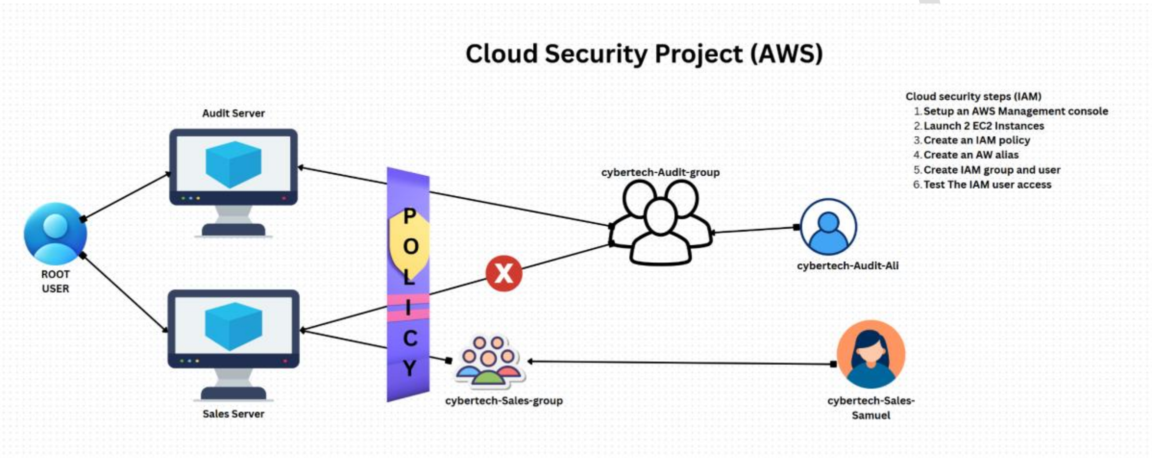
AWS IAM Cloud Security Project

1. Project Overview

I completed this project on cloud security controls in Amazon Web Services (AWS), focusing on Identity and Access Management (IAM). The goal was to create a least-privilege policy, attach it to a user group, and verify that the policy correctly restricts actions on two Amazon EC2 instances (audit and sales). I created S3 bucket, denied access from one IAM user-Audit to delete bucket, bucket policy and allowed access from the IAM user after IAM permissions was updated by Admin.


Cloud Security Project (AWS)
Cloud security steps (IAM)
1. Setup an AWS Management console
2. Launch 2 EC2 Instances
3. Create an IAM policy
4. Create an AW alias
5. Create IAM group and user
6. Test The IAM user access
Audit Server
ROOT USER
Sales Server
POLICY
cybertech-Audit-group
cybertech-Audit-Ali
cybertech-Sales-group
cybertech-Sales-Samuel

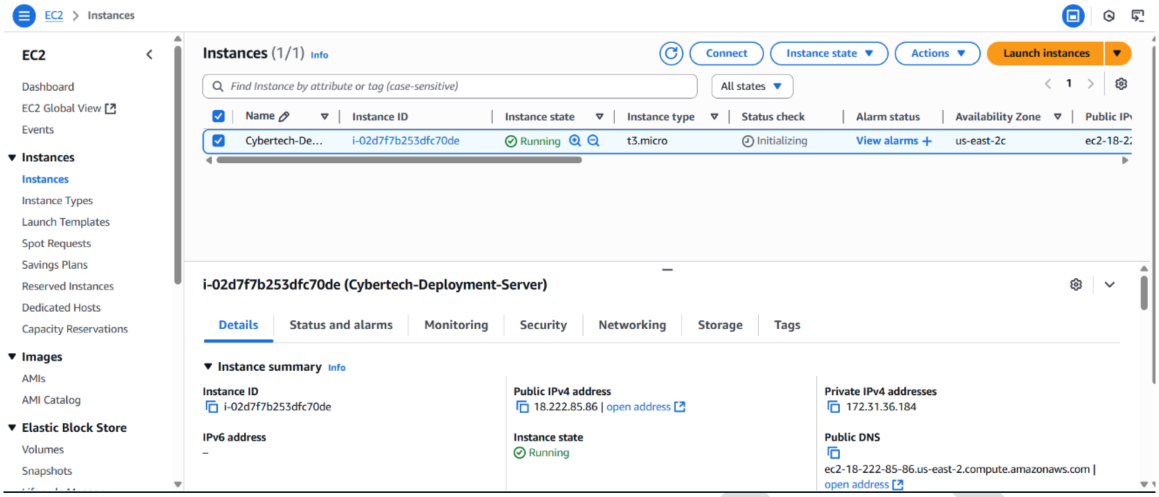
2. Tools & Concepts

- AWS IAM – users, groups, policies, account alias
- Amazon EC2 – instance tagging and lifecycle actions
- JSON policy syntax – Effect, Action, Resource
- Principle of least privilege and policy testing
- S3 Bucket- Storage
- Cloud Trail- Event Management

3. Tagging Strategy

I applied a descriptive tag to each EC2 instance:

Instance	Tag Key	Tag Value
audit	Environment	Audit
sales	Environment	Sales



Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
Cybertech-De…	i-02d7f7b253dfc70de	Running	t3.micro	Initializing	View alarms +	us-east-2c	ec2-18-2

i-02d7f7b253dfc70de (Cybertech-Deployment-Server)

