Deep Dive: Protect Mission- Critical Workloads with Amazon EBS

Eric Jones

Sr Manager, Product Management
Amazon EBS Snapshots

Agenda

- Introduction to the EBS Storage portfolio
- AWS resilience
- EBS volumes and snapshots
- EBS encryption and security
- Restoring from EBS Snapshots
- EBS Snapshot use cases
- Automating data protection and enhanced monitoring

EBS Storage Portfolio

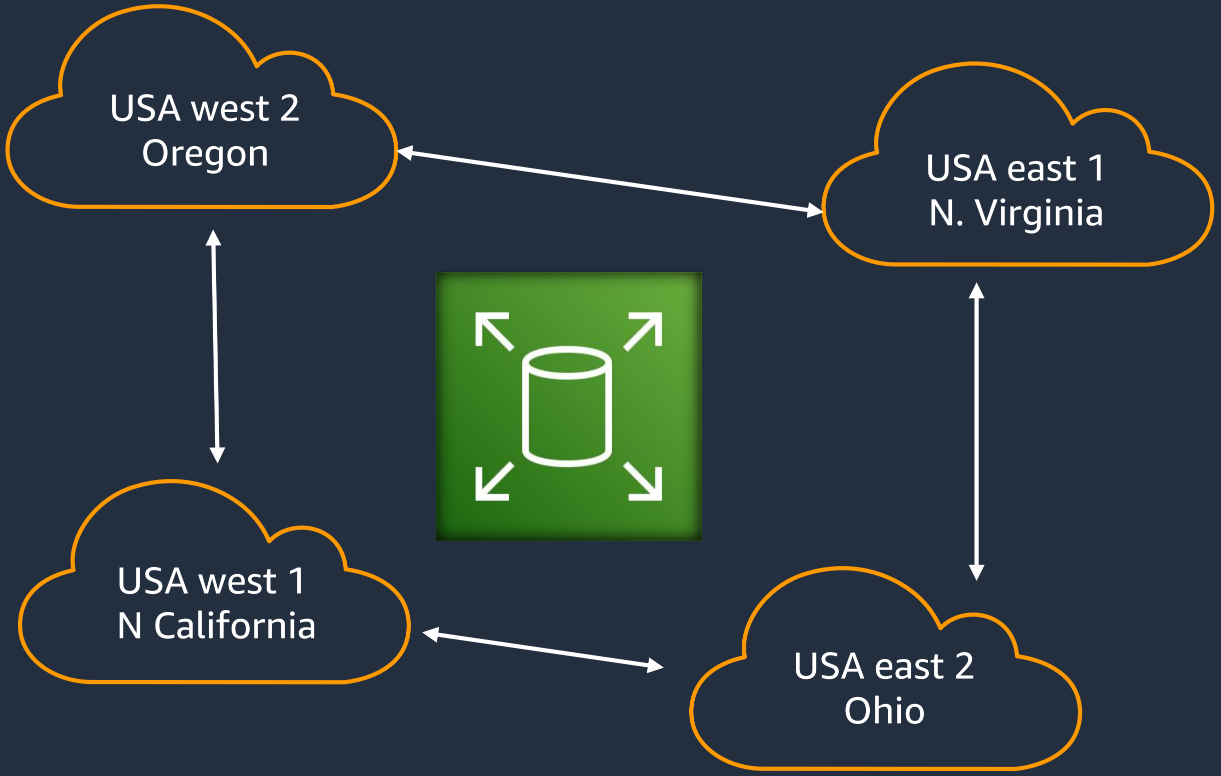
EBS Volumes

Easy to use, high performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction intensive workloads

EBS Snapshots

Incremental, point-in-time copies of your EBS data that can be used to restore new volumes, expand the size of a volume, or move volumes across Availability Zones

AWS Resilience

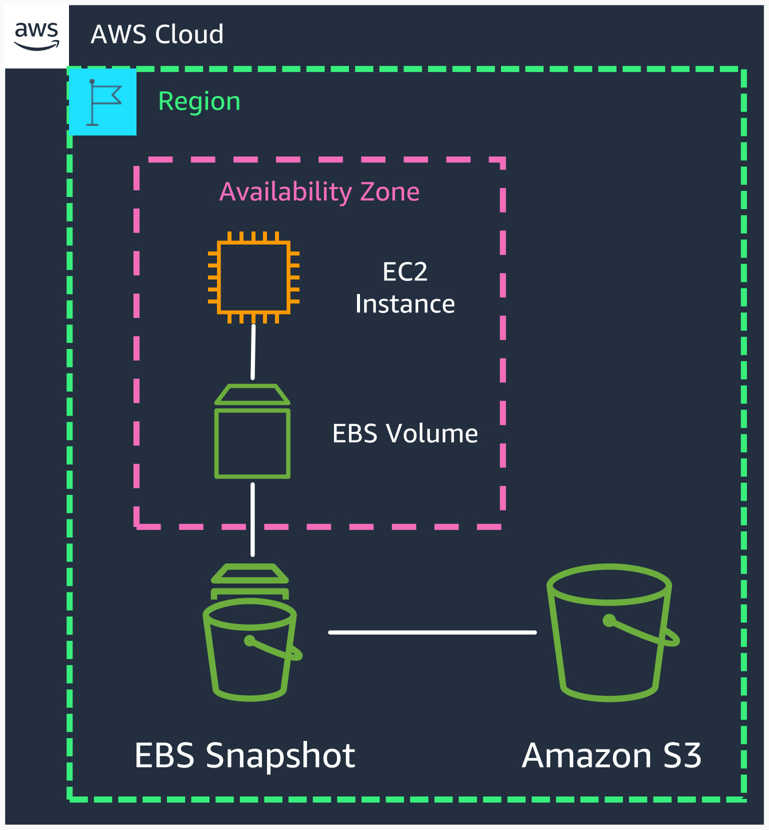


- 26 regions (2X more than the next largest cloud provider), each with multiple availability zones
- 84 availability zones provide high availability

EBS Volume Types

	SSD-backed volumes			HDD-backed volumes	
	gp3 General Purpose	io2 Provisioned IOPS	io2 BX Provisioned IOPS	st1 Throughput Optimized	sc1 Cold
Use-cases	Relational and non-relational databases, enterprise applications, containerized workloads, big data, file system, media workflows	Large database workloads, mission-critical business applications requiring sustained high performance	Critical applications and databases requiring sustained IOPS	Big data workloads, data warehouses, log processing, streaming workloads	Large volumes of infrequently accessed data, cost-sensitive workloads
Volume Size	1 GB – 16 TB	4 GB – 16 TB	4 GB – 64 TB	125 GB – 16 TB	125 GB – 16 TB
Max IOPS per volume	16,000	64,000	256,000	500	250
Max Throughput per volume	1,000 MB/s	1,000 MB/s	4,000 MB/s	500 MB/s	250 MB/s

What are EBS Snapshots?



