

IAM-Roles-Assignment—3

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

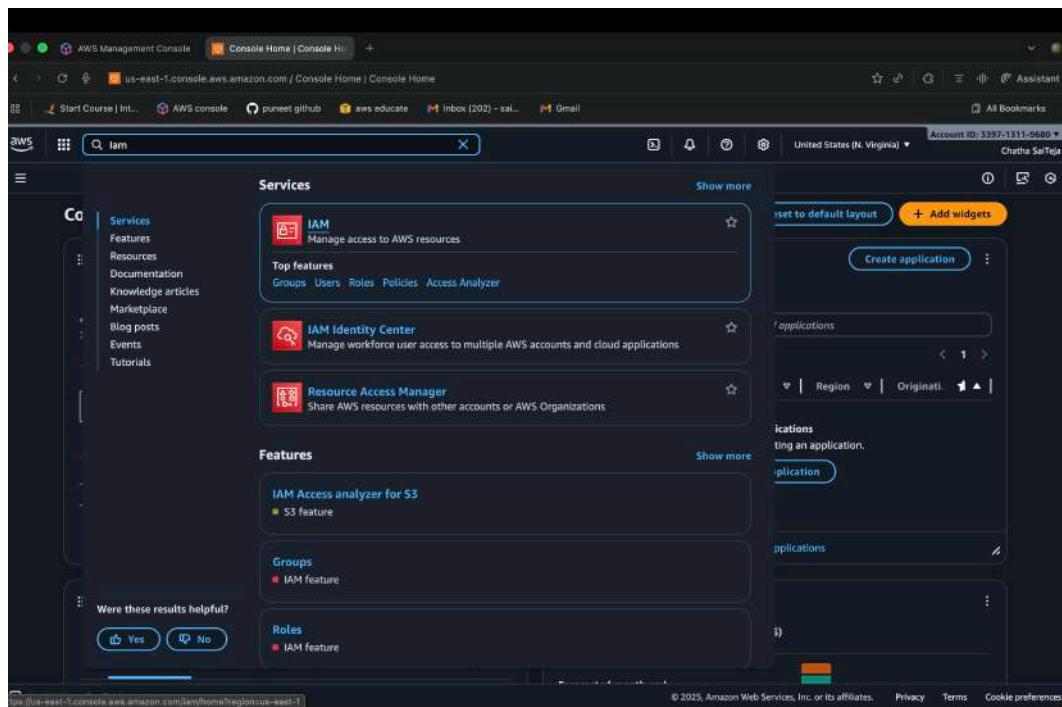
Tasks To Be Performed:

1. Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.
2. Login into user1 and shift to the role to test out the feature

Step-By-Step Procedure:-

Step 1:- Create an IAM role for user1 and user2, where user1 refers to Dev1 and user2 refers to Dev2 as specified in Task 1.

Step 2:- To create an IAM role search IAM in search bar and open the service and go to role in the dashboard.



