SETTING UP IAM-IDENTITY ACCESS MANAGEMENT ON CLOUD

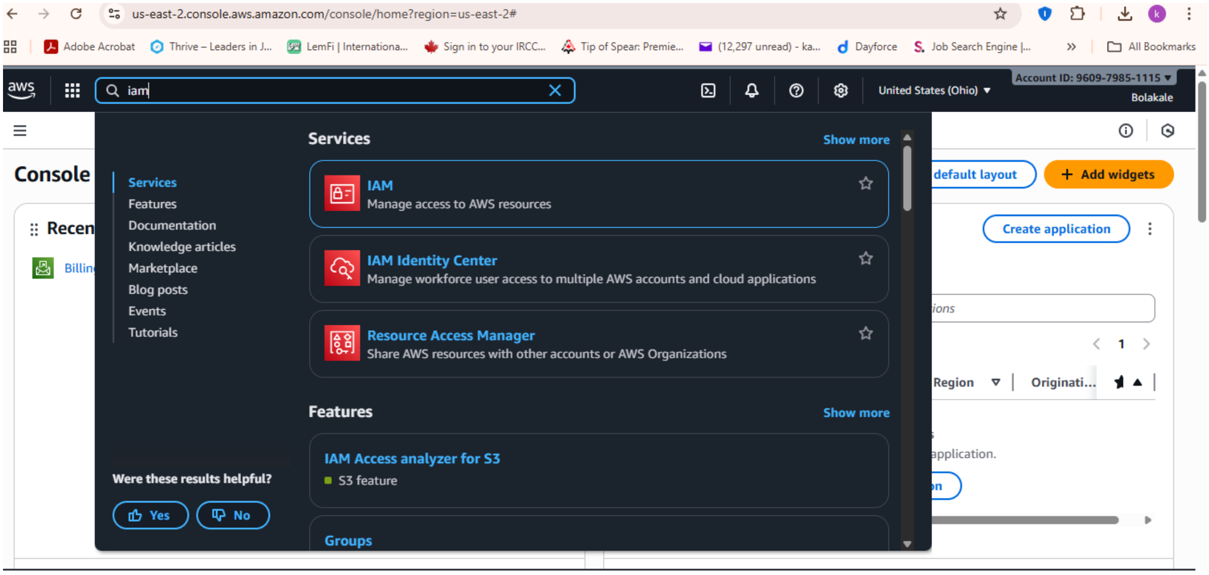
I recently completed a project where I deployed **AWS Identity and Access Management (IAM)** on the cloud, using **CYBERX** as the organization for implementation. When moving resources to the cloud, one of the first and most critical steps is controlling who can access what. That's precisely what IAM enables—it allows you to determine which people, systems, or applications can log in, what actions they are allowed to perform, and which areas should remain restricted.

During the project, I implemented key IAM best practices, including creating structured user accounts, defining precise roles, enabling multi-factor authentication, and enforcing the principle of least privilege. Properly setting up these controls is crucial because most security incidents occur when someone gains access they shouldn't have. By applying these measures, I significantly reduced potential security risks and ensured that access across CYBERX's cloud environment was secure, well-managed, and fully controlled.

This project reinforced the critical role of IAM as the foundation of cloud security. When structured correctly from the start, IAM makes all other cloud operations easier to manage, safer, and more controlled, providing CYBERX with a secure and scalable cloud infrastructure ready to support future growth.

THE FIRST PHASE IS:

- To sign up for AWS Platform
- Choose a location close to your customer or final user
- Create an IAM user to be given the **admin** privilege
- Go to the search bar and search for IAM service



us-east-2.console.aws.amazon.com/console/home?region=us-east-2#

Search: iam

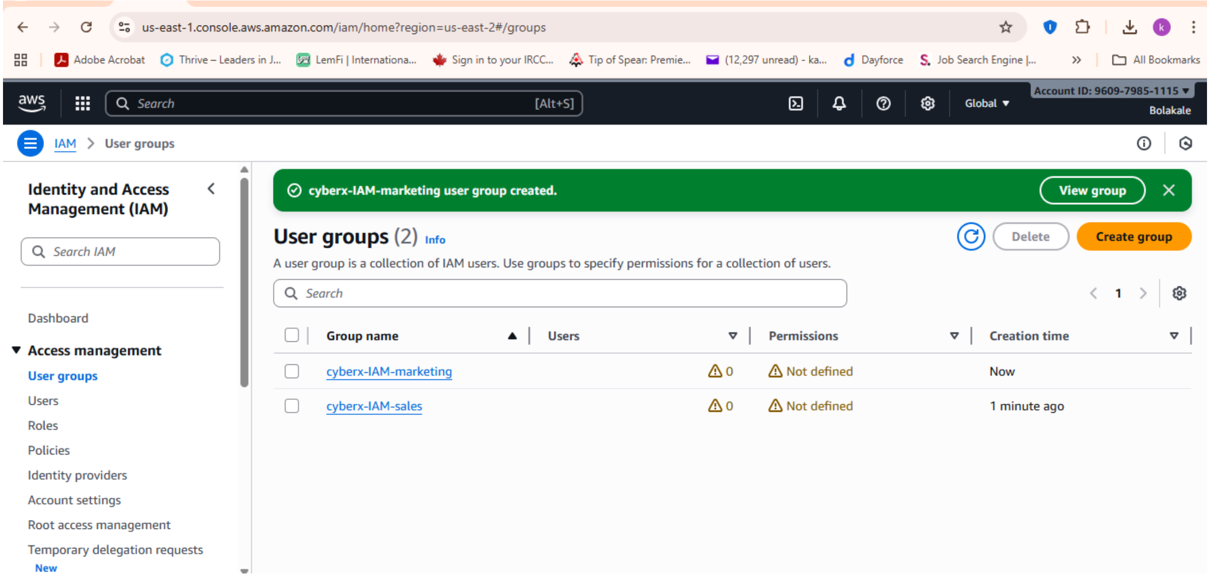
IAM — Manage access to AWS resources

IAM Identity Center — Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager — Share AWS resources with other accounts or AWS Organizations

IAM Access analyzer for S3 — S3 feature

After it loads you click on **USER GROUP** on the left-hand corner the click on **CREATE GROUP.** Name the group for example; **Cyberx -IAM-sales**, scroll down and click CREATE GROUP.



us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/groups

cyberx-IAM-marketing user group created.