Instance summary Info

Instance ID
i-02d7f7b253dfc70de

Public IPv4 address
18.222.85.86 | open address

Private IPv4 addresses
172.31.36.184

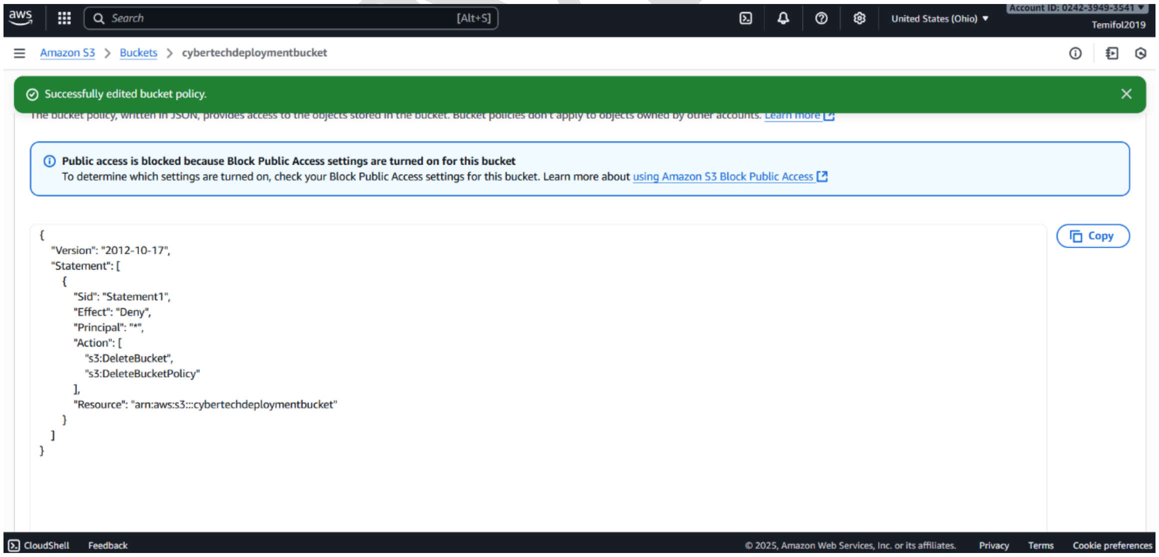
IPv6 address
–

Instance state
Running

Public DNS
ec2-18-222-85-86.us-east-2.compute.amazonaws.com | open address

4. Creating the IAM Policy

I authored the following JSON policy to deny access from all IAM users-Audit & Sales, for delete bucket, delete bucket policy from S3/start actions on the audit & sales servers.


aws
Search [Alt+S]
United States (Ohio)
Account ID: 0242-3949-3541
Temifol2019
Amazon S3 > Buckets > cybertechdeploymentbucket
Copy
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Successfully edited bucket policy.

