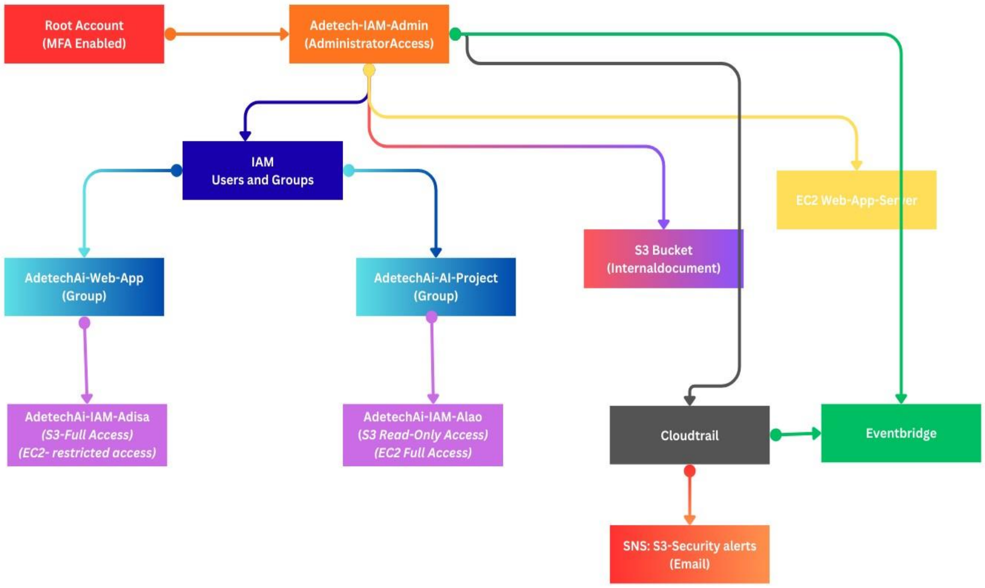
# Cloud Security Implementation Project
# (ISO 27001 / NIST / CIS Aligned)

## 1. Executive Summary

This project demonstrates the implementation of foundational cloud security controls aligned with ISO/IEC 27001:2022, NIST Cybersecurity Framework (CSF), and CIS Critical Security Controls. The objective was to establish a secure AWS environment with strong identity governance, access control, logging, monitoring, and alerting mechanisms.

The environment was designed to:

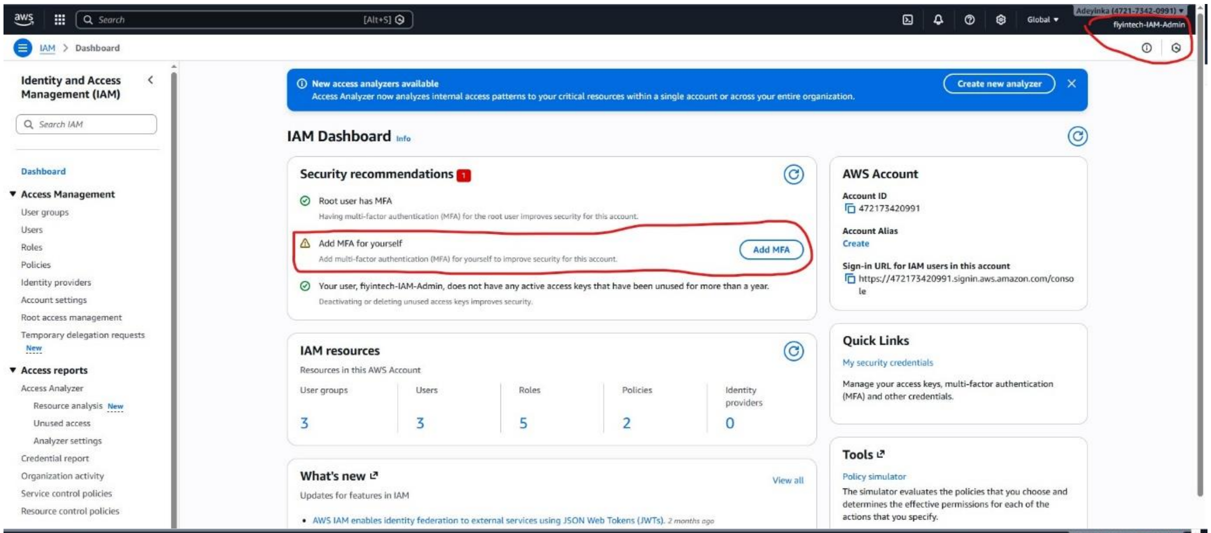
- Secure administrative access
- Enforce separation of duties
- Protect sensitive S3 resources
- Restrict EC2 administrative actions
- Capture and audit API activity
- Generate automated alerts for sensitive S3 actions



## 2. Governance and Account Security

ISO 27001 A.5 & A.6 | NIST CSF ID.GV | CIS Control 1

The AWS root account was secured with Multi-Factor Authentication (MFA) and restricted from daily use. In accordance with governance best practices, a dedicated administrative IAM user (Adetech-IAM-Admin) was created to handle operational activities, ensuring accountability and reducing single-point-of-failure risk.



**New access analyzers available**
Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization.

IAM Dashboard Info

Security recommendations 1

✓ Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.

⚠ Add MFA for yourself
Add multi-factor authentication (MFA) for yourself to improve security for this account.

✓ Your user, fiyintech-IAM-Admin, does not have any active access keys that have been unused for more than a year.
Deactivating or deleting unused access keys improves security.

IAM resources
Resources in this AWS Account

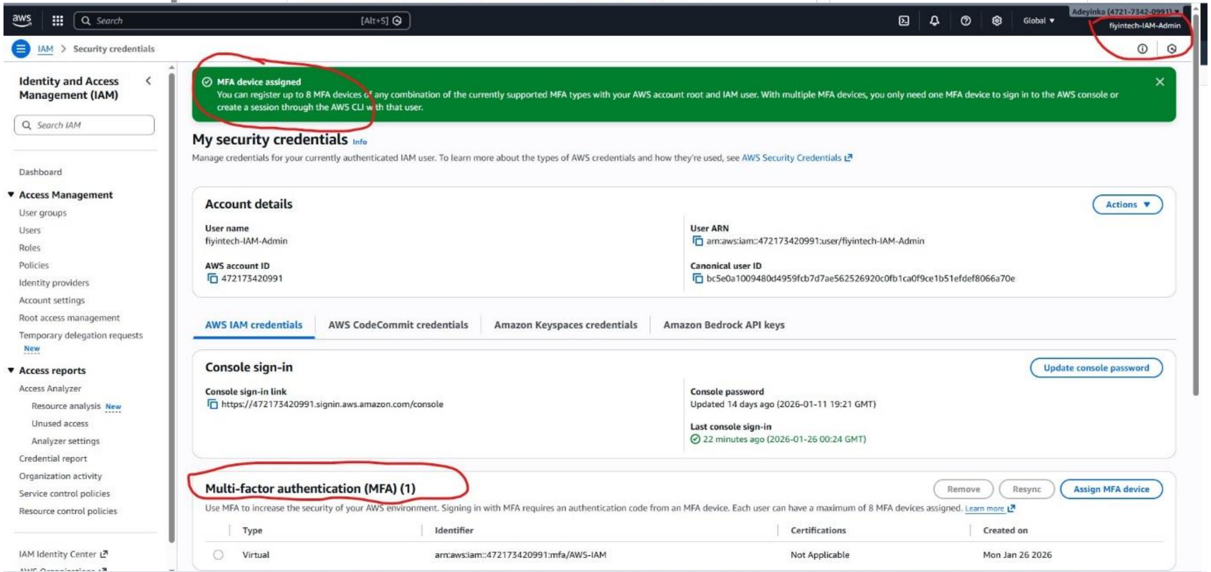
| User groups | Users | Roles | Policies | Identity providers |
|---|---|---|---|---|
| 3 | 3 | 5 | 2 | 0 |