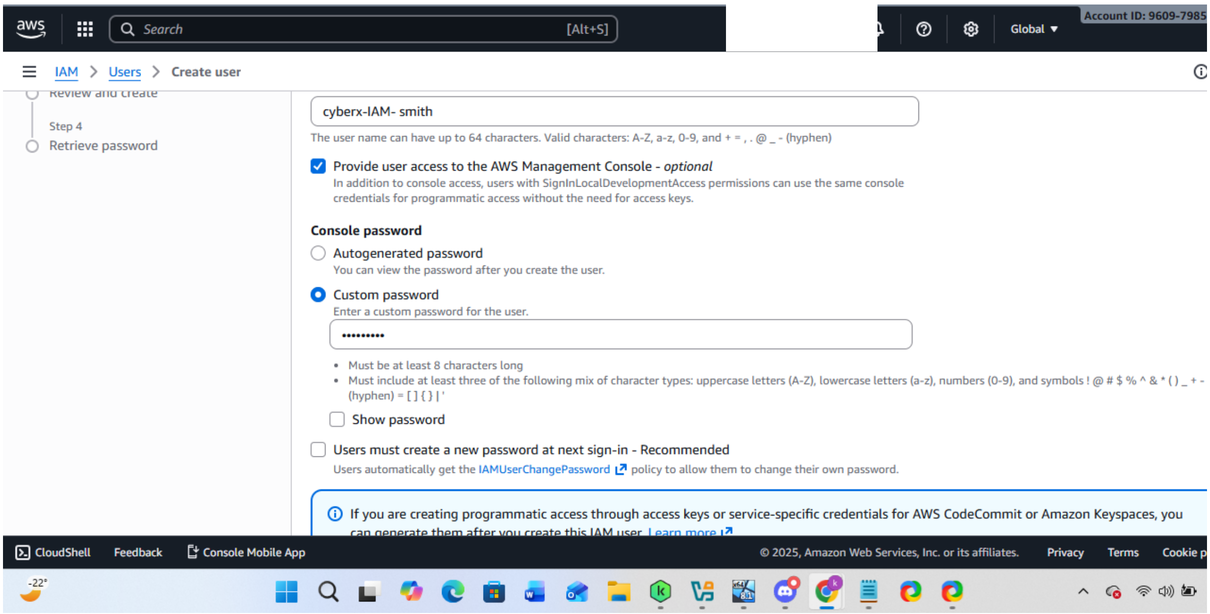
User groups (2)

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

Group name	Users	Permissions	Creation time
cyberx-IAM-marketing	⚠ 0	⚠ Not defined	Now
cyberx-IAM-sales	⚠ 0	⚠ Not defined	1 minute ago

NEXT STEP IS TO CREATE USERS:

- Click on **USER** on the left-hand side
- Click on **CREATE USER**
- Check the box **provide user access to the AWS Management Console- Optional**
- Create custom password and click on next.



IAM > Users > Create user

Review and create

Step 4
Retrieve password

cyberx-IAM- smith

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*
In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

Console password

○ Autogenerated password
You can view the password after you create the user.

● Custom password
Enter a custom password for the user.

•••••••••

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

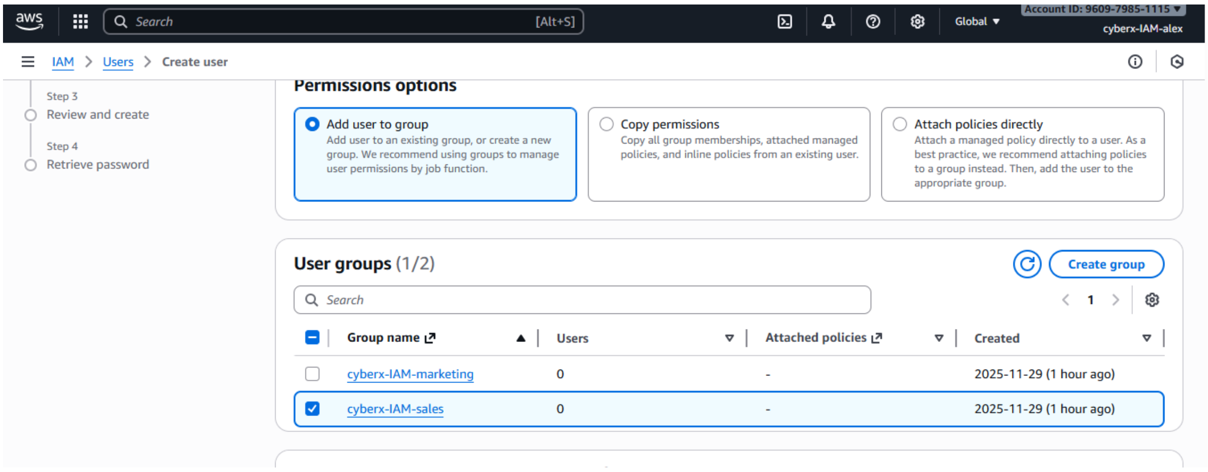
□ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

THE NEXT STEP IS TO SET PERMISSION AND CLICK NEXT

Set permission by clicking on **attach policies directly.**

- Create **user**, then copy the **URL link** and sign in with the new user login



IAM > Users > Create user

Step 3
Review and create

Step 4
Retrieve password

Permissions options

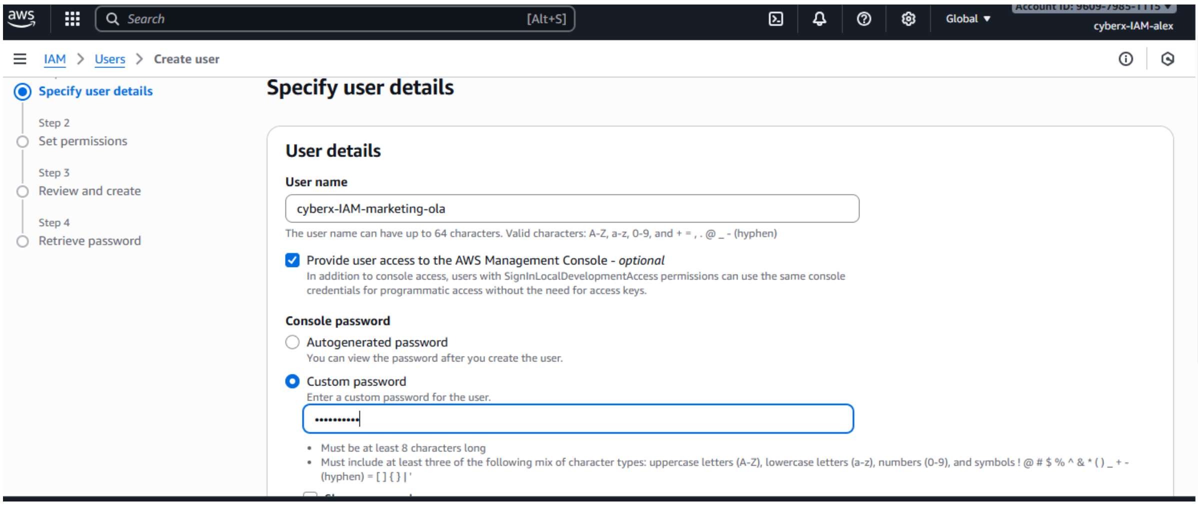
● Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/2)