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

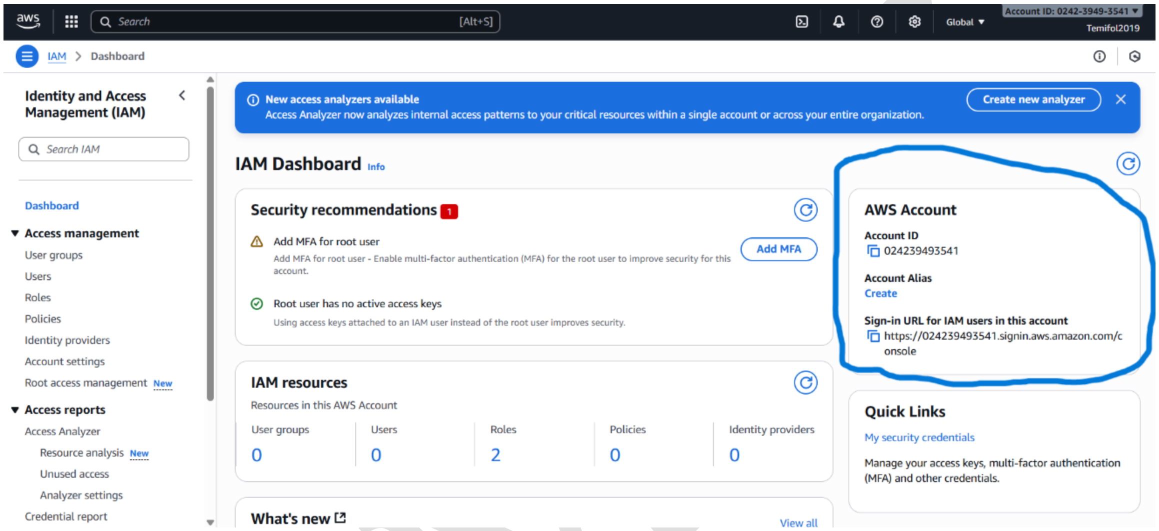
Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::cybertechdeploymentbucket"
    }
  ]
}
```

I log in as an IAM USER

5. Account Alias

I set a memorable account alias to replace the default numeric URL, making sign-in easier for team members.



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

Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve 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
0	0	2	0	0

What's new

AWS Account

Account ID
024239493541

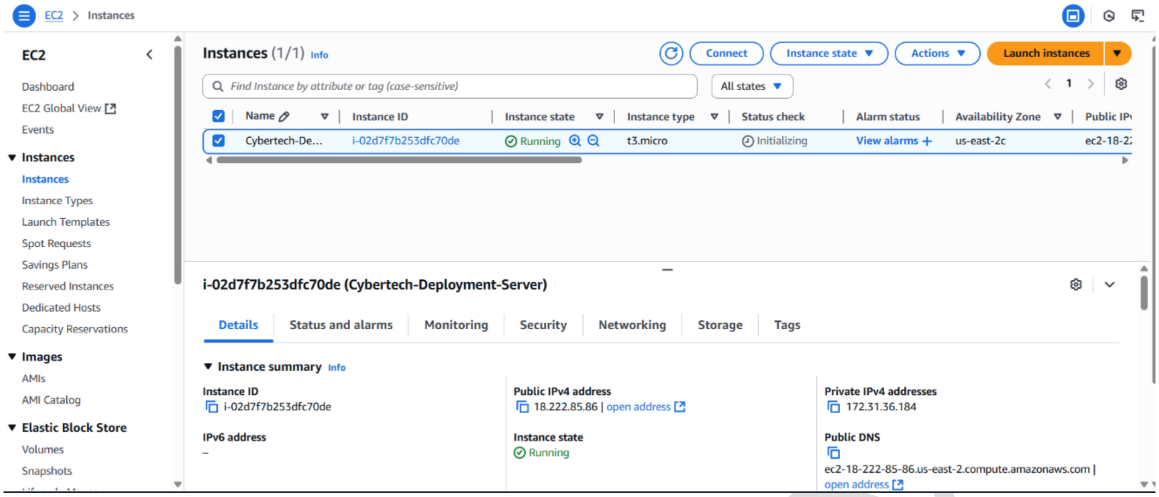
Account Alias
Create

Sign-in URL for IAM users in this account
https://024239493541.signin.aws.amazon.com/console

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

6. IAM Users & Groups

1. Created an IAM user group called Developers.
2. Attached the **CybertechAuditEnvPolicy** policy to the group.
3. Added individual IAM users who require controlled EC2 access.



Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
☑	Cybertech-De...	i-02d7f7b253dfc70de	Running	t3.micro	Initializing	View alarms +	us-east-2c	ec2-18-2

i-02d7f7b253dfc70de (Cybertech-Deployment-Server)

Instance summary Info

Instance ID
i-02d7f7b253dfc70de

Public IPv4 address
18.222.85.86 | open address

Private IPv4 addresses
172.31.36.184

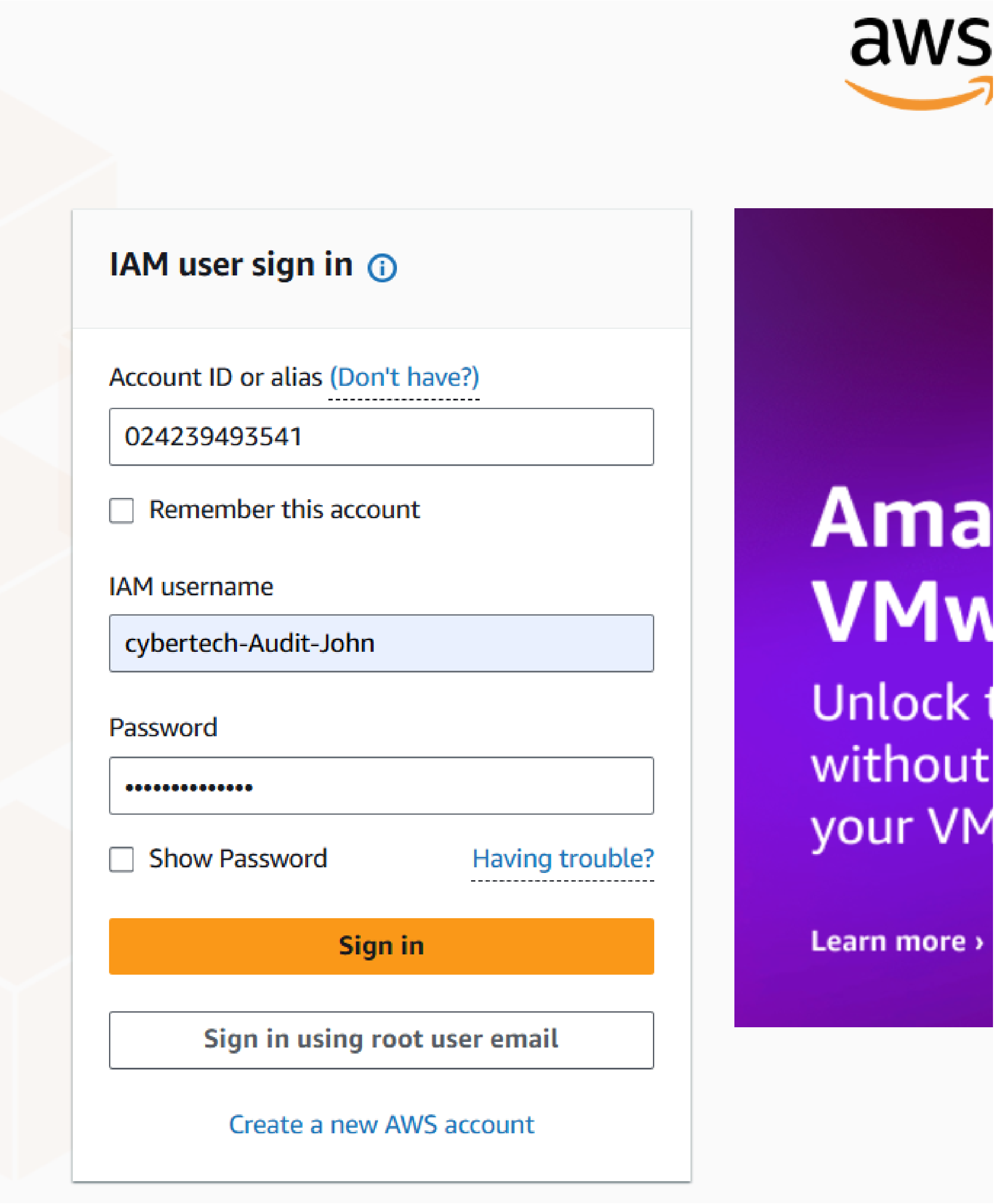
IPv6 address
–

Instance state
Running

Public DNS
ec2-18-222-85-86.us-east-2.compute.amazonaws.com | open address

7. Logging in as an IAM User

