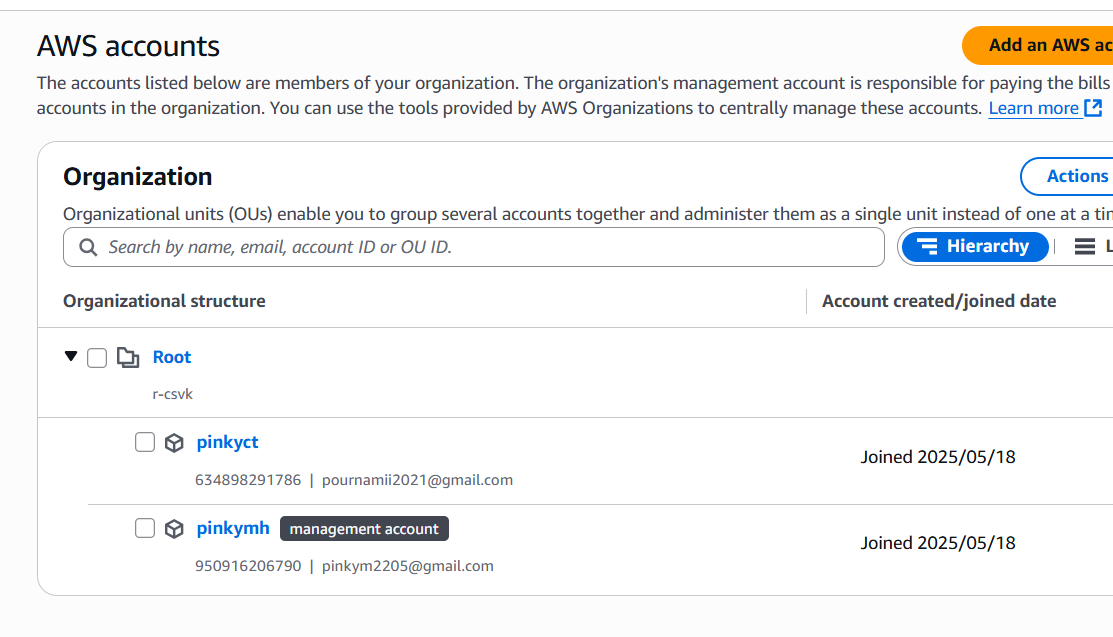
**Case Study-3:**

**Problem Statement:** A company is reviewing its AWS account security policies. The company has staff members in different countries and wants to monitor its AWS accounts for **unusual behavior** that is associated with an IAM identity. The company wants to send a **notification** to any staff member for whom unusual activity is detected. The company needs to manage its multiple AWS accounts to capture **consolidated billing** to help the finance team; store all billing reports in Account-B's S3 bucket. Along with this Account-A's EC2 instances need permissions to access Account-B's S3 bucket to develop the final report.

**CASE3 :TASK1:** The company has staff members in different countries and wants to monitor its AWS accounts for **unusual behavior** that is associated with an IAM identity. The company wants to send a **notification** to any staff member for whom unusual activity is detected

* TASK 1: Detect **unusual IAM activity** (e.g., login from foreign IP, use of sensitive APIs).
* Automatically **notify the specific IAM user** (staff) when that occurs.
* Works across **multiple AWS accounts** (via AWS Organizations).

Since I need to monitor different accounts for unusual behavior; created AWS organization as seen below:



To monitor AWS accounts for **unusual behavior associated with IAM identities** and **send notifications to staff**, implemented a solution using services such as:

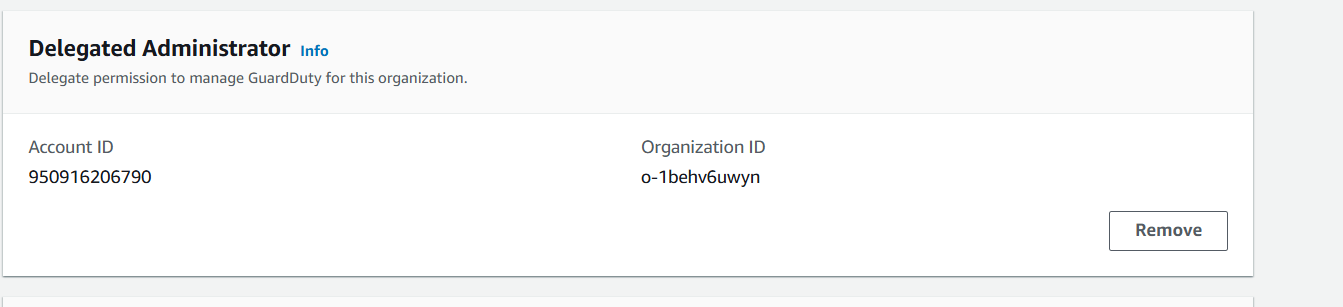
* **Amazon GuardDuty** (for threat detection)
* **Amazon CloudWatch / EventBridge** (for event monitoring and rules)
* **Amazon SNS** (for notifications)

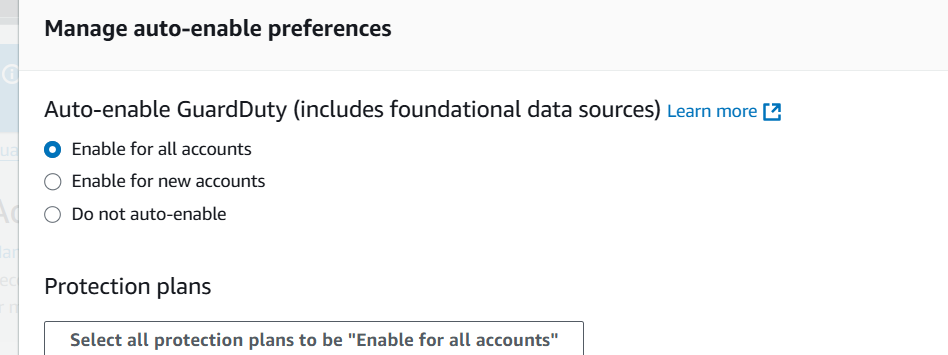
**Step 1: Enable GuardDuty**

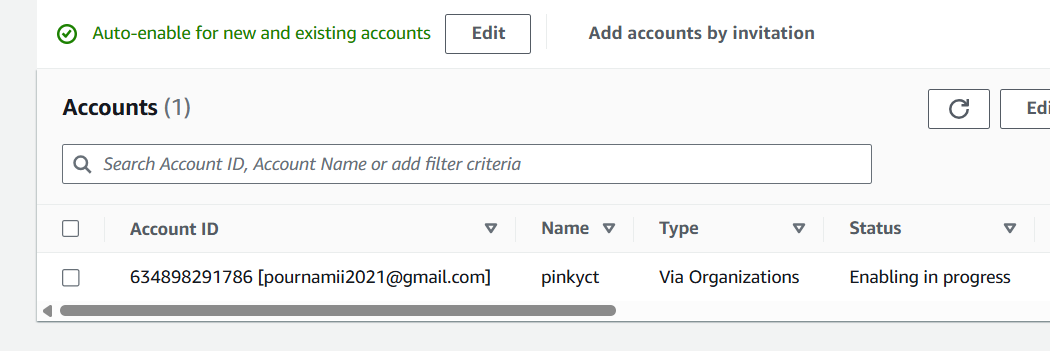
GuardDuty analyzes AWS logs (CloudTrail, VPC Flow Logs, DNS logs) to detect suspicious activity.

