AWS IAM Cloud Security Project

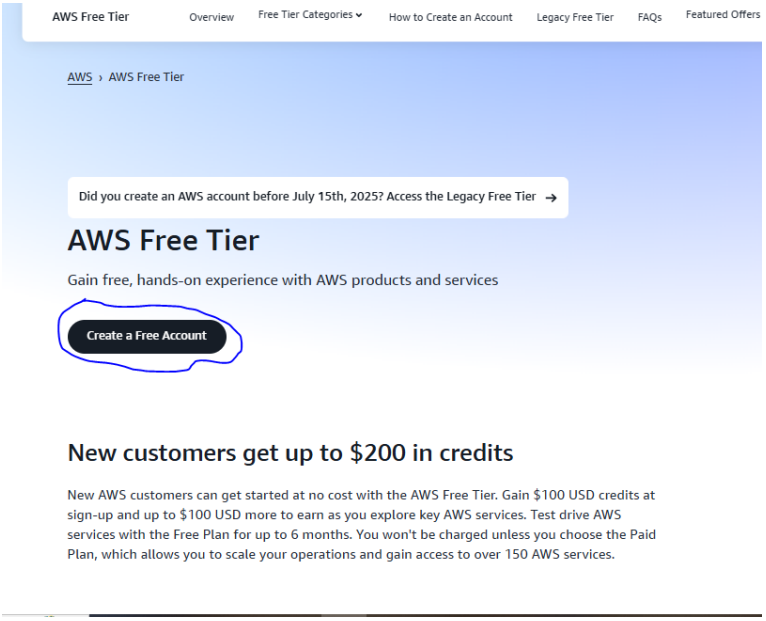
1. Project Overview

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).

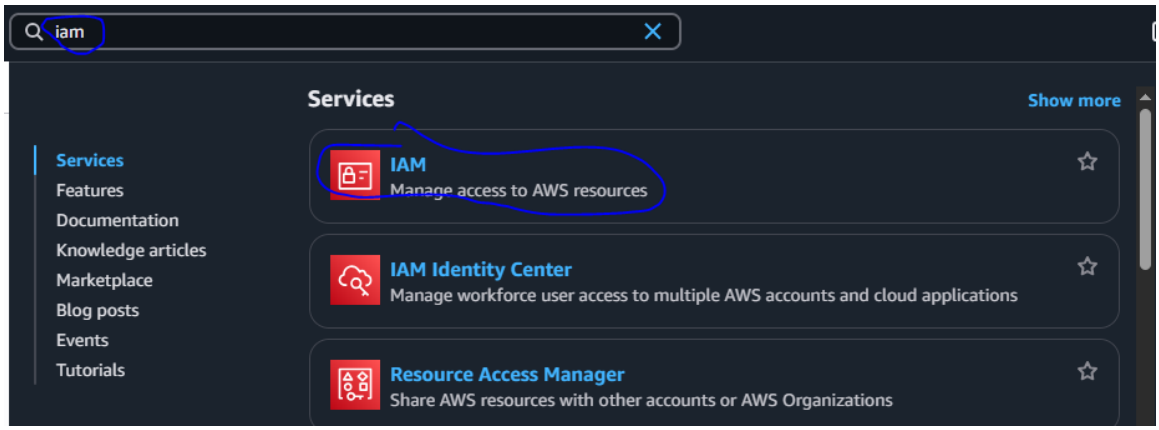
2. Tools & Concepts

- 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

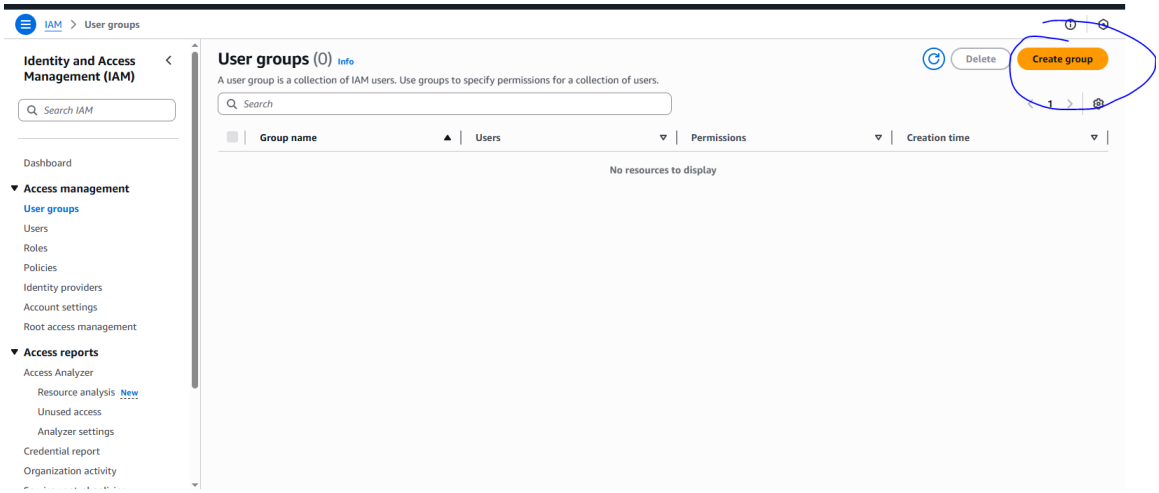
I created account using: https://aws.amazon.com/console/

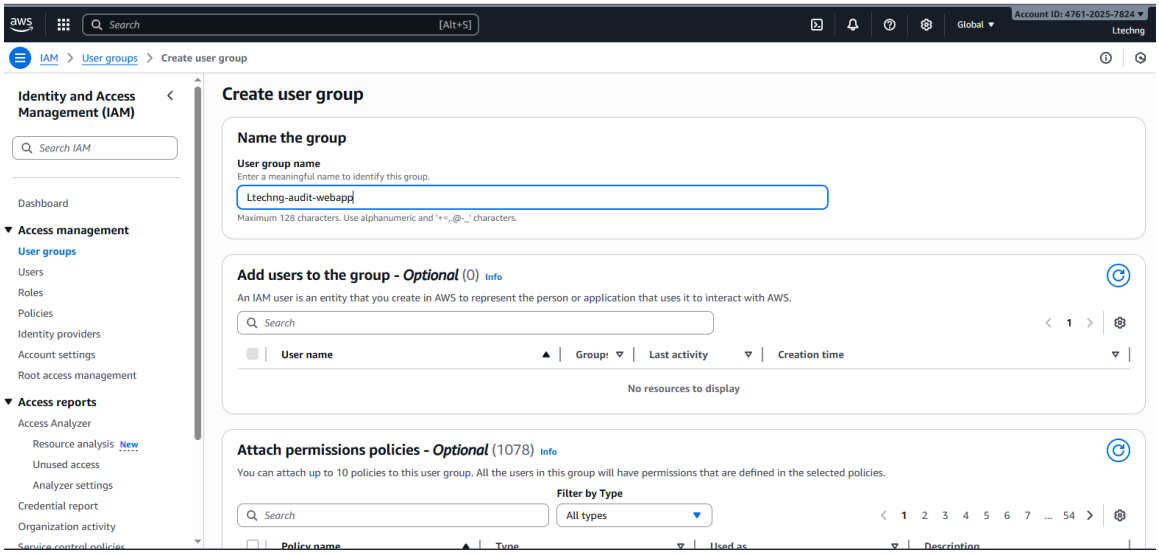


IAM service standard practice is that we don’t make configuration on the root users. We create an identity and access management user who has admin privileges.