IAM users can sign in through:
- AWS Management Console (using the new alias URL)
- AWS CLI via programmatic keys



IAM user sign in

Account ID or alias (Don't have?)

024239493541

□ Remember this account

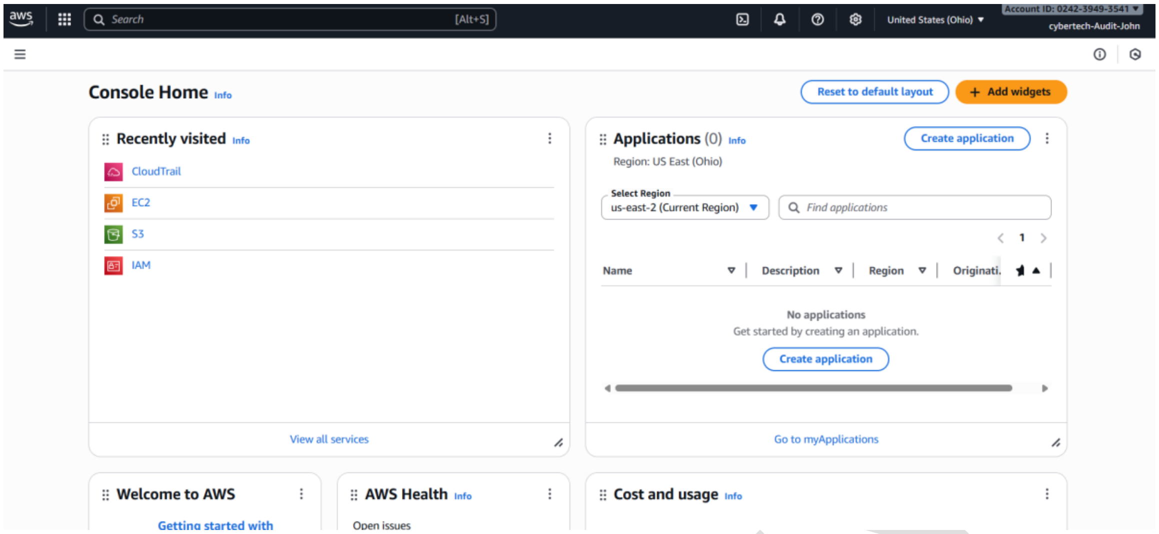
IAM username

cybertech-Audit-John

Password

••••••••••••••

□ Show Password



Console Home Info

Recently visited Info

- CloudTrail
- EC2
- S3
- IAM

Applications (0) Info

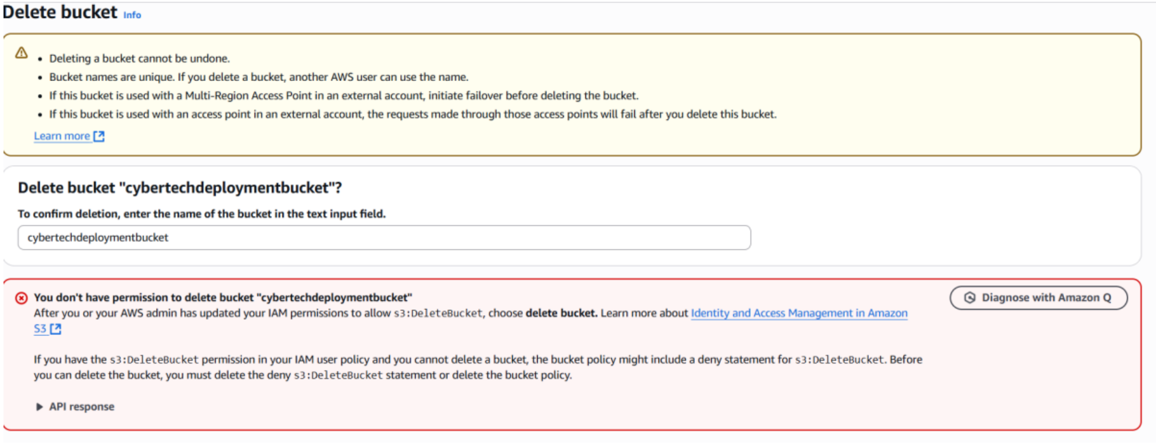
Region: US East (Ohio)

Name	Description	Region	Originati.

No applications
Get started by creating an application.

8. Testing the Policy

Test	Action	Expected	Result	Actual Result
Stop	S3 Bucket-IAM users (Audit & Sales)	Denied	Delete bucket & bucket policy	Denied error displayed
Start	User IAM permissions updated- Admin	Allowed	Delete bucket & policy	Bucket was deleted successfully



Delete bucket Info

- Deleting a bucket cannot be undone.
- Bucket names are unique. If you delete a bucket, another AWS user can use the name.
- If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
- If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.

Delete bucket "cybertechdeploymentbucket"?

To confirm deletion, enter the name of the bucket in the text input field.

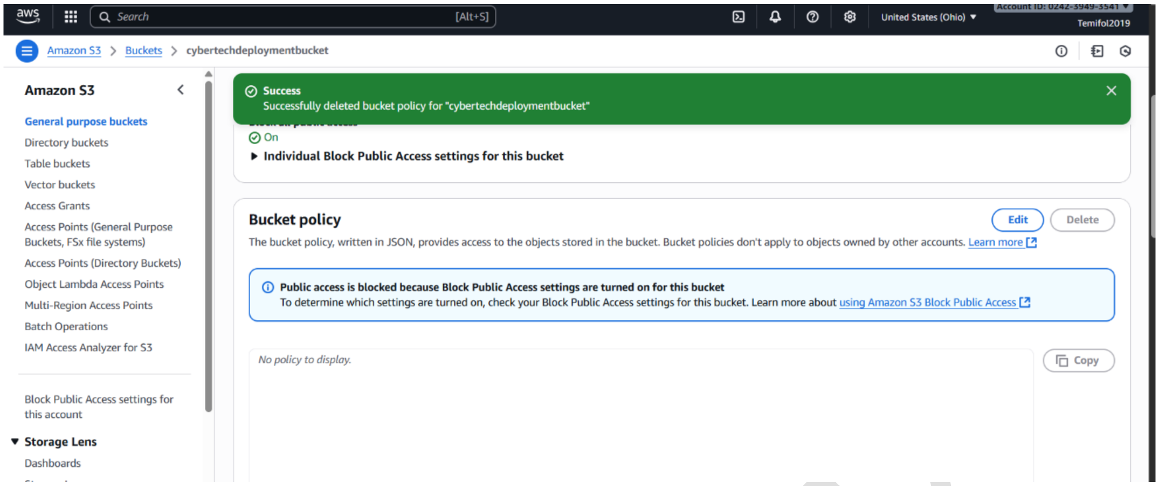
cybertechdeploymentbucket

You don't have permission to delete bucket "cybertechdeploymentbucket"

After you or your AWS admin has updated your IAM permissions to allow s3:DeleteBucket, choose **delete bucket.** Learn more about Identity and Access Management in Amazon S3