With multiple accounts, enabled **GuardDuty Organizations** for centralized findings.

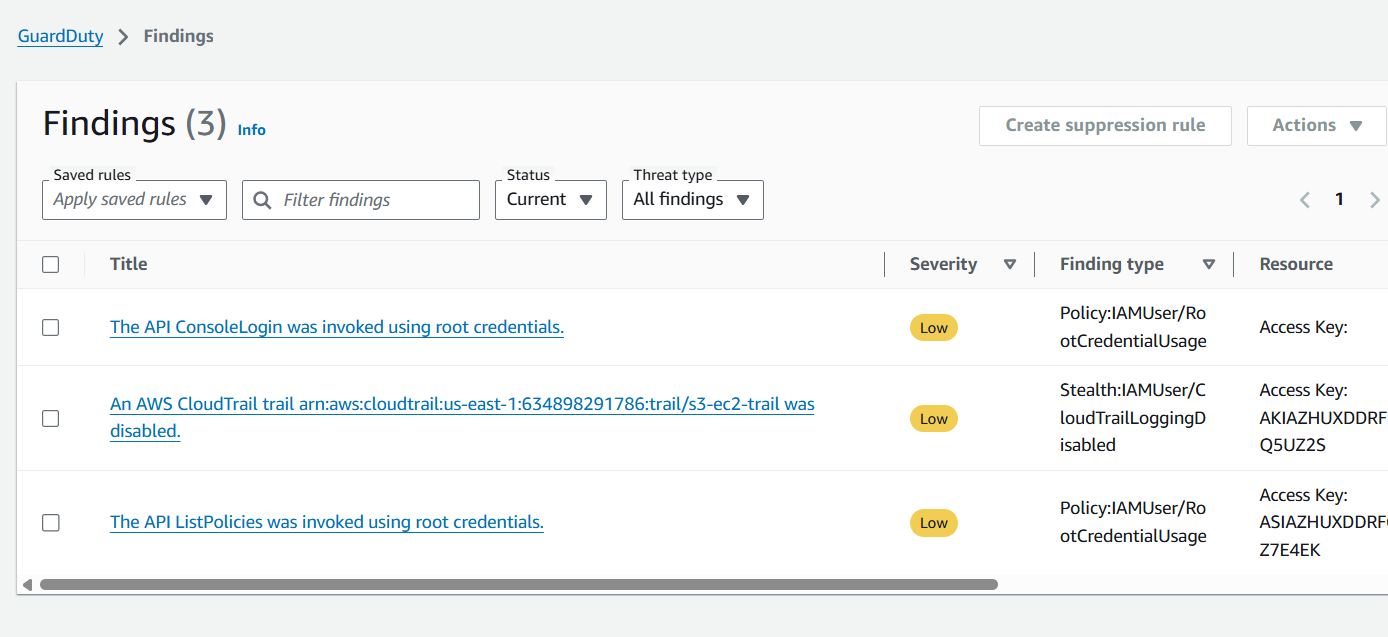
Since I was using Aws organisations;I delegate the Gurad duty administrator as management Account.. So the member account also has been added guarduty protection.

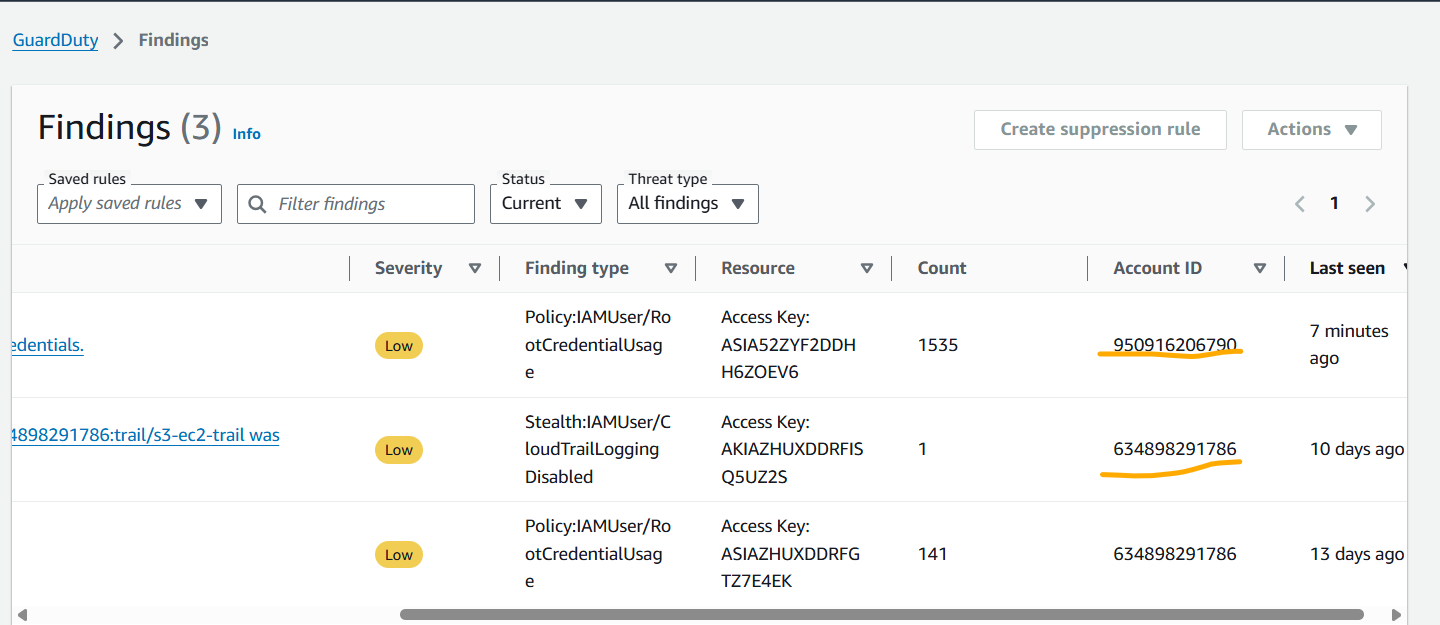






Enabled Guard Duty and it captured the findings for both the accounts as shown below:





Step 2: To enable notification

**Amazon SNS-> created a new Topic called: IAMUnusualActivityAlerts**

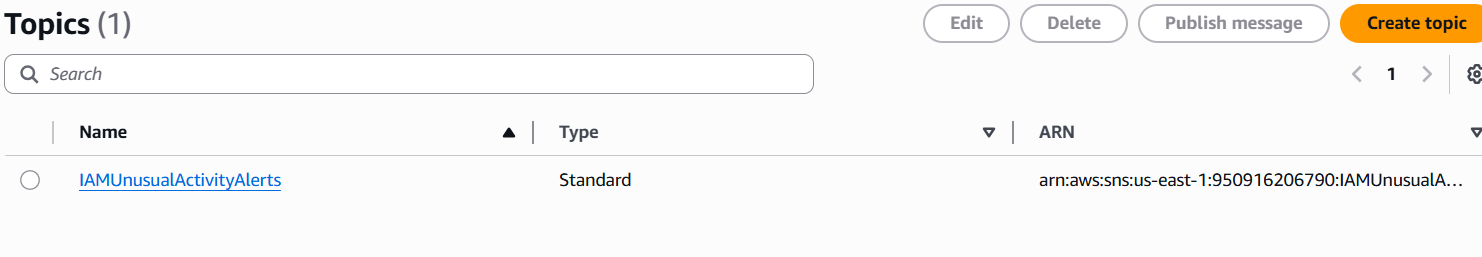
**Add Email Subscriptions**

**Configured the subscription by selecting email as protocol and endpoint as staff member's email address ( Here I given my email ID)**

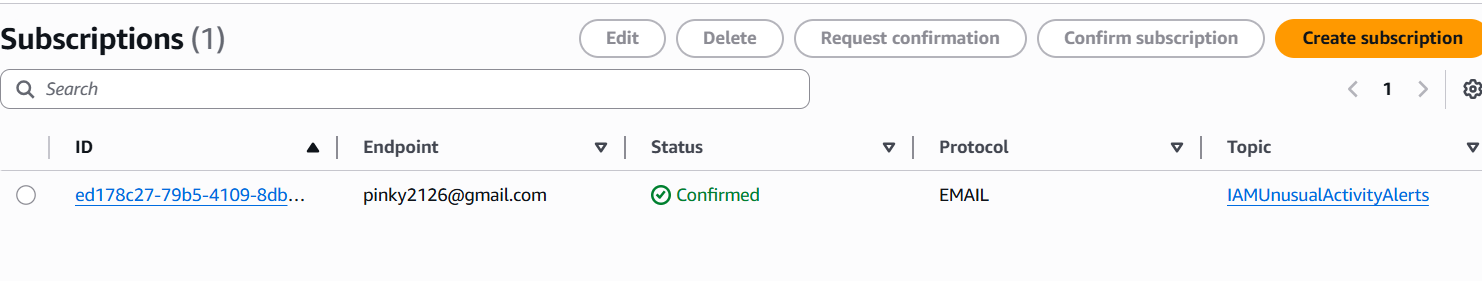
**Created subscription**

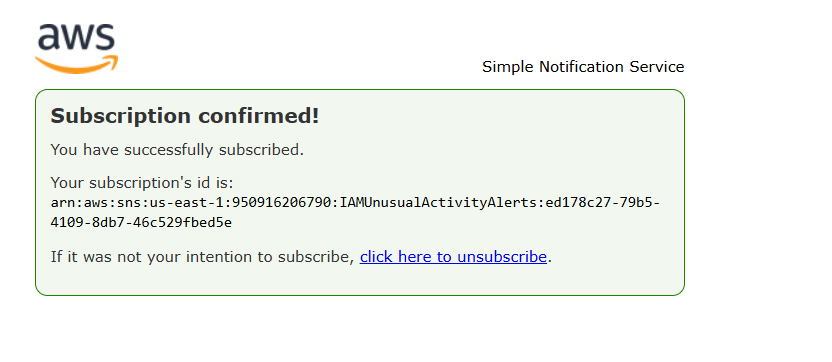
**SNS Screenshots:**

**Created Topic**

****

**Created subscription:**

****

****

**Step 3: Created an EventBridge Rule for GuardDuty Findings**

1. Event source: Guardduty
2. Added event pattern like:

{

"source": ["aws.guardduty"],

"detail-type": ["GuardDuty Finding"],

"detail": {

"resource": {

"accessKeyDetails": {

"userType": ["IAMUser"]

}

},

"severity": [4, 5, 6, 7, 8], // Medium to high severity

"type": [{

"prefix": "UnauthorizedAccess"

}]

