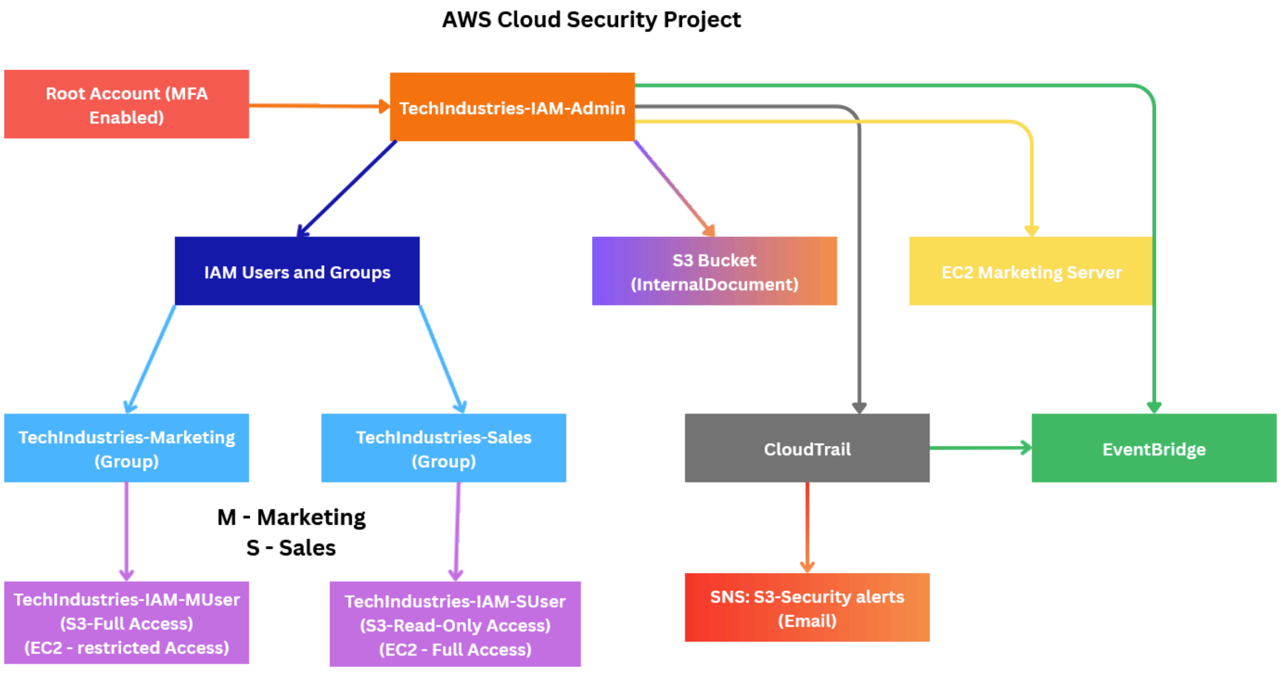
Cloud Security Implementation Project

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:

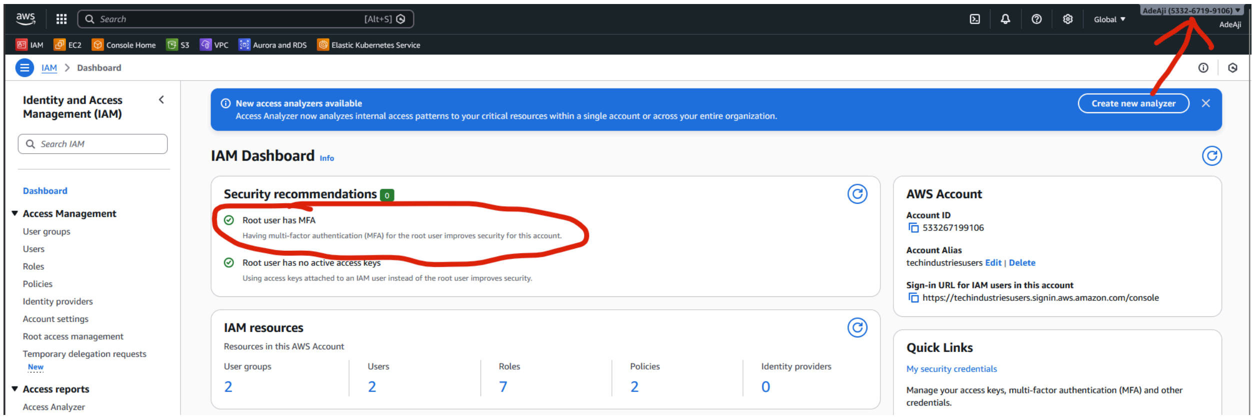
- Secure administrative access
- Enforce separation of duties
- Protect sensitive S3 resources
- Restrict EC2 administrative actions
- Capture and audit API activity
- Generate automated alerts for sensitive S3 actions


