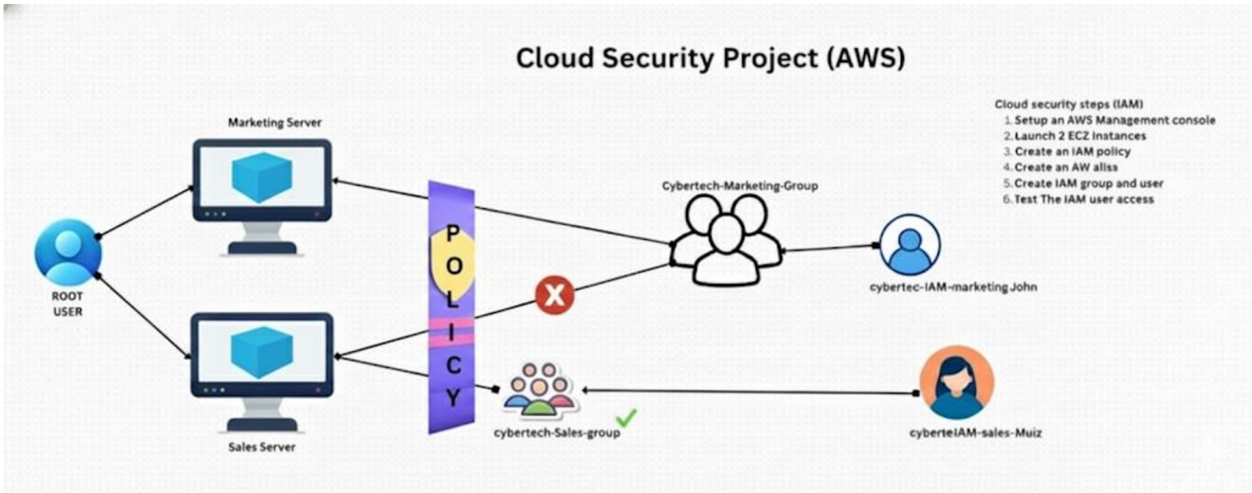
AWS IAM Cloud Security Project

1. Project Overview

This project demonstrates environment-based access control using AWS IAM policies applied to EC2 instances based on tags.



Cloud Security Project (AWS)

Cloud security steps (IAM)

1. Setup an AWS Management console
2. Launch 2 ECZ instances
3. Create an IAM policy
4. Create an AW aliss
5. Create IAM group and user
6. Test The IAM user access

2. Tools & Concepts Used

- AWS IAM: users, groups, policies, alias

- Amazon EC2: tags, lifecycle management

- IAM JSON policy syntax

- Least privilege security model

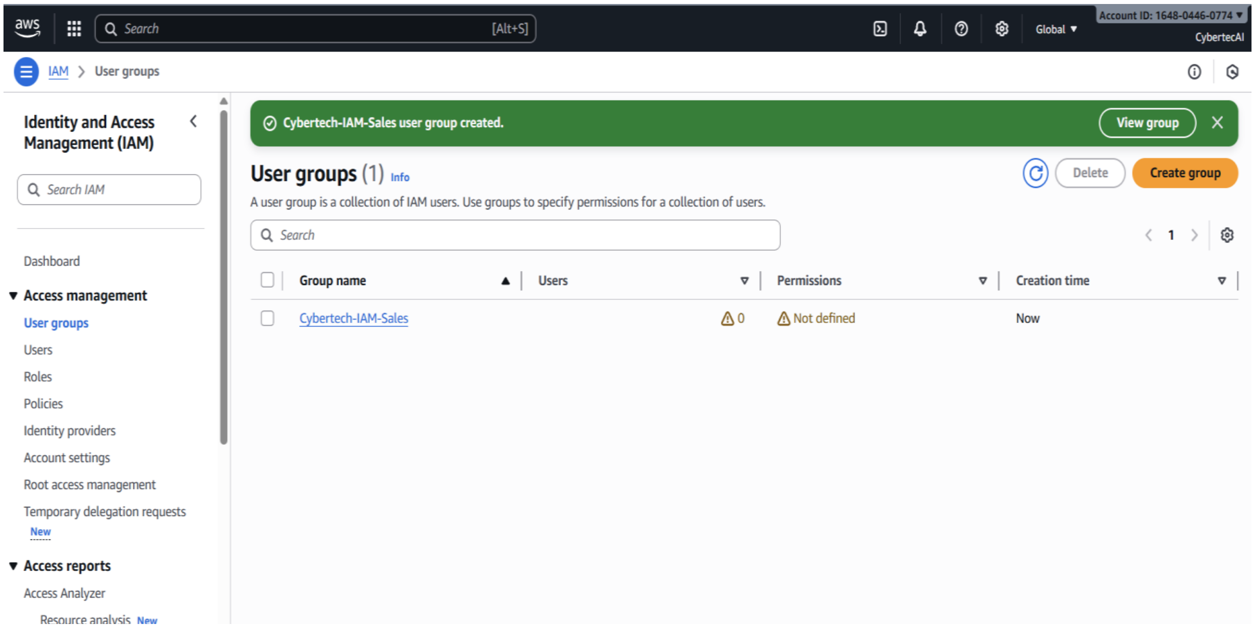
3. EC2 Tagging Strategy

Instances tagged as Marketing and Sales environments and setup buckets

4. IAM Policy (JSON)

Enforces restrictions on the Marketing instance while allowing control over the Sales instance.

User group Cybertech-IAM-Sales



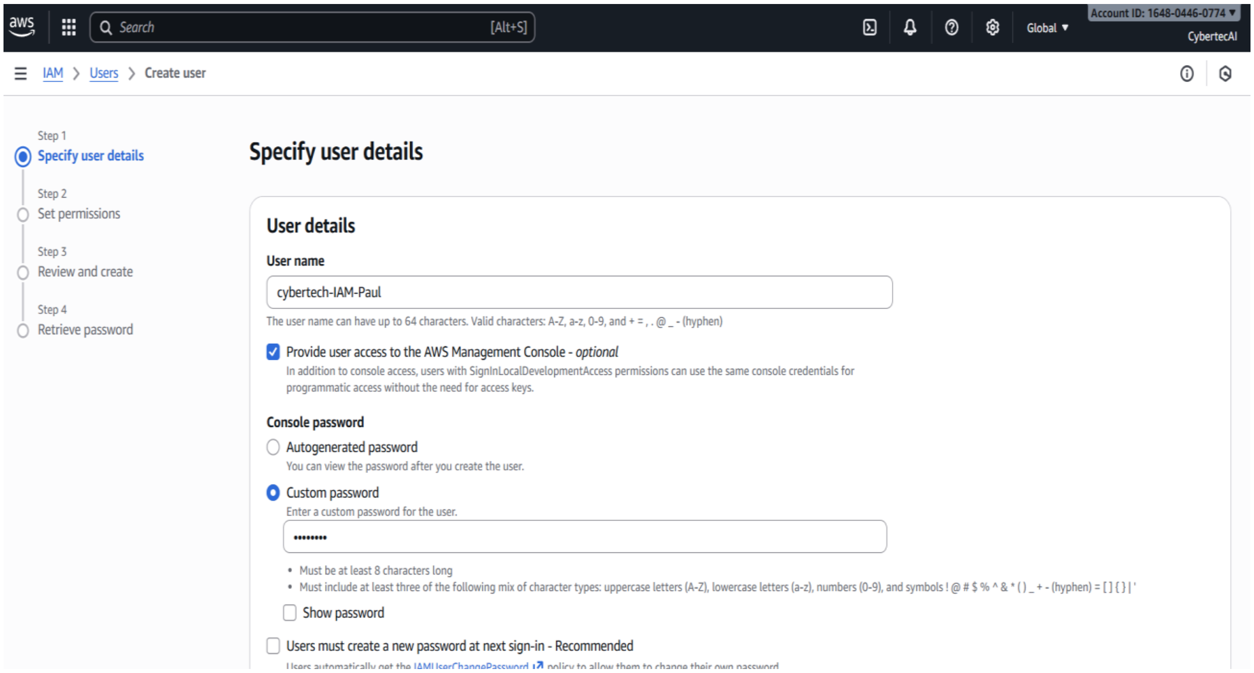
Cybertech-IAM-Sales user group created.

User groups (1)

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
□	Cybertech-IAM-Sales	⚠ 0	⚠ Not defined	Now

Creating User



Specify user details

User details

User name

cybertech-IAM-Paul

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.

