AWS re:Invent

STG361

Simplify and automate backup of AWS data

Chris Schilling

Product Manager, AWS Backup

Amazon Web Services

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Agenda

- **Introduction to backup** – Why we exist
- **AWS Backup: What we do** – Our value proposition
- **Solving a daily problem** – Let’s make it easy
- **Solving a complex problem** – Trying something harder
- **Closing out—and some good news** – Landing the plane

Introduction to AWS Backup

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Life is full of complications



There are geese (gooses?) everywhere

goose [goos] SHOW IPA

EXAMPLES | WORD ORIGIN | IDIOMS

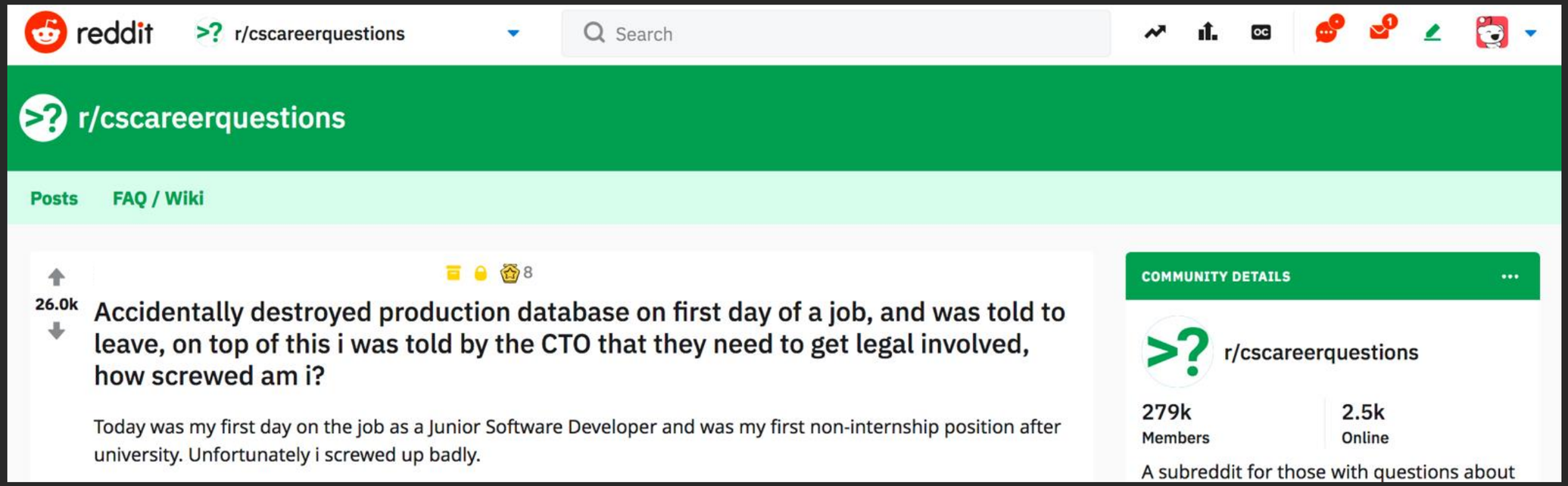
SEE MORE SYNONYMS FOR *goose* ON THESAURUS.COM

noun, plural **geese for 1, 2, 4, 8**; **goos·es for 5–7**.

1. any of numerous wild or domesticated, web-footed swimming birds of the family Anatidae, especially of the genera *Anser* and *Branta,* most of which are larger and have a longer neck and legs than the ducks.
2. the female of this bird, as distinguished from the male, or gander.
3. the flesh of a goose, used as food.
4. a silly or foolish person; simpleton.

SEE MORE

Sometimes you hire a goose



Sometimes you forget that geese exist

POLITICS

Baltimore IT department uses ‘mind-boggling,' outdated data storage method, audit finds



By LUKE BROADWATER
BALTIMORE SUN | SEP 27, 2019 | 11:26 AM

“One of the things I’ve learned in my short time here is a great number of Baltimore City employees store entity information on their local computers. And that’s it,” Pasch replied.

“Wow. That’s mind-boggling to me,” Costello said. “They’re the agency that should be tasked with educating people that that’s a problem.”

The goose isn’t going to change



- Moves files that shouldn’t be moved
- Deletes volumes you need
- ”Forgets” to lock the door behind it
- Documents nothing, goes home, sleeps well

So what can be done?



AWS Backup: What we do

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup: We help you stare the goose down



- Restore files and copy them to where they should be
- Recover volumes you thought were deleted
- Secure access to a separate copy of your data
- Automate everything, keep logs in one place, sleep well



AWS Backup

Centrally manage and automate backups across AWS services



AWS Backup

Centrally manage and automate backups across AWS services

Centralize compliance, automate backup, work across services



Centralized monitoring and security

Manage and monitor backup jobs and IAM policies/roles



Automated lifecycle and retention management

Simplify data retention for different backup tiers

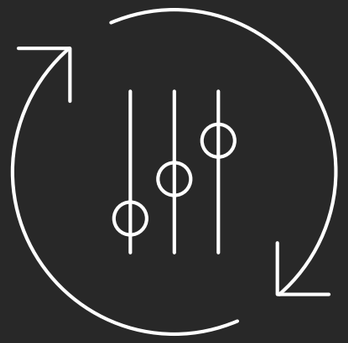


Operate across multiple services

Create plans to cover more than one service

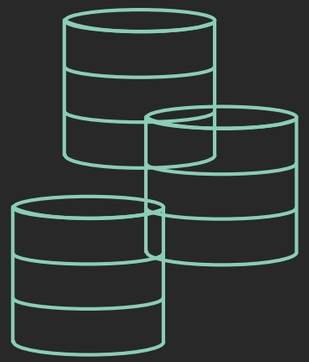
How AWS Backup integrates with source services

Control plane



Orchestration, monitoring, and reporting

Data plane



Independent storage and encryption from source



Lifecycle backups to lower cost tier

Services supported at AWS Backup launch

	 AWS Storage Gateway	 Amazon EBS	 Amazon RDS	 Amazon DynamoDB	 Amazon EFS
Automated backup schedules	✓	✓	✓	✓	✓
Automated retention management	✓	✓	✓	✓	✓
Centralized backup monitoring/logging	✓	✓	✓	✓	✓
AWS KMS integrated backup encryption	✓	✓	✓	✓	✓
Lifecycle to cold storage					✓

