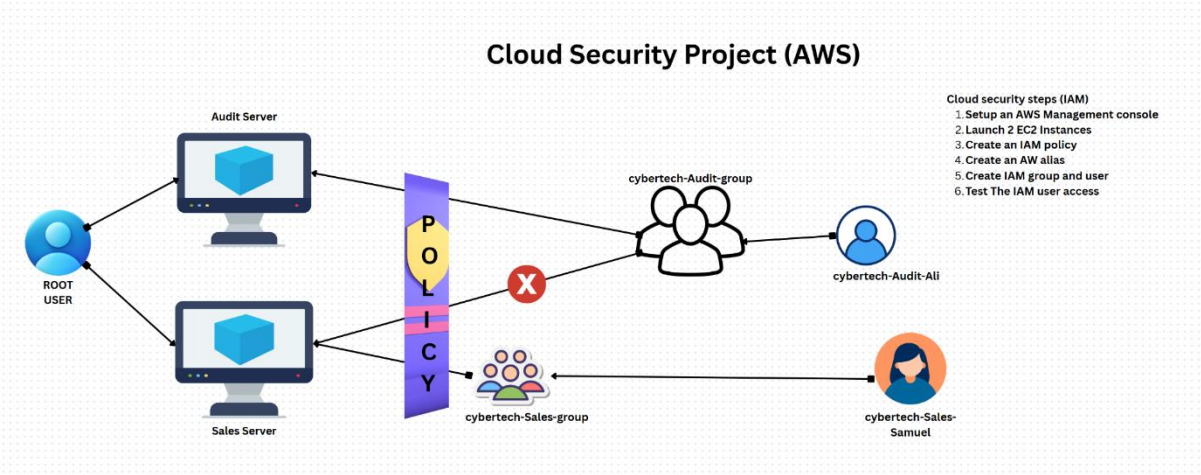
Identity Access Management(IAM) On Cloud Security with AWS (off premises)

Overview of the Project

I finished a project on Identity and Access Management (IAM)-focused AWS cloud security controls. In order to facilitate the creation of user accounts, I created a root account. Creating a least-privilege policy, allocating it to a user group, and confirming that it successfully limits actions on two Amazon EC2 instances (sales and audit) were the objectives.