	Group name	Users	Attached policies	Created
□	cyberx-IAM-marketing	0	-	2025-11-29 (1 hour ago)
☑	cyberx-IAM-sales	0	-	2025-11-29 (1 hour ago)



Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Specify user details

User details

User name

cyberx-IAM-marketing-ola

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*
In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

Console password

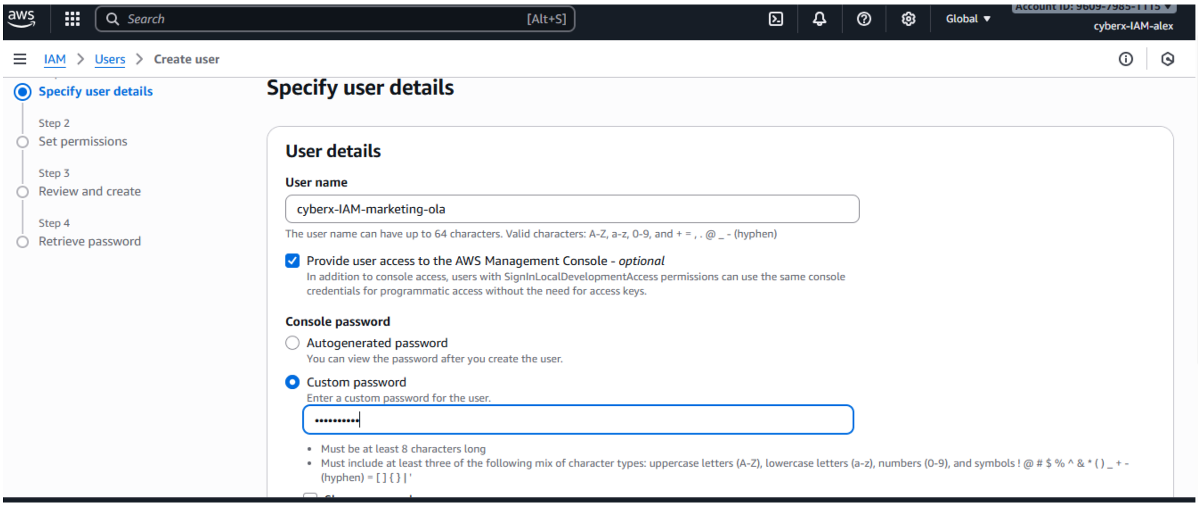
○ Autogenerated password
You can view the password after you create the user.

● Custom password
Enter a custom password for the user.

••••••••••

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

Note: We can create another user using the step used above, then put the user under one of the groups created- you have to check the box when you click on the **user group** you want to assign the new user and click next. (specify user detail).



Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Specify user details

User details

User name

cyberx-IAM-marketing-ola

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*
In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

Console password

○ Autogenerated password
You can view the password after you create the user.

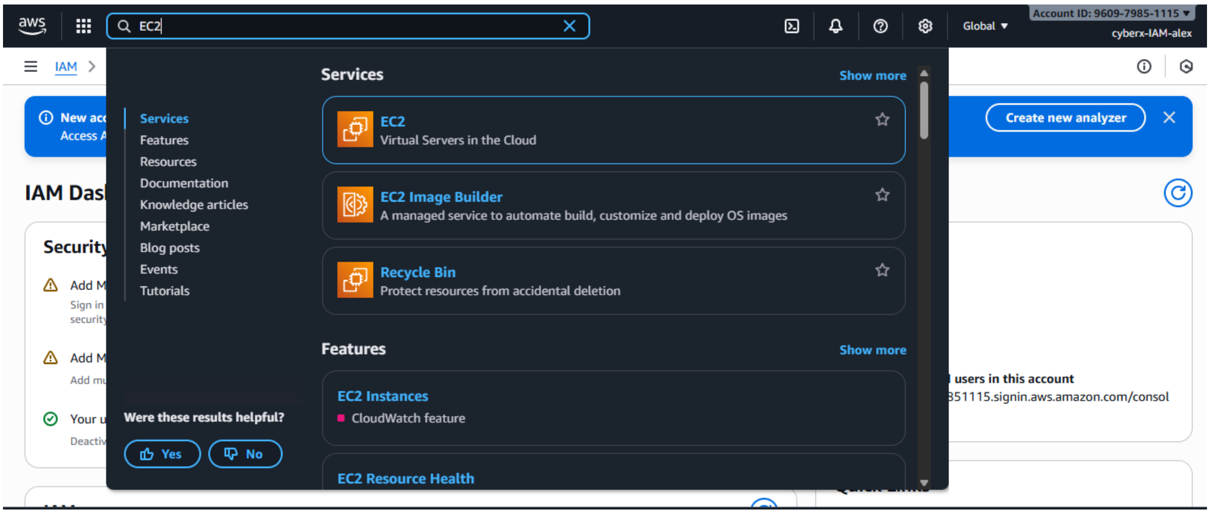
● Custom password
Enter a custom password for the user.

