

# Module 8 Assignment 3 - IAM

You have been asked to:

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

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

**Roles**

Policies

Introducing the new Roles list experience

We've redesigned the Roles list experience to make it easier to use. [Let us know what you think.](#)

IAM > Roles

Roles (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.

Search

Role name

Trusted entities

Last activity

Refresh

Delete

Create role

Create role

Select type of trusted entity

AWS service

EC2, Lambda and others

Another AWS account

Belonging to you or 3rd party

Web identity

Cognito or any OpenID provider

SAML 2.0 federation

Your corporate directory

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID\*

Options

Require external ID (Best practice when a third party will assume this role)

Require MFA

Filter policies

dynamo

Policy name

AmazonDynamoDBFullAccess

AmazonVPCFullAccess

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include a key and a value. You can use the tags to organize, track, or control access for this role.

Key

Value (optional)

Name

m8a3\_new\_role

CreatedBy

Hariharan Narayanan

Review

Provide the required information below and review this role before you create it.

Role name\*

m8a3\_new\_role

Use alphanumeric and '+' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+' characters.

Trusted entities

The account 098760042302

Policies

AmazonDynamoDBFullAccess

AmazonVPCFullAccess

Permissions boundary

Permissions boundary is not set

The new role will receive the following tags

Key

Value

Name

m8a3\_new\_role

CreatedBy

Hariharan Narayanan

The role m8a3\_new\_role has been created.

m8a3\_new\_role

1

2

3

4

5

6

7

1. Open IAM Console and click on "Roles"
2. In the Roles Console, click on "Create role"
3. In Step 1, select "Another AWS account" and provide your AWS account ID
4. Search and select DynamoDBFullAccess and VPCFullAccess. Click "Next"
5. Create Tags and click "Next"
6. In the Review page, name the role as "m8a3\_new\_role" and click on "Create role"
7. Verify that new role is created.



m8a3\_new\_role

8

Roles > m8a3\_new\_role

## Summary

Role ARN	arn:aws:iam:: <b>[REDACTED]</b> :role/m8
Role description	<a href="#">Edit</a>
Instance Profile ARNs	
Path	/
Creation time	2022-01-22 18:31 UTC+0530
Last activity	Not accessed in the tracking period
Maximum session duration	1 hour <a href="#">Edit</a>

Give this link to users who can switch roles in the console [https://signin.aws.amazon.com/switchrole?role=arn:aws:iam::\[REDACTED\]:role/m8a3\\_new\\_role](https://signin.aws.amazon.com/switchrole?role=arn:aws:iam::[REDACTED]:role/m8a3_new_role)

[Permissions](#) **[Trust relationships](#)** [Tags \(2\)](#) [Access Advisor](#) [Revoke sessions](#)

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

[Edit trust relationship](#)

**Trusted entities**

The following trusted entities can assume this role.

**Trusted entities**

The account **[REDACTED]**

## Edit Trust Relationship

You can customize trust relationships by editing the following access control

### Policy Document

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::[REDACTED]:user/user2",
9           "arn:aws:iam::[REDACTED]:root",
10          "arn:aws:iam::[REDACTED]:user/user1"
11        ]
12      },
13      "Action": "sts:AssumeRole",
14      "Condition": {}
15    }
16  ]
17 }
```

10

[Permissions](#) **[Trust relationships](#)** [Tags \(2\)](#) [Access Advisor](#)

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

[Edit trust relationship](#)

**Trusted entities**

The following trusted entities can assume this role.

**Trusted entities**

The account **[REDACTED]**

arn:aws:iam::**[REDACTED]**:user/user1

arn:aws:iam::**[REDACTED]**:user/user2

11

8. Open Roles Console. Click on the newly created role "m8a3\_new\_role"
9. Click on "Trust Relationships". Click on "Edit trust relationship"
10. . Add users user1 and user2 in the JSON. Save and return
11. In the Roles console, verify that the users user1 and user2 are now visible in Trusted entities.



## Sign in

☐ **Root user**  
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☒ **IAM user** 12  
User within an account that performs tasks. [Learn more](#)

Account ID (12 digits) or account alias

hariharannarayanan

Next



## Sign in as IAM user

Account ID (12 digits) or account alias

[Redacted]

IAM user name

user1 13

Password

[Redacted]

☐ Remember this account

Sign in

12. Logout. In the Login screen, choose "IAM user"
13. Type account ID or alias, choose "user1" as user name, type password, and sign in.
14. After login, verify from top-right that "user1" is logged in.

### Console Home [Info](#)

Actions ▼

#### Recently visited [Info](#)



IAM

Billing

#### Welcome to AWS [Info](#)



[Getting started with AWS](#)

Learn the fundamentals and find valuable information to get the most out of AWS.

14

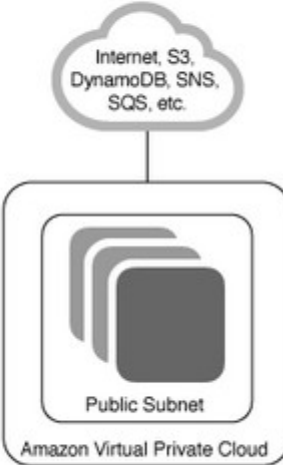
aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

## Step 1: Select a VPC Configuration

<b>VPC with a Single Public Subnet</b>	<p>Your instances run in a private, isolated section of the Amazon Web Services cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.</p> <p><b>Creates:</b></p> <p>A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.</p> <div><p><b>Important:</b></p><p>If you are using a Local Zone with your VPC <a href="#">follow this link</a> to create your VPC.</p></div> <div>15</div> <div>Select</div>	
VPC with Public and Private Subnets		
VPC with Public and Private Subnets and Hardware VPN Access		
VPC with a Private Subnet Only and Hardware VPN Access		

15. Open VPC wizard from VPC console to confirm that User1 has assumed the role correctly to create VPC.