# Project 1: Cloud Foundation & Access Control Setup for allwaystech.com

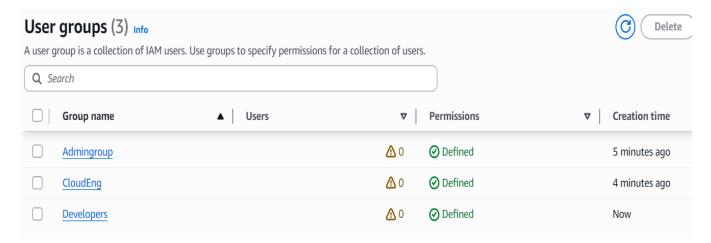
Goal: Set up a secure AWS cloud environment to onboard 6 employees and begin operations

### 1. Identity & Access Management (IAM)

### **Create IAM Groups:**

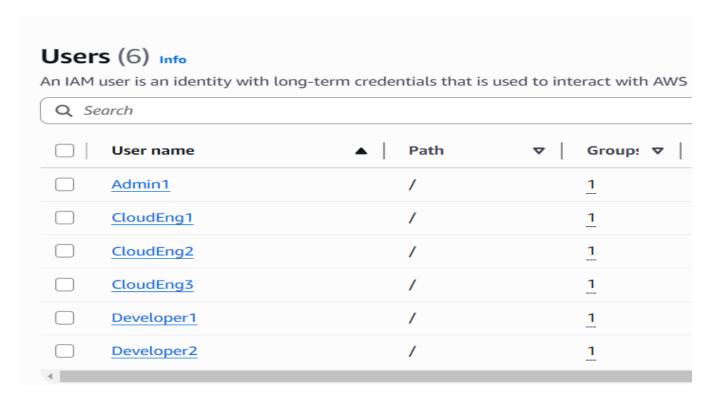
#### **Created 3 groups with least privileges:**

- 1. Admin- Attach AdministratorAccess and IAMfullaccess policy
- 2. CloudEng- Attach policies: AmazonEC2FullAccess, AmazonS3FullAccess, AWSLambda\_FullAccess, AmazonVPCFullAccess
- 3. Developers- policies: AWSLambda\_FullAccess, AmazonAPIGatewayAdministrator, AmazonECS\_FullAccess



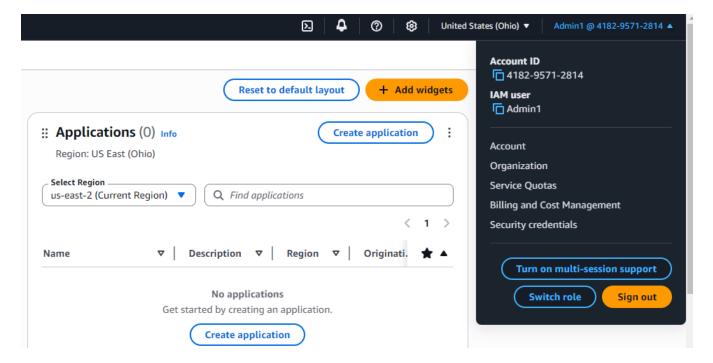
## 2. Create IAM Users:

- Create 6 users, and Assign users to respective groups.
- Sent the login instructions via Email.
- Created a custom policy for a user to access only a specific S3 bucket.
- Create a policy using JSON for a user to access only one S3 bucket



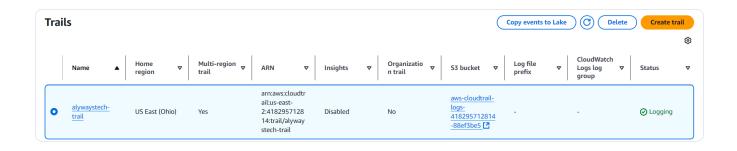
## 3. Security Enforcement:

- Enabled strong password policy (IAM > Account Settings)
- Enable **MFA** for each user (IAM > Users > Security credentials > Activate MFA) → if password lost or hacked, the account is not compromised.
- Make sure every user can able to login to their accounts without any difficulties.



### 4. Created S3 bucket for Governance & Monitoring Setup

- Create s3 bucket name: alywaystech-trail\_logs
- Integrate KMS with S3 (Bucket Encryption)
- Encryption type: **AWS Key Management Service key (SSE-KMS)** all objects uploaded to this bucket will be encrypted using your custom KMS key.
- Enabling CloudTrail and Store logs in S3 bucket
- This helps to check Logs who did what, when, from where (IP), and how (CLI, Console, SDK)
- Stores logs in your S3 bucket (alywaystech-trail) for analysis or compliance

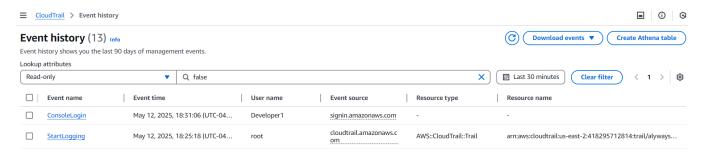


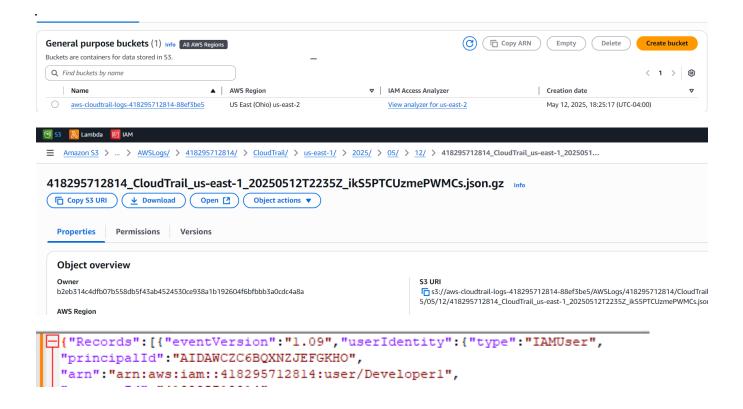
## **How it Benefits the Project**

- Ensures accountability for all team members
- Helps detect unauthorized or risky activity
- Allows compliance audits (e.g., SOC 2, HIPAA)
- Supports incident investigation if needed

#### Test If CloudTrail is Working

• It can log all the users' activity.





#### Summary:

#### **Key Accomplishments:**

- Identity & Access Management (IAM):
  - Created 3 IAM Groups (Admin, CloudEng, Developers) with least-privilege permissions.
  - o Onboarded **6 IAM Users**, assigned to groups based on roles.
  - Created a custom policy to allow access to a specific S3 bucket.

#### Security Enforcement:

- Enabled **strong password policy** and **MFA** for all users.
- Ensured users can securely access the console without issues.

#### • S3 & KMS Integration:

- Created an encrypted S3 bucket: alywaystech-trail\_logs
- Enabled SSE-KMS using a custom AWS KMS key to encrypt all uploaded logs.

#### Governance & Monitoring:

- o Set up AWS CloudTrail to log all account activities (who, when, from where, how).
- o Configured logs to be stored in the S3 bucket for future analysis and compliance.

# This setup provides:

- A secure, scalable access control system for a growing remote team.
- End-to-end encryption of sensitive company data.
- Full visibility into user activity and resource usage for audits or investigations.
- Alignment with **cloud security best practices** from Day 1.