

Implementation of :- An Amazon S3 File Upload

Notification System Using SNS

Objective of the Project

The main objective of this project is to **create a simple notification system** that sends an alert whenever a file is uploaded to an **Amazon S3 bucket** using **Amazon Simple Notification Service (SNS)**.

AWS Services Used in This Project and Their Usage

01 Amazon Simple Storage Service (Amazon S3)

- Amazon S3 is used to store the uploaded files/documents that are part of the project workflow.
- It acts as the core service where file upload events are detected and forwarded for notification processing.

02 Amazon Simple Notification Service (Amazon SNS)

- Amazon SNS is used to generate and deliver notifications when a file upload event occurs in the S3 bucket.
- It ensures timely alert delivery to subscribed endpoints, confirming successful file upload operations

03 Amazon Elastic Compute Cloud (Amazon EC2)

- Amazon EC2 is used as the execution environment to perform file upload operations to the S3 bucket.
- It also supports testing and validation of the notification system using AWS CLI commands.

04 AWS Identity and Access Management (IAM)

- IAM is used to define roles and permissions that allow secure interaction between S3, SNS, and EC2.
- It ensures controlled access by enforcing security policies for file uploads and notification publishing.

05 Amazon Virtual Private Cloud (Amazon VPC)

- Amazon VPC provides a secure and isolated network environment for the EC2 instance used in the project.
- It enhances security by managing network access and protecting cloud resources from unauthorized access.

The screenshot shows the AWS console search results for the query "vpd". The top navigation bar includes the AWS logo, a search bar with the text "vpd", the "Ask Amazon Q" button, and account information for "jay2025 (1827-1758-6119)" in "Asia Pacific (Mumbai)". The main content area displays search results under "Services" and "Features".

Services

- VPC Isolated Cloud Resources (highlighted with an orange box)
- AWS Global View
- AWS Firewall Manager

Features

- Dashboard (VPC feature)
- Route 53 VPCs (Route 53 feature)
- VPC links (API Gateway feature)

At the bottom, there's a "Were these results helpful?" section with "Yes" and "No" buttons, and a footer showing credits and days remaining.

This step is used to access the VPC service in AWS.

VPC provides a secure and isolated network for running the EC2 instance used in this project.

It ensures that the project resources are deployed in a controlled environment.

VPC dashboard < AWS Global View ▾ Filter by VPC ▾

Create VPC Launch EC2 Instances Note: Your Instances will launch in the Asia Pacific region.

Resources by Region You are using the following Amazon VPC resources

VPCs Mumbai 1 ▶ See all regions

Subnets Mumbai 3 ▶ See all regions

Route Tables Mumbai 1 ▶ See all regions

Internet Gateways Mumbai 2 ▶ See all regions

Egress-only Internet Gateways Mumbai 0 ▶ See all regions

Endpoint Services Mumbai 0 ▶ See all regions

NAT Gateways Mumbai 0 ▶ See all regions

VPC Peering Connections Mumbai 0 ▶ See all regions

Network ACLs Mumbai 1 ▶ See all regions

Security Groups Mumbai 4 ▶ See all regions

Refresh Resources

Service Health View complete service health details ▾

Settings Block Public Access Zones ▾ Console Experiments

Additional Information ▾ VPC Documentation All VPC Resources Forums Report an Issue

AWS Network Manager AWS Network Manager provides tools and features to help you manage and

Click on VPCs

The screenshot shows the AWS VPC dashboard with the 'Your VPCs' tab selected. The main area displays a table of existing VPCs. A red arrow originates from the 'Create VPC' button in the top right corner of the table header and points down to the instruction 'Click on Create VPC' located below the table.

VPC dashboard

AWS Global View

Filter by VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers

Security

- Network ACLs
- Security groups

Your VPCs

VPCs **VPC encryption controls**

Your VPCs (1) Info

Last updated less than a minute ago

Actions

Create VPC

Name	VPC ID	State	Encryption c...	Encryption control...	Block Public...	IPv4 C...
-	vpc-03dbf653ac9754b74	Available	-	-	Off	172.3

Select a VPC above

Click on Create VPC

- Create a Virtual Private Cloud for the project.



Search

[Alt+S]

Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025

≡ VPC > Your VPCs > Create VPC

i

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

 VPC only VPC and more

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

jay-vpc-01

IPv4 CIDR block Info

 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

 No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block IPv6 CIDR owned by me

- Go to the VPC service in AWS.
- Click Create VPC → choose “Only VPC.”
- Provide a Name tag **jay-vpc-01**
- Define the CIDR block **10.0.0.0/16**
- Disable IPv6 not required we use ipv4

Why Use: Establishes a secure, isolated network environment for project.



Search

[Alt+S]

Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025



VPC > Your VPCs > vpc-04f442fa7fd79f3b5



VPC dashboard <

AWS Global View ▾

Filter by VPC ▾

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

vpc-04f442fa7fd79f3b5 / jay-vpc-01

Actions ▾

Details InfoVPC ID
 vpc-04f442fa7fd79f3b5

DNS resolution

Enabled

Main network ACL

acl-0be81fdfb16f9a31b

IPv6 CIDR (Network border group)

-

Encryption control ID

-

State

Available

Tenancy

default

Default VPC

No

Network Address Usage metrics

Disabled

Encryption control mode

-

Block Public Access

Off

DHCP option set

dopt-01a8ff9e20cf0b89d

IPv4 CIDR

10.0.0.0/16

Route 53 Resolver DNS Firewall rule groups

-

DNS hostnames

Disabled

Main route table

rtb-012096622c831ea2f

IPv6 pool

-

Owner ID

182717586119

Resource map

CIDRs

Flow logs

Tags

Integrations

Resource map Info

VPC

Your AWS virtual network

Subnets (0)

Subnets within this VPC

Route tables (1)

Route network traffic to resources

Show all details

Click on internet gateways.

Why Use

- Required for EC2 instances in the public subnet to access the internet.
- Enables inbound and outbound traffic for public-facing applications.

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

RemoveAdd new tag

You can add 49 more tags.

[Cancel](#)[Create internet gateway](#)

Adding a Name tag **jay-ig** to the Internet Gateway.

The following internet gateway was created: igw-0df5d13c122df0bc2 - jay-ig. You can now attach to a VPC to enable the VPC to communicate with the internet.

igw-0df5d13c122df0bc2 / jay-ig

Details Info

Internet gateway ID igw-0df5d13c122df0bc2	State Detached	VPC ID -	Owner 182717586119
--	-------------------	-------------	-----------------------

Tags (1)

Key	Value
Name	jay-ig

Actions

- Attach to VPC
- Detach from VPC
- Manage tags
- Delete

Manage tags

Click on Attach vpc.

Why Use This Step

- Without attachment, the IGW exists but isn't connected to network.

Attach to VPC (igw-0df5d13c122df0bc2)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

▶ AWS Command Line Interface command

[Cancel](#)[Attach internet gateway](#)

Attach IGW to our VPC



Search

[Alt+S]

Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025



VPC > Internet gateways > igw-0df5d13c122df0bc2



VPC dashboard

AWS Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

igw-0df5d13c122df0bc2 / jay-ig

Details InfoInternet gateway ID
igw-0df5d13c122df0bc2State
AttachedVPC ID
vpc-04f442fa7fd79f3b5 | jay-vpc-01Owner
182717586119

Tags (1)

Manage tags

Search tags

Key	Value
Name	jay-ig

< 1 > |

Click on subnet

- Definition: Sub-divisions of VPC's IP range.
- Types:
- Public Subnet → connected to the internet via an Internet Gateway.
- Private Subnet → isolated, no direct internet access.

Why Use:

- Organizes resources by accessibility.
- Public subnet for web servers, private subnet for databases or backend services.

VPC dashboard < Subnets

AWS Global View ▾ Filter by VPC ▾

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

Subnets (3) Info

Last updated 5 minutes ago

Actions Create subnet

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-016688c668e8a5f89	Available	vpc-03dbf653ac9754b74	Off	172.31.16.0/20
-	subnet-04a061b62dd0957ce	Available	vpc-03dbf653ac9754b74	Off	172.31.32.0/20
-	subnet-0fc99767f2b93ac77	Available	vpc-03dbf653ac9754b74	Off	172.31.0.0/20

Select a subnet

Create new subnet

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-04f442fa7fd79f3b5 (jay-vpc-01)



Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key or 'Name' and a value that you specify.

jay-publics-1A

The name can be up to 256 characters long.

Availability Zone Info

Connect to my vpc and Defining a Name tag **jay-publics-1A** to mark this subnet as the public zone for internet-accessible resources.



Search

[Alt+S]

Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025

VPC > Subnets > Create subnet

i

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

jay-publics-1A

The name can be up to 256 characters long.

Availability Zone

Choose the AWS Availability Zone where the subnet will be created.

Asia Pacific (Mumbai) / aps1-az1 (ap-south-1a)

IPv4 VPC CIDR block

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.1.0/24

256 IPs

▼ Tags - optional

Key

Name

Value - optional

jay-publics-1A

Remove

Add new tag

You can add 49 more tags.

Remove

- **Availability Zone:** Select the AZ where the subnet will be created **ap-south-1a**.
- **IPv4 CIDR Block:** Define the IP range for the subnet **10.0.0.0/16**
- **VPC Association:** Attach the subnet to my project VPC **10.0.1.0/24**

Use

The public subnet is used to host resources (like EC2 instances) that need direct internet access. By enabling auto-assign public IPs, these resources can communicate with external services and users.

