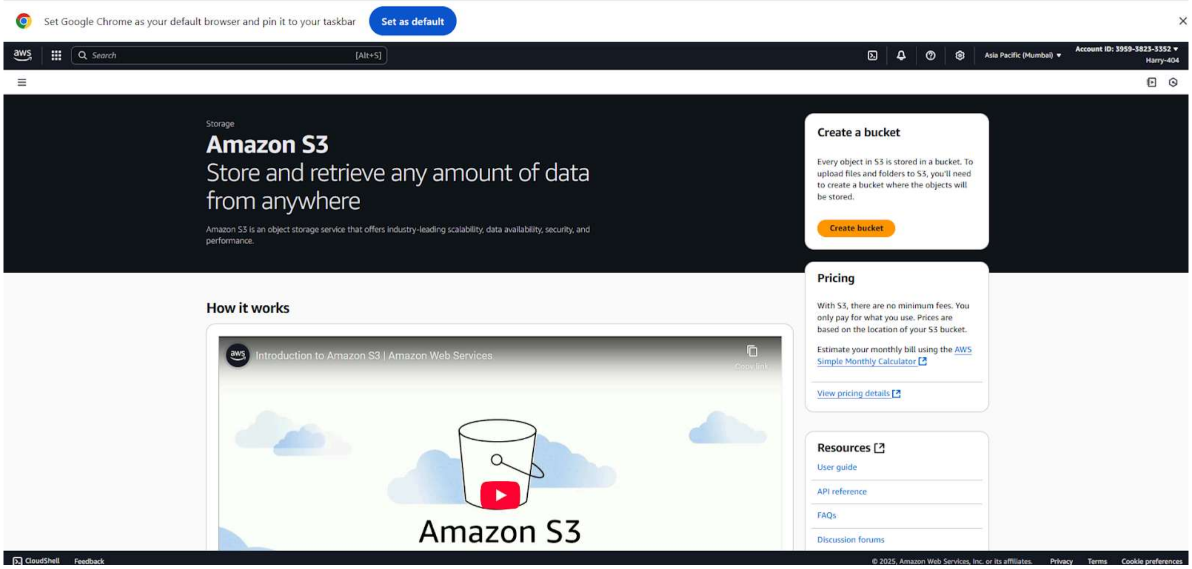
Syncing Content from S3 to EC2

1. Create an S3 Bucket

- Go to AWS S3 console.
- Click “Create bucket”.
- Name your bucket (e.g., `s3connectingec2`).
- Select region, keep defaults unless you have a reason to change.
- Leave “Block all public access” on *unless* you have a public website use case.
- Click Create bucket.


Set Google Chrome as your default browser and pin it to your taskbar
Set as default
aws
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 3959-3823-3352
Harry-404
Introduction to Amazon S3 | Amazon Web Services
Copy link
Amazon S3
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

How it works

Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

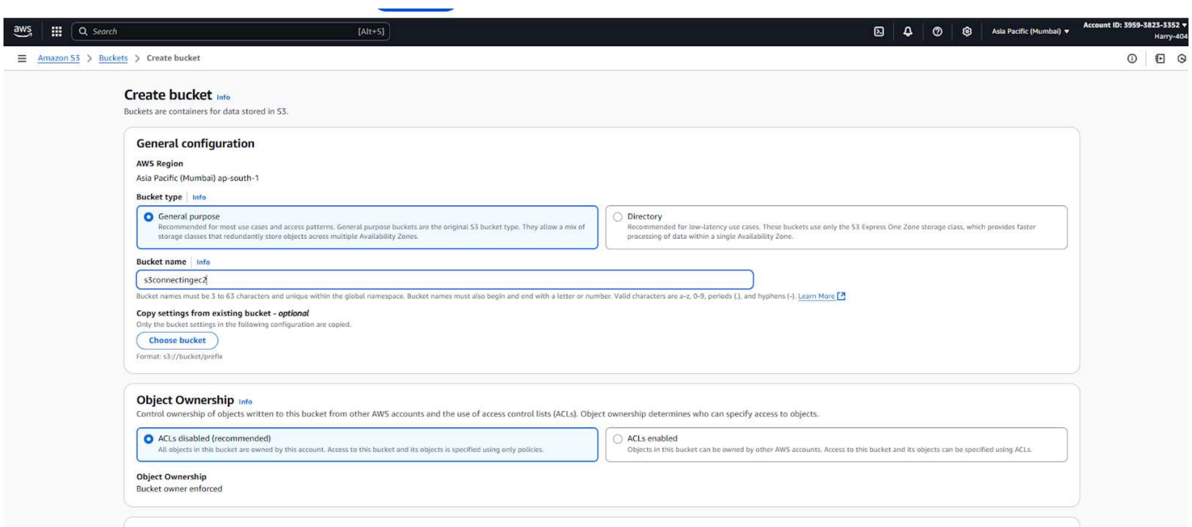
Resources

User guide

API reference

FAQs

Discussion forums


aws
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 3959-3823-3352
Harry-404
Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

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.

○ Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info

s3connectingec2

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

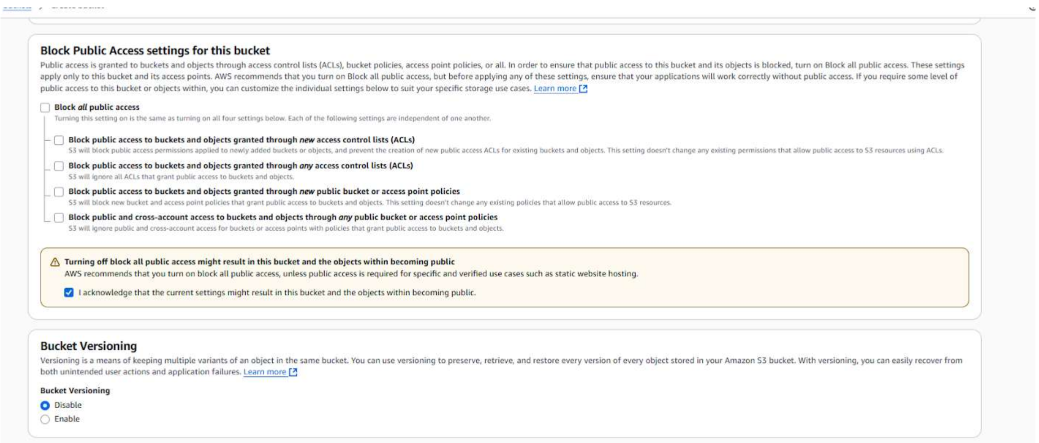
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● 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.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

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, or all. In order to ensure that public access to this bucket and its objects is blocked, 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, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket 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 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.

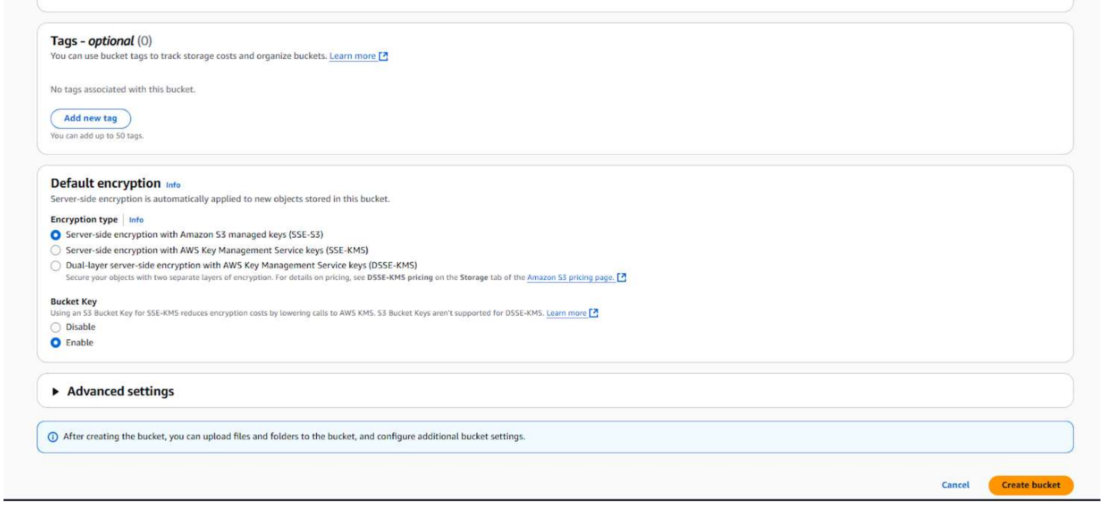
⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ 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.

You can add up to 50 tags.

Default encryption Info

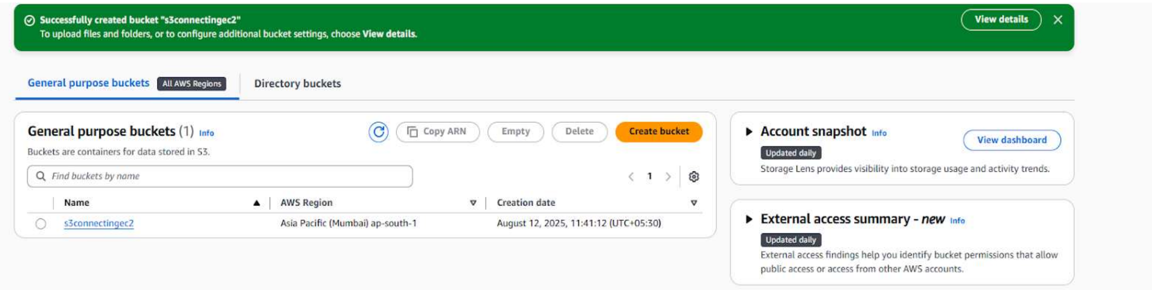
Server-side encryption is automatically applied to new objects stored in this bucket.

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** on the **Storage** tab of the Amazon S3 pricing page.

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
○ Disable
● Enable

▶ **Advanced settings**

ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.



Successfully created bucket "s3connectingec2"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets (1) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
s3connectingec2	Asia Pacific (Mumbai) ap-south-1	August 12, 2025, 11:41:12 (UTC+05:30)

▶ **Account snapshot** Info

Storage Lens provides visibility into storage usage and activity trends.

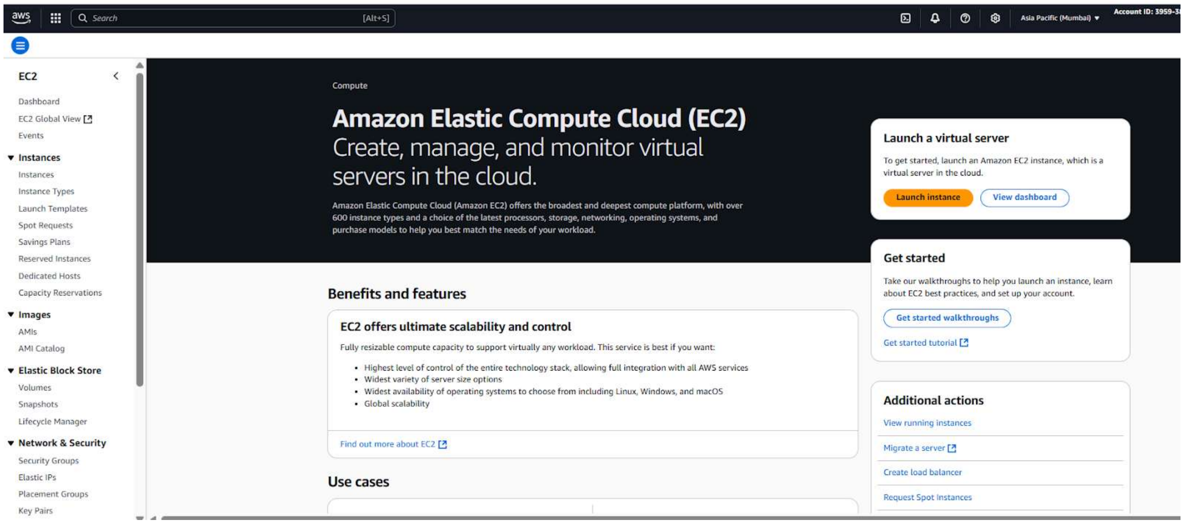
▶ **External access summary - *new*** Info

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

2. Launch & Connect to EC2 Instance

- Go to AWS EC2 console.
- Launch a new instance (choose Ubuntu 24.04 LTS for most setups).
- Choose t3.micro (if cost matters or free tier).
- Set up a key pair for SSH access.
- In “Configure Security Group”, allow SSH (port 22), HTTP (80) and HTTPS (443) from your IP or as needed.
- Launch and wait for instance state to be “running”.