••••••••••

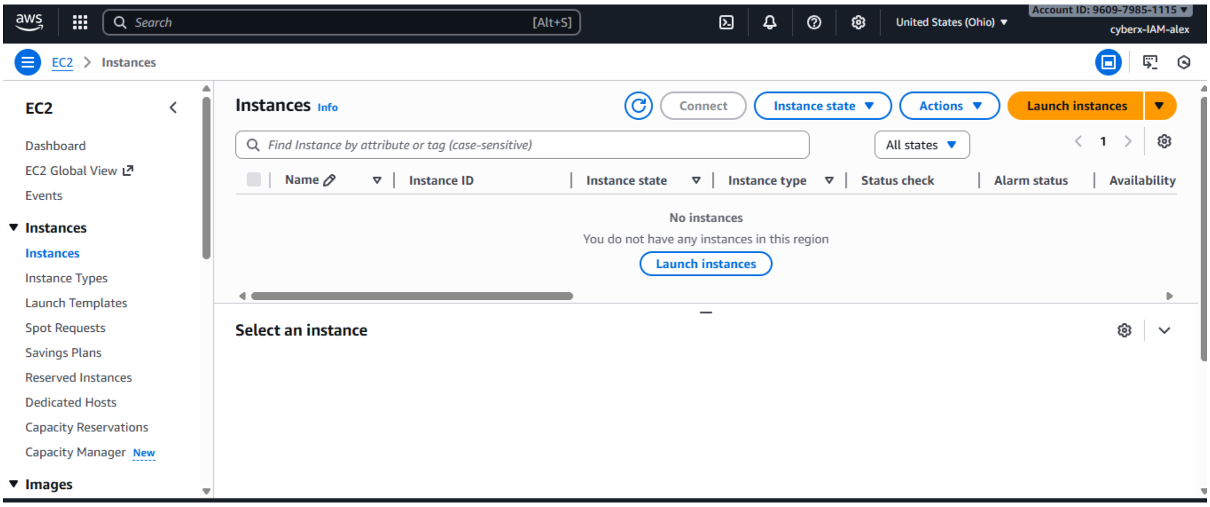
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

THE NEXT PHASE IS TO CREATE A SERVER WHERE WE PUSH PROJECT, WORK ON, DEPLOY IT:

- We are going to use another service on **AWS** to create and **INSTANCE** which is referred to server on the cloud platform.
- Go to the search bar on the **IAM** and search for **EC2** (Elastic Compute Cloud)



Click on **INSTANCES** on the right-hand corner.



Next is to name the **Instance** for example Sales-Server, select the Amazon Machine Image (AMI) and select instance type, the we move to selecting setting the key pair, give the create key pair a name: sales-server-key-pair.

(Note: ***Standard Practise***- when the key pair is downloaded should not be share through a different channel and stored in a separate place).

Move to network settings, click on **Allow SSH from** and choose **my IP** so you can access from **Command Line Interface** (CLI), then launch our instance.

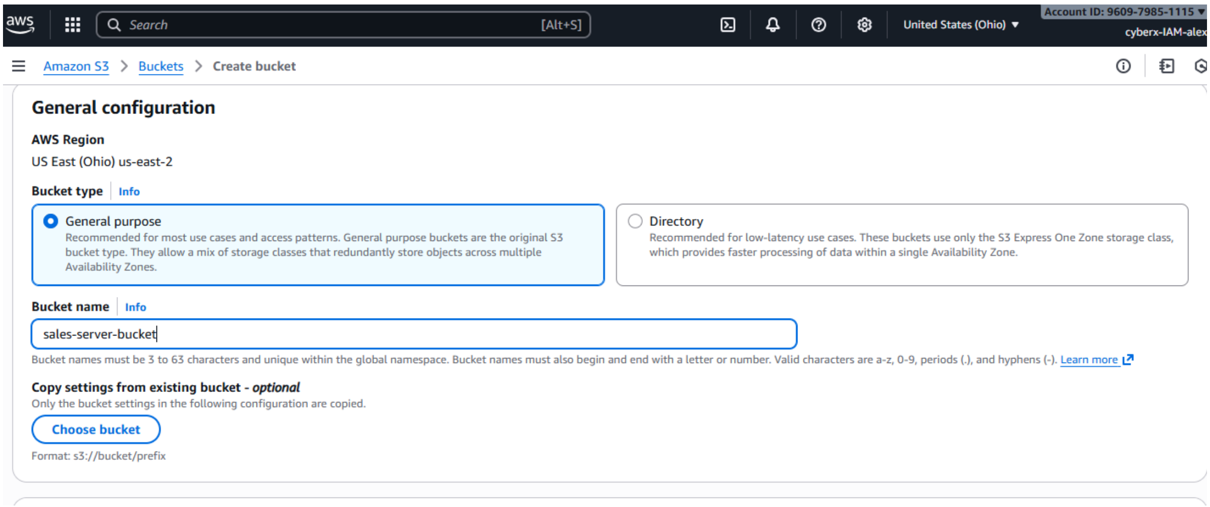
We can then use the same step to create another instance for marketing.

THE NEXT PHASE IS TO CREATE OUR BUCKET (STORAGE), USING A SERVICE CALLED S3:

- You will click on create bucket
- Choose general purpose
- Name the bucket- (Sales**-Server-Bucket**)

Note: (***Standard Practise****-* you are to **Enable Access** on object ownership but since we are using a free version of **AWS**, we will use the [ACLs DISABLE] Bucket versioning- DISABLE.

Then click – CREATE BUCKET.


aws
Search [Alt+S]
United States (Ohio) ▾
Account ID: 9609-7985-1115 ▾
cyberx-IAM-alex
Amazon S3 > Buckets > Create bucket

General configuration

AWS Region

US East (Ohio) us-east-2

Bucket type | Info

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

○ Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name | Info

sales-server-bucket

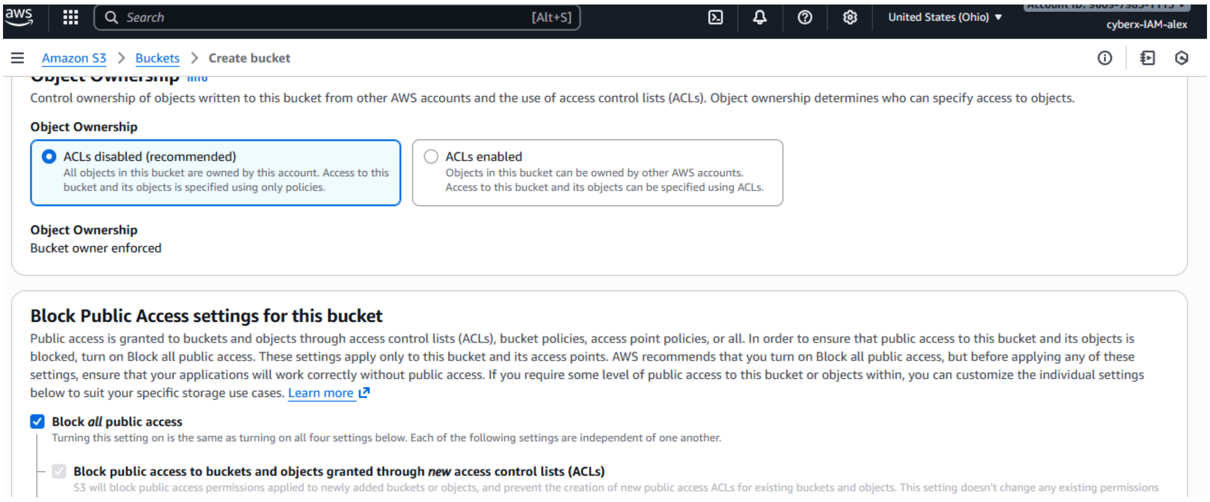
Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn more

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix


aws
Search [Alt+S]
United States (Ohio) ▾
Account ID: 9609-7985-1115 ▾
cyberx-IAM-alex
Amazon S3 > Buckets > Create bucket

Object Ownership Info

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 objects.

Object Ownership

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

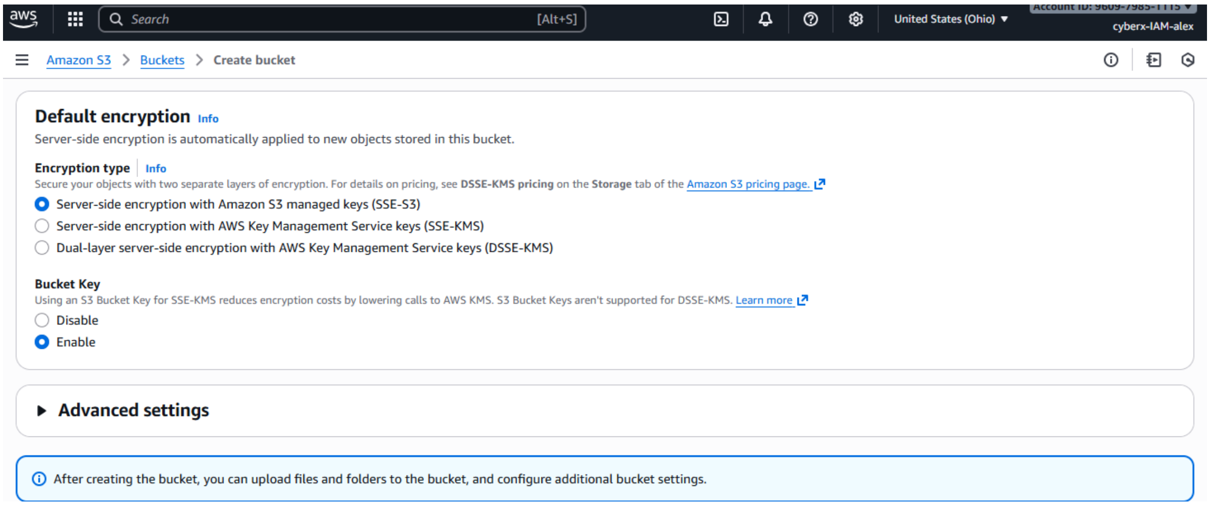
Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

☑ Block *all* public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☑ Block public access to buckets and objects granted through *new* access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions


aws
Search [Alt+S]
United States (Ohio) ▾
Account ID: 9609-7985-1115 ▾
cyberx-IAM-alex
Amazon S3 > Buckets > Create bucket

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

● Server-side encryption with Amazon S3 managed keys (SSE-S3)
○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

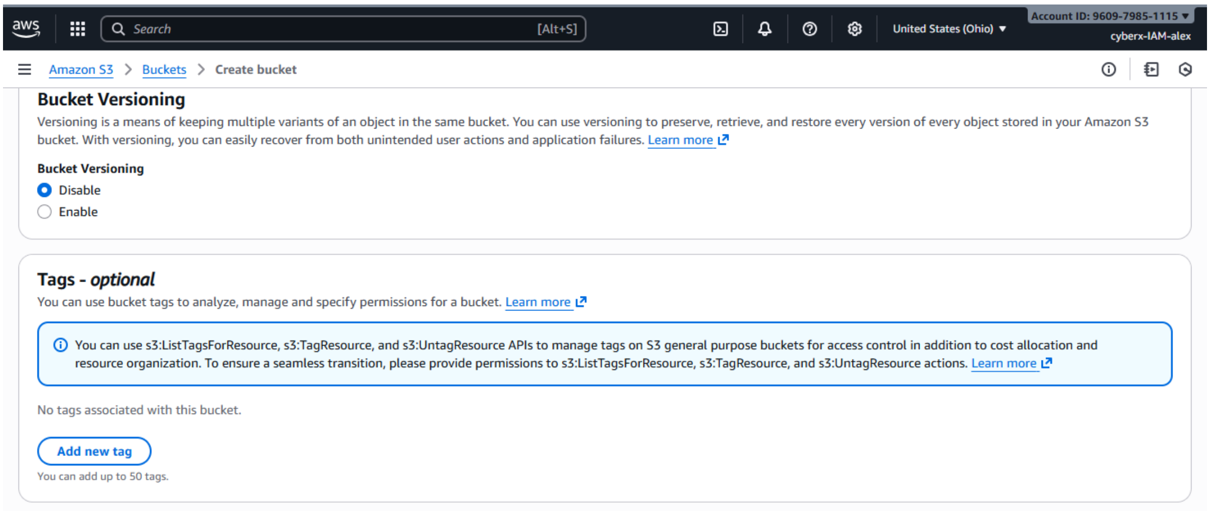
Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

○ Disable
● Enable

▶ Advanced settings

ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.


aws
Search
[Alt+S]
United States (Ohio) ▾
Account ID: 9609-7985-1115 ▾
cyberx-IAM-alex
Amazon S3 > Buckets > Create bucket

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

● Disable

○ Enable

Tags - *optional*

You can use bucket tags to analyze, manage and specify permissions for a bucket. Learn more

You can use s3:ListTagsForResource, s3:TagResource, and s3:UntagResource APIs to manage tags on S3 general purpose buckets for access control in addition to cost allocation and resource organization. To ensure a seamless transition, please provide permissions to s3:ListTagsForResource, s3:TagResource, and s3:UntagResource actions. Learn more

No tags associated with this bucket.