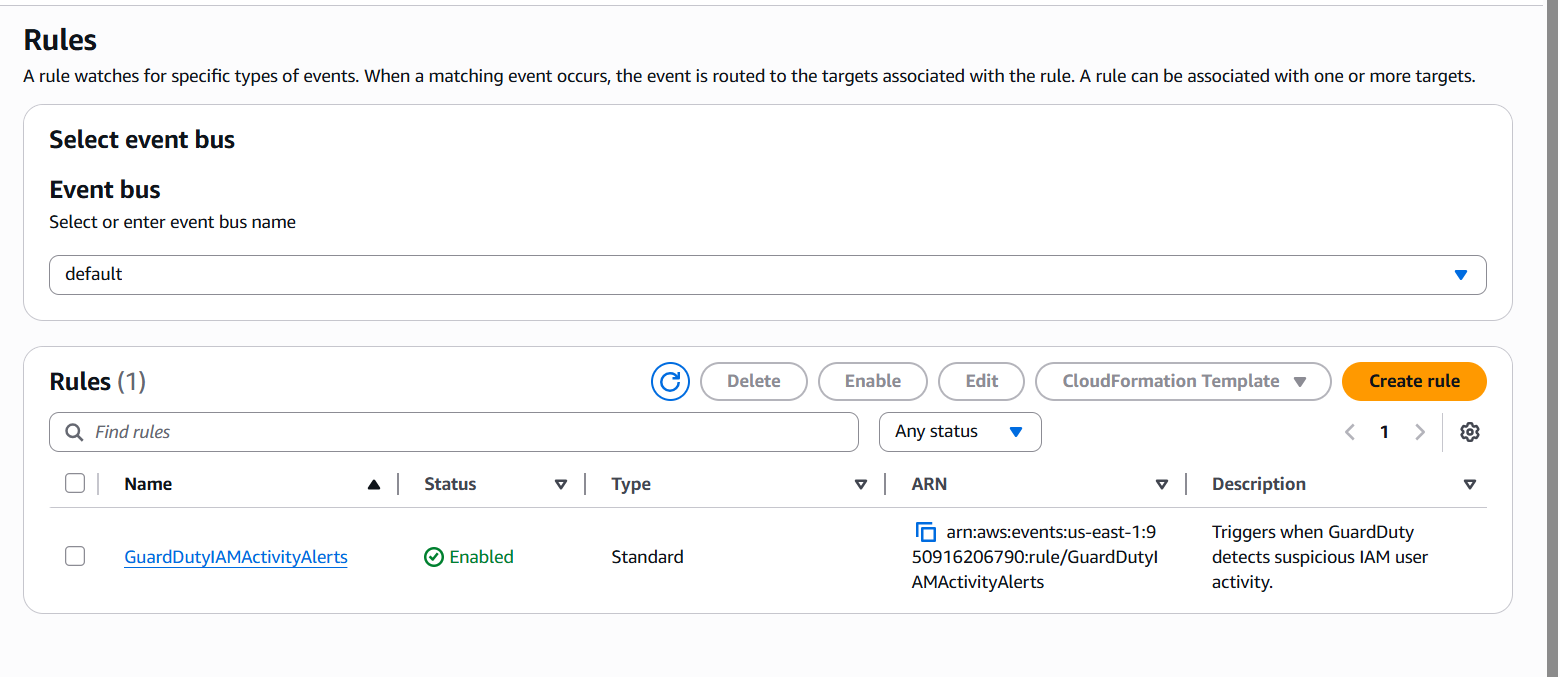
}

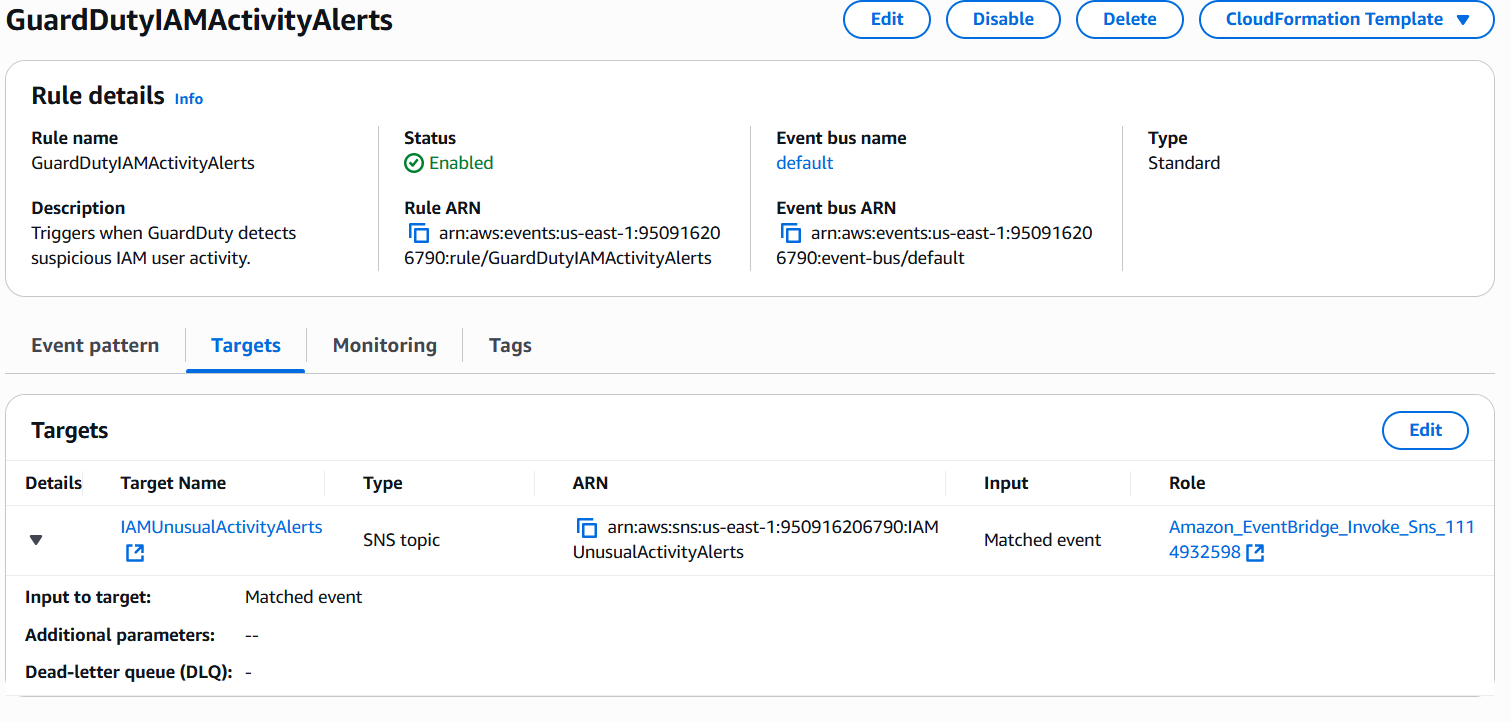
}

1. **Target**: **SNS Topic**, 🡪IAMUnusualActivityAlerts topic.

---------------------------------------------------------------

* This rule listens for security threats detected by Amazon GuardDuty,
* When such an event occurs, this rule Triggers an Amazon SNS Topic (named IAMUnusualActivityAlerts), which can notify staffs email.

