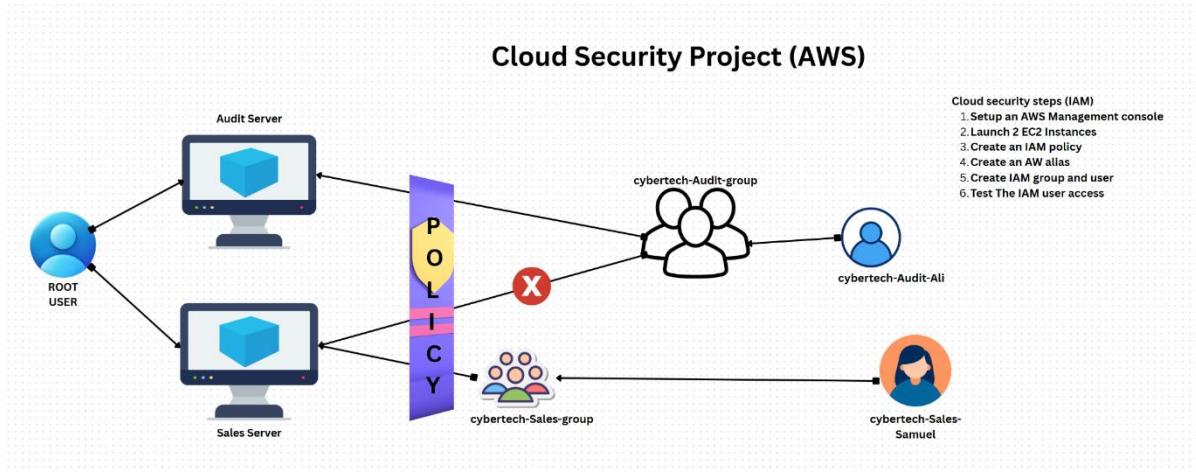


Identity Access Management(IAM) On Cloud Security with AWS

(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.

The screenshot shows the AWS Management Console IAM dashboard. On the left sidebar, under 'Access management', 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Root access management' are listed. Under 'Access reports', 'CloudShell' and 'Feedback' are shown. The main content area has a sidebar titled 'AWS Account' with 'Account ID' (653688727443) and 'Account Alias' (Create). It also includes a 'Sign-in URL for IAM users in this account' (https://653688727443.signin.aws.amazon.com/console). Below this is a 'Quick Links' section with 'My security credentials' and a note about managing access keys, MFA, and other credentials. A 'Tools' section is at the bottom. On the right, there's an 'Amazon Q' sidebar with a message from 'Hello! I'm Amazon Q, your AWS generative AI assistant.' and a 'Ask me anything about AWS' input field.

The screenshot shows the same AWS Management Console IAM dashboard as above, but with a modal dialog box in the center titled 'Create alias for AWS account 653688727443'. The dialog contains fields for 'Preferred alias' (jaytechusers) and 'New sign-in URL' (https://jaytechusers.signin.aws.amazon.com/console). A note below the URL states: 'IAM users will still be able to use the default URL containing the AWS account ID.' There are 'Cancel' and 'Create alias' buttons at the bottom. The right side of the screen still shows the 'Amazon Q' sidebar.

The screenshot shows the AWS Management Console IAM Dashboard. A green notification bar at the top right says "Alias jaytechusers created for this account." Below it, the "AWS Account" section displays the Account ID (653688727443) and Account Alias (jaytechusers). It also shows the Sign-in URL for IAM users. To the right, there's an "Amazon Q" sidebar with a message from AI assistant Amazon Q. At the bottom, the taskbar shows various open browser tabs and system icons.