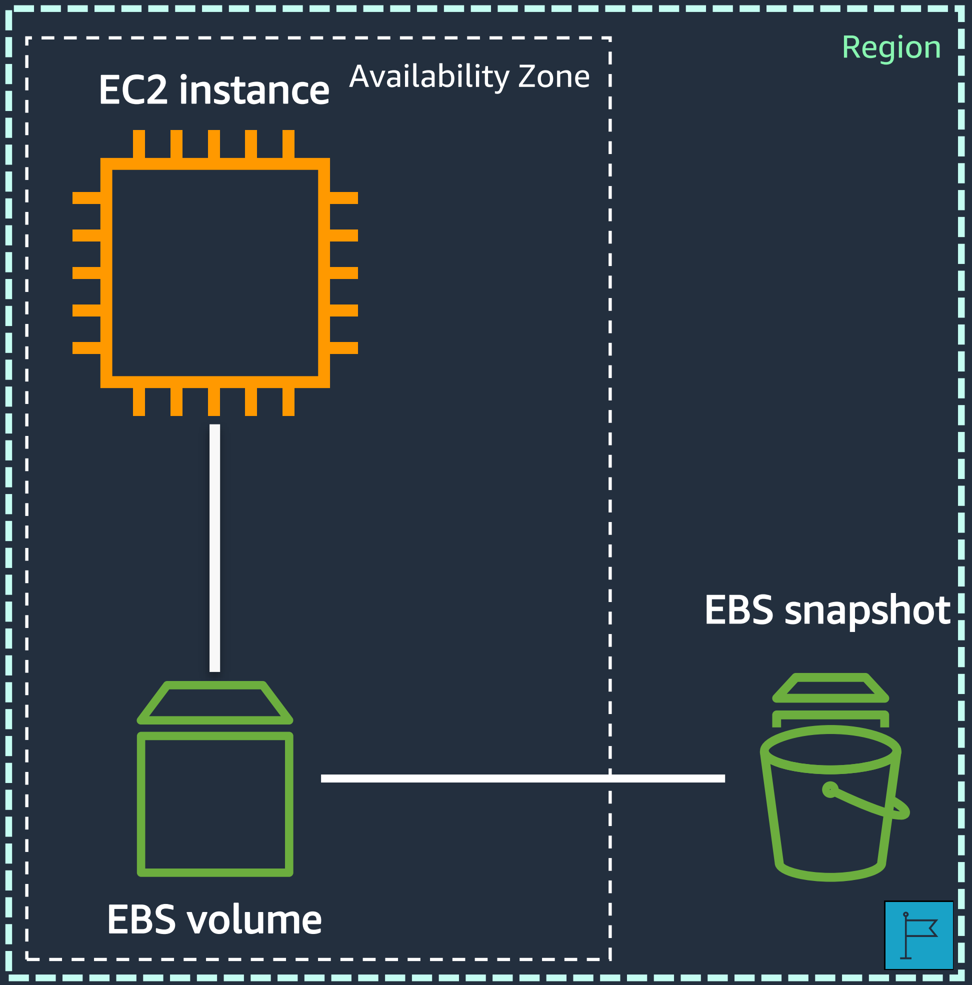
EBS backup and disaster recovery

Refresh, scale-up, data handoff workflows

Non-EBS backup and migration

- Point-in-time backups of EBS Volumes
- Stored on Amazon S3
- Properties:
  - Incremental – only changed blocks stored
  - Crash consistent – completed I/O’s persisted in next snapshot
  - Can be securely shared and copied across accounts and regions

EBS Snapshots - differences from EBS volumes



- Shared across accounts
- Copied across accounts
- Copied within accounts
- Copied across Regions
- Create AMIs