AWS Cloud Security Project
Root Account (MFA Enabled)
TechIndustries-IAM-Admin
IAM Users and Groups
S3 Bucket (InternalDocument)
EC2 Marketing Server
TechIndustries-Marketing (Group)
TechIndustries-Sales (Group)
CloudTrail
EventBridge
M - Marketing
S - Sales
TechIndustries-IAM-MUser (S3-Full Access) (EC2 - restricted Access)
TechIndustries-IAM-SUser (S3-Read-Only Access) (EC2 - Full Access)
SNS: S3-Security alerts (Email)

Governance & 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

Security recommendations 0

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

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

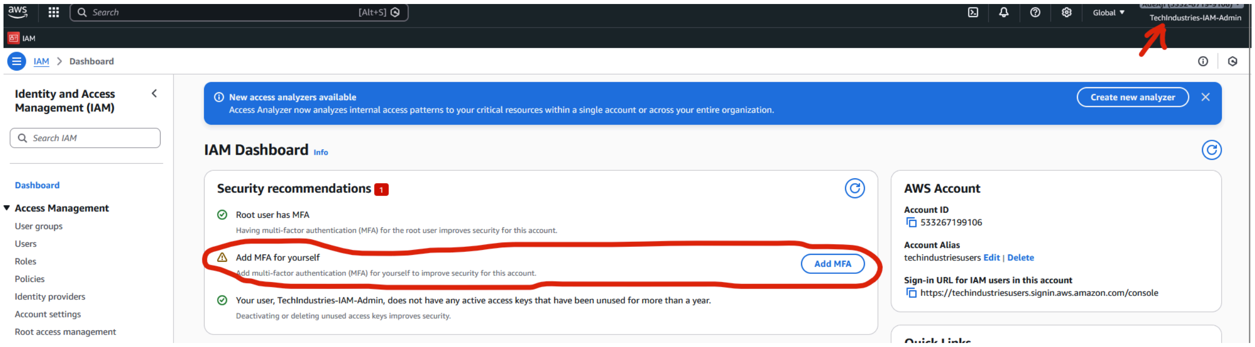
IAM resources
Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
2	2	7	2	0

AWS Account
Account ID
533267199106
Account Alias
techindustriesusers Edit | Delete
Sign-in URL for IAM users in this account
https://techindustriesusers.signin.aws.amazon.com/console

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

Root User has MFA Enabled



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

Security recommendations 1

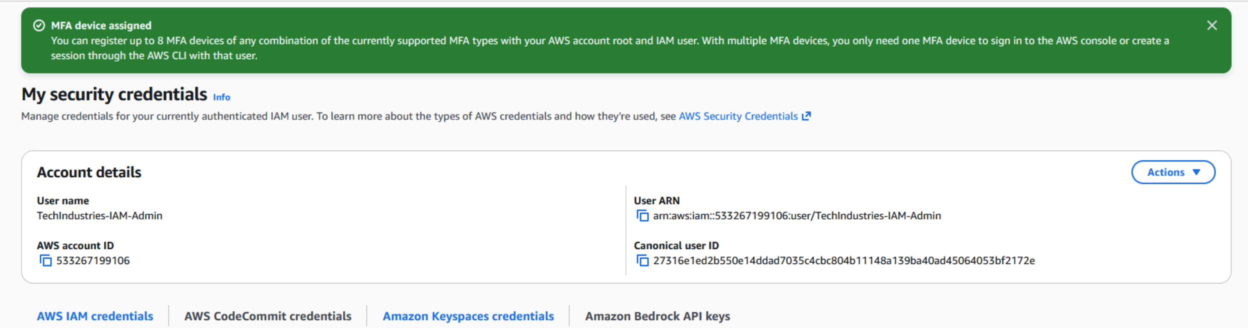
Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.

