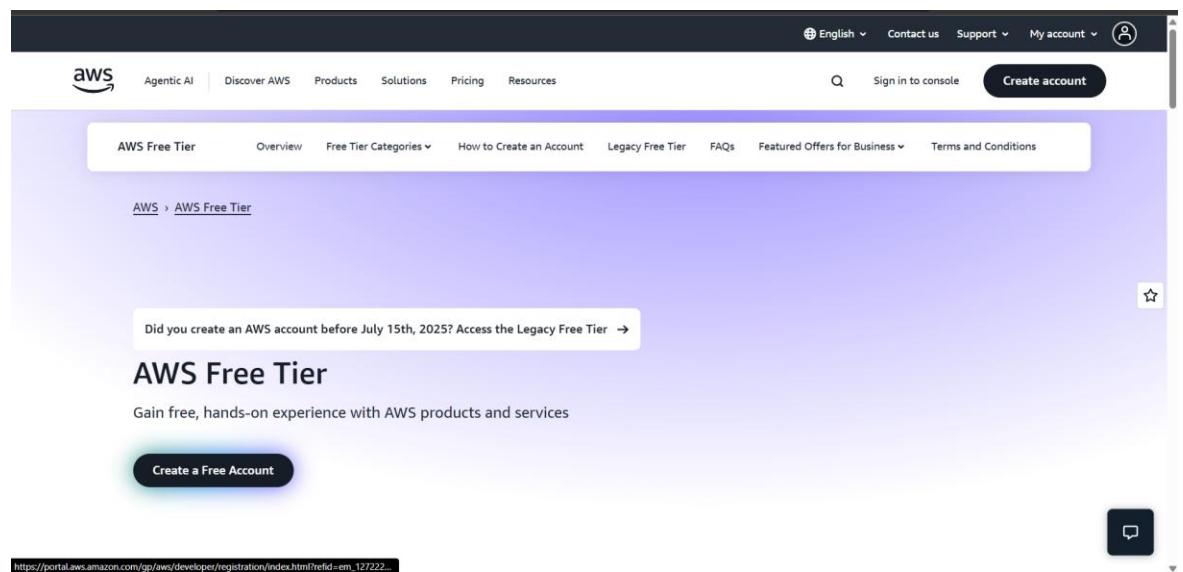


- **What AWS is and its key benefits**
  - Amazon Web Services is a cloud computing platform that provides scalable, reliable, and low-cost infrastructure. It is utilized to host websites, store files, run databases and more. The key benefits include:
    - Pay-as-you-go pricing
    - Scalable infrastructure
    - Global Reach
    - Access to 200 services
- **Signing up AWS for free**
  - To get started, sign up for the AWS Free Tier:
    - Go to [<https://aws.amazon.com/free>] and click, “Create a Free Account”



- Enter email address and AWS will send a verification code to your email. Enter the verification code and set up your password.

The screenshot shows the AWS sign-up process. At the top right is the AWS logo. Below it, a large blue button says "Sign up for AWS". To its left, a smaller button says "Verify email address". Between them is a link "OR". Below that is a link "Sign in to an existing AWS account". On the left side of the page, there's a section titled "Try AWS at no cost for up to 6 months" with a sub-section "Start with USD \$100 in AWS credits, plus earn up to USD \$100 by completing various activities." Below this text are three blue wireframe illustrations: a server rack, a rocket launching from a platform, and another server rack. The main sign-up form has fields for "Root user email address" (containing "faithgabriellegamboa046@gmail.com") and "AWS account name" (containing "Faith Gabrielle Gamboa").

- Provide contact information such as full name, phone number, and address.

This screenshot shows the "Contact Information" section of the AWS sign-up form. It includes fields for "Full Name" (containing "Faith Gabrielle Gamboa"), "Country Code" (containing "+63"), "Phone Number" (containing "9674306842"), "Country or Region" (containing "United States"), "Address line 1", "Address line 2" (containing "Apartment, suite, unit, building, floor, etc."), and "City". There are also "Next Step" and "Create Account" buttons at the bottom.

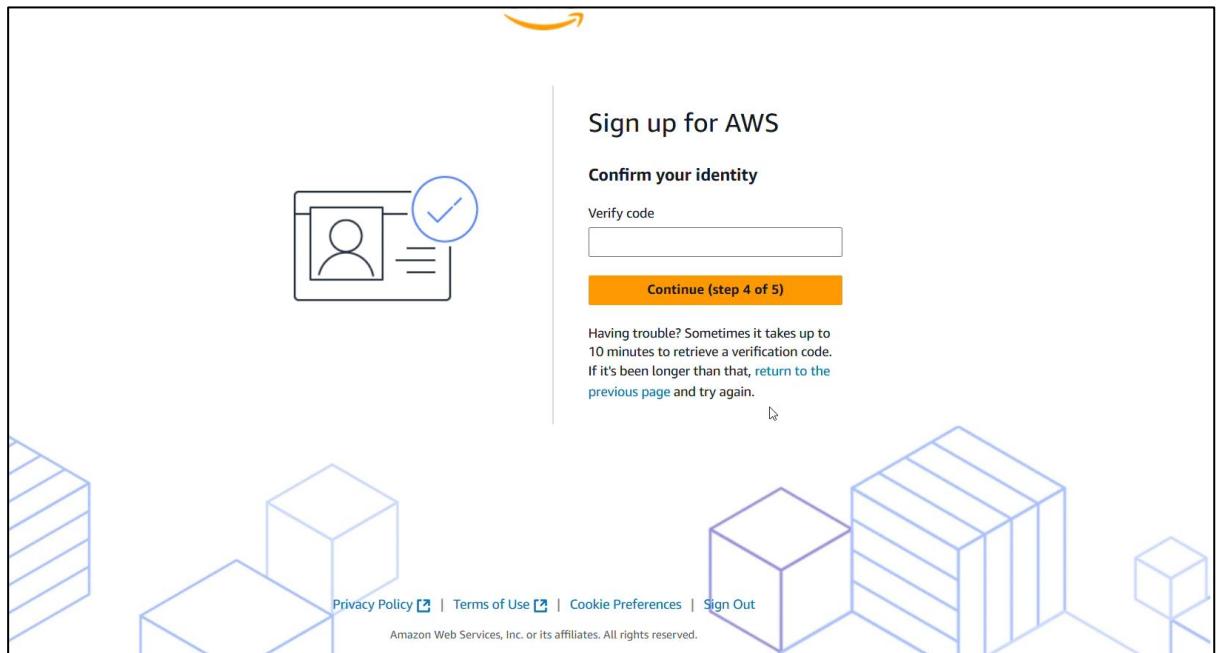
- Enter billing information.

The screenshot shows the AWS sign-up process. At the top right, there are links for "How is your experience?", "Provide Feedback", "Language", and "English". The AWS logo is at the top center. The main heading is "Sign up for AWS". On the left, there's a callout box titled "Why is this required?" explaining that verification holds USD \$1 for 3-5 days to prevent fraud. It also states that for the free plan, no charges occur until upgrade to a paid plan, and providing billing info enables a seamless upgrade. The right side contains fields for "Billing Information": "Billing country" (Philippines), "Credit or Debit card number" (input field), "Expiration date" (dropdowns for Month and Year), and "Security code" (CVV/CVC input field).

- AWS will ask you to confirm your identity by prompting you to provide your contact number, and a verification code will be sent.

The screenshot shows the AWS sign-up process. On the left, there's a graphic of a person icon with a checkmark. The main heading is "Sign up for AWS". Under "Confirm your identity", it says: "Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code." Below this, there are options for "How should we send you the verification code?": "Text message (SMS)" (selected) and "Voice call". A dropdown for "Country or region code" shows "Philippines (+63)". An input field for "Mobile phone number" contains "0967430684". A large orange button at the bottom right says "Send SMS (step 4 of 5)". The background features abstract blue geometric shapes.

- You will be asked to go through a security verification first before you can enter the code sent in your contact number.



