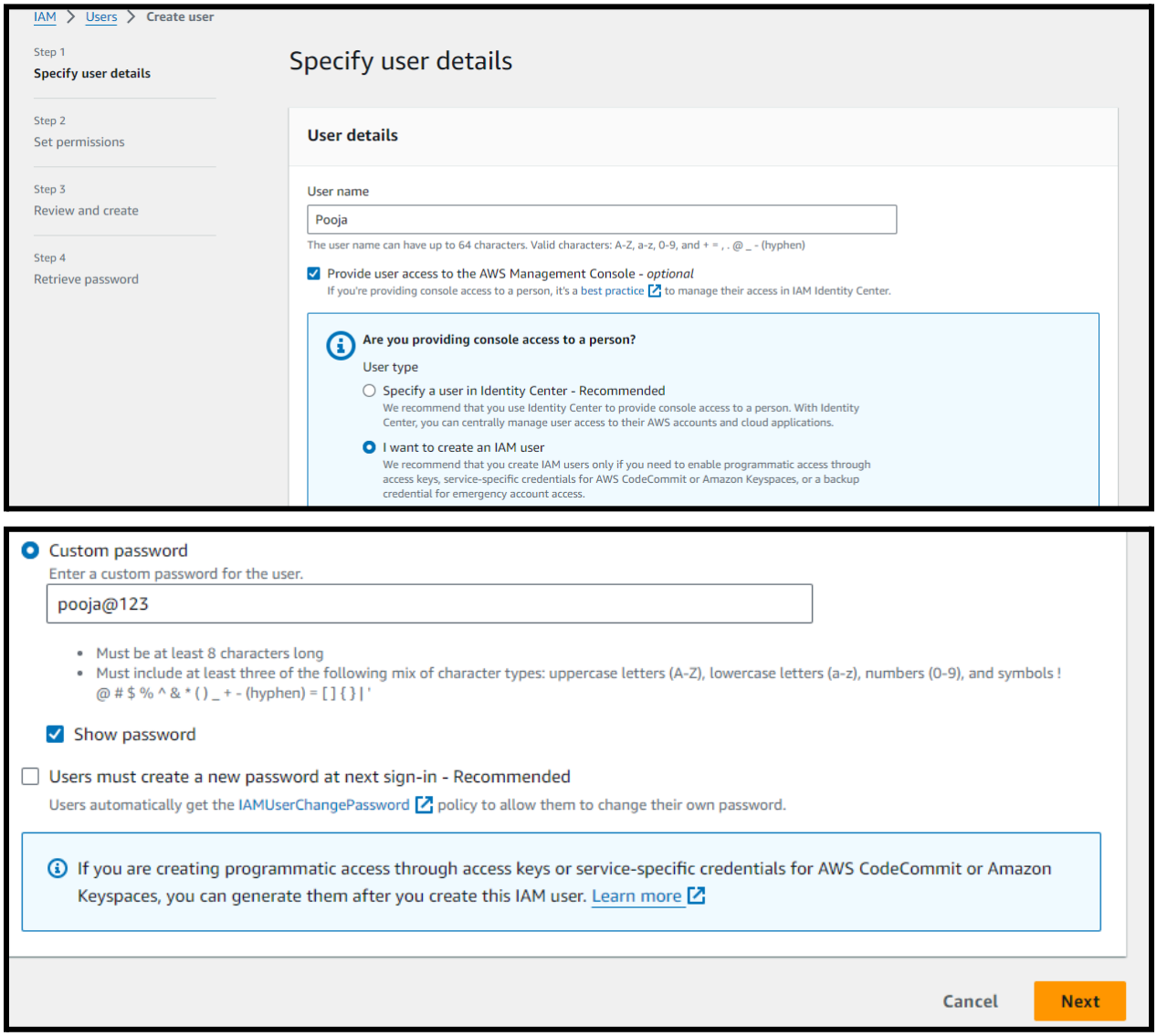
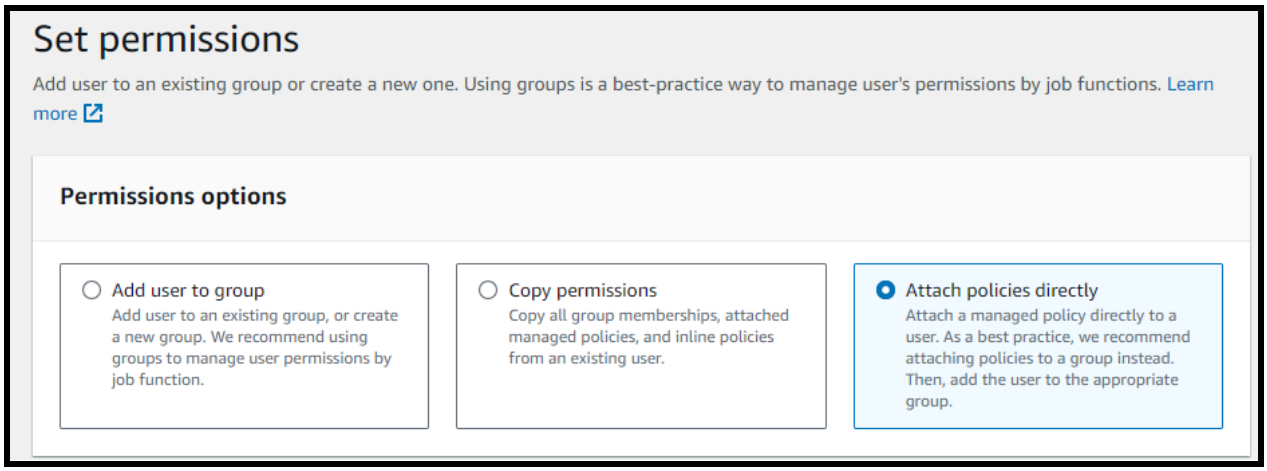
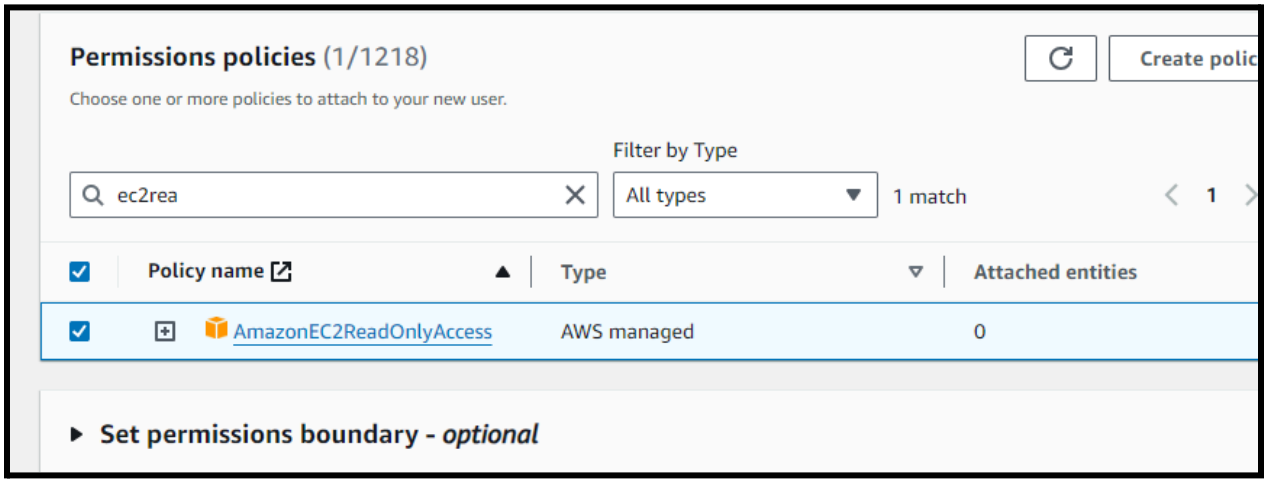
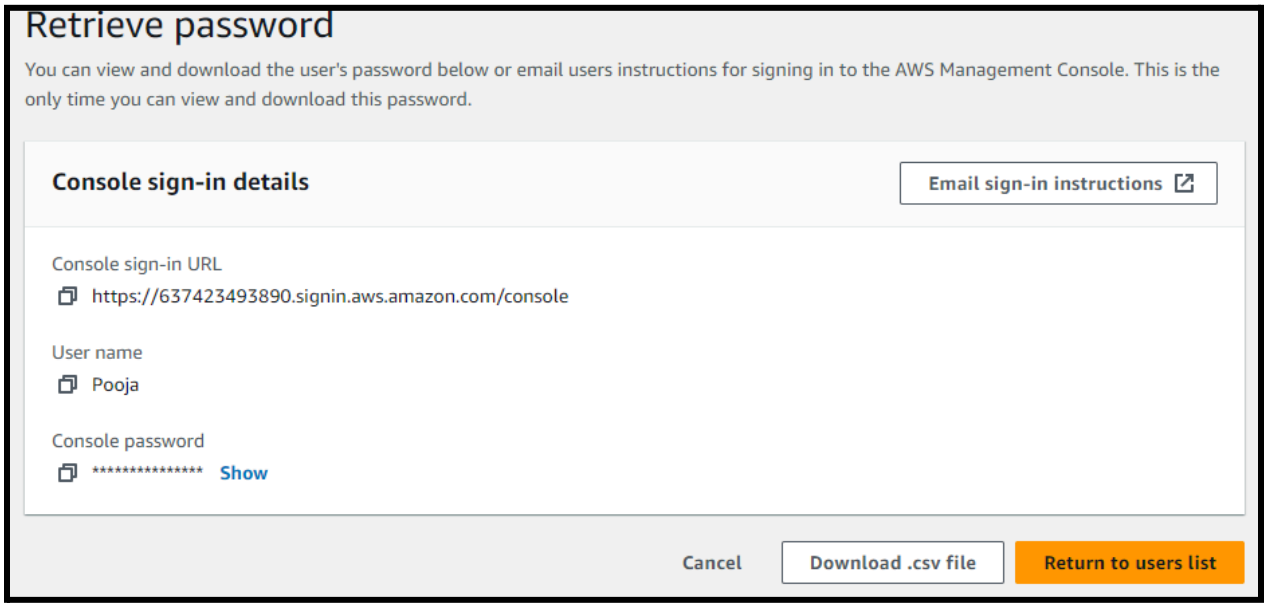
AWS PRACTICAL 02-07-24

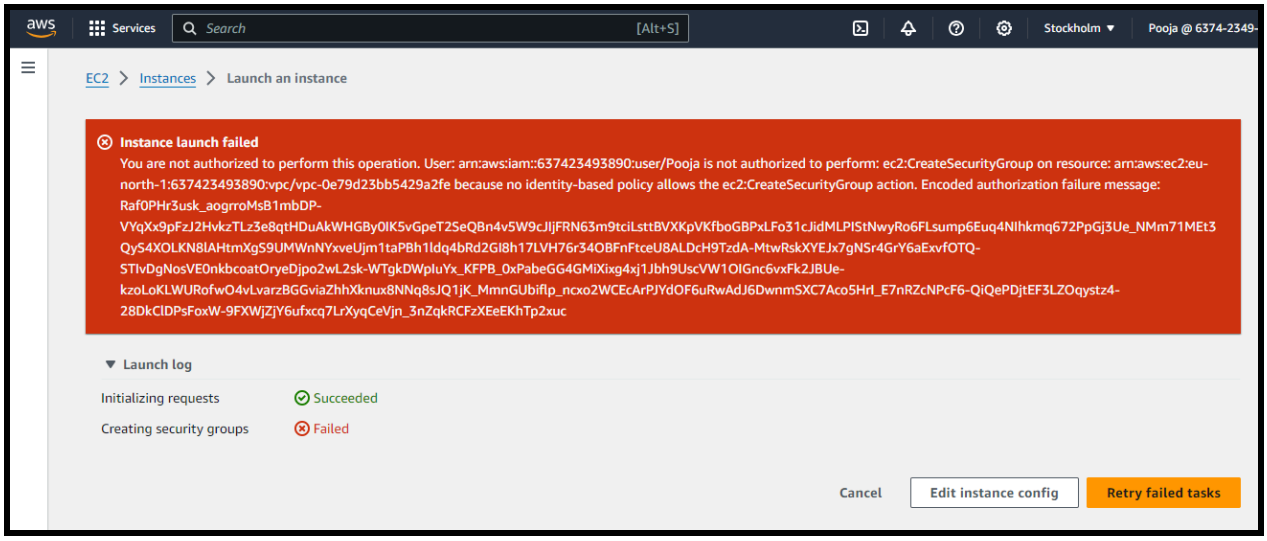




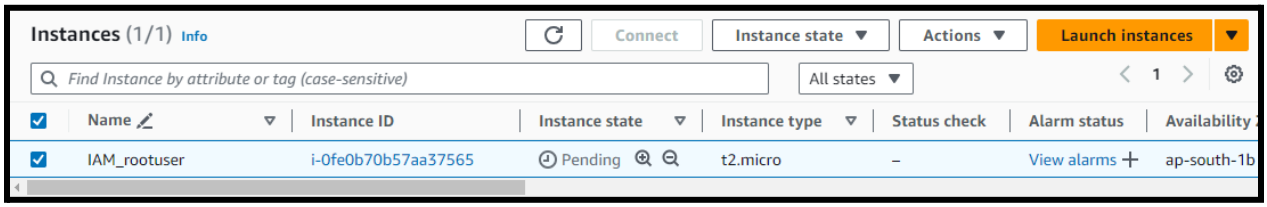


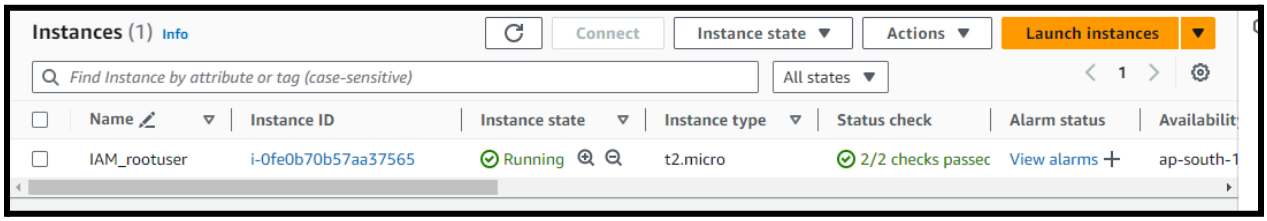


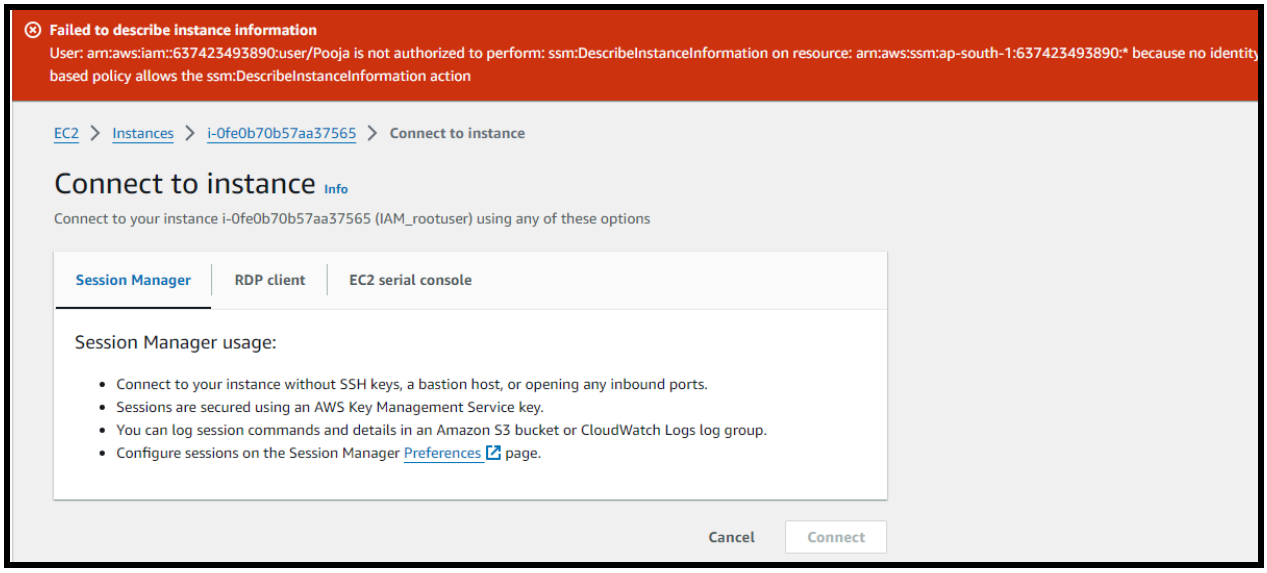
Trying to create an instance



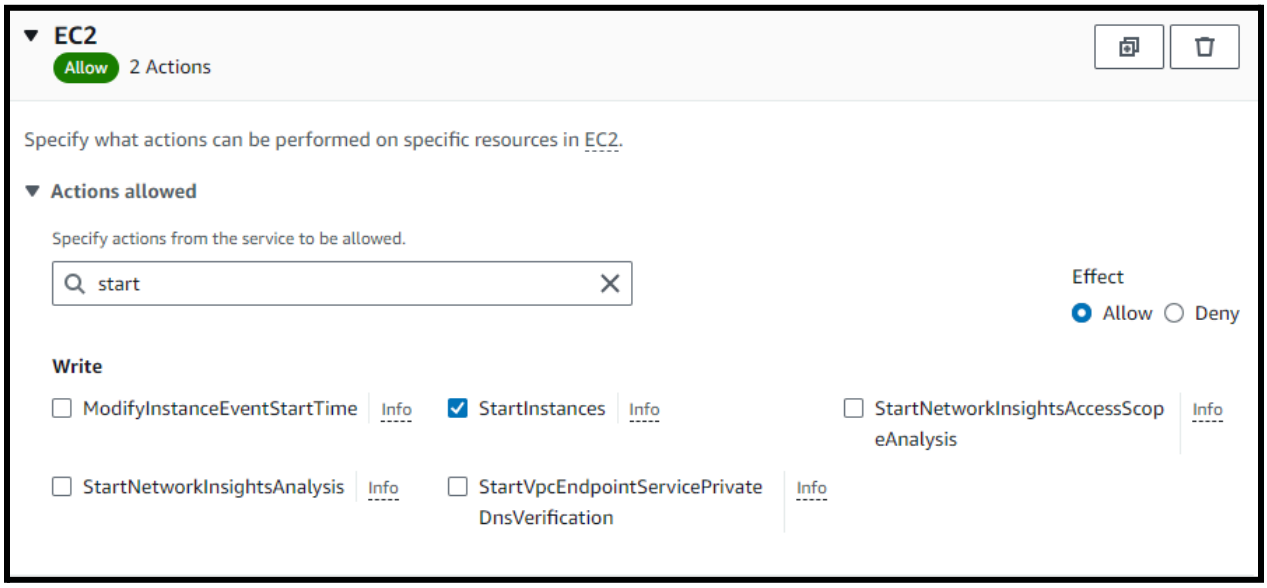
Launch instance in root user

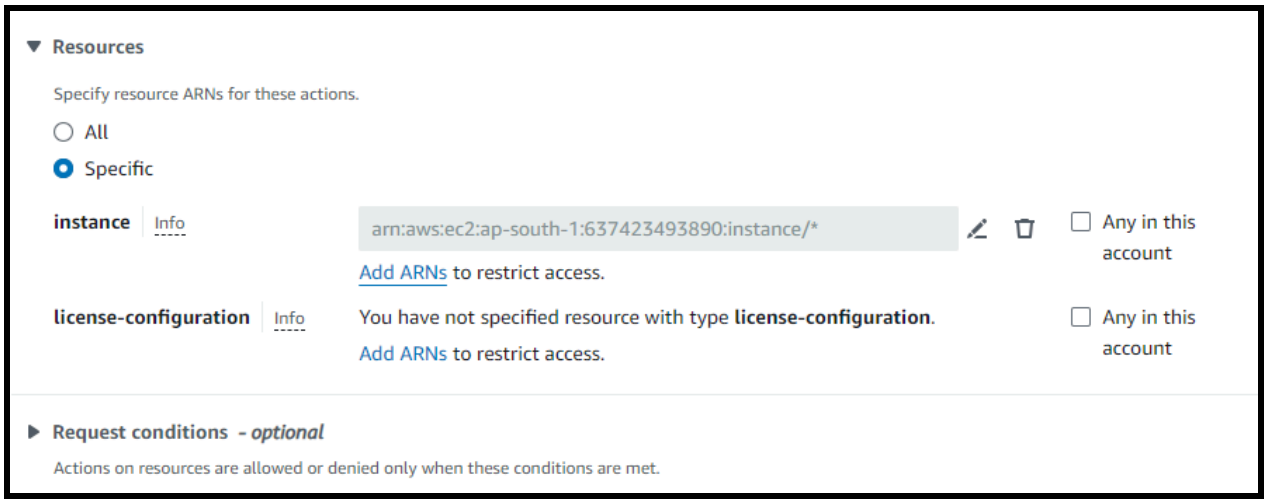


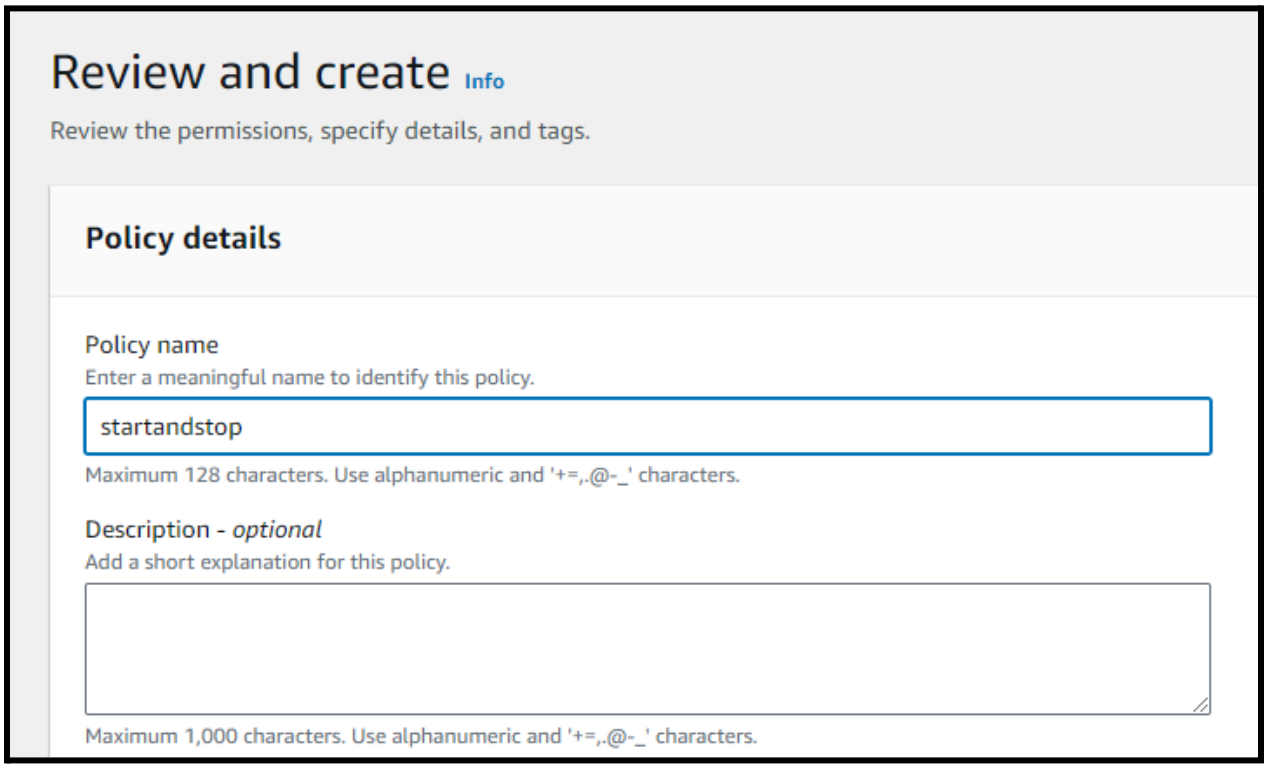


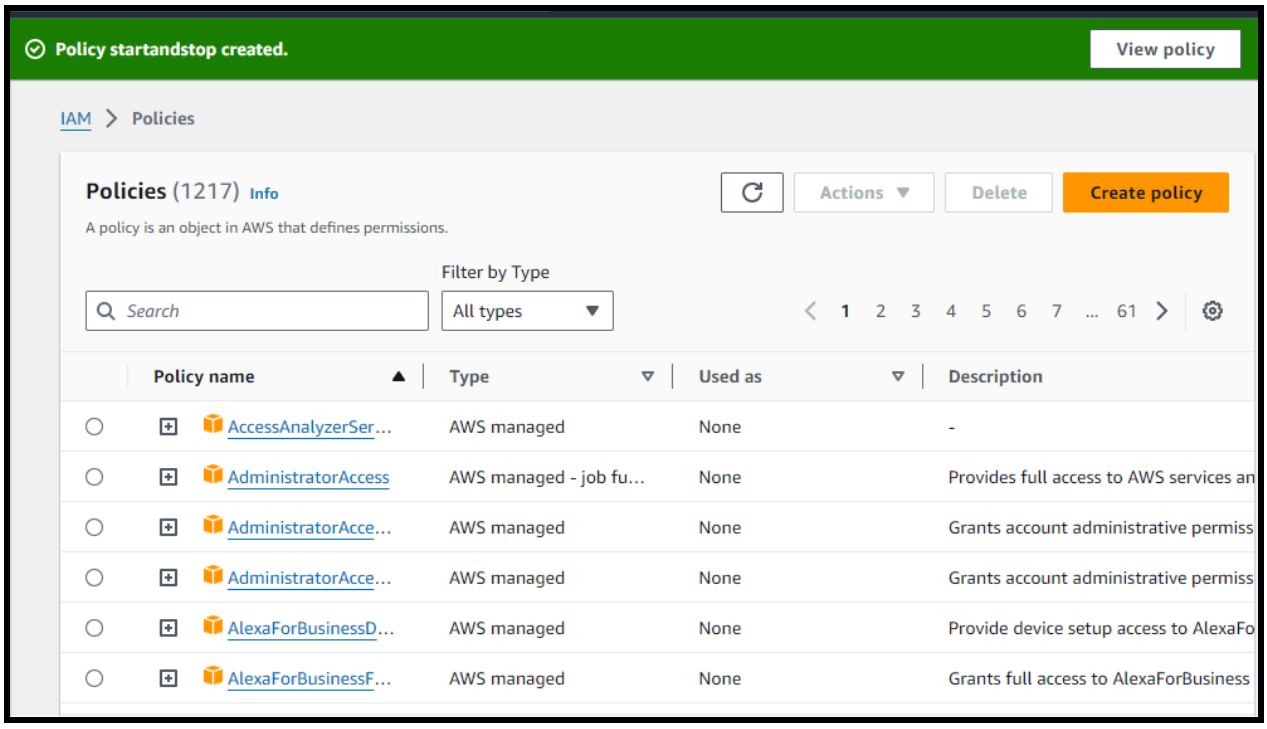


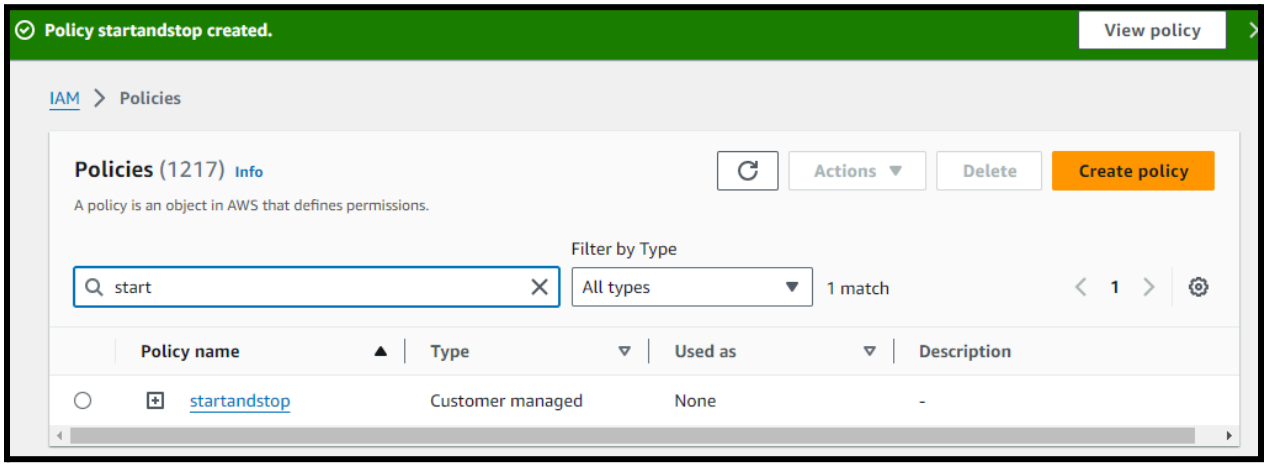
Create policy

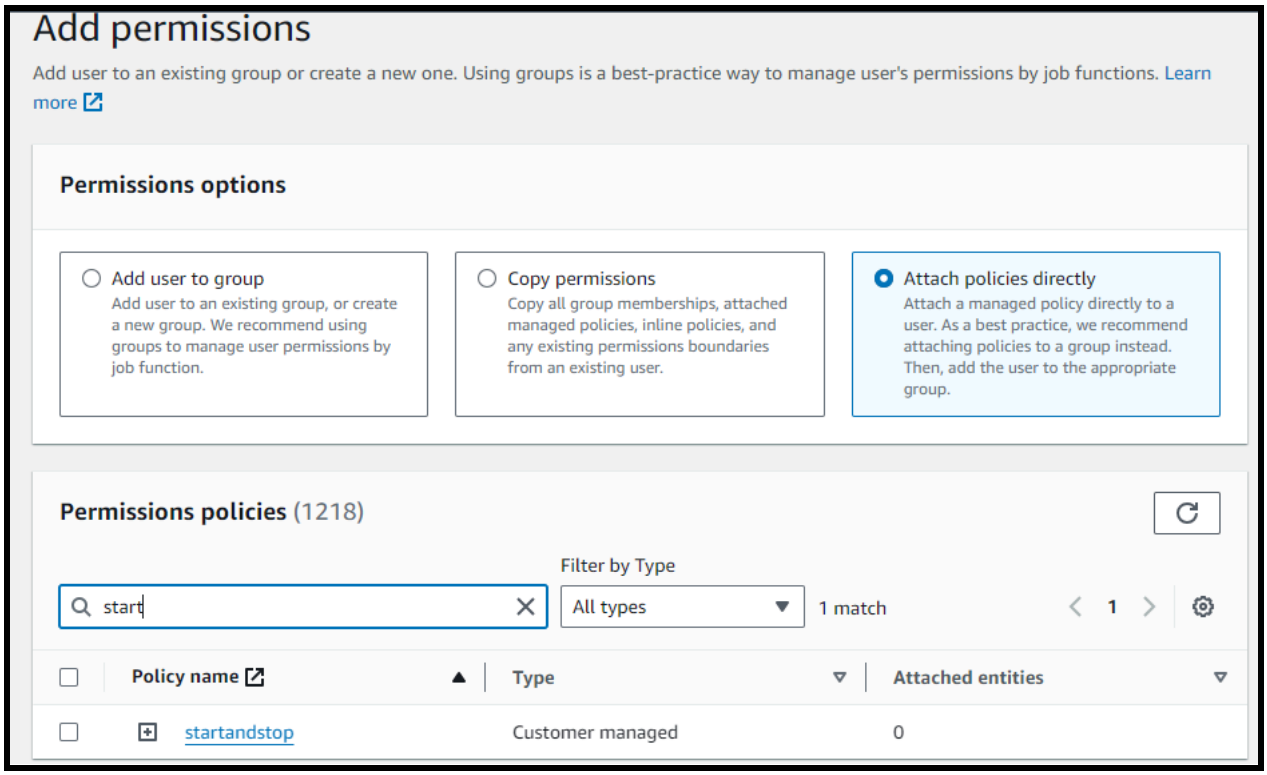


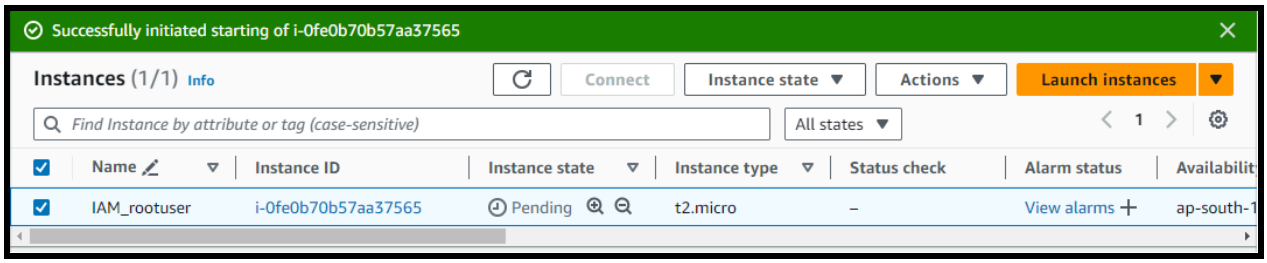

Resources
Specify resource ARNs for these actions.
All
Specific
instance
Info
arn:aws:ec2:ap-south-1:637423493890:instance/*
Add ARNs to restrict access.
Any in this account
license-configuration
Info
You have not specified resource with type license-configuration.
Add ARNs to restrict access.
Any in this account
Request conditions - optional
Actions on resources are allowed or denied only when these conditions are met.

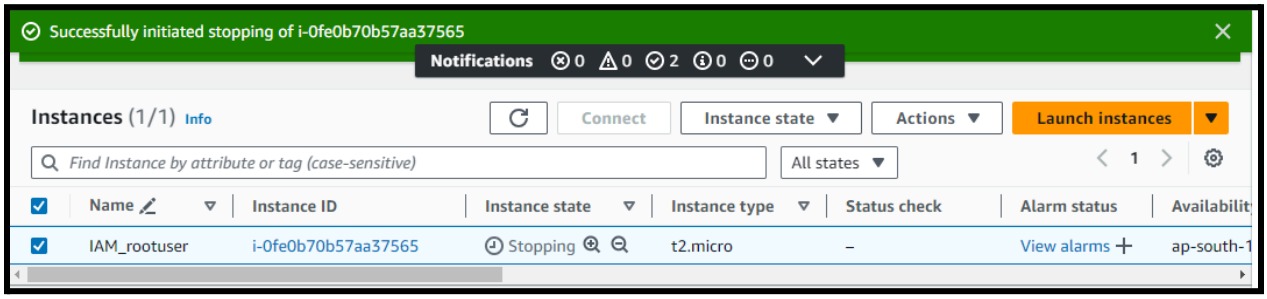

Review and create
Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
startandstop
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

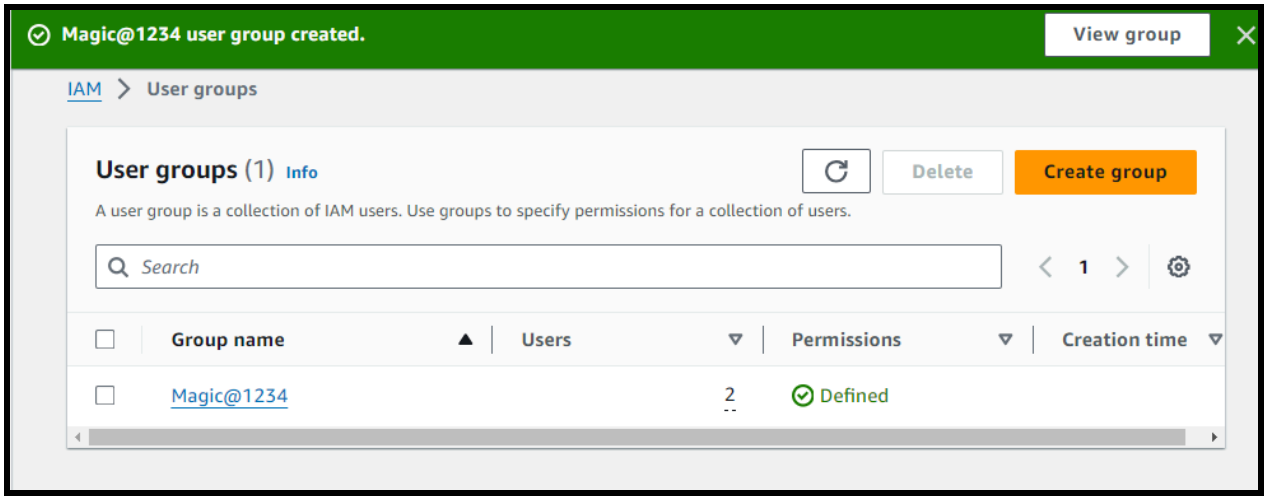

Policy startandstop created.
View policy
IAM > Policies
Policies (1217) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 61
Policy name
Type
Used as
Description
AccessAnalyzerSer...
AWS managed
None
-
AdministratorAccess
AWS managed - job fu...
None
Provides full access to AWS services an
AdministratorAcce...
AWS managed
None
Grants account administrative permiss
AdministratorAcce...
AWS managed
None
Grants account administrative permiss
AlexaForBusinessD...
AWS managed
None
Provide device setup access to AlexaFo
AlexaForBusinessF...
AWS managed
None
Grants full access to AlexaForBusiness

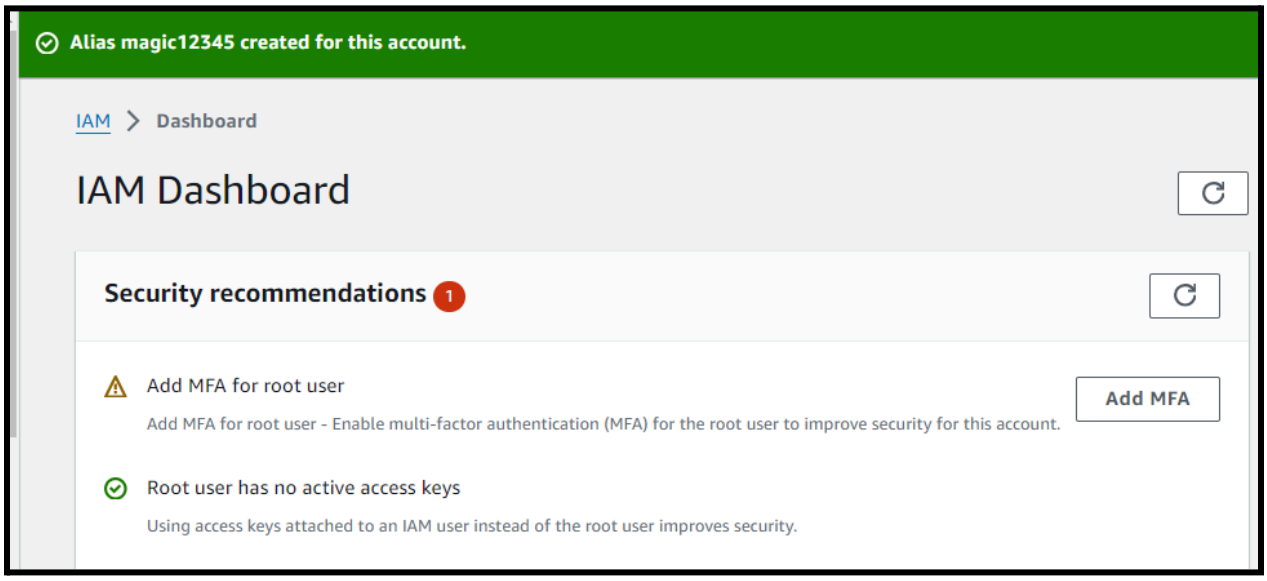

Policy startandstop created.
View policy
IAM > Policies
Policies (1217) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
start
All types
1 match
1
Policy name
Type
Used as
Description
startandstop
Customer managed
None
-

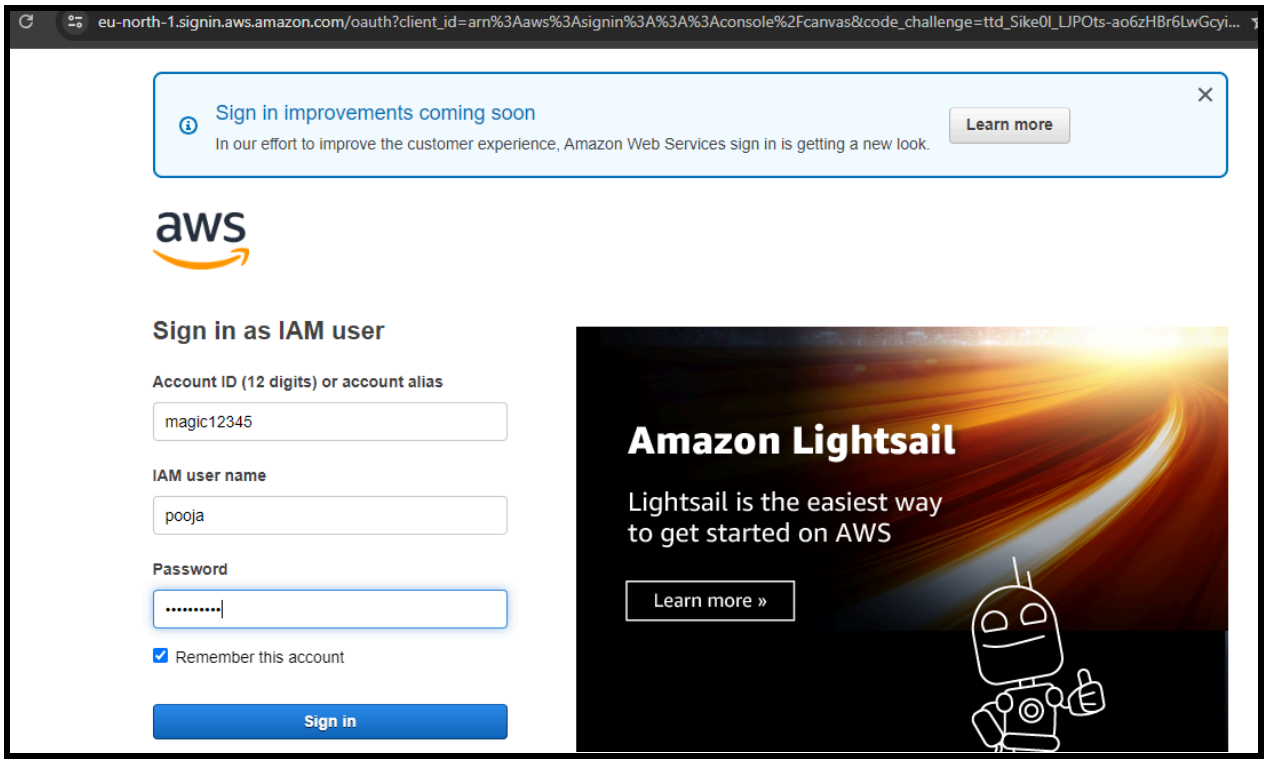

Add permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Permissions policies (1218)
Filter by Type
start
All types
1 match
1
Policy name
Type
Attached entities
startandstop
Customer managed
0

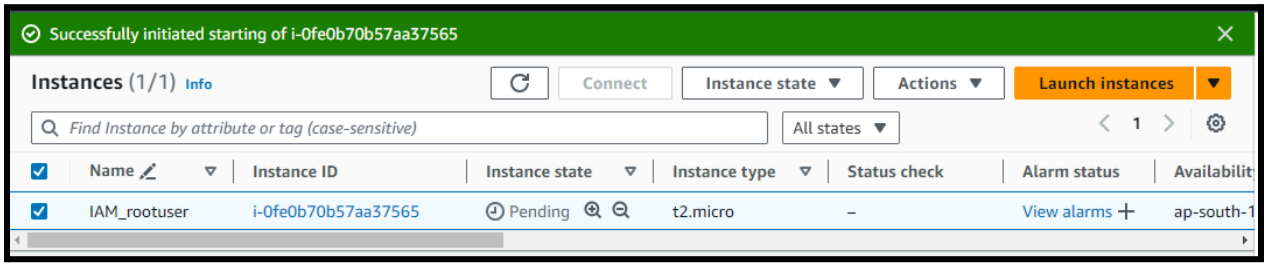

Successfully initiated starting of i-0fe0b70b57aa37565
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availabilit
IAM_rootuser
i-0fe0b70b57aa37565
Pending
t2.micro
–
View alarms
ap-south-1

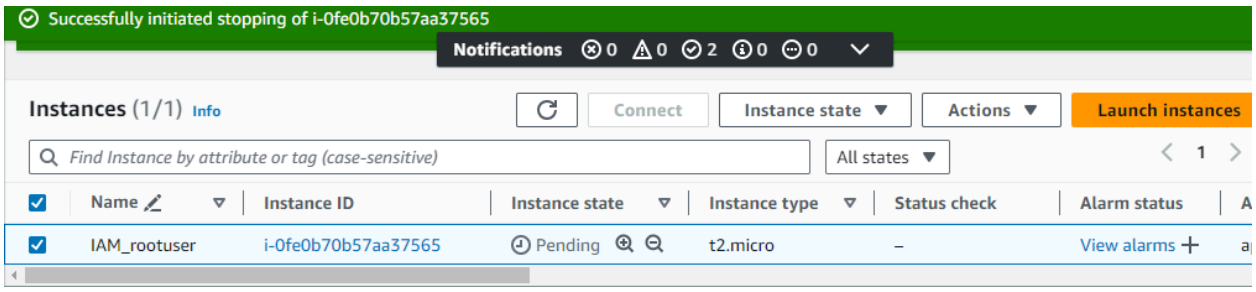

Successfully initiated stopping of i-0fe0b70b57aa37565
Notifications
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availabilit
IAM_rootuser
i-0fe0b70b57aa37565
Stopping
t2.micro
–
View alarms
ap-south-1


Magic@1234 user group created.
View group
IAM
User groups
User groups (1) Info
Delete
Create group
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Search
1
Group name
Users
Permissions
Creation time
Magic@1234
2
Defined

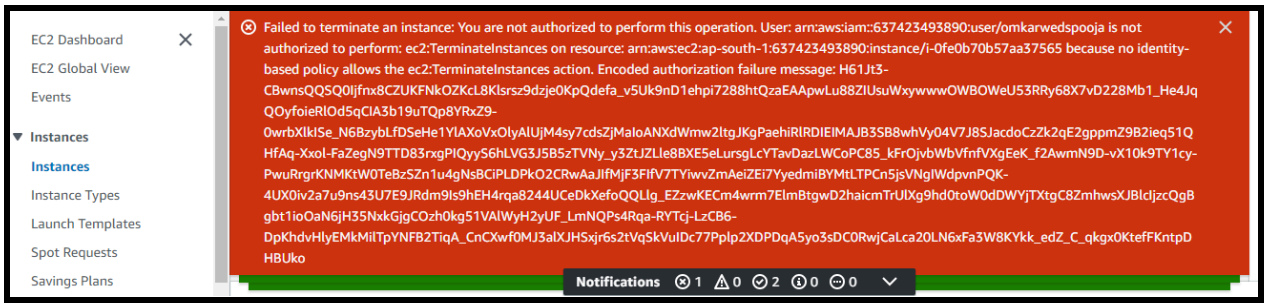

Alias magic12345 created for this account.
IAM
Dashboard
IAM Dashboard
Security recommendations 1
Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.
Add MFA
Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

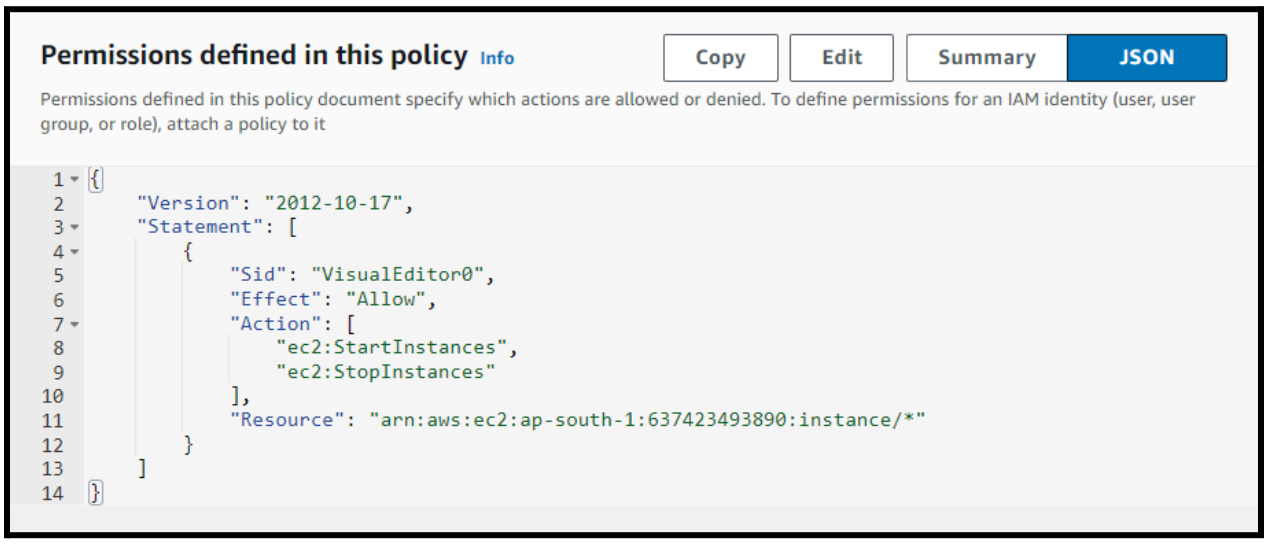






Cannot terminate

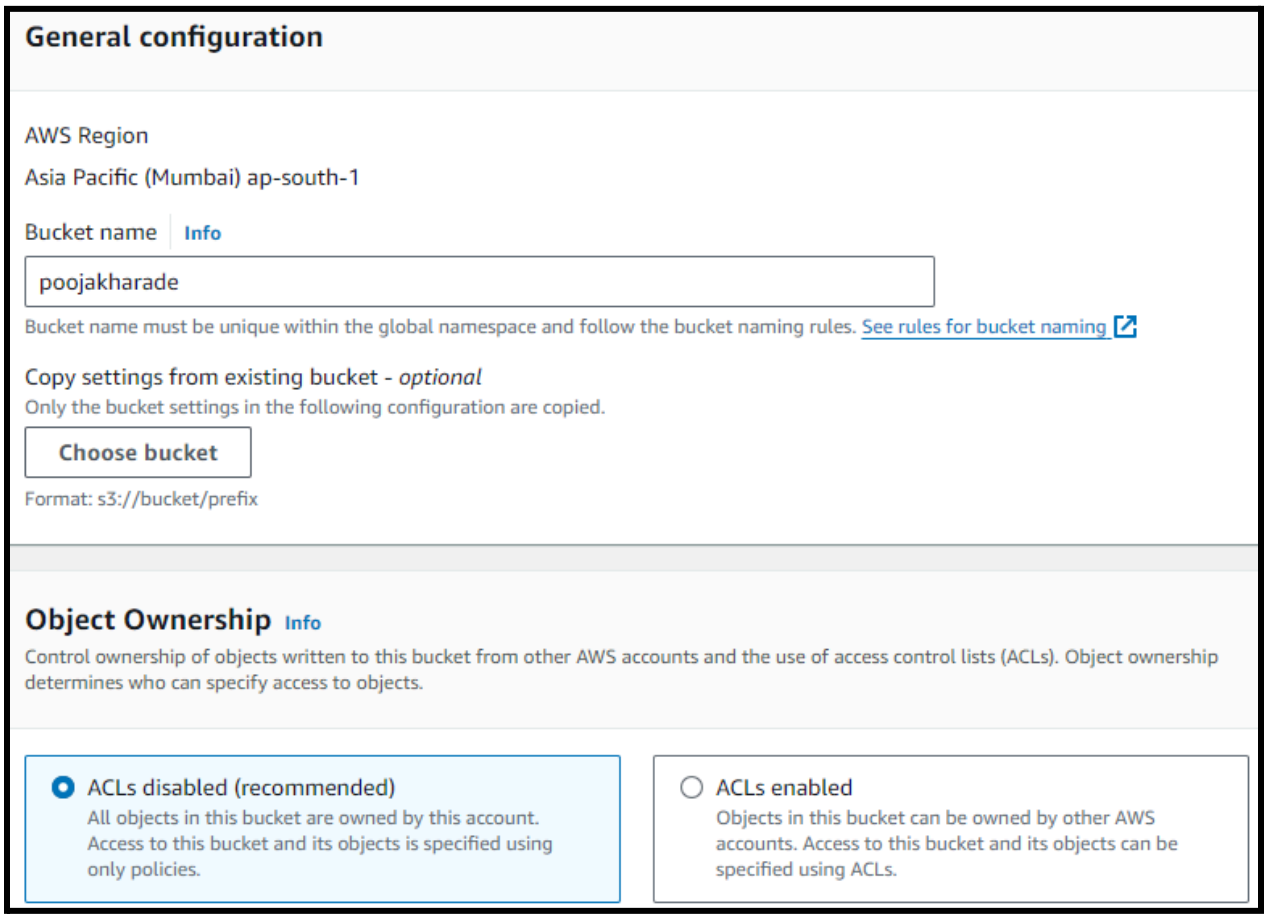

EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Failed to terminate an instance: You are not authorized to perform this operation. User: arn:aws:iam::637423493890:user/omkarwedspooja is not authorized to perform: ec2:TerminateInstances on resource: arn:aws:ec2:ap-south-1:637423493890:instance/i-0fe0b70b57aa37565 because no identity-based policy allows the ec2:TerminateInstances action. Encoded authorization failure message: H61Jt3-CBwnsQQ5Q0ljfnx8CZUKFNkOZKcL8Klsrsz9dzje0KpQdefa_v5Uk9nD1ehpi7288htQzaEAApwLu88ZIUsuWxywwwOWBOWeU53RRy68X7vD228Mb1_He4JqQOyfoieRlOd5qClA3b19uTQp8YRxZ9-0wrbXlkISe_N6BzybLfDSeHe1YlAXoVxOlyAlUjM4sy7cdsZjMaIoANXdWmw2ltgJKgPaehiRlRDIEIMAJB3SB8whVy04V7J8SJacdoCzZk2qE2gppmZ9B2ieq51QHfAq-XxoI-FaZegN9TTD83rxgPlQyyS6hLVG3J5B5zTVNy_y3ZtJZLle8BXE5eLursgLcYTavDazLWCoPC85_kFrOjvbWbVfnfVXgEeK_f2AwmN9D-vX10k9TY1cy-PwuRrgrKNMKtW0TeBzSZn1u4gNsBCiPLDPkO2CRwAaJIfMjF3FIfV7TYiwvZmAeiZEi7YyedmiBYMtLTPCn5jsVNgIWdpvnPQK-4UX0iv2a7u9ns43U7E9JRdm9Is9hEH4rqa8244UCeDkXefoQQLlg_EZzwKECm4wrm7ElmBtgwD2haicmTrUlXg9hd0toW0dDWYjTXtgC8ZmhwsXJBlcljzcQgBgbt1ioOaN6jH35NxkGjgCOzh0kg51VAlWyH2yUF_LmNQPs4Rqa-RYTcj-LzCB6-DpKhdvHlyEMkMilTpYNFB2TiqA_CnCXwf0MJ3alXJHSxjr6s2tVqSkVuIDc77Pplp2XDPDqA5yo3sDC0RwjCaLca20LN6xFa3W8KYkk_edZ_C_qkgx0KtefFKntpDHBUko
Notifications 1 0 2 0 0

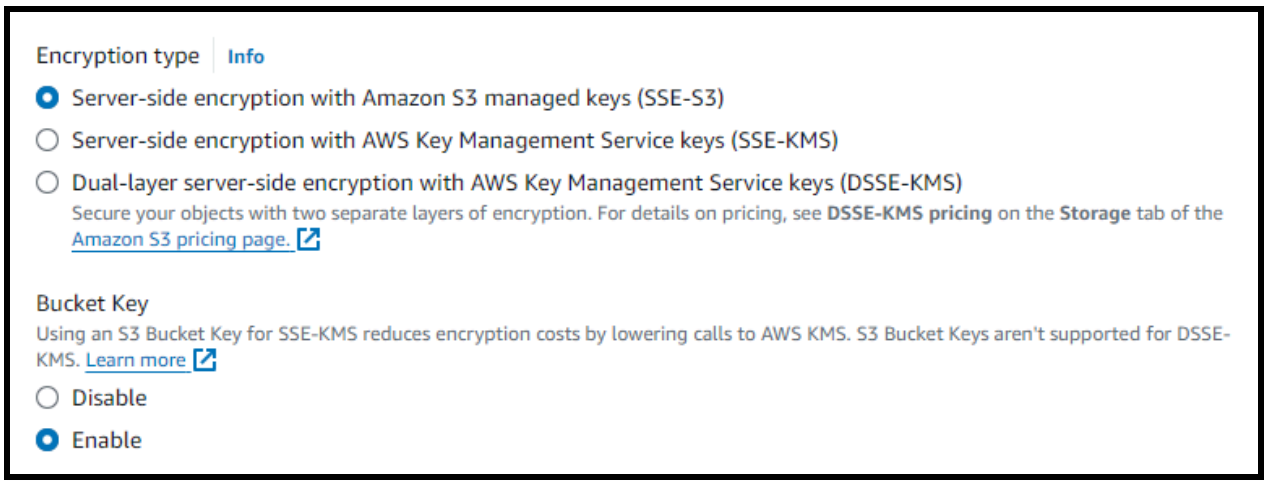

Permissions defined in this policy Info
Copy
Edit
Summary
JSON
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"ec2:StartInstances",
"ec2:StopInstances"
],
"Resource": "arn:aws:ec2:ap-south-1:637423493890:instance/*"
}
]
}

02-07-24

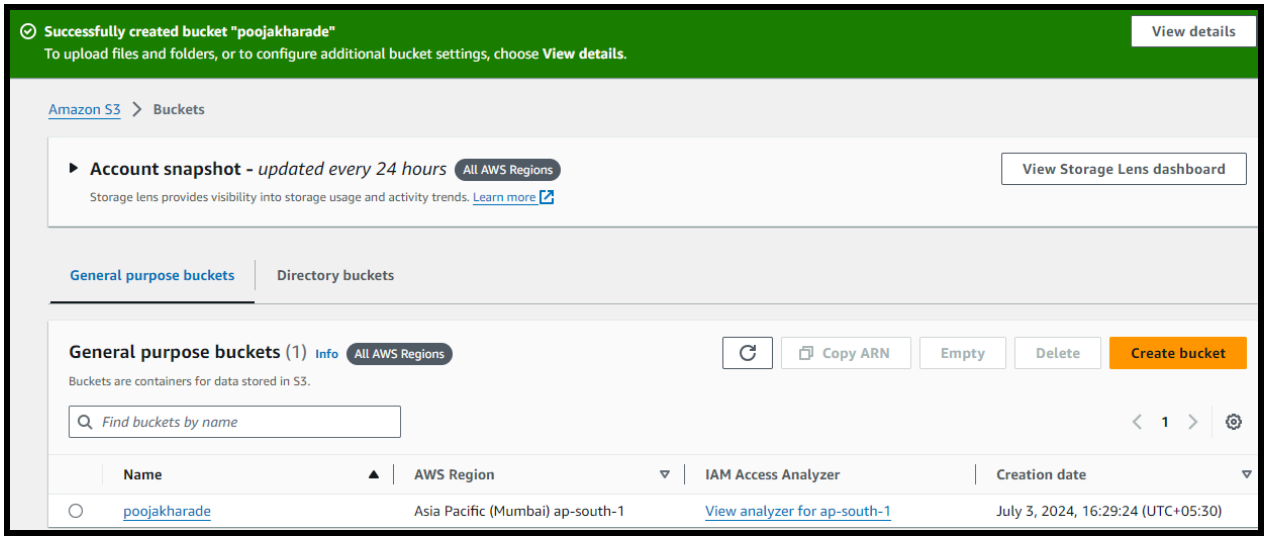
Creating bucket using S3 services
Store and retrieve any amount of data from anywhere

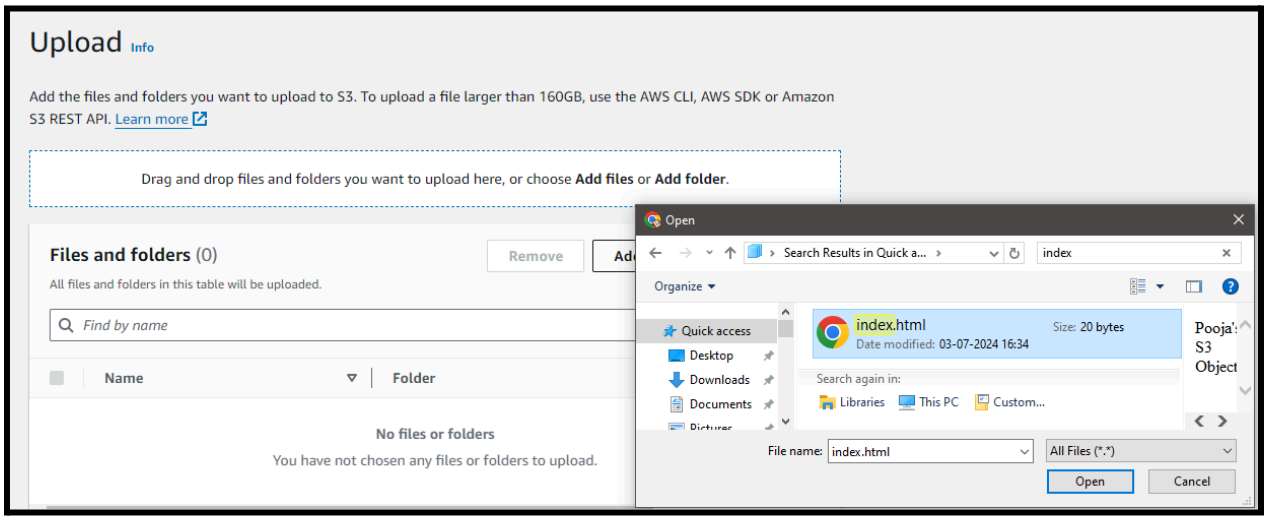
Create bucket



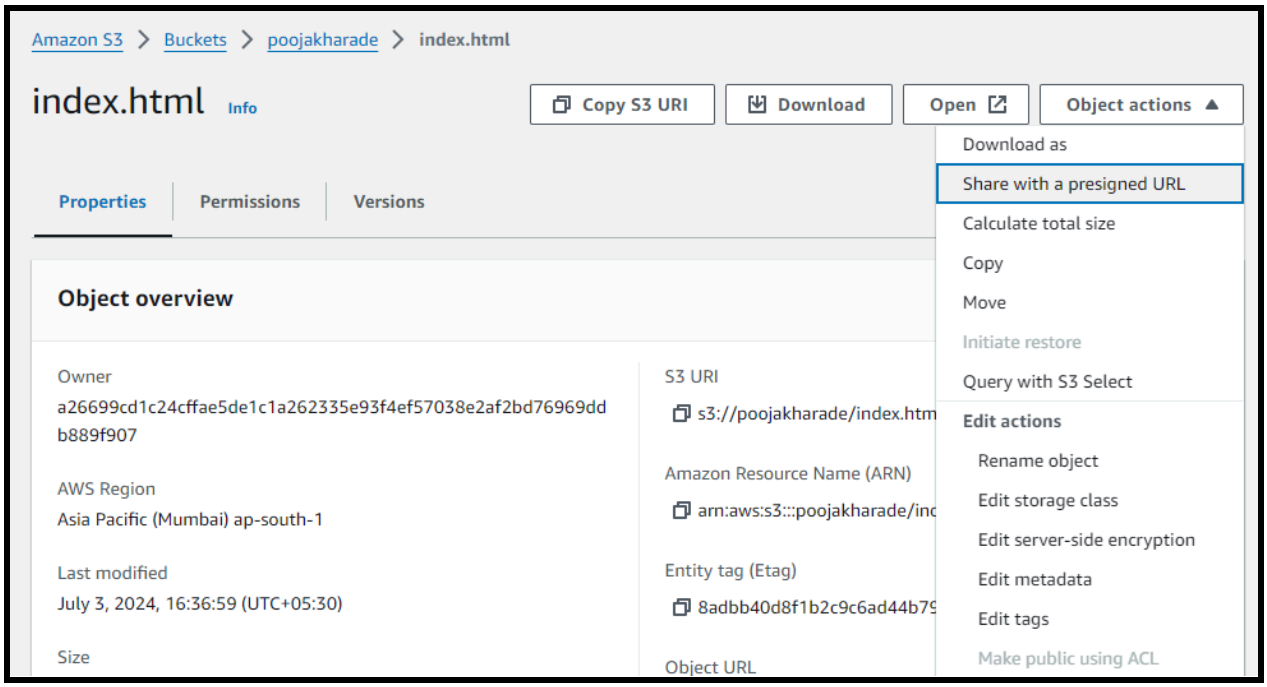


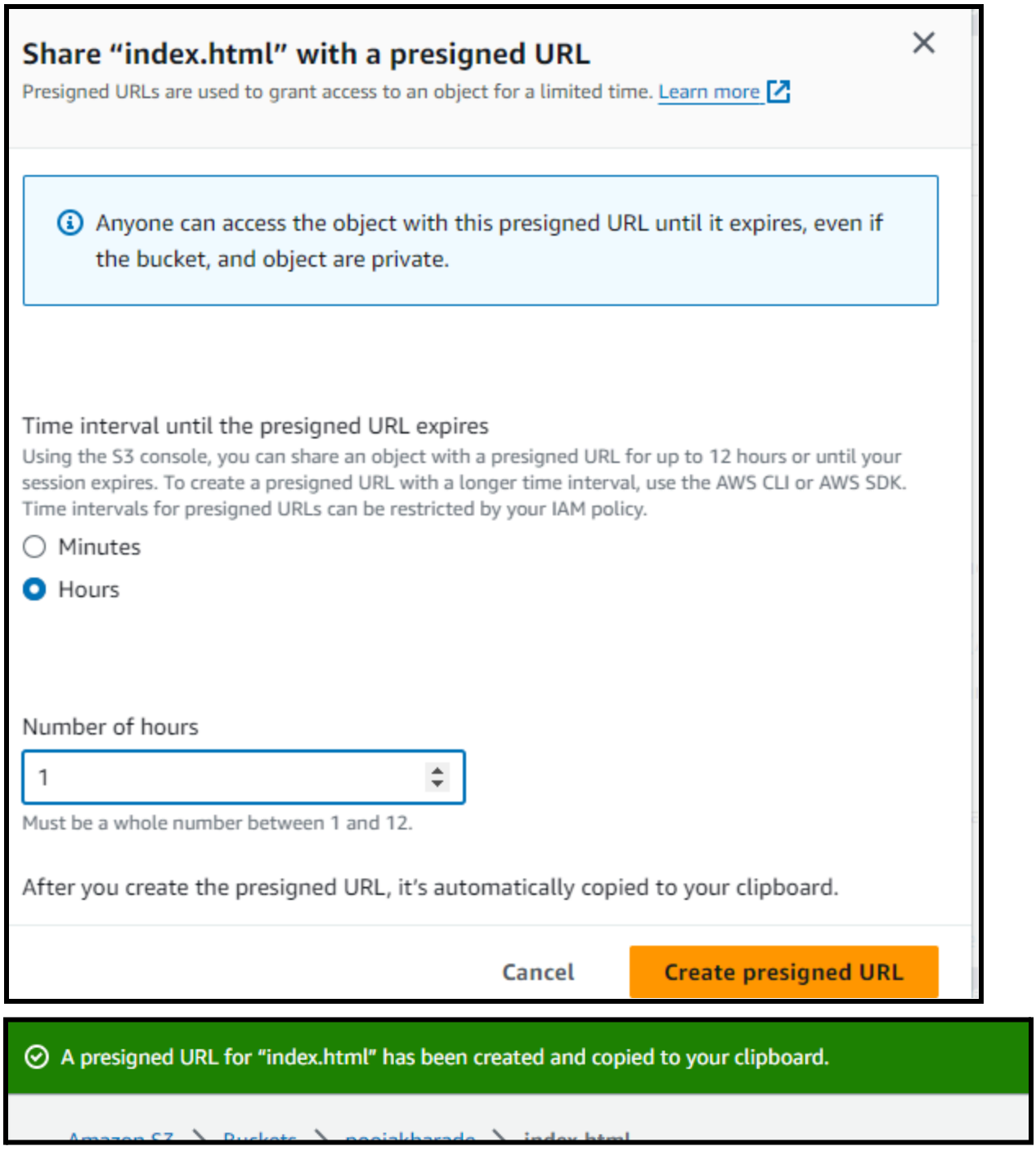
Bucket created





Share with a pre signed URL

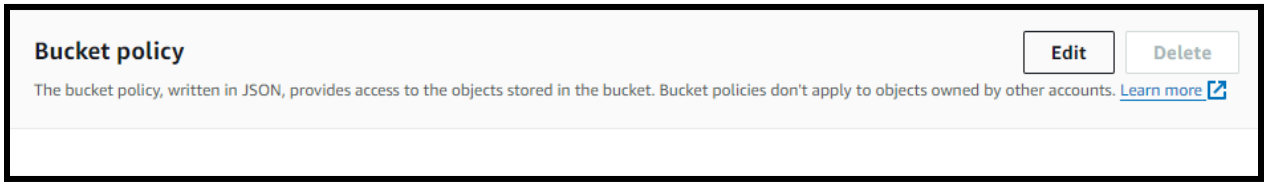

Amazon S3 > Buckets > poojakharade > index.html
index.html Info
Copy S3 URI
Download
Open
Object actions
Download as
Share with a presigned URL
Calculate total size
Copy
Move
Initiate restore
Query with S3 Select
Edit actions
Rename object
Edit storage class
Edit server-side encryption
Edit metadata
Edit tags
Make public using ACL
Properties
Permissions
Versions
Object overview
Owner
a26699cd1c24cffae5de1c1a262335e93f4ef57038e2af2bd76969ddb889f907
AWS Region
Asia Pacific (Mumbai) ap-south-1
Last modified
July 3, 2024, 16:36:59 (UTC+05:30)
Size
S3 URI
s3://poojakharade/index.htm
Amazon Resource Name (ARN)
arn:aws:s3:::poojakharade/inc
Entity tag (Etag)
8adbb40d8f1b2c9c6ad44b79
Object URL

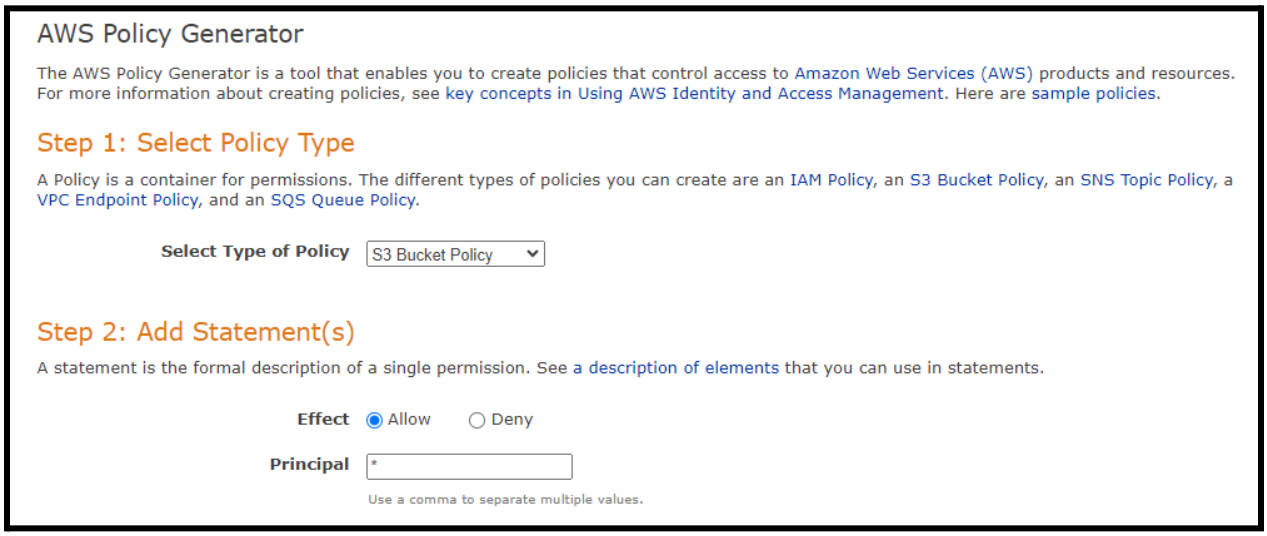

Share “index.html” with a presigned URL
Presigned URLs are used to grant access to an object for a limited time. Learn more
Anyone can access the object with this presigned URL until it expires, even if the bucket, and object are private.
Time interval until the presigned URL expires
Using the S3 console, you can share an object with a presigned URL for up to 12 hours or until your session expires. To create a presigned URL with a longer time interval, use the AWS CLI or AWS SDK. Time intervals for presigned URLs can be restricted by your IAM policy.
Minutes
Hours
Number of hours
1
Must be a whole number between 1 and 12.
After you create the presigned URL, it's automatically copied to your clipboard.
Cancel
Create presigned URL

A presigned URL for “index.html” has been created and copied to your clipboard.