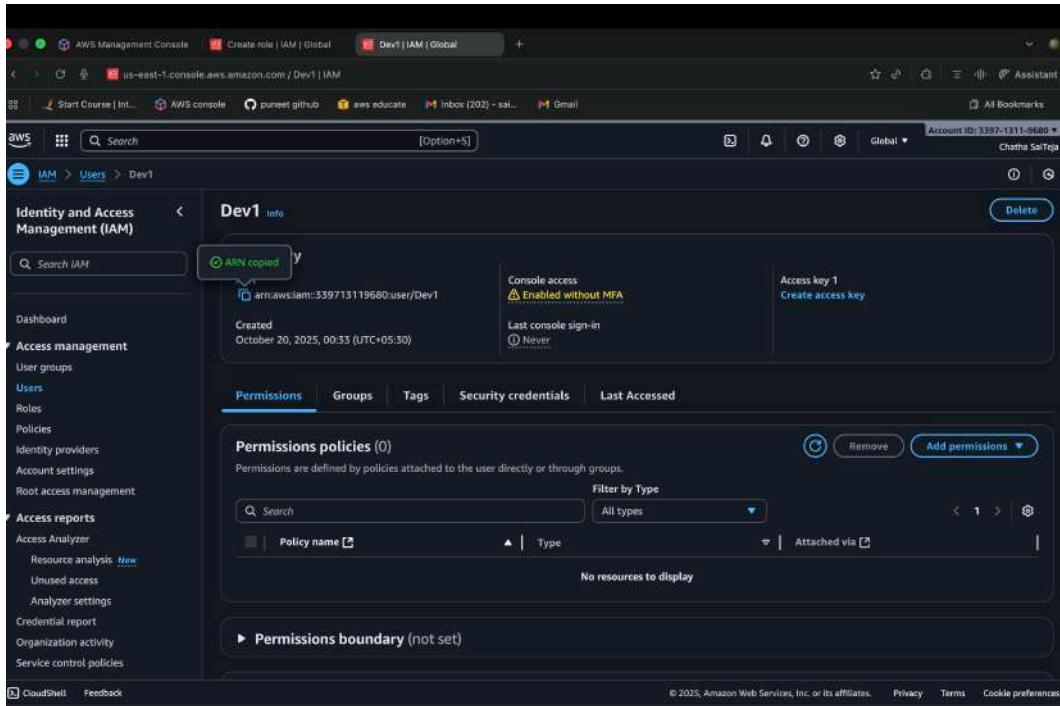
Search for IAM

Click roles In dashboard

Step3 :- Click on Create Role, then we have too select the trusted entity(it means for which we creating a role it can be AWS service, account or other resources) where we have “AWS service”, “AWS account”and “Custom Trust policy”, we select Custom Trust Policy because we are creating role especially for user1(Dev1) and user2(Dev2)

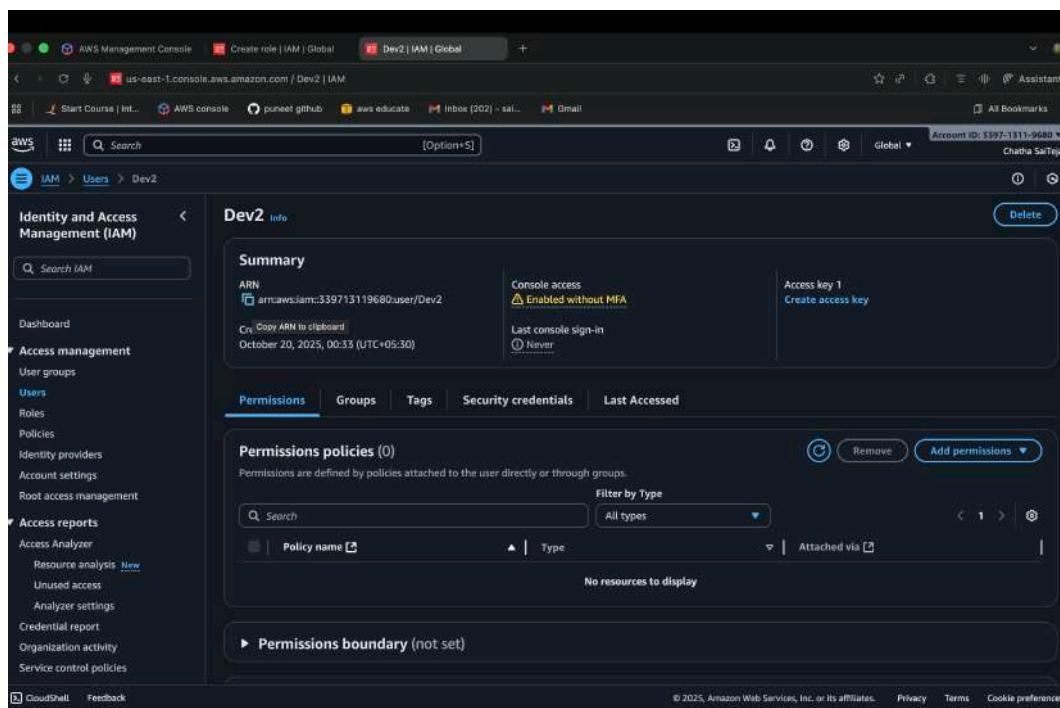
Select Custom Trust Policy

Step 4:- In trust policy we have to edit JSON where we have to copy the ARN's of user1(Dev1) and user2(Dev2) then we have to mention the ARN's Of users in principal of Custom Trust Policy and then allow all actions for "STS Assume Role"



The screenshot shows the AWS Management Console with the URL us-east-1.console.aws.amazon.com/iam/users/Dev1. The page displays the 'Dev1' user info. A green 'ARN copied' message is visible above the ARN field. The ARN is listed as `arn:aws:iam::339713119680:user/Dev1`. The 'Permissions' tab is selected, showing 'Permissions policies (0)' and a 'Permissions boundary (not set)' section. The sidebar on the left shows the IAM navigation menu.