VPC dashboard <

AWS Global View Filter by VPC 

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

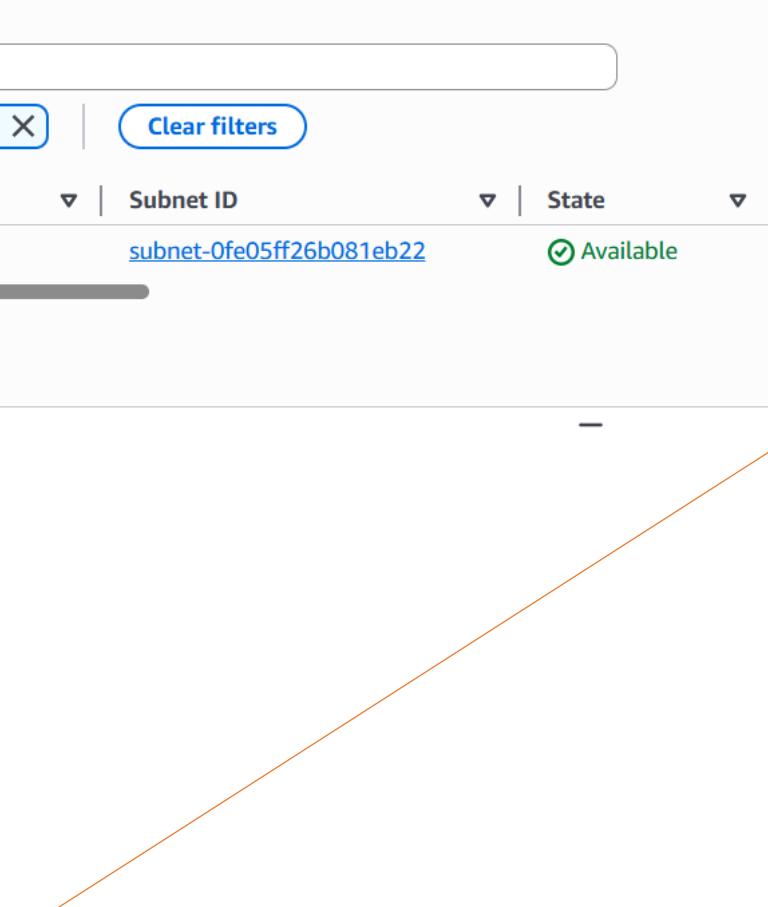
Security

Network ACLs

Security groups

 You have successfully created 1 subnet: subnet-0fe05ff26b081eb22Subnets (1) Find subnets by attribute or tag Subnet ID : subnet-0fe05ff26b081eb22  

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
<input type="checkbox"/>	jay-publics-1A	subnet-0fe05ff26b081eb22	 Available	vpc-04f442fa7fd79f3b5 jay-v...	 Off	10.0.1.0/24

Select a subnet Repeat the same process for the private subnet with some changes.

Create subnet Info

VPC

VPC ID

Create subnets in this VPC

vpc-04f442fa7fd79f3b5 (jay-vpc-01)



Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a unique 'Name' and a value that you specify.

jay-private-1B

The name can be up to 64 characters long.

Availability Zone Info

Assigning a Name tag **jay-private-1B** to indicate this subnet is isolated for backend resources.



Search

[Alt+S] Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025

☰ VPC > Subnets > Create subnet

i

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Mumbai) / aps1-az3 (ap-south-1b)

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.2.0/24

256 IPs

▼ Tags - optional

Key

Name

Value - optional

jay-privates-1B



Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create subnet

A private subnet is created in Availability Zone **ap-south-1B** with IPv4 CIDR block **10.0.2.0/24**, associated to my vpc.

Use

These resources remain isolated from direct internet access, ensuring higher security while still being able to reach the internet through a NAT Gateway if required

VPC dashboard < Subnets X

AWS Global View ↗ Filter by VPC ▾

Virtual private cloud

- Your VPCs
- Subnets**
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers

Security

- Network ACLs
- Security groups

You have successfully created 1 subnet: subnet-0834e09f089130fd9

Subnets (1/5) Info

Find subnets by attribute or tag

Name	Subnet ID	State	VPC
-	subnet-04a061b62dd095/ce	Available	vpc-05dbf653ac91
-	subnet-0fc99767f2b93ac77	Available	vpc-03dbf653ac91
jay-publics-1A	subnet-0fe05ff26b081eb22	Available	vpc-04f442fa7fd7
jay-privates-1B	subnet-0834e09f089130fd9	Available	vpc-04f442fa7fd7

Last updated less than a minute ago

Actions ▾ Create subnet

Edit subnet settings (highlighted)

IPv4 CIDR: 172.31.32.0/24
IPv6 CIDR: 172.31.0.0/20
Network ACL association: 10.0.1.0/24
Route table association: 10.0.2.0/24

subnet-0fe05ff26b081eb22 / jay-publics-1A

Details Flow logs Route table Network ACL CIDR reservations Sharing Tags

Details

Subnet ID: subnet-0fe05ff26b081eb22	Subnet ARN: arn:aws:ec2:ap-south-1:1827175861:19:subnet/subnet-0fe05ff26b081eb22	State: Available	Block Public Access: Off
IPv4 CIDR: 10.0.1.0/24	Available IPv4 addresses: 251	IPv6 CIDR:	IPv6 CIDR association ID:
Availability Zone: -		VPC: vpc-04f442fa7fd7	Route table: rt-04f442fa7fd7

Going to subnet setting in public subnet



Search

[Alt+S]

Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025

Auto-assign IP settings Info

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

Enable auto-assign public IPv4 address Info

Enable auto-assign customer-owned IPv4 address Info

Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch Info

Enable resource name DNS AAAA record on launch Info

Hostname type Info

Resource name

IP name

DNS64 settings

Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

Enable DNS64 Info

Cancel

Save

Enable this option so EC2 instances launched here automatically get a public IP.

AWS | Search [Alt+S] Ask Amazon Q Asia Pacific (Mumbai) jay2025 (1827-1758-6119) jay2025

VPC Subnets

You have successfully changed subnet settings:
Enable auto-assign public IPv4 address

Subnets (1/5) Info Last updated less than a minute ago Actions Create subnet

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-016688c668e8a5f89	Available	vpc-03dbf653ac9754b74	Off	172.31.16.0/2
-	subnet-04a061b62dd0957ce	Available	vpc-03dbf653ac9754b74	Off	172.31.32.0/2
-	subnet-0fc99767f2b93ac77	Available	vpc-03dbf653ac9754b74	Off	172.31.0.0/20
<input checked="" type="checkbox"/> jay-publics-1A	subnet-0fe05ff26b081eb22	Available	vpc-04f442fa7fd79f3b5 jay-v...	Off	10.0.1.0/24

subnet-0fe05ff26b081eb22 / jay-publics-1A

Details Flow logs Route table Network ACL CIDR reservations Sharing Tags

Details

Subnet ID subnet-0fe05ff26b081eb22	Subnet ARN arn:aws:ec2:ap-south-1:1827175861:subnet/subnet-0fe05ff26b081eb22	State Available	Block Public Access Off
IPv4 CIDR 10.0.1.0/24	Available IPv4 addresses 251	IPv6 CIDR -	IPv6 CIDR association ID -
Availability Zone ap-s1-az1 (ap-south-1a)	Network border group -	VPC vpc-01f412f77fd7af2b5 jay-v...	Route table -

Route tables

Click on Route tables



Search

[Alt+S] Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025

VPC > Route tables

VPC dashboard

AWS Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

Route tables (1) Info

Last updated
10 minutes ago

Actions

Create route table

Find route tables by attribute or tag

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-0b2b4eca9ff8c07f7	-	-	Yes	vpc-03dbf653ac9754b74

Select a route table



Create Route table

- Definition: Sets of rules that determine how traffic flows within my VPC.

Why Use

- Public route table → sends traffic to IGW.
- Private route table → sends traffic to NAT Gateway.



Search

[Alt+S] Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025

☰ VPC > Route tables > Create route table

ⓘ 🔍 🔍

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

jay-public-rt

VPC

The VPC to use for this route table.

vpc-04f442fa7fd79f3b5 (jay-vpc-01)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Name

Value - optional

jay-public-rt

Remove

Add new tag

You can add 49 more tags.

Cancel

Create route table

Naming the route table **jay-public-rt** and connect to my vpc



VPC > Route tables > rtb-04847c4166011e26c

Actions ▾

VPC dashboard <

AWS Global View ▾

Filter by VPC ▾

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

▼ Security

Network ACLs

Security groups

Route table rtb-04847c4166011e26c | jay-public-rt was created successfully.

rtb-04847c4166011e26c / jay-public-rt

Details Info

Route table ID

 rtb-04847c4166011e26c

Main

 No

Explicit subnet associations

-

Edge associations

-

VPC

vpc-04f442fa7fd79f3b5 | jay-vpc-01

Owner ID

 182717586119

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Filter routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	<input checked="" type="checkbox"/> Active	No	Create Route Table

Both ▾ Edit routes< 1 > 

Now going to edit the route.

Screenshot of the AWS VPC Route Tables interface showing the 'Edit routes' screen for a specific route table.

The table displays the following route entries:

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
0.0.0.0/0	Internet Gateway	-	No	CreateRoute

Actions available at the bottom right include **Add route**, **Cancel**, **Preview**, and **Save changes**.

The public route table is edited to send all outbound traffic (0.0.0.0/0 means all IPv4) from the public subnet to the Internet Gateway (jay-ig). This enables EC2 instances in the public subnet to access the internet.”



Search

[Alt+S] Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾
jay2025

☰ VPC > Route tables > rtb-04847c4166011e26c > Edit subnet associations



Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/> jay-publics-1A	subnet-0fe05ff26b081eb22	10.0.1.0/24	-	Main (rtb-012096622c831ea2f)
<input type="checkbox"/> jay-privates-1B	subnet-0834e09f089130fd9	10.0.2.0/24	-	Main (rtb-012096622c831ea2f)

Selected subnets

subnet-0fe05ff26b081eb22 / jay-publics-1A

Cancel

Save associations

Now going into Edit associations

The public subnet is associated with the public route table, enabling traffic to flow through the Internet Gateway for internet access.



Search

[Alt+S]

Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025



VPC > Route tables > rtb-04847c4166011e26c



VPC dashboard

AWS Global View

Filter by VPC

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

▼ Security

Network ACLs

Security groups

You have successfully updated subnet associations for rtb-04847c4166011e26c / jay-public-rt.

