PragmaEdge

PragmaEdge

Backup Policies for AWS Cloud

Prepared for Quest.

Version History

Version No.	Date	Brief description of changes	Author
1.0	02/27/2024	Created	Chandu.Boddula

PragmaEdge

Table of Contents

PragmaEdge

1. Introduction

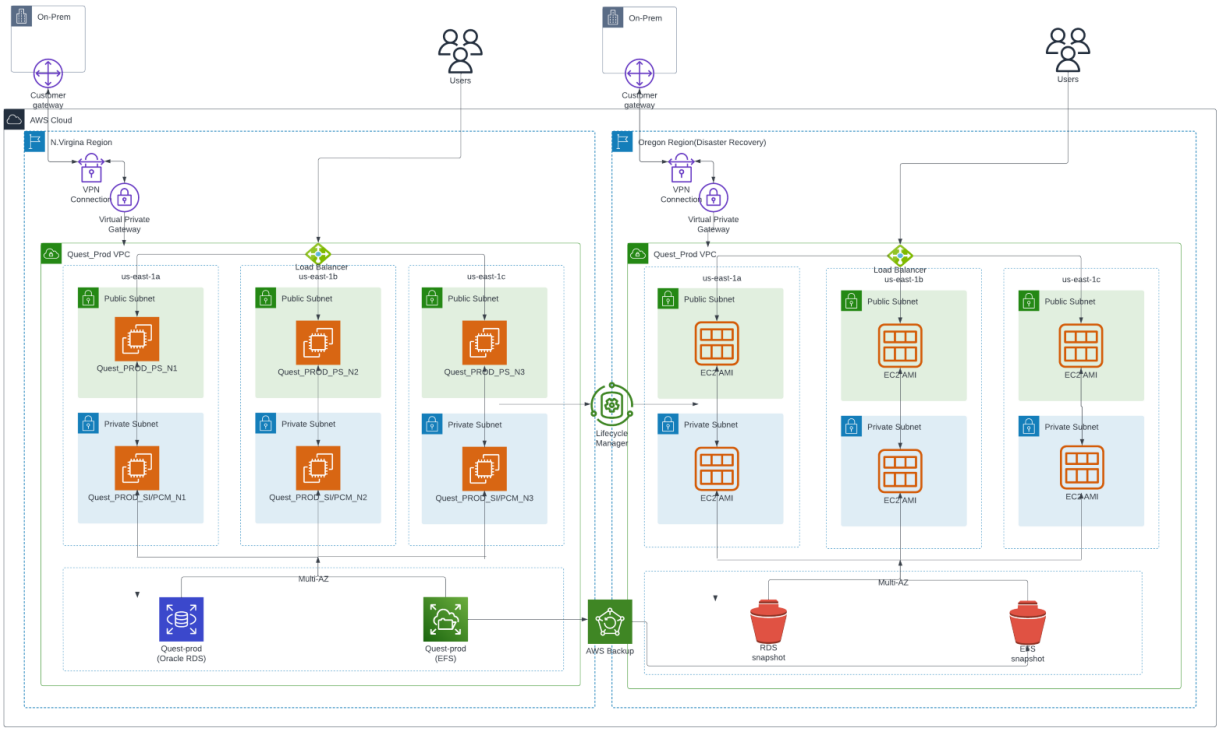
1.1 Purpose

This document walks you through the processes and procedures for backup policies and restoration within Quest infrastructure hosted in the AWS Cloud. Its primary purpose is to ensure regular backups with associated retention policies.

1.2 Scope

This document can be referred to for block storages of virtual machines, databases, EFS provisioned on Quest This document is used to keep track of the resources which we provisioned on AWS Cloud have all the required strategies for the backup and getting to the source state with the backups and to follow the process same for the resources.

2. Backup Policy Architecture of Block Storage Volumes



The above architecture is of Quest client and how we are prepared for disaster recovery.

2.1 Backup Policy for Quest Servers:

- Backup Policy of the Production instance is set up with 2 Volumes attached to the Instance, backed up with the retention of 15 Days and have the 2 recovery points.
- We have two policies configured for this backup policy which takes backups at 1st day of every month and 16th day in another month which stores two server images that are stored in another region which helps in disaster recovery.

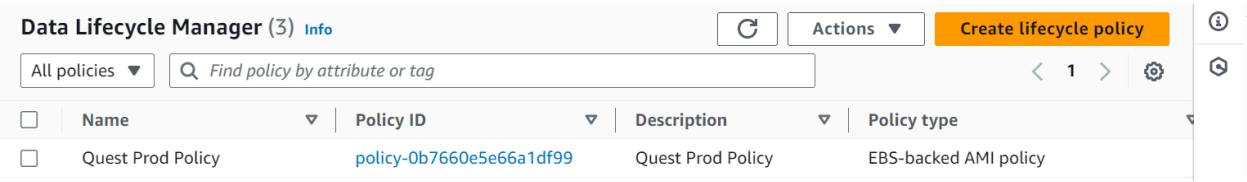
2.1.1 Backup policy for the Quest Production servers:

- We have configured a backup policy for Quest production servers which takes backup of servers twice a month. We have given **Backup:Quest_prod** tag to all the prod instances.

Backup Policy Name	Quest Prod Policy

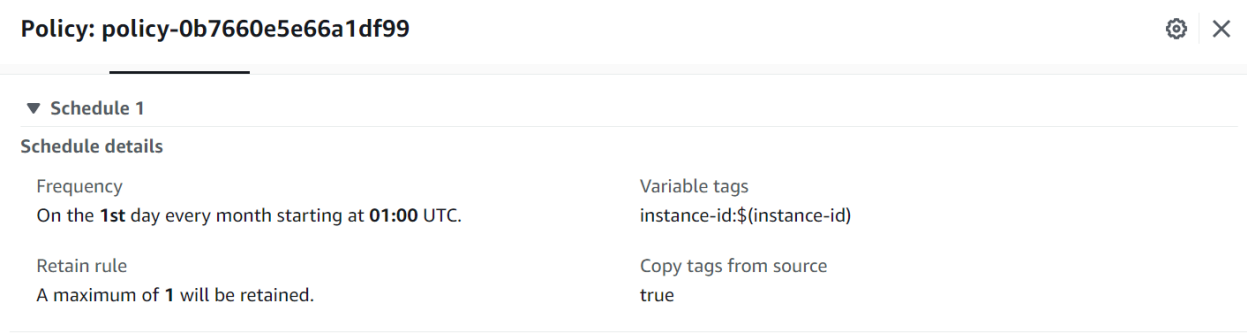
Applied Resources	9 Virtual Servers
Backup Plan Name	Quest Prod Policy
Retention Days	30 Days
Recovery Points	2 AMIs
Frequency	On 1st and 16th day of every month at 01:00 AM UTC

