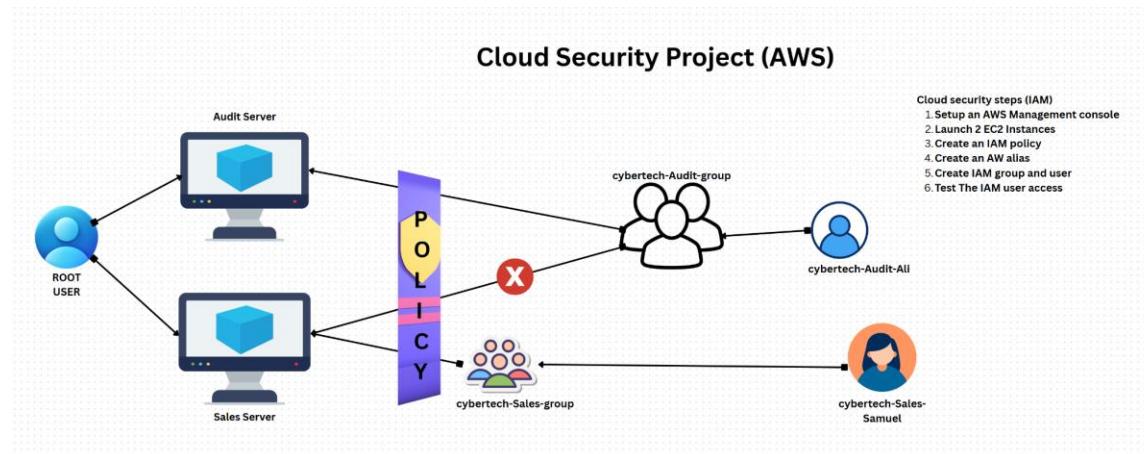


AWS IAM Cloud Security Project

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 or group, and verify that the policy correctly restricts actions on Amazon EC2 instance.



In this project, we will be creating Users, User groups, buckets, trails, polices implementing those policies and verifying them.

Standard practice prescribes that we don't do anything on root user, however we can use it to create a user with admin privileges.

In AWS, we use services to create everything

Firstly we can create an AWS trail account for 6 month on the website at [Cloud Computing Services - Amazon Web Services \(AWS\)](#), a credit card will be required however you will get a credit to use to run your simulation.

CREATING THE IAM USER AND GROUPS

Upon creating an account and logging in, it will be a root user, so we will set up MFA (to make it secure) and create a user with admin privileges.

Firstly, we change our geographical location

The screenshot shows the AWS Console Home page. At the top right, there is a dropdown menu labeled "United States (Ohio)". This menu is expanded to show a list of AWS Regions. The "Ohio" region is highlighted with a red circle. Other regions listed include N. Virginia, N. California, Oregon, Mumbai, Osaka, Seoul, Singapore, Sydney, Tokyo, Canada, Europe, and South America. A note at the bottom of the list states, "There are 17 Regions that are not enabled for this account". At the bottom of the dropdown, there are two buttons: "Manage Regions" and "Manage Local Zones".

In the search bar, find the IAM service , as best practice, set up MFA

The screenshot shows two main sections of the AWS console. On the left, a search results page for 'iam' is displayed, listing services like IAM, IAM Identity Center, and Resource Access Manager. A red arrow points to the 'IAM' service entry. On the right, the IAM Dashboard is shown, featuring a 'Security recommendations' section with a red arrow pointing to the 'Add MFA' button, and an 'AWS Account' section with various account details.

Searched Services:

- IAM
- IAM Identity Center
- Resource Access Manager

IAM Dashboard Security Recommendations:

- Add MFA for root user
- Root user has no active access keys

AWS Account Details:

- Account ID: 147322384378
- Account Alias: Create
- Sign-in URL for IAM users in this region: <https://147322384378.signin.aws>

Give the device a name and select a MFA device of your choice, in this instance we will use an Authentication app

MFA device name

Device name
This name will be used within the identifying ARN for this device:
 ←

Maximum 64 characters. Valid characters: A-Z, a-z, 0-9, and + - _ (hyphen)

MFA device

Device options
In addition to username and password, you will use this device to authenticate into your account.

 **Passkey or security key**
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

 **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.

 **Hardware TOTP token**
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

Cancel **Next** ↓

Set up device Info

Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 1** Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#) ←
- 2** 
Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#) ←
- 3** Type two consecutive MFA codes below
 Enter a code from your virtual app below ←

 Wait 30 seconds, and enter a second code entry ←

Cancel **Previous** **Add MFA**

Now, we will set up our user, on the left side, under Access management, select user and select “create user”

Identity and Access Management (IAM)

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. When you create a session through the AWS CLI with that user.

My security credentials Root user | Info

The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of AWS accounts, see [AWS account types](#).

Account details

Account name: morelzyglobal
AWS account ID: 147322384378
Email address: thewolphenphantom@gmail.com
Canonical user ID: 39b6f9301353a1

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 up to 8 MFA devices registered.

Type	Identifier
Virtual	arn:aws:iam::147322384378:mfa/morelzy

Access keys (0)
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have up to 2 access keys per user.

Access key ID	Created on	Access key last used	Region last used
No access keys			

As a best practice, avoid using long-term credentials like access keys; instead, use tools which automatically rotate them.

[Create access key](#)

Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

[Search](#)

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Access key status
No resources to display									

[Create user](#)

Give the user a name (have a naming convention that easily allows you identify the user, their unit and job)

Ensure you select “access to AWS management console” so this user can be used as admin account instead of the root account, create a password (and best practice select create a new password on sign in, however for this project we won’t choose this option)

Then set permission using the steps below and create the user

Users > Create user

Specify user details

Step 1 Specify user details
 Step 2 Set permissions
 Step 3 Review and create
 Step 4 Retrieve password

User details

User name: IAM-PROD-JOHN (red arrow)

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . _ - (hyphen). If you're providing console access to a person, it's a best practice [to manage their access in IAM Identity Center](#).

Provide user access to the AWS Management Console - optional!

Console password

Autogenerated password You can view the password after you create the user.
 Custom password Enter a custom password for the user: (red arrow)

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](#)

[Cancel](#) Next

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](#) (red arrow)

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 (1399) Create policy

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

Policy name	Type	Attached entities
AccessAnalyzerServiceRolePolicy	AWS managed	0
AdministratorAccess	AWS managed - job function	0
AdministratorAccess-Amplify	AWS managed	0
AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
AIOpsAssistantIncidentReportPolicy	AWS managed	0
AIOpsAssistantPolicy	AWS managed	0
AIOpsConsoleAdminPolicy	AWS managed	0
AIOpsOperatorAccess	AWS managed	0

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details	Console password type	Require password reset
User name IAM-PROD-JOHN	Custom password	No

Permissions summary

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

Once user is created, copy the sign-in URL and log in as the user created

User created successfully

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

[View user](#)

Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create
Step 4 Retrieve password

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

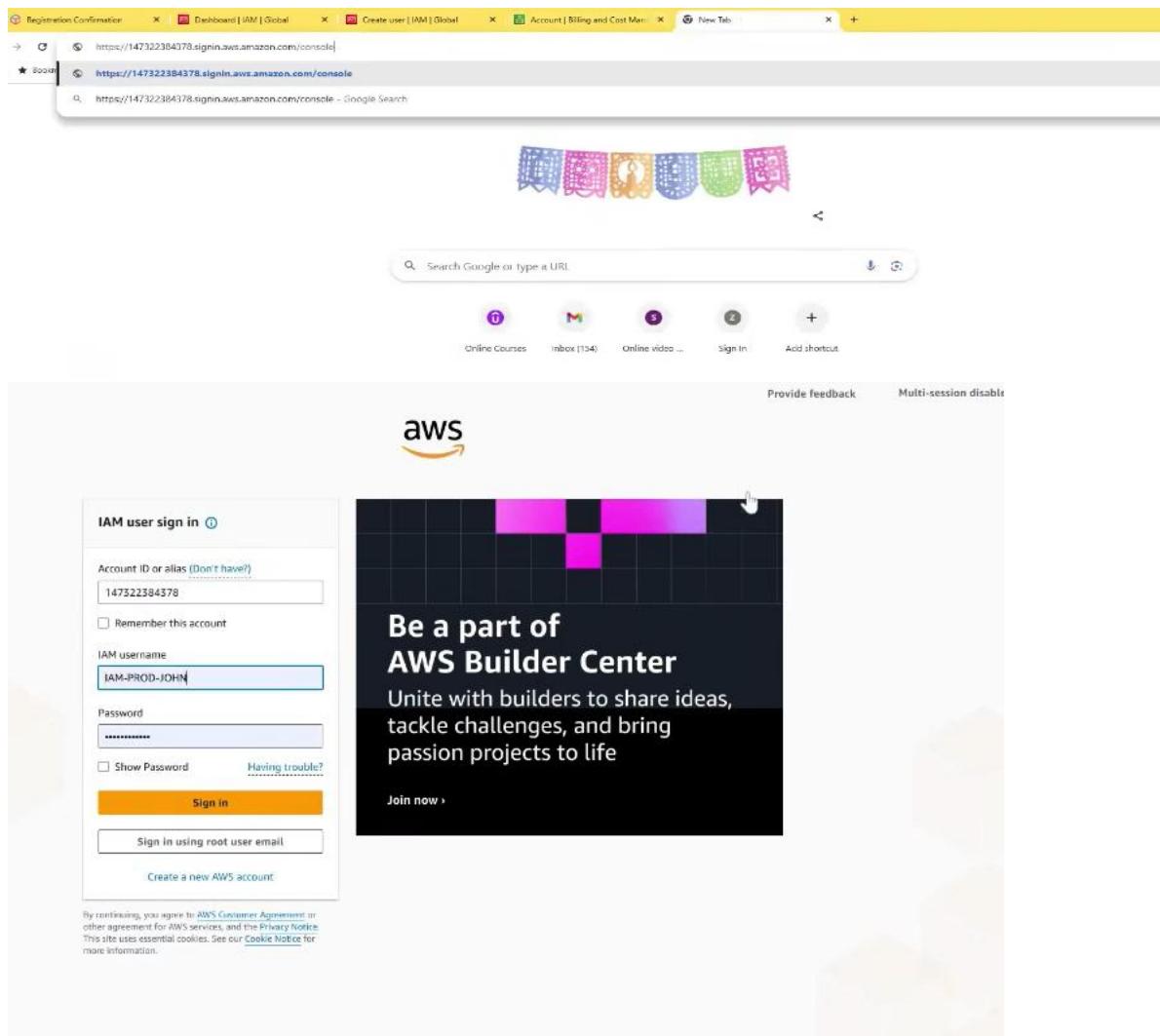
Console sign-in URL
 <https://147322584378.signin.aws.amazon.com/console> 

Email sign-in instructions

User name
 IAM-PROD-JOHN

Console password
 ***** [Show](#)

[Cancel](#) [Download .csv file](#) [Return to users list](#)



Change the location and let's create user groups

The screenshot shows the AWS Applications console. At the top, it displays the account ID: 1473-2250-6378 and the region: United States (Ohio). A red arrow points to the top right corner of the screen. Below the header, there's a section for 'Applications (0)' and a 'Select Region' dropdown set to 'us-east-2 (Current Region)'. A 'Create application' button is visible. The main area lists regions under 'Cost and usage' with a pie chart icon. A message states 'There are 16 Regions that are not enabled for this account.' At the bottom, there are 'Manage Regions' and 'Manage Local Zones' buttons.

The screenshot shows the AWS IAM User groups page. At the top, it displays the account ID: 1473-2250-6378 and the region: IAM-PROD-JOHN. A red arrow points to the 'User groups' link in the left navigation menu. The main content area shows a table titled 'User groups (0)'. The table has columns for 'Group name', 'Users', 'Permissions', and 'Creation time'. A message at the bottom says 'No resources to display'. On the far right of the table, there are 'Delete' and 'Create group' buttons, with a red arrow pointing to the 'Create group' button.

Give the group a name, select the user you want to add to the group and create group.

Create as many groups as required for the organization

User group name
Enter a meaningful name to identify this group.
MORELZY-PROD
Maximum 128 characters. Use alphanumeric and '-' characters.

Add users to the group - Optional (1)
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Attach permissions policies - Optional (1077)
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

User groups (1)
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

User groups (2)
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Using the same steps, create as many users as required and assign them to their respective groups

User created successfully

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

[View user](#)

Users (2) Info

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	Active key age	Access key status
IAM-DEPLOY-JANE	/	1	Now		8 minutes	7 minutes ago			
IAM-PROD-JOHN	/	1	Now		8 minutes	7 minutes ago			

CREATING THE EC2 INSTANCE

In the search bar, type EC2, under Instances select launch instance

(Instances are also referred to as Servers)

Search bar: ec

Services

- EC2 Virtual Servers in the Cloud
- Security Lake
- Security Hub

Features

- Direct Connect gateways
- Declarative policies for EC2
- AWS Shield network security director

Resources in ca-central-1

Were these results helpful? Yes No

EC2 > Instances

Instances

Find instance by attribute or tag (case-sensitive)

Launch instances

No instances

Select an instance

Give the instance a name and select the OS you would like to install and the configuration.

The screenshot shows the AWS Launch an instance wizard. It consists of three main sections:

- Name and tags**: A field where "PRODUCTION SERVER" is entered, highlighted by a red arrow.
- Application and OS Images (Amazon Machine Image)**: A section where "Windows" is selected from a grid of operating system icons, highlighted by a red arrow.
- Summary**: A final step showing the configuration summary, including the selected AMI (Amazon Linux 2023 AMI 2023.9.2...), instance type (t3.micro), and storage (1 volume(s) - 8 GiB). It includes a "Launch instance" button.