Output :

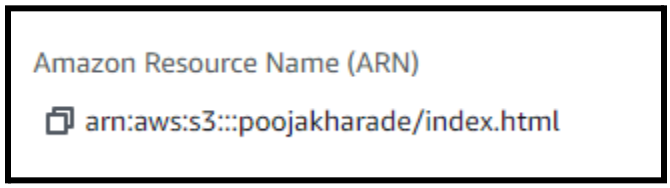
Permissions > generate policy





Get object and put object

Copy arn



Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bu

Bucket ARN

arn:aws:s3:::poojakharade

Add statement

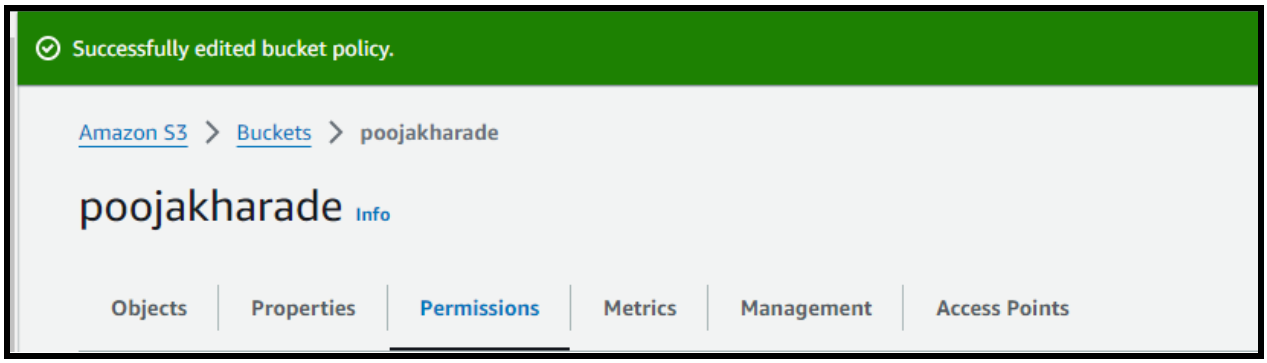
You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject • s3:PutObject	arn:aws:s3:::poojakharade/index.html	*None*

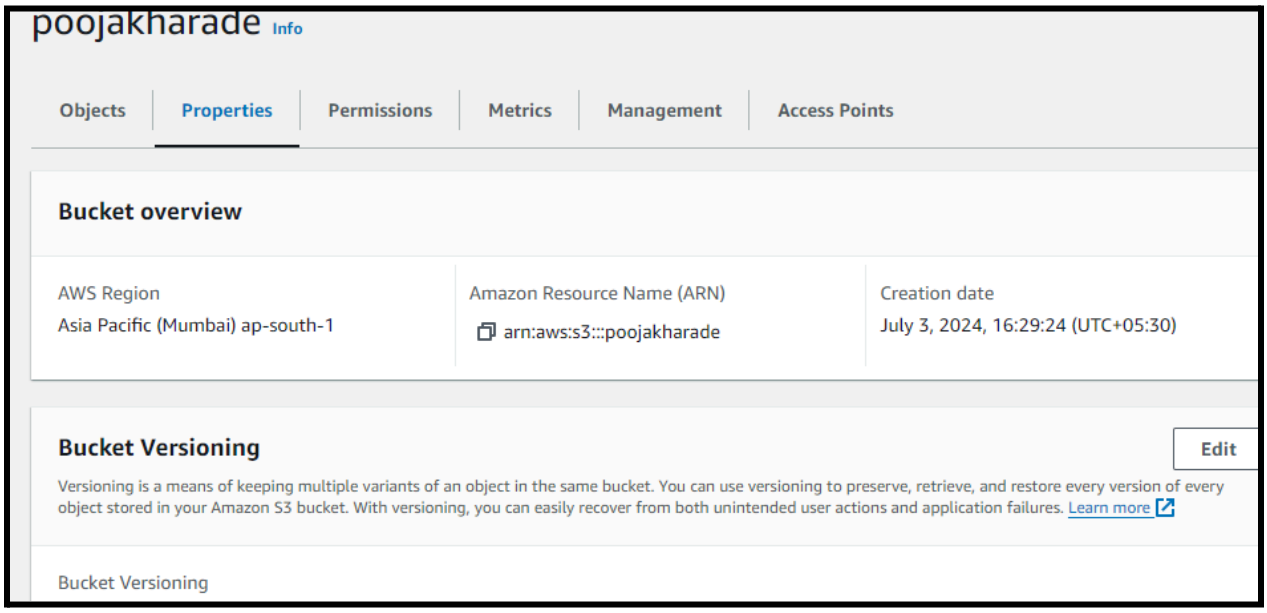
Policy JSON Document

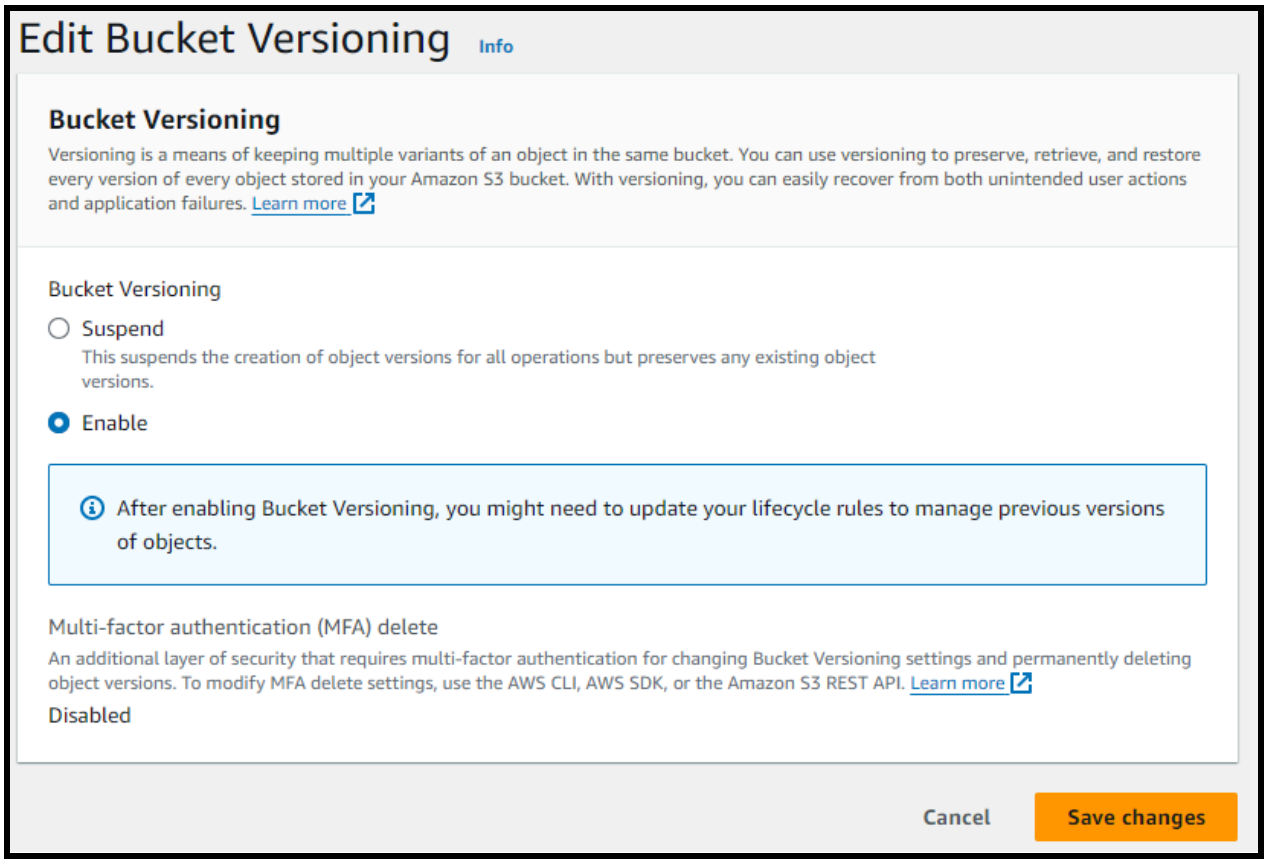
Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

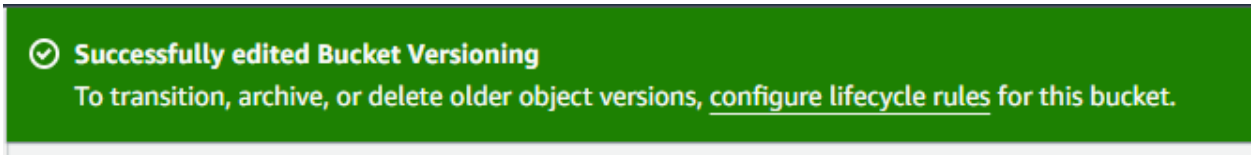

```
{
  "Id": "Policy1720005399043",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1720005362812",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::poojakharade/index.html",
      "Principal": "*"
    }
  ]
}
```

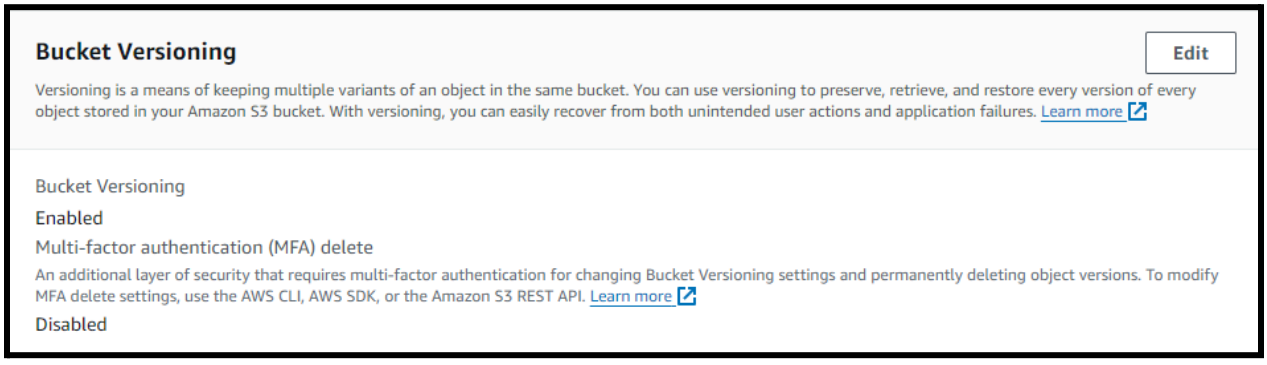


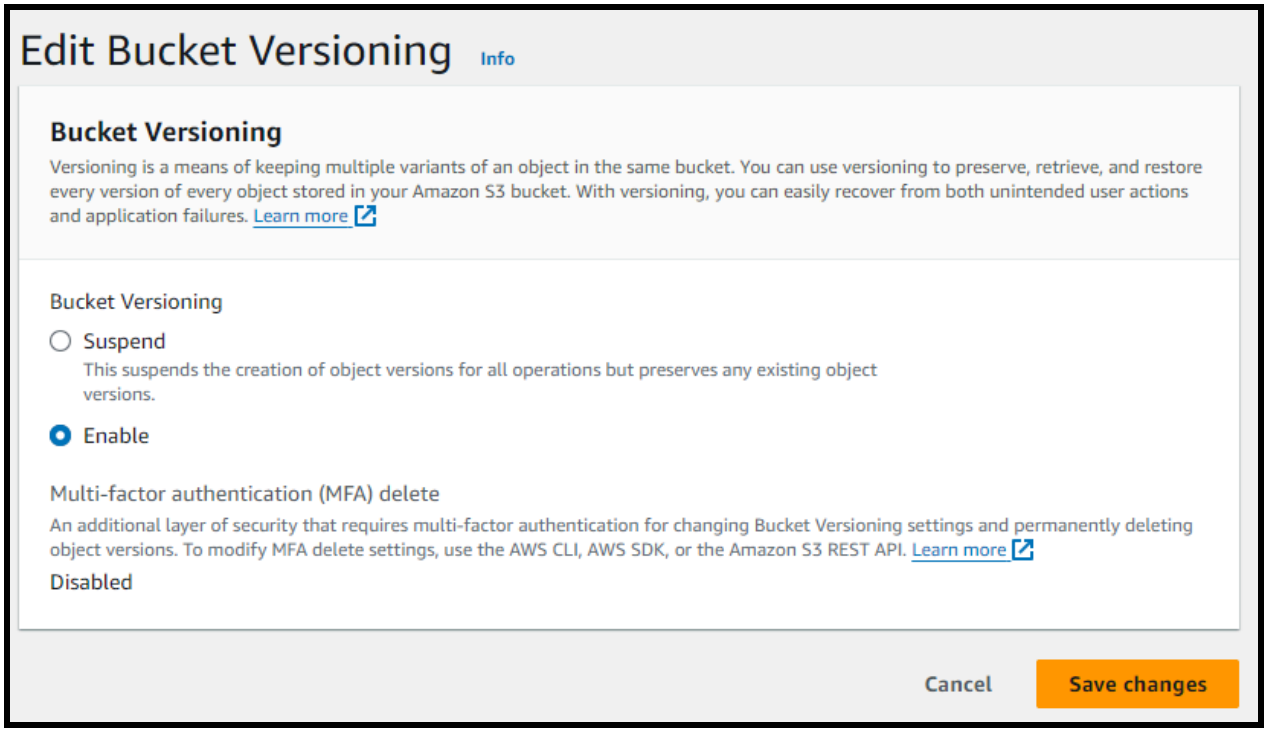
Bucket versioning



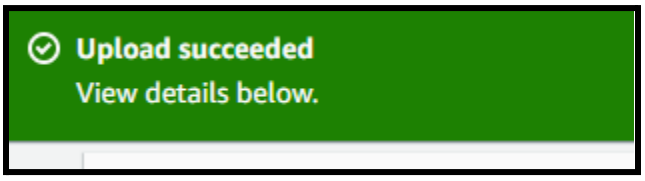

Edit Bucket Versioning
Info
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.
Enable
After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled
Cancel
Save changes


Successfully edited Bucket Versioning
To transition, archive, or delete older object versions, configure lifecycle rules for this bucket.

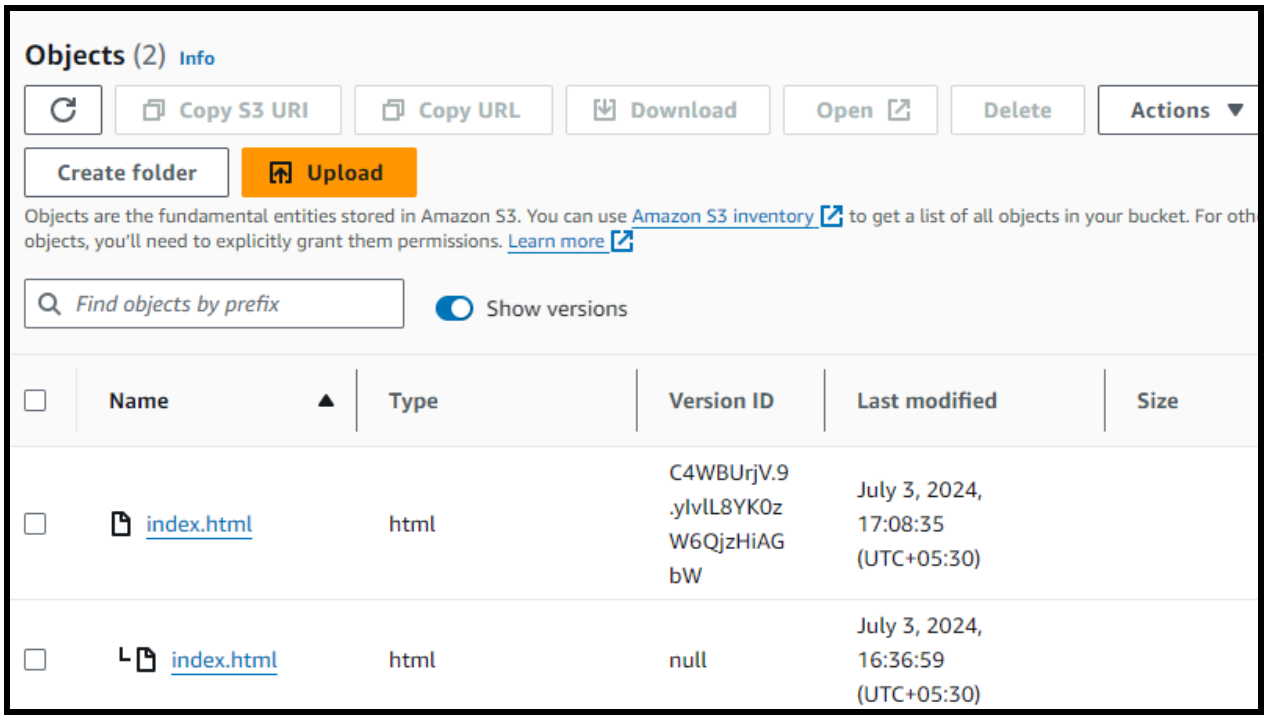

Bucket Versioning
Edit
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Enabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled



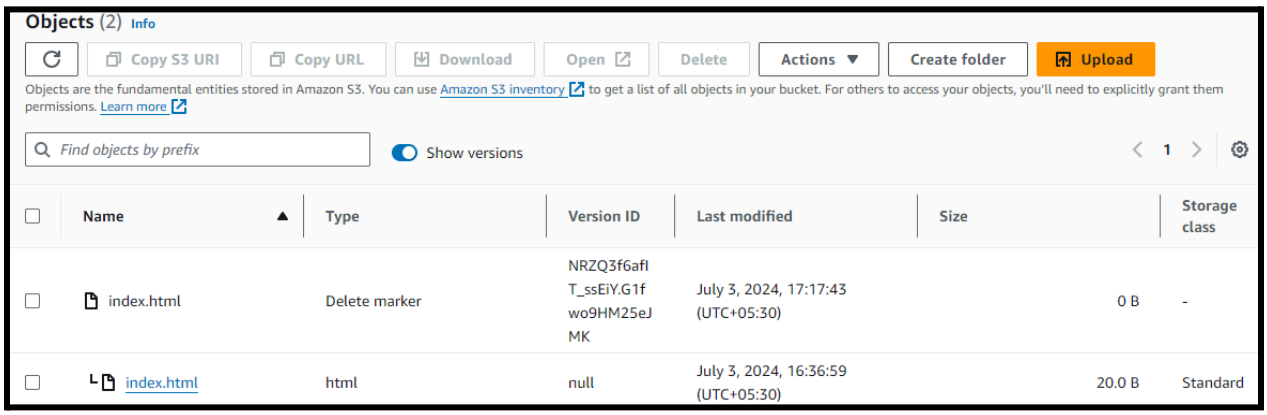
Upload again



Version created

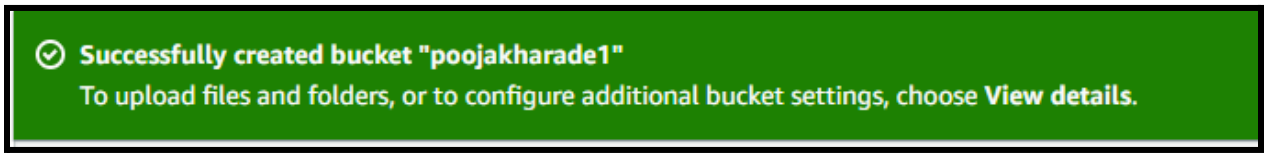


After permanently delete and delete operation performed so the files are retrieved

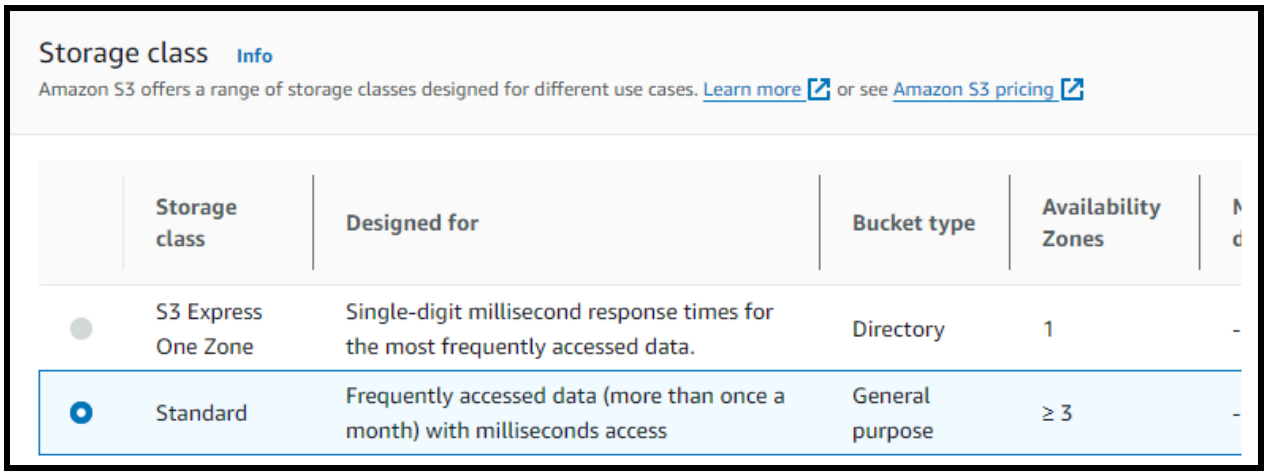


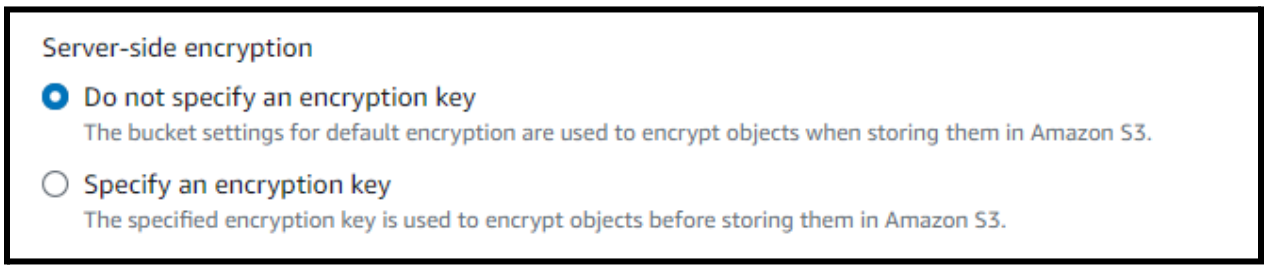
04-07-2024

Create bucket

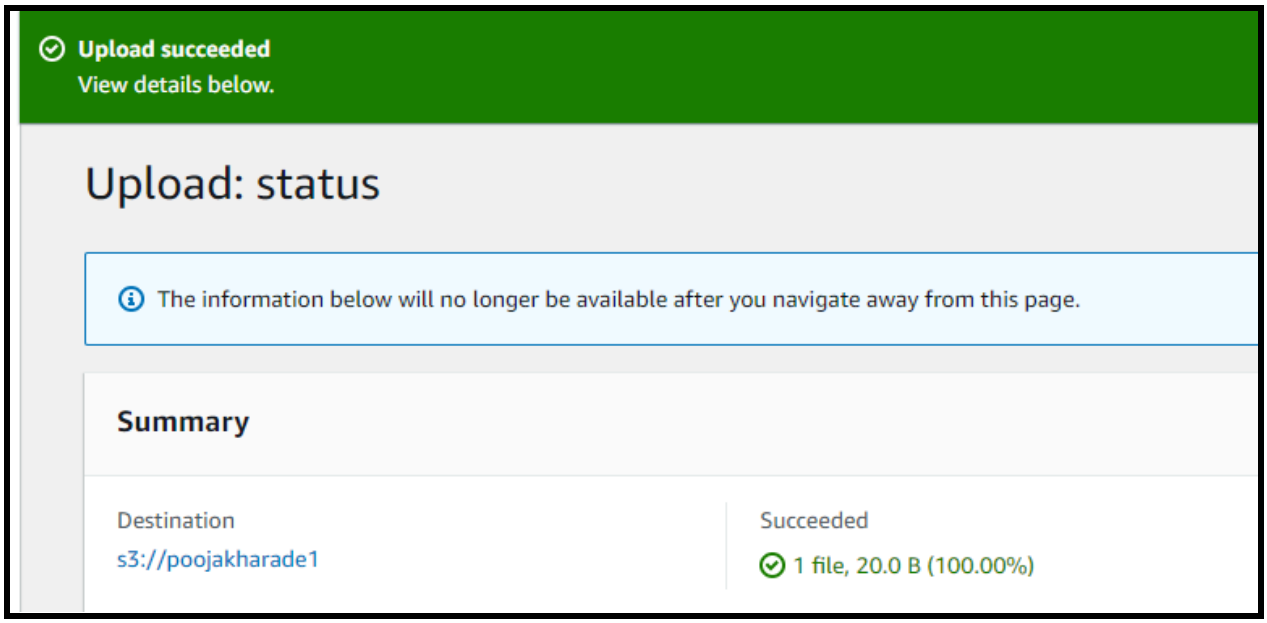


Select storage class

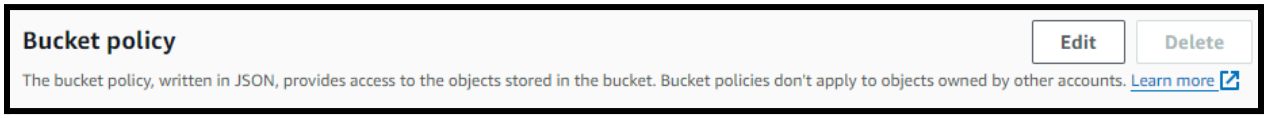


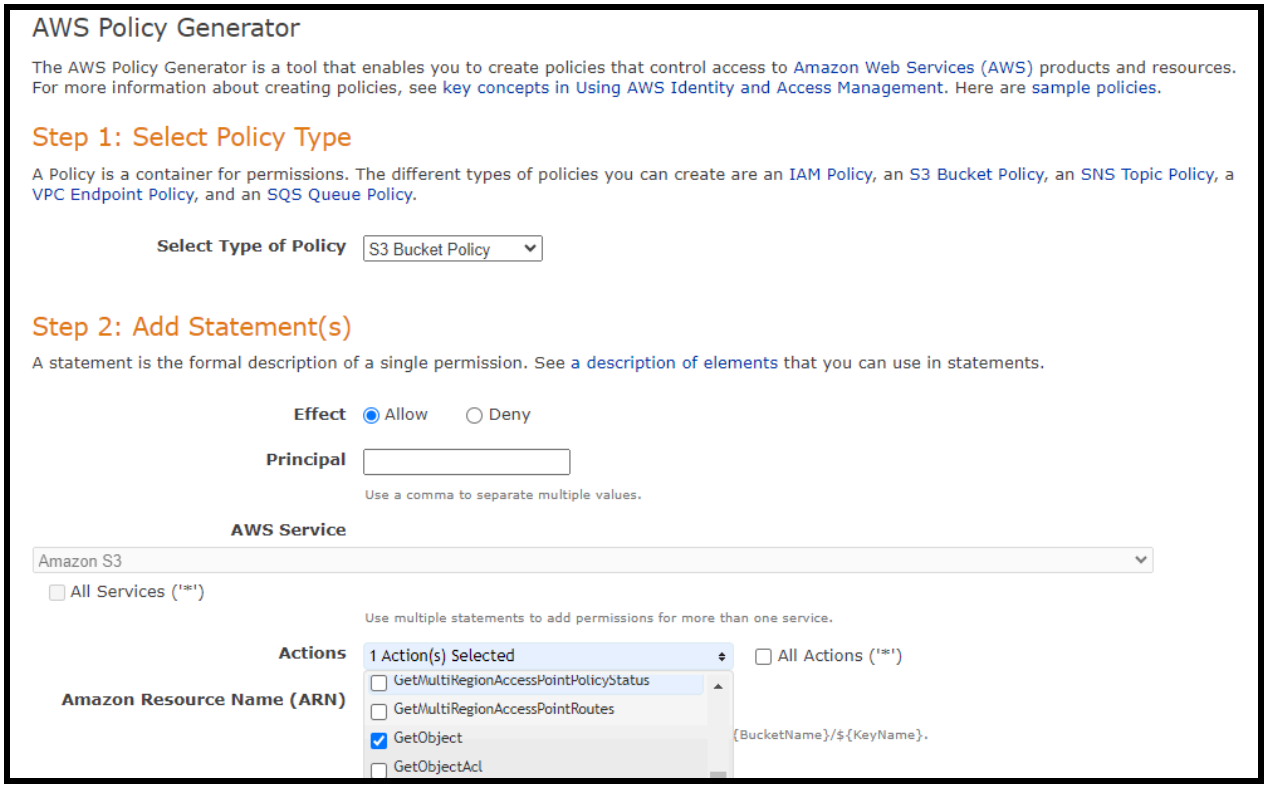


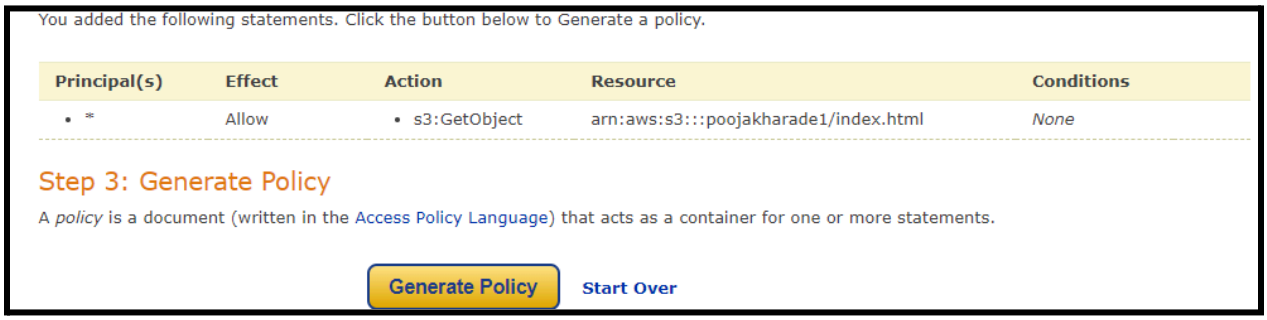
Upload object

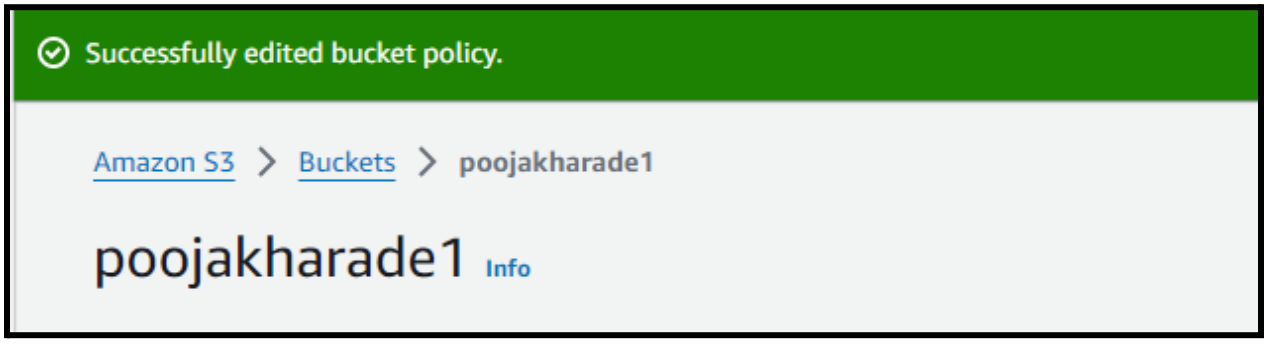


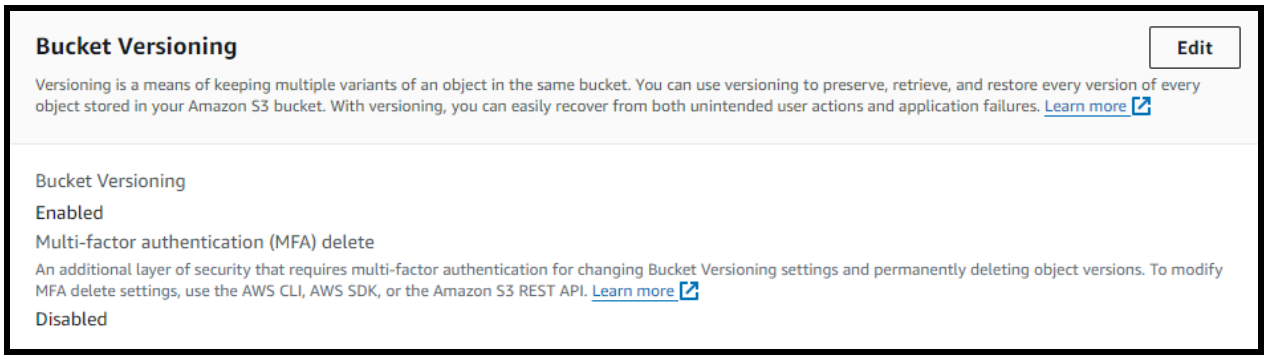
Permissions > bucket policy



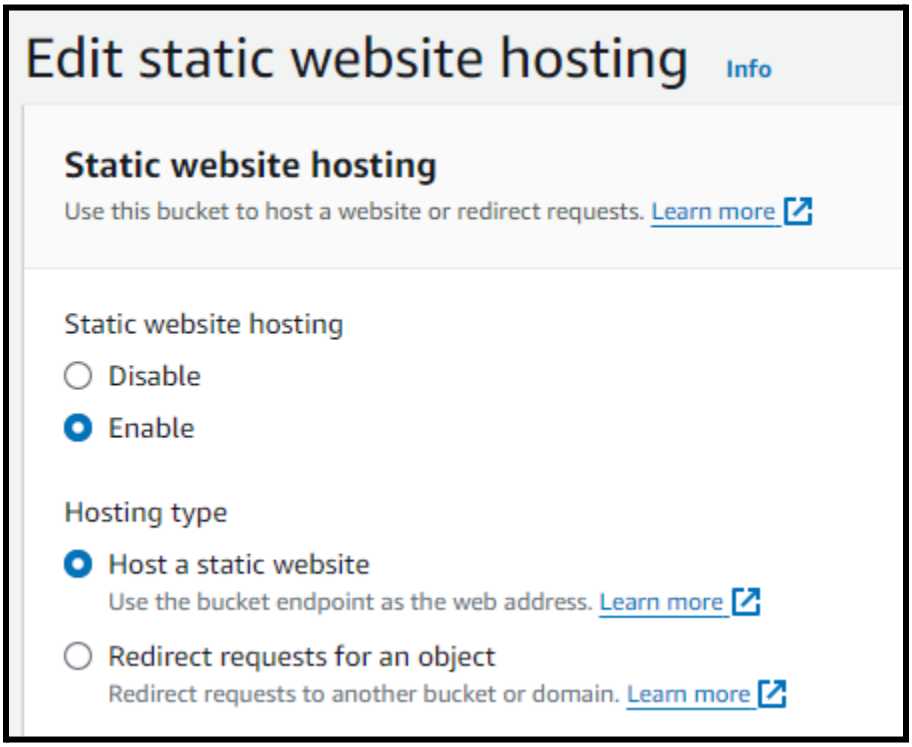

AWS Policy Generator
The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.
Step 1: Select Policy Type
A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.
Select Type of Policy
S3 Bucket Policy
Step 2: Add Statement(s)
A statement is the formal description of a single permission. See a description of elements that you can use in statements.
Effect
Allow
Deny
Principal
Use a comma to separate multiple values.
AWS Service
Amazon S3
All Services ('*')
Use multiple statements to add permissions for more than one service.
Actions
1 Action(s) Selected
All Actions ('*')
Amazon Resource Name (ARN)
GetMultiRegionAccessPointPolicyStatus
GetMultiRegionAccessPointRoutes
GetObject
GetObjectAcl
{BucketName}/${KeyName}.

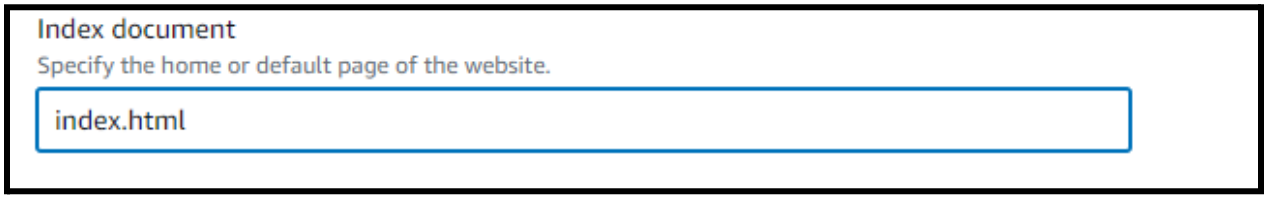

You added the following statements. Click the button below to Generate a policy.
Principal(s)
Effect
Action
Resource
Conditions
*
Allow
s3:GetObject
arn:aws:s3:::poojakharade1/index.html
None
Step 3: Generate Policy
A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.
Generate Policy
Start Over

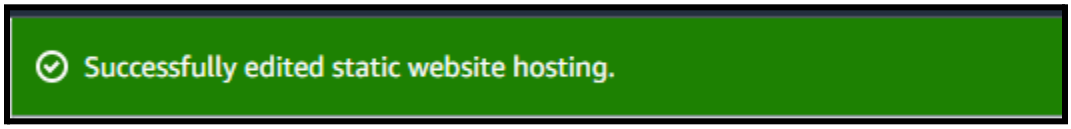

Successfully edited bucket policy.
Amazon S3 > Buckets > poojakharade1
poojakharade1 Info

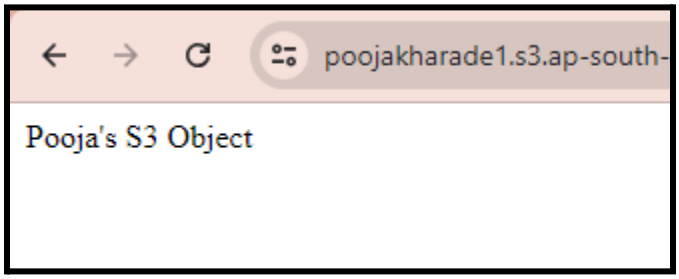


Static website hosting > enable






Successfully edited static website hosting.


poojakharade1.s3.ap-south-
Pooja's S3 Object

05-07-24

User data - *optional* Info

Upload a file with your user data or enter it in the field.

Choose file

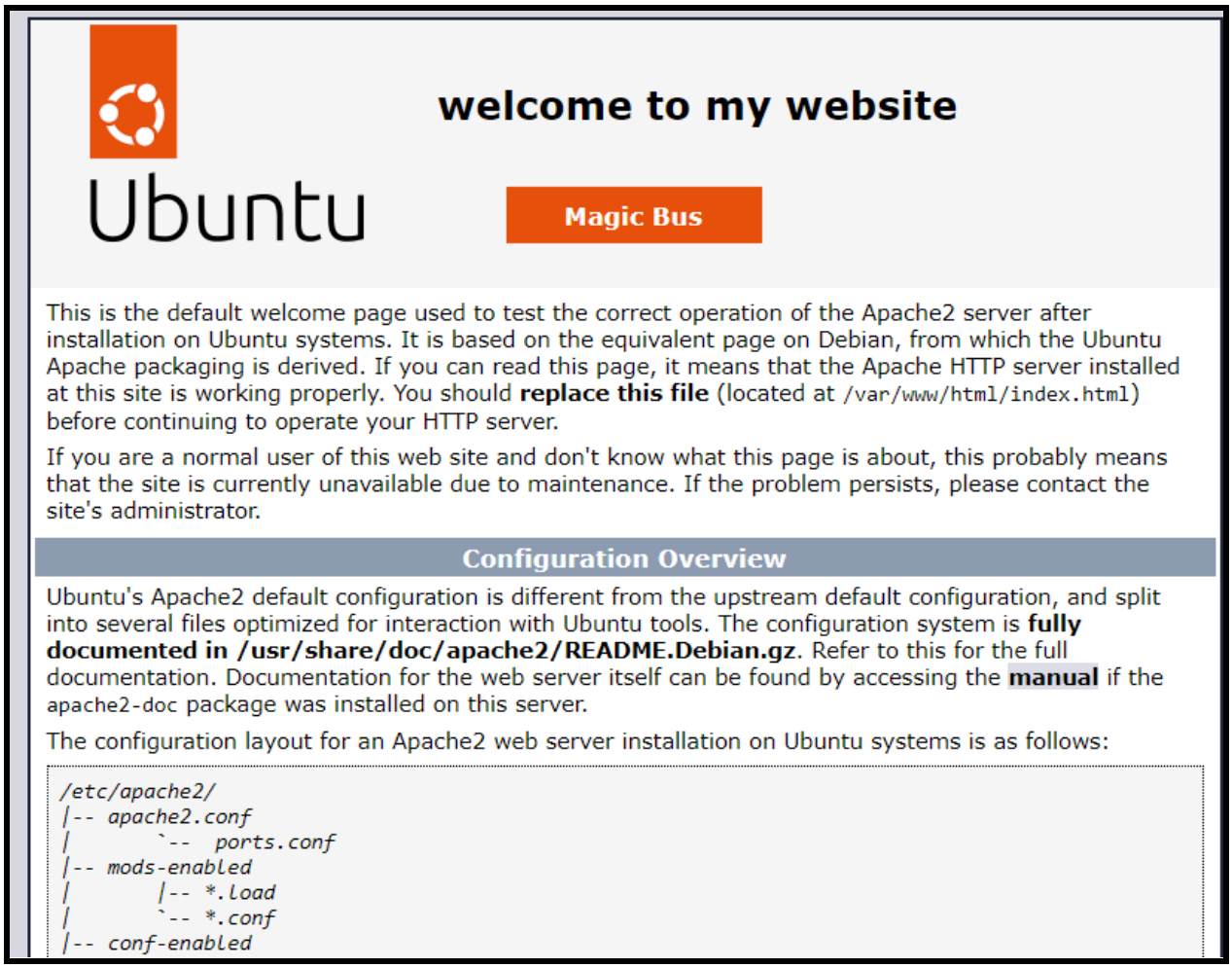
```
#!/bin/bash
sudo su
apt update -y
apt upgrade -y
apt install apache2 -y
echo "this is my website using bash command" > /var/www/html/index.html
```

EC2 > Instances > Launch an instance

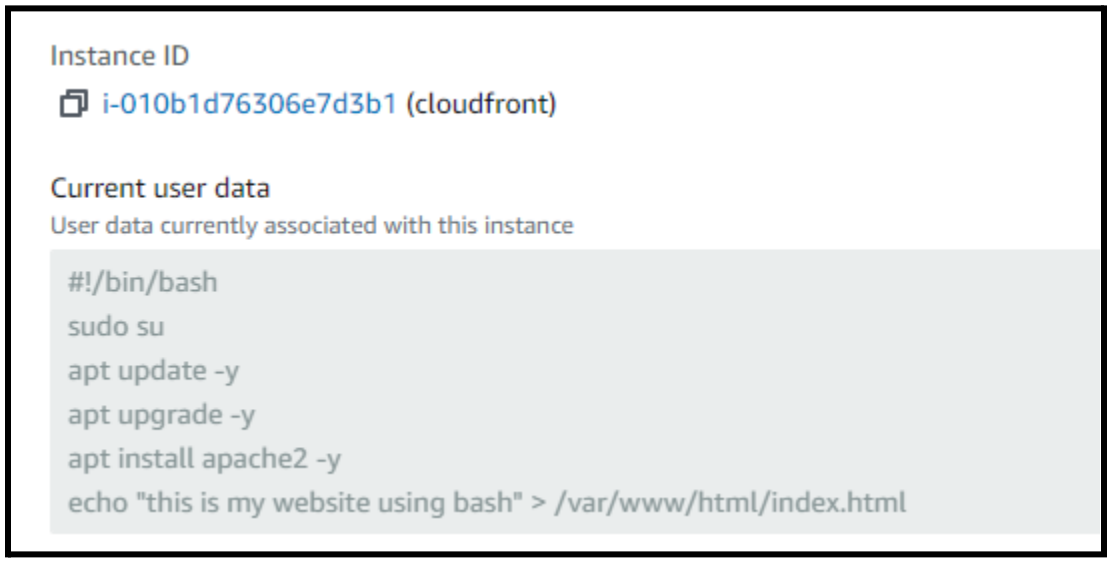
Success

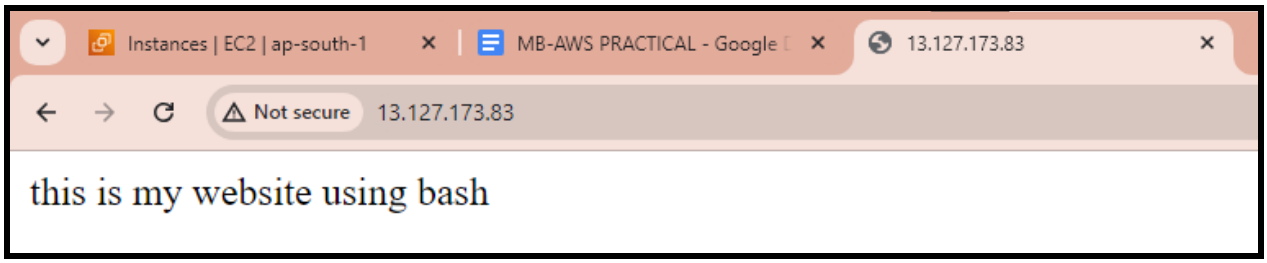
Successfully initiated launch of instance (i-014e9fe61f3c40e3f)

```
  The currently running kernel version is not the expected kernel version

Restarting the system to load the new kernel will not be handled automatic

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.
root@ip-172-31-40-181:/home/ubuntu# cd /var/www/html
root@ip-172-31-40-181:/var/www/html# ls
index.html
root@ip-172-31-40-181:/var/www/html# vi index.html
root@ip-172-31-40-181:/var/www/html#
```

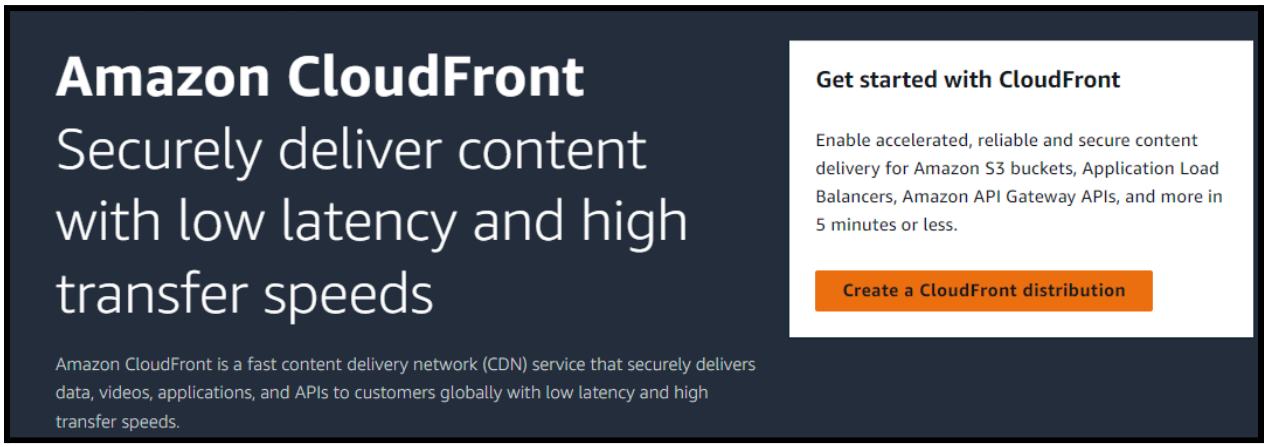

welcome to my website
Ubuntu
Magic Bus
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that 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

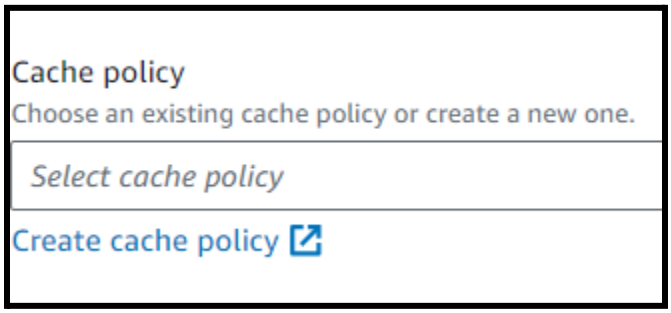
Output :

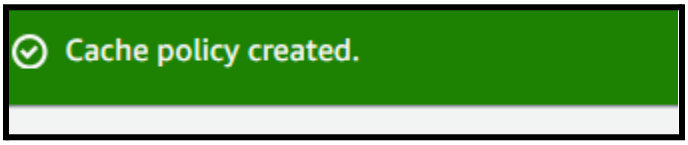

Instance ID
i-010b1d76306e7d3b1 (cloudfront)
Current user data
User data currently associated with this instance
#!/bin/bash
sudo su
apt update -y
apt upgrade -y
apt install apache2 -y
echo "this is my website using bash" > /var/www/html/index.html



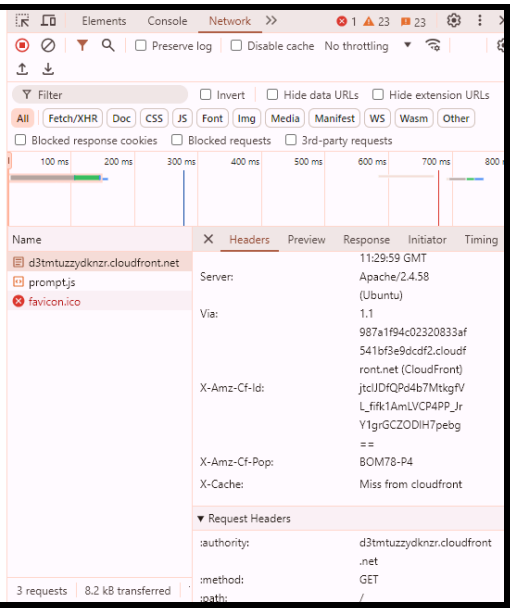
Create cloud front distribution







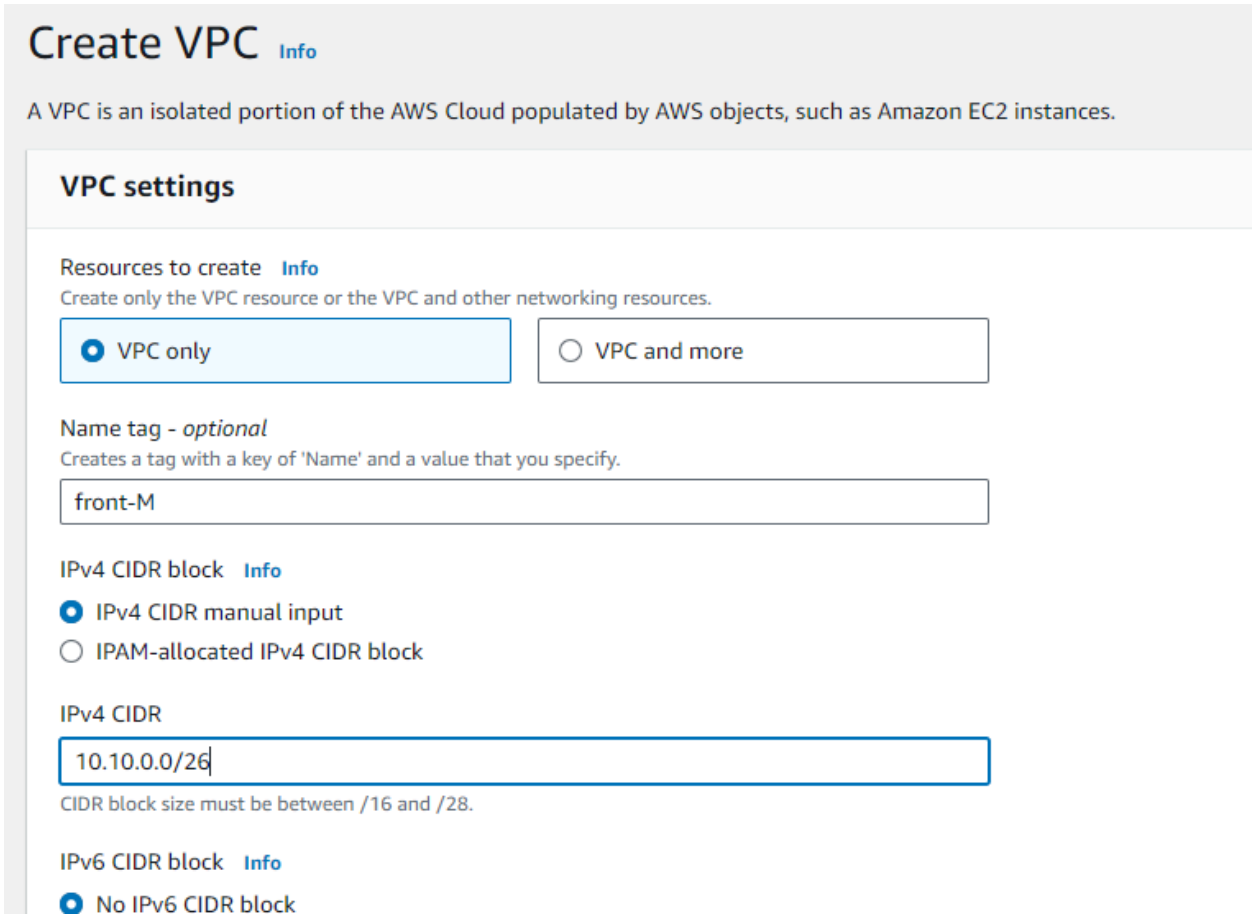
this is my website using bash

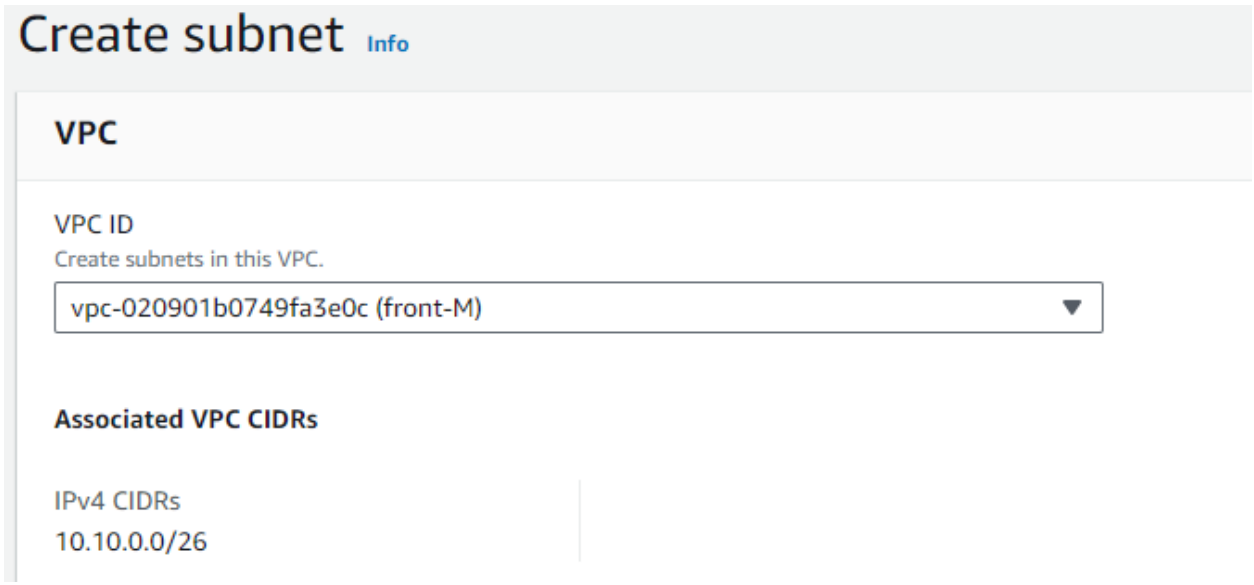


ICMP TASK 1

NAT GATEWAY

SAME ACCOUNT DIFF REGION





Adding two subnets

Subnet name

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

public-sub

The name can be up to 256 characters long.