- SSH into EC2:



Compute

Amazon Elastic Compute Cloud (EC2)
Create, manage, and monitor virtual servers in the cloud.

Amazon Elastic Compute Cloud (Amazon EC2) offers the broadest and deepest compute platform, with over 600 instance types and a choice of the latest processors, storage, networking, operating systems, and purchase models to help you best match the needs of your workload.

Launch a virtual server

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

Get started

Take our walkthroughs to help you launch an instance, learn about EC2 best practices, and set up your account.

Additional actions

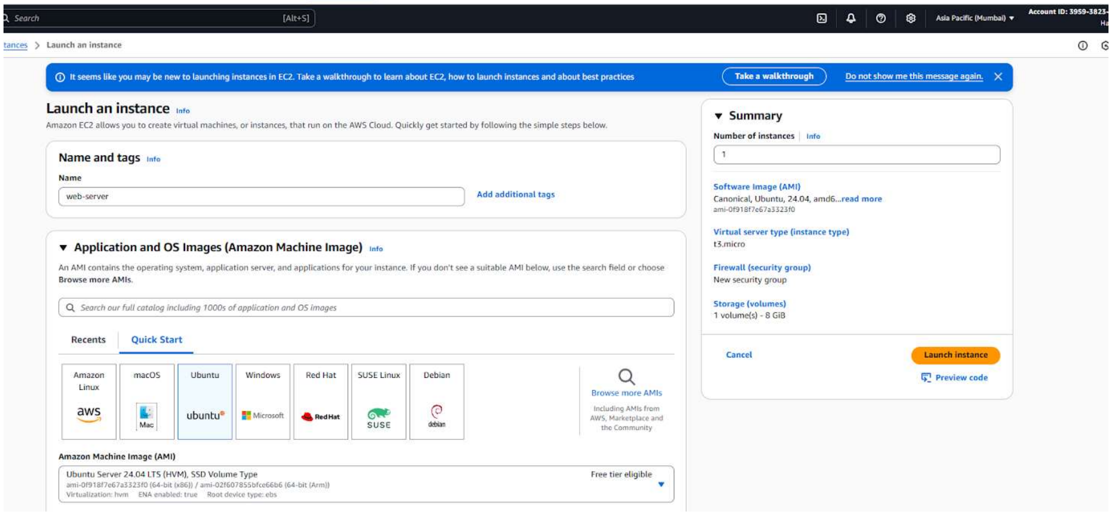
Benefits and features

EC2 offers ultimate scalability and control

Fully resizable compute capacity to support virtually any workload. This service is best if you want:

- Highest level of control of the entire technology stack, allowing full integration with all AWS services
- Widest variety of server size options
- Widest availability of operating systems to choose from including Linux, Windows, and macOS
- Global scalability

Use cases



It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

Launch an instance

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

Name: web-server

▾ 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

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-0f918f7e67a3323f0 (64-bit (x86)) / ami-02f607855bfce66b6 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

▾ Summary

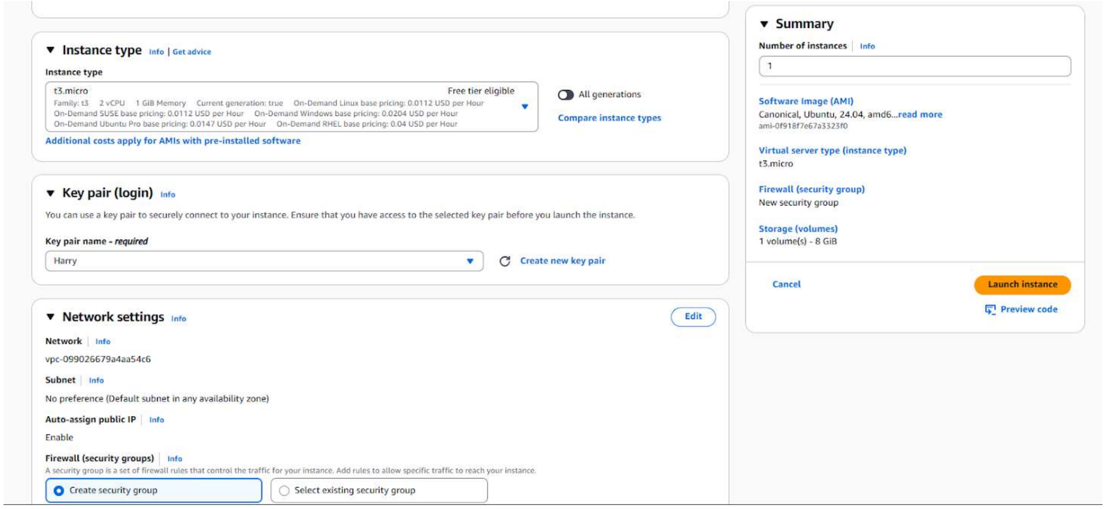
Number of instances: 1

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-0f918f7e67a3323f0

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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



▾ Instance type

Instance type

t3.micro — Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0112 USD per Hour
On-Demand SUSE base pricing: 0.0112 USD per Hour On-Demand Windows base pricing: 0.0204 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0147 USD per Hour On-Demand RHEL base pricing: 0.04 USD per Hour

Additional costs apply for AMIs with pre-installed software

▾ 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*: Harry

▾ Network settings

Network
vpc-099026679a4aa54c6

Subnet
No preference (Default subnet in any availability zone)

Auto-assign public IP
Enable

Firewall (security groups)
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

▾ Summary

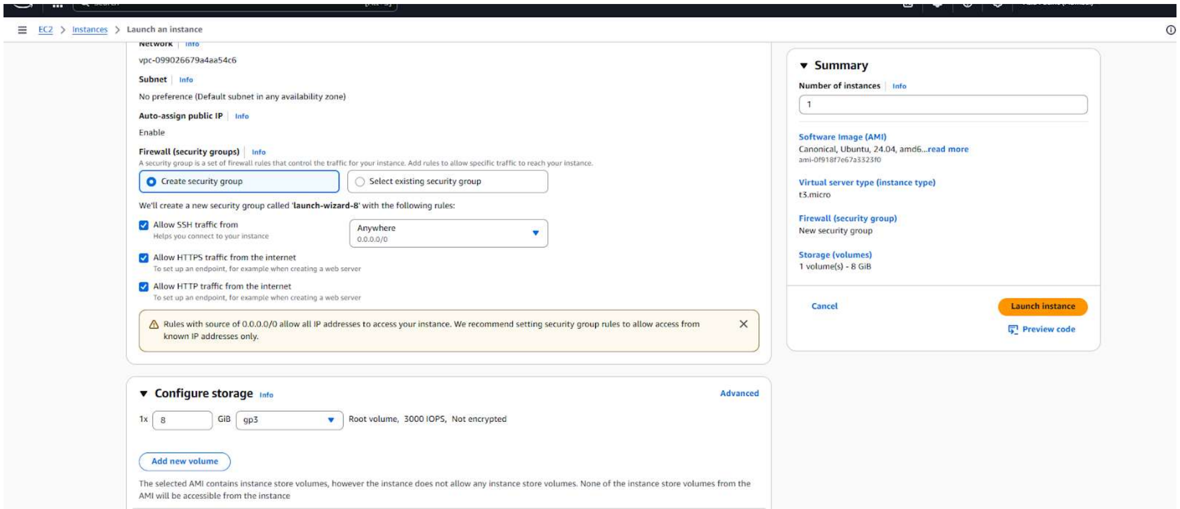
Number of instances: 1

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-0f918f7e67a3323f0

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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



Network | Info
vpc-099026679a4aa54c6

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-8**' with the following rules:

☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

☑ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☑ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

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

Configure storage Info — Advanced

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

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the instance store volumes from the AMI will be accessible from the instance

Summary

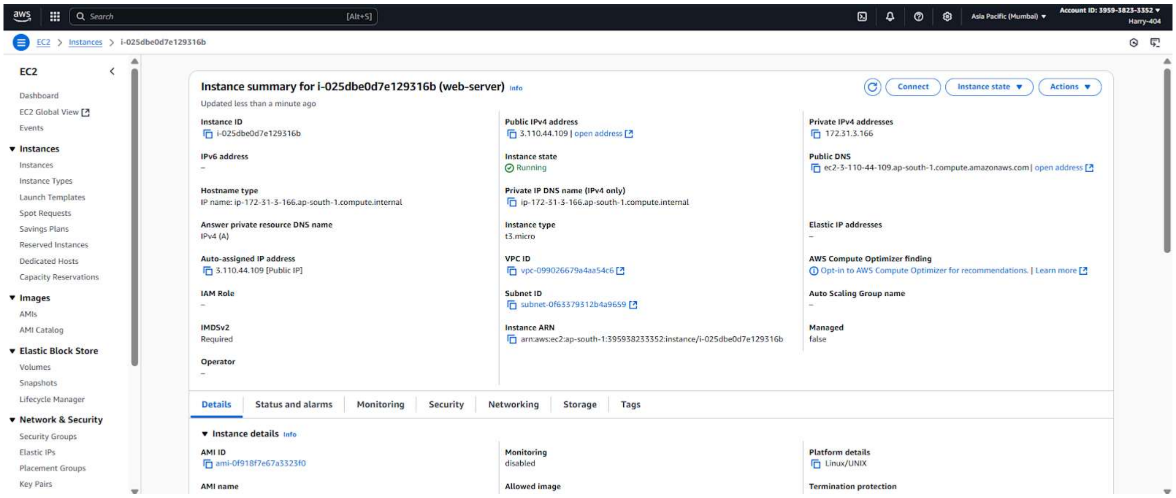
Number of instances | Info
1

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-0f918f7e67a3323f0

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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



Instance summary for i-025dbe0d7e129316b (web-server) Info
Updated less than a minute ago

Instance ID
i-025dbe0d7e129316b

IPv6 address
–

Hostname type
IP name: ip-172-31-3-166.ap-south-1.compute.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
3.110.44.109 [Public IP]

IAM Role
–

IMDSv2
Required

Operator
–

Public IPv4 address
3.110.44.109 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-3-166.ap-south-1.compute.internal

Instance type
t3.micro

VPC ID
vpc-099026679a4aa54c6

Subnet ID
subnet-0f63379312b4a9659

Instance ARN
arn:aws:ec2:ap-south-1:395938233352:instance/i-025dbe0d7e129316b

Private IPv4 addresses
172.31.3.166

Public DNS
ec2-3-110-44-109.ap-south-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

Instance details Info

AMI ID
ami-0f918f7e67a3323f0

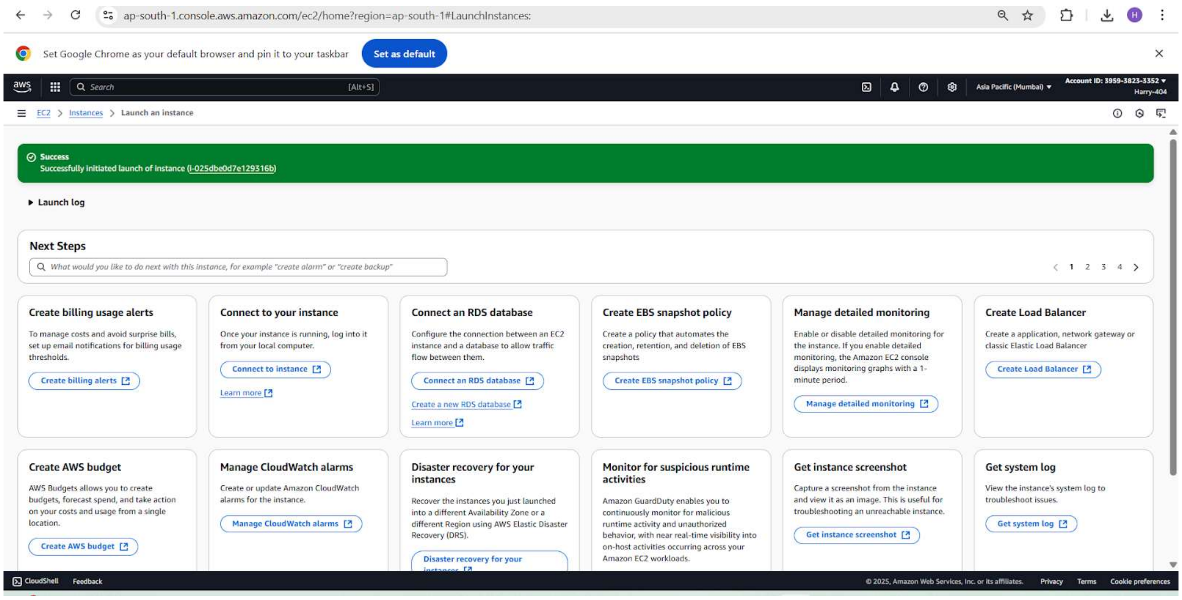
Monitoring
disabled

Platform details
Linux/UNIX

AMI name

Allowed image

Termination protection


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Set Google Chrome as your default browser and pin it to your taskbar
Set as default
aws
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 3959-3823-3352
Harry-404
EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-025dbe0d7e129316b)

▸ Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4

Create billing usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing usage thresholds.

Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots

Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer

Create AWS budget
AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

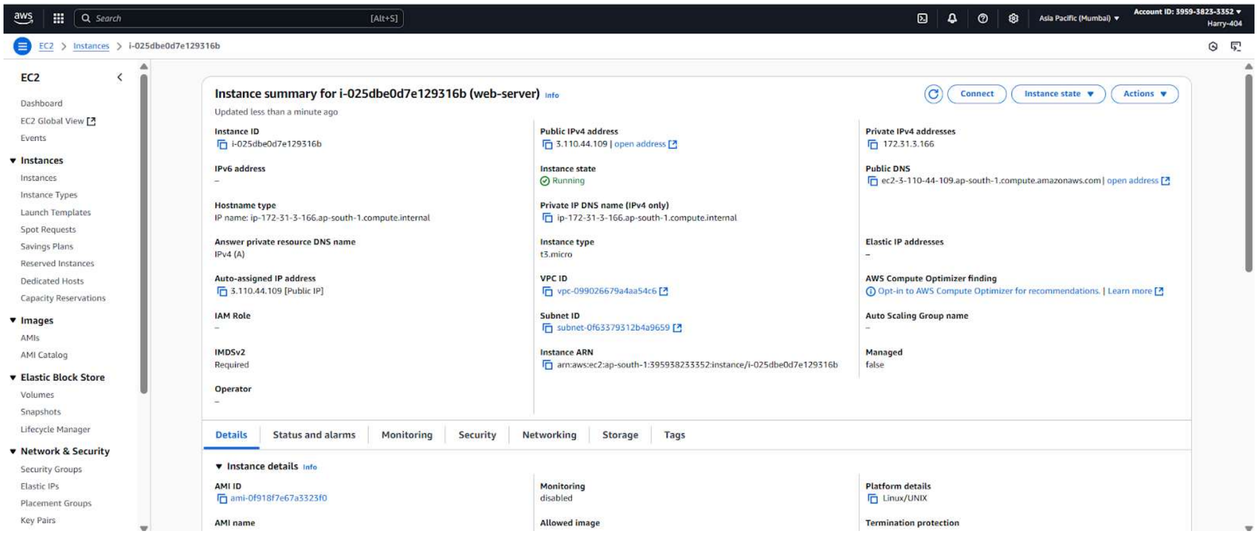
Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.

Disaster recovery for your instances
Recover the instances you just launched into a different Availability Zone or a different Region using AWS Elastic Disaster Recovery (DRS).

Monitor for suspicious runtime activities
Amazon GuardDuty enables you to continuously monitor for malicious runtime activity and unauthorized behavior, with near real-time visibility into on-host activities occurring across your Amazon EC2 workloads.

Get instance screenshot
Capture a screenshot from the instance and view it as an image. This is useful for troubleshooting an unreachable instance.

Get system log
View the instance's system log to troubleshoot issues.



Instance summary for i-025dbe0d7e129316b (web-server) Info

Updated less than a minute ago

Instance ID
i-025dbe0d7e129316b

IPv6 address
–

Hostname type
IP name: ip-172-31-3-166.ap-south-1.compute.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
3.110.44.109 [Public IP]

IAM Role
–

IMDSv2
Required

Operator
–

Public IPv4 address
3.110.44.109 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-3-166.ap-south-1.compute.internal

Instance type
t3.micro

VPC ID
vpc-099026679a4aa54c6

Subnet ID
subnet-0f63379312b4a9659

Instance ARN
arn:aws:ec2:ap-south-1:395938233352:instance/i-025dbe0d7e129316b

Private IPv4 addresses
172.31.3.166

Public DNS
ec2-3-110-44-109.ap-south-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

Instance details Info

AMI ID
ami-0f918f7e67a3323f0

AMI name

Monitoring
disabled

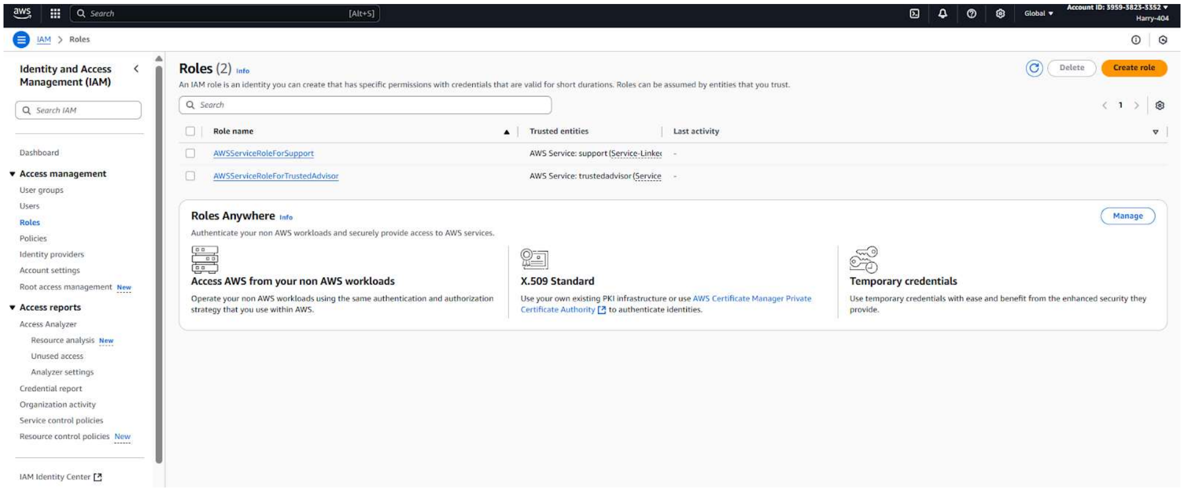
Allowed image

Platform details
Linux/UNIX

Termination protection

3. Configure IAM Role for S3 Access (Best Practice)

- Go to AWS IAM > Roles > Create role.
- Trusted entity: AWS service, Use case: EC2.
- Attach policy: `AmazonS3FullAccess` (or restrict to only this bucket for production).
- Name: e.g., `S3EC2Role`.
- Attach this role to your EC2 instance (Actions > Security > Modify IAM role).



Roles (2) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-

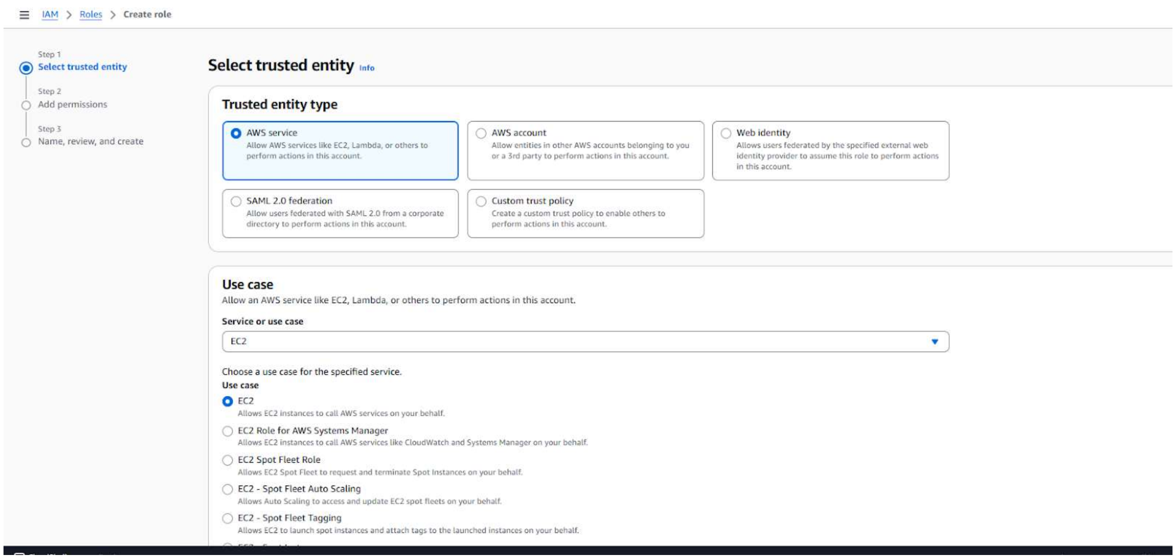
Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.



Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2 ▼

Choose a use case for the specified service.

Use case

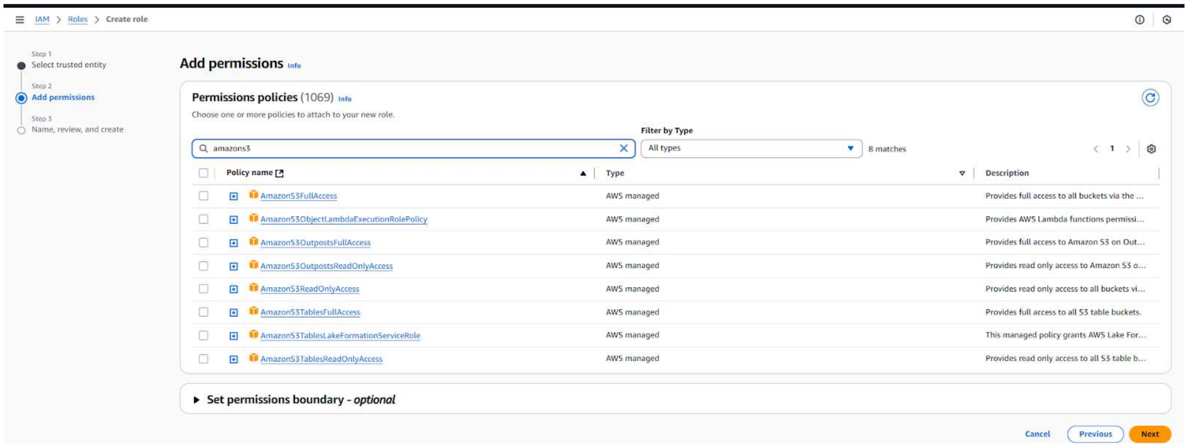
● EC2
Allows EC2 instances to call AWS services on your behalf.

○ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

○ EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

○ EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

○ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.



Add permissions Info

Permissions policies (1069) Info

Choose one or more policies to attach to your new role.

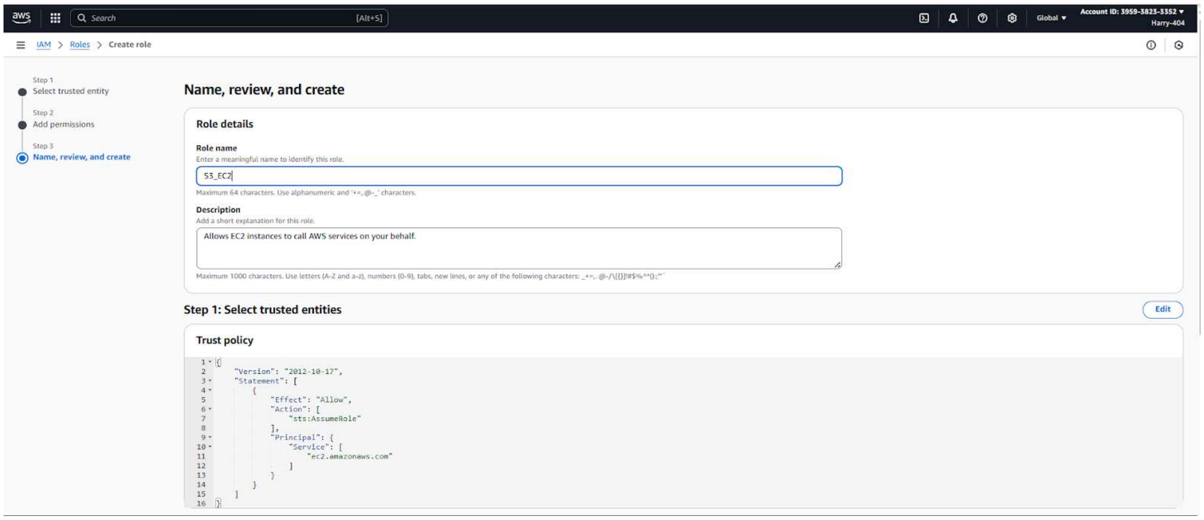
Search: amazons3

Filter by Type: All types ▼

8 matches

□	Policy name	Type	Description
□	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the ...
□	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda functions permissi...
□	AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on Out...
□	AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S3 o...
□	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all buckets vi...
□	AmazonS3TablesFullAccess	AWS managed	Provides full access to all S3 table buckets.
□	AmazonS3TablesLakeFormationServiceRole	AWS managed	This managed policy grants AWS Lake For...
□	AmazonS3TablesReadOnlyAccess	AWS managed	Provides read only access to all S3 table b...

▶ Set permissions boundary - *optional*



Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

S3_EC2

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

Add a short explanation for this role.

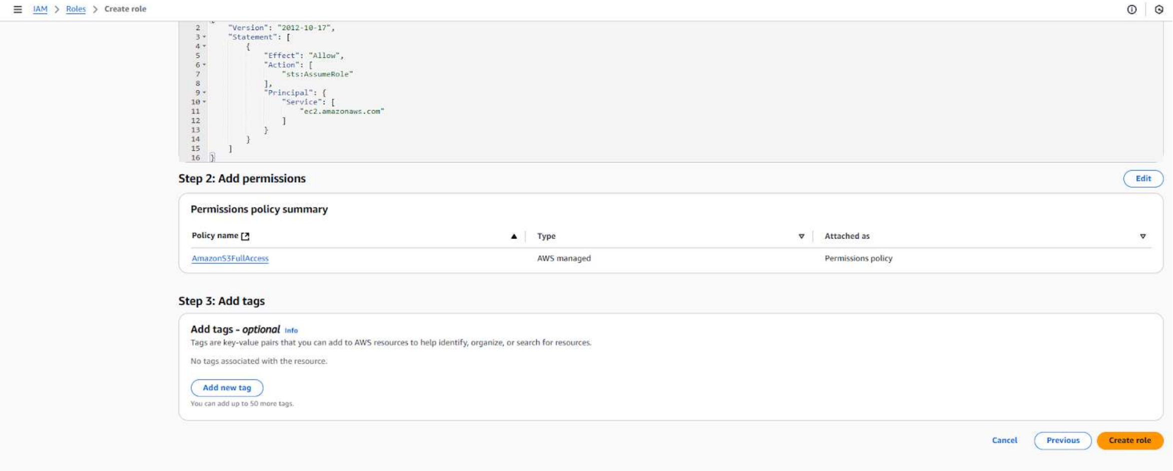
Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,.@-/\[{}]!#$%^*();:"`

Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    ]
}
```



```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

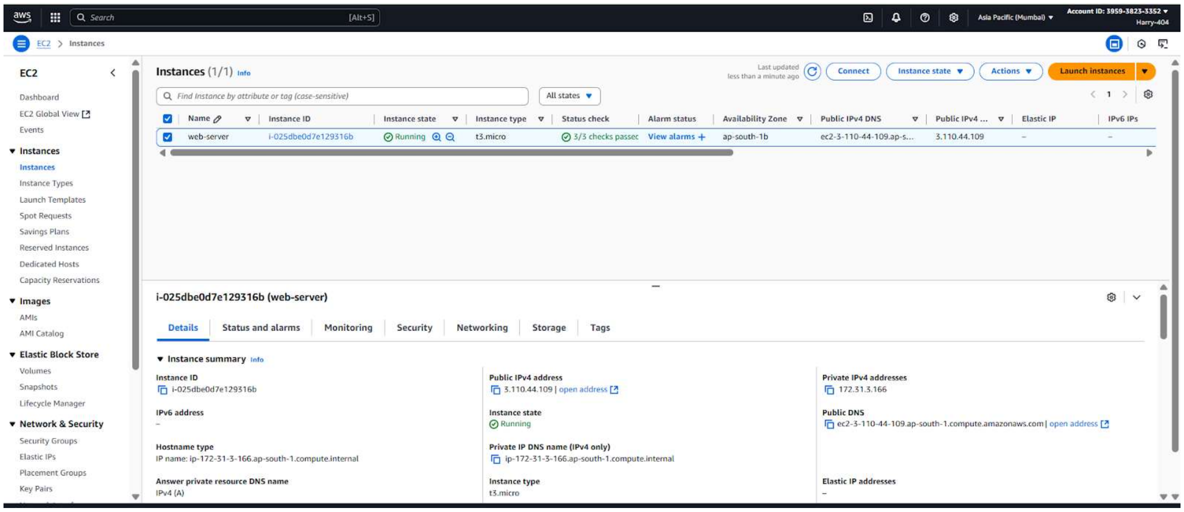
Step 3: Add tags

Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.



Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
☑	web-server	i-025dbe0d7e129316b	Running	t3.micro	3/3 checks passec	View alarms +	ap-south-1b	ec2-3-110-44-109.ap-s...	3.110.44.109	–	–

i-025dbe0d7e129316b (web-server)

Instance summary Info

Instance ID
i-025dbe0d7e129316b

Public IPv4 address
3.110.44.109 | open address

Private IPv4 addresses
172.31.3.166

IPv6 address
–

Instance state
Running

Public DNS
ec2-3-110-44-109.ap-south-1.compute.amazonaws.com | open address

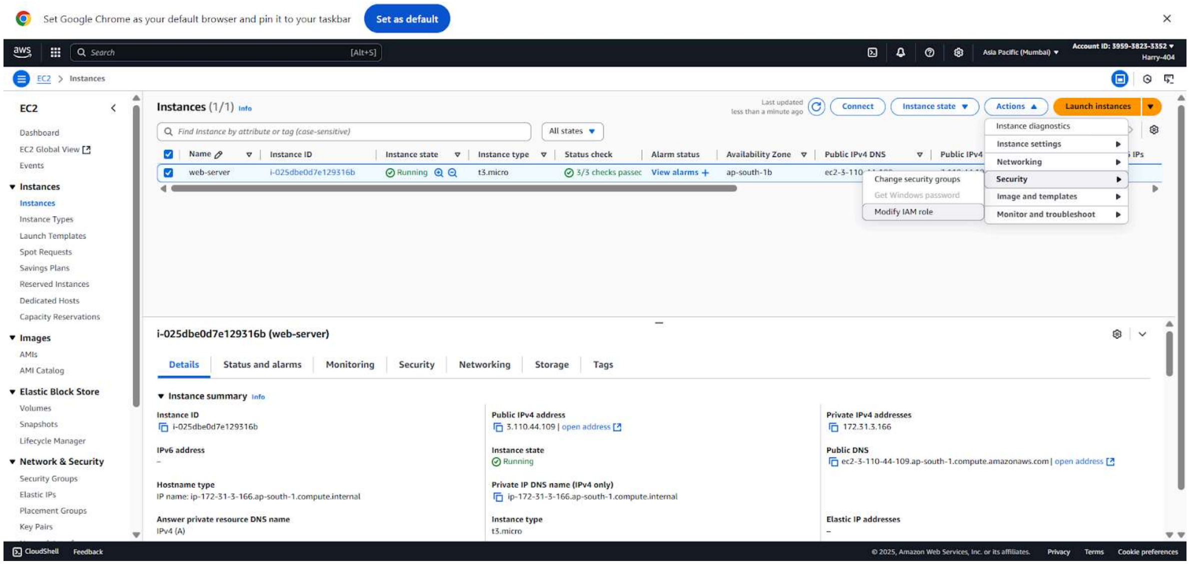
Hostname type
IP name: ip-172-31-3-166.ap-south-1.compute.internal

Private IP DNS name (IPv4 only)
ip-172-31-3-166.ap-south-1.compute.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t3.micro

Elastic IP addresses
–



Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	web-server	i-025dbe0d7e129316b	Running	t3.micro	3/3 checks passec	View alarms +	ap-south-1b	ec2-3-110

i-025dbe0d7e129316b (web-server)

Instance summary Info

Instance ID
i-025dbe0d7e129316b

Public IPv4 address
3.110.44.109 | open address

Private IPv4 addresses
172.31.3.166

IPv6 address
–

Instance state
Running

Public DNS
ec2-3-110-44-109.ap-south-1.compute.amazonaws.com | open address

Hostname type
IP name: ip-172-31-3-166.ap-south-1.compute.internal

Private IP DNS name (IPv4 only)
ip-172-31-3-166.ap-south-1.compute.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t3.micro

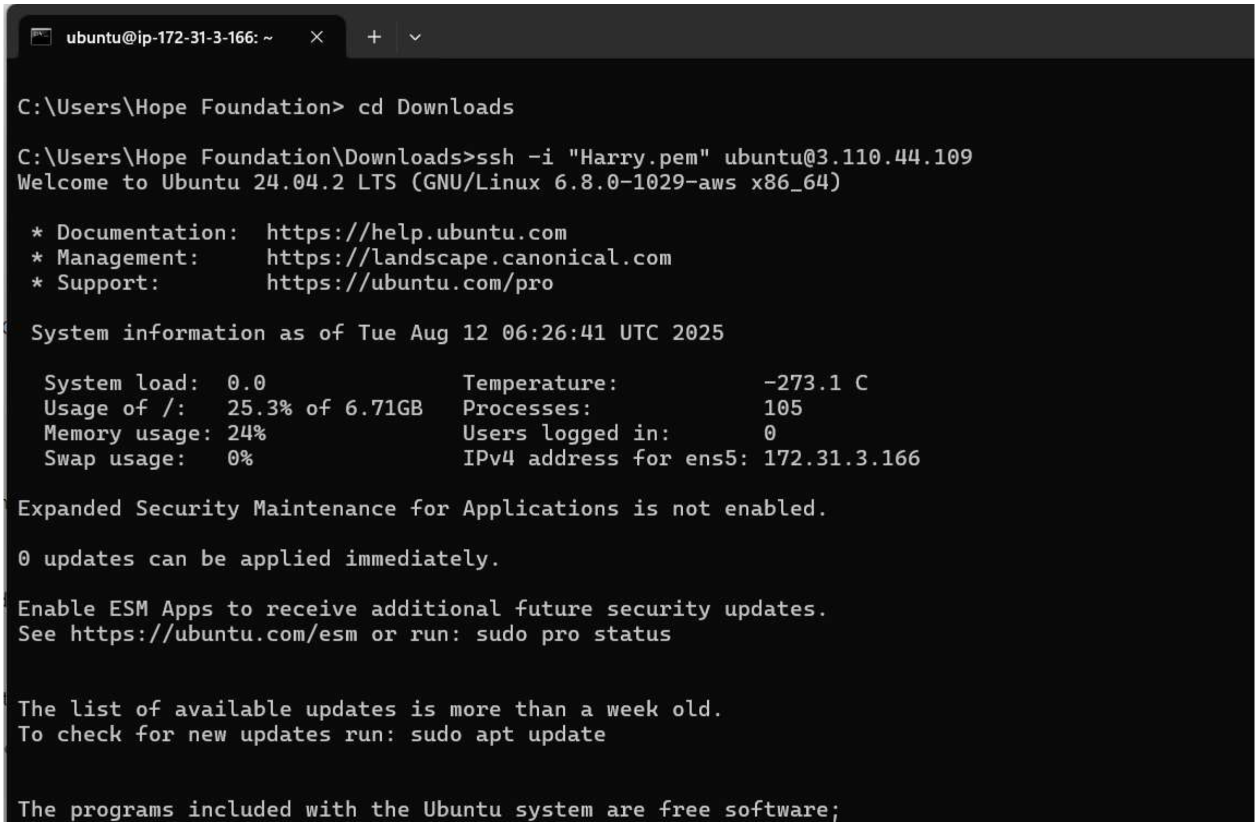
Elastic IP addresses
–

4. Connect to EC2 via SSH

- Use this exact command from your local terminal (replace `your-key.pem` and `<EC2_PUBLIC_IP>`):

```
ssh -i your-key.pem ubuntu@<EC2_PUBLIC_IP>
```

This connects you securely to your EC2 instance.



```
C:\Users\Hope Foundation> cd Downloads

C:\Users\Hope Foundation\Downloads>ssh -i "Harry.pem" ubuntu@3.110.44.109
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Aug 12 06:26:41 UTC 2025

  System load:  0.0               Temperature:           -273.1 C
  Usage of /:   25.3% of 6.71GB   Processes:             105
  Memory usage: 24%               Users logged in:       0
  Swap usage:   0%                IPv4 address for ens5: 172.31.3.166

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


The programs included with the Ubuntu system are free software;
```

5. Install Apache on EC2 Instance

Run these commands on your connected EC2 instance:

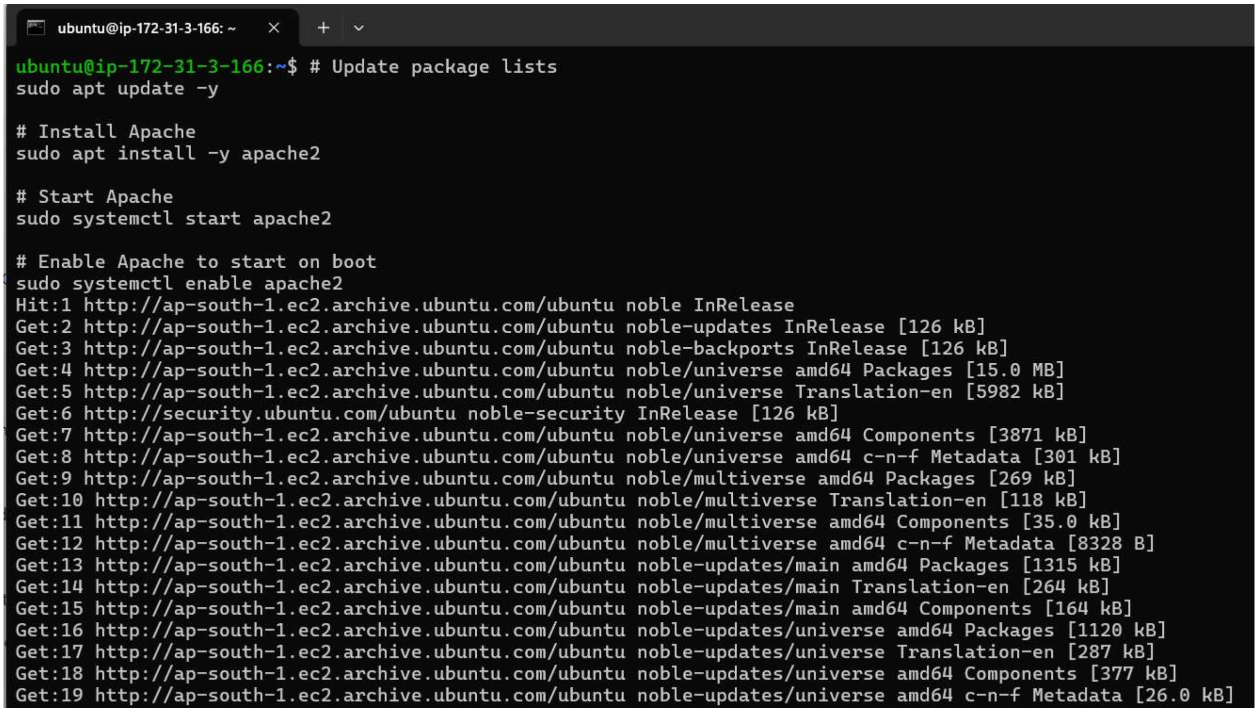
```
sudo apt update -y

sudo apt install -y apache2

sudo systemctl start apache2

sudo systemctl enable apache2
```

- `apt update`: updates package lists.

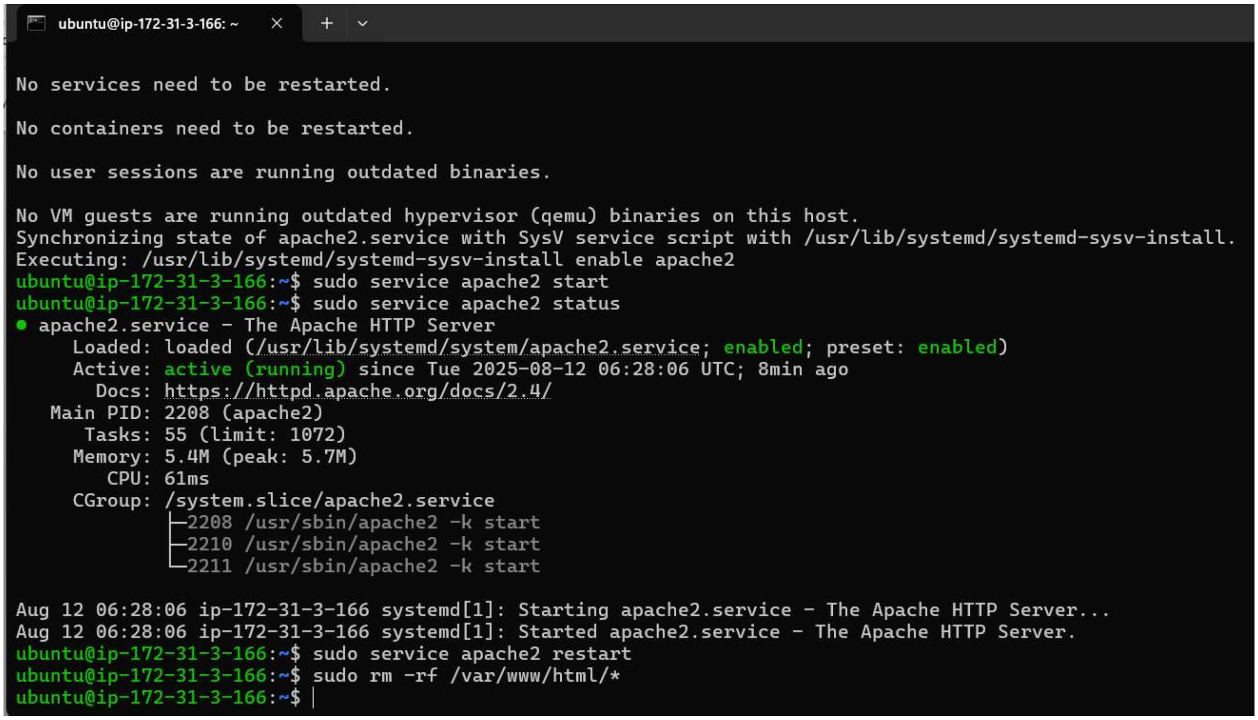
- `install apache2`: installs the Apache web server.
- `start apache2`: starts Apache service.
- `enable apache2`: ensures Apache runs on system boot.

You can check that Apache is running with:

```
sudo service apache2 status
```



```
ubuntu@ip-172-31-3-166:~$ # Update package lists
sudo apt update -y

# Install Apache
sudo apt install -y apache2

# Start Apache
sudo systemctl start apache2

# Enable Apache to start on boot
sudo systemctl enable apache2
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:7 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:8 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:9 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:10 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:11 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:12 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:13 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1315 kB]
Get:14 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [264 kB]
Get:15 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [164 kB]
Get:16 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1120 kB]
Get:17 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [287 kB]
Get:18 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [377 kB]
Get:19 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [26.0 kB]
```



```

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
ubuntu@ip-172-31-3-166:~$ sudo service apache2 start
ubuntu@ip-172-31-3-166:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-08-12 06:28:06 UTC; 8min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2208 (apache2)
      Tasks: 55 (limit: 1072)
     Memory: 5.4M (peak: 5.7M)
        CPU: 61ms
     CGroup: /system.slice/apache2.service
             ├─2208 /usr/sbin/apache2 -k start
             ├─2210 /usr/sbin/apache2 -k start
             └─2211 /usr/sbin/apache2 -k start

Aug 12 06:28:06 ip-172-31-3-166 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 12 06:28:06 ip-172-31-3-166 systemd[1]: Started apache2.service - The Apache HTTP Server.
ubuntu@ip-172-31-3-166:~$ sudo service apache2 restart
ubuntu@ip-172-31-3-166:~$ sudo rm -rf /var/www/html/*
ubuntu@ip-172-31-3-166:~$ 
```

6. Visit EC2 Public IP to See Default Apache Webpage

- Open a browser.
- Enter your EC2 instance’s public IP address.
- You should see the default Apache "It works!" webpage showing that Apache is serving content properly.

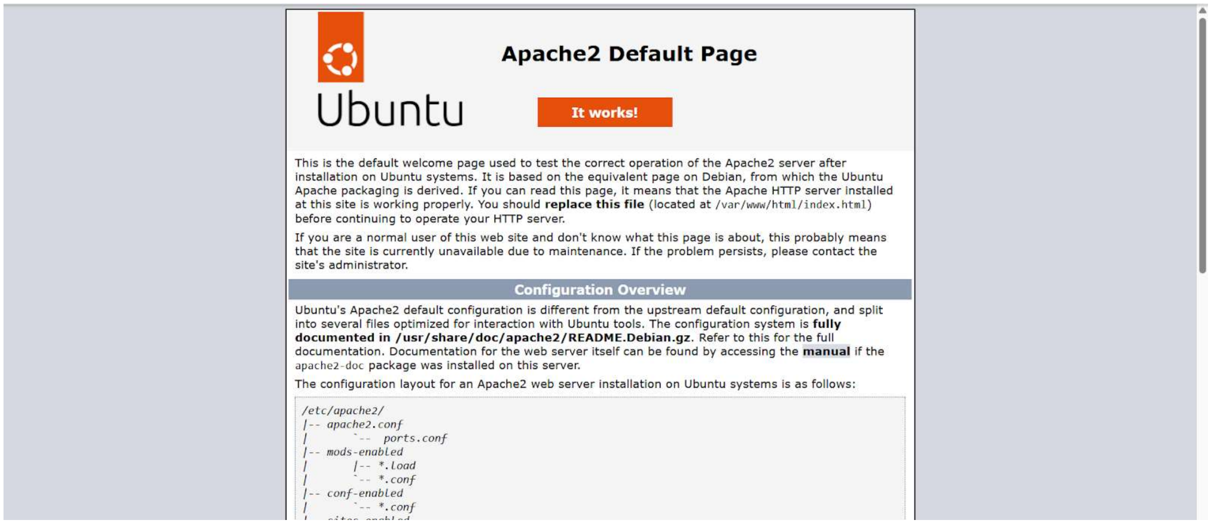
---

7. Remove the Default Apache Webpage

To remove the default Apache webpage files, run:

```
sudo rm -rf /var/www/html/*
```

- This deletes the default files served by Apache from the directory `/var/www/html`.



Ubuntu

Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

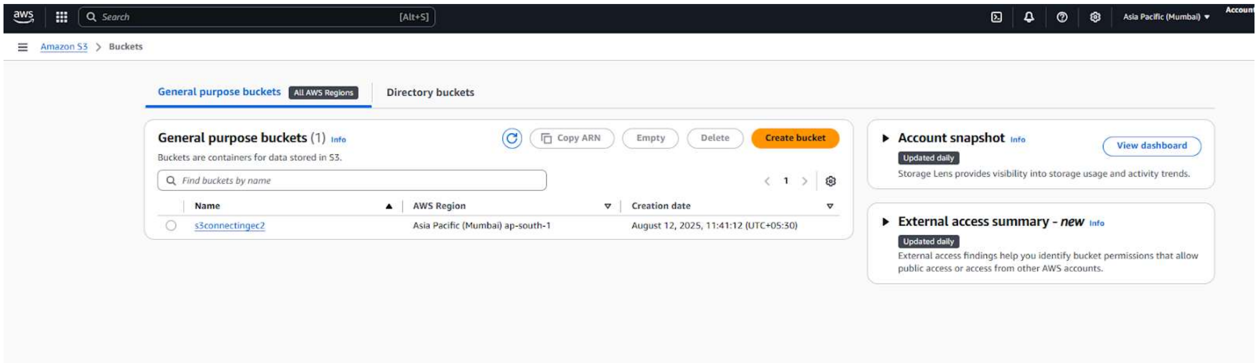
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
```

8. Upload Your Custom Image Webpage to S3 Bucket

Prepare your custom webpage (HTML file with your image) on your local machine.

Example file: `index.html` (make sure it references your image correctly).

Upload the file(s) to your S3 bucket



General purpose buckets (1) Info

Buttons: Copy ARN · Empty · Delete · Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

	Name ▲	AWS Region ▽	Creation date ▽
○	s3connectingec2	Asia Pacific (Mumbai) ap-south-1	August 12, 2025, 11:41:12 (UTC+05:30)

Account snapshot Info · View dashboard

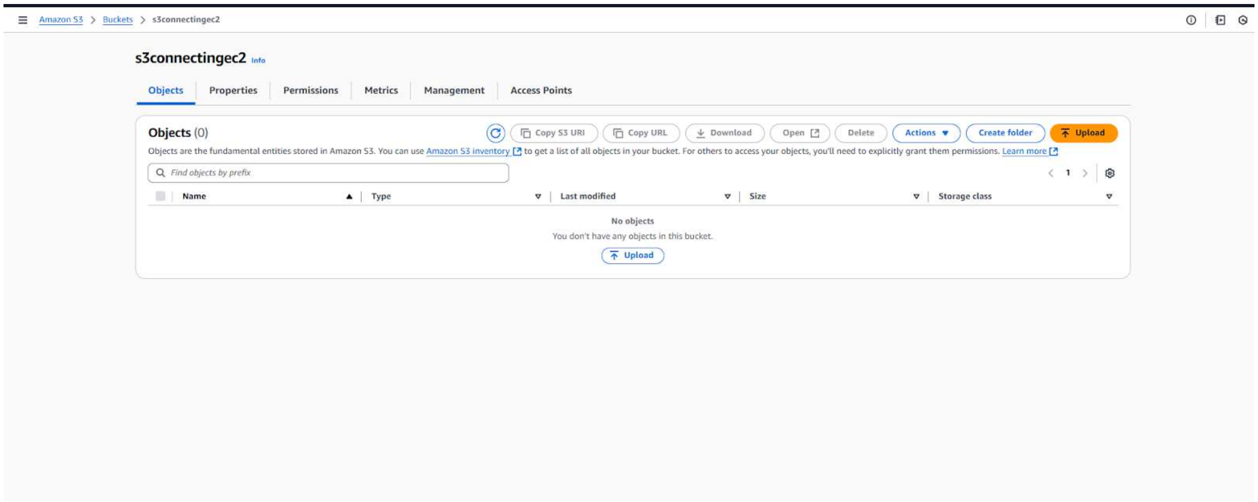
Updated daily

Storage Lens provides visibility into storage usage and activity trends.

External access summary - *new* Info

Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.



s3connectingec2 Info

Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

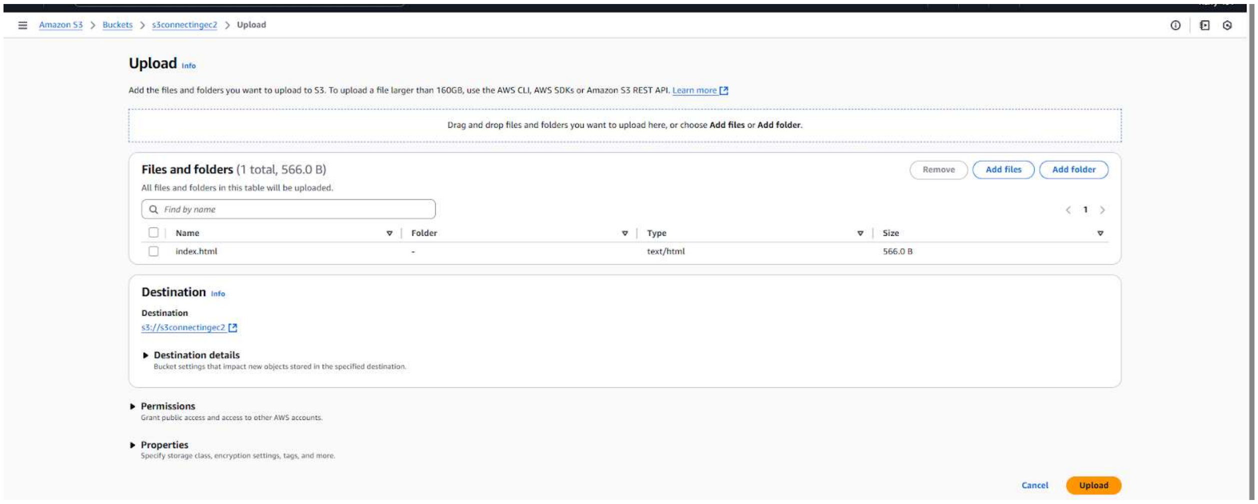
Find objects by prefix

□	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽

No objects

You don't have any objects in this bucket.

Upload



Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 total, 566.0 B)

All files and folders in this table will be uploaded.

Find by name

□	Name ▽	Folder ▽	Type ▽	Size ▽
□	index.html	-	text/html	566.0 B

Destination Info

Destination

s3://s3connectingec2

▶ Destination details

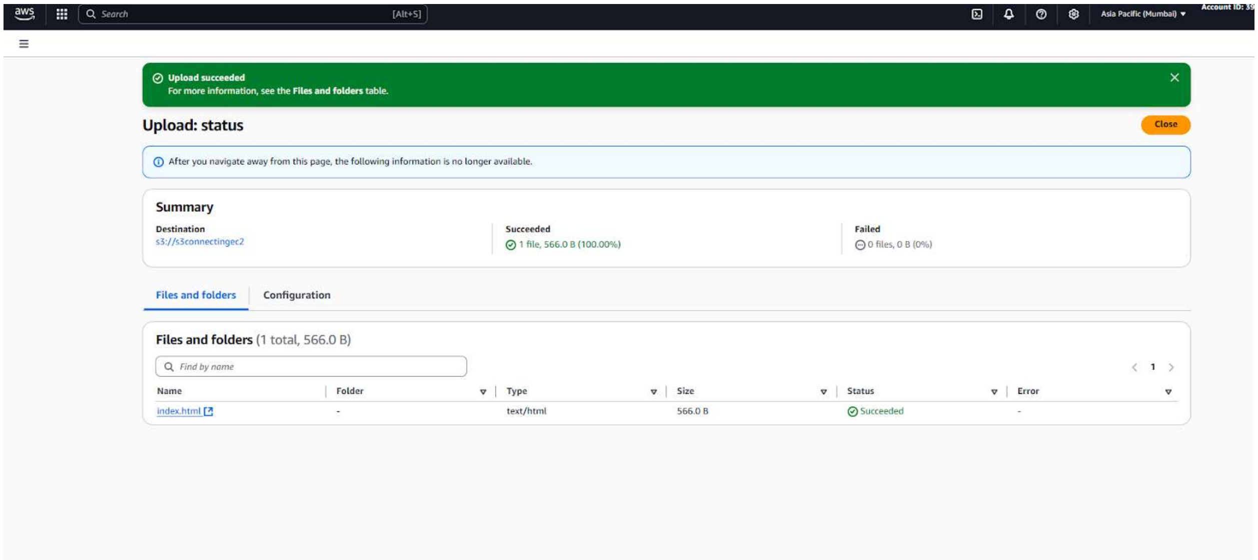
Bucket settings that impact new objects stored in the specified destination.

▶ Permissions

Grant public access and access to other AWS accounts.

▶ Properties

Specify storage class, encryption settings, tags, and more.



Upload succeeded
For more information, see the **Files and folders** table.

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary

Destination	Succeeded	Failed
s3://s3connectingec2	1 file, 566.0 B (100.00%)	0 files, 0 B (0%)

Files and folders | Configuration

Files and folders (1 total, 566.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	566.0 B	Succeeded	-

9. Apply a Bucket Policy to Enable Public Access to the Webpage

To allow public read access to your bucket objects, apply a bucket policy.

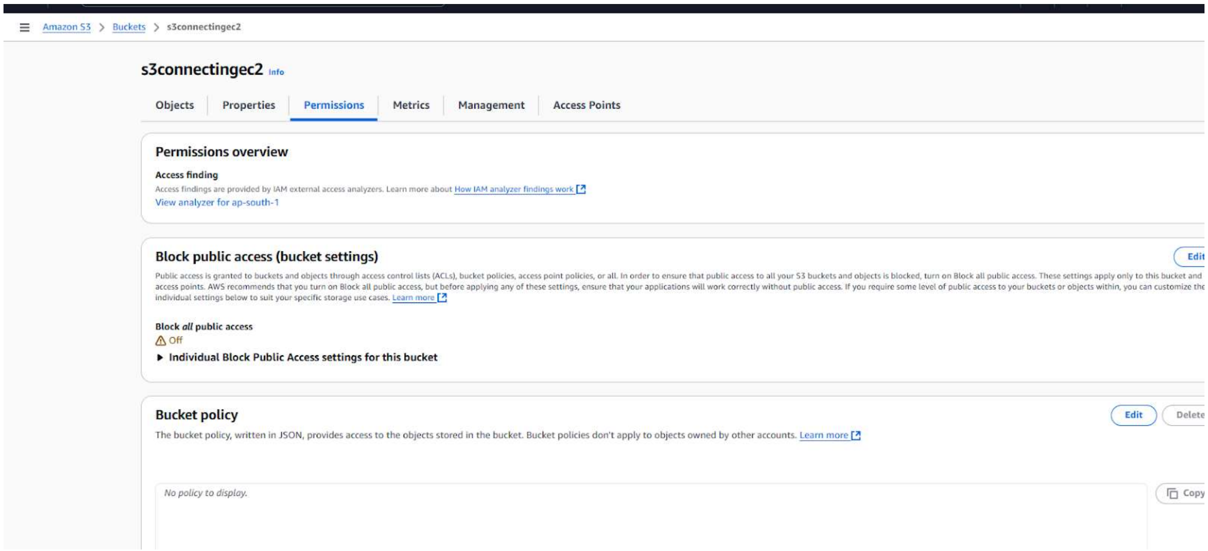
Here is a sample JSON bucket policy; replace `"s3connectingec2"` with your bucket name:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPublicRead",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::s3connectingec2/*"
    }
  ]
}
```

Steps to apply:

- Open AWS S3 console.

- Go to your bucket `s3connectingec2`.
- Click on Permissions tab.
- Scroll to Bucket Policy, click Edit.
- Paste the above JSON (with your bucket name changed).
- Save the policy.



s3connectingec2 Info

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work

View analyzer for ap-south-1

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. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block *all* public access

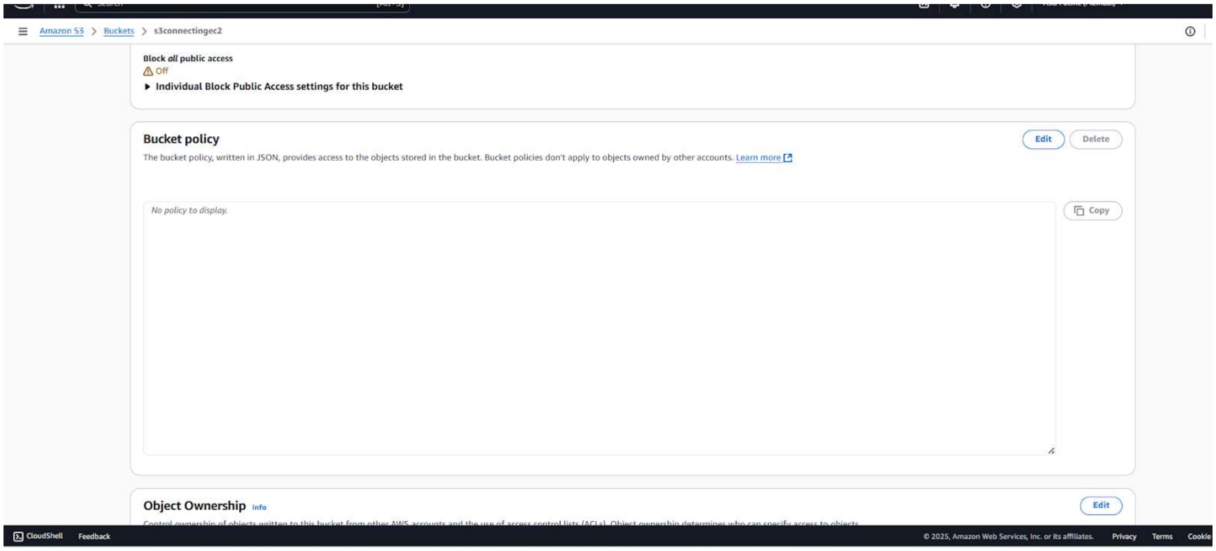
⚠ Off

▸ Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

No policy to display.