Copy Dev1(user1) ARN



The screenshot shows the AWS Management Console with the URL us-east-1.console.aws.amazon.com/iam/users/Dev2. The page displays the 'Dev2' user info. A green 'Copy ARN to clipboard' message is visible above the ARN field. The ARN is listed as `arn:aws:iam::339713119680:user/Dev2`. The 'Permissions' tab is selected, showing 'Permissions policies (0)' and a 'Permissions boundary (not set)' section. The sidebar on the left shows the IAM navigation menu.

Copy Dev2 (user2) ARN

```

1: {
2:   "Version": "2012-10-17",
3:   "Statement": [
4:     {
5:       "Effect": "Allow",
6:       "Principal": [
7:         "AWS: [",
8:           "arn:aws:iam::339713119680:user/Dev1",
9:           "arn:aws:iam::339713119680:user/Dev2"
10:         ],
11:       ],
12:       "Action": "sts:AssumeRole"
13:     }
14:   ]
15: }
16

```

Edit statement **Remove**

Add actions for STS

Search actions

All actions (sts:*)

Access level - read

GetAccessKeyInfo Info

GetCallerIdentity Info

GetFederationToken Info

GetServiceBearerToken Info

GetSessionToken Info

Access level - read or write

AssumeRole Info

AssumeRoleWithSAML Info

Add a principal **Add**

Add a condition (optional) **Add**

[+ Add new statement](#)

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Add ARNs of user1&2 in principal of Custom Trust Policy

```

1: {
2:   "Version": "2012-10-17",
3:   "Statement": [
4:     {
5:       "Effect": "Allow",
6:       "Principal": [
7:         "arn:aws:iam::339713119680:user/Dev1",
8:         "arn:aws:iam::339713119680:user/Dev2"
9:       ],
10:       "Action": "sts:AssumeRole"
11:     }
12:   ]
13: }
14
15
16

```

All actions (sts:*)

Access level - read

GetAccessKeyInfo Info

GetCallerIdentity Info

GetFederationToken Info

GetServiceBearerToken Info

GetSessionToken Info

Access level - read or write

AssumeRole Info

AssumeRoleWithSAML Info

Add a principal **Add**

Add a condition (optional) **Add**

[+ Add new statement](#)