If you have the s3:DeleteBucket permission in your IAM user policy and you cannot delete a bucket, the bucket policy might include a deny statement for s3:DeleteBucket. Before you can delete the bucket, you must delete the deny s3:DeleteBucket statement or delete the bucket policy.

Admin log in to update the IAM Permissions


aws
Search [Alt+S]
United States (Ohio)
Account ID: 0242-3949-3541
Temifol2019
Amazon S3 > Buckets > cybertechdeploymentbucket
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Vector buckets
Access Grants
Access Points (General Purpose Buckets, FSx file systems)
Access Points (Directory Buckets)
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Edit
Delete
Copy

Success
Successfully deleted bucket policy for "cybertechdeploymentbucket"

On

Individual Block Public Access settings for this bucket

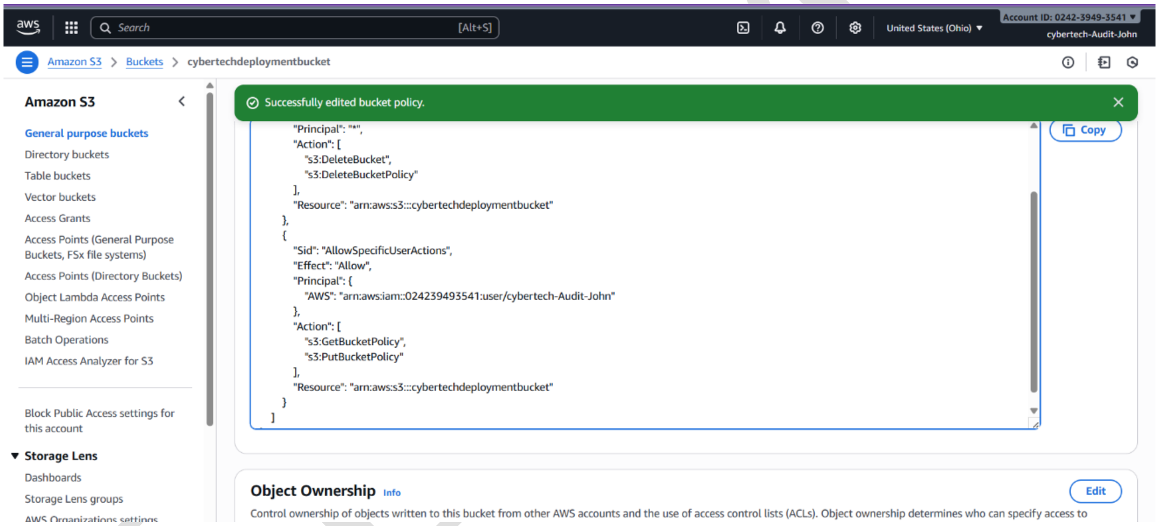
Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

No policy to display.

IAM Users allowed permission to delete Bucket

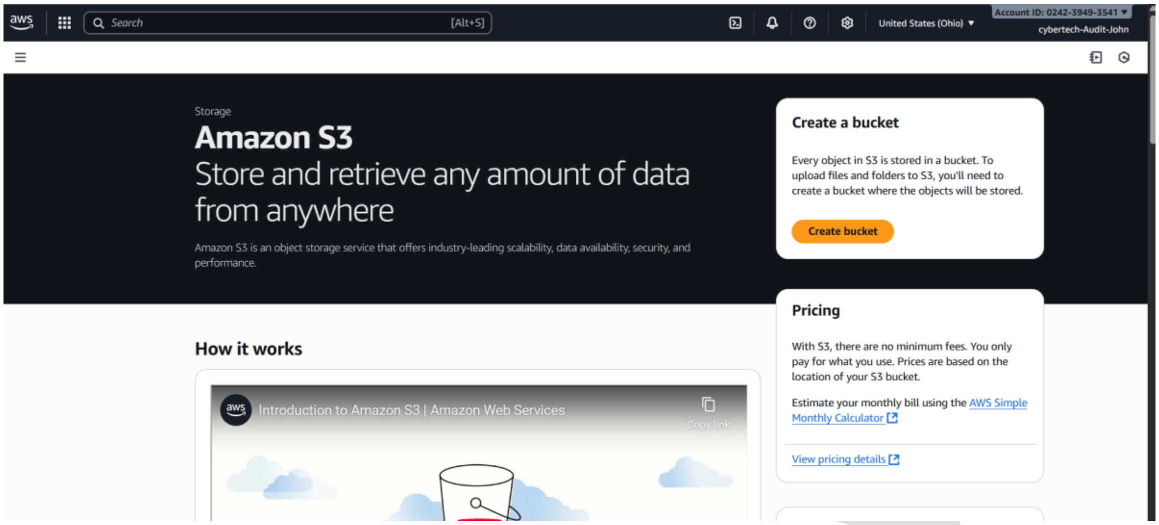

aws
Search [Alt+S]
United States (Ohio)
Account ID: 0242-3949-3541
cybertech-Audit-John
Amazon S3 > Buckets > cybertechdeploymentbucket
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Vector buckets
Access Grants
Access Points (General Purpose Buckets, FSx file systems)
Access Points (Directory Buckets)
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Copy
Edit
Info

Successfully edited bucket policy.