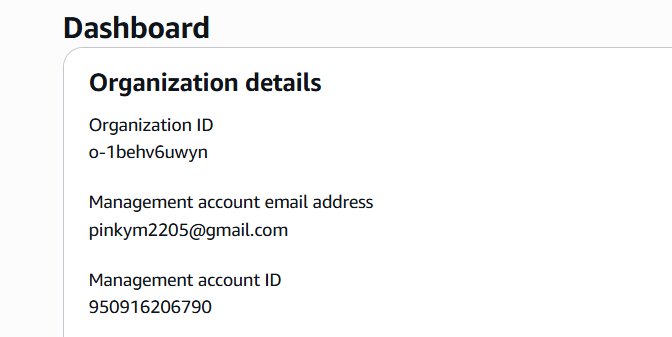


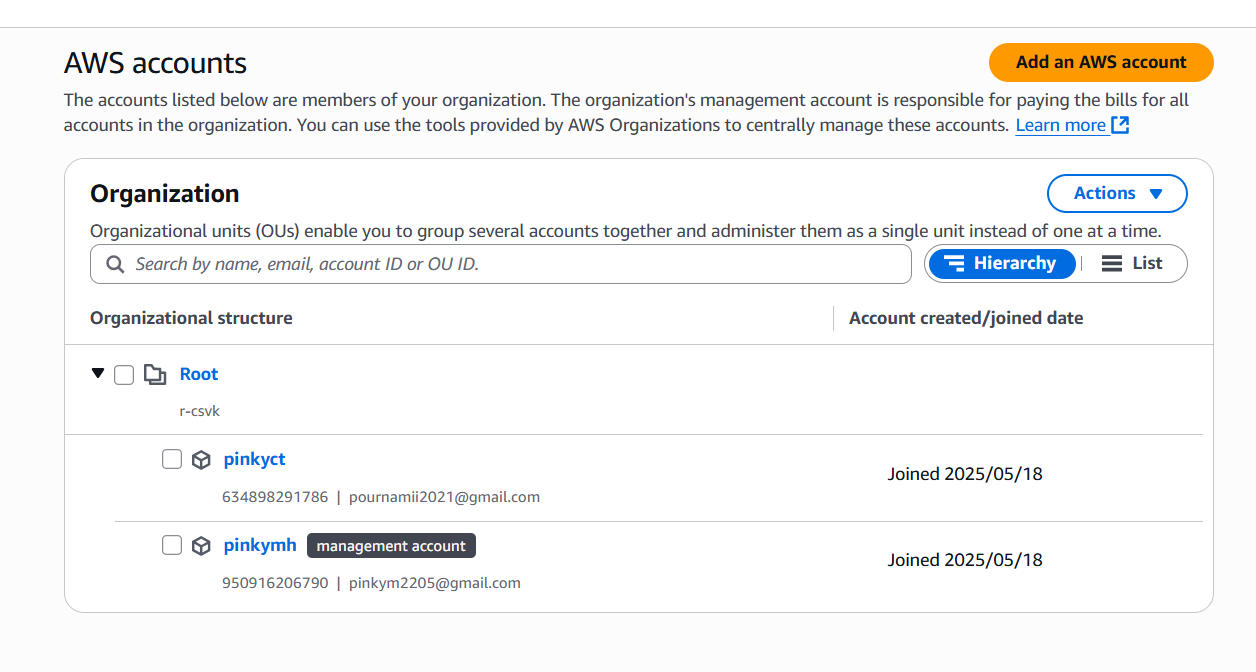


**The company needs to manage its multiple AWS accounts to capture consolidated billing to help the finance team; store all billing reports in Account-B's S3 bucket. Along with this Account-A's EC2 instances need permissions to access Account-B's S3 bucket to develop the final report.**

**Consolidated billing is automatically enabled in AWS Organizations.**

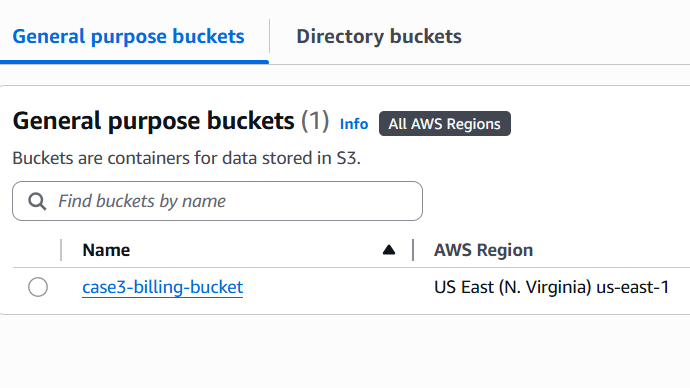
* **Once Account-A and Account-B are added, their charges will roll up to the management account.**
* **We can now generate a single invoice and detailed cost reports across all linked accounts.**

****

****

**Created an S3 Bucket**

**The Cost and Usage Report (CUR) will be stored in this bucket.**



**Configure the Bucket Policy in Account-B**

**Allow the Management Account to write CUR reports to this S3 bucket.**

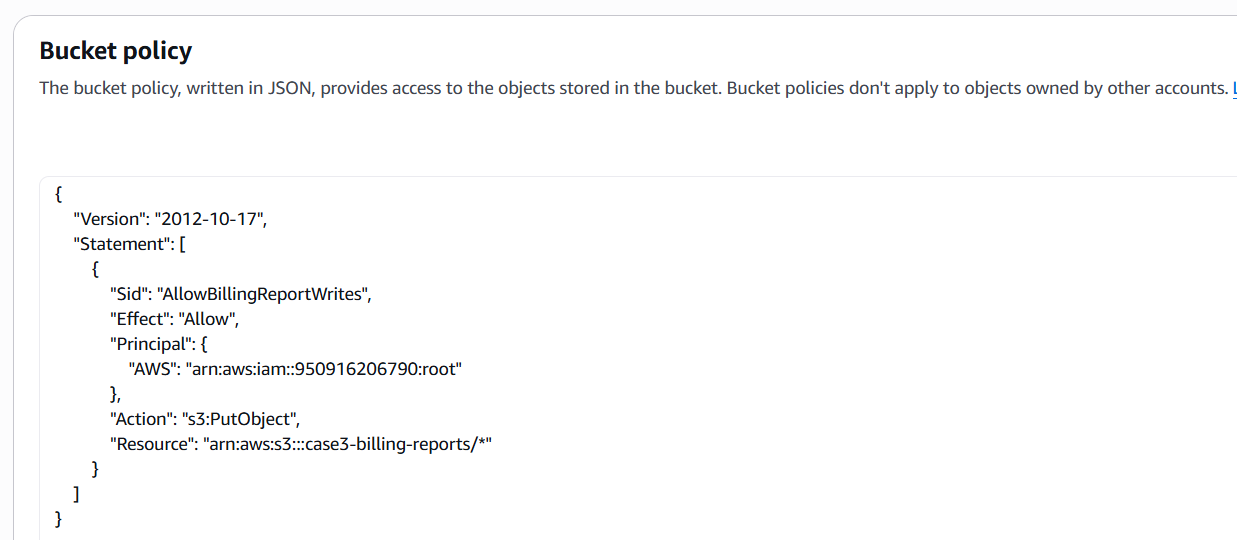
**Now we configure billing reports to go to Account-B’s S3 bucket.**

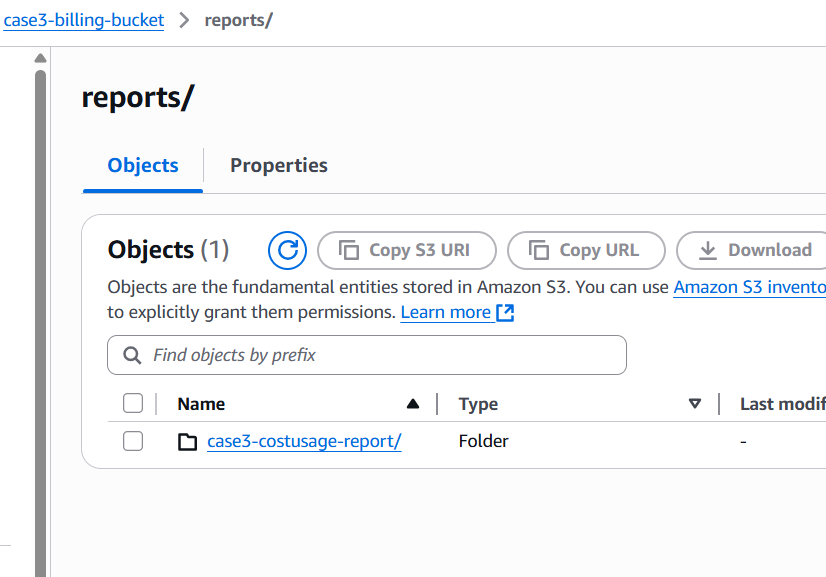
1. **Billing → Cost & Usage (left panel: bills🡪scroll down🡪under legacy pages🡪 cost and usage reportsReports**

