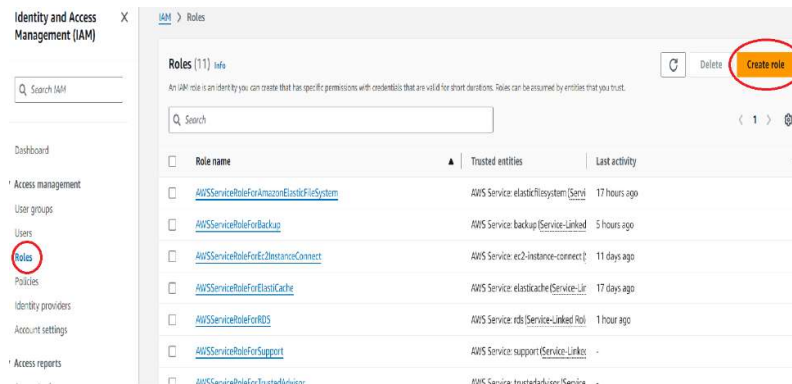


## Tasks To Be Performed:

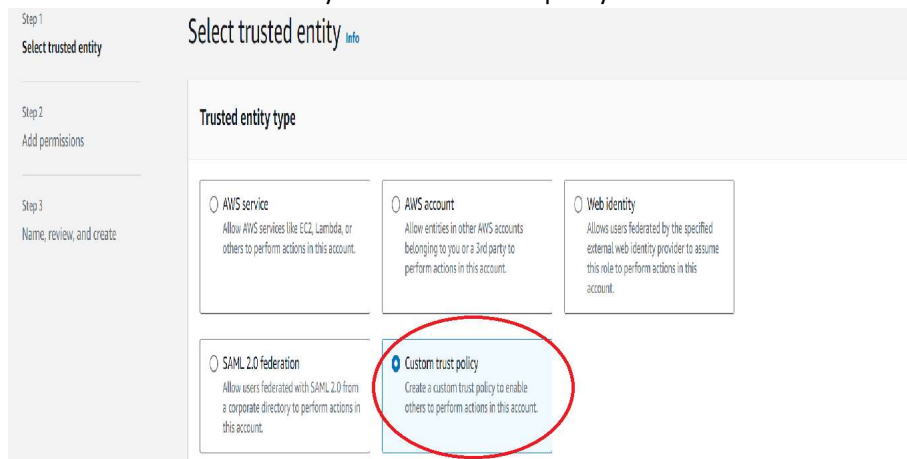
1. Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.
2. Login into user1 and shift to the role to test out the feature

## Solution:

- 1) Click on roles and click create role.



- 2) Under selected trusted entity click custom trust policy



- 3) Under custom trust policy mention:  
Effect": "Allow",  
"Principal": {"AWS": "arn:aws:iam::010526284257:user/Dev1"},  
"Action": "sts:AssumeRole".  
Principal is the Arn of user Dev1 who will be taking the role.

**Custom trust policy**  
Create a custom trust policy to enable others to perform actions in this account

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "arn:aws:iam::80826284257:user/Dev1"
9       },
10      "Action": "sts:AssumeRole"
11    }
12  ]
13 }

```

**Edit statement**  
Statement1 Remove

**Add actions for STS**

Filter actions

- ☐ GetFederationToken info
- ☐ GetServiceBearerToken info
- ☐ GetSessionToken info
- ☒ AssumeRole info
- ☐ AssumeRoleWithSAML info
- ☐ AssumeRoleWithWebIdentity info
- ☐ DecodeAuthorizationMessage info
- ☐ SetContext info
- ☐ GetSourceIdentity info

- 4) Click add new statement . in the same way as above add Dev2 as the principal. Same role is for 2 users.

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "arn:aws:iam::010526284257:user/Dev1"
9       },
10      "Action": "sts:AssumeRole"
11    },
12    {
13      "Sid": "Statement2",
14      "Effect": "Allow",
15      "Principal": {
16        "AWS": "arn:aws:iam::010526284257:user/Dev2"
17      },
18      "Action": "sts:AssumeRole"
19    }
20  ]
21 }

```

**Edit statement**  
Statement1 Statement2 Remove

**Add actions for STS**

Filter actions

- ☐ AssumeRole info
- ☐ AssumeRoleWithSAML info
- ☐ AssumeRoleWithWebIdentity info
- ☐ DecodeAuthorizationMessage info
- ☐ SetContext info
- ☐ GetSourceIdentity info

[+ Add new statement](#)

- 5) Under permission policies choose vpc full access and DynamoDb full access. Click next.