••••••••

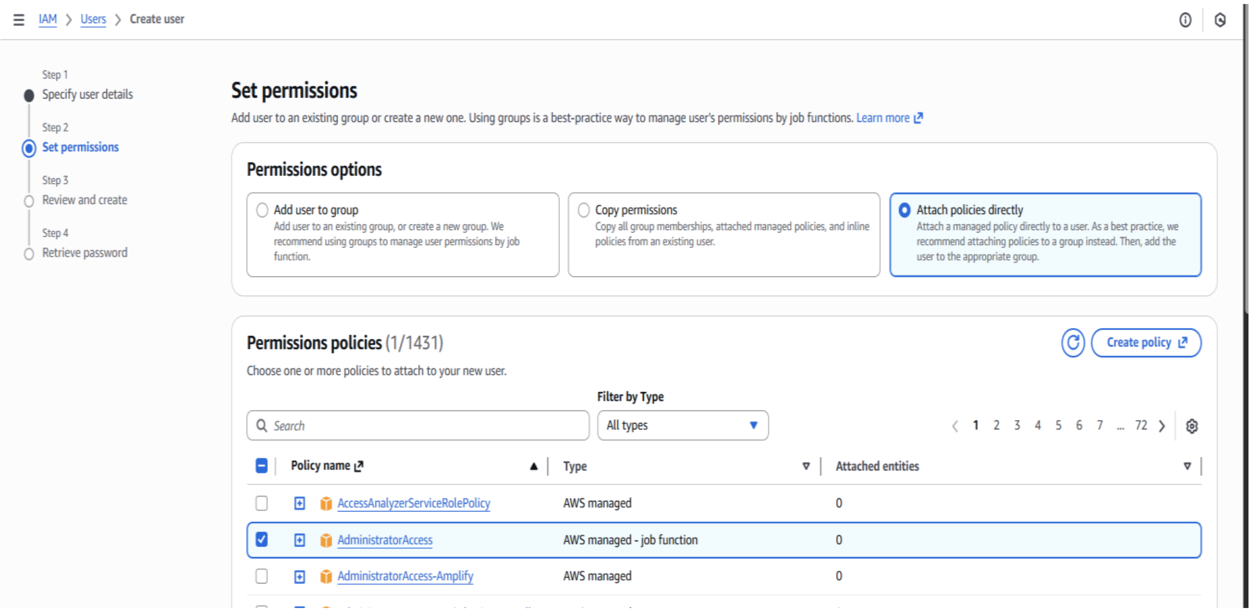
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ 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

Creating a user and assigning a policy



Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

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.

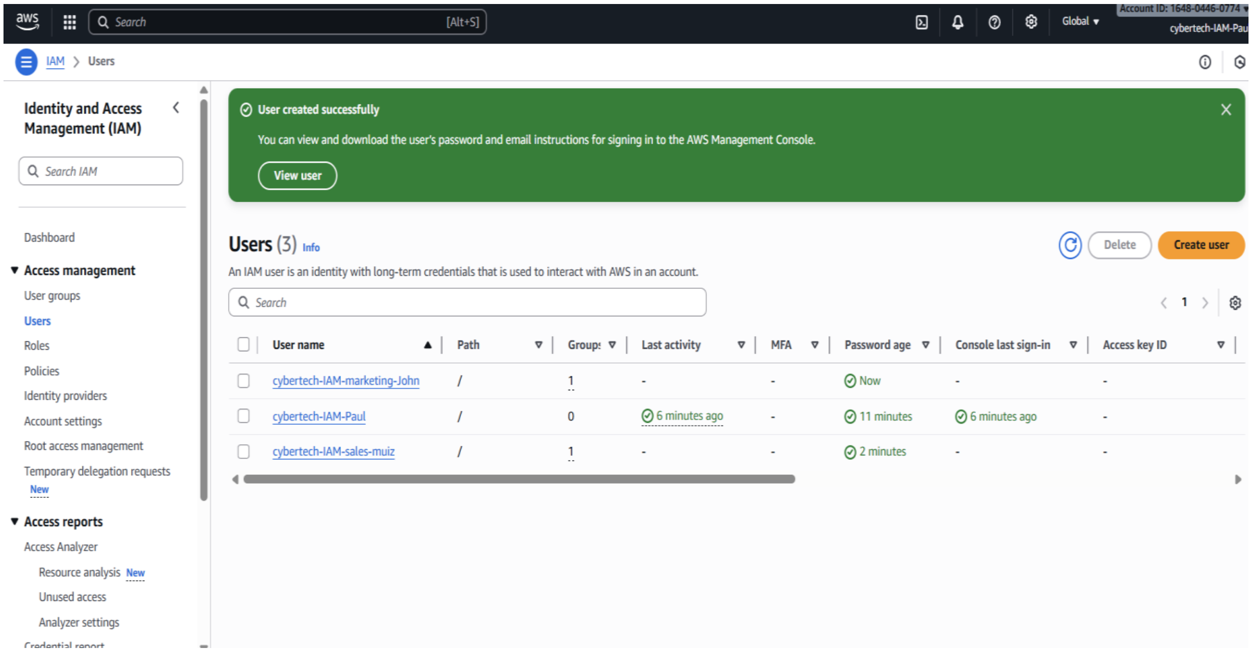
Permissions policies (1/1431)

Choose one or more policies to attach to your new user.

Filter by Type: All types

	Policy name	Type	Attached entities
□	AccessAnalyzerServiceRolePolicy	AWS managed	0
☑	AdministratorAccess	AWS managed - job function	0
□	AdministratorAccess-Amplify	AWS managed	0

User Created Sales



User created successfully

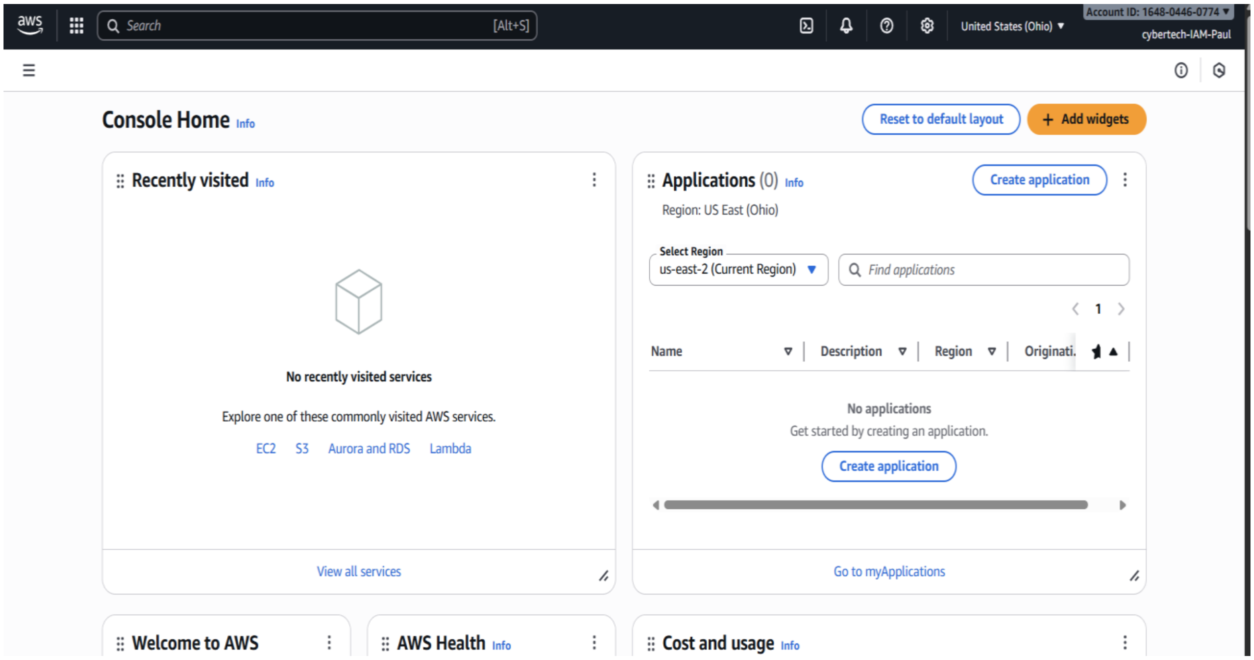
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

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
□	cybertech-IAM-marketing-John	/	1	-	-	✓ Now	-	-
□	cybertech-IAM-Paul	/	0	✓ 6 minutes ago	-	✓ 11 minutes	✓ 6 minutes ago	-
□	cybertech-IAM-sales-muiz	/	1	-	-	✓ 2 minutes	-	-

New User Sign in



Region: US East (Ohio)

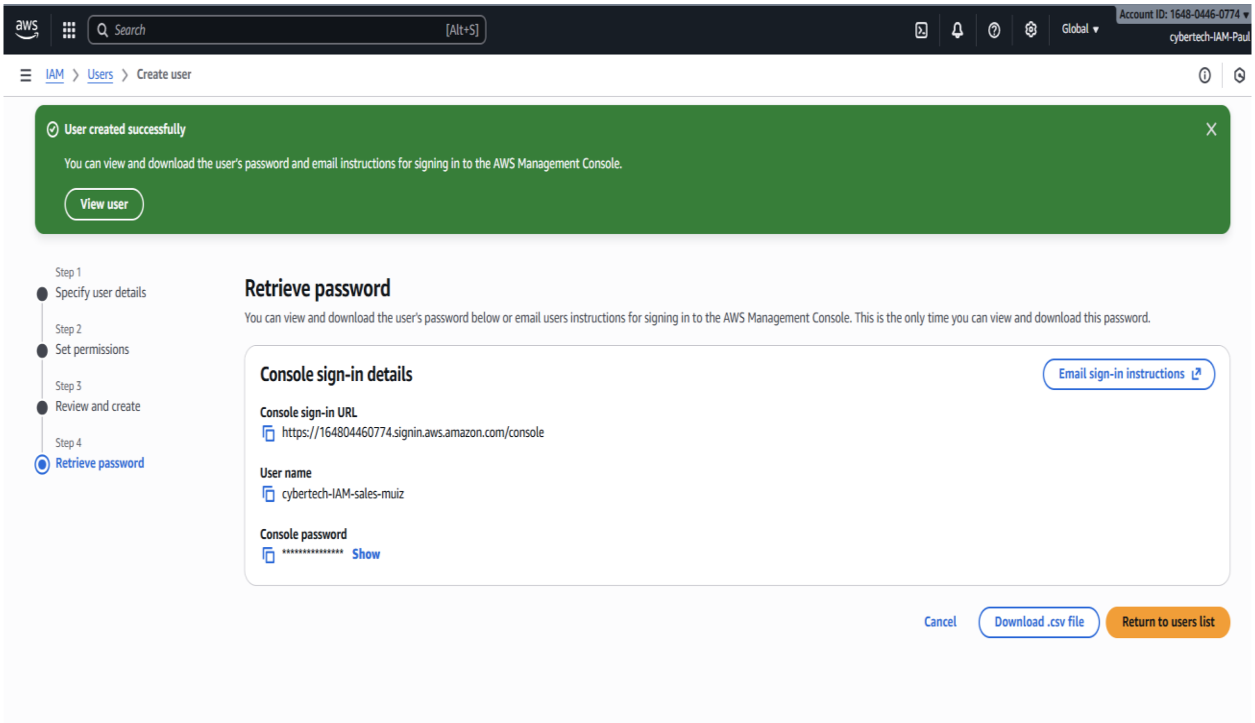
No recently visited services

Explore one of these commonly visited AWS services.

