**Implementing access control in a cloud service**

**Part 1: Setup**

**This stage involves enhancing security by implementing the multi-factor authentication (MFA) for both root and admin accounts, creating an admin group with specific administrative policies, and setting up individual admin accounts.**

Step 1: Implementing MFA for Root account

A close-up of a white background

Description automatically generated

Step 2 : Create Admin group with policy AdministratorAccess (only)

A screenshot of a computer

Description automatically generated

Step 3 :Create admin account and add to Admin group and policies

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Step 4 : Implement MFA for Admin Account

A screenshot of a computer

Description automatically generated

**Part 2: Monitoring**

**This involves configuring AWS CloudTrail to create a trail named after the user, enabling CloudWatch Logs without encryption, and monitoring event histories to track activities.**

Step 1: Go to AWS CloudTrail and create a trail and name it as SaiCharithaGudala-CloudTrail

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

Step 2 : Disable encryption and enable CloudWatch Logs

A screenshot of a computer

Description automatically generated

Step 3 : Check the events in Event History

A screenshot of a computer

Description automatically generated

**Part 3: IAM and Entitlements**

**This part details the creation of user groups and roles, specifically an EC2 Admin group with full access to EC2 instances. It also includes the creation of a specific policy named EC2ApplicationAdmin, which allows launching, starting, and stopping instances but denies termination. The policy's effectiveness is tested using the simulator provided in AWS.**

Step 1 : Create a user group called EC2 Admins and give permission to have full access to the EC2 instance

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Step 2 : Create a policy named **EC2ApplicationAdmin** which allows Run Instances , Start, and Stop instances and Deny Terminating instances . In the below screenshots we can see policy creation and JSON view of the policy.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

Step 3: Create a new group called EC2ApplicationAdmin and attach the EC2ApplicationAdmin policy created in the above step. In the simulator tab of the policy, we test the policy as shown in the below screenshots

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated