

Creating AWS Instance

Login to your AWS Console Account

Search for EC2 and click on EC2 you will be redirected to AWS EC2 Dashboard

Resources

You are using the following Amazon EC2 resources in the United States (N. Virginia) Region:

Instances (running)	1	Auto Scaling Groups	0
Capacity Reservations	0	Dedicated Hosts	0
Elastic IPs	0	Instances	4
Key pairs	22	Load balancers	0
Placement groups	1	Security groups	195
Snapshots	0	Volumes	4

EC2 Free Tier

Offers for all AWS Regions.

4 EC2 free tier offers in use

End of month forecast
⚠️ 1 offers forecasted to exceed free tier limit.

Exceeds free tier
⚠️ 1 offers exceeded and is now pay-as-you-go pricing.

[View Global EC2 resources](#)

Offer usage (monthly)

Linux EC2 Instances
623.305832 hours remaining 17%

Make sure your Zone must be us-east-1 (N. Virginia).

click on Launch Instance.

Launch instance

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

[Launch instance](#)

[Migrate a server](#)

Note: Your instances will launch in the United States (N. Virginia) Region

Service health

[AWS Health Dashboard](#)

Region
United States (N. Virginia)

Status
✅ This service is operating normally.

Zones

Launch an instance [Info](#)

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

Name and tags [Info](#)


Name

[Add additional tags](#)

Select Image (AMI) Amazon Linux

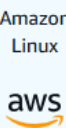






▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

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

Recents

Quick Start

 Amazon Linux	 macOS	 Ubuntu	 Windows	 Red Hat	 SUSE Linux	 Debian	 Browse more AMIs Including AMIs from AWS, Marketplace and the Community
---	--	---	--	--	--	---	---

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-053a45fff0a704a47 (64-bit (x86), uefi-preferred) / ami-0c518311db5640eff (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Instance Type: t2 micro

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

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

☒ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

Create key pair:

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

sonamvmke

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

Cancel

Create key pair

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

sonamvmkey

↻ [Create new key pair](#)

Security Groups to manage the firewall

▼ Network settings [Info](#)

Edit

Network | [Info](#)

vpc-0d28400f549296804

Subnet | [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP | [Info](#)

Enable

Additional charges apply when outside of free tier allowance

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-154' with the following rules:

☒ Allow SSH traffic from

click on Edit.

Give name and description of your security Group:

Enable

▼

Additional charges apply when outside of free tier allowance

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

Security group name - *required*

sonam-security

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!\$*

Description - *required* | [Info](#)

sonam-security created 2025-02-19T05:28:15.749Z

By default security added to use openssh

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type | [Info](#)

ssh

Protocol | [Info](#)

TCP

Port range | [Info](#)

22

Source type | [Info](#)

Anywhere

Source | [Info](#)

Q Add CIDR, prefix list or security gr

Description - *optional* | [Info](#)

e.g. SSH for admin desktop

Open one more port http

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your in group rules to allow access from known IP addresses only.

Add security group rule

click on add security group rule

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0, My HTTP)

Remove

Type | Info

HTTP

Protocol | Info

TCP

Port range | Info

80

Source type | Info

Anywhere

Source | Info

Q Add CIDR, prefix list or security gr

0.0.0.0/0 X

Description - optional | Info

My HTTP

▼ Configure storage | Info

Advanced

1x

8

GiB

gp3

Root volume 3000 IOPS (Not encrypted)

i Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

X

Add new volume

By default it is taking 8 GB for your storage.

▼ Summary

Number of instances | [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-053a45fff0a704a47

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

[Cancel](#)

[Launch instance](#)

[Preview code](#)

Verify the Summary and Launch Instance.

C Launching Instance
Creating security groups

27%

► Details

Please wait while we launch your instance.
Do not close your browser while this is loading.

Instance summary for i-08071460279647d74 (sonamvm) [Info](#)



[Connect](#)

[Instance state ▼](#)

[Actions ▼](#)

Updated less than a minute ago

Instance ID

[i-08071460279647d74](#)

IPv6 address

—

Public IPv4 address

[13.232.41.45](#) | [open address](#)

Instance state

✓ Running

Private IPv4 addresses

[172.31.2.238](#)

Public IPv4 DNS

[ec2-13-232-41-45.ap-south-1.compute.amazonaws.com](#)
| [open address](#)

Click on instance Link and click on connect,

Connect to instance [Info](#)

Connect to your instance i-08071460279647d74 (sonamm) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID
i-08071460279647d74 (sonamm)

Connection Type
☒ Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 or IPv6 address.
☐ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

☒ Public IPv4 address
13.232.41.45
☐ IPv6 address
—

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ubuntu.
Q ubuntu X

Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

Connect

Click on Connect and you can access Your instance.

```
* Support: https://ubuntu.com/pro

System information as of Wed Feb 19 09:34:51 UTC 2025

System load: 0.42          Processes: 108
Usage of /: 24.9% of 6.71GB Users logged in: 0
Memory usage: 21%         IPv4 address for enX0: 172.31.2.238
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Feb 19 09:34:52 2025 from 13.233.177.5
ubuntu@ip-172-31-2-238:~$
```

you can run your commands here to work with your instance.

