

# AWS IAM Cloud Security Project

---

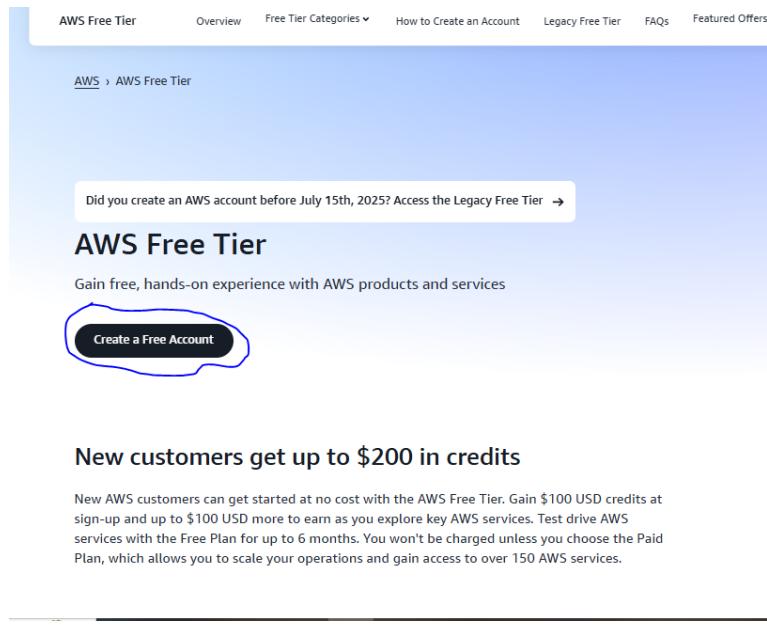
## 1. Project Overview

I completed this project on cloud security controls in Amazon Web Services (AWS), focusing on Identity and Access Management (IAM). The goal was to create a least-privilege policy, attach it to a user group, and verify that the policy correctly restricts actions on two Amazon EC2 instances (audit and sales).