Solving daily problems

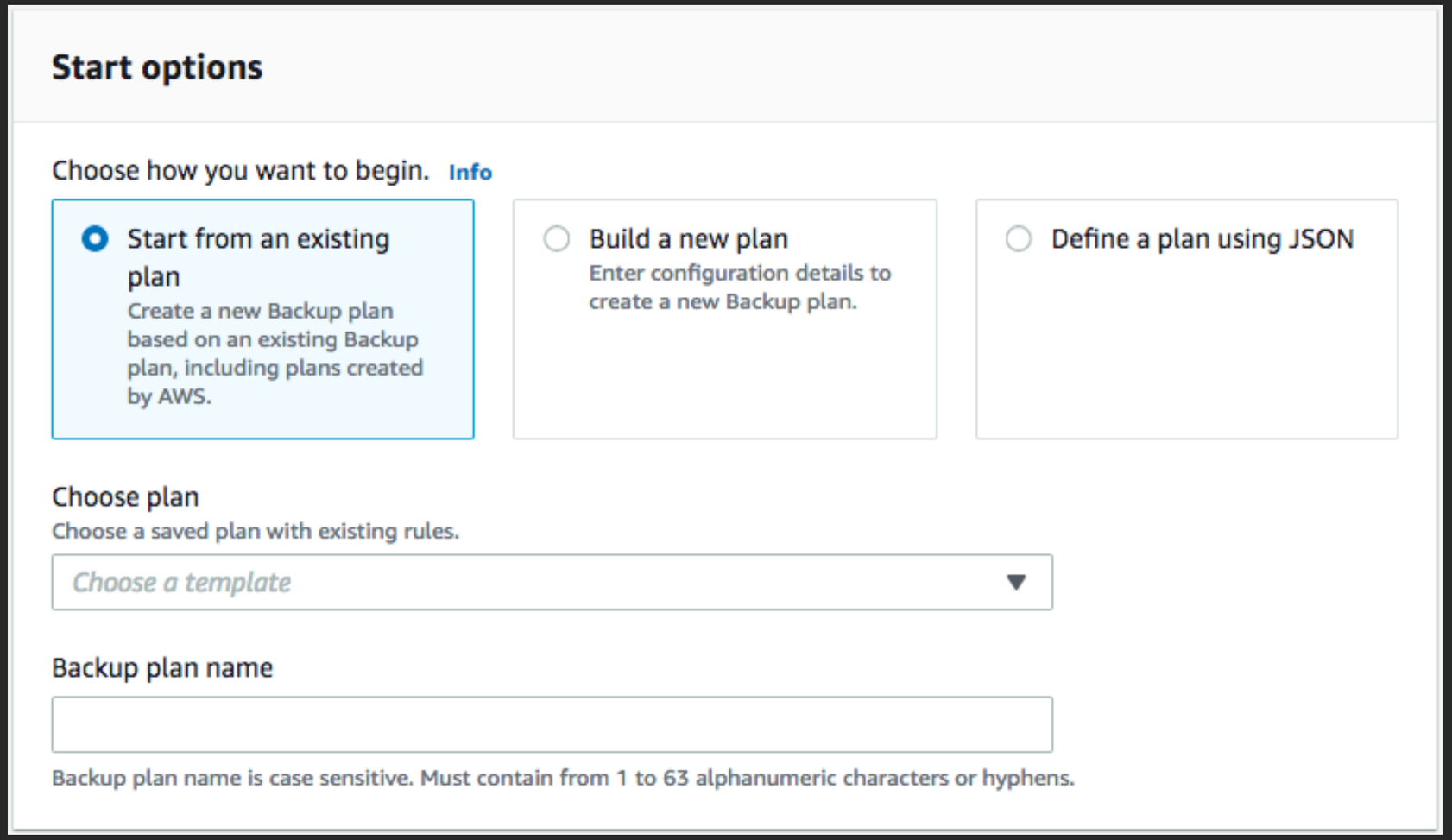
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Creating a backup plan and restoring from it

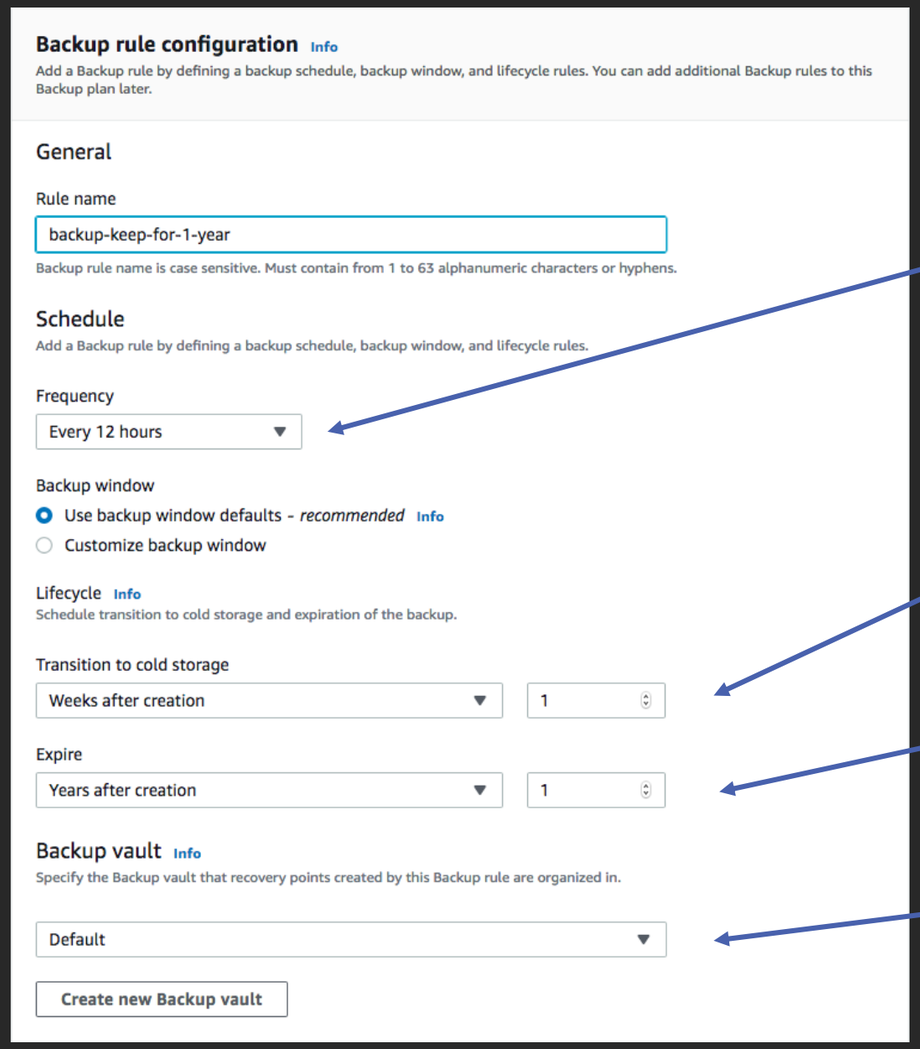


- Let’s create a backup plan to protect our data from being “misplaced” or deleted
- We’ll also view configuration options for a backup plan
- Finally, we’ll see how easy it is to find the right backup to restore

Creating a backup plan: High-level process



Configuring a backup rule in a backup plan



Set a frequency and backup window

Transition to cold for lifecycle management (for Amazon EFS)