What's new
Updates for features in IAM
- AWS IAM enables identity federation to external services using JSON Web Tokens (JWTs). 2 months ago

AWS Account
Account ID: 472173420991
Account Alias: Create
Sign-in URL for IAM users in this account: https://472173420991.signin.aws.amazon.com/console

Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.



**MFA device assigned**
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

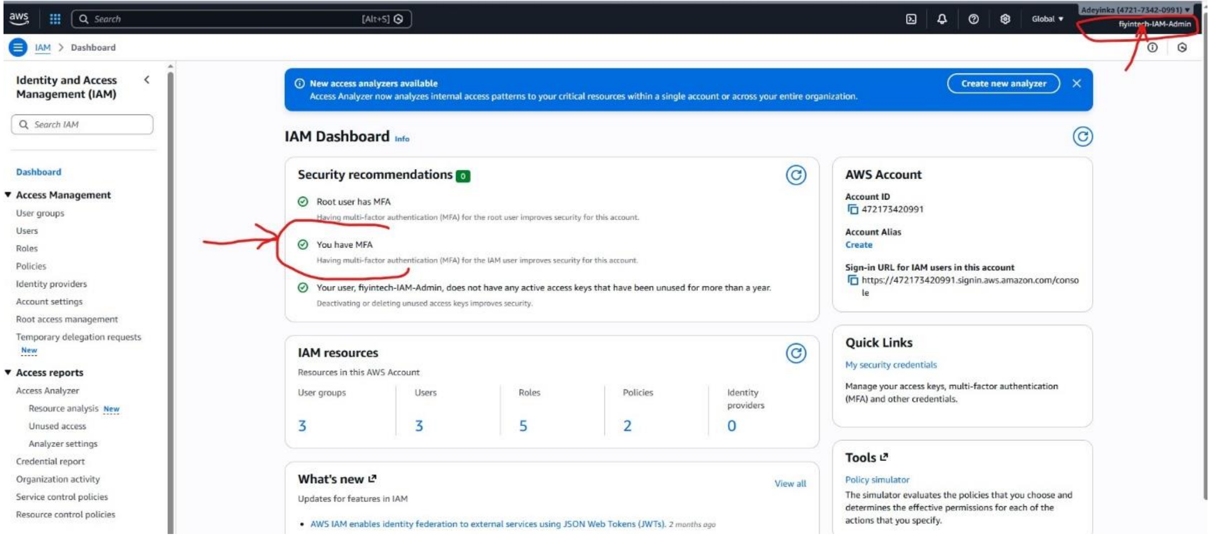
My security credentials Info
Manage credentials for your currently authenticated IAM user. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials

Account details
User name: fiyintech-IAM-Admin
AWS account ID: 472173420991
User ARN: arn:aws:iam::472173420991:user/fiyintech-IAM-Admin
Canonical user ID: bc5e0a1009480d4959fcb7d7ae562526920c0fb1ca0f9ce1b51efdef8066a70e

Console sign-in
Console sign-in link: https://472173420991.signin.aws.amazon.com/console
Console password: Updated 14 days ago (2026-01-11 19:21 GMT)
Last console sign-in: 22 minutes ago (2026-01-26 00:24 GMT)

Multi-factor authentication (MFA) (1)
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

| | Type | Identifier | Certifications | Created on |
|---|---|---|---|---|
| ○ | Virtual | arn:aws:iam::472173420991:mfa/AWS-IAM | Not Applicable | Mon Jan 26 2026 |



**New access analyzers available**
Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization.

IAM Dashboard Info

Security recommendations 0

✓ Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.

✓ You have MFA
Having multi-factor authentication (MFA) for the IAM user improves security for this account.

✓ Your user, fiyintech-IAM-Admin, does not have any active access keys that have been unused for more than a year.
Deactivating or deleting unused access keys improves security.

IAM resources
Resources in this AWS Account

| User groups | Users | Roles | Policies | Identity providers |
|---|---|---|---|---|
| 3 | 3 | 5 | 2 | 0 |

What's new
Updates for features in IAM
- AWS IAM enables identity federation to external services using JSON Web Tokens (JWTs). 2 months ago

AWS Account
Account ID: 472173420991
Account Alias: Create
Sign-in URL for IAM users in this account: https://472173420991.signin.aws.amazon.com/console

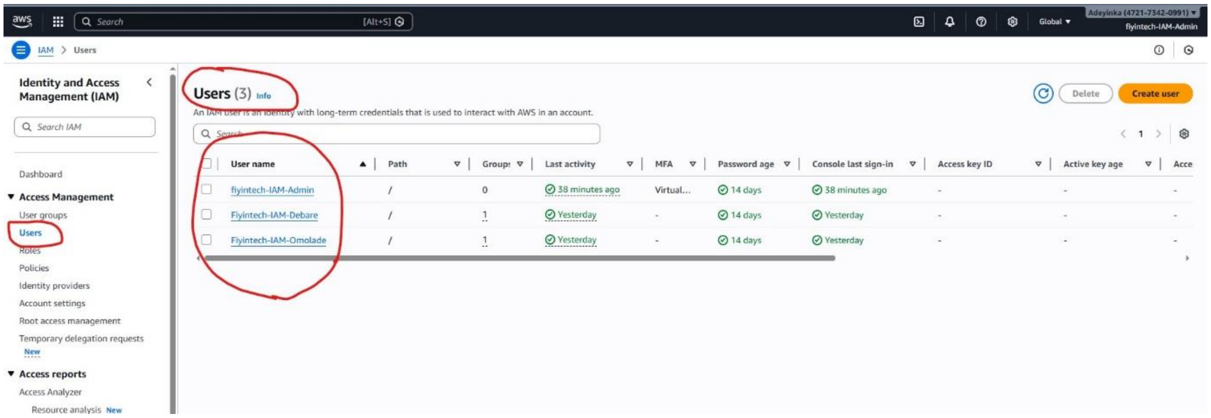
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