Actions ▾

rtb-04847c4166011e26c / jay-public-rt

Details Info

Route table ID

rtb-04847c4166011e26c

Main

No

Owner ID

182717586119

Explicit subnet associations

subnet-0fe05ff26b081eb22 / jay-publics-1A

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Filter routes

Both ▾

Edit routes



1

>



Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0df5d13c122df0bc2	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Click on Elastic IPs

VPC dashboard < Elastic IP addresses

AWS Global View ▾ Filter by VPC ▾

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs**
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers

Security

- Network ACLs
- Security groups

Elastic IP addresses Info

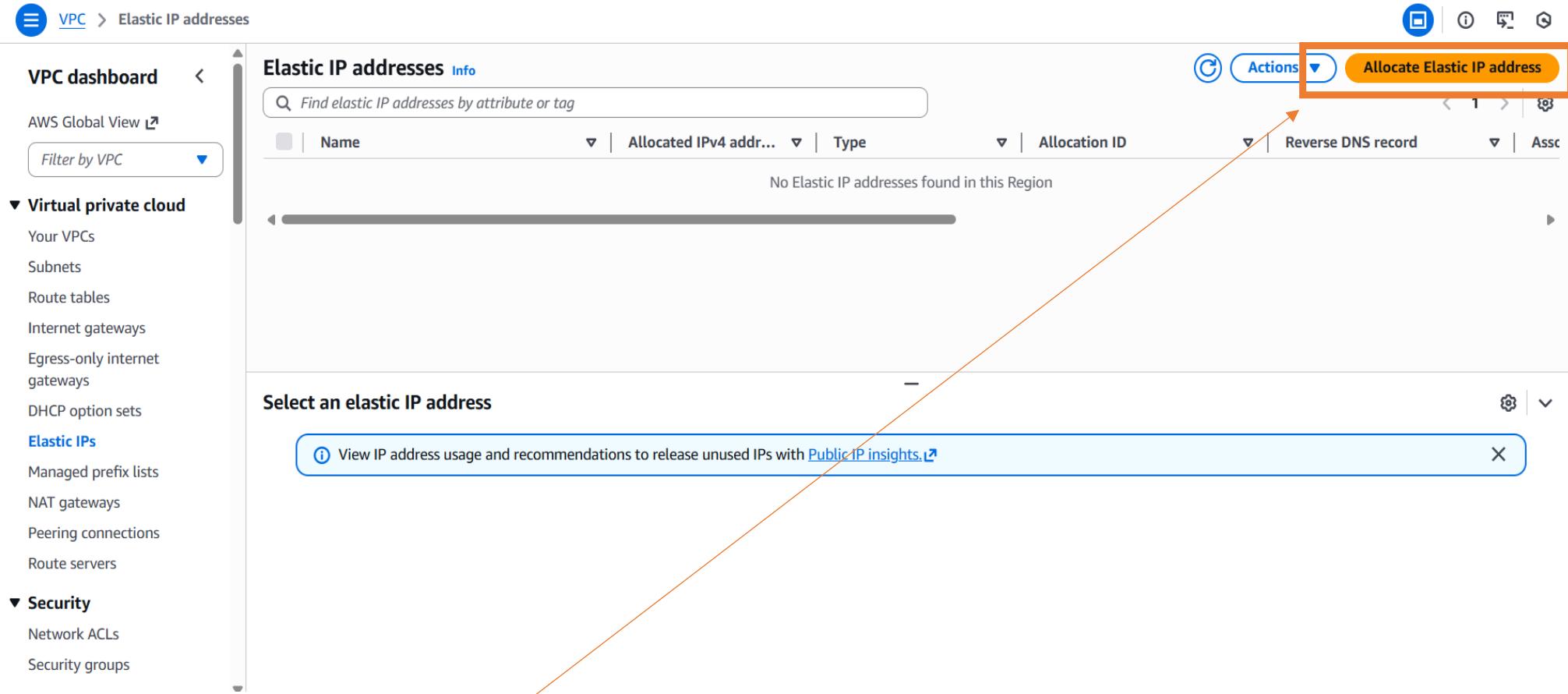
Find elastic IP addresses by attribute or tag

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Assoc...
No Elastic IP addresses found in this Region					

Select an elastic IP address

View IP address usage and recommendations to release unused IPs with [Public IP insights](#).

Actions ▾ Allocate Elastic IP address



Click on Allocate Elastic IP address

An Elastic IP is allocated to provide a static public IPv4 address. This address is attached to the NAT Gateway, ensuring consistent outbound internet access for private subnet resources.



Search

[Alt+S] Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025

≡ VPC > Elastic IP addresses > Allocate Elastic IP address



Allocate Elastic IP address Info

Elastic IP address settings Info

Public IPv4 address pool

- Amazon's pool of IPv4 addresses
- Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more ↗](#)
- Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more ↗](#)
- Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group Info

 ap-south-1 X

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more ↗](#)

[Create accelerator ↗](#)

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tag

Click on Available zone



Search

[Alt+S] Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾
jay2025

VPC > Elastic IP addresses



VPC dashboard

AWS Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

✓ Elastic IP address allocated successfully.
Elastic IP address 3.7.100.57

Associate this Elastic IP address

Elastic IP addresses (1) Info



Actions

Allocate Elastic IP address

Find elastic IP addresses by attribute or tag

Public IPv4 address : 3.7.100.57



Clear filters

<input type="checkbox"/> Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Assoc
<input type="checkbox"/> -	3.7.100.57	Public IP	eipalloc-0387e5e35a564f8f7	-	-

Select an elastic IP address

View IP address usage and recommendations to release unused IPs with [Public IP insights](#)



Click on NAT gateway



The screenshot shows the AWS VPC NAT gateways page. The top navigation bar includes the AWS logo, a search bar, and links for 'VPC dashboard', 'Ask Amazon Q', and account information ('jay2025 (1827-1758-6119)', 'Asia Pacific (Mumbai)', and 'jay2025'). On the left, a sidebar menu under 'Virtual private cloud' has 'NAT gateways' selected. The main content area displays a table titled 'NAT gateways' with columns for Name, NAT gateway ID, Connectivity..., State, State message, Availability..., Route table ID, and P. A search bar at the top of the table says 'Find NAT gateways by attribute or tag'. The table shows 'No NAT gateways found'. Below the table, a section titled 'Select a NAT gateway' is visible. The 'Actions' button in the top right of the table header is highlighted with a red box.

Create NAT gateway

A NAT Gateway (Network Address Translation Gateway) is a managed AWS service that allows instances in private subnets to connect to the internet or other AWS services, while preventing unsolicited inbound connections from the internet.



Search

[Alt+S] Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025

VPC > NAT gateways > Create NAT gateway

i

✓ Elastic IP address 13.126.255.241 (eipalloc-003c315adafc1c2d6) allocated.



Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - optional

Select a name for your NAT gateway, and a value that you specify.

The name can be up to 256 characters long.

Availability mode Info

Choose whether to deploy across all zones in the region or restrict to a single availability zone.

Regional - new

Scales automatically across all regional AZs, simplifying management for multi AZ deployments.

Zonal

Provides granular control within a specific availability zone, adhering to subnet level settings.

Subnet

Select a subnet in which to create the NAT gateway.



Connectivity type

Select a connectivity type for the NAT gateway.

Public

Private

Elastic IP allocation ID Info

NAT Gateway is created in a public subnet within Availability Zone ap-south-1a , using connectivity type Public and attached to Elastic IP . This setup enables secure outbound internet access for private subnet resources.

VPC dashboard < Actions ▾

AWS Global View

nat-0c0cedd144139ee58 / jay_gatway-01

Details

NAT gateway ID nat-0c0cedd144139ee58	Connectivity type Public	State Pending	State message Info -
NAT gateway ARN arn:aws:ec2:ap-south-1:182717586119:natgateway/nat-0c0cedd144139ee58	Primary public IPv4 address -	Primary private IPv4 address -	Primary network interface ID -
VPC vpc-04f442fa7fd79f3b5 / jay-vpc-01	Subnet subnet-0fe05ff26b081eb22 / jay-publics-1A	Created Friday, January 2, 2026 at 11:19:59 GM T+5:30	Deleted -

Secondary IPv4 addresses | Monitoring | Tags

Secondary IPv4 addresses

Search

Private IPv4 address	Network interface ID	Status	Failure message
Secondary IPv4 addresses are not available for this nat gateway.			

Edit secondary IPv4 address associations

Click on Route tables

The screenshot shows the AWS VPC Route Tables page. On the left, there's a navigation sidebar with sections like 'VPC dashboard', 'Virtual private cloud', 'Route tables', and 'Security'. The main area displays a table titled 'Route tables (3) Info' with columns for Name, Route table ID, Explicit subnet associa..., Edge associations, Main, and VPC. Three route tables are listed: one unnamed (-), 'jay-public-rt', and another unnamed (-). A search bar at the top says 'Find route tables by attribute or tag'. At the top right, there's an 'Actions' dropdown with a 'Create route table' button, which is highlighted with a red box and an orange arrow pointing to it.

Name	Route table ID	Explicit subnet associa...	Edge associations	Main	VPC
-	rtb-0b2b4eca9ff8c07f7	-	-	Yes	vpc-03dbf653ac9754b74
jay-public-rt	rtb-04847c4166011e26c	subnet-0fe05ff26b081eb...	-	No	vpc-04f442fa7fd79f3b5 jay-v...
-	rtb-012096622c831ea2f	-	-	Yes	vpc-04f442fa7fd79f3b5 jay-v..

Select a route table

Create private route table.

The private route table is configured to send all outbound traffic from the private subnet to the NAT Gateway. This allows private subnet instances to securely access the internet while remaining isolated from inbound connections.

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

VPC

The VPC to use for this route table.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

RemoveAdd new tag

You can add 49 more tags.

[Cancel](#)[Create route table](#)

Naming the route table **jay-private-rt** and connect to my vpc.



Search

[Alt+S] Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾

jay2025



VPC > Route tables > rtb-06de9107afb2f34f4



X

VPC dashboard



AWS Global View

Filter by VPC



Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

✓ Route table rtb-06de9107afb2f34f4 | jay_private-rt was created successfully.