Application and OS Images (Amazon Machine Image)

Image	Description	Free tier eligible
Microsoft Windows Server 2025 Base	ami-0f8f4e8fb1da429bf (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	✓
Microsoft Windows Server 2025 Core Base	ami-0cc7cd9b1fbc71aef (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	✓
Microsoft Windows Server 2022 Base	ami-07eebd26318fb3e (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	✓
Microsoft Windows Server 2019 Base	ami-0f81ac6ba4b54a0e (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	✓
Microsoft Windows Server 2022 Core Base	ami-0d0897223bea26fb (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	✓
Microsoft Windows Server 2025 Base	ami-0f8f4e8fb1da429bf (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	✓

Description
Microsoft Windows 2025 Datacenter edition. [English]

Architecture 64-bit (x86) **AMI ID** ami-0f8f4e8fb1da429bf **Publish Date** 2025-10-17 **Username** Administrator **Verified provider**

Instance type [Info](#) | [Get advice](#)

Instance type

Instance type	Family	CPU	Memory	Current generation	On-Demand RHEL base pricing	On-Demand Linux base pricing	On-Demand SUSE base pricing	On-Demand Ubuntu Pro base pricing	On-Demand Windows base pricing	Free tier eligible
t3.micro	t3	2 vCPU	1 GiB Memory	true	0.0404 USD per Hour	0.0116 USD per Hour	0.0116 USD per Hour	0.0151 USD per Hour	0.0208 USD per Hour	✓
t3.small	t3	2 vCPU	2 GiB Memory	true	0.0416 USD per Hour	0.0232 USD per Hour	0.052 USD per Hour	0.0267 USD per Hour	0.0542 USD per Hour	✓
c7i-flex.large	c7i-flex	2 vCPU	4 GiB Memory	true	0.14907 USD per Hour	0.09627 USD per Hour	0.05277 USD per Hour	0.12157 USD per Hour	0.18017 USD per Hour	✓
m7i-flex.large	m7i-flex	2 vCPU	8 GiB Memory	true	0.16303 USD per Hour	0.13553 USD per Hour	0.09413 USD per Hour	0.11023 USD per Hour	0.18017 USD per Hour	✓

Subnet [Info](#)

Summary

Number of instances: 1

Software Image (1)
Microsoft Windows 2025 Datacenter edition. [English]

Virtual server type: t3.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 30 G

[Cancel](#)

Next we create Key pair for encryption, we give it a name and create, a copy of the key will be downloaded to the PC

Create key pair

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

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 (Not supported for Windows instances)

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](#)

Cancel **Create key pair**

For the network setting, we choose RDP from “my IP” and launch instance

Network settings

Network vpc-02aba1fba0fc0c845

Subnet No preference (Default subnet in any availability zone)

Auto-assign public IP Enable

Firewall (security groups) A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

- Allow RDP traffic from your instance
- Allow HTTPS traffic from the internet
- Allow HTTP traffic from the internet

Summary

Number of instances 1

Software Image (AMI) Microsoft Windows Server 2025 ...read more ami-0fbf4e8fb1da429bf

Virtual server type (instance type) t3.micro

Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 30 GiB

Launch instance



▶ Details

Please wait while we launch your instance.
Do not close your browser while this is loading.

The screenshot shows the AWS EC2 Instances page. At the top, there's a green success message: "Successfully initiated launch of instance i-00ba5330bd6f385c9". Below this, there's a "Launch log" section and a "Next Steps" section with various links to other AWS services like CloudWatch and CloudWatch Metrics.

Success

Successfully initiated launch of instance i-00ba5330bd6f385c9

▶ Launch log

Next Steps

Q. 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 an application, network gateway or classic Elastic Load Balancer.

[Create Load Balancer](#)

Create AWS budget

AWS Budgets allows you to create

Manage CloudWatch alarms

Create or update Amazon CloudWatch

Disaster recovery for your instances

Monitor for suspicious runtime activities

Get instance screenshot

Capture a screenshot from the instance

Get system log

View the instance's system log to

The screenshot shows the AWS EC2 Instances page with a single instance listed: "i-00ba5330bd6f385c9 (PRODUCTION SERVER)". The instance is running and assigned to the "t3.micro" type. The "Actions" dropdown menu is open, showing options: "Stop instance", "Start instance", "Reboot instance", "Hibernate instance", and "Terminate (delete) instance".

i-00ba5330bd6f385c9 (PRODUCTION SERVER)

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

Instance summary [Info](#)

Instance ID

i-00ba5330bd6f385c9

IPv6 address

-

Hostname type

IP name: ip-172-31-14-200.ca-central-1.compute.internal

Answer private resource DNS name
IPv4 (A)

Public IPv4 address

[16.52.77.234 | open address](#)

Instance state

[Running](#)

Private IP DNS name (IPv4 only)

[ip-172-31-14-200.ca-central-1.compute.internal](#)

Instance type

t3.micro

Private IPv4 addresses

[172.31.14.200](#)

Public DNS

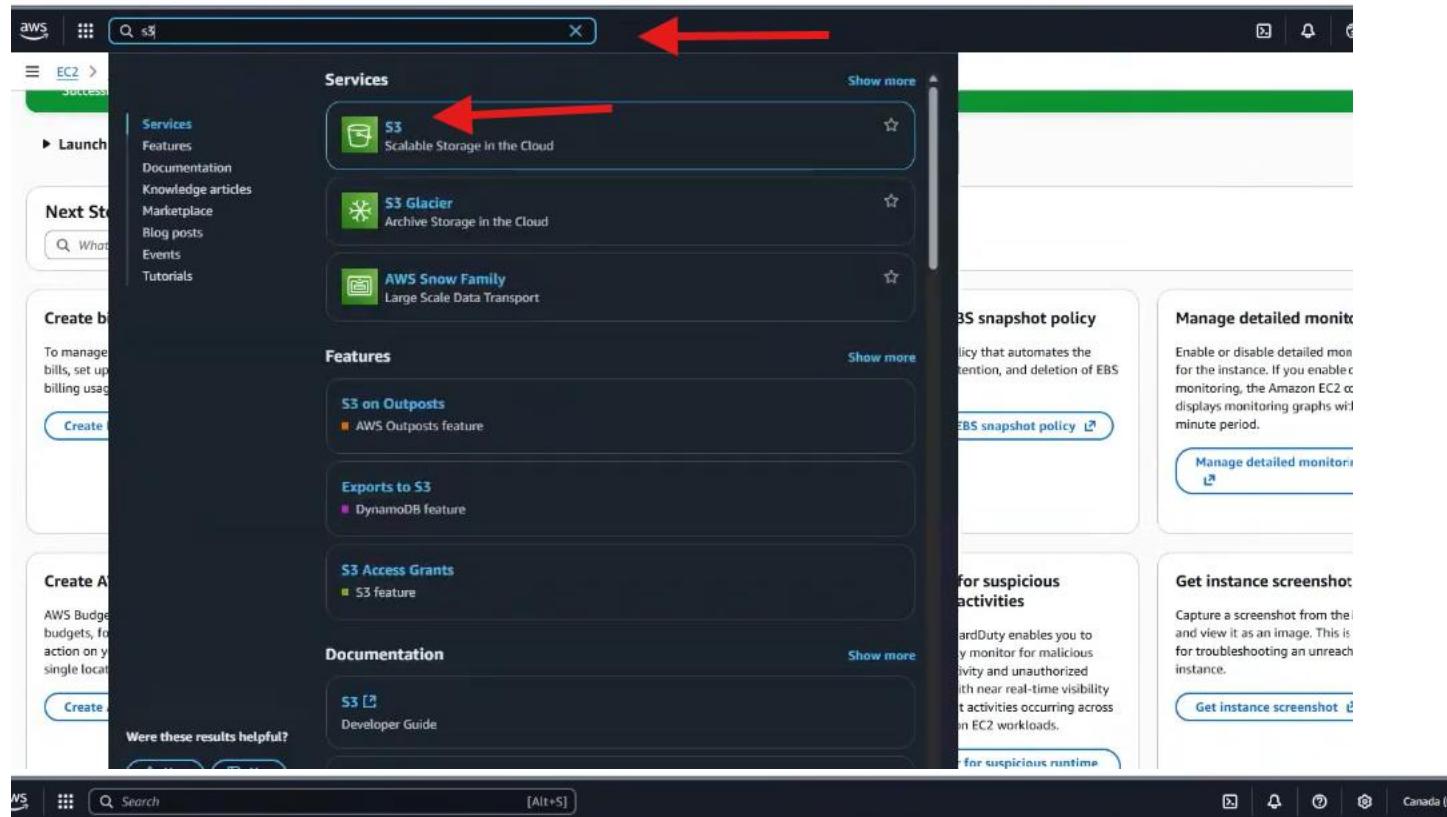
[ec2-16-52-77-234.ca-central-1.compute.amazonaws.com | open address](#)