EBS Snapshots are crash consistent

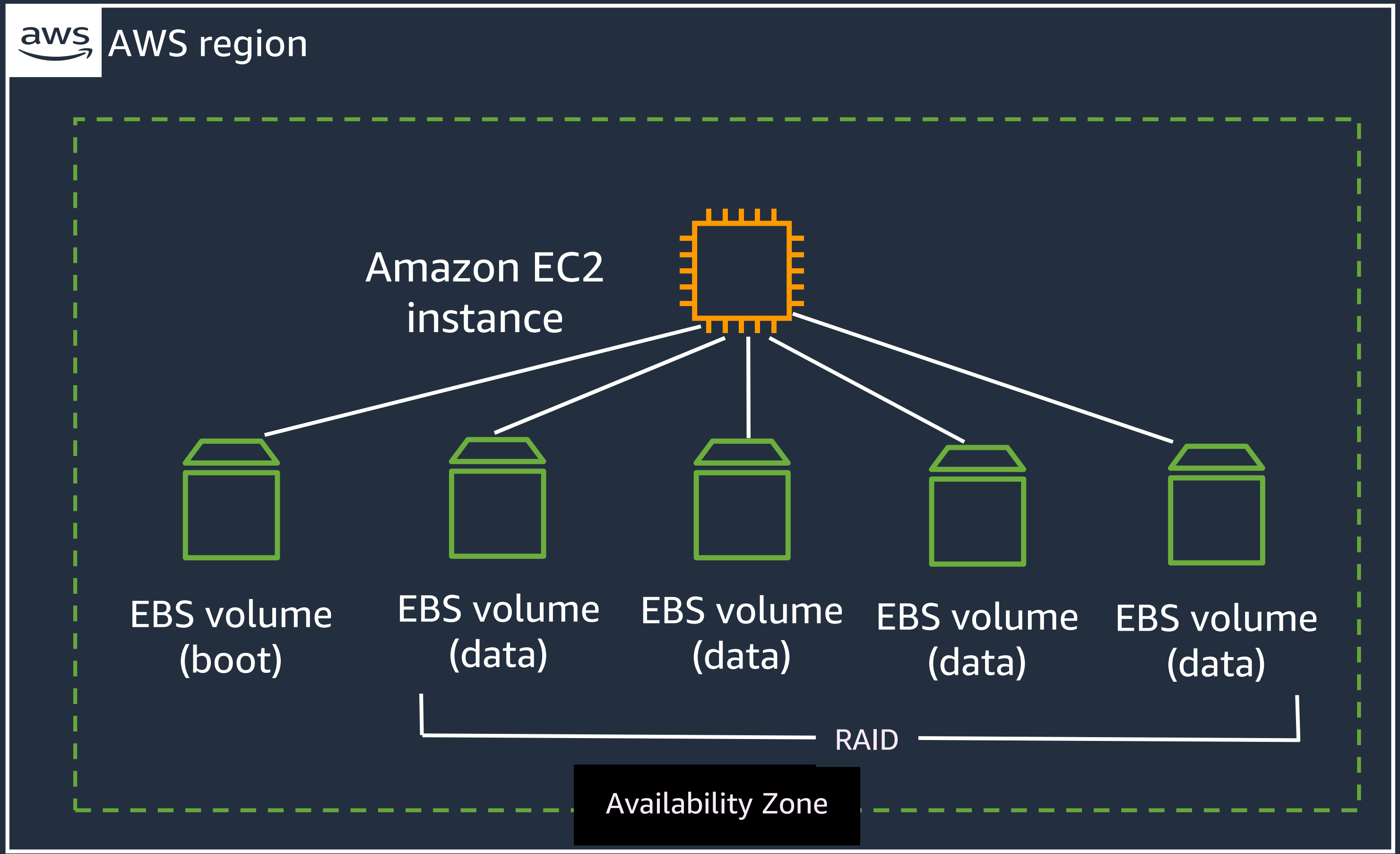
Crash consistency

- 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 completed

EBS multi-volume crash-consistent snapshots



One instance can have many volumes attached

Volumes attach to one instance

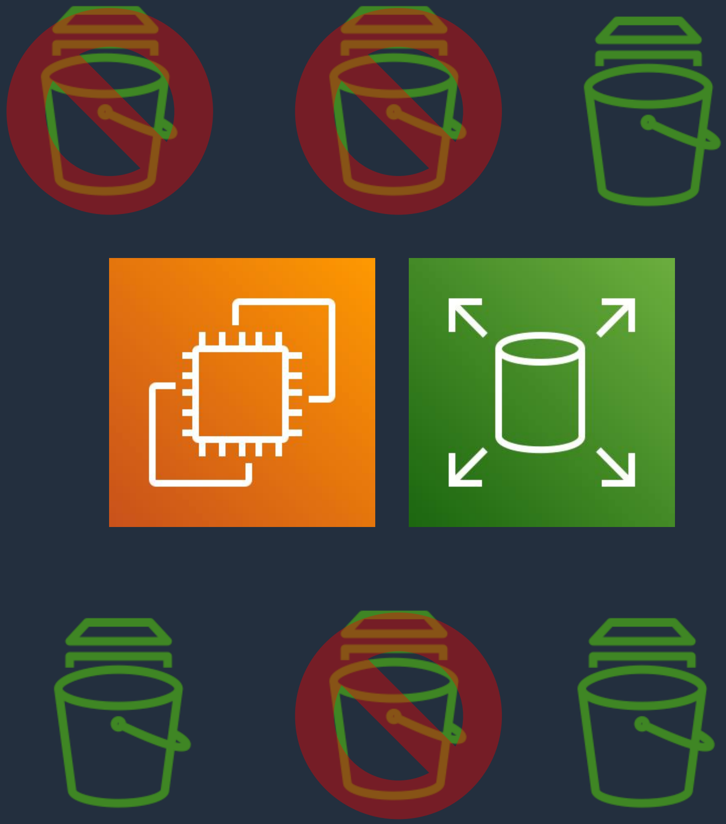
Best practice

- Separate boot and data volumes
- Snapshot regularly

https://docs.aws.amazon.com/cli/latest/reference/ec2/create-snapshots.html

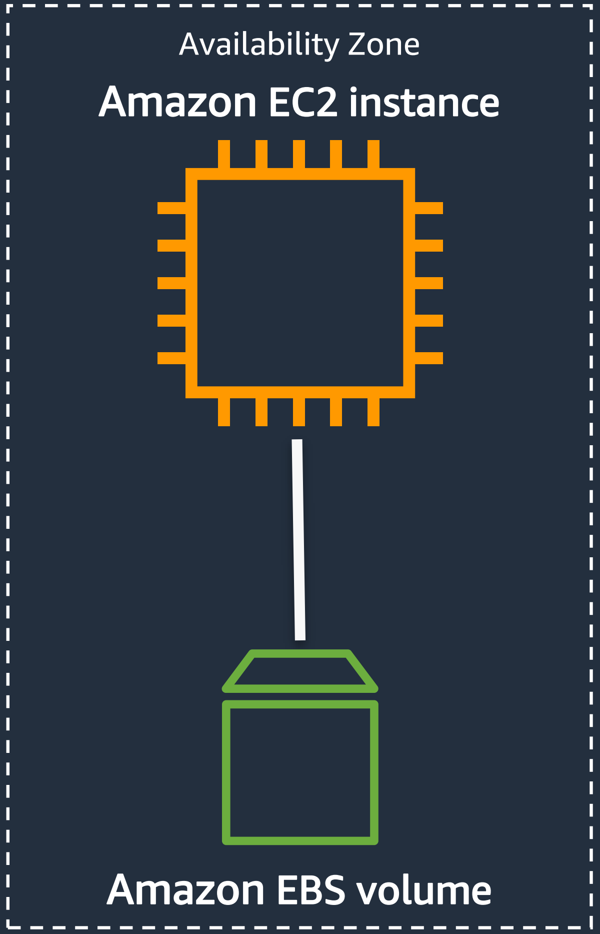
Launched Today!
Crash consistent snapshots for a subset of EBS volumes

Exclude EBS data volumes when taking multi-volume snapshots of EC2 instances



- Simple – replaces multiple API calls with a single API Call
- Automated - Set tags in Data Lifecyle Manager (DLM) policies to specify which volumes to exclude
- Saves cost – Only snapshot the multi attached volumes you select

Encryption and Security- EBS Volumes



- Integrates with AWS Key Management Service (AWS KMS) – AES-256 encryption
- Uses Customer-managed keys (CMKs) or Amazon-managed Keys (AMKs)
- Encrypted EBS volume implies the following are encrypted
  - Data at rest inside the volume
  - Data moving between the volume and instance
  - Snapshots created from the volume
  - Volumes created from such snapshots

Encryption – Amazon EBS Snapshots

- Snapshots of encrypted volumes are automatically encrypted
- Volumes created from encrypted snapshots are automatically encrypted
- You can encrypt an unencrypted snapshot when you copy a snapshot
- You can re-encrypt a snapshot you own with a different key when you copy a snapshot

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

EBS Snapshots – Direct API’s

- ***ListSnapshotBlocks*** - returns the block indexes and block tokens for blocks in the specified snapshot.
- ***ListChangedBlocks*** - returns the block indexes and block tokens for blocks that are different between two specified snapshots of the same volume/snapshot lineage.
- ***GetSnapshotBlock*** - returns the data in a block for the specified snapshot ID, block index, and block token.
- ***StartSnapshot***, ***PutSnapshotBlock***, ***CompleteSnapshot*** – used to create and write to a snapshot.

Amazon Data Lifecycle Manager

Simple, free, automated way to back up data stored on Amazon EC2 instances and EBS volumes by ensuring that snapshots and AMIs are created and deleted on a custom schedule

- Define policies to enforce regular backup schedules
- Policies use tags to identify volumes and instances to back up
- Retain backups for compliance/audit purposes
- Control costs by automatically deleting old backups
- Use IAM to control policy access
- Automatically copy across regions and accounts and set up retention policies.
- No cost to use

AMI Lifecycle Management

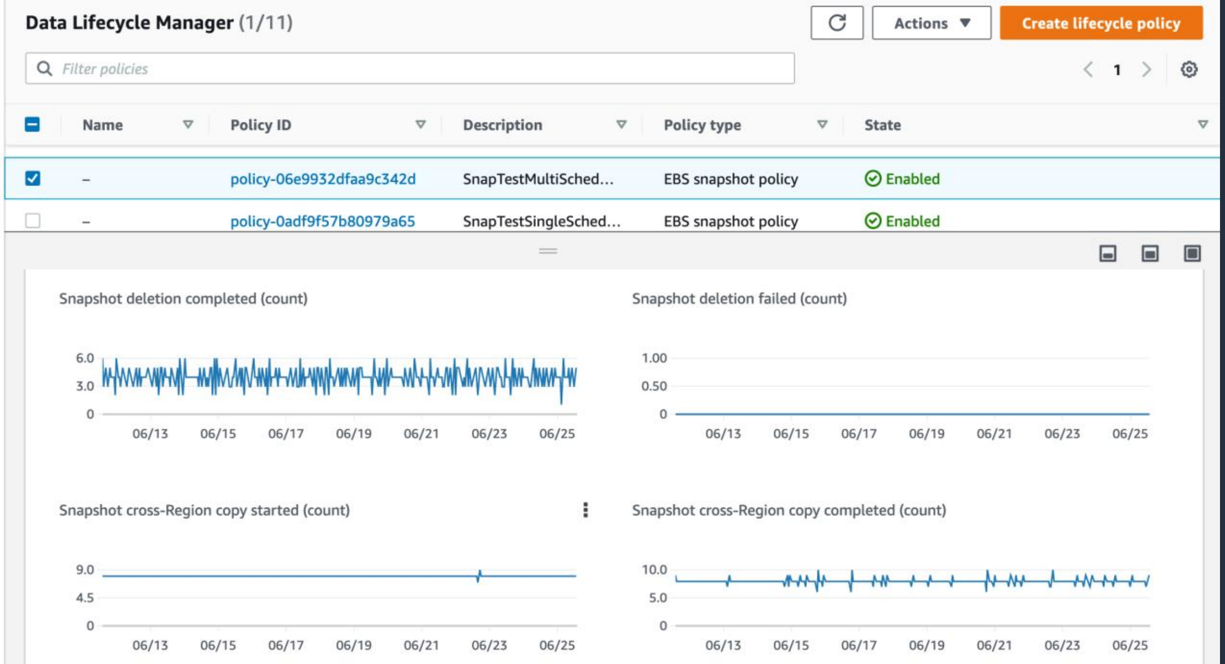
Ensure EBS-backed Amazon Machine Images (AMIs) are created and cleaned up regularly to keep their storage costs under control.

