

**Screenshot 1 – IAM User “Raju” Created**

* Shows the newly created IAM user named **Raju** in the **Users list**.
* Confirms successful creation of the user with console access enabled.
* Verifies that Raju currently has **no permissions or groups assigned**.

**Screenshot 2 – MFA Assigned to Raju**

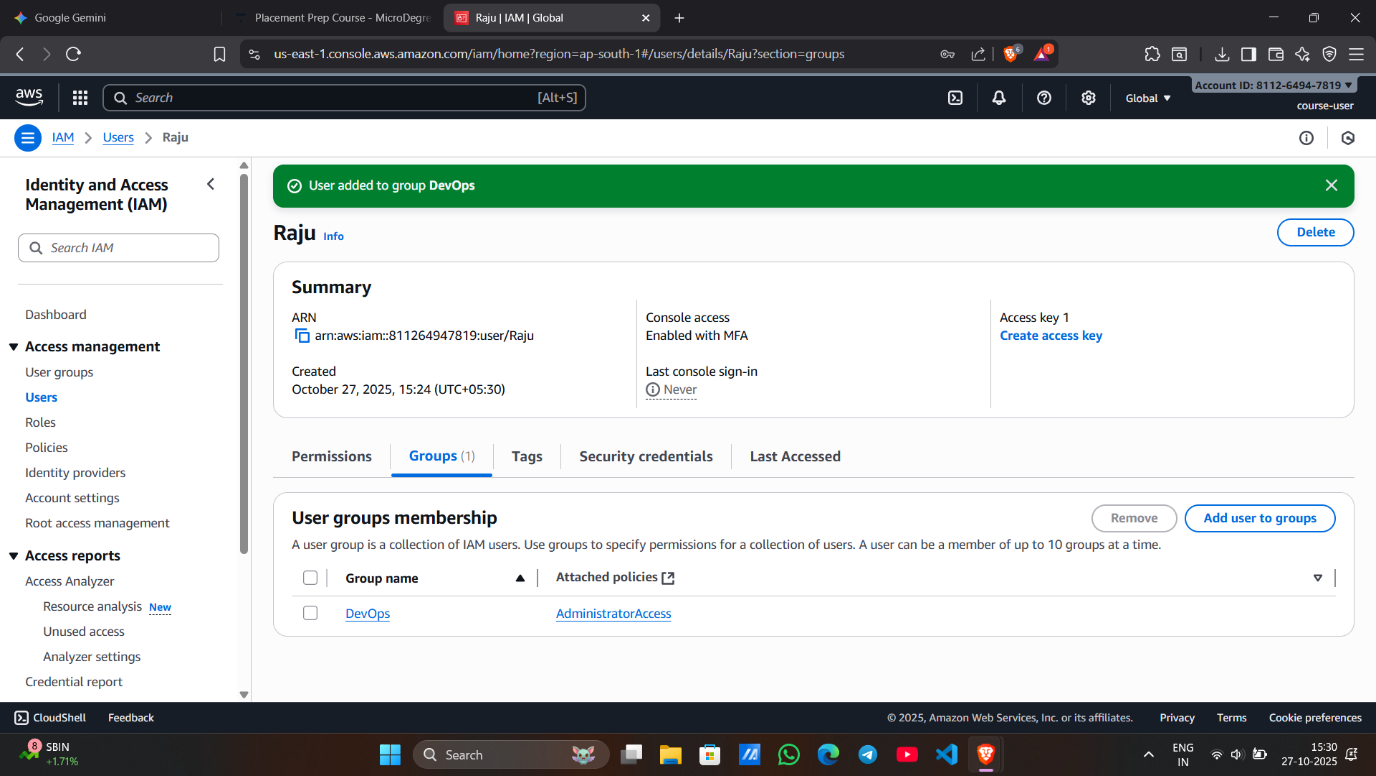
* Displays the **MFA device successfully assigned** to the Raju user.
* Indicates that Multi-Factor Authentication is now **enabled** for account security.
* Confirms that the **Virtual MFA device** setup was completed using an authenticator app.

A computer screen shot of a computer

AI-generated content may be incorrect.

**Screenshot 3 – DevOps Group Created**

* Shows the creation of a **new IAM group named DevOps**.
* The **AdministratorAccess policy** is attached to this group.
* Confirms that all users in this group will have **full administrative privileges**.