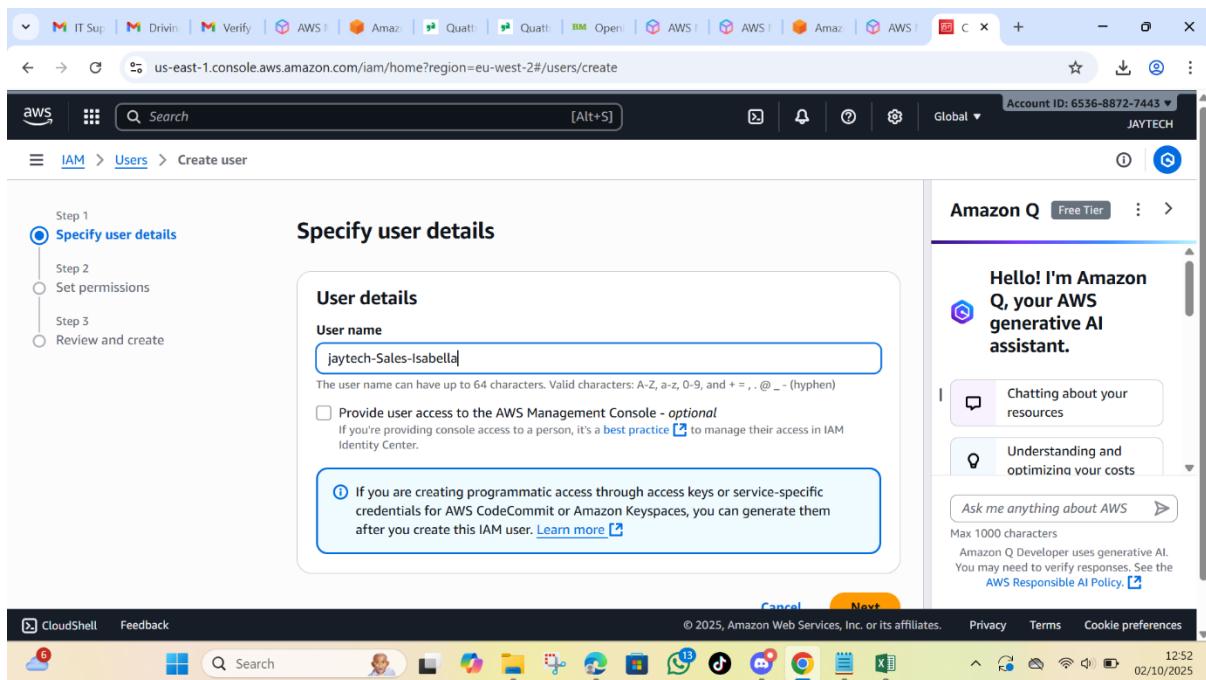
➤ Creation of users:

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.

The screenshot shows the AWS Management Console IAM Dashboard. The "Services" section has "IAM" selected, which is highlighted with a blue border. Other services listed include IAM Identity Center and Resource Access Manager. The "Features" section shows "IAM Access analyzer for S3". The "Amazon Q" sidebar is visible on the right. The taskbar at the bottom shows various open browser tabs and system icons.

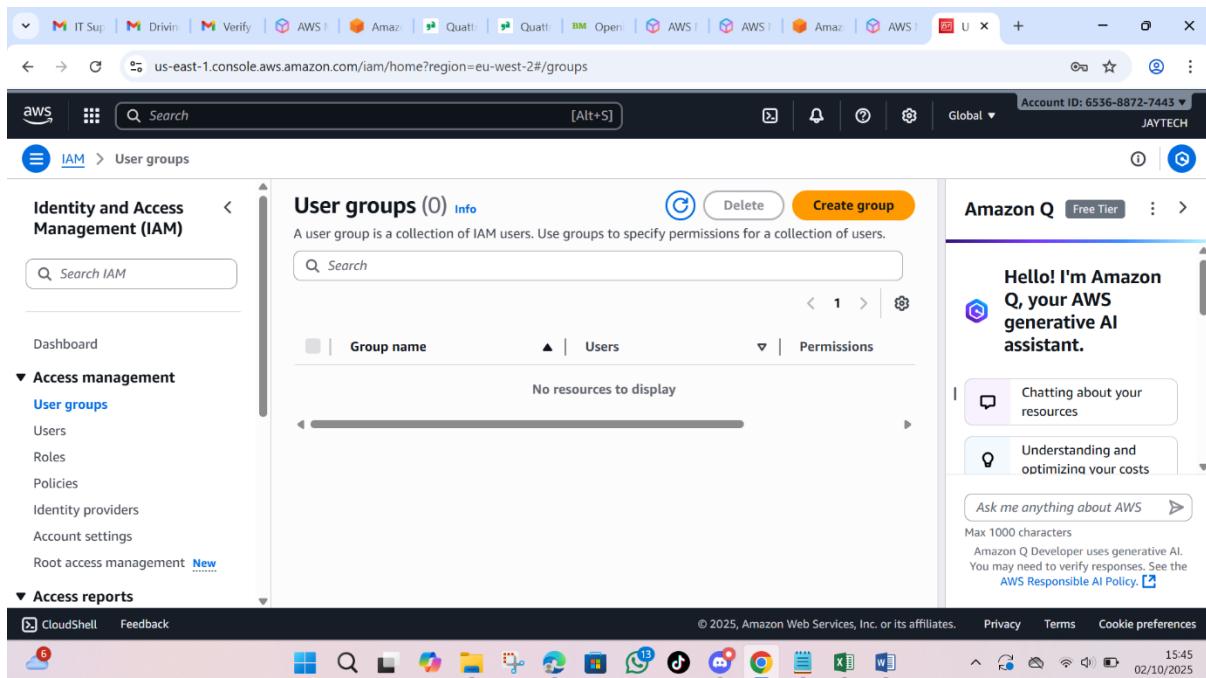
The screenshot shows the AWS IAM Users page. The left sidebar includes sections for Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management) and Access reports. The main content area displays a table titled "Users (0)" with columns for User name, Path, Group, and Last activity. A message states "No resources to display". On the right, there is an "Amazon Q" sidebar with a greeting, a search bar, and a section for asking about AWS. The bottom navigation bar includes CloudShell, Feedback, and links for Privacy, Terms, and Cookie preferences.