Setup an AWS management Console

Create an AW alias

Create user for each group that I created

Create group (Finance and Sales) and add user to the group

Launch EC2 instances

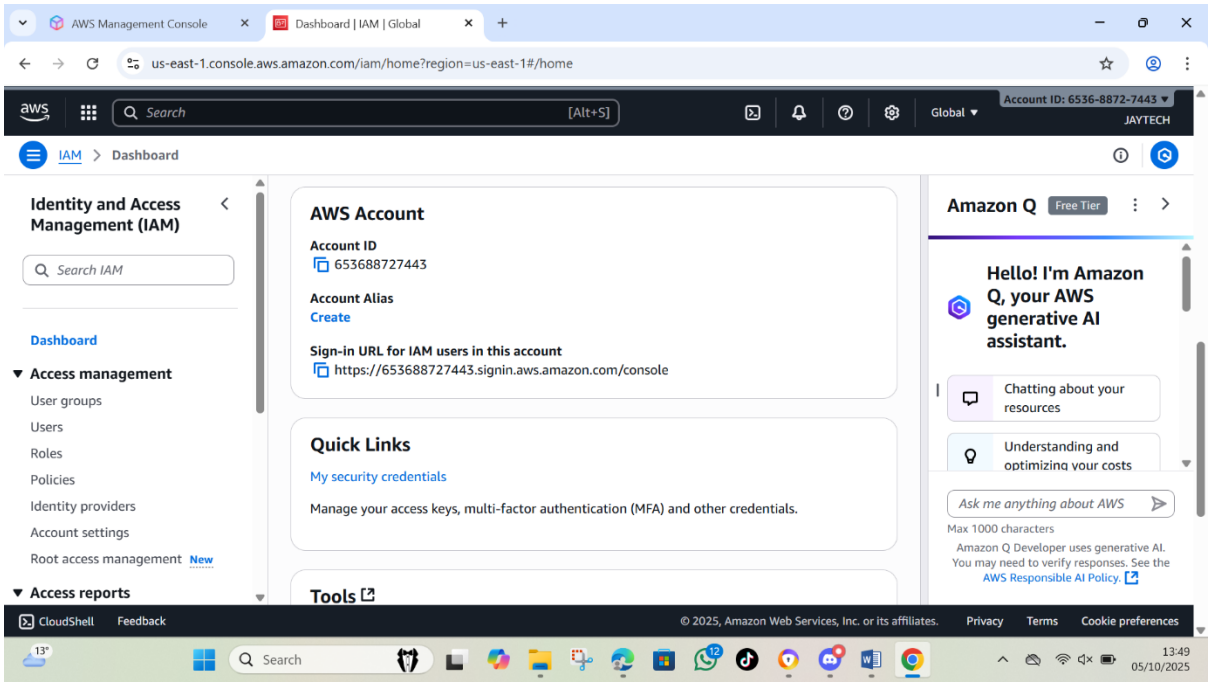
Create a policy

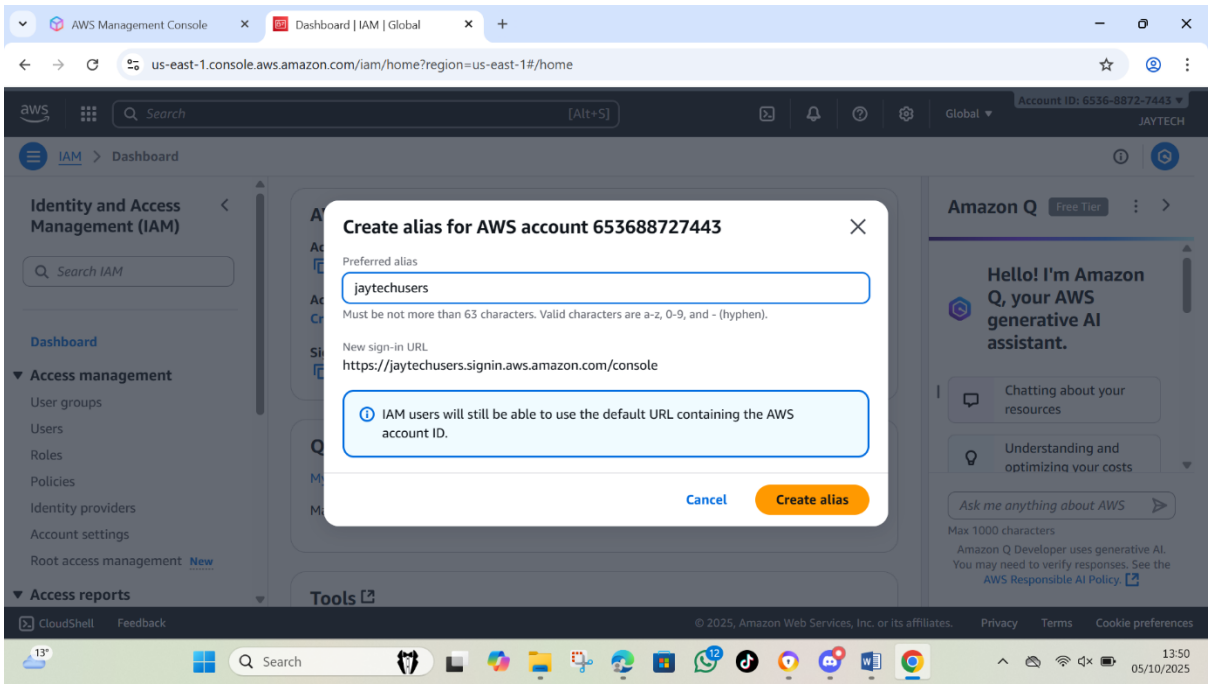
Test the IAM user access

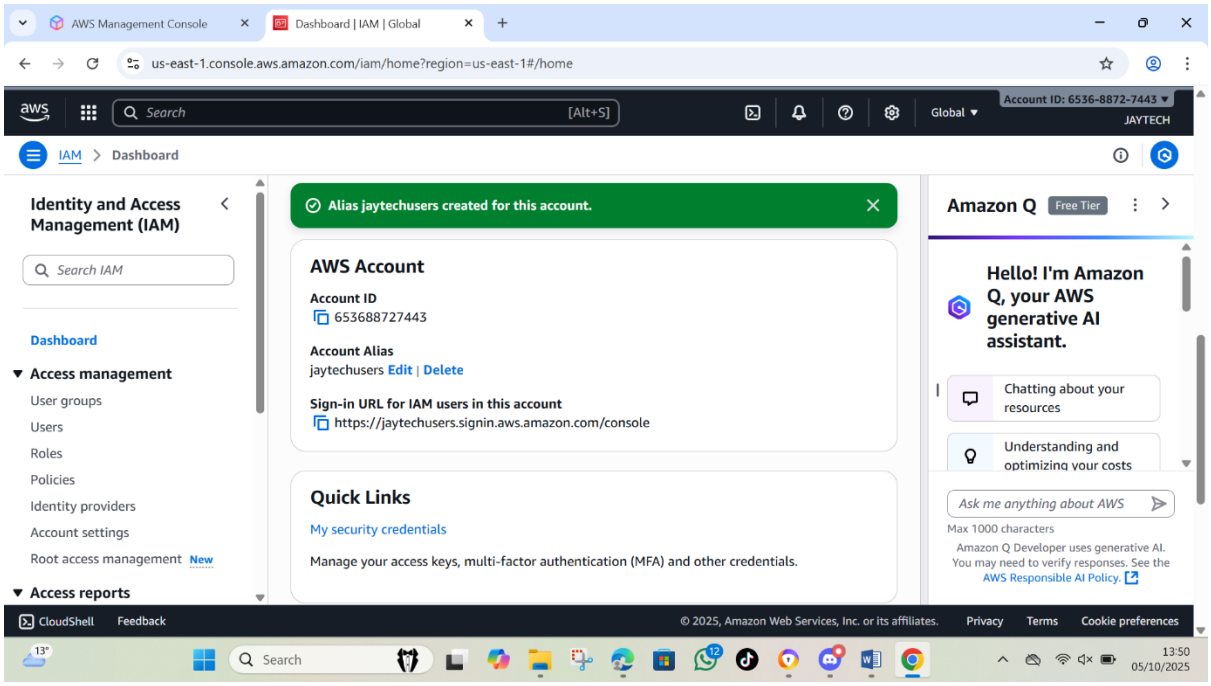
As the main account for handling IAM users and groups, I made an AWS root account. With the global rights granted by this account, I am able to create and administer user accounts and groups in IAM.

➢ Create an AW Alias

In order to enable people to log in using the alias as their ID rather than their account ID number, I went into the AWS Management Console and set it up.

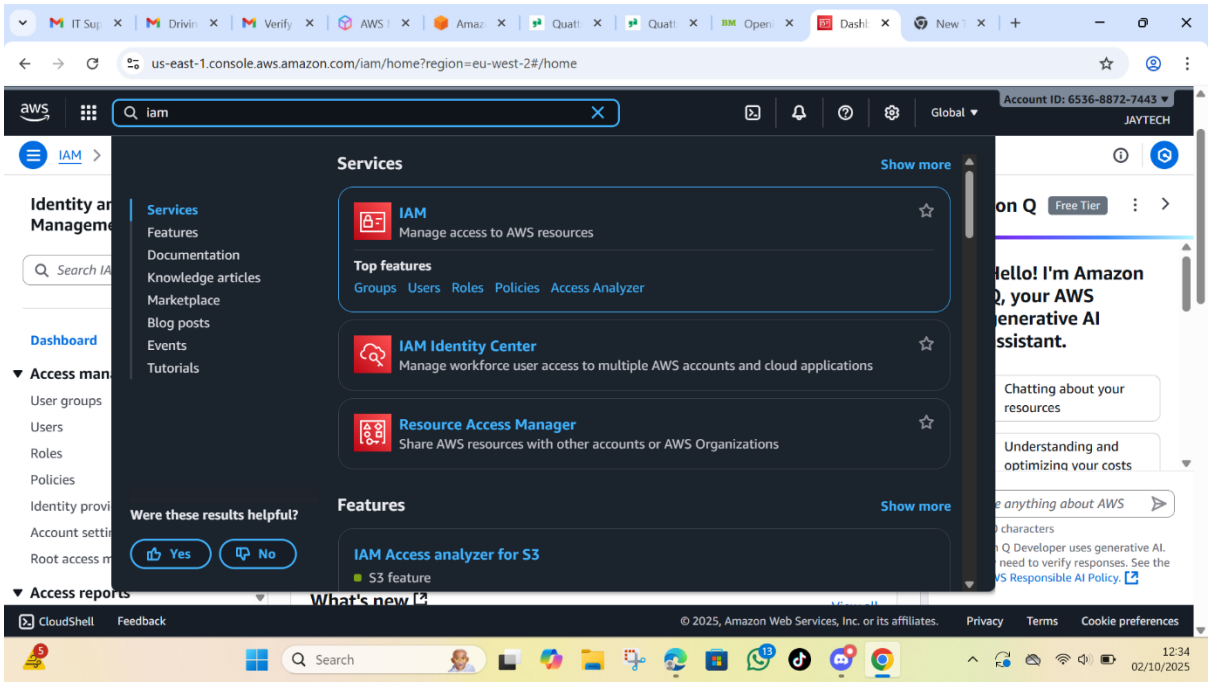

AWS Management Console
Dashboard | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home
Search
[Alt+S]
Global
Account ID: 6536-8872-7443
JAYTECH
IAM > Dashboard
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
AWS Account
Account ID
653688727443
Account Alias
Create
Sign-in URL for IAM users in this account
https://653688727443.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
Tools
Amazon Q
Free Tier
Hello! I'm Amazon Q, your AWS generative AI assistant.
Chatting about your resources
Understanding and optimizing your costs
Ask me anything about AWS
Max 1000 characters
Amazon Q Developer uses generative AI. You may need to verify responses. See the AWS Responsible AI Policy.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
13:49
05/10/2025

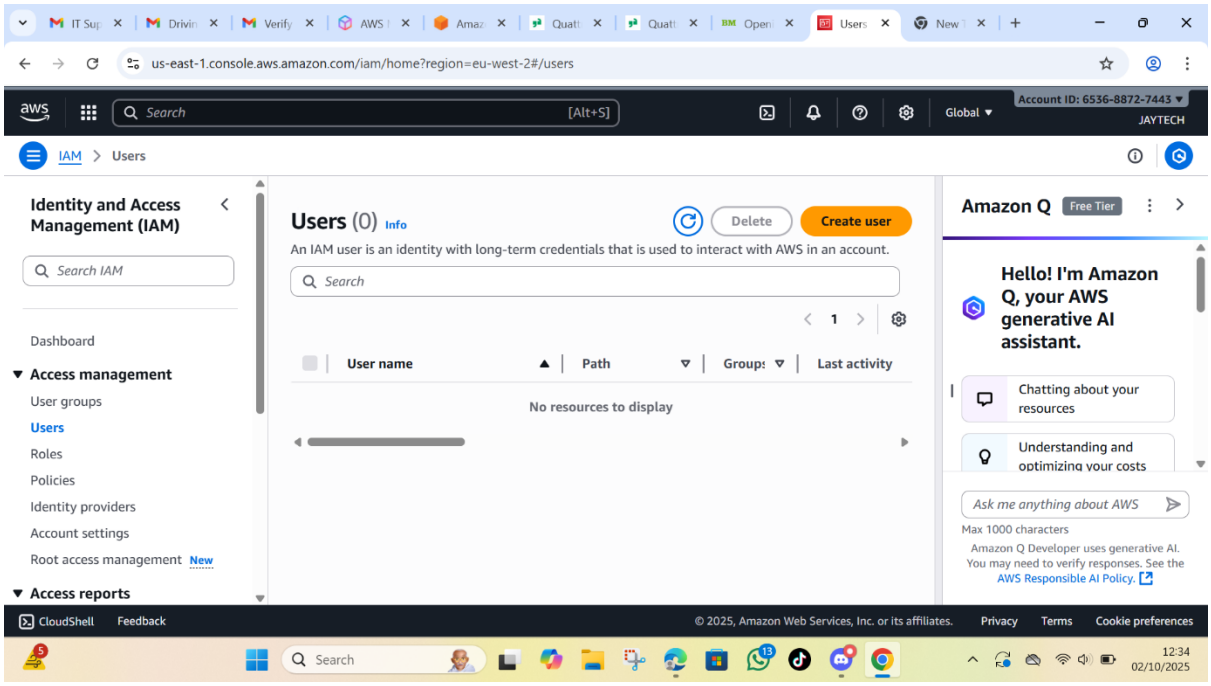

AWS Management Console
Dashboard | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home
Create alias for AWS account 653688727443
Preferred alias
jaytechusers
Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).
New sign-in URL
https://jaytechusers.signin.aws.amazon.com/console
IAM users will still be able to use the default URL containing the AWS account ID.
Cancel
Create alias
Identity and Access Management (IAM)
Amazon Q
Free Tier
Hello! I'm Amazon Q, your AWS generative AI assistant.
Tools
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
13:50
05/10/2025