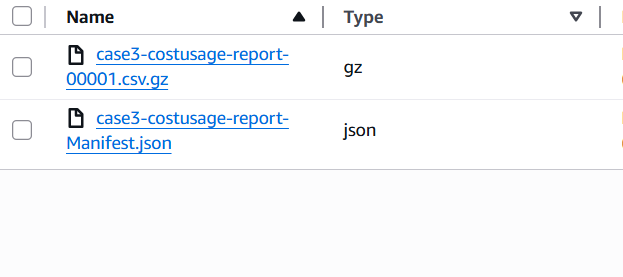
**Created report**

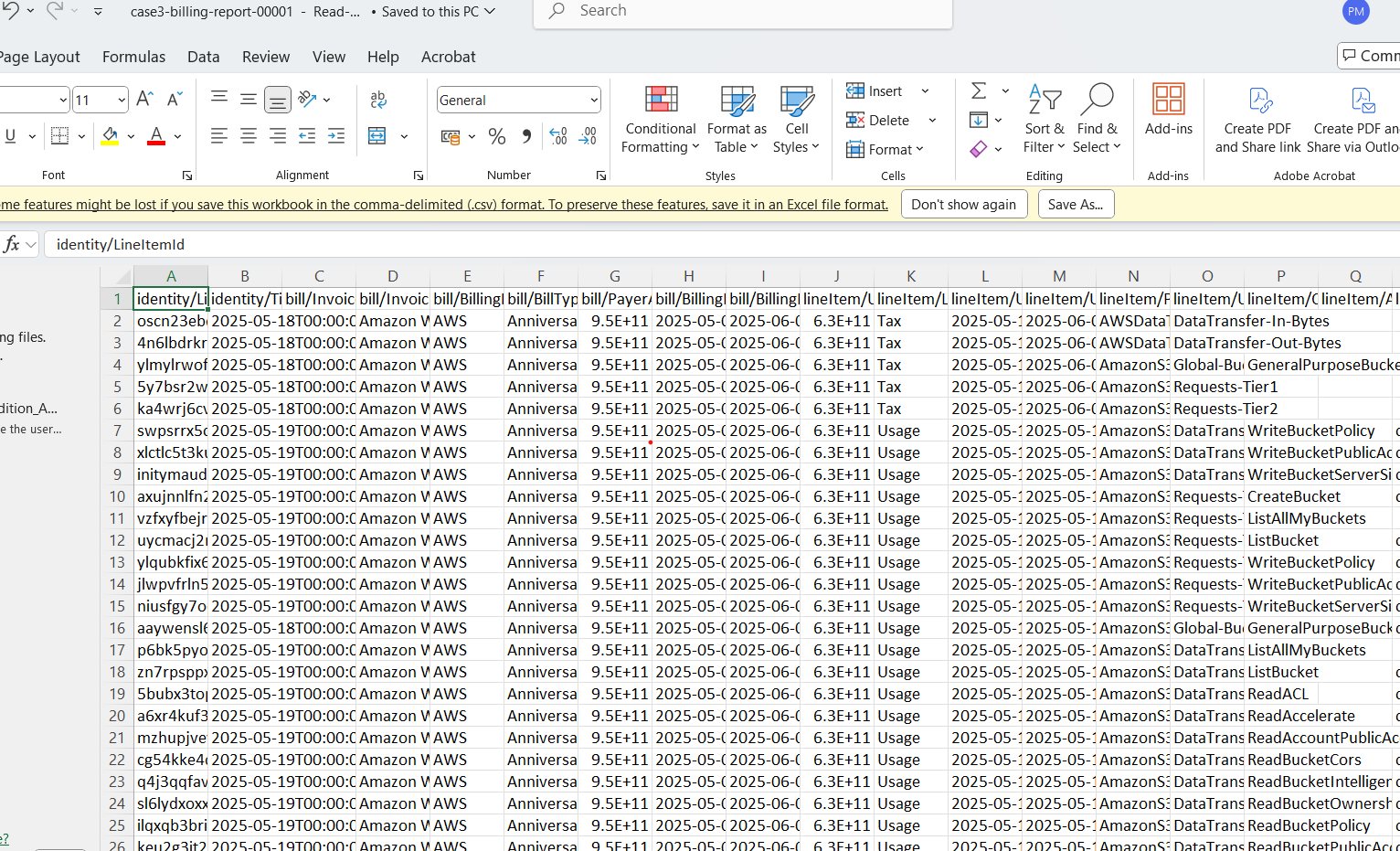
**Configure S3 bucket**

**After 24–48 hours, we can start seeing .csv.gz report files in s3 bucket.**

****

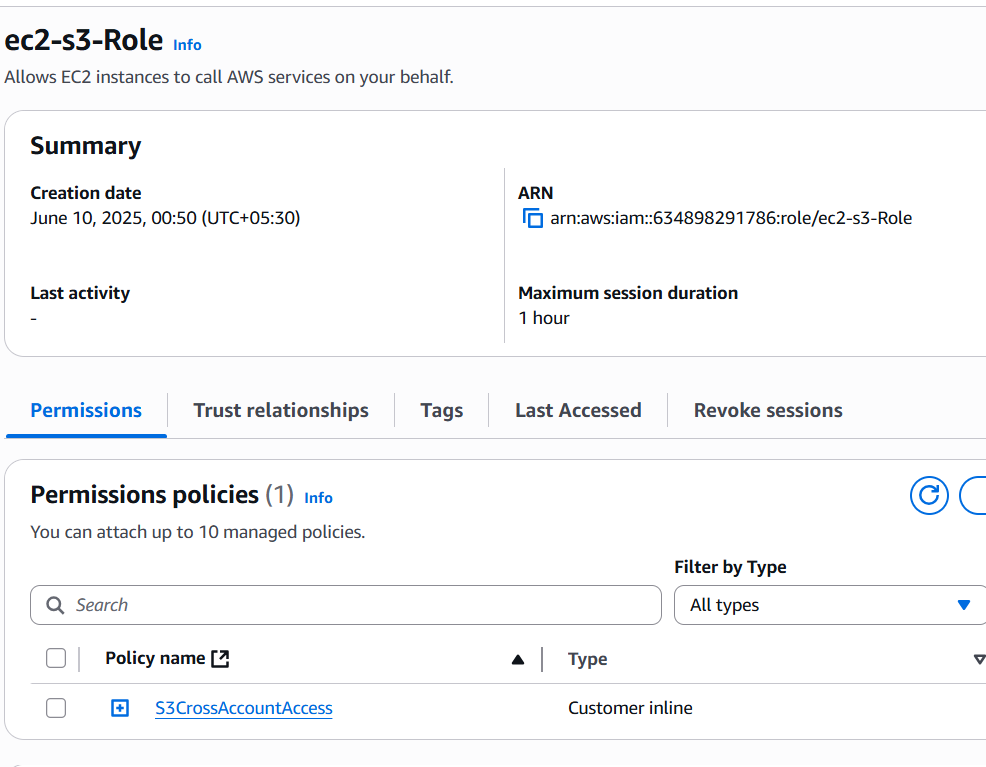


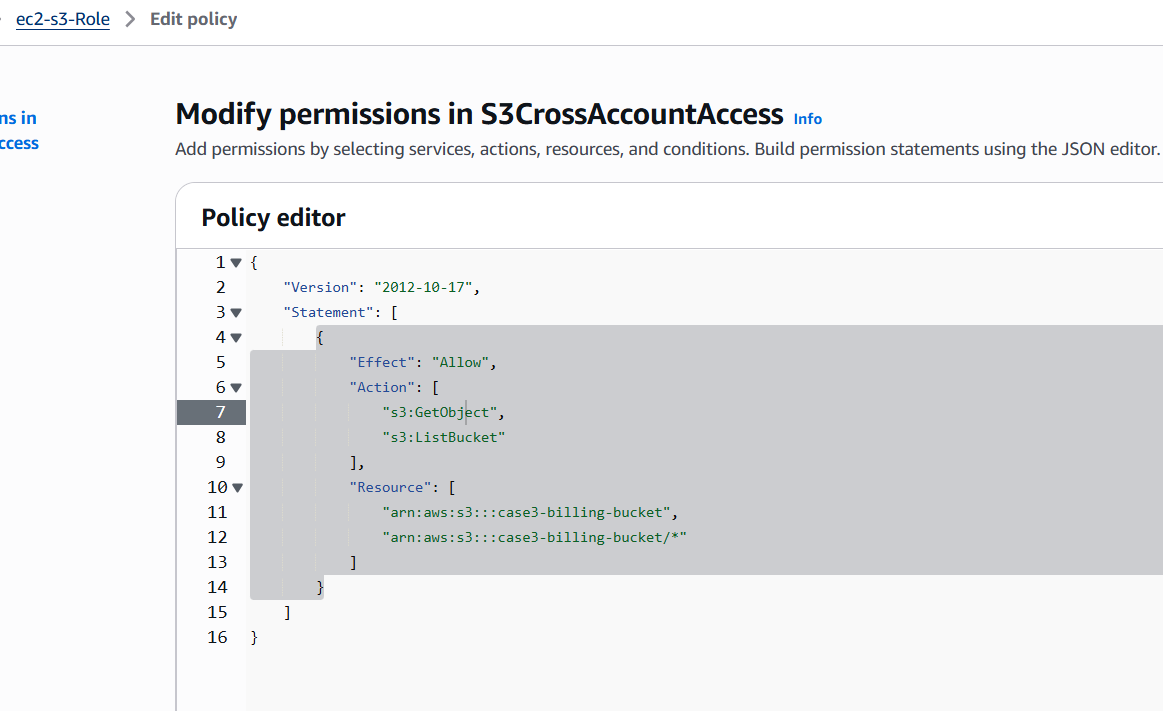




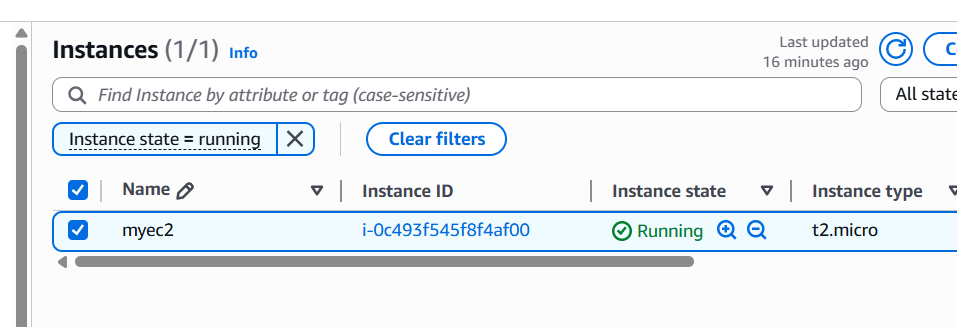