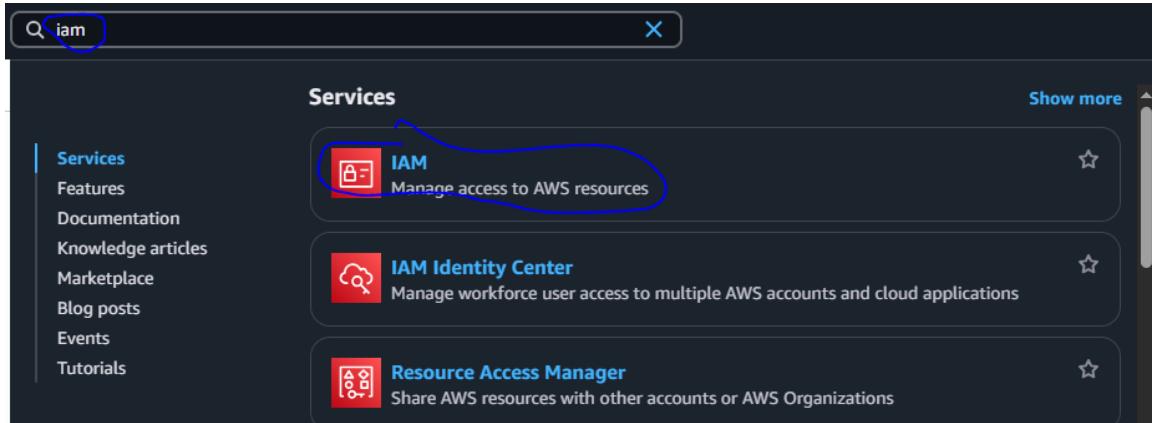
## 2. Tools & Concepts

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

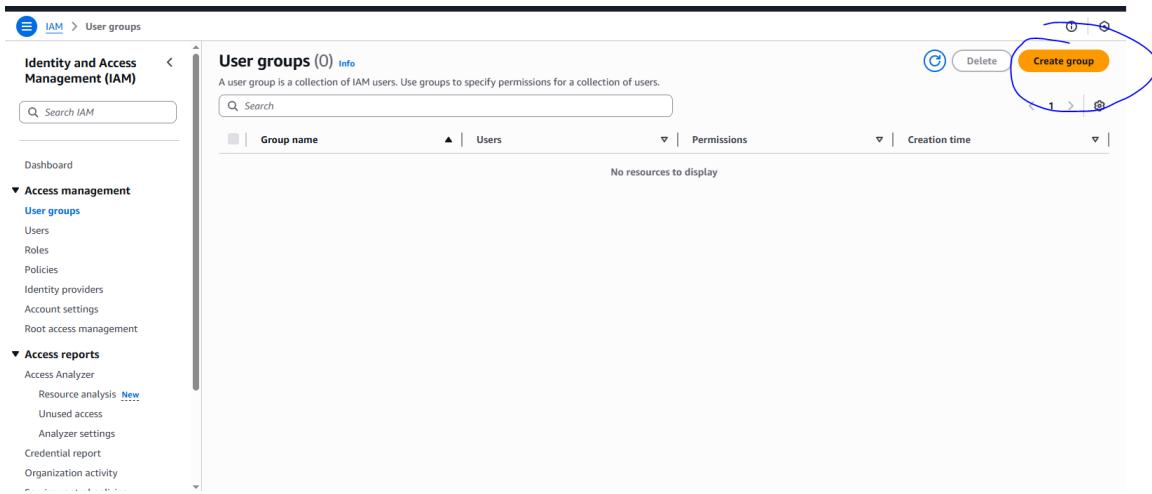
I created account using: <https://aws.amazon.com/console/>



IAM service standard practice is that we don't make configuration on the root users. We create an identity and access management user who has admin privileges.



Next we create user groups to which we can implement policies



**Create user group**

**Name the group**

**User group name**  
Enter a meaningful name to identify this group.  
**Lteching-audit-webapp**  
Maximum 128 characters. Use alphanumeric and '+,-,@,\_' characters.

**Add users to the group - Optional (0)** Info  
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Group	Last activity	Creation time
No resources to display			

**Attach permissions policies - Optional (1078)** Info  
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.

Policy name	Type	Used as	Description
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis...
<input type="checkbox"/> AdministratorAccess-AWSE...	AWS managed	None	Grants account administrative permis...
<input type="checkbox"/> AIOpsAssistantIncidentRep...	AWS managed	None	Provides permissions required by the A...
<input type="checkbox"/> AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
<input type="checkbox"/> AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...

During user group creation, we are also implementing the permission policies directly. Note you can decide to create user group and implement policies later on

**Add users to the group - Optional (0)** Info  
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Group	Last activity	Creation time
No resources to display			