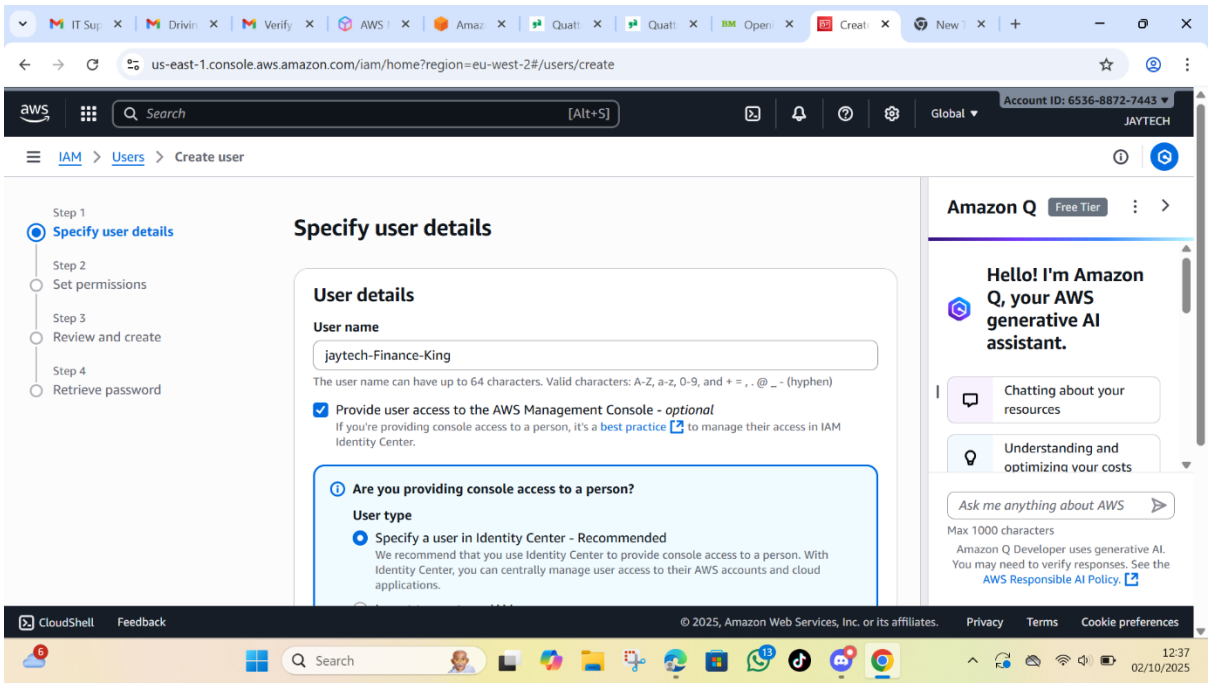


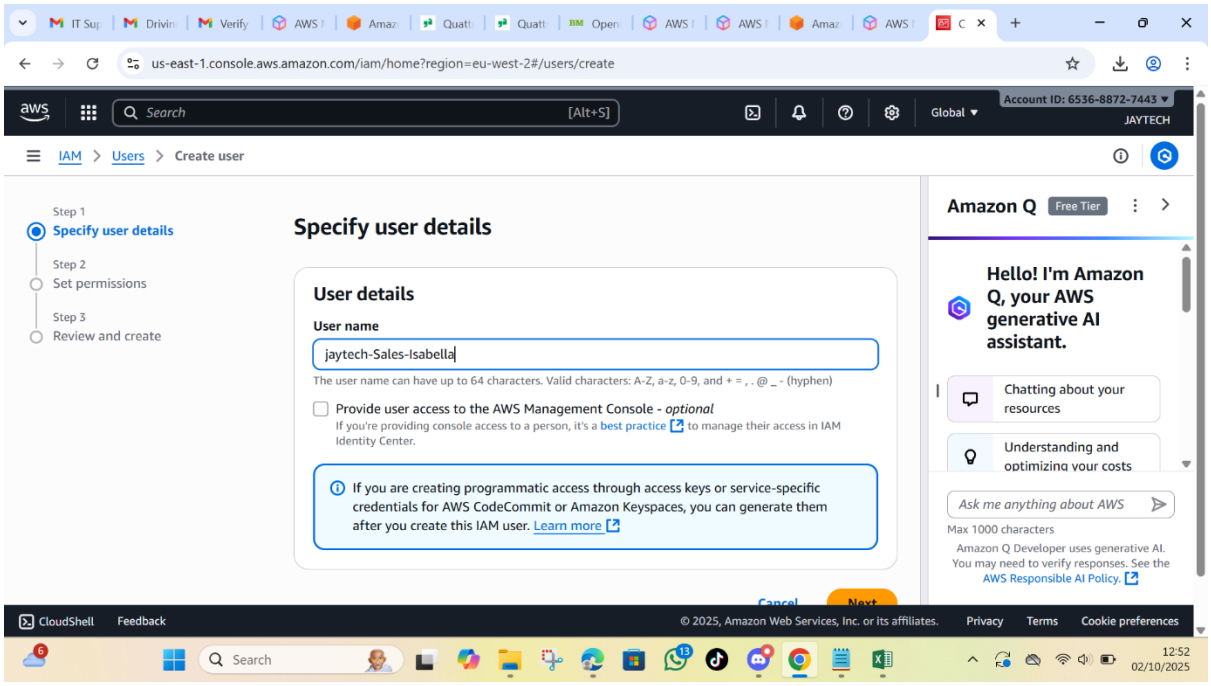
➢ Creation of users:

I went to the IAM service after logging into AWS with the root account "jaytech." I made 'Kng' for the finance staff and 'Isabella' for the sales team. I clicked 'Next' after inputting the information until the user creation process was totally finished.



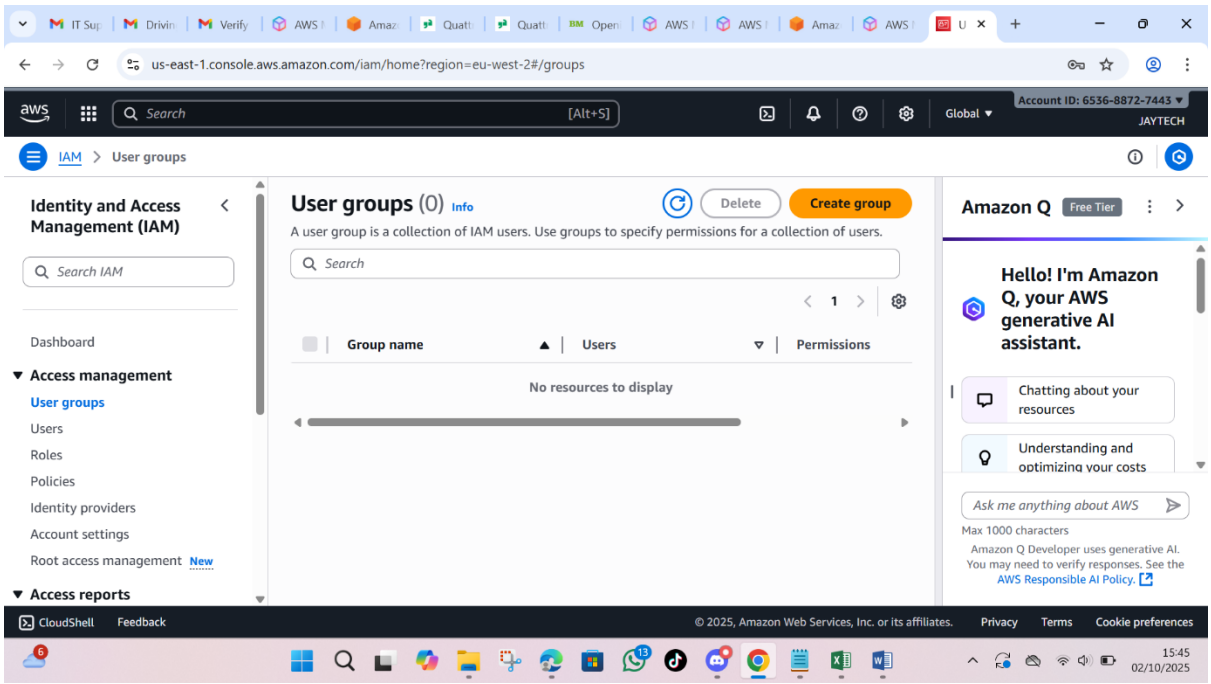

us-east-1.console.aws.amazon.com/iam/home?region=eu-west-2#/users
Search
[Alt+S]
Global
Account ID: 6536-8872-7443
JAYTECH
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Users (0) Info
Delete
Create user
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
User name
Path
Group:
Last activity
No resources to display
Amazon Q
Free Tier
Hello! I'm Amazon Q, your AWS generative AI assistant.
Chatting about your resources
Understanding and optimizing your costs
Ask me anything about AWS
Max 1000 characters
Amazon Q Developer uses generative AI. You may need to verify responses. See the AWS Responsible AI Policy.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
12:34
02/10/2025

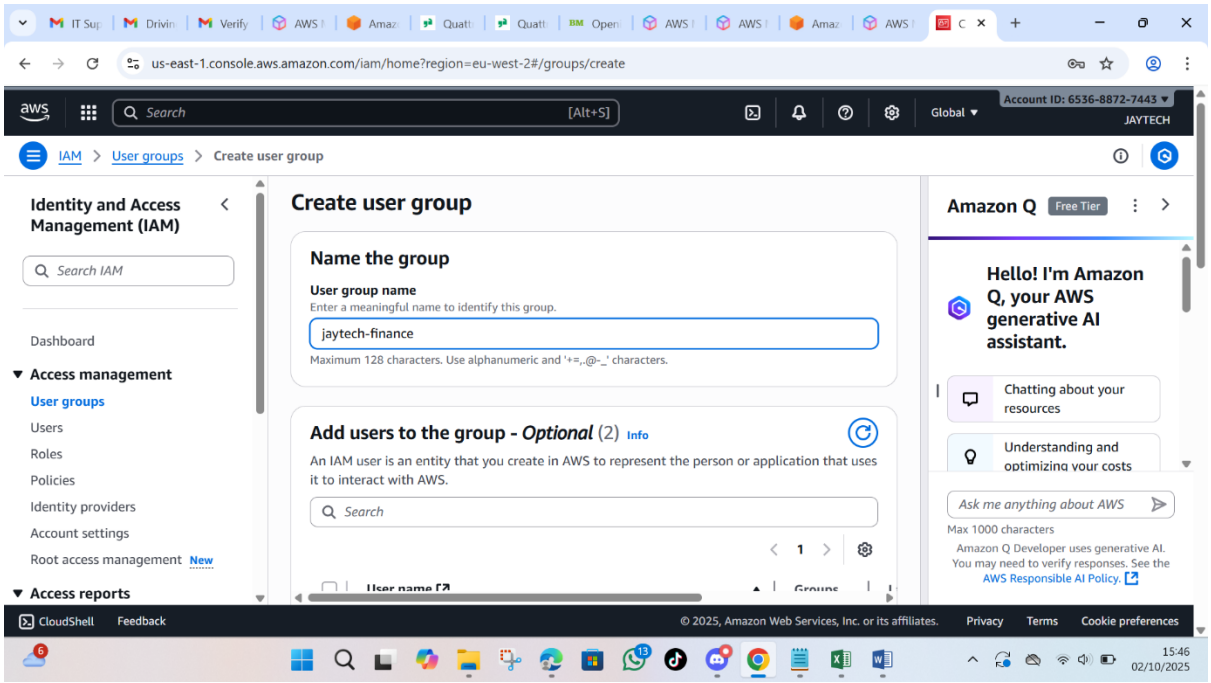

us-east-1.console.aws.amazon.com/iam/home?region=eu-west-2#/users/create
Search
[Alt+S]
Global
Account ID: 6536-8872-7443
JAYTECH
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
jaytech-Finance-King
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
Amazon Q
Free Tier
Hello! I'm Amazon Q, your AWS generative AI assistant.
Chatting about your resources
Understanding and optimizing your costs
Ask me anything about AWS
Max 1000 characters
Amazon Q Developer uses generative AI. You may need to verify responses. See the AWS Responsible AI Policy.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
12:37
02/10/2025

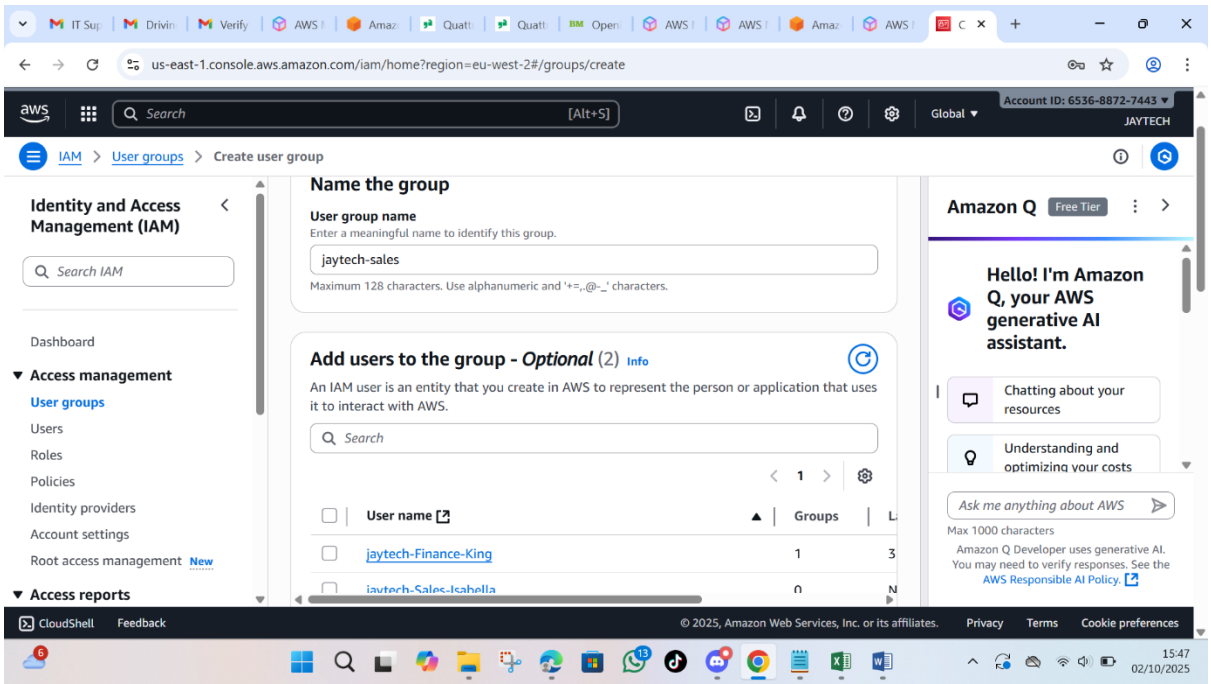


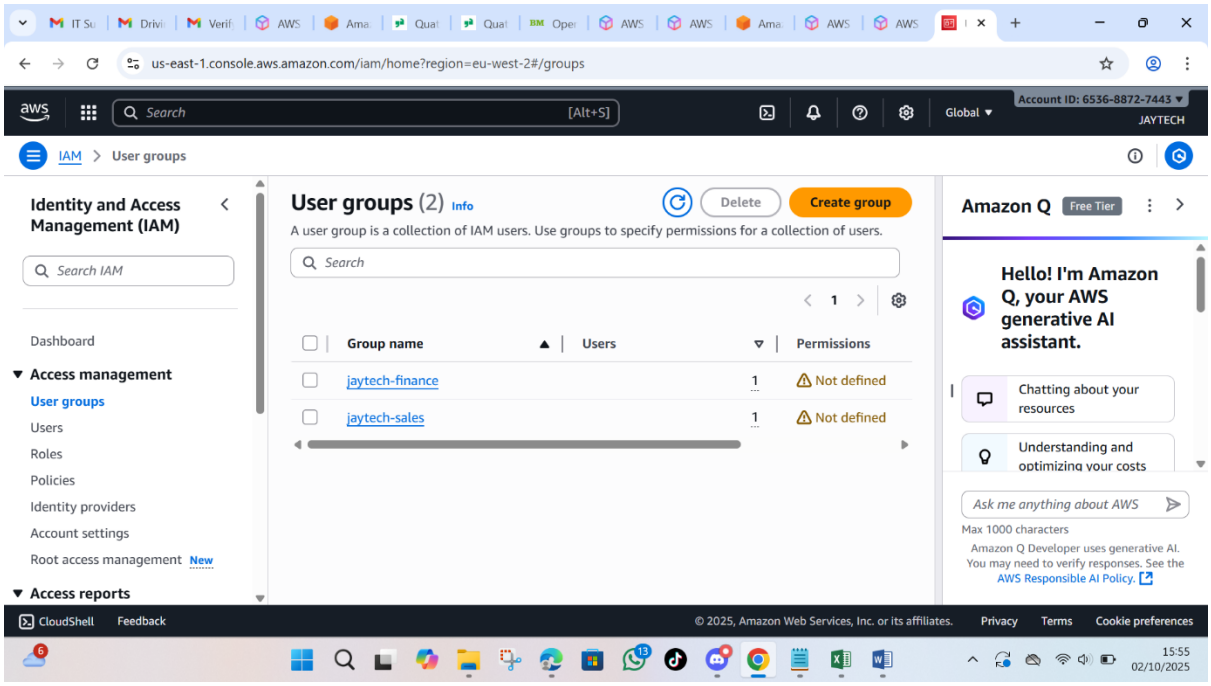
➢ Creation of users group:

I created two groups in AWS IAM: one for finance and one for sales. This allowed me to assign the previously created users, King and Isabella, to their respective groups. To create both groups, I followed the same process: I searched for IAM in the AWS Management Console, navigated to the "User Groups" section, and named the groups "Finance" and "Sales" respectively.