Next Allow **EC2 instance in Account-A (634898291786)** to access the S3 bucket named case3-billing-bucket in **Account-B (950916206790)**.

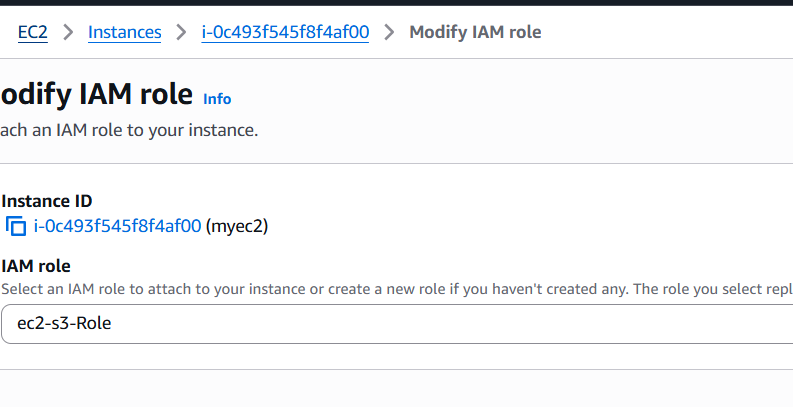
First ,I created role and inline policy attached to the role in the account where ec2 instances is residing.

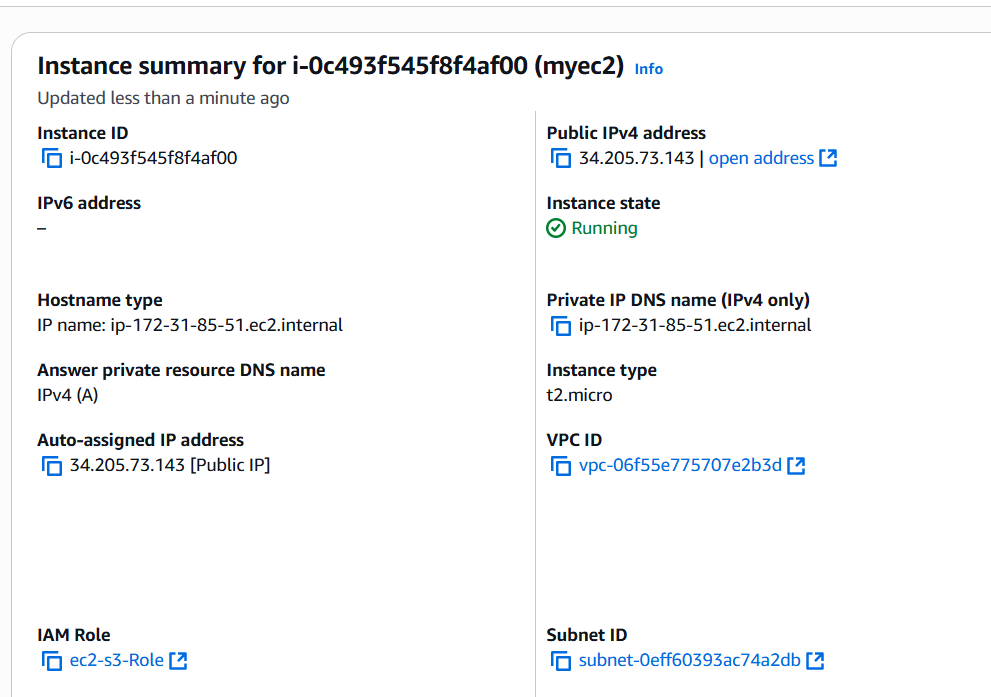




Created Ec2 instance and attached the role to the Ec2 instance.