JSON Ln 9, Col 11

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Preview external access

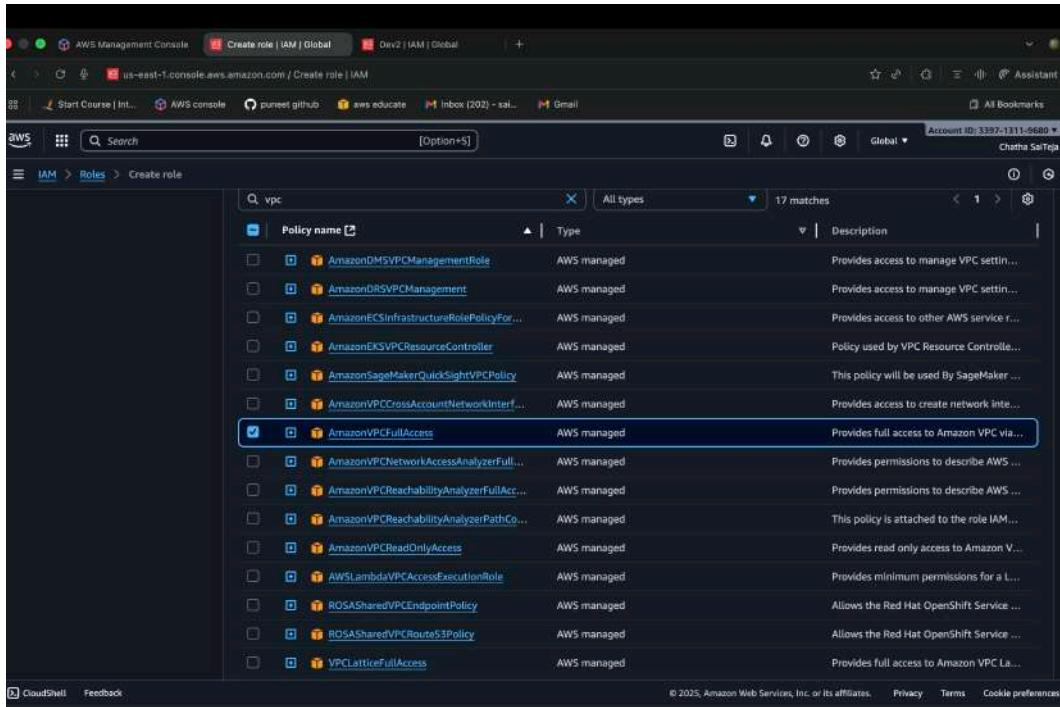
Cancel **Next**

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

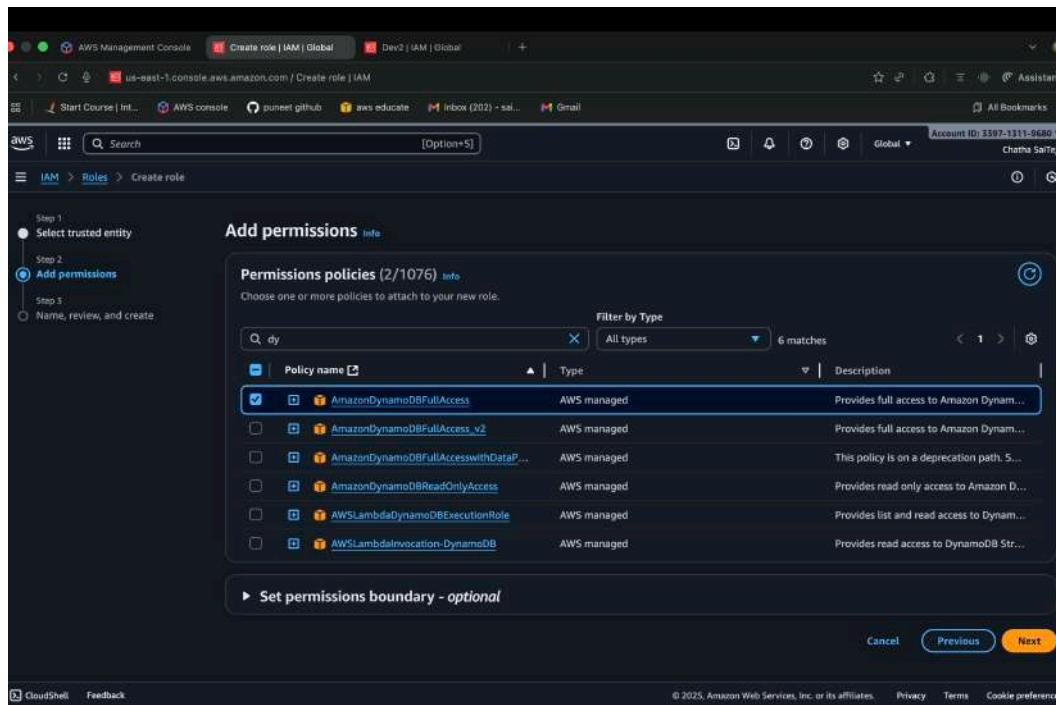
Click on next

Step 5:- After Clicking on next ,we have to specify the permission to the role ,here we have to give two permissions to the role that is full access to VPC & DynamoDb(as mentioned in the question).



The screenshot shows the AWS Management Console with the search bar set to 'vpc'. The results list contains 17 matches, with the 'AmazonVPCFullAccess' policy highlighted. This policy is described as providing full access to Amazon VPC via the AWS Management Console and AWS CLI.