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

Your user, TechIndustries-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.

AWS Account
Account ID
533267199106
Account Alias
techindustriesusers Edit | Delete
Sign-in URL for IAM users in this account
https://techindustriesusers.signin.aws.amazon.com/console

Admin user (IAM) does not have MFA



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
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

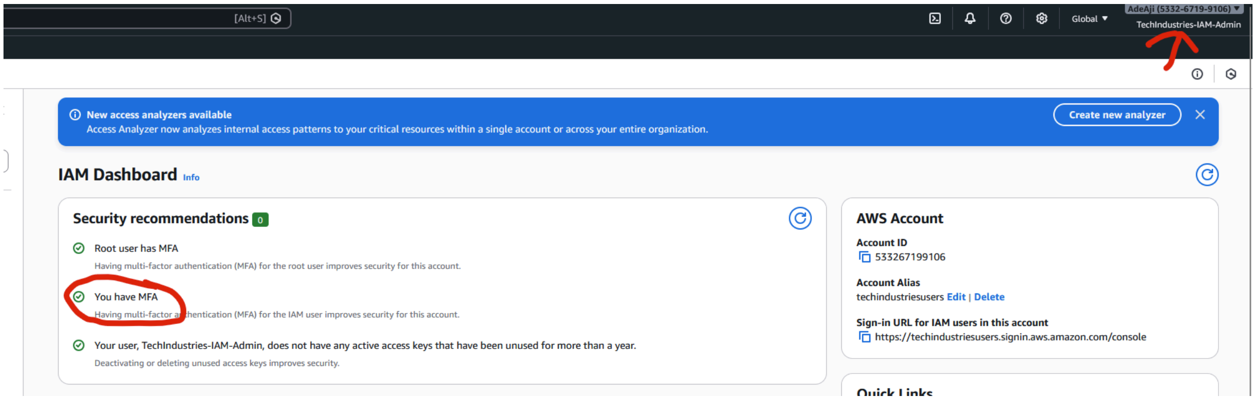
Account details

User name
TechIndustries-IAM-Admin

User ARN
arn:aws:iam::533267199106:user/TechIndustries-IAM-Admin

AWS account ID
533267199106

Canonical user ID
27316e1ed2b550e14ddad7035c4cbc804b11148a139ba40ad45064053bf2172e



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

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, TechIndustries-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.

AWS Account

Account ID
533267199106

Account Alias
techindustriesusers

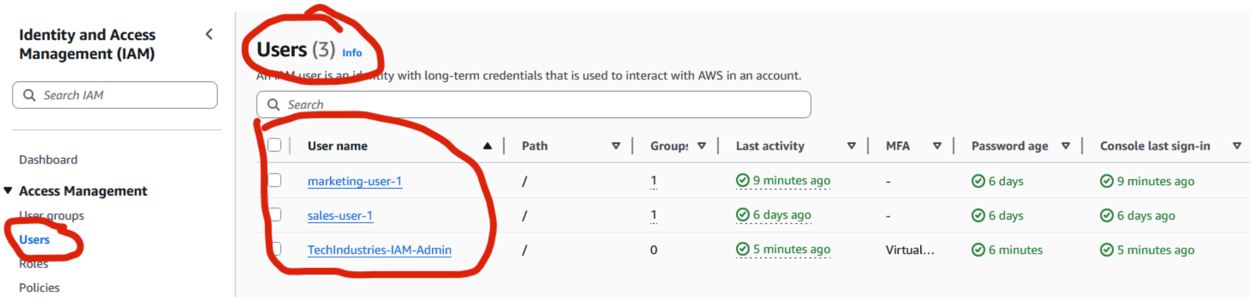
Sign-in URL for IAM users in this account
https://techindustriesusers.signin.aws.amazon.com/console

MFA Enabled for TechIndustries Admin (IAM)

Identity and Access Management (IAM)