```
      "Principal": "*",
      "Action": [
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::cybertechdeploymentbucket"
    },
    {
      "Sid": "AllowSpecificUserActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::024239493541:user/cybertech-Audit-John"
      },
      "Action": [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::cybertechdeploymentbucket"
    }
  ]
```

Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to



Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

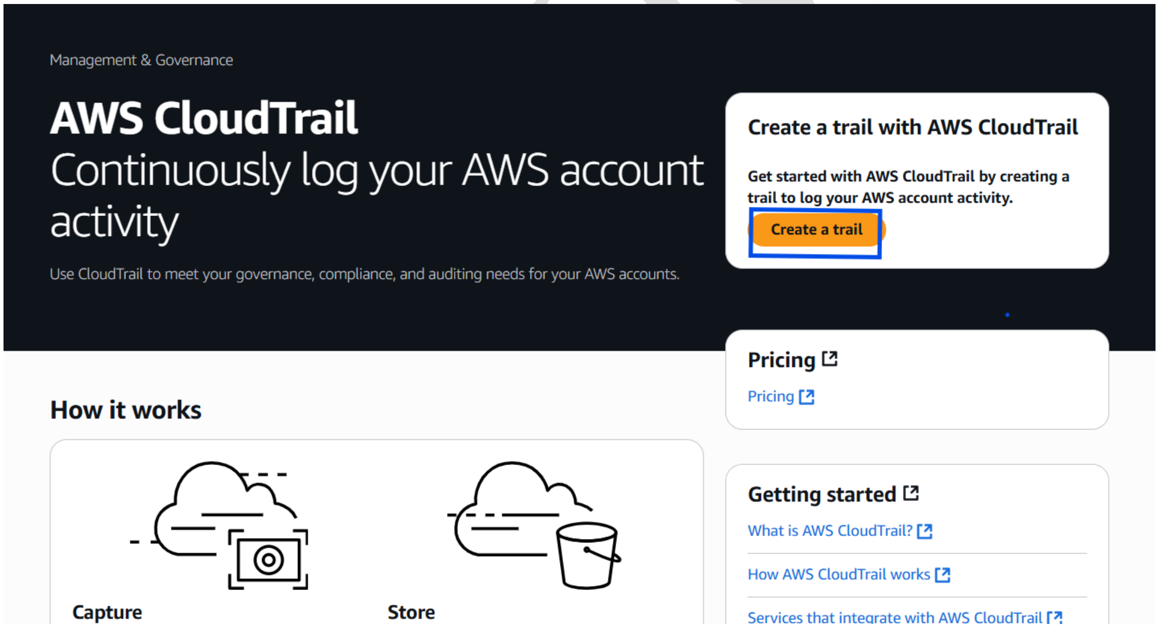
Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

How it works

9. Cloud Trail-Event management

See the steps below:



Management & Governance

AWS CloudTrail

Continuously log your AWS account activity

Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.

Create a trail with AWS CloudTrail

Get started with AWS CloudTrail by creating a trail to log your AWS account activity.

Pricing

Pricing

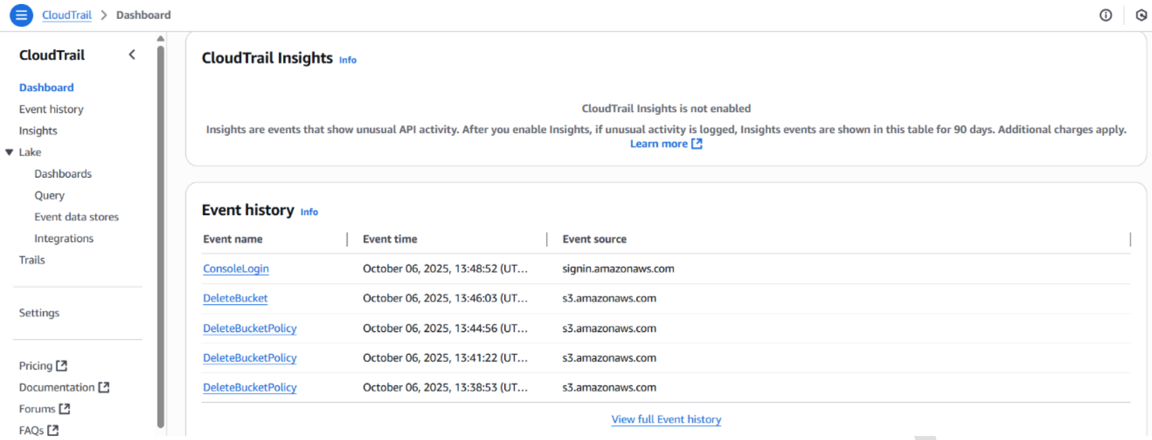
How it works

Getting started

What is AWS CloudTrail?

How AWS CloudTrail works

Services that integrate with AWS CloudTrail



CloudTrail Insights Info

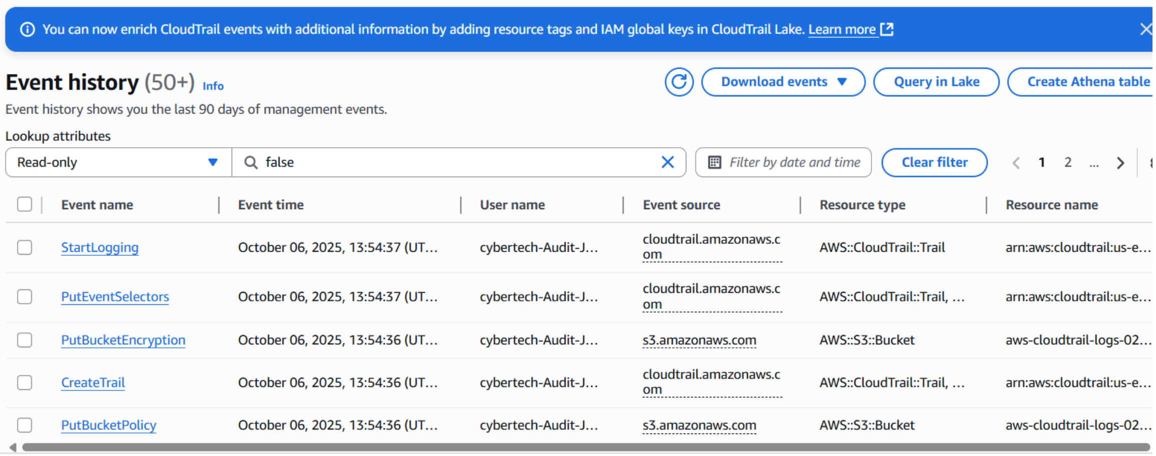
CloudTrail Insights is not enabled

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	October 06, 2025, 13:48:52 (UT...	signin.amazonaws.com
DeleteBucket	October 06, 2025, 13:46:03 (UT...	s3.amazonaws.com
DeleteBucketPolicy	October 06, 2025, 13:44:56 (UT...	s3.amazonaws.com
DeleteBucketPolicy	October 06, 2025, 13:41:22 (UT...	s3.amazonaws.com
DeleteBucketPolicy	October 06, 2025, 13:38:53 (UT...	s3.amazonaws.com

View full Event history



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

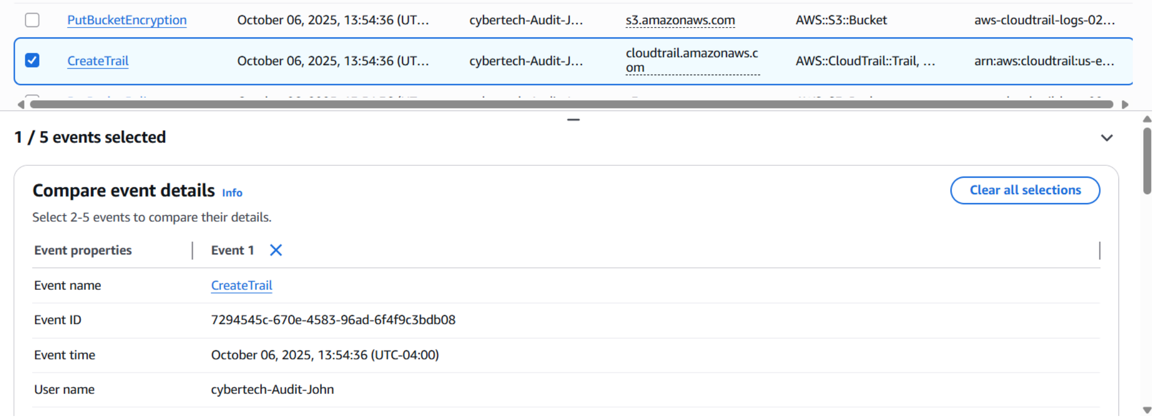
Event history (50+) Info

Event history shows you the last 90 days of management events.

Lookup attributes

Read-only | false

	Event name	Event time	User name	Event source	Resource type	Resource name
