

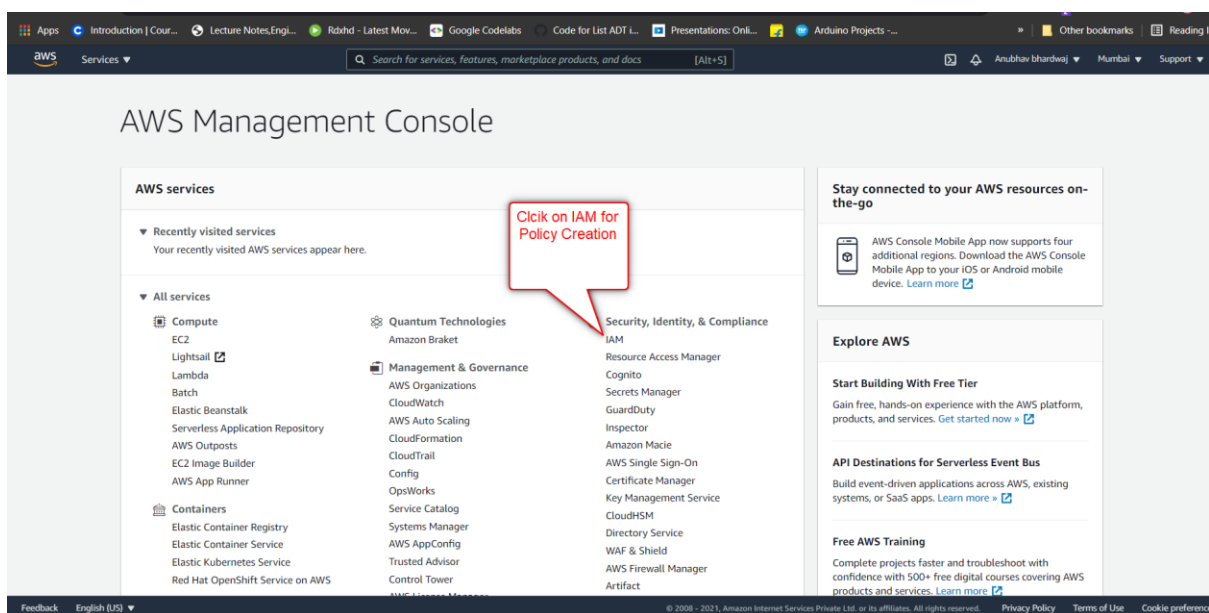
Configure IAM user who have access only specific ec2 and modify specific security group only

Overview

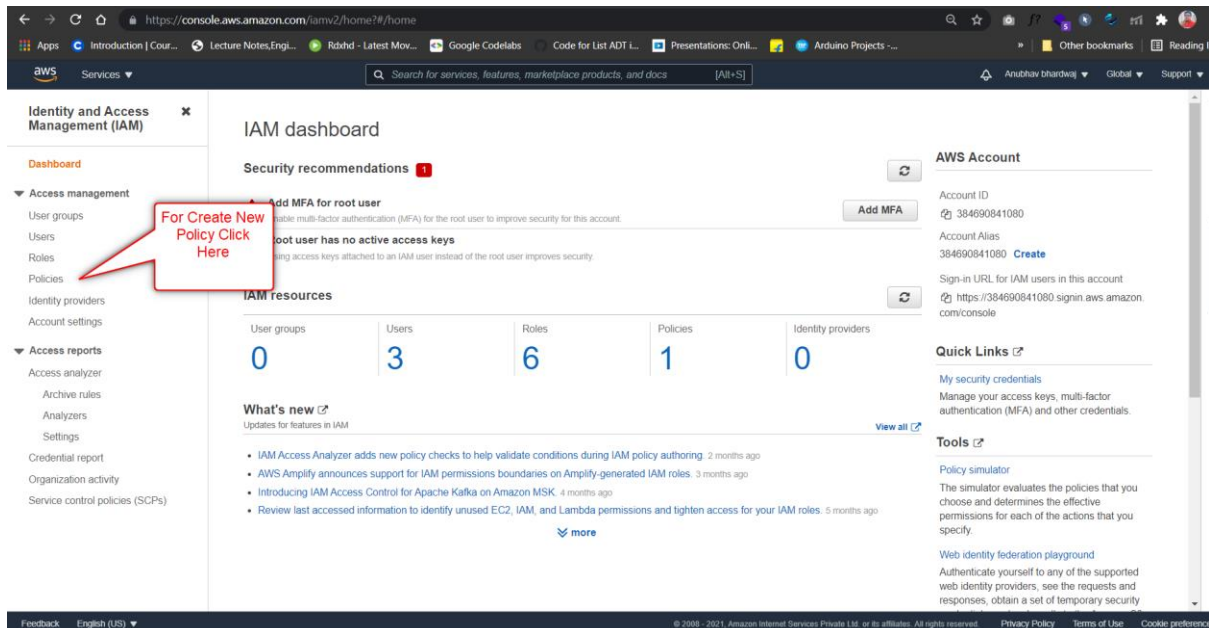
First We will go to IAM Service through AWS Management Console and there we will create a Policy of Access Specific EC-2 Instance and Modify Specific Security Group through their specific-id. After creating the Policy, We will attach that policy to the Newly Created IAM User and Login that user through the AWS Console and Perform the Particular Task.

