Assignment: IAM Role Access Control

Name: *Vikram*

Assignment Number: *IAM Role Access Control – VPC and DynamoDB*

🧩 Problem Statement

You work for **XYZ Corporation**. To maintain the security of the AWS account and its resources, you have been asked to implement a solution that helps easily recognize and monitor different users while maintaining strict access control.

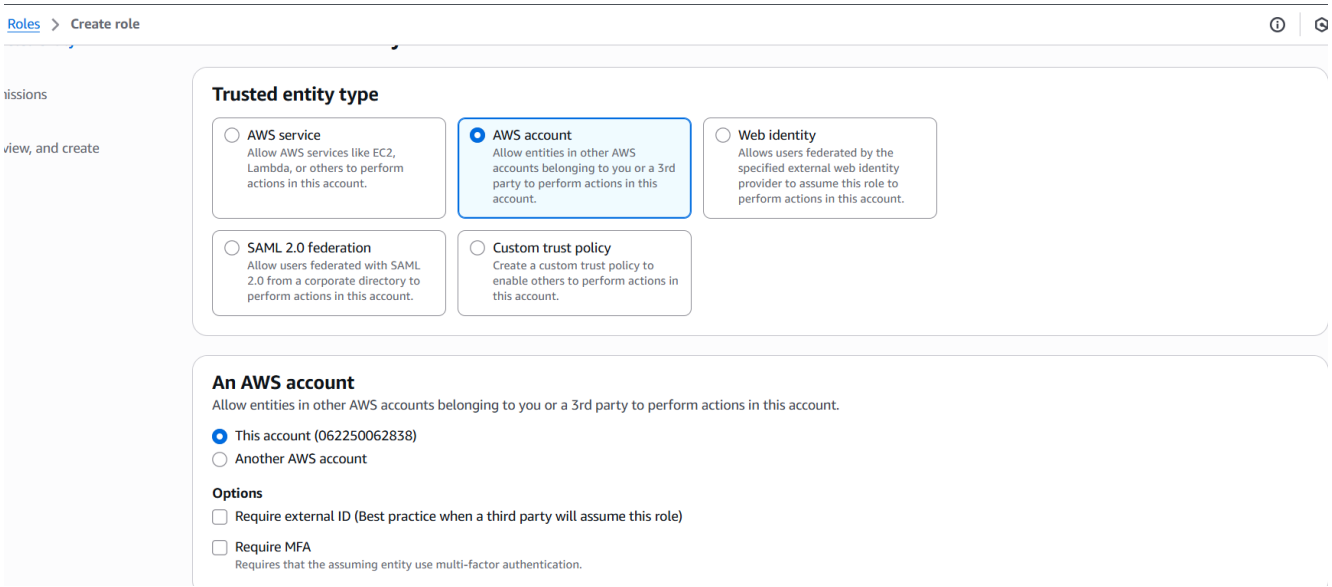
🎯 Objective

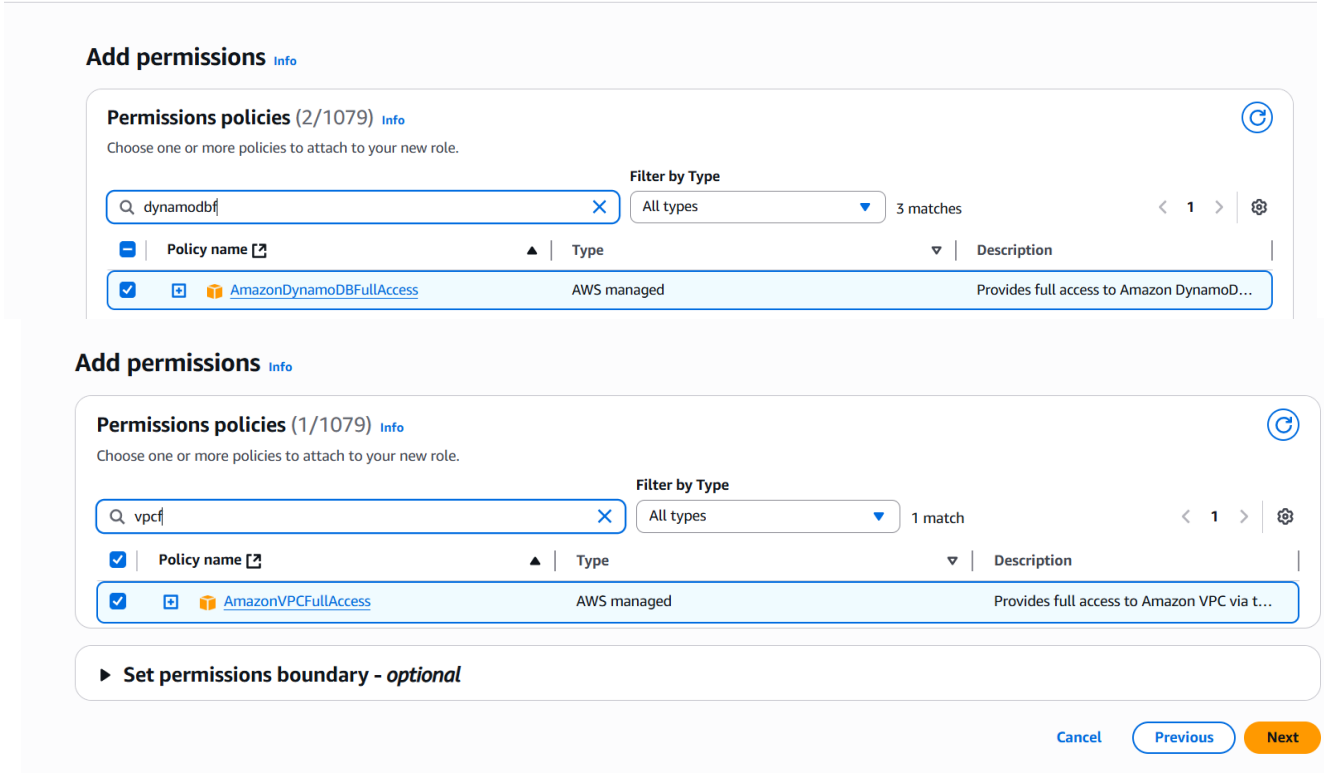
Create a secure IAM Role that grants full access to **VPC** and **DynamoDB** services, but can only be assumed by specific users — **user1** and **user2**.

