**Lesson 7 Demo 6**

**Create and Configure Cross-account Management Console Access Using IAM Roles**

**Objective:** To configure cross-account management console access using IAM roles

**Tools required:** AWS Lab

**Prerequisites:**

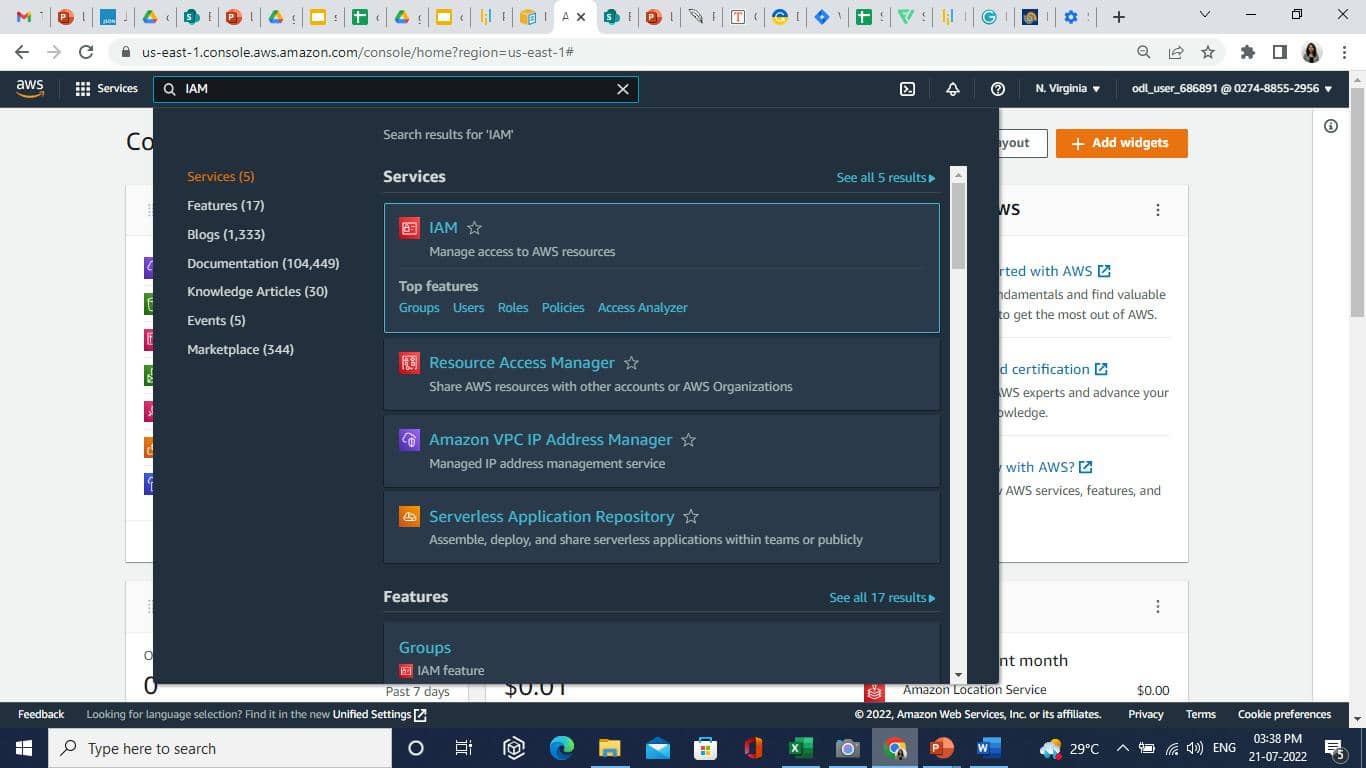
* + 1. One bucket should be created in the S3 bucket named (**asiproductionbucket**).
    2. In the **IAM** user group, one group should be created named (asi-developers).
    3. In the users, one user should be created named as (asi-dev).

**Steps to be followed:**

* + 1. Creating a role in the production account.
    2. Granting access to the role.
    3. Testing the access by switching roles.

**Step 1: Creating a role in the production account.**

* 1. Open the **IAM** console.



* 1. Select the **Policies** and click on the **Create policy** button.

A screenshot of a computer

Description automatically generated

* 1. Click on the **JSON** tab and paste the following code. After that click on the **Next: Tags** button.