No applications

Get started by creating an application.

New User Created: Sales



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

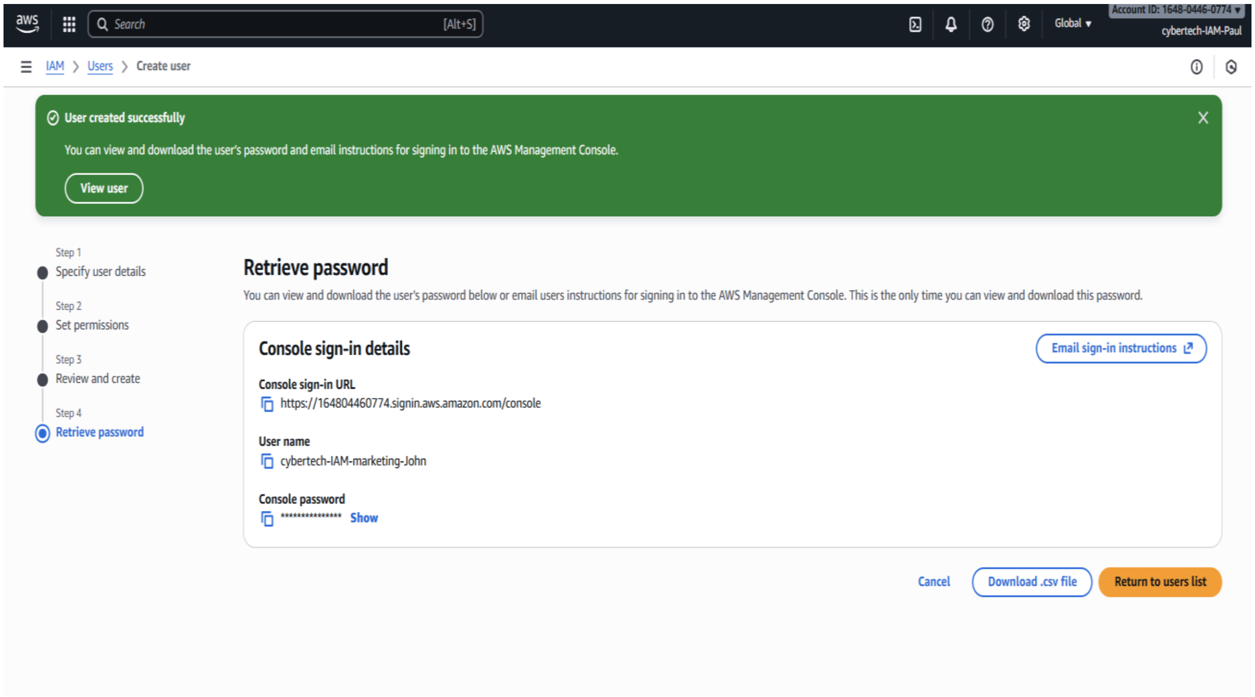
Console sign-in details

Console sign-in URL
https://164804460774.signin.aws.amazon.com/console

User name
cybertech-IAM-sales-muiz

Console password
****

New User Created: Marketing



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

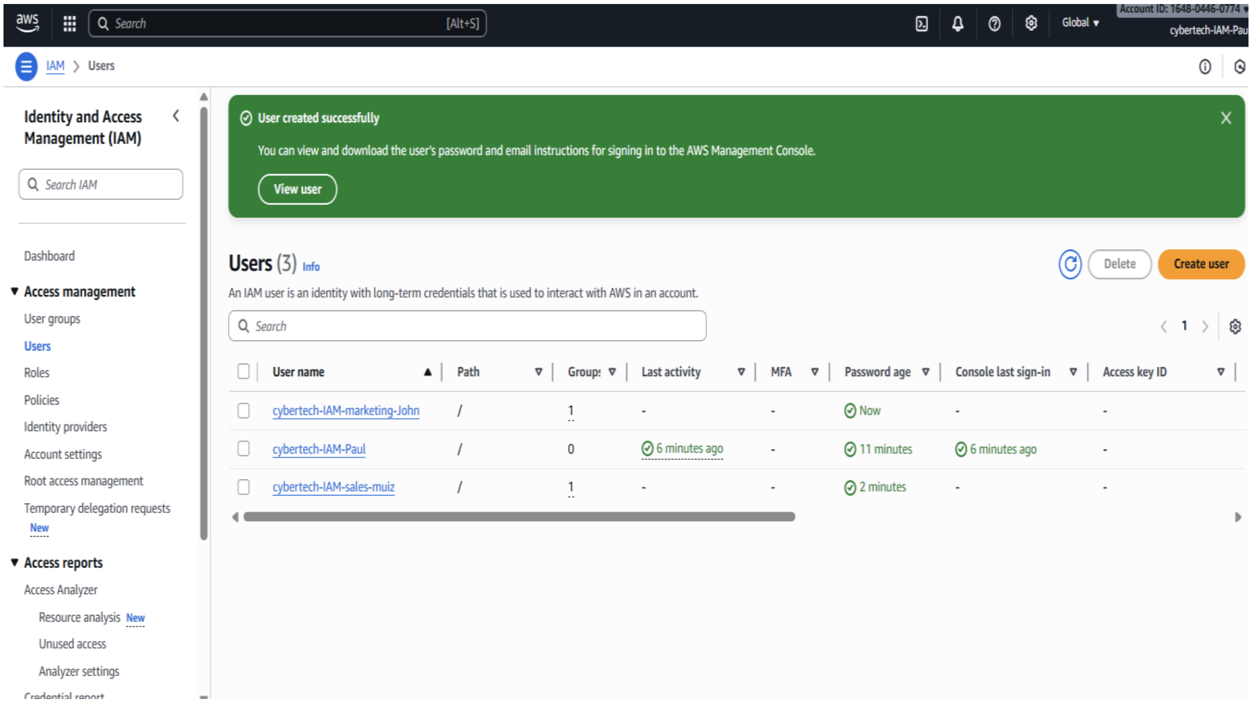
Console sign-in details

Console sign-in URL
https://164804460774.signin.aws.amazon.com/console

User name
cybertech-IAM-marketing-John

Console password
****

Users Created for different departments



User created successfully

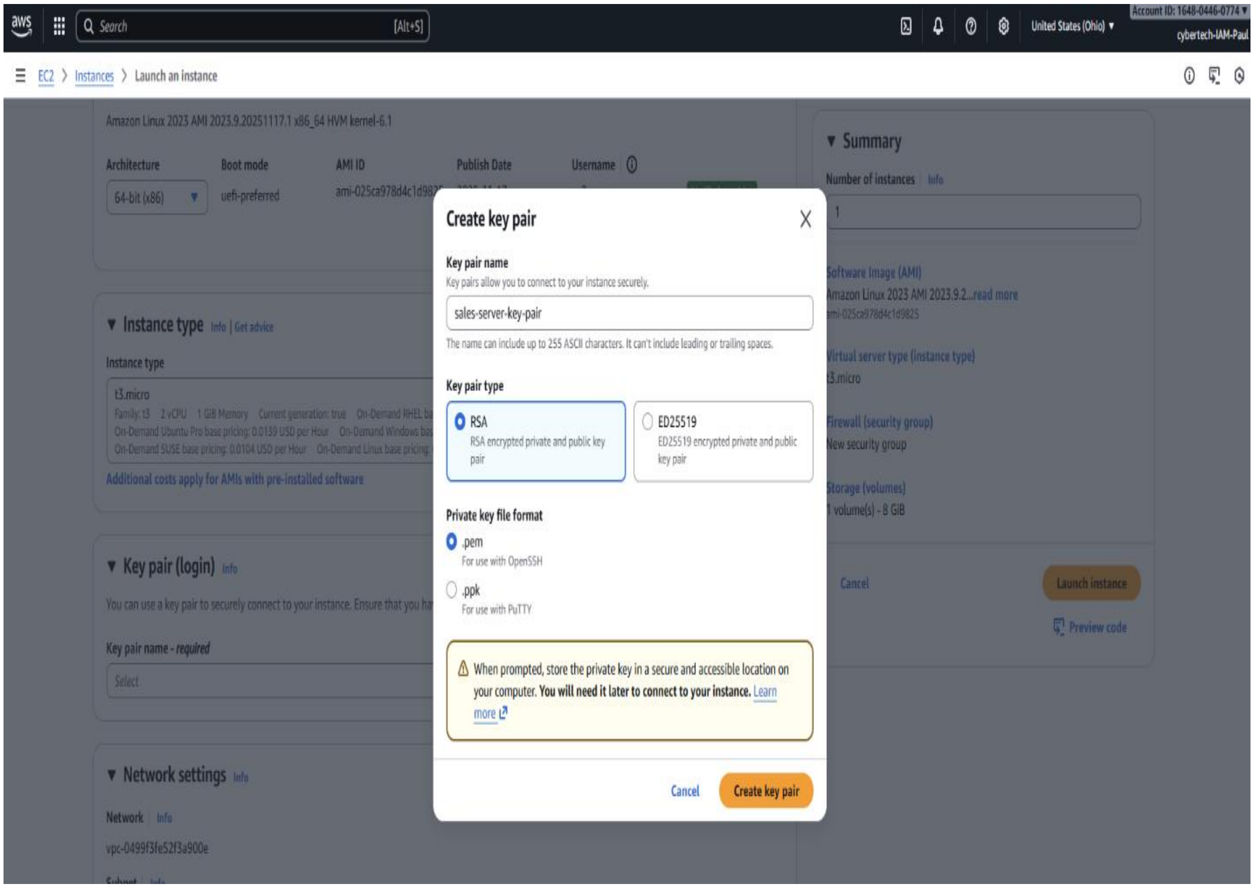
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