Availability Zone Info

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

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

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.

10.10.0.0/26

IPv4 subnet CIDR block

10.10.0.0/28 16 IPs

Subnet 2 of 2

Subnet name

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

public-sub2

The name can be up to 256 characters long.

Availability Zone Info

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

Asia Pacific (Mumbai) / 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.

10.10.0.0/26

IPv4 subnet CIDR block

10.10.0.16/28 16 IPs

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.

myigw

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*	
Name	myigw	Remove

Add new tag

You can add 49 more tags.

Cancel | Create internet gateway

Attach to VPC (igw-0b631fd53b931bf6f) Info

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.

Select a VPC

vpc-020901b0749fa3e0c - front-M

▶ AWS Command Line Interface command

Cancel | Attach internet gateway

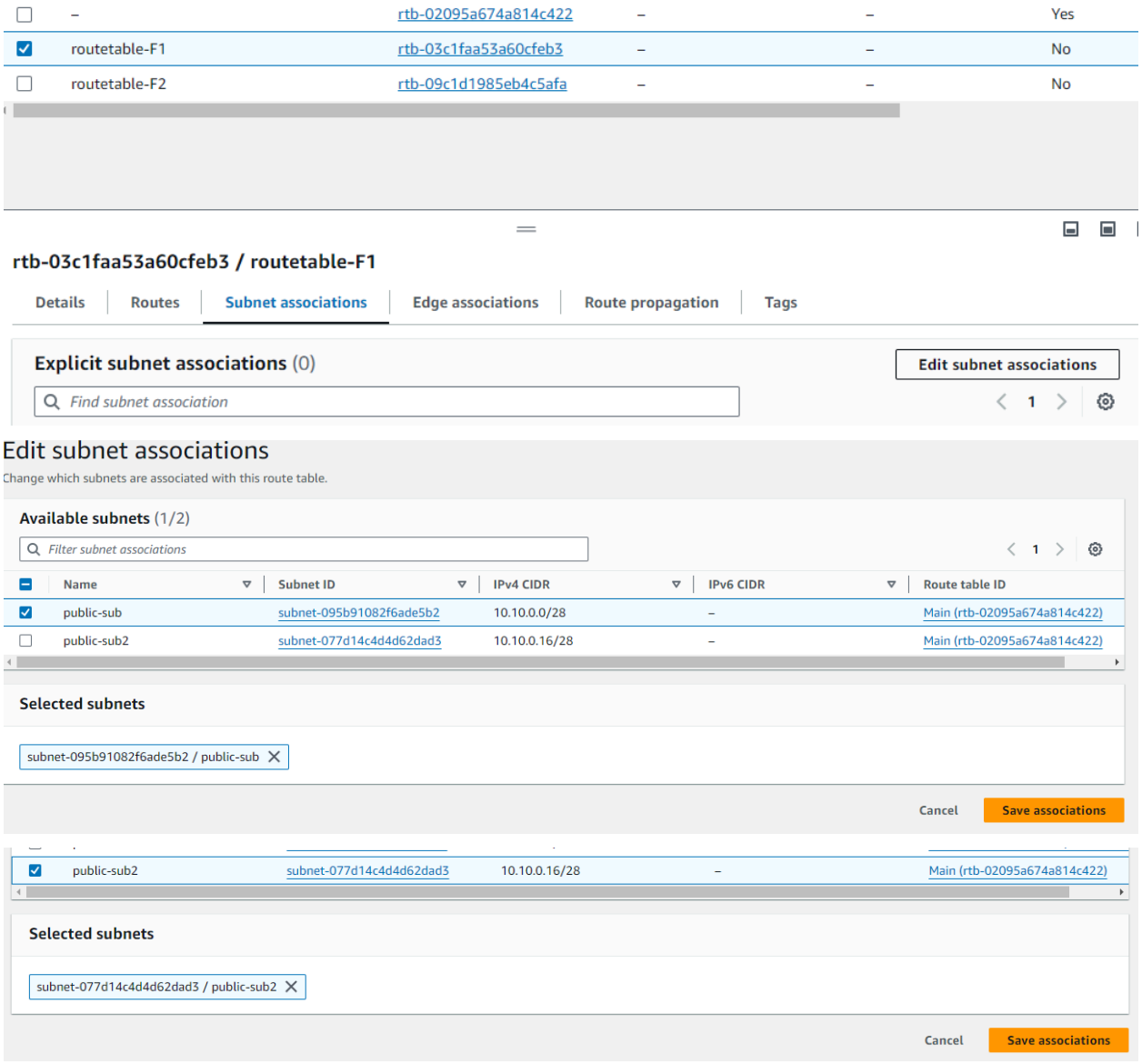
Route tables (3) Info

Last updated
less than a minute ago

Find resources by attribute or tag

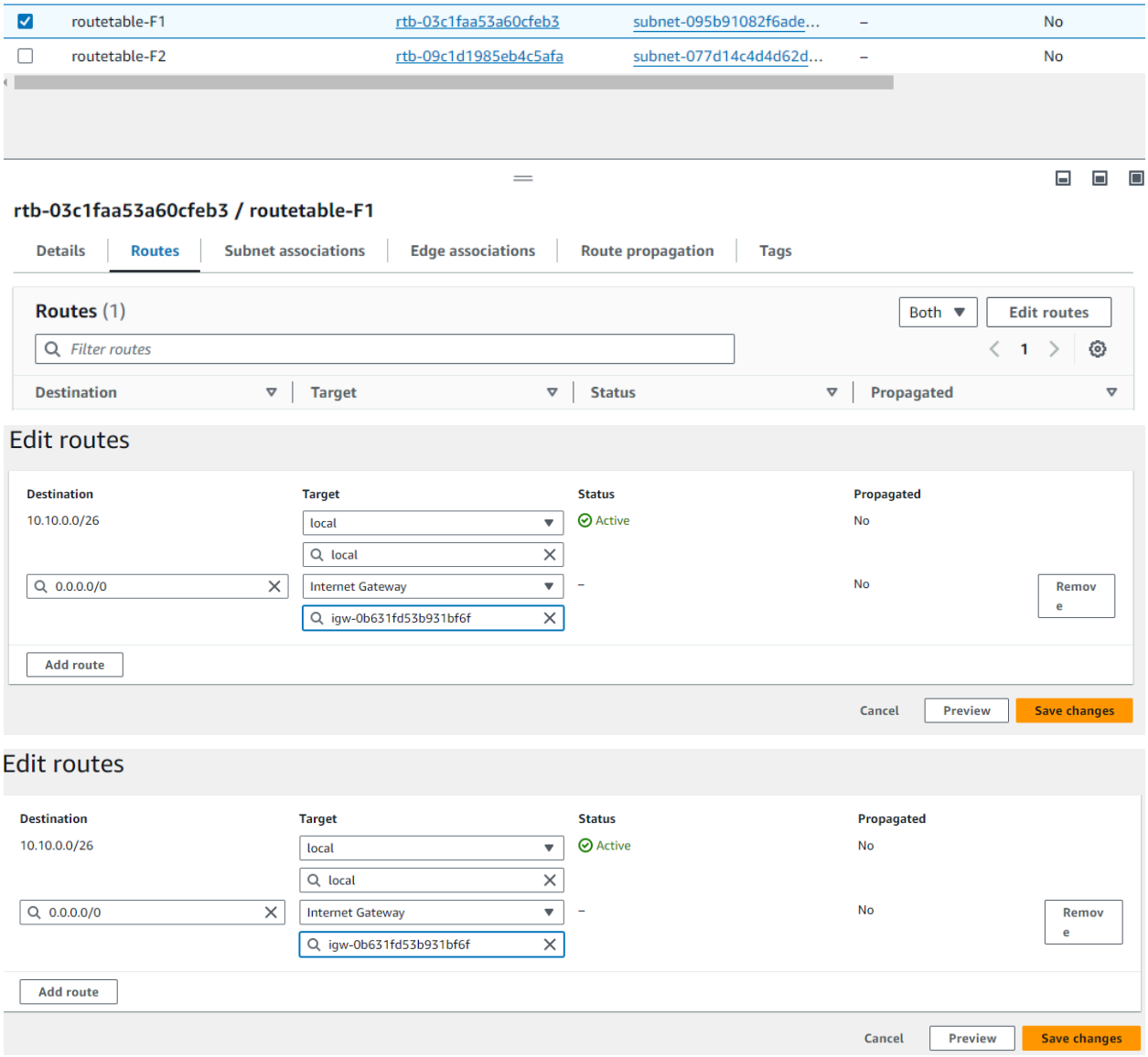
Name	Route table ID	Explicit subnet ass
–	rtb-02095a674a814c422	–
routetable-F1	rtb-03c1faa53a60cfeb3	–
routetable-F2	rtb-09c1d1985eb4c5afa	–

Edit subnet associations



Save associations

Edit routes



Change region to Ohio

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.

myvpc-ohio

IPv4 CIDR block Info

- (•) IPv4 CIDR manual input
- ( ) IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.10.0.64/26

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

Subnet 1 of 2

Subnet name

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

publicsub-backend

The name can be up to 256 characters long.

Availability Zone Info

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

US East (Ohio) / us-east-2a

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.

10.10.0.64/26

IPv4 subnet CIDR block

10.10.0.64/28 16 IPs

Subnet 2 of 2

Subnet name

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

privatesub-backend

The name can be up to 256 characters long.

Availability Zone Info

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

US East (Ohio) / us-east-2b

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.

10.10.0.64/26

IPv4 subnet CIDR block

10.10.0.80/28 16 IPs

Route table settings

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

routetable-1public

VPC
The VPC to use for this route table.

vpc-0af41499c7b1a7721 (myvpc-ohio)

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*	
Name	routetable-1public	Remove

Add new tag

You can add 49 more tags.

Cancel | Create route table

Route table settings

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

routetable-2private

VPC
The VPC to use for this route table.

vpc-0af41499c7b1a7721 (myvpc-ohio)

Tags

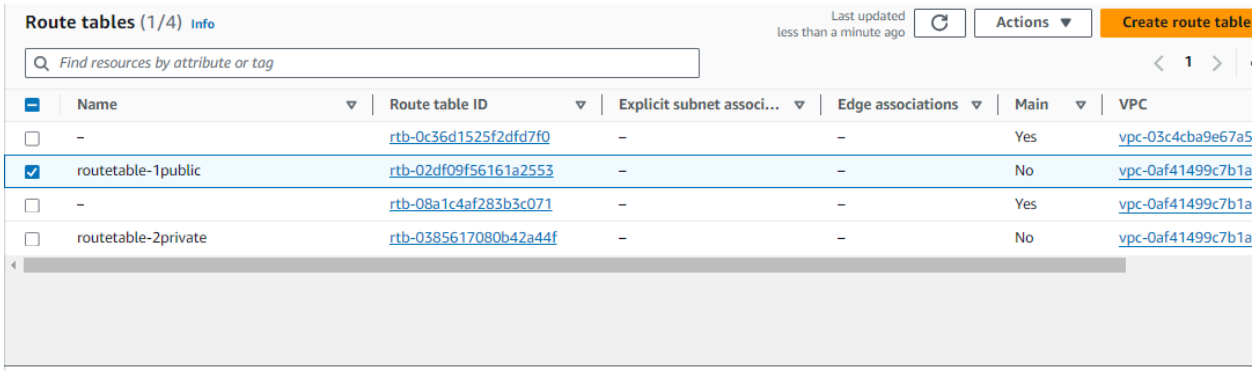
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	routetable-2private	Remove

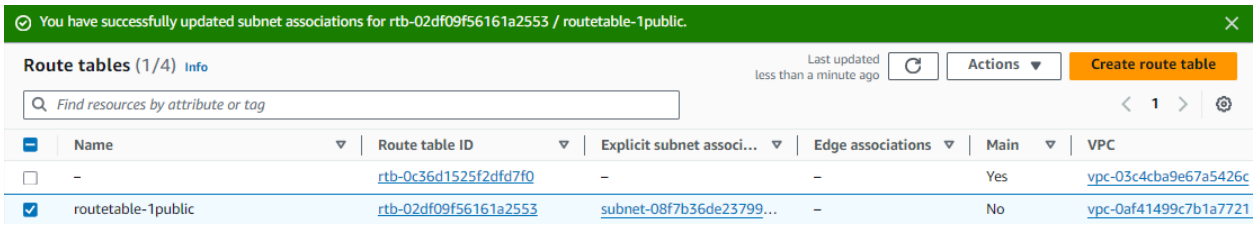
Add new tag

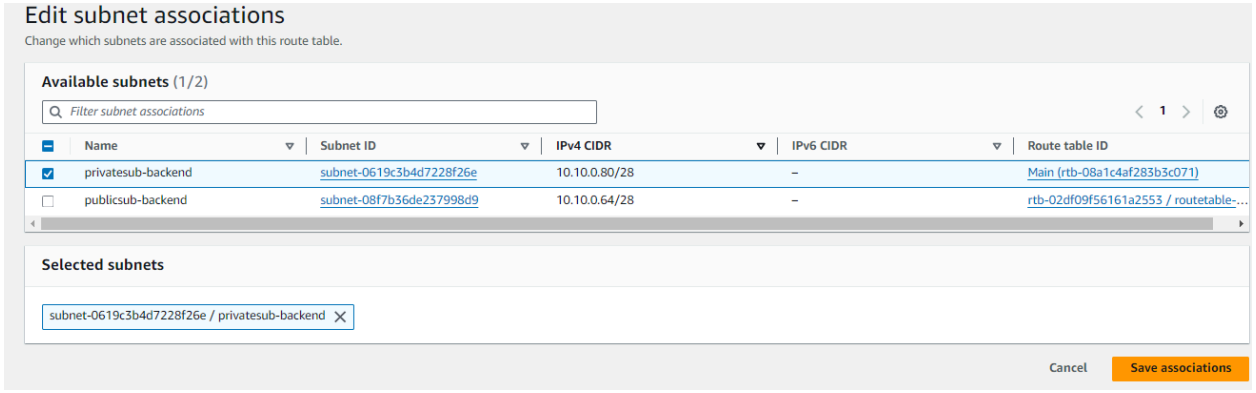
You can add 49 more tags.

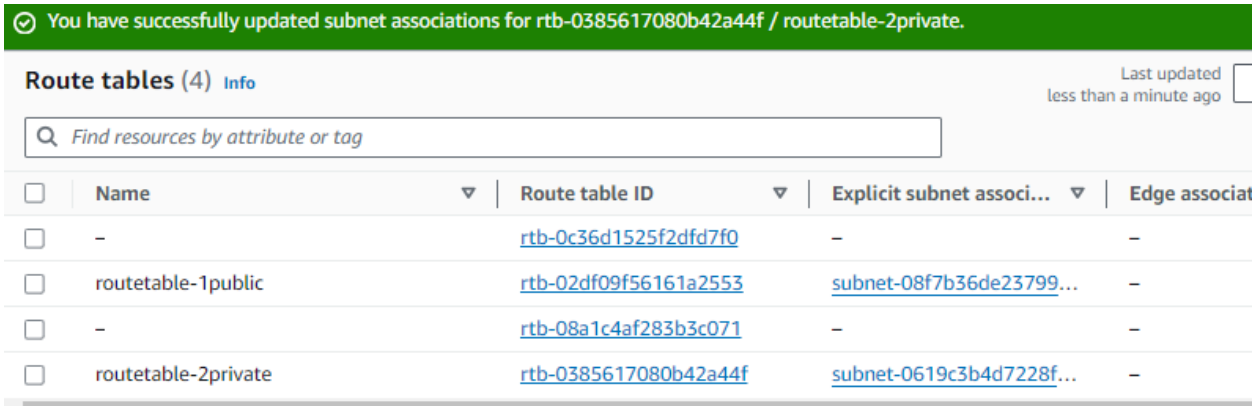
Cancel | Create route table

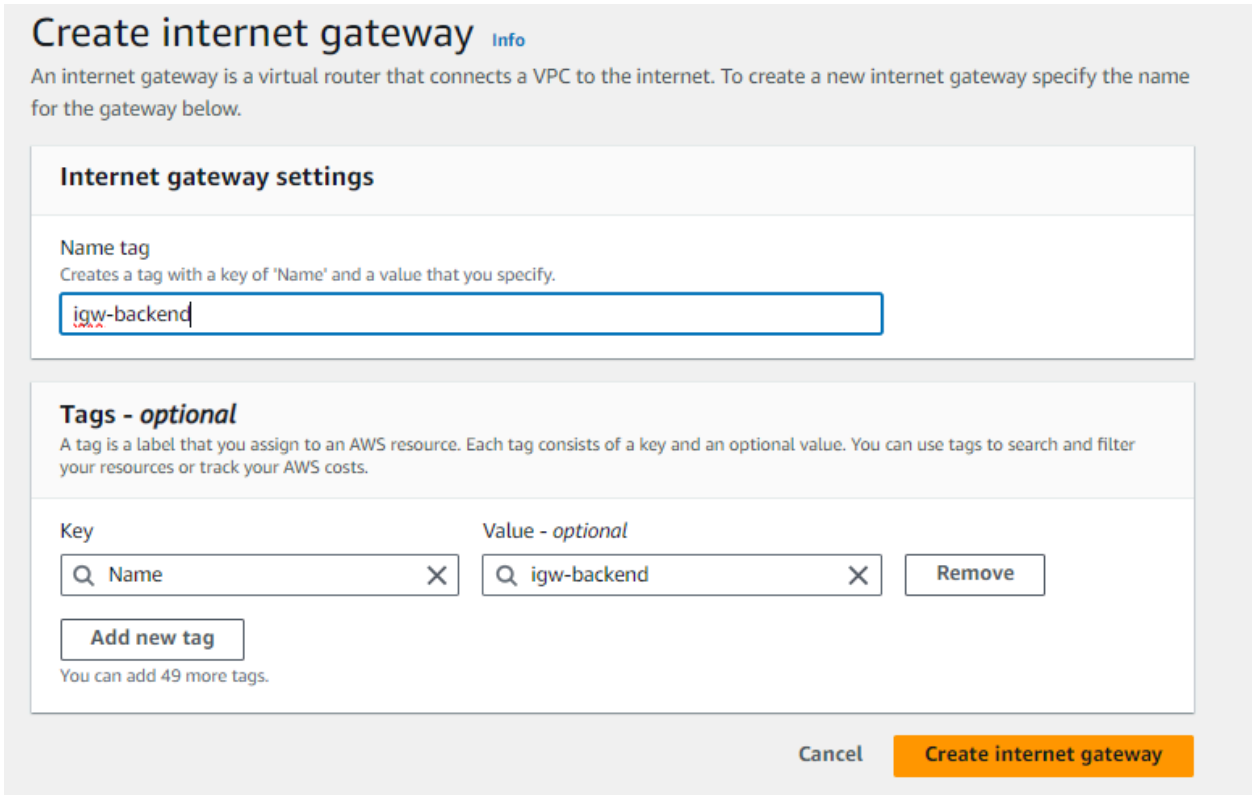

Route tables (1/4) Info
Last updated less than a minute ago
Actions
Create route table
Find resources by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
– rtb-0c36d1525f2dfd7f0 – – Yes vpc-03c4cba9e67a5
routetable-1public rtb-02df09f56161a2553 – – No vpc-0af41499c7b1a
– rtb-08a1c4af283b3c071 – – Yes vpc-0af41499c7b1a
routetable-2private rtb-0385617080b42a44f – – No vpc-0af41499c7b1a

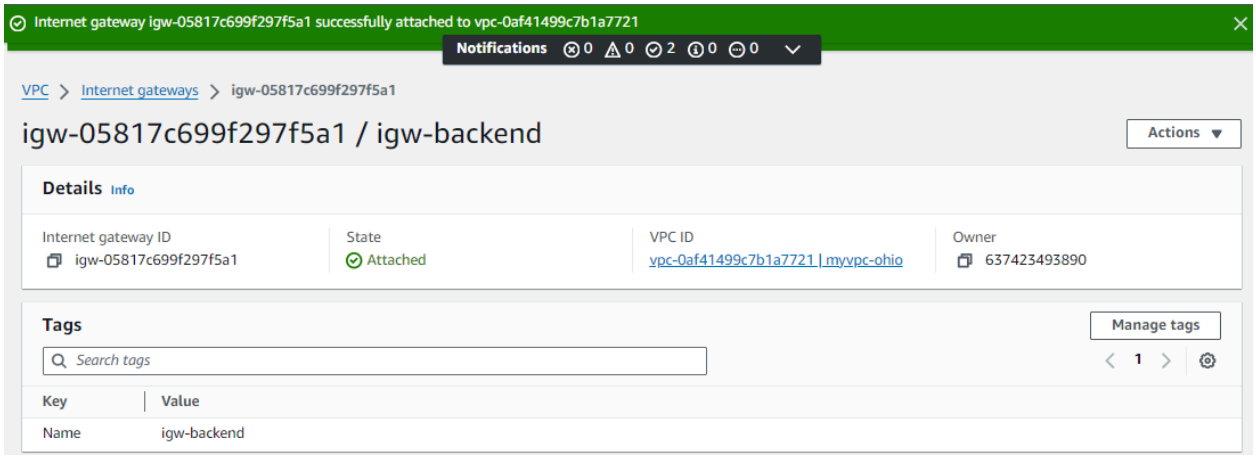

rtb-02df09f56161a2553 / routetable-1public
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (0)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR


You have successfully updated subnet associations for rtb-02df09f56161a2553 / routetable-1public.
Route tables (1/4) Info
Last updated less than a minute ago
Actions
Create route table
Find resources by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
– rtb-0c36d1525f2dfd7f0 – – Yes vpc-03c4cba9e67a5426c
routetable-1public rtb-02df09f56161a2553 subnet-08f7b36de23799... – No vpc-0af41499c7b1a7721

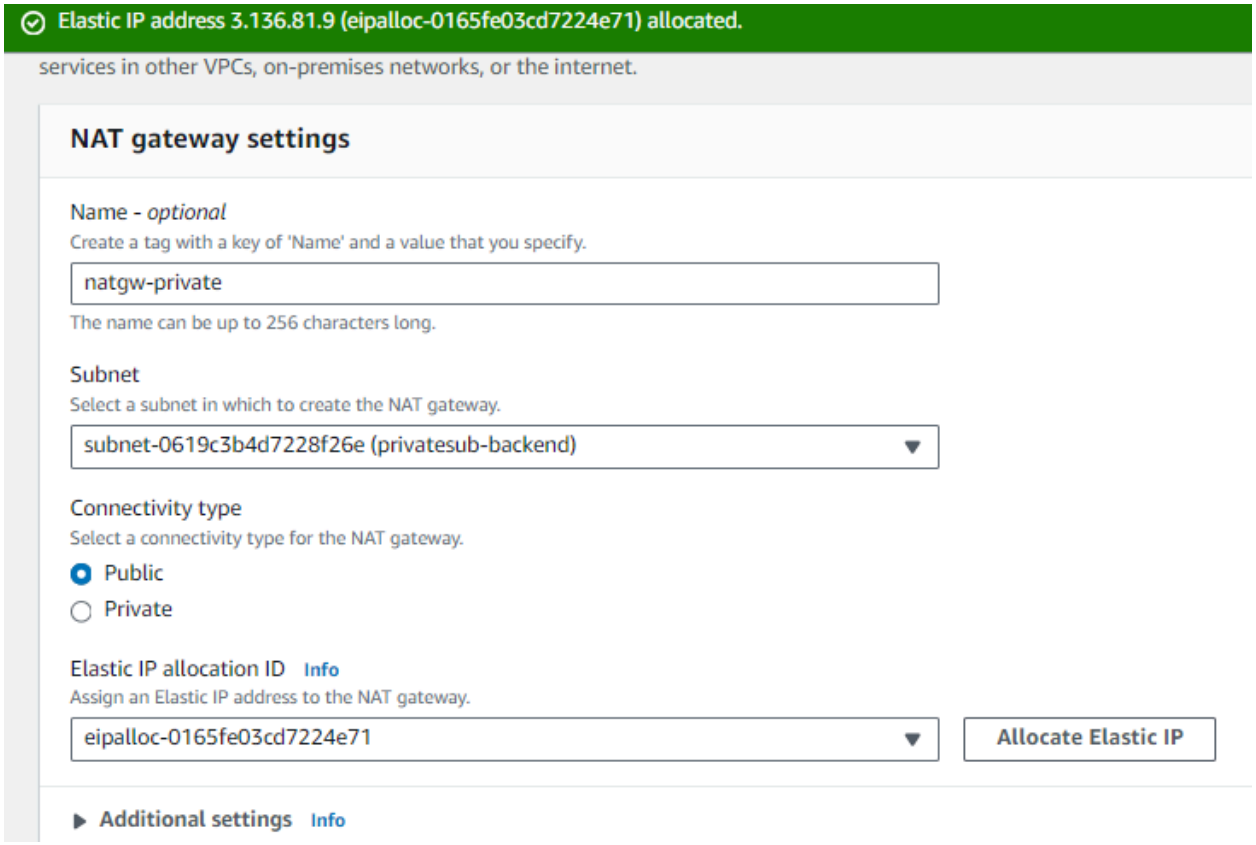

Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
privatesub-backend subnet-0619c3b4d7228f26e 10.10.0.80/28 – Main (rtb-08a1c4af283b3c071)
publicsub-backend subnet-08f7b36de237998d9 10.10.0.64/28 – rtb-02df09f56161a2553 / routetable-...
Selected subnets
subnet-0619c3b4d7228f26e / privatesub-backend
Cancel
Save associations


You have successfully updated subnet associations for rtb-0385617080b42a44f / routetable-2private.
Route tables (4) Info
Last updated
less than a minute ago
Find resources by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associat
– rtb-0c36d1525f2dfd7f0 – –
routetable-1public rtb-02df09f56161a2553 subnet-08f7b36de23799... –
– rtb-08a1c4af283b3c071 – –
routetable-2private rtb-0385617080b42a44f subnet-0619c3b4d7228f... –


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.
igw-backend
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
Name
igw-backend
Remove
Add new tag
You can add 49 more tags.
Cancel
Create internet gateway



CREATE NAT GATEWAY



LAUNCH AN INSTANCE IN OHIO REGION

Name

Public-server

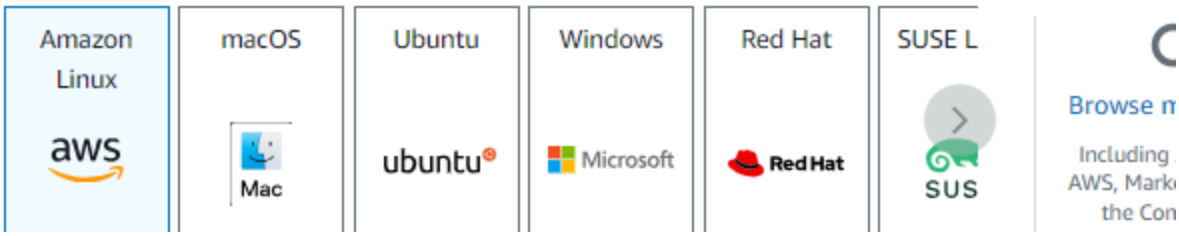
Add additiona

Application and OS Images (Amazon Machine Image) Info

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

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

Quick Start



Key pair name - *required*

key1 | Create new key pair

Network settings Info

VPC - *required* | Info

vpc-0af41499c7b1a7721 (myvpc-ohio)
10.10.0.64/26

Subnet | Info

subnet-08f7b36de237998d9 publicsub-backend
VPC: vpc-0af41499c7b1a7721 Owner: 637423493890 Availability Zone: us-east-2a
IP addresses available: 11 CIDR: 10.10.0.64/28)

Create new subnet

Auto-assign public IP | Info

Enable

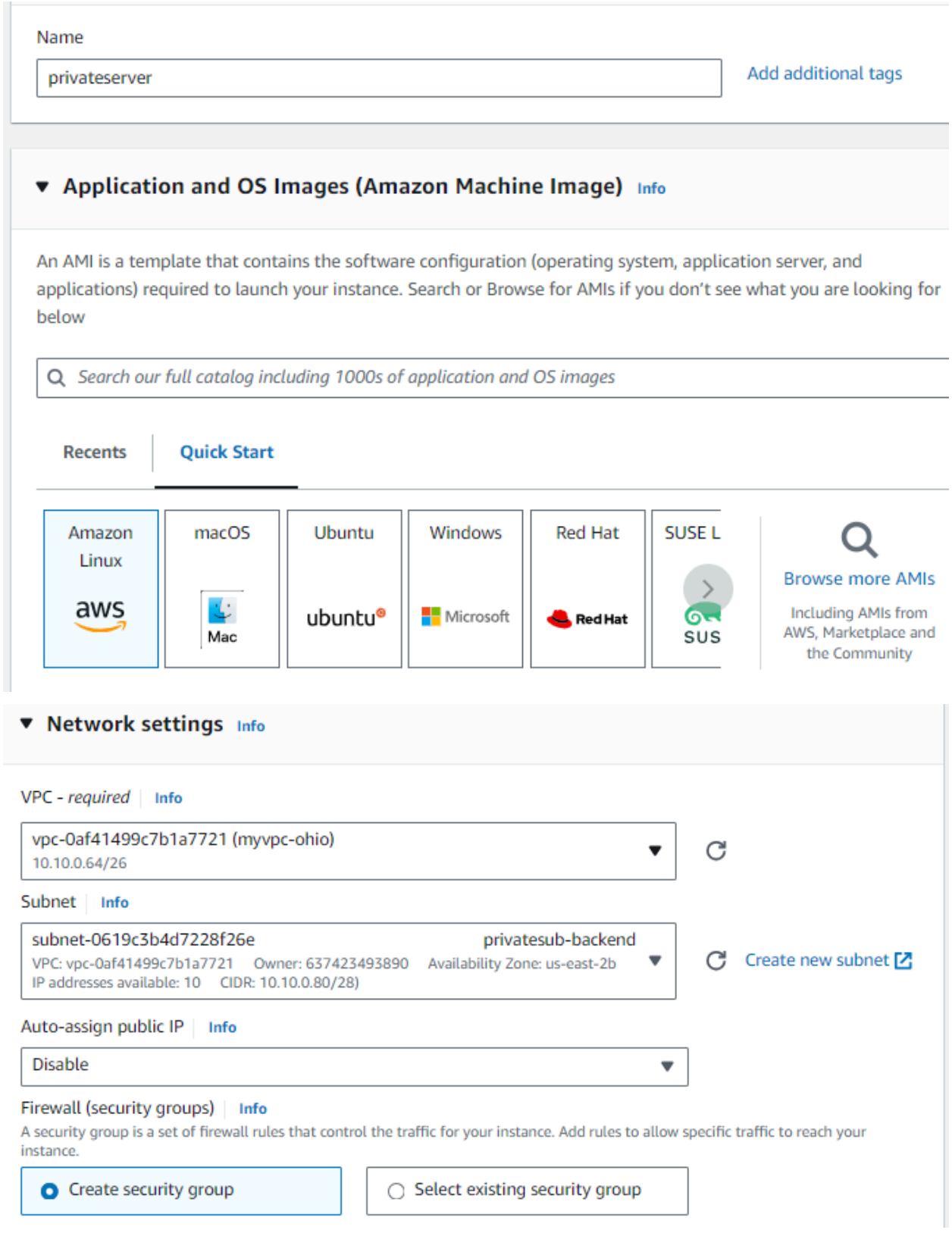
Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info

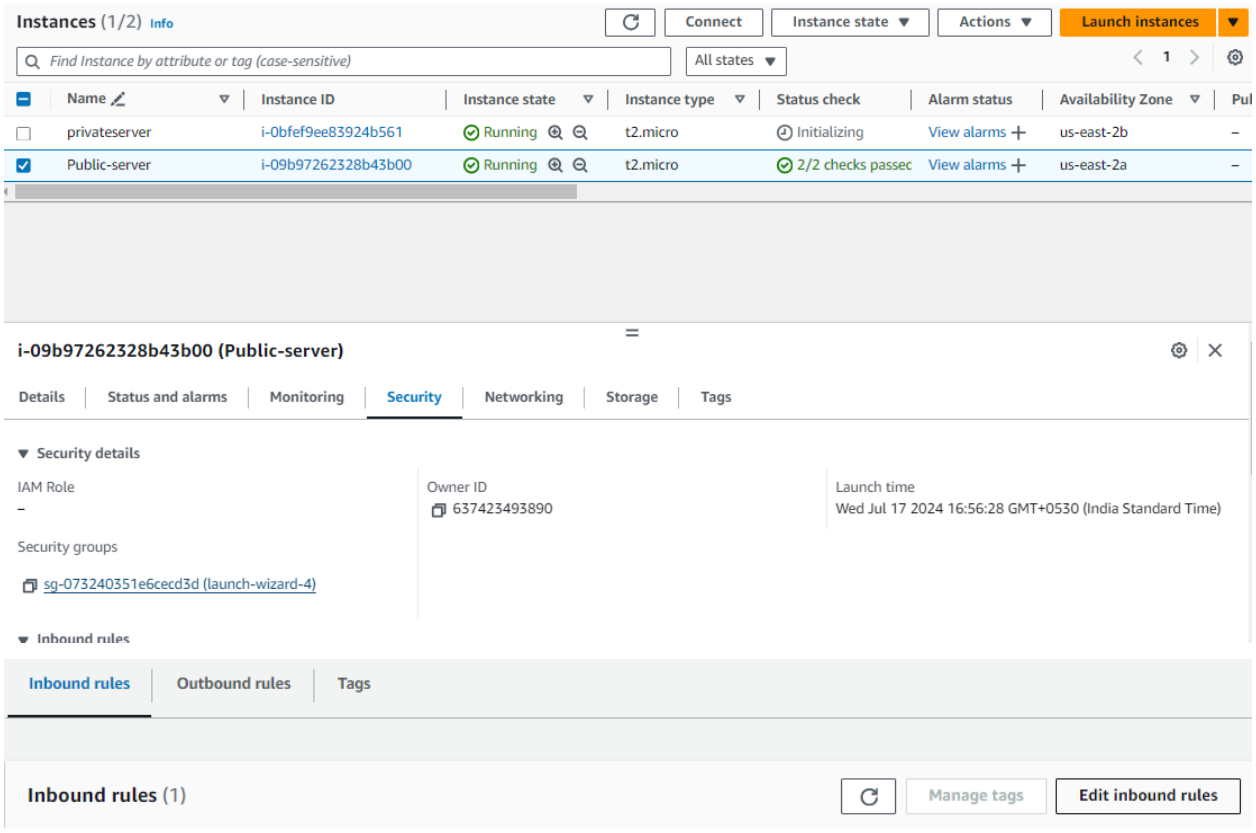
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

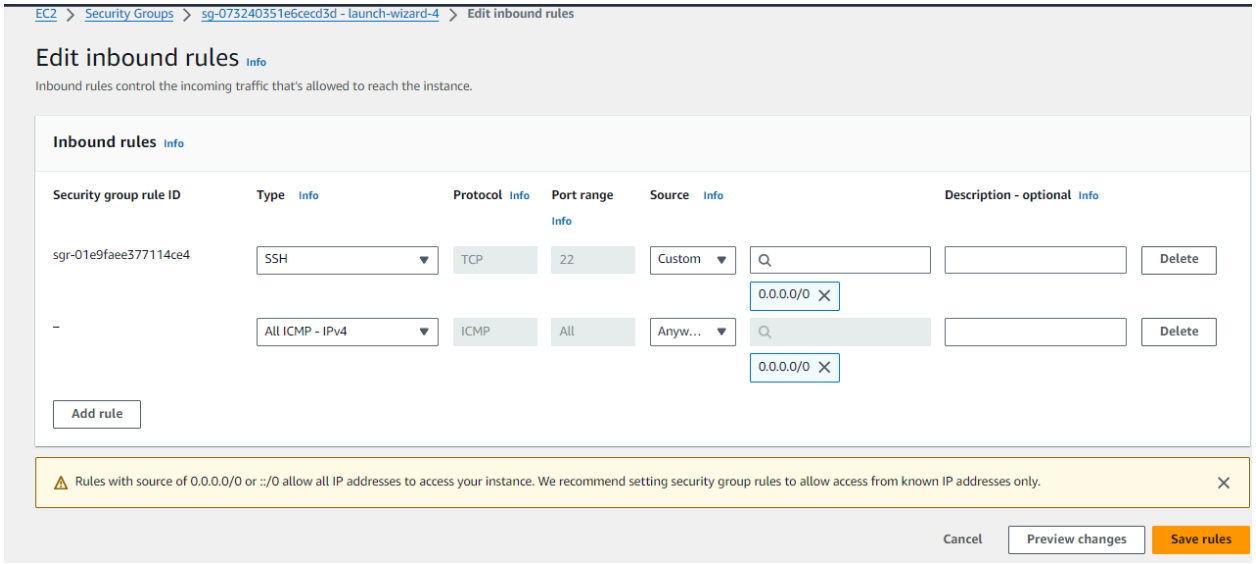
(•) Create security group ( ) Select existing security group

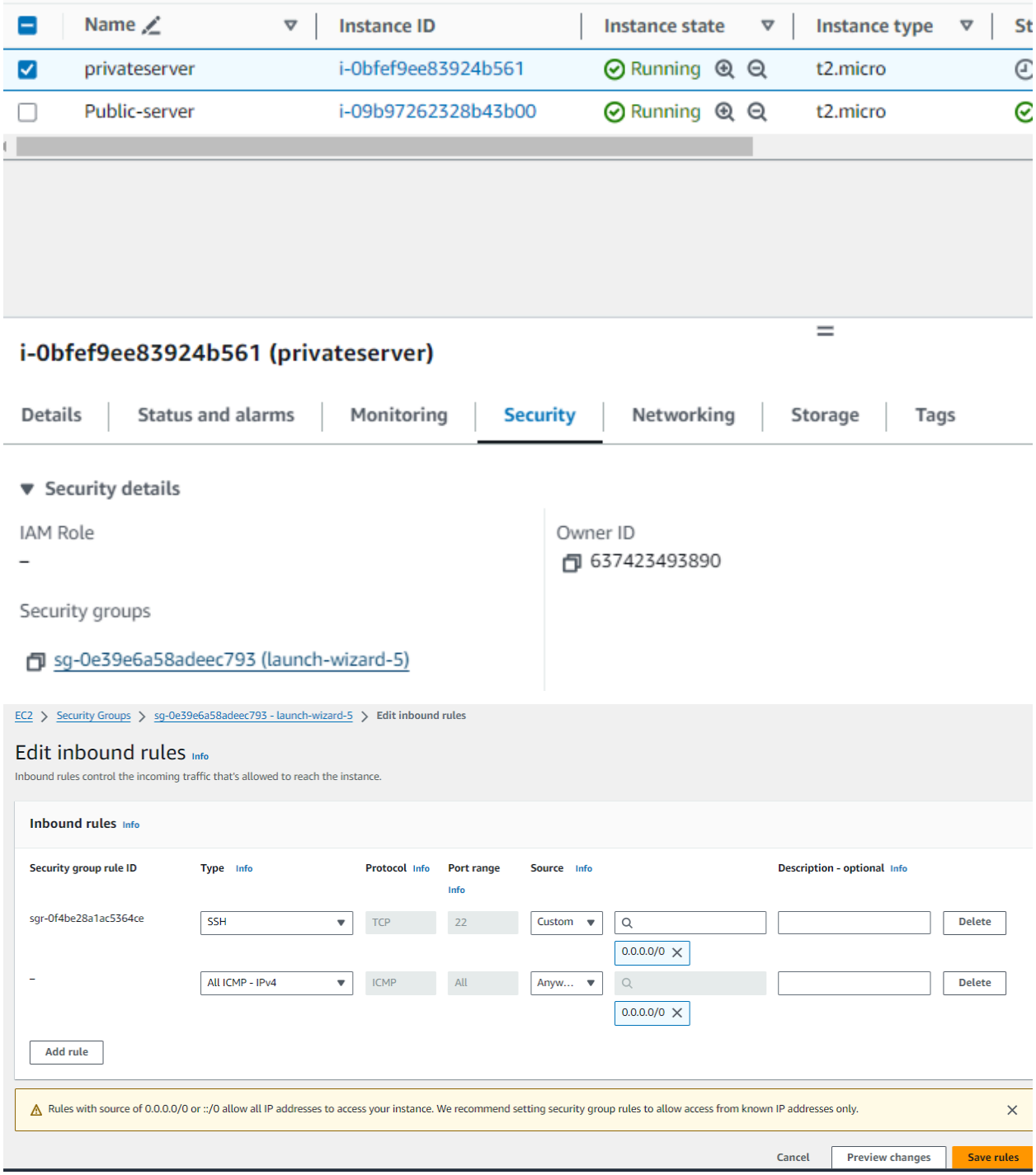
Create another ec2



ICMP


Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
privateserver
i-0bfef9ee83924b561
Running
t2.micro
Initializing
View alarms
us-east-2b
Public-server
i-09b97262328b43b00
Running
t2.micro
2/2 checks passed
View alarms
us-east-2a
i-09b97262328b43b00 (Public-server)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Security details
IAM Role
–
Owner ID
637423493890
Launch time
Wed Jul 17 2024 16:56:28 GMT+0530 (India Standard Time)
Security groups
sg-073240351e6cecd3d (launch-wizard-4)
Inbound rules
Outbound rules
Tags
Inbound rules (1)
Manage tags
Edit inbound rules


EC2 > Security Groups > sg-073240351e6cecd3d - launch-wizard-4 > Edit inbound rules
Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
sgr-01e9faee377114ce4
SSH
TCP
22
Custom
0.0.0.0/0
Delete
–
All ICMP - IPv4
ICMP
All
Anyw...
0.0.0.0/0
Delete
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Cancel
Preview changes
Save rules



In MUMBAI region

Network settings Info

VPC - *required* Info

vpc-020901b0749fa3e0c (front-M)
10.10.0.0/26

Subnet Info

subnet-095b91082f6ade5b2 public-sub
VPC: vpc-020901b0749fa3e0c Owner: 637423493890
Availability Zone: ap-south-1a IP addresses available: 11 CIDR: 10.10.0.0/28)

Create new subnet

Auto-assign public IP Info

Enable

Security group rule 2 (ICMP, All, 0.0.0.0/0)

Remove

Type Info	Protocol Info	Port range Info
All ICMP - IPv4	ICMP	All

Source type Info	Source Info	Description - *optional* Info
Anywhere	Add CIDR, prefix list or security	e.g. SSH for admin desktop

0.0.0.0/0

Services Search [Alt+S] Mumbai

EC2 > Instances > Launch an instance

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
publicserver-front2

Add additional tags

Application and OS Images (Amazon Machine Image) Info

Summary

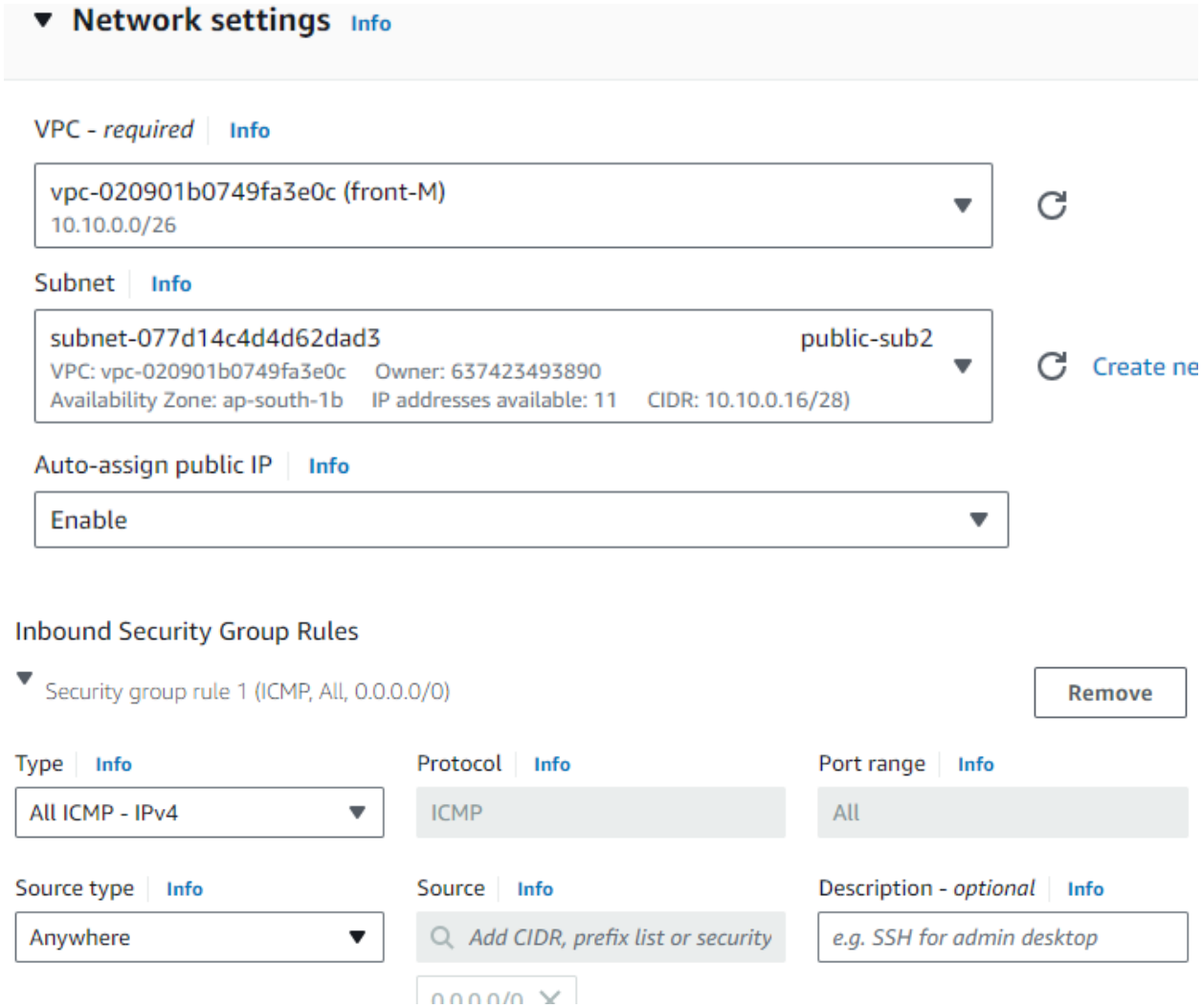
Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-0ec0e125bb6c6e8ec

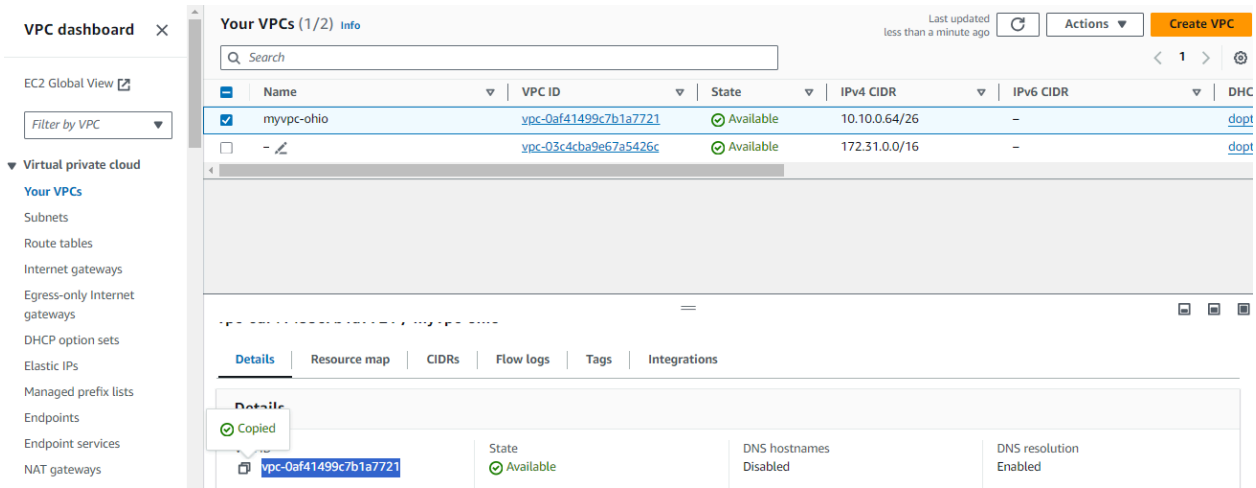
Virtual server type (instance type)
t2.micro

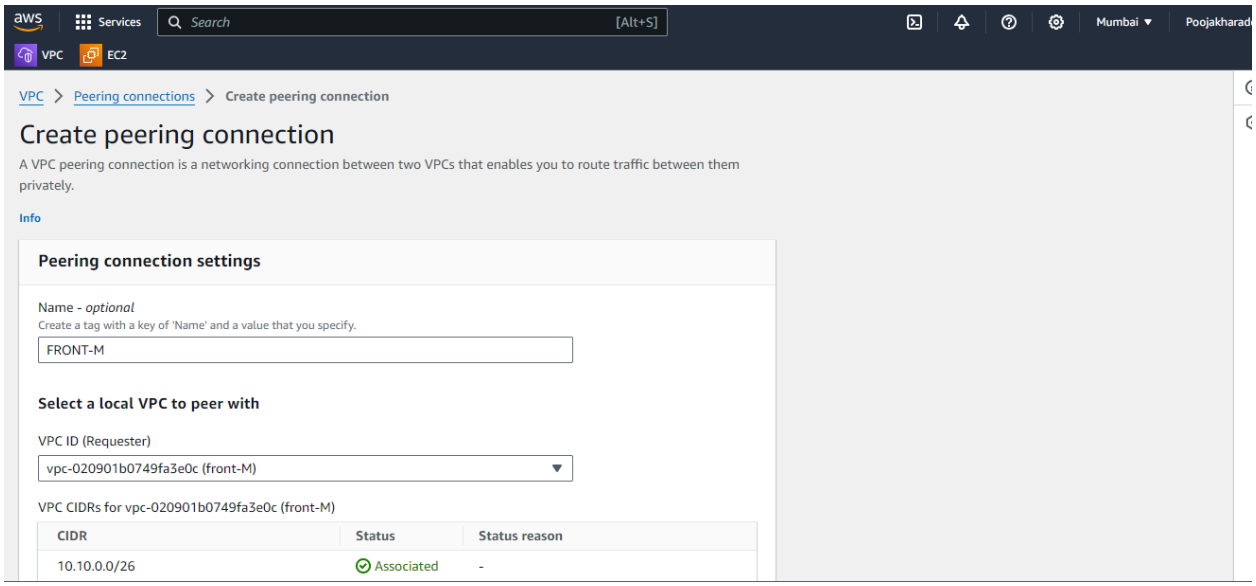
Firewall (security group)
New security group

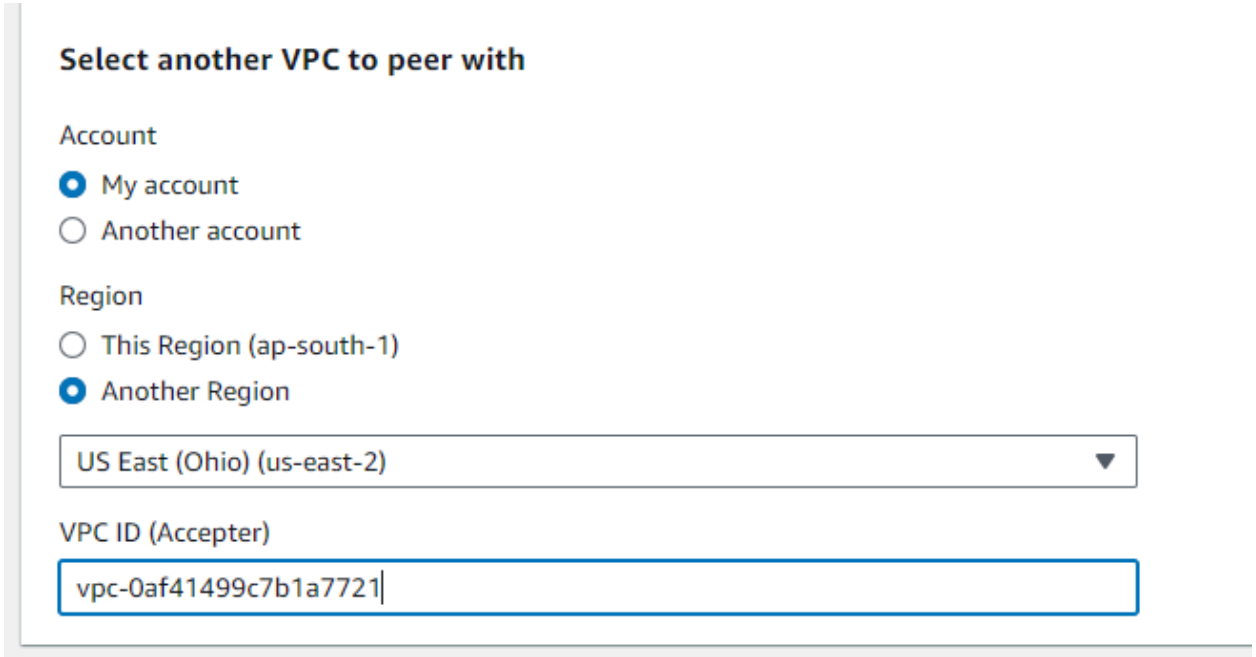
Storage (volumes)



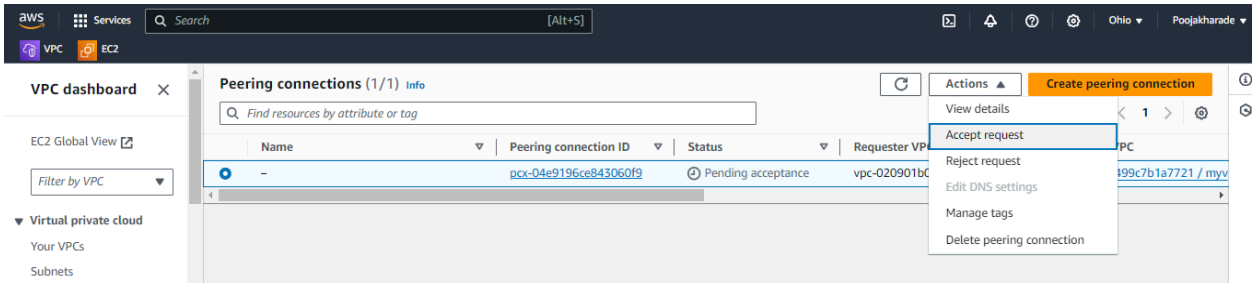
IN MUMBAI REGION (PUBLIC) - PEERING CONNECTIONS







ACCEPT REQUEST



Accept VPC peering connection request Info

Are you sure you want to accept this VPC peering connection request? (pcx-04e9196ce843060f9)

Requester VPC
vpc-020901b0749fa3e0c

Accepter CIDRs
–

Requester owner ID
637423493890
(This account)

Accepter VPC
vpc-0af41499c7b1a7721 / myvpc-ohio

Requester Region
Mumbai (ap-south-1)

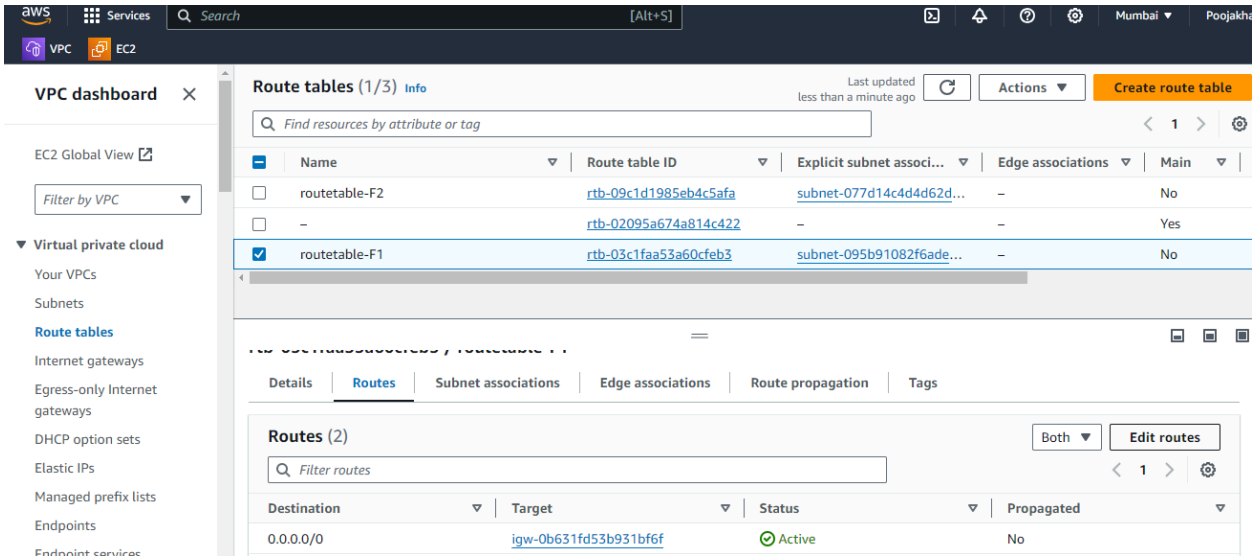
Accepter owner ID
637423493890
(This account)

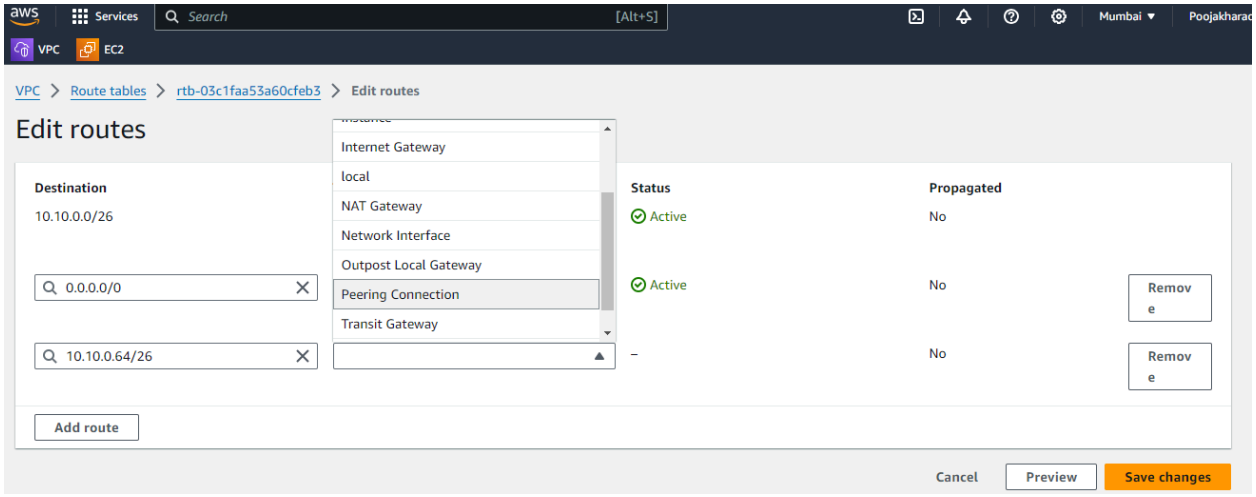
Requester CIDRs
10.10.0.0/26

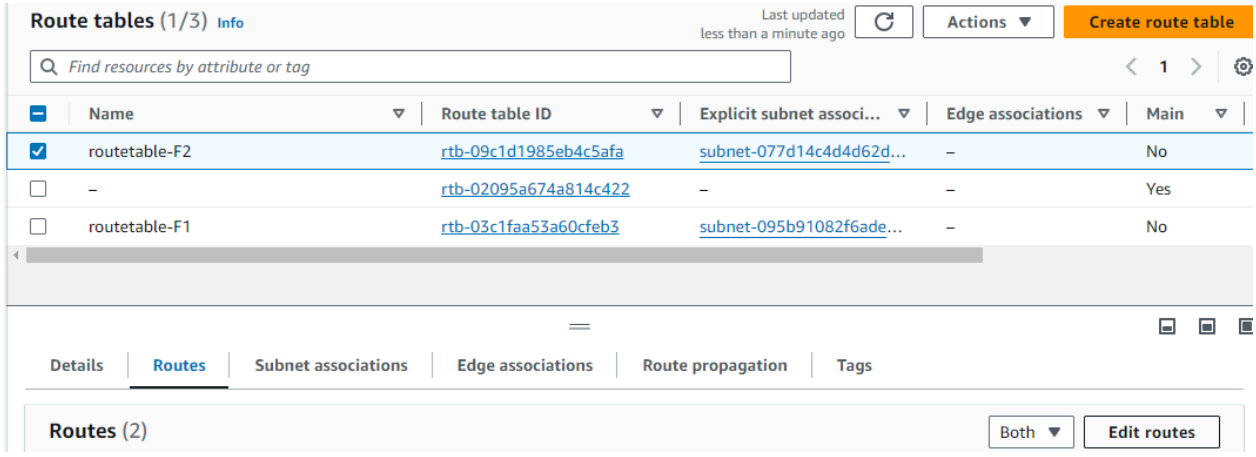
Accepter Region
Ohio (us-east-2)

