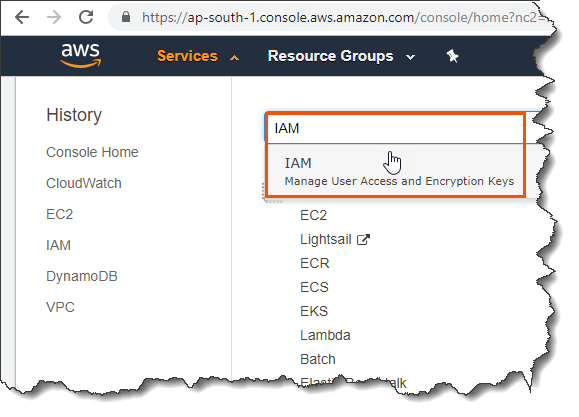
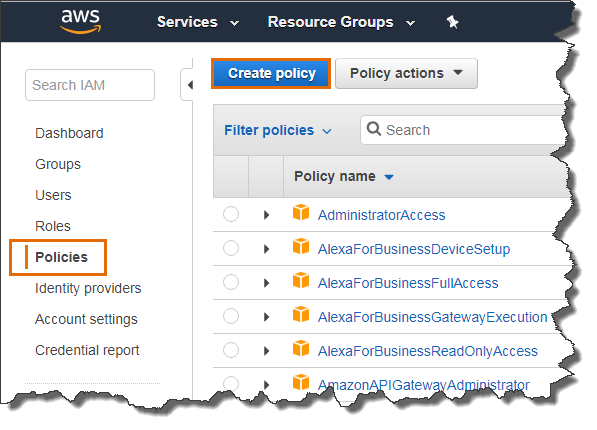
Create An IAM [Policies](https://console.aws.amazon.com/iam/home?region=ap-south-1#/policies)

Step 1: Login to AWS console and navigate to ‘IAM’.

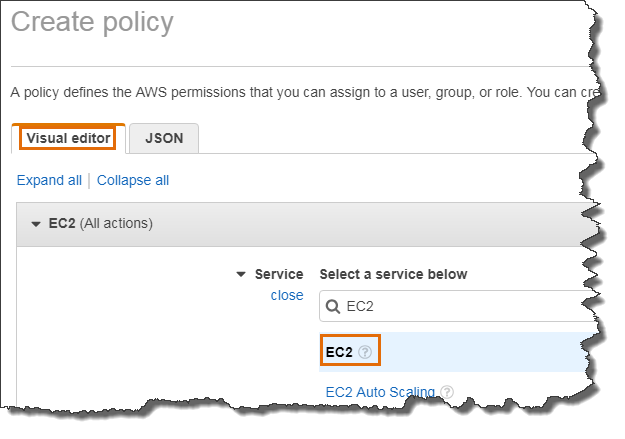


Step 2: Navigate to ‘Policies’ and click ‘Create policy’.

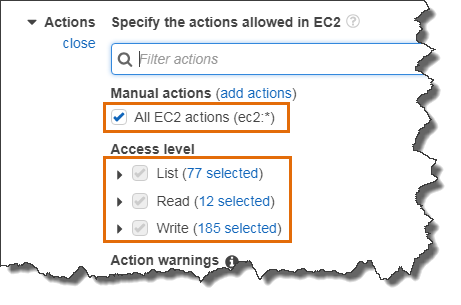


Step 3: Select service, actions and resources, Click ‘Review policy’

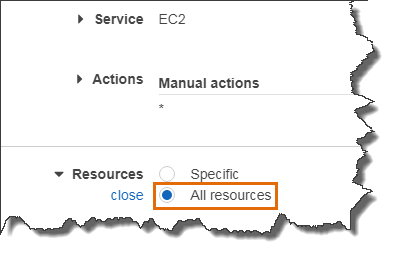
Service:



Actions:

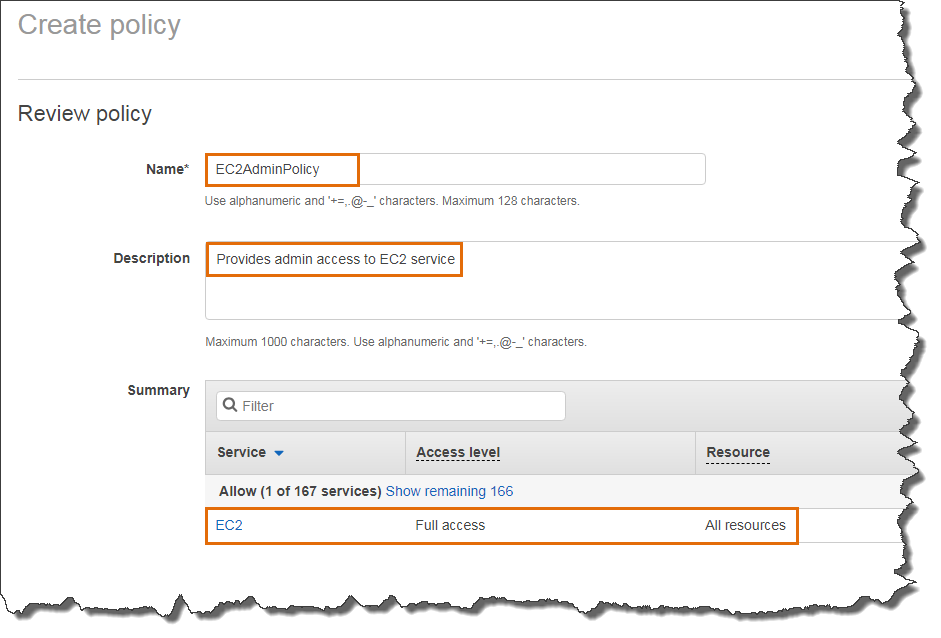


Resources:

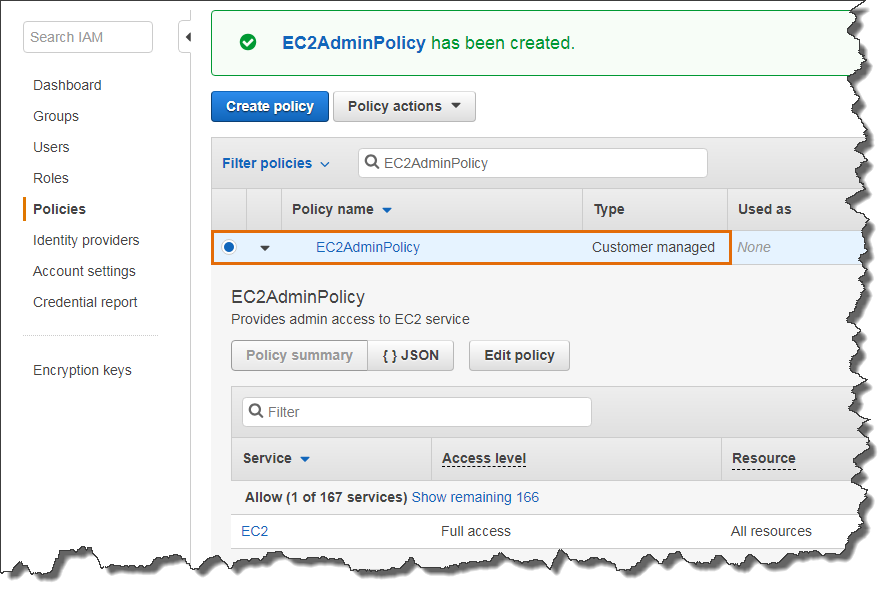


Note: We are providing full access to EC2 service using this policy.

Step 4: Provide name and description to the policy and click ‘Create policy’.

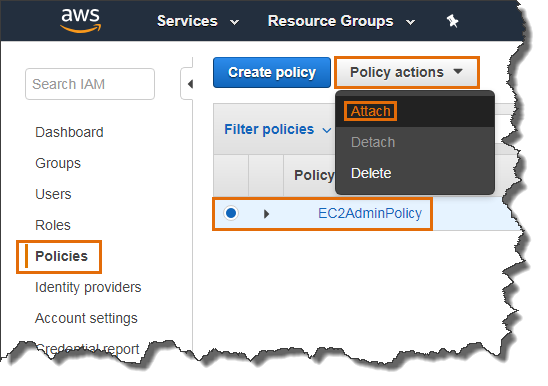


Our IAM policy successfully created.

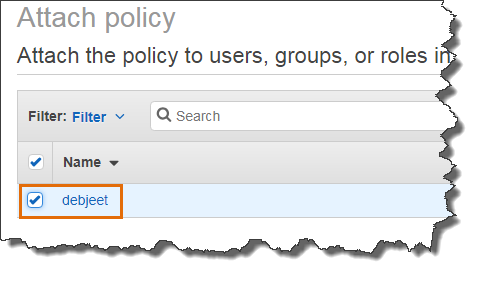


Next, we are going to attach this policy to the IAM user debjeet.

Step 5: Select the policy and from ‘Policy actions’ click ‘Attach’.



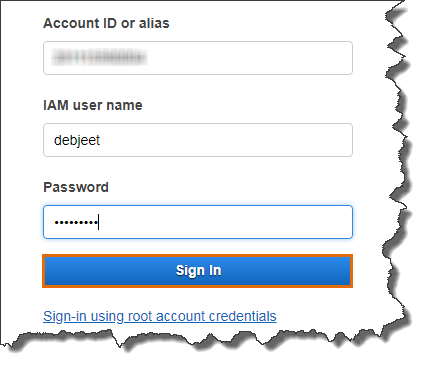
Step 6: Select the IAM user created in last blog post and click ‘Attach policy’.



You can check the access to EC2 service of the IAM user by login into the AWS console.

Login to AWS console using IAM user credential

https://<account\_id>.signin.aws.amazon.com/console



In this demo, we have directly attached the policy to the user which is not the recommended way of managing IAM user access. Instead we should have created a group with this policy and then include the user to that group.

To get more details on IAM, please refer below AWS documentation

<https://docs.aws.amazon.com/iam/index.html>