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

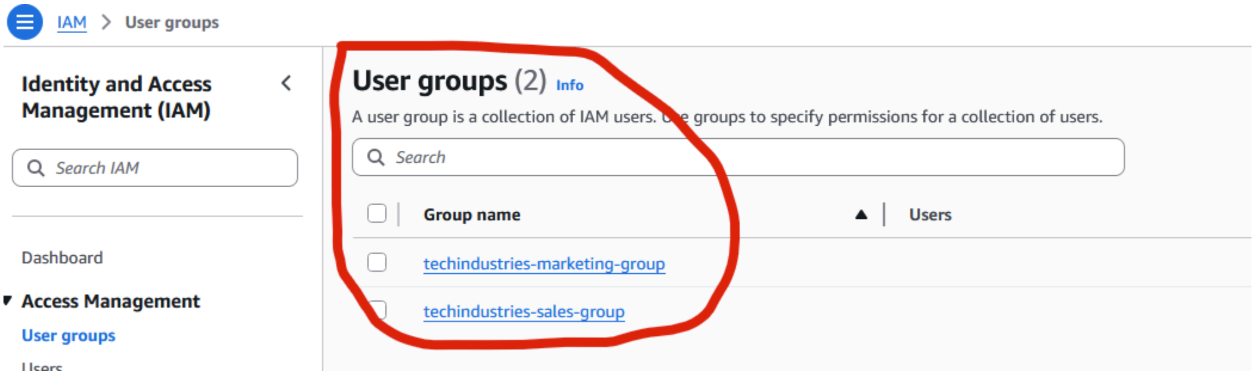
IAM users and groups were created to enforce role-based access control (RBAC). Users were assigned to groups based on job function, ensuring separation of duties and least privilege.



Users (3)

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
marketing-user-1	/	1	✓ 9 minutes ago	-	✓ 6 days	✓ 9 minutes ago
sales-user-1	/	1	✓ 6 days ago	-	✓ 6 days	✓ 6 days ago
TechIndustries-IAM-Admin	/	0	✓ 5 minutes ago	Virtual...	✓ 6 minutes	✓ 5 minutes ago



User groups (2)

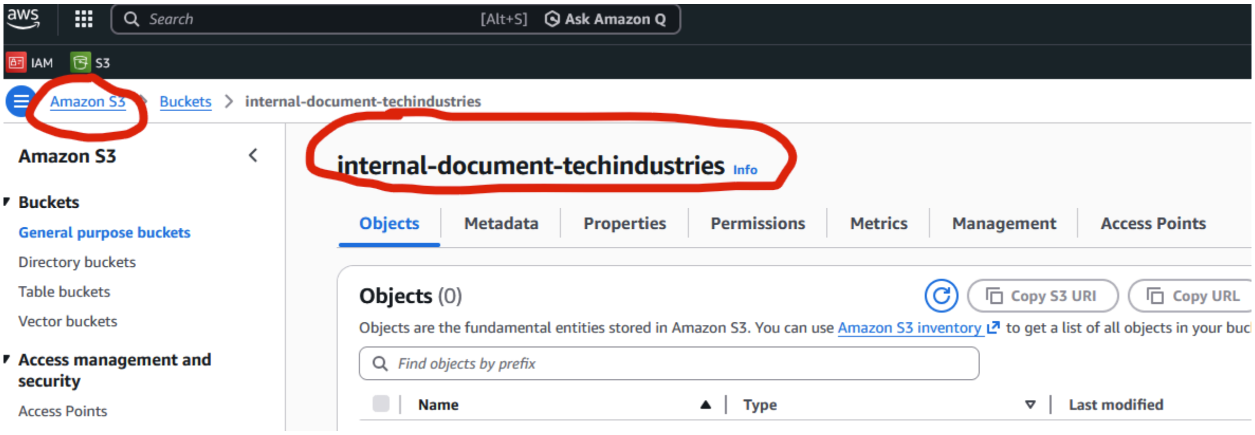
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users
techindustries-marketing-group	
techindustries-sales-group	

Object Storage Security (Amazon S3)