## 3. Identity and Access Management (IAM)

**ISO 27001 A.5.15, A.8 | NIST CSF PR.AC | CIS Control 5**

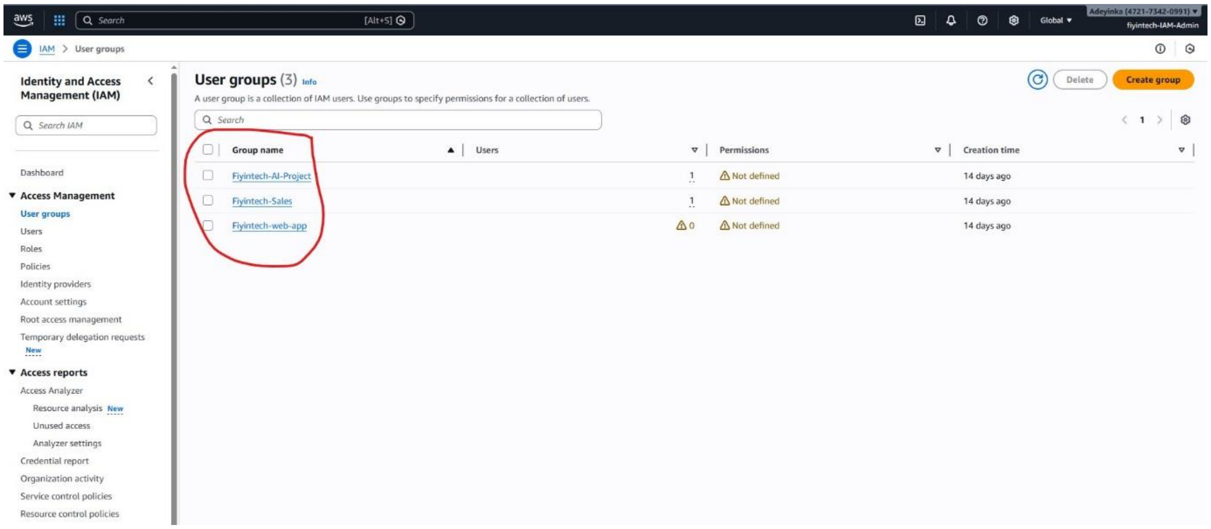
IAM users and groups were created to enforce role-based access control (RBAC). Users were assigned to groups based on job function, ensuring separation of duties and least privilege.



Users (3) Info

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

| | User name | Path | Groups | Last activity | MFA | Password age | Console last sign-in | Access key ID | Active key age | Acce |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | fiyintech-IAM-Admin | / | 0 | ✓ 38 minutes ago | Virtual... | ✓ 14 days | ✓ 38 minutes ago | - | - | - |
| □ | Fiyintech-IAM-Debare | / | 1 | ✓ Yesterday | - | ✓ 14 days | ✓ Yesterday | - | - | - |
| □ | Fiyintech-IAM-Omolade | / | 1 | ✓ Yesterday | - | ✓ 14 days | ✓ Yesterday | - | - | - |



User groups (3) Info

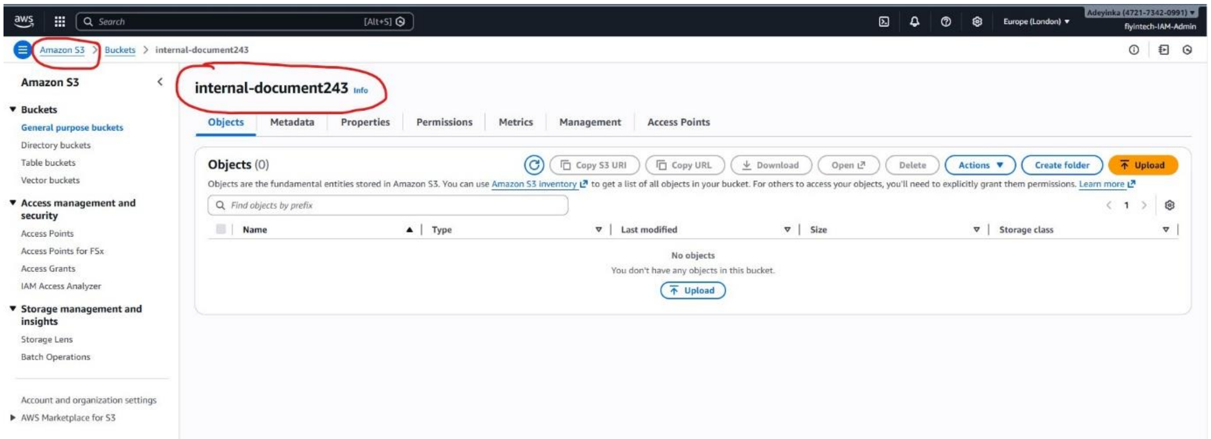
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

| | Group name | Users | Permissions | Creation time |
|---|---|---|---|---|
| □ | Fiyintech-AI-Project | 1 | ⚠ Not defined | 14 days ago |
| □ | Fiyintech-Sales | 1 | ⚠ Not defined | 14 days ago |
| □ | Fiyintech-web-app | ⚠ 0 | ⚠ Not defined | 14 days ago |

## 4. Object Storage Security (Amazon S3)

ISO 27001 A.8.2 | NIST CSF PR.DS | CIS Control 3

An S3 bucket containing internal documents was created and protected using IAM-based RBAC. One user was granted full S3 access while another was restricted to read-only permissions. Access validation confirmed enforcement of least privilege



internal-document243 Info

Objects (0)

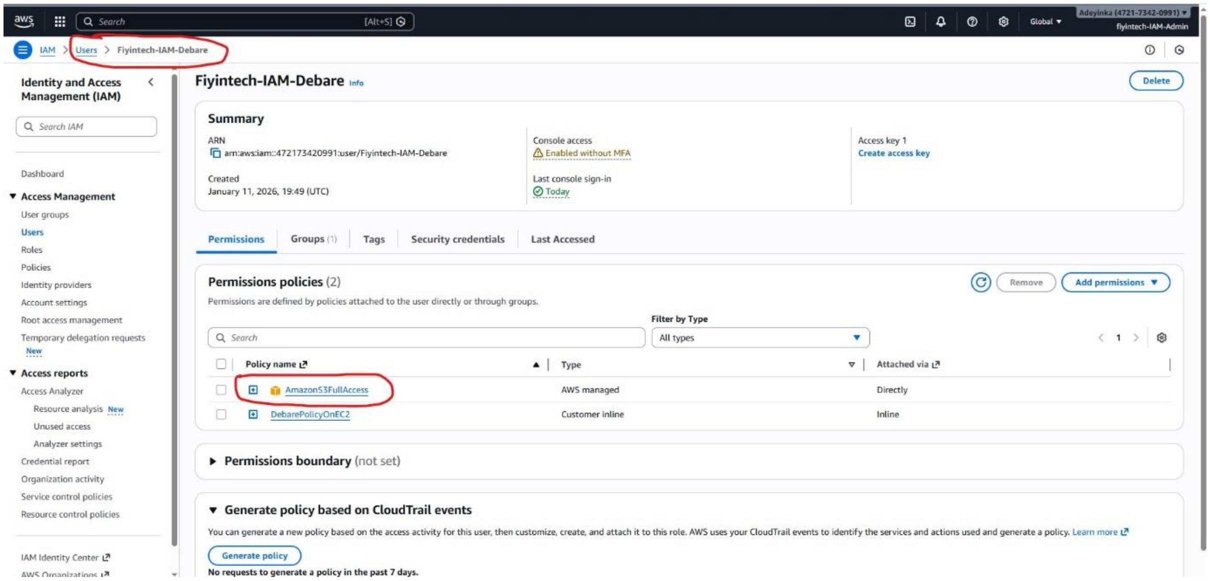
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

| Name | Type | Last modified | Size | Storage class |
|---|---|---|---|---|

No objects

You don't have any objects in this bucket.