□	StartLogging	October 06, 2025, 13:54:37 (UT...	cybertech-Audit-J...	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-e...
□	PutEventSelectors	October 06, 2025, 13:54:37 (UT...	cybertech-Audit-J...	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail, ...	arn:aws:cloudtrail:us-e...
□	PutBucketEncryption	October 06, 2025, 13:54:36 (UT...	cybertech-Audit-J...	s3.amazonaws.com	AWS::S3::Bucket	aws-cloudtrail-logs-02...
□	CreateTrail	October 06, 2025, 13:54:36 (UT...	cybertech-Audit-J...	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail, ...	arn:aws:cloudtrail:us-e...
□	PutBucketPolicy	October 06, 2025, 13:54:36 (UT...	cybertech-Audit-J...	s3.amazonaws.com	AWS::S3::Bucket	aws-cloudtrail-logs-02...



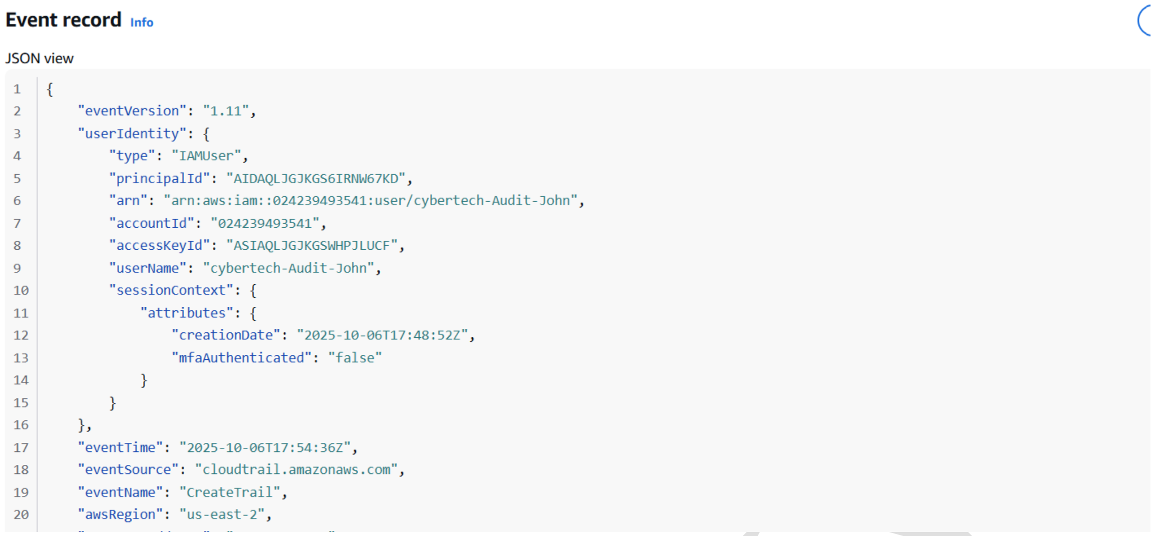
□	PutBucketEncryption	October 06, 2025, 13:54:36 (UT...	cybertech-Audit-J...	s3.amazonaws.com	AWS::S3::Bucket	aws-cloudtrail-logs-02...
☑	CreateTrail	October 06, 2025, 13:54:36 (UT...	cybertech-Audit-J...	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail, ...	arn:aws:cloudtrail:us-e...

1 / 5 events selected

Compare event details Info

Select 2-5 events to compare their details.

Event properties	Event 1
Event name	CreateTrail
Event ID	7294545c-670e-4583-96ad-6f4f9c3bdb08
Event time	October 06, 2025, 13:54:36 (UTC-04:00)
User name	cybertech-Audit-John

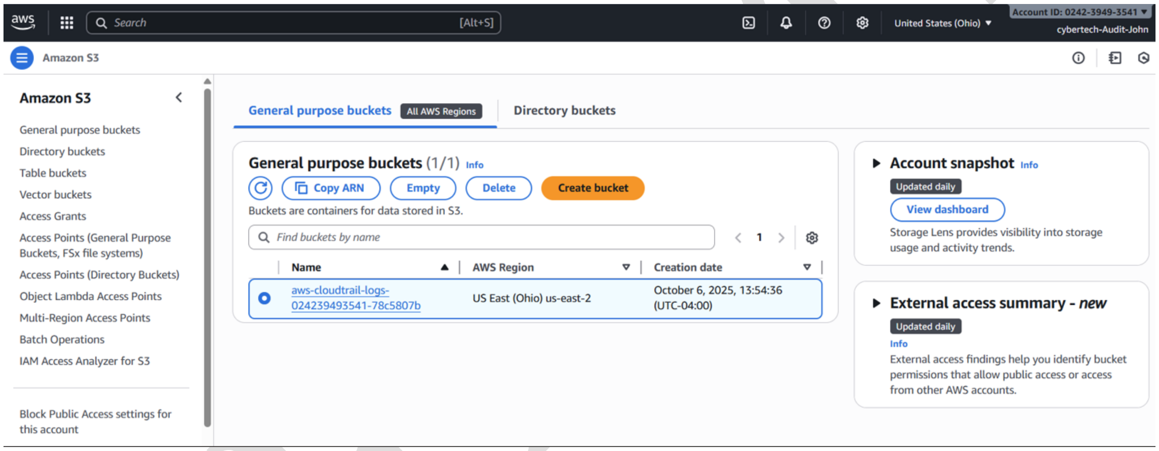


Event record Info

JSON view

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAQLJGJKGS6IRNW67KD",
        "arn": "arn:aws:iam::024239493541:user/cybertech-Audit-John",
        "accountId": "024239493541",
        "accessKeyId": "ASIAQLJGJKGSWHPJLUCF",
        "userName": "cybertech-Audit-John",
        "sessionContext": {
            "attributes": {
                "creationDate": "2025-10-06T17:48:52Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2025-10-06T17:54:36Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "CreateTrail",
    "awsRegion": "us-east-2",
```

