

TASK

Task 1. Create an IAM policy that grants an IAM user full Amazon EC2 access only when requests target the Paris region (eu-west-3) and explicitly denies EC2 access in all other regions; then provide step-by step instructions to create and attach that policy using the AWS Management Console.

Steps:

Step 1 . Sign in to the AWS Management Console with an account that can create IAM policies.

Step 2. Go into IAM Service , In the left menu click Policies.

The screenshot shows the AWS IAM Dashboard. The left sidebar includes sections for Identity and Access Management (IAM), Access Management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests), Access reports (Access Analyzer), and CloudShell, Feedback, and Console Mobile App links. The main content area displays Security recommendations (Root user has MFA, Root user has no active access keys), IAM resources (0 User groups, 0 Users, 26 Roles, 4 Policies, 0 Identity providers), and a What's new section. On the right, there are sections for AWS Account (Account ID: 076597402568, Account Alias: Create, Sign-in URL: https://076597402568.signin.aws.amazon.com/console), Quick Links (My security credentials), and links for Privacy, Terms, and Cookie preferences.

The screenshot shows the 'Create policy' wizard, Step 1: Specify permissions. It includes a sidebar with Step 1 (Specify permissions, selected), Step 2 (Review and create), and a Policy editor with Visual, JSON, and Actions tabs. The main content area shows a 'Select a service' dropdown labeled 'Choose a service'. At the bottom are 'Add more permissions' and 'Cancel' and 'Next' buttons.

Step 3. Click Create policy, Choose Visual editor tab, Select service EC2 and check the box contain all Ec2 action, Add First Statement.

The screenshot shows the AWS IAM 'Create policy' interface. On the left, there are two steps: 'Specify permissions' (selected) and 'Review and create'. The main area is titled 'Specify permissions' with a 'Visual' tab selected. Under the 'EC2' service, the 'All actions' checkbox is checked under 'Actions allowed'. The 'Effect' is set to 'Allow'. A 'Filter Actions' search bar is present. At the bottom right, there are 'Expand all' and 'Collapse all' buttons.

Step 4. Scroll down to Request Condition, Add Condition.

Add: Condition key : aws:RequestedRegion

Operator :StringEquals

Value: eu-west-3

The screenshot shows the 'Add request condition' dialog box overlaid on the IAM 'Create policy' page. The dialog box has the following fields: 'Condition key' set to 'aws:RequestedRegion', 'Qualifier' set to 'Default', 'Operator' set to 'StringEquals', and 'Value' set to 'eu-west-3'. At the bottom right of the dialog box is an 'Add condition' button, which is highlighted with a yellow background.

Click Add.

Means EC2 full access is allowed only if the region = Paris(eu-west-3)

**Step 5 . Add Second Statement, Select EC2 service , Change the effect Allow > Deny
Manual action – Select all in checkbox , Select Resource from specific to all.**

The screenshot shows the AWS IAM 'Create policy' interface. A green banner at the top indicates 'Policy paris-policy created.' On the left, a navigation tree shows 'Policies' and 'Create policy'. The main area is titled 'EC2' with a 'Deny' button. It says 'Specify what actions can't be performed on specific resources in EC2.' Below this is a section for 'Actions denied' with a 'Filter Actions' search bar. Under 'Manual actions | Add actions', there is a checked checkbox for 'All EC2 actions (ec2:*)'. To the right, there is an 'Effect' section with 'Allow' and 'Deny' radio buttons, currently set to 'Deny'. A link 'Expand all | Collapse all' is also present. A blue 'View policy' button is at the bottom right.

Step 6. Scroll to Request Conditions.