Fiyintech-IAM-Debare Fullaccess



Fiyintech-IAM-Debare Info

Summary

ARN
arn:aws:iam::472173420991:user/Fiyintech-IAM-Debare

Created
January 11, 2026, 19:49 (UTC)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
Create access key

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
All types

| Policy name | Type | Attached via |
|---|---|---|
| AmazonS3FullAccess | AWS managed | Directly |
| DebarePolicyOnEC2 | Customer inline | Inline |

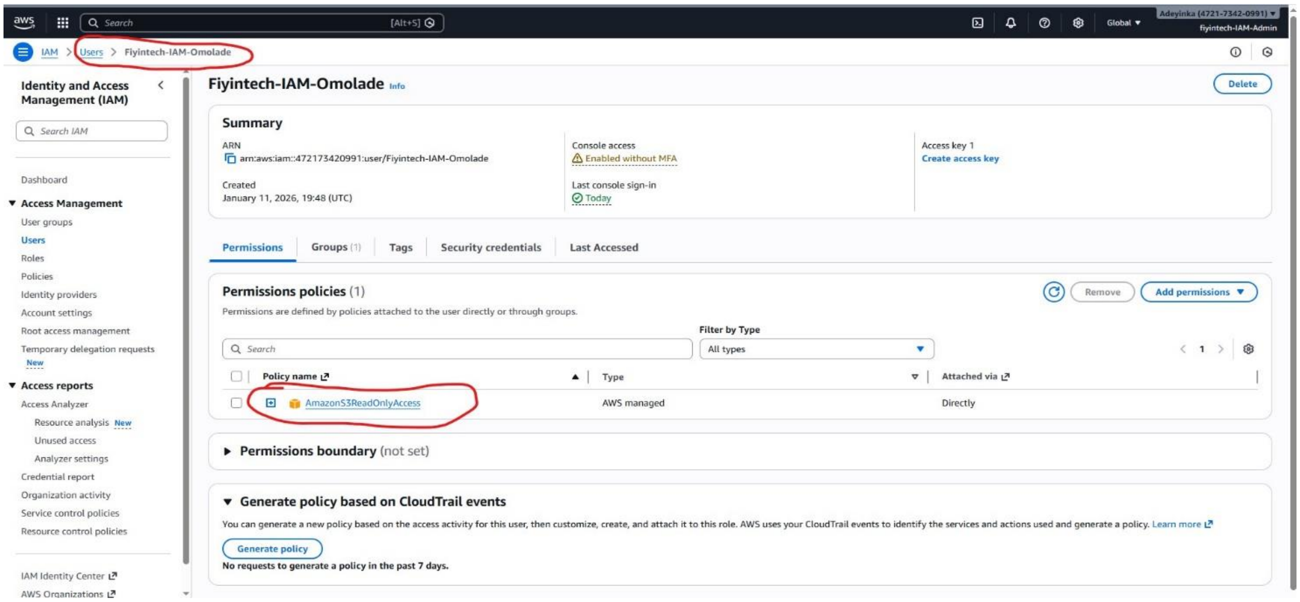
Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

No requests to generate a policy in the past 7 days.

Fiyintech-IAM-Omolade Readonlyaccess



Fiyintech-IAM-Omolade Info

Summary

ARN
arn:aws:iam::472173420991:user/Fiyintech-IAM-Omolade

Created
January 11, 2026, 19:48 (UTC)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
Create access key

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
All types

| Policy name | Type | Attached via |
|---|---|---|
| AmazonS3ReadOnlyAccess | AWS managed | Directly |

Permissions boundary (not set)

Generate policy based on CloudTrail events

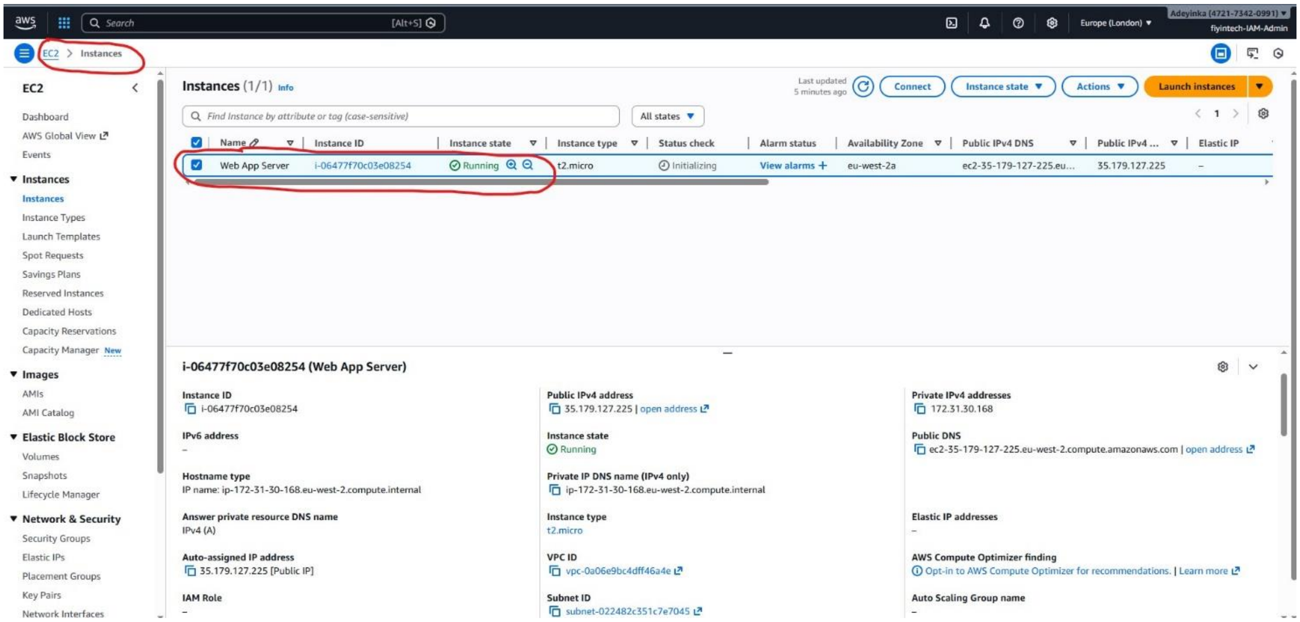
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

No requests to generate a policy in the past 7 days.

## 5. Compute Resource Access Control (EC2)

ISO 27001 A.8.9 | NIST CSF PR.AC-4 | CIS Control 4

An EC2 instance was deployed to simulate a web application server. Inline IAM policies were used to explicitly deny high-risk administrative actions such as instance termination and key pair creation for selected users. Policy enforcement was verified through controlled testing.