**{**

**"Version": "2012-10-17",**

**"Statement": [**

**{**

**"Effect": "Allow",**

**"Action": "s3:ListAllMyBuckets",**

**"Resource": "\*"**

**},**

**{**

**"Effect": "Allow",**

**"Action": [**

**"s3:ListBucket",**

**"s3:GetBucketLocation"**

**],**

**"Resource": " arn:aws:s3:::asiproductionbucket"**

**},**

**{**

**"Effect": "Allow",**

**"Action": [**

**"s3:GetObject",**

**"s3:PutObject",**

**"s3:DeleteObject"**

**],**

**"Resource": " arn:aws:s3:::asiproductionbucket"**

**}**

**]**

**}**

Note:

Replace the **Resource** value with the bucket **ARN**.

Graphical user interface, text, email

Description automatically generated

* 1. Click on the **Next: Review** button.

A screenshot of a computer

Description automatically generated

* 1. On the **Review policy** page, enter the **name** as **read-write-app-bucket,** then click on the **Create policy** button.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* 1. The policy is created successfully.

A screenshot of a computer

Description automatically generated

* 1. To create roles, select the **Roles** option, then click on the **Create role** button.

A screenshot of a computer

Description automatically generated

* 1. Click on the **AWS account** option.

Graphical user interface, text

Description automatically generated

* 1. Click on the **Another AWS account** and enter the **account ID**.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, email

Description automatically generated

1. Click on the **Next** button.
2. Select the created policy and click on the **Next** button.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Enter the **Role name** and **Description** as shown below:

Graphical user interface, text, application

Description automatically generated

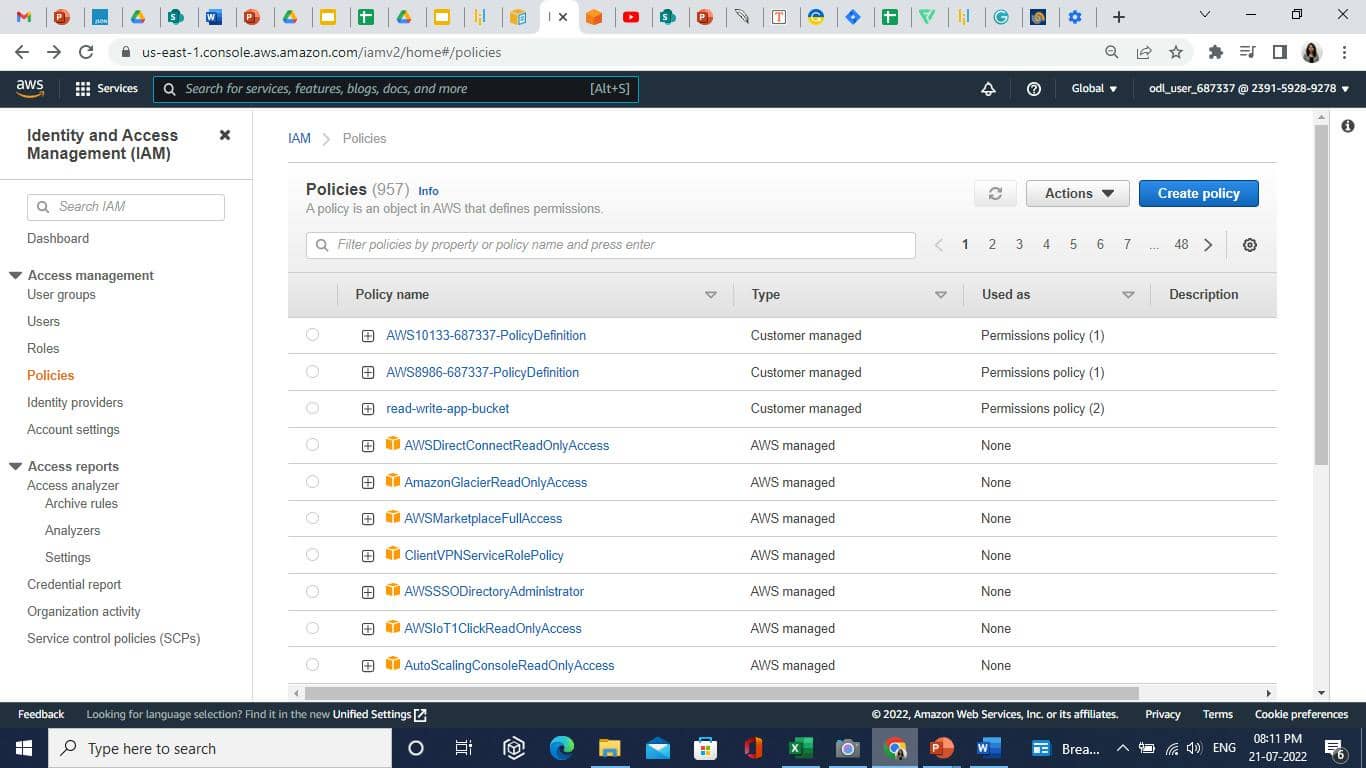
1. Click on the **Create role** button.
2. The role is created successfully.