Expiry/retention

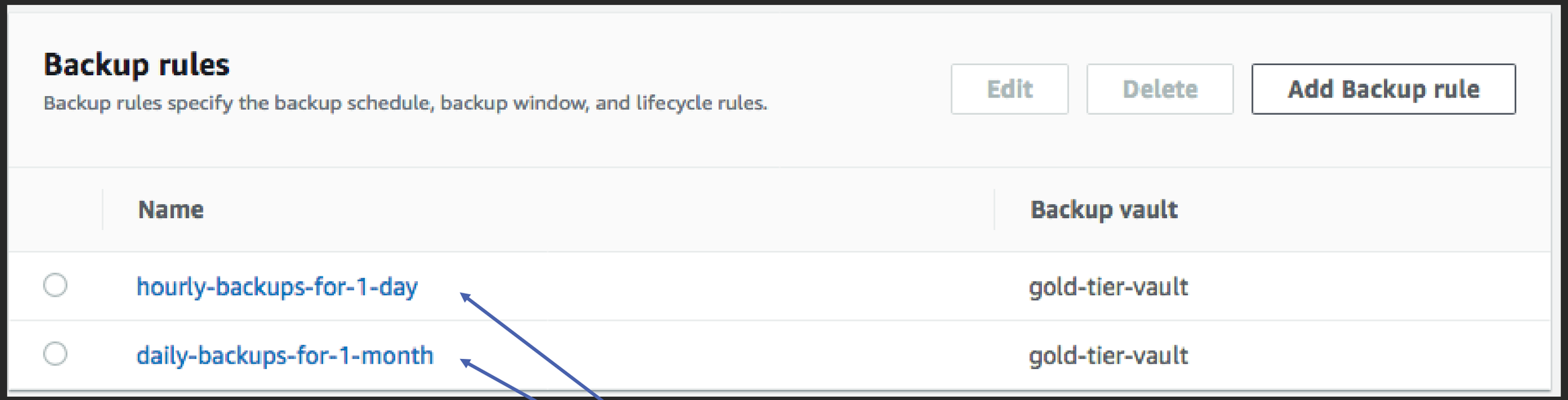
Backup vault

Backup vaults: Logical constructs for additional security



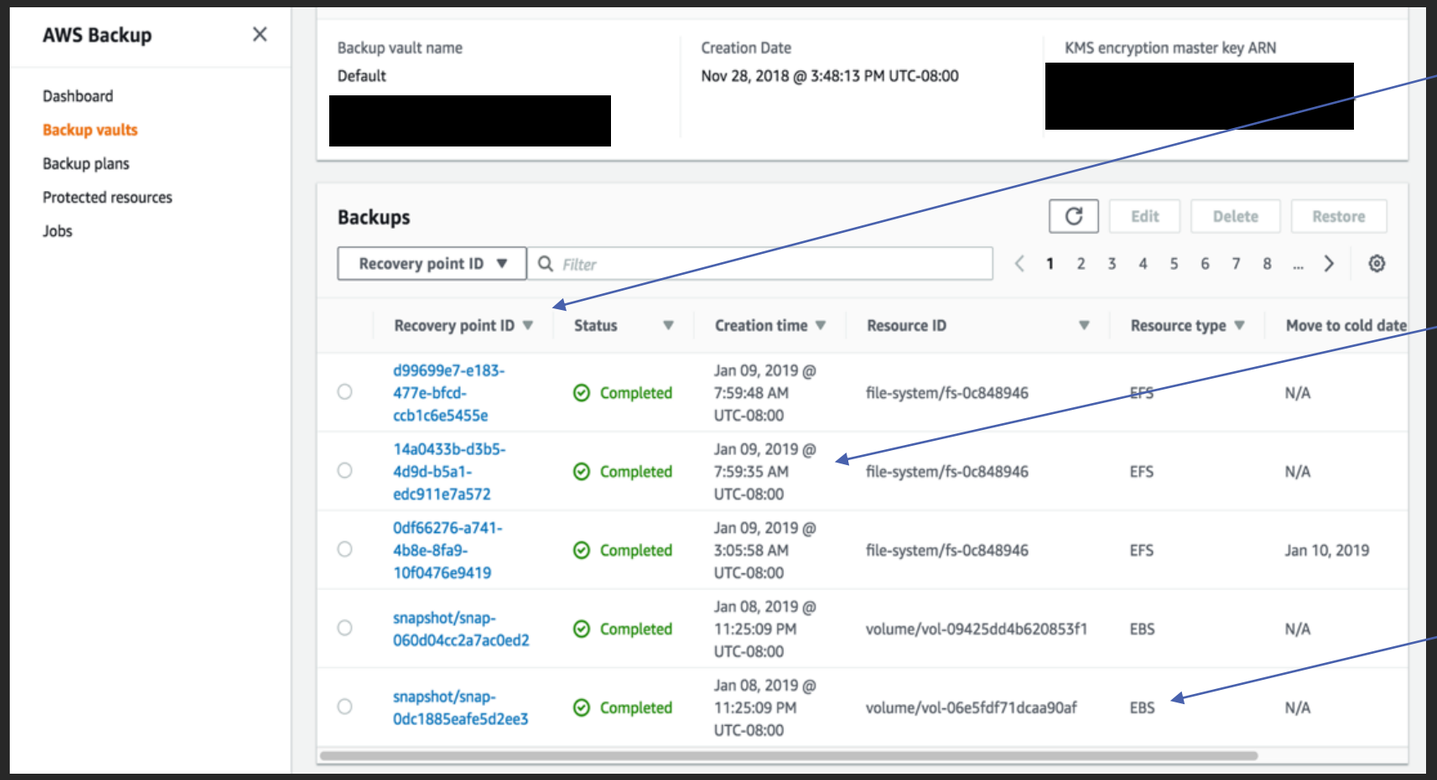
- Backup vaults are AWS Backup-managed resources for storing backup data
- Vaults are configurable to support resource-level permissions via AWS Identity and Access Management (IAM) and to separate permissions for different backups
- Vault data is visible to the respective service, managed under vault access policy

What happens when rules conflict



Once a day these rules will conflict. In that case the backup with the longest retention will win and the other backup will be skipped

Restoring from your backup



Select a specific backup (recovery point)

View the creation time for an incremental backup

Resource-specific (e.g., Amazon EBS)

Customer example #1: Leaving scripts behind

This customer, a services provider with multiple accounts, has created a custom script to take nightly backups of Amazon EBS and DynamoDB workloads. For five mission-critical applications, the customer needs to take backups every four hours.

After an accidental deletion, the customer struggled to identify the right EBS volumes to perform a restore. After a subsequent audit, the customer discovered ~15% of backups were missing, as jobs failed due to service-specific limits and access control.

How would the customer use AWS Backup?

Solving harder problems

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing access to your backup data



- We’ll start by talking about some of the options to secure data in AWS Backup
- Then, we’ll walk through how AWS Backup protects your backups from being deleted by other services
- Finally, we’ll show how access policies can further restrict actions taken for specific resources

Granular controls for security and compliance

Identity-based policies

Create IAM roles or use default service roles (e.g., backup operator vs. backup admin)

"Control what account users can do"

Execution identities (service roles)

Create roles to grant/limit AWS Backup permissions

"Control what AWS Backup can touch"

Resource-based policies

Assign policies to individual vaults to further control which users can access or restore

"Control how a resource can be accessed"

