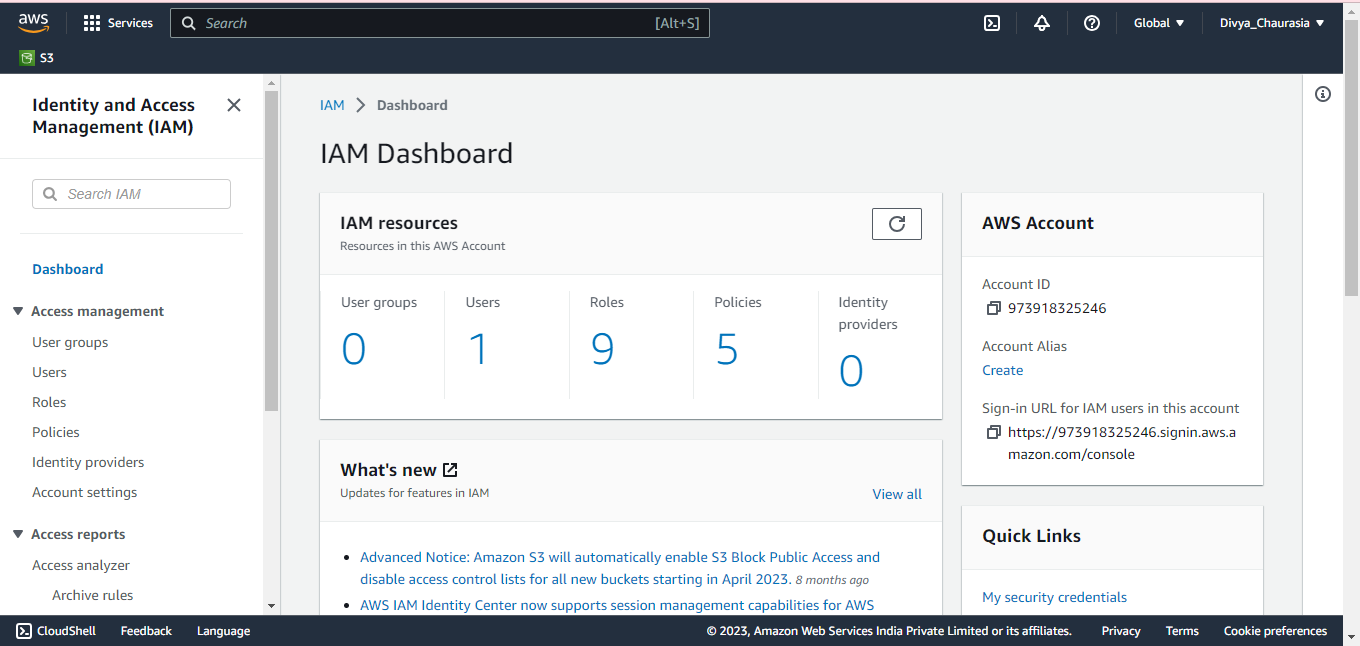
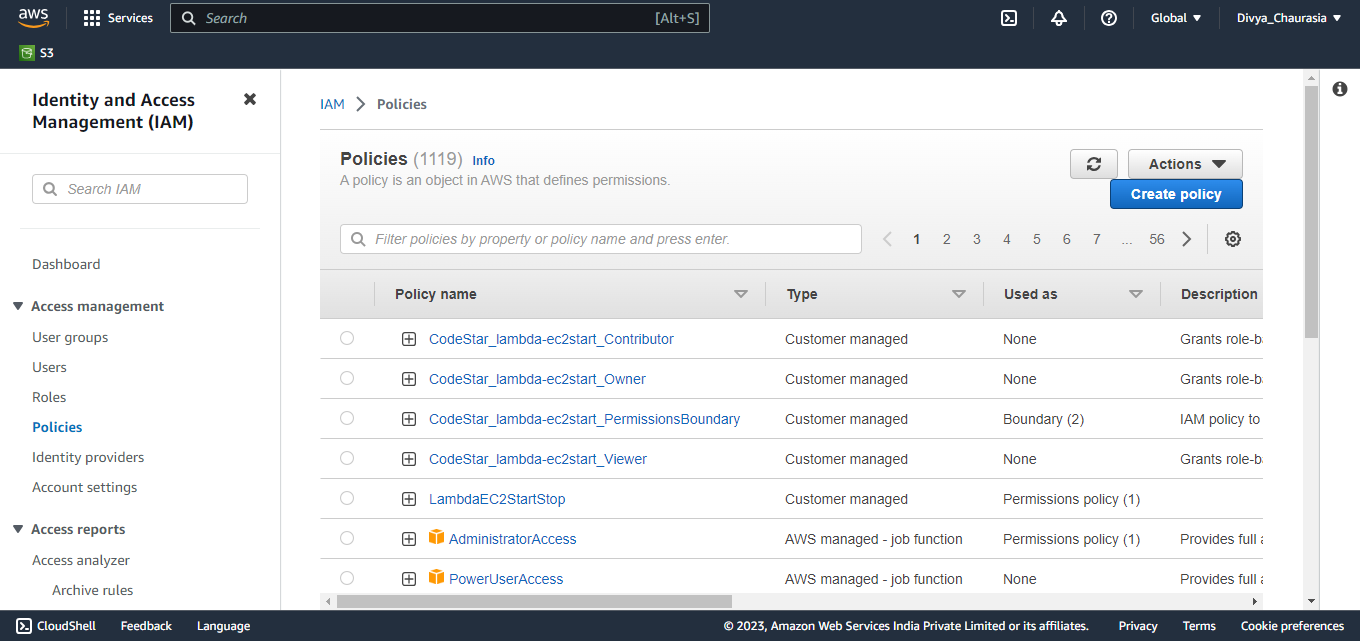
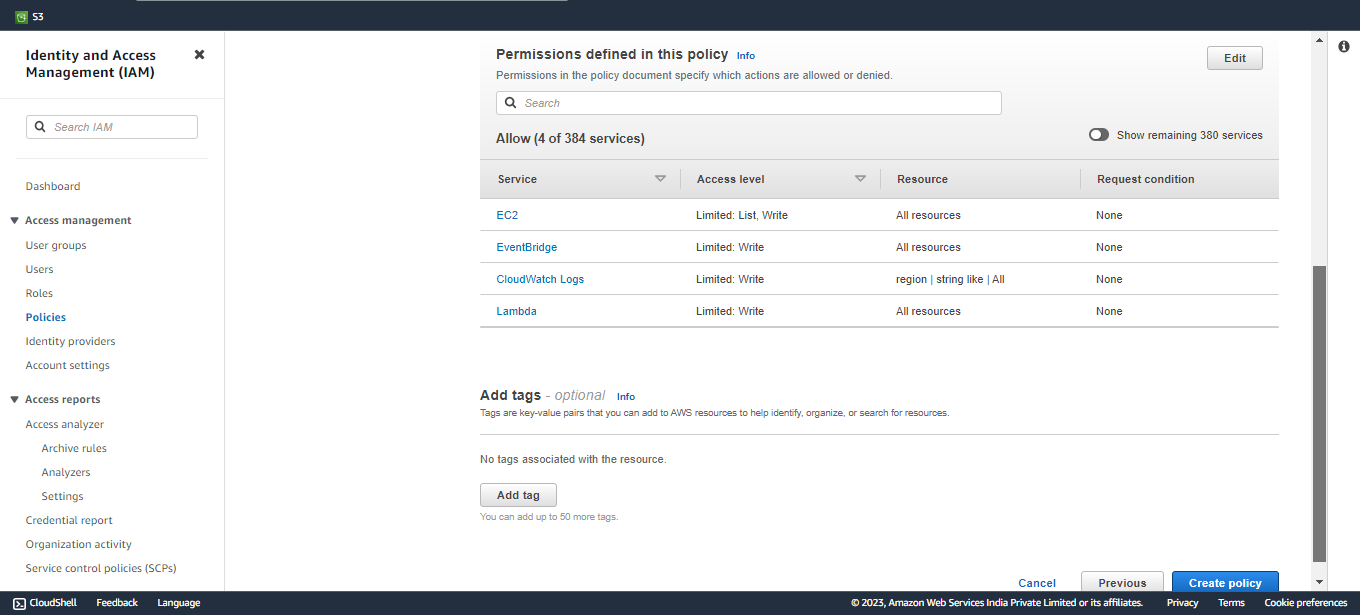
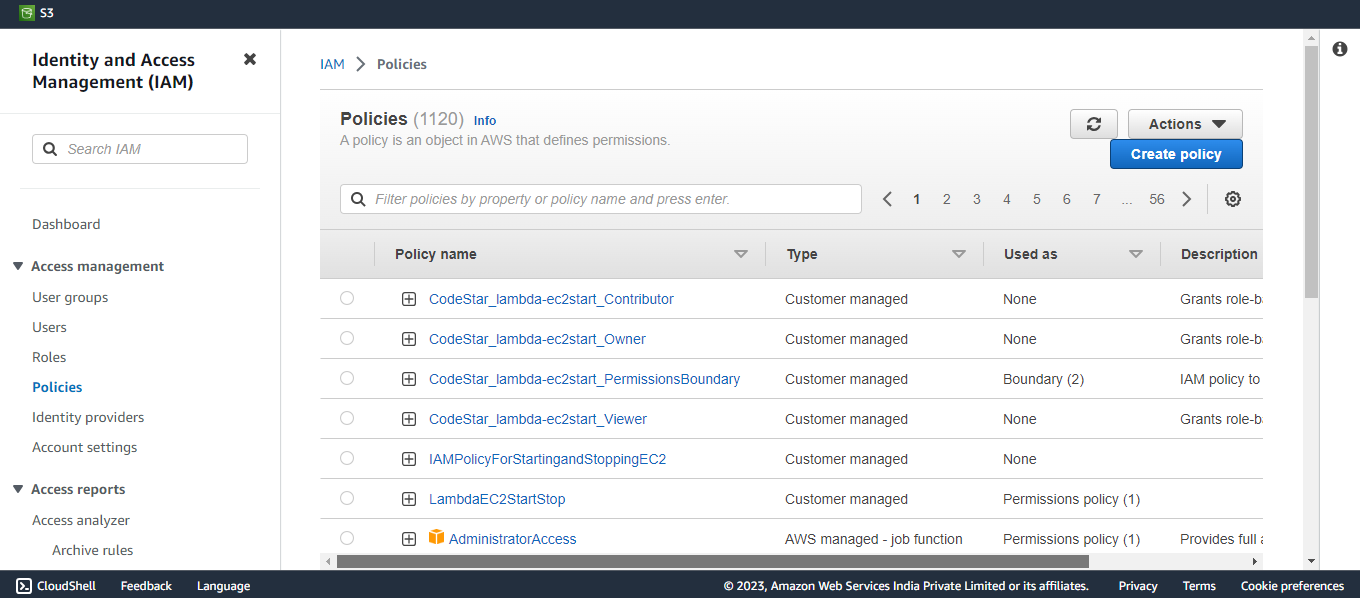
**Creating IAM Role:**