Actions ▾

rtb-06de9107afb2f34f4 / jay_private-rt

Details Info

Route table ID

rtb-06de9107afb2f34f4

Main

No

Owner ID

vpc-04f442fa7fd79f3b5 | jay-vpc-01

Explicit subnet associations

-

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Filter routes

Destination

Target

Status

Propagated

Both

Edit routes

10.0.0.0/16

local

Active

No

Route Origin

Create Route Table

Now going to edit routes.



Search

[Alt+S]

Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾
jay2025

Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
0.0.0.0/0	NAT Gateway	-	No	CreateRoute

[Add route](#)[Cancel](#) [Preview](#) [Save changes](#)

The private route table is edited to send all outbound traffic (0.0.0.0/0) from the private subnet to the NAT Gateway. This allows private subnet instances to securely access the internet while remaining isolated from inbound connections.

VPC dashboard < X

AWS Global View ↗

Filter by VPC ▾

Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers

Security

- Network ACLs
- Security groups

Updated routes for rtb-06de9107afb2f34f4 / jay_private-rt successfully
► Details

rtb-06de9107afb2f34f4 / jay_private-rt Actions ▾

Details Info

Route table ID rtb-06de9107afb2f34f4	Main <input type="checkbox"/> No	Explicit subnet associations -	Edge associations -
VPC vpc-04f442fa7fd79f3b5 jay-vpc-01	Owner ID 182717586119		

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (0)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnet associations You do not have any subnet associations.			

Subnets without explicit associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Edit subnet associations			

Now edit association



Search

[Alt+S] Ask Amazon Q



Asia Pacific (Mumbai) ▾

jay2025 (1827-1758-6119) ▾
jay2025

☰ VPC > Route tables > rtb-06de9107afb2f34f4 > Edit subnet associations



Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Available subnets (1/2)				
<input type="text"/> Filter subnet associations				
-	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	jay-publics-1A	subnet-0fe05ff26b081eb22	10.0.1.0/24	-
<input checked="" type="checkbox"/>	jay-privates-1B	subnet-0834e09f089130fd9	10.0.2.0/24	-

Selected subnets

[subnet-0834e09f089130fd9 / jay-privates-1B](#)

[Cancel](#)[Save associations](#)

The private subnet is associated with the private route table Saving this association ensures that all traffic from the private subnet is routed securely through the NAT Gateway.

The screenshot shows the AWS console search results for the term "ec2". The search bar at the top contains "ec2". Below the search bar, there is a navigation menu with "Services" selected, followed by links to "Features", "Resources", "Documentation", "Knowledge articles", "Marketplace", "Blog posts", "Events", and "Tutorials". The main content area displays two sections: "Services" and "Features". The "Services" section contains three items: "EC2 Virtual Servers in the Cloud" (highlighted with an orange box), "EC2 Image Builder A managed service to automate build, customize and deploy OS images", and "Recycle Bin Protect resources from accidental deletion". The "Features" section contains three items: "EC2 Instances" (with a note about CloudWatch feature), "EC2 Resource Health" (with a note about CloudWatch feature), and "Dashboard" (with a note about EC2 feature). On the right side of the screen, there is a sidebar with options like "Reset to default layout", "+ Add widgets", "Create application", "Find applications", "Upgrade plan", and "myApplications". The status bar at the bottom indicates "PREMIUM PRIME MEMBER FREE TRIAL ACCESS" and "Access to AWS services will end when credits run out".

In this slide, we search and select the **EC2 service** from the AWS console.

The screenshot shows the AWS EC2 console with the 'Security Groups' section selected. The left sidebar includes links for Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and Load Balancing (Load Balancers). The main area displays a table of existing security groups:

Name	Security group ID	Security group name	VPC ID	Description
-	sg-001ea43f3a1a233d6	launch-wizard-3	vpc-03dbf653ac9754b74 ↗	launch-wizard-3 cre
-	sg-0f0d260c5fc9b1839	launch-wizard-1	vpc-03dbf653ac9754b74 ↗	launch-wizard-1 cre
-	sg-0fa8661c393a515ab	launch-wizard-2	vpc-03dbf653ac9754b74 ↗	launch-wizard-2 cre
-	sg-0c681b978cbe8a8c7	default	vpc-00269c21e0b607fd0 ↗	default VPC security
-	sg-05f23bf248b344f5d	default	vpc-03dbf653ac9754b74 ↗	default VPC security

A red box highlights the 'Create security group' button in the top right corner of the table header. Below the table, a modal window titled 'Select a security group' is partially visible.

Open the Security Groups section under EC2.

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateSecurityGroup:

aws | Search [Alt+S] | Asia Pacific (Mumbai) | jay2025 (1827-1758-6119) | jay2025

EC2 > Security Groups > Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info: raval-ec2-server
Name cannot be edited after creation.

Description Info: Allows SSH access to developers

VPC Info: vpc-00269c21e0b607fd0 (jay_vpc-01)

Inbound rules Info

Type	Protocol	Port range
SSH	TCP	22
Custom TCP	TCP	80
Custom TCP	TCP	5000

Source Info: Anywhere (0.0.0.0/0)

Description - optional Info: (optional)

Add rule

we create a new security group by providing the **security group name**, **description**, and selecting the correct **VPC**. Inbound rules are added to allow **SSH (22)**, **HTTP (80)**, and **Custom TCP (5000)** access from **0.0.0.0/0**.

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateSecurityGroup:

aws | Search [Alt+S] | Asia Pacific (Mumbai) | jay2025 (1827-1758-6119) | jay2025

EC2 > Security Groups > Create security group

0.0.0.0/0 X

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. X

Outbound rules Info

Type	Info	Protocol	Info	Port range	Info
All traffic		All		All	

Destination Info

Custom Info

0.0.0.0/0 X

Description - optional Info

Delete

Add rule

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses. X

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags

Cancel Create security group

Outbound rules are configured to allow **all traffic** to **0.0.0.0/0**, enabling the EC2 instance to communicate with the internet and AWS services.

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles

aws Search [Alt+S] Global jay2025 (1827-1758-6119) jay2025

IAM > Roles

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings
- Root access management
- Temporary delegation requests
- New

Access reports

- Access Analyzer
- Resource analysis New
- Unused access
- Analyzer settings
- Credential report

Roles (3) 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
AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Service-Linked Role)	15 minutes ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	21 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

Create role

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.

Manage

- Displays all IAM roles created in my AWS account.
- Click on create role button to create new role.

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create

aws Search [Alt+S]

jay2025 (1827-1758-6119) jay2025

IAM > Roles > Create role

Step 1
 Select trusted entity
 Step 2
 Add permissions
 Step 3
 Name, review, and create

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.

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.

```
graph TD; A["AWS service"] --> B["EC2"]; B --> C["EC2"]
```

- Choose AWS service to allow EC2 to assume the role.
- Select EC2 as the use case for accessing other AWS services.
- Enables EC2 to interact with S3 and SNS securely.

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&selectedUseCase=EC2

Search [Alt+S] Global jay2025 (1827-1758-6119) jay2025

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Add permissions Info

Permissions policies (2/1109) Info

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

Filter by Type All types 8 matches

Policy name	Type	Description
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda functions permis...
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on ...
<input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S...
<input checked="" type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket...
<input type="checkbox"/> AmazonS3TablesFullAccess	AWS managed	Provides full access to all S3 table bu...
<input type="checkbox"/> AmazonS3TablesLakeFormationServiceRole	AWS managed	This managed policy grants AWS Lake ...
<input type="checkbox"/> AmazonS3TablesReadOnlyAccess	AWS managed	Provides read only access to all S3 tabl...

▶ Set permissions boundary - optional

- Search for and select S3 access policies for the EC2 role.
- Attach AmazonS3FullAccess and AmazonS3ReadOnlyAccess as needed.
- These permissions allow EC2 to interact with S3 buckets securely.



- Step 1
Select trusted entity
- Step 2
Add permissions
- Step 3
Name, review, and create

Name, review, and create

Role details

Role Name
Enter a meaningful name to identify this role:

jay-ec2-s3-sns

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

Edit

Trust policy

```
1 - {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Action": [  
7                 "sts:AssumeRole"  
8             ],
```

- Enter a clear role name like **jay-ec2-s3-sns** and add a description.
 - Review the trust policy allowing EC2 to assume the role.
 - Confirm and create the role for secure service access.

This completes the IAM role setup for my project. The role now allows EC2 to interact with S3 and SNS, which is essential for my file upload notification system.

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles

aws | Search [Alt+S] Global jay2025 (1827-1758-6119) jay2025

IAM > Roles

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings
- Root access management
- Temporary delegation requests **New**

Access reports

- Access Analyzer
- Resource analysis **New**
- Unused access
- Analyzer settings

Role jay-ec2-s3-sns created.