Defense in depth: How you can protect backups

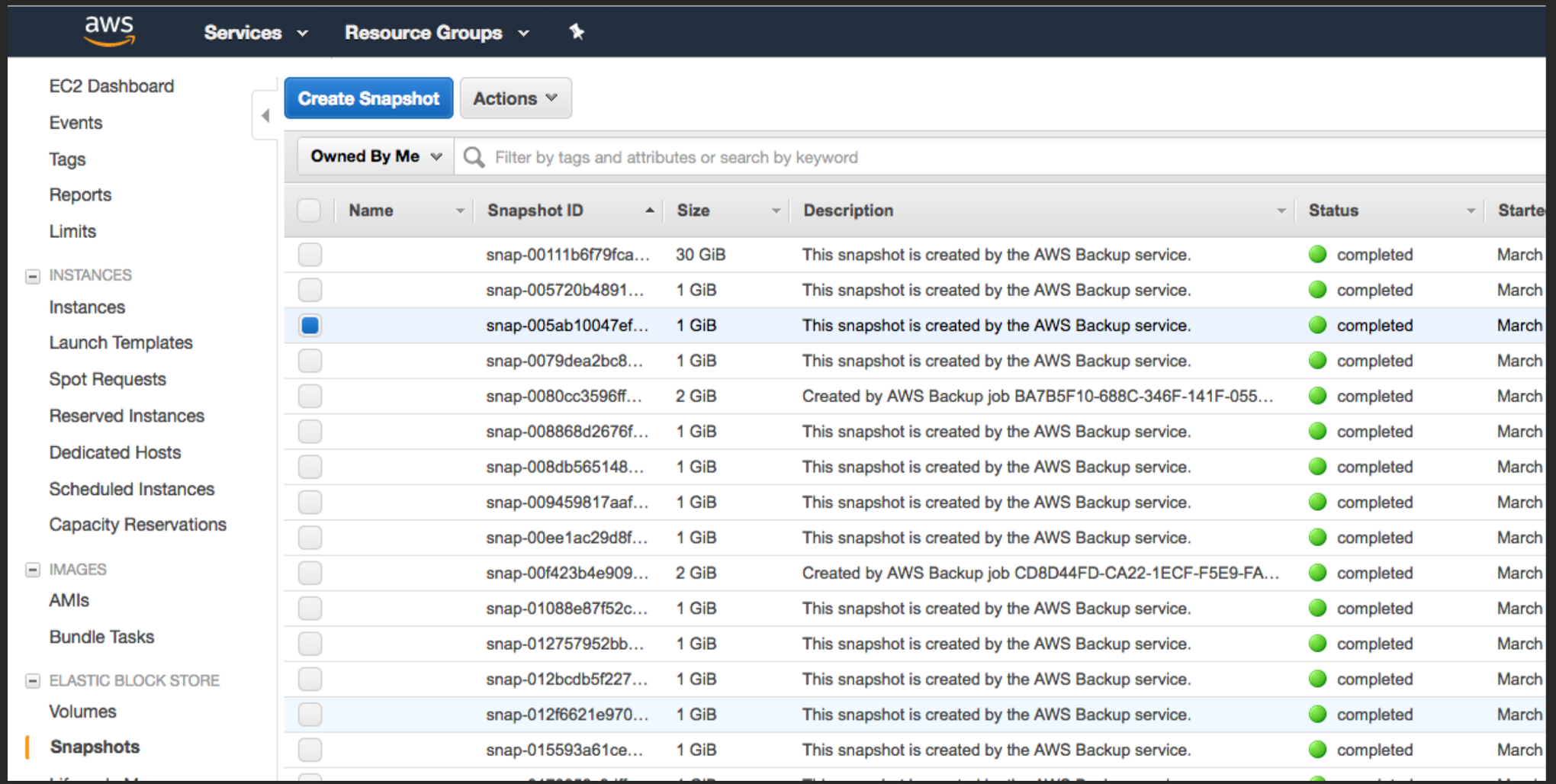
Default protection for all backups taken by AWS Backup