- Automate retention and cleanup of EBS-backed AMIs
- Control costs by automatically deleting snapshots of de-registered AMIs
- Enhance security by automatically deprecating outdated images

Enhanced monitoring of policies

Monitor your policies using CloudWatch metrics

- Track the number of resources targeted each time a policy is run
- Monitor when your snapshots and AMIs are created
- Setup alarm and be notified of failures

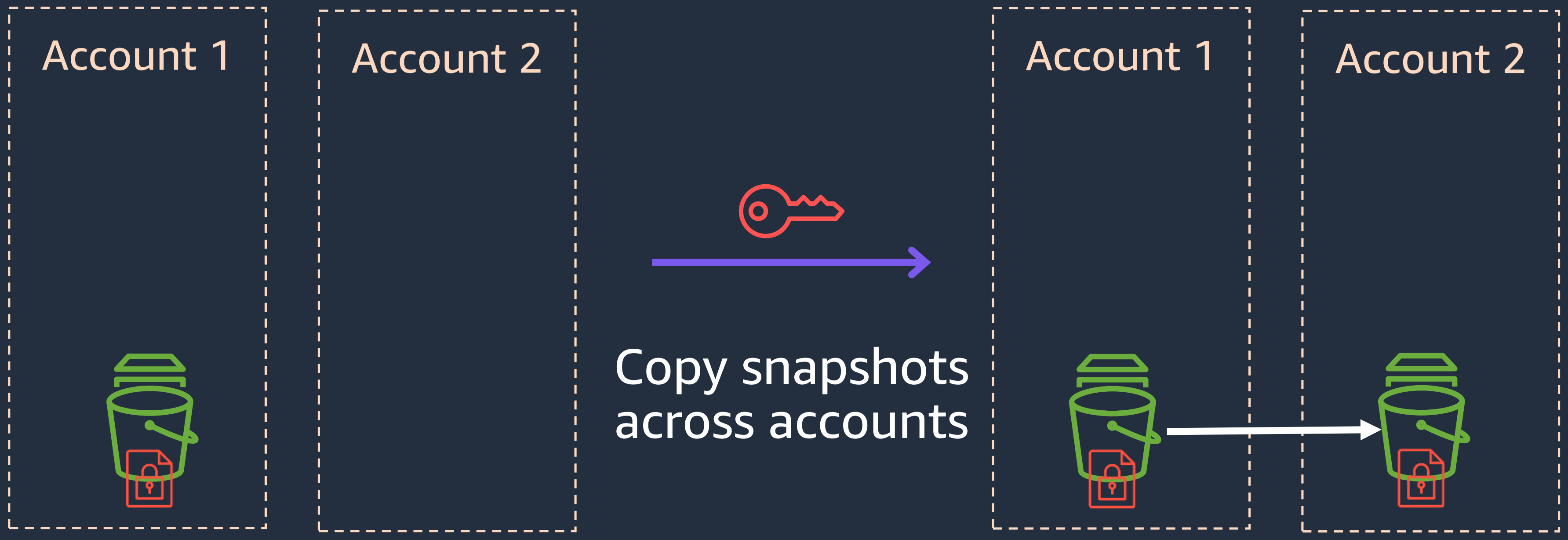


Data Lifecycle Manager (1/11)

▬	Name	Policy ID	Description	Policy type	State
☑	–	policy-06e9932dfaa9c342d	SnapTestMultiSched...	EBS snapshot policy	✓ Enabled
□	–	policy-0adf9f57b80979a65	SnapTestSingleSched...	EBS snapshot policy	✓ Enabled

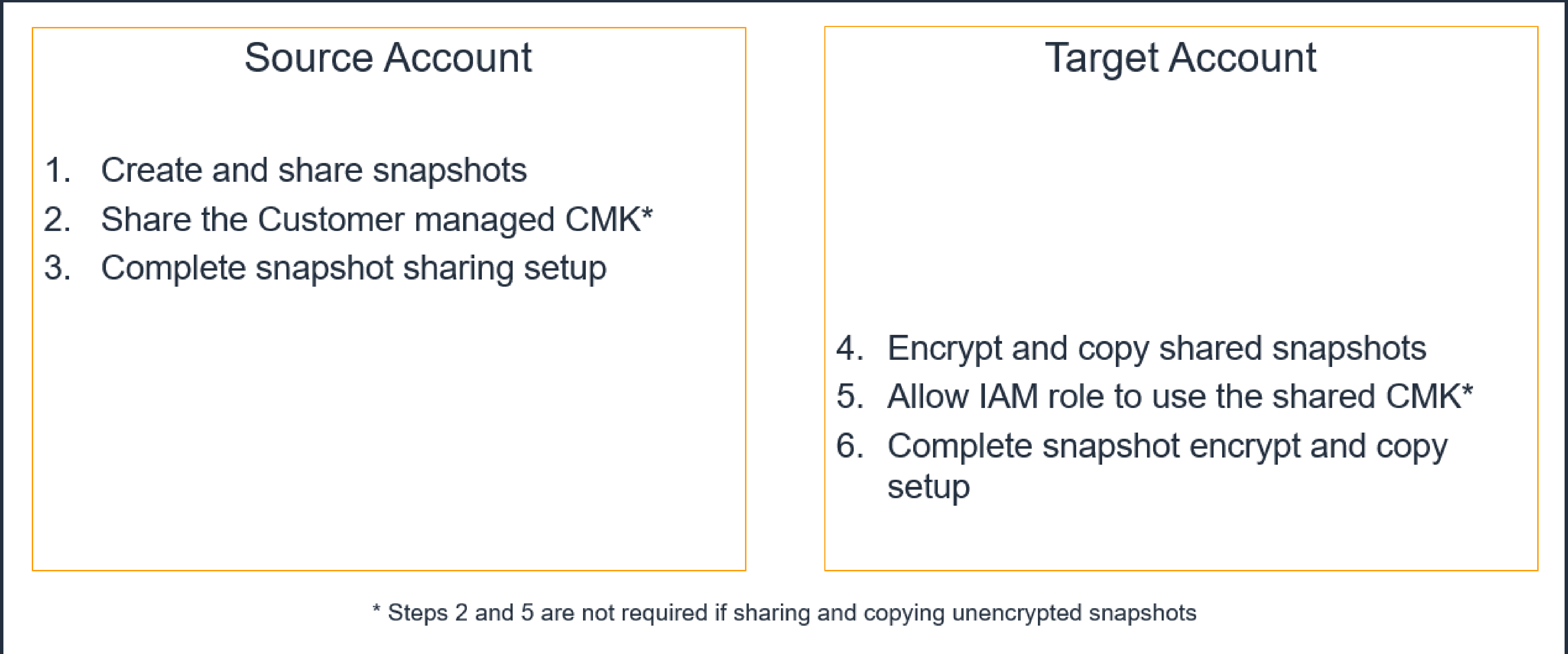
Use case #1 – Protect data across accounts

Protect my data in case my account is compromised by automatically copying snapshots to a separate account.



Snapshot encrypted with KMS Key

Use case #1 – Protect data across accounts



Source Account

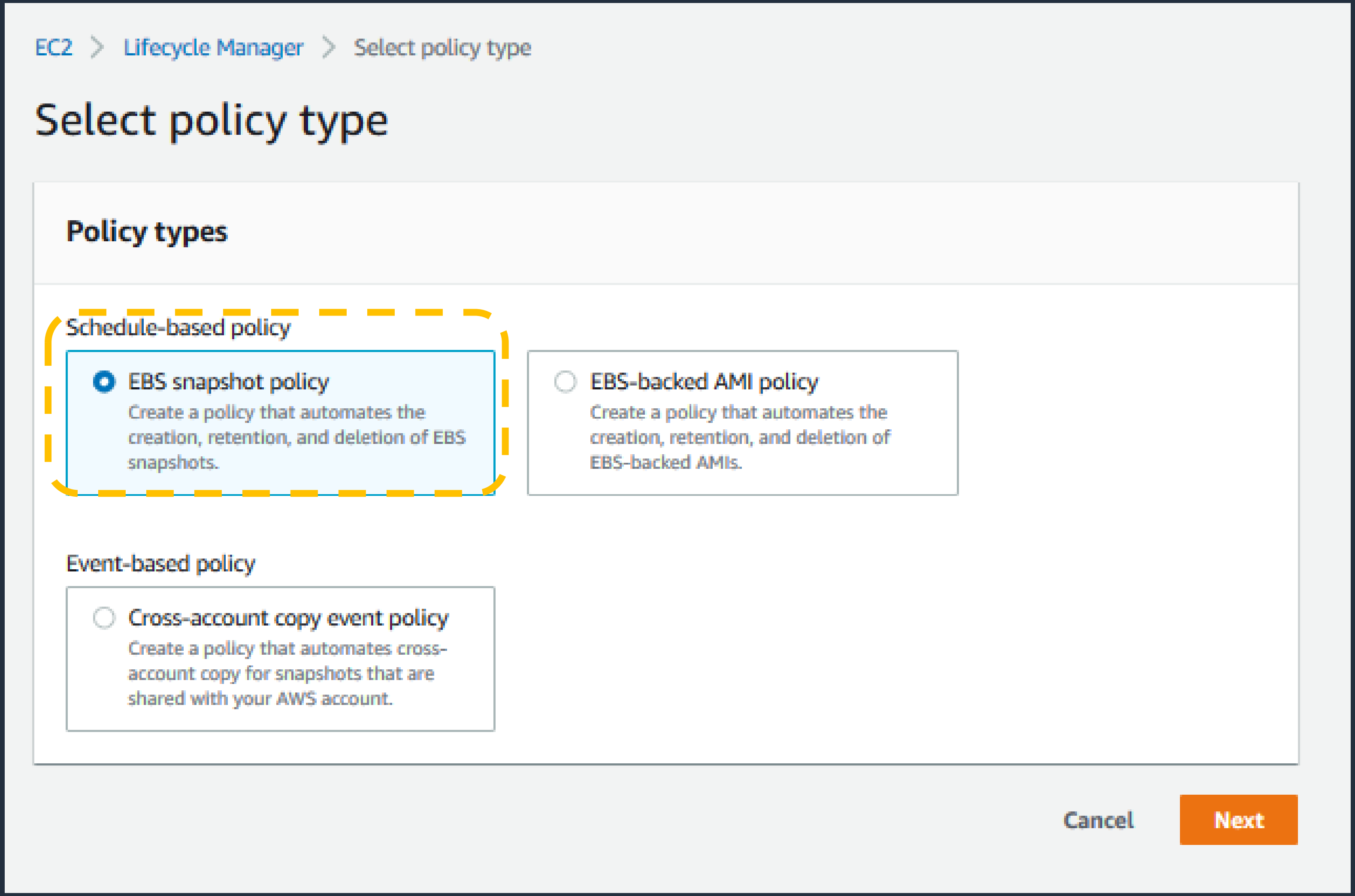
1. Create and share snapshots
2. Share the Customer managed CMK*
3. Complete snapshot sharing setup