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	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID
□	cybertech-IAM-marketing-John	/	1	-	-	✓ Now	-	-
□	cybertech-IAM-Paul	/	0	✓ 6 minutes ago	-	✓ 11 minutes	✓ 6 minutes ago	-
□	cybertech-IAM-sales-muiz	/	1	-	-	✓ 2 minutes	-	-

Creating key pair in EC2


aws
Search [Alt+S]
United States (Ohio) ▾
Account ID: 1648-0446-0774 ▾
cybertech-IAM-Paul
EC2 > Instances > Launch an instance

Amazon Linux 2023 AMI 2023.9.20251117.1 x86_64 HVM kernel-6.1

Architecture: 64-bit (x86)
Boot mode: uefi-preferred
AMI ID: ami-025ca978d4c1d982

▾ Instance type Info | Get advice

Instance type: t3.micro
Family: t3 2 vCPU 1 GiB Memory Current generation: true On-Demand RHEL ba
On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour On-Demand Windows bas
On-Demand SUSE base pricing: 0.0104 USD per Hour On-Demand Linux base pricing:

Additional costs apply for AMIs with pre-installed software

▾ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you ha

Key pair name - *required*: Select

▾ Network settings Info

Network: vpc-0499f3fe52f3a900e

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

sales-server-key-pair

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

● RSA
RSA encrypted private and public key pair

○ ED25519
ED25519 encrypted private and public key pair

Private key file format

● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

▾ Summary

Number of instances: 1

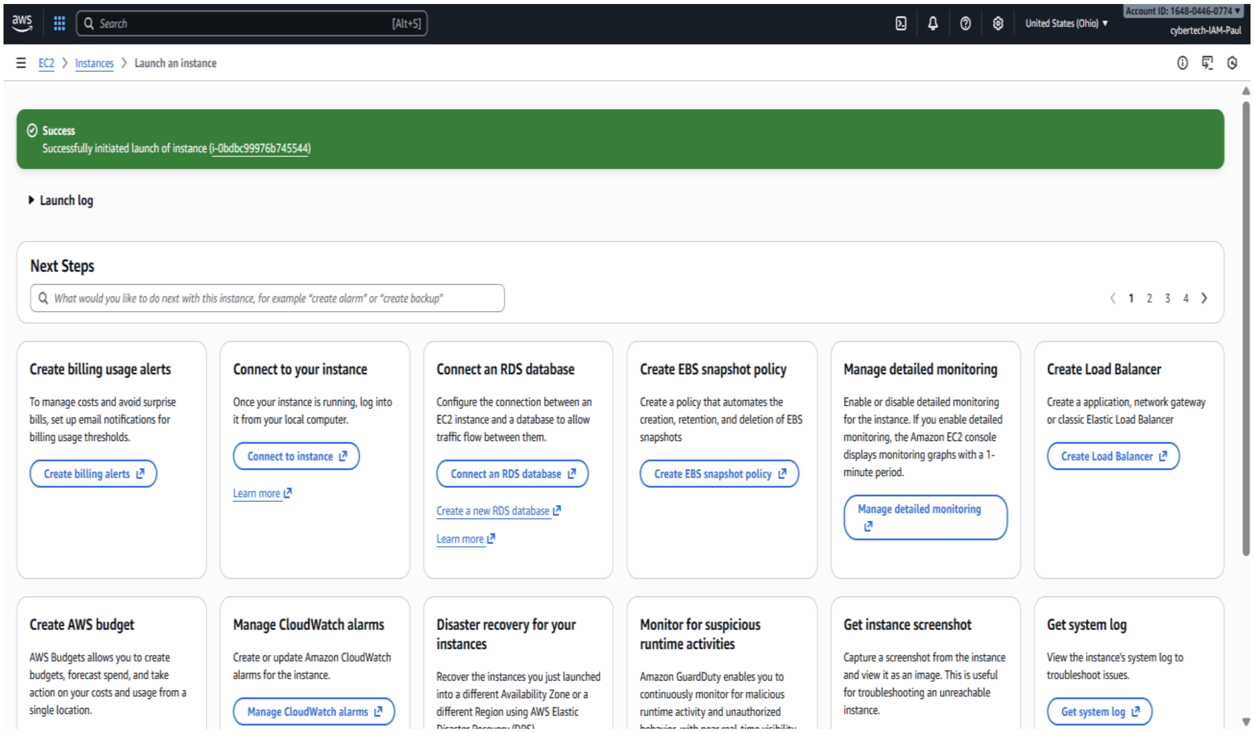
Software Image (AMI): Amazon Linux 2023 AMI 2023.9.2...read more
ami-025ca978d4c1d9825

Virtual server type (instance type): t3.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Lunched Sales Server Instance



Search [Alt+S] · United States (Ohio) ▼ · Account ID: 1648-0446-0774 ▼ · cybertech-IAM-Paul

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0bdbc99976b745544)

▸ Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

‹ 1 2 3 4 ›

Create billing usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing usage thresholds.
Create billing alerts

Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy

Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.
Manage detailed monitoring

Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer
Create Load Balancer

Create AWS budget
AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.
Manage CloudWatch alarms

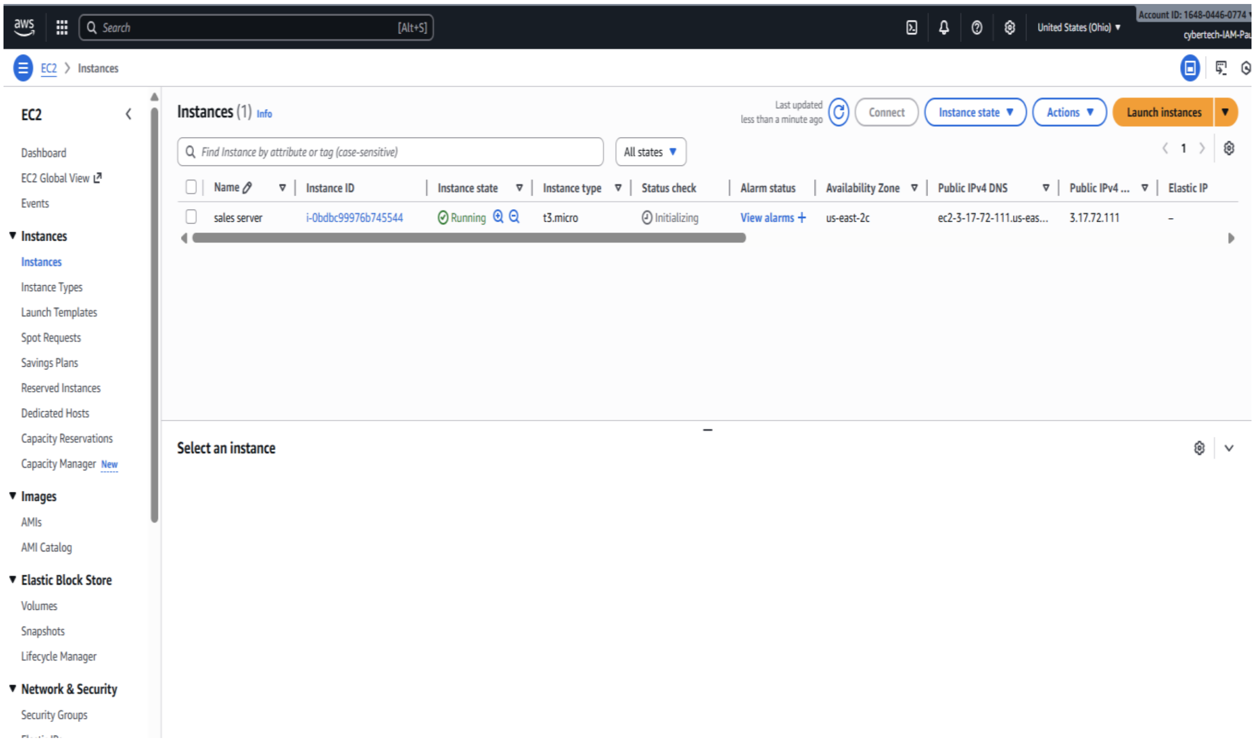
Disaster recovery for your instances
Recover the instances you just launched into a different Availability Zone or a different Region using AWS Elastic Disaster Recovery (DRS)

Monitor for suspicious runtime activities
Amazon GuardDuty enables you to continuously monitor for malicious runtime activity and unauthorized behavior with near real-time visibility

Get instance screenshot
Capture a screenshot from the instance and view it as an image. This is useful for troubleshooting an unreachable instance.