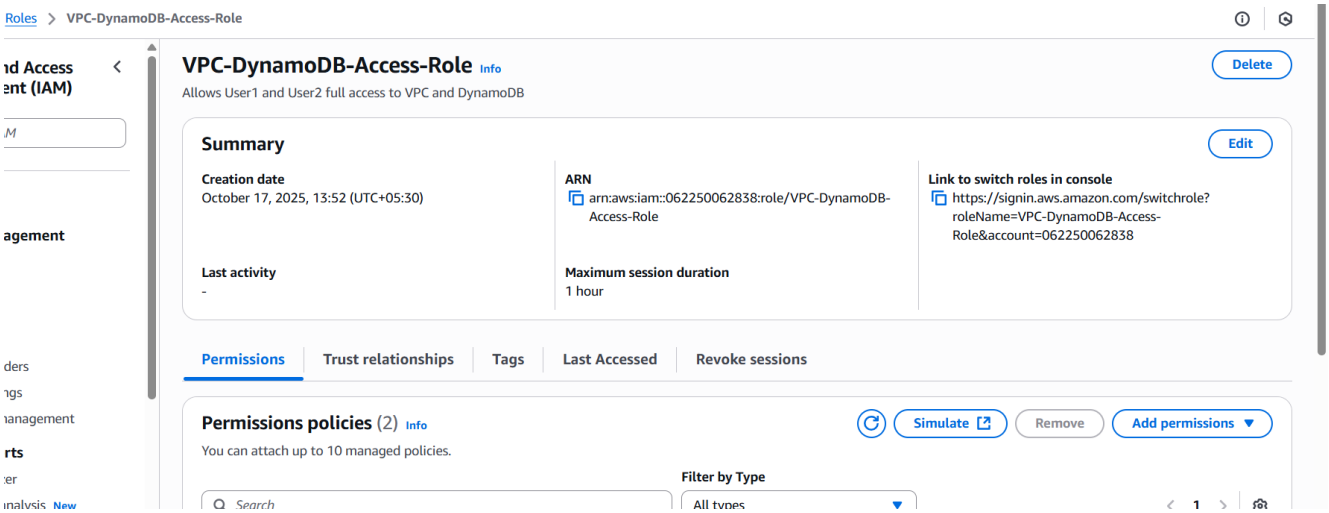
🧠 Tasks to be Performed

Step 1 — Create IAM Role

- Go to **IAM → Roles → Create Role**
- Select **Trusted entity type: AWS Account → This account**
- Attach the following managed policies:
    - AmazonVPCFullAccess
    - AmazonDynamoDBFullAccess
- Name the role: **VPC-DynamoDB-Access-Role**



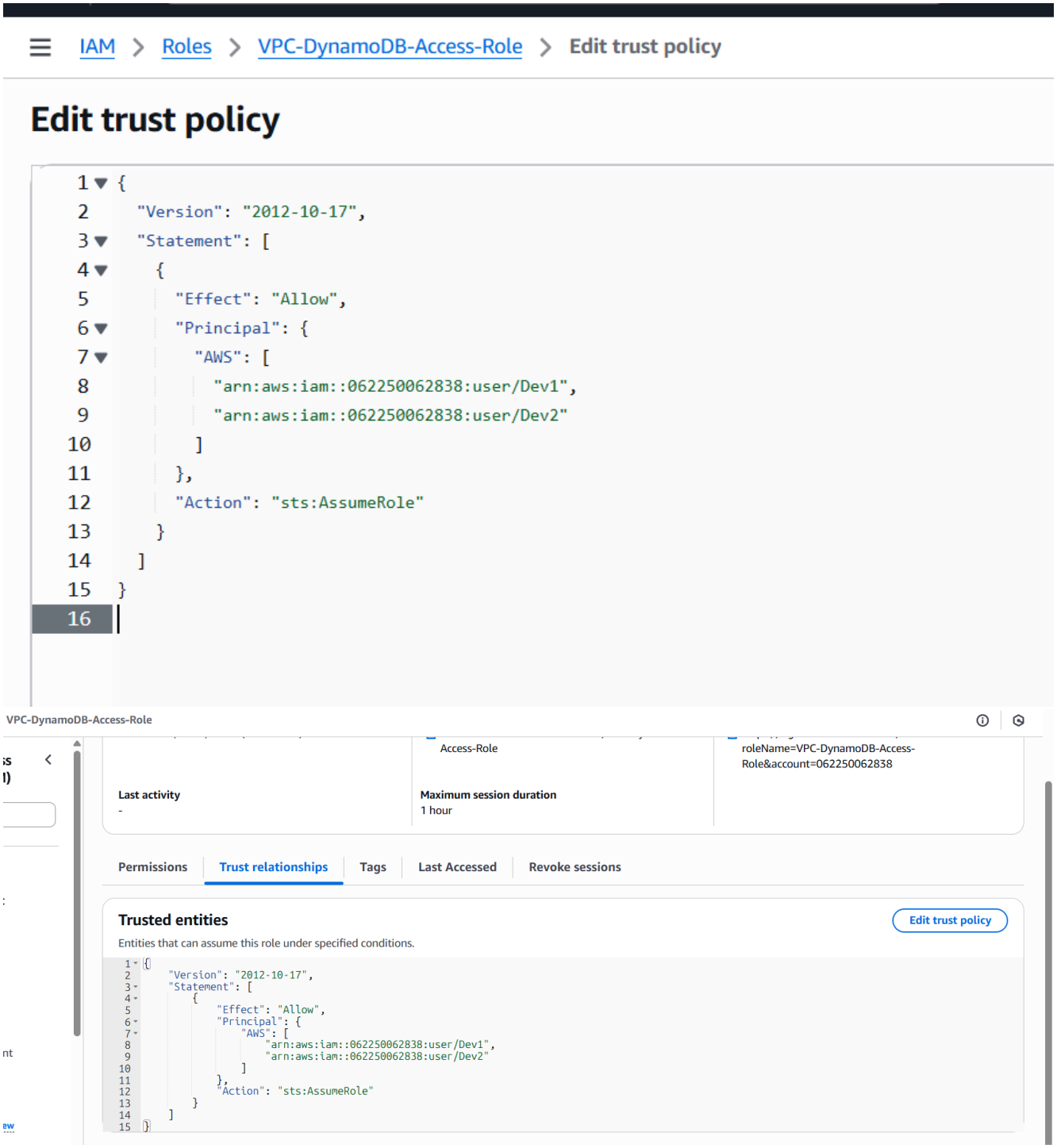

Add permissions Info
Permissions policies (2/1079) Info
Choose one or more policies to attach to your new role.
Filter by Type
dynamodbf
All types
3 matches
1
Policy name
Type
Description
AmazonDynamoDBFullAccess
AWS managed
Provides full access to Amazon DynamoD...
Add permissions Info
Permissions policies (1/1079) Info
Choose one or more policies to attach to your new role.
Filter by Type
vpcf
All types
1 match
1
Policy name
Type
Description
AmazonVPCFullAccess
AWS managed
Provides full access to Amazon VPC via t...