Target Account

4. Encrypt and copy shared snapshots
5. Allow IAM role to use the shared CMK*
6. Complete snapshot encrypt and copy setup

* Steps 2 and 5 are not required if sharing and copying unencrypted snapshots

Use case #1 – Protect data (source account)



Select policy type

Policy types

Schedule-based policy

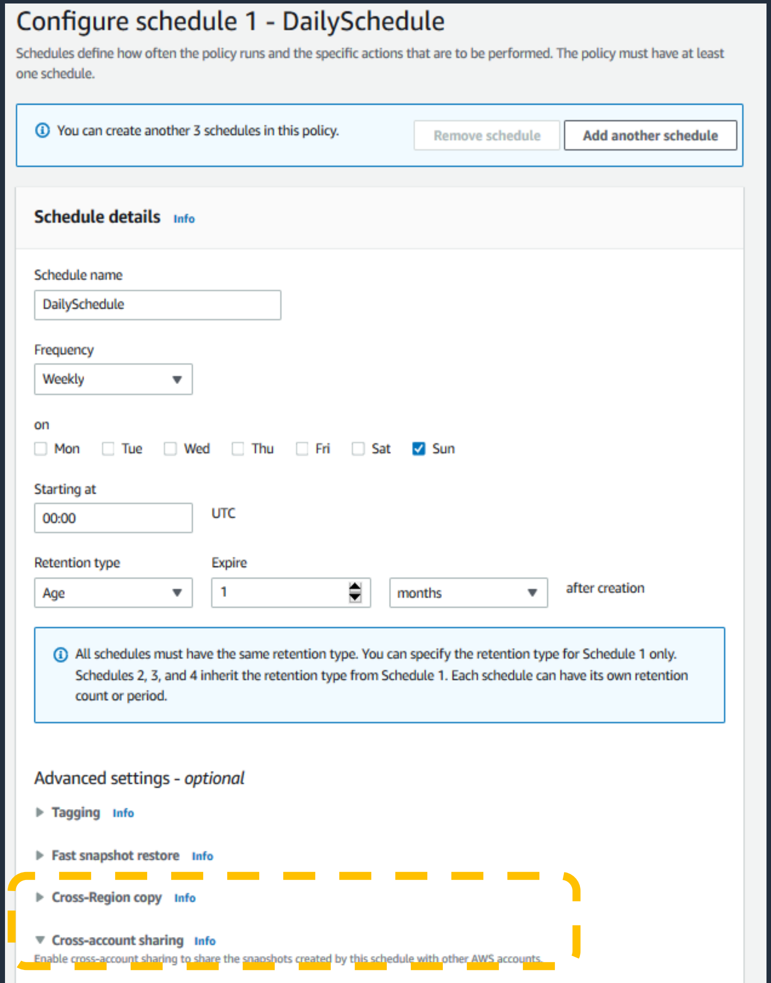
● EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots.

○ EBS-backed AMI policy
Create a policy that automates the creation, retention, and deletion of EBS-backed AMIs.

Event-based policy

○ Cross-account copy event policy
Create a policy that automates cross-account copy for snapshots that are shared with your AWS account.

Use case #1 – Protect Data (source account)



Configure schedule 1 - DailySchedule

Schedules define how often the policy runs and the specific actions that are to be performed. The policy must have at least one schedule.

ⓘ You can create another 3 schedules in this policy.

Schedule details Info

Schedule name: DailySchedule

Frequency: Weekly

on: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat ☑ Sun

Starting at: 00:00 UTC

Retention type: Age

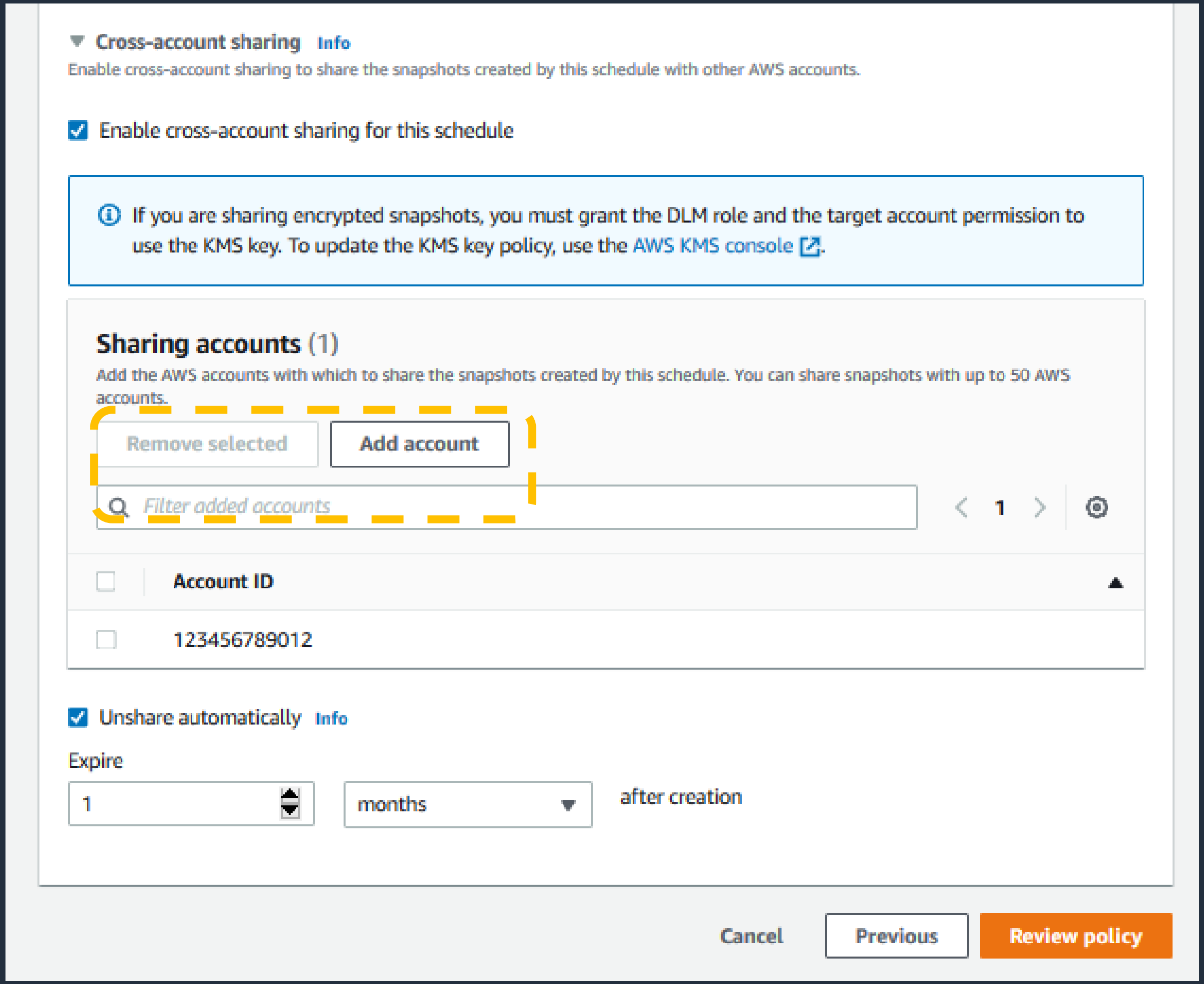
Expire: 1 months after creation

ⓘ All schedules must have the same retention type. You can specify the retention type for Schedule 1 only. Schedules 2, 3, and 4 inherit the retention type from Schedule 1. Each schedule can have its own retention count or period.

