

# 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**

Roles > Create role

missions

view, and create

### Trusted entity type

- ☐ AWS service  
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☒ AWS account  
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ Web identity  
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ SAML 2.0 federation  
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ Custom trust policy  
Create a custom trust policy to enable others to perform actions in this account.

### An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- ☒ This account (062250062838)
- ☐ Another AWS account

### Options

- ☐ Require external ID (Best practice when a third party will assume this role)
- ☐ Require MFA  
Requires that the assuming entity use multi-factor authentication.

**Info**


### Info

Choose one or more policies to attach to your new role.

**Info**

**Info**

Choose one or more policies to attach to your new role.

<input type="text" value="vpc"/> <span>All types</span> <span>1 match</span>			
<input checked="" type="checkbox"/>	Policy name	Type	Description
<input checked="" type="checkbox"/>	 <a href="#">AmazonVPCFullAccess</a>	AWS managed	Provides full access to Amazon VPC via t...

- Set permissions boundary - *optional*

**Next**

**Info**

Allows User1 and User2 full access to VPC and DynamoDB

## Summary


**Creation date**  
October 17, 2025, 13:52 (UTC+05:30)

### Last activity

**ARN**  
arn:aws:iam::062250062838:role/VPC-DynamoDB-Access-Role

**Maximum session duration**  
1 hour

**Link to switch roles in console**

 <https://signin.aws.amazon.com/switchrole?roleName=VPC-DynamoDB-Access-Role&account=062250062838>

## Permissions

## Trust relationships

## Tags

Last Accessed

## Revoke sessions

**Info**

You can attach up to 10 managed policies.

Q Search All types < 1 > 

## 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"
    }
  ]
}
```

---

## Edit trust policy

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::062250062838:user/Dev1",
9           "arn:aws:iam::062250062838:user/Dev2"
10        ]
11      },
12      "Action": "sts:AssumeRole"
13    }
14  ]
15 }
16

```

VPC-DynamoDB-Access-Role

Last activity	Access-Role	roleName=VPC-DynamoDB-Access-Role&account=062250062838
	Maximum session duration 1 hour	

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

**Trusted entities** [Edit trust policy](#)

Entities that can assume this role under specified conditions.

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::062250062838:user/Dev1",
9           "arn:aws:iam::062250062838:user/Dev2"
10        ]
11      },
12      "Action": "sts:AssumeRole"
13    }
14  ]
15 }

```

### 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**.

[IAM](#) > [Users](#) > [Dev1](#) > Create policy

Step 1  
**Specify permissions**

Step 2  
 Review and create

### Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

#### Policy editor

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Resource": "arn:aws:iam::062250062838:role/VPC-DynamoDB-Access-Role"
8     }
9   ]
10 }
11

```

Review the permissions, specify details, and tags.

#### Policy details

**Policy name**  
 Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+,=,\_,@,-' characters.

#### Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

**Allow (1 of 449 services)** Show remaining 448 services

Service	Access level	Resource	Request condition
STS	Limited: Write	RoleName  string like  VPC-DynamoDB-Access-Role	None

[Cancel](#)
[Previous](#)
[Create policy](#)

[Users](#) > Dev1

id Access

ment (IAM)

M

arn:aws:iam::062250062838:user/Dev1

Created

October 17, 2025, 13:03 (UTC+05:30)

Console access

Enabled without MFA

Last console sign-in

Today

Access key 1

Create access key

Permissions

Groups (2)

Tags

Security credentials

Last Accessed

Permissions policies (1/4)

Remove

Add permissions

Permissions are defined by policies attached to the user directly or through groups.

Search

Filter by Type

All types

Policy name

Type

Attached via

<input checked="" type="checkbox"/>	<a href="#">allowVPC-DynamoDBRole</a>	Customer inline	Inline
<input type="checkbox"/>	<a href="#">IAMUserChangePassword</a>	AWS managed	Directly
<input type="checkbox"/>	<a href="#">Policy1</a>	Customer managed	Group <a href="#">Dev-Team</a>
<input type="checkbox"/>	<a href="#">Policy2</a>	Customer managed	Group <a href="#">Ops-Team</a>

## 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.

Global ▼

Account ID: 0622-5006-2838 ▲

Dev1

1 other active session

Account ID: 0622-5006-2838

root

Turn off multi-session support

Add session

Current session

Account ID

0622-5006-2838

Account color

Access denied

IAM user

Dev1

Account

Organization

Service Quotas

Billing and Cost Management

Security credentials

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

ur VPCs

Your VPCs (1) Info

Last updated less than a minute ago

Actions

Create VPC

Find VPCs by attribute or tag

< 1 >

<input type="checkbox"/>	Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	-	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

< 1 >

<input checked="" type="checkbox"/>	Name	Status	Partition key	Sort key	Indexes	Replication Regions	Deletion protection	Favorite	Read capacity mode
<input checked="" type="checkbox"/>	demo-table	Creating	student-id (S)	-	0	0	Off	☆	On-demand

AWS

Search[Alt+S]

Europe (Stockholm)

Account ID: 0622-5006-2838

VPC-DynamoDB-Access-Role @ 062250062838

EC2

Dashboard

AWS Global View

Events

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Capacity Manager

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

EC2 Free Tier

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 use 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 use 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.