Identity and service policies

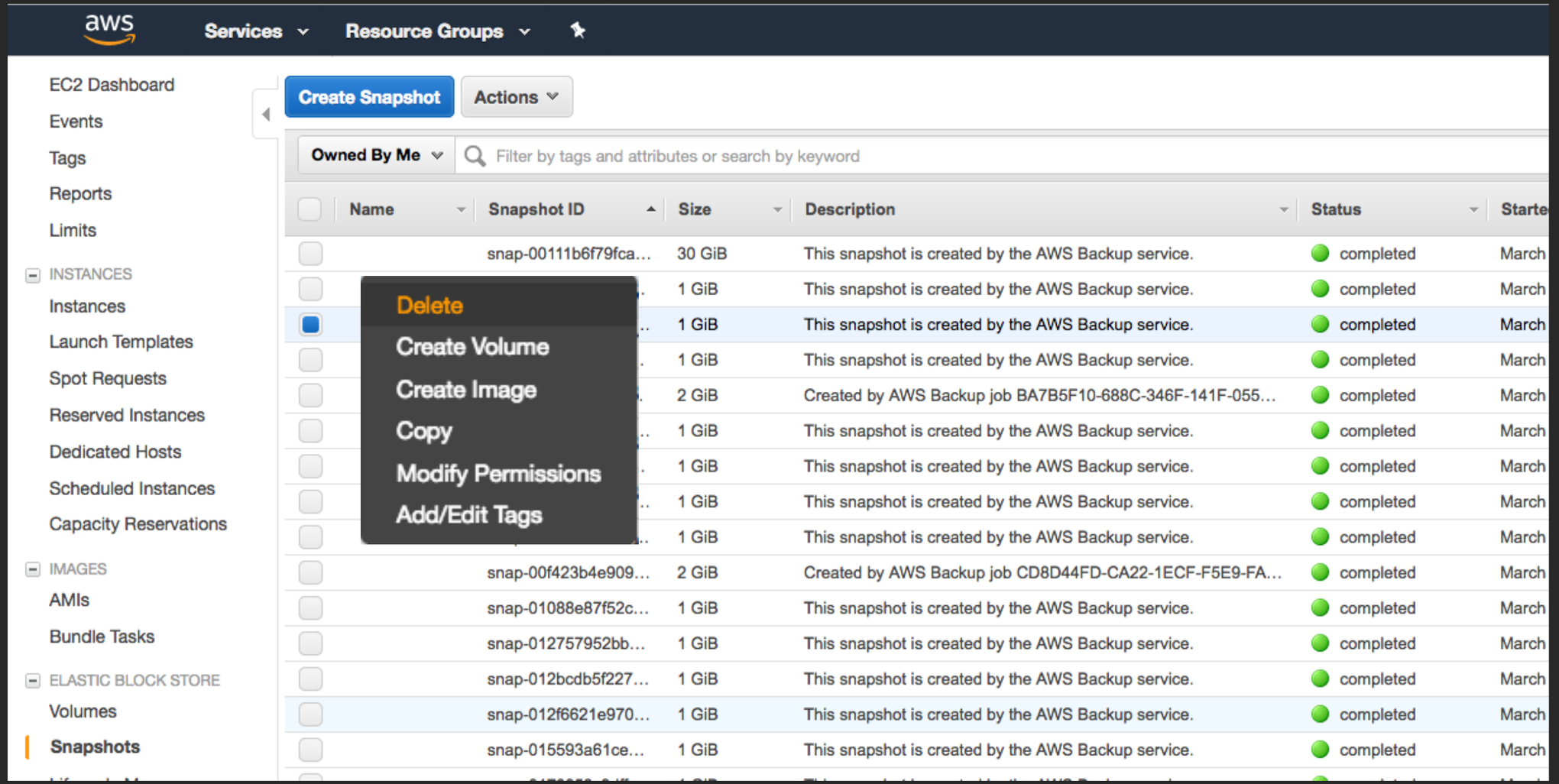
Resource (vault-specific) policies

Encryption

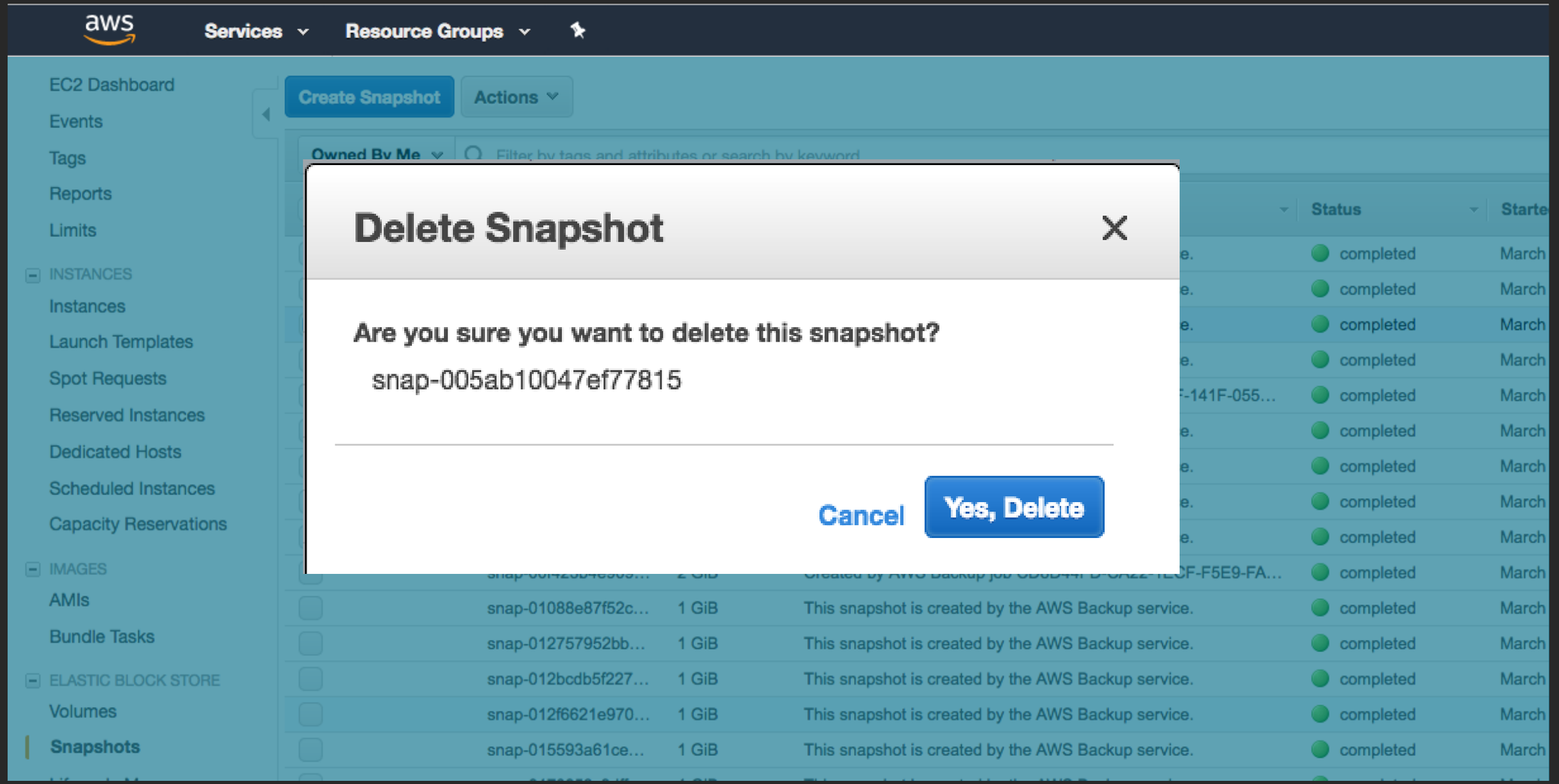
Securing backups walkthrough (1/9)



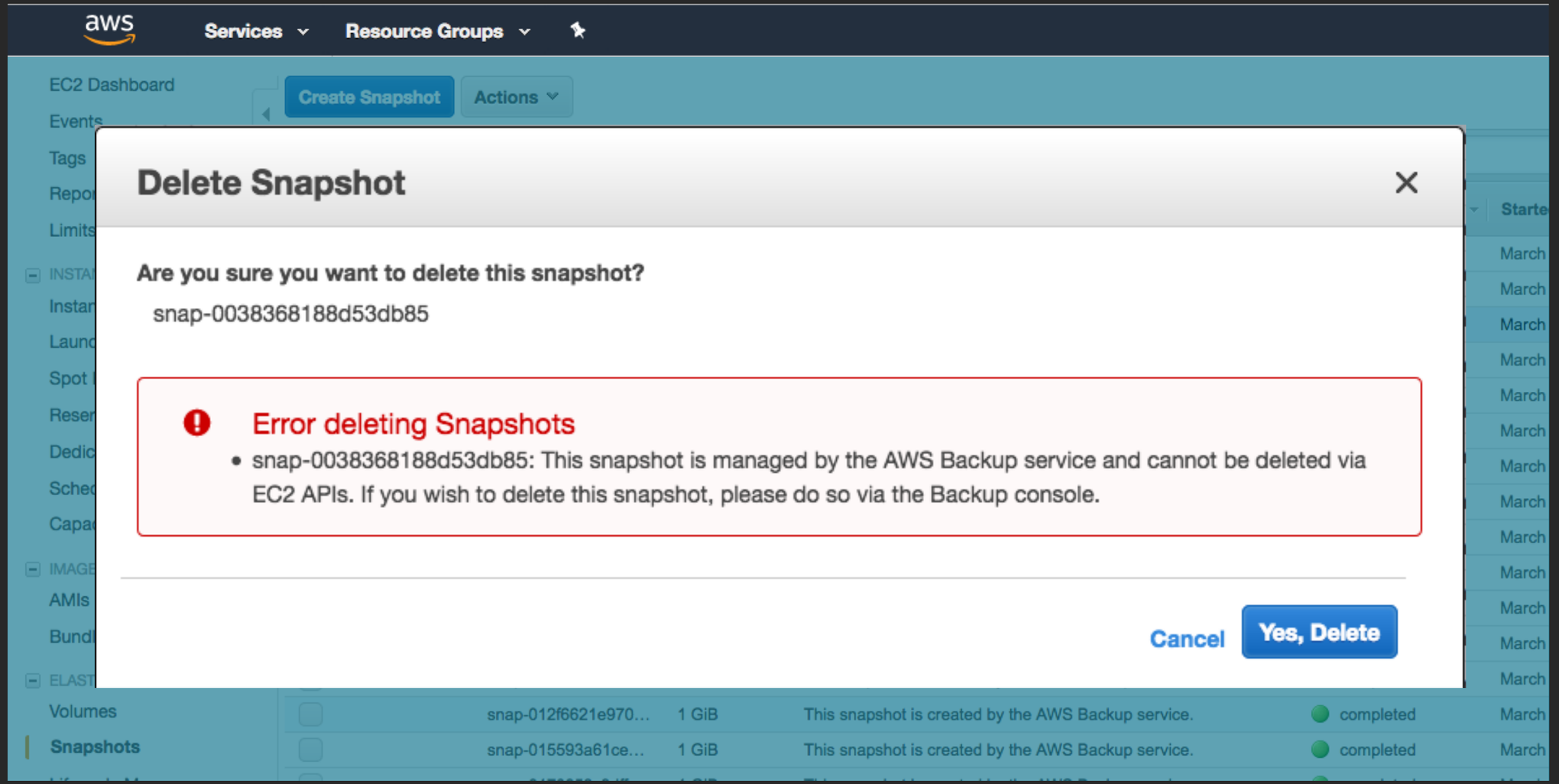
Securing backups walkthrough (2/9)