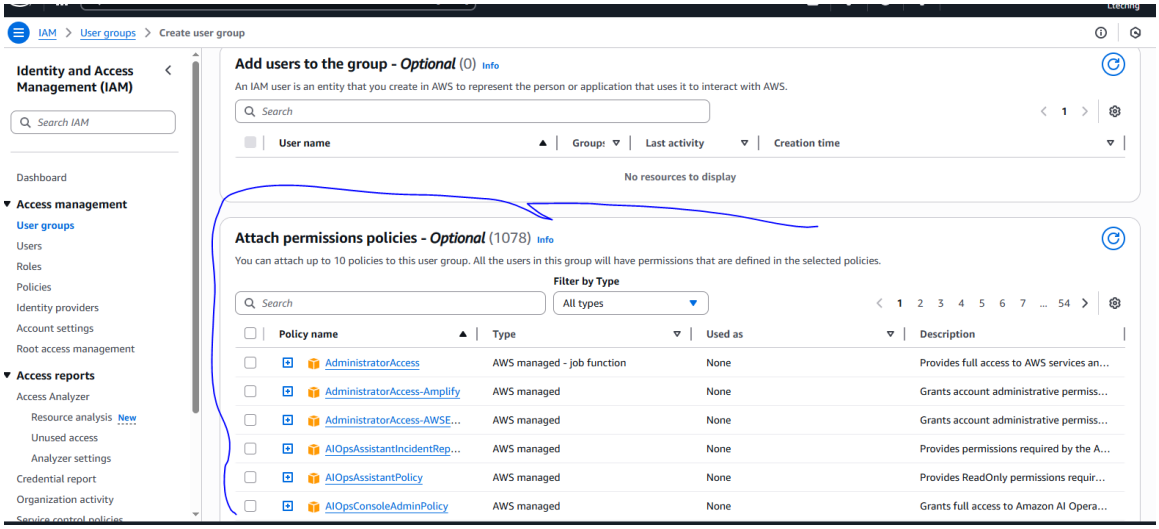


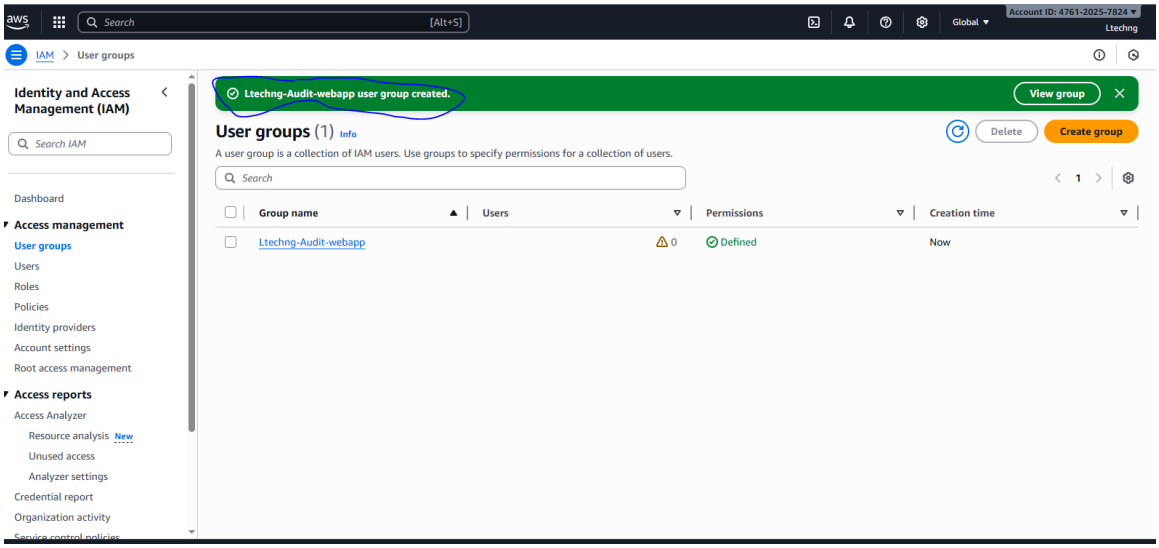
Next we create user groups to which we can implement policies



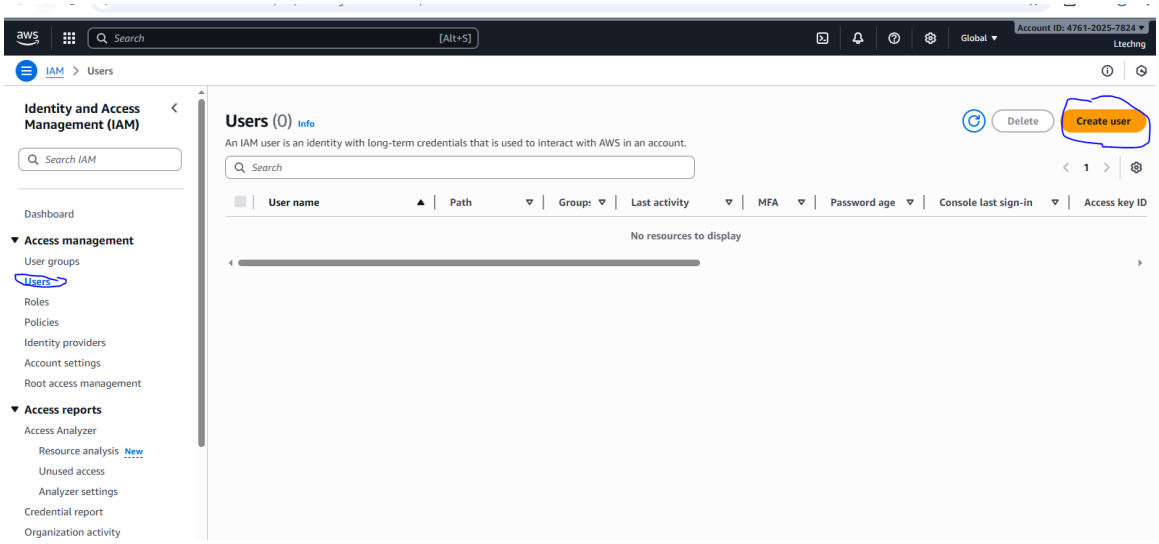


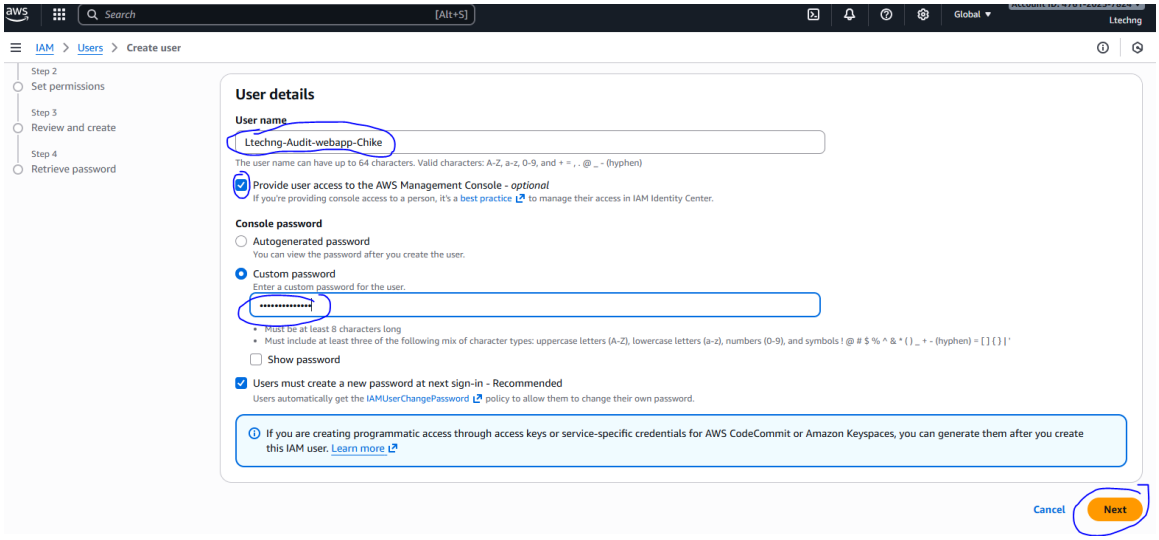
During user group creation, we are also implementing the permission policies directly. Note you can decide to create user group and implement policies later on