Creating a Policy

1. First we will go to AWS Management Console and Select the IAM Service

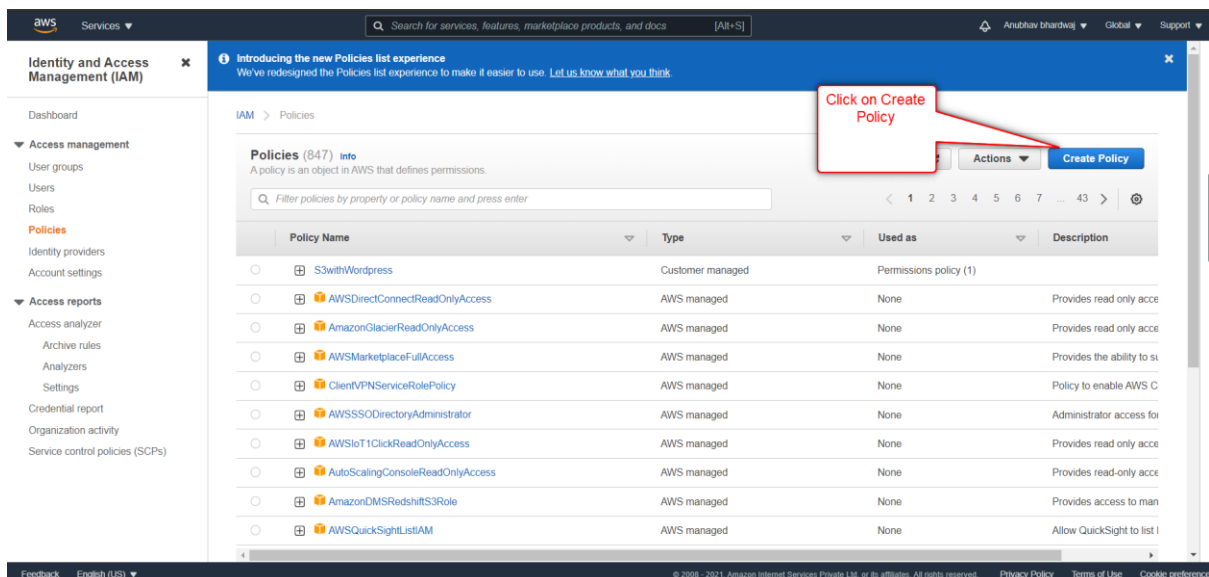


2. For Crating Policy Select the Policies Option



The screenshot shows the AWS IAM dashboard. In the left-hand navigation menu, the 'Policies' option is highlighted. A red callout bubble with the text 'For Create New Policy Click Here' points to this option. The main content area displays the 'IAM dashboard' with various security recommendations and IAM resources. The 'Policies' resource count is shown as '1'.

3. Click on Create Policy



The screenshot shows the 'Policies' page in the AWS IAM console. A red callout bubble with the text 'Click on Create Policy' points to the 'Create Policy' button in the top right corner of the page. The page displays a list of existing policies with columns for Policy Name, Type, Used as, and Description. The 'Create Policy' button is prominently displayed in blue.