### Created Account (Screenshot)

**Billing and Cost Management** > Account

**Account Info**

**Account details**

- Name: Faith Gabrielle Gamboa
- ID: 837563945083
- Service provider: Amazon Web Services, Inc.
- ARN: arn:aws:account:837563945083:account

**Account display settings - new**

Account color: None

To see the display settings, users must have `AWSManagementConsoleBasicUserAccess` permission. Use the [IAM console](#) [AWSManagementConsoleBasicUserAccess](#) to manage user policies. [Learn more](#)

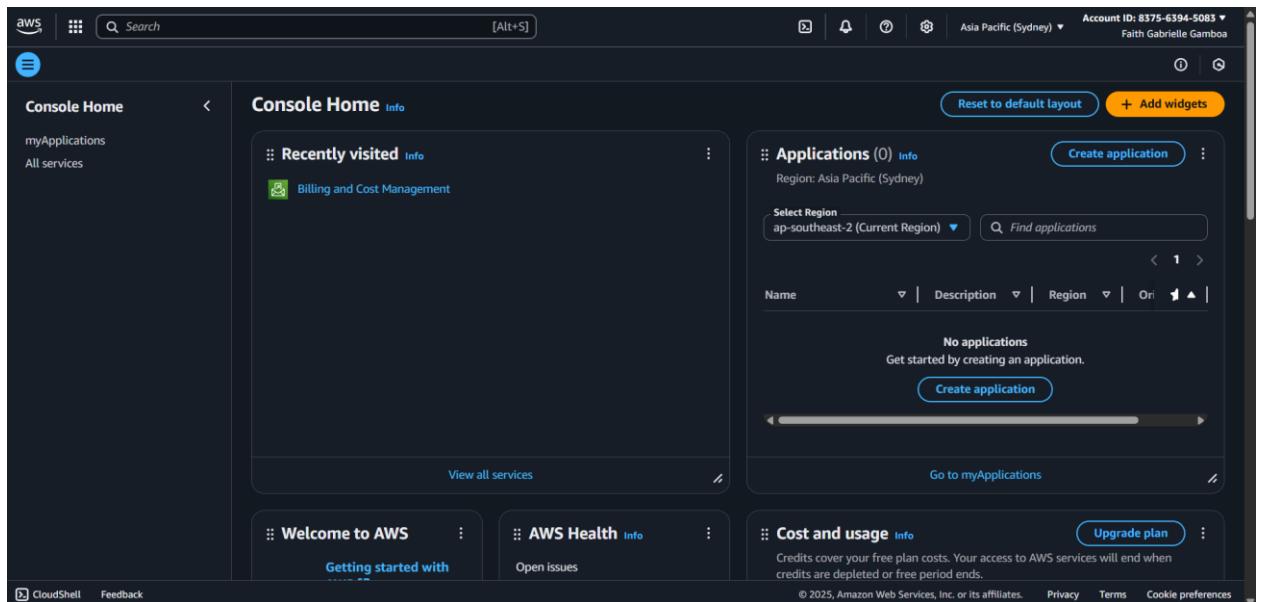
**Contact information**

Full name: Faith Gabrielle Gamboa	Company name: None	Address: Block 327 Lot 14 Paloma Circle Street, Barangay Rizal
-----------------------------------	--------------------	--

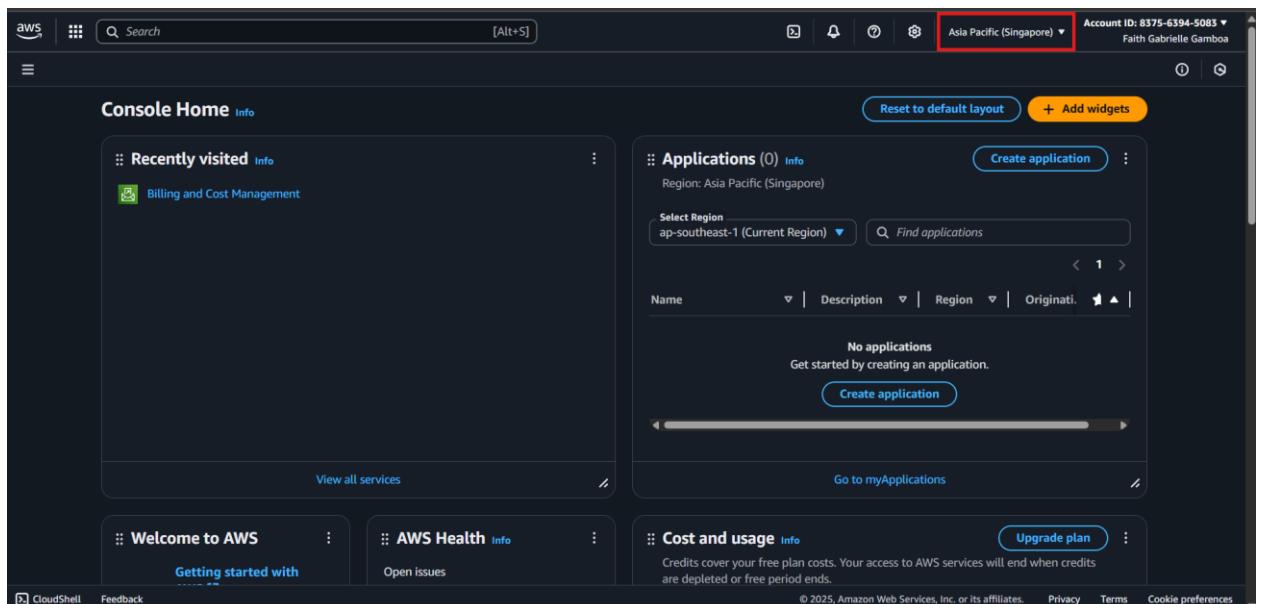
- Setting a goal: Hosting a website on AWS**
  - EC2 (Elastic Compute Cloud) for hosting
  - S3 (Simple Storage Service) for file storage
  - RDS (Relational Database Service) for database needs

- **Exploring the AWS Management Console**

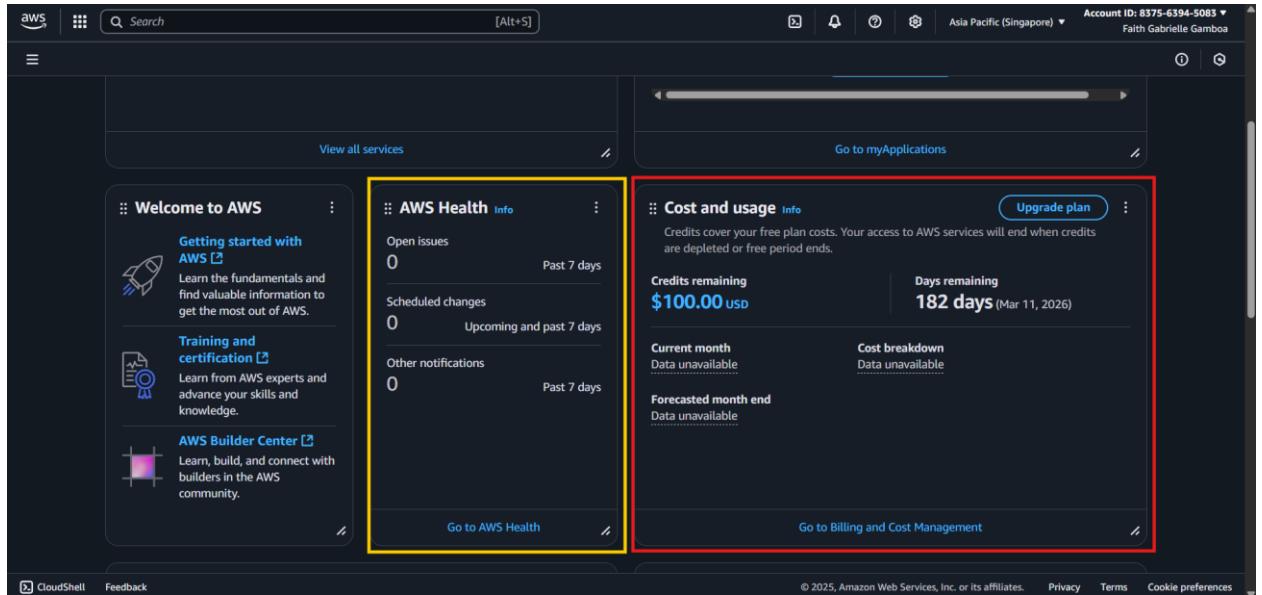
- Access the AWS Management Console which is an overview of your account and access all AWS services.