Elastic IP addresses

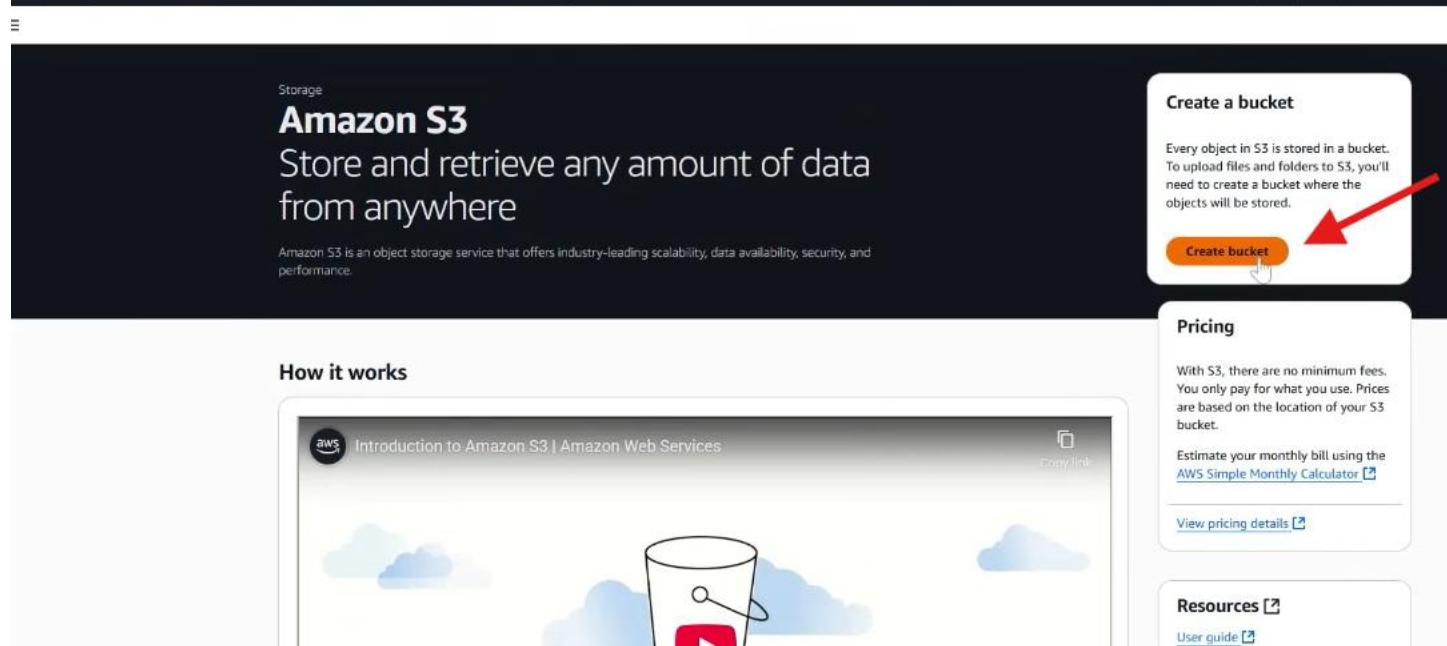
-

CREATING STORAGE BUCKETS

In the search bar, type S3 and create bucket, give it a name and leave default settings



The screenshot shows the AWS search results for 's3'. A red arrow points to the search bar at the top left. Another red arrow points to the 'S3 Scalable Storage in the Cloud' service card in the 'Services' section.



The screenshot shows the Amazon S3 landing page. At the top right, there is a 'Create a bucket' button highlighted with a red arrow. The main heading is 'Amazon S3' with the subtext 'Store and retrieve any amount of data from anywhere'. Below this, there is a brief description of what Amazon S3 is and a 'How it works' section featuring a video player.

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region
Canada (Central) ca-central-1

Bucket name Info 
morelzy-prod-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

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 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 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 that allow public access to S3 resources.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

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 both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

- Disable**
- Enable**

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Add new tag
You can add up to 50 tags.

Amazon S3 > Buckets

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

General purpose buckets All AWS Regions Directory buckets

General purpose buckets (2) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
morelzy-deploy-bucket	Canada (Central) ca-central-1	November 1, 2025, 11:27:54 (UTC-06:00)
morelzy-prod-bucket	Canada (Central) ca-central-1	November 1, 2025, 11:27:13 (UTC-06:00)

Account summary Updated daily Storage Lens preview

External access Updated daily External access public access or

Now we can add files to the bucket

morelzy-deploy-bucket Info

Objects Properties Permissions Metrics Management Access Points

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.

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose Add files or Add folder.

Files and folders (1 total, 223.6 KB)

All files and folders in this table will be uploaded.

Name	Folder	Type	Size
Networking_Basics_certificate_opezyajayi-gmail.com...	-	application/pdf	223.6 KB

Destination Info

Destination [s3://morelzy-deploy-bucket](#)

Destination details

Bucket settings that impact new objects stored in the specified destination.

Permissions

Grant public access and access to other AWS accounts.