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

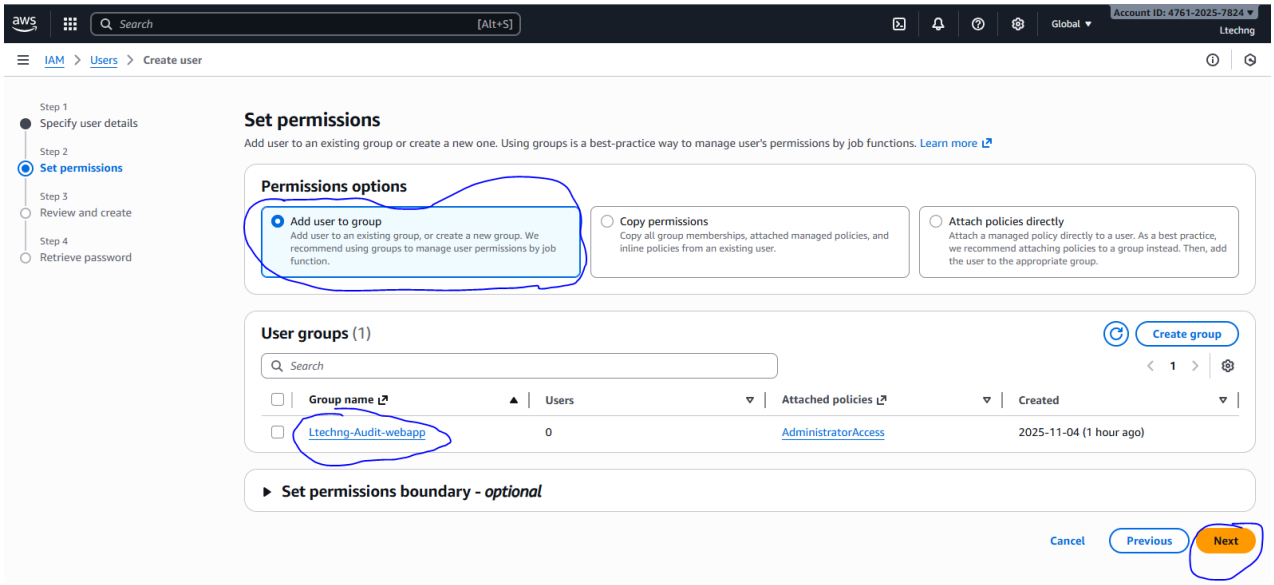


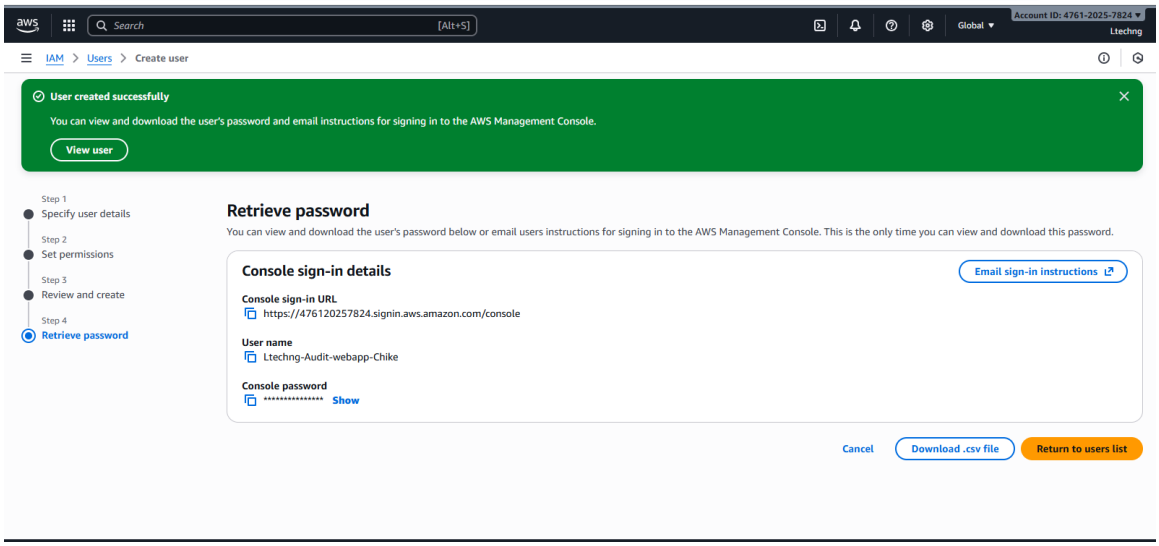


Next we would be setting the permission option. Option avaialable are

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 permissionsCopy all group memberships, attached managed policies, and inline policies from an existing user.
3. Attach policies directlyAttach 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





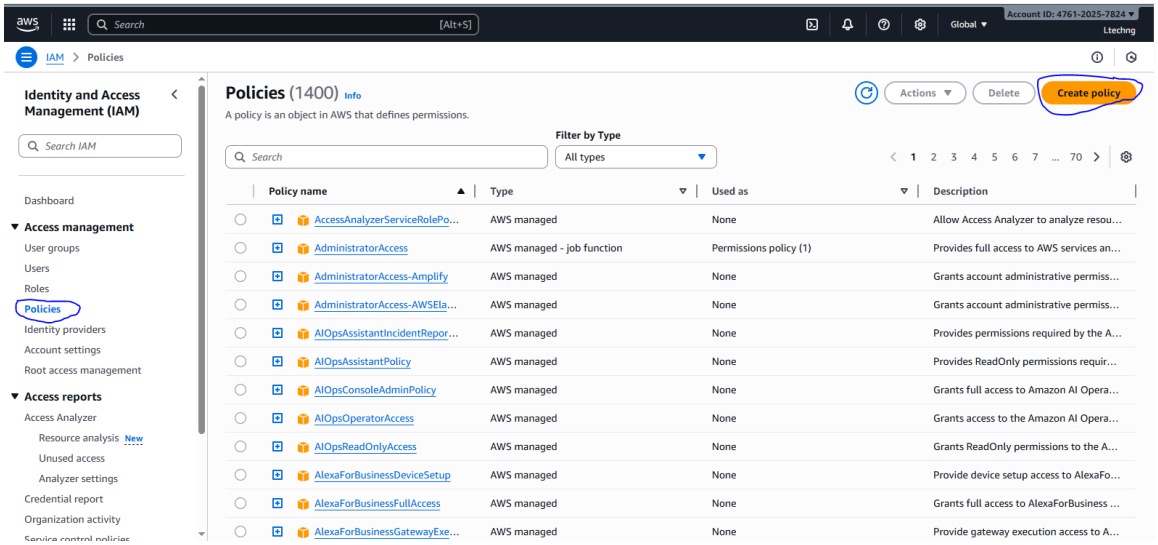
3. Tagging Strategy

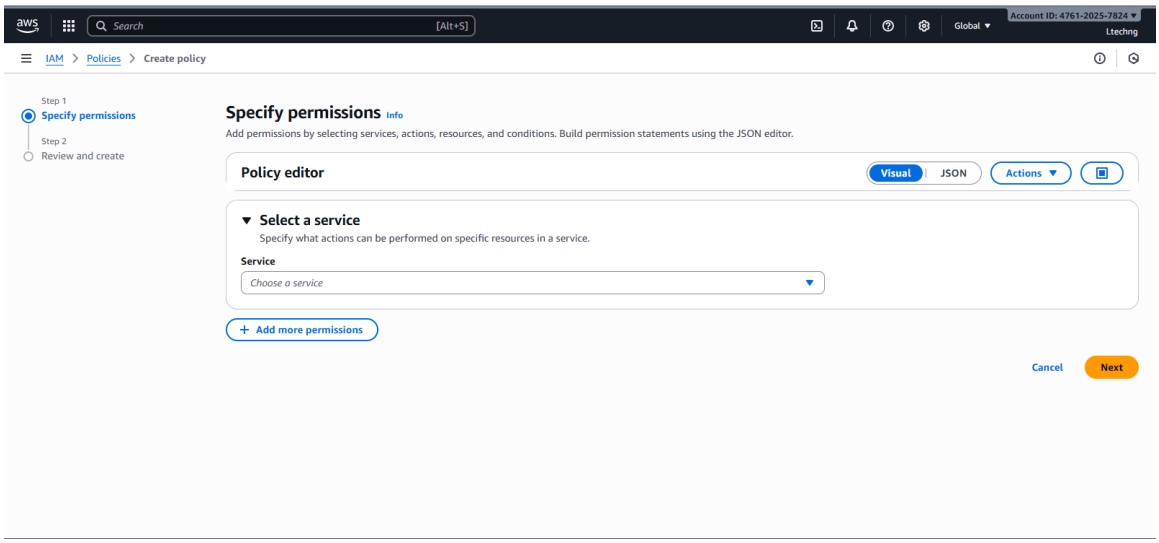
I applied a descriptive tag to each EC2 instance:

Instance	Tag Key	Tag Value
audit	Environment	Audit

4. Creating the IAM Policy

You can manually create policcies 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.

