

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

User groups (3) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

<input type="checkbox"/>	Group name	▲	Users	▼	Permissions	▼	Creation time
<input type="checkbox"/>	Admingroup				 0  Defined		5 minutes ago
<input type="checkbox"/>	CloudEng				 0  Defined		4 minutes ago
<input type="checkbox"/>	Developers				 0  Defined		Now

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

Users (6) [Info](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS

<input type="checkbox"/>	User name	▲	Path	▼	Group: ▼
<input type="checkbox"/>	Admin1		/		1
<input type="checkbox"/>	CloudEng1		/		1
<input type="checkbox"/>	CloudEng2		/		1
<input type="checkbox"/>	CloudEng3		/		1
<input type="checkbox"/>	Developer1		/		1
<input type="checkbox"/>	Developer2		/		1

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.

United States (Ohio) ▼ Admin1 @ 4182-9571-2814 ▲

Reset to default layout

+ Add widgets

Applications (0) [Info](#)

Region: US East (Ohio)

Select Region ▼
us-east-2 (Current Region)

< 1 >

Name	Description	Region	Originati.	★ ▲
No applications				
Get started by creating an application.				
<div>Create application</div>				

Account ID
4182-9571-2814

IAM user
Admin1

Account

Organization

Service Quotas

Billing and Cost Management

Security credentials

Turn on multi-session support

Switch role

Sign out

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

Trails												Copy events to Lake	Refresh	Delete	Create trail	
	Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status						
	alywaystech-trail	US East (Ohio)	Yes	arn:aws:cloudtrail:us-east-2:418295712814:trail/alywaystech-trail	Disabled	No	aws-cloudtrail-logs-418295712814-88ef3be5	-	-	Logging						

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.

CloudTrail > Event history							📄	🔍	🔄
Event history (13) Info							🔄	Download events	Create Athena table
Event history shows you the last 90 days of management events.									
Lookup attributes									
Read-only							🔍 false	Last 30 minutes	Clear filter
<input type="checkbox"/>	Event name	Event time	User name	Event source	Resource type	Resource name			
<input type="checkbox"/>	ConsoleLogin	May 12, 2025, 18:31:06 (UTC-04...	Developer1	signin.amazonaws.com	-	-			
<input type="checkbox"/>	StartLogging	May 12, 2025, 18:25:18 (UTC-04...	root	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-2:418295712814:trail/alyways...			

The screenshot shows the AWS S3 console interface. At the top, there's a header for 'General purpose buckets (1)' with an 'Info' link and a 'All AWS Regions' button. Below this, a search bar prompts 'Find buckets by name'. A table lists buckets with columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The selected bucket is 'aws-cloudtrail-logs-418295712814-88ef3be5' in the 'US East (Ohio) us-east-2' region. Below the table, a breadcrumb trail shows the navigation path: Amazon S3 > ... > AWSLogs/ > 418295712814/ > CloudTrail/ > us-east-1/ > 2025/ > 05/ > 12/ > 418295712814_CloudTrail_us-east-1_20250512... The main content area displays the object '418295712814_CloudTrail_us-east-1_20250512T2235Z_ikS5PTCUzmePwMCs.json.gz' with buttons for 'Copy S3 URI', 'Download', 'Open', and 'Object actions'. Below these are tabs for 'Properties', 'Permissions', and 'Versions'. The 'Properties' tab is active, showing an 'Object overview' section with 'Owner' (b2eb314c4dfb07b558db5f43ab4524530ce938a1b192604f6bfbb3a0cdc4a8a) and 'AWS Region' (US East (Ohio) us-east-2). To the right, the 'S3 URI' is displayed as 's3://aws-cloudtrail-logs-418295712814-88ef3be5/AWSLogs/418295712814/CloudTrail/5/05/12/418295712814_CloudTrail_us-east-1_20250512T2235Z_ikS5PTCUzmePwMCs.json.gz'. At the bottom, a preview of the JSON file content is shown, starting with '{ "Records": [{ "eventVersion": "1.09", "userIdentity": { "type": "IAMUser", "principalId": "AIDAWCZC6BQXNZJEFKHO", "arn": "arn:aws:iam::418295712814:user/Developer1", ... } }] }'.

Summary:

Key Accomplishments:

- **Identity & Access Management (IAM):**
 - Created **3 IAM Groups** (Admin, CloudEng, Developers) with least-privilege permissions.
 - 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:**

- Set up **AWS CloudTrail** to log all account activities (who, when, from where, how).
- 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.