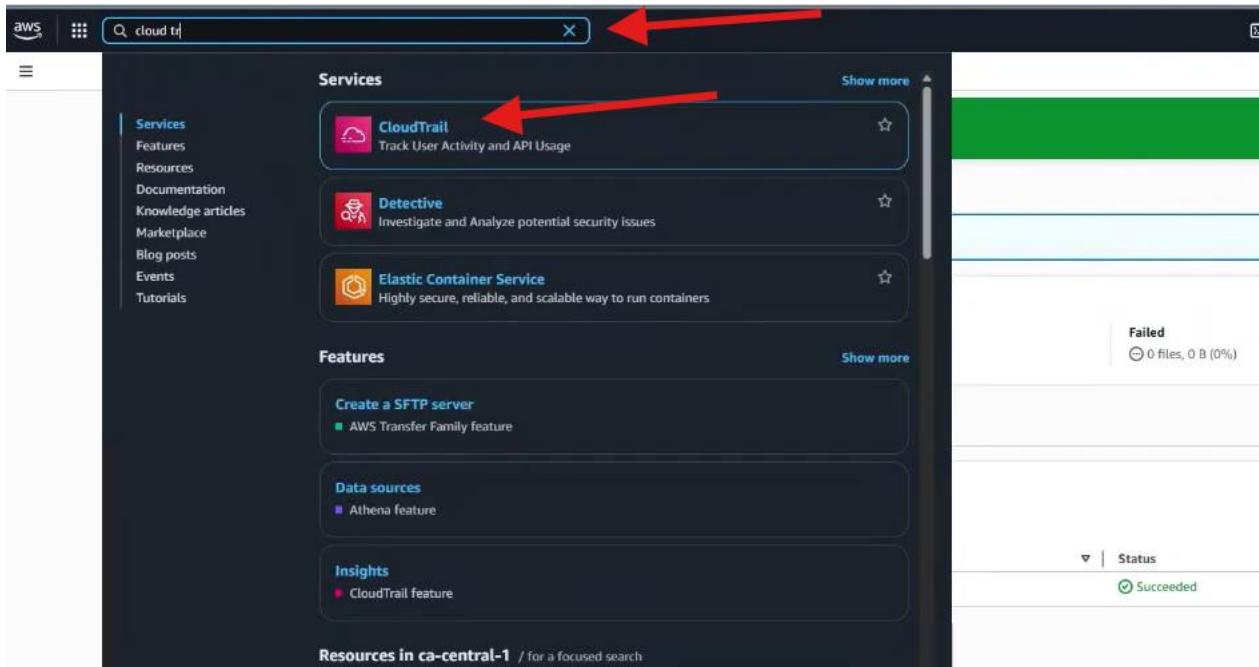
Properties

Specify storage class, encryption settings, tags, and more.

Cancel Upload

Create Trail

In the search bar, type Cloudtrail, this is a service to track all events and incidents



A screenshot of the AWS CloudTrail landing page. The page title is "AWS CloudTrail" and the subtitle is "Continuously log your AWS account activity". A call-to-action button "Create a trail" is highlighted with a red arrow. The page also features sections for "How it works", "Pricing", "Getting started", and "More resources".

How it works

- Capture**: Record activity in AWS services as AWS CloudTrail events.
- Store**: AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs.

Pricing

Getting started

- What is AWS CloudTrail?
- How AWS CloudTrail works
- Services that Integrate with AWS CloudTrail

More resources

- Documentation
- FAQs

The system already has been generation logs of all we have done so far, as depicted below

Screenshot of the AWS CloudTrail Dashboard showing the Event history section.

The dashboard displays the following sections:

- CloudTrail Insights**: Shows "No queries" and "No trails". A red arrow points to the "Create a trail" button.
- Event history**: Shows 22 events from November 01, 2025, including PutBucketEncryption, CreateBucket, PutBucketEncryption, CreateBucket, and RegisterManagedInstance. A red arrow points to the "View full Event history" link.

The Event history table includes columns for Event name, Event time, User name, Event source, Resource type, and Resource name. The table shows various AWS services and IAM users performing actions like creating buckets and instances.

Event name	Event time	User name	Event source	Resource type	Resource name
PutBucketEncryption	November 01, 2025, 11:27:54 (...)	s3.amazonaws.com	AWS::S3::Bucket	morelzy-deploy-bucket	
CreateBucket	November 01, 2025, 11:27:54 (...)	IAM-PROD-JOHN	AWS::S3::Bucket	morelzy-deploy-bucket	
PutBucketEncryption	November 01, 2025, 11:27:13 (...)	s3.amazonaws.com	AWS::S3::Bucket	morelzy-prod-bucket	
CreateBucket	November 01, 2025, 11:27:12 (...)	s3.amazonaws.com	AWS::S3::Bucket	morelzy-prod-bucket	
RegisterManagedInst...	November 01, 2025, 11:25:12 (...)	ssm.amazonaws.com	-	-	
SharedSnapshotVolu...	November 01, 2025, 11:24:00 (...)	-	ec2.amazonaws.com	-	
RunInstances	November 01, 2025, 11:23:58 (...)	IAM-PROD-JOHN	ec2.amazonaws.com	vpc-02aba1fba0fc0c845, ami-0fb4e8fb1da4298f, eni-09cff1522893511eb, i-05ebaac6eba94976, morelzy-dep-key, ...	
AuthorizeSecurityGro...	November 01, 2025, 11:23:56 (...)	IAM-PROD-JOHN	ec2.amazonaws.com	sg-029ece1e065618b09	
CreateSecurityGroup	November 01, 2025, 11:23:55 (...)	IAM-PROD-JOHN	ec2.amazonaws.com	vpc-02aba1fba0fc0c845, launch-wizard-2, sg-029ece1e065618b09	
CreateKeyPair	November 01, 2025, 11:23:02 (...)	IAM-PROD-JOHN	ec2.amazonaws.com	AWS::EC2::KeyPair	
RegisterManagedInst...	November 01, 2025, 11:16:10 (...)	i-00ba5330bd6f58...	ssm.amazonaws.com	morelzy-dep-key	
SharedSnapshotVolu...	November 01, 2025, 11:14:59 (...)	-	ec2.amazonaws.com	-	
RunInstances	November 01, 2025, 11:14:57 (...)	IAM-PROD-JOHN	ec2.amazonaws.com	vpc-02aba1fba0fc0c845, ami-0fb4e8fb1da4298f, eni-07cbc1fc7c71cc742, i-00ba5330bd6f385c9, morelzy-key, sg-0...	
AuthorizeSecurityGro...	November 01, 2025, 11:14:55 (...)	IAM-PROD-JOHN	ec2.amazonaws.com	sg-0d8f17d4be7bac81f	
CreateSecurityGroup	November 01, 2025, 11:14:53 (...)	IAM-PROD-JOHN	ec2.amazonaws.com	vpc-02aba1fba0fc0c845, sg-0d8f17d4be7bac81f, launch-wizard-1	

At the bottom left, it says "0 / 5 events selected".

The screenshot shows the AWS CloudTrail Dashboard. In the top right corner, there is a button labeled "Create trail". A large red arrow points directly at this button, indicating where the user should click to start creating a new CloudTrail.