A screenshot of a computer

Description automatically generated

**Step 2: Granting access to the role.**

* 1. Open the **IAM** console. Select **Policies** and click on the **Create policy** button.



* 1. In the JSON tab enter the following code and click on the **Next: Tags** button.

**{**

**"Version": "2012-10-17",**

**"Statement": {**

**"Effect": "Allow",**

**"Action": "sts:AssumeRole",**

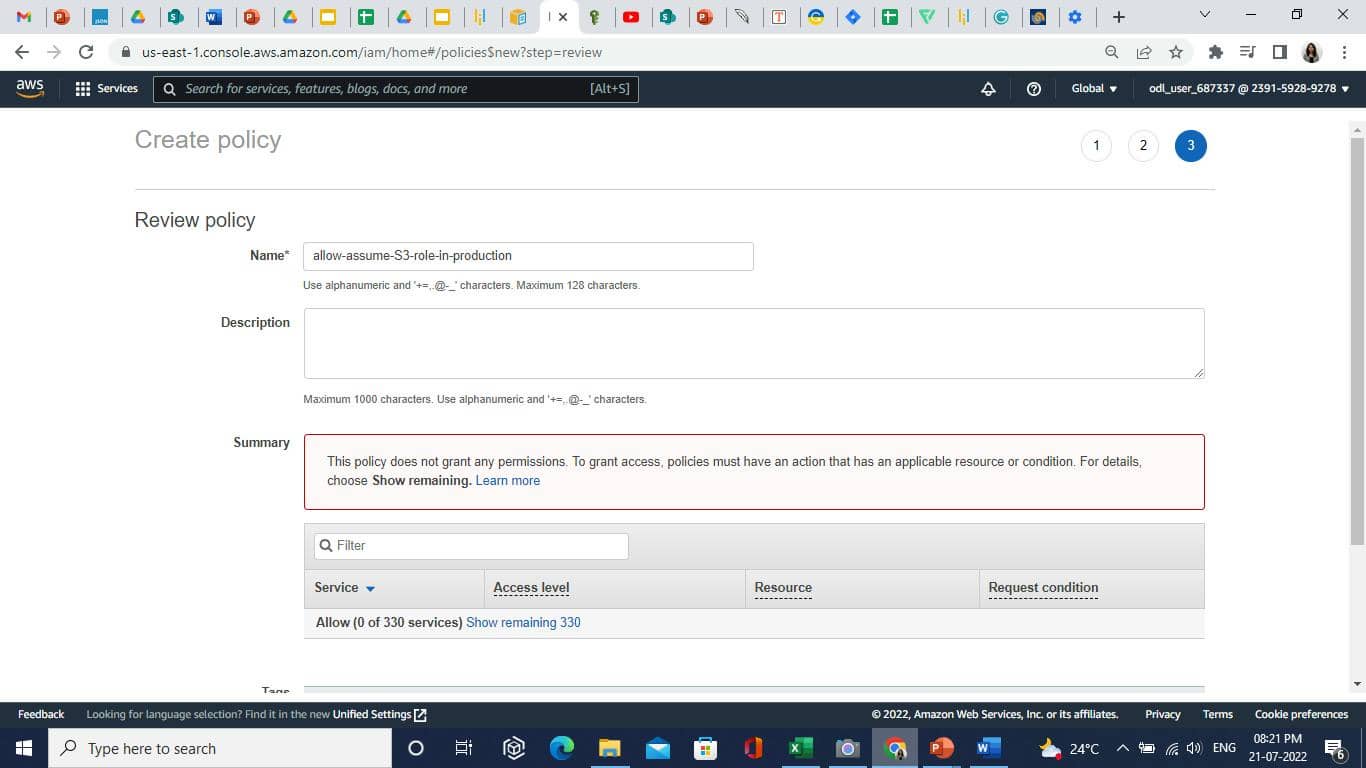
**"Resource": "arn:aws:iam::239159289278:policy/read-write-app-bucket"**

**}**

Note:

For the resource value, enter the read-write-app-bucket policy ARN.