Get system log
View the instance's system log to troubleshoot issues.
Get system log

New instance called sales server



Search [Alt+S] · United States (Ohio) ▼ · Account ID: 1648-0446-0774 ▼ · cybertech-IAM-Paul

EC2 > Instances

Instances (1) Info

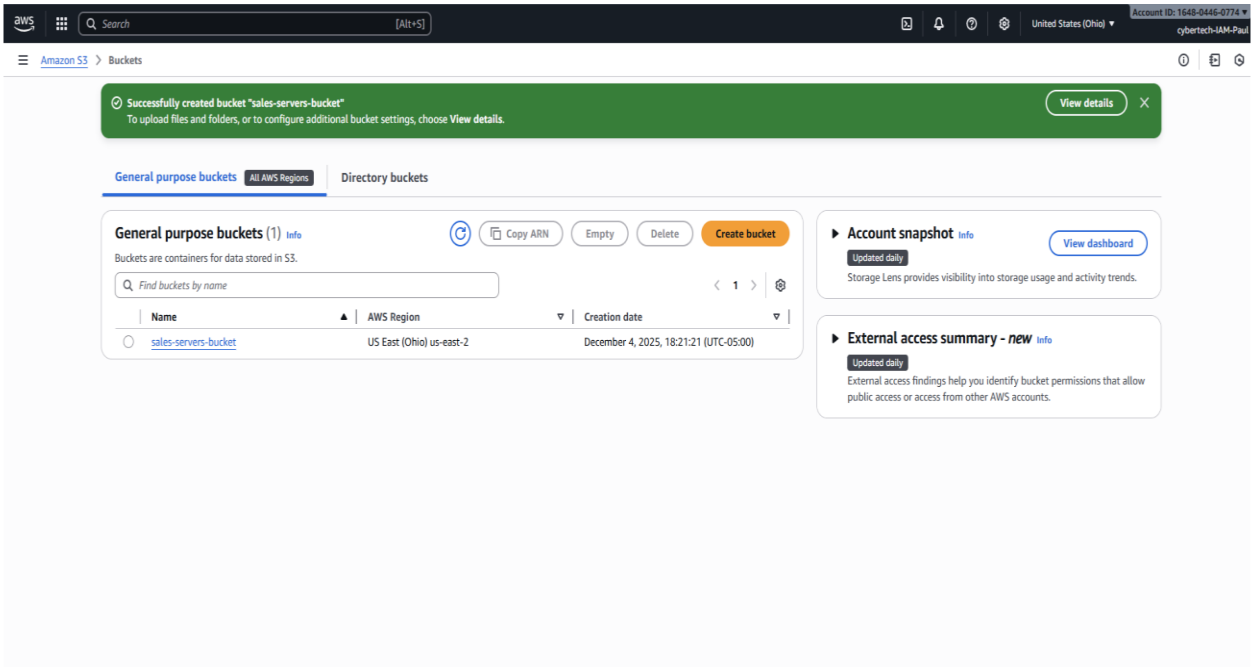
Last updated less than a minute ago · Connect · Instance state ▼ · Actions ▼ · Launch instances ▼

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
□	sales server	i-0bdbc99976b745544	Running	t3.micro	Initializing	View alarms +	us-east-2c	ec2-3-17-72-111.us-eas...	3.17.72.111	–

Select an instance

Sales server bucket created



Successfully created bucket "sales-servers-bucket"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets (1) Info

Buckets are containers for data stored in S3.

	Name	AWS Region	Creation date
○	sales-servers-bucket	US East (Ohio) us-east-2	December 4, 2025, 18:21:21 (UTC-05:00)

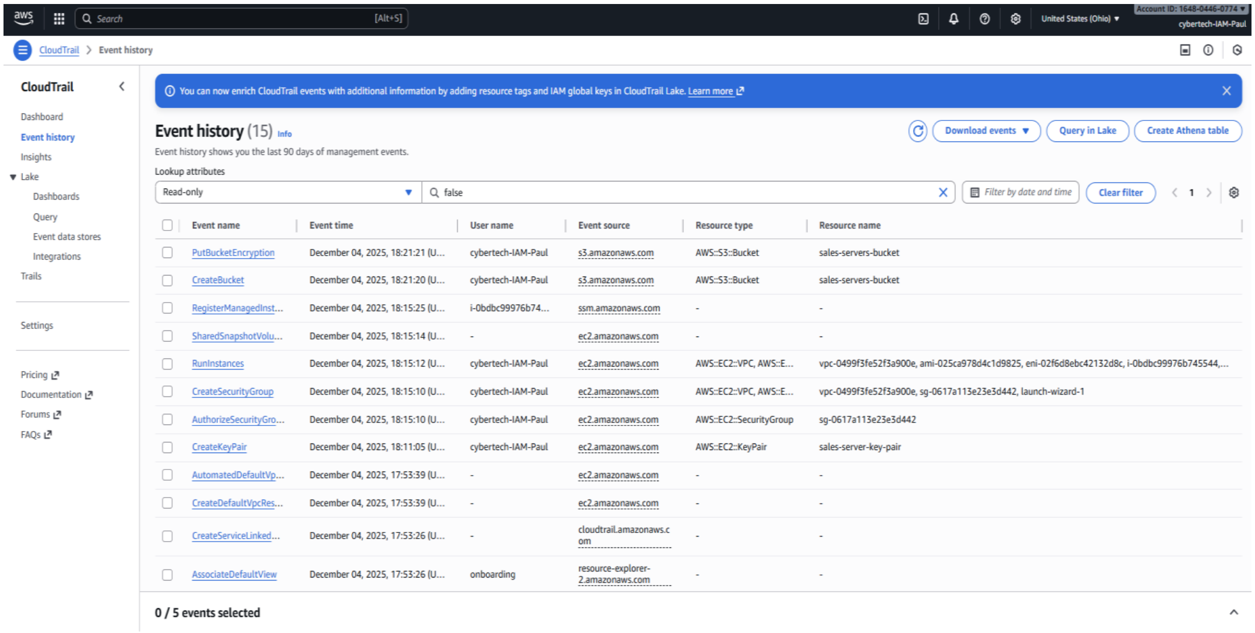
Account snapshot Info

Storage Lens provides visibility into storage usage and activity trends.

External access summary - *new* Info

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

Event history on IAM on cloud



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

Event history (15) Info

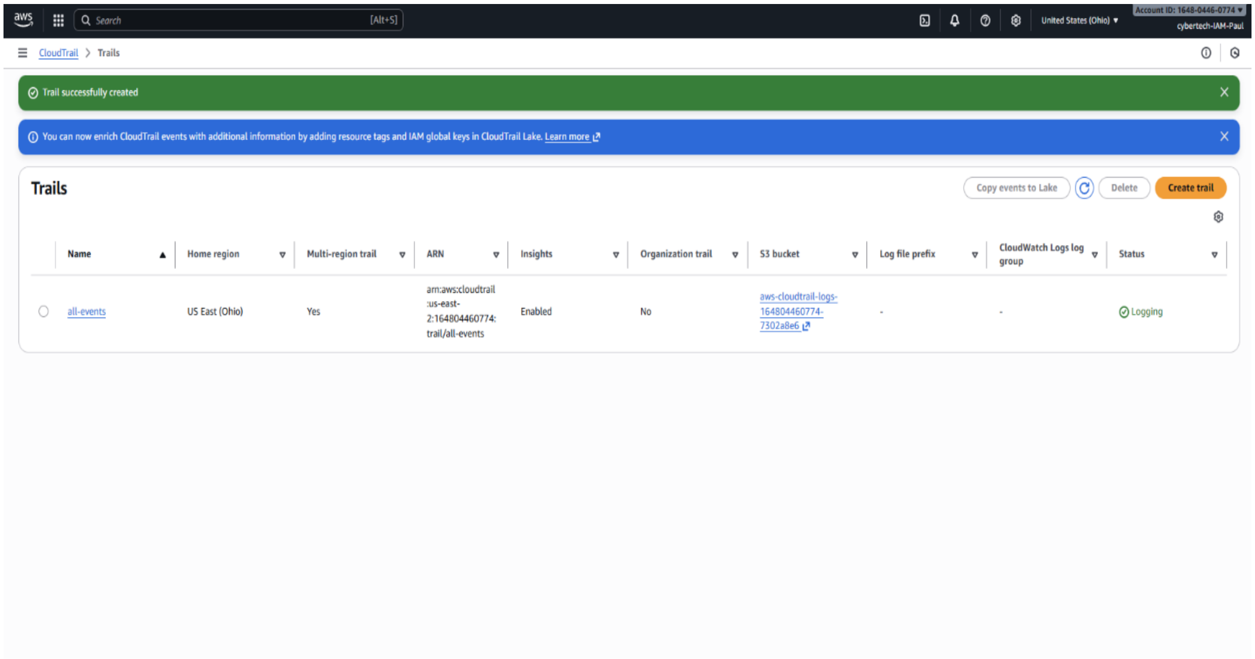
Event history shows you the last 90 days of management events.