4. Before going to Write Policy We need to find the id of Particular Security Group and Particular Instance for User

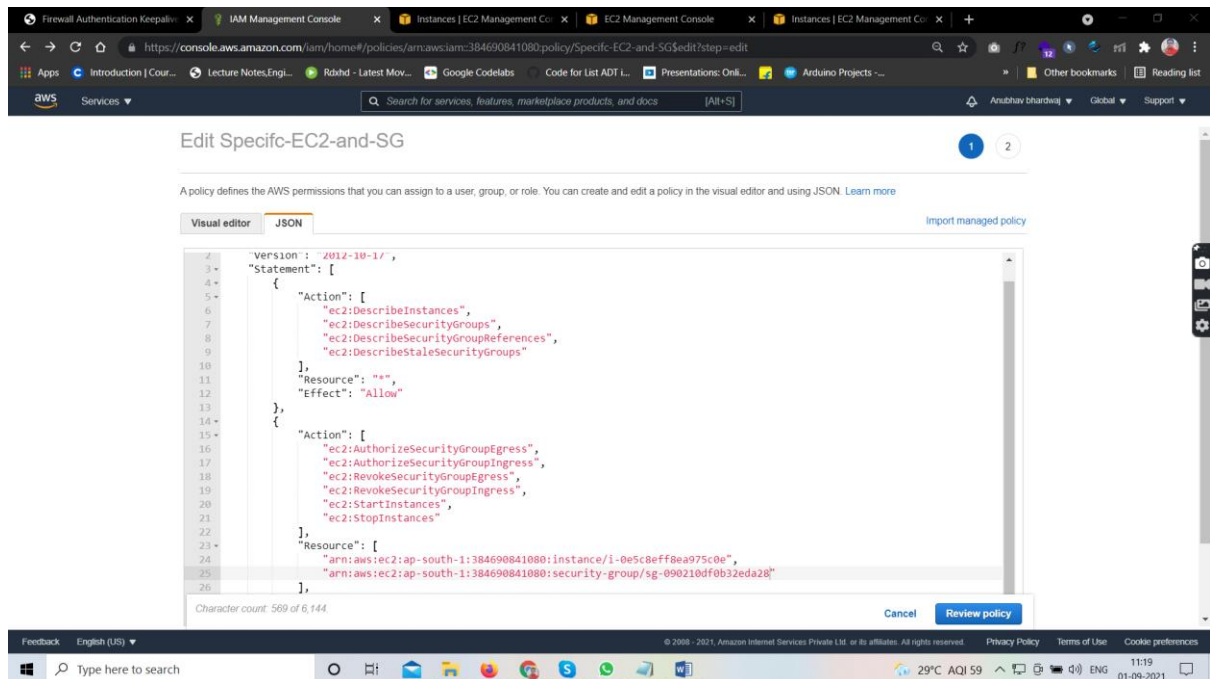
The screenshot shows the AWS Management Console 'Instances' page. The instance 'Wee3-Task(Check Private)' with ID 'i-0e5c8eff8ea975c0e' is selected. The 'Security groups' section shows 'sg-090210df0b32eda28 (launch-wizard-15)' is attached. A red box highlights this group, and a red arrow points to it with the text 'Attached Security Group in Policy'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
Wee3-Task(Check Private)	i-0e5c8eff8ea975c0e	Stopped	t2.micro	OK	No alarms	ap-south-1a	-	-
Wee3-Task(Check Private)	i-0189d631ef5b63c54	Stopped	t2.micro	OK	No alarms	ap-south-1a	-	-
terraform	i-00f7e475c233177a8	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-
Ansible Testing	i-0df175483b40d4c16	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-
Jenkins-Master	i-0e5e0f292187cd685	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-
pemkeychang...	i-007e063e99b7d38de	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-
Task-1	i-0be2c9c166d692cbb	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-