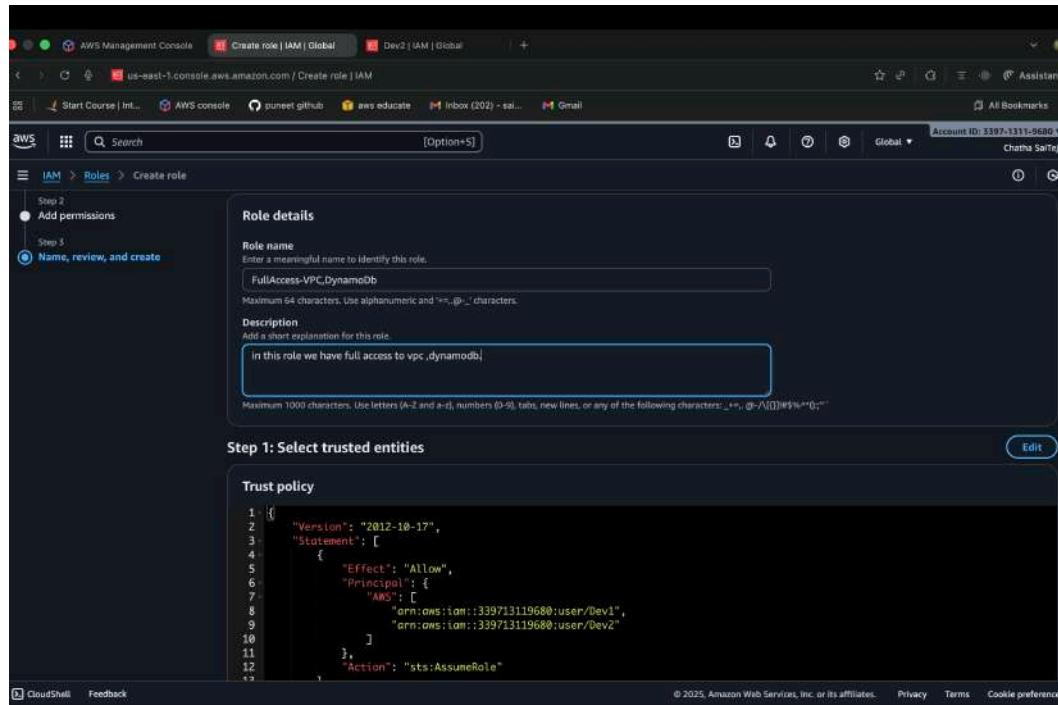
Giving full access to VPC



The screenshot shows the 'Add permissions' step of the 'Create role' wizard. The 'AmazonDynamoDBFullAccess' policy is selected and highlighted. This policy is described as providing full access to Amazon DynamoDB.

Giving Full Access to DynamoDB

Step 6:- In next step, we can review the total configurations of a role and we specify the name (FullAccess-VPC,DynamoDb) and description for a role then click on create role.



Role details

Role name: FullAccess-VPC,DynamoDb

Description: In this role we have full access to vpc ,dynamodb

Step 1: Select trusted entities

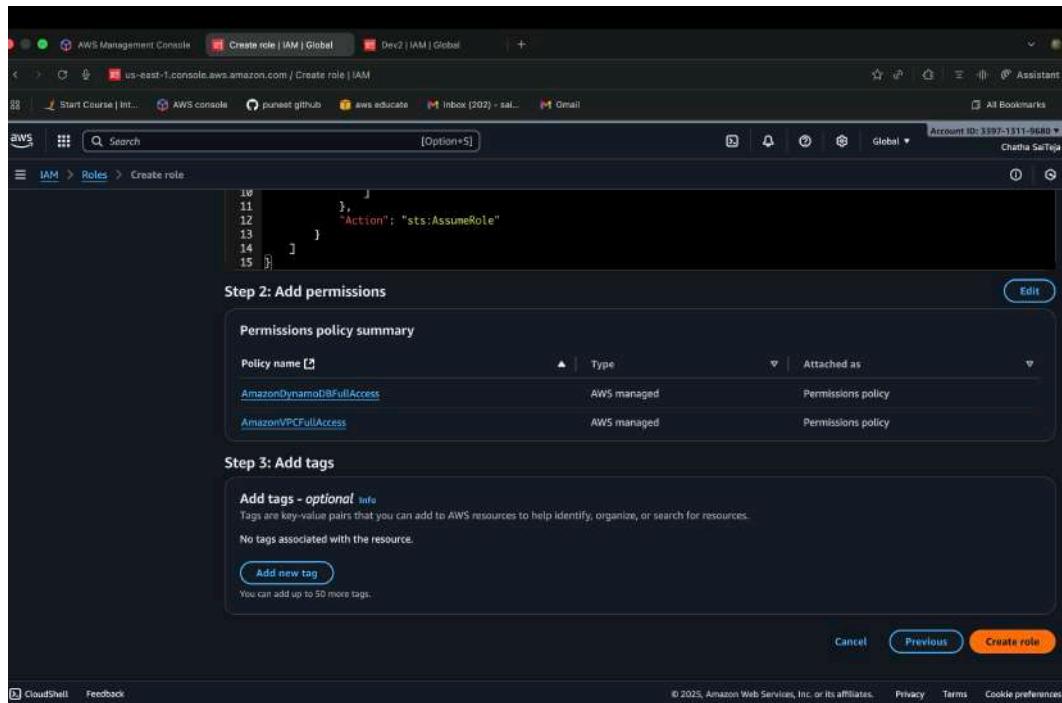
Trust policy

```

1: {
2:   "Version": "2012-10-17",
3:   "Statement": [
4:     {
5:       "Effect": "Allow",
6:       "Principal": {
7:         "AWS": [
8:           "arn:aws:iam::339713119680:user/Dev1",
9:           "arn:aws:iam::339713119680:user/Dev2"
10:        ],
11:       },
12:       "Action": "sts:AssumeRole"
13:     }
14:   ]
15: }