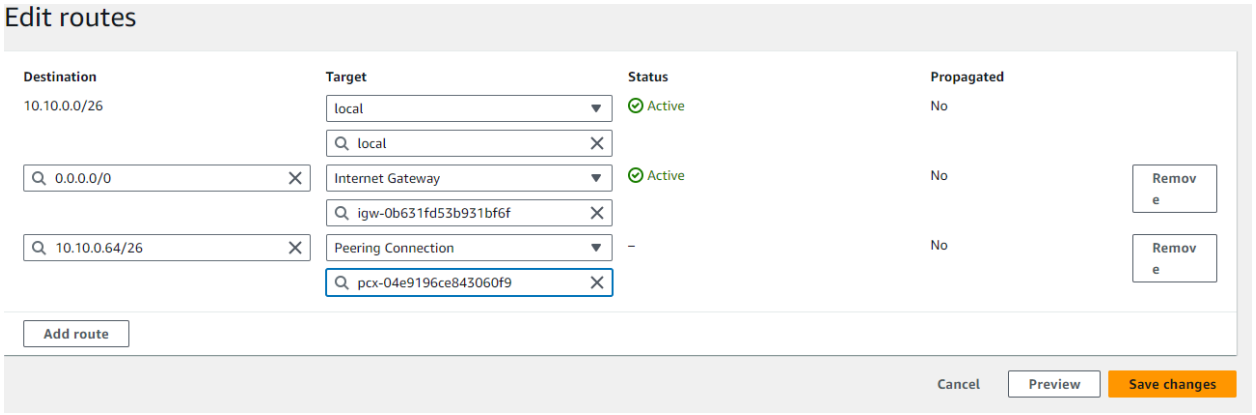
Cancel | Accept request

IN MUMBAI REGION

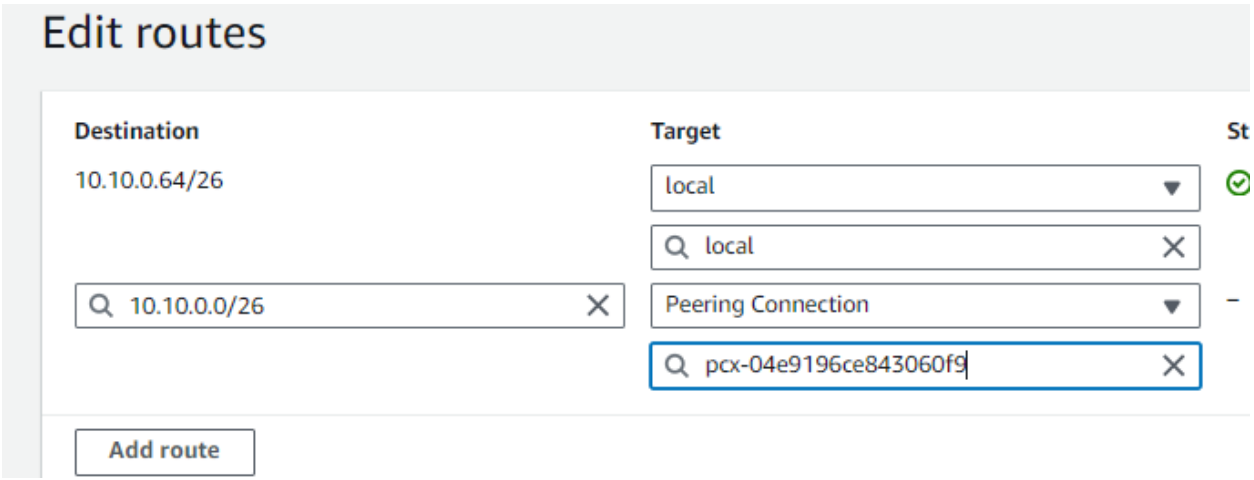


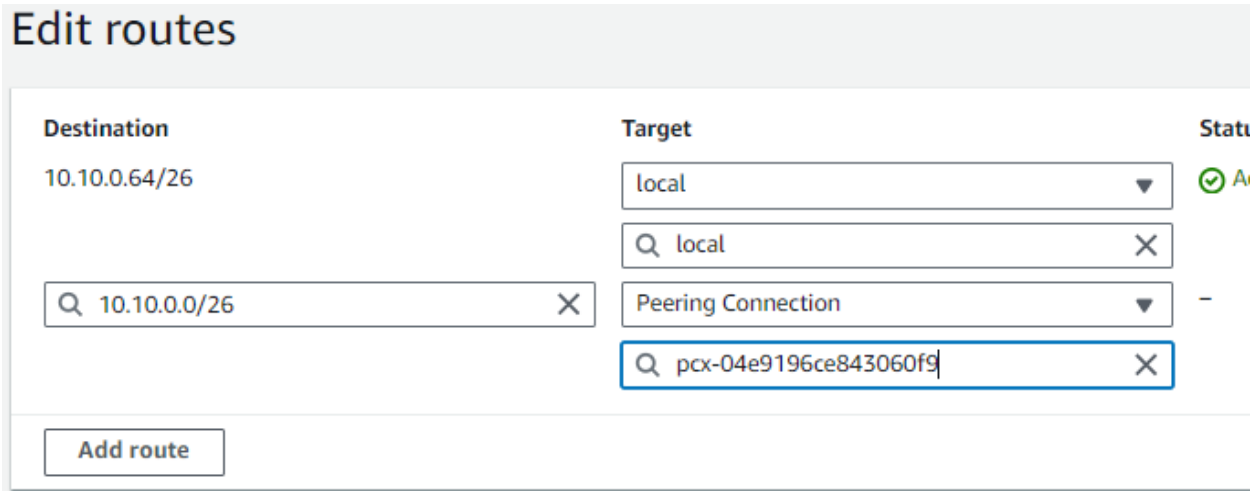




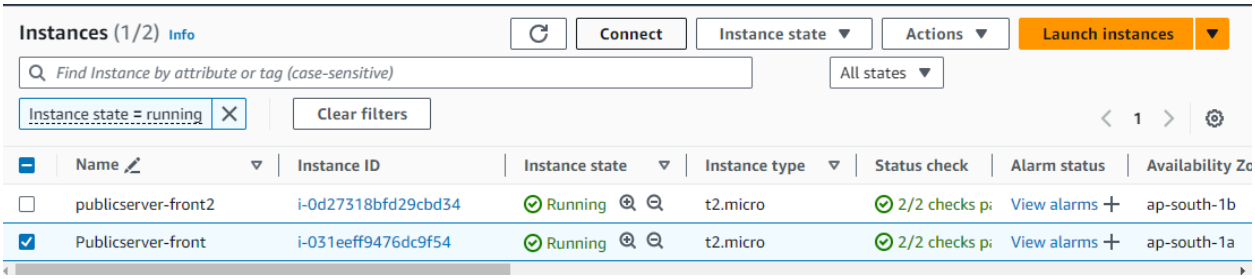


IN OHIO REGION





Connect

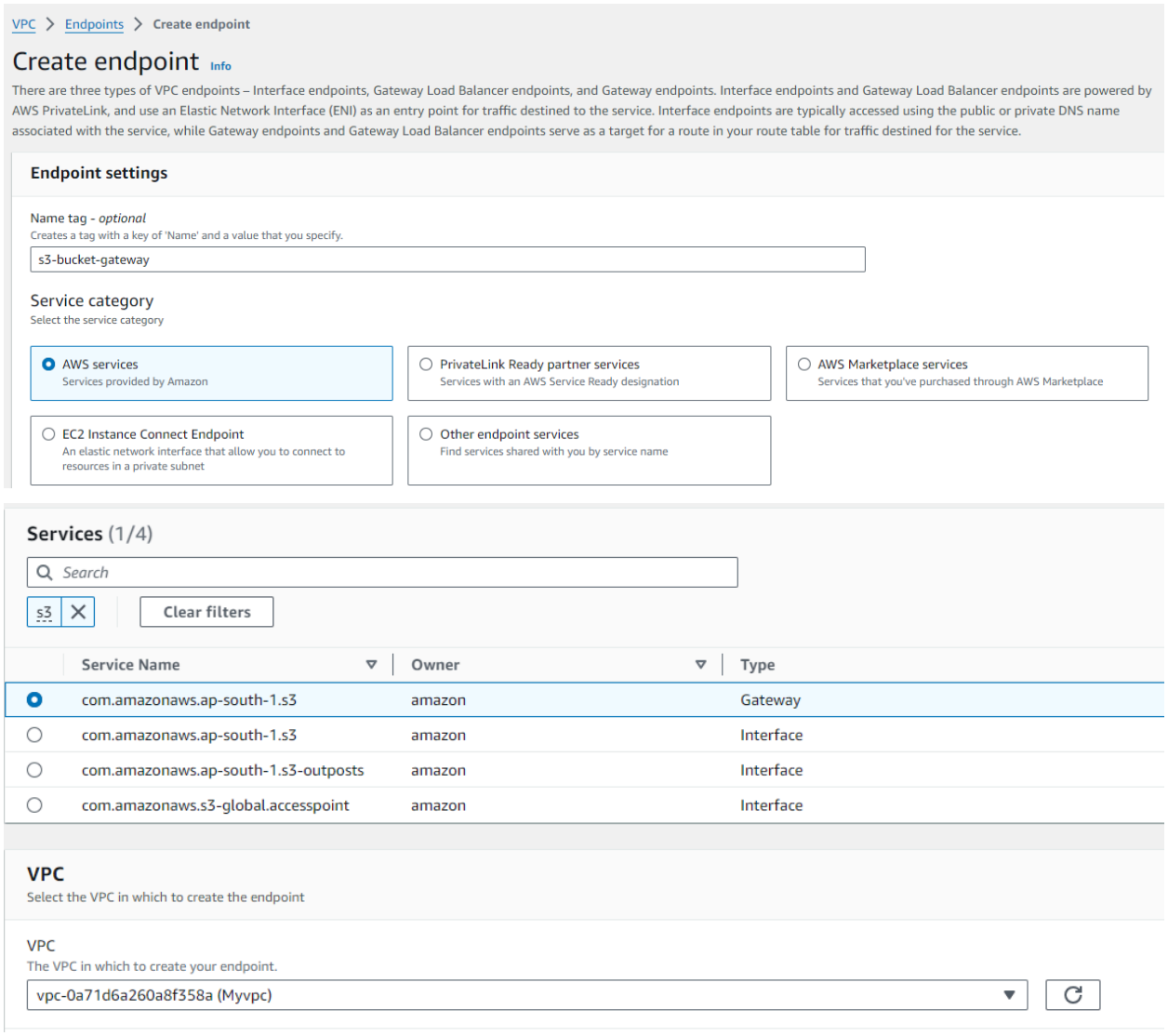


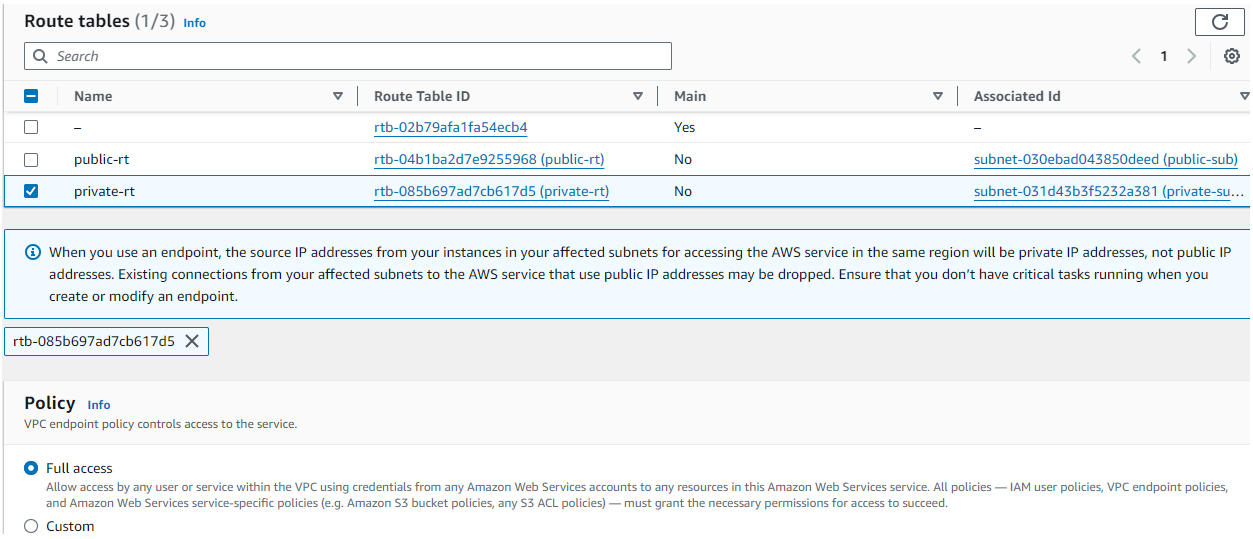
Output

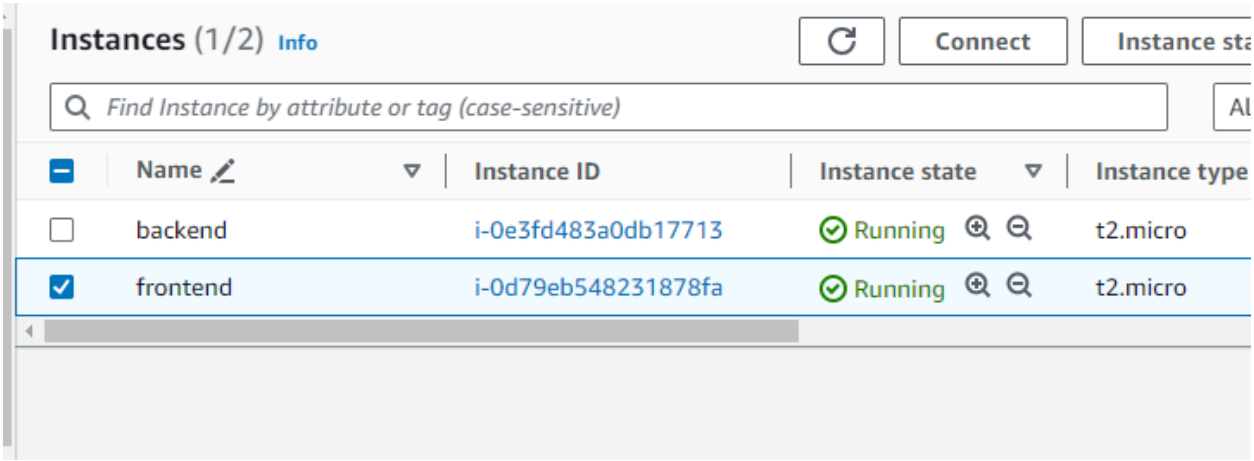
```
      _/m/'
[ec2-user@ip-10-10-0-11 ~]$ ping 10.10.0.25
PING 10.10.0.25 (10.10.0.25) 56(84) bytes of data.
64 bytes from 10.10.0.25: icmp_seq=1 ttl=127 time=1.27 ms
64 bytes from 10.10.0.25: icmp_seq=2 ttl=127 time=0.824 ms
64 bytes from 10.10.0.25: icmp_seq=3 ttl=127 time=0.817 ms
^C
--- 10.10.0.25 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.817/0.971/1.272/0.212 ms
[ec2-user@ip-10-10-0-11 ~]$ ping 10.10.0.86
PING 10.10.0.86 (10.10.0.86) 56(84) bytes of data.
64 bytes from 10.10.0.86: icmp_seq=1 ttl=127 time=212 ms
64 bytes from 10.10.0.86: icmp_seq=2 ttl=127 time=212 ms
^C
--- 10.10.0.86 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 212.066/212.145/212.224/0.079 ms
[ec2-user@ip-10-10-0-11 ~]$ vi key.pem
[ec2-user@ip-10-10-0-11 ~]$ chmod 400 key.pem
[ec2-user@ip-10-10-0-11 ~]$ ssh -i "key.pem" ec2-user@10.10.0.86
The authenticity of host '10.10.0.86 (10.10.0.86)' can't be established.
ED25519 key fingerprint is SHA256:7WnMWH6bNWwHIURkGD1yk6TQtpYVTpzBOLqxmCRLEzc.
This key is not known by any other names
```

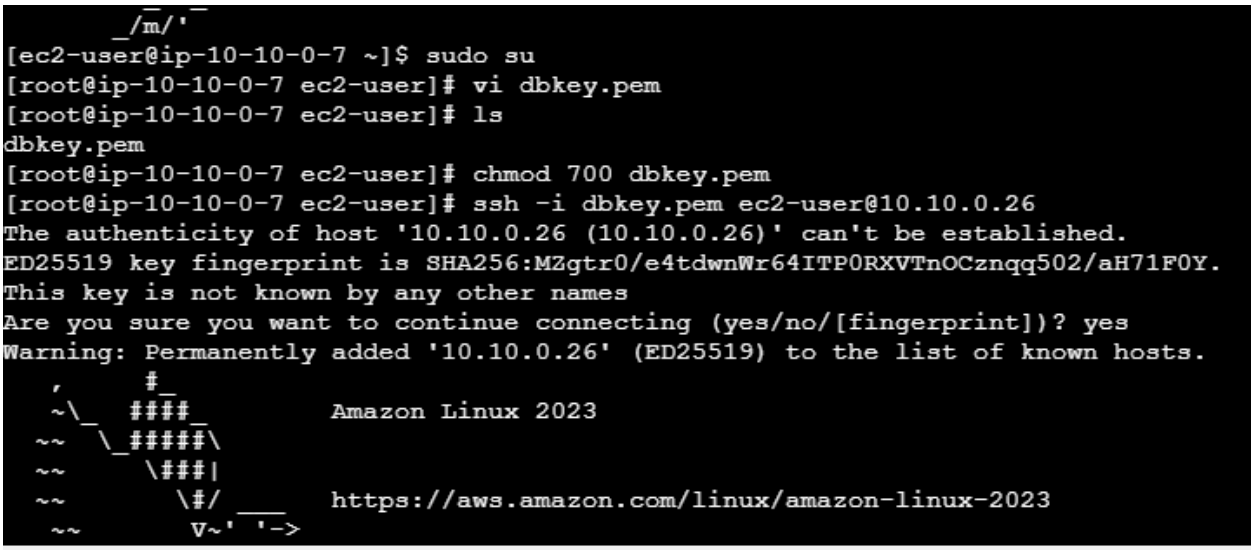
```
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.0.86' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-10-0-86 ~]$
```

18-07-24 S3 ENDPOINT

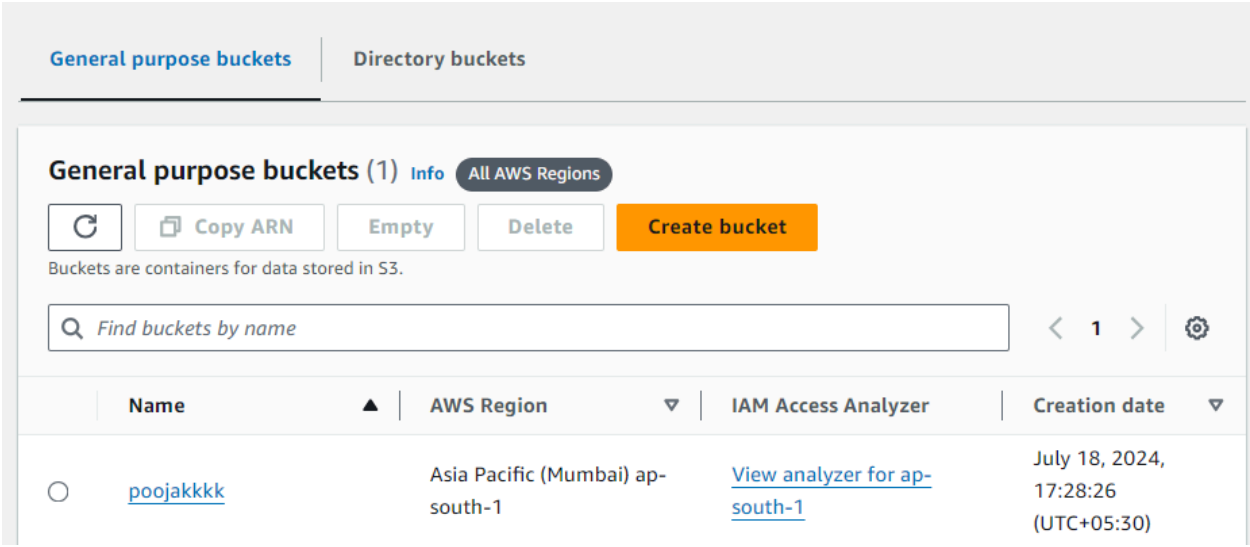



Route tables (1/3) Info
Search
1
Name
Route Table ID
Main
Associated Id
– rtb-02b79afa1fa54ecb4 Yes –
public-rt rtb-04b1ba2d7e9255968 (public-rt) No subnet-030ebad043850deed (public-sub)
private-rt rtb-085b697ad7cb617d5 (private-rt) No subnet-031d43b3f5232a381 (private-su...
When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.
rtb-085b697ad7cb617d5
Policy Info
VPC endpoint policy controls access to the service.
Full access
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.
Custom


Instances (1/2) Info
Connect
Find Instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
backend i-0e3fd483a0db17713 Running t2.micro
frontend i-0d79eb548231878fa Running t2.micro


[ec2-user@ip-10-10-0-7 ~]$ sudo su
[root@ip-10-10-0-7 ec2-user]# vi dbkey.pem
[root@ip-10-10-0-7 ec2-user]# ls
dbkey.pem
[root@ip-10-10-0-7 ec2-user]# chmod 700 dbkey.pem
[root@ip-10-10-0-7 ec2-user]# ssh -i dbkey.pem ec2-user@10.10.0.26
The authenticity of host '10.10.0.26 (10.10.0.26)' can't be established.
ED25519 key fingerprint is SHA256:MZgtr0/e4tdwnWr64ITP0RXVTnOCznqq502/aH71F0Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.0.26' (ED25519) to the list of known hosts.
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

```
[ec2-user@ip-10-10-0-26 ~]$ aws s3 mb s3://fghjk
make_bucket failed: s3://fghjk Unable to locate credentials
[ec2-user@ip-10-10-0-26 ~]$ aws configure
AWS Access Key ID [None]: AKIAZI2LGUMBNPAFSRF2
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]: json
[ec2-user@ip-10-10-0-26 ~]$ aws s3 mb s3://poojak
make_bucket failed: s3://poojak An error occurred (BucketAlreadyExists) when calling the CreateBucket operation: The requested bucket name is n
ot available. The bucket namespace is shared by all users of the system. Please select a different name and try again.
[ec2-user@ip-10-10-0-26 ~]$ aws s3 mb s3://pk1234
make_bucket failed: s3://pk1234 An error occurred (BucketAlreadyExists) when calling the CreateBucket operation: The requested bucket name is n
ot available. The bucket namespace is shared by all users of the system. Please select a different name and try again.
[ec2-user@ip-10-10-0-26 ~]$ aws s3 mb s3://poojakkkk
make_bucket: poojakkkk
[ec2-user@ip-10-10-0-26 ~]$
```

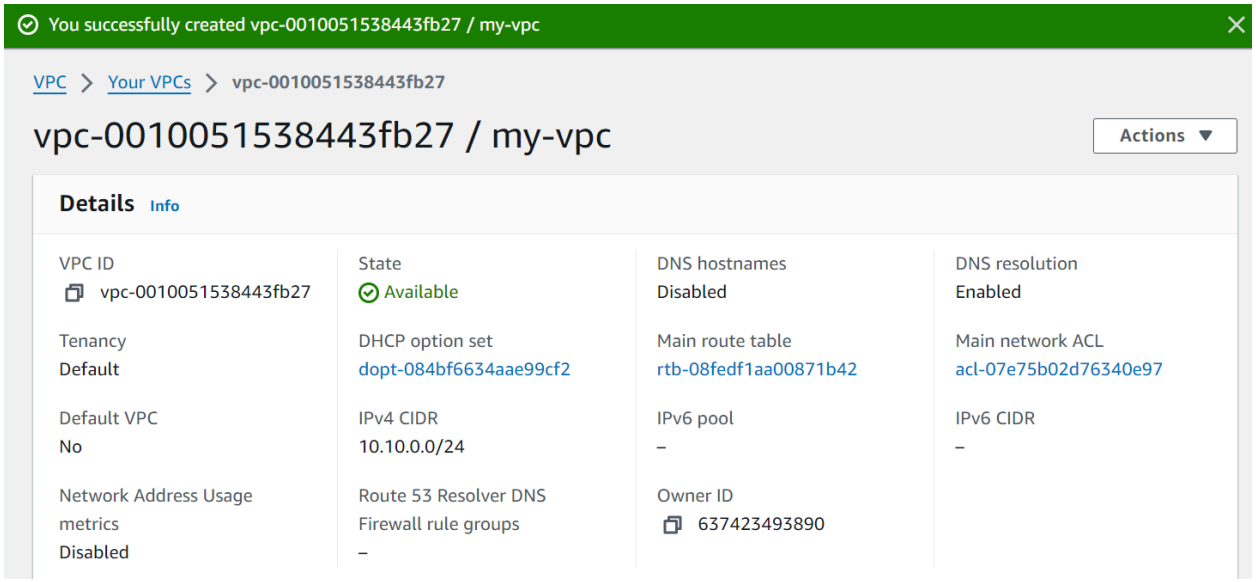


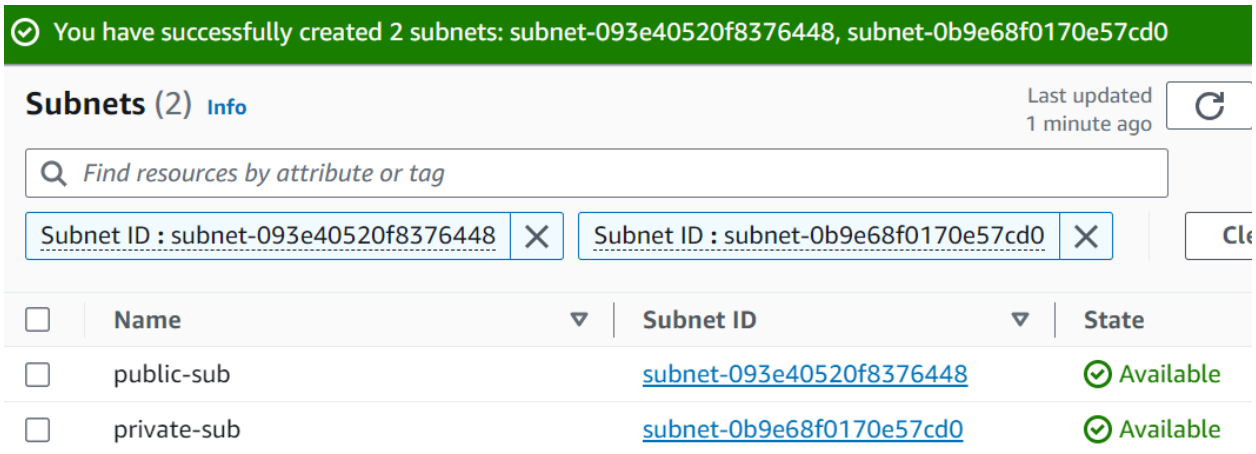

```
[ec2-user@ip-10-10-0-26 ~]$ aws s3 mb s3://fghjk
make_bucket failed: s3://fghjk Unable to locate credentials
[ec2-user@ip-10-10-0-26 ~]$ aws configure
AWS Access Key ID [None]: AKIAZI2LGUMBNPAFSRF2
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]: json
[ec2-user@ip-10-10-0-26 ~]$ aws s3 mb s3://poojak
make_bucket failed: s3://poojak An error occurred (BucketAlreadyExists) when calling the CreateBucket operation: The requested bucket name is n
ot available. The bucket namespace is shared by all users of the system. Please select a different name and try again.
[ec2-user@ip-10-10-0-26 ~]$ aws s3 mb s3://pk1234
make_bucket failed: s3://pk1234 An error occurred (BucketAlreadyExists) when calling the CreateBucket operation: The requested bucket name is n
ot available. The bucket namespace is shared by all users of the system. Please select a different name and try again.
[ec2-user@ip-10-10-0-26 ~]$ aws s3 mb s3://poojakkkk
make_bucket: poojakkkk
[ec2-user@ip-10-10-0-26 ~]$ ls
[ec2-user@ip-10-10-0-26 ~]$ aws s3 mb s3://poojakkkk
make_bucket failed: s3://poojakkkk An error occurred (BucketAlreadyOwnedByYou) when calling the CreateBucket operation: Your previous request t
o create the named bucket succeeded and you already own it.
[ec2-user@ip-10-10-0-26 ~]$ aws s3://poojakkkk
```

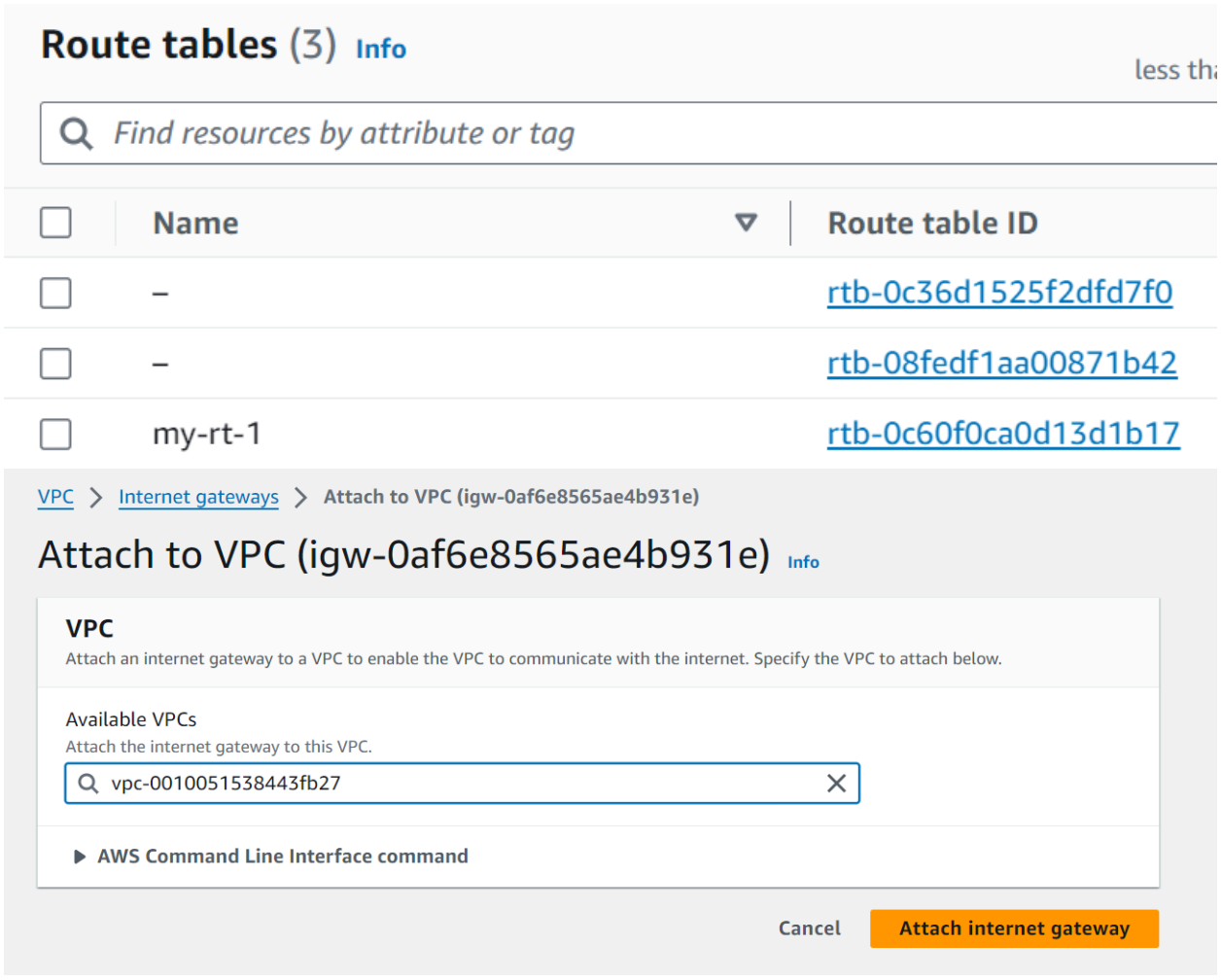
```
[ec2-user@ip-10-10-0-26 ~]$ aws s3 ls s3://poojakkkk
2024-07-18 12:00:27      34698 1.jpg
[ec2-user@ip-10-10-0-26 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-10-0-26 ~]$ cp ^C
[ec2-user@ip-10-10-0-26 ~]$ aws s3 cp s3://poojakkkk /home/ec2-user
[ec2-user@ip-10-10-0-26 ~]$ ls
[ec2-user@ip-10-10-0-26 ~]$ aws s3 cp s3://poojakkkk/  /home/ec2-user
[ec2-user@ip-10-10-0-26 ~]$ aws s3 cp s3://poojakkkk/1.jpg  /home/ec2-user
download: s3://poojakkkk/1.jpg to ./1.jpg
[ec2-user@ip-10-10-0-26 ~]$ aws s3 cp  /home/ec2-user s3://poojakkkk/1.jpg
upload failed: ./ to s3://poojakkkk/1.jpg [Errno 21] Is a directory: '/home/ec2-user/'
[ec2-user@ip-10-10-0-26 ~]$ aws s3 cp  /home/ec2-user/1.jpg  s3://poojakkkk/
upload: ./1.jpg to s3://poojakkkk/1.jpg
[ec2-user@ip-10-10-0-26 ~]$
```

23-7-24 SECURITY GROUP AND NACL

Create vpc





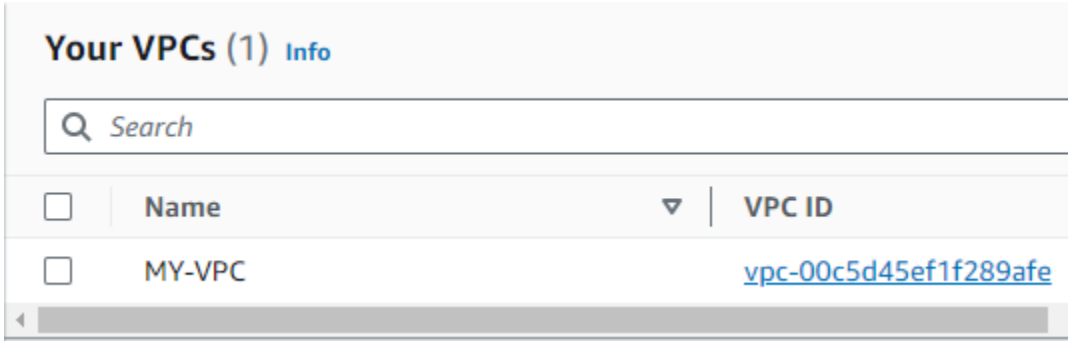


Create ec2 then create nacl

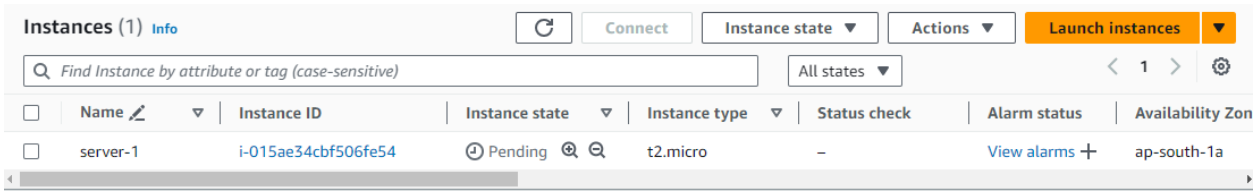
Cloudwatch

CLOUDTRAIL :

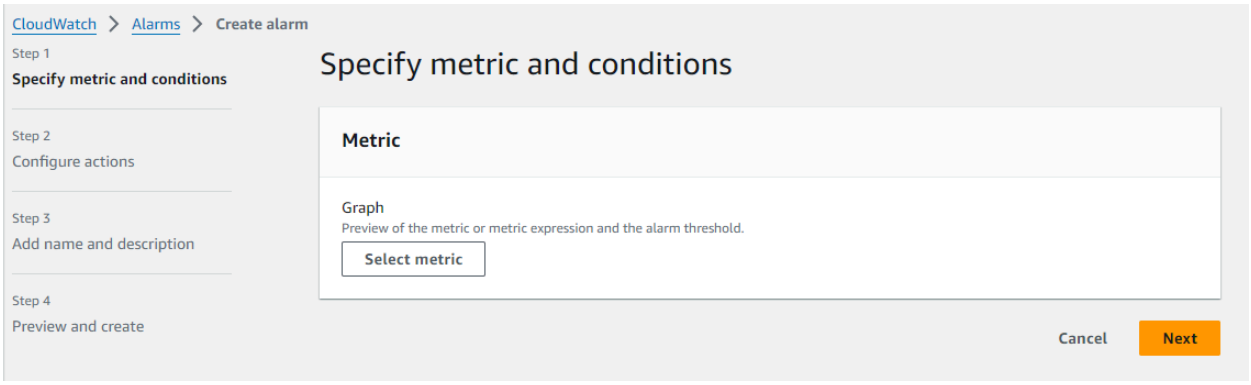
Create VPC > subnets > give Igw



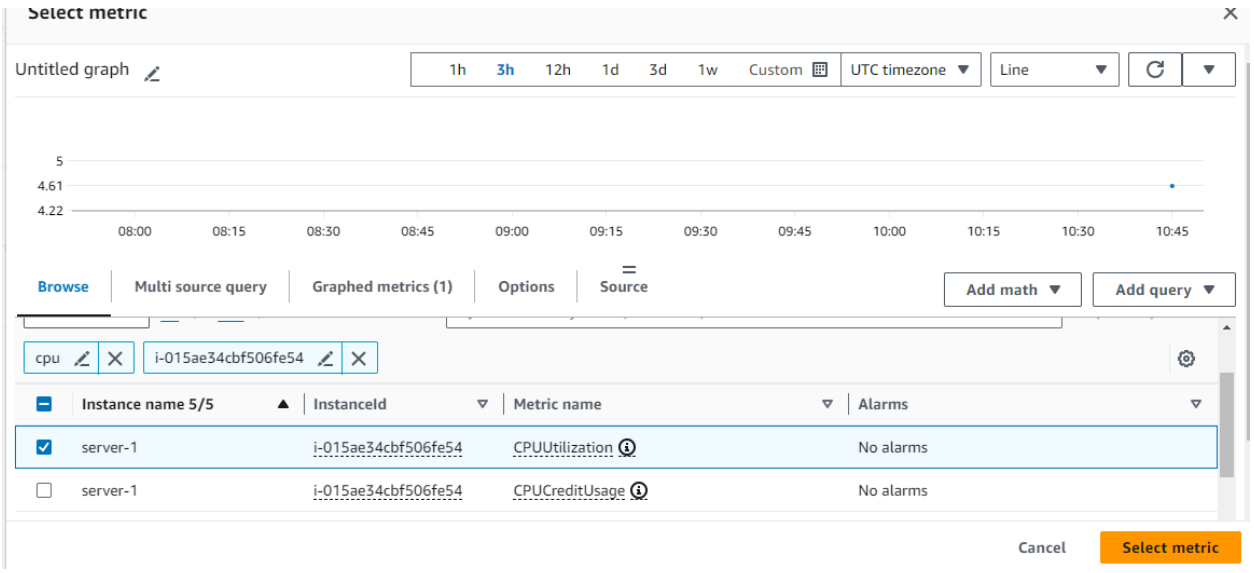
Create ec2



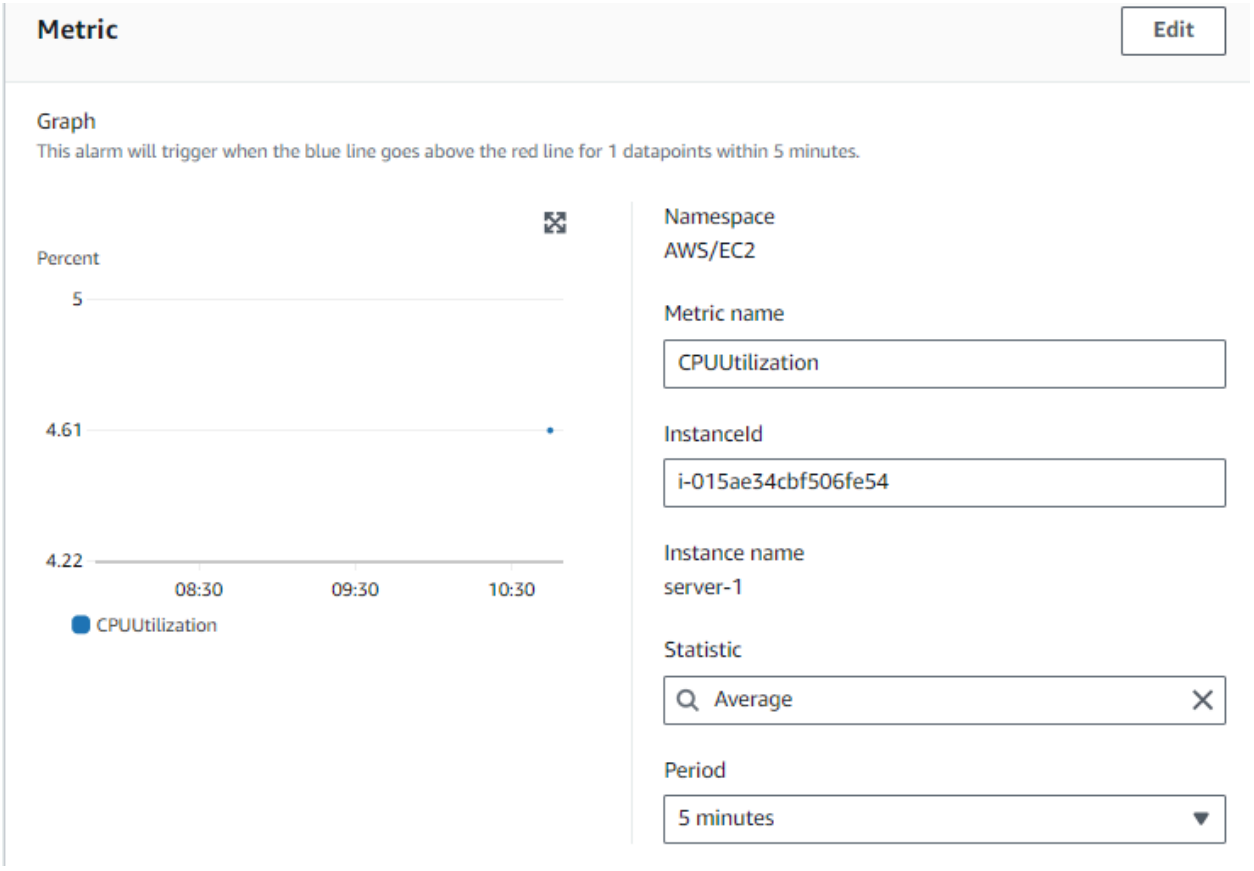
Cloudwatch > all alarms



Paste instance id : i-015ae34cbf506fe54



Select metric



Conditions

Threshold type

- (●) Static
  Use a value as a threshold
- ( ) Anomaly detection
  Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.

- (●) Greater
  > threshold
- ( ) Greater/Equal
  >= threshold
- ( ) Lower/Equal
  <= threshold
- ( ) Lower
  < threshold

than...
Define the threshold value.

50

Must be a number

▶ **Additional configuration**

Alarm state trigger
Define the alarm state that will trigger this action.

Remove

- (●) In alarm
  The metric or expression is outside of the defined threshold.
- ( ) OK
  The metric or expression is within the defined threshold.
- ( ) Insufficient data
  The alarm has just started or not enough data is available.

Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

- ( ) Select an existing SNS topic
- (●) Create new topic
- ( ) Use topic ARN to notify other accounts

Create a new topic...
The topic name must be unique.

pooja

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

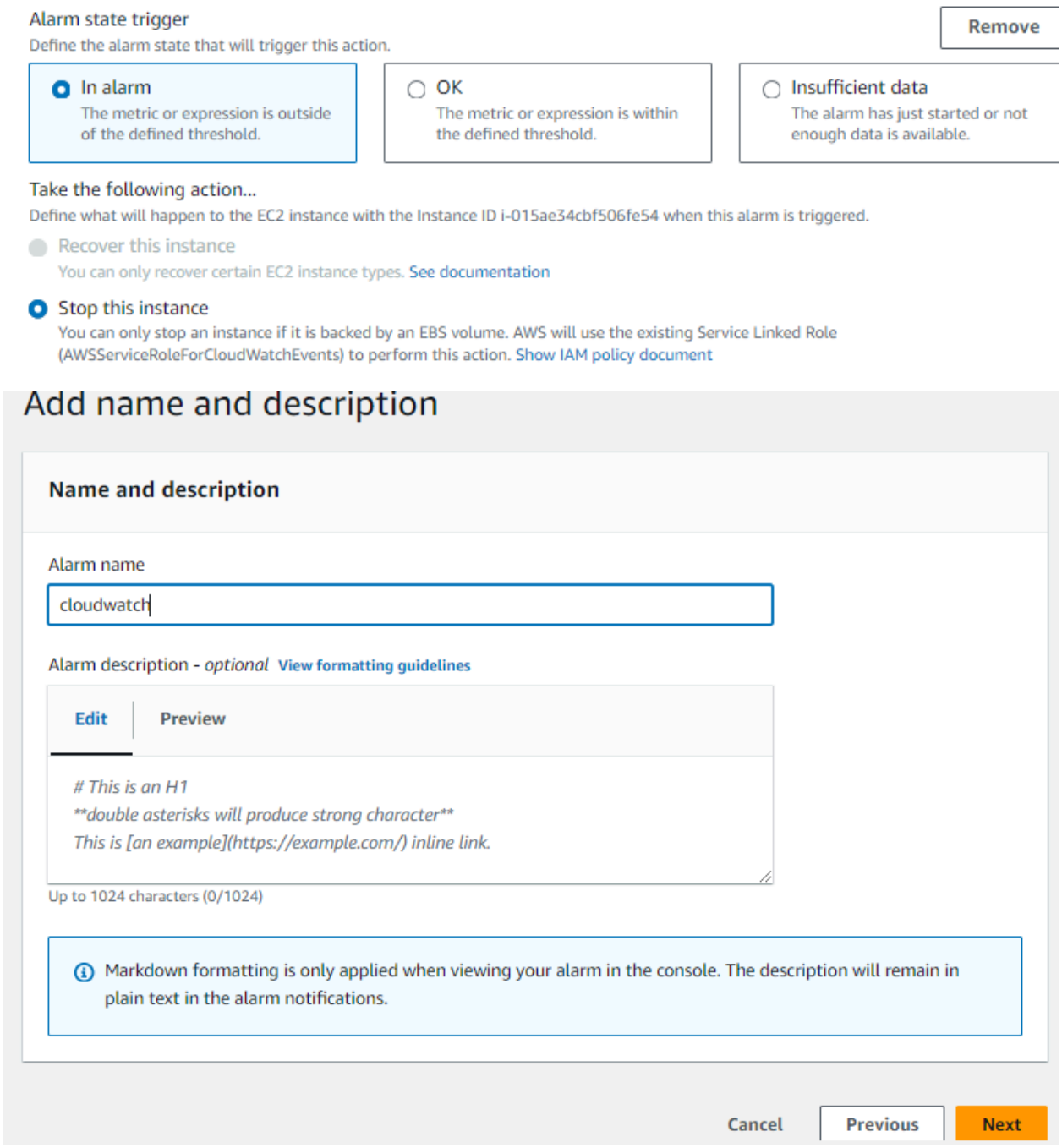
Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

pkharade2003@gmail.com

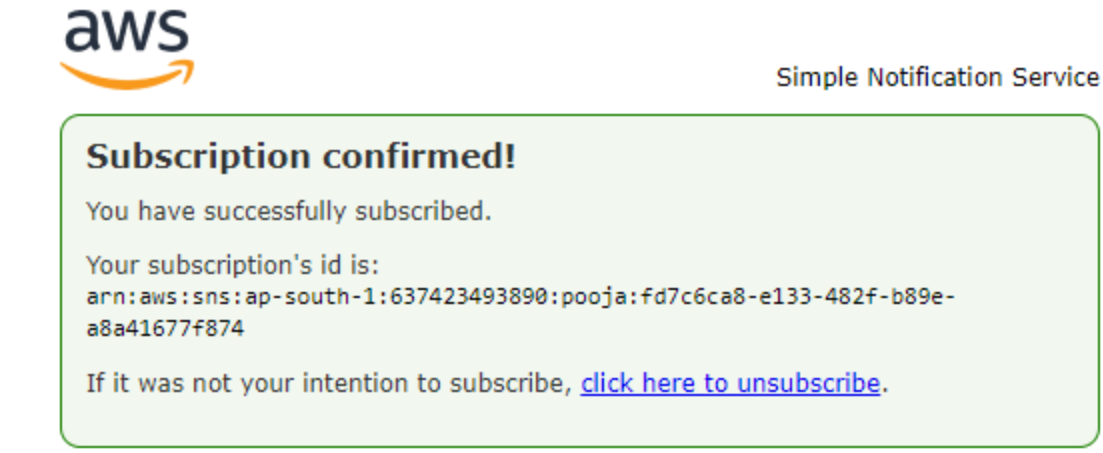
user1@example.com, user2@example.com

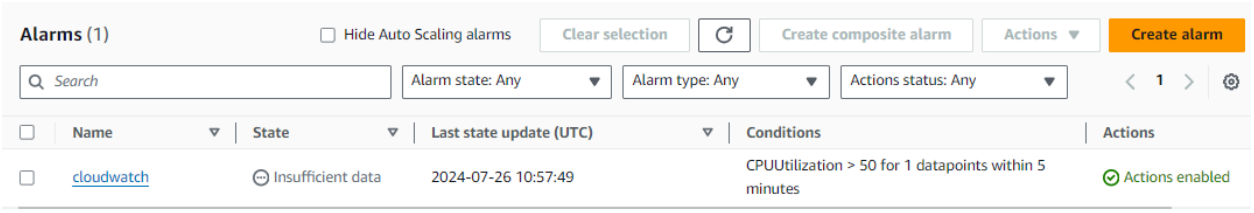
Create topic

Add notification



CONFIRM SUBSCRIPTION MAIL





Connect ec2 instance

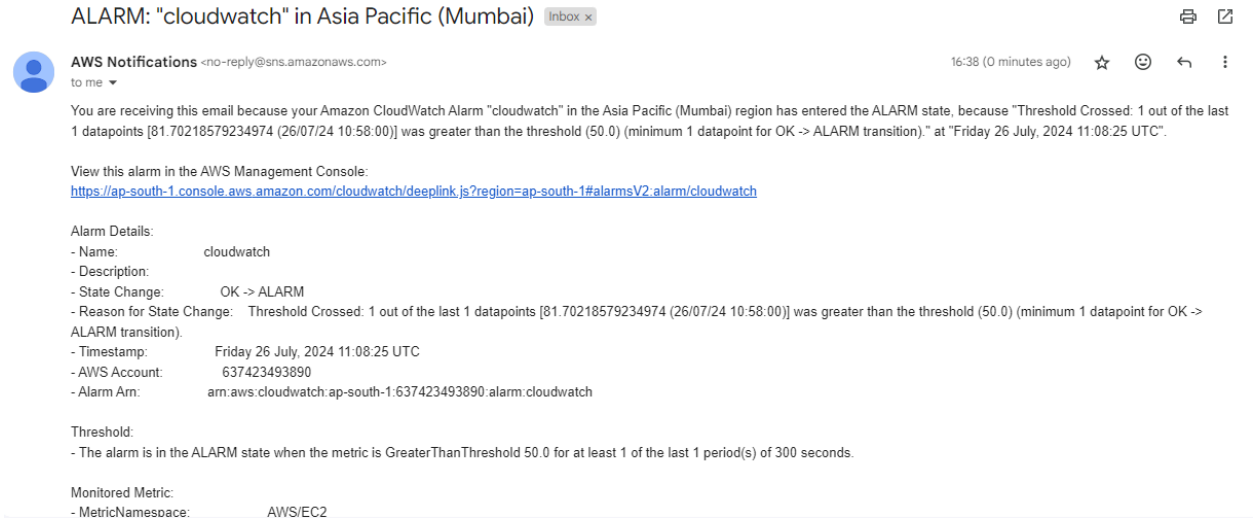
We have configured to get alram once cpu utilization goes greater than equal to 50 percent
Also note must confirm the subscription from your gmail to get a alarm msg directly to your mail
To see the cpu utilizaion
1)top -
To exit from top command do 2) ctrl c
3) yes > /dev/null &

```
Tasks: 100 total,   1 running,  99 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.3 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :    949.5 total,    652.4 free,    139.7 used,    157.4 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.    672.6 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   2985 ec2-user  20   0  223788   3208   2680 R   0.3   0.3   0:00.01 top
      1 root      20   0  105196  16412  10076 S   0.0   1.7   0:00.86 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.05 ksoftirqd/0
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.06 rcu_preempt
     16 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
     18 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
     21 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq
     22 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
     23 root      20   0       0      0      0 S   0.0   0.0   0:00.00 khungtaskd
[ec2-user@ip-10-0-0-14 ~]$ yes > /dev/null &
```

```
[ec2-user@ip-10-0-0-14 ~]$ yes > /dev/null &
[1] 3034
[ec2-user@ip-10-0-0-14 ~]$
```

Wait for 5 mins and check the mail for the alarm notification

Output :



ALARM: "cloudwatch" in Asia Pacific (Mumbai) Inbox ×

AWS Notifications <no-reply@sns.amazonaws.com> 16:38 (0 minutes ago)
to me

You are receiving this email because your Amazon CloudWatch Alarm "cloudwatch" in the Asia Pacific (Mumbai) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [81.70218579234974 (26/07/24 10:58:00)] was greater than the threshold (50.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Friday 26 July, 2024 11:08:25 UTC".

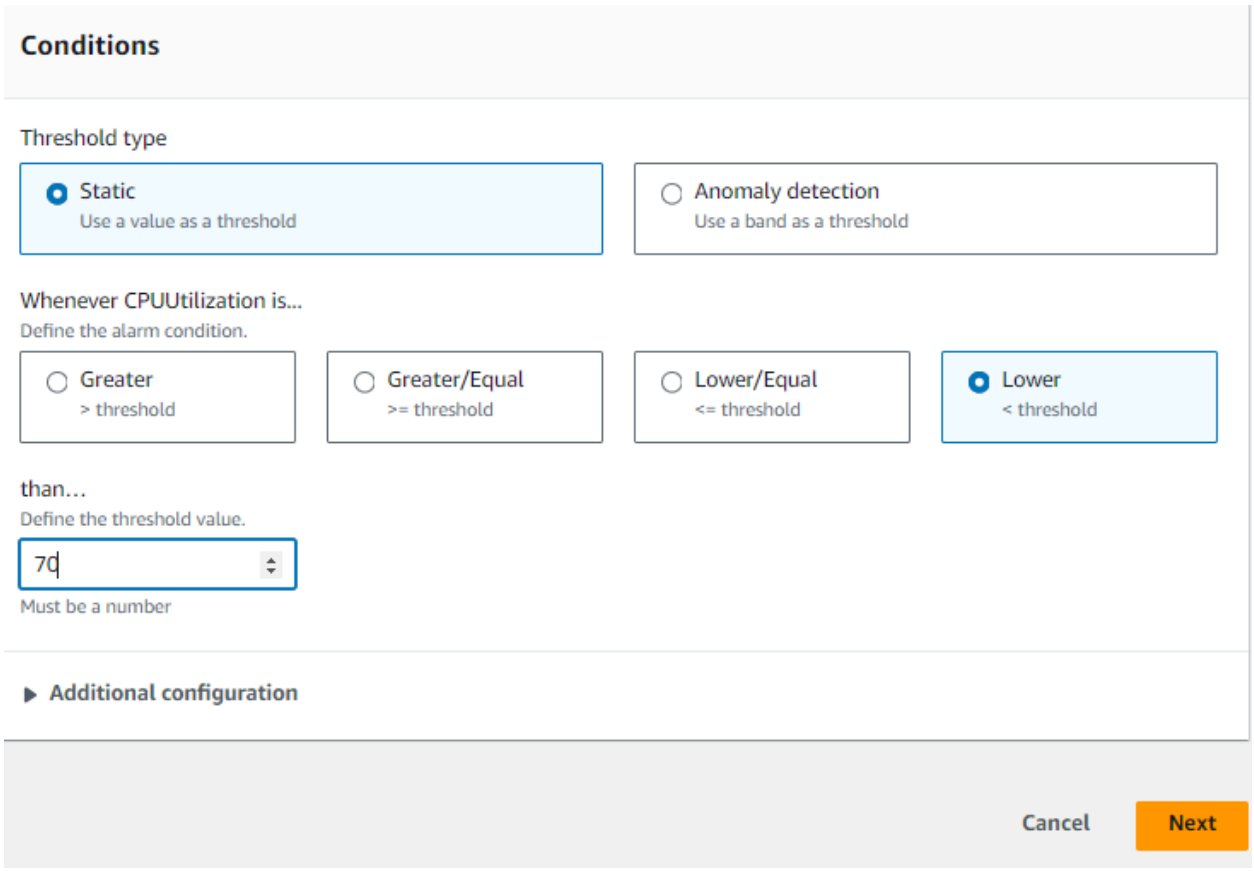
View this alarm in the AWS Management Console:
https://ap-south-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=ap-south-1#alarmsV2:alarm/cloudwatch

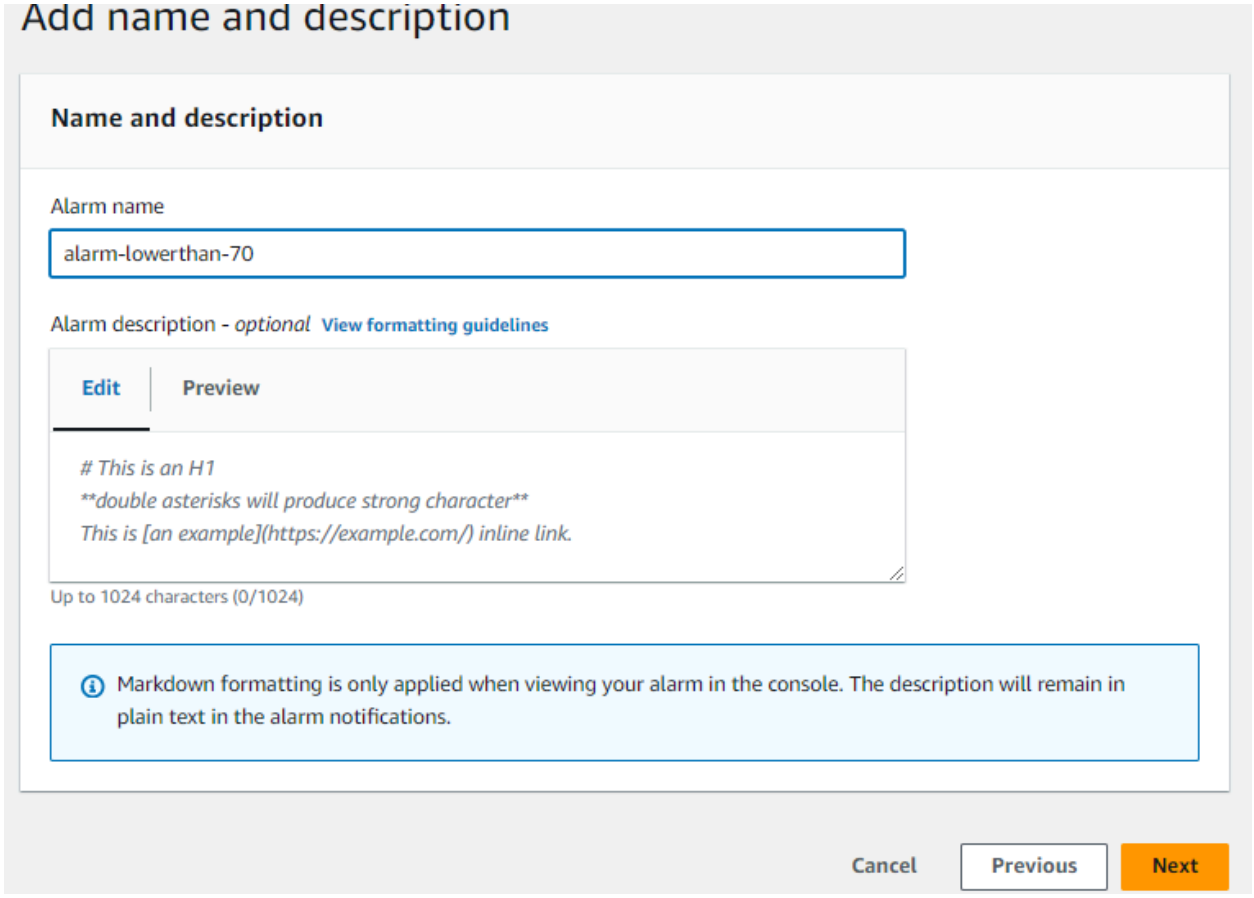
Alarm Details:
- Name: cloudwatch
- Description:
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [81.70218579234974 (26/07/24 10:58:00)] was greater than the threshold (50.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Friday 26 July, 2024 11:08:25 UTC
- AWS Account: 637423493890
- Alarm Arn: arn:aws:cloudwatch:ap-south-1:637423493890:alarm:cloudwatch

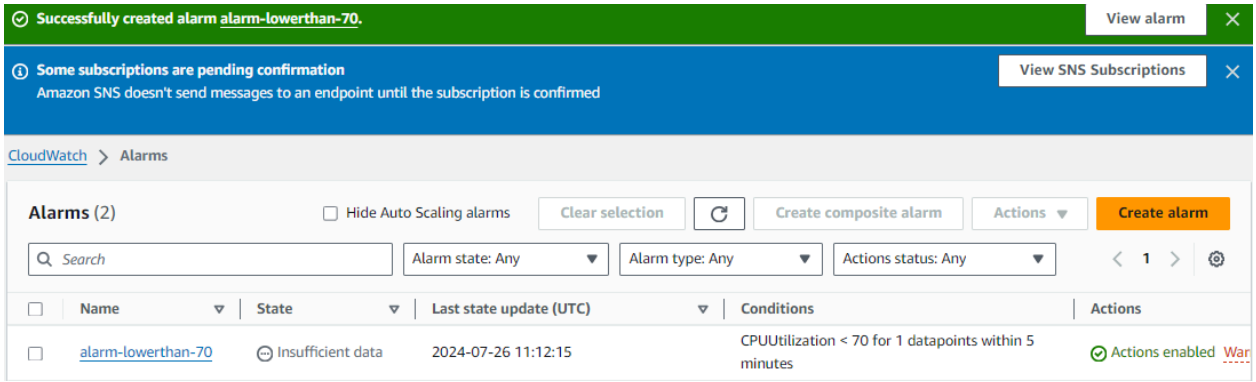
Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanThreshold 50.0 for at least 1 of the last 1 period(s) of 300 seconds.