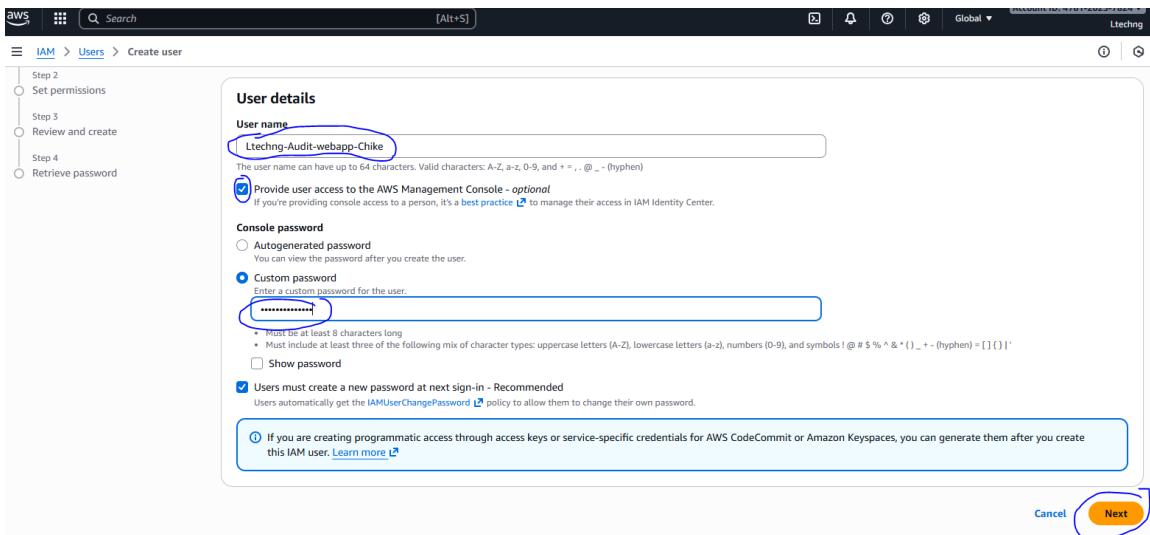
**Attach permissions policies - Optional (1078)** Info  
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Policy name	Type	Used as	Description
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis...
<input type="checkbox"/> AdministratorAccess-AWSE...	AWS managed	None	Grants account administrative permis...
<input type="checkbox"/> AIOpsAssistantIncidentRep...	AWS managed	None	Provides permissions required by the A...
<input type="checkbox"/> AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
<input type="checkbox"/> AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...

The screenshot shows the AWS IAM User Groups page. A green banner at the top indicates that 'Ltechng-Audit-webapp user group created.' Below the banner, the heading 'User groups (1) info' is displayed. A table lists one user group: 'Ltechng-Audit-webapp'. The table includes columns for Group name, Users, Permissions, and Creation time. The 'Create group' button is visible in the top right corner.

Next we would be creating users where we can also implement policies individually. The users would be under the group we just created. Once created, users can access via the management console or via command line interface

The screenshot shows the AWS IAM Users page. A green banner at the top indicates that 'Ltechng-Audit-webapp user group created.' Below the banner, the heading 'Users (0) info' is displayed. A table is shown with the following columns: User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, and Access key ID. A message 'No resources to display' is centered below the table. The 'Create user' button is highlighted with a blue oval.



Next we would be setting the permission option. Option available are

1. **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.
2. **Copy permissions:** Copy all group memberships, attached managed policies, and inline policies from an existing user.
3. **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.

For this project we would select the “Add user to group” so the policy we created then on the group Ltechng-Audit-Webapp will automatically be implemented on the user

**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.

**User groups (1)**

Group name	Users	Attached policies	Created
Ltechng-Audit-webapp	0	AdministratorAccess	2025-11-04 (1 hour ago)

**Set permissions boundary - optional**

[Create group](#)

[Cancel](#) [Previous](#) **Next**

**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  
 Set permissions  
 Review and create  
 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://476120257824.signin.aws.amazon.com/console> [Email sign-in instructions](#)

User name Ltechng-Audit-webapp-Chike

Console password  [Show](#)

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

### 3. Tagging Strategy

I applied a descriptive tag to each EC2 instance:

Instance   Tag Key	Tag Value
audit	Environment   Audit

## 4. Creating the IAM Policy

You can manually create policies to suit the needs of the organization. If the over 1400 policies (As of the date I compiled this project) available doesn't tailor to your policies need.

The screenshot shows two screenshots of the AWS IAM interface. The top screenshot displays the 'Policies' list with 1400 entries. The 'Create policy' button is highlighted with a blue oval. The bottom screenshot shows the 'Specify permissions' step of the 'Create policy' wizard, where users can select a service and add permissions. The 'Next' button is highlighted with a blue oval.

**Policies (1400)**

A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePo...	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 permis...
AdministratorAccess-AWSEA...	AWS managed	None	Grants account administrative permis...
AIOpsAssistantIncidentRepor...	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...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayExe...	AWS managed	None	Provide gateway execution access to A...