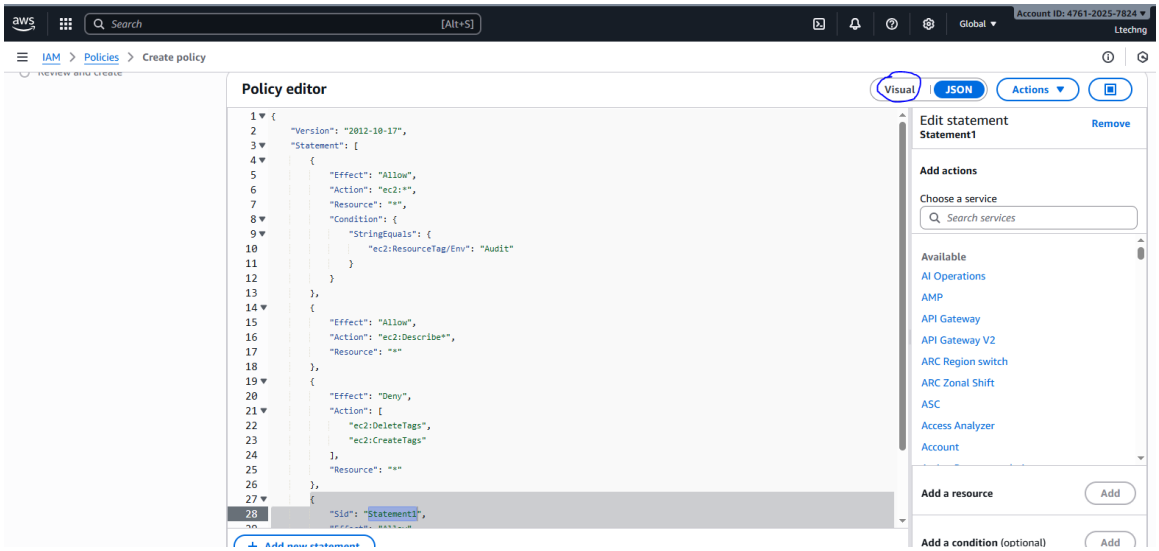




I authored the following JSON policy to block instance stop/start actions on the audit server.

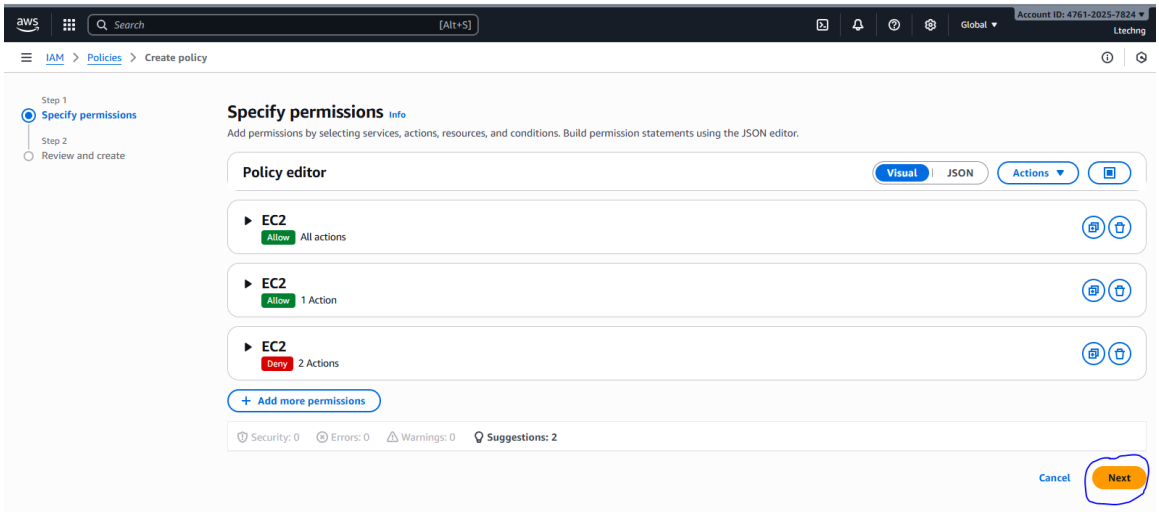
The policy can allow users :

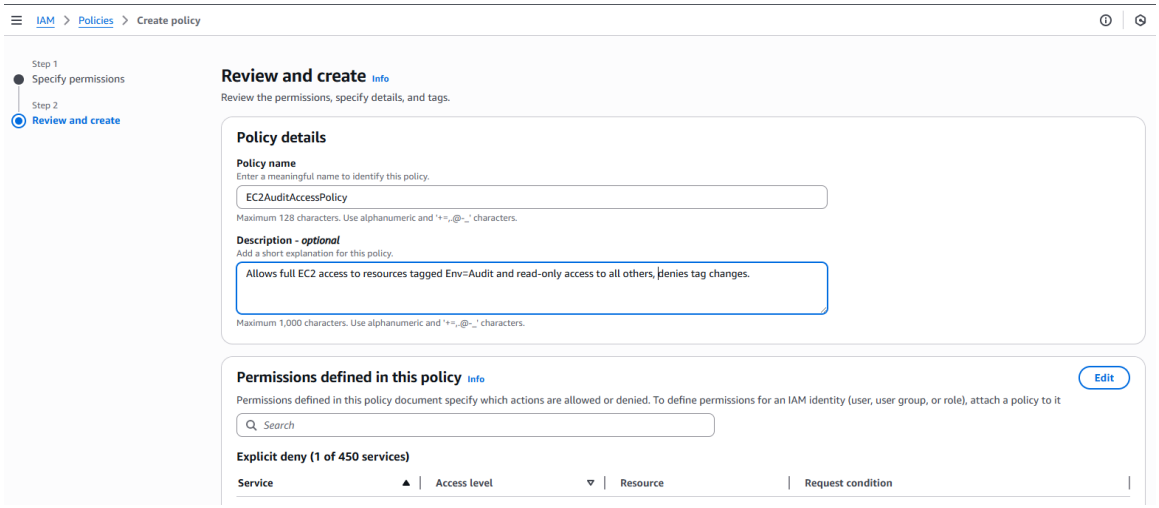
- View all EC2 resources.
- Fully manage (start, stop, reboot, terminate, etc.) EC2 instances tagged Env=Audit.
- **Cannot** create or delete tags — meaning they can't tag new instances as Env=Audit to bypass the restriction.