Monitored Metric:
- MetricNamespace: AWS/EC2

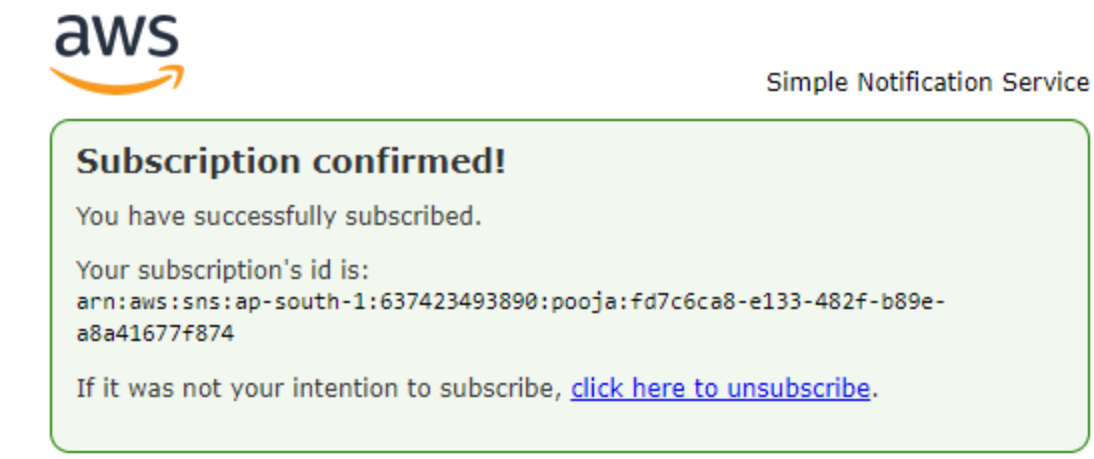
Lower :


Conditions
Threshold type
Static
Use a value as a threshold
Anomaly detection
Use a band as a threshold
Whenever CPUUtilization is...
Define the alarm condition.
Greater
> threshold
Greater/Equal
>= threshold
Lower/Equal
<= threshold
Lower
< threshold
than...
Define the threshold value.
70
Must be a number
Additional configuration
Cancel
Next


Add name and description
Name and description
Alarm name
alarm-lowerthan-70
Alarm description - optional View formatting guidelines
Edit
Preview
This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.
Up to 1024 characters (0/1024)
Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.
Cancel
Previous
Next


Successfully created alarm alarm-lowerthan-70.
View alarm
Some subscriptions are pending confirmation
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed
View SNS Subscriptions
CloudWatch > Alarms
Alarms (2)
Hide Auto Scaling alarms
Clear selection
Create composite alarm
Actions
Create alarm
Search
Alarm state: Any
Alarm type: Any
Actions status: Any
Name
State
Last state update (UTC)
Conditions
Actions
alarm-lowerthan-70
Insufficient data
2024-07-26 11:12:15
CPUUtilization < 70 for 1 datapoints within 5 minutes
Actions enabled

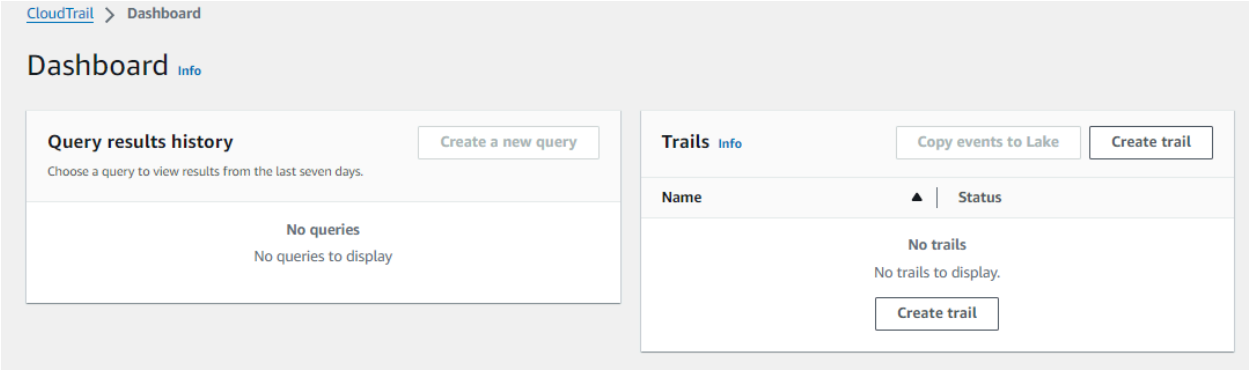
Confirm :




```
    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   2613 ec2-user  20   0  221356   1008    920 R  99.9   0.1  14:47.23 yes
      1 root      20   0  105048  16352  10068 S   0.0   1.7   0:00.90 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
      9 root      20   0       0      0      0 I   0.0   0.0   0:00.03 kworker/u30:0-events_unbound
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.05 ksoftirqd/0
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.05 rcu_preempt
     16 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
     18 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
     21 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq
     22 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
[ec2-user@ip-10-0-0-14 ~]$ kill 2613
```

Output :

CLOUDTRAIL


CloudTrail
Dashboard
Dashboard Info
Query results history
Create a new query
Choose a query to view results from the last seven days.
No queries
No queries to display
Trails Info
Copy events to Lake
Create trail
Name
Status
No trails
No trails to display.
Create trail

Choose trail attributes

General details

A trail created in the console is a multi-region trail. Learn more

Trail name

Enter a display name for your trail.

MANAGE-EVENTS

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. See all accounts

Storage location | Info

- Create new S3 bucket
  Create a bucket to store logs for the trail.
- Use existing S3 bucket
  Choose an existing bucket to store logs for this trail.

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-637423493890-8be34bd7

Logs will be stored in aws-cloudtrail-logs-637423493890-8be34bd7/AWSLogs/637423493890

Log file SSE-KMS encryption | Info

Enabled

Customer managed AWS KMS key

- New
- Existing

AWS KMS alias

Enter KMS alias

KMS key and S3 bucket must be in the same region.

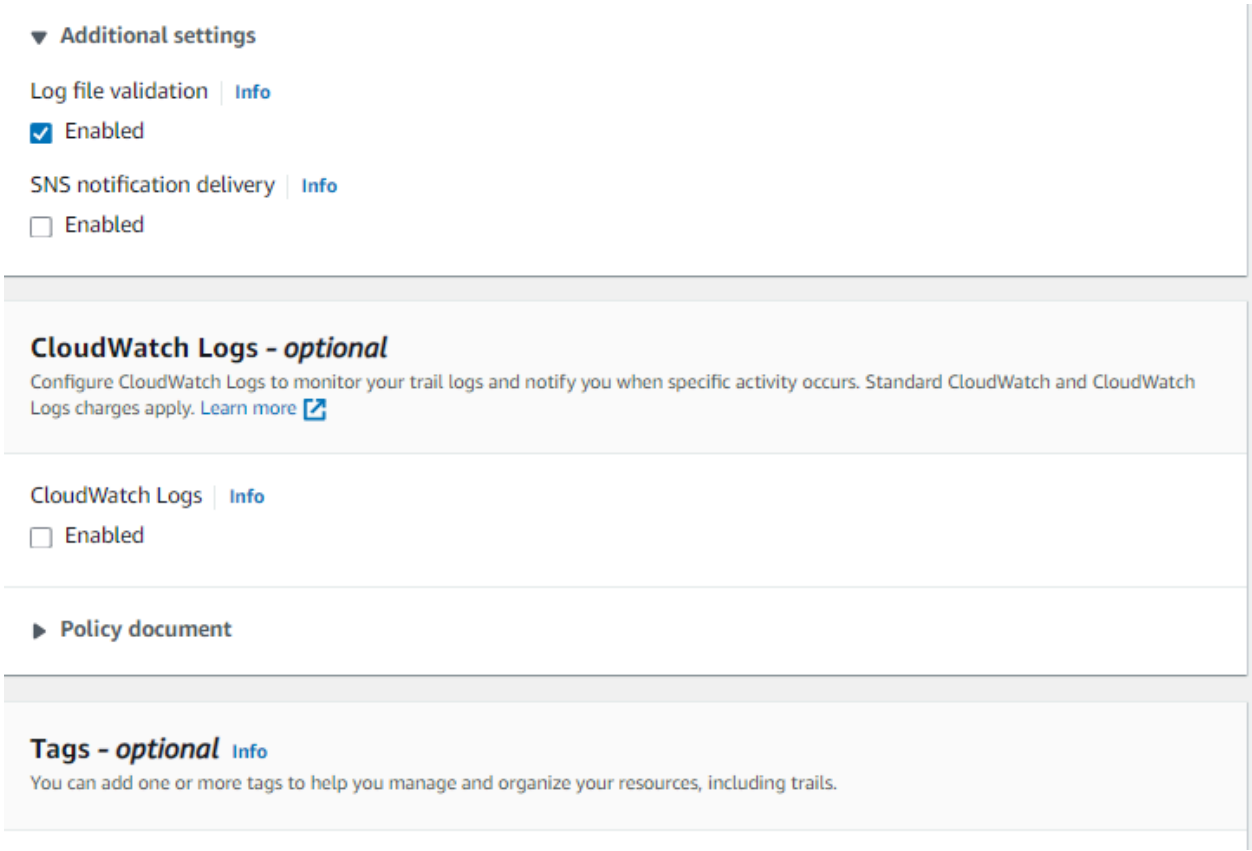
▼ Additional settings

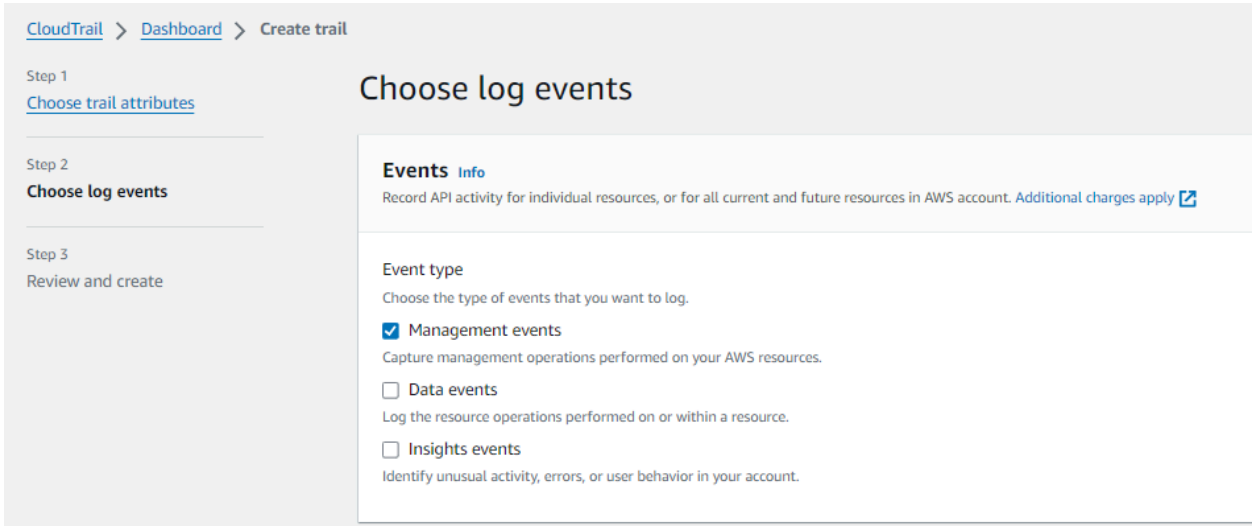
Log file validation | Info

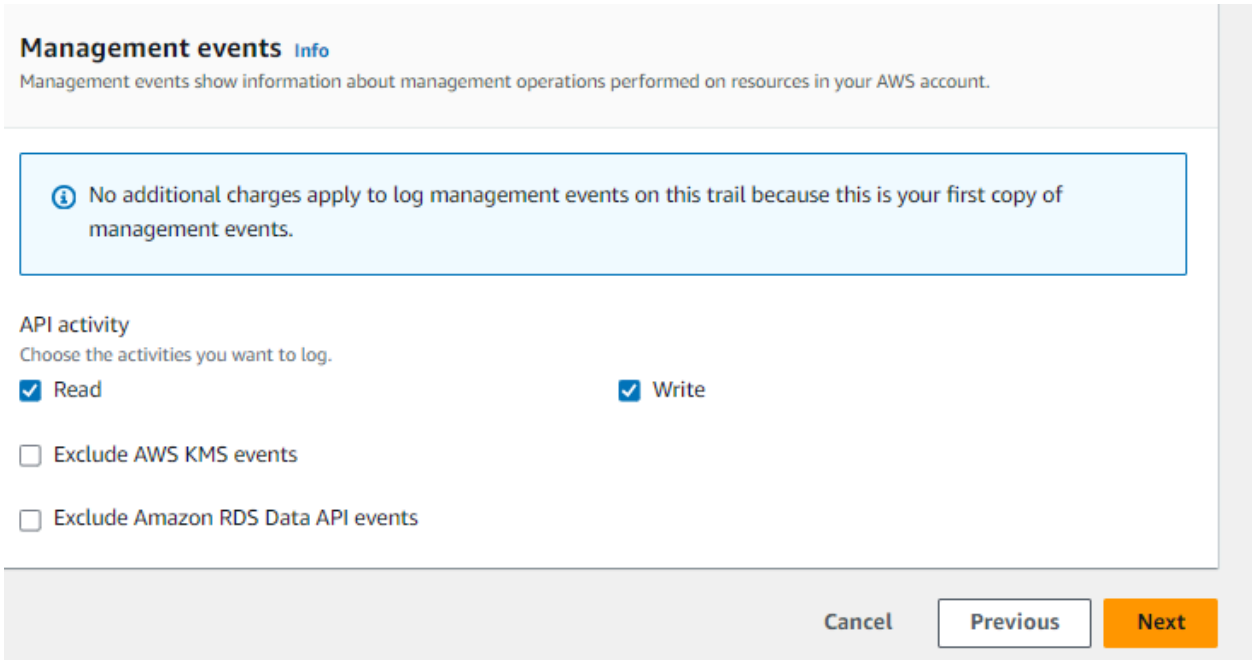
Enabled

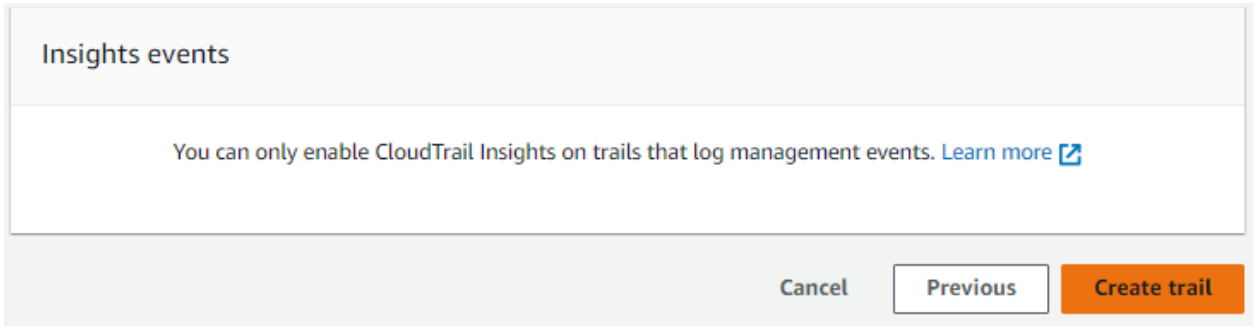
SNS notification delivery | Info

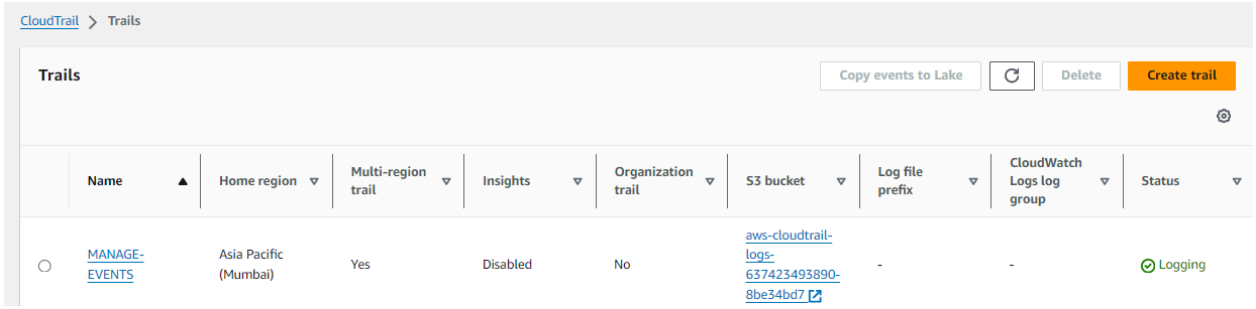
Enabled


Additional settings
Log file validation Info
Enabled
SNS notification delivery Info
Enabled
CloudWatch Logs - optional
Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. Learn more
CloudWatch Logs Info
Enabled
Policy document
Tags - optional Info
You can add one or more tags to help you manage and organize your resources, including trails.

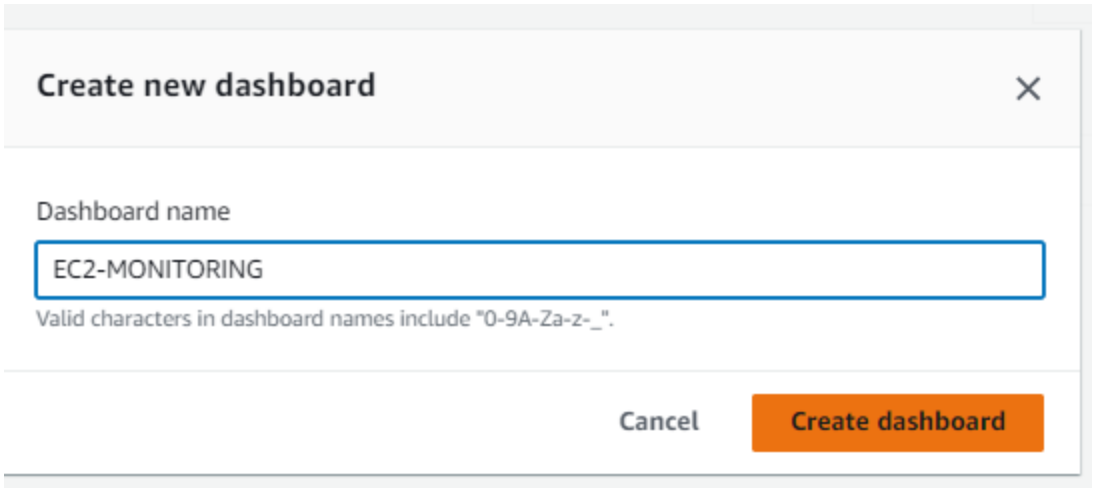

CloudTrail > Dashboard > Create trail
Step 1
Choose trail attributes
Step 2
Choose log events
Step 3
Review and create
Choose log events
Events Info
Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply
Event type
Choose the type of events that you want to log.
Management events
Capture management operations performed on your AWS resources.
Data events
Log the resource operations performed on or within a resource.
Insights events
Identify unusual activity, errors, or user behavior in your account.

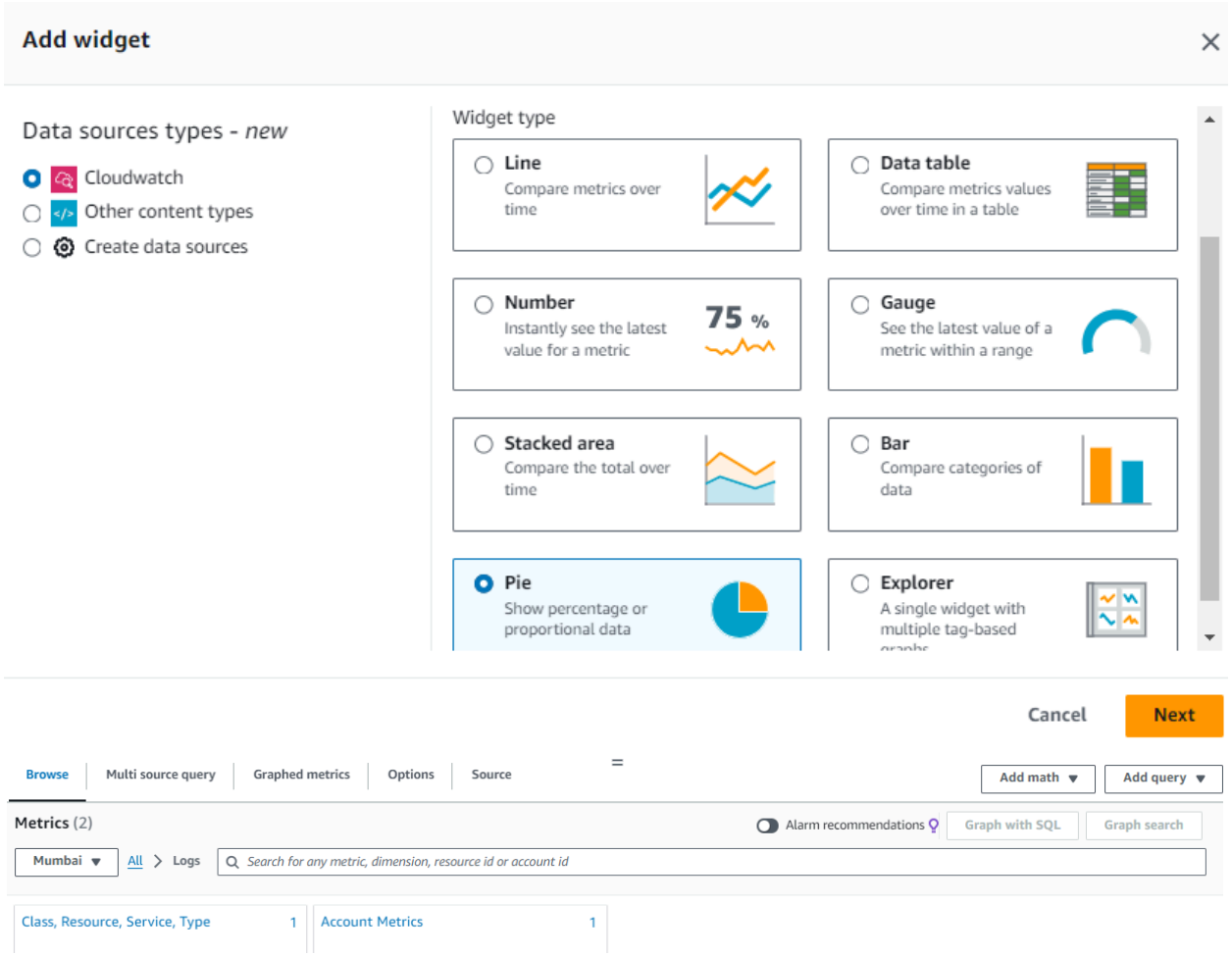




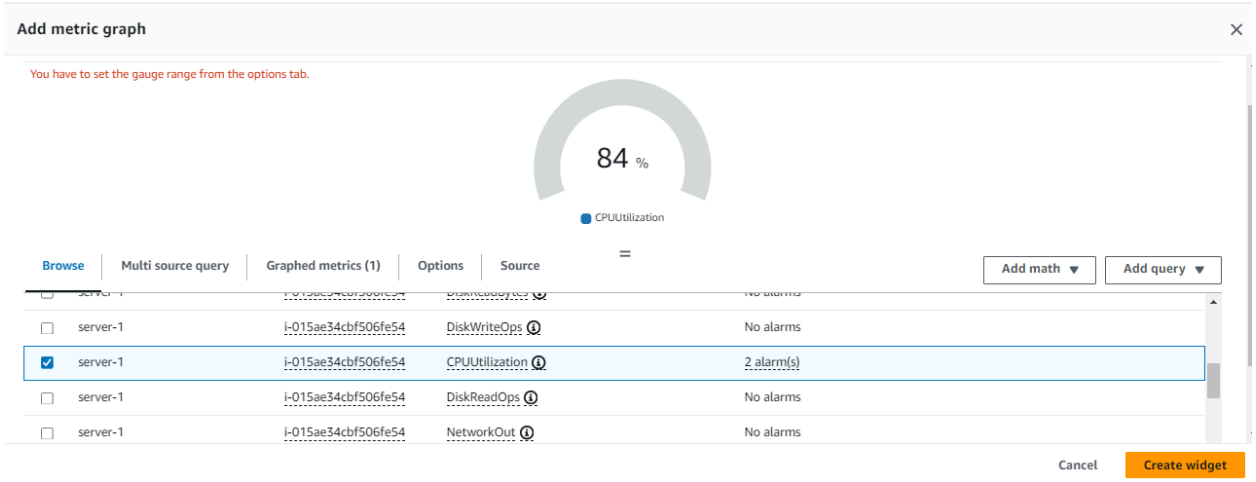


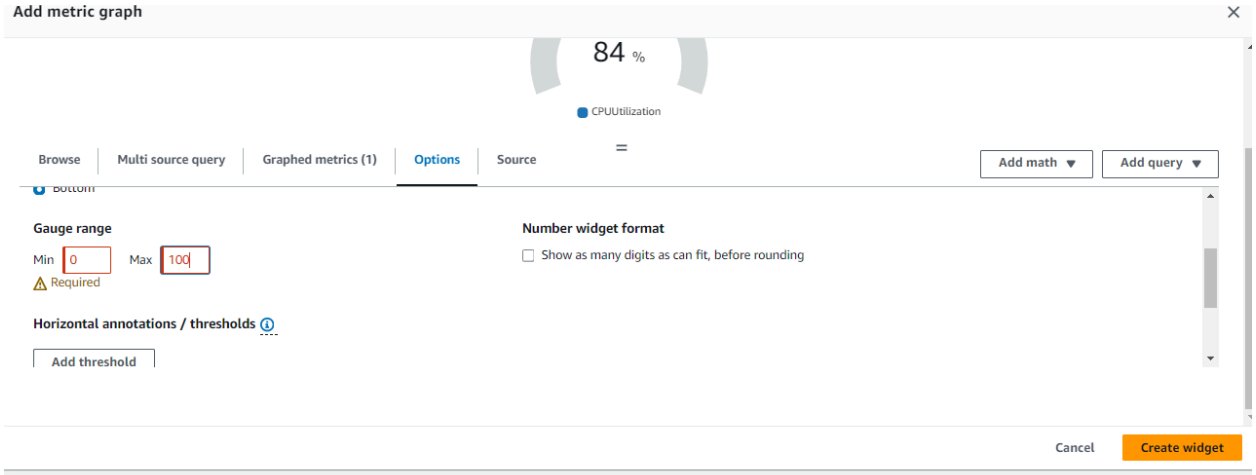
CREATE DASHBOARD IN CLOUDWATCH

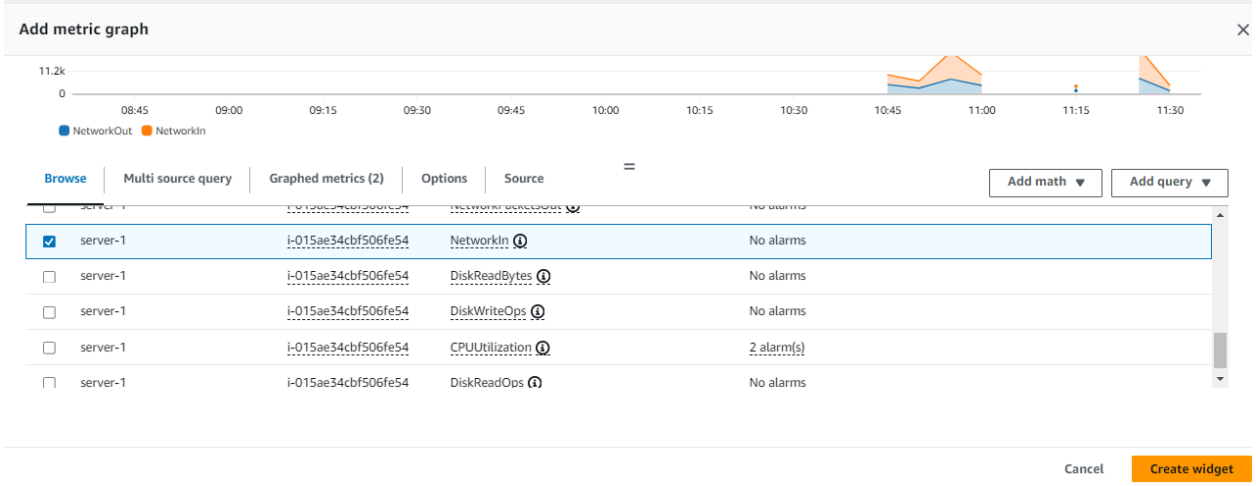

Create new dashboard
Dashboard name
EC2-MONITORING
Valid characters in dashboard names include "0-9A-Za-z-_".
Cancel
Create dashboard

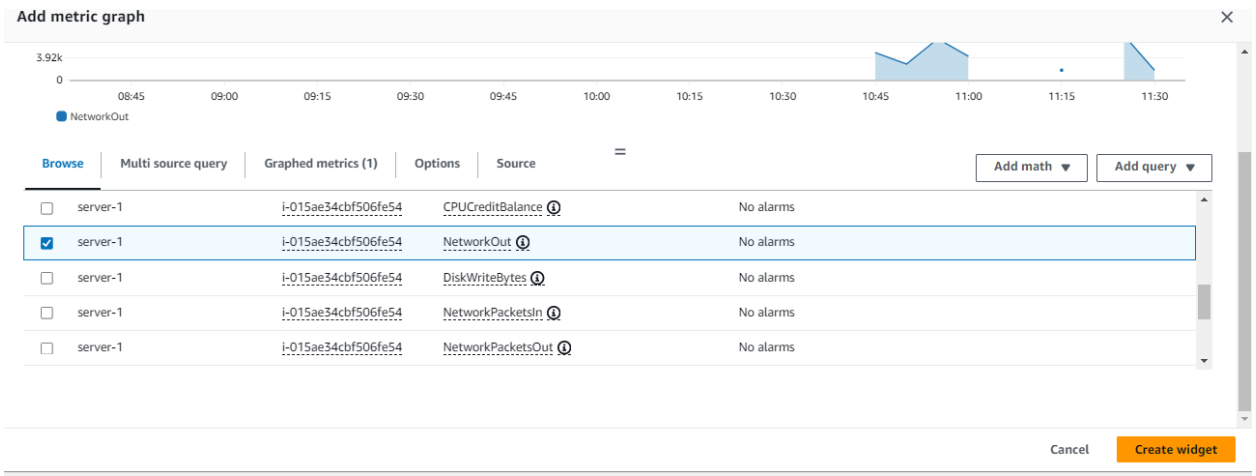

Add widget
Data sources types - new
Cloudwatch
Other content types
Create data sources
Widget type
Line
Compare metrics over time
Data table
Compare metrics values over time in a table
Number
Instantly see the latest value for a metric
75 %
Gauge
See the latest value of a metric within a range
Stacked area
Compare the total over time
Bar
Compare categories of data
Pie
Show percentage or proportional data
Explorer
A single widget with multiple tag-based
Cancel
Next

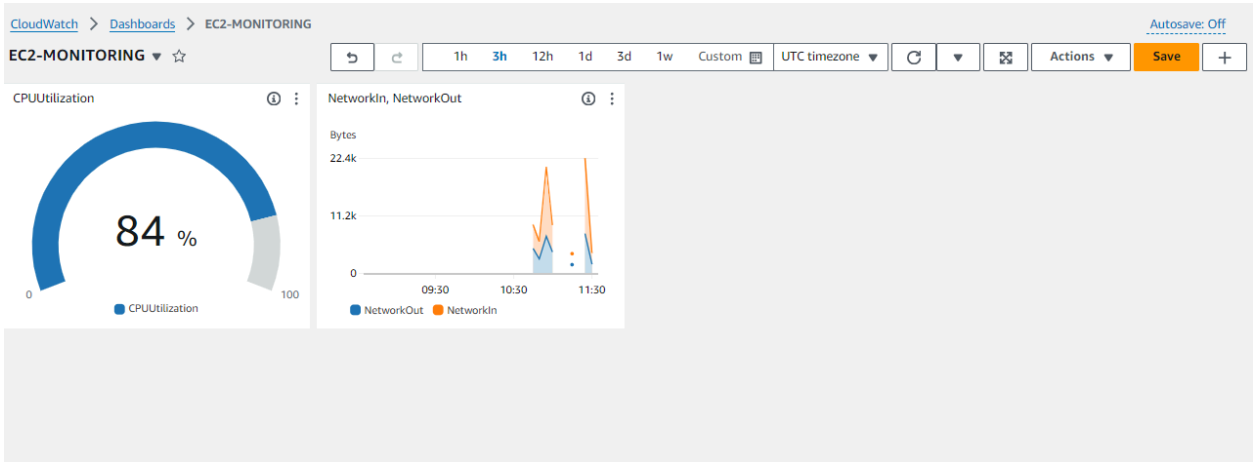
Browse
Multi source query
Graphed metrics
Options
Source
Add math
Add query
Metrics (2)
Alarm recommendations
Graph with SQL
Graph search
Mumbai
All
Logs
Search for any metric, dimension, resource id or account id
Class, Resource, Service, Type
1
Account Metrics
1


Add metric graph
You have to set the gauge range from the options tab.
84 %
CPUUtilization
Browse
Multi source query
Graphed metrics (1)
Options
Source
Add math
Add query
server-1 i-015ae34cbf506fe54 DiskWriteOps No alarms
server-1 i-015ae34cbf506fe54 CPUUtilization 2 alarm(s)
server-1 i-015ae34cbf506fe54 DiskReadOps No alarms
server-1 i-015ae34cbf506fe54 NetworkOut No alarms
Cancel
Create widget

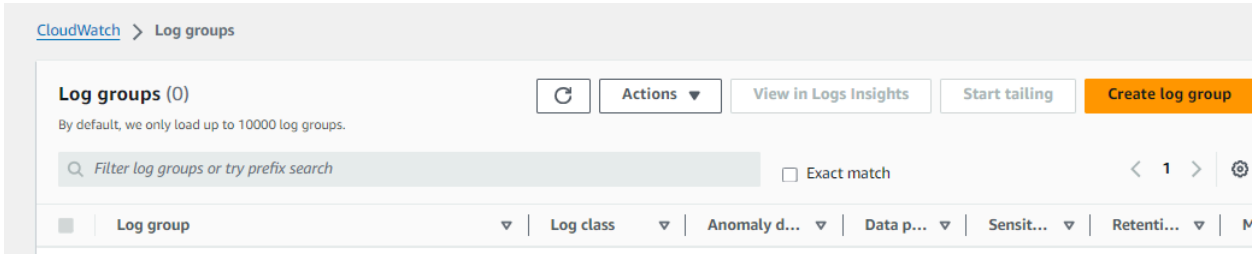

Add metric graph
84 %
CPUUtilization
Browse
Multi source query
Graphed metrics (1)
Options
Source
Add math
Add query
Gauge range
Min 0
Max 100
Required
Number widget format
Show as many digits as can fit, before rounding
Horizontal annotations / thresholds
Add threshold
Cancel
Create widget


Add metric graph
11.2k
0
08:45
09:00
09:15
09:30
09:45
10:00
10:15
10:30
10:45
11:00
11:15
11:30
NetworkOut
NetworkIn
Browse
Multi source query
Graphed metrics (2)
Options
Source
Add math
Add query
server-1 i-015ae34cbf506fe54 NetworkIn No alarms
server-1 i-015ae34cbf506fe54 DiskReadBytes No alarms
server-1 i-015ae34cbf506fe54 DiskWriteOps No alarms
server-1 i-015ae34cbf506fe54 CPUUtilization 2 alarm(s)
server-1 i-015ae34cbf506fe54 DiskReadOps No alarms
Cancel
Create widget





Create log group



Create log group

Log group details Info

CloudWatch Logs offers two log classes: Standard and Infrequent Access. Learn more about the features offered by each log class.

Log group name

logs

Retention setting

1 day

Log class | Info

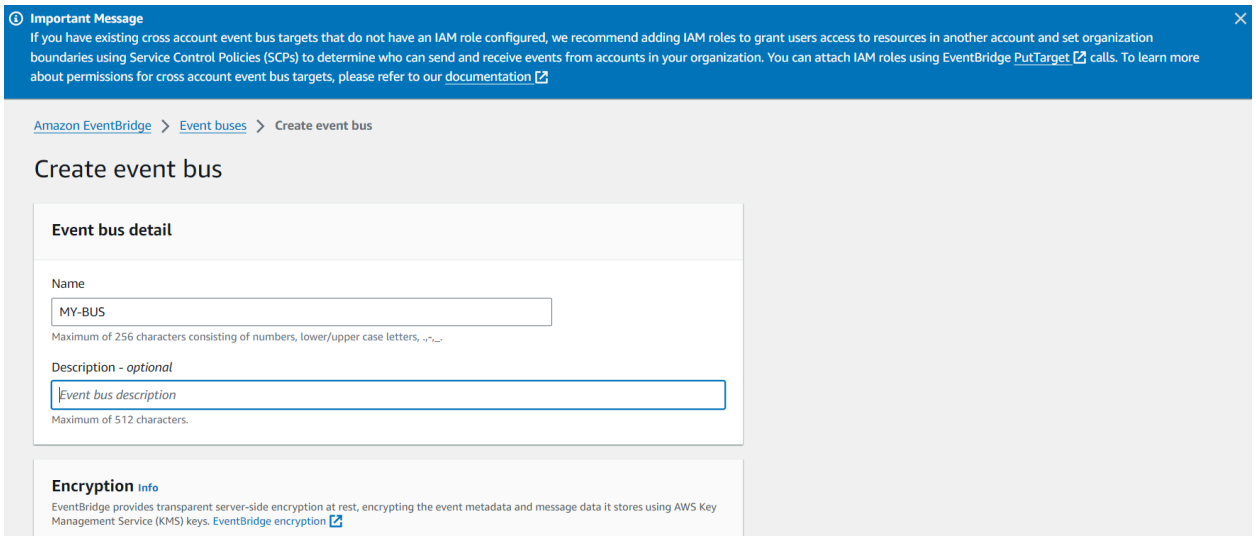
Infrequent Access

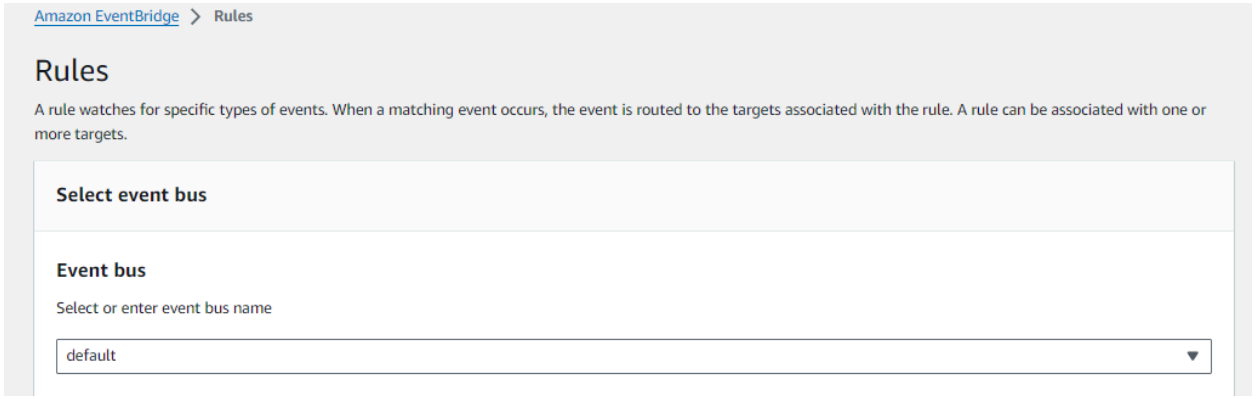
KMS key ARN - *optional*

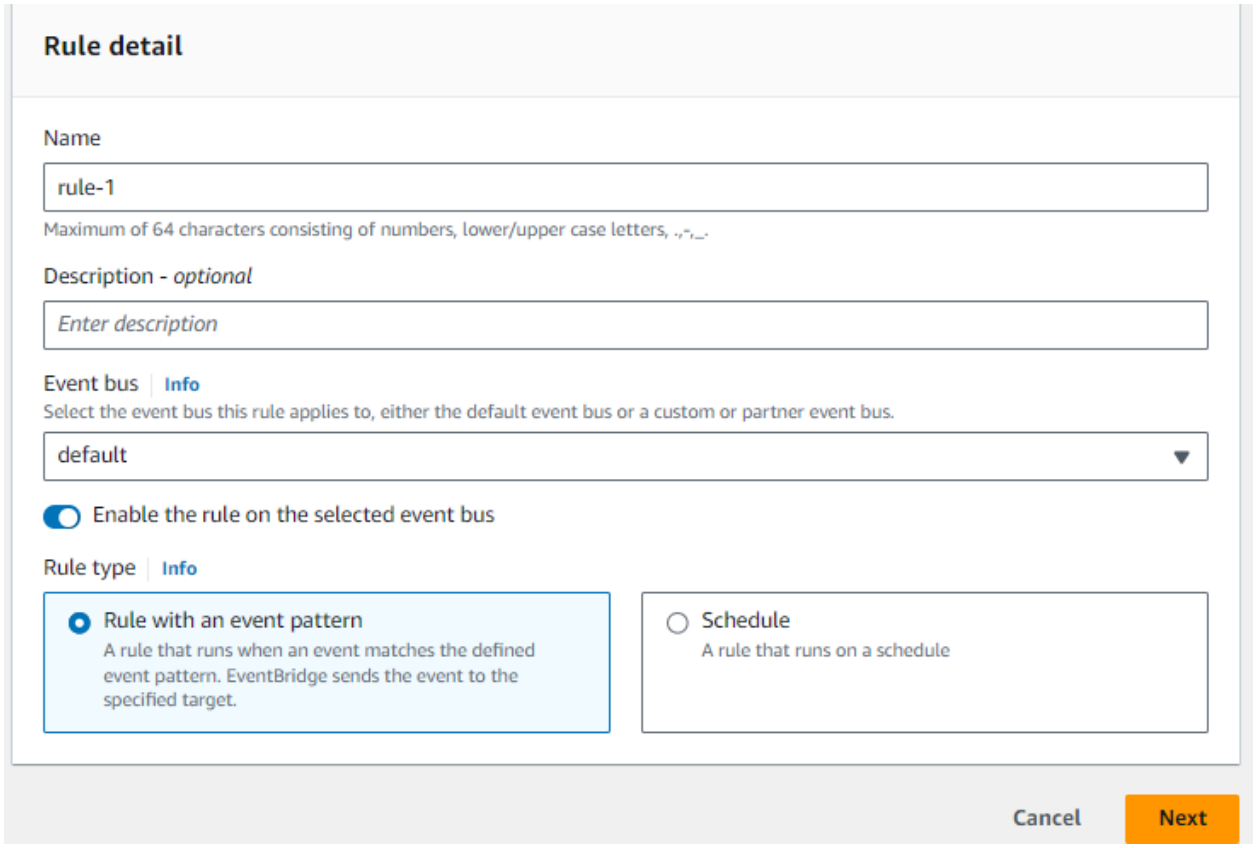
```
Last login: Fri Jul 26 11:27:30 2024 from 13.233.177.3
[ec2-user@ip-10-0-0-14 ~]$ sudo su
[root@ip-10-0-0-14 ec2-user]# yum update
Last metadata expiration check: 0:39:42 ago on Fri Jul 26 11:16:53 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-10-0-0-14 ec2-user]# yum upgrade
Last metadata expiration check: 0:39:59 ago on Fri Jul 26 11:16:53 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-10-0-0-14 ec2-user]# yum install httpd
Last metadata expiration check: 0:40:16 ago on Fri Jul 26 11:16:53 2024.
Dependencies resolved.
```

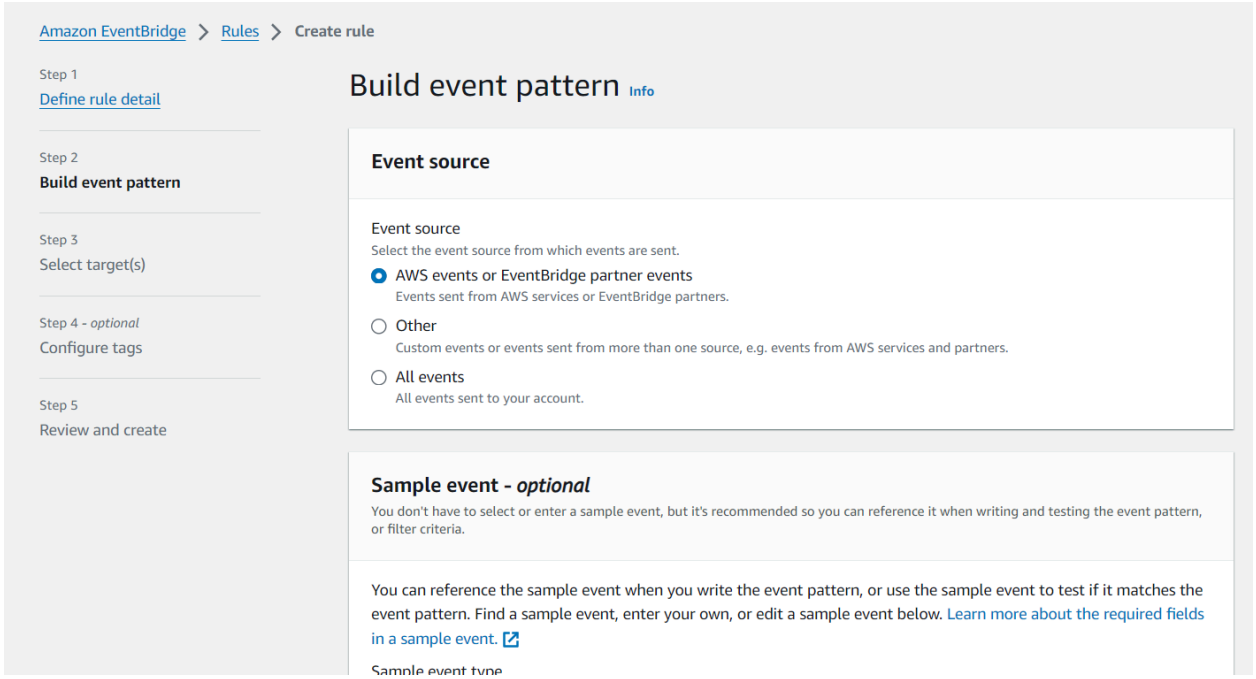
```
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
  Installing       : apr-1.7.2-2.amzn2023.0.2.x86_64
  Installing       : apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
  Installing       : apr-util-1.6.3-1.amzn2023.0.1.x86_64
  Installing       : mailcap-2.1.49-3.amzn2023.0.3.noarch
  Installing       : httpd-tools-2.4.61-1.amzn2023.x86_64
  Installing       : libbrotli-1.0.9-4.amzn2023.0.2.x86_64
  Running scriptlet: httpd-filesystem-2.4.61-1.amzn2023.noarch
  Installing       : httpd-filesystem-2.4.61-1.amzn2023.noarch
  Installing       : httpd-core-2.4.61-1.amzn2023.x86_64
  Installing       : mod_http2-2.0.27-1.amzn2023.0.2.x86_64
  Installing       : mod_lua-2.4.61-1.amzn2023.x86_64
  Installing       : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
  Installing       : httpd-2.4.61-1.amzn2023.x86_64
  Running scriptlet: httpd-2.4.61-1.amzn2023.x86_64
  Verifying        : apr-1.7.2-2.amzn2023.0.2.x86_64
  Verifying        : apr-util-1.6.3-1.amzn2023.0.1.x86_64
  Verifying        : apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
  Verifying        : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
  Verifying        : httpd-2.4.61-1.amzn2023.x86_64

Installed:
  apr-1.7.2-2.amzn2023.0.2.x86_64                apr-util-1.6.3-1.amzn2023.0.1.x86_64          apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
  generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch  httpd-2.4.61-1.amzn2023.x86_64            httpd-core-2.4.61-1.amzn2023.x86_64
  httpd-filesystem-2.4.61-1.amzn2023.noarch      httpd-tools-2.4.61-1.amzn2023.x86_64          libbrotli-1.0.9-4.amzn2023.0.2.x86_64
  mailcap-2.1.49-3.amzn2023.0.3.noarch           mod_http2-2.0.27-1.amzn2023.0.2.x86_64        mod_lua-2.4.61-1.amzn2023.x86_64

Complete!
[root@ip-10-0-0-14 ec2-user]#
```

EVENTBRIDGE






Rule detail
Name
rule-1
Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.
Description - optional
Enter description
Event bus Info
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.
default
Enable the rule on the selected event bus
Rule type Info
Rule with an event pattern
A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.
Schedule
A rule that runs on a schedule
Cancel
Next


Amazon EventBridge > Rules > Create rule
Step 1
Define rule detail
Step 2
Build event pattern
Step 3
Select target(s)
Step 4 - optional
Configure tags
Step 5
Review and create
Build event pattern Info
Event source
Event source
Select the event source from which events are sent.
AWS events or EventBridge partner events
Events sent from AWS services or EventBridge partners.
Other
Custom events or events sent from more than one source, e.g. events from AWS services and partners.
All events
All events sent to your account.
Sample event - optional
You don't have to select or enter a sample event, but it's recommended so you can reference it when writing and testing the event pattern, or filter criteria.
You can reference the sample event when you write the event pattern, or use the sample event to test if it matches the event pattern. Find a sample event, enter your own, or edit a sample event below. Learn more about the required fields in a sample event.
Sample event type

Sample events

Filter by event source and type or by keyword.

EC2 Instance State-change Notification

Sample event 1


```
{
  "version": "0",
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "EC2 Instance State-change Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2015-11-11T21:29:54Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"],
  "detail": {
    "instance-id": "i-abcd1111",
    "state": "pending"
  }
}
```


Copy

Creation method

Method

Event pattern Info

Event source
AWS service or EventBridge partner as source

AWS services

AWS service
The name of the AWS service as the event source

EC2

Event type
The type of events as the source of the matching pattern

EC2 Instance State-change Notification

Event Type Specification 1

- ○ Any state
- ◉ Specific state(s)

Specific state(s)

stopped ×

Event pattern
Event pattern, or filter to match the events

```
{
  "source": ["aws.ec2"],
  "detail-type": ["EC2 Instance State-change Notification"]
  "detail": {
    "state": ["stopped"]
  }
}
```

Copy | Test pattern | Edit pattern

Event Type Specification 2

- ○ Any instance
- ◉ Specific instance Id(s)

Specific instance Id(s)

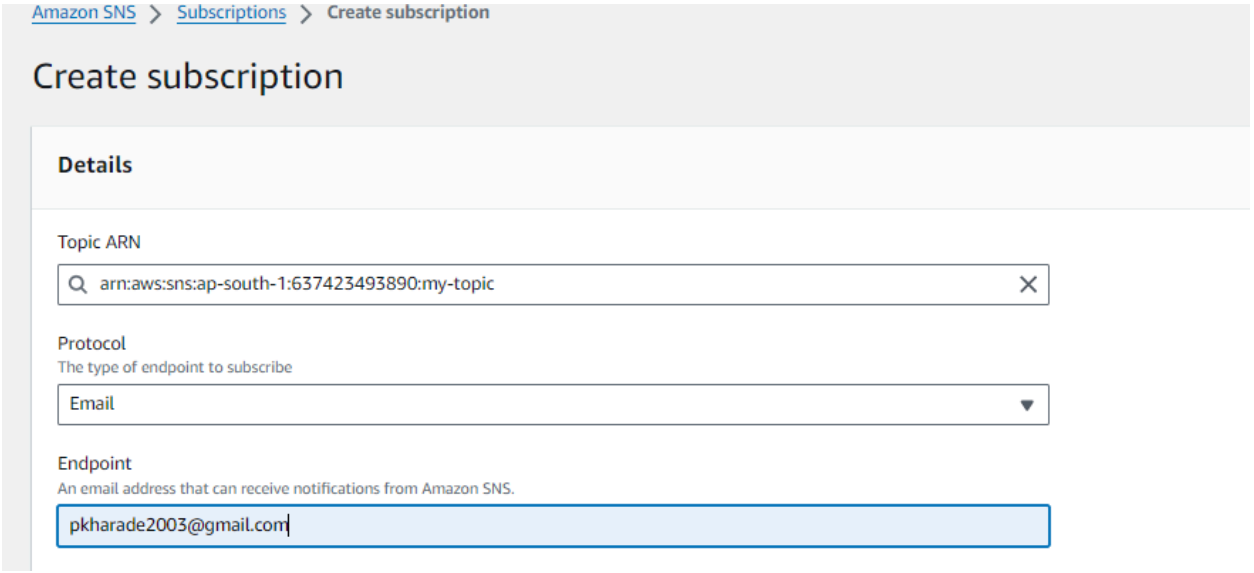
i-015ae34cbf506fe54

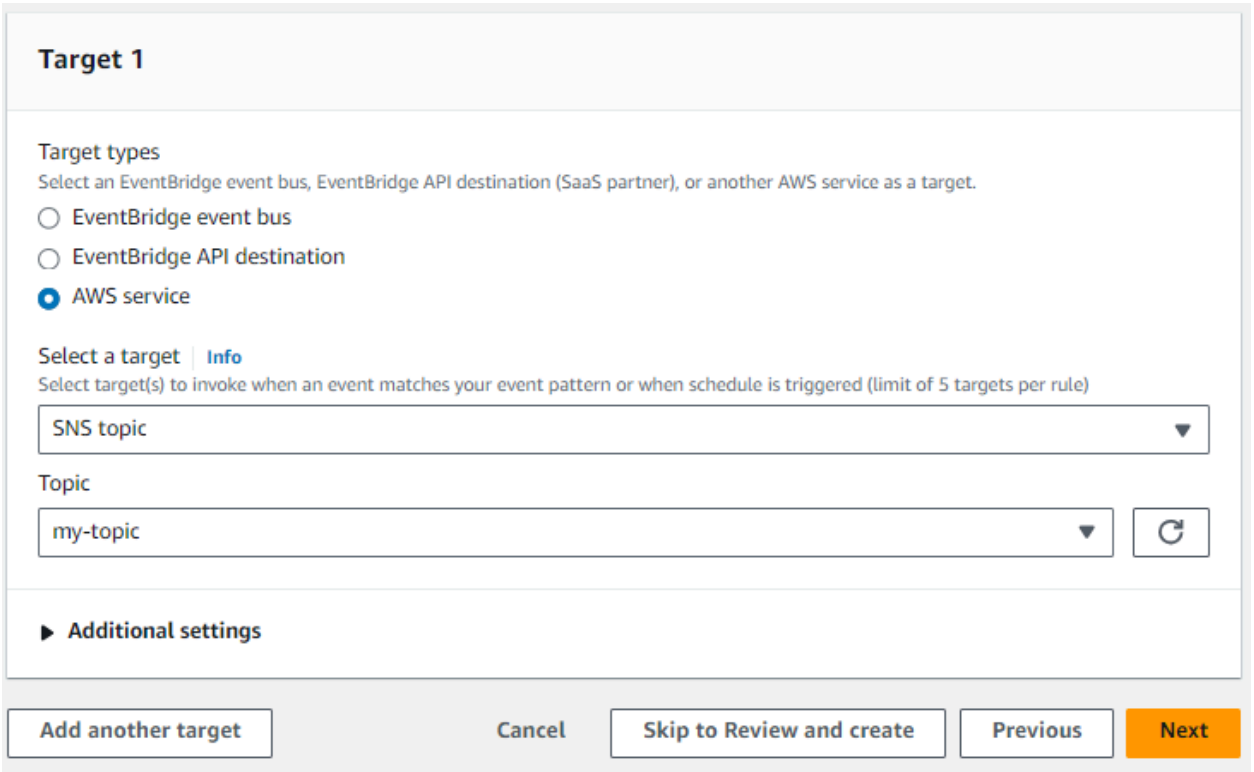
Remove

Add

CREATE SNS TOPIC

AND THEN CREATE SUBSCRIPTION - SELECT EMAIL





Confirm subscription

aws

Simple Notification Service

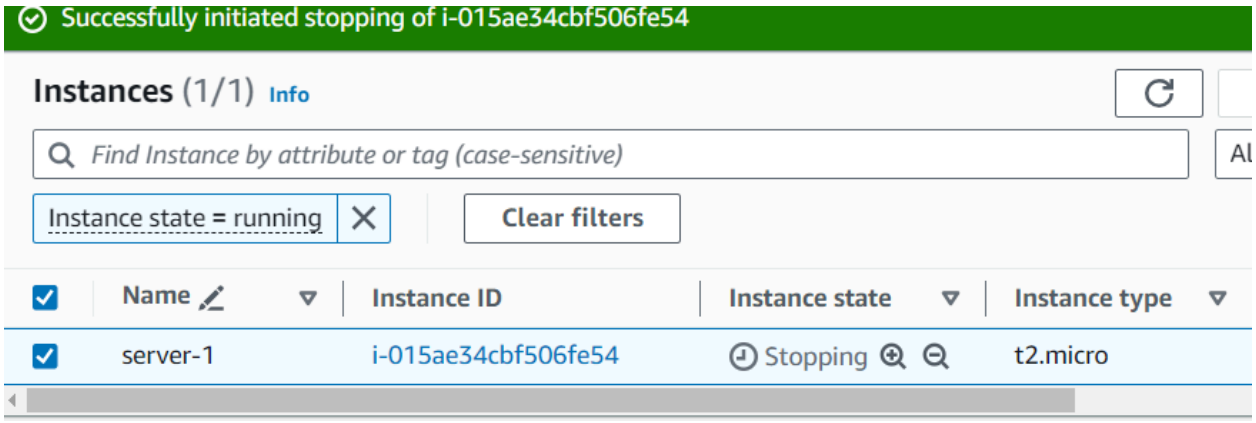
Subscription confirmed!

You have successfully subscribed.

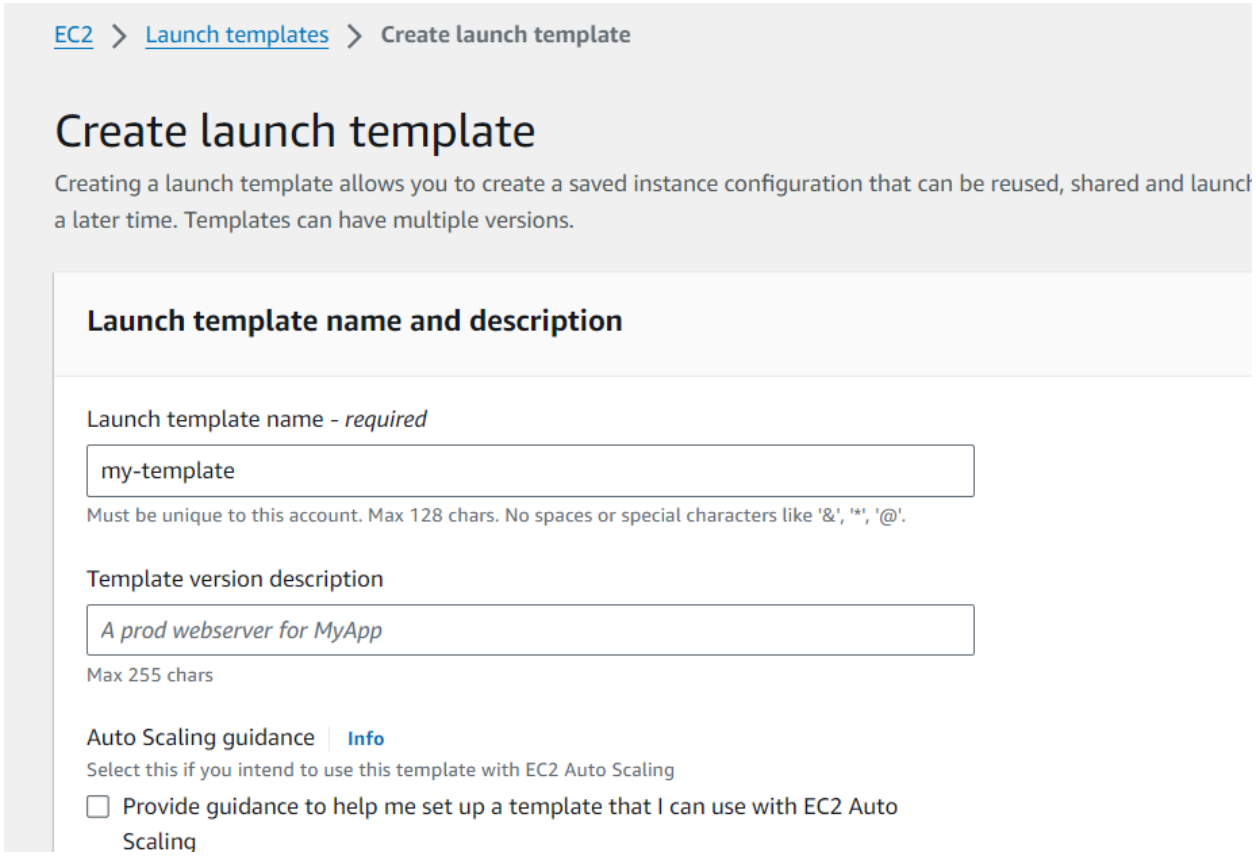
Your subscription's id is:
`arn:aws:sns:ap-south-1:637423493890:DEMO:29ffc132-7f91-4c86-9969-6d81220e19ac`

If it was not your intention to subscribe, click here to unsubscribe.

Stop ec2



AUTO SCALING GROUP



Application and OS Images (Amazon Machine Image) Info

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

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

Recents | Quick Start

Don't include in launch template | Amazon Linux | macOS | Ubuntu | Windows | Red H

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible

ami-068e0f1a600cd311c (64-bit (x86), uefi-preferred) / ami-00b2b1347d132e107 (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

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

Instance type Info | Get advice

Advanced

Instance type

t2.micro — Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

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

Key pair name

mykey

Create new key pair

Network settings Info

Subnet Info

subnet-07d8e423f9b69173f pri-subnet
VPC: vpc-00c5d45ef1f289afe Owner: 637423493890
Availability Zone: ap-south-1b IP addresses available: 11 CIDR: 10.0.0.16/28)

Create new subnet

When you specify a subnet, a network interface is automatically added to your template.

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.