The screenshot shows the "Specify user details" step of the AWS IAM Create User wizard. The left sidebar lists steps: Step 1 (Specify user details, which is selected), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main content area has a "User details" section with a "User name" field containing "jaytech-Finance-King". Below it is a note about character restrictions and a checkbox for "Provide user access to the AWS Management Console - optional". A callout box asks if the user is providing console access to a person, with a "Specify a user in Identity Center - Recommended" option selected. The right sidebar features the "Amazon Q" AI assistant. The bottom navigation bar includes CloudShell, Feedback, and links for Privacy, Terms, and Cookie preferences.



➤ 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.



Screenshot of the AWS IAM console showing the 'Create user group' page. The user is creating a new user group named 'jaytech-finance'. The 'Add users to the group - Optional (2)' section shows two users assigned to the group: 'jaytech-Finance-King' and 'lautorch-Sales-Isabella'. The right sidebar features the Amazon Q AI assistant.

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

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.

User name	Groups	Last modified
jaytech-Finance-King	1	3
lautorch-Sales-Isabella	0	N

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

Screenshot of the AWS IAM console showing the 'Create user group' page. The user is creating a new user group named 'jaytech-sales'. The 'Add users to the group - Optional (2)' section shows two users assigned to the group: 'jaytech-Finance-King' and 'lautorch-Sales-Isabella'. The right sidebar features the Amazon Q AI assistant.

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

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.

User name	Groups	Last modified
jaytech-Finance-King	1	3
lautorch-Sales-Isabella	0	N

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

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar has sections for Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management) and Access reports. The main content area is titled "User groups (2)" and lists two groups: "jaytech-finance" and "jaytech-sales". Both groups have "Not defined" permissions. A search bar and a "Create group" button are at the top of the list. On the right, there's an "Amazon Q" sidebar with a greeting, a search bar, and a message about AI assistance.

➤ 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.

The screenshot shows the AWS EC2 (Elastic Compute Cloud) home page. The left sidebar has sections for Dashboard, Instances (Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), and Images (AMIs). The main content area is divided into three main sections: "Resources" (listing Instances (running), Auto Scaling Groups, Capacity Reservations, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes), "EC2 cost" (Date range: Past 6 months, Region: Global, Costs in your free plan account are covered by credits, Credits remaining: \$100 USD, Days remaining: 177 (March 28, 2026)), and "Launch instance" (with a link to "AWS Health Dashboard"). A "CloudShell" and "Feedback" button are at the bottom.

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. On the left, under 'Name and tags', two tags are defined:

- Key: Name, Value: Jaytech deployment, Resource type: Instances
- Key: AI, Value: Deployment, Resource type: Instances

A button 'Add new tag' is visible. On the right, there are sections for 'Resource tags', 'Key' (with a note about Unicode characters), 'Value' (with a note about tag value length), and 'Resource types'.

At the bottom, the browser toolbar shows CloudShell and Feedback, and the status bar indicates 16:22 and 02/10/2025.

The screenshot shows the 'Launch an instance' wizard. In the 'Quick Start' section, several AMIs are listed:

- Amazon Linux
- macOS
- Ubuntu
- Windows
- Red Hat
- SUSE Linux
- Debian

A 'Browse more AMIs' link is available. Below this, the 'Amazon Machine Image (AMI)' section shows:

Microsoft Windows Server 2025 Base
ami-06973b278573729cc (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

The 'Free tier eligible' status is shown. The 'Description' section notes: Microsoft Windows 2025 Datacenter edition. [English]. The 'Architecture', 'AMI ID', 'Publish Date', and 'Username' columns are listed at the bottom.

On the right, the 'Resource tags' section is expanded, along with 'Key' and 'Value' definitions. The 'Resource types' section is also visible.

At the bottom, the browser toolbar shows CloudShell and Feedback, and the status bar indicates 16:22 and 02/10/2025.