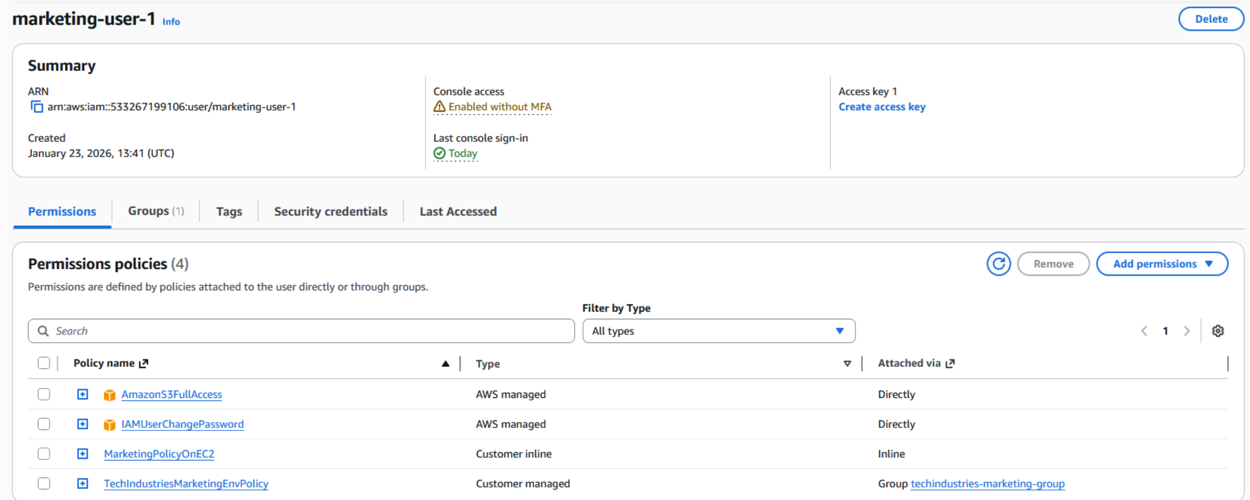
ISO 27001 A.8.2 | NIST CSF PR.DS | CIS Control 3

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.



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 buc



Summary

ARN
arn:aws:iam::533267199106:user/marketing-user-1

Created
January 23, 2026, 13:41 (UTC)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
Create access key

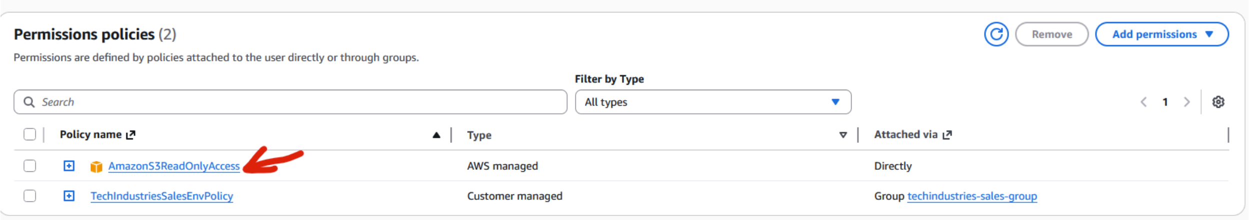
Permissions policies (4)

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
□	IAMUserChangePassword	AWS managed	Directly
□	MarketingPolicyOnEC2	Customer inline	Inline
□	TechIndustriesMarketingEnvPolicy	Customer managed	Group techindustries-marketing-group

Full Access for Marketing users to S3 Bucket



Permissions policies (2)

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

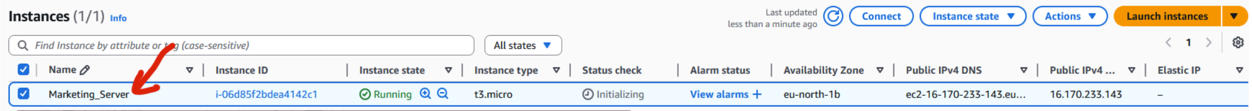
□	Policy name	Type	Attached via
□	AmazonS3ReadOnlyAccess	AWS managed	Directly
□	TechIndustriesSalesEnvPolicy	Customer managed	Group techindustries-sales-group

Read access for Sales users to S3 Bucket

Compute Resource Access Control (EC2)