- ○ Select existing security group
- ◉ Create security group

Security group name - *required*

my-sg

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

Description - *required* Info

Allows SSH access to developers

VPC Info

vpc-00c5d45ef1f289afe

Inbound Security Group Rules

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

Type Info	Protocol Info	Port range Info
ssh ▼	TCP	22

Source type Info	Source Info	Description - *optional* Info
Anywhere ▼	Add CIDR, prefix list or security	e.g. SSH for admin desktop
	0.0.0.0/0 ✕	

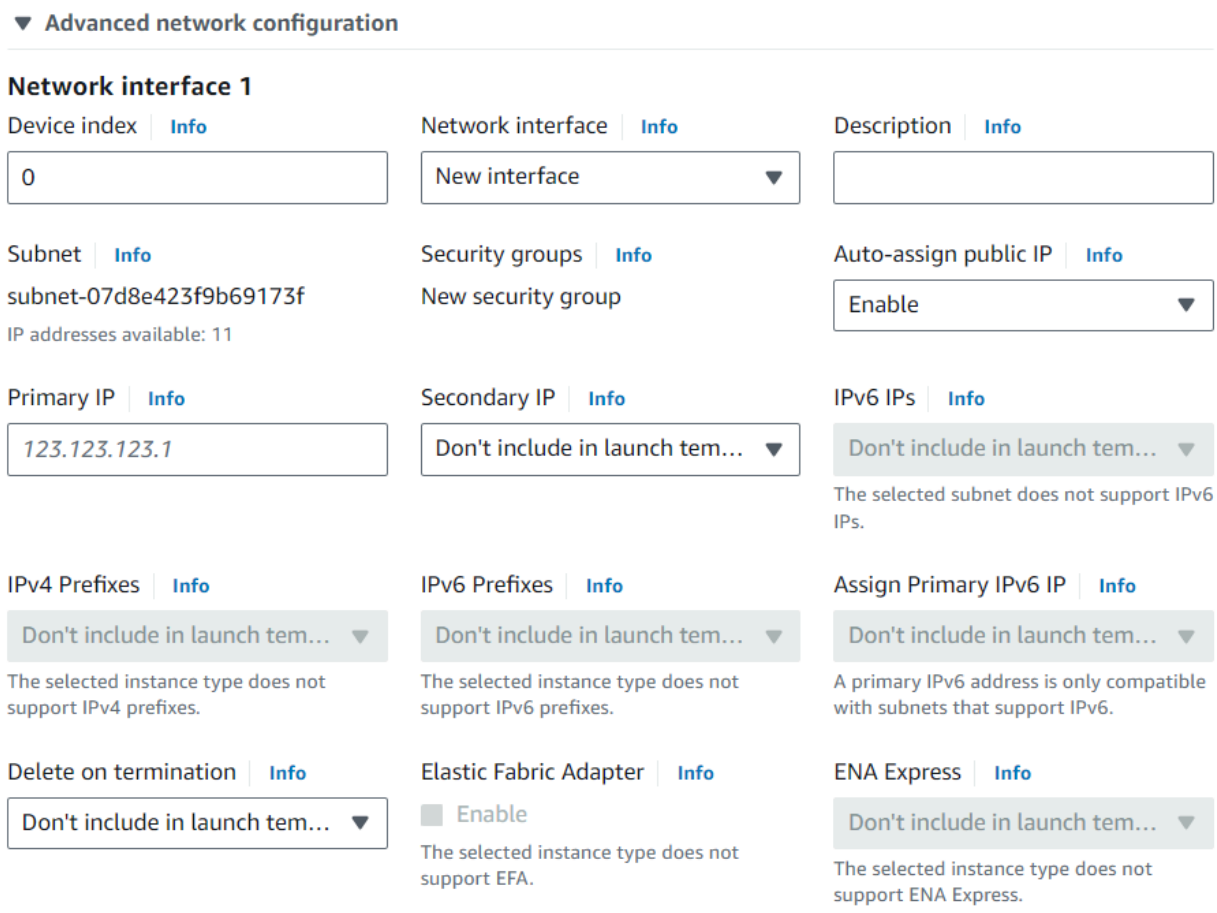
▼ Security group rule 2 (TCP, 80, 0.0.0.0/0) **Remove**

Type Info	Protocol Info	Port range Info
HTTP ▼	TCP	80

Source type Info	Source Info	Description - *optional* Info
Anywhere ▼	Add CIDR, prefix list or security	e.g. SSH for admin desktop
	0.0.0.0/0 ✕	

Add security group rule

▼ **Advanced network configuration**




```
#!/bin/bash
sudo su
yum install update -y
yum install httpd -y
systemctl start httpd
systemctl enable httpd
echo "Hello Zainab" > /var/www/html/index.html
```

User data - *optional* | Info

Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
sudo su
yum install update -y
yum install httpd -y
systemctl start httpd
systemctl enable httpd
echo "Hello Student !" > /var/www/html/index.html
```

☐ User data has already been base64 encoded

Choose launch template Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name

Enter a name to identify the group.

my-asg

Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

my-template

Create a launch template

Version

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, security groups.

my-template

Create a launch template

Version

2

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-00c5d45ef1f289afe (MY-VPC)
10.0.0.0/26

Create a VPC

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

ap-south-1a | subnet-03356b50f4c0b2ff1 (pri-subnet)
10.0.0.0/28

ap-south-1b | subnet-07d8e423f9b69173f (pri-subnet)
10.0.0.16/28

Create a subnet

Cancel | Skip to review | Previous | Next

Configure advanced options - *optional* Info

Integrate your Auto Scaling group with other services to distribute network traffic across multiple servers using a load balancer or to establish service-to-service communications using VPC Lattice. You can also set options that give you more control over health check replacements and monitoring.

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

- (●) **No load balancer**
  Traffic to your Auto Scaling group will not be fronted by a load balancer.
- ( ) **Attach to an existing load balancer**
  Choose from your existing load balancers.
- ( ) **Attach to a new load balancer**
  Quickly create a basic load balancer to attach to your Auto Scaling group.

VPC Lattice integration options Info

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

Select VPC Lattice service to attach

- (●) **No VPC Lattice service**
  VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.
- ( ) **Attach to VPC Lattice service**
  Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.

Scaling Info

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

1

Equal or less than desired capacity

Max desired capacity

3

Equal or greater than desired capacity

Automatic scaling - *optional*

Choose whether to use a target tracking policy | Info

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

- ○ No scaling policies
  Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.
- ◉ Target tracking scaling policy
  Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

Target Tracking Policy

Metric type | Info

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization

Configure group size and scaling - *optional* Info

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

Group size Info

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances)

Desired capacity

Specify your group size.

1

Instance maintenance policy Info

Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.

Choose a replacement behavior depending on your availability requirements

Mixed behavior

- (●) No policy
  For rebalancing events, new instances will launch before terminating others. For all other events, instances terminate and launch at the same time.

Prioritize availability

- ( ) Launch before terminating
  Launch new instances and wait for them to be ready before terminating others. This allows you to go above your desired capacity by a given percentage and may temporarily increase costs.

Control costs

- ( ) Terminate and launch
  Terminate and launch instances at the same time. This allows you to go below your desired capacity by a given percentage and may temporarily reduce availability.

Flexible

- ( ) Custom behavior
  Set custom values for the minimum and maximum amount of available capacity. This gives you greater flexibility in setting how far below and over your desired capacity EC2 Auto Scaling goes when replacing instances.

Add notifications - *optional* Info

Send notifications to SNS topics whenever Amazon EC2 Auto Scaling launches or terminates the EC2 instances in your Auto Scaling group.

Notification 1

Remove

SNS Topic

Choose an SNS topic to use to send notifications

my-topic

Create a topic

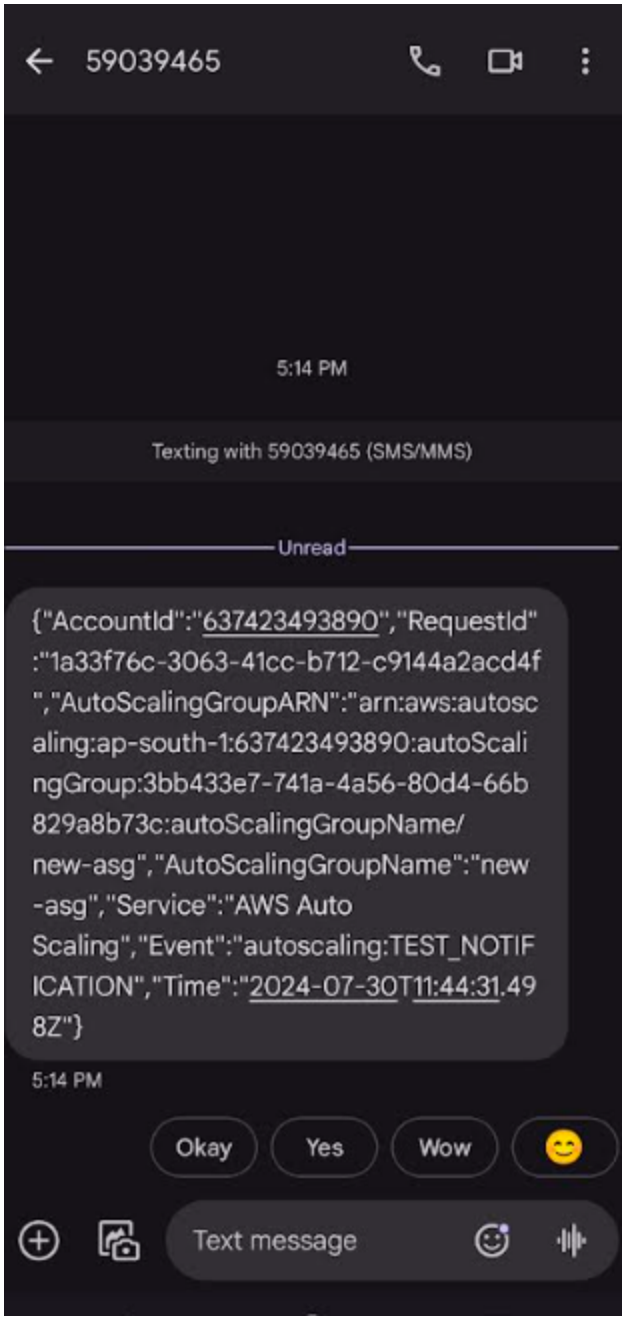
Event types

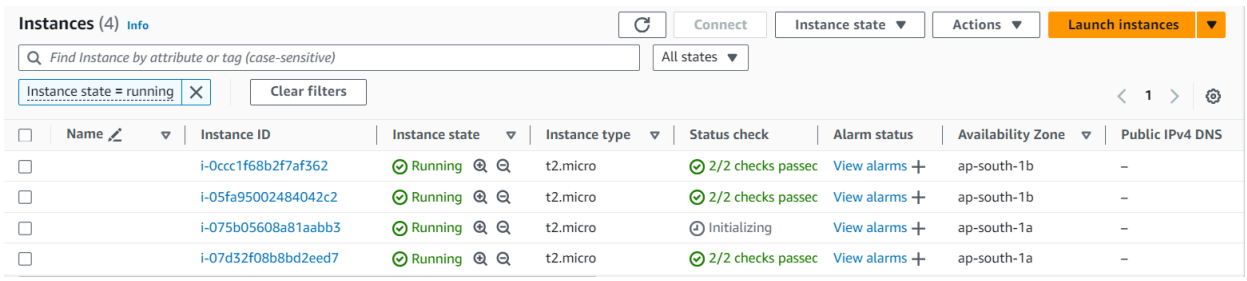
Notify subscribers whenever instances

- [x] Launch
- [ ] Terminate
- [ ] Fail to launch
- [ ] Fail to terminate

Add notification

Cancel | Skip to review | Previous | Next


59039465
5:14 PM
Texting with 59039465 (SMS/MMS)
Unread
{"AccountId":"637423493890","RequestId":"1a33f76c-3063-41cc-b712-c9144a2acd4f","AutoScalingGroupARN":"arn:aws:autoscaling:ap-south-1:637423493890:autoScalingGroup:3bb433e7-741a-4a56-80d4-66b829a8b73c:autoScalingGroupName/new-asg","AutoScalingGroupName":"new-asg","Service":"AWS Auto Scaling","Event":"autoscaling:TEST_NOTIFICATION","Time":"2024-07-30T11:44:31.498Z"}
5:14 PM
Okay
Yes
Wow
Text message


Instances (4) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
i-0ccc1f68b2f7af362 Running t2.micro 2/2 checks passec View alarms ap-south-1b –
i-05fa95002484042c2 Running t2.micro 2/2 checks passec View alarms ap-south-1b –
i-075b05608a81aabb3 Running t2.micro Initializing View alarms ap-south-1a –
i-07d32f08b8bd2eed7 Running t2.micro 2/2 checks passec View alarms ap-south-1a –

```
Tasks: 115 total,   3 running, 112 sleeping,   0 stopped,   0 zombie
%Cpu(s): 61.8 us, 38.2 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :    949.5 total,    496.6 free,    157.6 used,    295.3 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.    648.7 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  26559 root      20   0  221356   1008    920 R  49.8   0.1   0:04.45 yes
  26132 root      20   0  221356   1008    920 R  49.5   0.1   1:10.70 yes
    985 root      20   0       0      0      0 S   0.3   0.0   0:00.05 xfsaild/xvda1
      1 root      20   0  171208  16768  10036 S   0.0   1.7   0:01.24 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      7 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0-events
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
      9 root      20   0       0      0      0 I   0.0   0.0   0:00.03 kworker/u30:0-events_unbound
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.11 ksoftirqd/0
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.06 rcu_preempt
     16 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
     17 root      20   0       0      0      0 I   0.0   0.0   0:00.03 kworker/0:1-cgroup_destroy
[root@ip-10-10-0-30 ec2-user]#
```

i-0cf0ef4ded095e6d9

PublicIPs: 3.111.41.65 PrivateIPs: 10.10.0.30

```
Tasks: 112 total,   2 running, 110 sleeping,   0 stopped,   0 zombie
%Cpu(s): 80.0 us, 20.0 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :    949.5 total,    501.2 free,    152.8 used,    295.5 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.    653.5 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  26371 root      20   0  221356   1008    920 R  99.9   0.1   0:03.49 yes
      1 root      20   0  105668  16788  10068 S   0.0   1.7   0:01.28 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
      9 root      20   0       0      0      0 I   0.0   0.0   0:00.12 kworker/u30:0-events_unbound
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.13 ksoftirqd/0
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.09 rcu_preempt
     16 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
     17 root      20   0       0      0      0 I   0.0   0.0   0:00.08 kworker/0:1-inet_frag_wq
     18 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
     21 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq
[root@ip-10-10-0-9 ec2-user]#
```

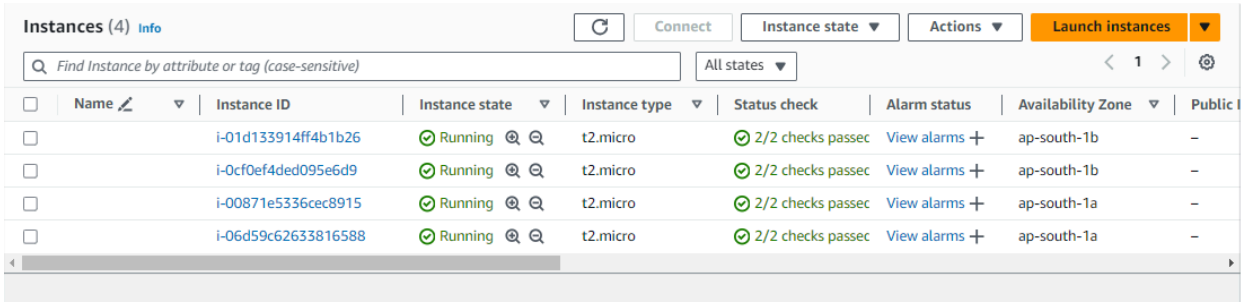
i-06d59c62633816588

PublicIPs: 13.127.233.178 PrivateIPs: 10.10.0.9

In both the instances run top and yes > /dev/null & command

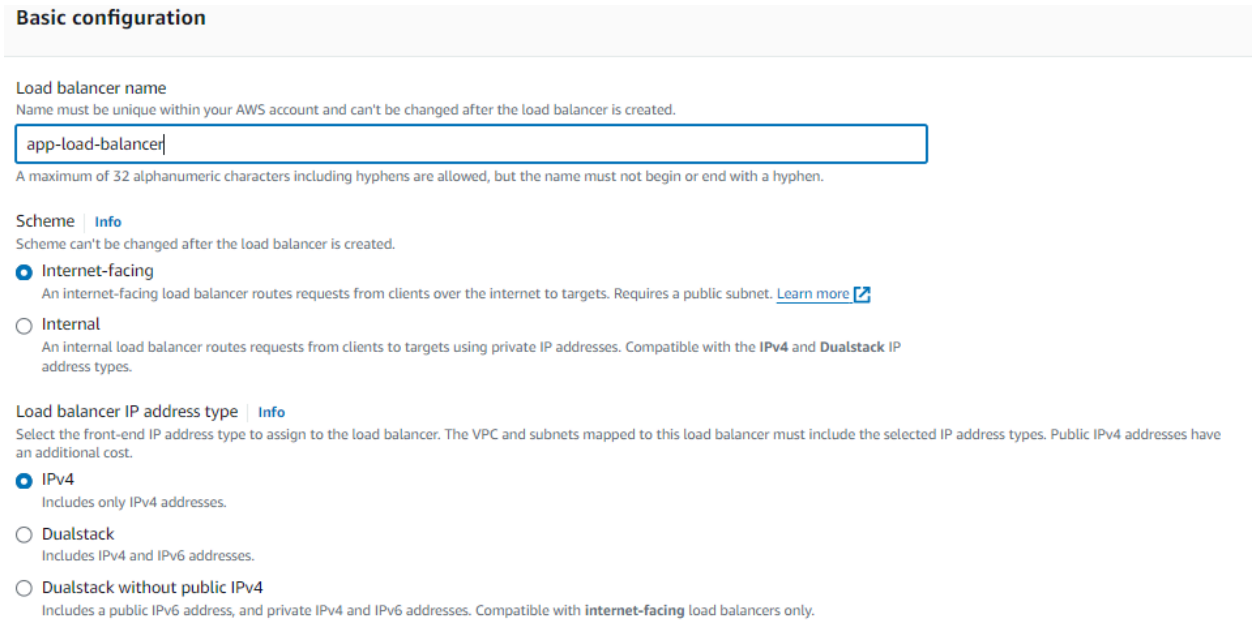
Then , in auto scaling group edit - automatic scaling and create dynamic scaling policy

Output :



31-07–2024

Create load balancer



VPC | Info

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda c using VPC peering. To confirm the VPC for your targets, view target groups. For a new VPC, create a VPC.

vpc-1
vpc-08050bb18da06dc57
IPv4 VPC CIDR: 10.10.0.0/24

Mappings | Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that ar balancer or the VPC are not available for selection.

Availability Zones

ap-south-1a (aps1-az1)

Subnet

subnet-0d1c7c1c2f69ac914 pri-sub
IPv4 subnet CIDR: 10.10.0.0/28

IPv4 address
Assigned by AWS

ap-south-1b (aps1-az3)

Subnet

subnet-0876cb9de19588fb9 pub-sub
IPv4 subnet CIDR: 10.10.0.16/28

IPv4 address
Assigned by AWS

EC2 > Security Groups > Create security group

Create security group Info

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

app load balancer sec-grp

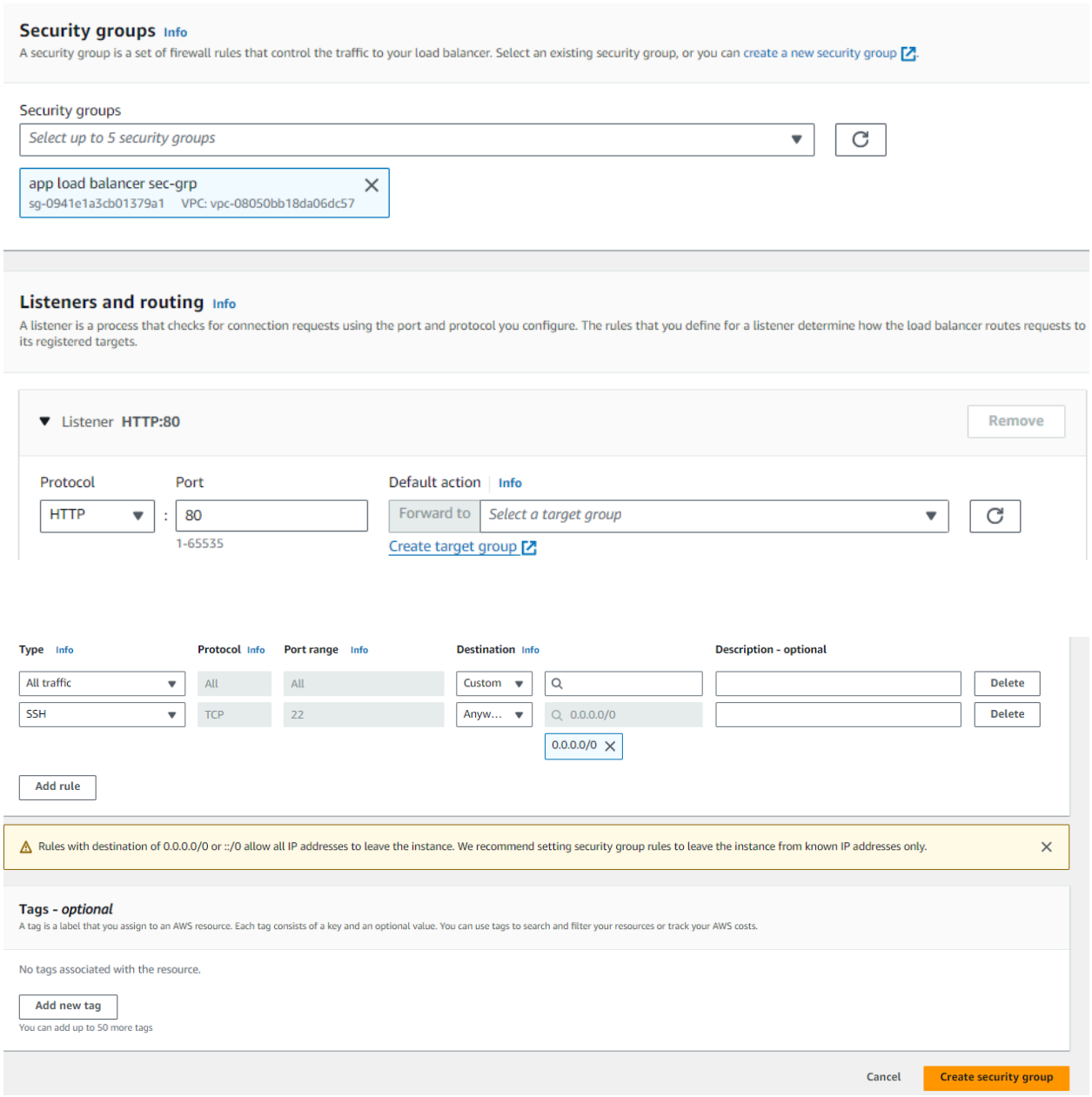
Name cannot be edited after creation.

Description Info

Allows SSH access to developers

VPC Info

vpc-08050bb18da06dc57 (vpc-1)



Create target group

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

- (•) Instances
  - Supports load balancing to instances within a specific VPC.
  - Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity.

Target group name

target grp

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP | 80

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

- (•) IPv4
  Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.
- ( ) IPv6
  Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). Learn more

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

vpc-1
vpc-08050bb18da06dc57
IPv4 VPC CIDR: 10.10.0.0/24

Protocol version

- (●) HTTP1
  Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
- ( ) HTTP2
  Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
- ( ) gRPC
  Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

HTTP ▼

Health check path

Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

▼ **Advanced health check settings**

Restore defaults

Healthy threshold

The number of consecutive health checks successes required before considering an unhealthy target healthy.

5

2-10

Unhealthy threshold

The number of consecutive health check failures required before considering a target unhealthy.

2

2-10

Timeout

The amount of time, in seconds, during which no response means a failed health check.

5 seconds

2-120

Interval

The approximate amount of time between health checks of an individual target

30 seconds

5-300

Success codes

The HTTP codes to use when checking for a successful response from a target. You can specify multiple values (for example, "200,202") or a range of values (for example, "200-299").

200

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2/4)

Filter instances

1

Instance ID	Name	State	Security groups	Zone
i-05d1fcc45155540df		Running	mysecurityg	ap-south-1a
i-070b4886a3e147080	server-2	Running	mysecurityg	ap-south-1b
i-0e39b30c9c4d7d75d		Running	mysecurityg	ap-south-1b
i-01311292de5ef4baa	server-1	Running	mysecurityg	ap-south-1a

2 selected

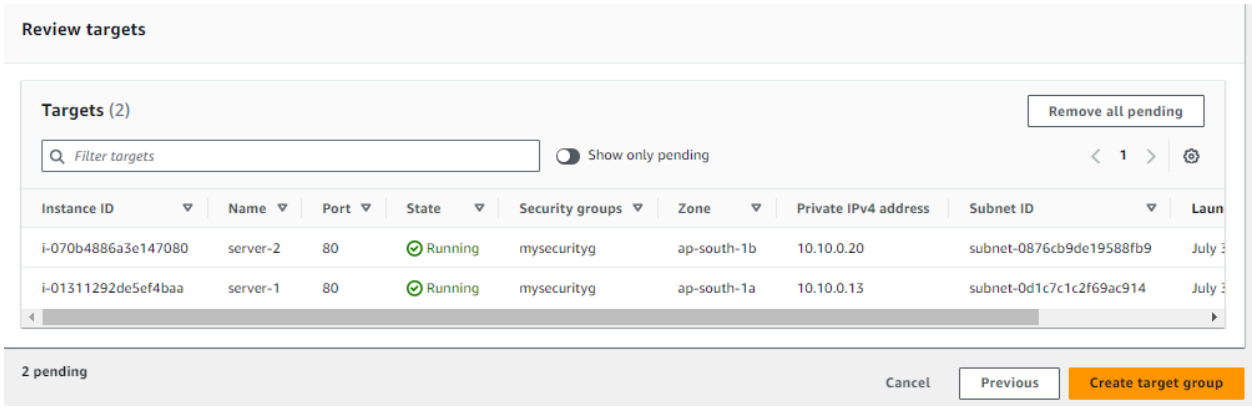
Ports for the selected instances

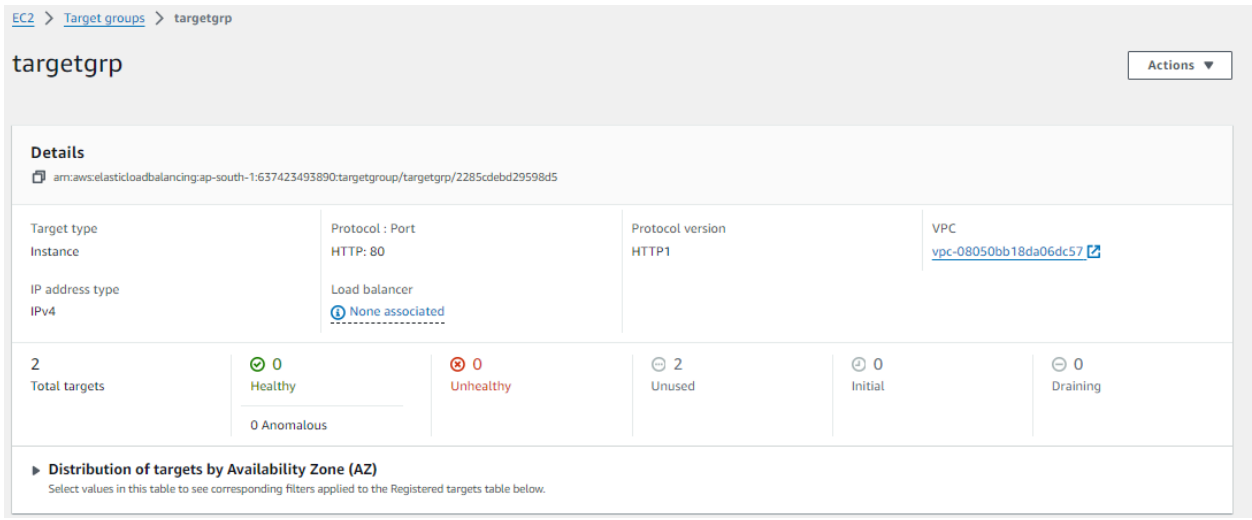
Ports for routing traffic to the selected instances.

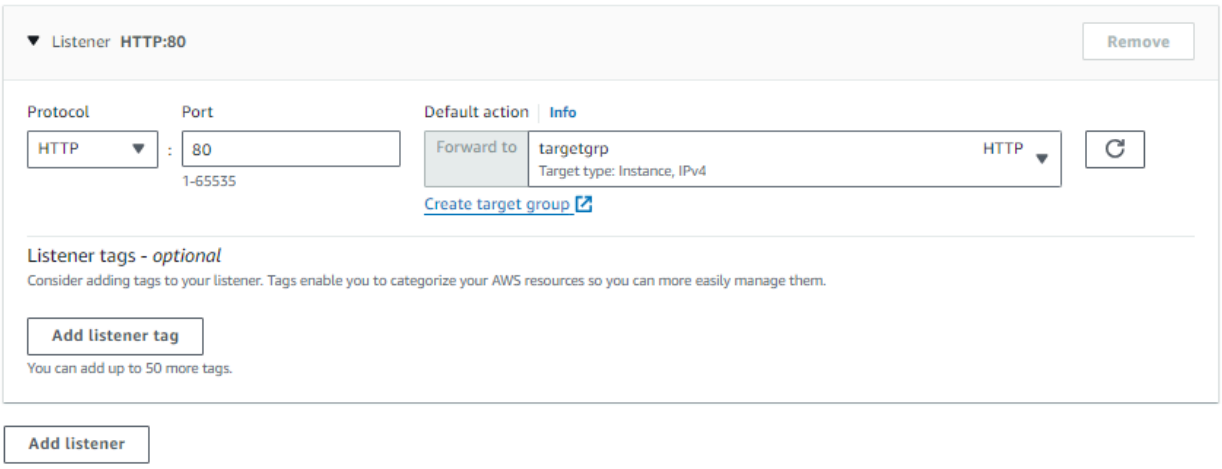
80

1-65535 (separate multiple ports with commas)

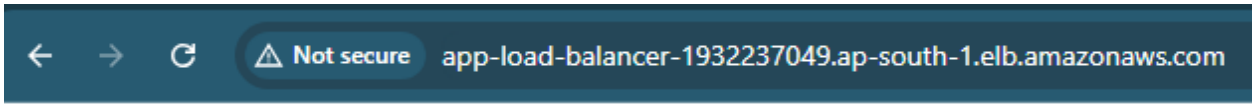
Include as pending below



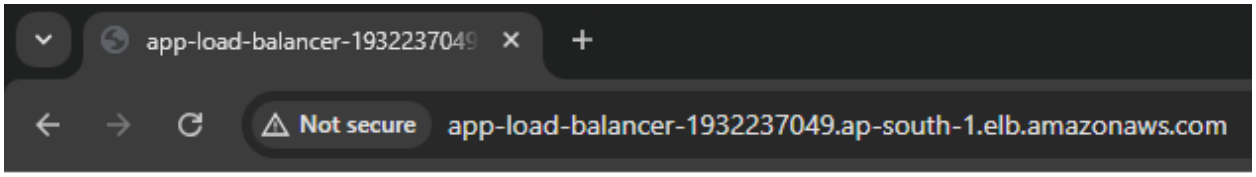




Add listener



Hello Student !



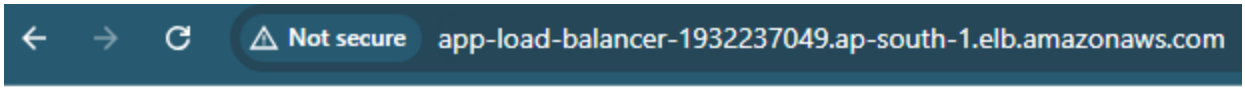
bye Student !

```
[ec2-user@ip-10-10-0-20 ~]$ sudo su
[root@ip-10-10-0-20 ec2-user]# yum install  httpd
Last metadata expiration check: 0:29:33 ago on Wed Jul 31 11:27:48 2024.
Package httpd-2.4.61-1.amzn2023.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-10-10-0-20 ec2-user]# systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
     Active: active (running) since Wed 2024-07-31 11:27:55 UTC; 29min ago
       Docs: man:httpd.service(8)
   Main PID: 3496 (httpd)
     Status: "Total requests: 45; Idle/Busy workers 100/0;Requests/sec: 0.0253; Bytes served/sec:  10 B/sec"
      Tasks: 230 (limit: 1114)
     Memory: 18.1M
        CPU: 1.168s
     CGroup: /system.slice/httpd.service
             ├─ 3496 /usr/sbin/httpd -DFOREGROUND
             ├─ 3578 /usr/sbin/httpd -DFOREGROUND
             ├─ 3584 /usr/sbin/httpd -DFOREGROUND
             ├─ 3585 /usr/sbin/httpd -DFOREGROUND
             ├─ 3586 /usr/sbin/httpd -DFOREGROUND
             └─26733 /usr/sbin/httpd -DFOREGROUND

Jul 31 11:27:55 ip-10-10-0-20.ap-south-1.compute.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Jul 31 11:27:55 ip-10-10-0-20.ap-south-1.compute.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Jul 31 11:27:55 ip-10-10-0-20.ap-south-1.compute.internal httpd[3496]: Server configured, listening on: port 80
[root@ip-10-10-0-20 ec2-user]# cd /var/www/html
[root@ip-10-10-0-20 html]# ls
index.html
[root@ip-10-10-0-20 html]# vi index.html
```

Edit inbound rules in both servers

In server 2 : connect

>sudo su
>systemctl stop httpd
>systemctl refresh httpd
>systemctl start httpd



Hello Student !

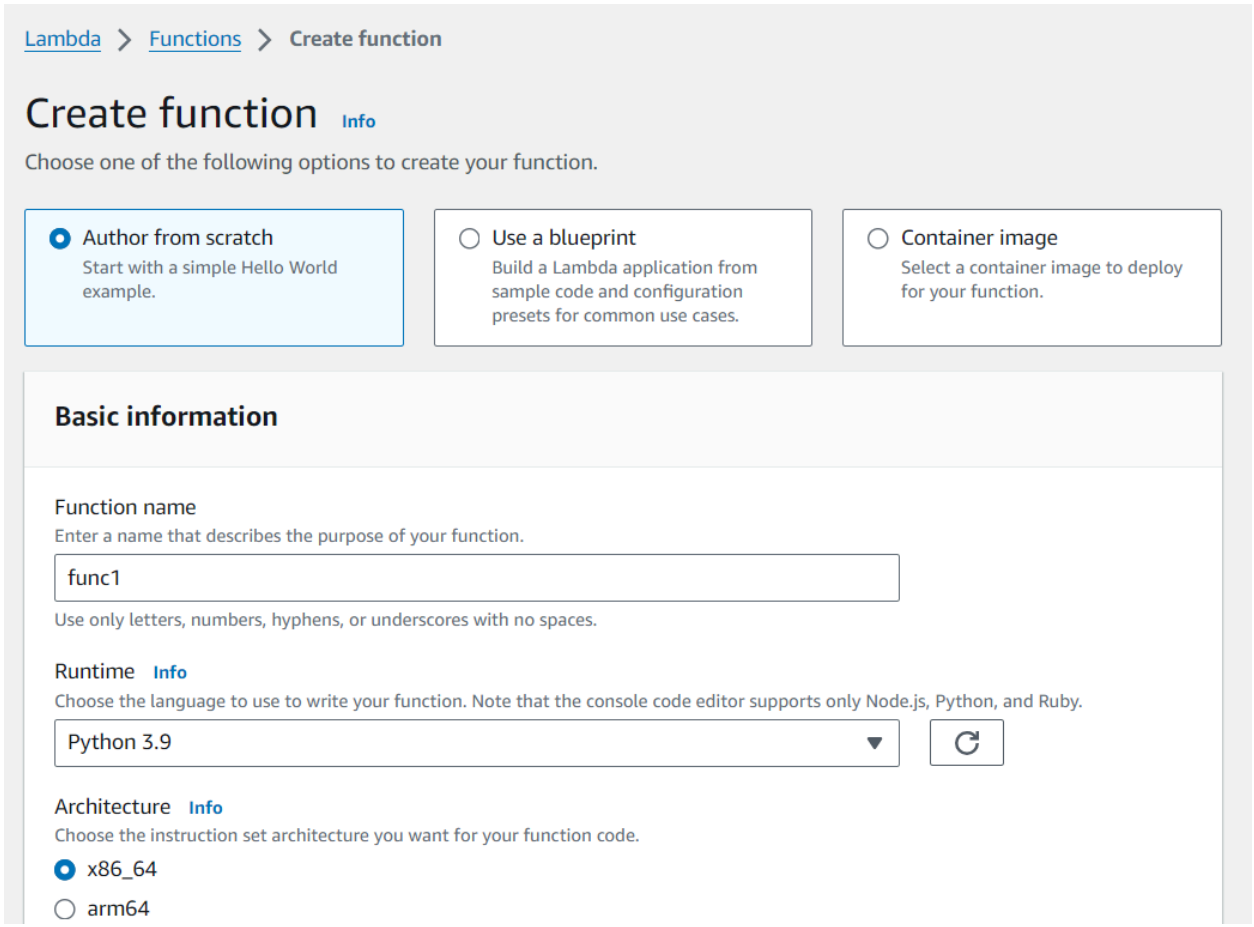
LAMBDA WITH SNS date : 07/08/24

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.

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



Create iam role

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

Lambda ▼

Choose a use case for the specified service.

Use case

- (●) **Lambda**
  Allows Lambda functions to call AWS services on your behalf.

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

role-1

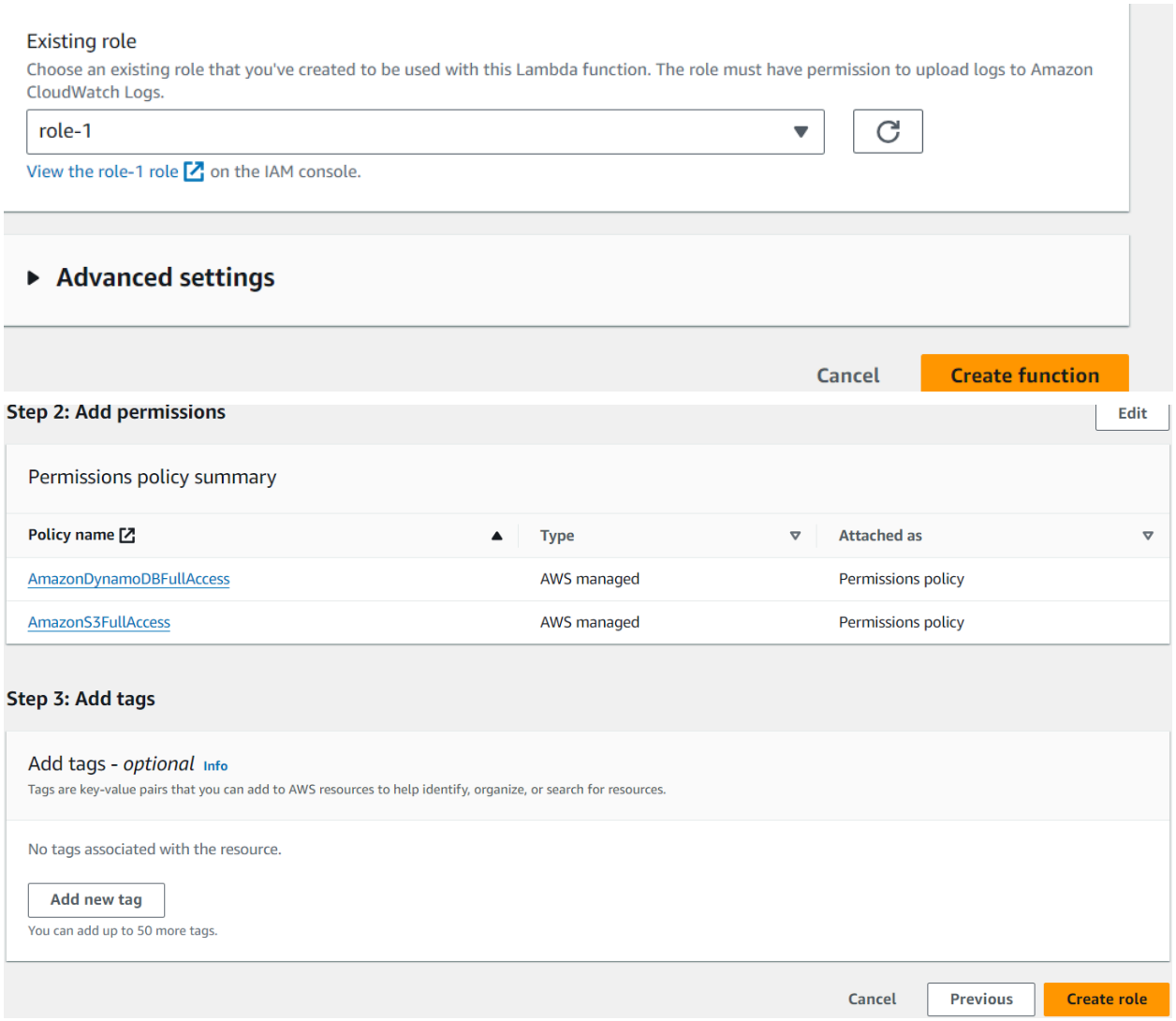
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

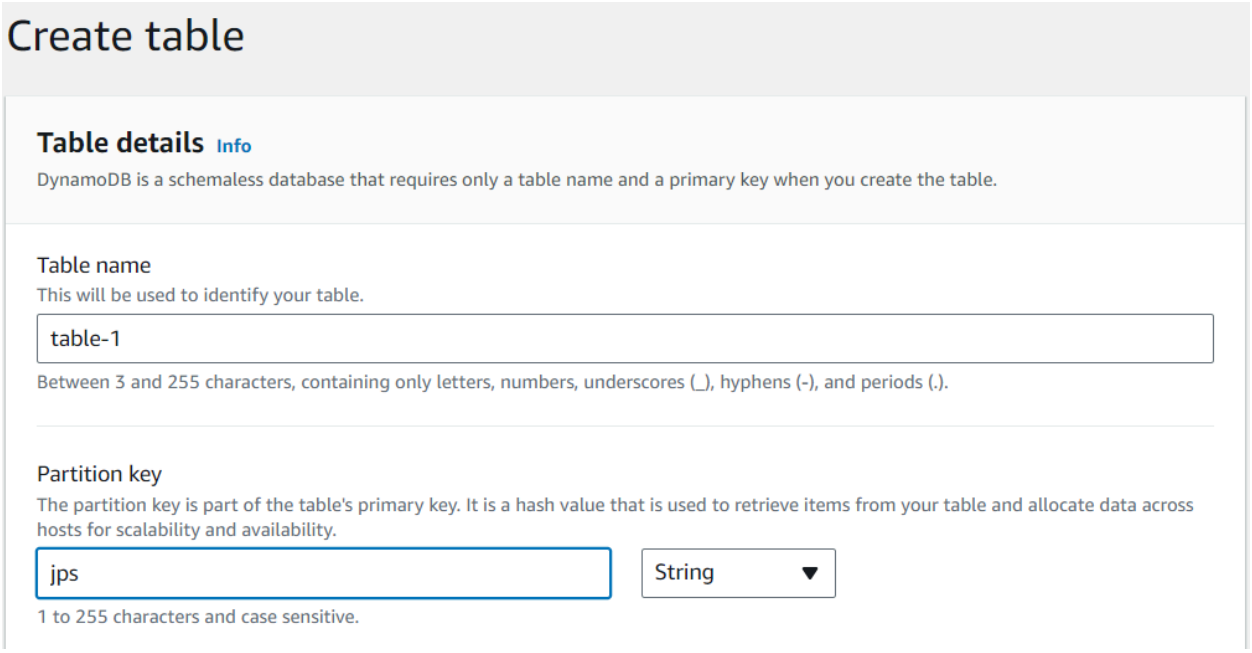
Add a short explanation for this role.

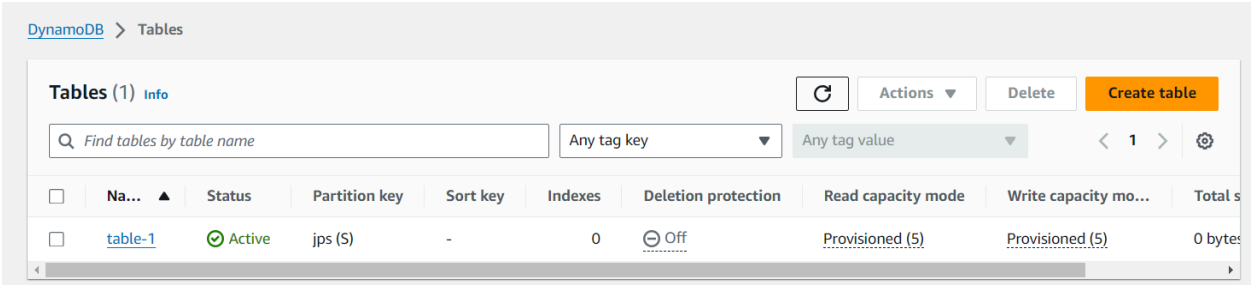
Allows Lambda functions to call AWS services on your behalf.

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

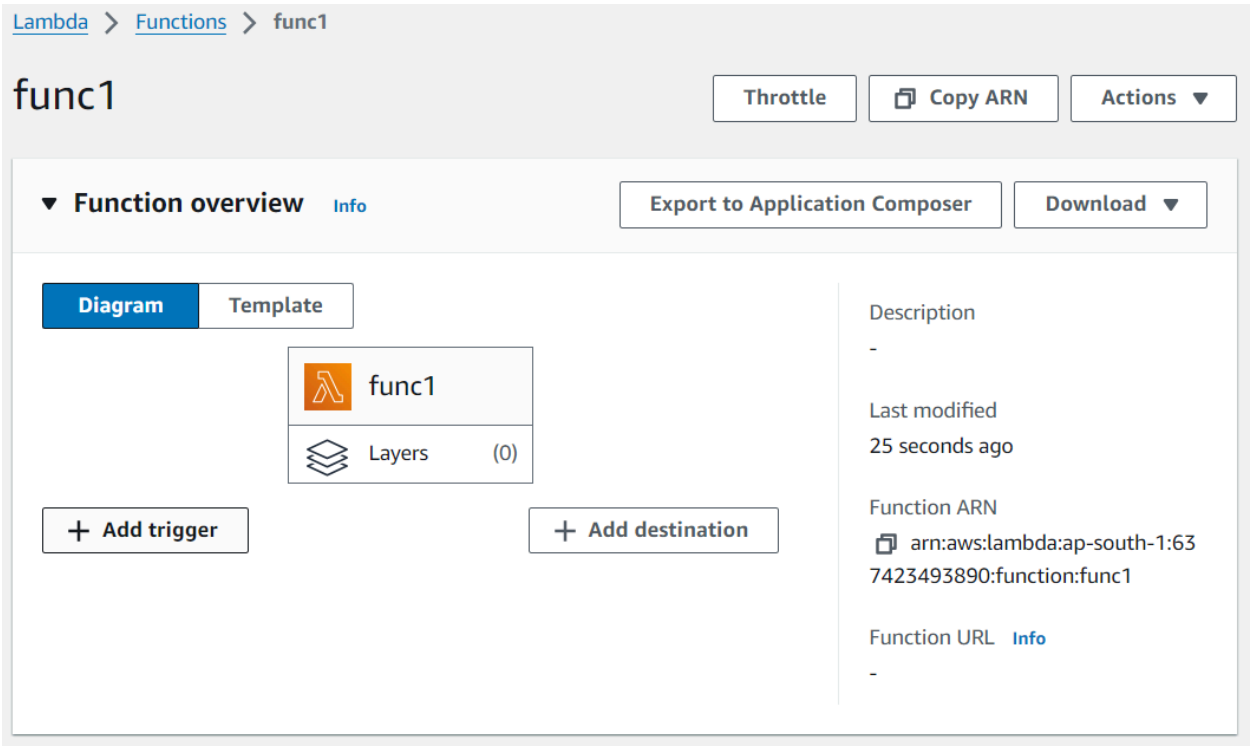

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.
role-1
View the role-1 role on the IAM console.
Advanced settings
Cancel
Create function
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
AmazonDynamoDBFullAccess
AWS managed
Permissions policy
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.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create role

Dynamo-db >





Add trigger



Trigger configuration Info

S3
aws asynchronous storage

Bucket

Choose or enter the ARN of an S3 bucket that serves as the event source. The bucket must be in the same region as the function.

s3/mynewbuketttt

Bucket region: ap-south-1

Event types

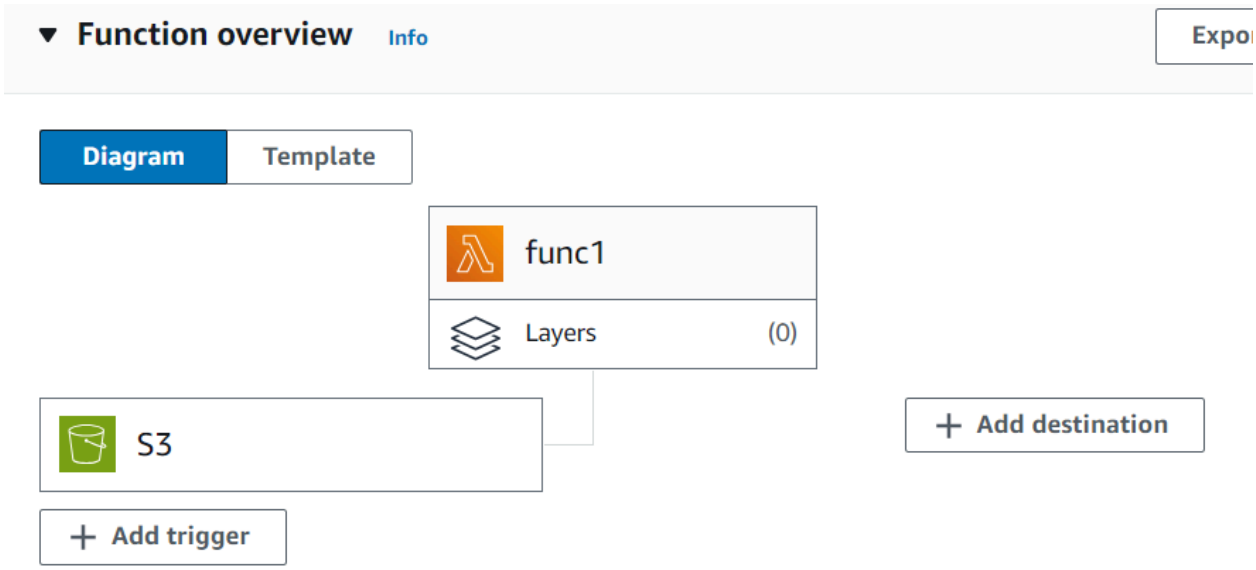
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.

PUT

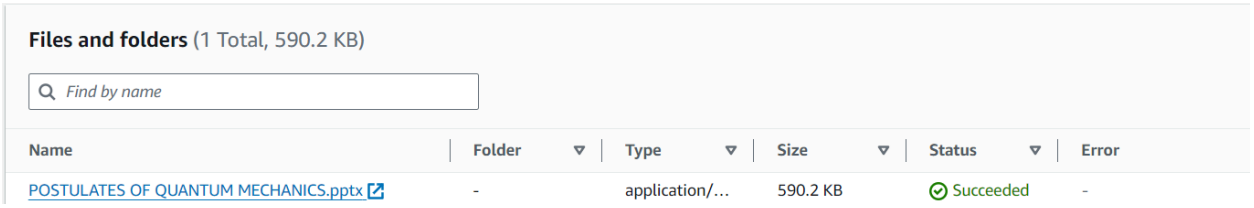
All object delete events

Permanently deleted

Delete marker created



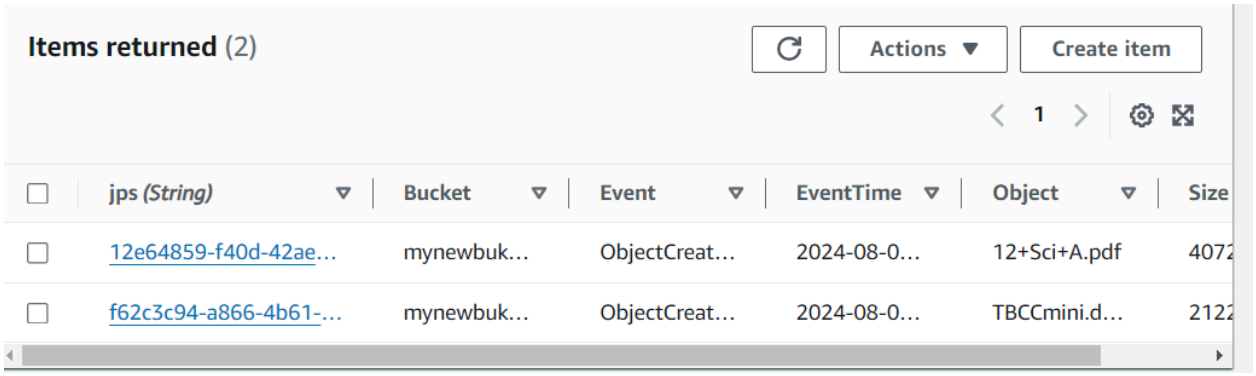
Upload a file in s3 bucket




```
import boto3
from uuid import uuid4

def lambda_handler(event, context):
        s3 = boto3.client("s3")
        dynamodb = boto3.resource('dynamodb')

        for record in event['Records']:
                bucket_name = record['s3']['bucket']['name']
                object_key = record['s3']['object']['key']
                size = record['s3']['object'].get('size', -1)
                event_name = record['eventName']
                event_time = record['eventTime']

                dynamo_table = dynamodb.Table('table-1')  # Replace 'table1' with your actual table name

                dynamo_table.put_item(
                        Item={
                                'jps': str(uuid4()),
                                'Bucket': bucket_name,
                                'Object': object_key,
```

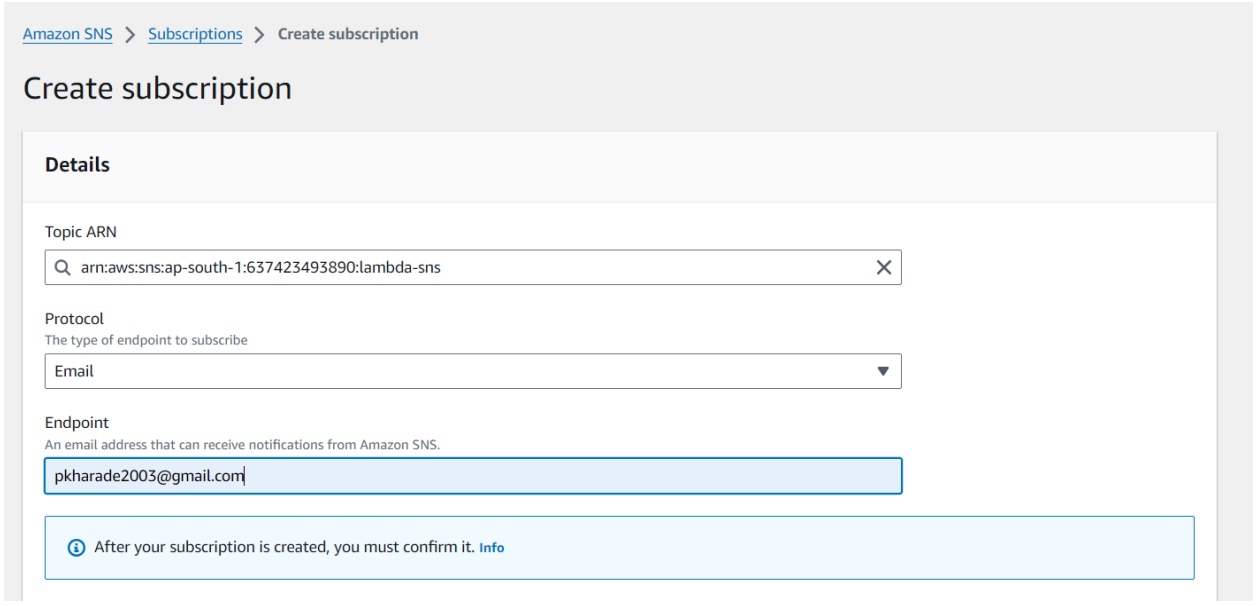
```
                    'Size': size,
                    'Event': event_name,
                    'EventTime':event_time
                }
            )
```

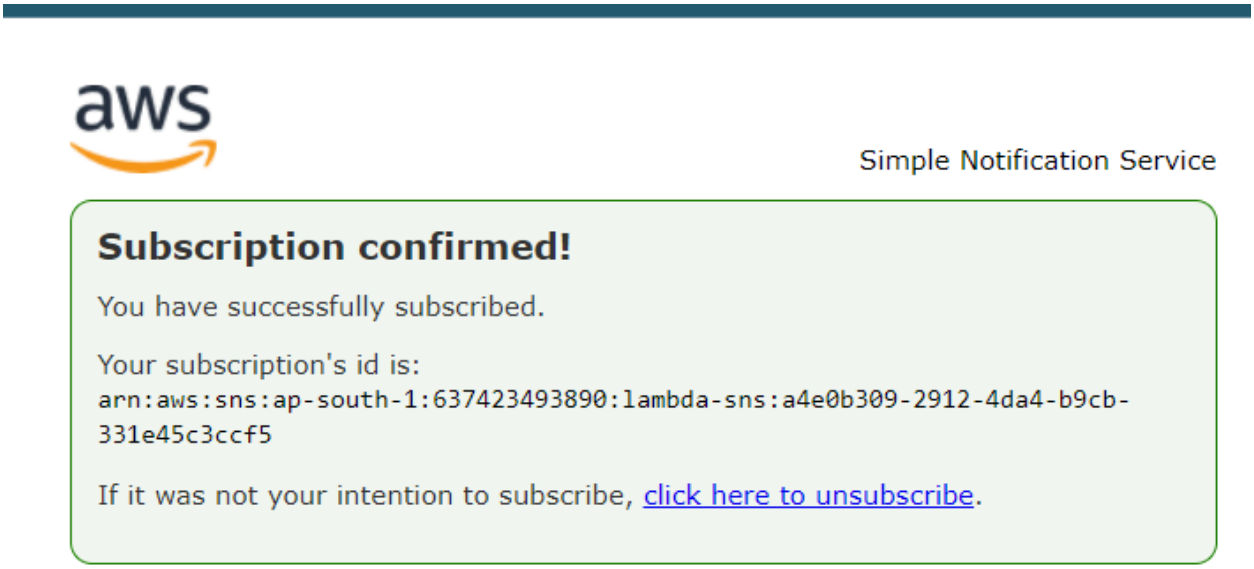
Save and deploy the code and then upload the files > go to s3 items and check retrieved files

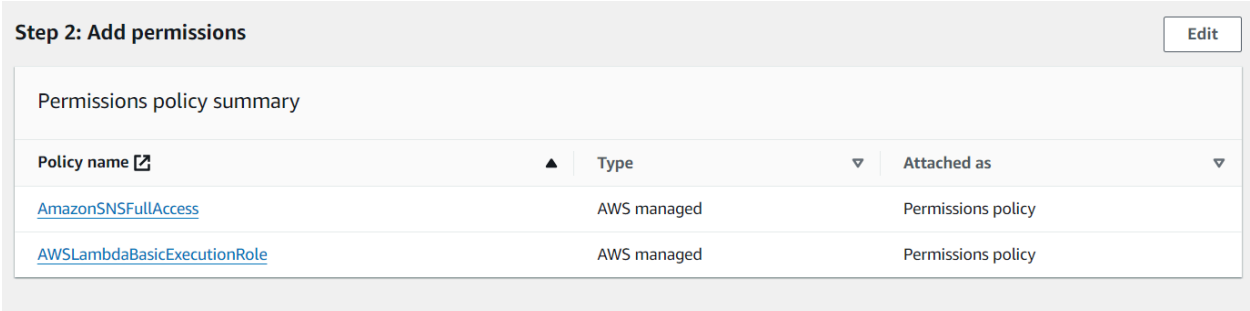


TASK - ADD SNS (EMAIL) TO LAMBDA

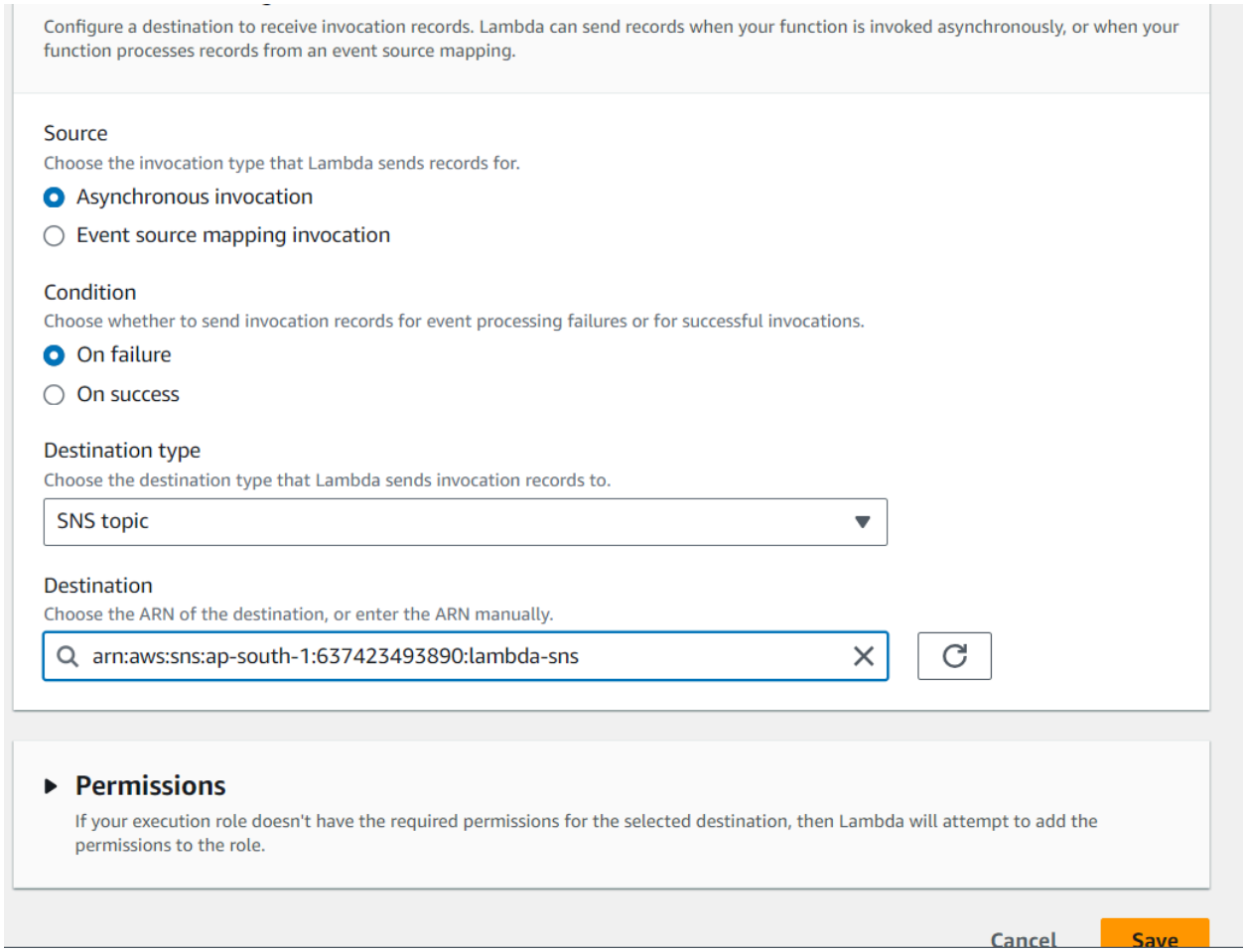
Sns

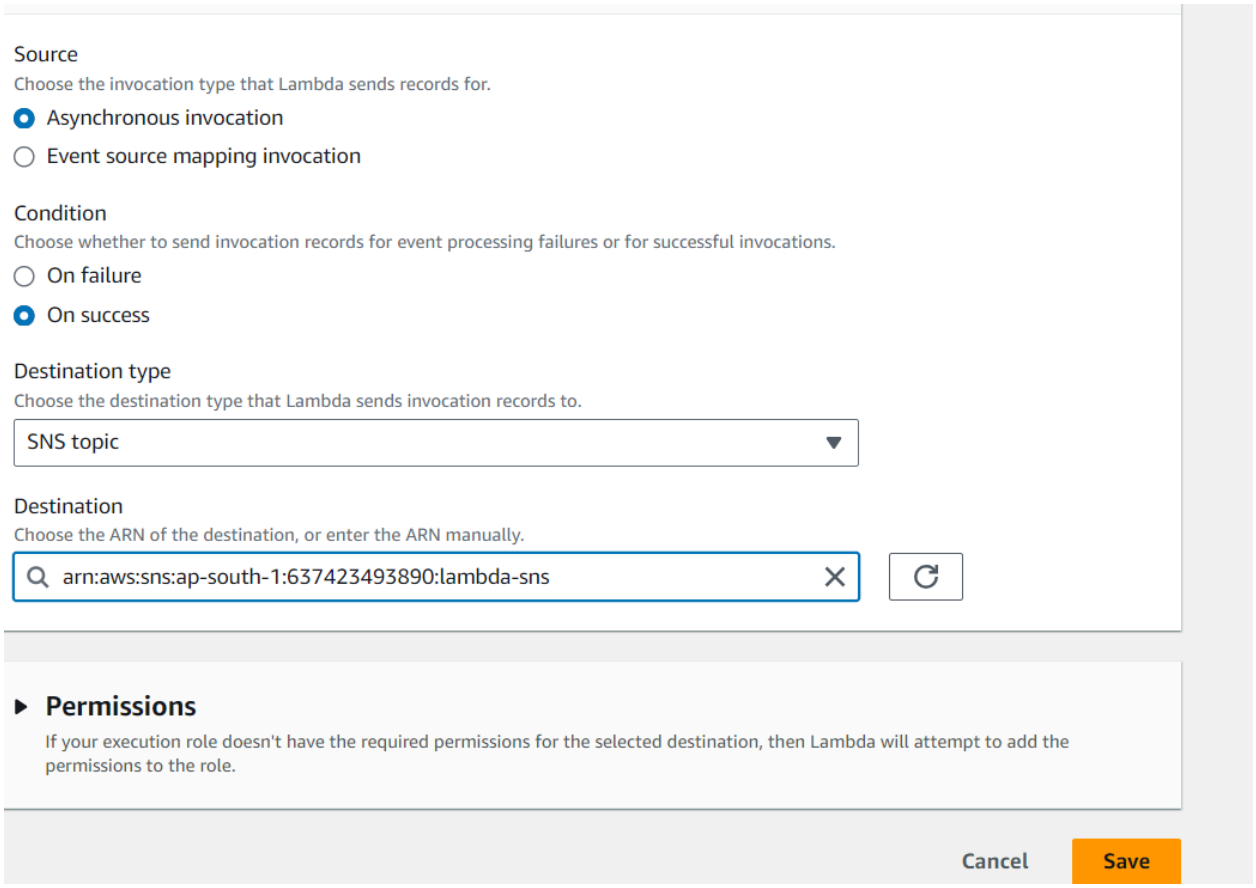


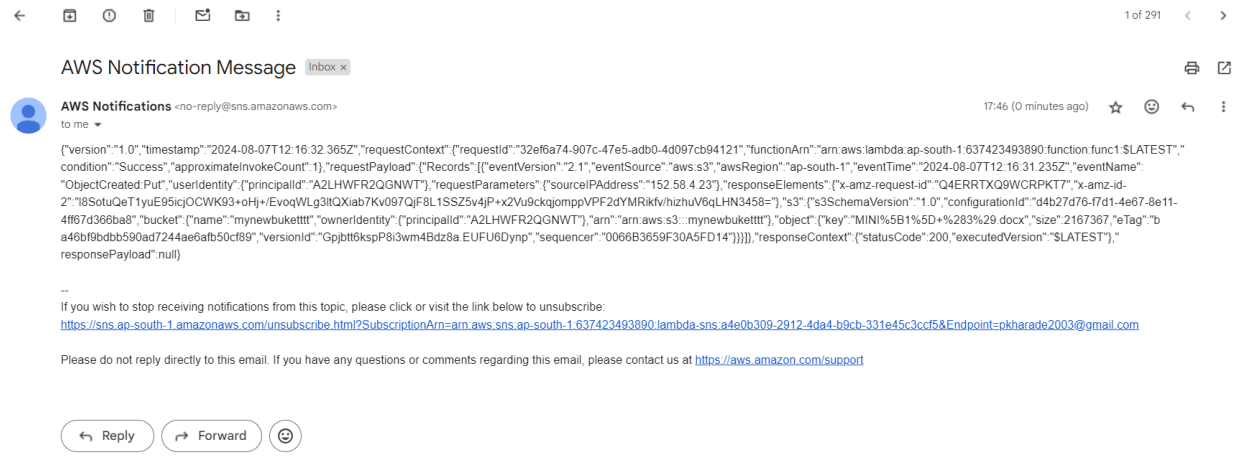

aws
Simple Notification Service
Subscription confirmed!
You have successfully subscribed.
Your subscription's id is:
arn:aws:sns:ap-south-1:637423493890:lambda-sns:a4e0b309-2912-4da4-b9cb-331e45c3ccf5
If it was not your intention to subscribe, click here to unsubscribe.


Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
AmazonSNSFullAccess
AWS managed
Permissions policy
AWSLambdaBasicExecutionRole
AWS managed
Permissions policy

At destination

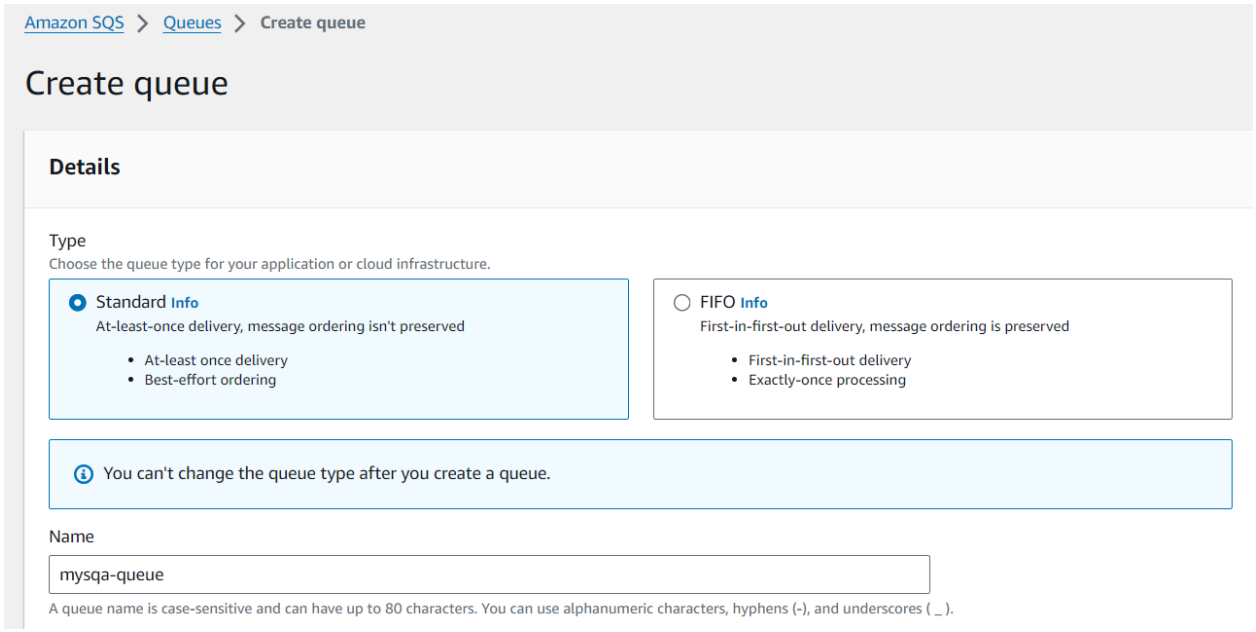


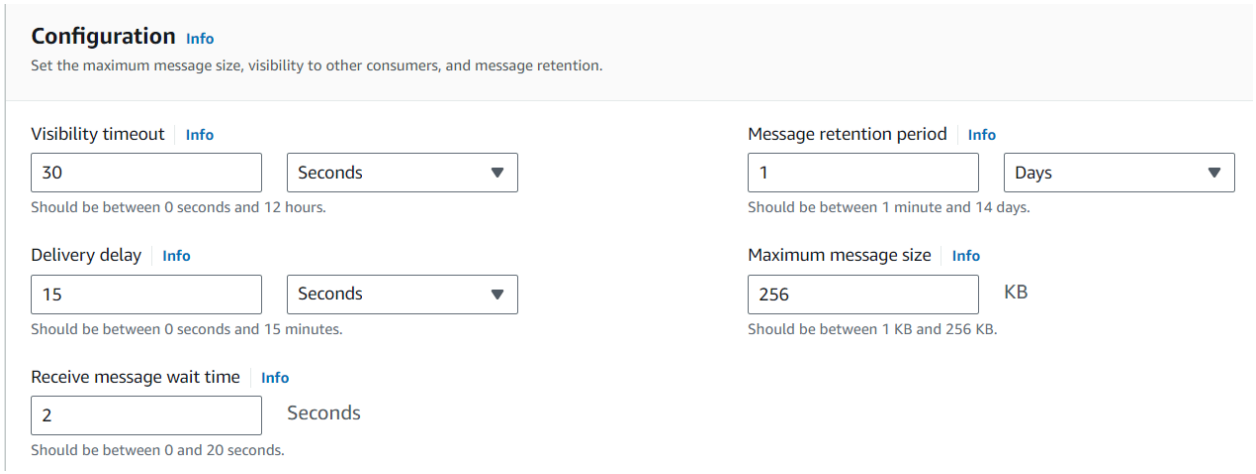

Source
Choose the invocation type that Lambda sends records for.
Asynchronous invocation
Event source mapping invocation
Condition
Choose whether to send invocation records for event processing failures or for successful invocations.
On failure
On success
Destination type
Choose the destination type that Lambda sends invocation records to.
SNS topic
Destination
Choose the ARN of the destination, or enter the ARN manually.
arn:aws:sns:ap-south-1:637423493890:lambda-sns
Permissions
If your execution role doesn't have the required permissions for the selected destination, then Lambda will attempt to add the permissions to the role.
Cancel
Save


1 of 291
AWS Notification Message
Inbox ×
AWS Notifications <no-reply@sns.amazonaws.com>
to me
17:46 (0 minutes ago)
{"version":"1.0","timestamp":"2024-08-07T12:16:32.365Z","requestContext":{"requestId":"32ef6a74-907c-47e5-adb0-4d097cb94121","functionArn":"arn:aws:lambda:ap-south-1:637423493890:function:func1:$LATEST","condition":"Success","approximateInvokeCount":1},"requestPayload":{"Records":[{"eventVersion":"2.1","eventSource":"aws:s3","awsRegion":"ap-south-1","eventTime":"2024-08-07T12:16:31.235Z","eventName":"ObjectCreated:Put","userIdentity":{"principalId":"A2LHWFR2QGNWT"},"requestParameters":{"sourceIPAddress":"152.58.4.23"},"responseElements":{"x-amz-request-id":"Q4ERRTXQ9WCRPKT7","x-amz-id-2":"l8SotuQeT1yuE95icjOCWK93+oHj+/EvoqWLg3ltQXiab7Kv097QjF8L1SSZ5v4jP+x2Vu9ckqjomppVPF2dYMRikfv/hizhuV6qLHN3458="},"s3":{"s3SchemaVersion":"1.0","configurationId":"d4b27d76-f7d1-4e67-8e11-4ff67d366ba8","bucket":{"name":"mynewbuketttt","ownerIdentity":{"principalId":"A2LHWFR2QGNWT"},"arn":"arn:aws:s3:::mynewbuketttt"},"object":{"key":"MINI%5B1%5D+%283%29.docx","size":2167367,"eTag":"ba46bf9bdbb590ad7244ae6afb50cf89","versionId":"Gpjbtt6kspP8i3wm4Bdz8a.EUFU6Dynp","sequencer":"0066B3659F30A5FD14"}}}],"responseContext":{"statusCode":200,"executedVersion":"$LATEST"},"responsePayload":null}
--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.ap-south-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:ap-south-1:637423493890:lambda-sns:a4e0b309-2912-4da4-b9cb-331e45c3ccf5&Endpoint=pkharade2003@gmail.com
Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support
Reply
Forward

Simple Queue Services **Date : 08-08-2024**

Step 1: Create queue





Choose method

- **Basic**
  Use simple criteria to define a basic access policy.
- **Advanced**
  Use a JSON object to define an advanced access policy.

Define who can send messages to the queue

- **Only the queue owner**
  Only the owner of the queue can send messages to the queue.
- **Only the specified AWS accounts, IAM users and roles**
  Only the specified AWS account IDs, IAM users and roles can send messages to the queue.

Define who can receive messages from the queue

- **Only the queue owner**
  Only the owner of the queue can receive messages from the queue.
- **Only the specified AWS accounts, IAM users and roles**
  Only the specified AWS account IDs, IAM users and roles can receive messages from the queue.

JSON (read-only)