```

Specifying the role details



Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonDynamoDBFullAccess	AWS managed	Permissions policy
AmazonVPCFullAccess	AWS managed	Permissions policy

Step 3: Add tags

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Create role

Click on create role

Identity and Access Management (IAM)

FullAccess-VPC,DynamoDb

Summary

Creation date: October 20, 2025, 00:44 (UTC+05:30)

Last activity: -

ARN: arn:aws:iam::339713119680:role/FullAccess-VPC,DynamoDb

Maximum session duration: 1 hour

Link to switch roles in console: <https://signin.aws.amazon.com/switchrole?roleName=FullAccess-VPC,DynamoDb&account=339713119680>

Permissions | Trust relationships | Tags | Last Accessed | Revoke sessions

Permissions policies (2)

Filter by Type: All types

Policy name	Type	Attached entities
AmazonDynamoDBFullAccess	AWS managed	1
AmazonVPCFullAccess	AWS managed	1

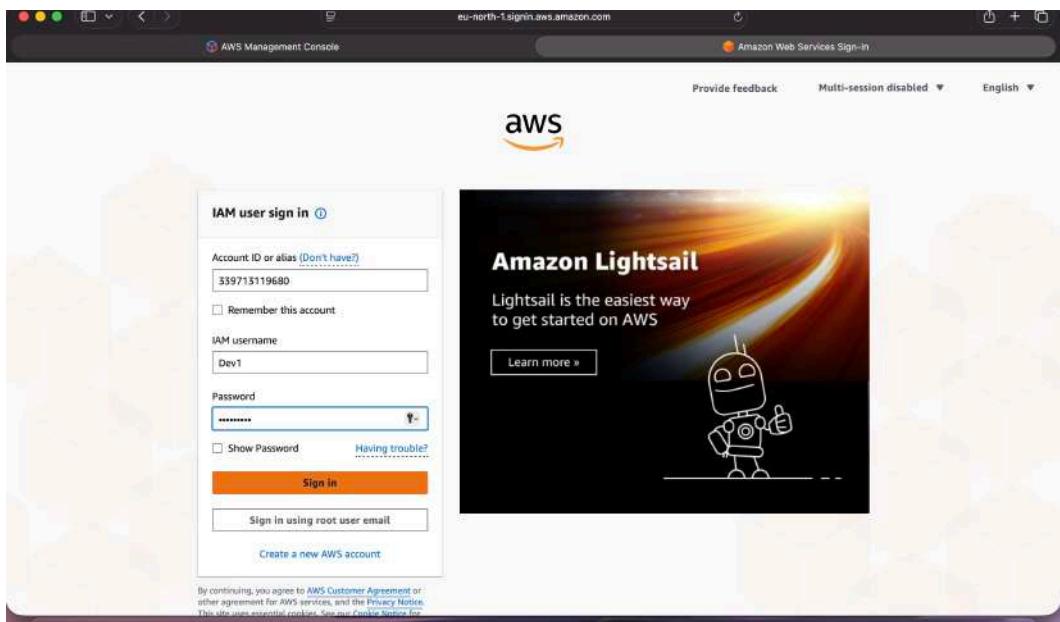
Summary of Role(FullAccess-VPC,DynamoDb)

Step 7:-As role is created we have to try out the role by signing into user1(Dev1) it should be done in other browser by providing the account id, username and password.