Instances (1/1) Info

| ☑ | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 ... | Elastic IP |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | Web App Server | i-06477f70c03e08254 | Running | t2.micro | Initializing | View alarms + | eu-west-2a | ec2-35-179-127-225.eu... | 35.179.127.225 | – |

i-06477f70c03e08254 (Web App Server)

Instance ID
i-06477f70c03e08254

IPv6 address
–

Hostname type
IP name: ip-172-31-30-168.eu-west-2.compute.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
35.179.127.225 [Public IP]

IAM Role
–

Public IPv4 address
35.179.127.225 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-30-168.eu-west-2.compute.internal

Instance type
t2.micro

VPC ID
vpc-0a06e9bc4dff46a4e

Subnet ID
subnet-022482c351c7e7045

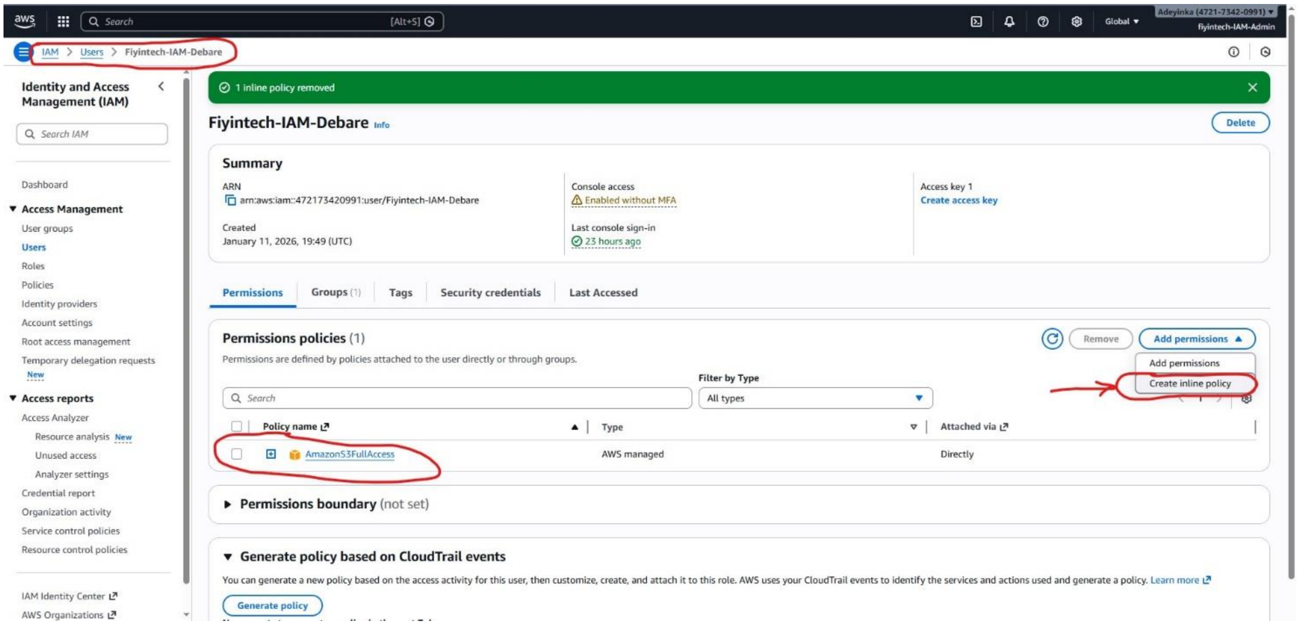
Private IPv4 addresses
172.31.30.168

Public DNS
ec2-35-179-127-225.eu-west-2.compute.amazonaws.com | open address

Elastic IP addresses
–

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–



1 inline policy removed

Fiyintech-IAM-Debare Info

Summary

ARN
arn:aws:iam::472173420991:user/Fiyintech-IAM-Debare

Created
January 11, 2026, 19:49 (UTC)

Console access
Enabled without MFA

Last console sign-in
23 hours ago

Access key 1
Create access key

Permissions policies (1)

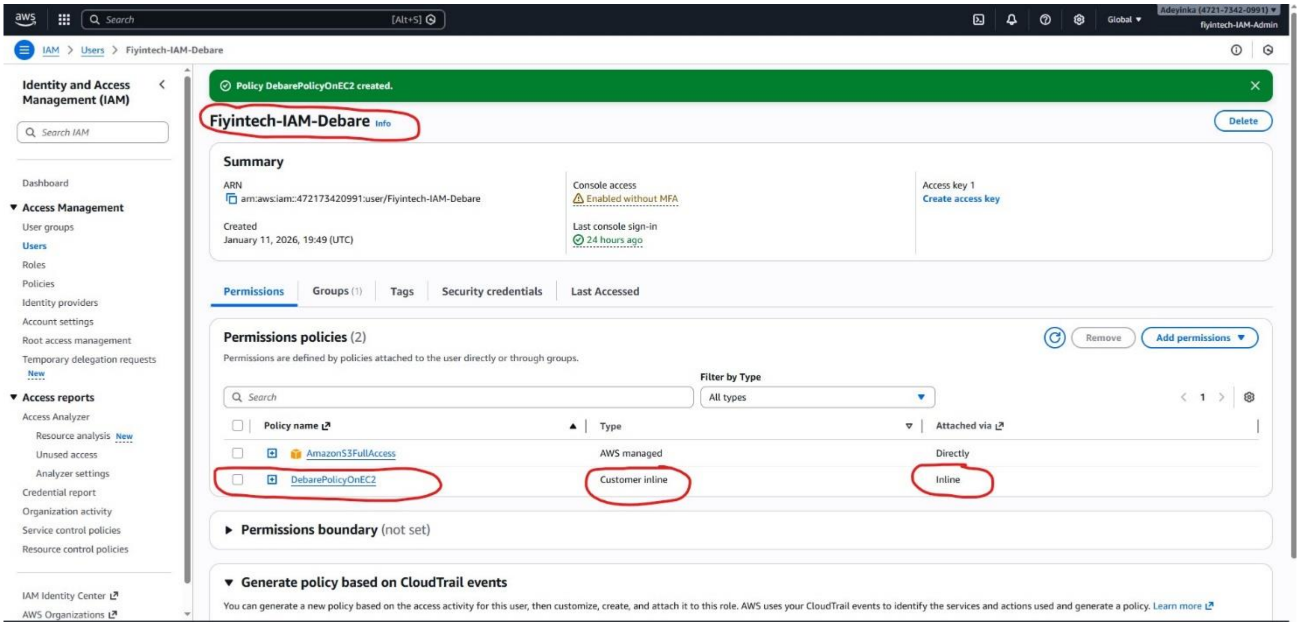
Permissions are defined by policies attached to the user directly or through groups.

| □ | Policy name | Type | Attached via |
|---|---|---|---|
| □ | AmazonS3FullAccess | AWS managed | Directly |

▶ Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more



Policy DebarePolicyOnEC2 created.