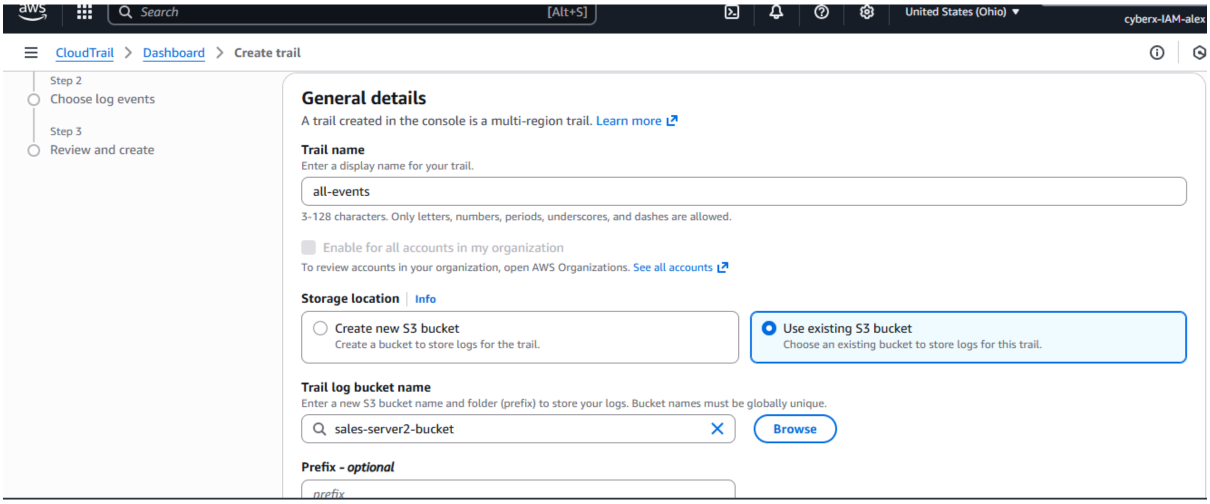
Add new tag

You can add up to 50 tags.

You can upload files to be stored in the bucket.

THE NEXT PHASE IS TO SET UP A TRAIL USING A SERVICE ON THE IAM CALLED CLOUD TRAIL ITS LIKE THE EVENT MANAGER LOGIN ACTIVITIES, ETC.

- Click on the search button on the dashboard and search for cloud trail
- Then create cloud trail and click next



General details

A trail created in the console is a multi-region trail. Learn more

Trail name

Enter a display name for your trail.

all-events

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

□ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. See all accounts

Storage location | Info

○ Create new S3 bucket
Create a bucket to store logs for the trail.

● Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

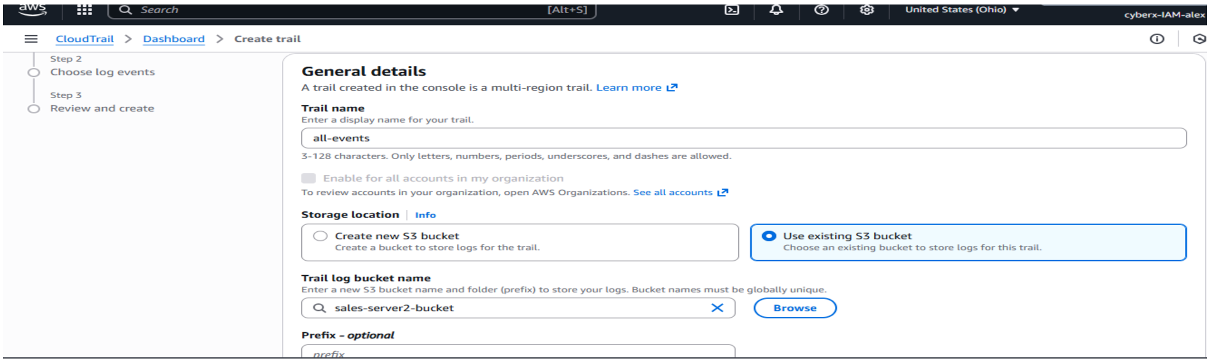
Trail log bucket name

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

sales-server2-bucket ✕ Browse

Prefix - *optional*

prefix


aws
Search [Alt+S]
United States (Ohio) ▾
cyberx-IAM-alex
CloudTrail > Dashboard > Create trail
Step 2
Choose log events
Step 3
Review and create

General details

A trail created in the console is a multi-region trail. Learn more

Trail name

Enter a display name for your trail.

all-events

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

□ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. See all accounts

Storage location | Info

○ Create new S3 bucket
Create a bucket to store logs for the trail.

● Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

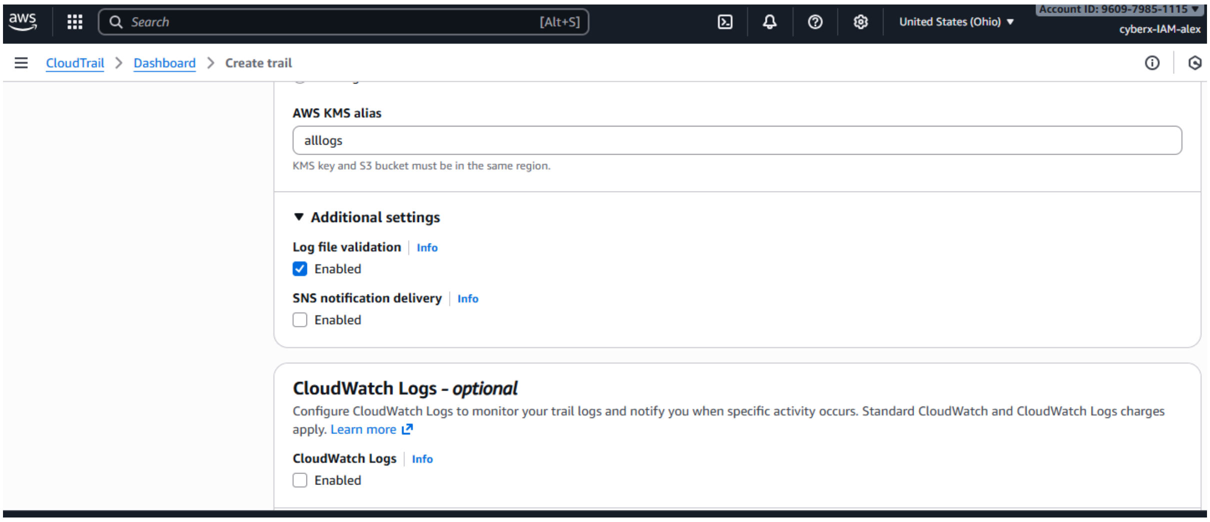
Trail log bucket name

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

sales-server2-bucket ✕ Browse

Prefix - optional

prefix


aws
Search [Alt+S]
United States (Ohio) ▾
Account ID: 9609-7985-1115 ▾
cyberx-IAM-alex
CloudTrail > Dashboard > Create trail

AWS KMS alias

alllogs

KMS key and S3 bucket must be in the same region.