Set permissions boundary - optional
Cancel
Previous
Next


Roles > VPC-DynamoDB-Access-Role
VPC-DynamoDB-Access-Role Info
Allows User1 and User2 full access to VPC and DynamoDB
Delete
Summary
Edit
Creation date
October 17, 2025, 13:52 (UTC+05:30)
ARN
arn:aws:iam::062250062838:role/VPC-DynamoDB-Access-Role
Link to switch roles in console
https://signin.aws.amazon.com/switchrole?roleName=VPC-DynamoDB-Access-Role&account=062250062838
Last activity
-
Maximum session duration
1 hour
Permissions
Trust relationships
Tags
Last Accessed
Revoke sessions
Permissions policies (2) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
Search
All types

Step 2 — Edit Trust Relationship

- Navigate to the created role → **Trust relationships → Edit trust policy**
- Update the JSON to allow only user1 and user2:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": [
     "arn:aws:iam::<your-account-id>:user/user1",
     "arn:aws:iam::<your-account-id>:user/user2"
    ]
   },
   "Action": "sts:AssumeRole"
  }
 ]
}
```



Step 3 — Allow user1 and user2 to Assume the Role

For both users:

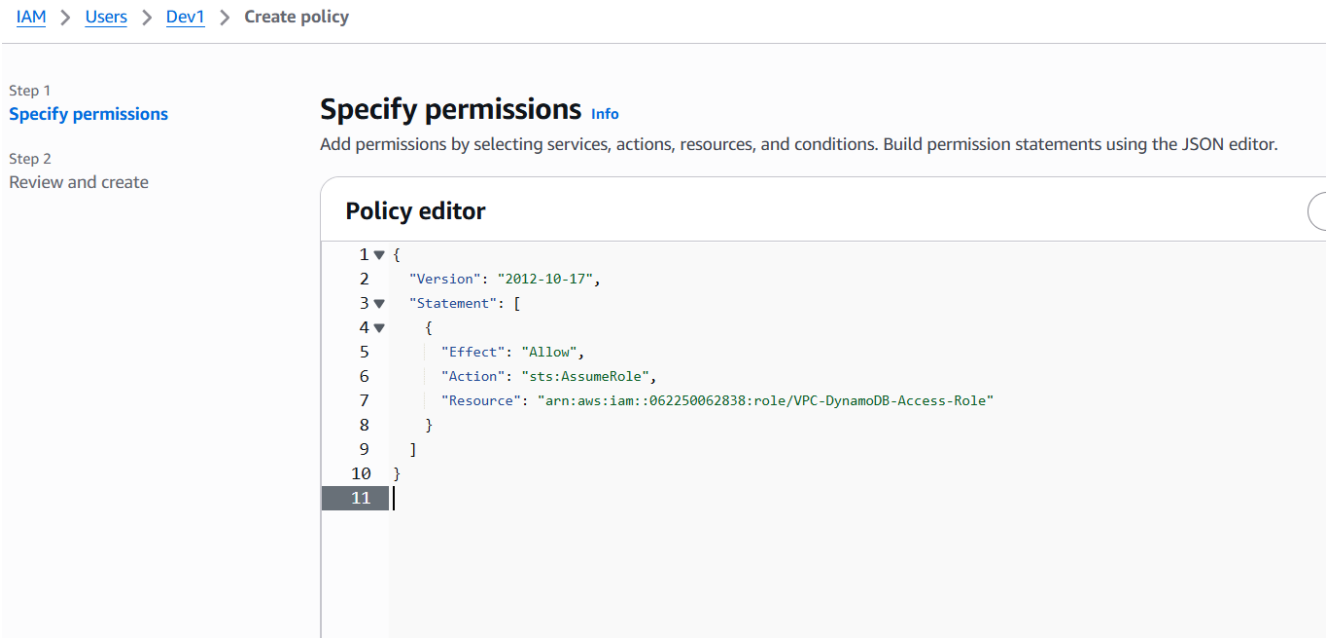
- Go to **IAM → Users → user1 → Add inline policy**
- Choose **JSON** and add the following:

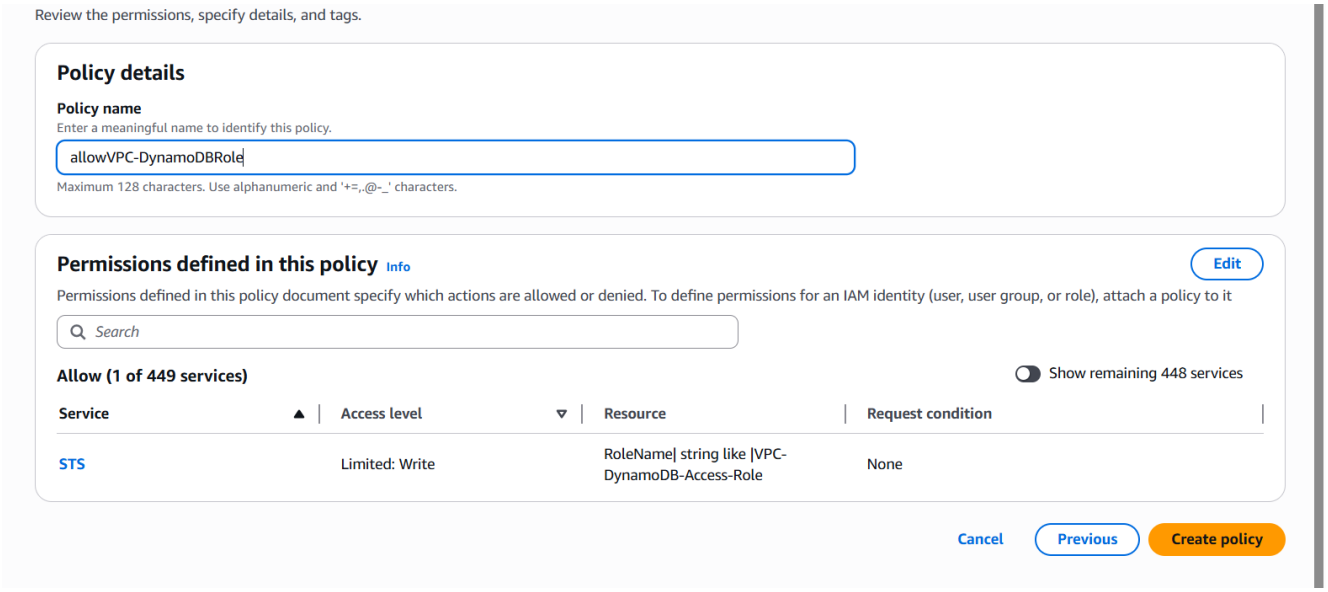
```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
```

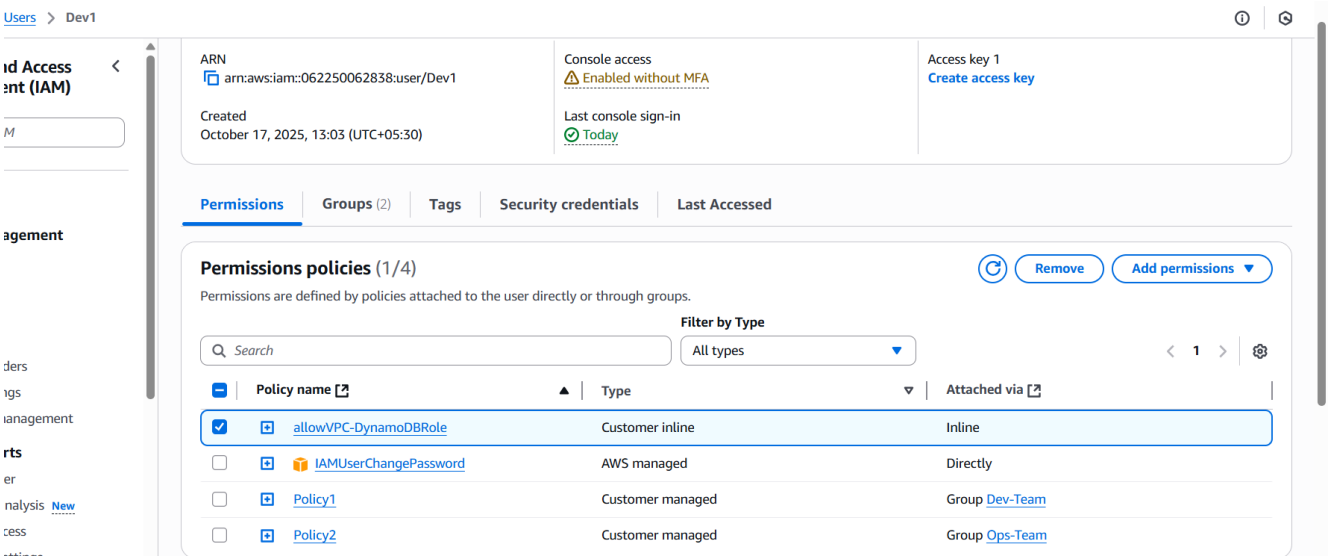
```
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::<your-account-id>:role/VPC-DynamoDB-Access-Role"
  }
 ]
}
```

- Name the policy: **AllowAssumeVPC-DynamoDBAccessRole**

Repeat the same for **user2**.

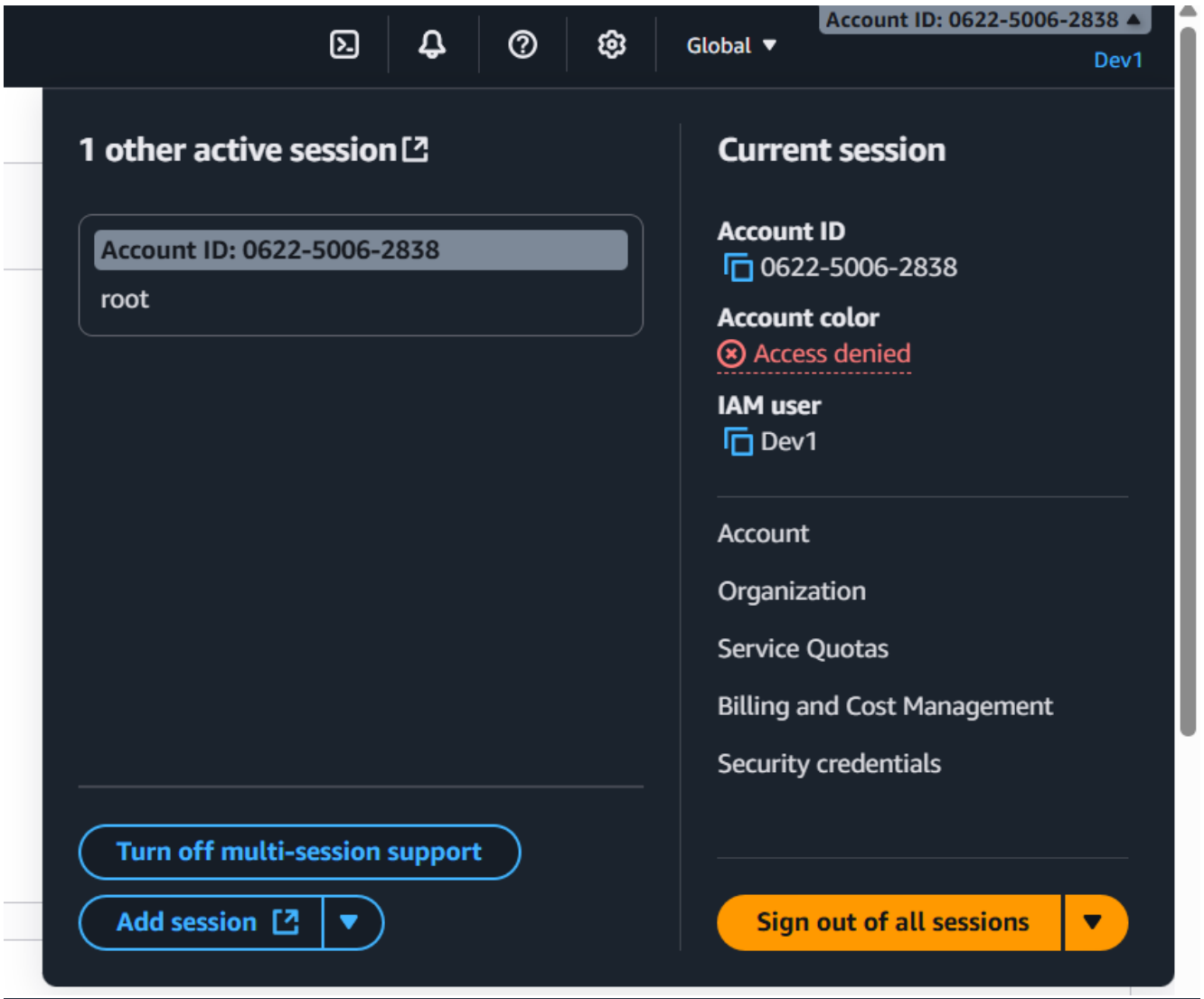


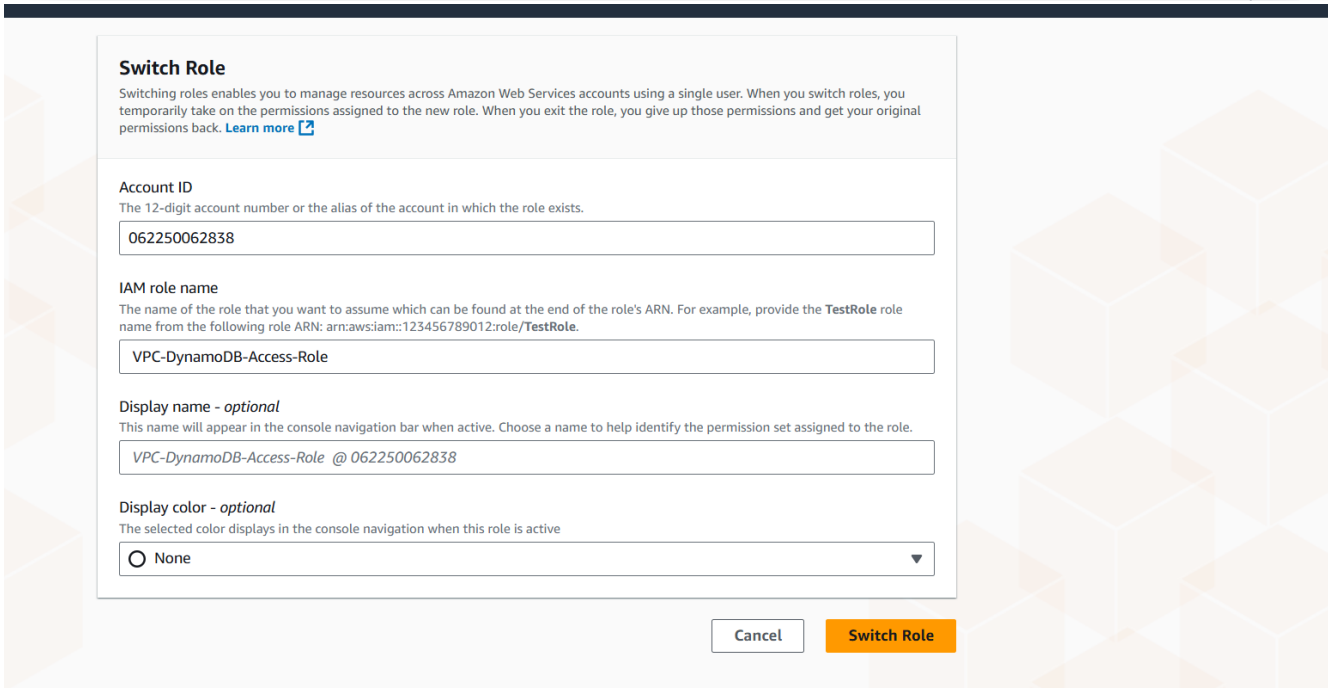


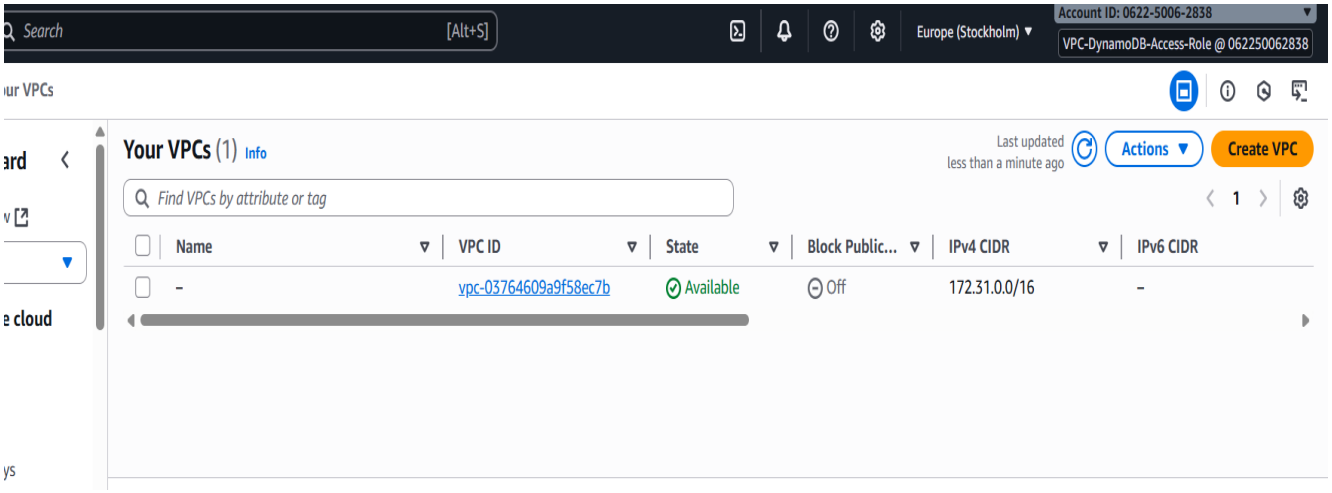


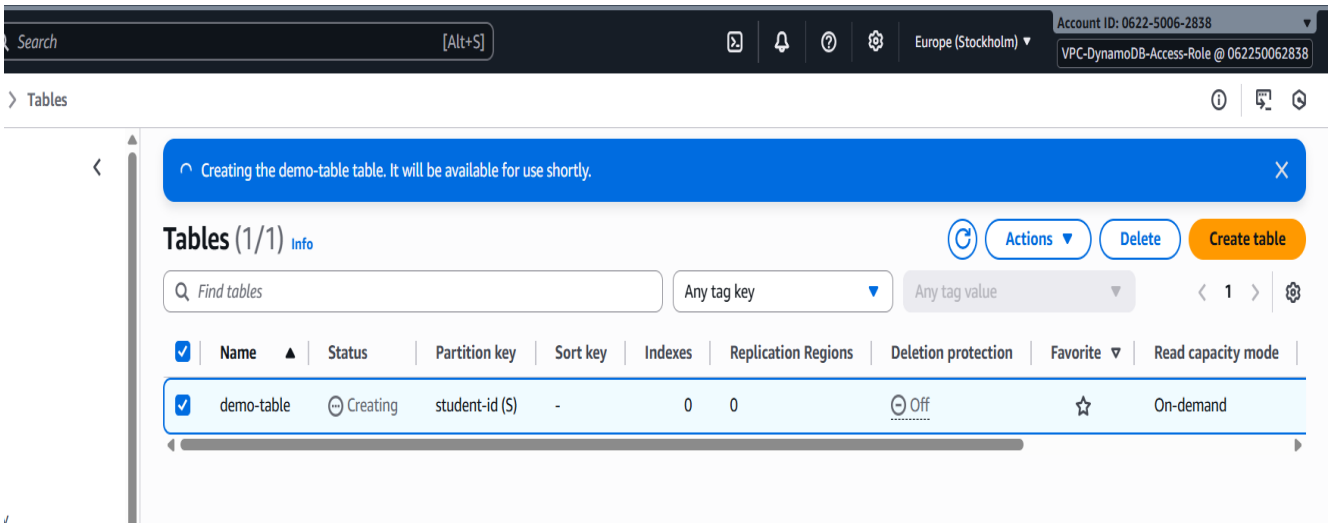
Step 4 — Test the Configuration

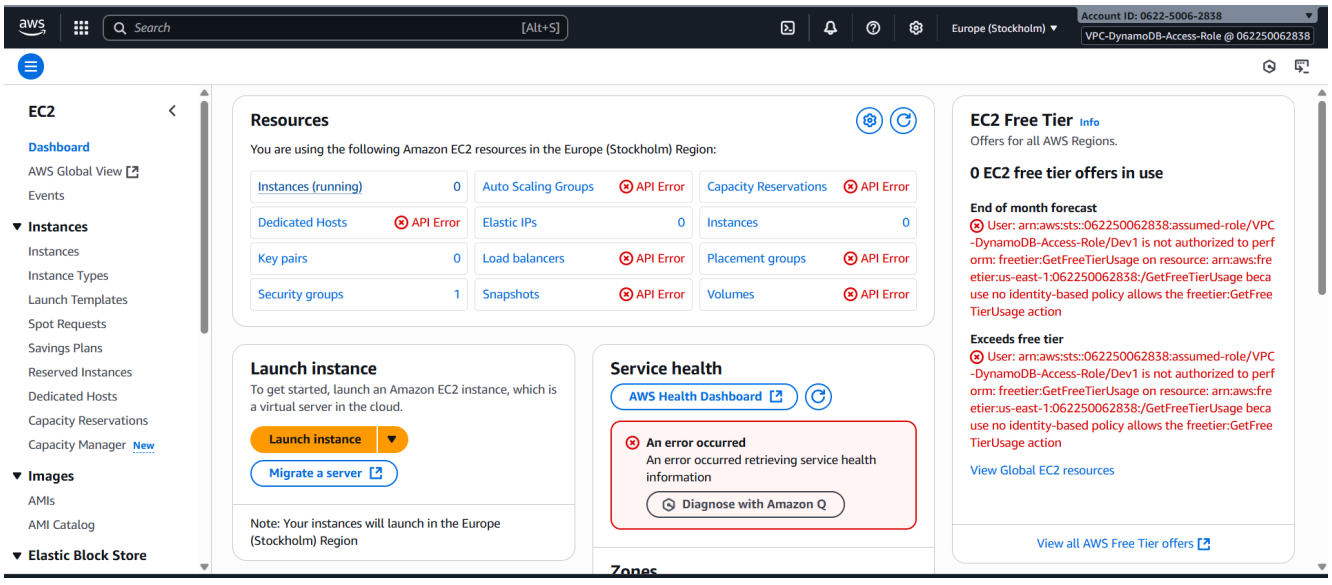