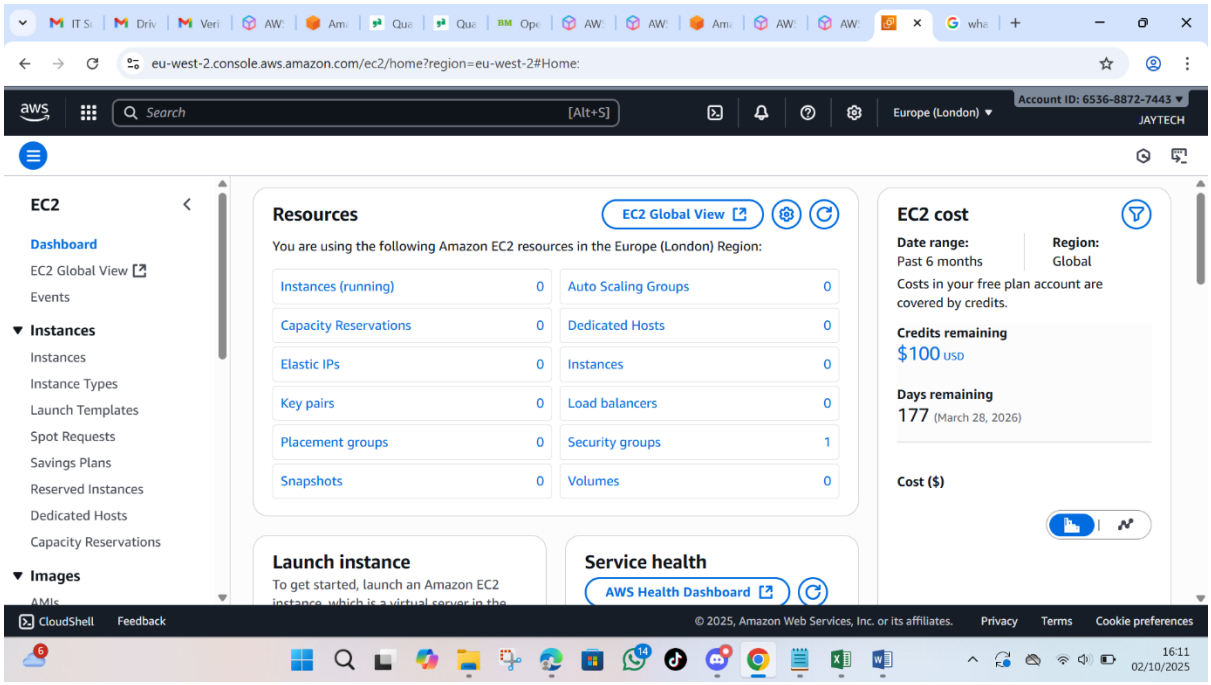

us-east-1.console.aws.amazon.com/iam/home?region=eu-west-2#/groups/create
Search [Alt+S]
Global
Account ID: 6536-8872-7443
JAYTECH
IAM > User groups > Create user group
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
jaytech-finance
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (2) 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.
Search
1
User name
Groups
Amazon Q
Free Tier
Hello! I'm Amazon Q, your AWS generative AI assistant.
Chatting about your resources
Understanding and optimizing your costs
Ask me anything about AWS
Max 1000 characters
Amazon Q Developer uses generative AI. You may need to verify responses. See the AWS Responsible AI Policy.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
15:46
02/10/2025

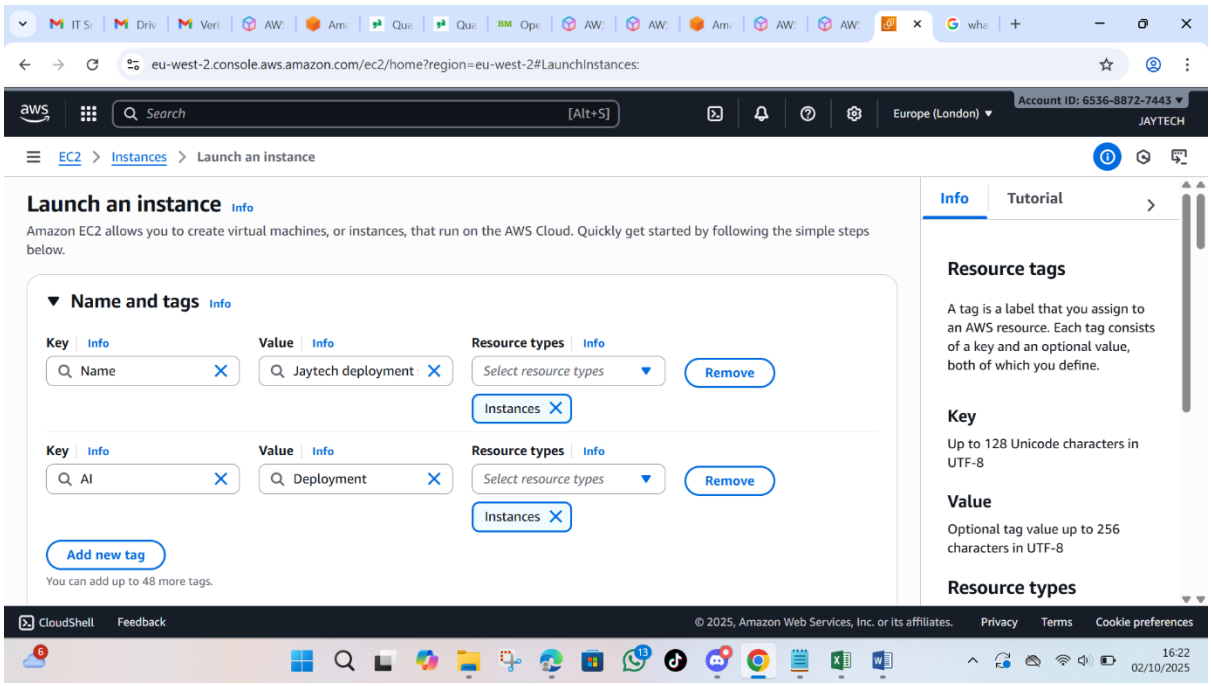

us-east-1.console.aws.amazon.com/iam/home?region=eu-west-2#/groups/create
Search [Alt+S]
Global
Account ID: 6536-8872-7443
JAYTECH
IAM > User groups > Create user group
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Name the group
User group name
Enter a meaningful name to identify this group.
jaytech-sales
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (2) 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.
Search
1
User name
Groups
jaytech-Finance-King
1
3
jaytech-Sales-Isabella
0
Amazon Q
Free Tier
Hello! I'm Amazon Q, your AWS generative AI assistant.
Chatting about your resources
Understanding and optimizing your costs
Ask me anything about AWS
Max 1000 characters
Amazon Q Developer uses generative AI. You may need to verify responses. See the AWS Responsible AI Policy.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
15:47
02/10/2025