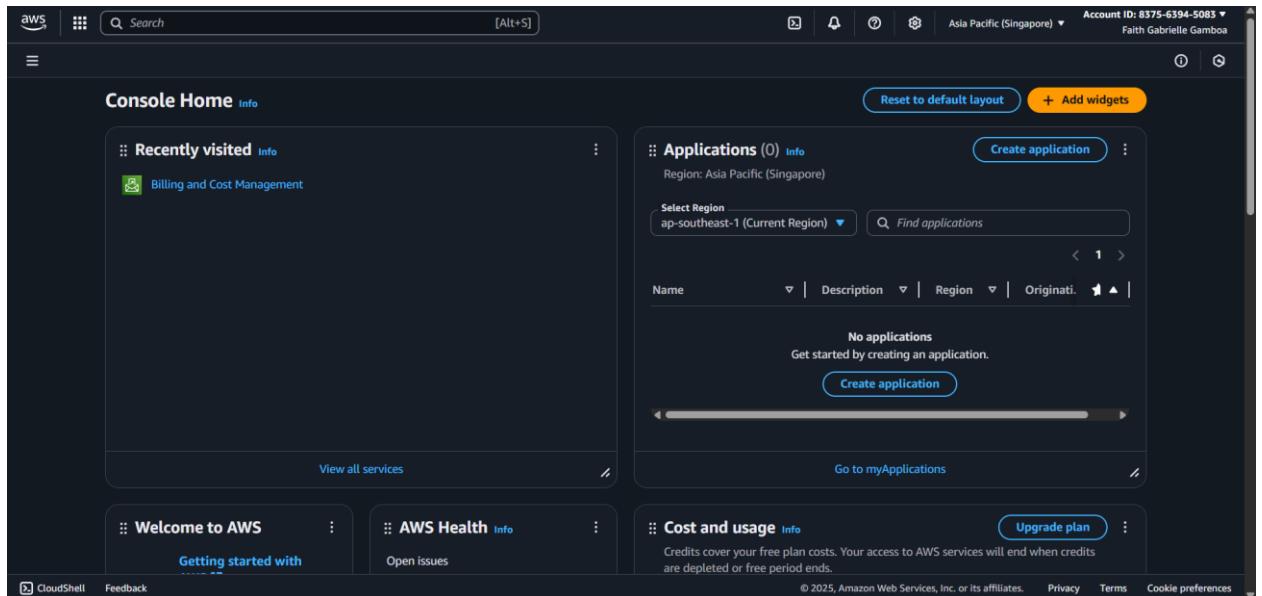
- It is important to pick the right region, since each one is a different physical location (data center), and things such as services and pricing can change depending on where you choose.



- The cost and usage panel shows how much you are using AWS services and how much it is costing you. The AWS Health panels shows any notifications, or any updates that may affect AWS services.



- Scroll down the page to access the documentation if you need more help.
- EC2 – Launching a virtual server**
- Go to Console Home



- Click All Services to view all services provided by AWS. Click EC2.

The screenshot shows the AWS All Services console. The top navigation bar includes 'Console Home' and 'All services'. Below it, the main title is 'All services'. A section titled 'Services by category' lists three main categories: Compute, Quantum Technologies, and Security, Identity, & Compliance. Under Compute, 'EC2' is listed and highlighted with a red box. Other services in Compute include Lightsail, Lambda, Batch, Elastic Beanstalk, Serverless Application Repository, AWS Outposts, EC2 Image Builder, AWS App Runner, AWS SimSpace Weaver, Parallel Computing Service, and AWS Global View. The Quantum Technologies and Security sections also contain several AWS services each.

- To create a new EC2 instance, click the Launch Instance button.

The screenshot shows the AWS EC2 service dashboard. The left sidebar menu includes 'Dashboard', 'Instances' (with sub-options like Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), 'Images' (AMIs, AMI Catalog), and 'Elastic Block Store' (Volumes, Snapshots, Lifecycle Manager). The main content area has a 'Resources' summary table and a 'Launch instance' section. The 'Launch instance' button is highlighted with a red box. Other buttons in this section include 'Migrate a server'. Below these are notes about launching instances in the Asia Pacific (Singapore) Region and a note about CloudWatch metrics. The right side of the dashboard displays 'EC2 cost' (date range: Past 6 months, Region: Global, credits remaining \$100 usd, days remaining 181), 'Service health' (status: operating normally), 'Zones' (Zone name and Zone ID), and 'Account attributes' (Default VPC: vpc-0fc0901fe7a3b955b, Settings: Data protection and security, Allowed AMIs, Zones).

- Enter the important details such as the Web Server Name, Operating System Image, Instance Type, Key Pair, Network Settings and Storage Configuration. Once you are finished, click the Launch Instance button.

**Name and tags**

Name: MyWebServer

**Application and OS Images (Amazon Machine Image)**

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

**Summary**

Number of instances: 1

**Software Image (AMI)**

Amazon Linux 2023 AMI 2023.8.2... [read more](#)  
ami-0abd2d0501963c350

**Virtual server type (instance type)**

t3.micro

**Firewall (security group)**

New security group

**Storage (volumes)**

1 volume(s) - 8 GiB

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

**Amazon Machine Image (AMI)**

Amazon Linux 2023 kernel-6.1 AMI  
ami-0abd2d0501963c350 (64-bit (x86), uefi-preferred) / ami-0787fd46c032f549c (64-bit (Arm), uefi)  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.8.20250908.0 x86\_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username	Verified provider
64-bit (x86)	uefi-preferred	ami-0abd2d0501963c350	2025-09-06	ec2-user	

**Instance type**

t3.micro

Family: t3 2 vCPU 1 GiB Memory Current generation: true  
On-Demand Windows base pricing: 0.0224 USD per Hour  
On-Demand SUSE base pricing: 0.0132 USD per Hour On-Demand Linux base pricing: 0.0132 USD per Hour  
On-Demand Ubuntu Pro base pricing: 0.0167 USD per Hour  
On-Demand RHEL base pricing: 0.042 USD per Hour

Free tier eligible

All generations

Compare instance types

**Summary**

Number of instances: 1

**Software Image (AMI)**

Amazon Linux 2023 AMI 2023.8.2... [read more](#)  
ami-0abd2d0501963c350

**Virtual server type (instance type)**

t3.micro

**Firewall (security group)**

New security group

**Storage (volumes)**

1 volume(s) - 8 GiB

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

Screenshot of the AWS EC2 Launch Wizard - Step 2: Set Instance Details

**Key pair (login)**

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

**Network settings**

**Network** Info vpc-0fc0901fe7a3b955b

**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 SSH traffic from Anywhere 0.0.0.0/0 Helps you connect to your instance

**Summary**

Number of instances 1

Software Image (AMI) Amazon Linux 2023 AMI 2023.8.2... [read more](#) ami-0abd2d0501963c350

Virtual server type (instance type) t3.micro

Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 8 GiB

Screenshot of the AWS EC2 Launch Wizard - Step 2: Set Instance Details

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

**Configure storage**

1x 8 GiB gp3 Root volume, 3000 IOPS, Not encrypted Advanced

Add new volume

Click refresh to view backup information The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

**Advanced details** Info

**Summary**

Number of instances 1

Software Image (AMI) Amazon Linux 2023 AMI 2023.8.2... [read more](#) ami-0abd2d0501963c350

Virtual server type (instance type) t3.micro

Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 8 GiB

- Once the instance is created, click the link to take a look.

The screenshot shows the AWS EC2 Instances "Launch an instance" page. At the top, there is a green success message: "Success Successfully initiated launch of instance (i-0c012e6afe098d12)". Below this, there is a "Next Steps" section with several options:

- Create billing usage alerts**: To manage costs and avoid surprise bills, set up email notifications for billing usage thresholds. Includes a "Create billing alerts" button.
- Connect to your instance**: Once your instance is running, log into it from your local computer. Includes a "Connect to instance" button and a "Learn more" link.
- Connect an RDS database**: Configure the connection between an EC2 instance and a database to allow traffic flow between them. Includes a "Connect an RDS database" button and a "Create a new RDS database" link.
- Create EBS snapshot policy**: Create a policy that automates the creation, retention, and deletion of EBS snapshots. Includes a "Create EBS snapshot policy" button.

Below these steps are three additional buttons: "Manage detailed monitoring", "Create Load Balancer", and "Create AWS budget". At the bottom of the page, there are links for CloudShell, Feedback, and a footer with copyright information and links for Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS EC2 Instances page for the instance i-0c012e6afe098d12. On the left, there is a navigation sidebar with categories like Dashboard, EC2 Global View, Events, Instances, Images, Elastic Block Store, and more. The main content area displays the "Instance summary for i-0c012e6afe098d12 (MyWebServer)" with the following details:

Detail	Value
Instance ID	i-0c012e6afe098d12
IPv6 address	-
Hostname type	IP name: ip-172-31-21-166.ap-southeast-1.compute.internal
Answer private resource DNS name	IPv4 (A)
Auto-assigned IP address	54.151.249.140 [Public IP]
IAM Role	-
IMDSv2	Required
Public IPv4 address	54.151.249.140   open address
Instance state	Running
Private IP DNS name (IPv4 only)	ip-172-31-21-166.ap-southeast-1.compute.internal
Instance type	t3.micro
VPC ID	vpc-0fc0901fe7a3b955b
Subnet ID	subnet-07c055291641f3336
Instance ARN	arn:aws:ec2:ap-southeast-1:837563945083:instance/i-0c012e6afe098d12
Private IPv4 addresses	172.31.21.166
Public DNS	ec2-54-151-249-140.ap-southeast-1.compute.amazonaws.com   open address
Elastic IP addresses	-
AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto Scaling Group name	-
Managed	false

At the bottom of the page, there are links for CloudShell, Feedback, and a footer with copyright information and links for Privacy, Terms, and Cookie preferences.

- Scroll down and go to the Security tab.

The screenshot shows the AWS EC2 Instances page for an instance named i-0c012e6afe098d12. The 'Security' tab is highlighted with a red box. In the 'Security groups' section, the group 'sg-09a36936c3f7d734c (launch-wizard-1)' is listed. The 'Inbound rules' table shows one rule: Name sgr-02eae5aceb10c86bf, Port range 22, Protocol TCP, Source 0.0.0.0/0, and Security group launch-wizard-1. The 'Outbound rules' table is empty.

- Click the 'launch-wizard-1' to create a new rule for the HTTP traffic.

This screenshot is identical to the previous one, showing the AWS EC2 Instances page for the same instance. However, the link 'sg-09a36936c3f7d734c (launch-wizard-1)' in the 'Security groups' section is highlighted with a red box and a yellow underline, indicating it has been clicked.

- Click on the Edit Inbound Rules button.

The screenshot shows the AWS EC2 Security Groups console. The left sidebar is collapsed. The main area displays the details of a security group named "sg-09a36936c3f7d734c - launch-wizard-1". The "Inbound rules" tab is selected. A red box highlights the "Edit inbound rules" button at the top right of the "Inbound rules (1)" table. Below the table, a warning message states: "⚠️ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only." At the bottom right of the dialog are "Cancel", "Preview changes", and "Save rules" buttons.

Name	Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-02eae5aceb10c86bf	SSH	TCP	22	Custom	0.0.0.0/0	

- Click the Add Rule button.

**Edit inbound rules**

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-02eae5aceb10c86bf	SSH	TCP	22	Custom	0.0.0.0/0

Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Preview changes Save rules

- Enter the port number 8080 and pick the default range of IP addresses which 0.0.0.0/0 in order to allow all IP addresses. Once done, click the Save Rules button.

**Edit inbound rules**

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-02eae5aceb10c86bf	SSH	TCP	22	Custom	0.0.0.0/0
-	Custom TCP	TCP	8080	Anywhere	0.0.0.0/0

Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Preview changes Save rules

- **S3 – Configuring file storage**

- Go to the search bar on top of the screen and type in S3. Click S3 in the first result to jump over to the S3 service.

The screenshot shows the AWS Management Console search results for 'S3'. The search bar at the top contains the text 'S3'. The 'Services' section is expanded, showing the 'S3 Scalable Storage in the Cloud' service card, which is highlighted with an orange box. Other services listed include S3 Glacier and AWS Snow Family. To the right, there's a VPC configuration panel showing a VPC ID and inbound rules.

- You are going to store your files in what Amazon calls a ‘bucket.’ A bucket is like a root folder or a drive utilized to organize your files. Start by clicking the Create Bucket button.

The screenshot shows the Amazon S3 landing page. The main heading is 'Amazon S3' with the subtext 'Store and retrieve any amount of data from anywhere'. To the right, there's a 'Create a bucket' button, which is highlighted with an orange box. Below the main heading, there's a 'How it works' section with a video thumbnail and a 'Pricing' section with a link to the Simple Monthly Calculator.

- Fill the necessary fields, such as Bucket Type, Bucket Name, Object Ownership, Public Access Settings, Bucket Versioning, Tags, and lives the rest to their default values. Once done, click the Create Bucket button.

**Create bucket** info

Buckets are containers for data stored in S3.

### General configuration

AWS Region  
Asia Pacific (Singapore) ap-southeast-1

Bucket type Info

General purpose  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory  
Recommended for specialized low-latency use cases supported by AWS Availability Zones or data residency use cases supported by AWS Local Zones.

Bucket name Info  
my-server-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 Info  
Bucket owner enforced

Block Public Access settings for this bucket

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 using ACLs.
- 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.

**Create bucket** info

Buckets are containers for data stored in S3.

### General configuration

AWS Region  
Asia Pacific (Singapore) ap-southeast-1

Bucket type Info

General purpose  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory  
Recommended for specialized low-latency use cases supported by AWS Availability Zones or data residency use cases supported by AWS Local Zones.

Bucket name Info  
my-server-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 Info  
Bucket owner enforced

Block Public Access settings for this bucket

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 using ACLs.
- 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.

**Turning off block all public access might result in this bucket and the objects within becoming public**

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

**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 easily recover from 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.

**Default encryption**

Server-side encryption is automatically applied to new objects stored in this bucket.

**Encryption type** [Info](#)

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

Server-side encryption with Amazon S3 managed keys (SSE-S3)  
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)  
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

**Bucket Key**

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Enable  
 Disable

**Advanced settings**

[After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.](#)

[CloudShell](#) [Feedback](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

**Default encryption** [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

**Encryption type** [Info](#)

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

Server-side encryption with Amazon S3 managed keys (SSE-S3)  
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)  
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

**Bucket Key**

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Enable  
 Disable

**Advanced settings**

[After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.](#)

[Create bucket](#)

[Cancel](#)

[CloudShell](#) [Feedback](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

- Click on the bucket, navigate to the Permissions tab, scroll down to the Bucket Policy section, and click Edit.

The screenshot shows the AWS S3 Buckets page. At the top, there is a green success message: "Successfully created bucket 'my-serving-bucket-8797564'". Below this, there are two tabs: "General purpose buckets" (selected) and "Directory buckets". A table lists one bucket:

Name	AWS Region	Creation date
my-serving-bucket-8797564	Asia Pacific (Singapore) ap-southeast-1	September 11, 2025, 19:42:10 (UTC+08:00)

On the right side of the page, there are two cards: "Account snapshot" and "External access summary - new".