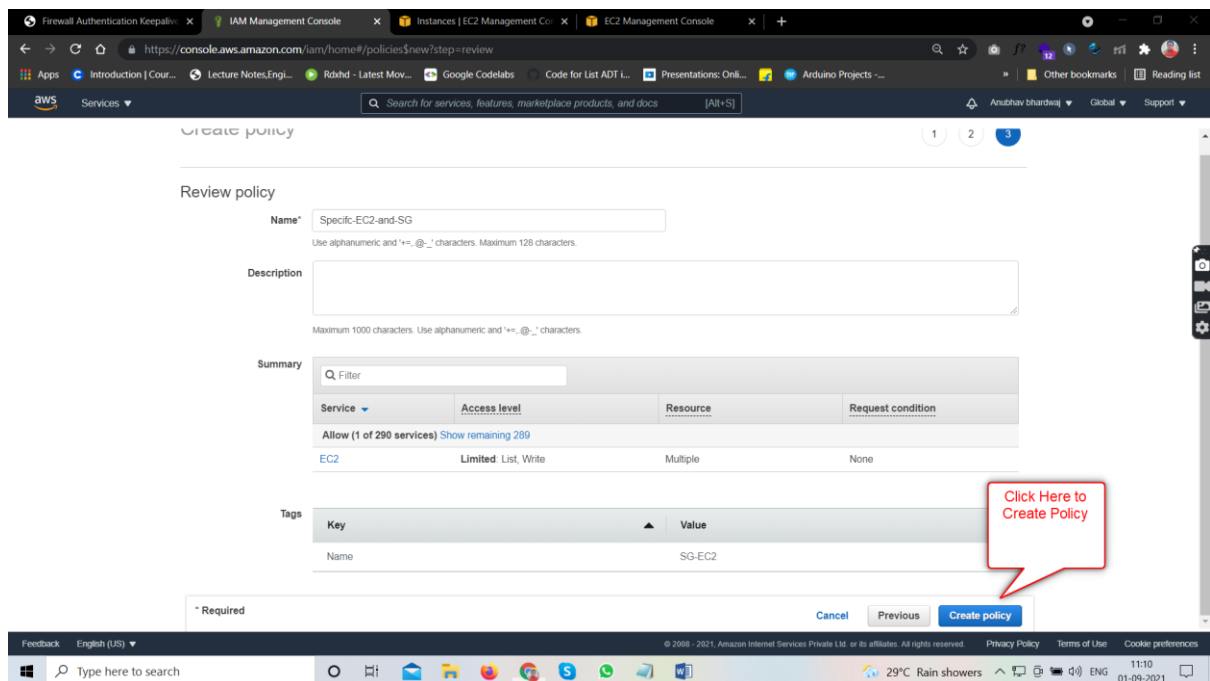
The screenshot shows the AWS Management Console 'Instances' page. The instance 'Wee3-Task(Check Private)' with ID 'i-0e5c8eff8ea975c0e' is selected. A red box highlights the 'Instance ID' field, and a red arrow points to it with the text 'Instance ID'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
Wee3-Task(Check Private)	i-0e5c8eff8ea975c0e	Stopped	t2.micro	OK	No alarms	ap-south-1a	-	-
Wee3-Task(Check Private)	i-0189d631ef5b63c54	Stopped	t2.micro	OK	No alarms	ap-south-1a	-	-
terraform	i-00f7e475c233177a8	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-
Ansible Testing	i-0df175483b40d4c16	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-
Jenkins-Master	i-0e5e0f292187cd685	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-
pemkeychang...	i-007e063e99b7d38de	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-
Task-1	i-0be2c9c166d692cbb	Stopped	t2.micro	OK	No alarms	ap-south-1b	-	-