* 1. Click on the **Next: Review** button.
  2. Enter the name as shown below:



* 1. Open the IAM console. Select the **User groups.**

A screenshot of a computer

Description automatically generated

1. Click on the **asi-developers** group. Then in the **Permissions** tab, click on the **Add permissions** button.

A screenshot of a computer

Description automatically generated

1. Click on the **Attach policies** and select the policy that was created previously.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Click on the **Add permissions** button.
2. The policy is added successfully.

A screenshot of a computer

Description automatically generated

**Step 3: Testing the access by switching roles.**

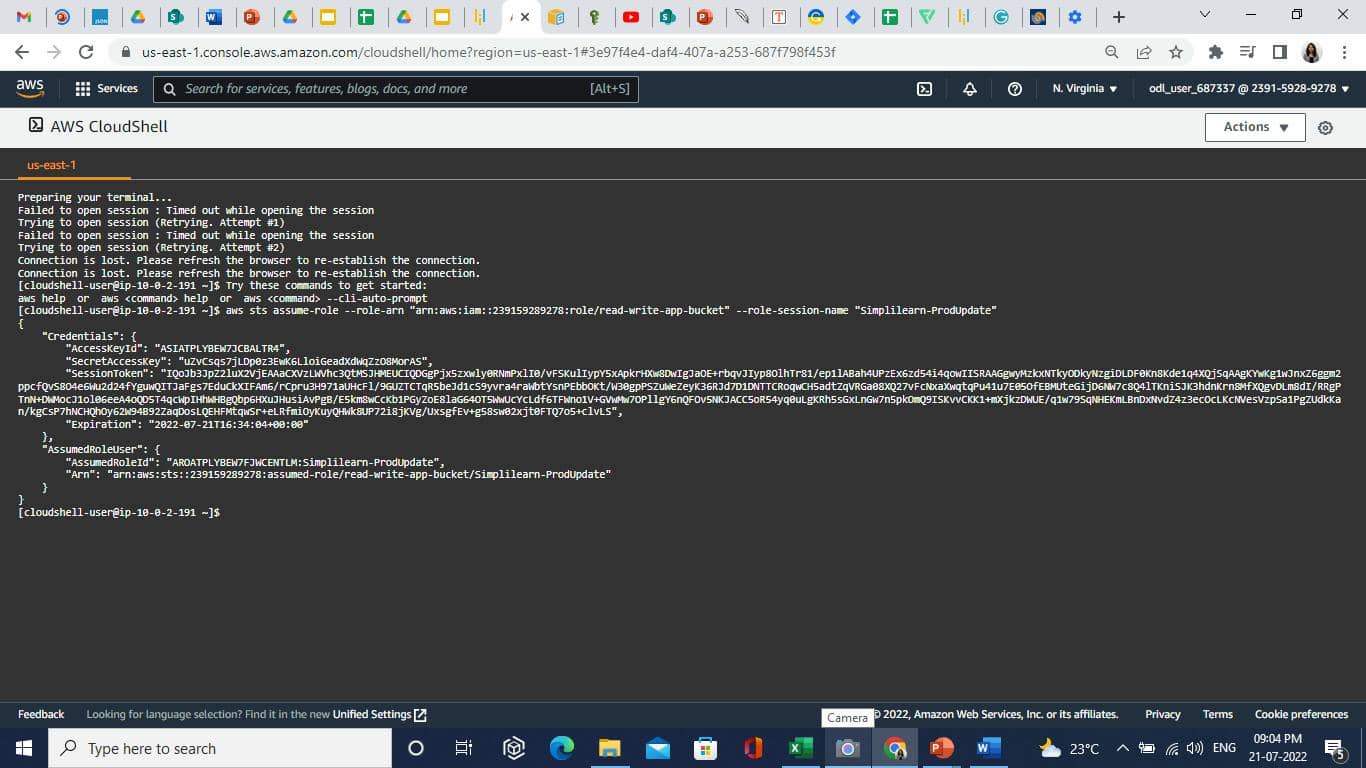
* 1. Open the **cloudShell**.