Lookup attributes: Read-only ▼ | false

☐	Event name	Event time	User name	Event source	Resource type	Resource name
☐	PutBucketEncryption	December 04, 2025, 18:21:21 (U...	cybertech-IAM-Paul	s3.amazonaws.com	AWS::S3::Bucket	sales-servers-bucket
☐	CreateBucket	December 04, 2025, 18:21:20 (U...	cybertech-IAM-Paul	s3.amazonaws.com	AWS::S3::Bucket	sales-servers-bucket
☐	RegisterManagedInst...	December 04, 2025, 18:15:25 (U...	i-0bdbc99976b74...	ssm.amazonaws.com	-	-
☐	SharedSnapshotVolu...	December 04, 2025, 18:15:14 (U...	-	ec2.amazonaws.com	-	-
☐	RunInstances	December 04, 2025, 18:15:12 (U...	cybertech-IAM-Paul	ec2.amazonaws.com	AWS::EC2::VPC, AWS::E...	vpc-0499f3fe52f3a900e, ami-025ca978d4c1d9825, eni-02f6d8ebc42132d8c, i-0bdbc99976b745544,...
☐	CreateSecurityGroup	December 04, 2025, 18:15:10 (U...	cybertech-IAM-Paul	ec2.amazonaws.com	AWS::EC2::VPC, AWS::E...	vpc-0499f3fe52f3a900e, sg-0617a113e23e3d442, launch-wizard-1
☐	AuthorizeSecurityGro...	December 04, 2025, 18:15:10 (U...	cybertech-IAM-Paul	ec2.amazonaws.com	AWS::EC2::SecurityGroup	sg-0617a113e23e3d442
☐	CreateKeyPair	December 04, 2025, 18:11:05 (U...	cybertech-IAM-Paul	ec2.amazonaws.com	AWS::EC2::KeyPair	sales-server-key-pair
☐	AutomatedDefaultVp...	December 04, 2025, 17:53:39 (U...	-	ec2.amazonaws.com	-	-
☐	CreateDefaultVpcRes...	December 04, 2025, 17:53:39 (U...	-	ec2.amazonaws.com	-	-
☐	CreateServiceLinked...	December 04, 2025, 17:53:26 (U...	-	cloudtrail.amazonaws.com	-	-
☐	AssociateDefaultView	December 04, 2025, 17:53:26 (U...	onboarding	resource-explorer-2.amazonaws.com	-	-

0 / 5 events selected

Trail successfully created



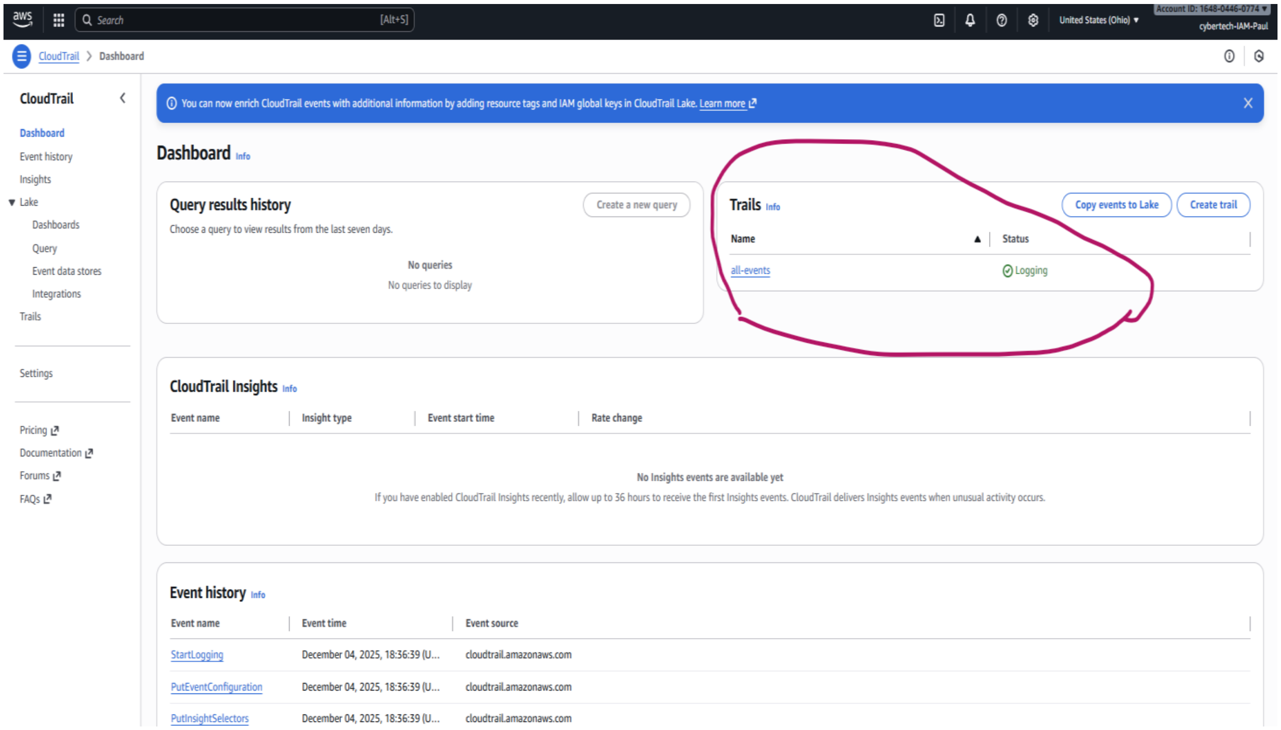
Trail successfully created

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-2:164804460774:trail/all-events	Enabled	No	aws-cloudtrail-logs-164804460774-7302a8e6	-	-	✓ Logging

New trail Added



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
all-events	✓ Logging

CloudTrail Insights Info

Event name	Insight type	Event start time	Rate change

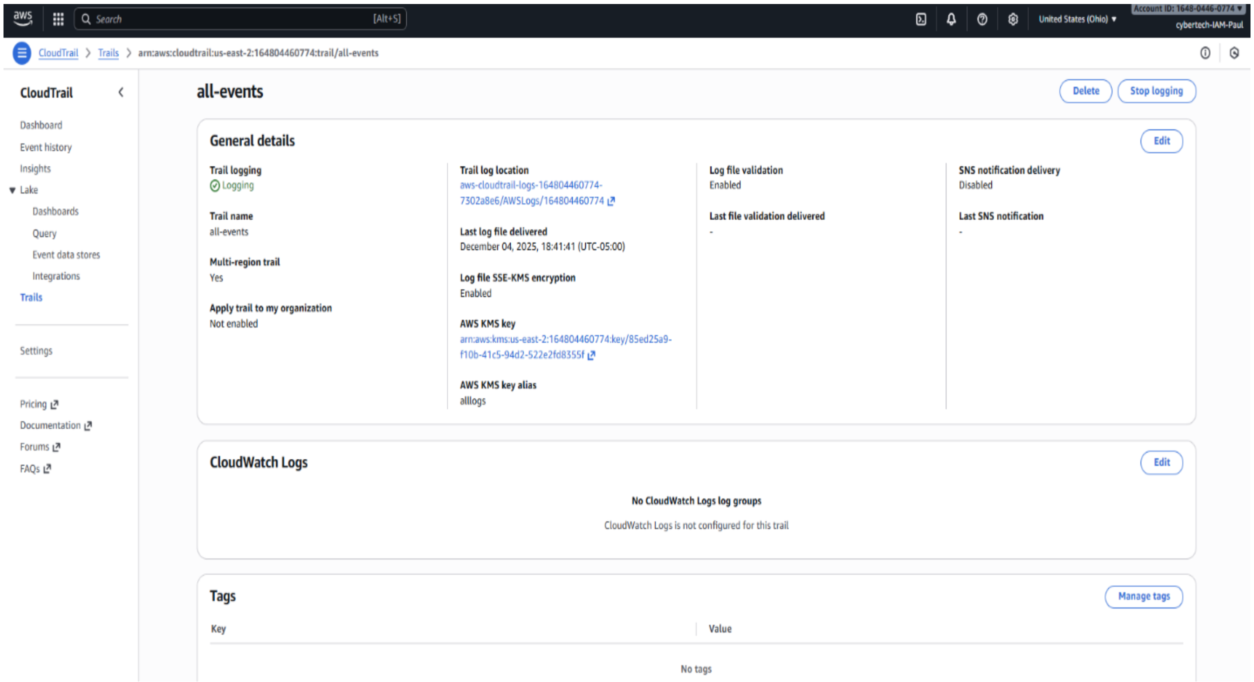
No Insights events are available yet

If you have enabled CloudTrail Insights recently, allow up to 36 hours to receive the first Insights events. CloudTrail delivers Insights events when unusual activity occurs.