The screenshot shows the AWS EC2 'Launch an instance' page. At the top, there's a green success message: 'Successfully initiated launch of instance (i-0f90f7679b5c36374)'. Below it, there's a 'Launch log' section. Under 'Next Steps', there are three cards: 'Create billing usage alerts', 'Connect to your instance', and 'Connect an RDS database'. The 'Connect to your instance' card has a 'Connect to instance' button. On the right side, there's an 'Instance type' section with a note about selecting a type that meets computing, memory, networking, or storage needs. It also includes a 'Pricing' section with a note about prices for common operating systems and links to the Amazon EC2 On-Demand Pricing and AWS Pricing Calculator. The bottom of the screen shows the Windows taskbar with various pinned icons.

➤ 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.

The screenshot shows the AWS IAM 'Policies' page. The left sidebar has sections for 'Identity and Access Management (IAM)', 'Access management', 'Policies', and 'Access reports'. The main area displays a table of policies with columns for 'Policy name', 'Type', and 'Used as'. Policies listed include 'AccessAnalyzerSer...', 'AdministratorAccess', 'AdministratorAcce...', 'AdministratorAcce...', 'AIOpsAssistantPolicy', and 'AIOpsConsoleAdmi...'. The right side features an 'Amazon Q' AI assistant interface with a greeting, a search bar, and a message input field. The bottom of the screen shows the Windows taskbar.

Screenshot of the AWS Management Console showing the 'Create policy' wizard - Step 1: Specify permissions.

The Policy editor interface is displayed, with the 'JSON' tab selected. A sample JSON policy document is shown:

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "Statement1",  
6             "Effect": "Allow",  
7             "Action": [],  
8             "Resource": []  
9         }  
10    ]  
11 }
```

The 'Add more permissions' button is visible at the bottom left of the editor.

On the right side of the screen, the Amazon Q AI assistant is open, displaying a greeting and some sample conversational prompts.

Screenshot of the AWS Management Console showing the 'Create policy' wizard - Step 1: Specify permissions.

The Policy editor interface is displayed, with the 'JSON' tab selected. A sample JSON policy document is shown, identical to the one in the previous screenshot:

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "Statement1",  
6             "Effect": "Allow",  
7             "Action": [],  
8             "Resource": []  
9         }  
10    ]  
11 }
```

The 'Add more permissions' button is visible at the bottom left of the editor.

On the right side of the screen, the Amazon Q AI assistant is open, displaying a greeting and some sample conversational prompts.

The screenshot shows the AWS Management Console with the URL us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create. The top navigation bar includes tabs for 'Create policy | IAM | Global'. The main content area is titled 'Review and create' with a sub-section 'Policy details'. Under 'Policy name', the value 'Access Deny' is entered. A note states: 'Maximum 128 characters. Use alphanumeric and '+,-,_,@-' characters.' Below it, 'Description - optional' is listed with a note: 'Add a short explanation for this policy.' A large text input field is present. The bottom of the page shows a progress bar with 'Step 1: Specify permissions' and 'Step 2: Review and create'. On the right, the Amazon Q AI assistant is visible, displaying a greeting and several conversational options like 'Chatting about your resources' and 'Understanding and optimizing your costs'. The status bar at the bottom shows 'CloudShell Feedback' and various system icons.

The screenshot shows the AWS Management Console with the URL us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies. The top navigation bar includes tabs for 'Policies | IAM | Global'. The main content area shows a list of policies under 'Policies (1394)'. A green success message box says 'Policy AccessDeny created.' with a 'View policy' button. The table lists policies by name, type, and used as. The sidebar features the Amazon Q AI assistant. The status bar at the bottom shows 'CloudShell Feedback' and various system icons.

➤ 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.

User groups (2) Info

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

Group name	Users	Permissions	Creation time
jaytech-finance	1	Defined	2 days ago
jaytech-sales	1	Defined	2 days ago

➤ 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.

The screenshot shows the AWS EC2 Home page. On the left, the navigation menu includes EC2, Dashboard, Instances, and Images. Under Instances, there are links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations. Under Images, there is a link for AMIs.

The main content area has two sections: "Launch instance" and "Migrate a server". A note states: "Note: Your instances will launch in the Europe (Stockholm) Region". Below this is the "Instance alarms" section with a "View in CloudWatch" button.

A red box highlights an error message: "An error occurred An error occurred retrieving service health information Diagnose with Amazon Q".

On the right side, there is a sidebar titled "Account attributes" which lists the Default VPC (vpc-055d409b64ff198de), Settings (Data protection and security, Allowed AMIs, Zones, EC2 Serial Console, Default credit specification), and a "CloudWatch Metrics" section.

At the bottom, there is an "Explore AWS" section with a "Save up to 90% on EC2 with Spot Instances" offer and an "Introducing Spot Blueprints, a Real-Time Template Generator" section.

At the very bottom, the status bar shows the date (05/10/2025) and time (14:53).