Add. Condition key: **aws:RequestedRegion**

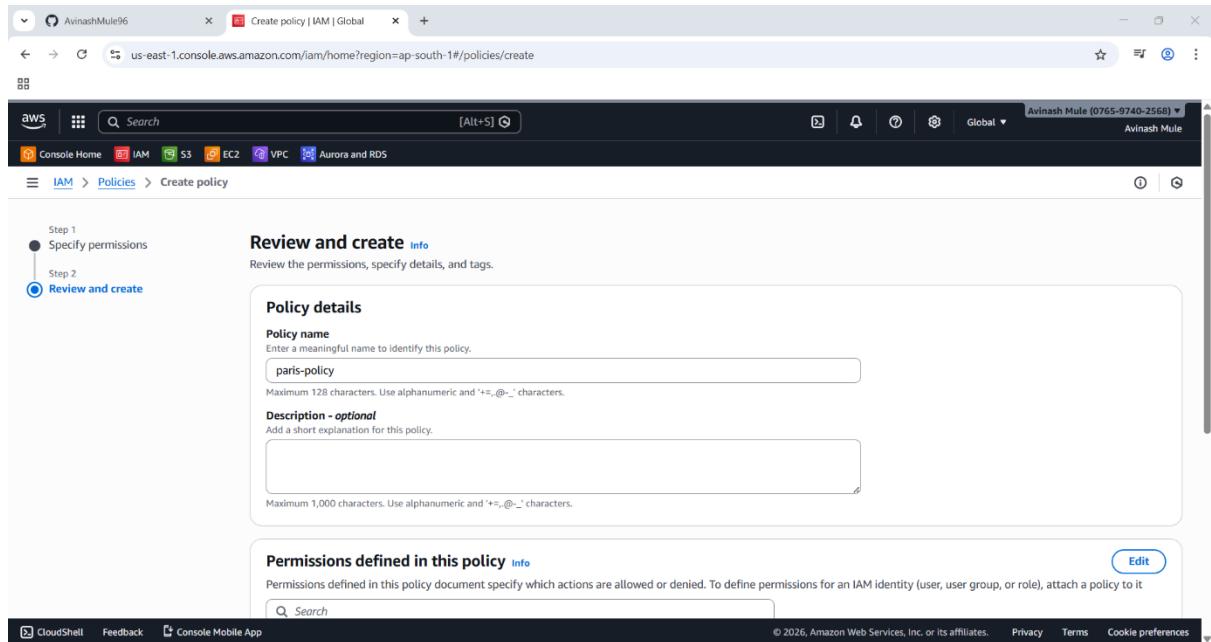
Operator : **StringNotEquals**

Value: **eu-west-3**

The screenshot shows the 'Add request condition' dialog box overlaid on the IAM policy creation screen. The dialog has fields for 'Condition key' (set to 'aws:RequestedRegion'), 'Qualifier' (set to 'Default'), 'Operator' (set to 'StringNotEquals'), and 'Value' (set to 'eu-west-3'). There are 'Cancel' and 'Add condition' buttons at the bottom. The background shows the IAM policy creation interface with a green banner for 'Policy paris-policy created.'

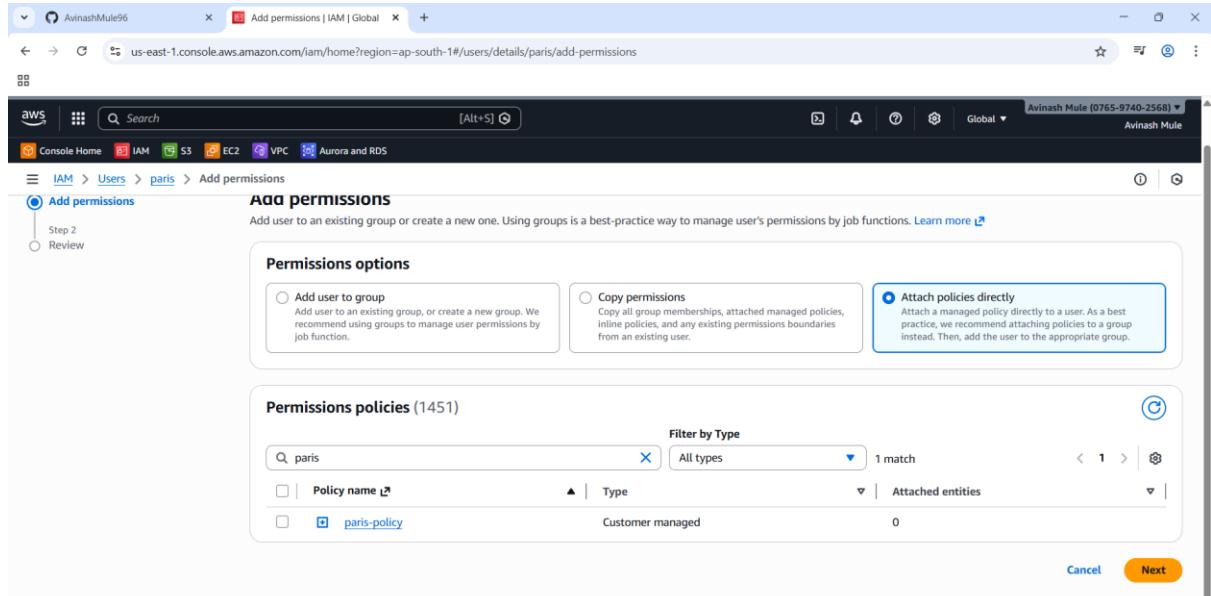
This means deny EC2 if the region is Not Paris. Click on next .

Step 7. Review and Create.