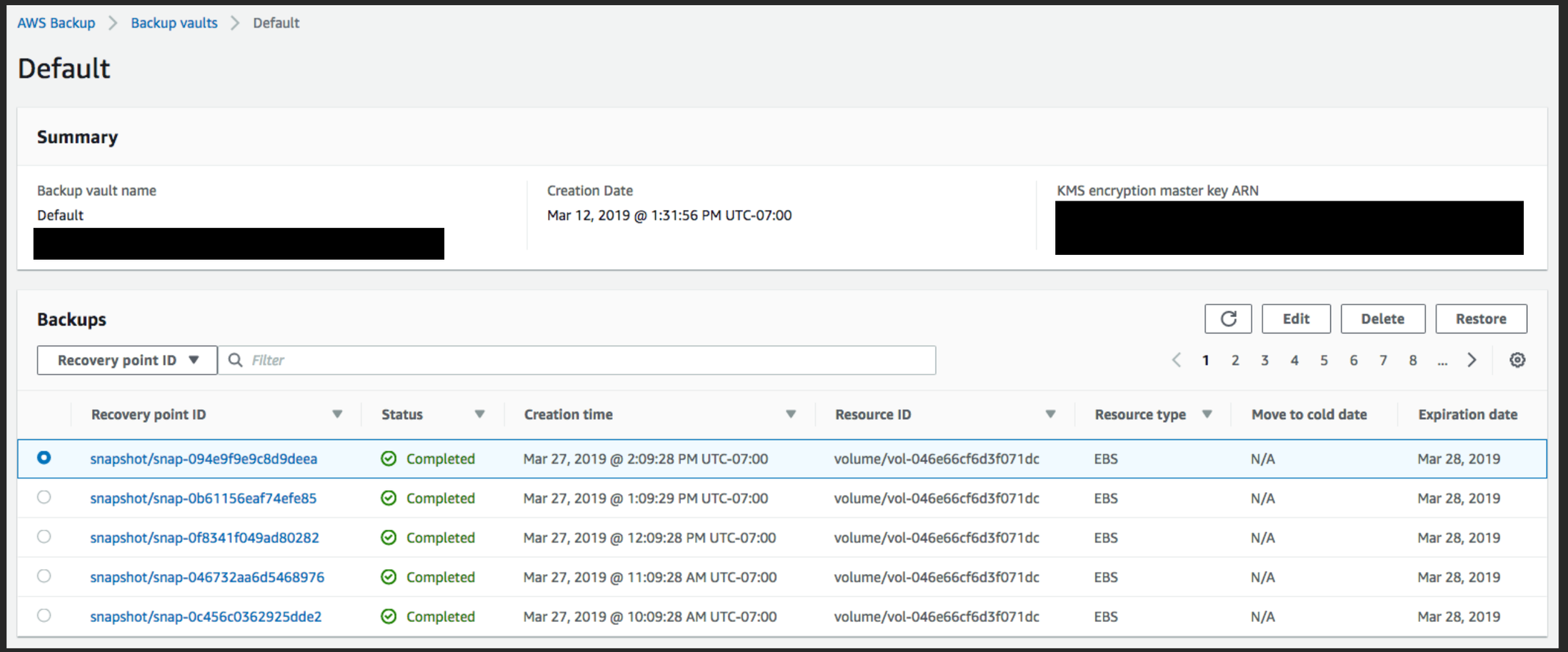
Securing backups walkthrough (3/9)



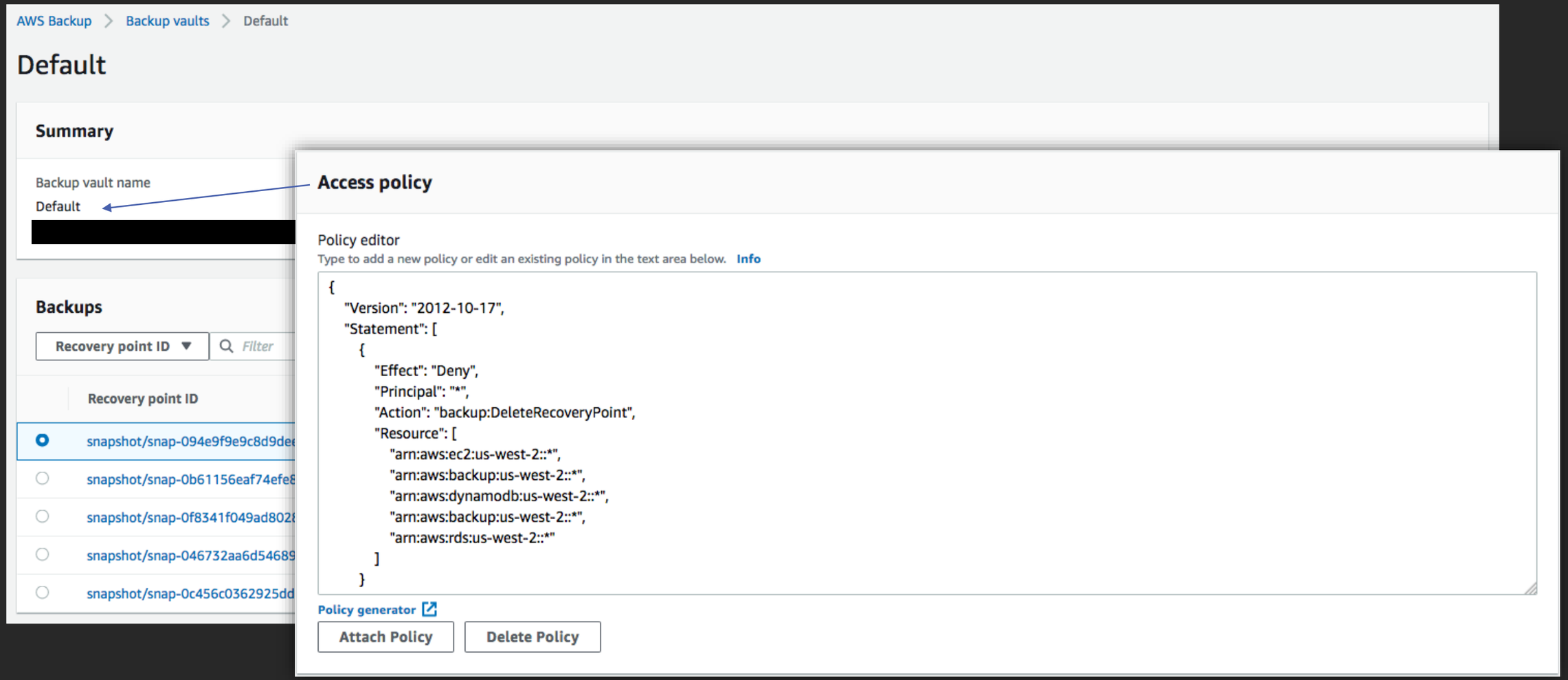
Securing backups walkthrough (4/9)