Advanced settings - *optional*

▼ Cross-account sharing Info

Enable cross-account sharing to share the snapshots created by this schedule with other AWS accounts.



▼ Cross-account sharing Info

Enable cross-account sharing to share the snapshots created by this schedule with other AWS accounts.

☑ Enable cross-account sharing for this schedule

ⓘ If you are sharing encrypted snapshots, you must grant the DLM role and the target account permission to use the KMS key. To update the KMS key policy, use the AWS KMS console.

Sharing accounts (1)

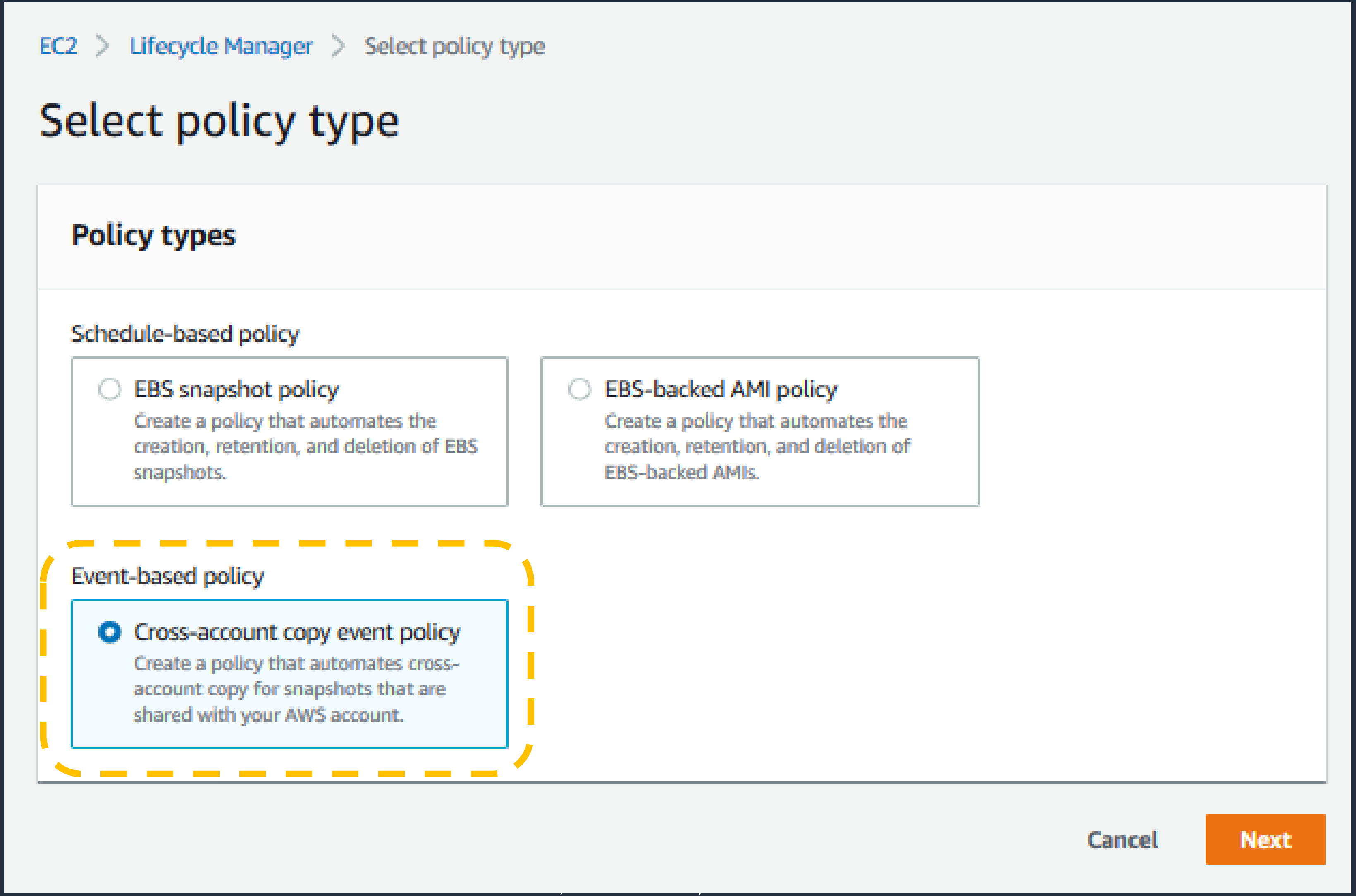
Add the AWS accounts with which to share the snapshots created by this schedule. You can share snapshots with up to 50 AWS accounts.

□	Account ID
□	123456789012

☑ Unshare automatically Info

Expire: 1 months after creation

Use case #1 – Protect Data (target account)



EC2 > Lifecycle Manager > Select policy type

Select policy type

Policy types

Schedule-based policy

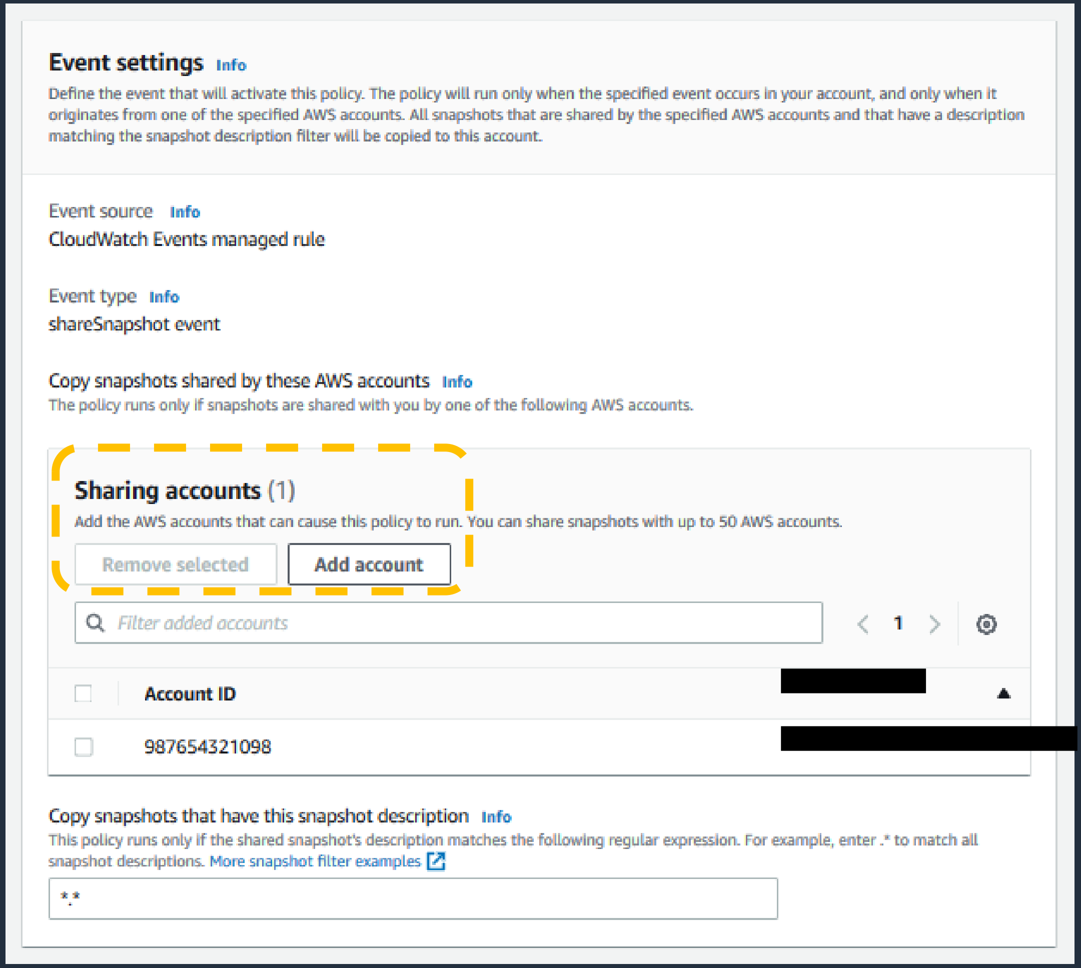
○ EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots.