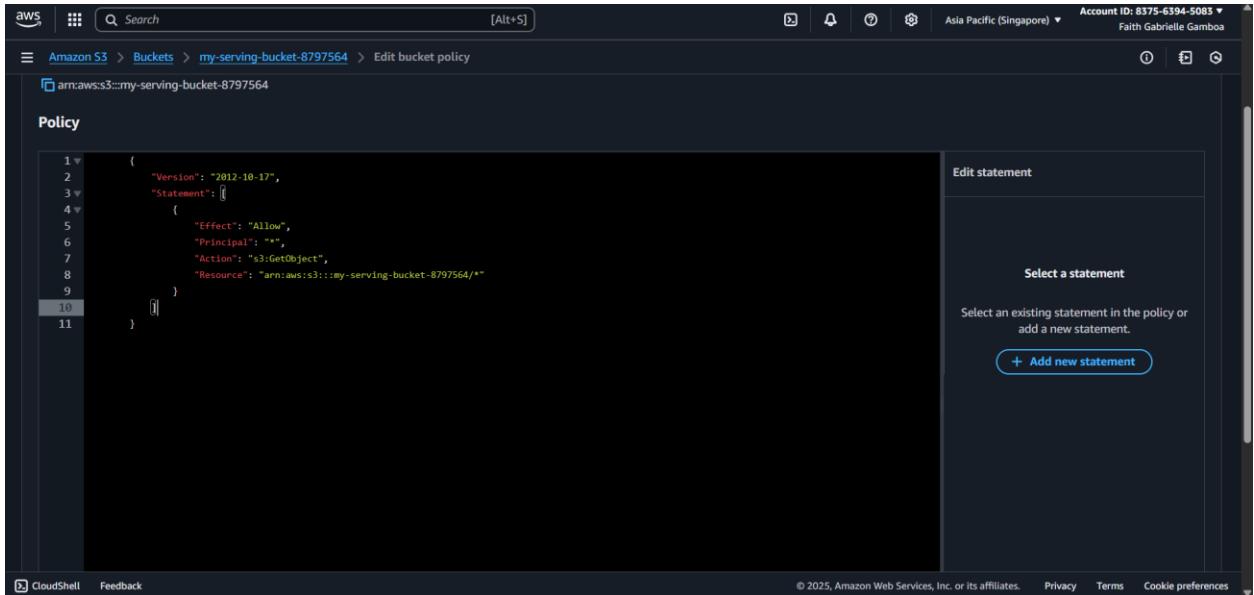
The screenshot shows the AWS S3 Bucket Permissions page for the bucket "my-serving-bucket-8797564". The "Permissions" tab is selected. The page is divided into sections: "Permissions overview", "Block public access (bucket settings)", and "Bucket policy".

**Permissions overview**: Contains "Access finding" information and a link to "View analyzer for ap-southeast-1".

**Block public access (bucket settings)**: Shows "Block all public access" status as "Off". There is a link to "Individual Block Public Access settings for this bucket".

**Bucket policy**: Shows the JSON for the bucket policy and includes an "Edit" button (which is highlighted with a green box).

- Paste the bucket policy into the console. Make sure to update the resource name if your bucket has a different name. This makes the bucket public which allows everyone to read or download all files. Once done, scroll down and click Save Changes.



The screenshot shows the AWS S3 Bucket Policy editor. The left pane displays a JSON policy document:

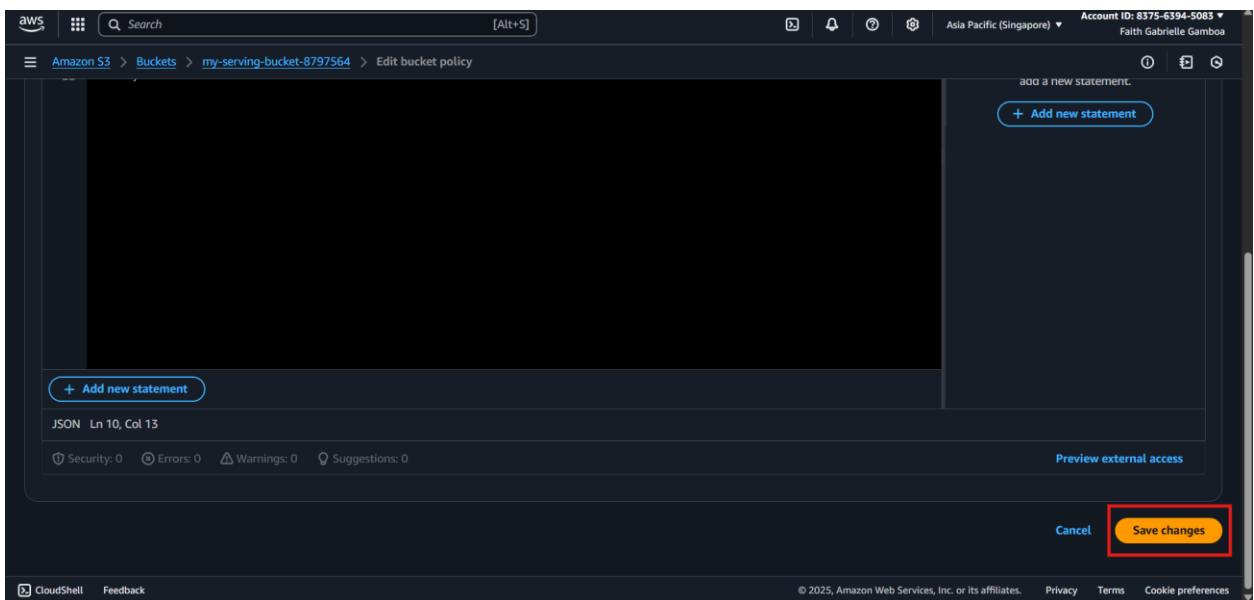
```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Principal": "*",
7        "Action": "s3:GetObject",
8        "Resource": "arn:aws:s3:::my-serving-bucket-8797564/*"
9      }
10     ]
11   }

```

The right pane contains a sidebar with the following interface:

- Edit statement**: A large text area for viewing and editing statements.
- Select a statement**: A section for selecting existing statements.
- Add new statement**: A button to add a new statement.



The screenshot shows the AWS S3 Bucket Policy editor with the following interface elements:

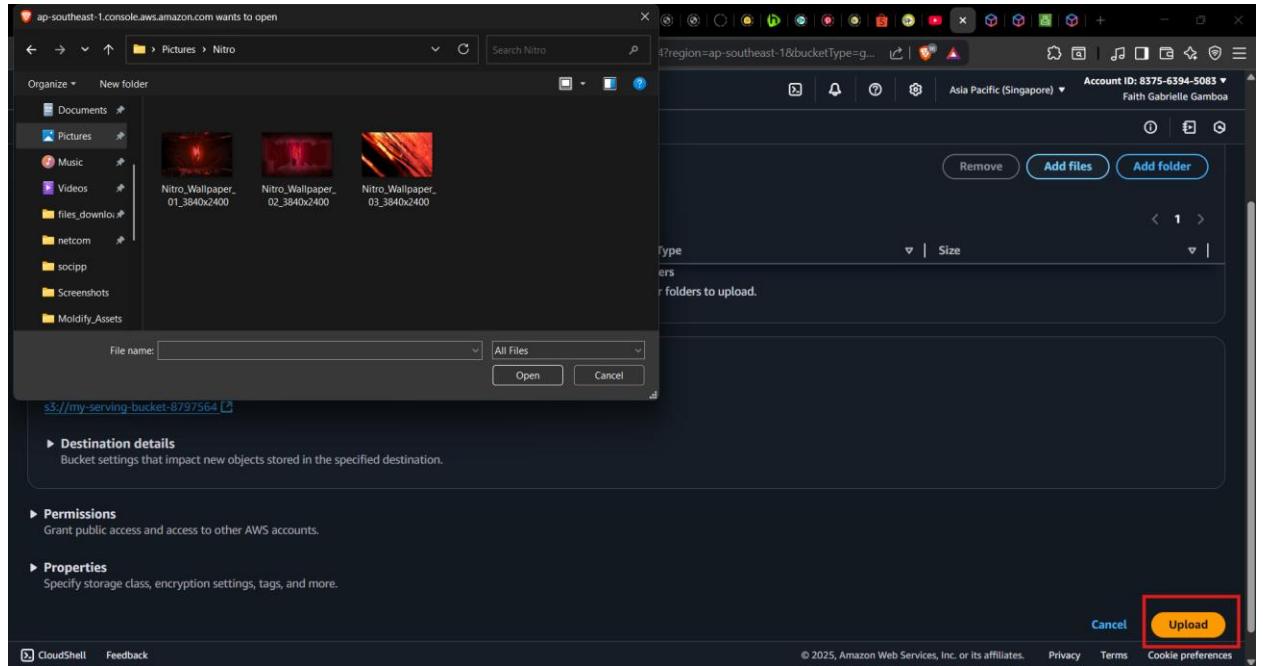
- + Add new statement**: A button to add a new statement.
- JSON Ln 10, Col 13**: A status message indicating the current position in the JSON code.
- Security: 0 Errors: 0 Warnings: 0 Suggestions: 0**: A status bar showing analysis results.
- Preview external access**: A link to preview external access.
- Cancel** and **Save changes**: Buttons at the bottom right.