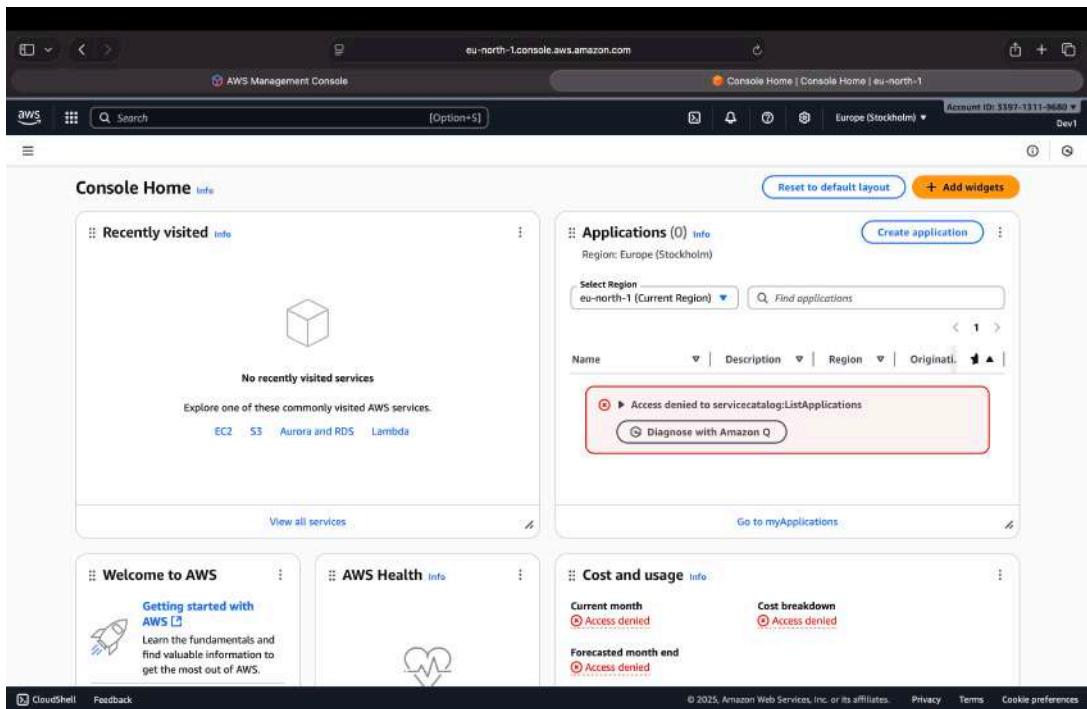
Sign in

Hi, I can connect you with an AWS representative or answer questions you have on AWS.

Click on SignIn



Signing into Dev1



Management Console of Dev1

Step 8:- In right corner of Dev1(user1) console we have account related information in that there is an option of “ Switch Role”, after clicking on switch role we have to mention the account id and name of the role to access the role we created, then we get the access to the role

The screenshot shows the AWS Management Console Console Home page. In the top right corner, there is a sidebar with account information: Account ID (3397-1311-9680), Account color (Access denied), IAM user (Dev1), and a 'Switch role' button. Below this, there are links for Account, Organization, Service Quotas, Billing and Cost Management, and Security credentials. The main content area includes sections for Recently visited services (No recently visited services), Applications (0), Cost and usage, and Welcome to AWS.

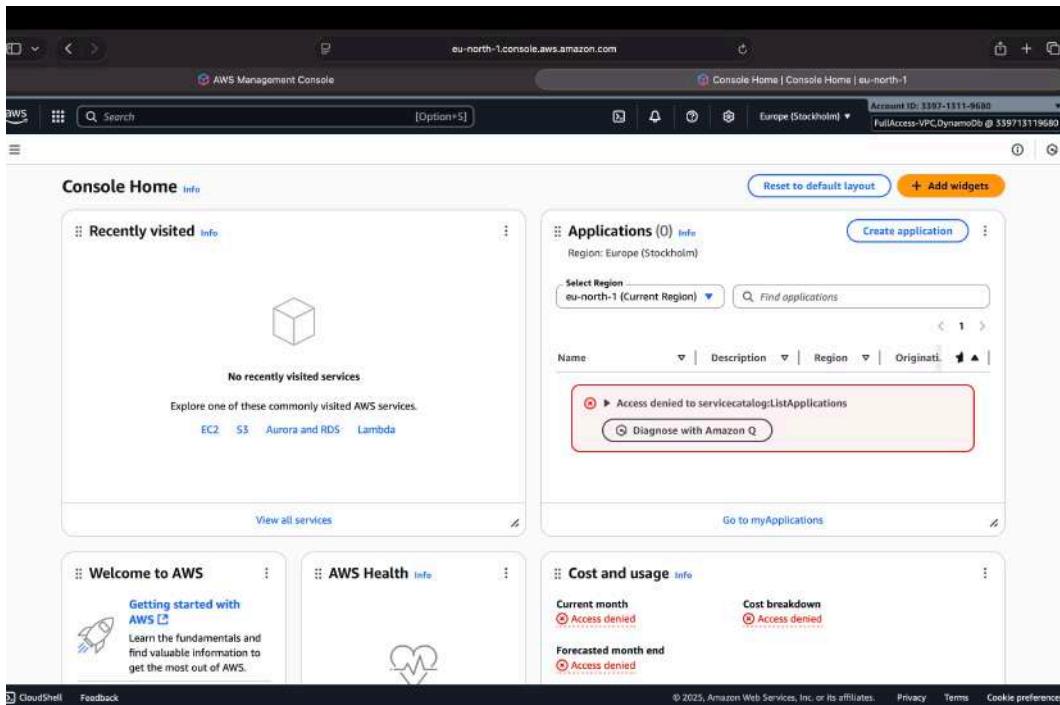
Click on Switch Role

The screenshot shows the 'Amazon Web Services Switch Role' dialog box. It contains the following fields:

- Account ID:** 339713119680
- IAM role name:** FullAccess-VPC,DynamoDb
- Display name - optional:** FullAccess-VPC,DynamoDb @ 339713119680
- Display color - optional:** None

At the bottom right are 'Cancel' and 'Switch Role' buttons, with 'Switch Role' being the highlighted button.