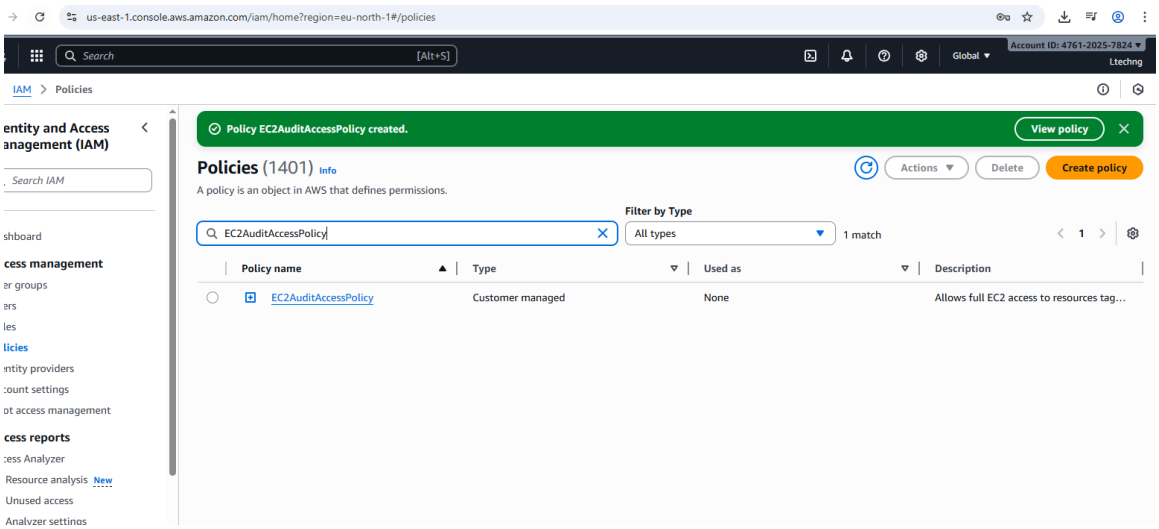


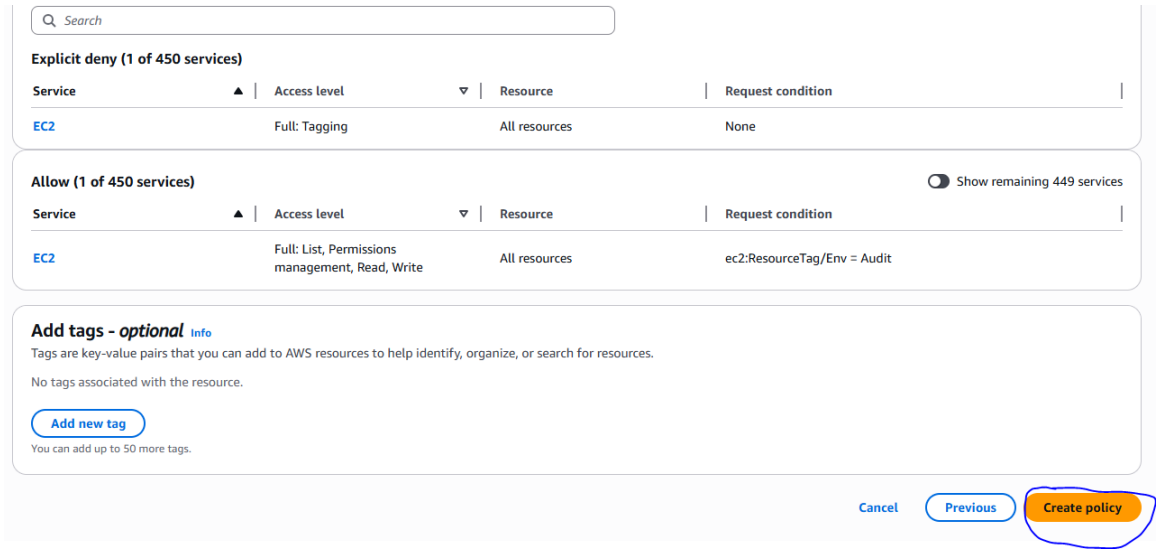

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ec2:*",
   "Resource": "*",
   "Condition": {
```

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


aws
Search
[Alt+S]
Global
Account ID: 4761-2025-7824
Ltechng
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
EC2
Allow All actions
EC2
Allow 1 Action
EC2
Deny 2 Actions
Add more permissions
Security: 0
Errors: 0
Warnings: 0
Suggestions: 2
Cancel
Next


IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
EC2AuditAccessPolicy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Allows full EC2 access to resources tagged Env=Audit and read-only access to all others, denies tag changes.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
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
Explicit deny (1 of 450 services)
Service
Access level
Resource
Request condition





5. Creating CloudTrails

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

It automatically records actions taken by:

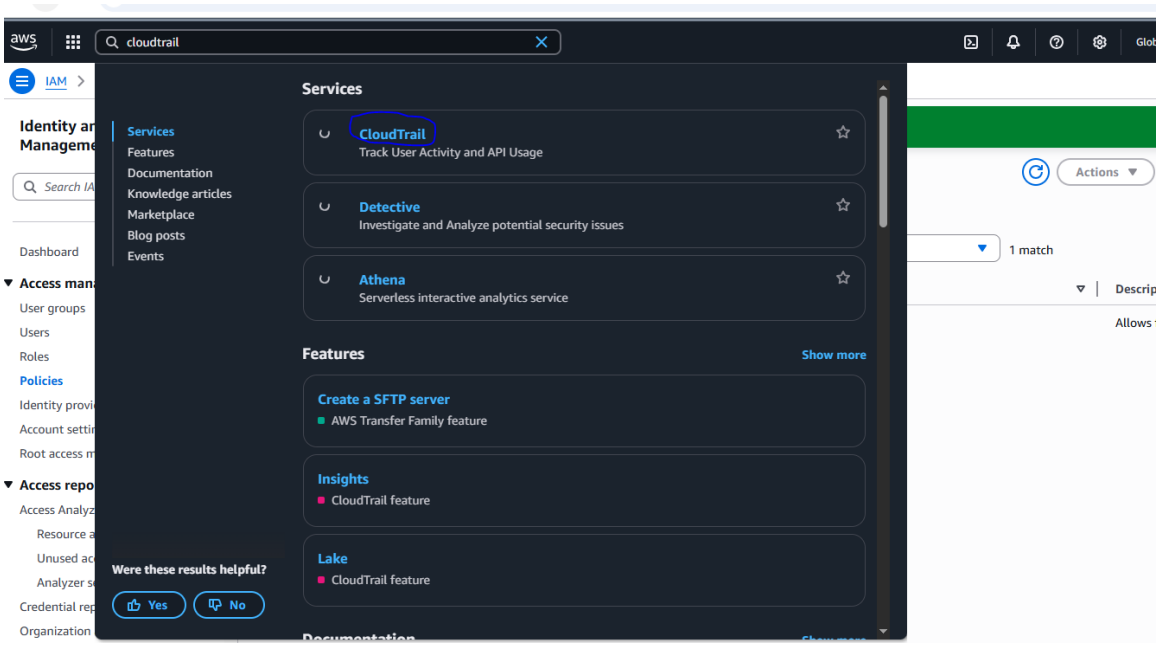
- Users (IAM users or federated users)
- Roles (like those assumed by applications)

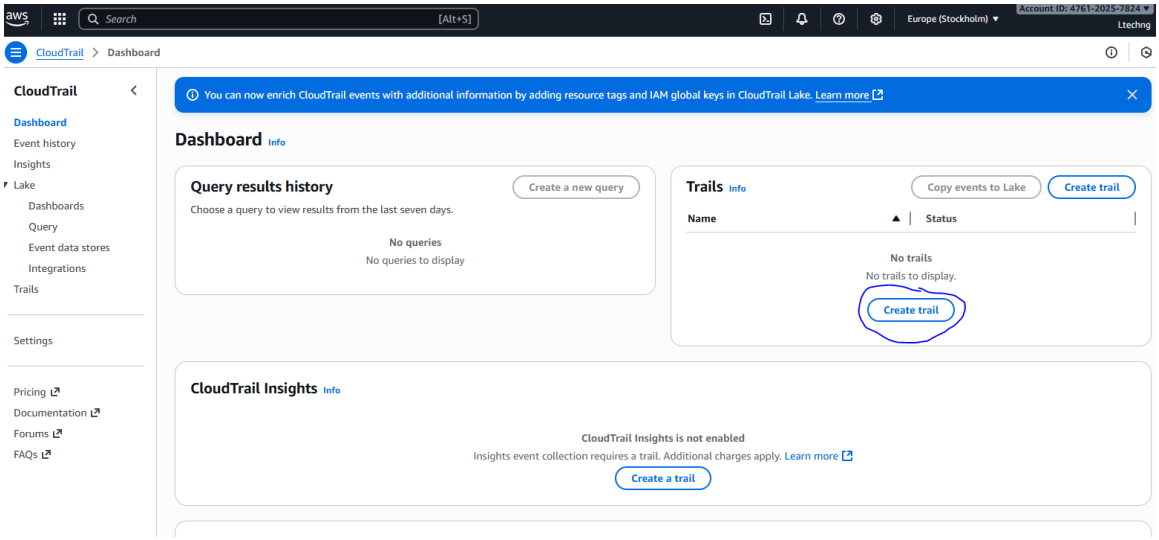
- AWS services (automated actions)

