IAM ROLE

This guide explains how to create an IAM role in your AWS account that is specifically assumable by an IAM user named "john." The role is created using a custom trust policy that restricts role assumption to only that user.

Prerequisites

- An AWS account with permissions to create and manage IAM roles and users.
- The IAM user "john" must already exist in your account.
- Familiarity with the AWS Management Console (or AWS CLI) is helpful.

Step 1: Sign in to the AWS Management Console

1. Open your web browser and navigate to the AWS Management Console.
2. Log in using your AWS credentials.

Step 2: Navigate to the IAM Console

1. In the AWS Management Console, type **IAM** in the search bar and select the **IAM** service.
2. In the left-hand navigation pane, click on **Roles**.

Step 3: Create a New Role

1. Click the **Create role** button.
2. Under **Select trusted entity**, choose **AWS account**.
3. Select **This account** since the user "john" exists in the same account.
4. Click **Next: Permissions**.

Step 4: Attach Permissions Policies (Optional)

1. On the **Attach permissions policies** page, select one or more policies that you want this role to have.
   Example: Choose **AmazonS3ReadOnlyAccess** if you want to grant read-only access to Amazon S3.
2. Click **Next: Tags**.
3. (Optional) Add tags to help organize your roles.

4. Click **Next: Review**.

Step 5: Configure the Trust Policy

1. On the **Review** page, enter a **Role name** (e.g., `RoleForJohn`) and a description (e.g., "Role for user john with custom trust policy").
2. Click the **Edit trust policy** button to modify the trust relationship.
3. Replace the default trust policy with the following custom trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<YOUR_ACCOUNT_ID>:user/john"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

> **Note:** Replace `<YOUR_ACCOUNT_ID>` with your actual AWS account ID.

Step 6: Review and Create the Role

- Review all the role details, including the permissions and the custom trust policy.
- Click **Create role** to finalize the creation of the IAM role.

Step 7: Verify the Role

1. In the IAM console, go to the **Roles** section and locate the newly created role (`RoleForJohn`).
2. Click on the role, then select the **Trust relationships** tab.
3. Verify that the trust policy correctly lists the IAM user **"john"** as the only principal allowed to assume the role.

Step 8: How John Can Use This Role from the AWS Console

Once the role is created and assigned, **John** can assume the role using the AWS Management Console by following these steps:

1. **Log in** to the AWS Management Console using John's IAM user credentials.
2. In the top-right corner, click on **John's username** and select **Switch Role**.
3. Click on **Switch Role** again.
4. Enter the following details:
    - **Account ID or Alias**: `<YOUR_ACCOUNT_ID>`
    - **Role Name**: `RoleForJohn`
5. (Optional) Add a **Display Name** for easier identification.
6. Click **Switch Role**.

Now, John will be acting with the permissions of `RoleForJohn` and can access AWS services based on the assigned permissions.

Install AWS cli

https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

---

Step-by-Step Guide: Creating an IAM Role for EC2 to Access S3

Step 1: Create an IAM Role for EC2 to Access S3

1.1 Sign in to AWS Management Console

1. Go to the **IAM** service in the AWS console.
2. Click on **Roles** from the left navigation panel.
3. Click **Create role**.

1.2 Select Trusted Entity

1. Under **Trusted entity type**, choose **AWS service**.
2. Select **EC2** as the use case.
3. Click **Next**.

1.3 Attach S3 Permissions

1. Search for and select the **AmazonS3FullAccess** policy *(or a custom policy with required permissions)*.
2. Click **Next**.

1.4 Add Role Name and Tags

1. Enter a **Role name** (e.g., `EC2S3AccessRole`).
2. (Optional) Add **tags** for tracking.
3. Click **Create role**.

Step 2: Attach the IAM Role to an EC2 Instance

2.1 Navigate to the EC2 Instance

1. Open the **EC2 Dashboard** in the AWS Console.
2. Select the EC2 instance that needs access to S3.
3. Click on **Actions** → **Security** → **Modify IAM Role**.

2.2 Attach the Role

1. Select the **EC2S3AccessRole** from the list.
2. Click **Update IAM role**.

Step 3: Verify EC2 Role Permissions

3.1 Connect to EC2 Instance

- SSH into your EC2 instance:

```
ssh -i <your-key.pem> ec2-user@<ec2-public-ip>
```

3.2 List S3 Buckets

Run the following command:

```
aws s3 ls
```