Event history Info

Event name	Event time	Event source
StartLogging	December 04, 2025, 18:36:39 (U...	cloudtrail.amazonaws.com
PutEventConfiguration	December 04, 2025, 18:36:39 (U...	cloudtrail.amazonaws.com
PutInsightSelectors	December 04, 2025, 18:36:39 (U...	cloudtrail.amazonaws.com

Trail all events



all-events

General details

Trail logging
✓ Logging

Trail name
all-events

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
aws-cloudtrail-logs-164804460774-7302a8e6/AWSLogs/164804460774

Last log file delivered
December 04, 2025, 18:41:41 (UTC-05:00)

Log file SSE-KMS encryption
Enabled

AWS KMS key
arn:aws:kms:us-east-2:164804460774:key/85ed25a9-f10b-41c5-94d2-522e2fd8355f

AWS KMS key alias
alllogs

Log file validation
Enabled

Last file validation delivered
-

SNS notification delivery
Disabled

Last SNS notification
-

CloudWatch Logs

No CloudWatch Logs log groups

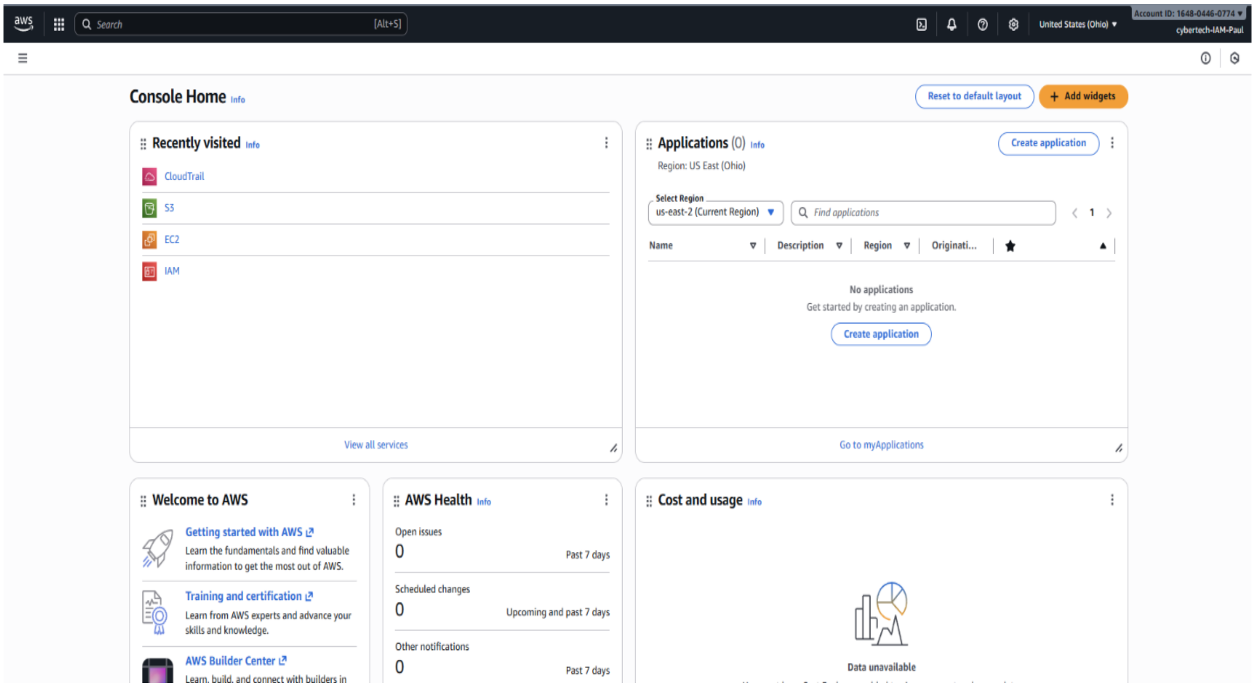
CloudWatch Logs is not configured for this trail

Tags

Key	Value

No tags

Services created on IAM on cloud



Console Home

Recently visited

- CloudTrail
- S3
- EC2
- IAM

Applications (0)

Region: US East (Ohio)

No applications

Get started by creating an application.

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification
Learn from AWS experts and advance your skills and knowledge.

AWS Builder Center
Learn, build, and connect with builders in

AWS Health

Open issues
0 Past 7 days

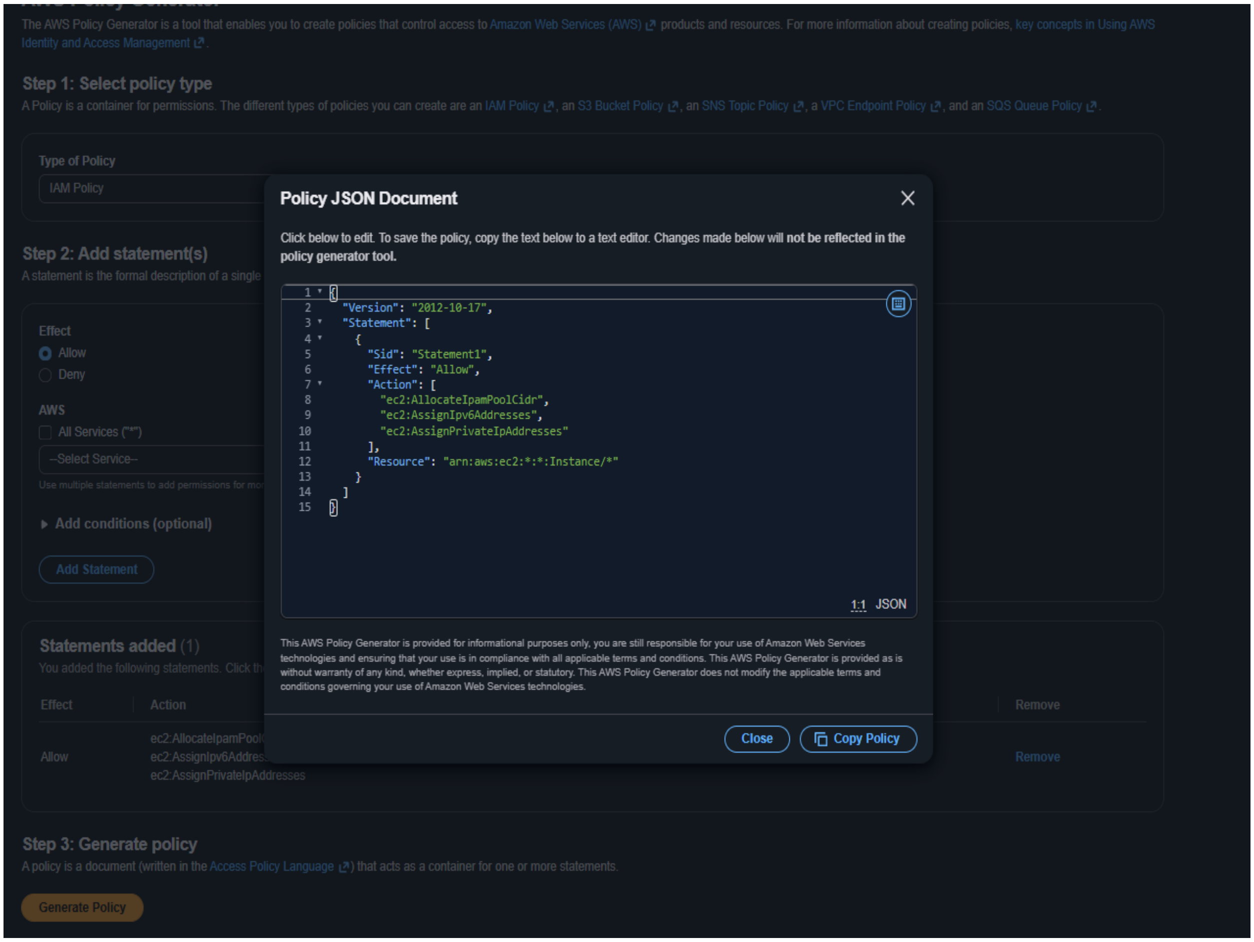
Scheduled changes
0 Upcoming and past 7 days

Other notifications
0 Past 7 days

Cost and usage

Data unavailable

Policy JSON Document



The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, key concepts in Using AWS Identity and Access Management.

Step 1: Select policy type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Type of Policy: IAM Policy

Step 2: Add statement(s)

A statement is the formal description of a single

Effect
● Allow
○ Deny

AWS
□ All Services ("*")
--Select Service--

Use multiple statements to add permissions for mor

Add conditions (optional)

Statements added (1)

You added the following statements. Click th

Effect	Action	Remove
Allow	ec2:AllocateIpamPool ec2:AssignIpv6Addres ec2:AssignPrivateIpAddresses	Remove