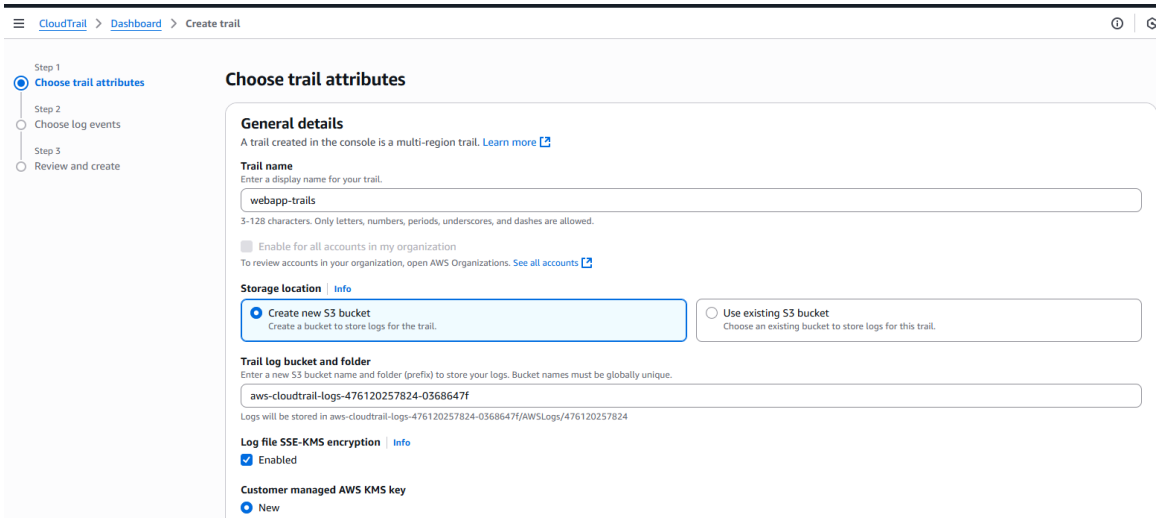
CloudTrail helps you **monitor, secure, and troubleshoot** AWS operations.

What CloudTrail (the service) does

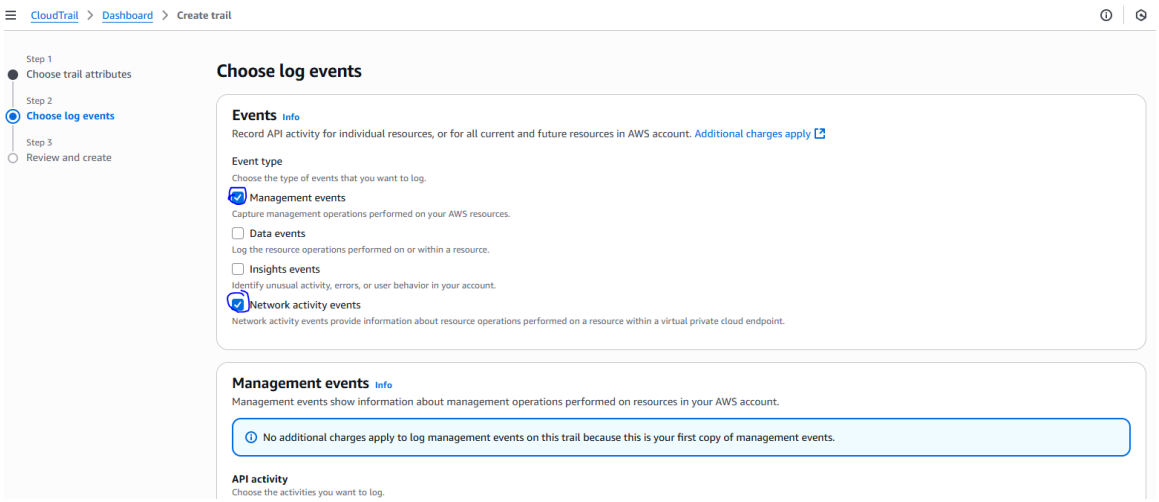
- Logs every **API call** and **console action**.
- Captures:
    - **Who** performed the action (user or service)
    - **What** action was performed
    - **When** it occurred
    - **From where** (IP, region)
    - **Which resource** was affected
- Stores logs in **S3**, and optionally sends them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

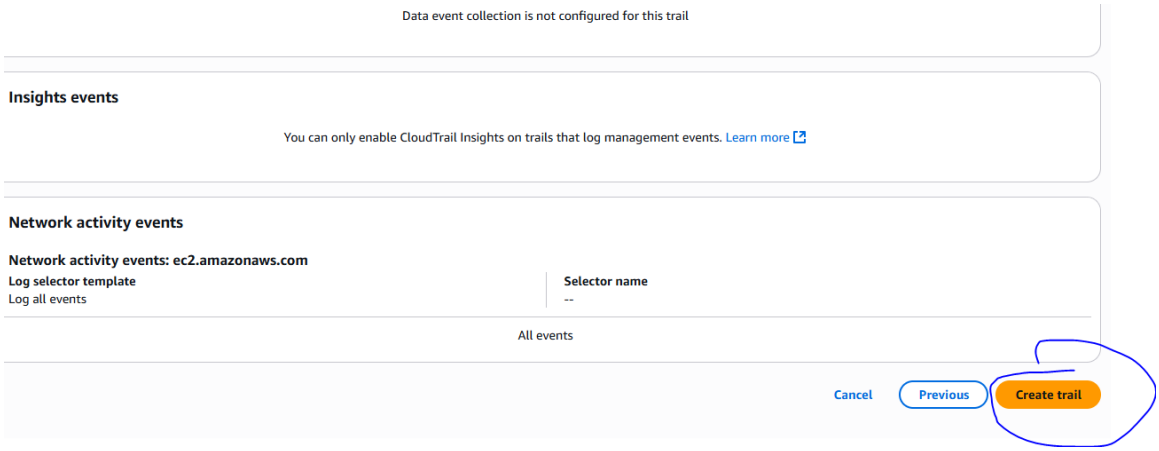


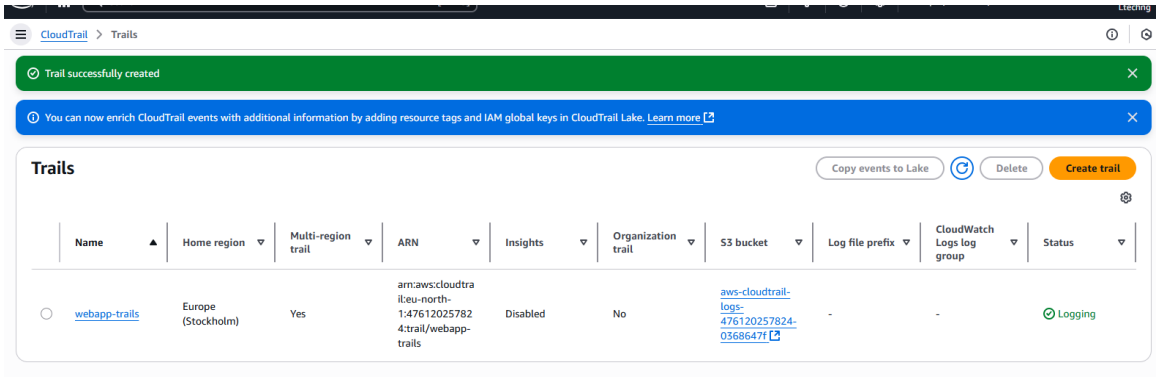


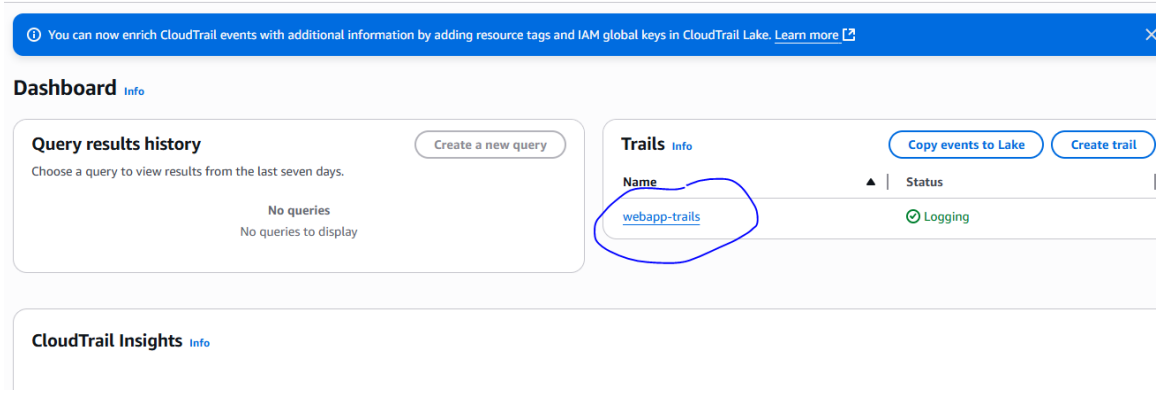


Click on next


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.
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.

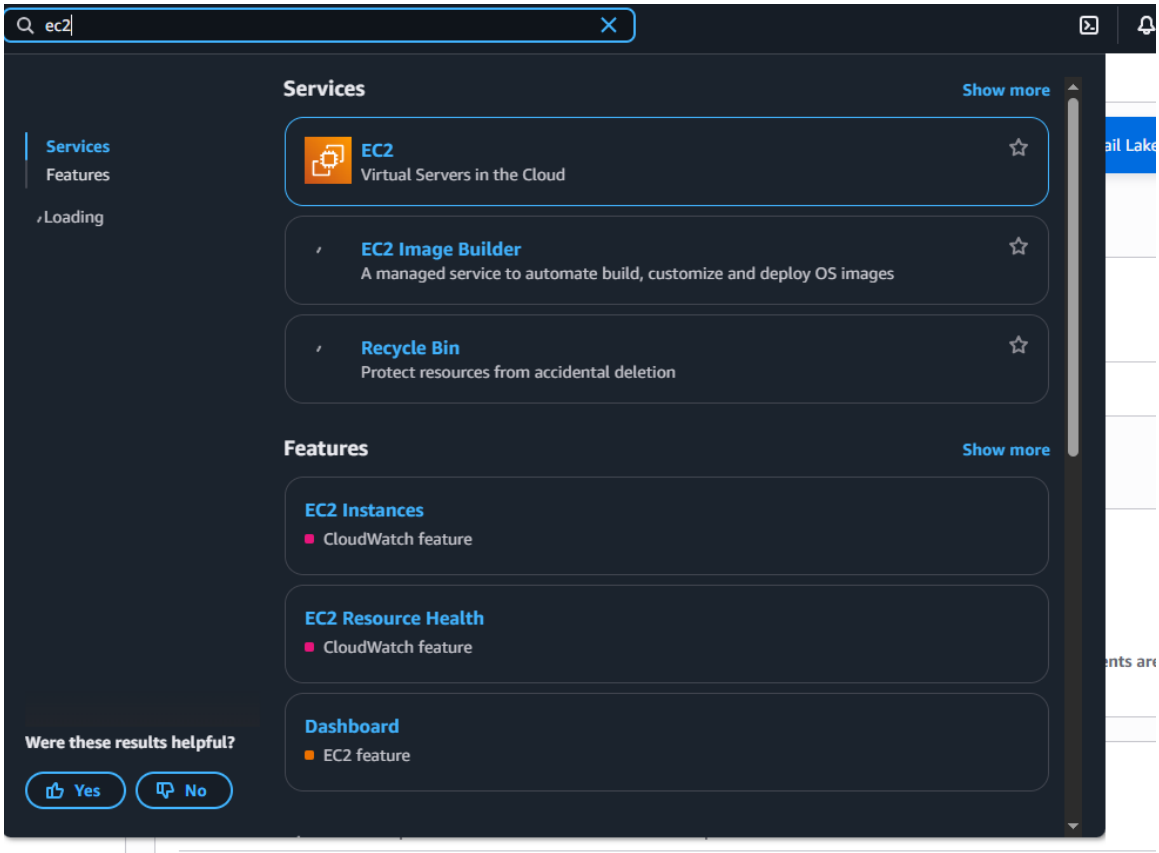

Data event collection is not configured for this trail
Insights events
You can only enable CloudTrail Insights on trails that log management events. Learn more
Network activity events
Network activity events: ec2.amazonaws.com
Log selector template
Log all events
Selector name
--
All events
Cancel
Previous
Create trail

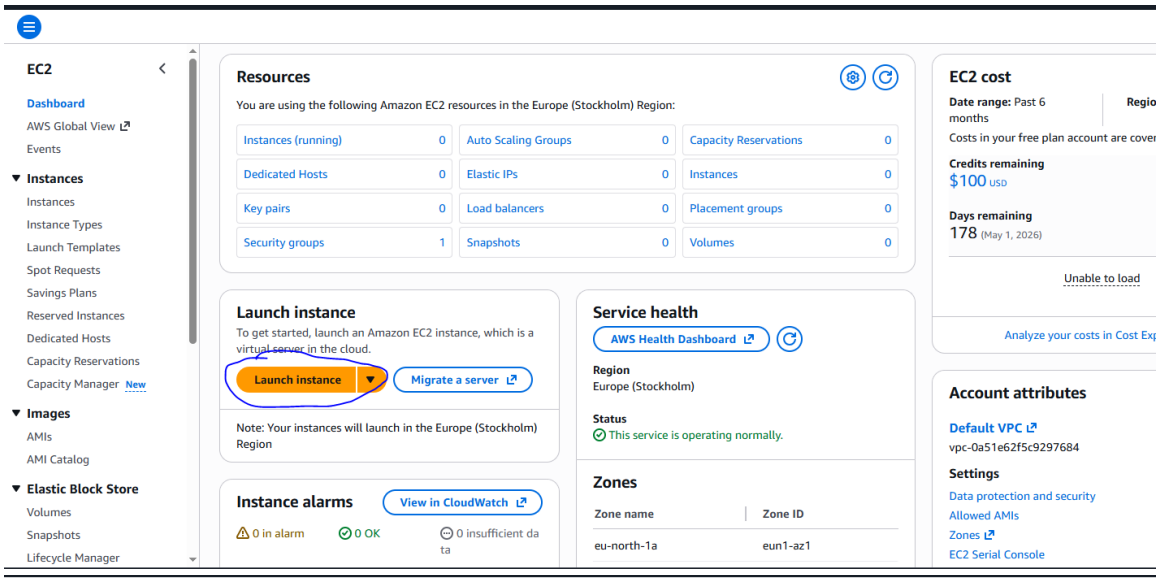

CloudTrail > Trails
Trail successfully created