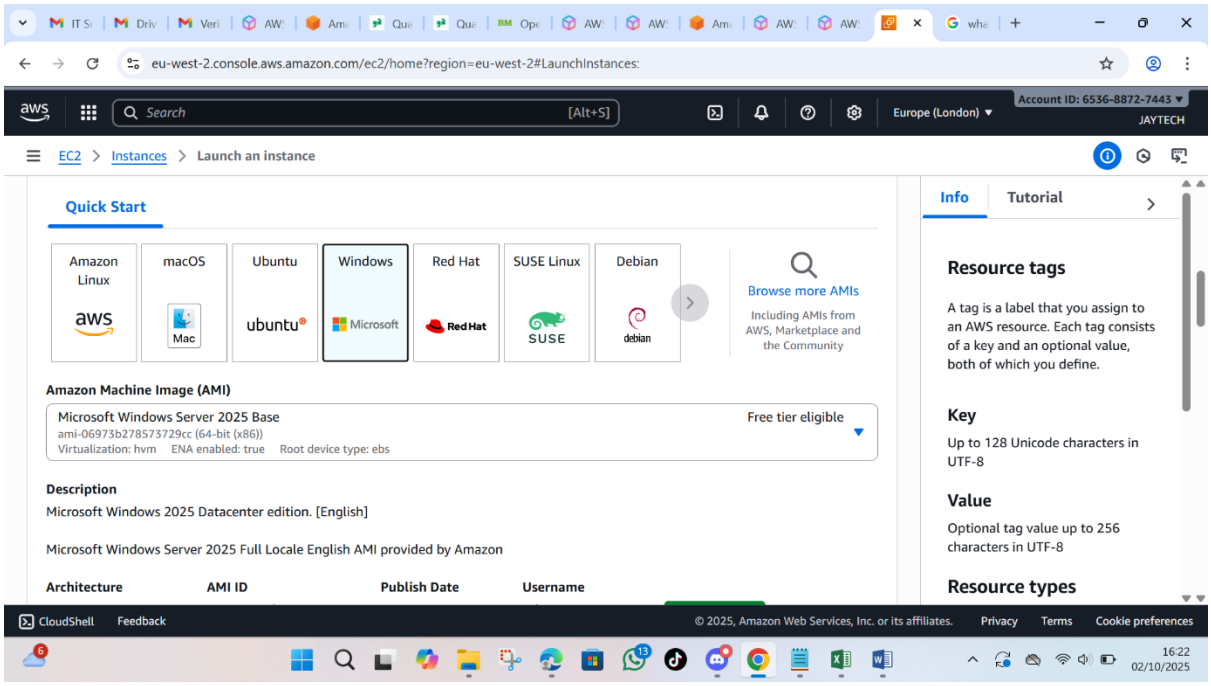


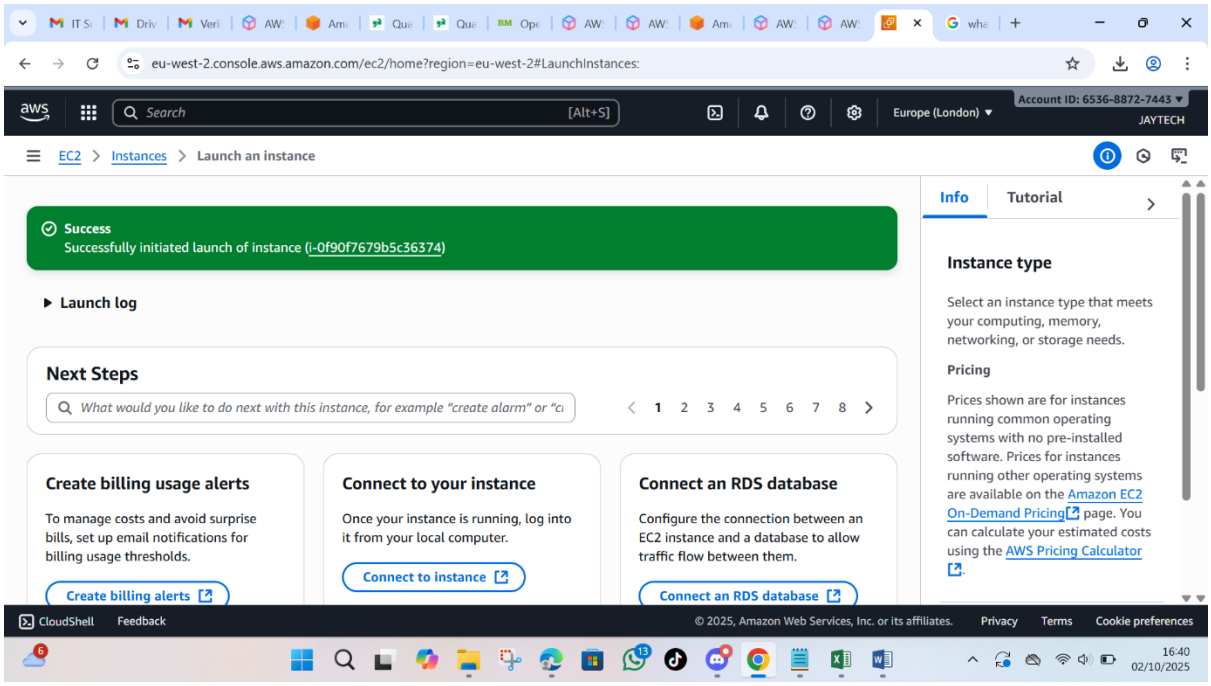
➢ The service I used to create the instance is called EC2 (Elastic Compute Cloud)

I utilized the AWS EC2 (Elastic Compute Cloud) service to create an instance. In the AWS Management Console, I looked up "EC2," chose "Launch Instance," and gave the instance the tag "jaytech deployment." I selected an Amazon Windows AMI, set the instance count to 1, and generated a key pair. Upon selecting "Next," the instance was successfully established.



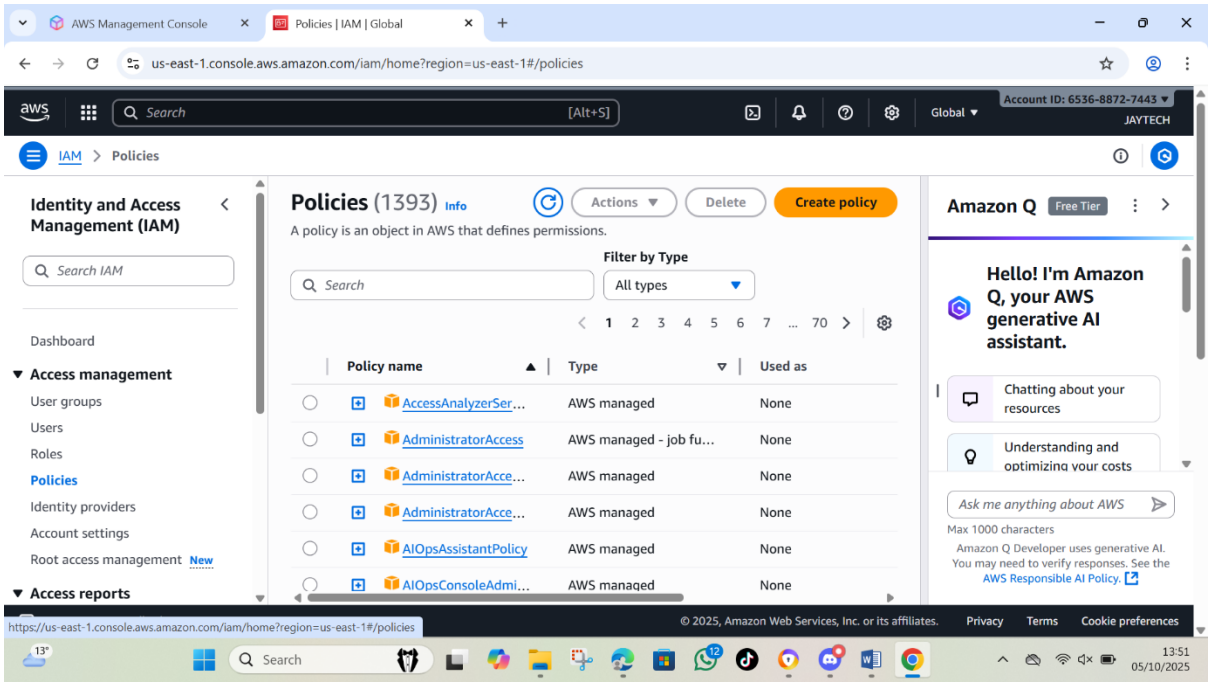

eu-west-2.console.aws.amazon.com/ec2/home?region=eu-west-2#LaunchInstances:
Search [Alt+S]
Europe (London)
Account ID: 6536-8872-7443
JAYTECH
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Key Info
Name
Value Info
Jaytech deployment
Resource types Info
Select resource types
Instances
Remove
Key Info
AI
Value Info
Deployment
Resource types Info
Select resource types
Instances
Remove
Add new tag
You can add up to 48 more tags.
Info
Tutorial
Resource tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define.
Key
Up to 128 Unicode characters in UTF-8
Value
Optional tag value up to 256 characters in UTF-8
Resource types
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
16:22
02/10/2025

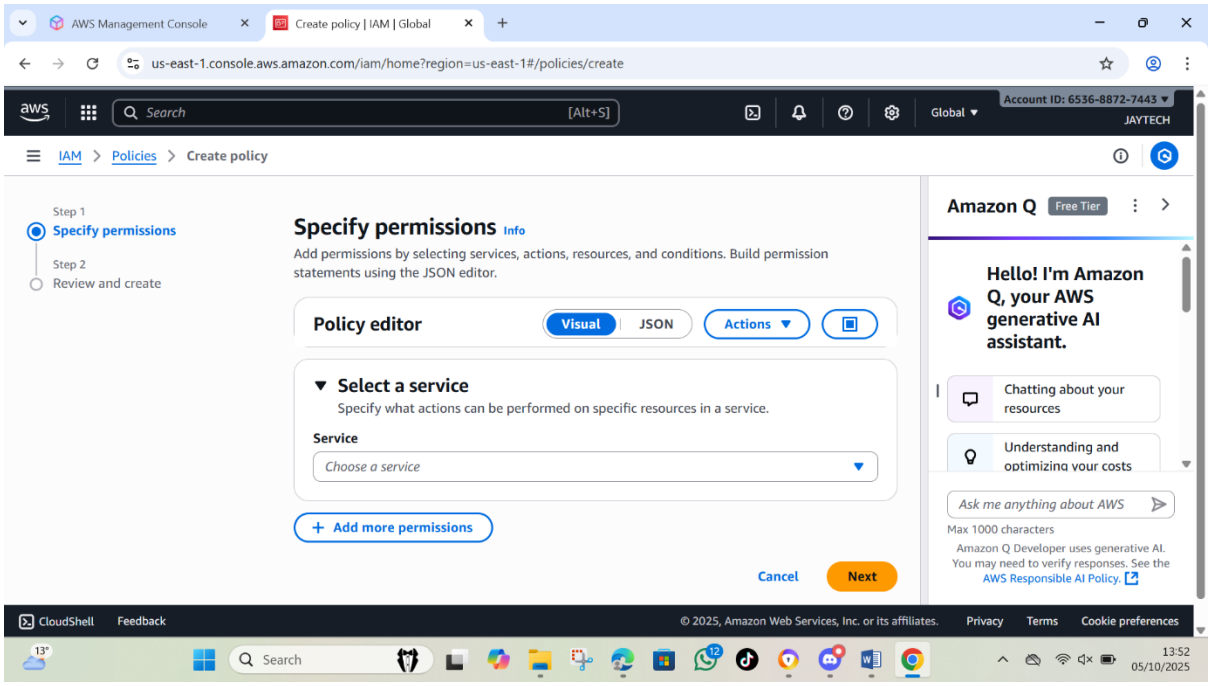

eu-west-2.console.aws.amazon.com/ec2/home?region=eu-west-2#LaunchInstances:
Search [Alt+S]
Europe (London)
Account ID: 6536-8872-7443
JAYTECH
EC2 > Instances > Launch an instance
Quick Start
Amazon Linux
macOS
Mac
Ubuntu
Windows
Red Hat
SUSE Linux
SUSE
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Microsoft Windows Server 2025 Base
ami-06973b278573729cc (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
AMI ID
Publish Date
Username
Info
Tutorial
Resource tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define.
Key
Up to 128 Unicode characters in UTF-8
Value
Optional tag value up to 256 characters in UTF-8
Resource types
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
16:22
02/10/2025

