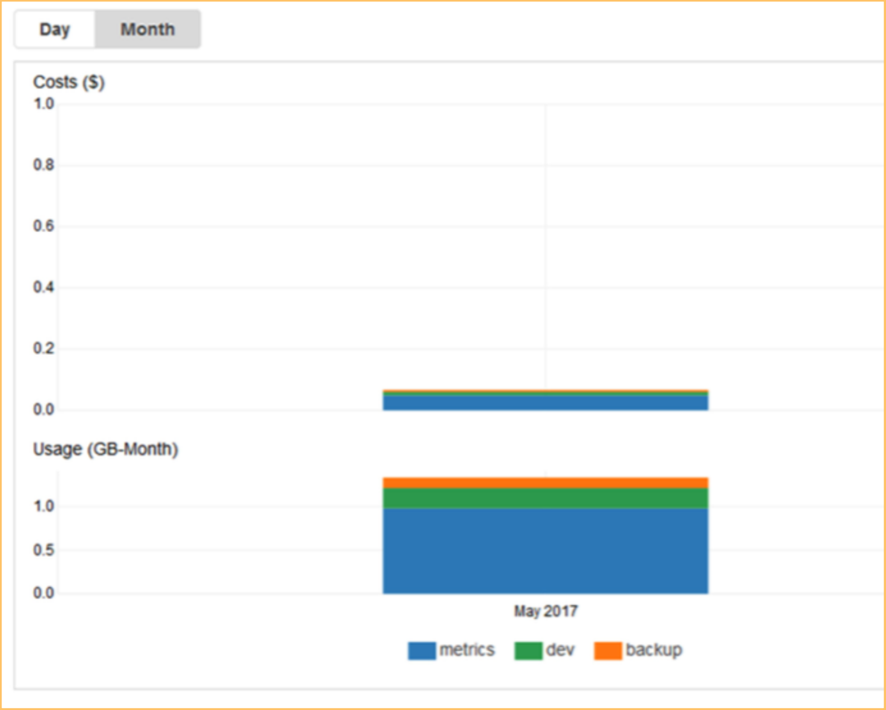
Generate reports…



AWS Cost and Usage Reports

□		Report name	S3 bucket	Time unit	La
□	▸	DailySnapshotUsage	jbarr-billing	Daily	201
□	▸	MyReport	jbarr-bcm	Hourly	201
□	▸	MyReportDaily	jbarr-bcm	Daily	201

View usage and costs broken down by “usage” tag value



Wrap Up

Summary

- Snapshots are incremental
- New: Amazon Data Lifecycle Manager for EBS snapshots
- VSS via EC2 SSM
- New: Tag on Create
- New: Resource-level permissions
- Use custom CMKs for encryption
- Use tags for management and cost monitoring

Thank You!