**Screenshot 4 – Raju Added to DevOps Group**

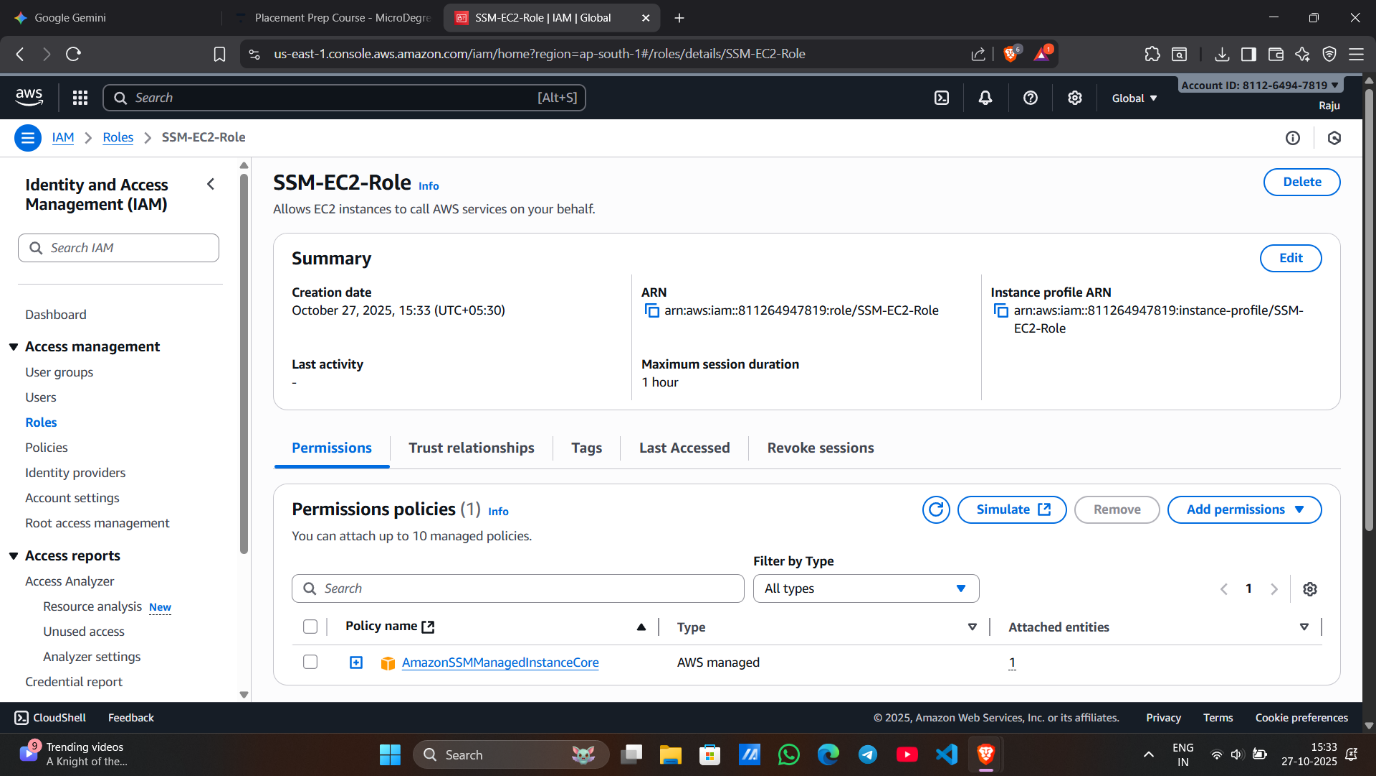
* Displays that user **Raju has been added to the DevOps group**.
* Confirms Raju now inherits **AdministratorAccess permissions** from the group.
* Verifies successful group membership under the user’s **Groups tab**.

A screenshot of a computer

AI-generated content may be incorrect.

**Screenshot 5 – Login as Raju (with MFA)**

* Shows successful login to the AWS Console as the **IAM user Raju**.
* Indicates that login was completed using the **password and MFA code**.
* The top-right corner of the console confirms the **active IAM user session (Raju)**.



**Screenshot 6 – IAM Role for SSM Created**

* Displays the creation of the **IAM Role named SSM-EC2-Role**.
* Shows the attached policy **AmazonSSMManagedInstanceCore** for Systems Manager access.
* Confirms that this role can be used by **EC2 instances in private subnets** for SSM communication.