Use an existing S3 bucket or create a new one

The screenshot shows the "Choose trail attributes" configuration page. It includes sections for "General details", "Storage location", "Trail log bucket and folder", "Log file SSE-KMS encryption", "Customer managed AWS KMS key", and "AWS KMS alias".

- General details:** A trail created in the console is a multi-region trail. Learn more [\[?\]](#)
- Trail name:** Enter a display name for your trail. A red arrow points to this input field.
- Storage location:**
 - 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 and folder:** Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.
aws-cloudtrail-logs-147322384378-5036a78b/AWSLogs/147322384378
- Log file SSE-KMS encryption:** Enabled
- Customer managed AWS KMS key:**
 - New
 - Existing
- AWS KMS alias:** A red arrow points to this input field.
 - AWS KMS alias cannot be emptyKMS key and S3 bucket must be in the same region.

Select the type of events you want to log and create trail

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.

ⓘ No additional charges apply to log management events on this trail because this is your first copy of management events.

API activity

Choose the activities you want to log.

Read

Write

Exclude AWS KMS events

Exclude Amazon RDS Data API events

Data events Info

Management events Info

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

ⓘ No additional charges apply to log management events on this trail because this is your first copy of management events.

API activity

Choose the activities you want to log.

Read

Write

Exclude AWS KMS events

Exclude Amazon RDS Data API events

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: ECS container instance

Resource type

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

ECS container instance



[Remove](#)

Log selector template

Log all events



Selector name - optional

Enter a name

1,000 character limit

Choose Insights types

Insights measure unusual activity against a seven-day baseline.

API call rate
A measurement of write-only management API calls that occur per minute against a baseline API call volume.

API error rate
A measurement of management 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: ec2.amazonaws.com

Network activity event source
Select a source for network activity events to log.

ec2.amazonaws.com

Log selector template
Log all events

Selector name - optional
Enter a name
1,000 character limit

► JSON view

Add network activity event selector

Cancel Previous Next

Trail successfully created

Trails												
Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status	Copy events to Lake	Delete	Create trail
GENERAL-TRAIL	Canada (Central)	Yes	arn:aws:cloudtrail:ca-central-1:147322384378:trail/GENERAL-TRAIL	Enabled	No	aws-cloudtrail-logs-147322384378-5036a78b	-	-	Logging			

CREATE POLICES

AWS comes with predefined policies we can choose from, however we will be creating some policies with the JOHN account and assigning them the JANE account to test them.

Most users once created will be assigned denied access due to least privilege.

First we log in to JANE account and confirm what is denied and create a policy to allow it. In this case JANE has no access to list of users as shown below

Screenshot of the AWS IAM Users page showing a permission denied error for listing users.

The page title is "Users (0) Info". A message states: "An IAM user is an identity with long-term credentials that is used to interact with AWS in an account." Below this is a search bar and a table header with columns: User name, Path, Groups, Last activity, MFA, and Password age.

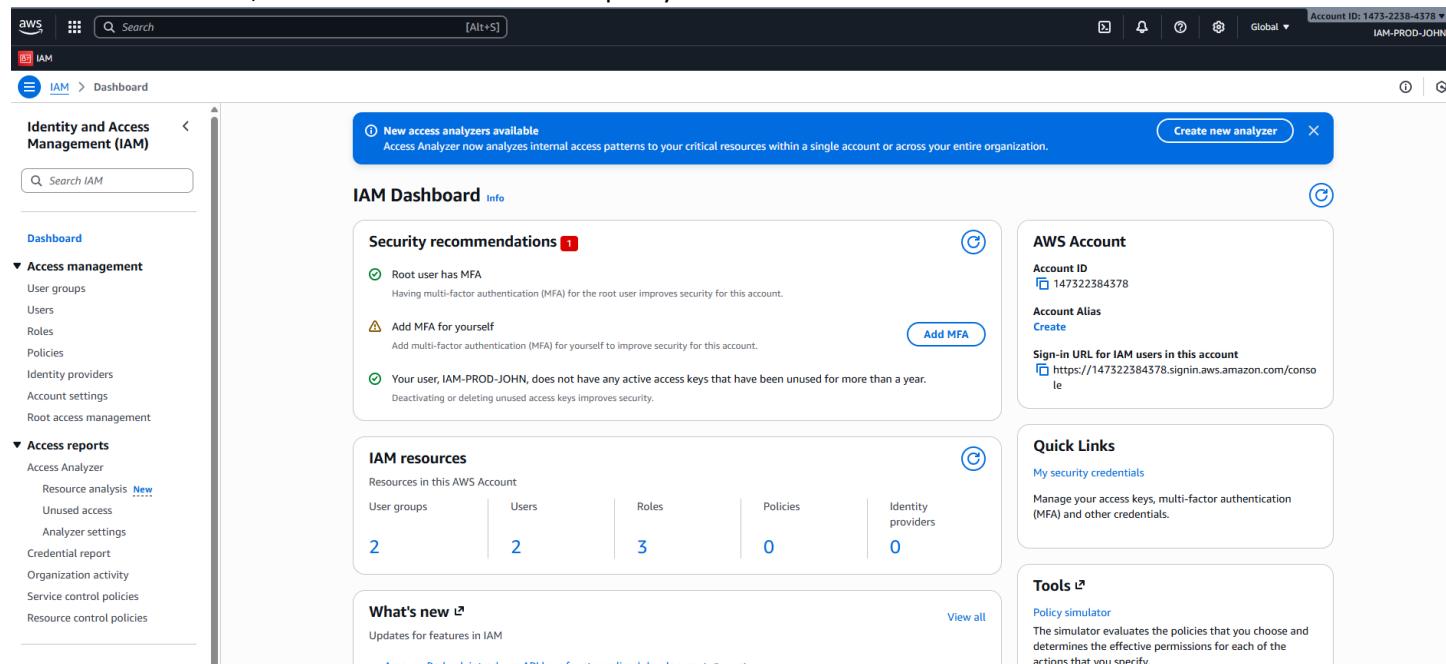
A red box highlights an error message: "Access denied to iam>ListUsers". It says: "You don't have permission to iam>ListUsers. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)"

Table details:

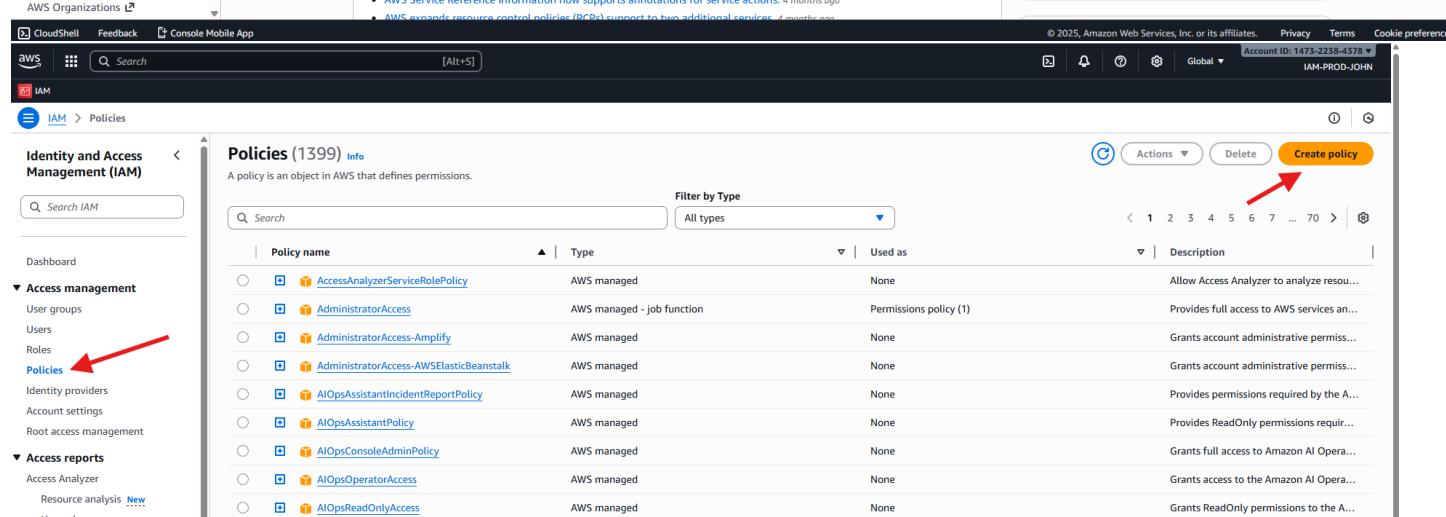
User name	Path	Groups	Last activity	MFA	Password age
User: arn:aws:iam::147322384378:user/IAM-DEPLOY-JANE					
Action: iam>ListUsers					
On resource(s): arn:aws:iam::147322384378:user/					
Context: no identity-based policy allows the action					

Page footer: CloudShell, Feedback, Console Mobile App, © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, Cookie preferences.

So on JOHN account, we create an allow 'listuser' policy and attach to user JANE



The screenshot shows the AWS IAM Dashboard. On the left sidebar, under 'Access management', the 'Policies' link is highlighted with a red arrow. The main area displays security recommendations, IAM resources (2 user groups, 2 users, 3 roles, 0 policies, 0 identity providers), and a 'What's new' section. A blue button labeled 'Create new analyzer' is visible at the top right.



The screenshot shows the 'Policies (1399)' list page. The 'Policies' link in the left sidebar is also highlighted with a red arrow. The main area shows a table of policies with columns for Policy name, Type, Used as, and Description. A blue 'Actions' dropdown and a 'Delete' button are at the top right, and a 'Create policy' button is highlighted with a red arrow at the far right.

When specifying permissions we can use VISUAL OR JSON (SCRIPTS), in this example we use Visual.

Drop down list>> check listuser>> check effect 'allow'

Give policy a name and description and click create policy

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

Policy editor

IAM Set permissions for IAM

Specify what actions can be performed on specific resources in IAM.

Actions allowed Specify actions from the service to be allowed.

Filter Actions

Manual actions | Add actions

All IAM actions (iam:*)

Access level

List (39)

All list actions

GetAccountSummary | Info

ListAccountAliases | Info

ListAttachedUserPolicies | Info

ListGroupPolicies | Info

ListInstanceProfiles | Info

ListMFADevices | Info

ListOpenIDConnectProviderTags | Info

ListPoliciesGrantingServiceAccess | Info

ListRolePolicies | Info

ListSAMLProviders | Info

ListServerCertificateTags | Info

ListSSHPublicKeys | Info

ListUsers | Info

GetLoginProfile | Info

ListAttachedGroupPolicies | Info

ListCloudFrontPublicKeys | Info

ListGroups | Info

ListInstanceProfilesForRole | Info

ListMFADeviceTags | Info

ListOrganizationsFeatures | Info

ListPolicyTags | Info

ListRoles | Info

ListSAMLPublisherTags | Info

ListServiceSpecificCredentials | Info

ListSTSRegionalEndpointsStatus | Info

ListUserTags | Info

ListAccessKeys | Info

ListAttachedRolePolicies | Info

ListEntitiesForPolicy | Info

ListGroupsForUser | Info

ListInstanceProfileTags | Info

ListOpenIDConnectProviders | Info

ListPolicies | Info

ListPolicyVersions | Info

ListRoleTags | Info

ListServerCertificates | Info

ListSigningCertificates | Info

ListUserPolicies | Info

ListVirtualMFADevices | Info

Effect Allow Deny

Expand all | Collapse all

Read (32)

Review and create Info
Review the permissions, specify details, and tags.

Policy details

Policy name Enter a meaningful name to identify this policy.

list_users

Maximum 128 characters. Use alphanumeric and '+-,.,@,-' characters.

Description - optional Add a short explanation for this policy.

Allow access to list of users

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

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.

Add tags - optional Info Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag You can add up to 50 more tags.

Create policy

Policy list created.

Policies (1/1400) Info
A policy is an object in AWS that defines permissions.

Filter by Type All types 7 matches

Policy name	Type	Used as	Description
AWSIdentityCenterAllowListForIdentityContext	AWS managed	None	Provides the list of actions that are all...
AWSSIoTDeviceDefenderPublishFindingsToSNSSubscription	AWS managed	None	Provides messages publish access to S...
AWSSIoTWirelessFullPublishAccess	AWS managed	None	Provides IoT Wireless full access to pu...
AWSPriceListServiceFullAccess	AWS managed	None	Provides full access to AWS Price List S...
AWSQuickSightListIAM	AWS managed	None	Allow QuickSight to list IAM entities
watchNetworkFlowMonitorAgentPublishPolicy	AWS managed	None	You can use this policy in IAM roles tha...
list_users	Customer managed	None	Allow access to list of users

Now we attach policy to JANE

The screenshot shows the AWS IAM console interface. On the left, the navigation pane is visible with sections like Dashboard, Access management, Users, Groups, Policies, Identity providers, and Account settings. A red arrow points to the 'User name' column in the 'Users (2) Info' table, highlighting the row for 'IAM-DEPLOY-JANE'. The main content area shows the 'IAM-DEPLOY-JANE Info' page. At the top, there's a summary section with ARN (arn:aws:iam::147322384378:user/IAM-DEPLOY-JANE), Created date (November 01, 2025, 10:55 (UTC-06:00)), and a note about Console access being Enabled without MFA. Below this is a 'Permissions' tab, which is currently selected. A red arrow points to the 'Add permissions' button at the top right of this section. The 'Permissions policies (0)' section indicates no policies are attached. A red arrow points to the 'Add permissions' button at the bottom right of this section. Further down, there are sections for 'Permissions boundary (not set)', 'Generate policy based on CloudTrail events' (with a 'Generate policy' button), and a note about no requests in the past 7 days.