View role X

Roles (4) 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
AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Service)	22 minutes ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	22 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
jay-ec2-s3-sns	AWS Service: ec2	-

Search

Roles Anywhere Info

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

Manage

Access AWS from your non AWS workloads

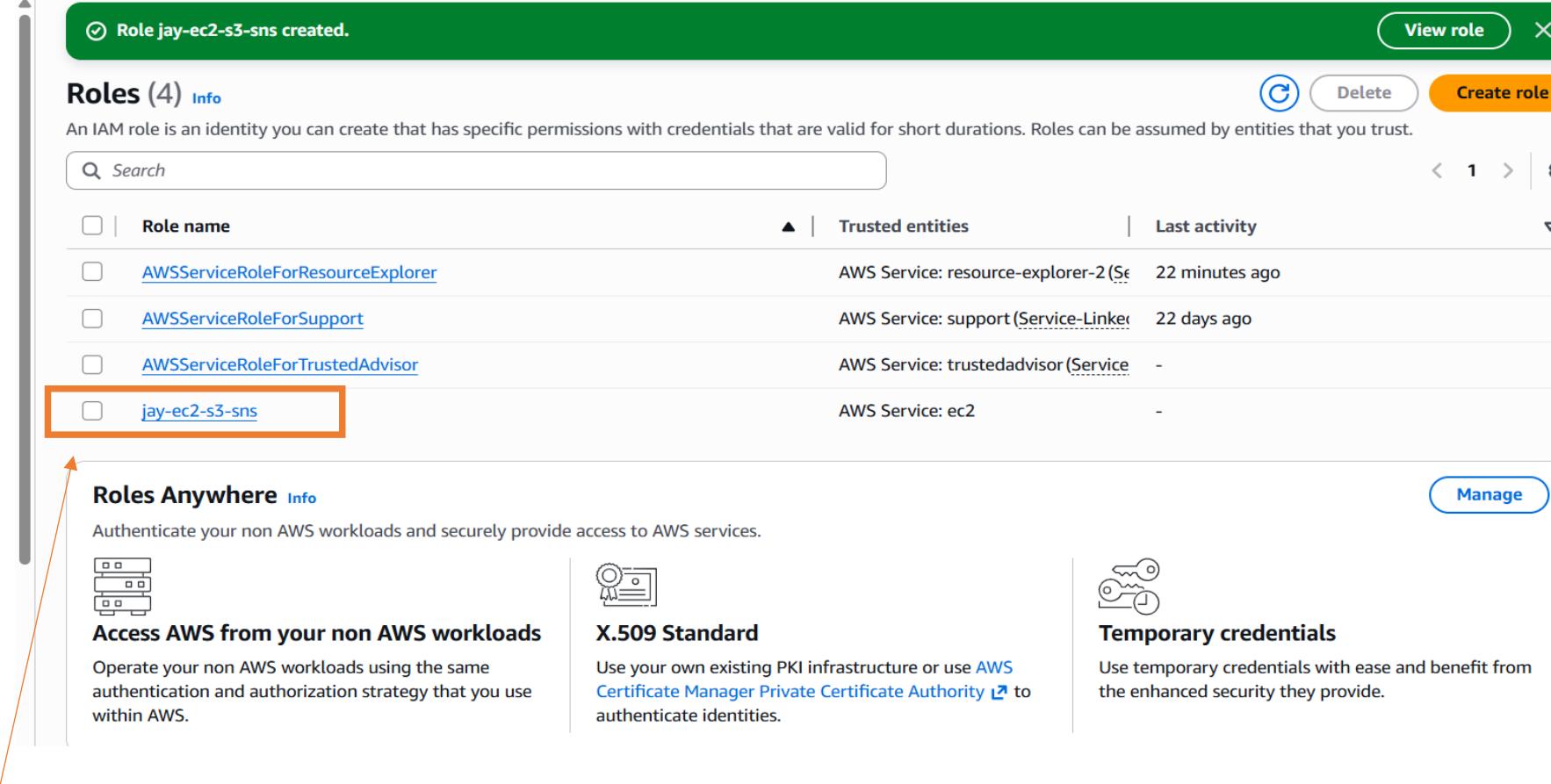
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

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.



- Confirms successful creation of the **jay-ec2-s3-sns IAM role**.
- Role is now listed and ready for EC2 to assume.
- Enables secure access to S3 and SNS for my notification system.

The screenshot shows the AWS search results for the query "ec2". The top navigation bar includes the AWS logo, a search bar with the text "ec2", an "Ask Amazon Q" button, and account information for "jay2025 (1827-1758-6119)" in the "Asia Pacific (Mumbai)" region. The main content area is titled "Services" and displays several items:

- EC2**: Virtual Servers in the Cloud (highlighted with an orange box and an orange arrow)
- EC2 Image Builder**: A managed service to automate build, customize and deploy OS images
- Recycle Bin**: Protect resources from accidental deletion

Below this, under "Features", are:

- EC2 Instances**: CloudWatch feature
- EC2 Resource Health**: CloudWatch feature
- Dashboard**: EC2 feature

A sidebar on the right contains a "Create application" button, a "Find applications" search bar, and a "Region" dropdown. The bottom of the page includes a "Were these results helpful?" section with "Yes" and "No" buttons, and a note about AWS credits.

- Use the AWS search bar to find EC2 services

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

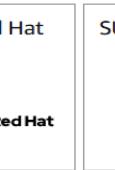
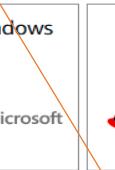
Name

project-sns-01

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) Info

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[Recents](#)[Quick Start](#)**Amazon Machine Image (AMI)**

Amazon Linux 2023 kernel-6.1 AMI

ami-00ca570c1b6d79f36 (64-bit (x86), uefi-preferred) / ami-061d45d4bd9c71ba1 (64-bit (Arm), uefi)

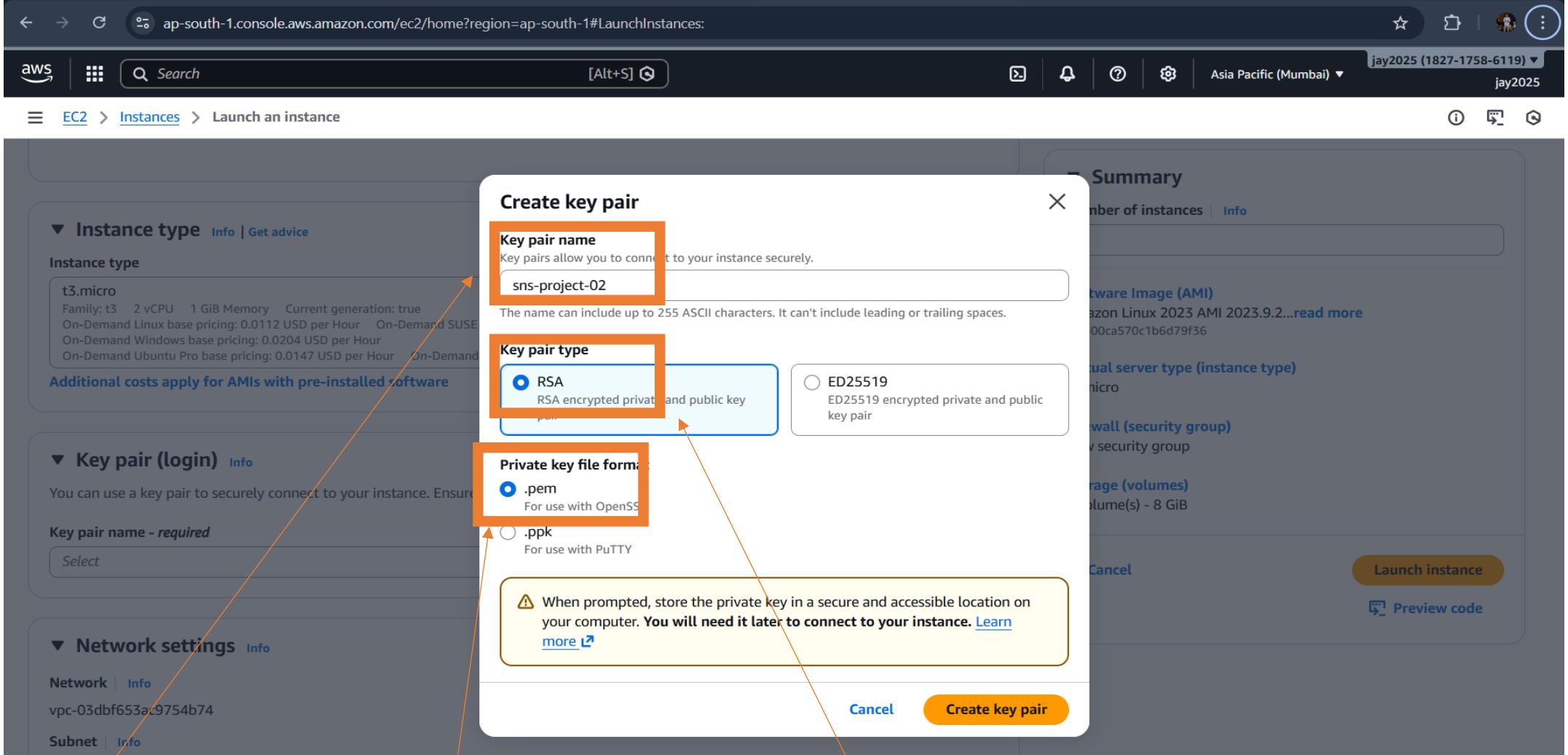
Free tier eligible

[Browse more AMIs](#)

Including AMIs from
AWS, Marketplace and
the Community

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

- Launch a new EC2 instance for file upload testing.
- Select Amazon Linux as the operating system.
- Name the instance **project-sns-01**.



- Generate a key pair named **sns-project-02** for SSH access.
- Choose RSA encryption and format for OpenSSH.
- And creat key pair.

- Select my custom VPC and subnet .
- Enable auto-assign public IP for internet access.
- Apply the existing security group for firewall rules.

Why Use This Step

- Ensures the EC2 instance is placed inside a secure, isolated network.
- Public IP assignment allows external access for uploads and testing.
- Security group rules control inbound/outbound traffic for safe operations.

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

aws | Search [Alt+S] | Asia Pacific (Mumbai) | jay2025 (1827-1758-6119) | jay2025

EC2 > Instances > Launch an instance

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 Edit

Advanced details Info

Domain join directory | Info Select Create new directory ↗

IAM instance profile | Info jay-ec2-s3-sns arn:aws:iam::182717586119:instance-profile/jay-ec2-s3-sns Create new IAM profile ↗

Hostname type | Info IP Name

DNS Hostname | Info

Enable IP name IPv4 (A record) DNS requests

Enable resource-based IPv4 (A record) DNS requests

Enable resource-based IPv6 (AAAA record) DNS requests

Summary

Number of instances | Info 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more ami-00ca570c1b6d79f36

Virtual server type (instance type)
t3.micro

Firewall (security group)
raval-ec2-server

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

Cancel Launch instance Preview code

- Attach IAM role to the EC2 instance.

Why Use This Step

- IAM role gives EC2 permission to access S3 and publish to SNS.