2.1.2Production Backup Policy setup:

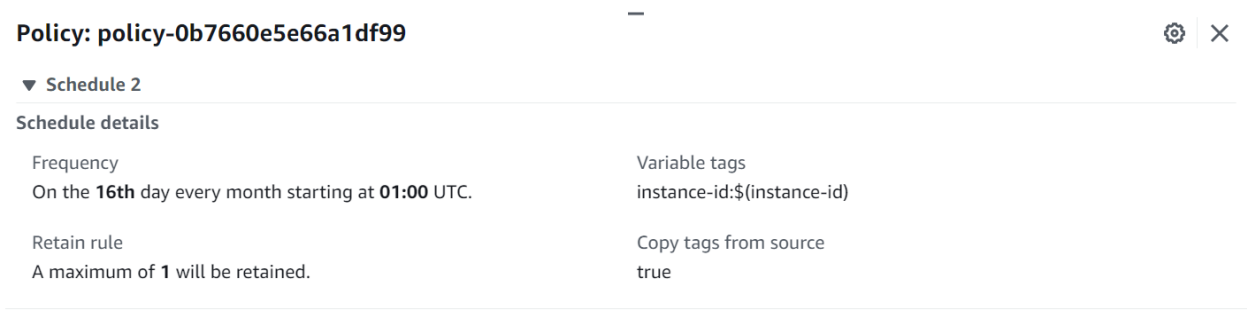


2.2 Backup Plan for the Policy:

Schedule - 1

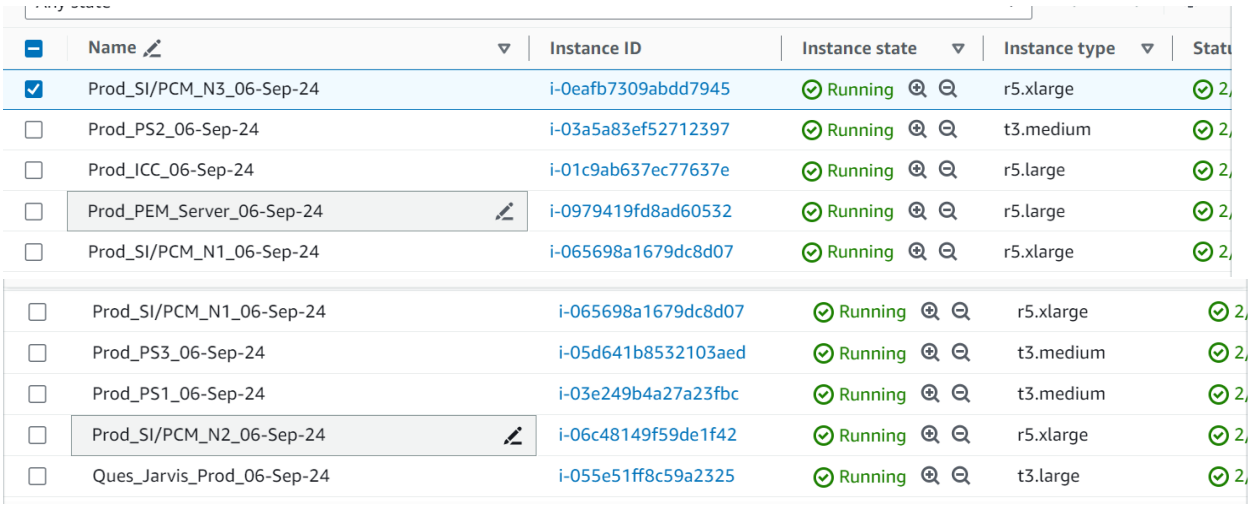


Schedule – 2



Backup Policy Applied Resources:

The instances with the tag: Quest_PROD will be backed up with two schedules



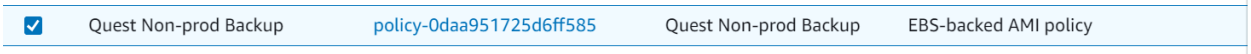
Name	Instance ID	Instance state	Instance type	Statu
Prod_SI/PCM_N3_06-Sep-24	i-0eafb7309abdd7945	Running	r5.xlarge	2/
Prod_PS2_06-Sep-24	i-03a5a83ef52712397	Running	t3.medium	2/
Prod_ICC_06-Sep-24	i-01c9ab637ec77637e	Running	r5.large	2/
Prod_PEM_Server_06-Sep-24	i-0979419fd8ad60532	Running	r5.large	2/
Prod_SI/PCM_N1_06-Sep-24	i-065698a1679dc8d07	Running	r5.xlarge	2/
Prod_SI/PCM_N1_06-Sep-24	i-065698a1679dc8d07	Running	r5.xlarge	2/
Prod_PS3_06-Sep-24	i-05d641b8532103aed	Running	t3.medium	2/
Prod_PS1_06-Sep-24	i-03e249b4a27a23fbc	Running	t3.medium	2/
Prod_SI/PCM_N2_06-Sep-24	i-06c48149f59de1f42	Running	r5.xlarge	2/
Ques_Jarvis_Prod_06-Sep-24	i-055e51ff8c59a2325	Running	t3.large	2/

2.3 Non-production Backup Policy

Non-Production backup policy is used to back up the volumes attached to the Non-Production Virtual Instances by using tags. These volumes will be backed up with consistency groups which includes Boot volume and Data volume of the Virtual Instance.

Backup Policy Name	Quest Non-prod Backup
Applied Resources	05 Virtual Instances
Backup Plan Name	Quest Non-prod Backup
Retention Days	30 Days
Recovery Points	2 AMIs
Frequency	On 1st and 16th day of every month at 01:00 AM UTC

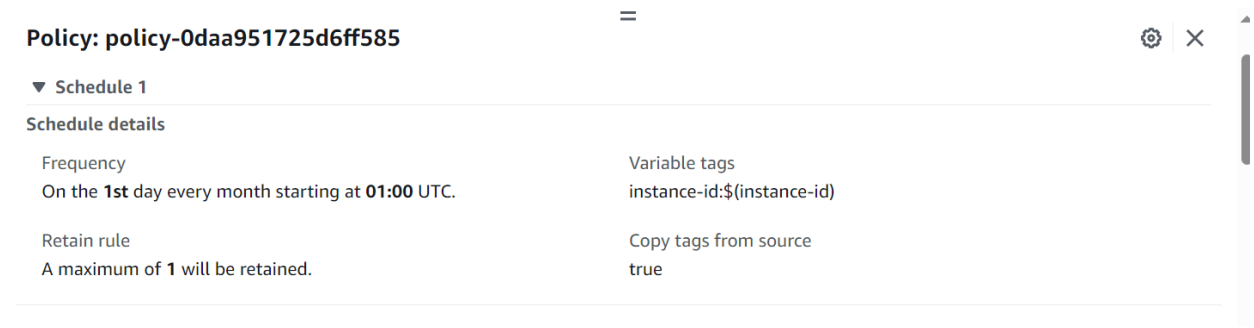
2.3.1 Non_Production Backup Policy setup:



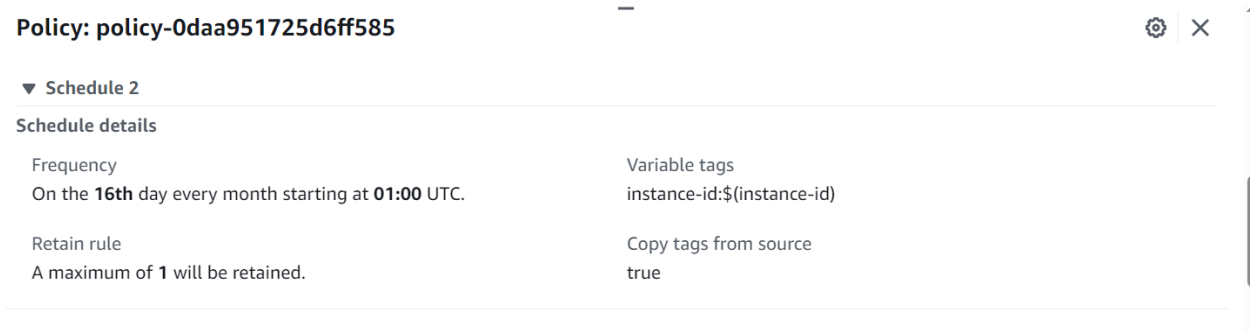
Quest Non-prod Backup	policy-0daa951725d6ff585	Quest Non-prod Backup	EBS-backed AMI policy

Backup Plan for the Policy:

Schedule –1



Schedule –2



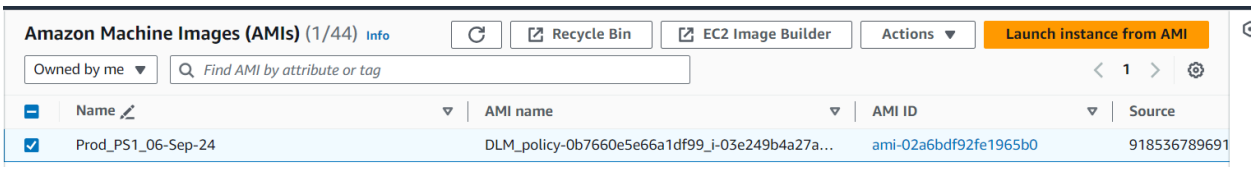
Backup Policy Applied Resources:

The instances with the tag: Quest_NP will be backed up with two schedules

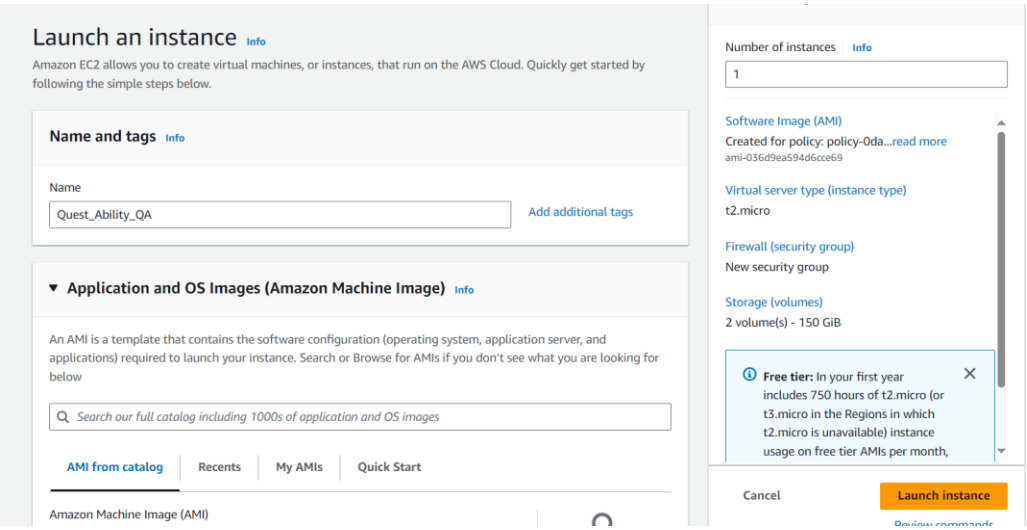
Name	Instance ID	Instance state	Instance type	Stat
QA_PS_N2_06-Sep-24	i-0a17ddfc689bead8e	Running	t3.small	
QA_ICC_06-Sep-24	i-09f5a15ac820875d4	Running	r5.large	
QA_SI/PCM_N2_06-Sep-24	i-0f9cf23aebfa07eb2	Running	r5.large	
QA_PS_N1_06-Sep-24	i-06419d8ff7cf749ef	Running	t3.small	
QA_SI/PCM_N1_06-Sep-24	i-05731bd7c57759305	Running	r5.large	

2.4 Restore Process:

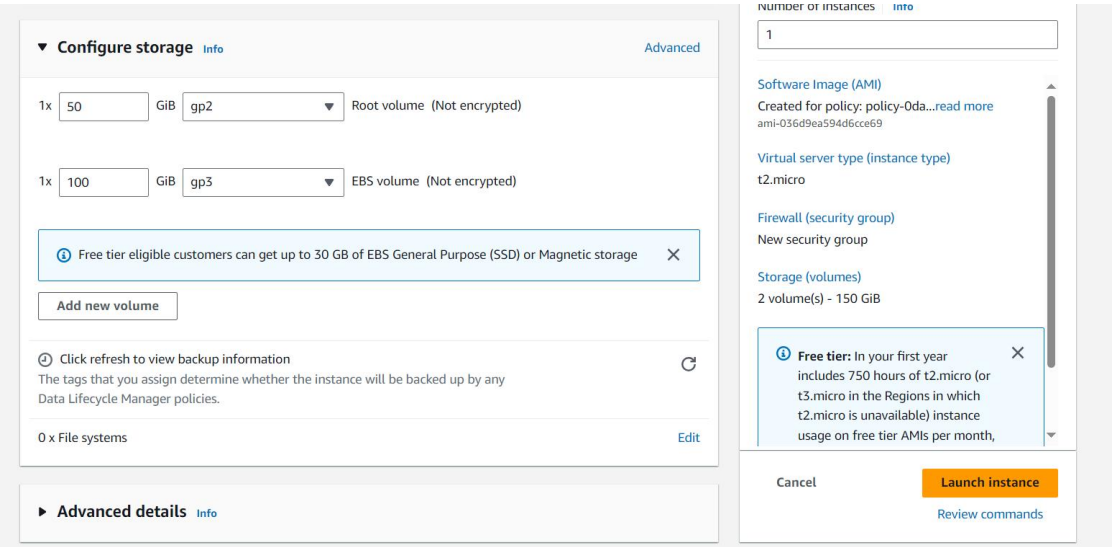
- Navigate to the Amazon Machine Image (AMI) and from the console click on Launch Instance from AMI so that it includes the location, image, data and boot snapshots from the Source Instance.