Fiyintech-IAM-Debare Info

Summary

ARN
arn:aws:iam::472173420991:user/Fiyintech-IAM-Debare

Created
January 11, 2026, 19:49 (UTC)

Console access
Enabled without MFA

Last console sign-in
24 hours ago

Access key 1
Create access key

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

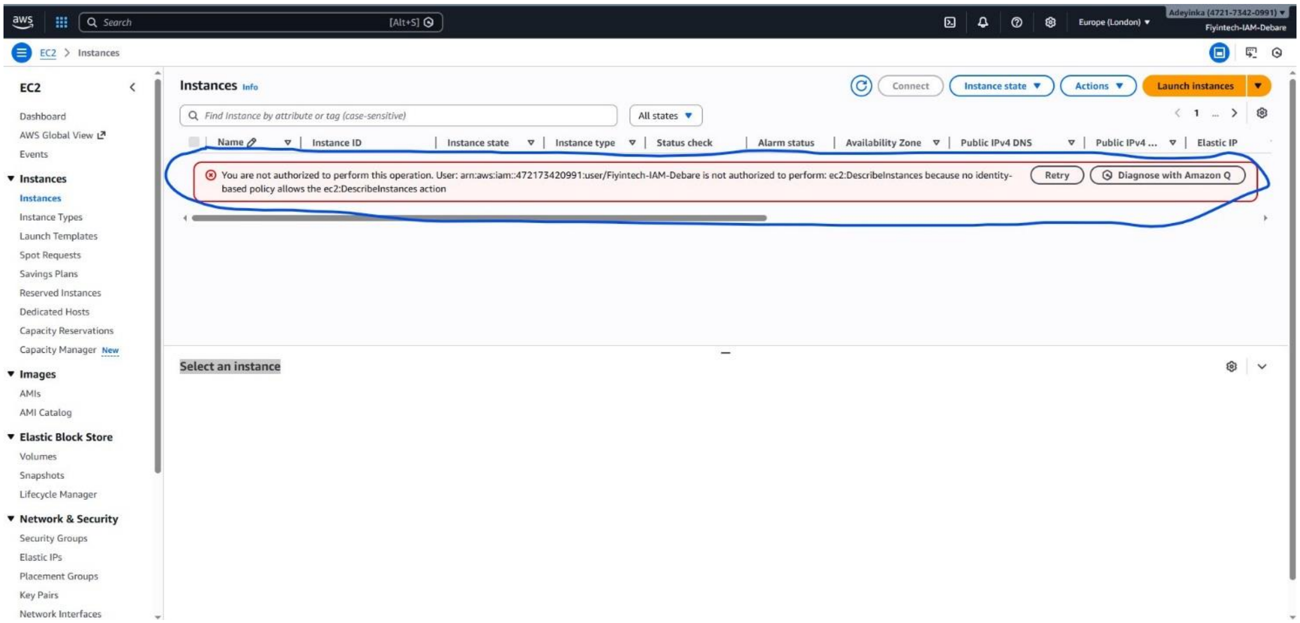
Filter by Type: All types

| Policy name | Type | Attached via |
|---|---|---|
| AmazonS3FullAccess | AWS managed | Directly |
| DebarePolicyOnEC2 | Customer inline | Inline |

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy.



Instances Info

Find Instance by attribute or tag (case-sensitive)

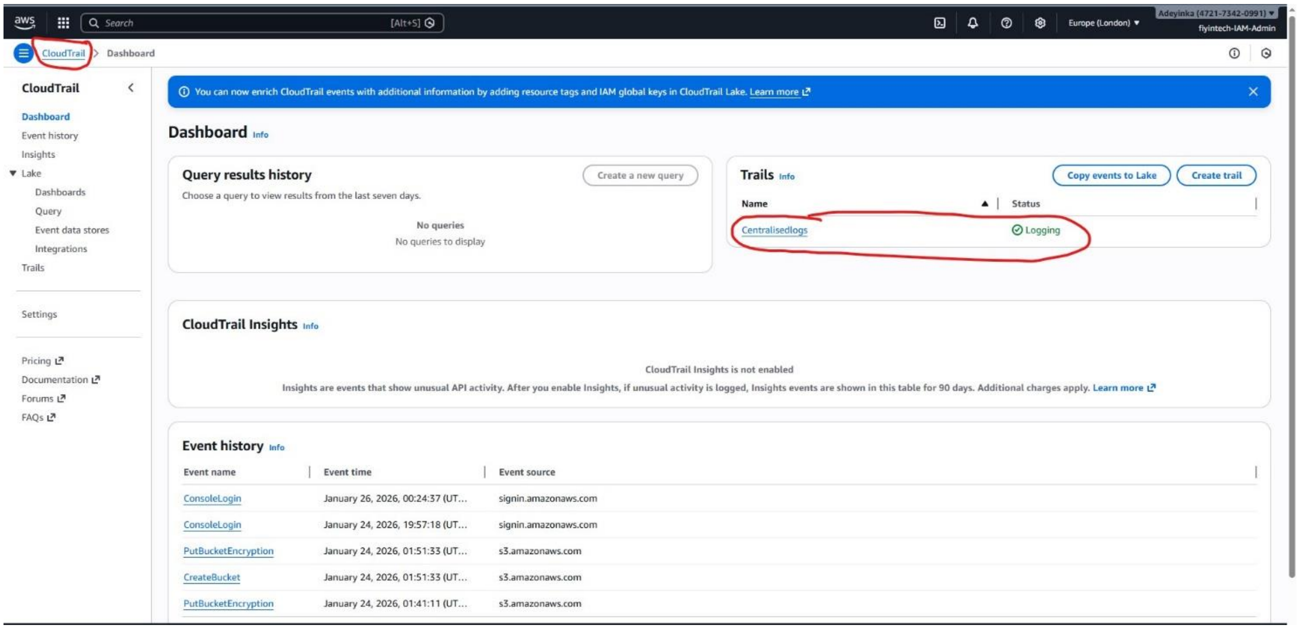
| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 ... | Elastic IP |
|---|---|---|---|---|---|---|---|---|---|

You are not authorized to perform this operation. User: arn:aws:iam::472173420991:user/Fiyintech-IAM-Debare is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action

## 6. Logging and Monitoring

ISO 27001 A.8.15 | NIST CSF DE.CM | CIS Control 8

AWS CloudTrail was configured to capture management events across all IAM users. Centralized logging ensures traceability, supports incident response, and enables compliance auditing.



You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more

Dashboard Info

Query results history

Choose a query to view results from the last seven days.