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

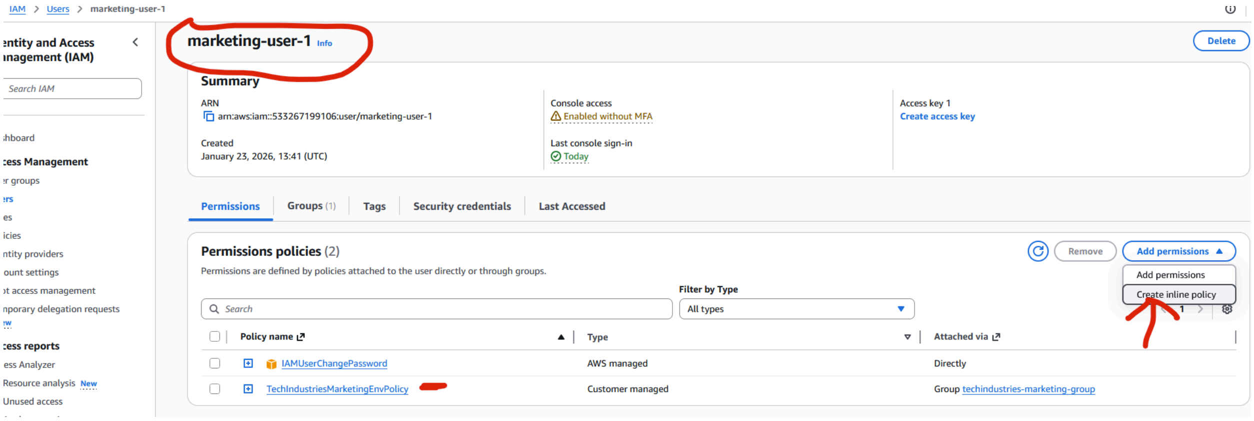
An EC2 instance was deployed to simulate an ec2 marketing server. Inline IAM policies were used to explicitly deny high-risk administrative actions such as instance termination and key pair creation for selected users. Policy enforcement was verified through controlled testing.



Instances (1/1) Info

Last updated less than a minute ago

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☑	Marketing_Server	i-06d85f2bdea4142c1	Running	t3.micro	Initializing	View alarms +	eu-north-1b	ec2-16-170-233-143.eu...	16.170.233.143	–



IAM > Users > marketing-user-1

marketing-user-1 Info

Summary

ARN
arn:aws:iam::533267199106:user/marketing-user-1

Created
January 23, 2026, 13:41 (UTC)

Console access
Enabled without MFA

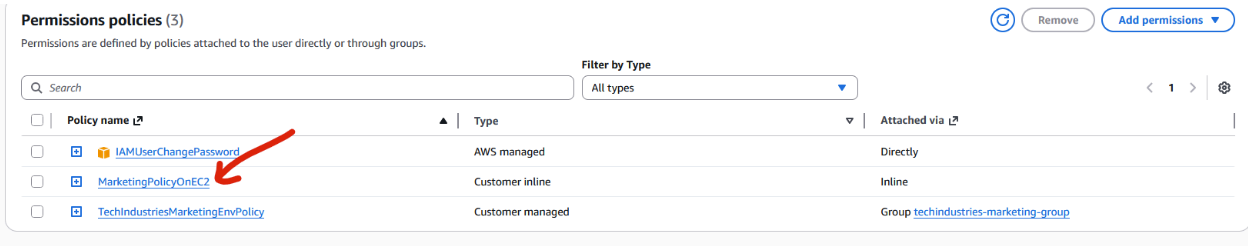
Last console sign-in
Today

Access key 1
Create access key

Permissions policies (2)

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

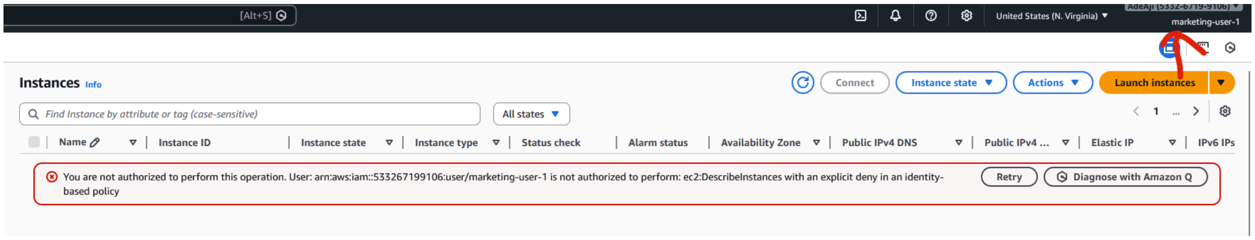
□	Policy name	Type	Attached via
□	IAMUserChangePassword	AWS managed	Directly
□	TechIndustriesMarketingEnvPolicy	Customer managed	Group techindustries-marketing-group



Permissions policies (3)

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

□	Policy name	Type	Attached via
□	IAMUserChangePassword	AWS managed	Directly
□	MarketingPolicyOnEC2	Customer inline	Inline
□	TechIndustriesMarketingEnvPolicy	Customer managed	Group techindustries-marketing-group


[Alt+S]
United States (N. Virginia) ▼
AdeAji (5332-6719-9106) ▼
marketing-user-1
Instances Info
Connect
Instance state ▼
Actions ▼
Launch instances ▼
Find Instance by attribute or tag (case-sensitive)
All states ▼
1 ...