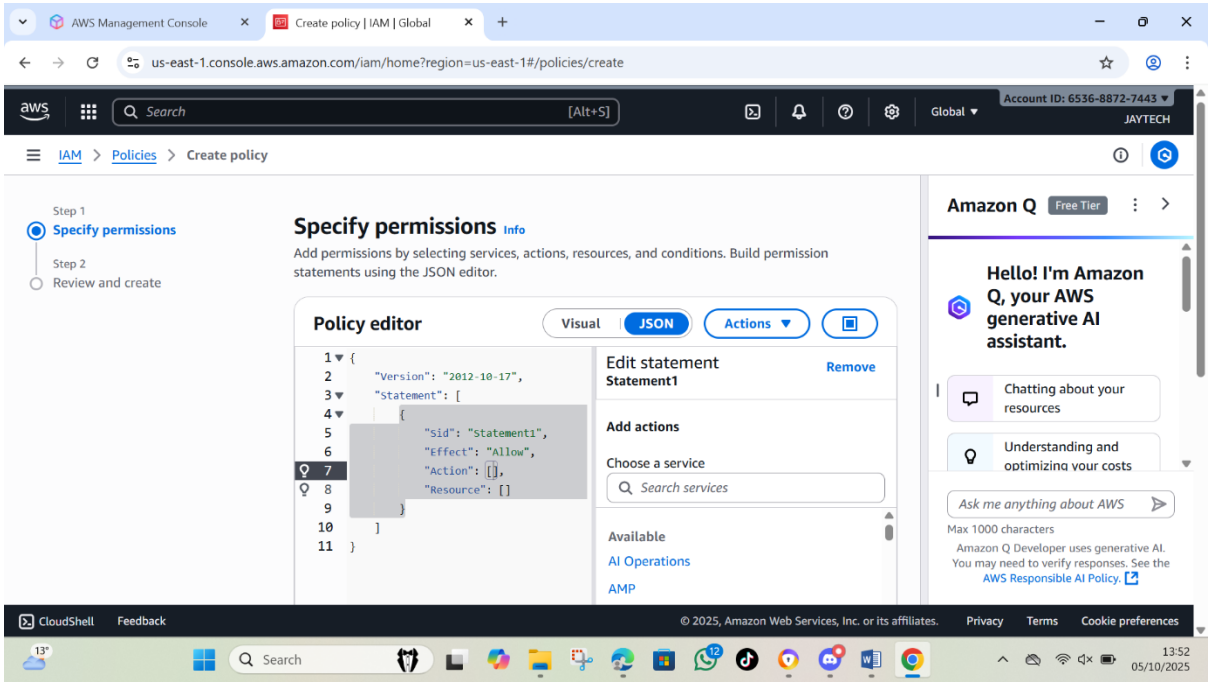


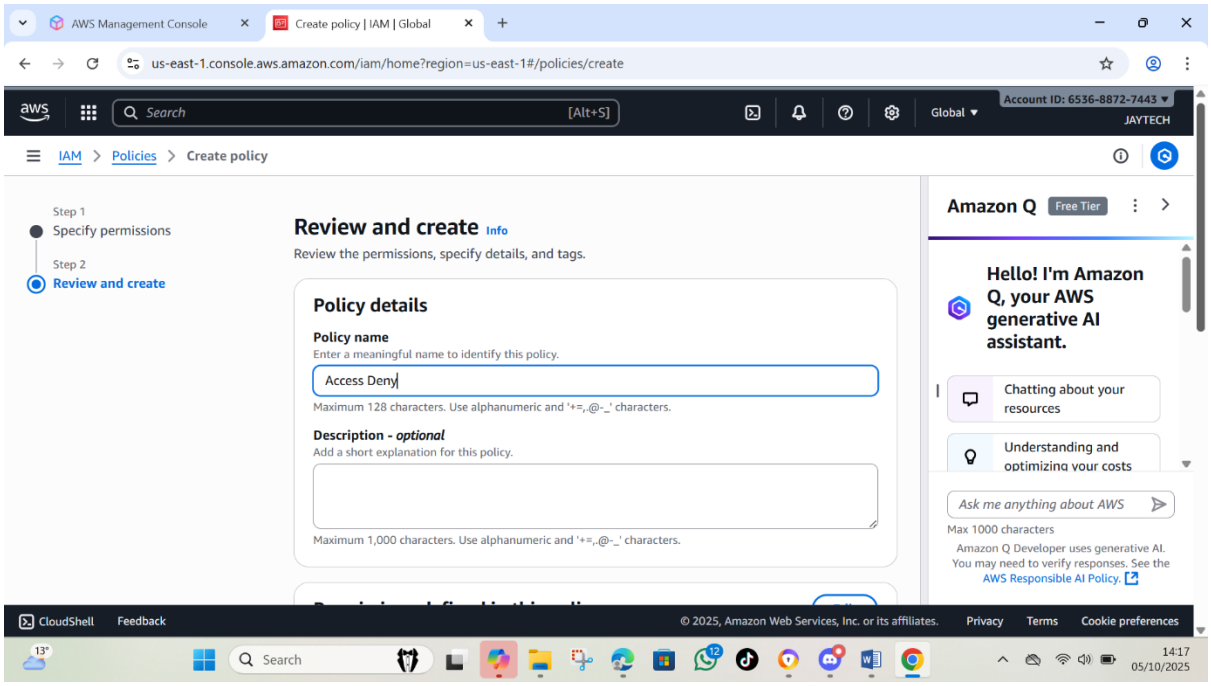
➢ Policy creation:

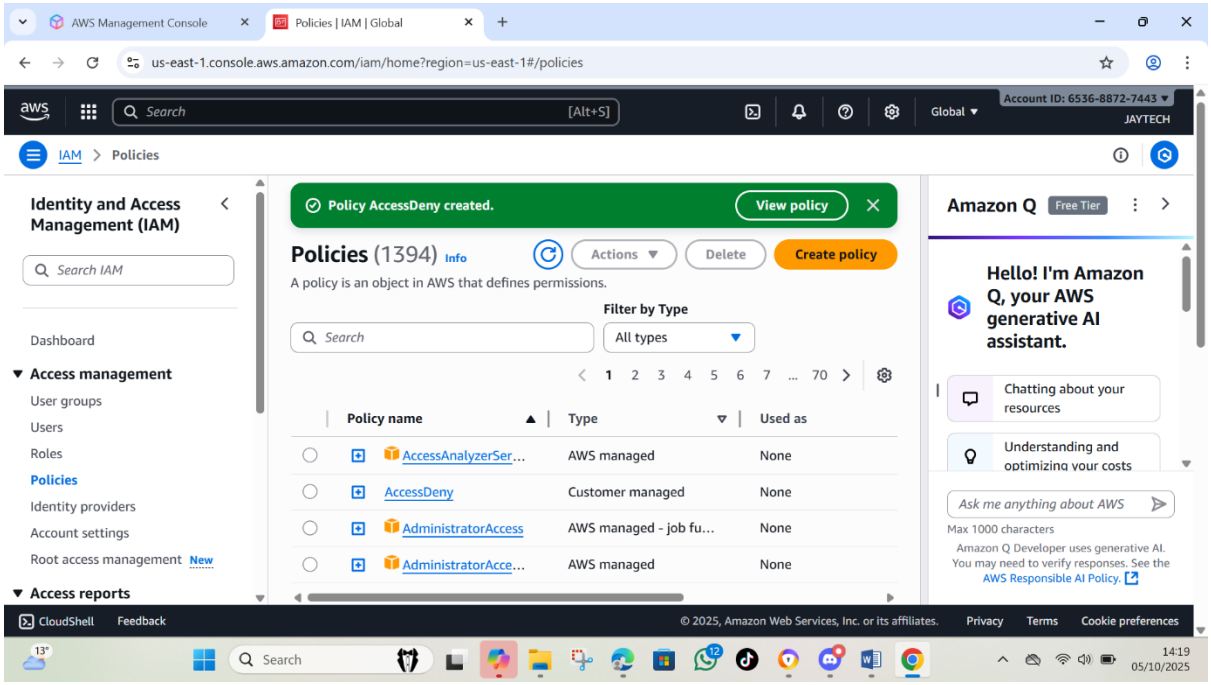
At this stage, I created a policy in AWS IAM to restrict specific user actions. I navigated to IAM, selected "Policies," and clicked "Create Policy." Using the policy editor, I chose the JSON option to customize the policy to my requirements. I named the policy "Access Deny," clicked "Next," and successfully completed the policy creation.