1. Open the IAM console from [here](https://console.aws.amazon.com/iam/).
2. ****Upon accessing the **IAM Dashboard**, you will be presented with a view like the one shown below:
3. To create a role, we have the option to either **create a custom IAM policy** first or select from the **available AWS managed policies**.
4. In the left navigation pane, choose **Policies.**
5. Choose **Create policy**.
6. Click on JSON, copy the IAM Policy from the GitHub (Copy from here), and paste it in the open policy editor for further use.
7. Ensure there are **no syntax errors** (unlikely but just in case) and remove any if found, then proceed to the Next tab.
8. A window will open named as **Review and create**.
9. For **Name**, enter a name for your IAM policy, for example [**IAM\_EC2StartStop**](https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A973918325246%3Apolicy%2FLambdaEC2StartStop)**\_Policy** or [**IAMPolicyForStartingandStoppingEC2**](https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A973918325246%3Apolicy%2FIAMPolicyForStartingandStoppingEC2). You’re going use this name when you’ll create an IAM role to associate with your Lambda Function. You can also add an optional **Description** value here.
10. Please verify if all the mentioned services, including EC2, CloudWatch Logs, EventBridge and Lambda, are listed under the **'permissions defined in this policy'** tab.
11. Adding tags is optional, but you have the flexibility to use them as per your requirements.
12. Choose **Create policy**.
13. After completing these steps, you’ll encounter a window identical to the one shown previously in Step 5. The created policy will also be displayed in this window this time.