**Specify permissions**

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

**Policy editor**

**Select a service**

Specify what actions can be performed on specific resources in a service.

Service: Choose a service

+ Add more permissions

Cancel Next

I authored the following JSON policy to block instance stop/start actions on the audit server.

The policy can allow users :

- View all EC2 resources.
- Fully manage (start, stop, reboot, terminate, etc.) EC2 instances tagged Env=Audit.
- **Cannot** create or delete tags — meaning they can't tag new instances as Env=Audit to bypass the restriction.

The screenshot shows the AWS IAM Policy editor interface. The left pane displays the JSON code for a policy named "Statement1". The right pane shows the visual representation of the policy, including service actions like "ec2:Describe\*", conditions like "StringEquals" for the tag "Env" being "Audit", and deny statements for actions like "ec2:DeleteTags" and "ec2:CreateTags".

```
1 Version: "2012-10-17",
2 Statement: [
3   {
4     Effect: "Allow",
5     Action: "ec2:*",
6     Resource: "*",
7     Condition: {
8       StringEquals: {
9         "ec2:ResourceTag/Env": "Audit"
10      }
11    }
12  },
13  {
14    Effect: "Allow",
15    Action: "ec2:Describe*",
16    Resource: "*"
17  },
18  {
19    Effect: "Deny",
20    Action: [
21      "ec2:DeleteTags",
22      "ec2:CreateTags"
23    ],
24    Resource: "*"
25  },
26  {
27    Sid: "Statement1",
28  }
29 ]
```

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": "ec2:\*",

"Resource": "\*",

"Condition": {

```
"StringEquals": {  
    "ec2:ResourceTag/Env": "Audit"  
}  
}  
},  
{  
    "Effect": "Allow",  
    "Action": "ec2:Describe*",  
    "Resource": "*"  
},  
{  
    "Effect": "Deny",  
    "Action": [  
        "ec2>DeleteTags",  
        "ec2>CreateTags"  
    ],  
    "Resource": "*"  
}  
]
```

Screenshot of the AWS IAM 'Create policy' wizard - Step 1: Specify permissions.

The page shows a list of permissions assigned to the EC2 service:

- EC2 (Allow All actions)
- EC2 (Allow 1 Action)
- EC2 (Deny 2 Actions)

Buttons at the bottom include 'Cancel' and 'Next' (highlighted with a blue oval).

Screenshot of the AWS IAM 'Create policy' wizard - Step 2: Review and create.

The review section shows the following details:

- Policy name:** EC2AuditAccessPolicy
- Description - optional:** Allows full EC2 access to resources tagged Env=Audit and read-only access to all others. Denies tag changes.

The 'Permissions defined in this policy' section lists the explicit deny rule:

Explicit deny (1 of 450 services)			
Service	Access level	Resource	Request condition
EC2	Deny	All actions	

The screenshot shows the AWS IAM Policies creation wizard. At the top, a green banner indicates "Policy EC2AuditAccessPolicy created." Below it, the "Policies (1401)" list is shown with a search bar and filter options. A table lists the policy details: Name is "EC2AuditAccessPolicy", Type is "Customer managed", and Description is "Allows full EC2 access to resources tagged...".

**Explicit deny (1 of 450 services)**

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

**Allow (1 of 450 services)**

Service	Access level	Resource	Request condition
EC2	Full: List, Permissions management, Read, Write	All resources	ec2:ResourceTag/Env = Audit

**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.

Buttons at the bottom: Cancel, Previous, **Create policy** (highlighted with a blue oval).

## 5. Creating CloudTrails

AWS CloudTrail is the auditing and activity logging service for your AWS account.