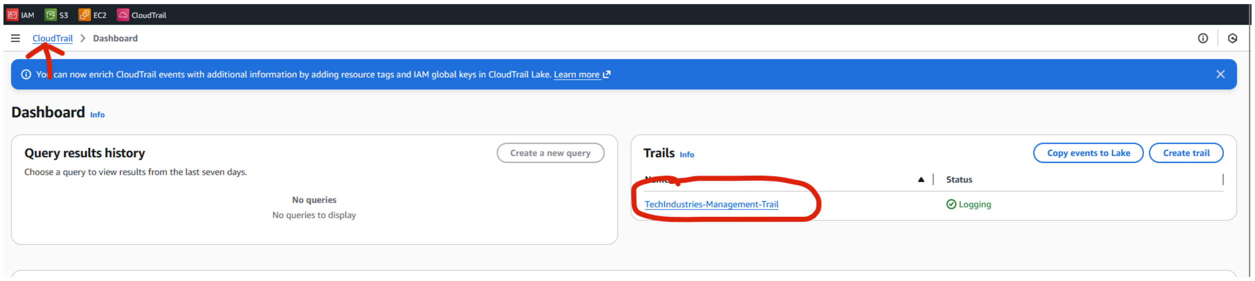
□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs

You are not authorized to perform this operation. User: arn:aws:iam::533267199106:user/marketing-user-1 is not authorized to perform: ec2:DescribeInstances with an explicit deny in an identity-based policy

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

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

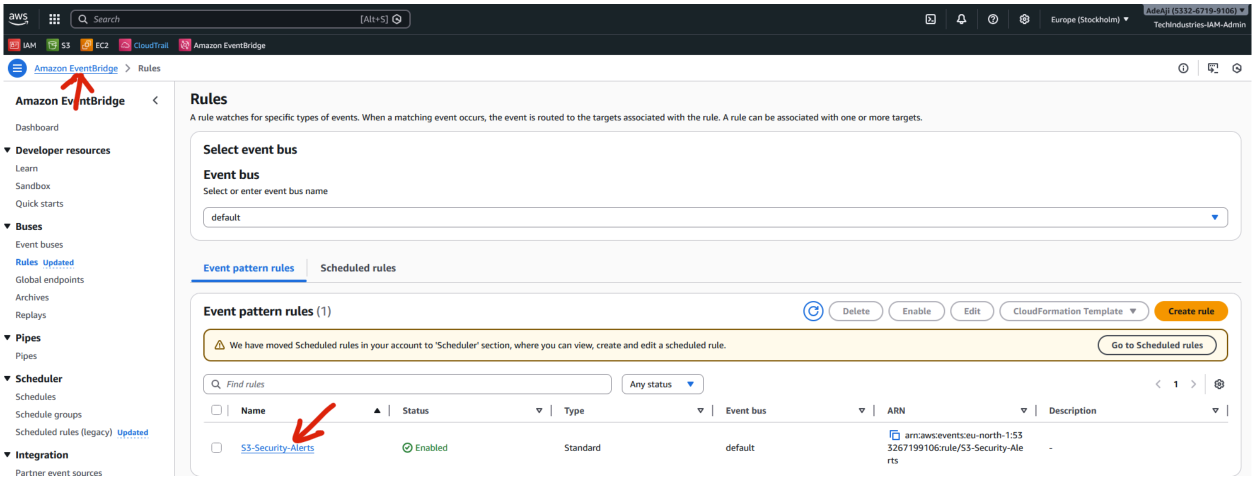
No queries
No queries to display

Name ▲	Status
TechIndustries-Management-Trail	✓ Logging

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

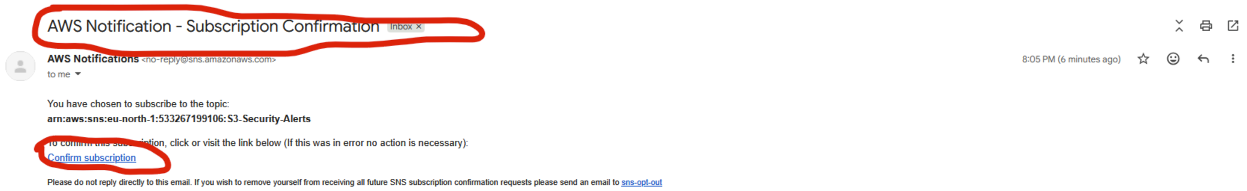
Select or enter event bus name

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-north-1:533267199106:rule/S3-Security-Alerts	-