Bucket Policy Generation Steps:

Create Bucket using Some unique name.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-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.

Bucket name [Info](#)

sonamsoni123

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

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

- ☒ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, and public access block. To block public access, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access to ensure that your applications will work correctly without public access. If you require some level of public access, turn off Block all public access and configure the settings below to suit your specific storage use cases. [Learn more](#)

☒ 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 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

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. With versioning, you can easily recover from both unintended user actions and malware.

Bucket Versioning

☐ Disable

☒ Enable

No tags required to add

Default encryption [Info](#)

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

Encryption type [Info](#)

☒ 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)

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

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys are available for SSE-KMS.

☐ Disable

☒ Enable

Click on Create Bucket

✓ **Successfully created bucket "sonamsoni123"**
To upload files and folders, or to configure additional bucket settings, choose **View details**.

sonamsoni123 [Info](#)

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (0)



Copy S3 URI



Copy URL



Download



Open

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects and their permissions. [Learn more](#)



Find objects by prefix



Show versions



Name



Type



Last modified

No objects

You don't have any objects in this bucket.

See the details of your bucket here.

you can add objects inside the bucket.

Click on upload --> select files --> upload

Files and folders

Configuration

Files and folders (1 total, 218.6 KB)




Find by name

Name	Folder	Type	Size	Status
laptop.jpg	-	image/jpeg	218.6 KB	✓ Succeeded

Individual files become a bucket Object.


See the object details by clicking on It

laptop.jpg Info

 Copy S3 URI

 Download

 Open

 Object actions

Properties

Permissions

Versions

Object overview

Owner

7c32e1d4de217232bf796250d603d9811438ad0462a9f6d1ab4d619f0c6dde62

AWS Region

Asia Pacific (Mumbai) ap-south-1

Last modified

February 19, 2025, 17:35:53 (UTC+05:30)


Size

218.6 KB


S3 URI

 s3://sonamsoni123/laptop.jpg


Amazon Resource Name (ARN)

 arn:aws:s3:::sonamsoni123/laptop.jpg

Entity tag (Etag)

 f3c0aa676dfb02da3882100152984ed7

Object URL

 https://sonamsoni123.s3.ap-south-1.amazonaws.com/laptop.jpg

This Object URL is not accessible directly.

To give the access permission. Go to your Bucket permission.

[sonamsoni123](#) > [Edit Block public access \(bucket settings\)](#)

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. If buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. All access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **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

☐ **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. 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 permissions 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.

Save the changes.

Now to give access generate Policy by clicking on Policy Generate.

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web S](#). For more information about creating policies, see [key concepts in Using AWS Identity and Access Managem](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy

S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use.

Effect

☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service

Amazon S3

Use multiple statements to add permissions for more than one service.

Use multiple statements to add permissions for more than one servi

Actions

1 Action(s) Selected

☐ GetMultiRegionAccessPointPolicyStatus

☐ GetMultiRegionAccessPointRoutes

☒ GetObject

☐ GetObjectAcl

☐ All Ac

Resource Name (ARN)

{BucketNam

Click on Add Statement:

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions	
<ul style="list-style-type: none">*	Allow	<ul style="list-style-type: none">s3:GetObject	arn:aws:s3:::sonamsoni123/*	None	


Generate Policy:

Changes made below will not be reflected in the policy generator tool.

```
{
  "Id": "Policy1739967011716",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1739966293071",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::sonamsoni123/*",
      "Principal": "*"
    }
  ]
}
```

Copy and paste in your Policy:

Bucket ARN

 arn:aws:s3:::sonamsoni123

Policy

```
1 {
2   "Id": "Policy1739967011716",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stmt1739966293071",
7       "Action": [
8         "s3:GetObject"
9       ],
10      "Effect": "Allow",
11      "Resource": "arn:aws:s3:::sonamsoni123/*",
12      "Principal": "*"
13    }
14  ]
15 }
```

Save Changes.

✔ Successfully edited bucket policy.

Then you can Try to access Objects of your buckets.