- And click on Lanch instance and connect to powershell

```
ec2-user@ip-10-0-1-115:~      + | ~
PS C:\Users\JAY\downloads> ssh -i "sns-project-02.pem" ec2-user@3.6.40.217
The authenticity of host '3.6.40.217 (3.6.40.217)' can't be established.
ED25519 key fingerprint is SHA256:fESsGr202/f400BFndevb9TIQWZh19g6/qJUGvu3uY4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.6.40.217' (ED25519) to the list of known hosts.

          #_
  ~\_\_ #####_      Amazon Linux 2023
  ~~ \_\#\#\#\#
  ~~ \#\#\#
  ~~ \#/  _--> https://aws.amazon.com/linux/amazon-linux-2023
  ~~ V~' '-->
  ~~~   /
  ~~.~. /-
  ~/m/' /-
[ec2-user@ip-10-0-1-115 ~]$
```

- Use the key file to securely connect to EC2.
- Run the SSH command with my public IP and username.
- Confirm login to Amazon Linux terminal for testing.

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](#)

- Click on create bucket

ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1

aws Search [Alt+S] Asia Pacific (Mumbai) jay2025 (1827-1758-6119) jay2025

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
sns-project-bucket

Bucket name must be unique and can contain lowercase letters or numbers. 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

- Create a general-purpose bucket named .
- Select region for storage location.
- Use default settings for object ownership and access control.

Why Use This Step

- S3 stores uploaded files that trigger SNS notifications.
- Buckets are scalable, durable, and accessible from EC2.
- Region selection ensures low latency and compliance.

ap-south-1.console.aws.amazon.com/s3/buckets?region=ap-south-1

aws Search [Alt+S] Asia Pacific (Mumbai) jay2025 (1827-1758-6119) jay2025

Amazon S3 > Buckets

Successfully created bucket "jay-projectfile-bucket"
To upload files and folders, or to configure additional bucket settings, choose View details.

General purpose buckets All AWS Regions Directory buckets

General purpose buckets (1) Info

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	Creation date
jay-projectfile-bucket	Asia Pacific (Mumbai) ap-south-1	December 30, 2025, 16:39:29 (UTC+05:30)

Copy ARN Empty Delete Create bucket

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.

- Confirms successful creation of **jay-projectfile-bucket**
- Bucket is now ready to receive file uploads from EC2.

```
ec2-user@ip-10-0-1-115:~      X + 
Error: Unable to find a match: python3-pip
[ec2-user@ip-10-0-1-115 ~]$ sudo yum install -y python3 python3-pip
Last metadata expiration check: 0:01:12 ago on Tue Dec 26 11:10:34 2023.
Package python3-3.9.25-1.amzn2023.0.1.x86_64 is already installed.
Dependencies resolved.
=====
 Package           Architecture   Version            Repository      Size
=====
Installing:
python3-pip        noarch       21.3.1-2.amzn2023.0.14    amazonlinux    1.8 M
Installing weak dependencies:
libxcrypt-compat  x86_64       4.4.33-7.amzn2023          amazonlinux   92 k
Transaction Summary
=====
Install 2 Packages

Total download size: 1.9 M
Installed size: 11 M
Downloading Packages:
(1/2): libxcrypt-compat-4.4.33-7.amzn2023.x86_64.rpm           2.6 MB/s |  92 kB     00:00
(2/2): python3-pip-21.3.1-2.amzn2023.0.14.noarch.rpm           35 MB/s | 1.8 MB     00:00
Total                                         22 MB/s | 1.9 MB     00:00

Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : libxcrypt-compat-4.4.33-7.amzn2023.x86_64           1/2
Installing : python3-pip-21.3.1-2.amzn2023.0.14.noarch           2/2
Running scriptlet: python3-pip-21.3.1-2.amzn2023.0.14.noarch   2/2
Verifying  : libxcrypt-compat-4.4.33-7.amzn2023.x86_64           1/2
Verifying  : python3-pip-21.3.1-2.amzn2023.0.14.noarch           2/2

Installed:
libxcrypt-compat-4.4.33-7.amzn2023.x86_64                  python3-pip-21.3.1-2.amzn2023.0.14.noarch

Complete!
```

- Run `sudo yum install -y python3 python3-pip` to install pip.
- pip allows you to install Python packages like boto3.

Why Use This Step

- Python and pip are needed to write and run upload scripts.

```
ec2-user@ip-10-0-1-115:~ pip3 install flask boto3
Defaulting to user install because normal site-packages is not writeable
Collecting flask
  Downloading flask-3.1.2-py3-none-any.whl (103 kB)
    |████████| 103 kB 17.5 MB/s
Collecting boto3
  Downloading boto3-1.42.18-py3-none-any.whl (140 kB)
    |████████| 140 kB 33.7 MB/s
Collecting click>=8.1.3
  Downloading click-8.1.8-py3-none-any.whl (98 kB)
    |████████| 98 kB 13.5 MB/s
Collecting werkzeug>=3.1.0
  Downloading werkzeug-3.1.4-py3-none-any.whl (224 kB)
    |████████| 224 kB 80.7 MB/s
Collecting blinker>=1.9.0
  Downloading blinker-1.9.0-py3-none-any.whl (8.5 kB)
Collecting jinja2>=3.1.2
  Downloading jinja2-3.1.6-py3-none-any.whl (134 kB)
    |████████| 134 kB 125.9 MB/s
Collecting importlib-metadata>=3.6.0
  Downloading importlib_metadata-8.7.1-py3-none-any.whl (27 kB)
Collecting markupsafe>=2.1.1
  Downloading markupsafe-3.0.3-cp39-cp39-manylinux2014_x86_64.manylinux_2_17_x86_64.manylinux_2_28_x86_64.whl (20 kB)
Collecting itsdangerous>=2.2.0
  Downloading itsdangerous-2.2.0-py3-none-any.whl (16 kB)
Collecting botocore<1.43.0,>=1.42.18
  Downloading botocore-1.42.18-py3-none-any.whl (14.5 MB)
    |████████| 14.5 MB 117.5 MB/s
Collecting s3transfer<0.17.0,>=0.16.0
  Downloading s3transfer-0.16.0-py3-none-any.whl (86 kB)
    |████████| 86 kB 11.2 MB/s
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/lib/python3.9/site-packages (from boto3) (0.10.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3.9/site-packages (from botocore<1.43.0,>=1.42.18->boto3) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3.9/site-packages (from botocore<1.43.0,>=1.42.18->boto3) (1.25.10)
Collecting zipp>=3.20
  Downloading zipp-3.23.0-py3-none-any.whl (10 kB)
Requirement already satisfied: six>=1.5 in /usr/lib/python3.9/site-packages (from python-dateutil<3.0.0,>=2.1->botocore<1.43.0,>=1.42.18->boto3) (1.15.0)
Installing collected packages: zipp, markupsafe, botocore, werkzeug, s3transfer, jinja2, itsdangerous, importlib-metadata, click, blinker, flask, boto3
Successfully installed blinker-1.9.0 boto3-1.42.18 botocore-1.42.18 click-8.1.8 flask-3.1.2 importlib-metadata-8.7.1 itsdangerous-2.2.0 jinja2-3.1.6 markupsafe-3.0.3 s3transfer-0.16.0 werkzeug-3.1.4 zipp-3.23.0
[ec2-user@ip-10-0-1-115 ~]$
```

- Run [pip3 install flask boto3](#) on EC2 terminal.
- Flask is used to build a simple web interface.
- boto3 is the AWS SDK for Python to access S3 and SNS.

Why Use This Step

- Flask lets you create a lightweight upload form or API.
- boto3 enables your Python code to interact with AWS services.

```
[ec2-user@ip-10-0-1-115 ~]$ cd myapp
[ec2-user@ip-10-0-1-115 myapp]$ cat > myapp.py << 'EOF'
> from flask import Flask, request          # Import Flask and request object for handling HTTP and file uploads
import boto3, os                           # boto3 for AWS API calls, os for environment variables

# Get bucket name from environment variable; default to your bucket if env var is not set
BUCKET = os.environ.get("UPLOAD_BUCKET", "project-file-upload-bucket-vighnesh")

app = Flask(__name__)                      # Create Flask application instance
s3 = boto3.client("s3")                    # Create an S3 client using EC2 IAM role credentials

# Simple HTML form for uploading a file
FORM = """
<h2>Upload file</h2>
<form method="post" enctype="multipart/form-data">
  <input type="file" name="file">
  <button type="submit">Upload</button>
</form>
"""

@app.route("/", methods=["GET", "POST"]) # Define route for "/" that supports GET and POST
def upload():
    if request.method == "POST":           # If this is a form submission
        f = request.files.get("file")      # Retrieve the uploaded file from the form
        if not f or f.filename == "":       # Basic validation: no file selected
            return "No file selected", 400
        key = f"uploads/{f.filename}"       # Build S3 object key inside 'uploads/' prefix
        # Upload the file object directly to S3 using streaming API
        s3.upload_fileobj(f, BUCKET, key)
        # Return a simple confirmation message with full S3 URI
        return f"Uploaded to s3://{BUCKET}/{key}"
    # For GET requests, just show the upload form
    return FORM