AWS Management Console
Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Search [Alt+S]
Global
Account ID: 6536-8872-7443
JAYTECH
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
Select a service
Specify what actions can be performed on specific resources in a service.
Service
Choose a service
Add more permissions
Cancel
Next
Amazon Q
Free Tier
Hello! I'm Amazon Q, your AWS generative AI assistant.
Chatting about your resources
Understanding and optimizing your costs
Ask me anything about AWS
Max 1000 characters
Amazon Q Developer uses generative AI. You may need to verify responses. See the AWS Responsible AI Policy.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
13:52
05/10/2025

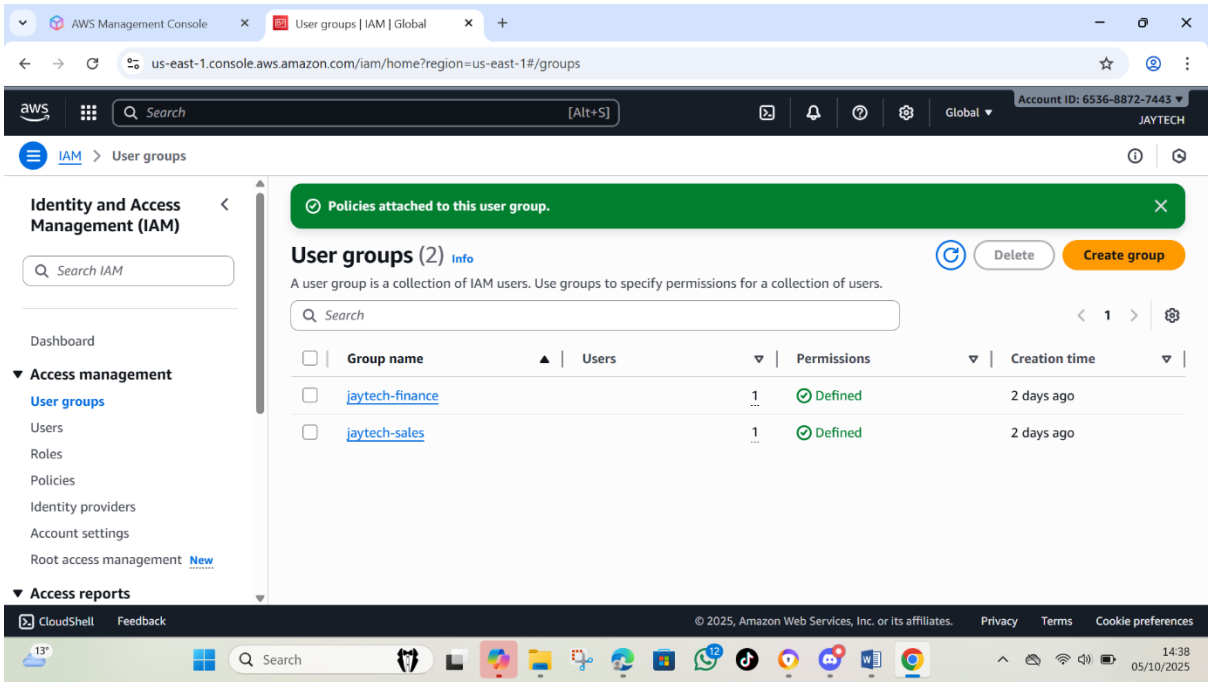

AWS Management Console
Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Search [Alt+S]
Global
Account ID: 6536-8872-7443
JAYTECH
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Action": [],
"Resource": []
}
]
}
Edit statement
Statement1
Remove
Add actions
Choose a service
Search services
Available
AI Operations
AMP
Amazon Q
Free Tier
Hello! I'm Amazon Q, your AWS generative AI assistant.
Chatting about your resources
Understanding and optimizing your costs
Ask me anything about AWS
Max 1000 characters
Amazon Q Developer uses generative AI. You may need to verify responses. See the AWS Responsible AI Policy.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
13:52
05/10/2025





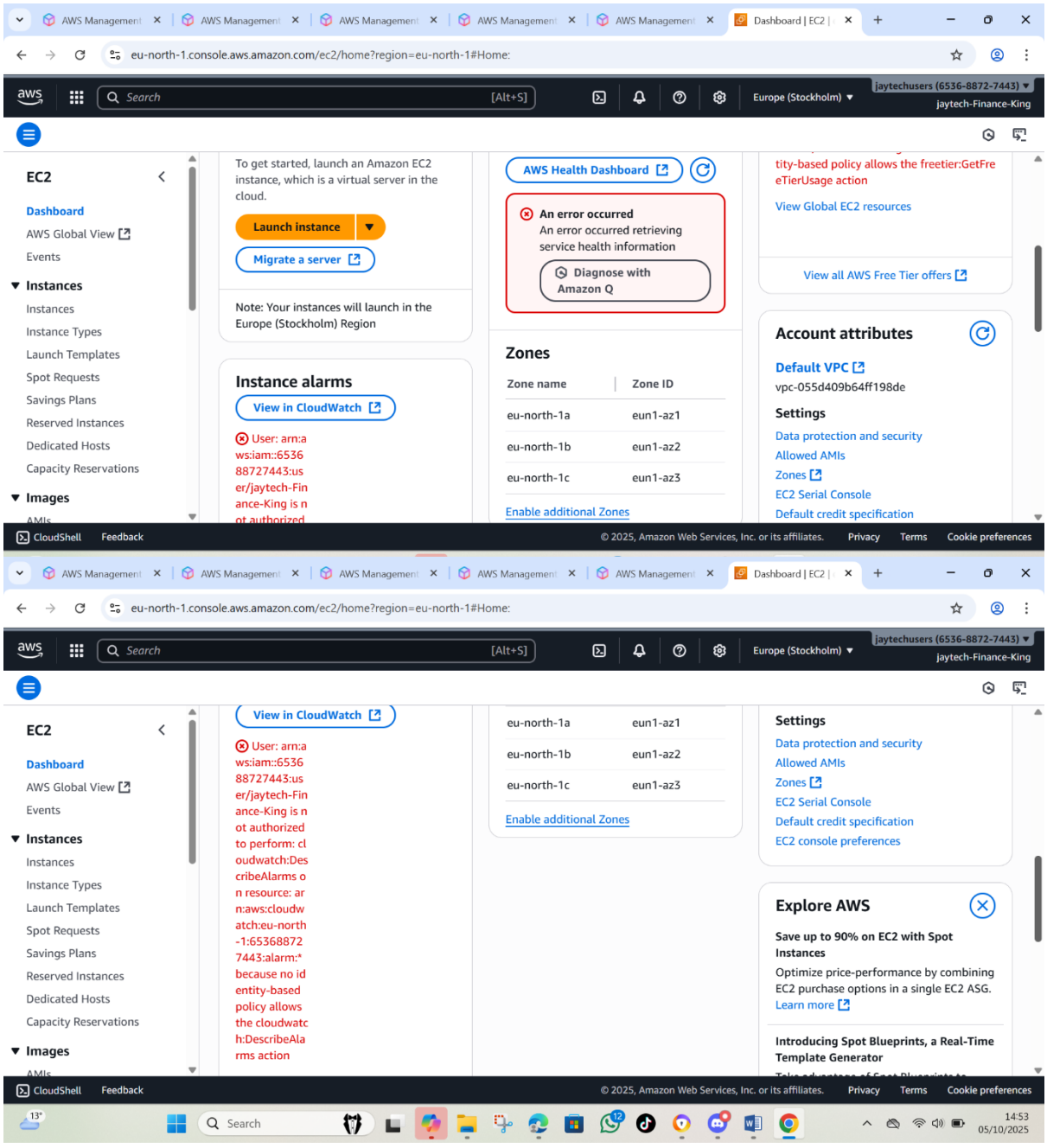
➢ Assign Policy to the group;

I made the policy and then gave it to each group I had made. I went into AWS IAM, chose the Finance and Sales groups, and then attached the "Access Deny" policy. As a result, each group's permissions were set and defined appropriately.



➢ Testing the policy:

I used the AWS account alias and each user's unique login information to access each user's account in order to confirm the policy that was issued to the users in the Finance and Sales groups. I verified upon signing in that the users lacked the root user's rights and had restricted access as specified by the "Access Deny" policy.


AWS Management
Dashboard | EC2
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Home:
Search [Alt+S]
Europe (Stockholm)
jaytechusers (6536-8872-7443)
jaytech-Finance-King
EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
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
User: arn:aws:iam::653688727443:user/jaytech-Finance-King is not authorized
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Diagnose with Amazon Q
Zones
Zone name
Zone ID
eu-north-1a
eun1-az1
eu-north-1b
eun1-az2
eu-north-1c
eun1-az3
Enable additional Zones
tity-based policy allows the freetier:GetFreeTierUsage action
View Global EC2 resources
View all AWS Free Tier offers
Account attributes
Default VPC
vpc-055d409b64ff198de
Settings
Data protection and security
Allowed AMIs
Zones
EC2 Serial Console
Default credit specification
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

AWS Management
Dashboard | EC2
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Home:
Search [Alt+S]
Europe (Stockholm)
jaytechusers (6536-8872-7443)
jaytech-Finance-King
EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
View in CloudWatch
User: arn:aws:iam::653688727443:user/jaytech-Finance-King is not authorized to perform: cloudwatch:DescribeAlarms on resource: arn:aws:cloudwatch:eu-north-1:653688727443:alarm:* because no identity-based policy allows the cloudwatch:DescribeAlarms action
eu-north-1a
eun1-az1
eu-north-1b
eun1-az2
eu-north-1c
eun1-az3
Enable additional Zones
Settings
Data protection and security
Allowed AMIs
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences
Explore AWS
Save up to 90% on EC2 with Spot Instances
Optimize price-performance by combining EC2 purchase options in a single EC2 ASG.
Learn more
Introducing Spot Blueprints, a Real-Time Template Generator
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
14:53
05/10/2025