It automatically records actions taken by:

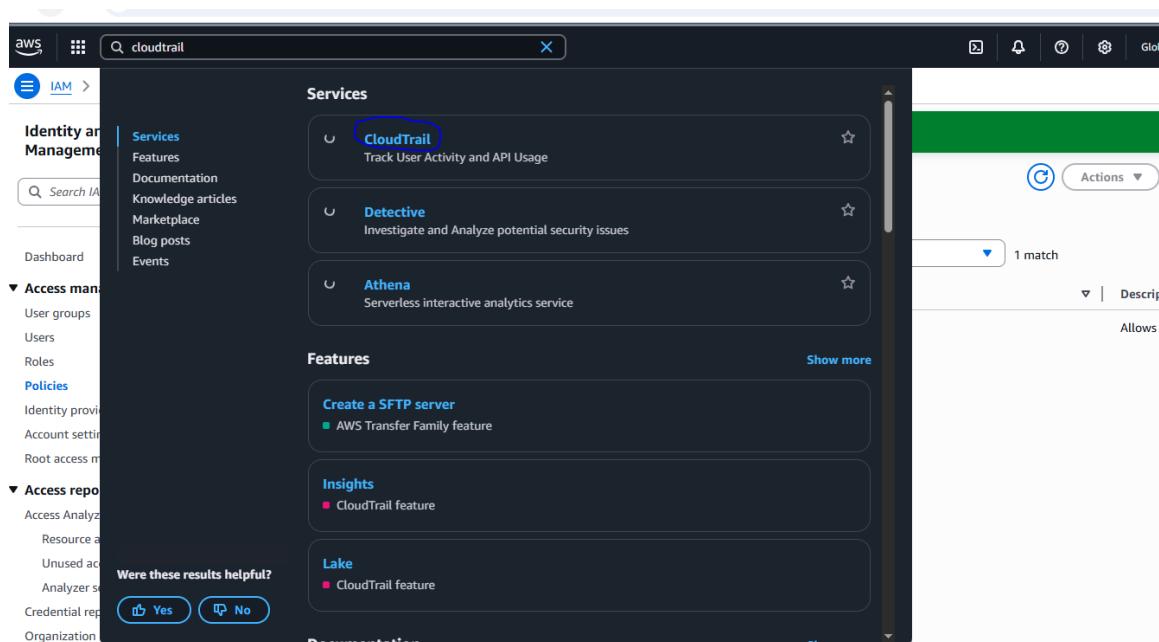
- Users (IAM users or federated users)
- Roles (like those assumed by applications)

- AWS services (automated actions)

CloudTrail helps you **monitor, secure, and troubleshoot** AWS operations.

## What CloudTrail (the service) does

- Logs every **API call** and **console action**.
- Captures:
  - **Who** performed the action (user or service)
  - **What** action was performed
  - **When** it occurred
  - **From where** (IP, region)
  - **Which resource** was affected
- Stores logs in **S3**, and optionally sends them to **CloudWatch Logs** or **EventBridge** for alerts.



The screenshot shows the AWS CloudTrail Dashboard. On the left, there's a sidebar with options like 'Dashboards', 'Event history', 'Insights', 'Lake', 'Pricing', 'Documentation', 'Forums', and 'FAQs'. The main area has three sections: 'Query results history' (empty), 'Trails' (empty), and 'CloudTrail Insights' (disabled). A blue oval highlights the 'Create trail' button in the 'Trails' section.

This screenshot shows the 'Choose trail attributes' step of the 'Create trail' wizard. It's Step 1 of 3. The user has selected 'Create new S3 bucket' under 'Storage location'. Other options include 'Use existing S3 bucket'. The 'Trail name' is set to 'webapp-trails'. Other settings shown include 'Trail log bucket and folder' (prefix 'aws-cloudtrail-logs-476120257824-0368647f'), 'Log file SSE-KMS encryption' (Enabled), and 'Customer managed AWS KMS key' (New).

Click on next

CloudTrail > Dashboard > Create trail

Step 1  
 Choose trail attributes  
 Step 2  
 Choose log events  
 Step 3  
 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.

(i) 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.