- If you want to manually upload all files, navigate to the Objects tab and click the Upload button.

The screenshot shows the AWS S3 console with the 'Objects' tab selected. At the top right of the main content area, there is a prominent 'Upload' button. This button is highlighted with a yellow box. Below it, there is a message stating 'No objects' and 'You don't have any objects in this bucket.' A search bar and filter options are visible above the object list.

- Click Add files, and the file explorer will open to prompt you to upload your files. Click the Upload button from the bottom right to successfully upload your files.

The screenshot shows the 'Upload' page within the AWS S3 console. In the 'Files and folders' section, there is a 'Find by name' search bar and a table with columns for Name, Folder, Type, and Size. At the top right of this section, there are 'Remove', 'Add files', and 'Add folder' buttons. The 'Add files' button is highlighted with a red box. Below the table, a message says 'No files or folders' and 'You have not chosen any files or folders to upload.' Further down, there is a 'Destination' section with a 'Destination' field set to '\$3://my-serving-bucket-8797564' and a 'Destination details' link.



- If your website uploads files to the S3 bucket, you need to create an accessed key, in order for it to have permission to connect. Click on the Account Menu on the top right.

**Free plan status**

Credits remaining \$100.00 USD	Days remaining 182 days
-----------------------------------	----------------------------

Your free access to AWS services will end on Mar 11, 2026 or when you have depleted all credits. To ensure uninterrupted AWS access, see [upgrading your plan](#) for details.

**Account ID**  
8375-6394-5083

**Account**  
Organization  
Service Quotas  
Billing and Cost Management  
Security credentials

**Turn on multi-session support** **Sign out**

- Click security credentials. Scroll down to the Access Key section and click the Access Key button.

The screenshot shows the AWS S3 Bucket Details page for 'my-serving-bucket-8797564'. The 'Destination' section is expanded, showing the destination URL 's3://my-serving-bucket-8797564'. The 'Security credentials' link in the 'Billing and Cost Management' section is highlighted with a red box. The top right corner shows account information: Account ID: 8375-6394-5083, Credits remaining: \$100.00 USD, Days remaining: 182 days.

The screenshot shows the AWS IAM Security credentials page. The 'Access keys' section is expanded, showing the 'Create access key' button highlighted with a red box. The 'CloudFront key pairs' section is also visible. The left sidebar shows the navigation menu for IAM, including 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Access logs'.

- You'll see a warning that using root user access keys is not a best practice. If you still want to proceed, check the box to acknowledge the warning, then click Create Access Key. Once created, AWS will display your access keys. Make sure to store them securely because you won't be able to view the secret key again later.

The screenshot shows the AWS IAM 'Create access key' interface. At the top, there's a navigation bar with the AWS logo, search bar, and account information (Account ID: 8375-6394-5063, Global, Faith Gabrielle Gamboa). Below the navigation, the path is IAM > Security credentials > Create access key. On the left, a sidebar shows 'Step 1 Alternatives to root user access keys' (selected) and 'Step 2 Retrieve access key'. The main content area has a title 'Alternatives to root user access keys' with a 'Info' link. A warning message states: 'Root user access keys are not recommended. We don't recommend that you create root user access keys. Because you can't specify the root user in a permissions policy, you can't limit its permissions, which is a best practice.' It suggests using alternatives like IAM roles or users in IAM Identity Center. A note says: 'If your use case requires an access key, create an IAM user with an access key and apply least privilege permissions for that user.' There's a checkbox labeled 'I understand creating a root access key is not a best practice, but I still want to create one.' Below the checkbox are 'Cancel' and 'Create access key' buttons.

The screenshot shows the AWS IAM 'Create access key' interface after the access key has been created. The top navigation bar and account information are the same as the previous screenshot. The path is IAM > Security credentials > Create access key. The sidebar shows 'Step 1 Alternatives to root user access keys' (disabled) and 'Step 2 Retrieve access key' (selected). A green success message at the top says: 'Access key created. This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.' The main content area has a title 'Retrieve access key' with an 'Info' link. It shows the 'Access key' section with the access key ID 'AKIA4GAVTSB56Z3C3FLT' and the secret access key, which is partially obscured with asterisks and has a 'Show' link. Below this is the 'Access key best practices' section with a bulleted list: 'Never store your access key in plain text, in a code repository, or in code.', 'Disable or delete access key when no longer needed.', 'Enable least-privilege permissions.', and 'Rotate access keys regularly.' There's a note: 'For more details about managing access keys, see the [best practices for managing AWS access keys](#).' At the bottom are 'Download .csv file' and 'Done' buttons.

- **RDS - Creating a database instance**

- Another way to find the services you are looking for in AWS is to use the Services Menu.  
Click the button on the top left and click Database, then click on Aurora and RDS.

The screenshot shows the AWS Services menu on the left, with the 'Database' link highlighted by a red box. The main content area displays the 'Database' section of the AWS console. The 'Aurora and RDS' service is highlighted with a green box. Other services listed include Aurora DSQL, Amazon DocumentDB, DynamoDB, ElastiCache, Amazon Keyspaces, Amazon MemoryDB, and Neptune. To the right, there are sections for AWS Account (Account ID: 837563945083), Quick Links (My security credentials), and Tools.

- Click the Create Database button and fill in all the necessary details such as Database Creation Method, Configuration, Database Size, Database Instance Name, Username and Password, then Set up the EC2 Connection. Once done, click the Create Database Button.

The screenshot shows the Aurora and RDS Dashboard. On the left, there is a sidebar with options like Dashboard, Databases, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Zero-ETL integrations, Events, and Event subscriptions. The main content area has sections for 'Create a database' (with a red box around the 'Create a database' button) and 'Service health'. To the right, there are 'Recommended services' (No recommendations yet) and 'Recommended for you' sections (Time-Series Tables in PostgreSQL, Test Your DR Strategy in Minutes, Migrate SSRS to RDS for SQL Server).

Aurora and RDS > Create database

### Create database Info

Free plan has access to limited features and resources The free plan limits the features and resources that are available for RDS and Aurora databases. Upgrade your account plan to remove all limitations. [Learn more](#) [?] [Upgrade plan](#) [?]

#### Choose a database creation method

Standard create You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

#### Configuration

Engine type Info

Aurora (MySQL Compatible) 

PostgreSQL 

Aurora (PostgreSQL Compatible) 

MariaDB 

MySQL 

Oracle 

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Aurora and RDS > Create database

### Create database Info

PostgreSQL 

MariaDB 

Oracle 

Microsoft SQL Server 

#### DB instance size

Production db.r7xlarge  
4 vCPUs  
32 GiB RAM  
400 GiB  
2.203 USD/hour

Dev/Test db.r7g.large  
2 vCPUs  
16 GiB RAM  
200 GiB  
0.325 USD/hour

Free tier db.t4g.micro  
2 vCPUs  
1 GiB RAM  
20 GiB  
0.029 USD/hour

#### DB instance identifier

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

#### Master username Info

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Aurora and RDS > Create database

**DB instance identifier**  
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

**Master username** Info  
Type a login ID for the master user of your DB instance.  
  
1 to 16 alphanumeric characters. The first character must be a letter.

**Credentials management**  
You can use AWS Secrets Manager or manage your master user credentials.

**Managed in AWS Secrets Manager - most secure**  
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

**Self managed**  
Create your own password or have RDS create a password that you manage.

**Auto generate password**  
Amazon RDS can generate a password for you, or you can specify your own password.

ⓘ You can view your credentials after you create your database. Click the 'View credential details' in the database creation banner to view the password.