**Add permissions** info

**Permissions policies (1/957)** info  
Choose one or more policies to attach to your new role.

Filter by Type: All types 13 matches

Policy name	Type
<a href="#">AmazonDMSVPCManagementRole</a>	AWS managed
<a href="#">AmazonDRSVPCManagement</a>	AWS managed
<a href="#">AmazonEKSVPCResourceController</a>	AWS managed
<a href="#">AmazonVPCCrossAccountNetworkInterfaceOperations</a>	AWS managed
<input checked="" type="checkbox"/> <a href="#">AmazonVPCFullAccess</a>	AWS managed
<a href="#">AmazonVPCNetworkAccessAnalyzerFullAccessPolicy</a>	AWS managed

**Add permissions** info

**Permissions policies (2/537)** info  
Choose one or more policies to attach to your new role.


Filter by Type: All types 4 matches

Policy name	Type	Description
<input checked="" type="checkbox"/> <a href="#">AmazonDynamoDBFullAccess</a>	AWS managed	Provides full access to Amazon Dynam...
<input type="checkbox"/> <a href="#">AmazonDynamoDBReadOnlyAccess</a>	AWS managed	Provides read-only access to Amazon D...
<input type="checkbox"/> <a href="#">AWSLambdaDynamoDBAccessRole</a>	AWS managed	Provides list and read access to Dynam...
<input type="checkbox"/> <a href="#">AWSLambdaInvocationDynamoDB</a>	AWS managed	Provides read access to DynamoDB Sta...

**Set permissions boundary - optional**

Cancel Previous **Next**

- 6) Under review and create give a role name, check all the details and create role.



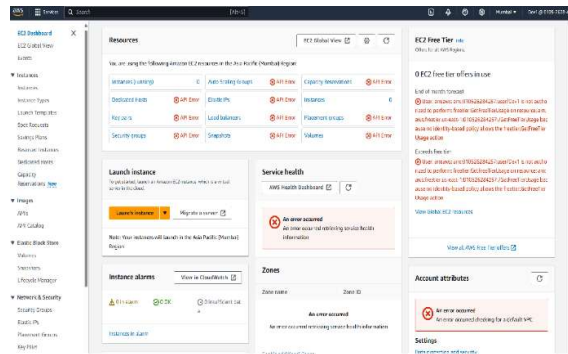
The screenshot shows the 'Name, review, and create' step of the IAM role creation process. The 'Role name' field is highlighted with a red circle and contains the text 'Demo-role'. Below it, the 'Description' field is empty. The 'Permissions' section is partially visible at the bottom.