Now we must write the Name of the server, SSH Key, Network Interface and rest of the components such as Image, Profile, Volumes and VPC are default included as same as the source Instance



Below are the snips to create the server with the snapshots created as the consistency group, including volumes attached to the Virtual Instance.

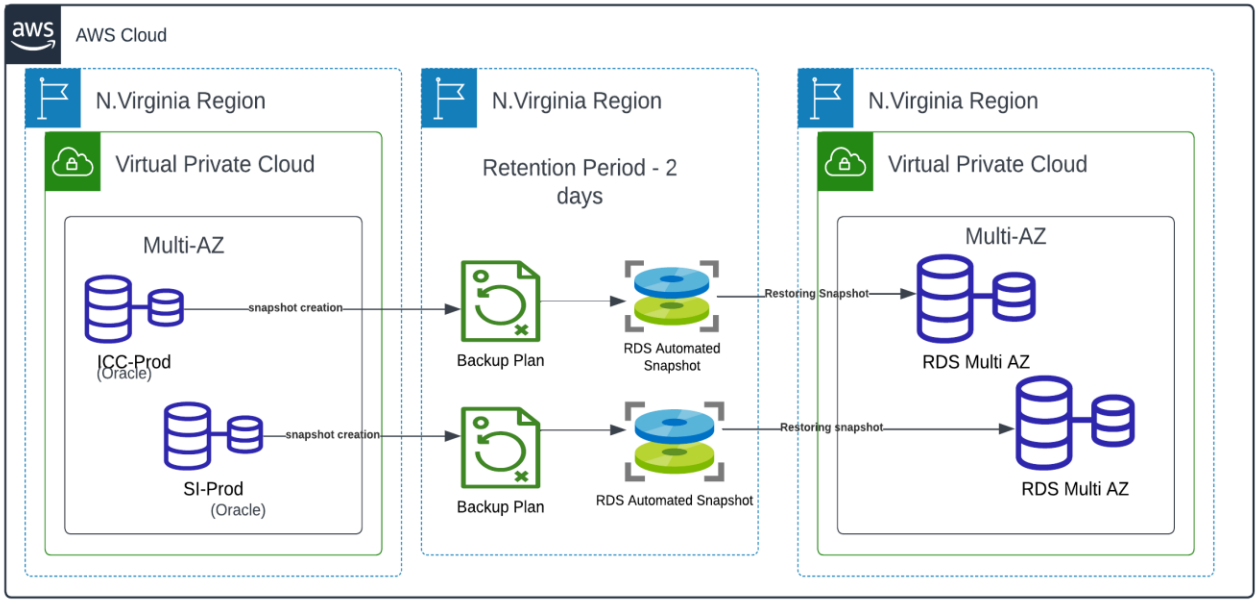


Now we must write the Name of the server, SSH Key, Network Interface and rest of the components such as Image, Profile, Volumes and VPC are default included as same as the source Instance.

Note: We have Included the Backup Policy for Production and Non-Production and the procedure for the backups to be taken.

3. RDS Database

3.1 RDS Database Backup Architecture

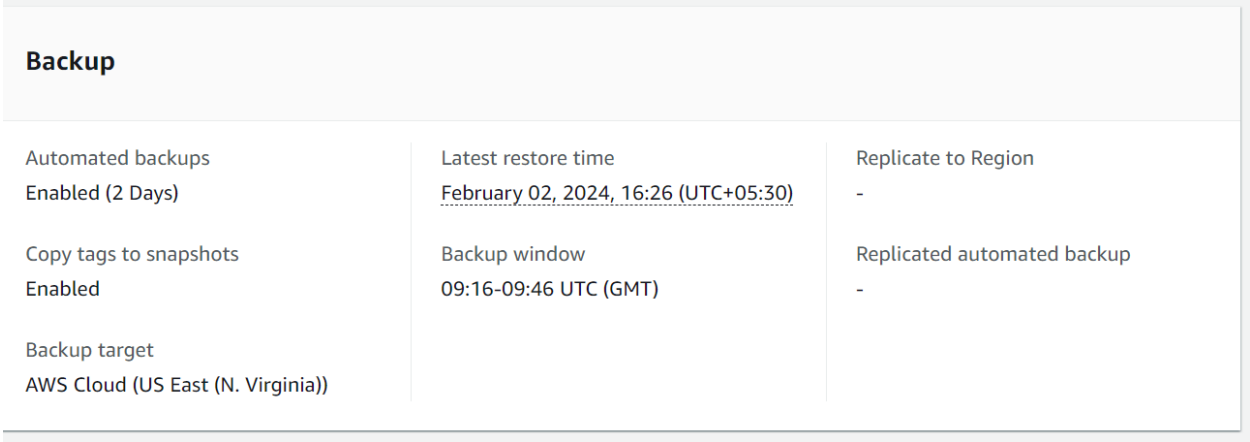


1. We have Two RDS (Oracle) in Quest Production environment Prod-ICC and SI-Prod with multi-AZ for high availability.
2. For both the databases Primary AZ will be US-east-1c and Secondary will be US-east-1b.
3. The RDS has an automatic backup method while launching the DB instance itself
4. We have enabled automatic backup in both the RDS.