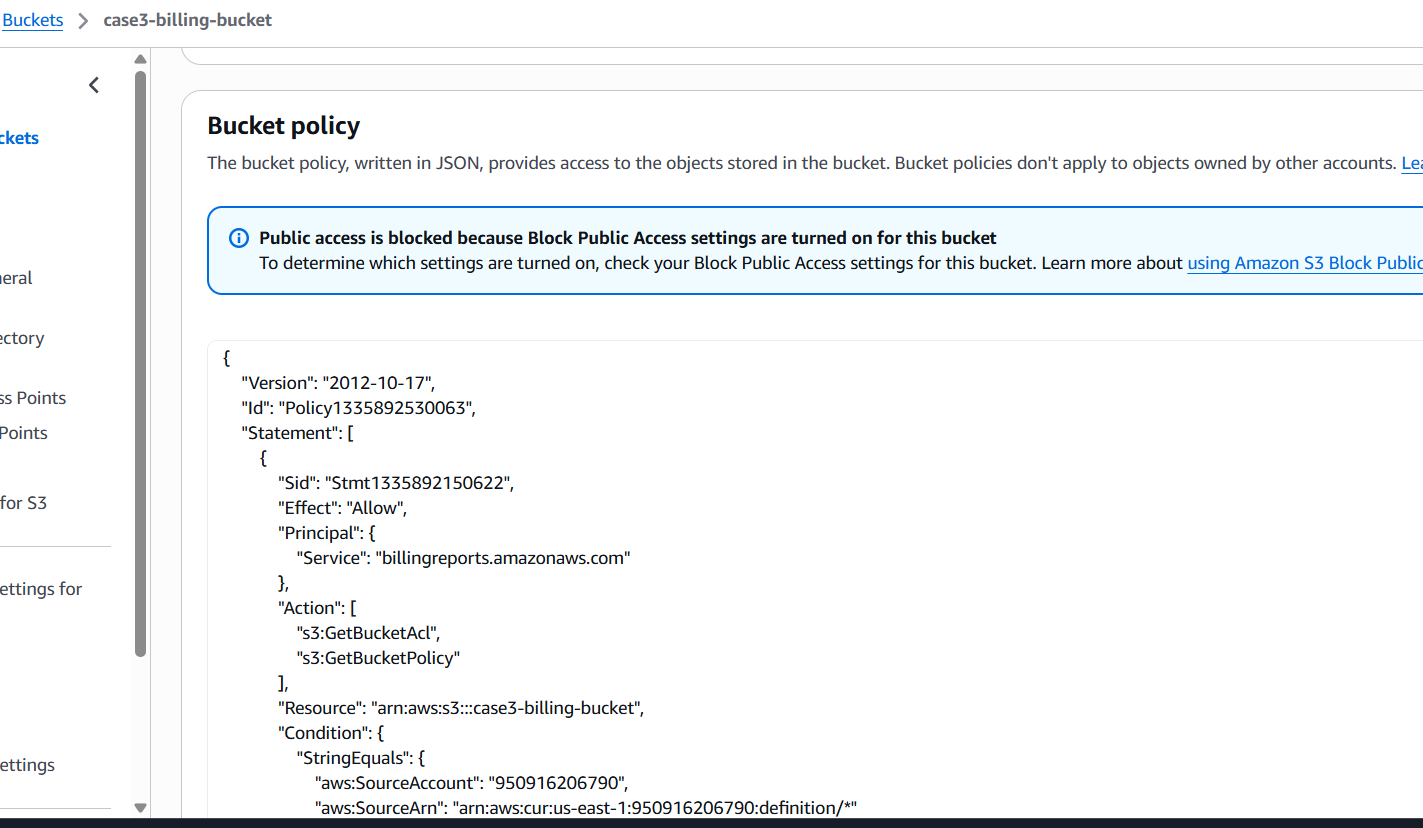


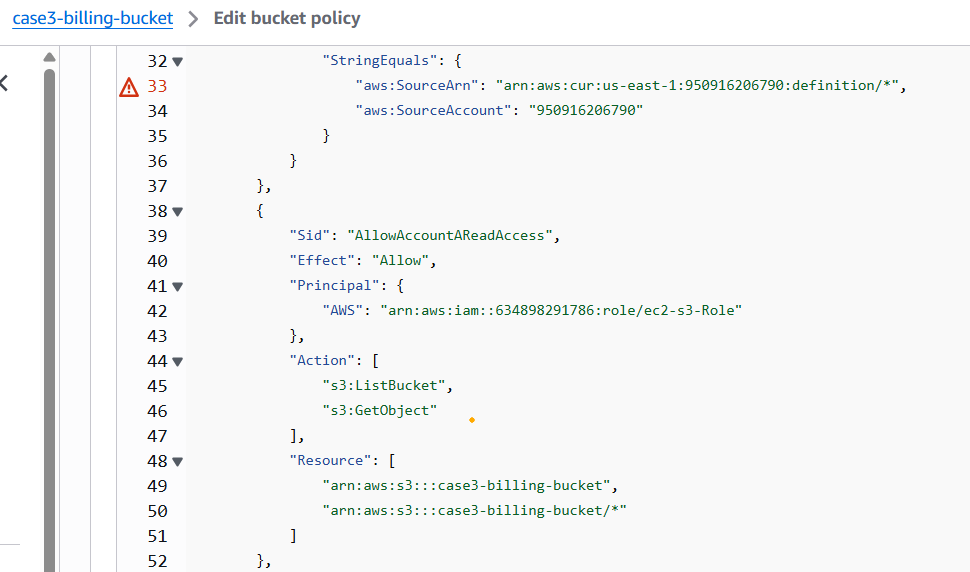


Next in the account where s3 bucket resides.

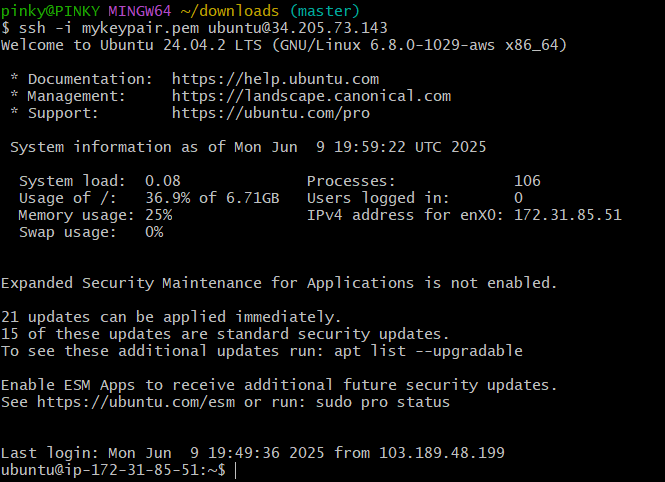
Grant Account-A (634898291786) permission to access the S3 bucket case3-billing-bucket.

**Bucket Policy** needs to updated to allow that role to read s3 bucket .





ssh -i mykeypair.pem ubuntu@ 34.205.73.143



aws s3 ls s3://case3-billing-bucket --region us-east-1