```
{
  "Version": "2012-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__owner_statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "637423493890"
      },
      "Action": [
        "SQS:*"
      ],
      "Resource": "arn:aws:sqs:ap-south-
1:637423493890:mysqa-queue"
```


Select which source queues can use this queue as the dead-letter queue.

- Disabled
- Enabled

Dead-letter queue - *Optional* Info

Send undeliverable messages to a dead-letter queue.

Set this queue to receive undeliverable messages.

- Disabled
- Enabled

Tags - *Optional* Info

A tag is a label assigned to an AWS resource. Use tags to search and filter your resources or track your AWS costs.

Key — Enter key

Value - *optional* — Enter value

Remove

Add new tag

You can add 49 more tags.

Cancel | Create queue

Amazon SQS > Queues

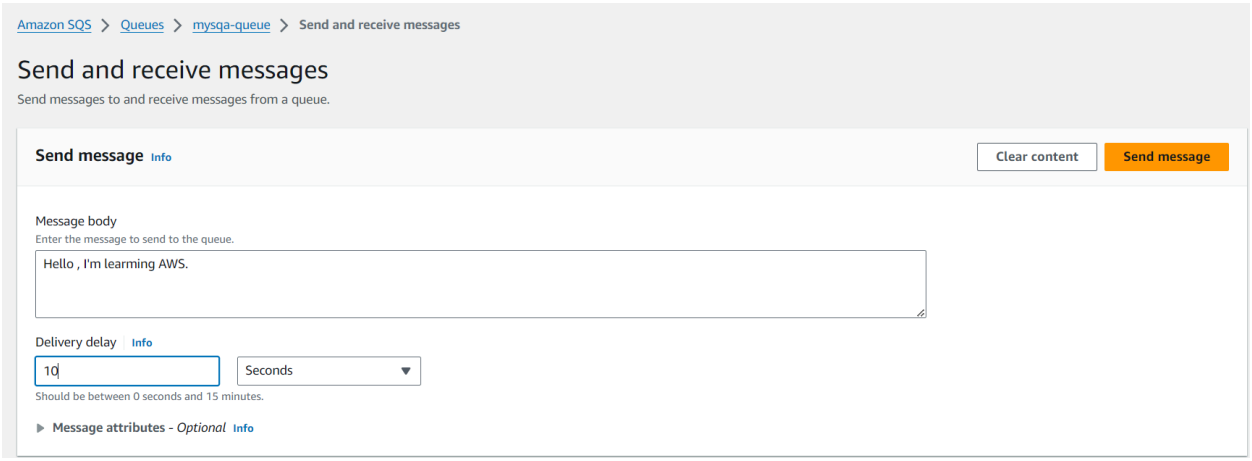
Queues (1)

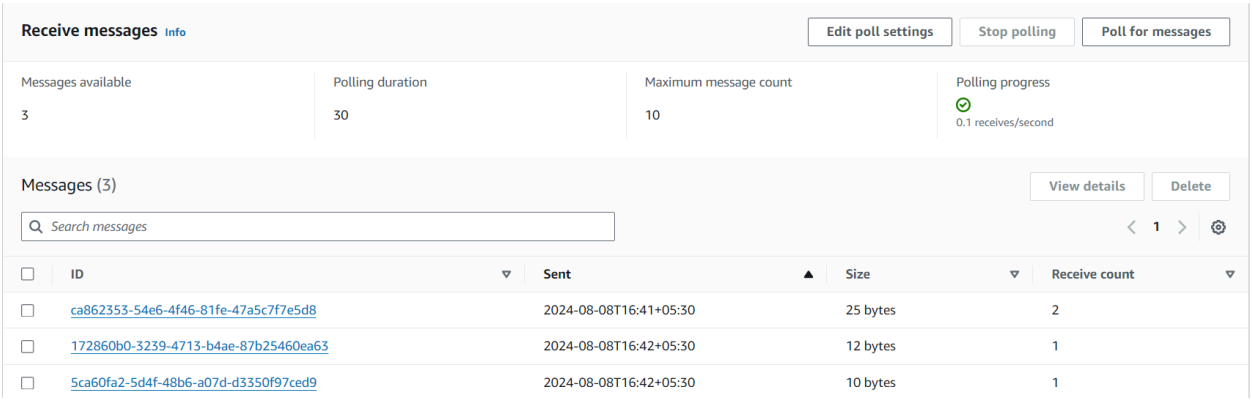
Edit | Delete | Send and receive messages | Actions | Create queue

Search queues by prefix

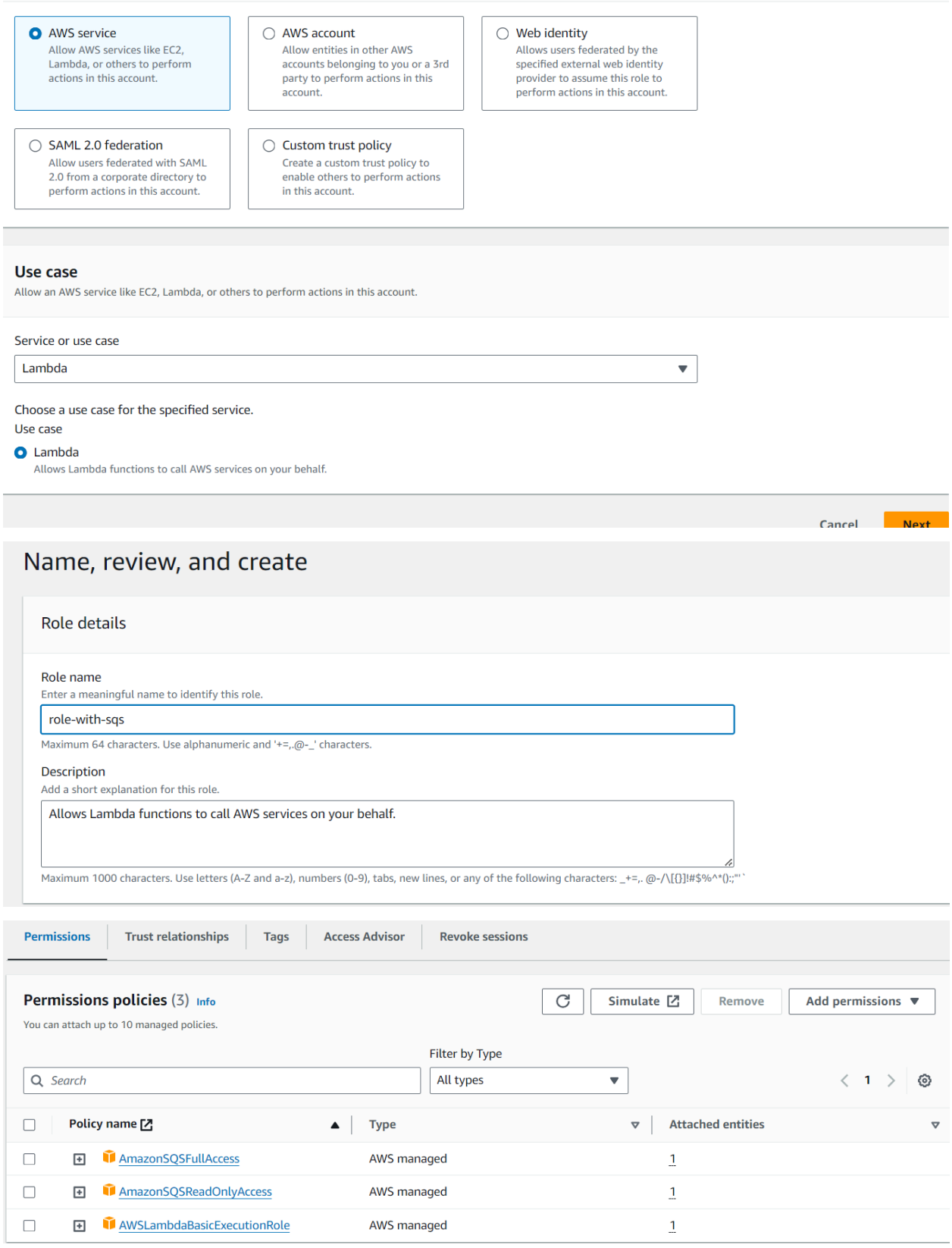
1

Name	Type	Created	Messages available	Messages in flight	Encryption	Content-based deduplication
mysqa-queue	Standard	2024-08-08T16:34+05:30	0	0	Disabled	-

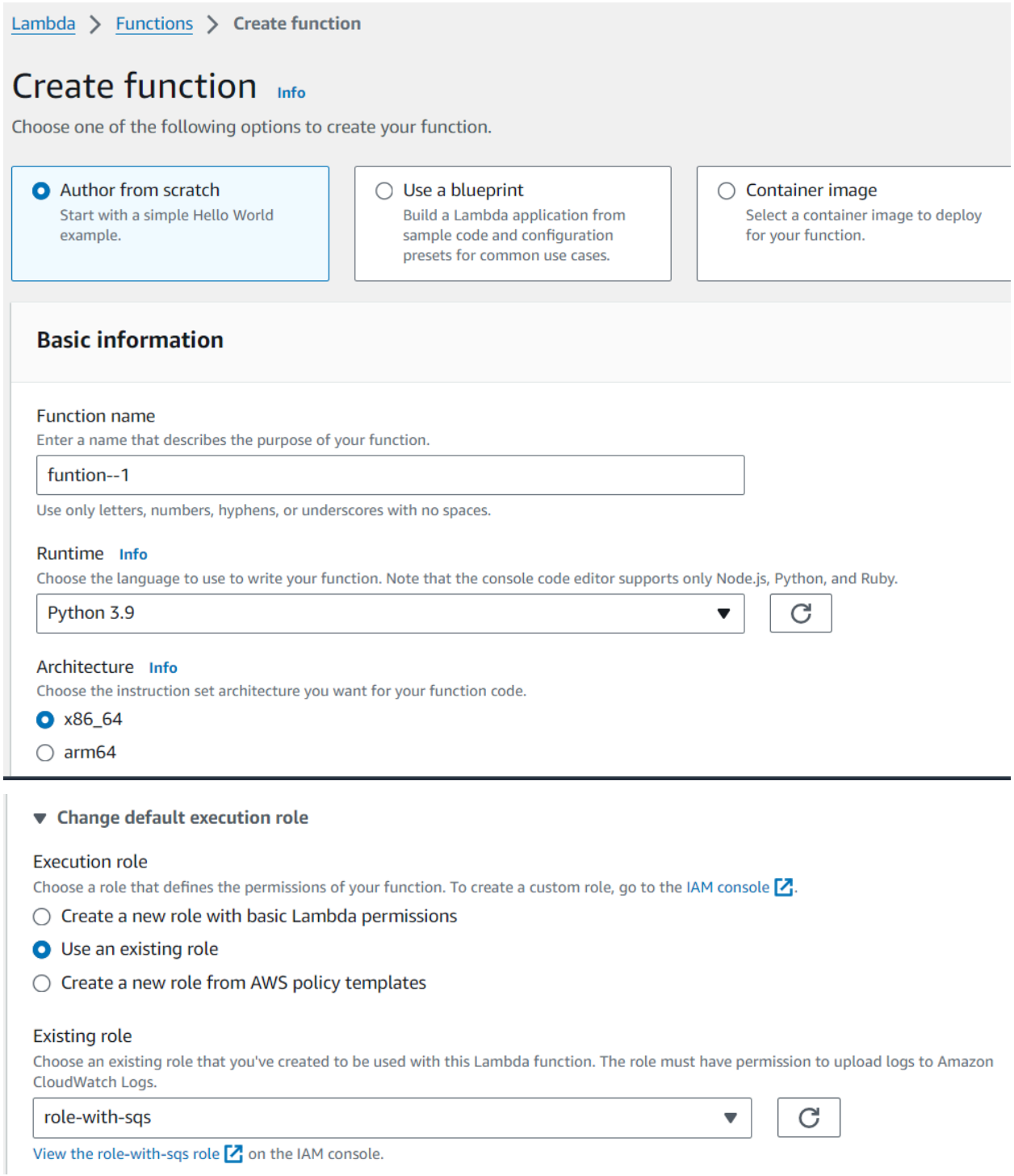




Create IAM role


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
Lambda
Choose a use case for the specified service.
Use case
Lambda
Allows Lambda functions to call AWS services on your behalf.
Cancel
Next
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
role-with-sqs
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows Lambda functions 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: _+=,. @-/\[{}]!#$%^*();:"'`
Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions
Permissions policies (3) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
Search
All types
1
Policy name
Type
Attached entities
AmazonSQSFullAccess
AWS managed
1
AmazonSQSReadOnlyAccess
AWS managed
1
AWSLambdaBasicExecutionRole
AWS managed
1

Create lambda function



Add trigger

Lambda > Add triggers

Add trigger

Trigger configuration Info

SQS
aws event-source-mapping polling queue

SQS queue
Choose or enter the ARN of an SQS queue.

arn:aws:sqs:ap-south-1:637423493890:mysqa-queue

Activate trigger
Select to activate the trigger now. Keep unchecked to create the trigger in a deactivated state for testing (recommended).

Batch size - *optional*
The number of records in each batch to send to the function.

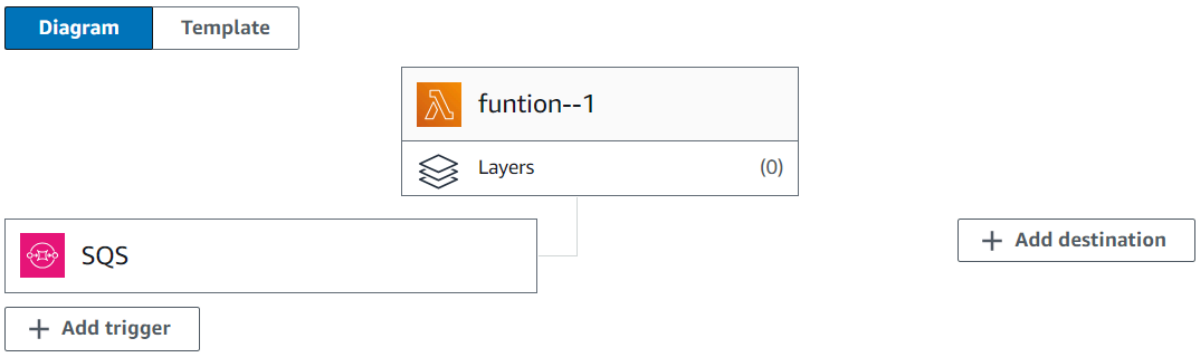
10

The maximum is 10,000 for standard queues and 10 for FIFO queues.

Batch window - *optional*
The maximum amount of time to gather records before invoking the function, in seconds.

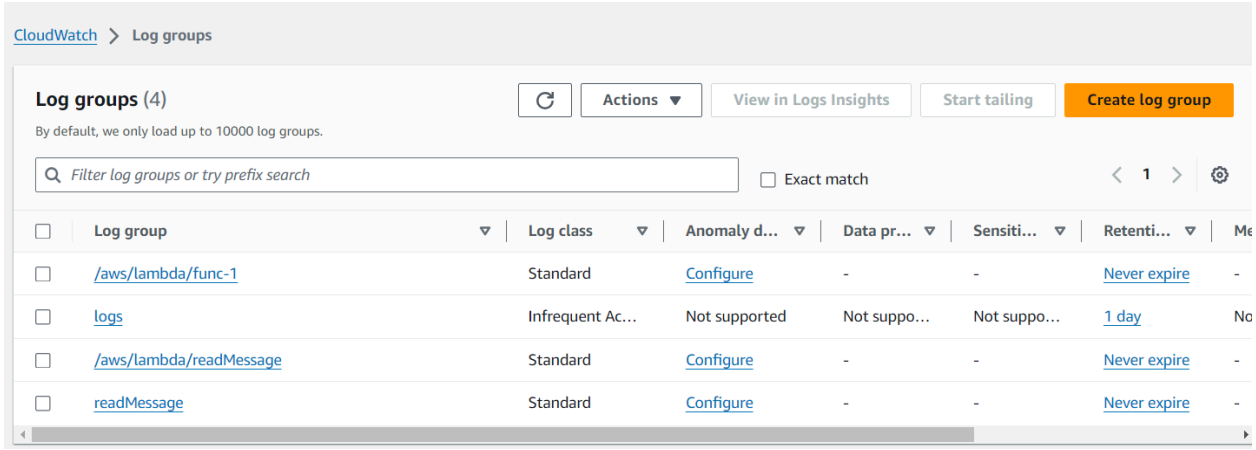
0

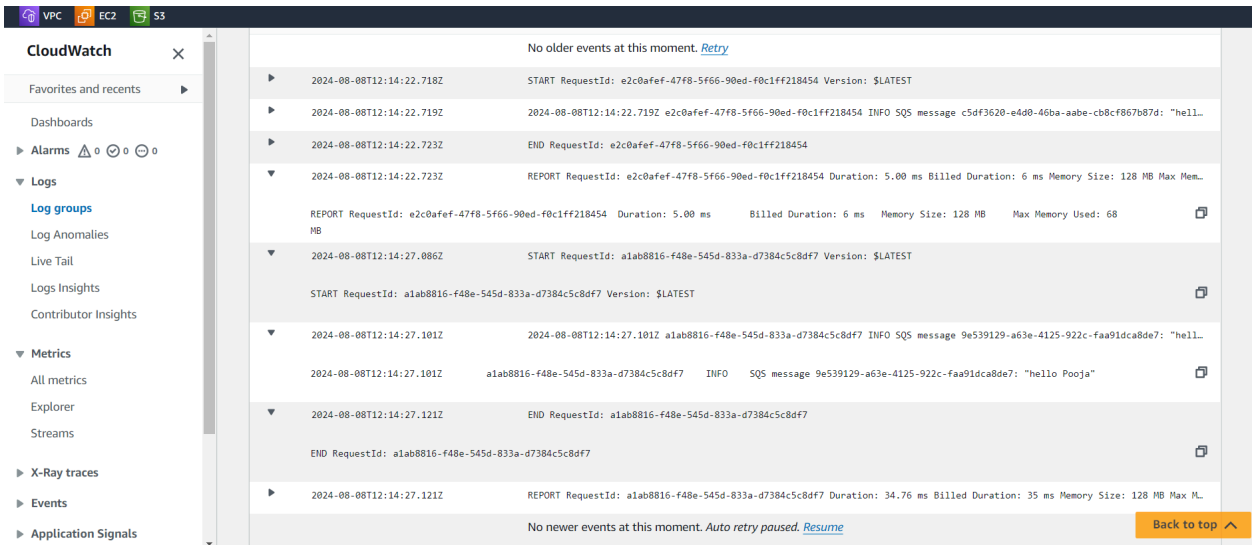
Function overview Info




```
2024-08-08T12:14:27.086Z        START RequestId: a1ab8816-f48e-545d-833a-d7384c5c8df7 Version: $LATEST
START RequestId: a1ab8816-f48e-545d-833a-d7384c5c8df7 Version: $LATEST
2024-08-08T12:14:27.101Z        2024-08-08T12:14:27.101Z a1ab8816-f48e-545d-833a-d7384c5c8df7 INFO SQS message 9e539129-a63e-4125-922c-faa91dca8de7: "hell…
2024-08-08T12:14:27.101Z        a1ab8816-f48e-545d-833a-d7384c5c8df7    INFO    SQS message 9e539129-a63e-4125-922c-faa91dca8de7: "hello Pooja"
```

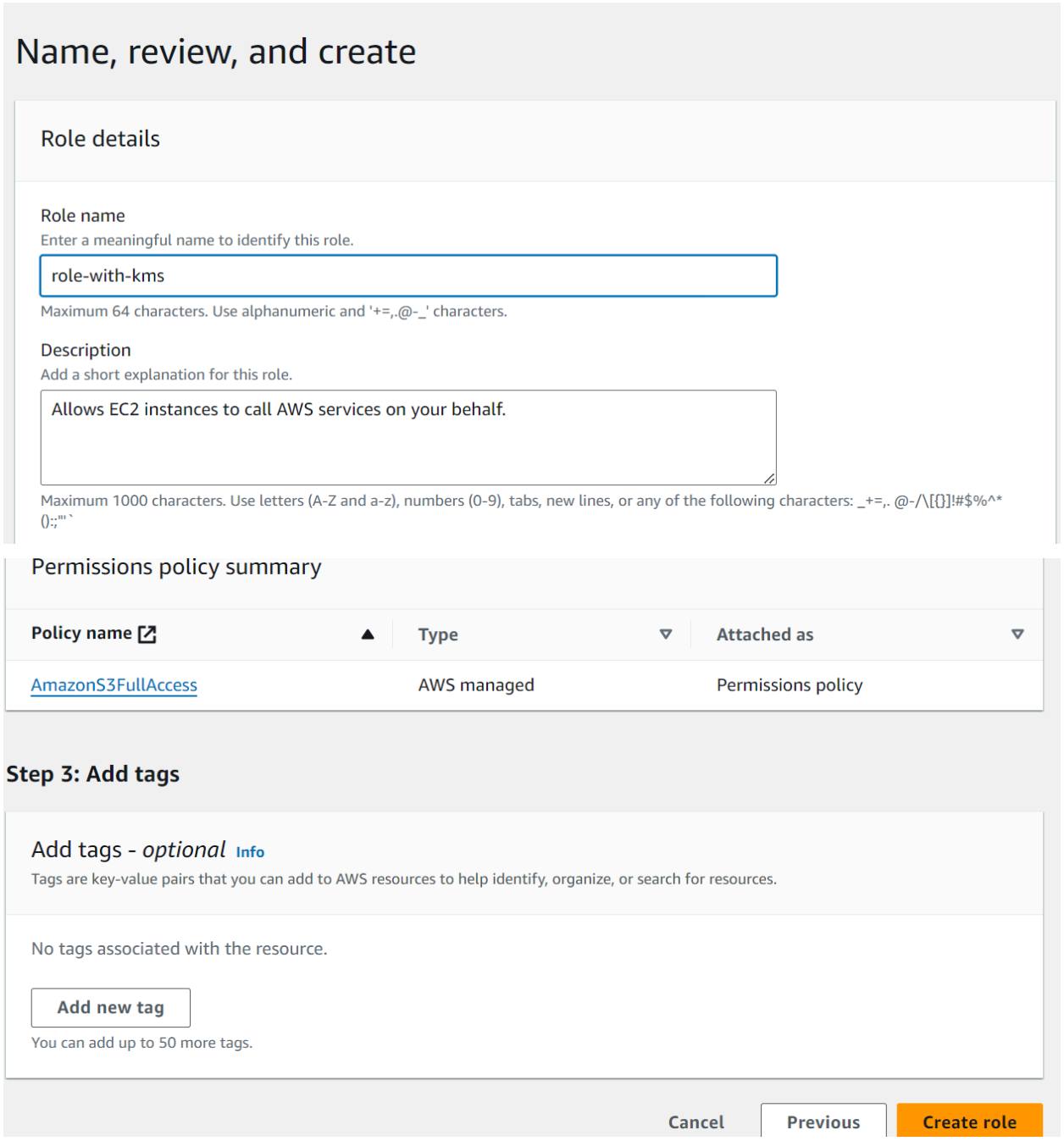
monitor> view cloudwatch logs





AIM : KMS (KEY MANAGEMENT SERVICE) date : 09-8-24

Create iam user and role



Configure key

Key type Help me choose

- (●) Symmetric
  A single key used for encrypting and decrypting data or generating and verifying HMAC codes
- ( ) Asymmetric
  A public and private key pair used for encrypting and decrypting data, signing and verifying messages, or deriving shared secrets

Key usage Help me choose

- (●) Encrypt and decrypt
  Use the key only to encrypt and decrypt data.
- ( ) Generate and verify MAC
  Use the key only to generate and verify hash-based message authentication codes (HMAC).

▼ Advanced options

Key material origin

Key material origin is a KMS key property that represents the source of the key material when creating the KMS key. Help me choose

- ( ) KMS - *recommended*
  AWS KMS creates and manages the key material for the KMS key.
- (●) External (Import Key material)
  You create and import the key material for the KMS key.
- ( ) AWS CloudHSM key store
  AWS KMS creates the key material in the AWS CloudHSM cluster of your AWS CloudHSM key store.
- ( ) External key store
  The key material for the KMS key is in an external key manager outside of AWS.

You can import key material from your key management infrastructure into AWS KMS and use it like any other AWS KMS key.

[ ] I understand the security and durability implications of using an imported key.

Regionality

Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions. Help me choose

- (●) Single-Region key
  Never allow this key to be replicated into other Regions
- ( ) Multi-Region key
  Allow this key to be replicated into other Regions

Cancel Next

Create key

Add labels

Alias

You can change the alias at any time. Learn more

Alias

parent_key

Define key administrative permissions

Key administrators (1/4)

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. Learn more

Search Key administrators

1

Name	Path	Type
AWSServiceRoleForSupport	/aws-service-role/support.am…	Role
AWSServiceRoleForTrustedAd…	/aws-service-role/trustedadvis…	Role
role-with-kms	/	Role
Pooja	/	User

Key deletion

Allow key administrators to delete this key.

Cancel Previous Next

Define key usage permissions

Key users (1/4)

Select the IAM users and roles that can use the KMS key in cryptographic operations. Learn more

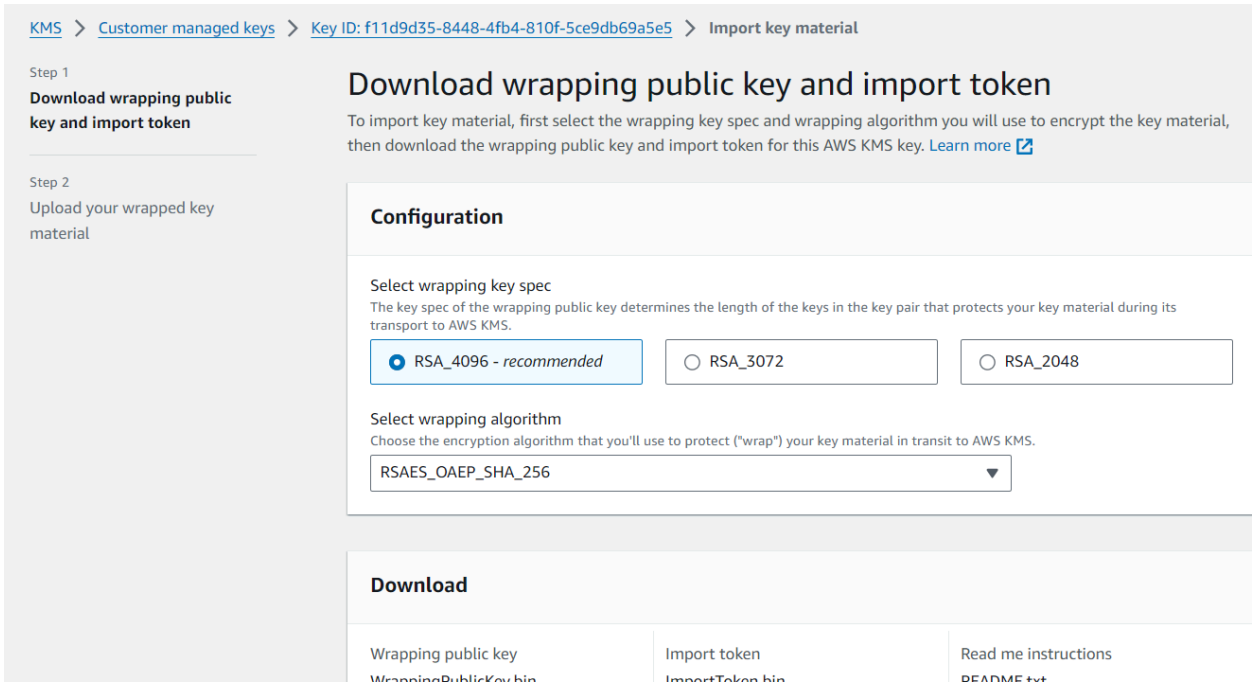
Search Key users

1

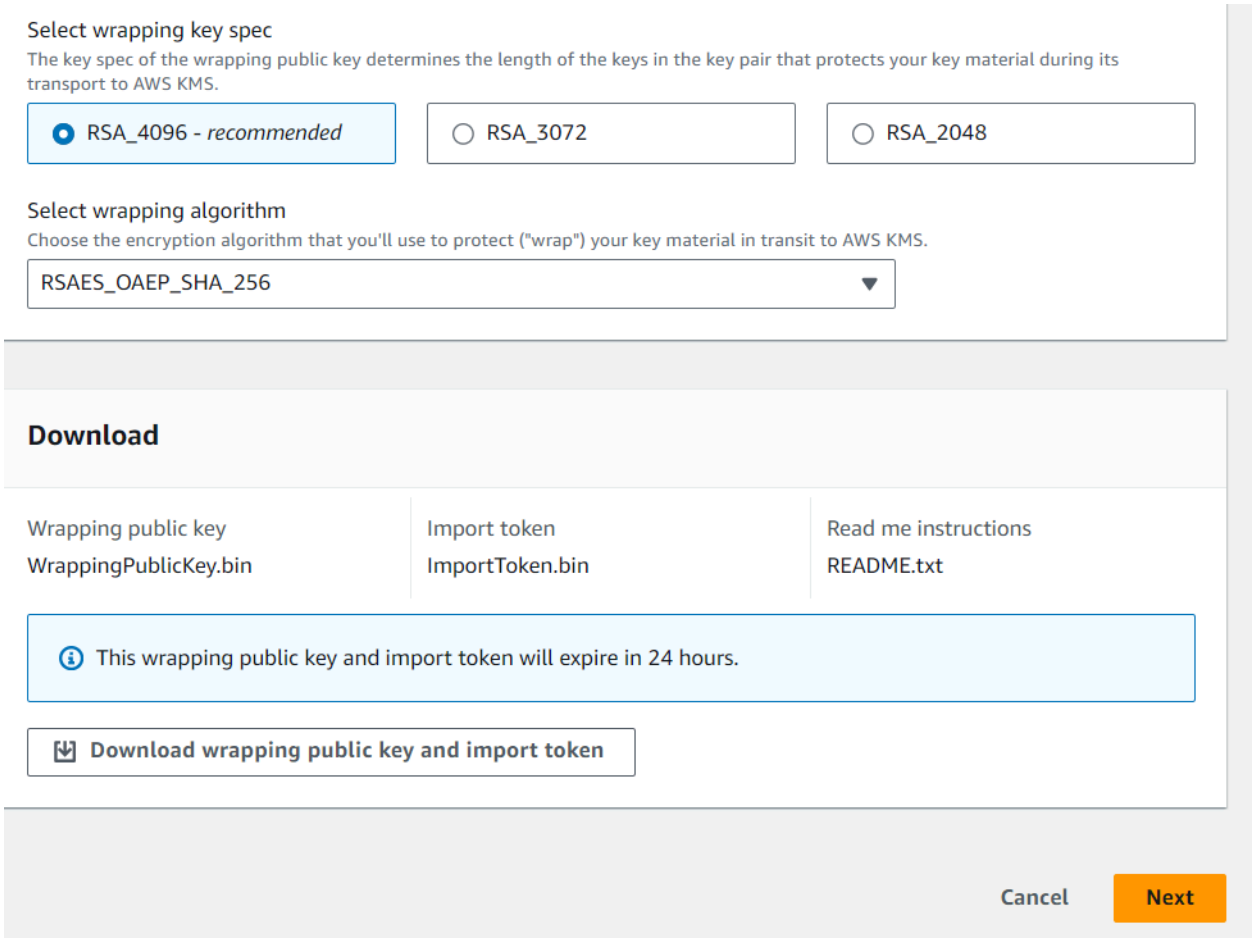
Name	Path	Type
Pooja	/	User
AWSServiceRoleForSupport	/aws-service-role/support.am…	Role
AWSServiceRoleForTrustedAd…	/aws-service-role/trustedadvis…	Role
role-with-kms	/	Role

Other AWS accounts

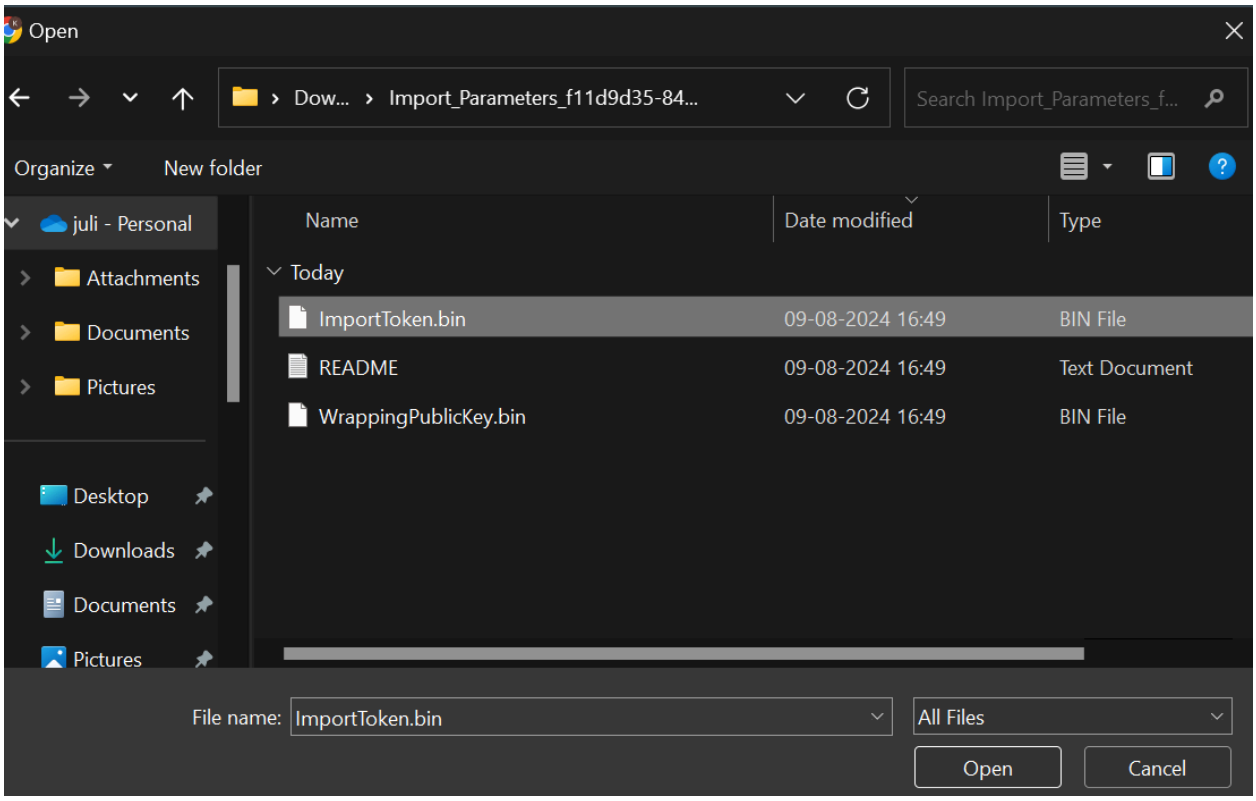
Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. Learn more



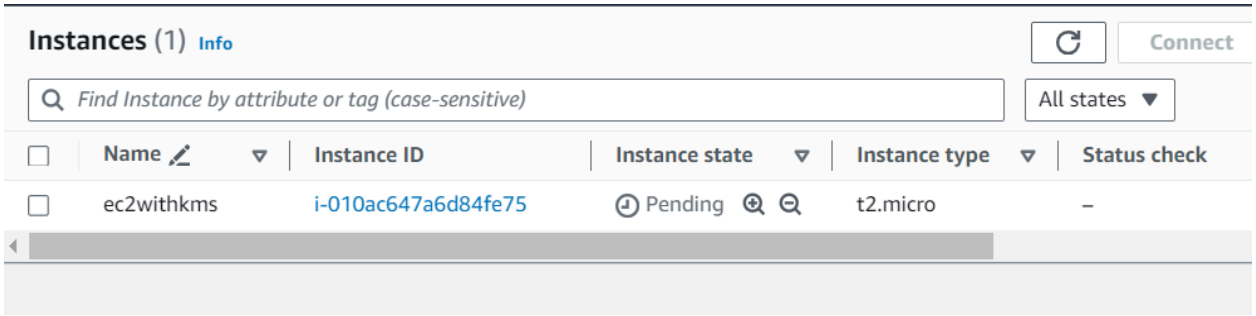
Download key



Import token

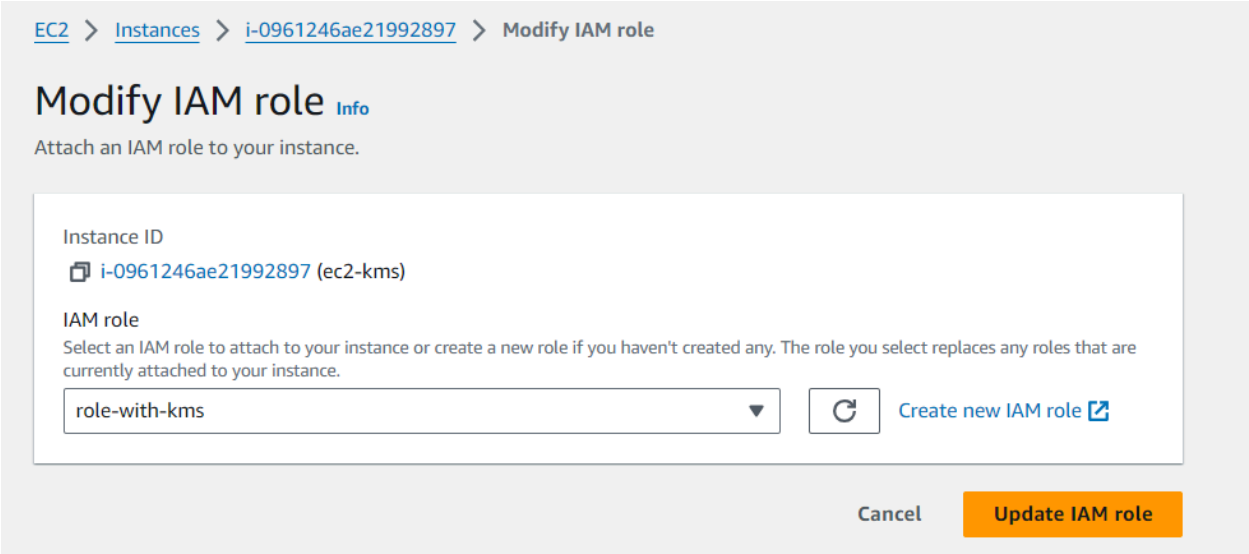


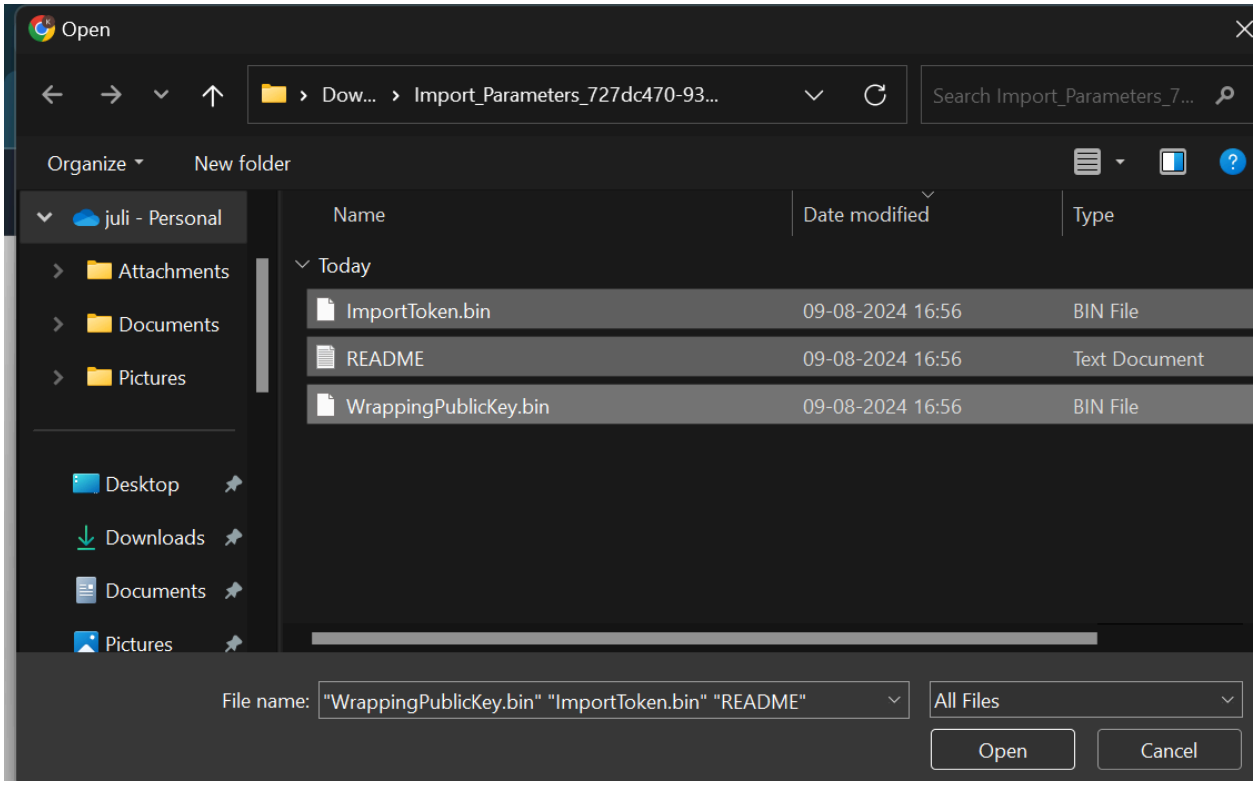
Launch an EC2



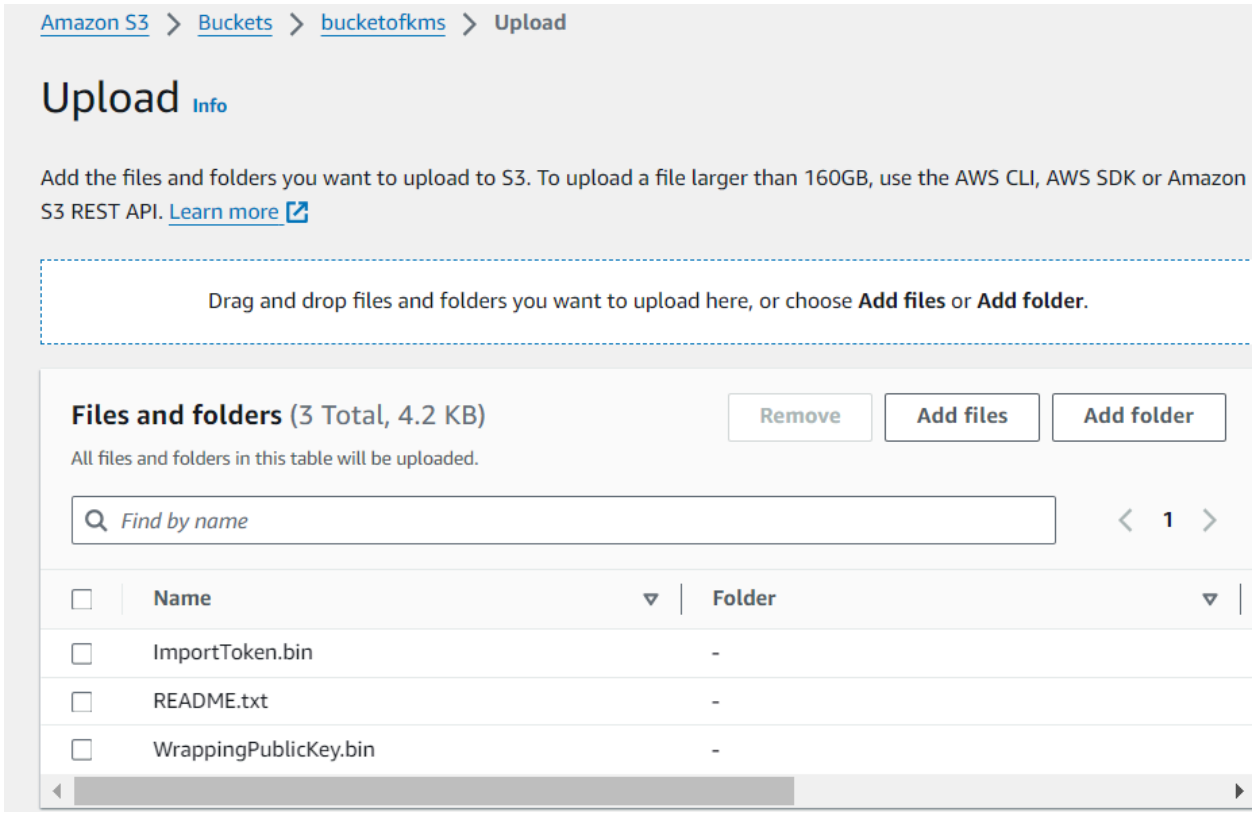
Create S3 bucket

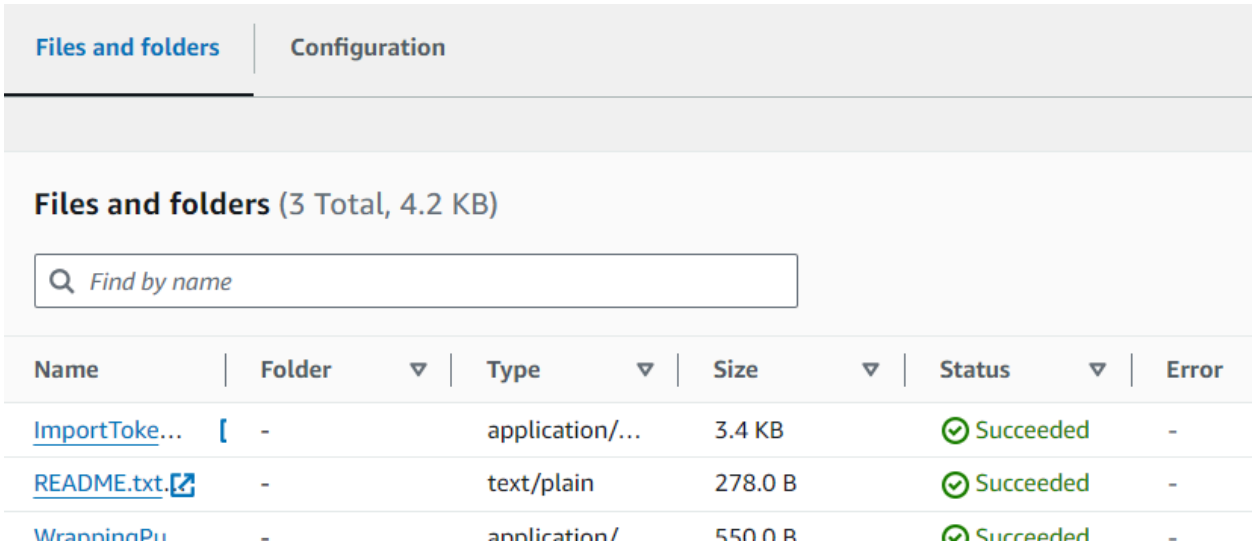
Connect EC2 instance

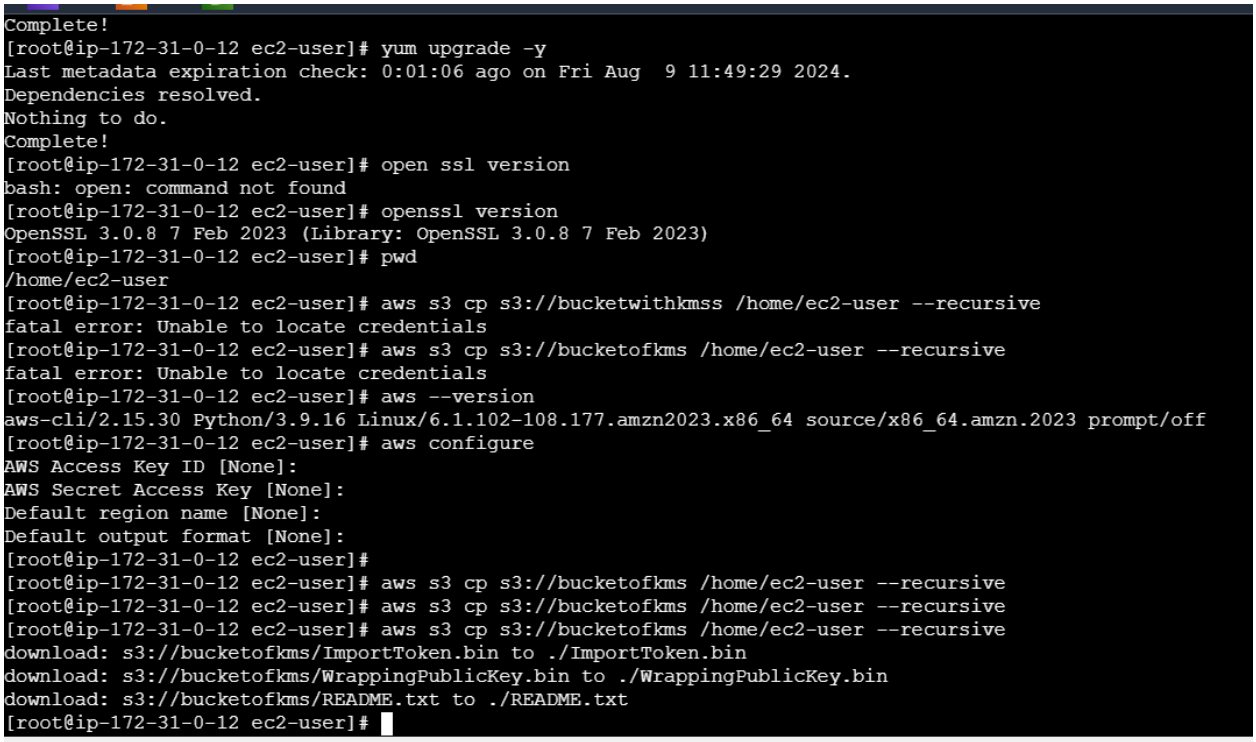




Upload in s3


Amazon S3 > Buckets > bucketofkms > 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 SDK 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 (3 Total, 4.2 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
Name
Folder
ImportToken.bin
-
README.txt
-
WrappingPublicKey.bin
-


Files and folders
Configuration
Files and folders (3 Total, 4.2 KB)
Find by name
Name
Folder
Type
Size
Status
Error
ImportToke...
-
application/...
3.4 KB
Succeeded
-
README.txt
-
text/plain
278.0 B
Succeeded
-



openssl version

aws s3 cp s3://tlbucket01 /home/ec2-user --recursive

openssl rand -out plaintextkeymaterial.bin 32

openssl pkeyutl -in plaintextkeymaterial.bin -out EncryptedKeyMaterial.bin -inkey <wrapping key> -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256

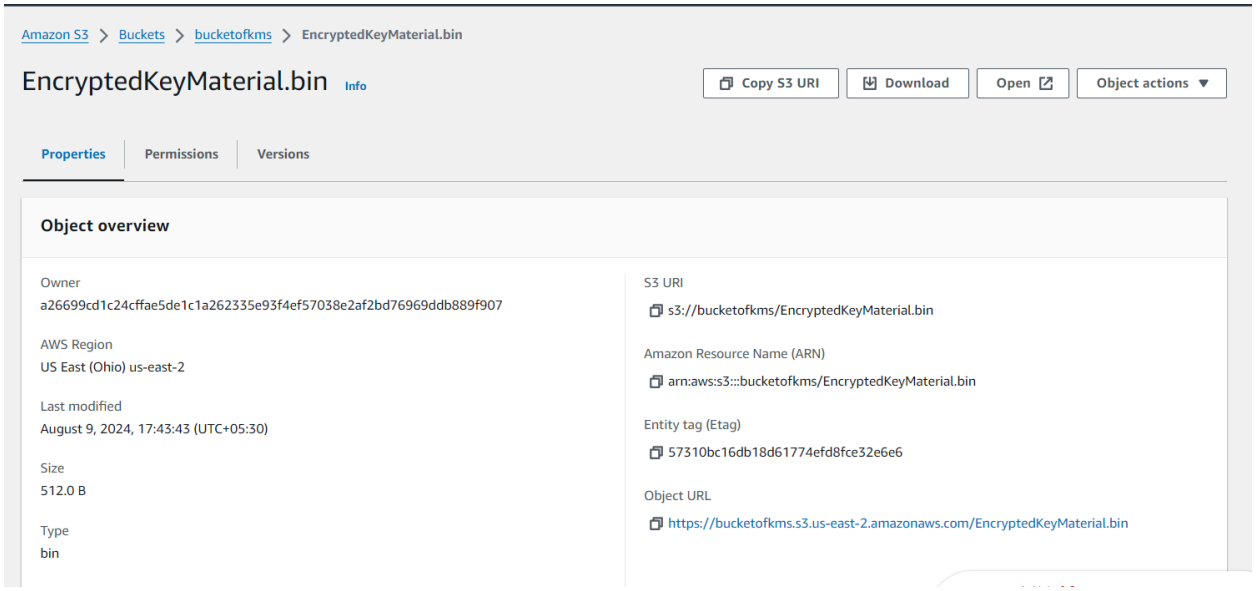
aws s3 cp /home/ec2-user s3://tlbucket01 --recursive