1. Login as **user1** (using IAM user login URL).
2. Click on the **profile name → Switch Role**.
3. Enter:
    - Account ID: <your-account-id>
    - Role name: VPC-DynamoDB-Access-Role
4. Confirm successful switch (you'll see a red banner on top).
5. Verify:
    - ☑ Able to access VPC and DynamoDB services.
    - ⃠ No access to other services like EC2 or S3.


Account ID: 0622-5006-2838
Global
Dev1
1 other active session
Account ID: 0622-5006-2838
root
Current session
Account ID
0622-5006-2838
Account color
Access denied
IAM user
Dev1
Account
Organization
Service Quotas
Billing and Cost Management
Security credentials
Turn off multi-session support
Add session
Sign out of all sessions


Switch Role
Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. Learn more
Account ID
The 12-digit account number or the alias of the account in which the role exists.
062250062838
IAM role name
The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the TestRole role name from the following role ARN: arn:aws:iam::123456789012:role/TestRole.
VPC-DynamoDB-Access-Role
Display name - optional
This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.
VPC-DynamoDB-Access-Role @ 062250062838
Display color - optional
The selected color displays in the console navigation when this role is active
None
Cancel
Switch Role


Search
[Alt+S]
Europe (Stockholm)
Account ID: 0622-5006-2838
VPC-DynamoDB-Access-Role @ 062250062838
Your VPCs (1) Info
Last updated less than a minute ago
Actions
Create VPC
Find VPCs by attribute or tag
Name
VPC ID
State
Block Public...
IPv4 CIDR
IPv6 CIDR
vpc-03764609a9f58ec7b
Available
Off
172.31.0.0/16


Search
[Alt+S]
Europe (Stockholm)
Account ID: 0622-5006-2838
VPC-DynamoDB-Access-Role @ 062250062838
Tables
Creating the demo-table table. It will be available for use shortly.
Tables (1/1) Info
Actions