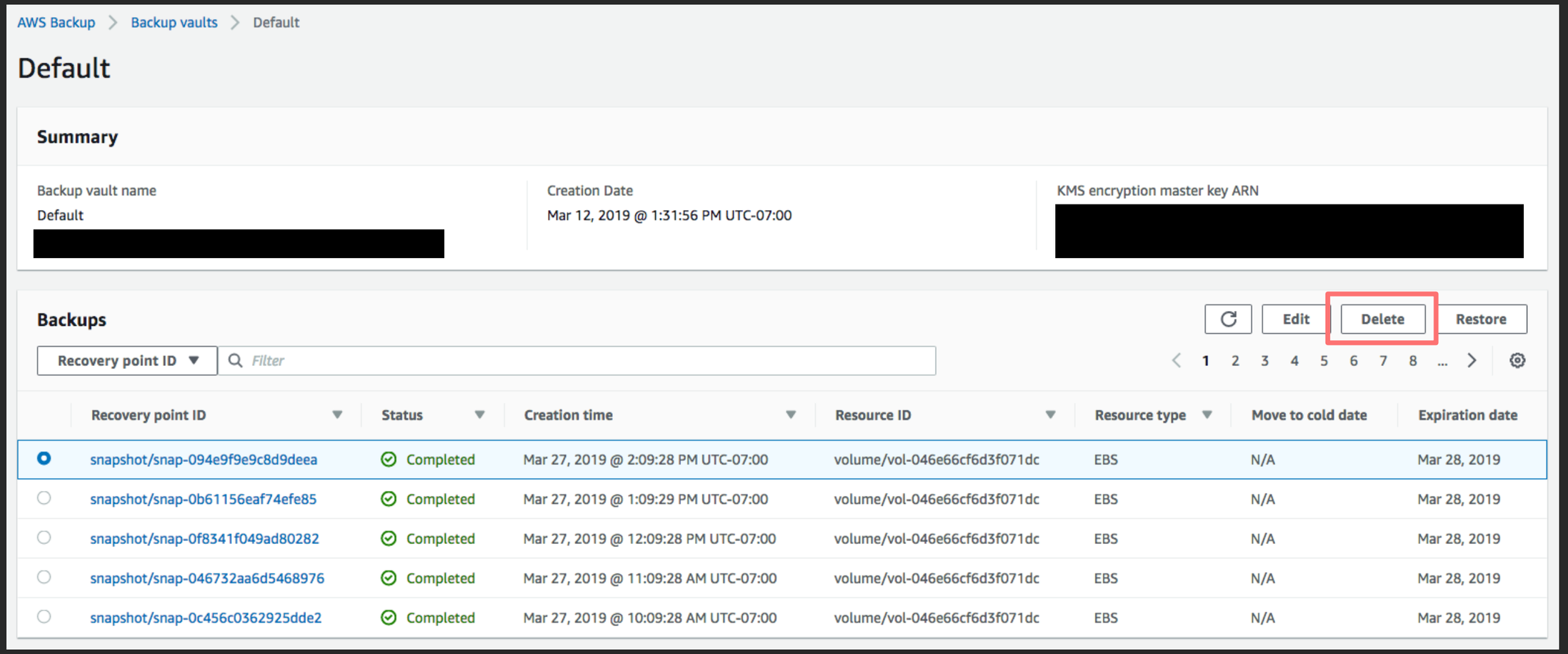
Securing backups walkthrough (5/9)



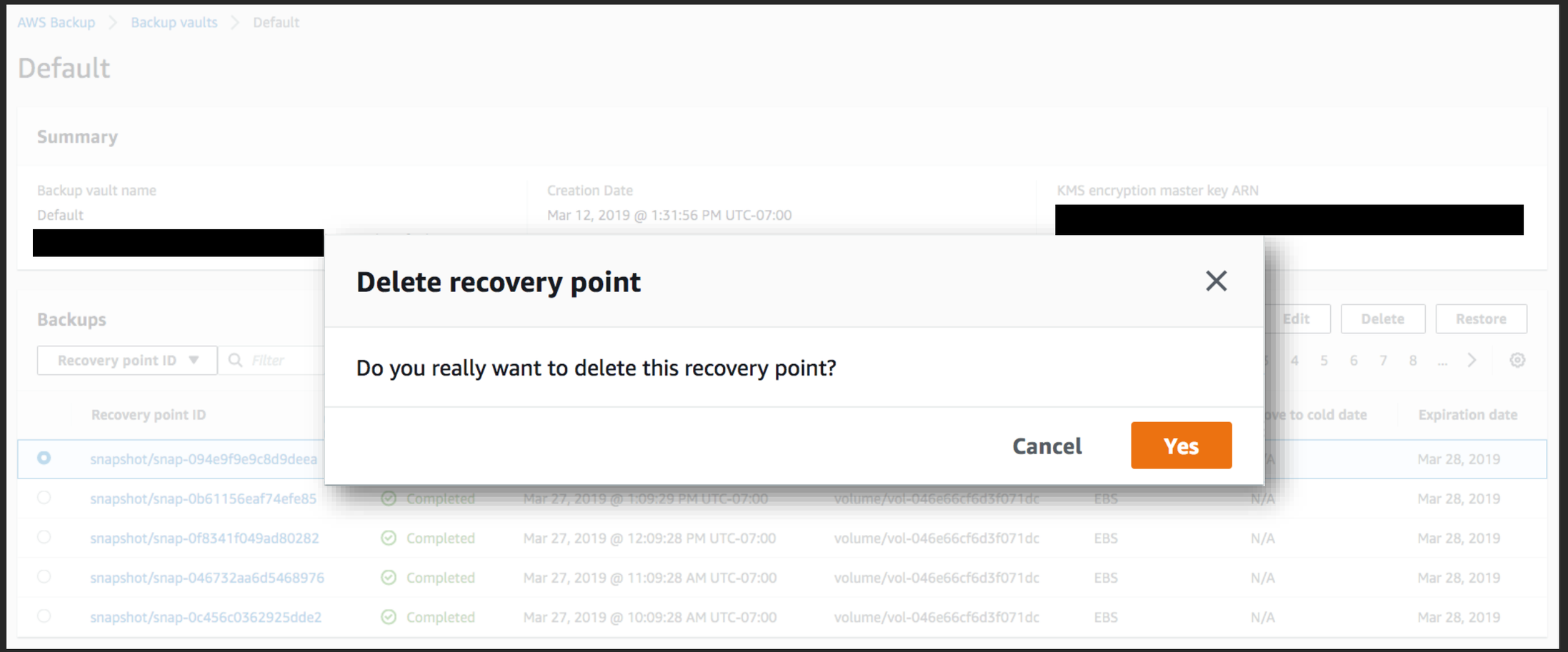
Securing backups walkthrough (6/9)



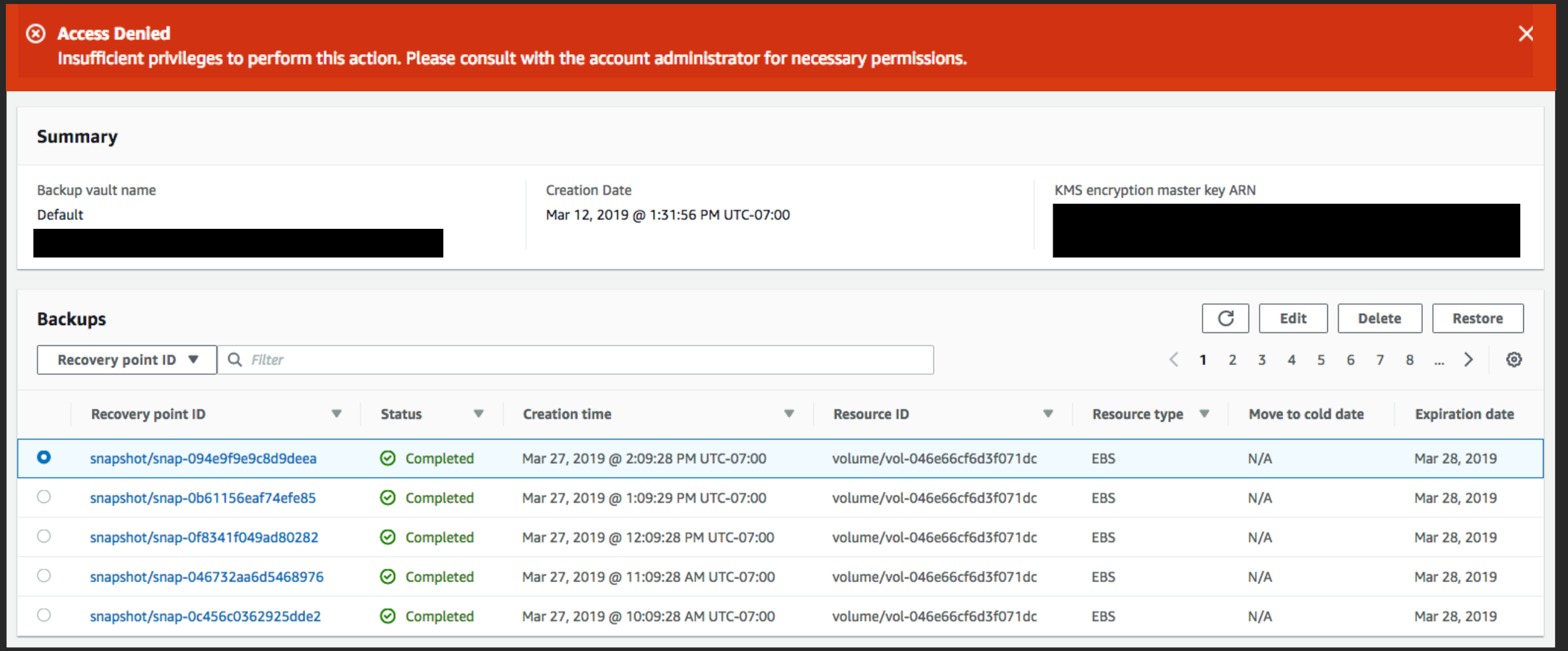
Securing backups walkthrough (7/9)



