**Lesson 7 Demo 1**

**Using Identity-Based Policy Implicit Denies and Explicit Allow**

**Objective:** To use identity-based policy implicit deny and explicit allow

**Tools required:** AWS Lab

**Prerequisites:** None

**Steps to be followed:**

1. Configuring identity-based policy
2. Performing implicit denial on the bucket
3. Performing explicit allow

**Step 1: Configuring identity-based policy.**

* 1. Go to your Amazon console and search for IAM in the search bar.

Graphical user interface, application

Description automatically generated

* 1. In the IAM dashboard, select **Users** then click on **Add users** button.

Graphical user interface

Description automatically generated

* 1. Enter the User name as **user1** and select **Access Key - Programmatic access**,then click on **Next: Permissions** as shown below:

Graphical user interface, text, email

Description automatically generated

* 1. Click on **Next: Tags.**

Graphical user interface, text, application

Description automatically generated

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

Graphical user interface, text

Description automatically generated

* 1. Click on **Create user** button.

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

* 1. Follow the above procedure for creating **user2.**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Graphical user interface, text

Description automatically generated

* 1. Now, to add the permissions in **user1** click on **user1.**

A screenshot of a computer

Description automatically generated

* 1. Click on **Add permissions** button.

Graphical user interface, text, email

Description automatically generated

* 1. Click on **Attach existing policy directly.**

A screenshot of a computer

Description automatically generated

* 1. In **Filter policies** search **s3** and click on **AmazonS3FullAccess** then click on **Next: Review.**

A screenshot of a computer

Description automatically generated

* 1. Click on **Add permissions** button.

Graphical user interface, text, application, Word

Description automatically generated

* 1. Policy is added successfully.

Graphical user interface, text

Description automatically generated

**Step 2: Performing implicit denial on the bucket**

* 1. Create and select a bucket name as **implicitdenydemo.**

A screenshot of a computer

Description automatically generated

* 1. In the **Permissions** section, click on **Edit** in Bucket policy.

Graphical user interface, text, email

Description automatically generated

A screenshot of a computer

Description automatically generated

* 1. Paste the following code into the **Bucket policy** editor as shown below:

**{**

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

**"Statement": [**

**{**

**"Sid": "Stmt1657599426763",**

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

**"Principal": {**

**"AWS": "arn:aws:iam::350558460714:user/user1"**

**},**

**"Action": "s3:\*",**

**"Resource": "arn:aws:s3:::implicitbucketdemo"**

**},**

**{**

**"Sid": "DenyReports",**

**"Effect": "Deny",**

**"Principal": {**

**"AWS": "arn:aws:iam::350558460714:user/user1"**

**},**

**"Action": "s3:\*",**

**"Resource": "arn:aws:s3:::implicitbucketdemo"**

**}**

**]**

**}**

**Note:**

For sid- refer to policy generator sid.

For AWS: In the Users section refer to **User1 ARN.**

For Resources: In **Buckets** select **implicitdemo** and refer to **copy ARN.**

Graphical user interface, text

Description automatically generated

* 1. Click on the **Save changes** button.

Graphical user interface, text, application

Description automatically generated

* 1. Policy is added successfully.

A screenshot of a computer

Description automatically generated

**Step 3: Performing explicit allow**

* 1. Create and select a bucket demo as **explicitbucketdemo.**

Graphical user interface, text, email

Description automatically generated

* 1. In the **permissions** section, click on **Edit** in Bucket policy.

Graphical user interface, text, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* 1. Paste the following code into the editor:

**{**

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

**"Statement": [**

**{**

**"Sid": "Stmt1657613189151",**

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

**"Principal": {**

**"AWS": "arn:aws:iam::350558460714:user/user2"**

**},**

**"Action": "s3:\*",**

**"Resource": "arn:aws:s3:::explicitbucketdemo"**

**},**

**{**

**"Sid": "AllowS3Self",**

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

**"Principal": {**

**"AWS": "arn:aws:iam::350558460714:user/user2"**

**},**

**"Action": "s3:\*",**

**"Resource": "arn:aws:s3:::explicitbucketdemo"**

**}**

**]**

**}**

**Note:**

For sid- reffer policy generator sid.

For AWS: In the Users section refer to **User ARN.**

For Resources: In **Buckets** select **explicitdemo** and refer to **copy ARN.**

* 1. Policy is added successfully.

Graphical user interface, text, application, email

Description automatically generated