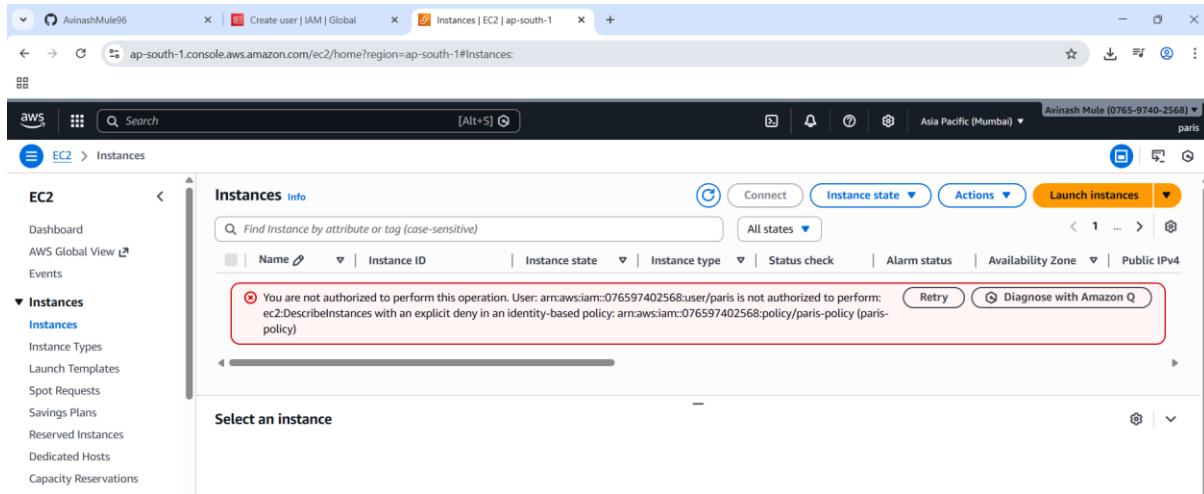
Step 8. Create policy.

Step 10 . Go to IAM service > Users > paris > Add Permissions > Attach Policies directly > Select your policy name > Tik the checkbox > Click Add Permissions.



Step 11. Policy added Successfully.

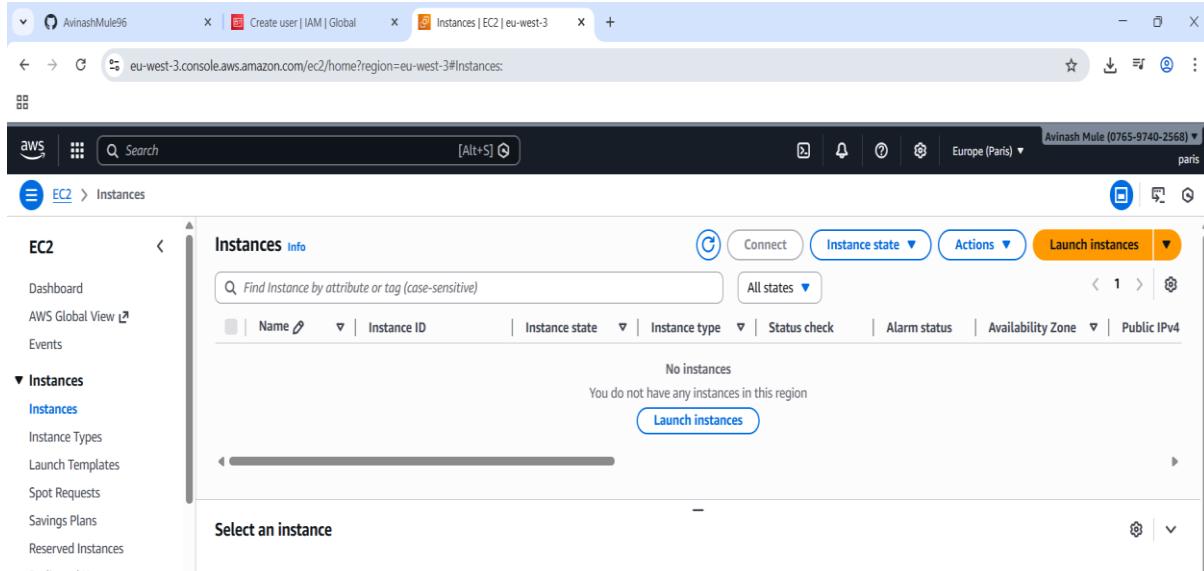
Step 12. Lets check wheather the policy is working or not . Login into IAM User > Select the region Mumbai > Open EC2 instance and try to launch instance.



The screenshot shows the AWS EC2 Instances page in the Mumbai region. The URL in the browser is ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#instances. The navigation bar includes tabs for Create user | IAM | Global, Instances | EC2 | ap-south-1, and Instances | EC2 | ap-south-1. The main content area is titled 'Instances info' with a search bar and filter options (Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4). A prominent red box highlights a message: 'You are not authorized to perform this operation. User: arn:aws:iam:076597402568:user/paris is not authorized to perform: ec2:DescribeInstances with an explicit deny in an identity-based policy: arn:aws:iam:076597402568:policy/paris-policy (paris-policy)'. Below this message is a 'Select an instance' section.

In Mumbai region> Permission Denied for creating instance.

Step 13. Select the region Paris > Open EC2 instance and try to launch instance.



The screenshot shows the AWS EC2 Instances page in the Paris region. The URL in the browser is eu-west-3.console.aws.amazon.com/ec2/home?region=eu-west-3#instances. The navigation bar includes tabs for Create user | IAM | Global, Instances | EC2 | eu-west-3, and Instances | EC2 | eu-west-3. The main content area is titled 'Instances info' with a search bar and filter options (Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4). A message 'No instances' is displayed, followed by 'You do not have any instances in this region'. Below this message is a large blue 'Launch instances' button. Below the button is a 'Select an instance' section.

Resource accessed successfully .