AWS Notification - Subscription Confirmation

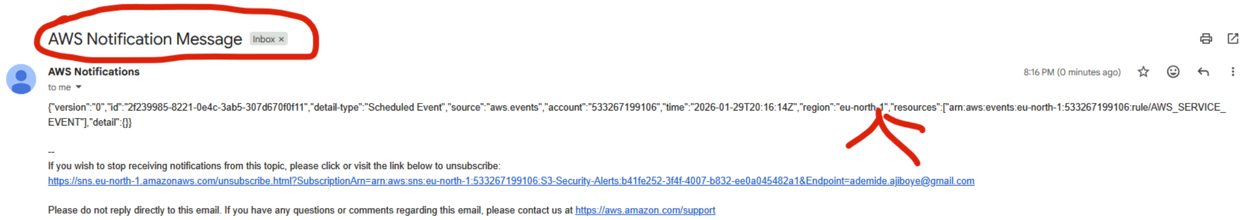
AWS Notifications <no-reply@sns.amazonaws.com>
to me

8:05 PM (6 minutes ago)

You have chosen to subscribe to the topic:
arn:aws:sns:eu-north-1:533267199106:S3-Security-Alerts

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
to me

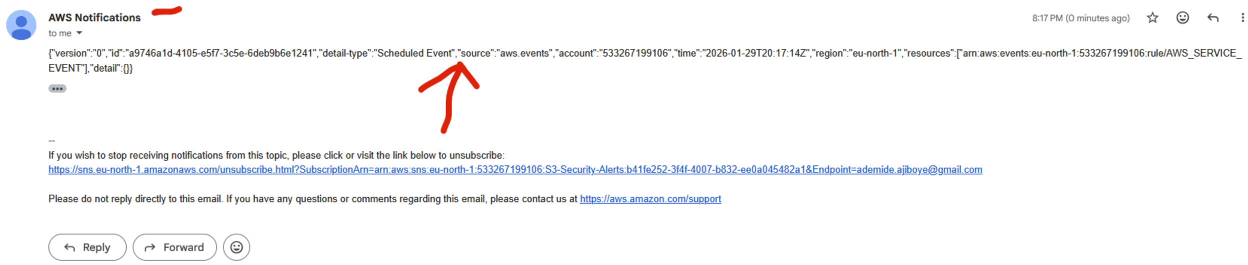
8:16 PM (0 minutes ago)

```
{"version":"0","id":"2f239985-8221-0e4c-3ab5-307d670f0f11","detail-type":"Scheduled Event","source":"aws.events","account":"533267199106","time":"2026-01-29T20:16:14Z","region":"eu-north-1","resources":["arn:aws:events:eu-north-1:533267199106:rule/AWS_SERVICE_EVENT"],"detail":{}}
```

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.eu-north-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:eu-north-1:533267199106:S3-Security-Alerts:b41fe252-3f4f-4007-b832-ee0a045482a1&Endpoint=ademide.ajiboye@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

Uploaded a file to InternalDocument (S3 bucket)



AWS Notifications
to me

8:17 PM (0 minutes ago)

```
{"version":"0","id":"a9746a1d-4105-e5f7-3c5e-6deb9b6e1241","detail-type":"Scheduled Event","source":"aws.events","account":"533267199106","time":"2026-01-29T20:17:14Z","region":"eu-north-1","resources":["arn:aws:events:eu-north-1:533267199106:rule/AWS_SERVICE_EVENT"],"detail":{}}
```

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.eu-north-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:eu-north-1:533267199106:S3-Security-Alerts:b41fe252-3f4f-4007-b832-ee0a045482a1&Endpoint=ademide.ajiboye@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

Delete the file in the S3 bucket

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 use.