1. In the navigation pane, choose **Roles**.
2. Choose **Create role**.
3. Under **Trusted entity type**, choose **Custom trust policy**.
4. Under **Custom trust policy**, select the statement and delete it.
5. Now, copy this and paste in as a statement.

{

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

"Statement": [

{

"Effect": "Allow",

"Principal": {

"Service": [

"lambda.amazonaws.com",

"scheduler.amazonaws.com"

]

},

"Action": "sts:AssumeRole"

}

]

}

}

1. **"lambda.amazonaws.com", "scheduler.amazonaws.com":** This identifies the services that are allowed to assume the role. The services listed are AWS Lambda (lambda.amazonaws.com) and AWS EventBridge (scheduler) (scheduler.amazonaws.com).
2. **"sts:AssumeRole":** This action allows the specified principal (Lambda and EventBridge services) to assume the role.
3. Choose **Next** button.
4. On the **Permissions policies** page, search the name of your policy in the Filter field and select it. Choose **Next**.
5. In **Name, review, and create** section under **Role details**, fill following:
   1. **Role name:** Enter a name for your IAM role, for example “**EC2\_StartandStop\_Rule**” or “**IAMRole\_STARTINGandSTOPPING\_EC2**”.
   2. **Description**: You can write a short and clear description for this role to help you quickly understand its purpose when you look at it again.
6. Choose **Create role.**

**And there you have it! Your IAM role is now fully prepared for use. Happy coding and automating!**