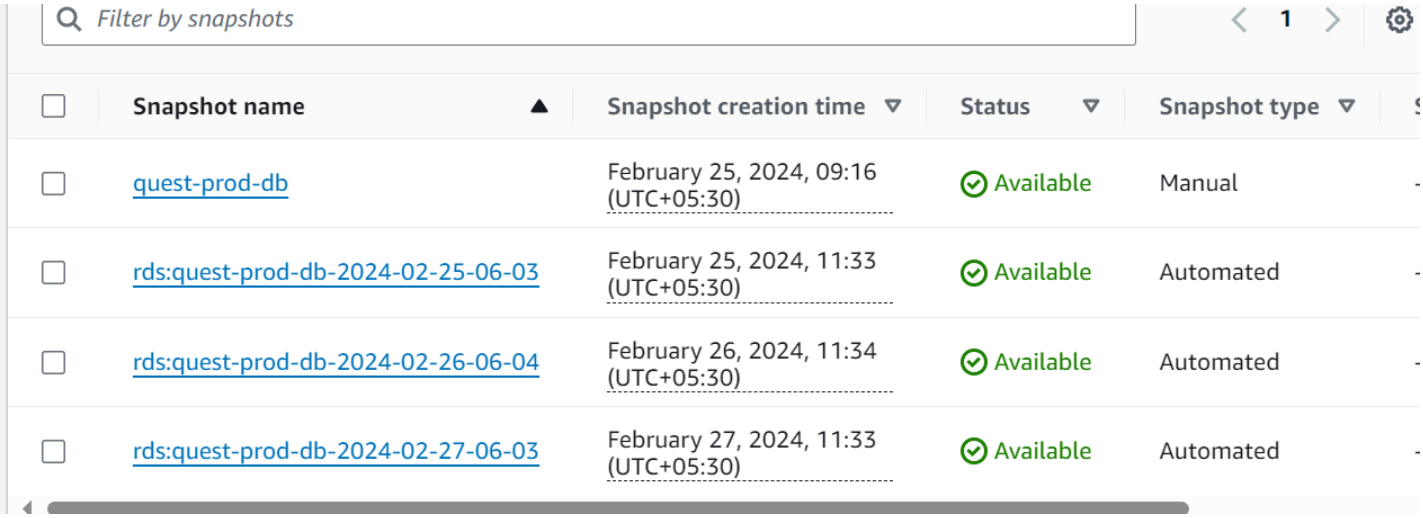
5. Backup Frequency for ICC-Prod-DB: Every day at 09:16AM UTC.
6. Backup Frequency for SI-DB: Every day at 05:55AM UTC.

Backup Policy Retention	2 Days
Recovery Points	1 RDS
Replicas	Replicas across 2 Zones within the region.
Backup Process	Automatic, Manual Backups
Frequency	Every day at 05:55AM UTC.

3.2 RDS Database Backup Policy



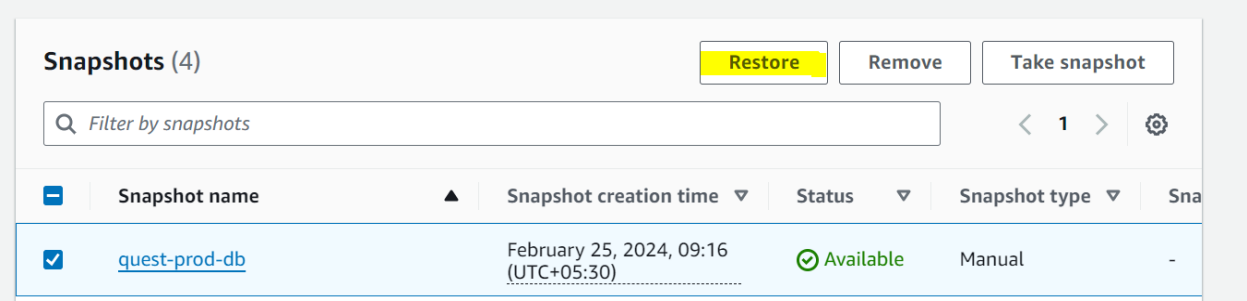
Below is the snip for Ongoing Backups of an RDS instance.



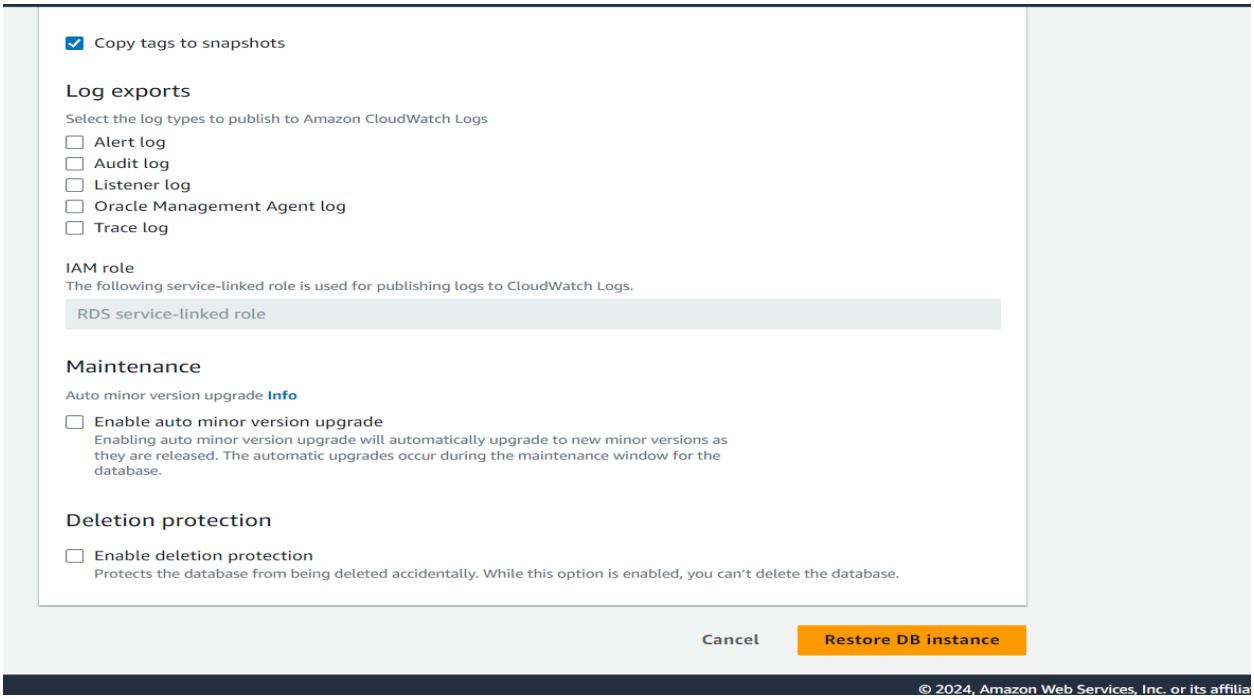
3.3 RDS Database Restore Process:

Database Name: Quest-prod-db

Select the Target DB and click on Backup and Maintenance then click on Restore.