**▼ Set up EC2 connection - optional**  
You can also set up a connection to an EC2 instance after creating the database. Go to the database list page or the database details page, choose Actions, and then choose Set up to EC2 connection.

**Compute resource**  
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

**Don't connect to an EC2 compute resource**  
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

**Connect to an EC2 compute resource**  
Set up a connection to an EC2 compute resource for this database.

**EC2 instance** Info  
Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.  
  
MyWebServer

ⓘ Some VPC settings can't be changed when a compute resource is added  
Adding an EC2 compute resource automatically selects the VPC, DB subnet group, and public access settings for this database. To allow the EC2 instance to access the database, a VPC security group rds-ec2-X is added to the database and another called ec2-rds-X to the EC2 instance. You can remove the new security group for the database only by removing the compute resource.

Aurora and RDS > Create database

**▼ Set up EC2 connection - optional**  
You can also set up a connection to an EC2 instance after creating the database. Go to the database list page or the database details page, choose Actions, and then choose Set up to EC2 connection.

**Compute resource**  
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

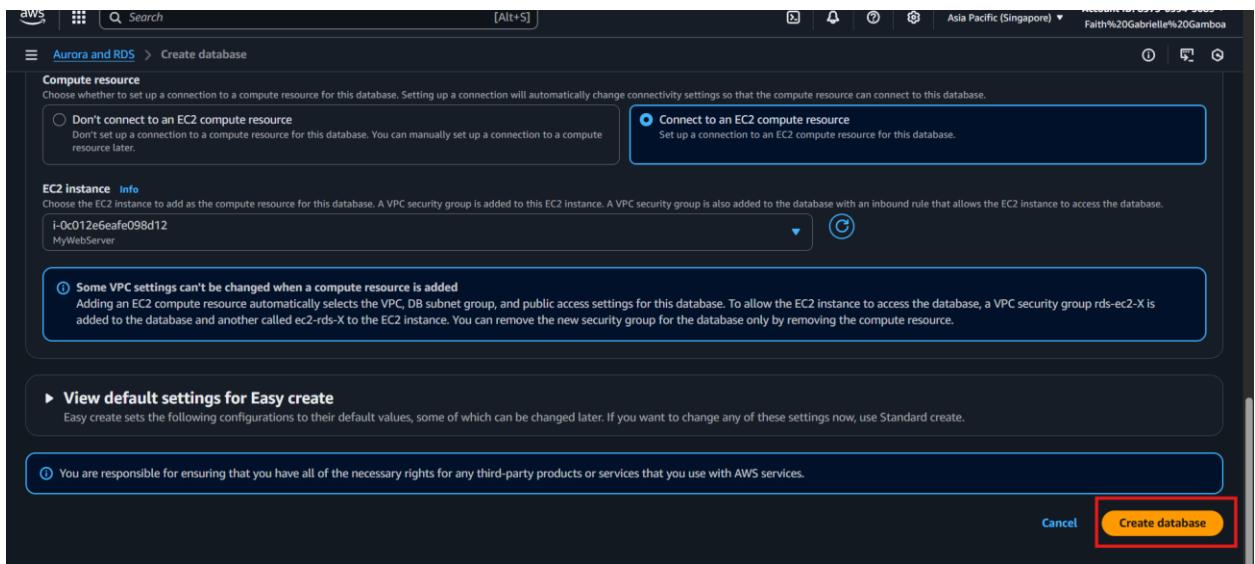
**Don't connect to an EC2 compute resource**  
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

**Connect to an EC2 compute resource**  
Set up a connection to an EC2 compute resource for this database.

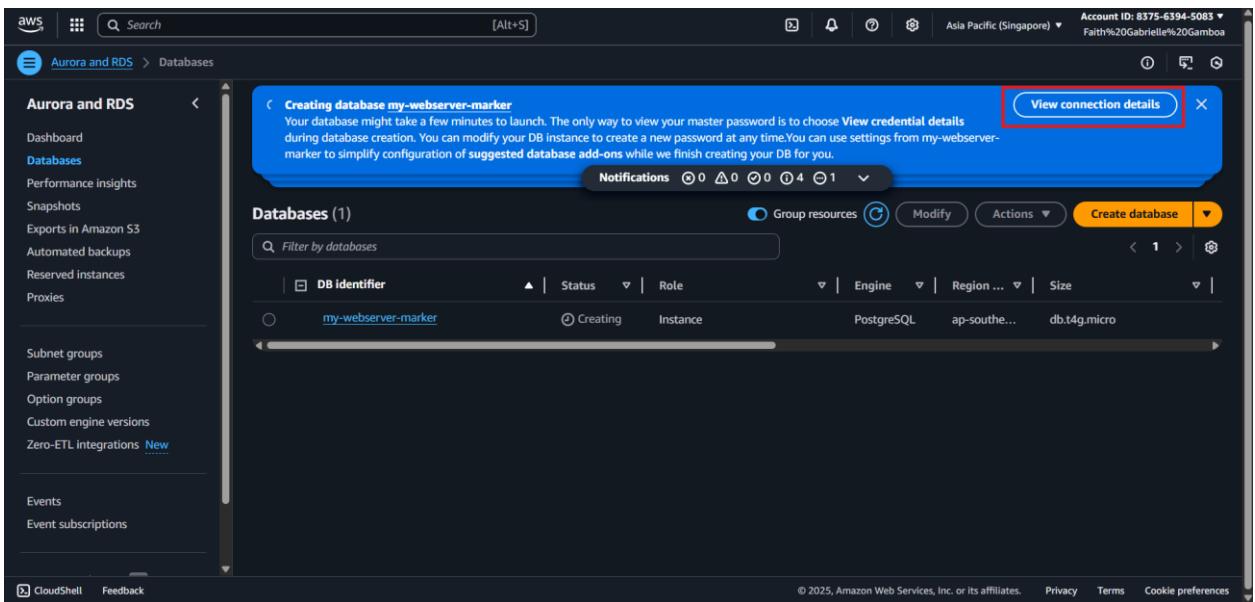
**EC2 instance** Info  
Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.  
  
MyWebServer

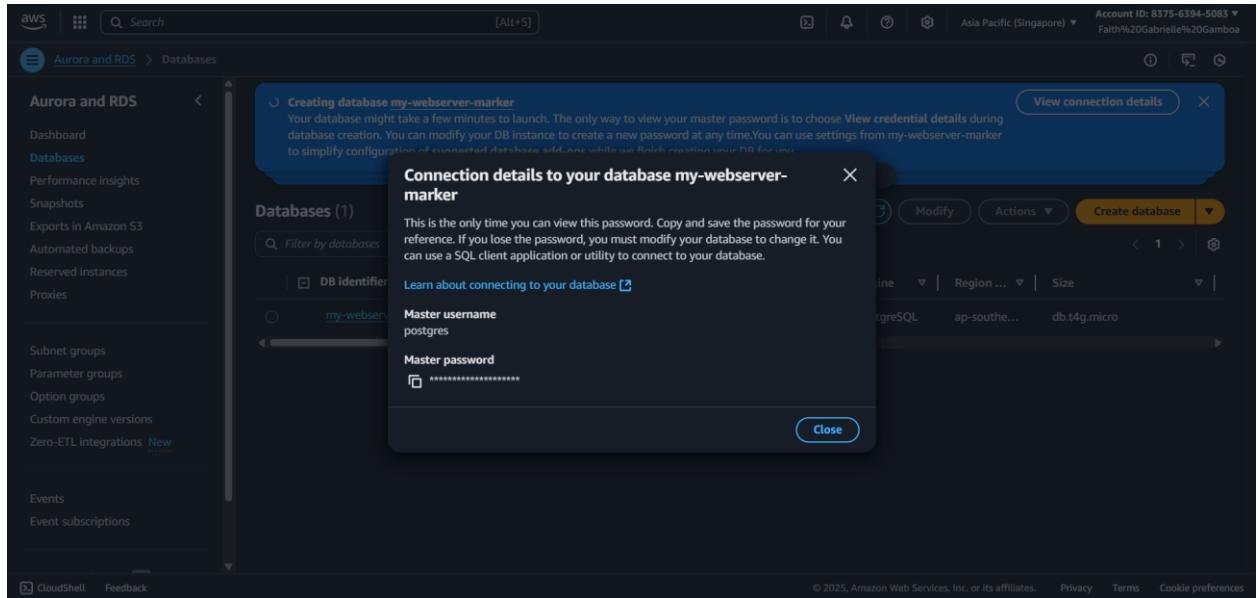
ⓘ Some VPC settings can't be changed when a compute resource is added  
Adding an EC2 compute resource automatically selects the VPC, DB subnet group, and public access settings for this database. To allow the EC2 instance to access the database, a VPC security group rds-ec2-X is added to the database and another called ec2-rds-X to the EC2 instance. You can remove the new security group for the database only by removing the compute resource.