▼ **Additional settings**

Log file validation | Info

☑ Enabled

SNS notification delivery | Info

□ Enabled

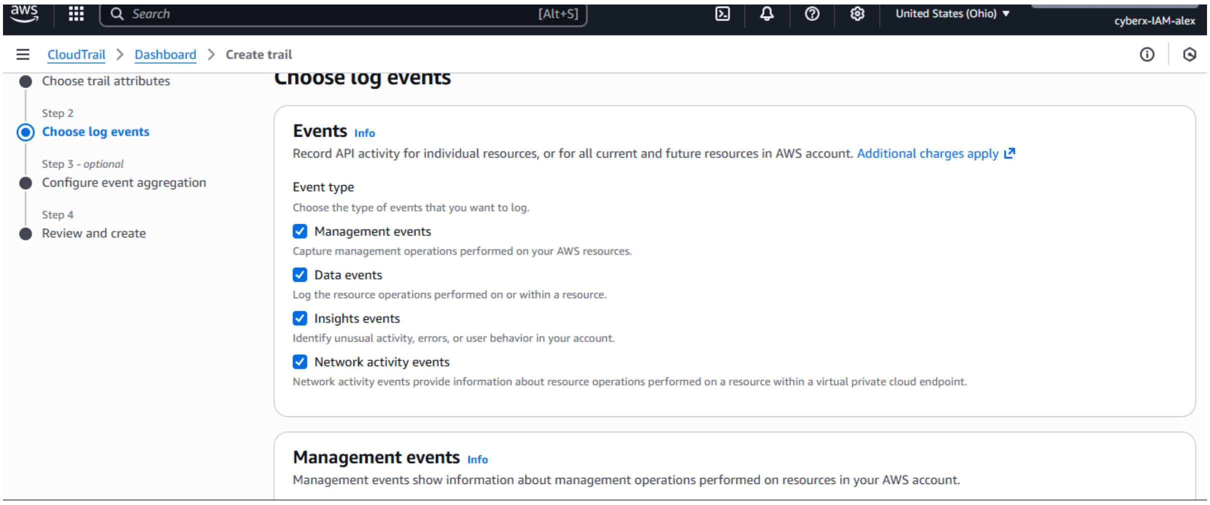
CloudWatch Logs - *optional*

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. Learn more

CloudWatch Logs | Info

□ Enabled

Then choose log events, Resource type - S3, check API error rate, network activities, s3.amazonaws.com. – Configure event aggregation- Review and Create.



CloudTrail > Dashboard > Create trail

- Choose trail attributes
- Step 2
  Choose log events
- Step 3 - *optional*
  Configure event aggregation
- Step 4
  Review and create

Choose log events

Events Info

Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply

Event type

Choose the type of events that you want to log.

☑ Management events

Capture management operations performed on your AWS resources.

☑ Data events

Log the resource operations performed on or within a resource.

☑ Insights events

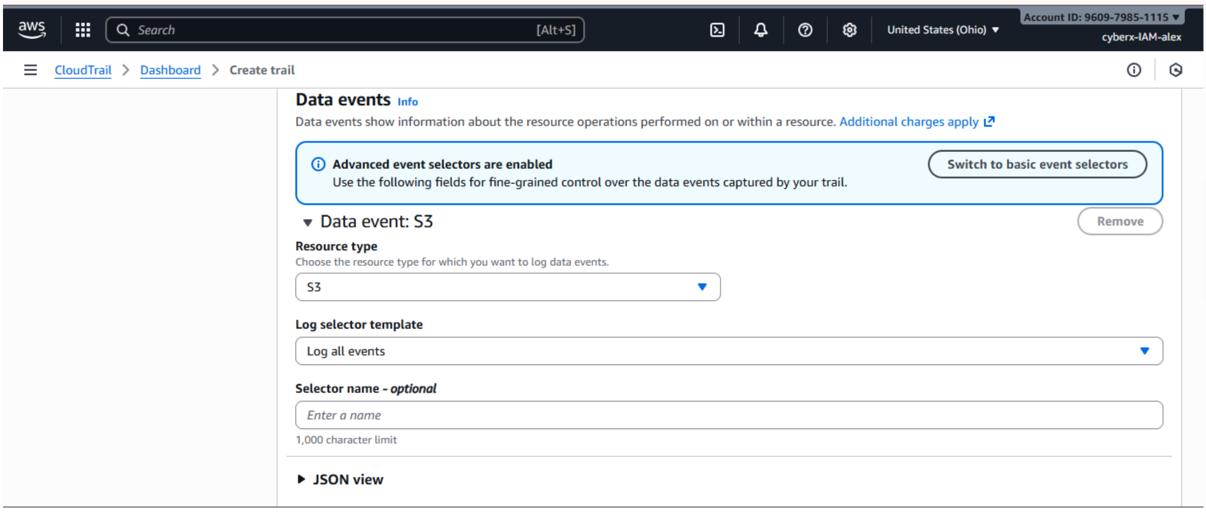
Identify unusual activity, errors, or user behavior in your account.

☑ Network activity events

Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.

Management events Info

Management events show information about management operations performed on resources in your AWS account.



CloudTrail > Dashboard > Create trail

Data events Info

Data events show information about the resource operations performed on or within a resource. Additional charges apply

Advanced event selectors are enabled
Use the following fields for fine-grained control over the data events captured by your trail.

Switch to basic event selectors

▾ Data event: S3 — Remove

Resource type

Choose the resource type for which you want to log data events.