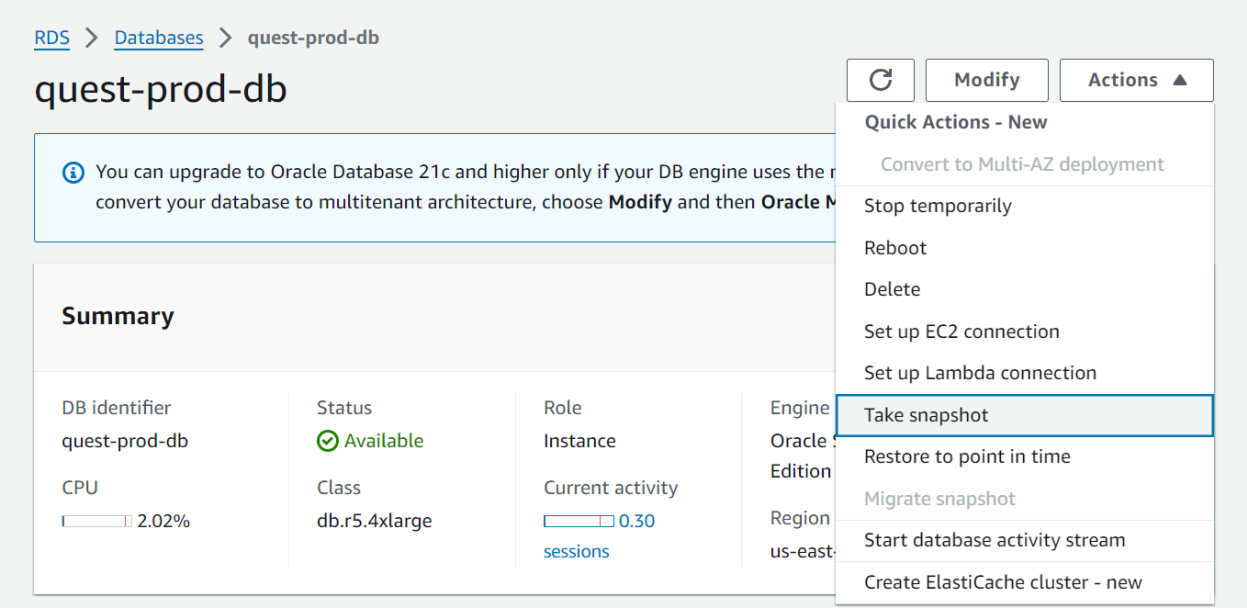


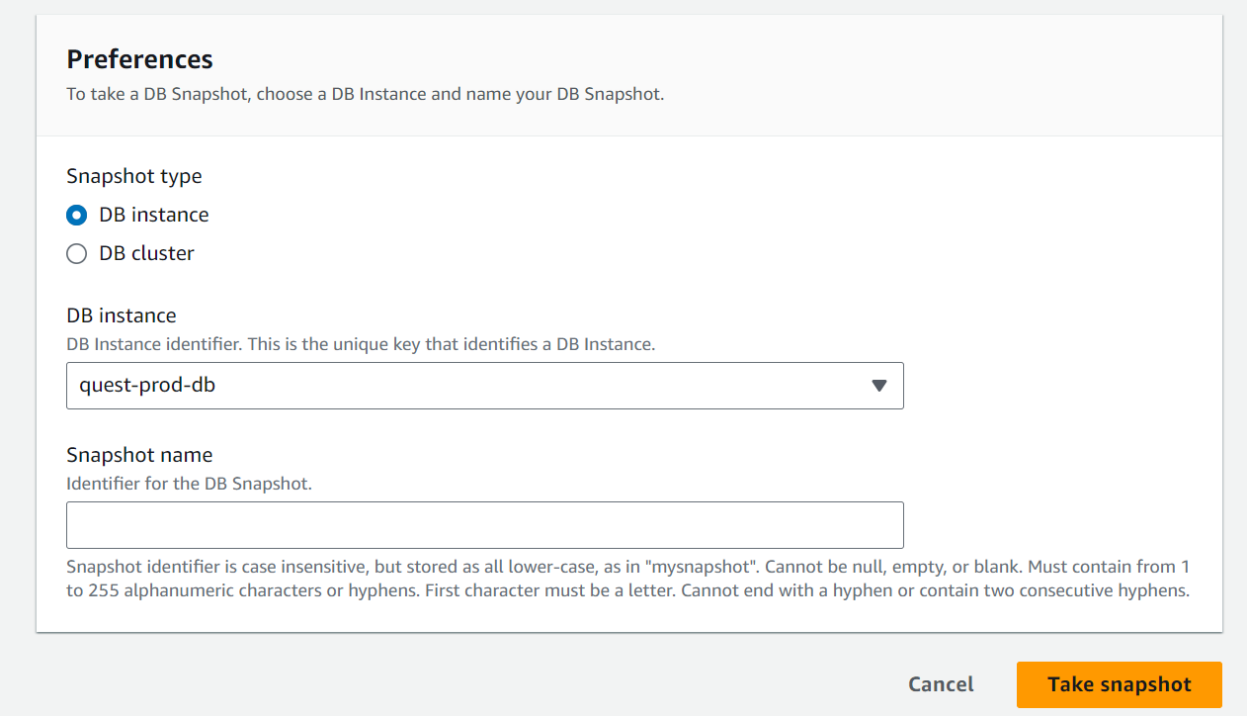
Keep all the configurations as it is and click on Restore DB Instance.



3.4 Manual Backup Process in RDS

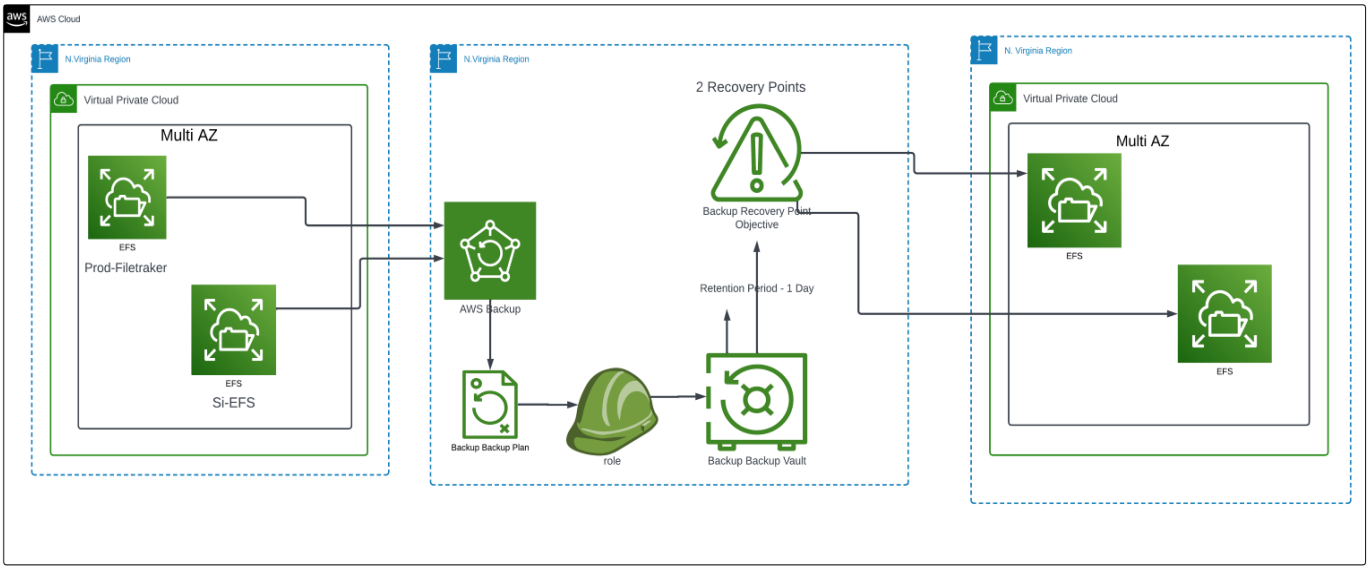
For taking the backup manually. We need to select the database. Go to the action, select take snapshot option