Securing backups walkthrough (8/9)



Securing backups walkthrough (9/9)



Customer example #2: Safeguarding essential data

This customer, a global enterprise with hundreds of accounts, needs to lock down backups. Specifically, they are concerned about an insider threat and want to separate access to backup data and production data. They also want to ensure that all data is encrypted.

The customer has been experimenting with AWS Backup to protect its assets. They have now asked the service to help them select an option (or options) to protect their backups.

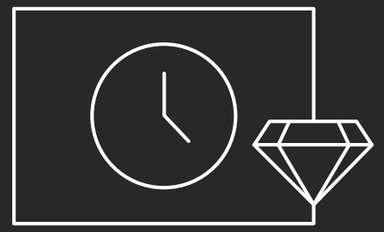
What features can the customer use to provide defense in depth?

Closing out—and some good news

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Preannouncement: Single-file restore for Amazon EFS

January 2020



Restore at the item and folder level in Amazon EFS

- What it does: Allows users to restore individual files or folders in Amazon EFS (by providing the exact path)
- Key benefits: Faster and more granular restores, with overall lower TCO

Preannouncement: Amazon EC2 backup and recovery

January 2020



\+ Amazon EC2

Coordinate backup and restore of whole EC2 instances

- What it does: Allows users to back up and recover at the Amazon EC2/running instance level
- Key benefits: Restore EC2 instances as they were, simplified backup workflow for Amazon EC2

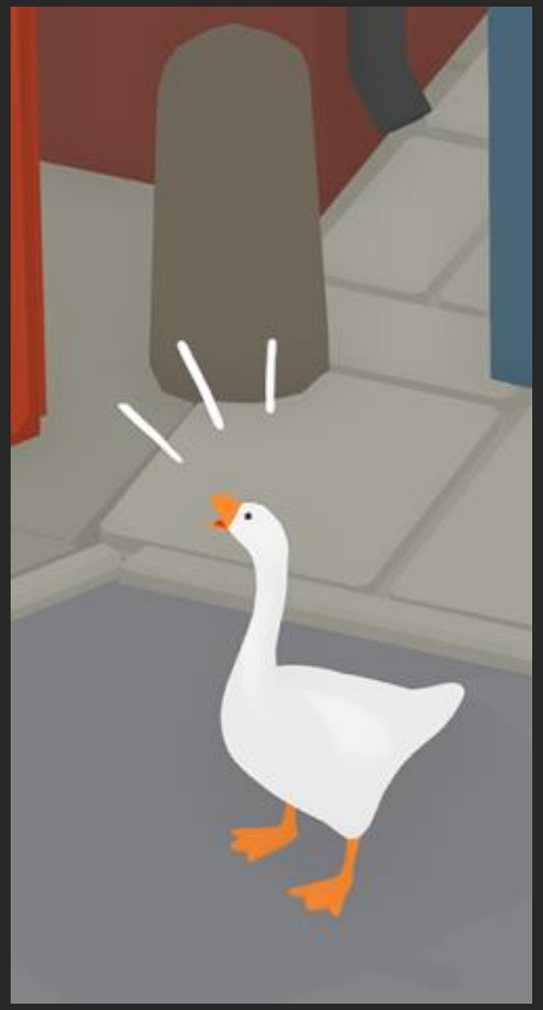
Preannouncement: Cross-Region backup

January 2020



- What it does: Customers can now orchestrate backup copies across regions
- Key benefits: Meet compliance requirements to store data copies a set distance from prod, enable a holistic business continuity strategy

In conclusion



The world is full of geese

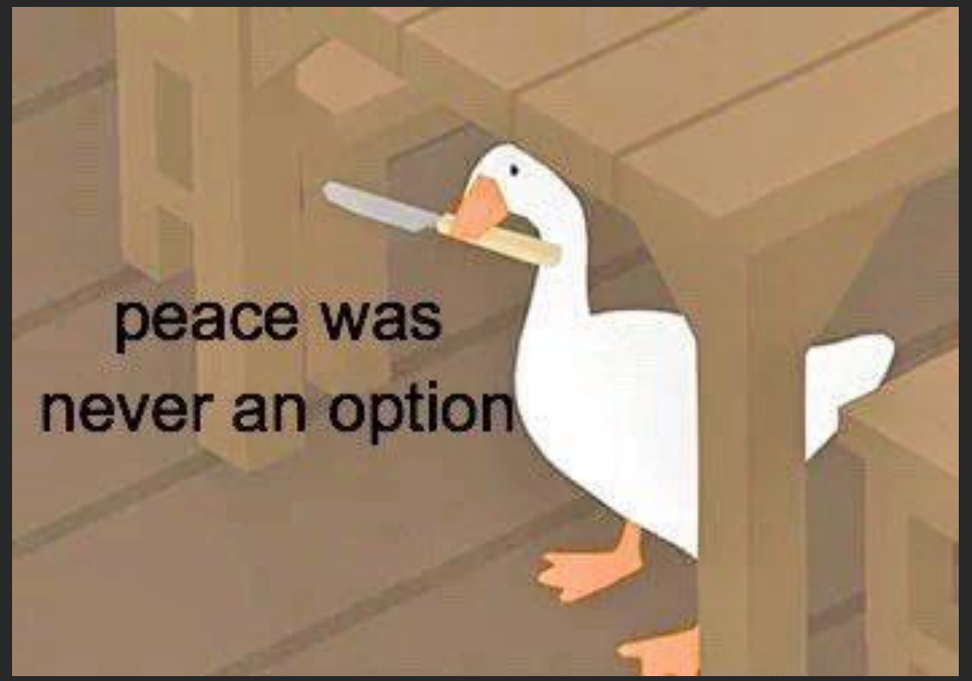
AWS Backup can help you thrive in a goose-strewn world:

- By making it easy to automate backup and recover tasks
- By making it possible to provide layers of security for backup data across multiple services

Want to learn more about AWS Backup and the team?

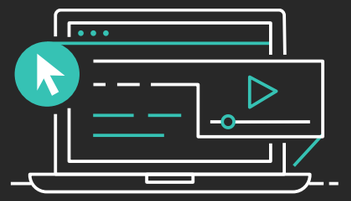
- schilchr@amazon.com

Fin.



Learn storage with AWS Training and Certification

Resources created by the experts at AWS to help you build cloud storage skills



45+ free digital courses cover topics related to cloud storage, including:

- Amazon S3
- AWS Storage Gateway
- Amazon S3 Glacier
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Block Store (Amazon EBS)



Classroom offerings, like Architecting on AWS, feature AWS expert instructors and hands-on activities

Visit aws.amazon.com/training/path-storage/

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws training and certification

Thank you!

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws



Please complete the session survey in the mobile app.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.