**Roles** (1/12) [info](#)

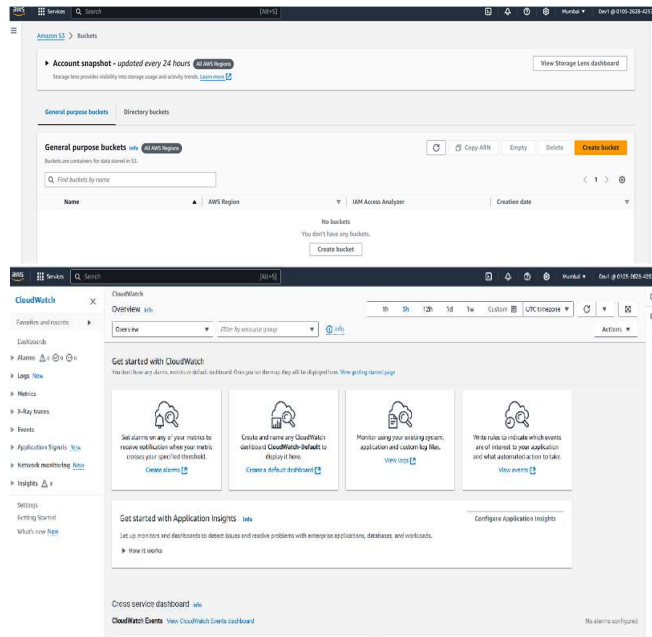
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	Role name	Trusted entities	Last activity
<input type="checkbox"/>	<a href="#">AWSServiceRoleForElasticCache</a>	AWS Service: elasticache (Service-Linked Role)	17 days ago
<input type="checkbox"/>	<a href="#">AWSServiceRoleForRDS</a>	AWS Service: rds (Service-Linked Role)	2 hours ago
<input type="checkbox"/>	<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service-Linked Role)	-
<input checked="" type="checkbox"/>	<a href="#">Demo-role</a>	Account: 010526284257	-
<input type="checkbox"/>	<a href="#">ec2-access-cw</a>	AWS Service: ec2	47 days ago
<input type="checkbox"/>	<a href="#">fullaccess</a>	Account: 010526284257	64 days ago
<input type="checkbox"/>	<a href="#">rds-monitoring-role</a>	AWS Service: monitoring.rds	-
<input type="checkbox"/>	<a href="#">s3err_role_for_poulomi-bucket-1</a>	AWS Service: s3	27 days ago

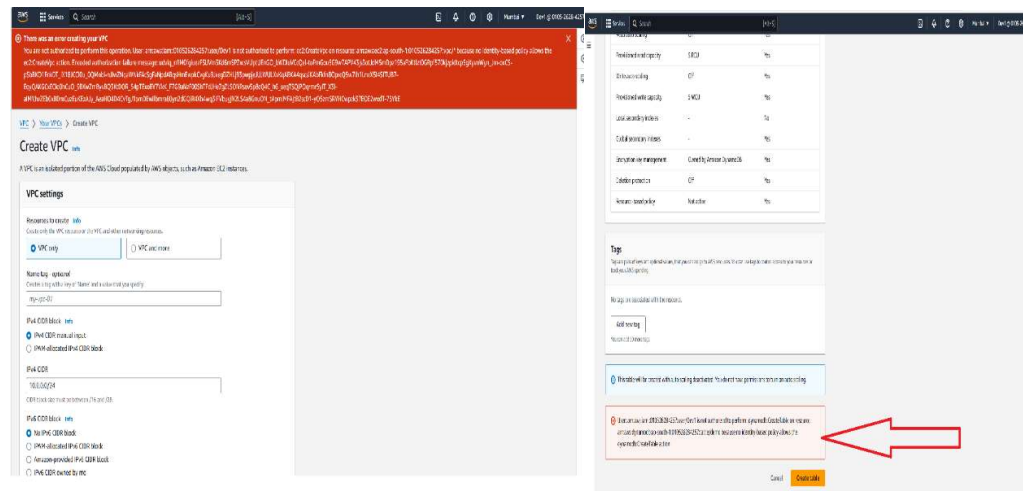
The screenshot shows the AWS IAM console interface for signing in as an IAM user. The page title is 'Sign in as IAM user'. Below the title, the account ID '0156284257' is displayed, followed by the IAM user name 'Dev1'. The 'Sign in as IAM user' button is highlighted with a red circle. To the left of the main content, there is a sidebar with the AWS logo and the text 'Sign in'. Below the sidebar, there is a section titled 'Account ID (12 digits) or account alias' with the value '0156284257'. At the bottom of the sidebar, there is a link 'Sign in as root user email' and a link 'Forgot password?'. The main content area has a blue header with the text 'AWS End User Computing named a Leader' and a Gartner Magic Quadrant for Desktop as a Service (DaaS) 2024. The footer of the page contains the text '© 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved.' and a 'Feedback' button.