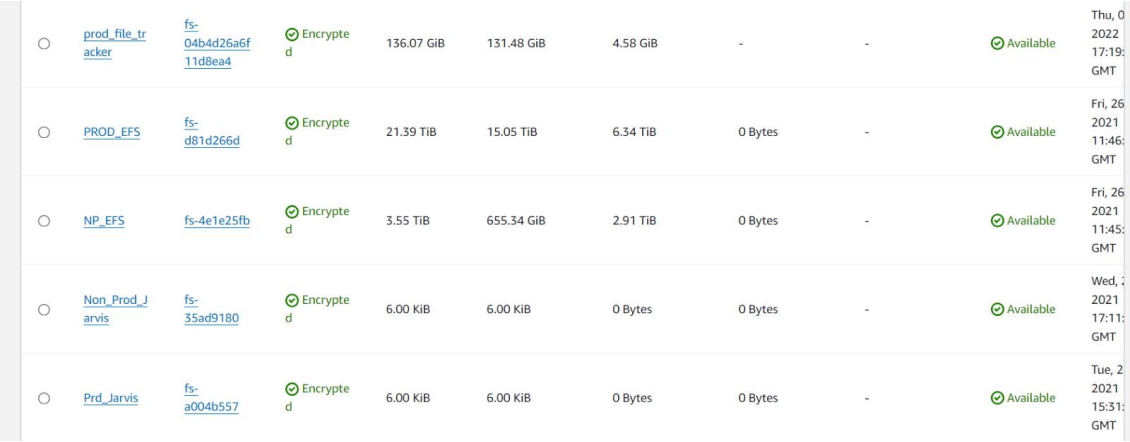
Select DB Instance , Click on take Snapshot to create a snapshot manually.

4. EFS PROD BACKUP ARCHITECTURE



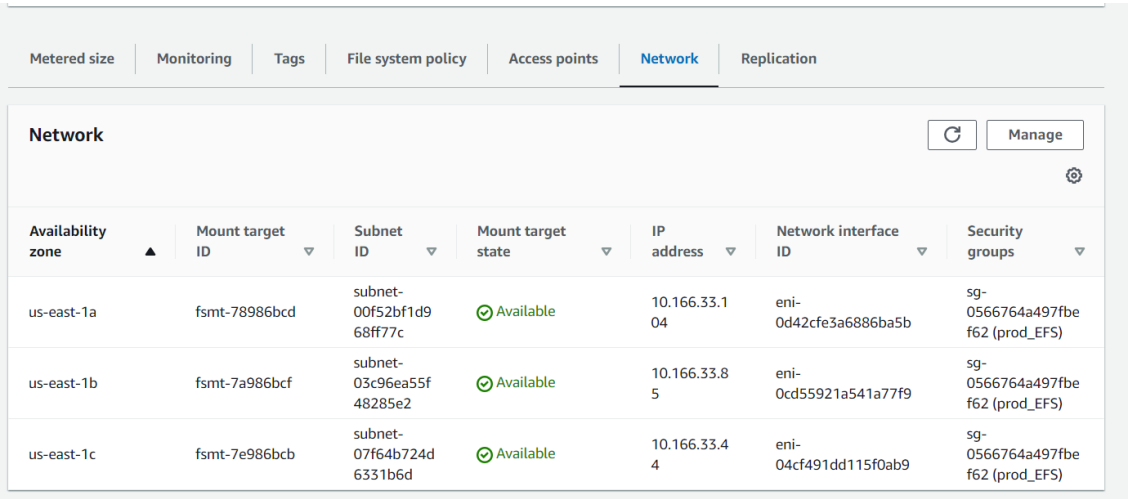
1. We have two EFS in Quest Production Environment within regional type which is in N.Virginia, us east-1a, us east-1b and us east-1c
2. We have an AWS Backup service to create snapshots of EFS based on the configurations defined in Backup plan/rule and it uses an IAM role to have full access of EFS for snapshot creation. Once aws backup creates a snapshot it stores in Backup Vault as a Recovery point. From that Recovery point we can restore the EFS backup as required.
3. We can restore the EFS using recovery point as per our requirement for example, whole EFS or a particular path of EFS.
4. It has a single copy backup in N.Virginia
5. Backup Frequency: Every day at 5AM UTC.
6. Backup Retention: 1 Day

Backup Policy Name	aws/efs/automatic-backup-plan
Applied Resources	2 EFS
Backup Plan Name	aws/efs/automatic-backup-plan
Retention Days	1 Day
Recovery Points	1 EFS
Frequency	Every day at 5Am UTC



○	prod_file_tracker	fs-04b4d26a6f11d8ea4	Encrypted	136.07 GiB	131.48 GiB	4.58 GiB	-	-	Available	Thu, 0 2022 17:19: GMT
○	PROD_EFS	fs-d81d266d	Encrypted	21.39 TiB	15.05 TiB	6.34 TiB	0 Bytes	-	Available	Fri, 26 2021 11:46: GMT
○	NP_EFS	fs-4e1e25fb	Encrypted	3.55 TiB	655.34 GiB	2.91 TiB	0 Bytes	-	Available	Fri, 26 2021 11:45: GMT
○	Non_Prod_Jarvis	fs-35ad9180	Encrypted	6.00 KiB	6.00 KiB	0 Bytes	0 Bytes	-	Available	Wed, 2021 17:11: GMT
○	Prd_Jarvis	fs-a004b557	Encrypted	6.00 KiB	6.00 KiB	0 Bytes	0 Bytes	-	Available	Tue, 2 2021 15:31: GMT

- The Quest Prod EFS is highly available in 3 availability zones: us-east-1a, us-east-1b and us-east-1c



Metered size | Monitoring | Tags | File system policy | Access points | **Network** | Replication