○ EBS-backed AMI policy
Create a policy that automates the creation, retention, and deletion of EBS-backed AMIs.

Event-based policy

● Cross-account copy event policy
Create a policy that automates cross-account copy for snapshots that are shared with your AWS account.

Use case #1 – Protect Data (target account)



Event settings Info

Define the event that will activate this policy. The policy will run only when the specified event occurs in your account, and only when it originates from one of the specified AWS accounts. All snapshots that are shared by the specified AWS accounts and that have a description matching the snapshot description filter will be copied to this account.

Event source Info
CloudWatch Events managed rule

Event type Info
shareSnapshot event

Copy snapshots shared by these AWS accounts Info
The policy runs only if snapshots are shared with you by one of the following AWS accounts.

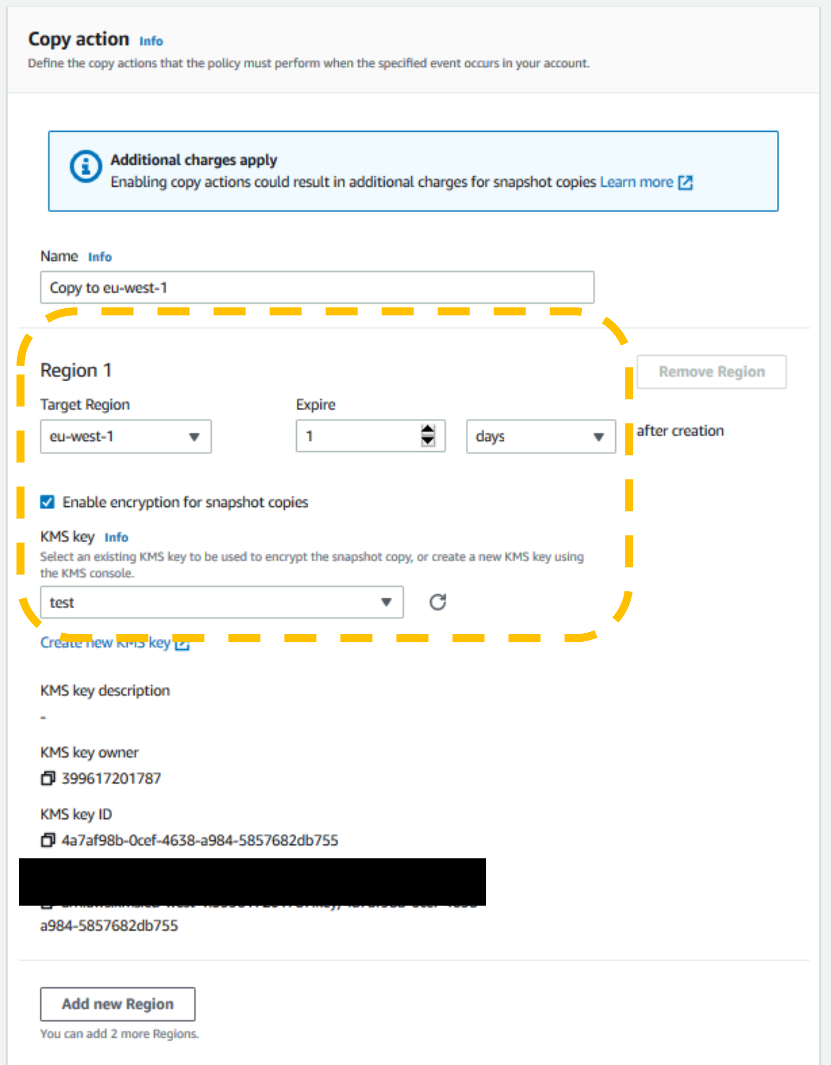
Sharing accounts (1)

Add the AWS accounts that can cause this policy to run. You can share snapshots with up to 50 AWS accounts.

□	Account ID	[redacted]
□	987654321098	[redacted]

Copy snapshots that have this snapshot description Info
This policy runs only if the shared snapshot's description matches the following regular expression. For example, enter .* to match all snapshot descriptions. More snapshot filter examples

.*



Copy action Info

Define the copy actions that the policy must perform when the specified event occurs in your account.

Additional charges apply
Enabling copy actions could result in additional charges for snapshot copies Learn more

Name Info
Copy to eu-west-1

Region 1

Target Region: eu-west-1

Expire: 1 days after creation

☑ Enable encryption for snapshot copies

KMS key Info
Select an existing KMS key to be used to encrypt the snapshot copy, or create a new KMS key using the KMS console.

test

KMS key description
-

KMS key owner
399617201787

KMS key ID
4a7af98b-0cef-4638-a984-5857682db755

[redacted]
a984-5857682db755

You can add 2 more Regions.

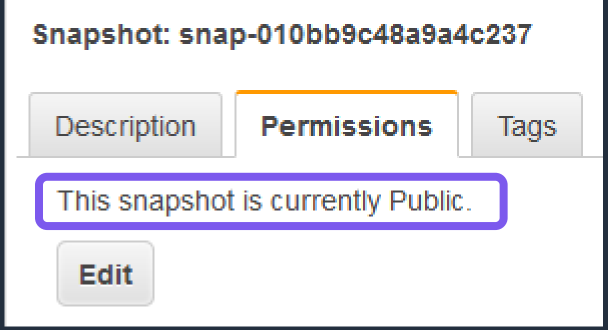
Use case #2 – Automate AMI management and distribution across Regions

Automate deregistration of my EBS-backed Amazon Machine Images (AMIs) and deletion of supporting snapshots

- Create a EBS-backed AMI policy targeting a group of EC2 Instances
- Create a single schedule to create AMIs on a weekly basis
- Replicate AMI to multiple regions
- Deregister the AMI after three months
- Delete its underlying EBS snapshots.

Sharing Snapshots and AMIs

- Public sharing: Reasonable use case for AMIs – AWS Marketplace AMIs
- Share non-AMI snapshots with specific accounts
- To launch a volume from a snapshot, you need a copy of snapshot in-Region