Amazon S3 > Buckets > s3connectingec2
Edit
Delete
Copy
Edit
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie

Block *all* public access

⚠ Off

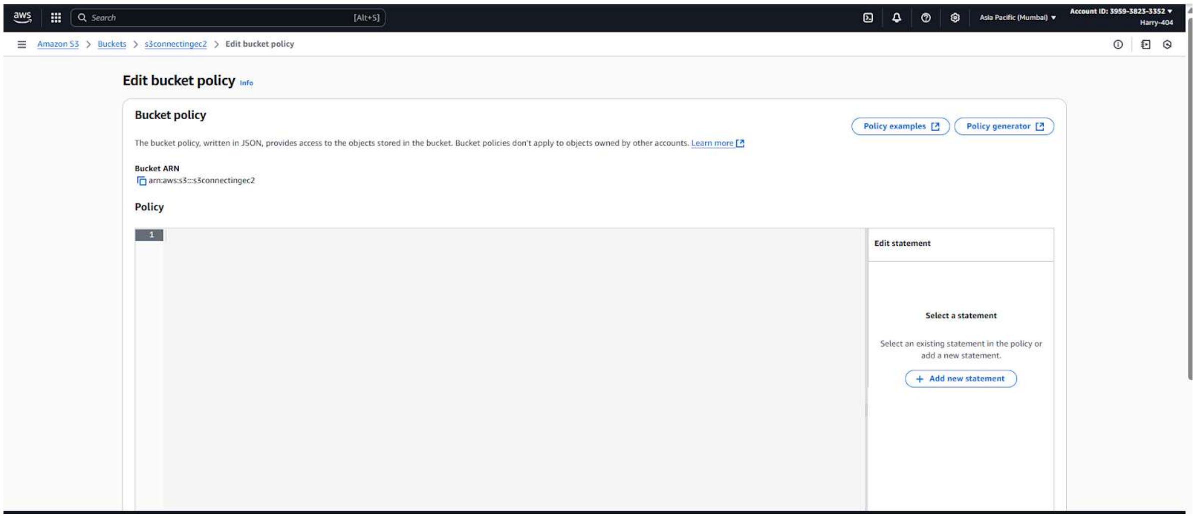
▸ Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

No policy to display.

Object Ownership Info



aws
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 3959-3823-3352
Harry-404
Amazon S3 > Buckets > s3connectingec2 > Edit bucket policy

Edit bucket policy

Bucket policy

Policy examples
Policy generator

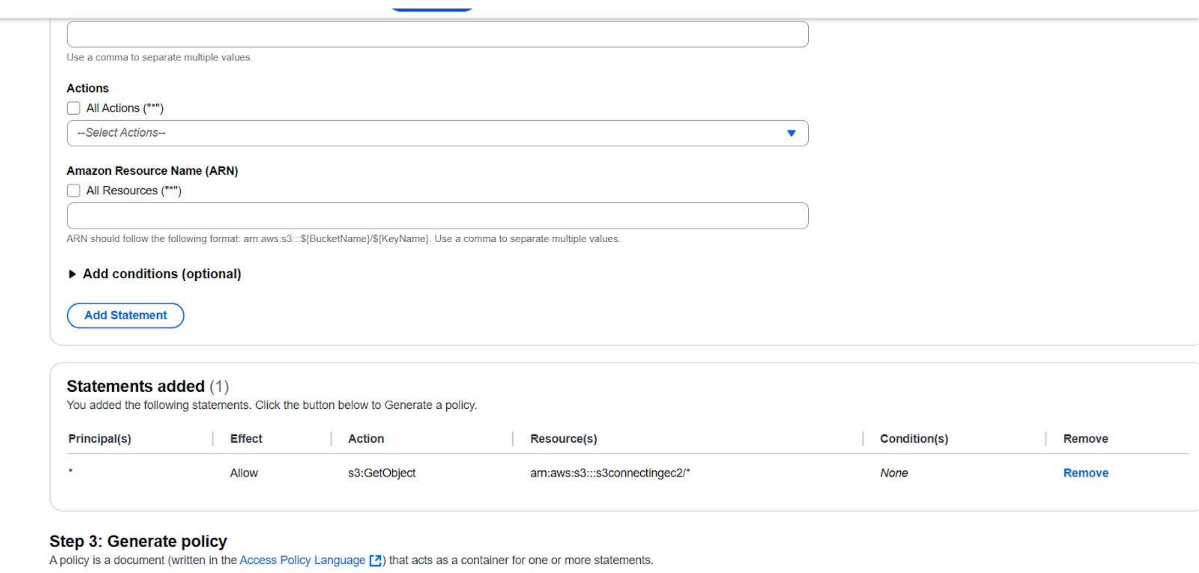
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Bucket ARN
arn:aws:s3:::s3connectingec2

Policy

```
1
```

Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement



Use a comma to separate multiple values.

Actions

□ All Actions ("*")

--Select Actions--

Amazon Resource Name (ARN)

□ All Resources ("*")

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}. Use a comma to separate multiple values.

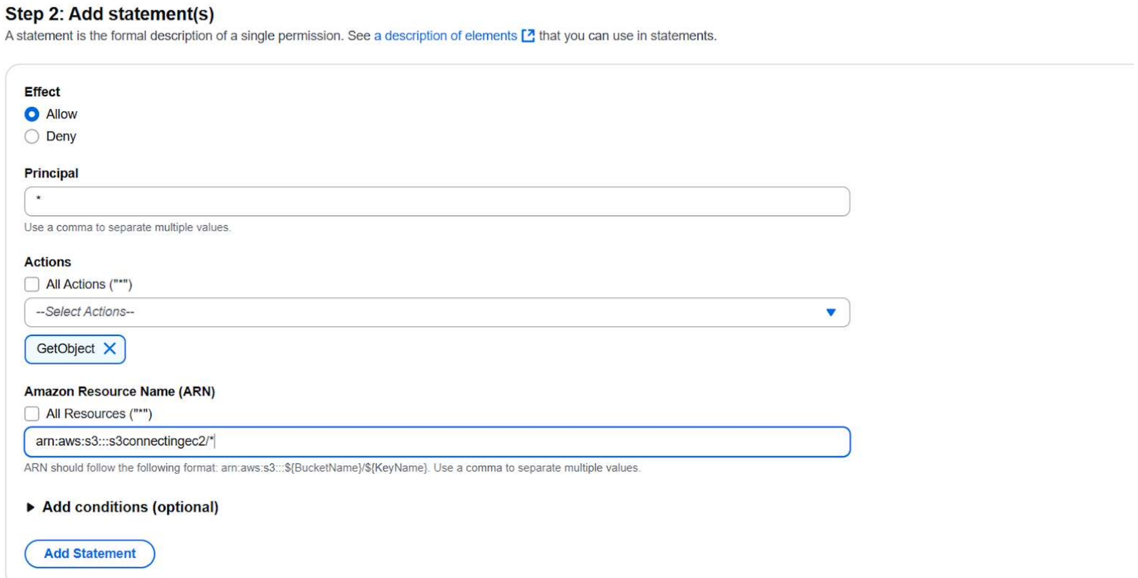
Statements added (1)

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

Principal(s)	Effect	Action	Resource(s)	Condition(s)	Remove
*	Allow	s3:GetObject	arn:aws:s3:::s3connectingec2/*	*None*	Remove

Step 3: Generate policy

A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.



Step 2: Add statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect

● Allow
○ Deny

Principal

*

Use a comma to separate multiple values.

Actions

□ All Actions ("*")

--Select Actions--

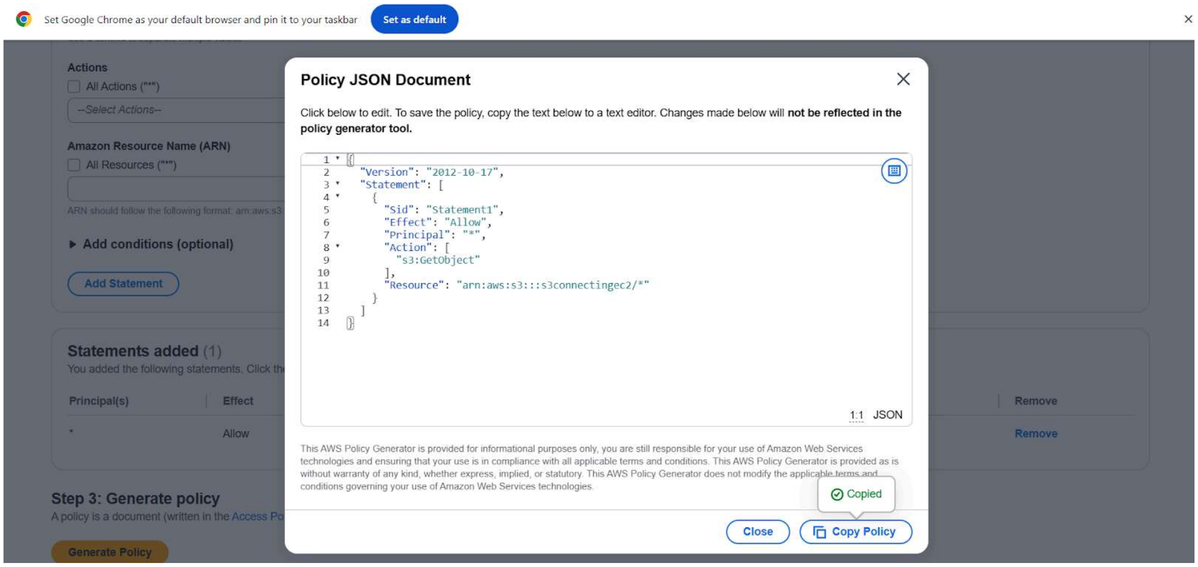
GetObject ✕

Amazon Resource Name (ARN)

□ All Resources ("*")

arn:aws:s3:::s3connectingec2/*

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}. Use a comma to separate multiple values.



ARN should follow the following format: arn:aws:s3

Statements added (1)

You added the following statements. Click th

Principal(s)	Effect	Remove
*	Allow	Remove

Step 3: Generate policy

A policy is a document (written in the Access Po

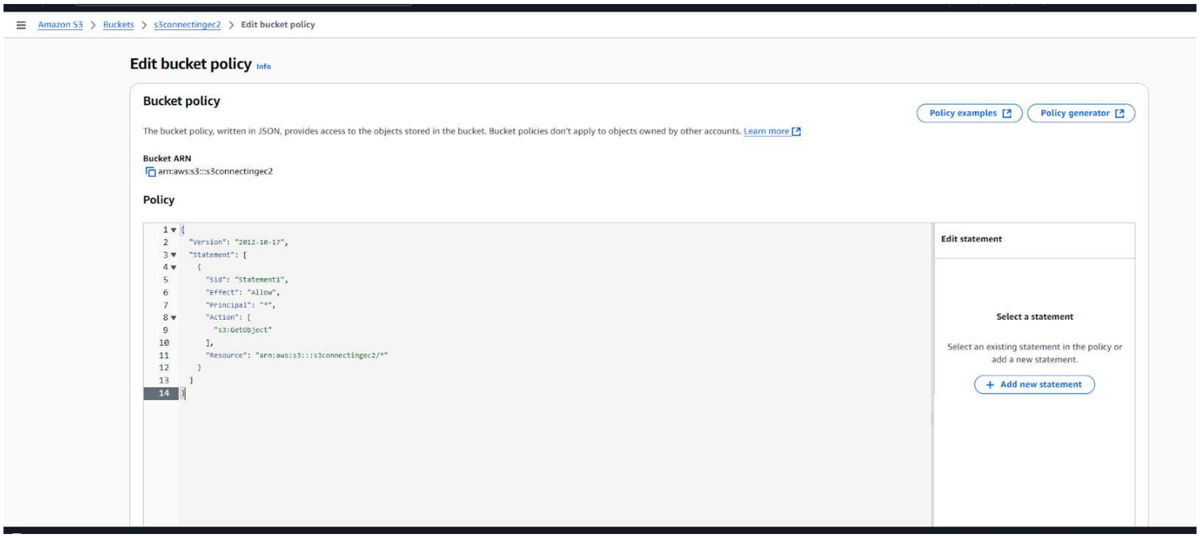
Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor. Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::s3connectingec2/*"
    }
  ]
}
```

1:1 JSON

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.



Edit bucket policy

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.

Bucket ARN

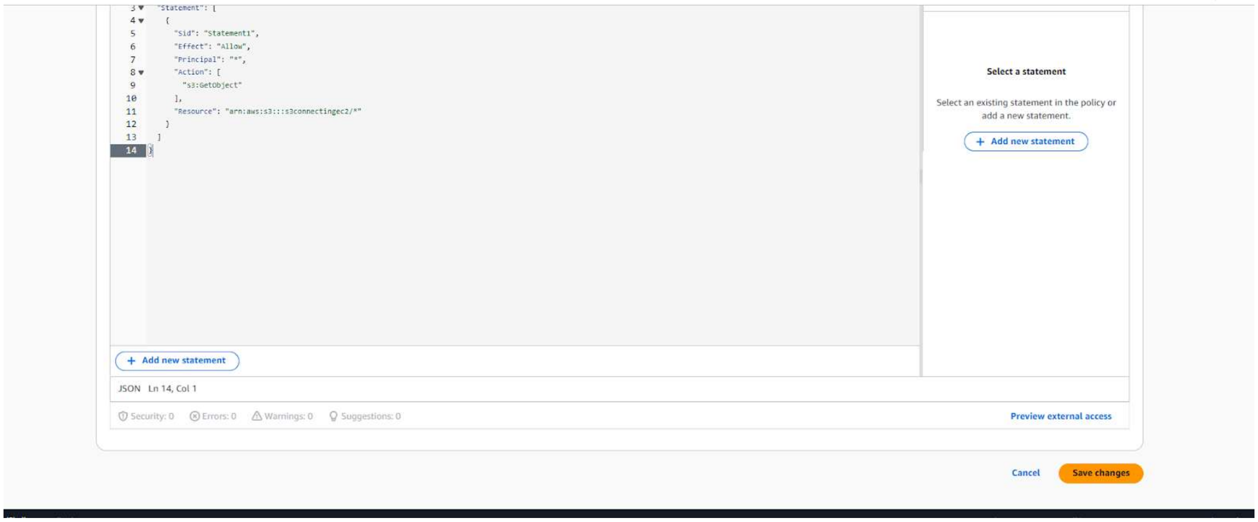
arn:aws:s3:::s3connectingec2

Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::s3connectingec2/*"
    }
  ]
}
```