Graphical user interface, text, application

Description automatically generated

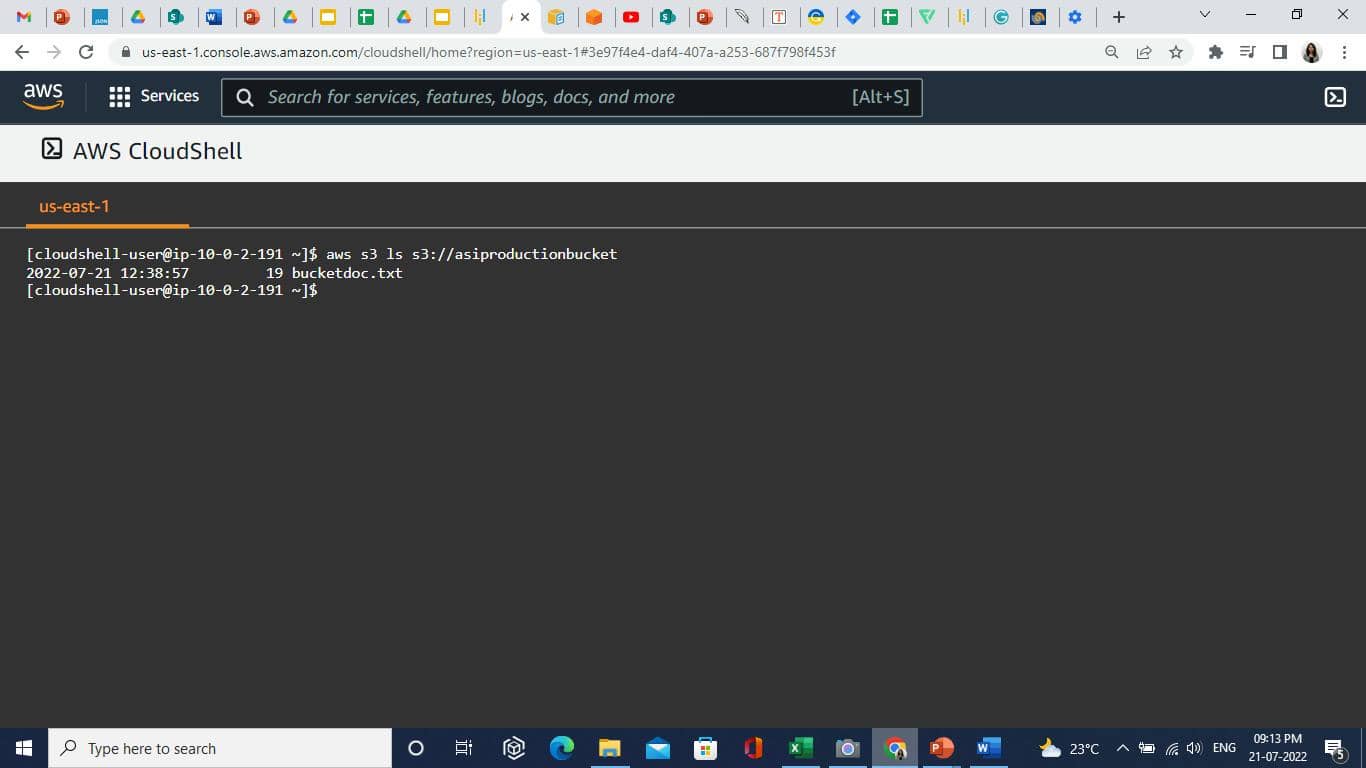
* 1. Enter the following command in **CloudShell**:

**aws sts assume-role --role-arn "arn:aws:iam::239159289278:role/read-write-app-bucket" --role-session-name "Simplilearn-ProdUpdate"**



* 1. To access the resources in the production account, paste the following command:

**aws s3 ls s3://asiproductionbucket**



The user got access to the S3 bucket from the development user successfully.