No queries
No queries to display

Trails Info

| Name | Status |
|---|---|
| Centralisedlogs | ✓ Logging |

CloudTrail Insights Info

CloudTrail Insights is not enabled
Insights are events that show unusual API activity. After you enable Insights, if unusual activity is logged, Insights events are shown in this table for 90 days. Additional charges apply. Learn more

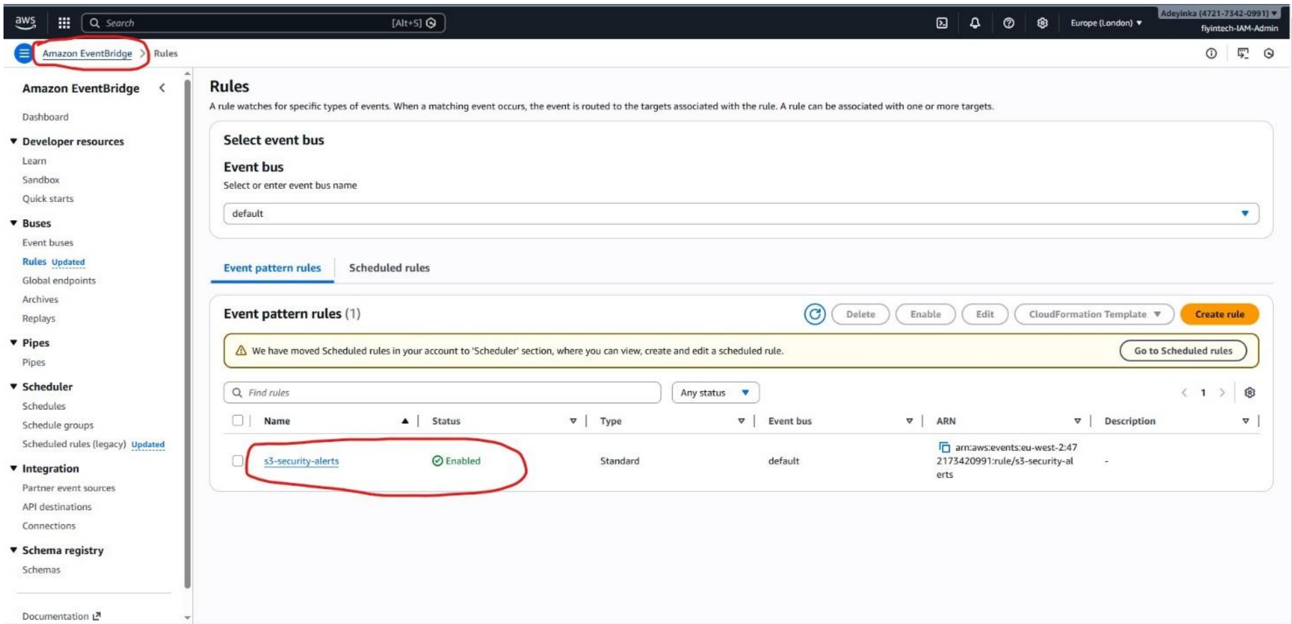
Event history Info

| Event name | Event time | Event source |
|---|---|---|
| ConsoleLogin | January 26, 2026, 00:24:37 (UT... | signin.amazonaws.com |
| ConsoleLogin | January 24, 2026, 19:57:18 (UT... | signin.amazonaws.com |
| PutBucketEncryption | January 24, 2026, 01:51:33 (UT... | s3.amazonaws.com |
| CreateBucket | January 24, 2026, 01:51:33 (UT... | s3.amazonaws.com |
| PutBucketEncryption | January 24, 2026, 01:41:11 (UT... | s3.amazonaws.com |

## 7. Security Event Detection and Alerting

ISO 27001 A.8.16 | NIST CSF DE.AE | CIS Control 8

EventBridge rules were created to detect sensitive S3 actions captured by CloudTrail. Detected events trigger notifications via Amazon SNS, delivering near real-time alerts to security personnel.



Rules

A rule watches for specific types of events. When a matching event occurs, the event is routed to the targets associated with the rule. A rule can be associated with one or more targets.

Select event bus

Event bus

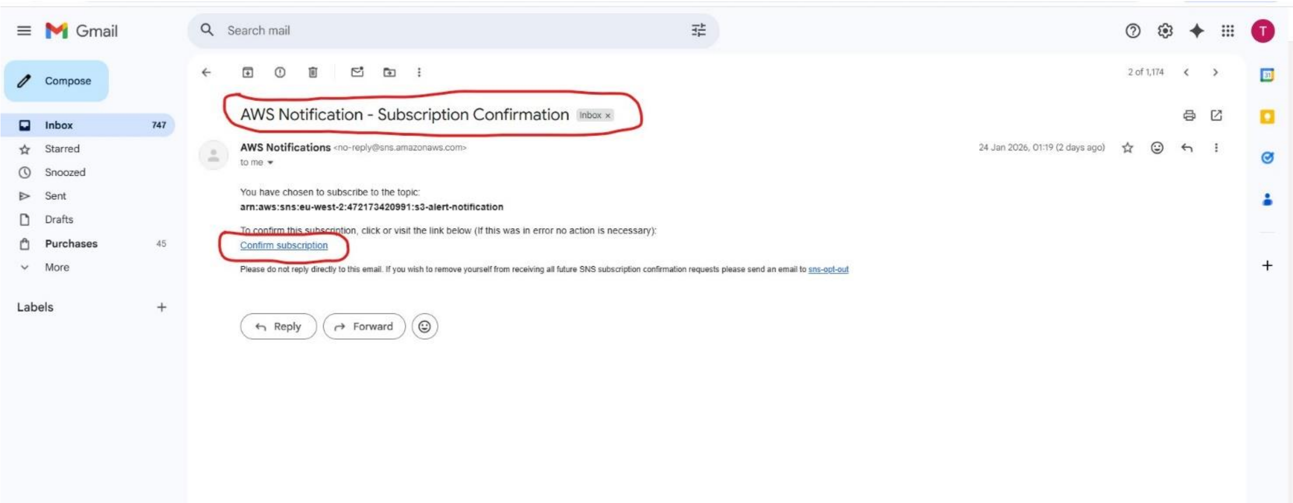
Select or enter event bus name

default

Event pattern rules (1)

We have moved Scheduled rules in your account to 'Scheduler' section, where you can view, create and edit a scheduled rule.

| Name | Status | Type | Event bus | ARN | Description |
|---|---|---|---|---|---|
| s3-security-alerts | ✓ Enabled | Standard | default | arn:aws:events:eu-west-2:472173420991:rule/s3-security-alerts | - |