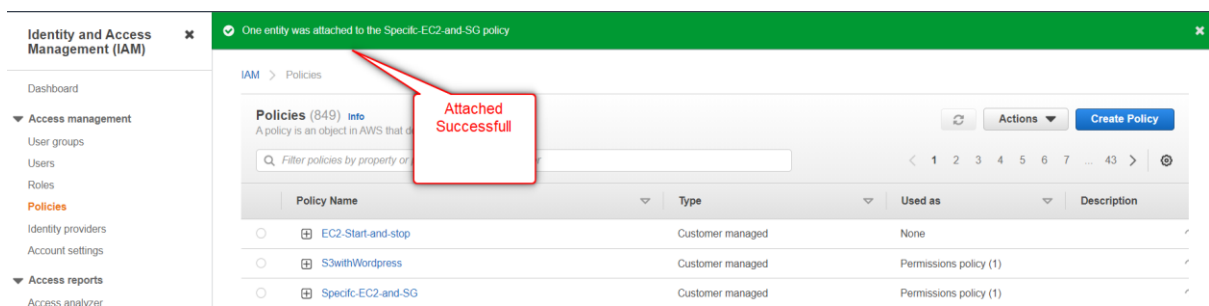
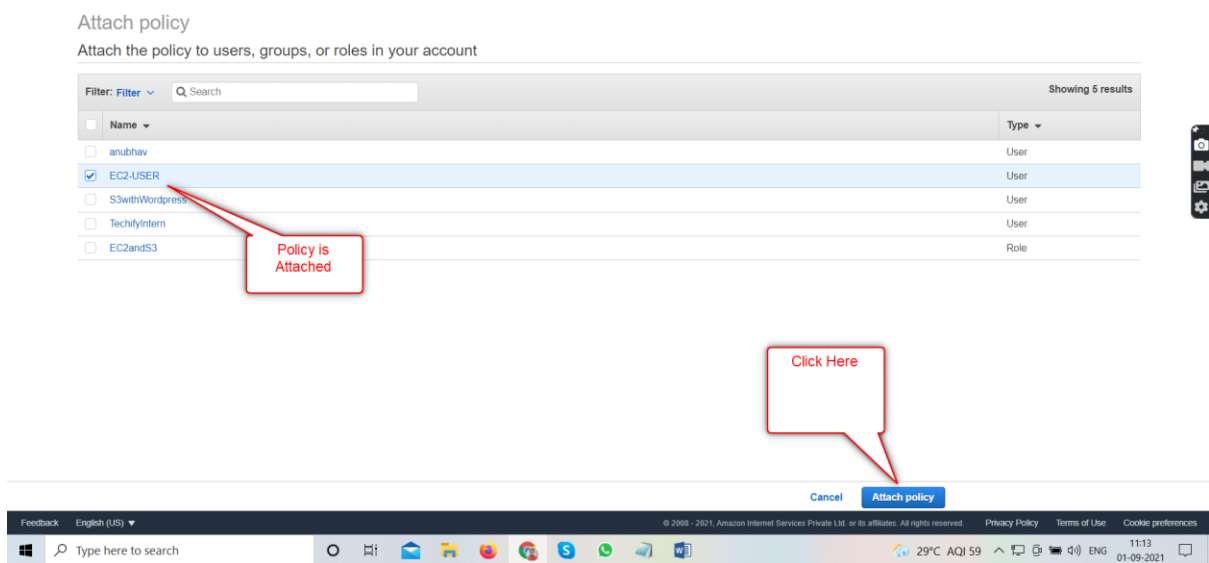
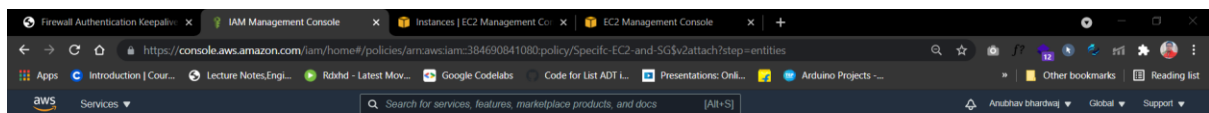
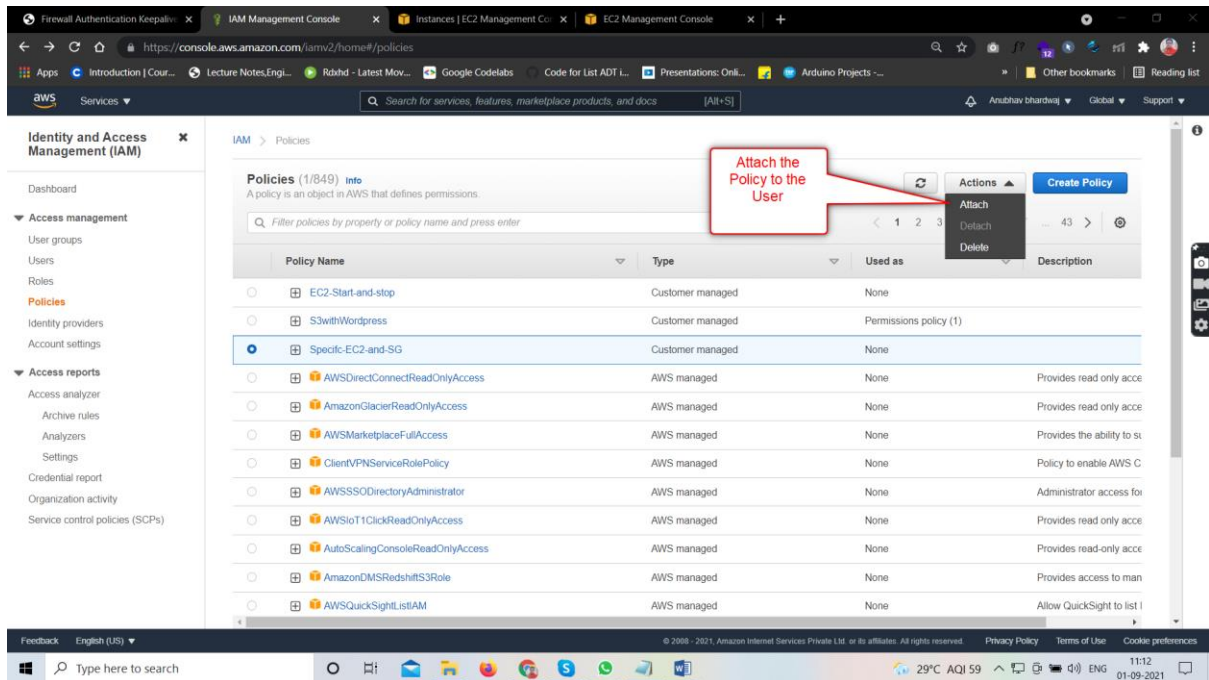
5. Create the Policy and Assign these ID of Security Group and Instance