Step 3: Generate policy

A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Policy JSON Document

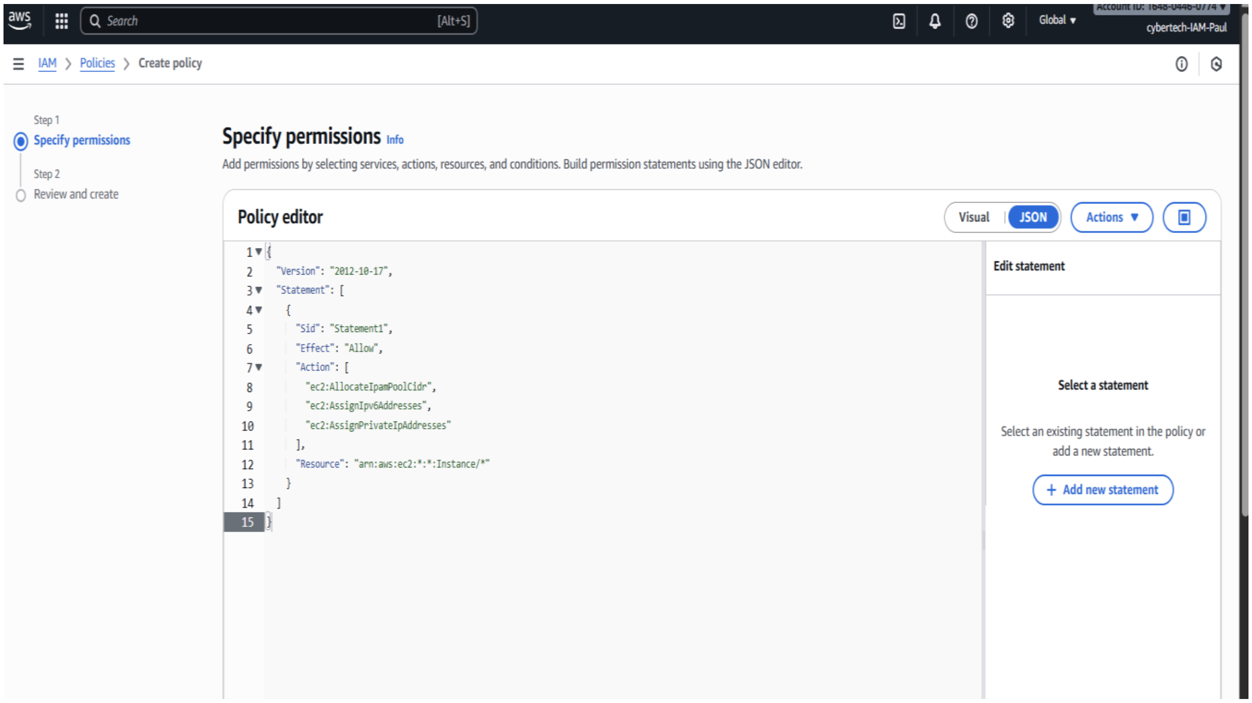
Click below to edit. To save the policy, copy the text below to a text editor. Changes made below **will not be reflected in the policy generator tool.**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "ec2:AllocateIpamPoolCidr",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource": "arn:aws:ec2:*:*:Instance/*"
    }
  ]
}
```

1:1 JSON

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

Policy generation in IAM



Specify permissions

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "ec2:AllocateIpamPoolCidr",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource": "arn:aws:ec2:*:*:Instance/*"
    }
  ]
}
```

Select a statement

Select an existing statement in the policy or add a new statement.

5. AWS Account Alias

A custom sign-in alias was created to simplify access for IAM users and replace the long numeric login URL.

6. IAM Users & Groups

Steps carried out:

1. Created an IAM group named **Developers**
2. Attached the CybertechMarketingEnvPolicy to the group
3. Added team members as IAM users with controlled EC2 permissions

7. IAM User Login Options

IAM users can authenticate via:

- **AWS Management Console** (using the account alias)
- **AWS CLI** (configured with Access Key ID & Secret Access Key)

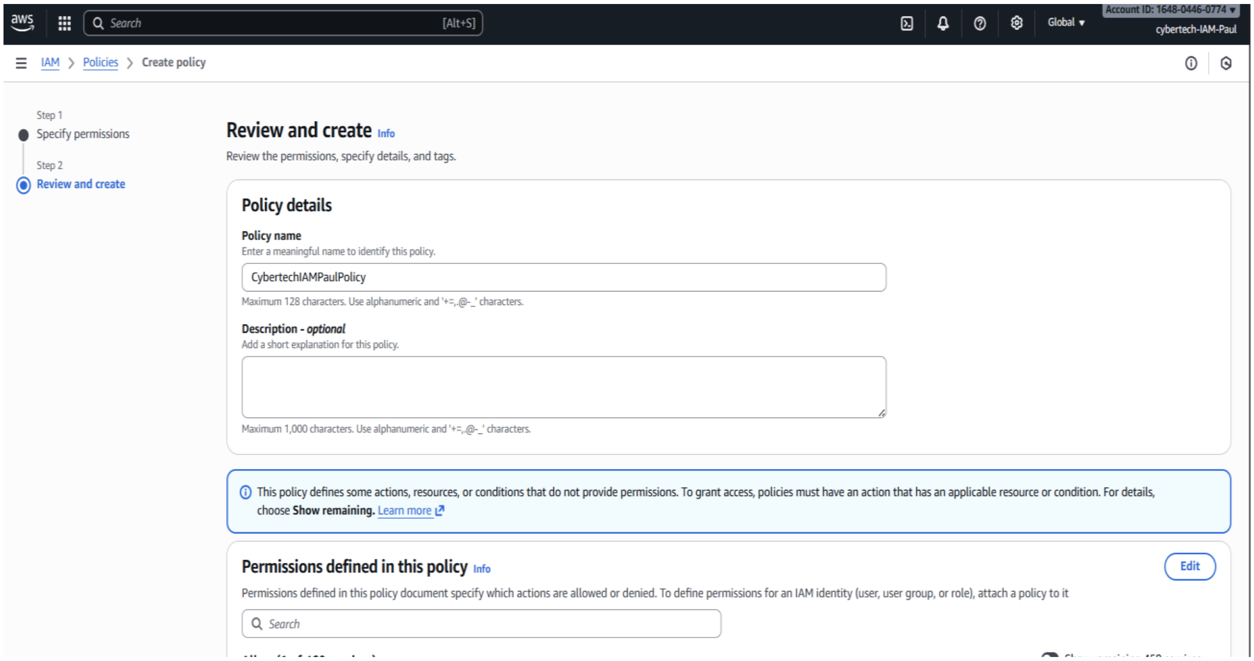
8. Policy Testing & Validation

Real-world validation was performed by attempting EC2 operations as an IAM user.

Test Action	Expected Result	Actual Result
Stop Marketing instance	Denied	Access denied
Stop sales instance	Allowed	Successful
Start Marketing instance	Denied	Access denied
Start sales instance	Allowed	Successful

The test outcomes confirmed that the tag-based policy operates exactly as designed.

Policy named



Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.
CybertechIAMPaulPolicy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

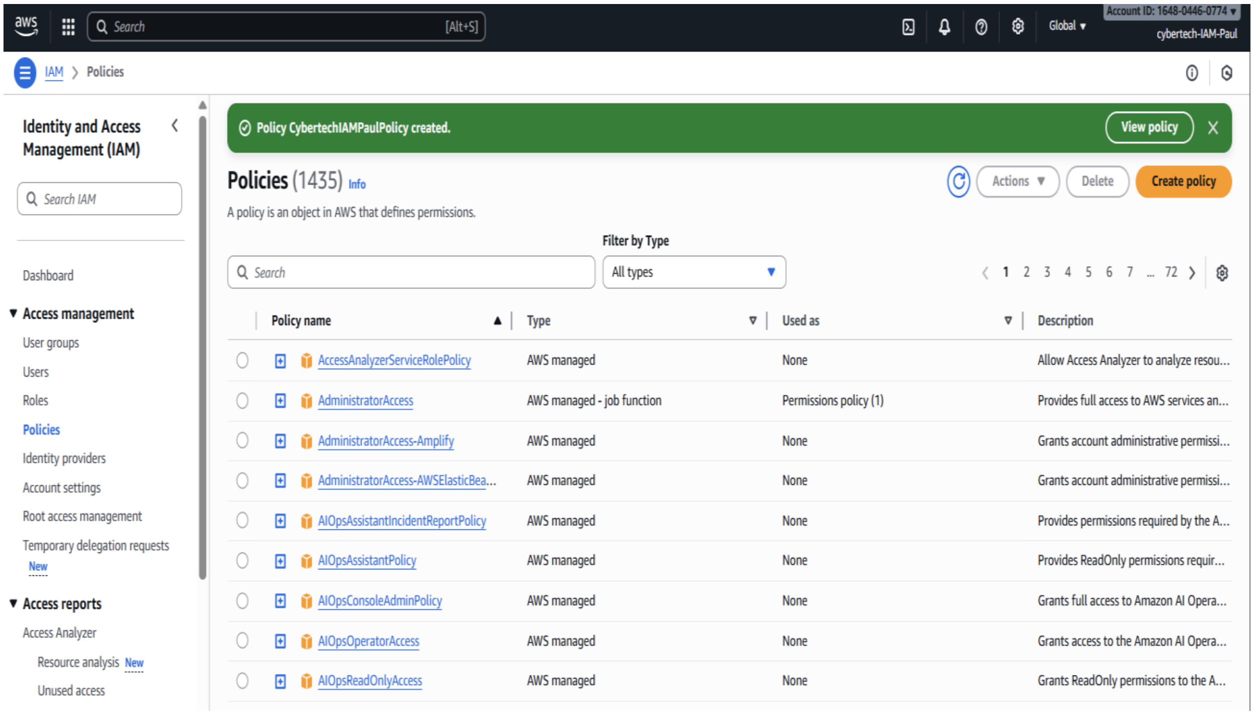
This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining.** Learn more

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Policy named 2



Policy CybertechIAMPaulPolicy created.

Policies (1435)

A policy is an object in AWS that defines permissions.

Filter by Type: All types

	Policy name	Type	Used as	Description
○	AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze resou...
○	AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an...
○	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissi...
○	AdministratorAccess-AWSElasticBea...	AWS managed	None	Grants account administrative permissi...
○	AIOpsAssistantIncidentReportPolicy	AWS managed	None	Provides permissions required by the A...
○	AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
○	AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...
○	AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
○	AIOpsReadOnlyAccess	AWS managed	None	Grants ReadOnly permissions to the A...