AWS Notification - Subscription Confirmation

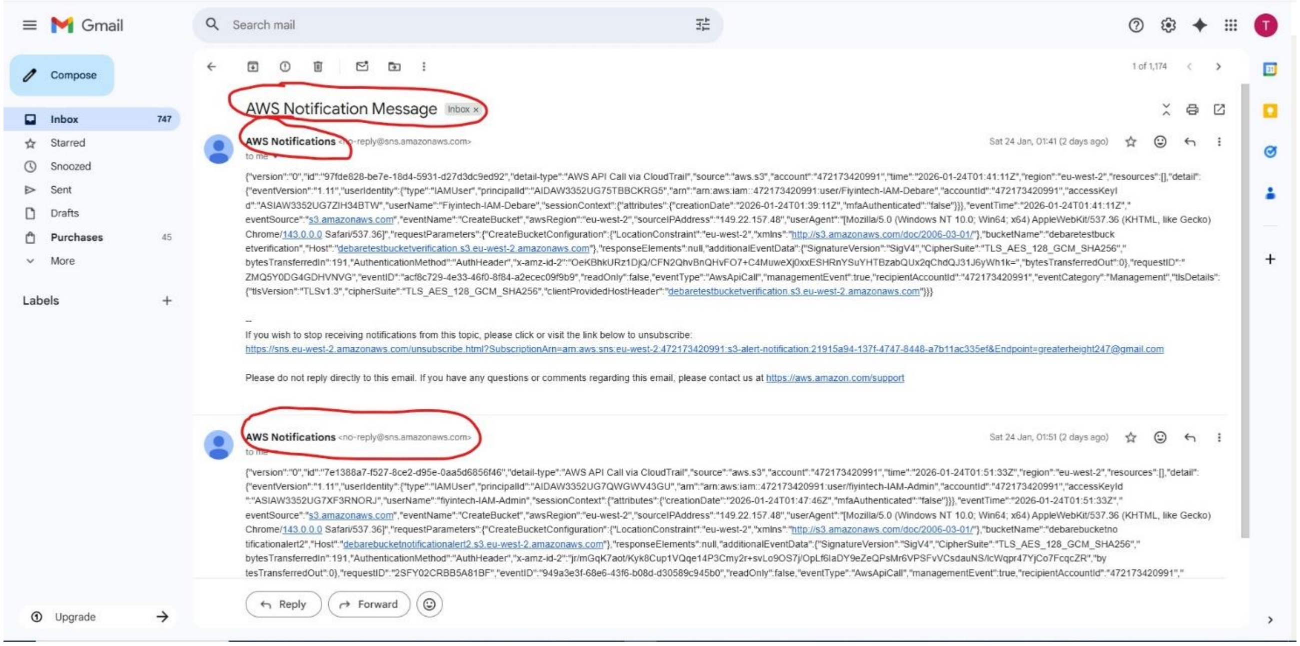
**AWS Notifications** <no-reply@sns.amazonaws.com>
to me

24 Jan 2026, 01:19 (2 days ago)

You have chosen to subscribe to the topic:
**arn:aws:sns:eu-west-2:472173420991:s3-alert-notification**

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out



AWS Notification Message

**AWS Notifications** <no-reply@sns.amazonaws.com>
to me

Sat 24 Jan, 01:41 (2 days ago)

```
{"version":"0","id":"97fde828-be7e-18d4-5931-d27d3dc9ed92","detail-type":"AWS API Call via CloudTrail","source":"aws.s3","account":"472173420991","time":"2026-01-24T01:41:11Z","region":"eu-west-2","resources":[],"detail":
{"eventVersion":"1.11","userIdentity":{"type":"IAMUser","principalId":"AIDAW3352UG75TBBCKRG5","arn":"arn:aws:iam::472173420991:user/Fiyintech-IAM-Debare","accountId":"472173420991","accessKeyI
d":"ASIAW3352UG7ZIH34BTW","userName":"Fiyintech-IAM-Debare","sessionContext":{"attributes":{"creationDate":"2026-01-24T01:39:11Z","mfaAuthenticated":"false"}}},"eventTime":"2026-01-24T01:41:11Z","
eventSource":"s3.amazonaws.com","eventName":"CreateBucket","awsRegion":"eu-west-2","sourceIPAddress":"149.22.157.48","userAgent":"[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36]","requestParameters":{"CreateBucketConfiguration":{"LocationConstraint":"eu-west-2","xmlns":"http://s3.amazonaws.com/doc/2006-03-01/"},"bucketName":"debaretestbuck
etverification","Host":"debaretestbucketverification.s3.eu-west-2.amazonaws.com"},"responseElements":null,"additionalEventData":{"SignatureVersion":"SigV4","CipherSuite":"TLS_AES_128_GCM_SHA256","
bytesTransferredIn":191,"AuthenticationMethod":"AuthHeader","x-amz-id-2":"OeKBhkURz1DjQ/CFN2QhvBnQHvFO7+C4MuweXj0xxESHRnYSuYHTBzabQUx2qChdQJ31J6yWh1k=","bytesTransferredOut":0},"requestID":"
ZMQ5Y0DG4GDHVNVG","eventID":"acf8c729-4e33-46f0-8f84-a2ecec09f9b9","readOnly":false,"eventType":"AwsApiCall","managementEvent":true,"recipientAccountId":"472173420991","eventCategory":"Management","tlsDetails":
{"tlsVersion":"TLSv1.3","cipherSuite":"TLS_AES_128_GCM_SHA256","clientProvidedHostHeader":"debaretestbucketverification.s3.eu-west-2.amazonaws.com"}}}
```

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.eu-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:eu-west-2:472173420991:s3-alert-notification:21915a94-137f-4747-8448-a7b11ac335ef&Endpoint=greaterheight247@gmail.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support

**AWS Notifications** <no-reply@sns.amazonaws.com>
to me

Sat 24 Jan, 01:51 (2 days ago)

```
{"version":"0","id":"7e1388a7-f527-8ce2-d95e-0aa5d6856f46","detail-type":"AWS API Call via CloudTrail","source":"aws.s3","account":"472173420991","time":"2026-01-24T01:51:33Z","region":"eu-west-2","resources":[],"detail":
{"eventVersion":"1.11","userIdentity":{"type":"IAMUser","principalId":"AIDAW3352UG7QWGWV43GU","arn":"arn:aws:iam::472173420991:user/fiyintech-IAM-Admin","accountId":"472173420991","accessKeyId
":"ASIAW3352UG7XF3RNORJ","userName":"fiyintech-IAM-Admin","sessionContext":{"attributes":{"creationDate":"2026-01-24T01:47:46Z","mfaAuthenticated":"false"}}},"eventTime":"2026-01-24T01:51:33Z","
eventSource":"s3.amazonaws.com","eventName":"CreateBucket","awsRegion":"eu-west-2","sourceIPAddress":"149.22.157.48","userAgent":"[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36]","requestParameters":{"CreateBucketConfiguration":{"LocationConstraint":"eu-west-2","xmlns":"http://s3.amazonaws.com/doc/2006-03-01/"},"bucketName":"debarebucketno
tificationalert2","Host":"debarebucketnotificationalert2.s3.eu-west-2.amazonaws.com"},"responseElements":null,"additionalEventData":{"SignatureVersion":"SigV4","CipherSuite":"TLS_AES_128_GCM_SHA256","
bytesTransferredIn":191,"AuthenticationMethod":"AuthHeader","x-amz-id-2":"jr/mGqK7aot/Kyk8Cup1VQqe14P3Cmy2r+svLo9OS7j/OpLf6IaDY9eZeQPsMr6VPSFvVCsdauNS/lcWqpr47YjCo7FcqcZR","by
tesTransferredOut":0},"requestID":"2SFY02CRBB5A81BF","eventID":"949a3e3f-68e6-43f6-b08d-d30589c945b0","readOnly":false,"eventType":"AwsApiCall","managementEvent":true,"recipientAccountId":"472173420991","
```

## 8. Conclusion

The project demonstrates practical application of internationally recognized security frameworks in a cloud environment. Controls implemented align with governance, protection, detection, and response requirements, making the environment audit-ready and suitable for enterprise u