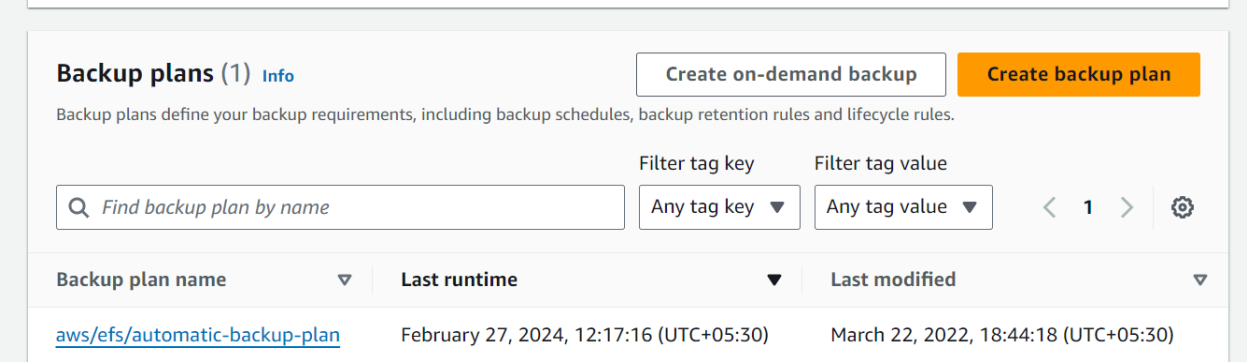
Network

Manage

Availability zone	Mount target ID	Subnet ID	Mount target state	IP address	Network interface ID	Security groups
us-east-1a	fsmt-78986bcd	subnet-00f52bf1d968ff77c	Available	10.166.33.104	eni-0d42cfe3a6886ba5b	sg-0566764a497fbef62 (prod_EFS)
us-east-1b	fsmt-7a986bcf	subnet-03c96ea55f48285e2	Available	10.166.33.85	eni-0cd55921a541a77f9	sg-0566764a497fbef62 (prod_EFS)
us-east-1c	fsmt-7e986bcb	subnet-07f64b724d6331b6d	Available	10.166.33.44	eni-04cf491dd115f0ab9	sg-0566764a497fbef62 (prod_EFS)

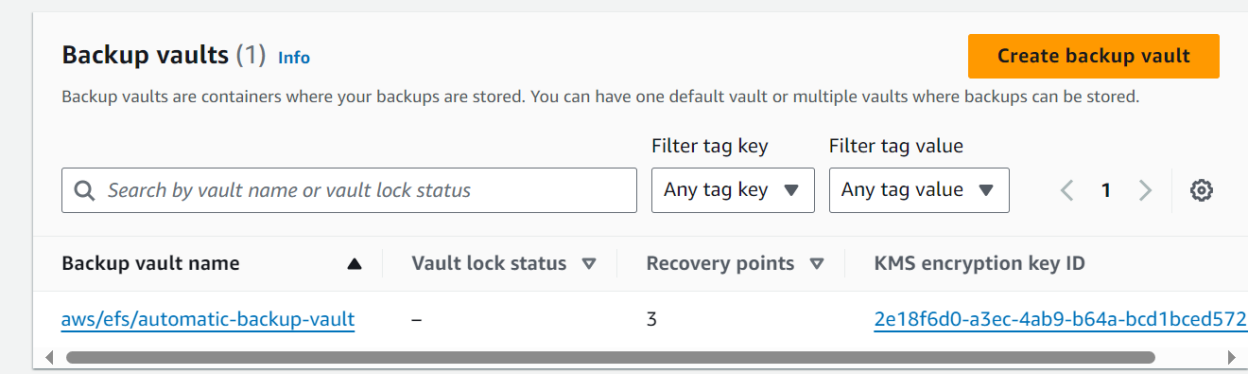
4.1 EFS backup Policy

We have AWS Backup plan for automatic backup of EFS which takes backup of file share with frequency of every day

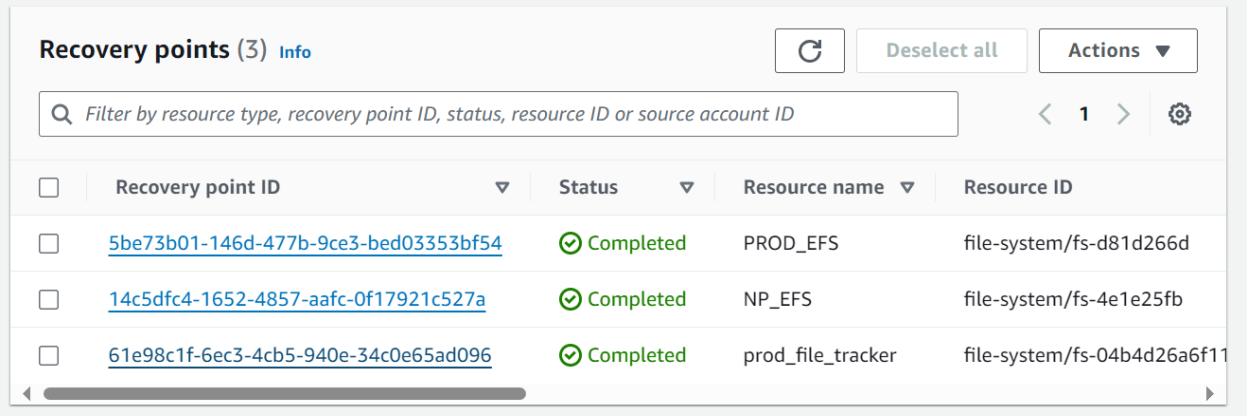


4.2 Restore EFS from AWS Backup Vault

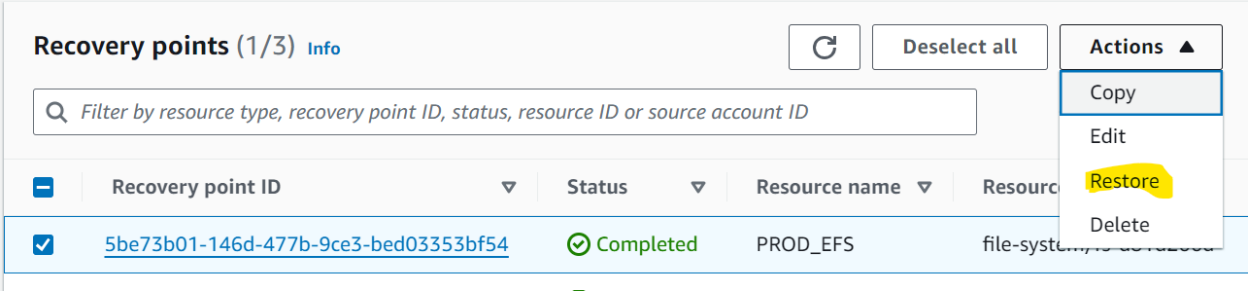
Go to AWS Backup--> Backup Vaults



Select the backup vault where you have the EFS backups stored.



Select the latest recovery point.



Select the restore type and other required settings --> Restore Backup.