if __name__ == "__main__":
    # Start the Flask development server, listening on all interfaces, port 5000
```

- Create a Python script using Flask and boto3.
- Build a simple web form to upload files.

Why Use This Step

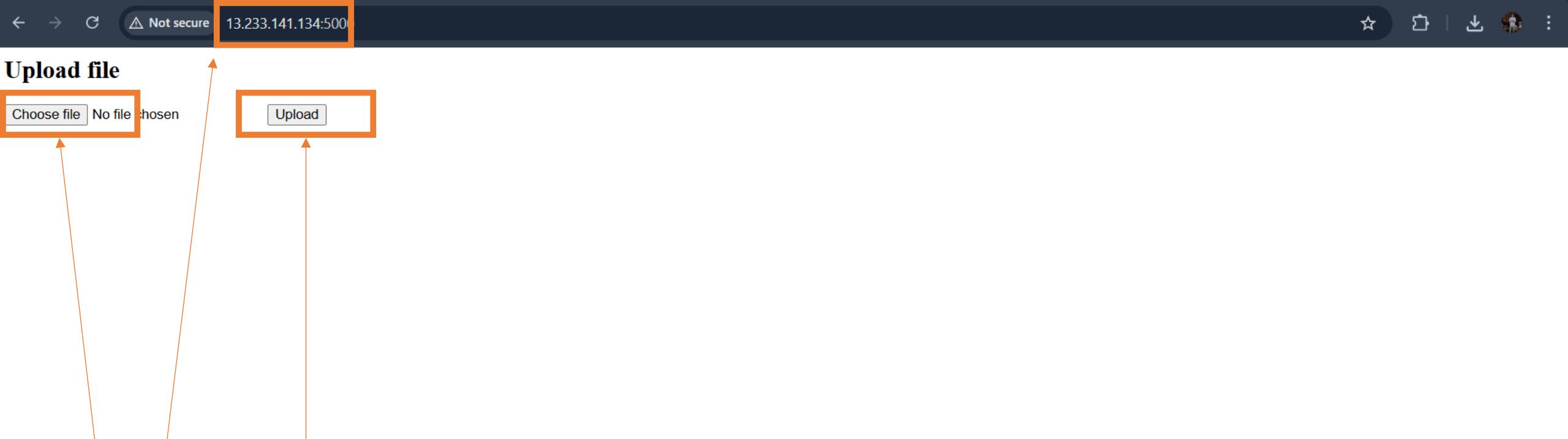
- Flask provides a clean interface for file uploads.
- boto3 handles secure S3 uploads using EC2 IAM role.

```
[ec2-user@ip-10-0-1-115 myapp]$ python3 myapp.py &
[1] 2741
[ec2-user@ip-10-0-1-115 myapp]$ /home/ec2-user/.local/lib/python3.9/site-packages/boto3/compat.py:89: PythonDeprecationWarning: Boto3 will no longer support Python 3.9 starting April 29, 2026. To continue receiving service updates, bug fixes, and security updates please upgrade to Python 3.10 or later. More information can be found here: https://aws.amazon.com/blogs/developer/python-support-policy-updates-for-aws-sdks-and-tools/
  warnings.warn(warning, PythonDeprecationWarning)
* Serving Flask app 'myapp'
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5000
* Running on http://10.0.1.115:5000
Press CTRL+C to quit
```

- Start the Flask app using .
- App runs on port 5000 and listens on all interfaces.
- Accessible via EC2 public IP for file uploads.

Why Use This Step

- Launches the upload interface for testing S3 integration.



- Open my EC2 public ip with :5000 port no in browser.
- Use the form to select and upload a file.
- The file will be sent to S3 bucket via Flask + boto3.

Why Use This Step

- Confirms your EC2 app is publicly accessible.
- Allows manual testing of file uploads to S3.

ap-south-1.console.aws.amazon.com/s3/buckets/jay-projectfile-bucket?region=ap-south-1&tab=objects

aws Search [Alt+S] Asia Pacific (Mumbai) jay2025 (1827-1758-6119) jay2025

Amazon S3 > Buckets > jay-projectfile-bucket

Amazon S3

Buckets

- General purpose buckets
- Directory buckets
- Table buckets
- Vector buckets [New](#)

Access management and security

- Access Points
- Access Points for FSx
- Access Grants
- IAM Access Analyzer

Storage management and insights

- Storage Lens
- Batch Operations

Account and organization settings

AWS Marketplace for S3

jay-projectfile-bucket [Info](#)

Objects | Metadata | Properties | Permissions | Metrics | Management | Access Points

Objects (1) [C](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

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](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	uploads/	Folder	-	-	-

- Open the S3 **bucket jay-projectfile-bucket** in AWS Console.
- Confirm the uploads/ folder was created.

Application Integration

Amazon Simple Notification Service

Pub/sub messaging for microservices and serverless applications.

Amazon SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and event-driven serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging.

Create topic

Topic name
A topic is a message channel. When you publish a message to a topic, it fans out the message to all subscribed endpoints.

Next step

[Start with an overview](#)

Pricing

Amazon SNS has no upfront costs. You pay based on the number of messages you publish, the number of messages you deliver, and any additional API calls for managing topics and subscriptions. Delivery pricing varies by endpoint type.

Benefits and features

Reliably deliver messages with durability Automatically scale your workload

- Go to Amazon SNS and click “Create topic.”
 - Enter a topic name **jay-upload-alert**
- Why Use This Step**
- SNS enables real-time alerts when files are uploaded to S3.

ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/create-topic

aws | Search [Alt+S] Asia Pacific (Mumbai) jay2025

Amazon SNS > Topics > Create topic

Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

▼ Access policy - optional [Info](#)

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

Choose method

Basic
Use simple criteria to define a basic access policy.

Advanced
Use a JSON object to define an advanced access policy.

JSON editor