Logs were automatically stored in the S3 Bucket following the Trail my trail creation.



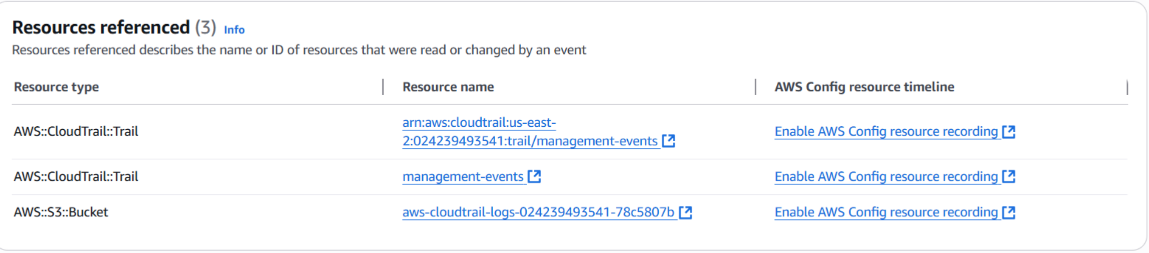
General purpose buckets (1/1) Info

Buckets are containers for data stored in S3.

	Name	AWS Region	Creation date
●	aws-cloudtrail-logs-024239493541-78c5807b	US East (Ohio) us-east-2	October 6, 2025, 13:54:36 (UTC-04:00)

Storage Lens provides visibility into storage usage and activity trends.

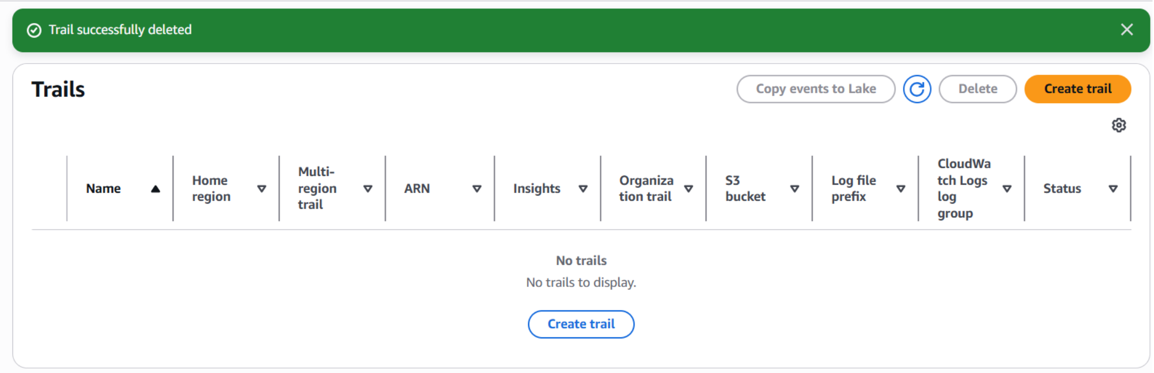
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.



Resources referenced (3) Info

Resources referenced describes the name or ID of resources that were read or changed by an event

Resource type	Resource name	AWS Config resource timeline
AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-2:024239493541:trail/management-events	Enable AWS Config resource recording
AWS::CloudTrail::Trail	management-events	Enable AWS Config resource recording
AWS::S3::Bucket	aws-cloudtrail-logs-024239493541-78c5807b	Enable AWS Config resource recording



Trail successfully deleted

Trails

	Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status

No trails

No trails to display.