**► View default settings for Easy create**  
Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use Standard create.



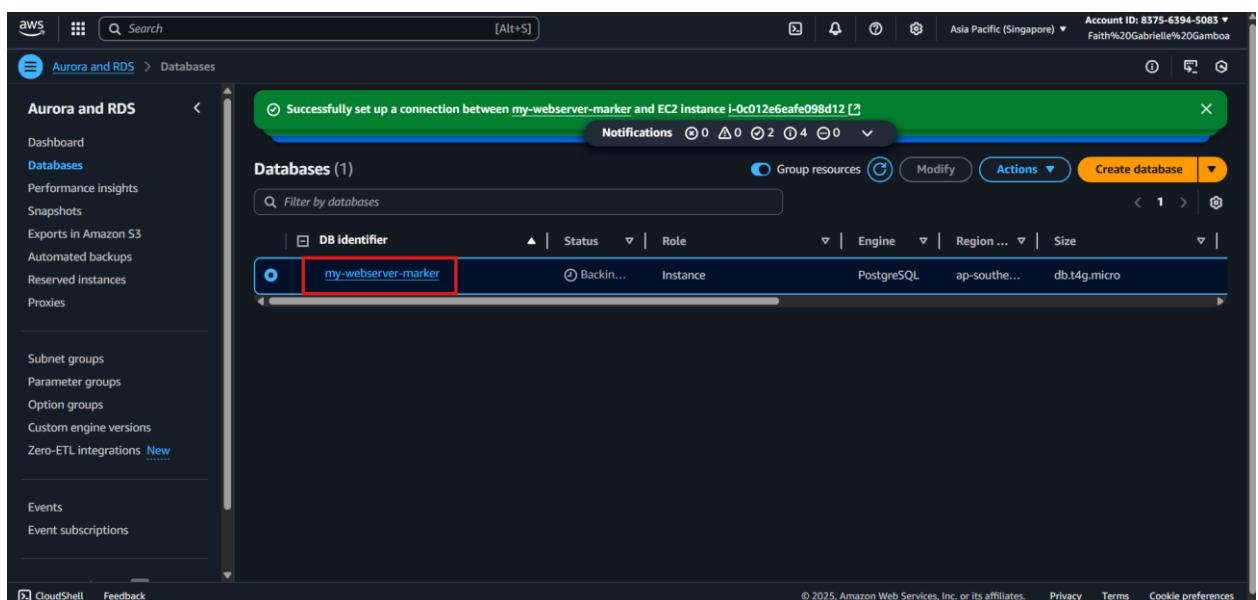
- To view your credentials, click the View Connection Details button which will show the username, and password generated by AWS for you. Make sure to save it in a secure location as it will be used for configuration later.





- **Connecting to an EC2 instance and running commands**

- Click the database name, then scroll down to find the EC2 instance name to go directly there. Once there, click on the instance again, and click the Connect button.



Aurora and RDS > Databases > my-webserver-marker

Network type: IPv4

Connected compute resources (1) Info

Connections to compute resources that were created automatically by RDS are shown here. Connections to compute resources that were created manually aren't shown.

Filter by compute resources

Resource identifier	Resource type	Availability Zone	VPC security group	Compute resource security group	Connected proxy
i-0c012e6eafe098d12	EC2 instance	ap-southeast-1b	rds-ec2-1	ec2-rds-1	

Proxies (0) Create proxy

No proxies

You don't have any proxies.

Create proxy

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Account ID: 8375-6394-5083 ▾  
Faith%20Gabrielle%20Gamboa

EC2 > Instances

Instances (1/1) Info

Last updated 1 minute ago

Connect Instance state Actions Launch instances

Find Instance by attribute or tag (case-sensitive)

Instance ID = i-0c012e6eafe098d12 Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
MyWebServer	i-0c012e6eafe098d12	Running	t3.micro	3/3 checks passed	View alarms +	ap-southeast-1b	ec2-54-1

i-0c012e6eafe098d12 (MyWebServer)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary Info

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Account ID: 8375-6394-5083 ▾  
Faith%20Gabrielle%20Gamboa

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, and Elastic Block Store. The main area displays the 'Instance summary for i-0c012e6afe098d12 (MyWebServer)'. It includes fields for Instance ID (i-0c012e6afe098d12), Public IPv4 address (54.151.249.140), Instance state (Running), Hostname type (IP name: ip-172-31-21-166.ap-southeast-1.compute.internal), Private IP DNS name (ip-172-31-21-166.ap-southeast-1.compute.internal), Instance type (t3.micro), Auto-assigned IP address (54.151.249.140 [Public IP]), VPC ID (vpc-0fc0901fe7a3b955b), Subnet ID (subnet-07c055291641f3336), Instance ARN (arn:aws:ec2:ap-southeast-1:837563945085:instance/i-0c012e6afe098d12), IAM Role (None), IMDSv2 (Required), and AWS Compute Optimizer finding (Opt-in to AWS Compute Optimizer for recommendations). At the bottom right, there are links for Elastic IP addresses, Auto Scaling Group name, and Managed.

- There are multiple ways to connect an instance, the easiest way to connect is to pick the EC2 Instance Connect. Once picked, click the Connect button.

The screenshot shows the 'Connect to instance' dialog. It has tabs for EC2 Instance Connect, Session Manager, SSH client, and EC2 serial console. The EC2 Instance Connect tab is selected and highlighted with a green box. It shows the instance ID (i-0c012e6afe098d12) and connection type. The 'Public IPv4 address' (54.151.249.140) is selected and highlighted with a blue box. Below it, there's a 'Username' field with 'ec2-user' entered. A note at the bottom says 'Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' At the bottom right, there are 'Cancel' and 'Connect' buttons, with the 'Connect' button highlighted with a yellow box.

- Next, run the commands in the console after you click the Connect button.
  - Install Git using the dnf package manager:
    - sudo dnf install git -y
  - Clone the website source code from the GitHub repository:
    - git clone <repository-url>
  - Navigate to the project folder:
    - cd <project-folder-name>
  - Install Node.js and npm using dnf:
    - sudo dnf install nodejs -y

- Install project dependencies with npm:
  - npm install
- Start the Node.js web application with npm start.
  - npm start
- To keep the web server running after closing SSH session:
  - Start the process as a background job by appending &:
    - npm start &
  - Then, detach it from your terminal using:
    - disown

```

aws | [Alt+S] | Search | Account ID: 8375-6394-5083 | Asia Pacific (Singapore) | Faith%20Gabrielle%20Gamboa
-----
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-21-166 ~]$ 

i-0c012e6afe098d12 (MyWebServer)
Public IPs: 54.151.249.140 Private IPs: 172.31.21.166
CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```

- **Tips for cost savings on AWS**
  - Prices can vary depending on the region you choose. Regions in the US and Europe are usually the cheapest. Just try to avoid US West (N. California) since it's often more expensive.
  - If you're going to use something like EC2 regularly, you can prepay to get a discount. If you're flexible with your usage, you can also use Spot Instances, which let you bid on extra AWS capacity at lower prices.
  - It's a good idea to set a spending limit or billing alert in your AWS account. This helps you stay within the Free Tier and avoid unexpected charges.
- **Continuing your AWS journey with AI, Machine Learning, and AWS Certifications**
  - AWS offers a wide range of services like AI, machine learning, fraud detection, and analytics. Plus, getting AWS certifications is a great way to boost your career.