Data event collection is not configured for this trail

### Insights events

You can only enable CloudTrail Insights on trails that log management events. [Learn more](#)

### Network activity events

**Network activity events: ec2.amazonaws.com**

Log selector template	Selector name
Log all events	--

All events

Cancel Previous **Create trail**

CloudTrail > Trails

**Trail successfully created**

(i) 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
<a href="#">webapp-trails</a>	Europe (Stockholm)	Yes	arn:aws:cloudtrail:eu-north-1:476120257824:trail/webapp-trails	Disabled	No	aws-cloudtrail-logs-476120257824-0368647f	-	-	

Copy events to Lake Delete **Create trail**

① 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

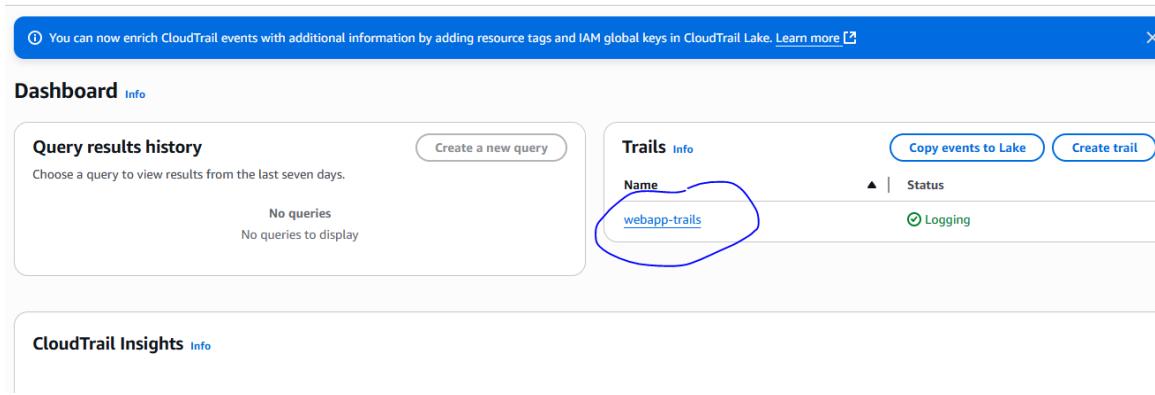
**Create a new query**

**Trails** [Info](#)

**Name** [Copy events to Lake](#) [Create trail](#)

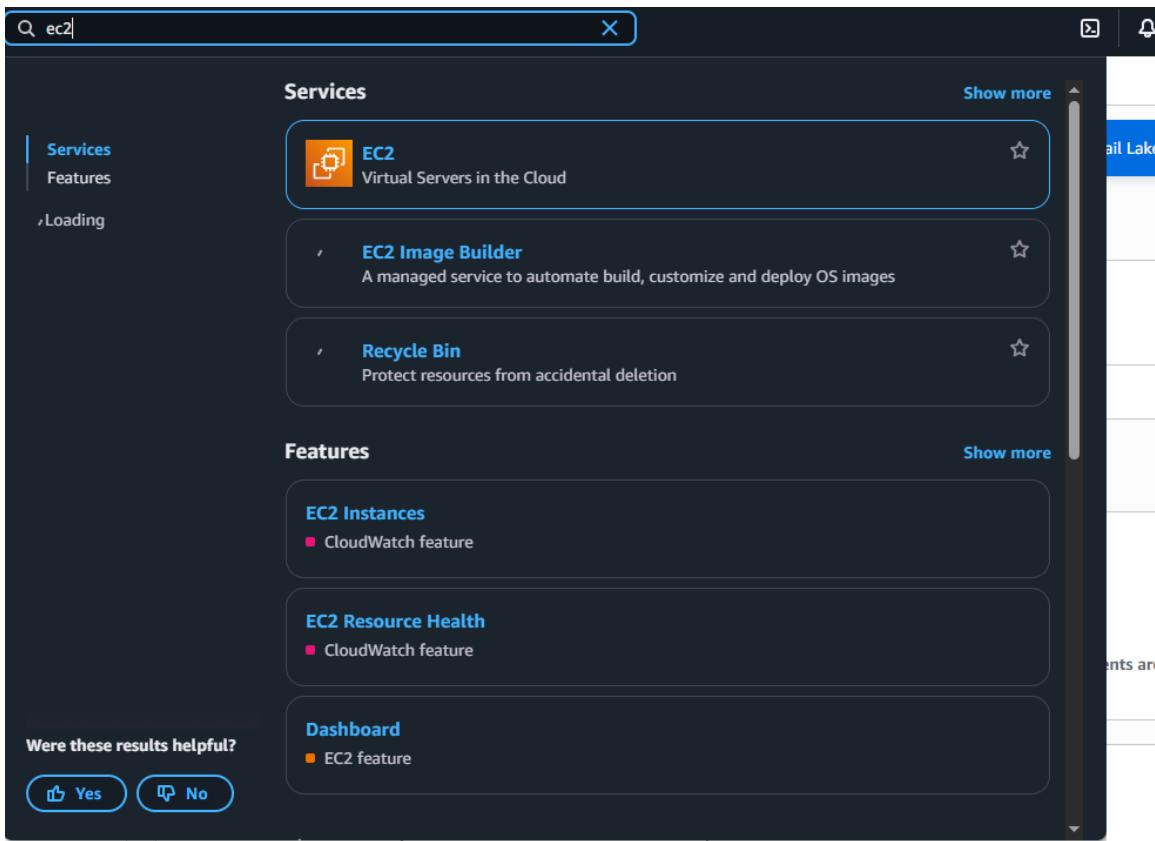
**webapp-trails** Status Logging

**CloudTrail Insights** [Info](#)



## 6. Created Instances

This is used to basically create servers



Q ec2 X

**Services**

**EC2** Virtual Servers in the Cloud

**EC2 Image Builder** A managed service to automate build, customize and deploy OS images

**Recycle Bin** Protect resources from accidental deletion

**Show more**

**Features**

**EC2 Instances** ■ CloudWatch feature

**EC2 Resource Health** ■ CloudWatch feature

**Dashboard** ■ EC2 feature

Were these results helpful?

Yes No

**EC2**

- Dashboard
- AWS Global View
- Events
- Instances**
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity Reservations
  - Capacity Manager [New](#)
- Images**
  - AMIs
  - AMI Catalog
- Elastic Block Store**
  - Volumes
  - Snapshots
  - Lifecycle Manager

