

Module 3: IAM Users Assignment

1. Policy number 1 created. Find the below.

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Policies, and Access reports. The main content area displays the details for 'Policy_number_1'. The 'Policy details' section shows the policy is 'Customer managed', created on 'August 22, 2023, 17:22 (UTC+05:30)', and has an ARN of 'arn:aws:iam::556609594559:policy/Policy_number_1'. The 'Permissions' tab is selected, showing a table of permissions defined in the policy. The table lists three services: RDS, S3, and EC2, all with 'Full access' or 'Limited: Write' permissions on 'All resources' and 'None' request conditions. Blue arrows point to the 'Request condition' column for each service.

Service	Access level	Resource	Request condition
RDS	Full access	All resources	None
S3	Full access	All resources	None
EC2	Limited: Write	All resources	None

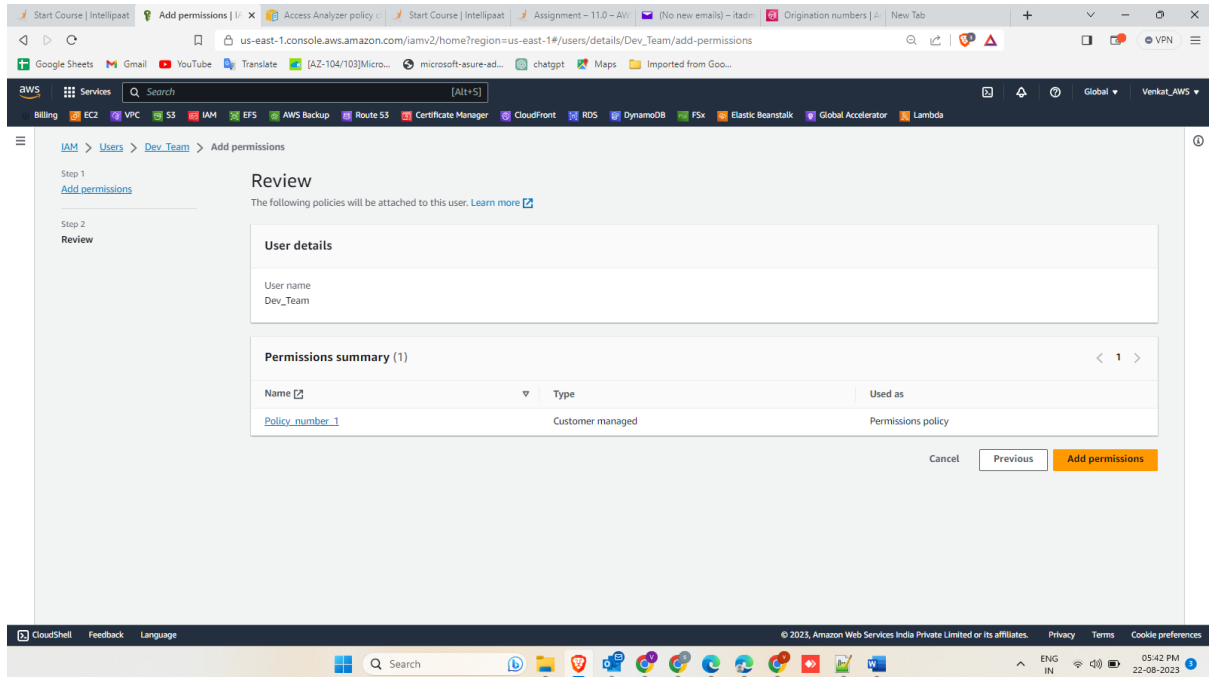
2. Policy number 2 created. Find the below.

The screenshot shows the AWS IAM console interface for 'Policy_number_2'. The 'Policy details' section shows the policy is 'Customer managed', created on 'August 22, 2023, 17:37 (UTC+05:30)', and has an ARN of 'arn:aws:iam::556609594559:policy/Policy_number_2'. The 'Permissions' tab is selected, showing a table of permissions defined in the policy. The table lists four services: S3, CloudWatch, EC2, and Billing, with 'Limited: List' or 'Full access' permissions on 'All resources' and 'None' request conditions. Blue arrows point to the 'Request condition' column for each service.

Service	Access level	Resource	Request condition
S3	Limited: List	All resources	None
CloudWatch	Full access	All resources	None
EC2	Limited: List	All resources	None
Billing	Full access	All resources	None

Module 3: IAM Users Assignment

3. Attached policy number 1 to the Dev Team.



4. Attached policy number 2 to the Ops Team.