You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more
Trails
Copy events to Lake
Delete
Create trail
Name
Home region
Multi-region trail
ARN
Insights
Organization trail
S3 bucket
Log file prefix
CloudWatch Logs log group
Status
webapp-trails
Europe (Stockholm)
Yes
arn:aws:cloudtrail:eu-north-1:476120257824:trail/webapp-trails
Disabled
No
aws-cloudtrail-logs-476120257824-0368647f
-
-
Logging

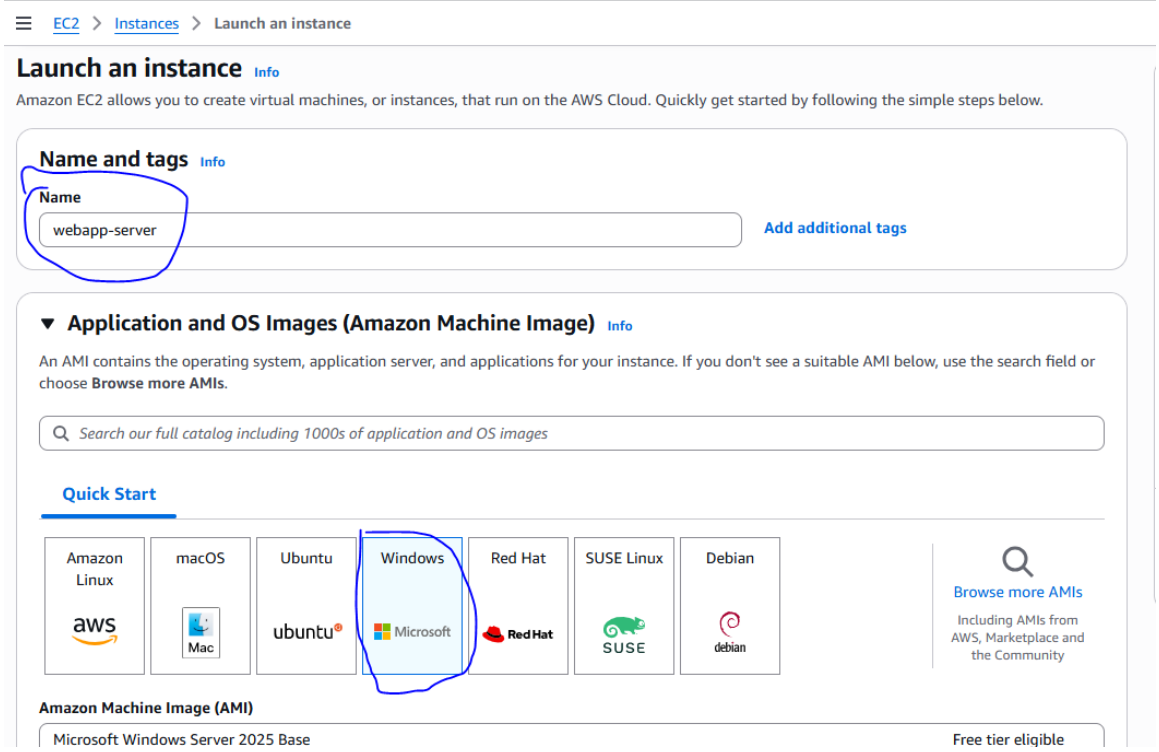


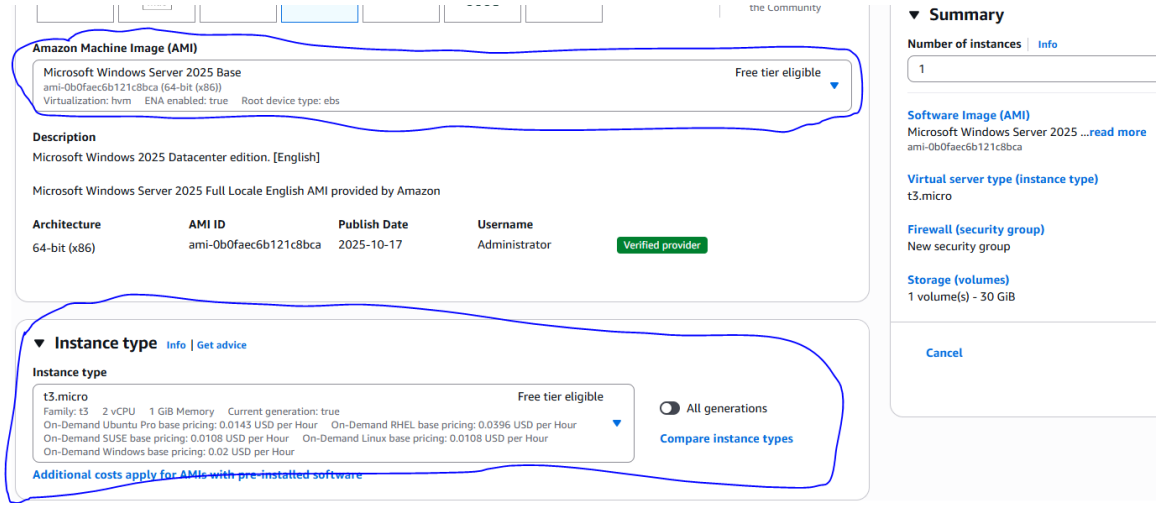
6. Created Instances

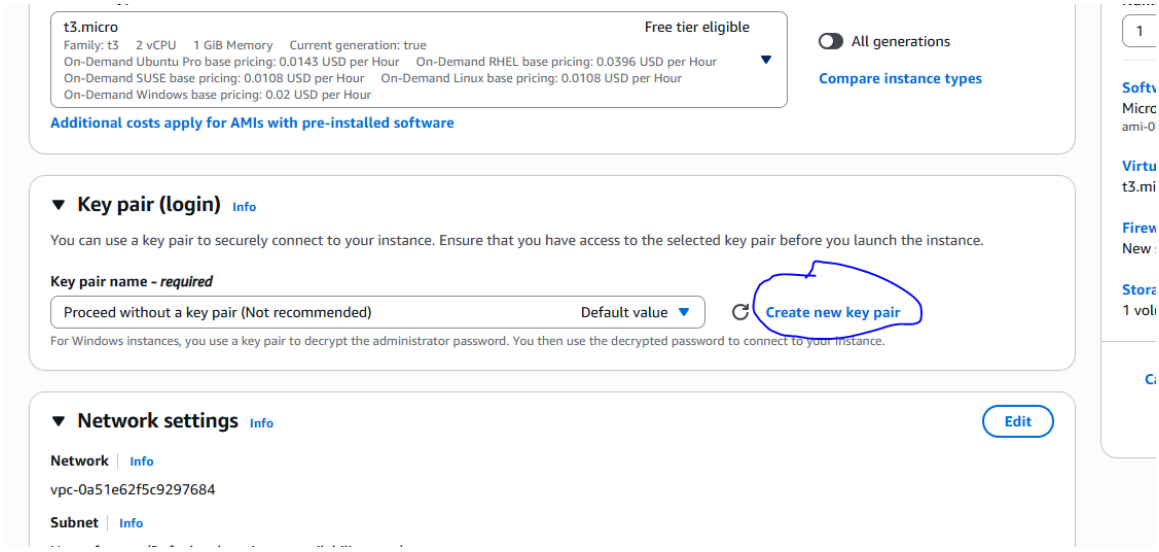
This is used to basically create servers

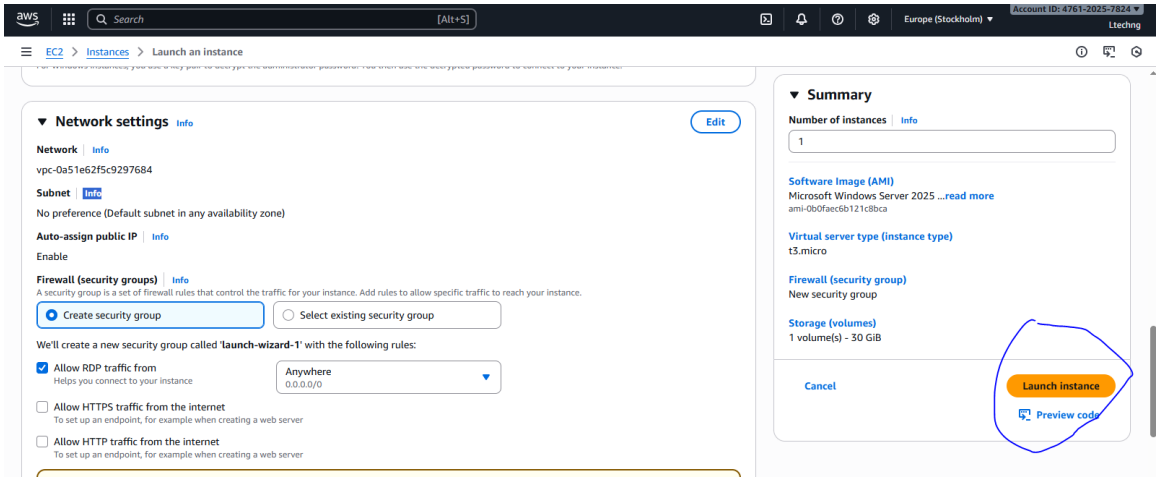


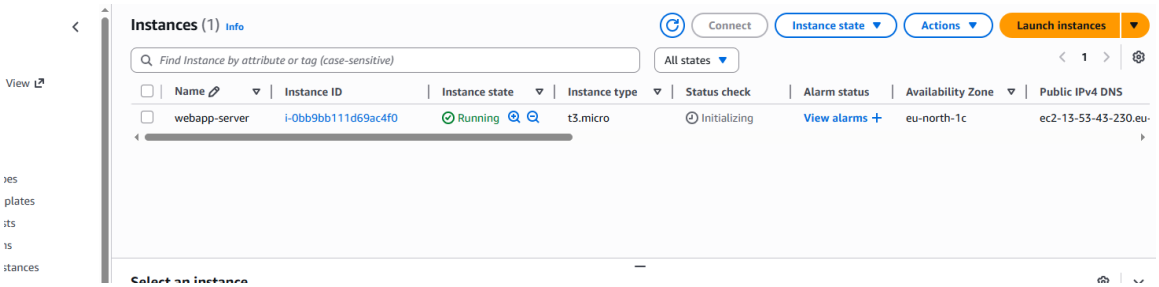

EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Resources
You are using the 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
Instance alarms
View in CloudWatch
0 in alarm
0 OK
0 insufficient data
Service health
AWS Health Dashboard
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
Regio
Costs in your free plan account are cover
Credits remaining
$100 USD
Days remaining
178 (May 1, 2026)
Unable to load
Analyze your costs in Cost Exp
Account attributes
Default VPC
vpc-0a51e62f5c9297684
Settings
Data protection and security
Allowed AMIs
Zones
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
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
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
Free tier eligible
Description
Microsoft Windows 2025 Datacenter edition. [English]
Microsoft Windows Server 2025 Full Locale English AMI provided by Amazon
Architecture
64-bit (x86)
AMI ID
ami-0b0faec6b121c8bca
Publish Date
2025-10-17
Username
Administrator
Verified provider
Instance type Info | Get advice
Instance type
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
Summary
Number of instances Info
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
Create new key pair
For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.
Network settings Info
Edit
Network Info
vpc-0a51e62f5c9297684
Subnet Info


aws
Search
[Alt+S]
Europe (Stockholm)
Account ID: 4761-2025-7824
Ltechng
EC2 > Instances > Launch an instance
Network settings Info
Edit
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
Helps you connect to your instance
Anywhere
0.0.0.0/0
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 Info
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
Launch instance
Preview code



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	Okechukw	https://476120257824.signin.aws.amazon.com/console