6. Click here to Create policy



7. Attach the Created Policy to the IAM User

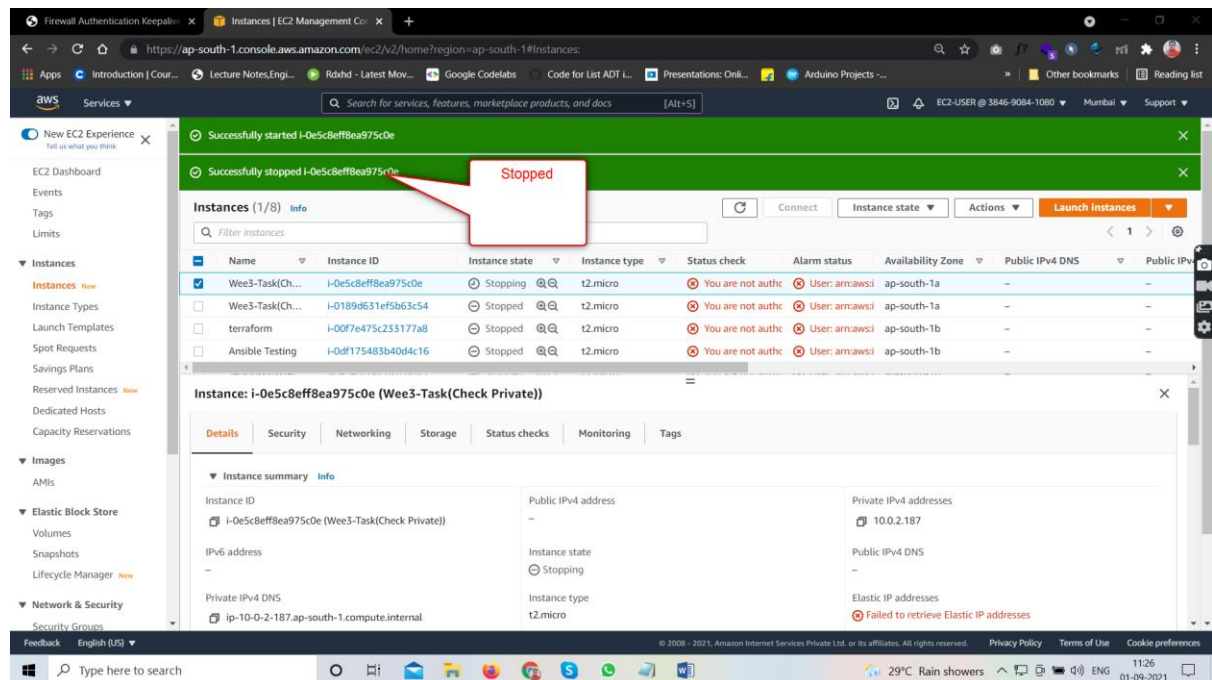


The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a search bar, and a user profile dropdown. The main content area displays the 'Instances' page with a table of EC2 instances. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Actions. Three instances are listed: 'Wee3-Task(Ch...', 'Wee3-Task(Ch...', and 'terraform'. The first instance is in a 'Stopped' state. A red box highlights the 'Login into EC2-User' button in the 'Actions' column.