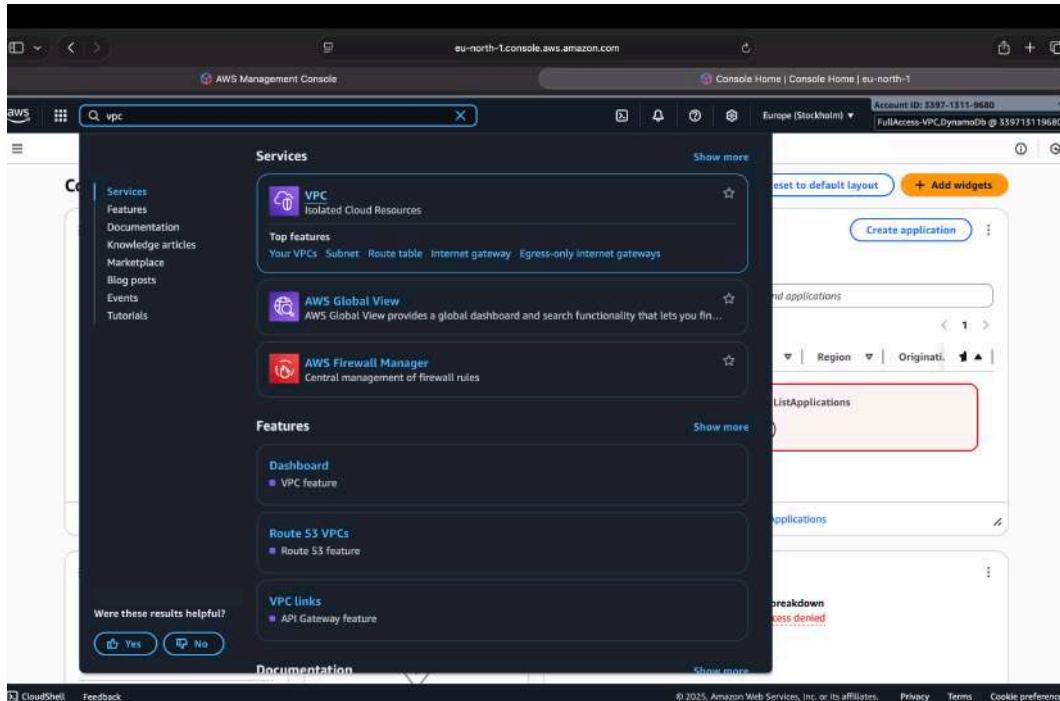
Specifying the Role details then click on switch role



The screenshot shows the AWS Management Console Console Home page. The 'Applications' section displays a red error box with the message 'Access denied to servicelogicatalog>ListApplications'. The search bar at the top contains the text 'vpc'. The page also includes sections for 'Recently visited', 'Welcome to AWS', 'AWS Health', and 'Cost and usage'.

We are in FullAccess-VPC,DynamoDb (role)

Step 9:- Now we have access to the role so we try out the VPC & DynamoDb for checking role is working or not.



The screenshot shows the AWS Management Console search results for 'vpc'. The results list includes 'VPC' (Isolated Cloud Resources), 'AWS Global View' (Provides a global dashboard and search functionality), and 'AWS Firewall Manager' (Central management of firewall rules). The search bar at the top contains the text 'vpc'.

Search for VPC

VPC dashboard

Resources by Region

Service Health

Settings

Additional Information

AWS Network Manager

VPC Dashboard

Services

Features

Documentation

Knowledge articles

Marketplace

Blog posts

Events

Tutorials

Were these results helpful?

Yes

No

Documentation

Service Health

Settings

Additional Information

AWS Network Manager

Search for Dynamo Db

DynamoDb Dashboard

Step 10:- As you can see we can access the VPC, DynamoDb then the role is working , to switch back the role click on account information and there is an option to switch back the role and sign out the user1(Dev1).

Click on Switch back and SignOut