```
1 {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "OwnerPermissions",
6             "Effect": "Allow",
7             "Principal": {
8                 "AWS": "arn:aws:iam::586549103866:root"
9             },
10            "Action": [
11                "SNS:GetTopicAttributes",
12                "SNS:SetTopicAttributes",
13                "SNS:AddPermission",
14                "SNS:RemovePermission",
15                "SNS:DeleteTopic",

```

► Data protection policy - optional [Info](#)

The screenshot shows the AWS SNS 'Create topic' interface. The 'Access policy' section is open, showing two options: 'Basic' and 'Advanced'. The 'Advanced' option is selected and highlighted with an orange box. Below it is a 'JSON editor' containing a sample JSON policy. A large orange rectangle highlights the entire JSON editor area, and two orange arrows point upwards from the 'Data protection policy' section towards the JSON editor.

- Use the “Advanced” option to write a custom JSON policy.
- Grant permissions to IAM user or root account.
- Allow actions like GetTopicAttributes, SetTopicAttributes, and DeleteTopic.

Why Use This Step

- Controls who can manage and interact with SNS topic.
- Ensures only trusted identities can modify or delete the topic.
- Prepares the topic for secure integration with S3 notifications.

← → ⌂ ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/topics

aws | Search [Alt+S] ⓘ | Asia Pacific (Mumbai) ▾ jay2025 (1827-1758-6119) ▾ jay2025

Amazon SNS Topics

New Feature Amazon SNS now supports High Throughput FIFO topics. [Learn more ↗](#)

Topics (1)

Name	Type	ARN
jay-upload-alerts	Standard	arn:aws:sns:ap-south-1:182717586119:jay-upload-a...

Search

Edit Delete Publish message Create topic

< 1 > ⚙

The screenshot shows the AWS SNS Topics page. On the left, there's a sidebar with 'Amazon SNS' and 'Mobile' sections. The 'Topics' section is selected. The main area displays a blue banner about High Throughput FIFO topics. Below it, a table lists one topic: 'jay-upload-alerts'. The table has columns for Name, Type, and ARN. The 'Name' column contains a link to the topic details. An orange arrow points from the text 'SNS topic jay-upload-alerts created successfully.' at the bottom to the 'jay-upload-alerts' link in the table.

- SNS topic **jay-upload-alerts** created successfully.

AWS | Search [Alt+S] ⓘ | Asia Pacific (Mumbai) ▾ jay2025 (1827-1758-6119) ▾ jay2025

Amazon SNS > Subscriptions

Amazon SNS X

Dashboard

Topics

Subscriptions

▼ Mobile

Push notifications

Text messaging (SMS)

New Feature
Amazon SNS now supports High Throughput FIFO topics. [Learn more ↗](#)

Subscriptions (0)

Edit Delete Request confirmation Confirm subscription **Create subscription**

Search

ID	Endpoint	Status	Protocol	Topic
No subscriptions found				

Create subscription

Click Create subscription

Details

Topic ARN
arn:aws:sns:ap-south-1:182717586119:jay-upload-alert X

Protocol
The type of endpoint to subscribe
Email ▼

Endpoint
An email address that can receive notifications from Amazon SNS.
jr012fail@gmail.com

i After your subscription is created, you must confirm it. [Info](#)

► **Subscription filter policy - optional** [Info](#)
This policy filters the messages that a subscriber receives.

► **Redrive policy (dead-letter queue) - optional** [Info](#)
Send undeliverable messages to a dead-letter queue.

[Cancel](#) Create subscription

- Subscribe to topic **jay-upload-alert** using protocol: Email.
- Enter email address as the endpoint.
- Confirm the subscription via the email link sent by AWS.

Why Use This Step

- Enables real-time email alerts when files are uploaded to S3.

← → C ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/subscriptions

aws | Search [Alt+S] | [Alt+S] | Asia Pacific (Mumbai) | jay2025 (1827-1758-6119) | jay2025

Amazon SNS Subscriptions

New Feature
Amazon SNS now supports High Throughput FIFO topics. [Learn more ↗](#)

Subscriptions (1)

Edit Delete Request confirmation Confirm subscription Create subscription

Search

ID	Endpoint	Status	Protocol	Topic
1c6ead81-1c78-4f07-8ea0-...	jr012fail@gmail.com	Confirmed	EMAIL	jay-upload-alerts

< 1 > |

The screenshot shows the AWS SNS Subscriptions page. On the left, there's a navigation sidebar with 'Amazon SNS' at the top, followed by 'Dashboard', 'Topics', 'Subscriptions' (which is selected and highlighted in blue), and 'Mobile' with 'Push notifications' and 'Text messaging (SMS)' options. The main content area has a blue header bar with the text 'New Feature' and a link to learn more about High Throughput FIFO topics. Below this is a table titled 'Subscriptions (1)'. The table has columns for ID, Endpoint, Status, Protocol, and Topic. A single row is listed, showing an ID starting with '1c6ead81', an endpoint of 'jr012fail@gmail.com', a status of 'Confirmed' with a green checkmark, a protocol of 'EMAIL', and a topic of 'jay-upload-alerts'. The entire row is highlighted with an orange border. An orange arrow points from the bottom bullet point in the text below to the 'Status' column of the highlighted row.

- Email subscription to topic **jay-upload-alert** is now confirmed.

AWS Notification - Subscription Confirmation Inbox x**AWS Notifications** <no-reply@sns.amazonaws.com>
to me ▾

Wed, Dec 31, 2025, 4:45 PM (1 day ago)



You have chosen to subscribe to the topic:

arn:aws:sns:ap-south-1:182717586119:jay-upload-alerts

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):

[Confirm subscription](#)Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

- AWS sends a confirmation email to my email.



Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:

arn:aws:sns:ap-south-1:182717586119:jay-upload-alert:aa972abb-649c-4395-a64d-d4a0dec4acdc

If it was not your intention to subscribe, [click here to unsubscribe.](#)

ap-south-1.console.aws.amazon.com/s3/buckets/jay-projectfile-bucket?region=ap-south-1&tab=properties

aws Search [Alt+S] Asia Pacific (Mumbai) jay2025 jay2025

Amazon S3 > Buckets > jay-projectfile-bucket

You can view and configure CloudTrail data events for Amazon S3 bucket object-level operations in the AWS CloudTrail console.

AWS CloudTrail

Event notifications (0)

Send a notification when specific events occur in your bucket. [Learn more](#)

Edit Delete Create event notification

No event notifications

Choose **Create event notification** to be notified when a specific event occurs.

Create event notification

Amazon EventBridge

For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. [Learn more](#) or [see EventBridge pricing](#)

Send notifications to Amazon EventBridge for all events in this bucket

Off

Edit

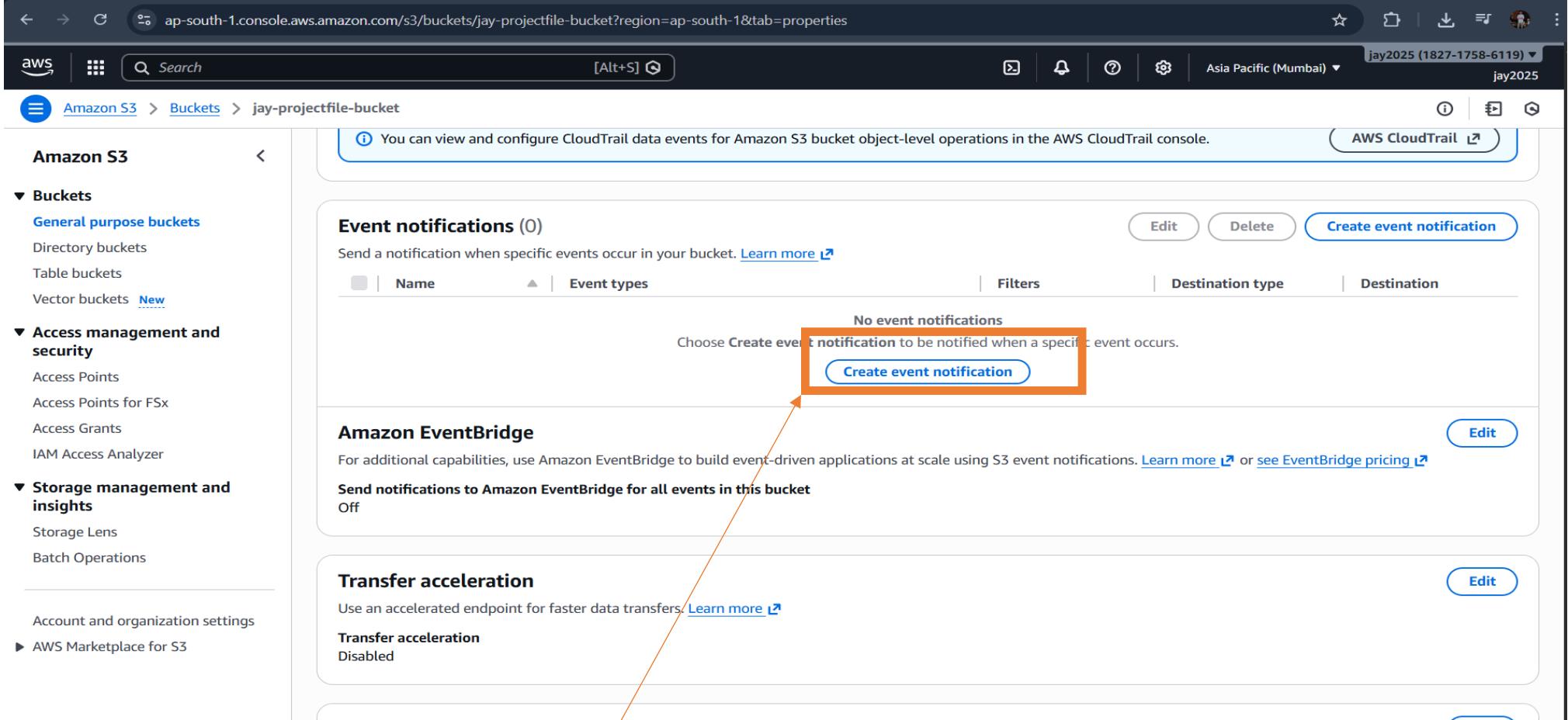
Transfer acceleration

Use an accelerated endpoint for faster data transfers. [Learn more](#)

Transfer acceleration

Disabled

Edit



- Go to the S3 bucket **jay-projectfile-bucket** > Properties > Event notifications.
- Click “Create event notification.”

Why Use This Step

- Automatically triggers SNS alerts when a new file is uploaded.

The screenshot shows the AWS S3 console with the path: Amazon S3 > Buckets > demo-bucket-02020 > Create event notification. The main section is titled 'Create event notification' with a sub-section 'General configuration'. It includes fields for 'Event name' (jay-notify-onuploads), 'Prefix - optional' (uploads/), and 'Suffix - optional' (jpg). Below this is the 'Event types' section, which is currently collapsed. A red box highlights the 'Event name' field, and another red box highlights the 'Prefix' field. An orange arrow points from the 'Event name' field towards the 'Prefix' field.

Create event notification Info

To enable notifications, you must first add a notification configuration that identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications.

General configuration

Event name

jay-notify-onuploads

Event name can contain up to 255 characters.

Prefix - optional

Limit the notifications to objects with key starting with specified characters.

uploads/

Suffix - optional

Limit the notifications to objects with key ending with specified characters.

.jpg

Event types

Specify at least one event for which you want to receive notifications. For each group, you can choose an event type for all events, or you can choose one or more individual events.

Object creation

All object create events

Put

- Event name: jay-notify-onuploads
- Prefix: uploads/ — triggers only for files in the uploads folder
- Event type: All object create events
- Destination: SNS topic

Why Use This Step

- Filters notifications to match specific file types and locations.
- Completes the automation: S3 → SNS → Email alert.

Destination

Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. [Learn more](#)

Destination

Choose a destination to publish the event. [Learn more](#)

Lambda function

Run a Lambda function script based on S3 events.

SNS topic

Fanout messages to systems for parallel processing or directly to people.

SQS queue

Send notifications to an SQS queue to be read by a server.

Specify SNS topic

Choose from your SNS topics

Enter SNS topic ARN

SNS topic

jay-upload-alert

Cancel

Save changes

- Destination type: SNS topic
- Selected topic: **jay-upload-alert**
- Region: Asia Pacific (Mumbai)
- Ensure S3 has permission to publish to the SNS topic

Why Use This Step

- Connects S3 uploads directly to your SNS alert system

Amazon S3 > Buckets > jay-projectfile-bucket

AWS CloudTrail data events

You can view and configure CloudTrail data events for Amazon S3 bucket object-level operations in the AWS CloudTrail console.

[AWS CloudTrail ↗](#)

Event notifications (1)

Send a notification when specific events occur in your bucket. [Learn more ↗](#)

Name	Event types	Filters	Destination type	Destination
jay-notify-onuploads	All object create events	uploads/	SNS topic	jay-upload-alerts ↗

[Edit](#) [Delete](#) [Create event notification](#)

Amazon EventBridge

For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. [Learn more ↗](#) or [see EventBridge pricing ↗](#)

Send notifications to Amazon EventBridge for all events in this bucket

Off [Edit](#)

Transfer acceleration

Use an accelerated endpoint for faster data transfers. [Learn more ↗](#)

Transfer acceleration

Disabled [Edit](#)

Done

Upload file

docker build.pdf



File select and upload to s3



AWS Notifications <no-reply@sns.amazonaws.com>

to me ▾

Wed, Dec 31, 2025, 4:49 PM (1 day ago)

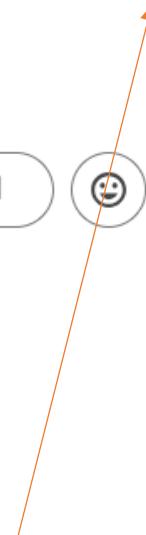


```
{"Records":[{"eventVersion":"2.1","eventSource":"aws:s3","awsRegion":"ap-south-1","eventTime":"2025-12-31T11:19:26.525Z","eventName":"ObjectCreated:Put","userIdentity":{"principalId":"AWS:AROASVCWRDLDVHUPX6DQ:i-000baed15445bf0d1"},"requestParameters":{"sourceIPAddress":"13.233.99.175"},"responseElements":{"x-amz-request-id":"SETKV9ZDKX2WSG6X","x-amz-id-2":"0mCko17VhRldW2qIK0NBrRJB5LktdwRY/Ct/Ga5Eq28f+yvNyLNDXpJFFGjirrytKPYf8IURViYdcnfBskM0LHzNr8kAgZz"},"s3":{"s3SchemaVersion":"1.0","configurationId":"jay-notify-onuploads","bucket":{"name":"jay-projectfile-bucket","ownerIdentity":{"principalId":"ACTB0XIJLYM1B"},"arn":"arn:aws:s3:::jay-projectfile-bucket"},"object":{"key":"uploads/docker+build.pdf","size":307077,"eTag":"e5ca5817d8f5d047833e7c5b56c91f73","sequencer":"00695506BE74A27B4A"}}}}
```

...

Reply

Forward



An email notification is received from AWS SNS.

Thank you.

Presented By
JAY