Snapshot: snap-010bb9c48a9a4c237

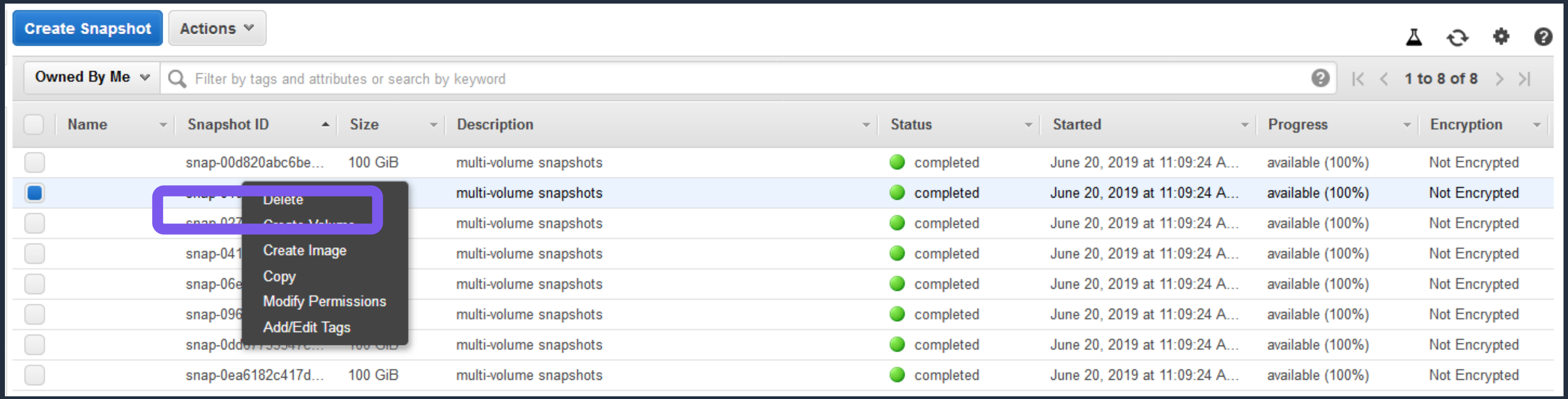
This snapshot is currently Public.

```
snap-010bb9c48a9a4c237 --attribute createVolumePermission
{
   "SnapshotId": "snap-010bb9c48a9a4c237",
   "CreateVolumePermissions": [
      {
         "Group": "all"
      }
   ]
}
```

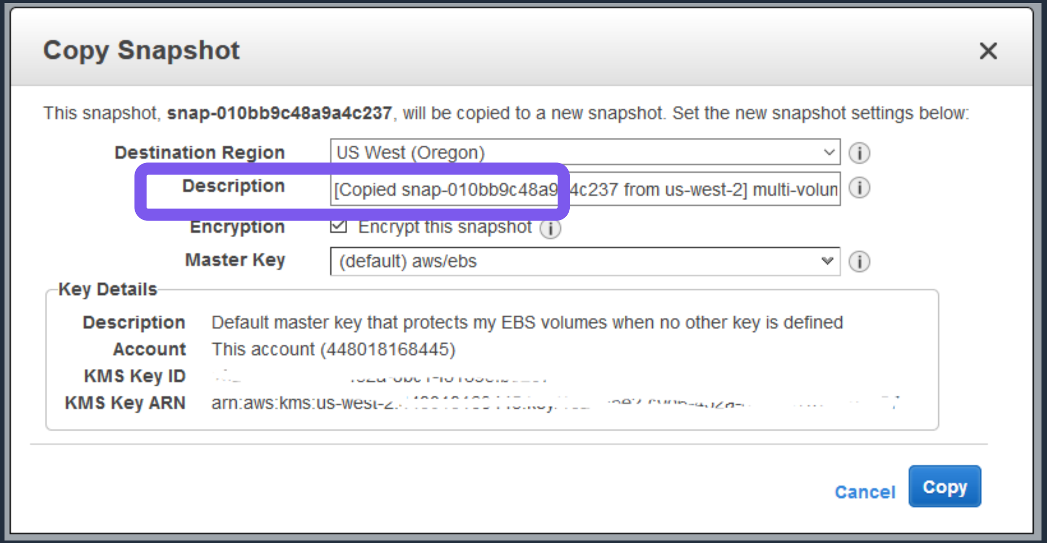
Use Case #3: Copy Snapshots

- Amazon S3 encryption protects snapshots in-transit during the copy operation
- Unencrypted snapshots can be encrypted during copy
- Encrypted snapshots can be re-encrypted during copy
- First copy across Regions is a full copy
- Snapshots are incremental after first copy
  - Same CMK needed on both ends to support incremental copies

Copy Snapshots: Encrypt or re-encrypt



	Name	Snapshot ID	Size	Description	Status	Started	Progress	Encryption
☐		snap-00d820abc6be...	100 GiB	multi-volume snapshots	completed	June 20, 2019 at 11:09:24 A...	available (100%)	Not Encrypted
☑				multi-volume snapshots	completed	June 20, 2019 at 11:09:24 A...	available (100%)	Not Encrypted
☐		snap-027		multi-volume snapshots	completed	June 20, 2019 at 11:09:24 A...	available (100%)	Not Encrypted
☐		snap-041		multi-volume snapshots	completed	June 20, 2019 at 11:09:24 A...	available (100%)	Not Encrypted
☐		snap-06e		multi-volume snapshots	completed	June 20, 2019 at 11:09:24 A...	available (100%)	Not Encrypted
☐		snap-096		multi-volume snapshots	completed	June 20, 2019 at 11:09:24 A...	available (100%)	Not Encrypted
☐		snap-0dd		multi-volume snapshots	completed	June 20, 2019 at 11:09:24 A...	available (100%)	Not Encrypted
☐		snap-0ea6182c417d...	100 GiB	multi-volume snapshots	completed	June 20, 2019 at 11:09:24 A...	available (100%)	Not Encrypted



Copy Snapshot

This snapshot, **snap-010bb9c48a9a4c237**, will be copied to a new snapshot. Set the new snapshot settings below:

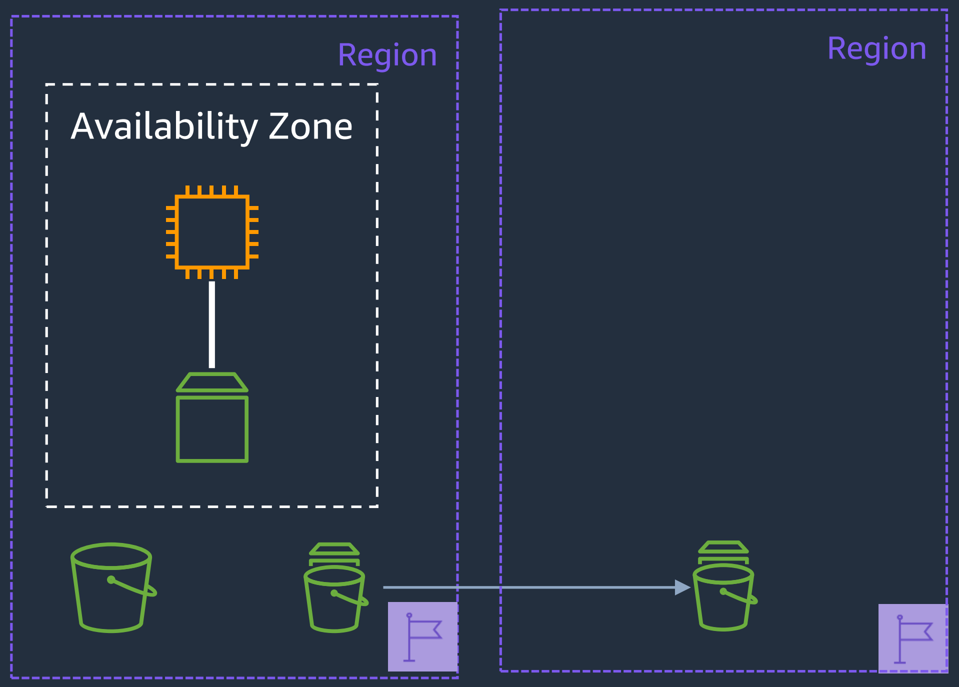
Destination Region	US West (Oregon)
Description	[Copied snap-010bb9c48a9a4c237 from us-west-2] multi-volun
Encryption	☑ Encrypt this snapshot
Master Key	(default) aws/ebs

Key Details

Description	Default master key that protects my EBS volumes when no other key is defined
Account	This account (448018168445)
KMS Key ID	[redacted]
KMS Key ARN	arn:aws:kms:us-west-2:[redacted]

```
aws ec2 copy-snapshot --source-snapshot-id
snap-010bb9c48a9a4c237 --destination-region
us-west-1 --encrypted --kms-key-id
key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Copy Snapshots across Regions



- Copy Snapshots across accounts, across Regions
- Lock down resource-level permissions on target snapshot copy
- Multi-region = Protection against Regional events
- Permission lock down = malicious or unintentional deletes of data

Learn in-demand AWS Cloud skills

AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand

Train now

AWS Certifications

Earn an industry-recognized credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits

Access **new** exam guides

Thank you!

Eric Jones