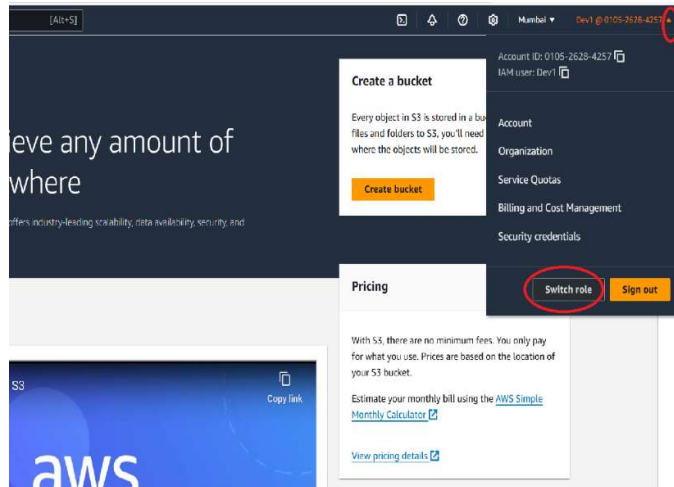
10) If we go to s3, RDS, Cloudwatch , billing we can see Dev1 is authorised to do all actions.



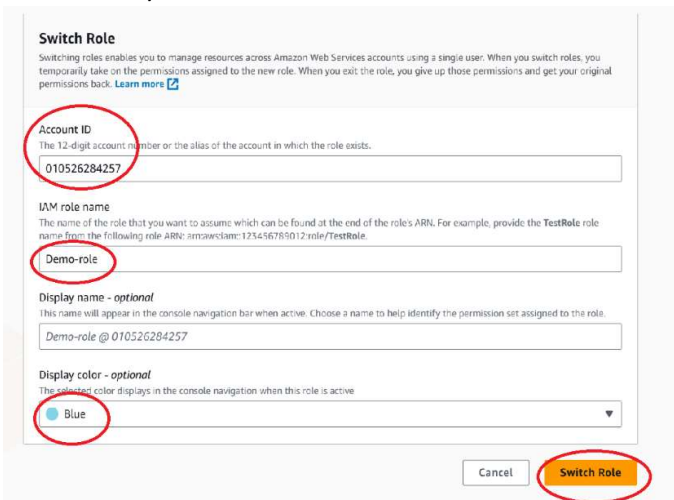
11) Earlier we created a role for Dev1 where he can access vpc and dynamodb . so let us check whether he can access or not. We are not able to access vpc or dynamodb as shown below.



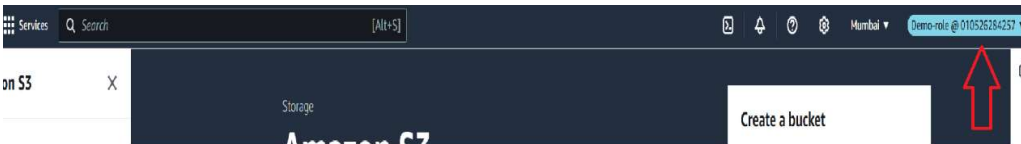
- 12) As we can see Dev1 user cant access Vpc and Dynamodb. So first he needs to assume the role and then only he can access both of the above services. To assume role click on the arrow beside the Dev1 username top right corner and then click switch role.



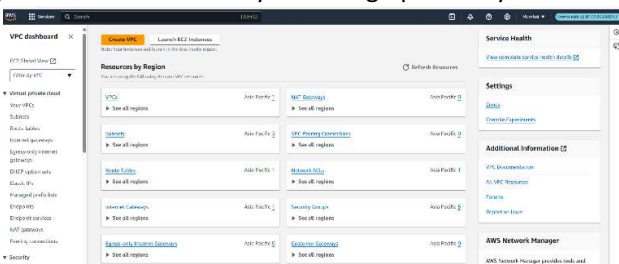
- 13) Enter the account id , IAM role name and a display color to show that the role is active. Then you can switch role.



- 14) As soon as Dev1 assumes the role the color changes to blue to show that the role is active.



- 15) Now we can try accessing Vpc and dynamodb. Vpc and dynamodb is accessible.





18) Dev1 get all his permission back and the role is inactive .