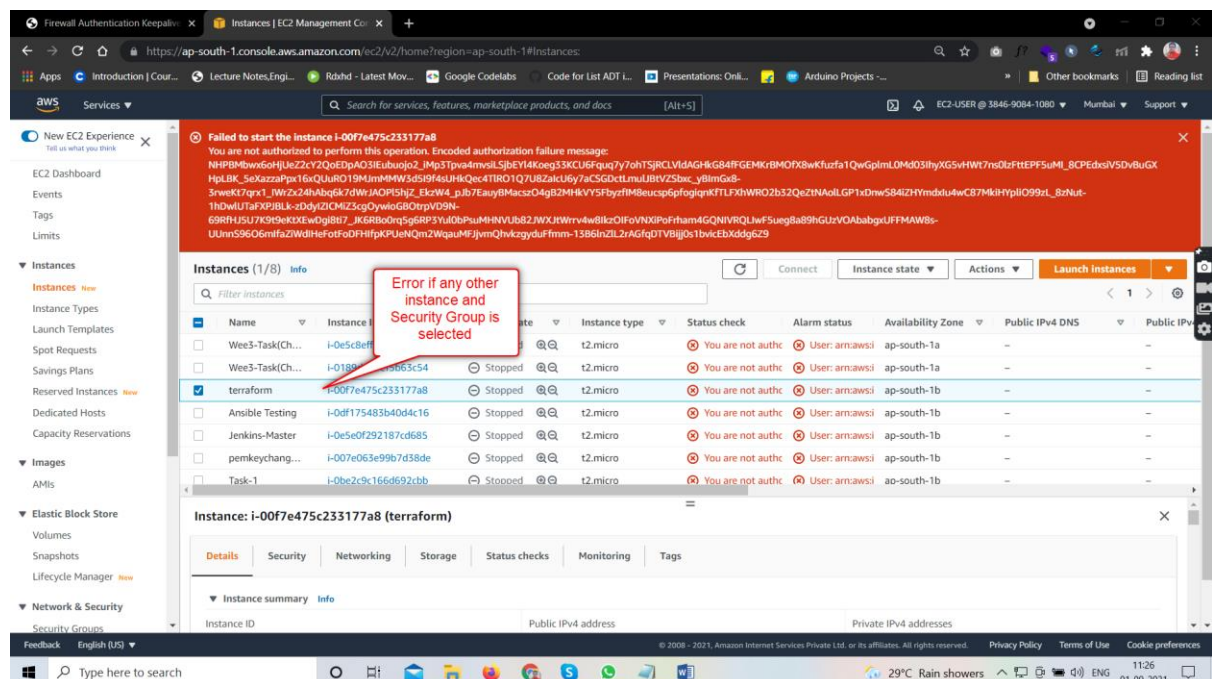
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Actions
Wee3-Task(Ch...	i-0e5c8eff8ea975c0e	Stopped	t2.micro	You are not auth...	User: am...	Public IPv4 DNS
Wee3-Task(Ch...	i-0189d631ef5b63c54	Stopped	t2.micro	You are not auth...	User: am...	Public IPv4 DNS
terraform	i-00f7e475c233177a8	Stopped	t2.micro	You are not auth...	User: am...	Public IPv4 DNS

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, a search bar, and user information 'EC2-USER @ 5846-9084-1080' with location 'Mumbai' and 'Support' link. On the left, there's a sidebar with 'New EC2 Experience' (with a feedback icon), 'EC2 Dashboard', 'Events', 'Tags', and 'Limits'. The main content area has a green header bar that says 'Successfully started i-0e5cbeff8ea975c0e'. Below this, the 'Instances (1/8)' section is active. It includes a search bar, a 'Filter instances' dropdown, and a table of instances. The table has columns: Name, Instance ID, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, and Public IPv4. The first instance is selected (checkbox checked) and highlighted in blue. Its details are: Name 'Wee3-Task(Cl...', Instance ID 'i-0e5cbeff8ea975c0e', Instance type 'micro', Status check 'You are not auth...', Alarm status 'User: awsamz...', Availability Zone 'ap-south-1a', Public IPv4 DNS '-', and Public IPv4 '-'. A red callout box with a white border points to the instance name 'i-0e5cbeff8ea975c0e' with the text 'Selected Instance is Started'. Above the table, there are buttons for 'Connect', 'Instance state' dropdown, 'Actions' dropdown, and a 'Launch instances' button. There are also pagination controls showing '1' of 8 pages.

11. Try to Stop the Instance



12. Try to Stop the Instance



We won't be able to start other instance because we haven't provided the instance id in policy