**Resources**

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	0	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0	Placement groups	0
Security groups	1	Snapshots	0	Volumes	0

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) [Migrate a server](#)

Note: Your instances will launch in the Europe (Stockholm) Region

**Service health**

[AWS Health Dashboard](#) [C](#)

Region: Europe (Stockholm)

Status: ● This service is operating normally.

**Zones**

Zone name	Zone ID
eu-north-1a	eun1-az1

**EC2 cost**

Date range: Past 6 months

Credits in your free plan account are covered

Credits remaining: \$100 USD

Days remaining: 178 (May 1, 2026)

Unable to load

Analyze your costs in Cost Explorer

**Account attributes**

Default VPC [vpc-0a51e62f5c9297684](#)

Settings

Data protection and security

Allowed AMIs

Zones [L](#)

EC2 Serial Console

EC2 > Instances > Launch an instance

## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

### Name and tags [Info](#)

Name

webapp-server

Add additional tags

### ▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search our full catalog including 1000s of application and OS images

#### Quick Start



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

#### Amazon Machine Image (AMI)

Microsoft Windows Server 2025 Base

Free tier eligible

**Amazon Machine Image (AMI)**

Microsoft Windows Server 2025 Base  
ami-0b0faec6b121c8bca (64-bit (x86))  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**  
Microsoft Windows 2025 Datacenter edition. [English]

**Microsoft Windows Server 2025 Full Locale English AMI provided by Amazon**

Architecture	AMI ID	Publish Date	Username	Verified provider
64-bit (x86)	ami-0b0faec6b121c8bca	2025-10-17	Administrator	Verified provider