Delete
Create table
Find tables
Any tag key
Any tag value
Name
Status
Partition key
Sort key
Indexes
Replication Regions
Deletion protection
Favorite
Read capacity mode
demo-table
Creating
student-id (S)
Off
On-demand


Search
[Alt+S]
Europe (Stockholm)
Account ID: 0622-5006-2838
VPC-DynamoDB-Access-Role @ 062250062838
EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Resources
You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:
Instances (running) 0
Auto Scaling Groups API Error
Capacity Reservations API Error
Dedicated Hosts API Error
Elastic IPs 0
Instances 0
Key pairs 0
Load balancers API Error
Placement groups API Error
Security groups 1
Snapshots API Error
Volumes API Error
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Migrate a server
Note: Your instances will launch in the Europe (Stockholm) Region
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Diagnose with Amazon Q
Zones
EC2 Free Tier Info
Offers for all AWS Regions.
0 EC2 free tier offers in use
End of month forecast
User: arn:aws:sts::062250062838:assumed-role/VPC-DynamoDB-Access-Role/Dev1 is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:062250062838:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
Exceeds free tier
User: arn:aws:sts::062250062838:assumed-role/VPC-DynamoDB-Access-Role/Dev1 is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:062250062838:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
View Global EC2 resources
View all AWS Free Tier offers

☑ Result

- Successfully created a secure IAM role (**VPC-DynamoDB-Access-Role**) with access only to **VPC** and **DynamoDB**.
- Verified that only **user1** and **user2** can assume the role and perform actions in these services.
- Confirmed that other AWS services remain restricted, ensuring proper security and role-based access control.