At the bottom of the page, the URL is 'Users > IAM-DEPLOY-JANE > Add permissions'. The 'Add permissions' step is shown, with three options: 'Add user to group', 'Copy permissions', and 'Attach policies directly'. The 'Attach policies directly' option is selected, indicated by a blue border and checked radio button. A red arrow points to this selection. The 'Permissions policies (1400)' table lists several policies, with a red arrow pointing to the 'list_users' policy. The table includes columns for Policy name, Type, and Attached entities. At the bottom right of the table, there are 'Cancel' and 'Next' buttons, with a red arrow pointing to the 'Next' button.

Review
The following policies will be attached to this user. Learn more [Learn more](#)

User details
User name
IAM-DEPLOY-JANE

Permissions summary (1)

Name	Type	Used as
list_users	Customer managed	Permissions policy

[Cancel](#) [Previous](#) [Add permissions](#)

[Alt+S] Account ID: 1473-2238-4578 Global IAM-PROD-JOHN

1 policy added

IAM-DEPLOY-JANE [Info](#) [Delete](#)

Summary

ARN arn:aws:iam::147322384378:user/IAM-DEPLOY-JANE	Console access Enabled without MFA	Access key 1 Create access key
Created November 01, 2025, 10:55 (UTC-06:00)	Last console sign-in Today	

Permissions [Groups \(1\)](#) [Tags](#) [Security credentials](#) [Last Accessed](#)

Permissions policies (1)

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

Policy name	Type	Attached
list_users	Customer managed	Direct

[Remove](#) [Add permissions](#)

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](#)

[Generate policy](#)

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

Policy is now assigned. To confirm its in effect, we log into JANE account and users list is now displayed

The screenshot shows the AWS IAM 'Users' page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' and a search bar. The main area is titled 'Users (2) Info'. It lists two users: 'IAM-DEPLOY-JANE' and 'IAM-PROD-JOHN'. Both users are marked with a red circle around them. The status for both users is 'Access denied'. There are buttons for 'Delete' and 'Create user' at the top right.

We can also create a policy that allows Jane to view instances but restricts JANE from creating or deleting.

Following the same steps prior, we create an EC2 policy

The screenshot shows the 'Specify permissions' page for creating a new policy. The 'Policy editor' section is open, showing a tree structure of actions under 'EC2'. The 'Tagging' section is expanded and highlighted with a red circle. Under 'Tagging', the 'DeleteTags' action is also highlighted with a red circle. The 'Effect' dropdown shows 'Allow' is selected. At the bottom, there are buttons for 'Visual', 'JSON', 'Actions', and a save icon.

: policy

Policy details

Policy name
Enter a meaningful name to identify this policy.
 

Maximum 128 characters. Use alphanumeric and '+,-,.,@-' characters.

Description - optional
Add a short explanation for this policy.
 

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

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.

Explicit deny (1 of 450 services)

Service	Access level	Resource	Request condition
EC2	Full: Tagging	All resources	None

Allow (0 of 450 services)

Service	Access level	Resource	Request condition
			No resources to display

Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

All policies assigned to JANE are now listed,

IAM-DEPLOY-JANE Info [Delete](#)

Summary

ARN arn:aws:iam::147322384378:user/IAM-DEPLOY-JANE	Console access Enabled without MFA	Access key 1 Create access key
Created November 01, 2025, 10:55 (UTC-06:00)	Last console sign-in Today	

Permissions [Groups \(1\)](#) [Tags](#) [Security credentials](#) [Last Accessed](#)

Permissions policies (3)

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

Policy name	Type	Attached to
allow_describe_instances	Customer managed	Directly to user
disable_create_delete_ability	Customer managed	Directly to user
list_users	Customer managed	Directly to user

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](#)

[Generate policy](#)

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

Using JANE account, we try to delete an instance but we get an error

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
MORELZY-DE...	i-05ebaac6ebaf94976	Running	t3.micro	You are not auth.	User: arn:aws:	ca-central-1b	ec2-35-182-68-59.ca.c...	35.182.68.59	You are not auth.
PRODUCTION ...	i-00ba5330bd6f385c9	Running	t3.micro	You are not auth.	User: arn:aws:	ca-central-1b	ec2-35-182-230-251.ca...	35.182.230.251	You are not auth.

i-00ba5330bd6f385c9 (PRODUCTION SERVER)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary **Info**

Failed to stop the instance i-00ba5330bd6f385c9

You are not authorized to perform this operation. User: arnawsiam:147322384378user/IAM-DEPLOY-JANE is not authorized to perform: ec2StopInstances on resource: arn:aws:ec2:ca-central-1:147322384378:instance/i-00ba5330bd6f385c9 because no identity-based policy allows the ec2StopInstances action. Encoded authorization failure message: jHPgKu3rEaSXH8Be3sbg9swnePj4l0B6R-H-jnRHauSsgqAjsmV6l7fOQOkvwsxQLUmR2-lOm0a0jz1ttxdjb2khsBQG500GRnJu0JUm2zRH3t3E5W28w5l-PQjUUhic8t9MTW8AtqGqSufQ04-LmUuQaHu_uxSrRil_6nUfUeBXAMcdi8J5uPWoY95h7aiIs0-hb137Tr3mtfOlcbyr1sF46U_lPtinbGu9Ah5xdUfz3BB057ahvcunTldSNwvey17c1XPYlLzZfZTnshkVdns-sqa5opLeNyt5dg5nfzD2HxwlctUylalU3D7Pf7QEv25RxDH9Nk82Mp0tNhINayQnD7IKGWhh89yQltz883fHEHy-XvZg2m_BCP7QQ15dyJFLKMe5MfpMMav97YCmQWjbJ775WtCw1wfWap_OCoBJ6tpz1BmxxyWpL7752KwRpQ-626x6lbWmYmjCkw52SWbE33HqcLSFa_TFyID07aUczbNH8NbKlkd32Va6EzMckAHviAoNlllylhsh4HKxSW877_jRbyLoogyJOYtfaB5_pJWcJ-z7XocBqihgKGNboc7Yf9d94sy75PDyjn8OeSr2ZqcxeTuimnfk828gnsPaeZ1-0fGfdJz8jxOoQnAlqNBVFqSEzypWCPf9ezIBqWFAvwTlmUCoszSFipNNyocIVzA8q6DbCG7RqnRx9tmQBM_pbC6Qgw8eXvdByq724kWbQvbGodzinMzsyN1VbVmwmMsPlwHcvGLBCRVhVIL-4cIQbCmZDK_z7dxNmDyh5Pgr4Bktjuubfyfj2sWKRAVfty-E-fhlN8pMt6rL_G2z31e3a4pow

Diagnose with Amazon Q

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
MORELZY-DE...	i-05ebaac6ebaf94976	Running	t3.micro	You are not auth.	User: arn:aws:	ca-central-1b	ec2-35-182-68-59.ca.c...	35.182.68.59	You are not auth.
PRODUCTION ...	i-00ba5330bd6f385c9	Running	t3.micro	You are not auth.	User: arn:aws:	ca-central-1b	ec2-35-182-230-251.ca...	35.182.230.251	You are not auth.