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

**Instance type**

t3.micro  
Family: t3 2 vCPU 1 GiB Memory Current generation: true  
On-Demand Ubuntu Pro base pricing: 0.0143 USD per Hour On-Demand RHEL base pricing: 0.0396 USD per Hour  
On-Demand SUSE base pricing: 0.0108 USD per Hour On-Demand Linux base pricing: 0.0108 USD per Hour  
On-Demand Windows base pricing: 0.02 USD per Hour

**Free tier eligible**

All generations [Compare instance types](#)

**Additional costs apply for AMIs with pre-installed software**

**Summary**

Number of instances: 1

Software Image (AMI)  
Microsoft Windows Server 2025 ... [read more](#)  
ami-0b0faec6b121c8bca

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
New security group

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

[Cancel](#)

**t3.micro** [Free tier eligible](#)

Family: t3 2 vCPU 1 GiB Memory Current generation: true  
On-Demand Ubuntu Pro base pricing: 0.0143 USD per Hour On-Demand RHEL base pricing: 0.0396 USD per Hour  
On-Demand SUSE base pricing: 0.0108 USD per Hour On-Demand Linux base pricing: 0.0108 USD per Hour  
On-Demand Windows base pricing: 0.02 USD per Hour

**All generations** [Compare instance types](#)

**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 have access to the selected key pair before you launch the instance.

**Key pair name - required**

Proceed without a key pair (Not recommended) Default value [Edit](#)

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

**Create new key pair**

**Network settings** [Info](#)

**Network** [Info](#)  
vpc-0a51e62f5c9297684

**Subnet** [Info](#)

[Edit](#)

**Network settings** [Info](#)

**Network** [Info](#)  
vpc-0a51e62f5c9297684

**Subnet** [Info](#)  
No preference (Default subnet in any availability zone)

**Auto-assign public IP** [Info](#)  
Enable

**Firewall (security groups)** [Info](#)  
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 Anywhere 0.0.0.0/0  
Helps you connect to your instance

Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

**Summary**

Number of instances: 1

Software Image (AMI)  
Microsoft Windows Server 2025 ... [read more](#)  
ami-0b0faec6b121c8bca

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
New security group

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

[Launch instance](#) [Preview code](#)

The screenshot shows the AWS Management Console interface for the 'Instances' section. At the top, there are buttons for 'Connect', 'Instance state', 'Actions', and 'Launch instances'. A search bar at the top left contains the placeholder 'Find Instance by attribute or tag (case-sensitive)'. Below the search bar is a table header with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. A single row is listed in the table, representing an EC2 instance named 'webapp-server' with the ID 'i-0bbb9b111d69ac4f0'. The instance is currently 'Running' and is of type 't3.micro'. Its status is 'Initializing'. It is located in the 'eu-north-1c' availability zone and has a public IPv4 address 'ec2-13-53-43-230.eu'. There are also buttons for 'View alarms' and 'Launch instances'.

## 7. Logging in as an IAM User

IAM users can sign in through:

- AWS Management Console (using the new alias URL)
- AWS CLI via programmatic keys

A	B	C
User name	Password	Console sign-in URL
Ltechng-Audit-wel	Okechukwu	<a href="https://476120257824.signin.aws.amazon.com/console">https://476120257824.signin.aws.amazon.com/console</a>

The screenshot shows the AWS Management Console 'Console Home' page. At the top, there is a search bar and a 'Reset to default layout' button. The top right corner displays the account ID '4761-2025-7624', the region 'Europe (Stockholm)', and the user 'Ltechng-Audit-webapp-Chike'. Below the header, there are two main sections: 'Recently visited' and 'Applications'. The 'Recently visited' section shows a placeholder message 'No recently visited services' and links to 'EC2', 'S3', 'Aurora and RDS', and 'Lambda'. The 'Applications' section shows a placeholder message 'No applications' and a 'Create application' button. At the bottom of the page, there are links to 'View all services' and 'Go to myApplications'.