S3 ▾

Log selector template

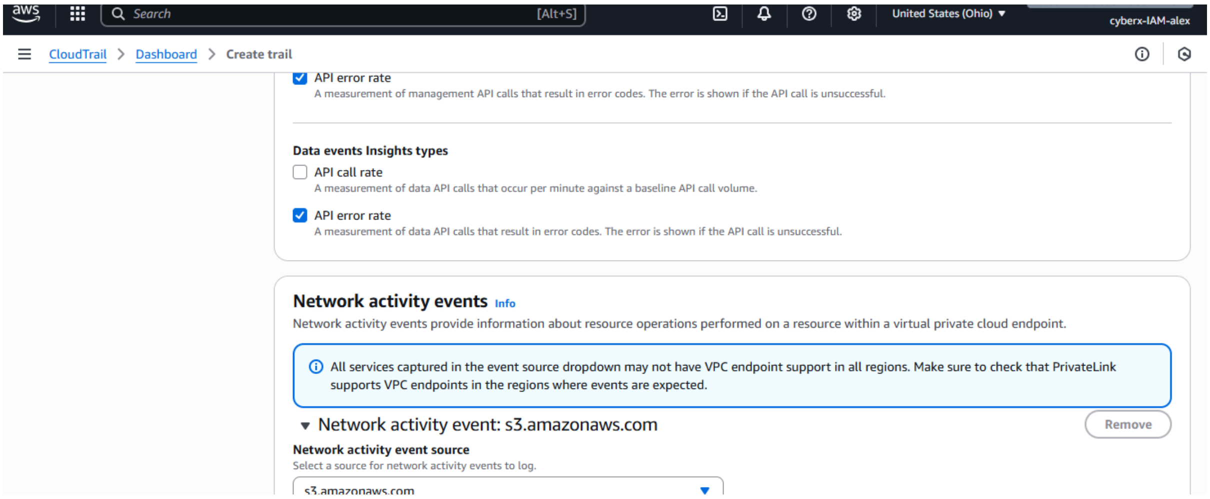
Log all events ▾

Selector name - *optional*

Enter a name

1,000 character limit

▸ **JSON view**



CloudTrail > Dashboard > Create trail

☑ API error rate

A measurement of management API calls that result in error codes. The error is shown if the API call is unsuccessful.

Data events Insights types

□ API call rate

A measurement of data API calls that occur per minute against a baseline API call volume.

☑ API error rate

A measurement of data API calls that result in error codes. The error is shown if the API call is unsuccessful.

Network activity events Info

Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.

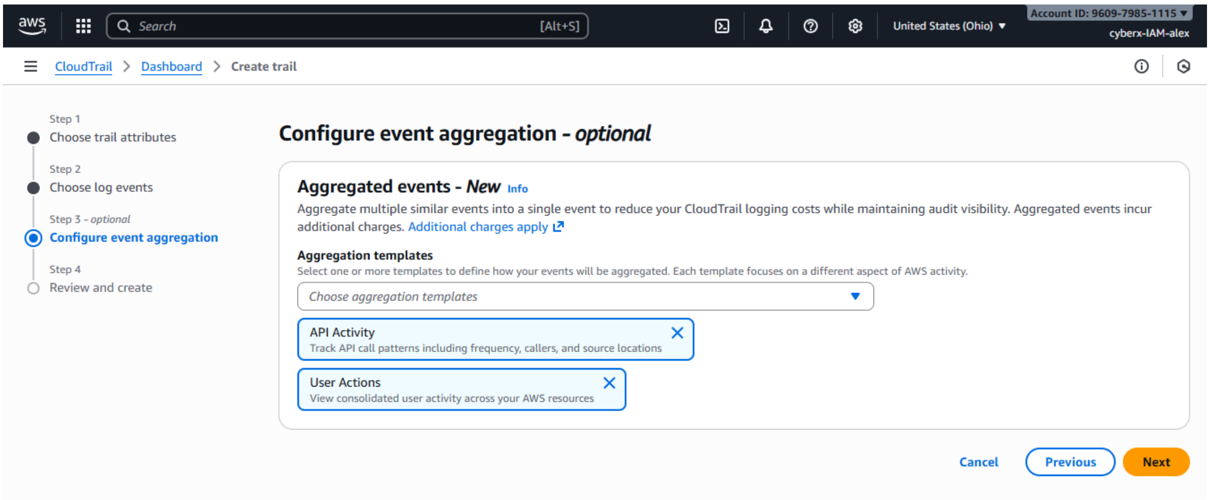
All services captured in the event source dropdown may not have VPC endpoint support in all regions. Make sure to check that PrivateLink supports VPC endpoints in the regions where events are expected.

▾ Network activity event: s3.amazonaws.com — Remove

Network activity event source

Select a source for network activity events to log.

s3.amazonaws.com ▾



Configure event aggregation - *optional*

Aggregated events - *New* Info

Aggregate multiple similar events into a single event to reduce your CloudTrail logging costs while maintaining audit visibility. Aggregated events incur additional charges. Additional charges apply

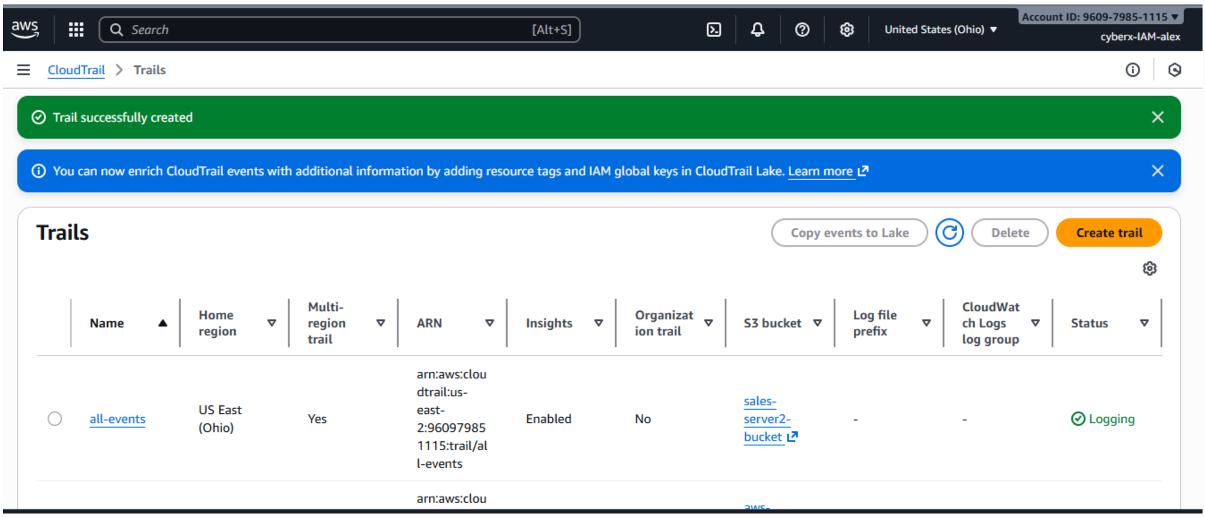
Aggregation templates

Select one or more templates to define how your events will be aggregated. Each template focuses on a different aspect of AWS activity.

Choose aggregation templates ▼

API Activity ✕
Track API call patterns including frequency, callers, and source locations

User Actions ✕
View consolidated user activity across your AWS resources



Trail successfully created ✕

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

Trails

	Name ▲	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
○	all-events	US East (Ohio)	Yes	arn:aws:cloudtrail:us-east-2:960979851115:trail/all-events	Enabled	No	sales-server2-bucket	-	-	✓ Logging
				arn:aws:clou			aws-			