Select a statement

Select an existing statement in the policy or add a new statement.



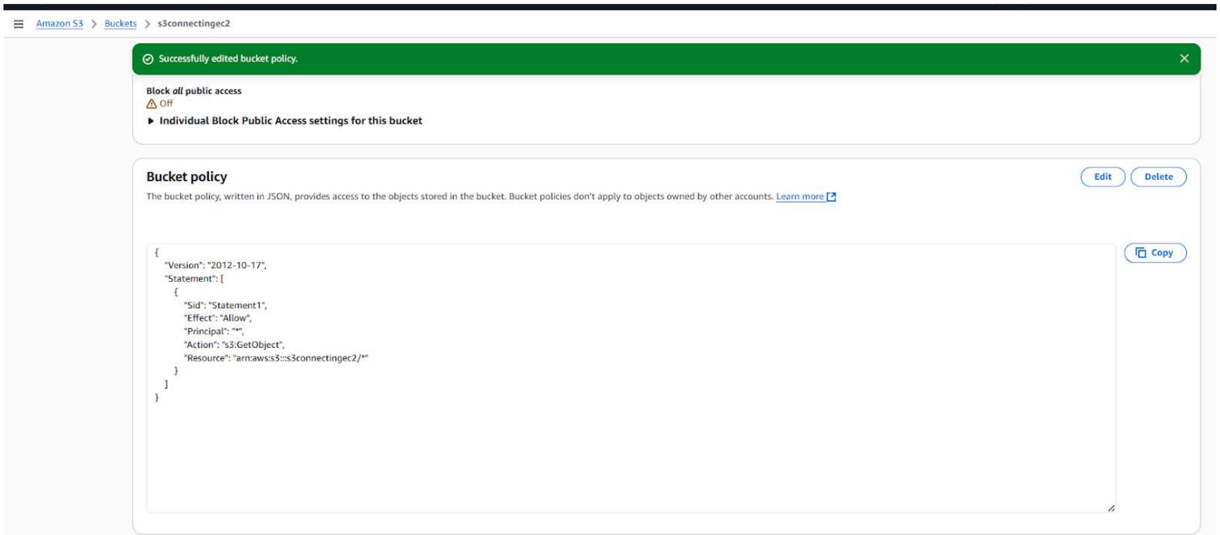
```
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::s3connectingec2/*"
    }
  ]
}
```

Select a statement

Select an existing statement in the policy or add a new statement.

JSON Ln 14, Col 1

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0



Successfully edited bucket policy.

Block *all* public access
⚠ Off

▶ Individual Block Public Access settings for this bucket

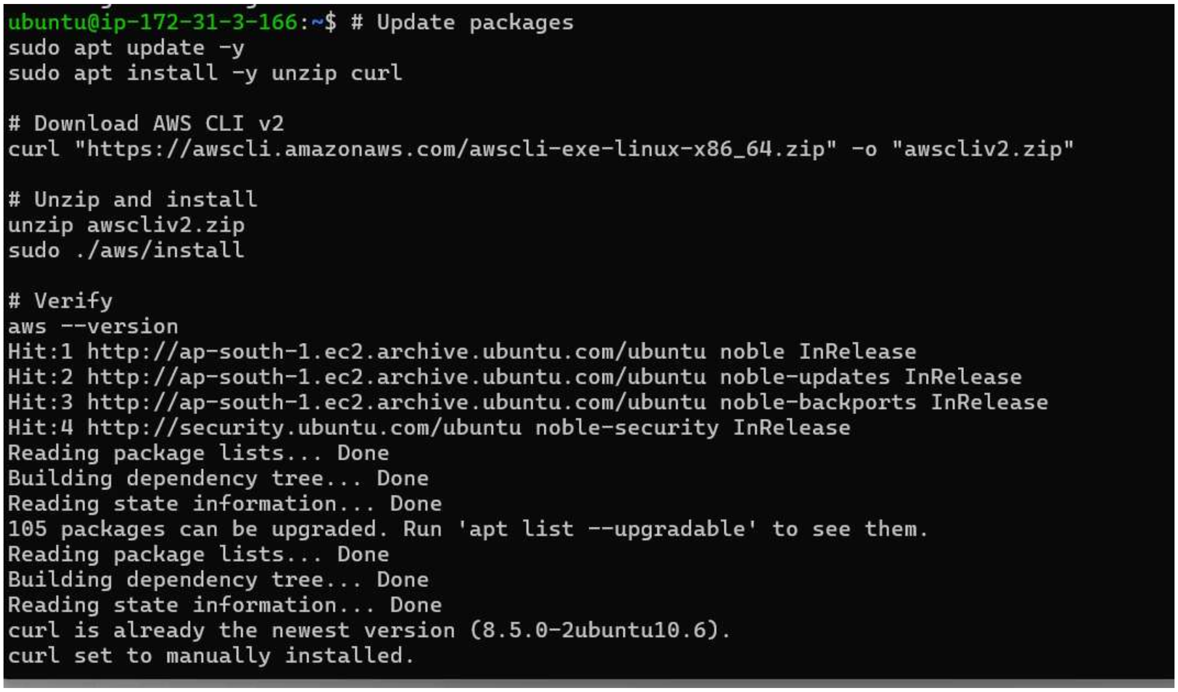
Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::s3connectingec2/*"
    }
  ]
}
```

10. Install AWS CLI on EC2

```
sudo apt update -y
sudo apt install -y unzip curl
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
aws --version
```



```
ubuntu@ip-172-31-3-166:~$ # Update packages
sudo apt update -y
sudo apt install -y unzip curl

# Download AWS CLI v2
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"

# Unzip and install
unzip awscliv2.zip
sudo ./aws/install

# Verify
aws --version
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
105 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (8.5.0-2ubuntu10.6).
curl set to manually installed.
```

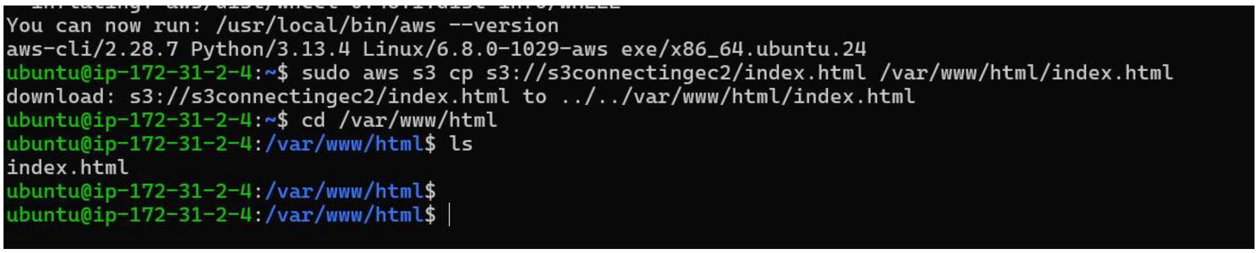
11. Sync Files from S3 to EC2 Bucket

- Download single file from S3 to EC2:

```
aws s3 cp s3://s3connectingec2/index.html /var/www/html/index.html
```

- To list files in S3 bucket:

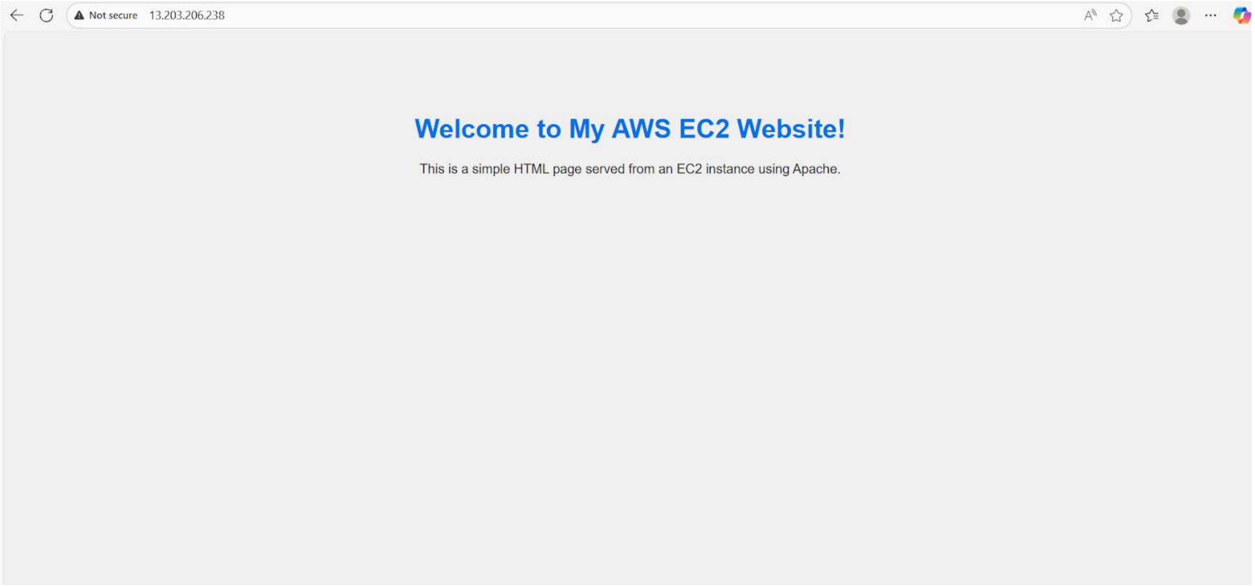
```
aws s3 ls s3://s3connectingec2
```



```
You can now run: /usr/local/bin/aws --version
aws-cli/2.28.7 Python/3.13.4 Linux/6.8.0-1029-aws exe/x86_64.ubuntu.24
ubuntu@ip-172-31-2-4:~$ sudo aws s3 cp s3://s3connectingec2/index.html /var/www/html/index.html
download: s3://s3connectingec2/index.html to ../../var/www/html/index.html
ubuntu@ip-172-31-2-4:~$ cd /var/www/html
ubuntu@ip-172-31-2-4:/var/www/html$ ls
index.html
ubuntu@ip-172-31-2-4:/var/www/html$
ubuntu@ip-172-31-2-4:/var/www/html$ |
```

12. Validate Your Setup

- To check Apache is serving files, simply navigate to your EC2 public IP via browser.



Welcome to My AWS EC2 Website!

This is a simple HTML page served from an EC2 instance using Apache.