```
[root@ip-172-31-0-12 ec2-user]#
[root@ip-172-31-0-12 ec2-user]# aws s3 cp s3://bucketofkms /home/ec2-user --recursive
[root@ip-172-31-0-12 ec2-user]# aws s3 cp s3://bucketofkms /home/ec2-user --recursive
[root@ip-172-31-0-12 ec2-user]# aws s3 cp s3://bucketofkms /home/ec2-user --recursive
download: s3://bucketofkms/ImportToken.bin to ./ImportToken.bin
download: s3://bucketofkms/WrappingPublicKey.bin to ./WrappingPublicKey.bin
download: s3://bucketofkms/README.txt to ./README.txt
[root@ip-172-31-0-12 ec2-user]#
openssl rand -out plaintextkeymaterial.bin 32
[root@ip-172-31-0-12 ec2-user]# openssl rand -out plaintextkeymaterial.bin 32
[root@ip-172-31-0-12 ec2-user]# openssl pkeyutl -in plaintextkeymaterial.bin -out EncryptedKeyMaterial.bin -inkey WrappingPublicKey.bin -keyform der -pubin -encrypt -pkeyopt rsa_paddi
ode:oaep -pkeyopt rsa_oaep_md:sha256
[root@ip-172-31-0-12 ec2-user]#
[root@ip-172-31-0-12 ec2-user]# openssl pkeyutl -in plaintextkeymaterial.bin -out EncryptedKeyMaterial.bin -inkey WrappingPublicKey.bin -keyform der -pubin -encrypt -pkeyopt rsa_paddi
ode:oaep -pkeyopt rsa_oaep_md:sha256
[root@ip-172-31-0-12 ec2-user]# aws s3 cp /home/ec2-user s3://bucketofkms --recursive
upload: ./.bash_logout to s3://bucketofkms/.bash_logout
upload: ./ImportToken.bin to s3://bucketofkms/ImportToken.bin
upload: ./WrappingPublicKey.bin to s3://bucketofkms/WrappingPublicKey.bin
upload: ./EncryptedKeyMaterial.bin to s3://bucketofkms/EncryptedKeyMaterial.bin
upload: ./plaintextkeymaterial.bin to s3://bucketofkms/plaintextkeymaterial.bin
upload: ./README.txt to s3://bucketofkms/README.txt
upload: ./.bash_profile to s3://bucketofkms/.bash_profile
upload: .ssh/authorized_keys to s3://bucketofkms/.ssh/authorized_keys
upload: ./.bashrc to s3://bucketofkms/.bashrc
[root@ip-172-31-0-12 ec2-user]#
```

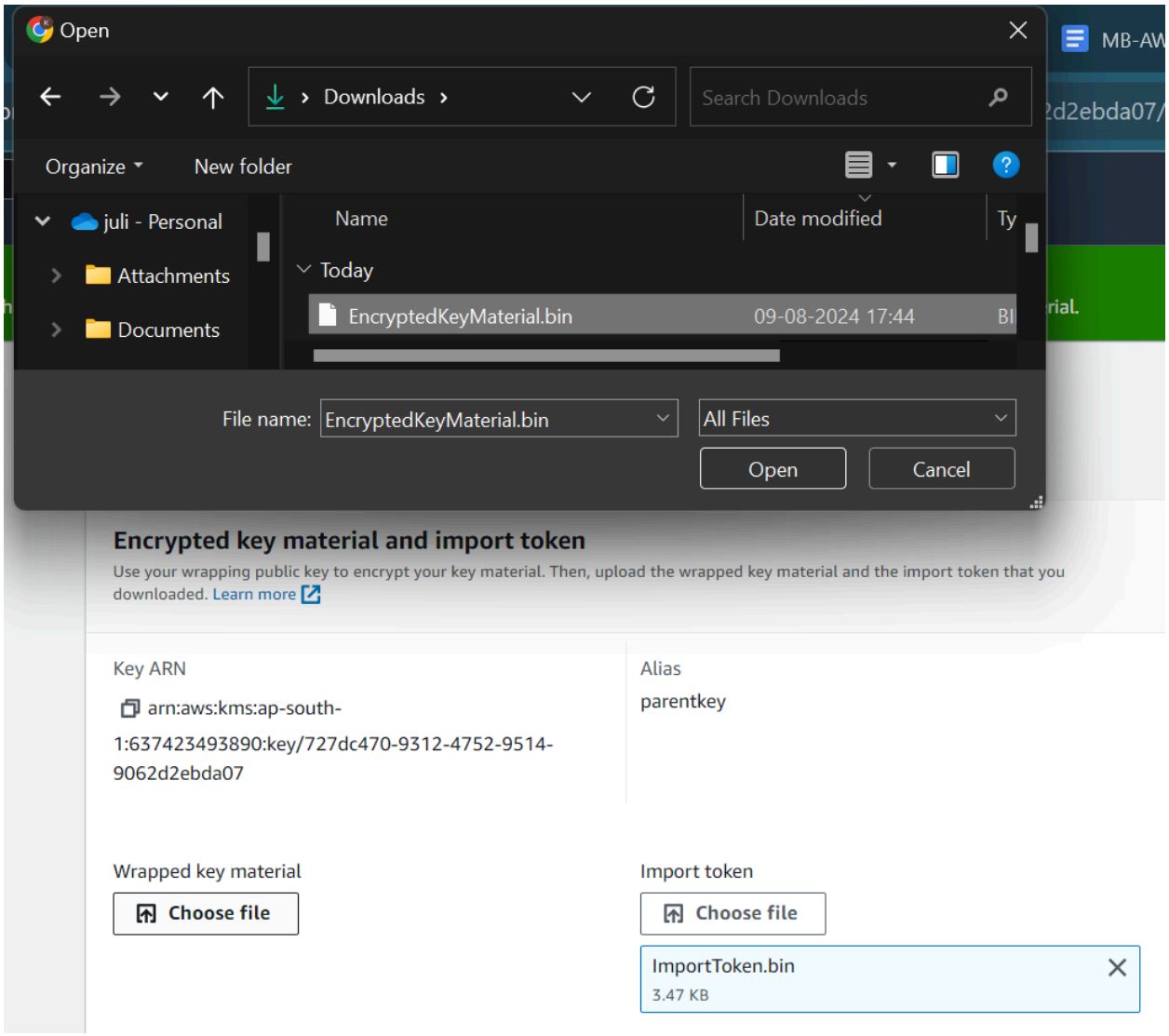
>aws s3 cp /home/ec2-user/EncryptedKeyMaterial.bin s3://bucketofkms

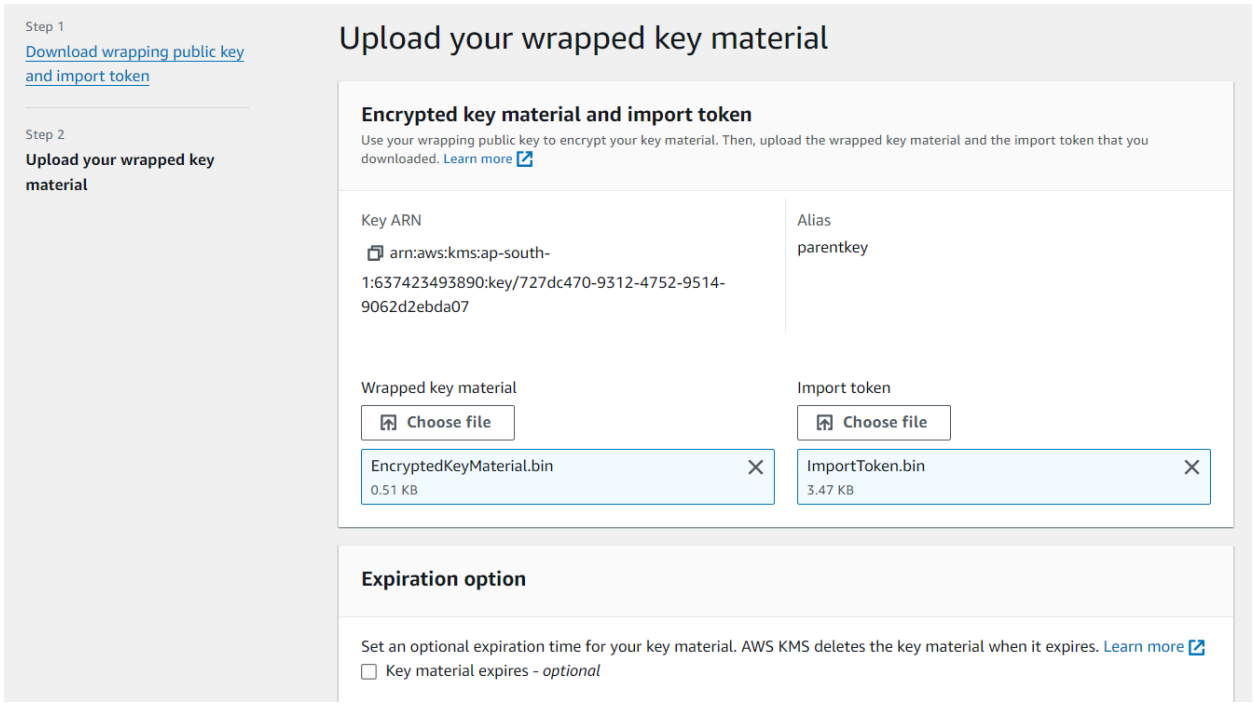
```
[root@ip-172-31-0-12 ec2-user]# aws s3 cp /home/ec2-user/EncryptedKeyMaterial.bin s3://bucketofkms
upload: ./EncryptedKeyMaterial.bin to s3://bucketofkms/EncryptedKeyMaterial.bin
[root@ip-172-31-0-12 ec2-user]#
```

Download encrypted file

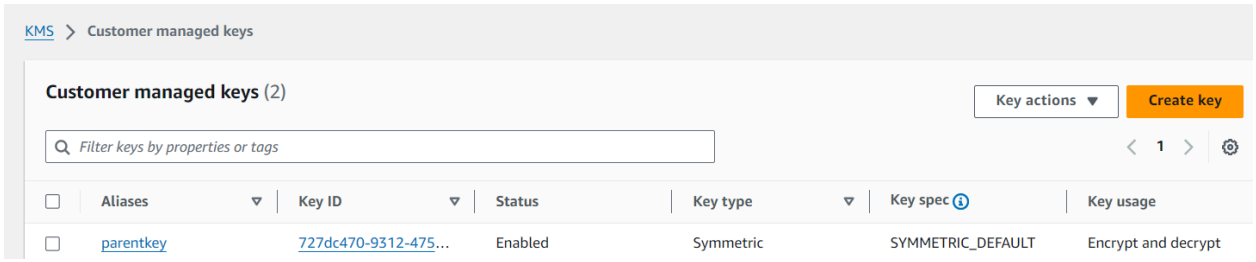


Upload


Open
Downloads
Search Downloads
Organize
New folder
juli - Personal
Attachments
Documents
Name
Date modified
Today
EncryptedKeyMaterial.bin
09-08-2024 17:44
File name:
EncryptedKeyMaterial.bin
All Files
Open
Cancel
Encrypted key material and import token
Use your wrapping public key to encrypt your key material. Then, upload the wrapped key material and the import token that you downloaded. Learn more
Key ARN
arn:aws:kms:ap-south-1:637423493890:key/727dc470-9312-4752-9514-9062d2ebda07
Alias
parentkey
Wrapped key material
Choose file
Import token
Choose file
ImportToken.bin
3.47 KB



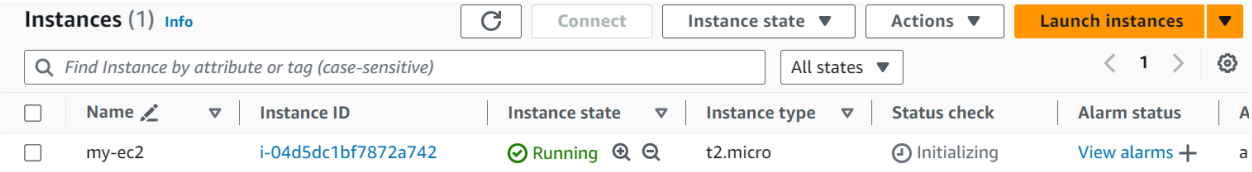
Key is enabled now



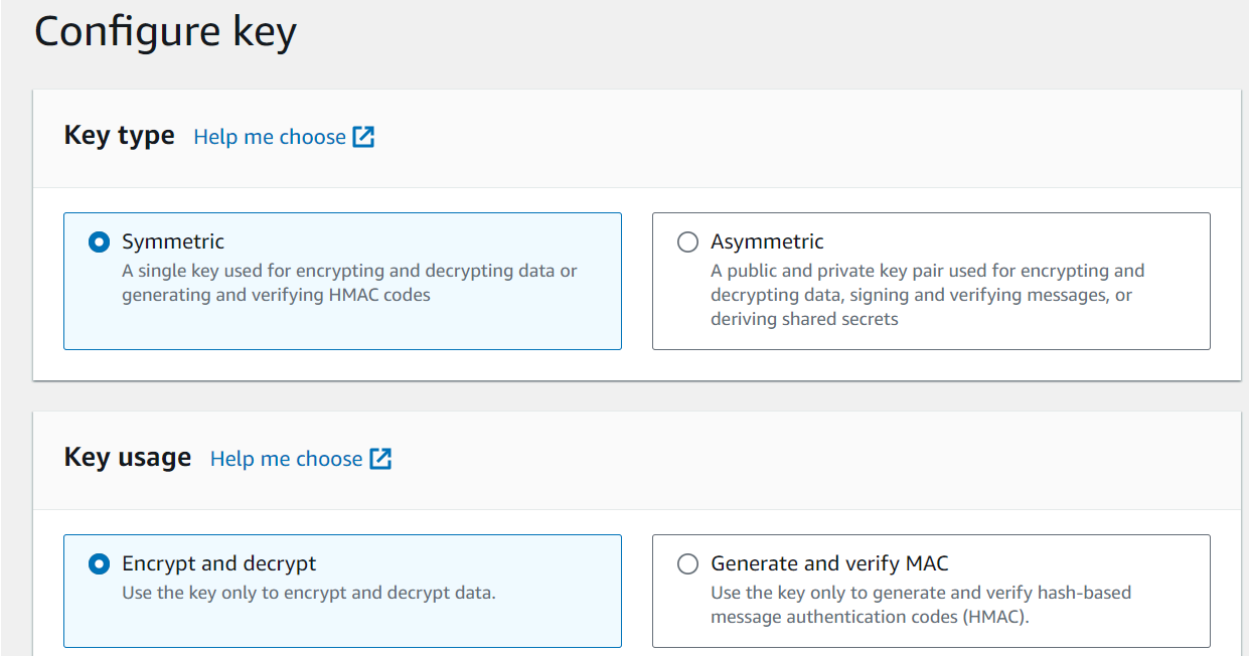
Date : 12-8-2024

AIM : KEY MANAGEMENT SERVICE WITH EC2

Step 1 : launch an EC2 machine



Step 2 : create KMS



Advanced options

Key material origin

Key material origin is a KMS key property that represents the source of the key material when creating the KMS key. Help me choose

- ○ KMS - *recommended*
  AWS KMS creates and manages the key material for the KMS key.
- ◉ External (Import Key material)
  You create and import the key material for the KMS key.
- ○ AWS CloudHSM key store
  AWS KMS creates the key material in the AWS CloudHSM cluster of your AWS CloudHSM key store.
- ○ External key store
  The key material for the KMS key is in an external key manager outside of AWS.

You can import key material from your key management infrastructure into AWS KMS and use it like any other AWS KMS key.

☐ I understand the security and durability implications of using an imported key.

Regionality

Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions. Help me choose

◉ Single-Region key
Never allow this key to be replicated into other Regions

KMS > Customer managed keys

Customer managed keys (1)

Key actions ▼ | Create key

Filter keys by properties or tags

1

☐	Aliases	Key ID	Status	Key type	Key spec	Key usage
☐	kms-key	33936a2e-7…	Pending imp…	Symmetric	SYMMETRIC_…	Encrypt and …

Download

Wrapping public key	Import token	Read me instructions
WrappingPublicKey.bin	ImportToken.bin	README.txt

ⓘ This wrapping public key and import token will expire in 24 hours.

Download wrapping public key and import token

Cancel | Next

Encrypted key material and import token

Use your wrapping public key to encrypt your key material. Then, upload the wrapped key material and the import token that you downloaded. Learn more

Key ARN

arn:aws:kms:ap-southeast-1:637423493890:key/33936a2e-790c-4c3b-9098-efc66d70d9fa

Alias

kms-key

Wrapped key material

Choose file

Import token

Choose file

ImportToken.bin
3.47 KB

Create s3 bucket

kms-bucket-ec2 Info

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

Objects (0) Info

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

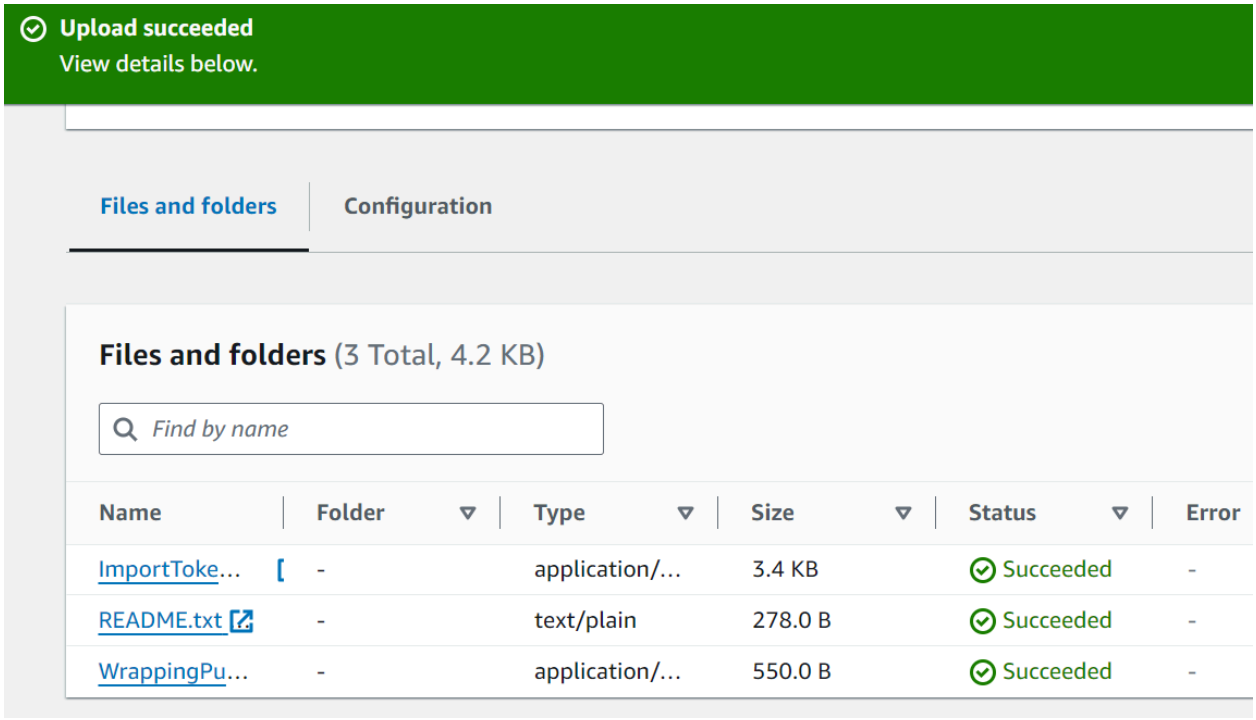
Find objects by prefix | Show versions | 1

Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Upload files



openssl version

aws s3 cp s3://tlbucket01 /home/ec2-user --recursive

openssl rand -out plaintextkeymaterial.bin 32

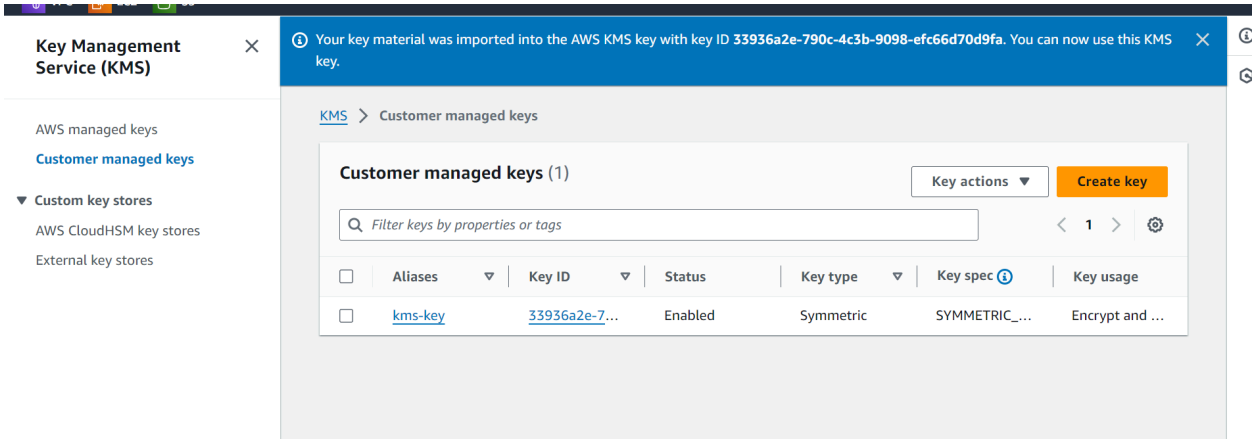
openssl pkeyutl -in plaintextkeymaterial.bin -out EncryptedKeyMaterial.bin -inkey <wrapping key> -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256

aws s3 cp /home/ec2-user s3://tlbucket01 --recursive

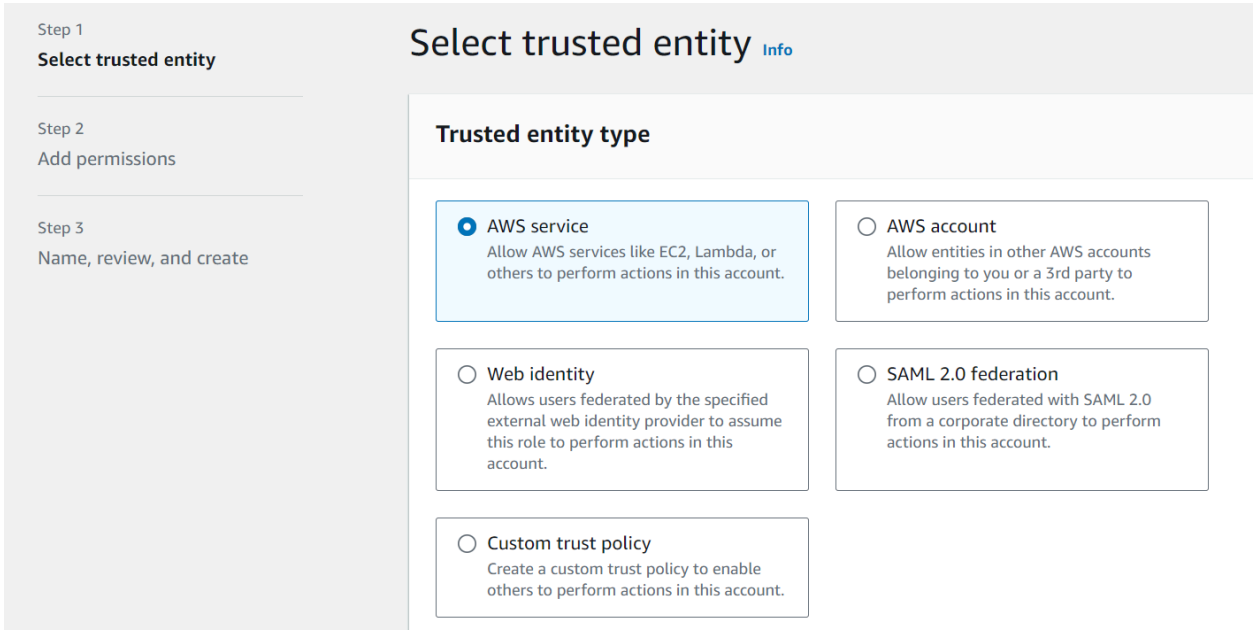
```
OpenSSL 3.0.8 7 Feb 2023 (Library: OpenSSL 3.0.8 7 Feb 2023)
[root@ip-172-31-44-52 ec2-user]# aws s3 cp s3://kms-bucket-ec2 /home/ec2-user --recursive
download: s3://kms-bucket-ec2/ImportToken.bin to ./ImportToken.bin
download: s3://kms-bucket-ec2/WrappingPublicKey.bin to ./WrappingPublicKey.bin
[root@ip-172-31-44-52 ec2-user]# openssl rand -out plaintextkeymaterial.bin 32
[root@ip-172-31-44-52 ec2-user]# openssl pkeyutl -in plaintextkeymaterial.bin -out EncryptedKeyMaterial.bin -inkey <wrapping key> -keyfo
rm der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256
bash: wrapping: No such file or directory
[root@ip-172-31-44-52 ec2-user]# openssl pkeyutl -in plaintextkeymaterial.bin -out EncryptedKeyMaterial.bin -inkey WrappingPublicKey.bin
 -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256
[root@ip-172-31-44-52 ec2-user]# aws s3 cp /home/ec2-user s3://kms-bucket-ec2 --recursive
upload: ./ImportToken.bin to s3://kms-bucket-ec2/ImportToken.bin
upload: ./file.txt to s3://kms-bucket-ec2/file.txt
upload: ./.bash_logout to s3://kms-bucket-ec2/.bash_logout
upload: ./plaintextkeymaterial.bin to s3://kms-bucket-ec2/plaintextkeymaterial.bin
upload: ./WrappingPublicKey.bin to s3://kms-bucket-ec2/WrappingPublicKey.bin
upload: .ssh/authorized_keys to s3://kms-bucket-ec2/.ssh/authorized_keys
upload: ./.bashrc to s3://kms-bucket-ec2/.bashrc
upload: ./EncryptedKeyMaterial.bin to s3://kms-bucket-ec2/EncryptedKeyMaterial.bin
upload: ./.bash_profile to s3://kms-bucket-ec2/.bash_profile
[root@ip-172-31-44-52 ec2-user]#
```

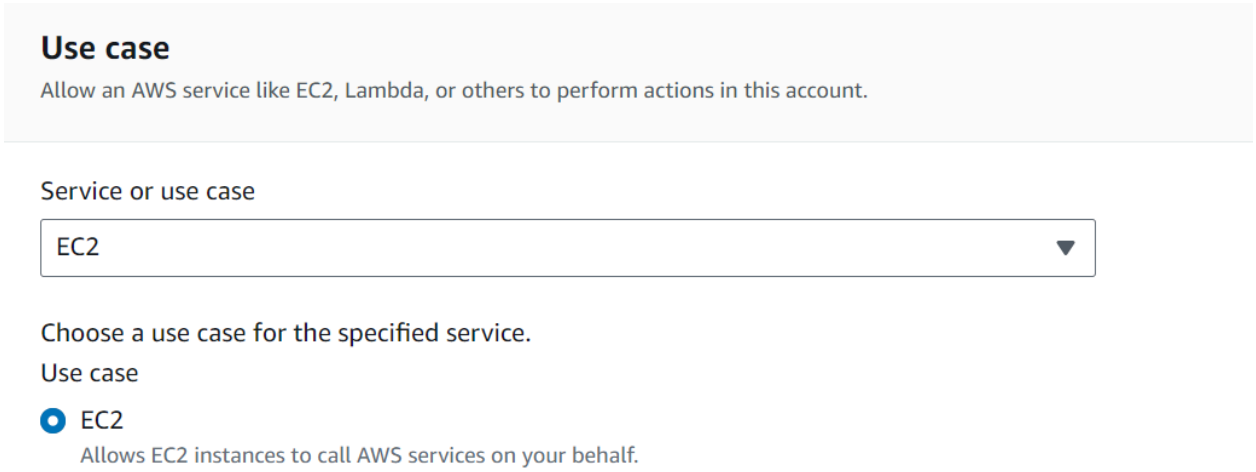
i-04d5dc1bf7872a742 (my-ec2)

PublicIPs: 47.129.204.84 PrivateIPs: 172.31.44.52

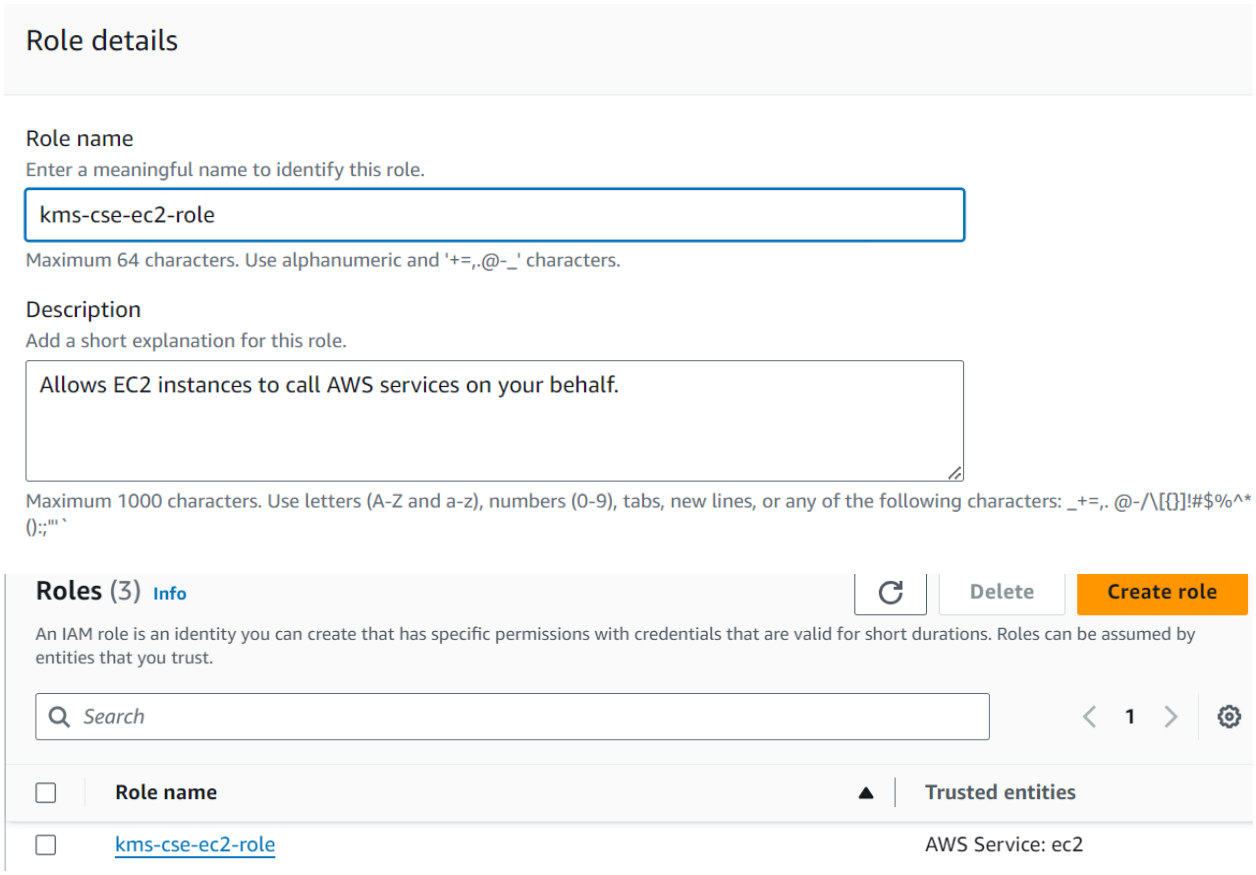


Step 3 : create role

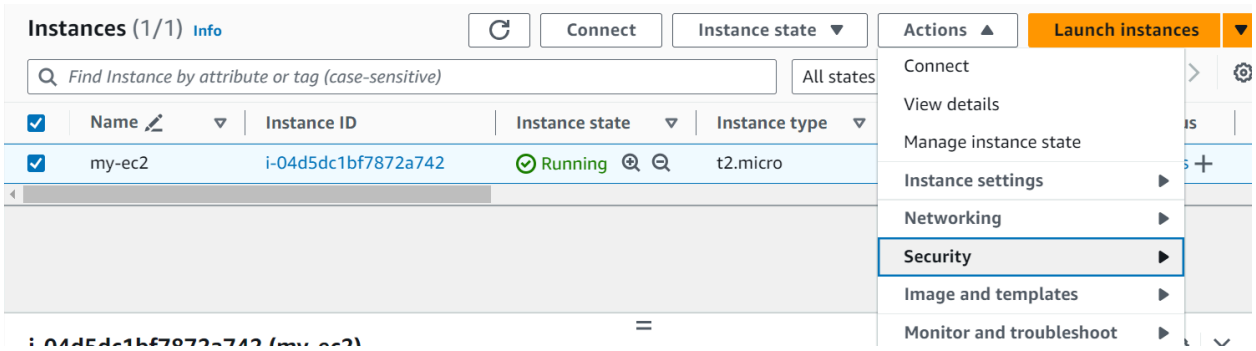


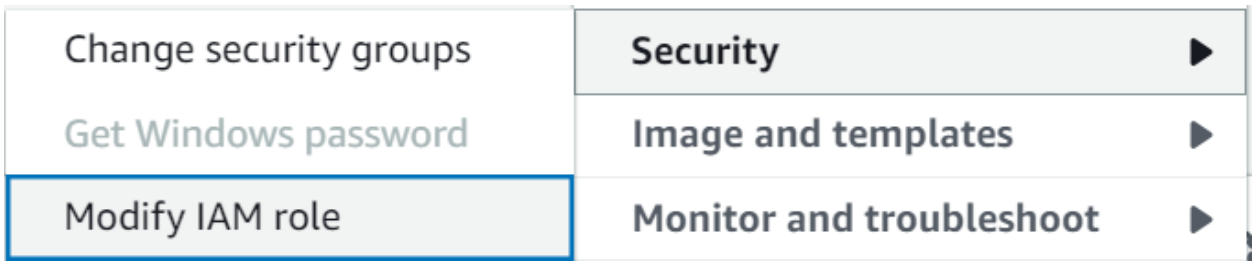


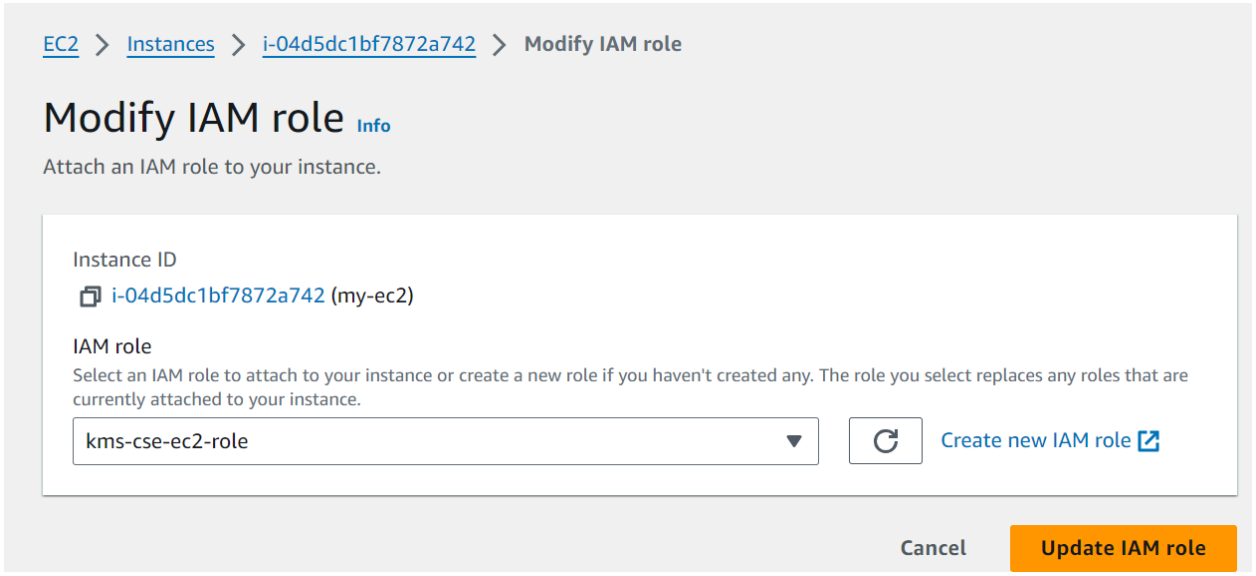
No policy attached



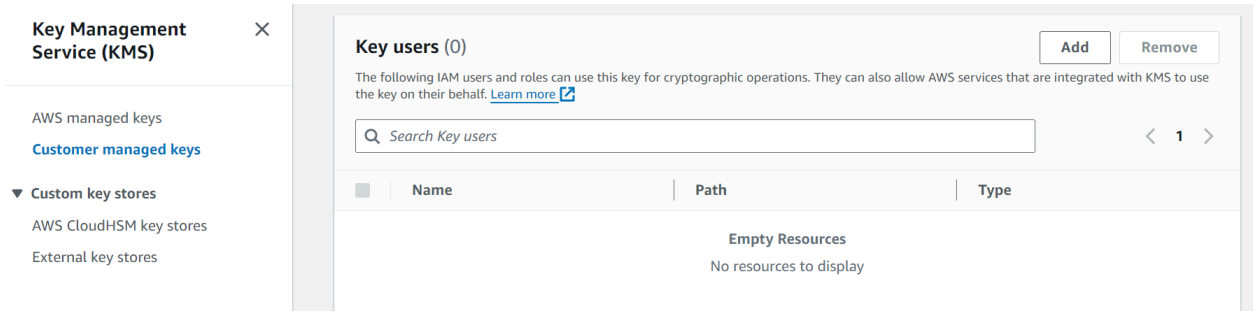
Go to > ec2 > modify security







KMS > key users > add IAM role



Add key users

The following IAM users and roles can use this key to encrypt and decrypt data from within applications and when using AWS services integrated with KMS.

Key users (5)

kms

1 matches

1

Name	Path	Type
kms-cse-ec2-role	/	Role

Cancel Add

Connect EC2 machine

1. **Create a file with data which you want to ecrypt**

echo "Hello,Pooja! Encrypt Me." > file.txt

```
[ec2-user@ip-172-31-44-52 ~]$ sudo su
[root@ip-172-31-44-52 ec2-user]# yum update -y
Last metadata expiration check: 0:14:19 ago on Mon Aug 12 10:59:03 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-172-31-44-52 ec2-user]# yum upgrade -y
Last metadata expiration check: 0:14:27 ago on Mon Aug 12 10:59:03 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-172-31-44-52 ec2-user]# echo "Hello,Pooja! Encrypt Me." > file.txt
[root@ip-172-31-44-52 ec2-user]#
```

i-04d5dc1bf7872a742 (my-ec2)

PublicIPs: 47.129.204.84 PrivateIPs: 172.31.44.52

Generate data key using CMK
> aws kms generate-data-key --key-id alias/kms-key --key-spec AES_256 --region ap-southeast-1

```
[root@ip-172-31-44-52 ec2-user]# echo "Hello, Pooja! Please encrypt me ." > file.txt
[root@ip-172-31-44-52 ec2-user]# aws kms generate-data-key --key-id alias/kms-key --key-spec AES_256 --region ap-southeast-1
{
    "CiphertextBlob": "AQIDAHgh/QSZkrrkP+tAydUWGaUNhoxg44VQxAiTEW7NYikXUwEpRTK5vCJ8QTdHe4nA2fGzAAAAfjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGCSqGS
Ib3DQEHATAeBglghkgBZQMEAS4wEQQMCQ8O6+ZSy0sd9ftqAgEQgDvl0qIINxOUw74TX9rOubKKrImbilNKOQ074rUEN8E6n7S2B5EIC+0PZivDtYpKZOOsJ+KJMK5h7smlEQ==",
    "Plaintext": "v/SjBZL9hWrfAscs3oQBuDo6S5F8G/JsFOzlkpqGzFk=",
    "KeyId": "arn:aws:kms:ap-southeast-1:637423493890:key/33936a2e-790c-4c3b-9098-efc66d70d9fa"
}
[root@ip-172-31-44-52 ec2-user]#
```

Create a data key file which contain decoded Plaintext
> echo v/SjBZL9hWrfAscs3oQBuDo6S5F8G/JsFOzlkpqGzFk= | base64 --decode > datakey

```
[root@ip-172-31-44-52 ec2-user]# echo v/SjBZL9hWrfAscs3oQBuDo6S5F8G/JsFOzlkpqGzFk= | base64 --decode > datakey
[root@ip-172-31-44-52 ec2-user]#
```

7. Create a encrypted data key file which contains decoded

> echo 7. Create a encrypted data key file which contains decoded

echo <ciphertext-bob> | base64 --decode > encrypteddatakey

| base64 --decode > encrypteddatakey

```
[root@ip-172-31-44-52 ec2-user]# echo AQIDAHgh/QSZkrrkP+tAydUWGaUNhoxg44VQxAiTEW7NYikXUwEpRTK5vCJ8QTdHe4nA2fGzAAAAfjB8BgkqhkiG9w0BBwagbz
BtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMCQ8O6+ZSy0sd9ftqAgEQgDvl0qIINxOUw74TX9rOubKKrImbilNKOQ074rUEN8E6n7S2B5EIC+0PZivDtYpKZOOsJ+
KJMK5h7smlEQ== | base64 --decode > encrypteddatakey
[root@ip-172-31-44-52 ec2-user]#
```

.Encrypt file using data key

openssl enc -in ./file.txt -out ./encrypted-file.txt -e -aes256 -k fileb://./datakey

```
[root@ip-172-31-44-52 ec2-user]# ll
total 32
-rw-r--r--. 1 root root  512 Aug 12 12:07 EncryptedKeyMaterial.bin
-rw-r--r--. 1 root root 3466 Aug 12 11:58 ImportToken.bin
-rw-r--r--. 1 root root  550 Aug 12 11:58 WrappingPublicKey.bin
-rw-r--r--. 1 root root   32 Aug 12 12:18 datakey
-rw-r--r--. 1 root root   64 Aug 12 12:22 encrypted-file.txt
-rw-r--r--. 1 root root  184 Aug 12 12:21 encrypteddatakey
-rw-r--r--. 1 root root   34 Aug 12 12:15 file.txt
-rw-r--r--. 1 root root   32 Aug 12 12:06 plaintextkeymaterial.bin
[root@ip-172-31-44-52 ec2-user]# cat file.,,txt
cat: file.,,txt: No such file or directory
[root@ip-172-31-44-52 ec2-user]# cat file.txt
Hello, Pooja! Please encrypt me .
[root@ip-172-31-44-52 ec2-user]#
```

Remove datakey and datafile

rm datakey

rm file.txt

```
[root@ip-172-31-44-52 ec2-user]# rm datakey
rm: remove regular file 'datakey'? y
[root@ip-172-31-44-52 ec2-user]# rm file.txt
rm: remove regular file 'file.txt'? y
[root@ip-172-31-44-52 ec2-user]#
```

.Decrypt "encrypted data key"

aws kms decrypt --ciphertext-blob fileb://./encrypteddatakey --region ap-south-1

```
[root@ip-172-31-44-52 ec2-user]# aws kms decrypt --ciphertext-blob fileb://./encrypteddatakey --region ap-southeast-1
{
    "KeyId": "arn:aws:kms:ap-southeast-1:637423493890:key/33936a2e-790c-4c3b-9098-efc66d70d9fa",
    "Plaintext": "v/SjBZL9hWrfAscs3oQBuDo6S5F8G/JsFOzlkpqGzFk=",
    "EncryptionAlgorithm": "SYMMETRIC_DEFAULT"
}
```

Create a Data Key file which contains plaintext

echo <plaintext> | base64 --decode > datakey

Decrypt "encrypted data file" using the data key

openssl enc -in ./encrypted-file.txt -out ./file.txt -d -aes256 -k fileb://./datakey

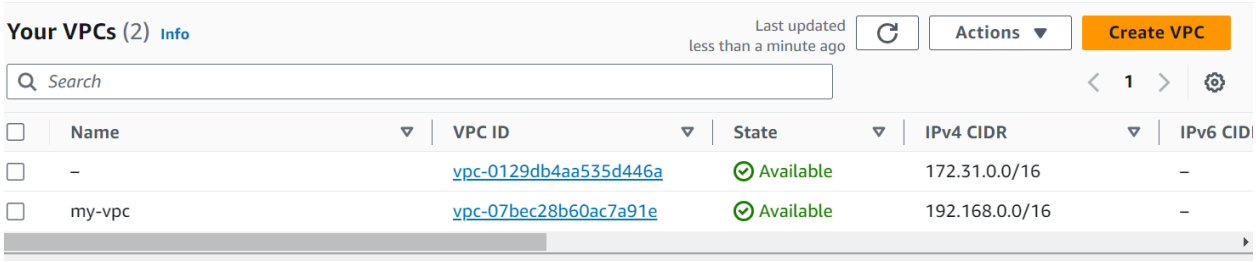
```
[root@ip-172-31-44-52 ec2-user]# echo v/SjBZL9hWrfAscs3oQBuDo6S5F8G/JsFOzlkpqGzFk= | base64 --decode > datakey
[root@ip-172-31-44-52 ec2-user]# openssl enc -in ./encrypted-file.txt -out ./file.txt -d -aes256 -k fileb://./datakey
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[root@ip-172-31-44-52 ec2-user]# ll
total 32
-rw-r--r--. 1 root root  512 Aug 12 12:07 EncryptedKeyMaterial.bin
-rw-r--r--. 1 root root 3466 Aug 12 11:58 ImportToken.bin
-rw-r--r--. 1 root root  550 Aug 12 11:58 WrappingPublicKey.bin
-rw-r--r--. 1 root root   32 Aug 12 12:29 datakey
-rw-r--r--. 1 root root   64 Aug 12 12:22 encrypted-file.txt
-rw-r--r--. 1 root root  184 Aug 12 12:21 encrypteddatakey
-rw-r--r--. 1 root root   34 Aug 12 12:29 file.txt
-rw-r--r--. 1 root root   32 Aug 12 12:06 plaintextkeymaterial.bin
[root@ip-172-31-44-52 ec2-user]#
```

```
[root@ip-172-31-44-52 ec2-user]# cat file.txt
Hello, Pooja! Please encrypt me .
[root@ip-172-31-44-52 ec2-user]#
```

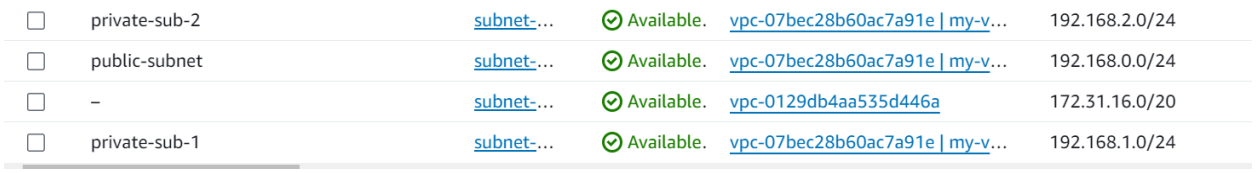
Date : 13/08/2024

AIM : Connecting RDS (relational database services) with EC2

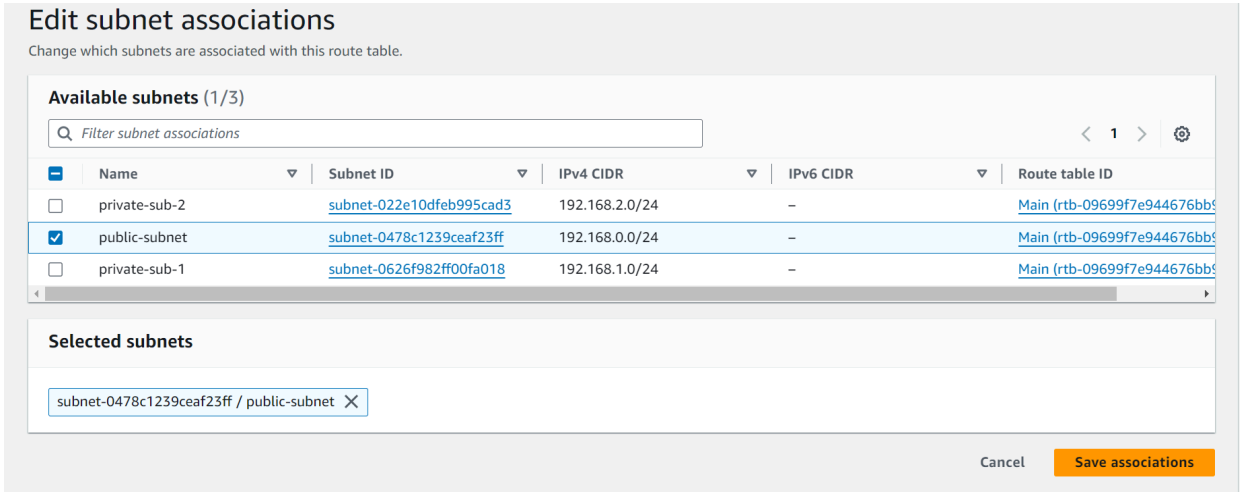
1. Create VPC



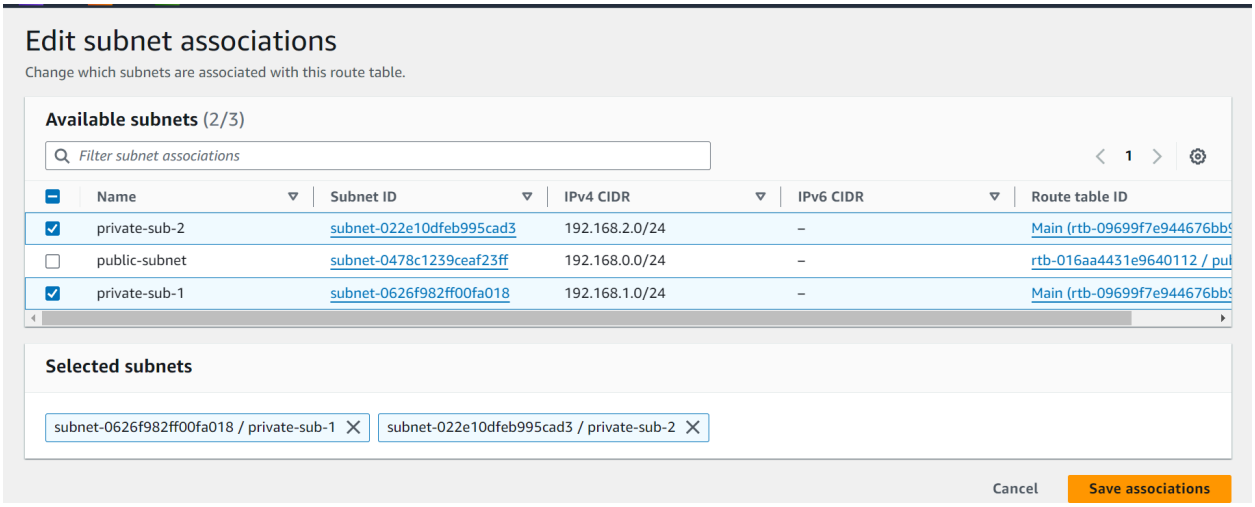
Give subnets



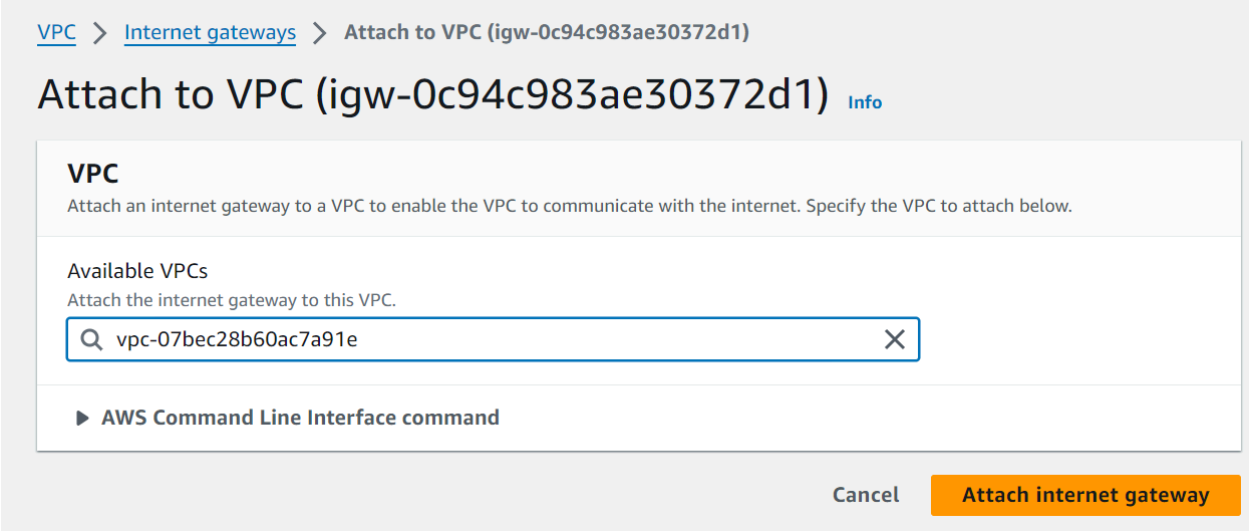
Give subnet associations public-rt to public-subnet



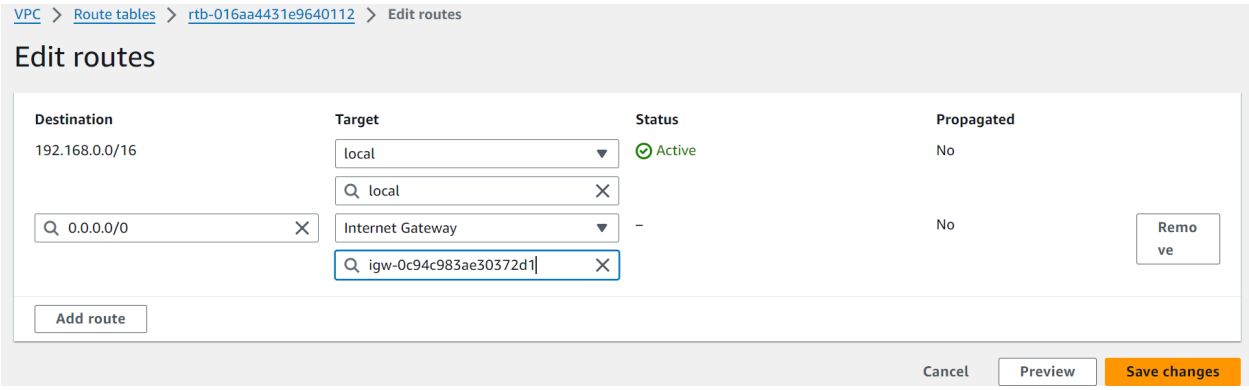
Give subnet associations private-rt to both private-subnet



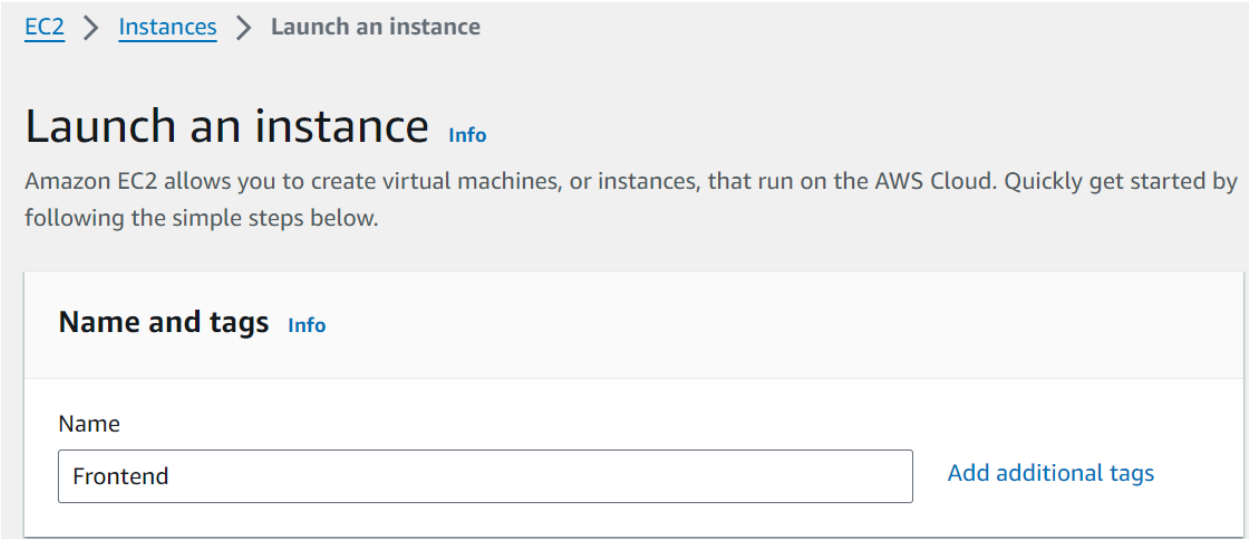
Attach internet gateway to your VPC

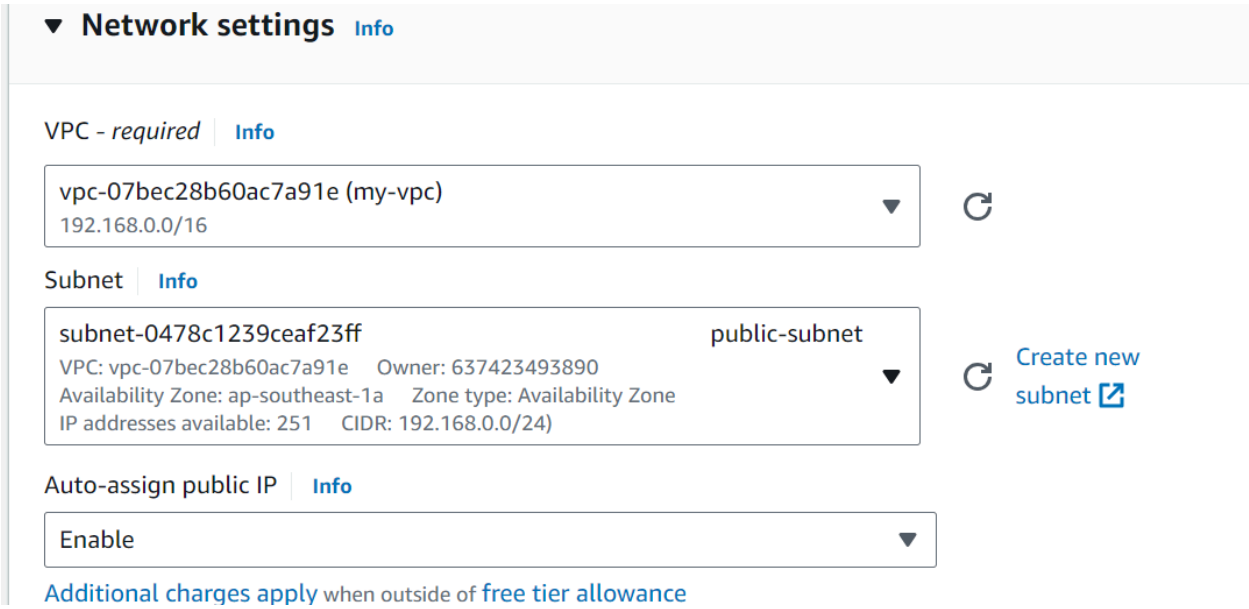


Edit routes in Public-rt

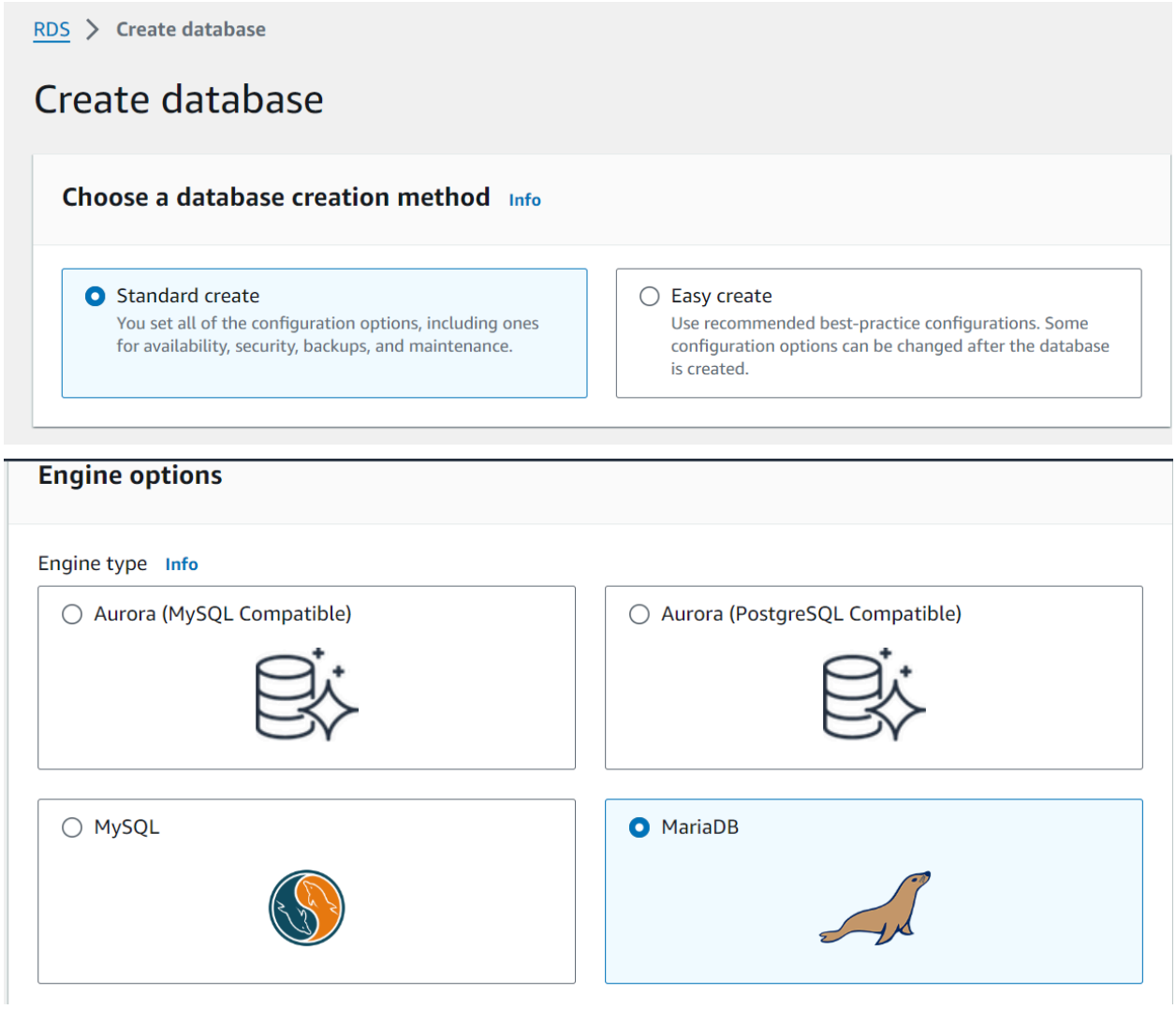


Create EC2 in Singapore Region





Go to > RDS > databases > create database



▼ Hide filters

Show versions that support the Amazon RDS Optimized Writes Info

Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Engine Version

MariaDB 10.11.8

Templates

Choose a sample template to meet your use case.

- ○ Production
  Use defaults for high availability and fast, consistent performance.
- ○ Dev/Test
  This instance is intended for development use outside of a production environment.
- ◉ Free tier
  Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. Info

Settings

DB instance identifier Info

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

Pooja-database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username Info

Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management

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

- ○ Managed in AWS Secrets Manager - *most secure*
  RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.
- ◉ Self managed
  Create your own password or have RDS create a password that you manage.

Password - Magicbus1234

Master password Info

••••••••••••

Password strength Strong

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

Confirm master password Info

••••••••••••

Burstable classes (includes t classes)

db.t3.micro
2 vCPUs 1 GiB RAM Network: 2,085 Mbps

Storage

Storage type Info

Provisioned IOPS SSD (io2) storage volumes are now available.

General Purpose SSD (gp2)
Baseline performance determined by volume size

Allocated storage Info

20 GiB

The minimum value is 20 GiB and the maximum value is 6,144 GiB

Connectivity Info

Compute resource

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

- (●) **Don't connect to an EC2 compute resource**
  Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.
- ( ) **Connect to an EC2 compute resource**
  Set up a connection to an EC2 compute resource for this database.

Network type Info

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

- (●) **IPv4**
  Your resources can communicate only over the IPv4 addressing protocol.
- ( ) **Dual-stack mode**
  Your resources can communicate over IPv4, IPv6, or both.

DB subnet group Info

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

Create new DB Subnet Group ▼

Public access Info

- ( ) **Yes**
  RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
- (●) **No**
  RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

In RDS > create subnet group

Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name

You won't be able to modify the name after your subnet group has been created.

rds-security-grp

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

to assign security grp to rds

VPC

Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

my-vpc (vpc-07bec28b60ac7a91e)

Add subnets

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone

ap-southeast-1b ✕ ap-southeast-1c ✕

Subnets

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets

subnet-0626f982ff00fa018 (192.168.1.0/24) ✕

subnet-022e10dfeb995cad3 (192.168.2.0/24) ✕

Subnets selected (2)

Availability zone	Subnet ID	CIDR block
ap-southeast-1b	subnet-0626f982ff00fa018	192.168.1.0/24
ap-southeast-1c	subnet-022e10dfeb995cad3	192.168.2.0/24

Cancel | Create

Successfully created rds-security-grp. View subnet group

RDS > Subnet groups

Subnet groups (1) | Edit | Delete | Create DB subnet group

Filter by subnet group | 1

Name	Description	Status	VPC
rds-security-grp	to assign security grp to rds	Complete	vpc-07bec28b60ac7a91e

In RDS >

Additional configuration

Database options, encryption turned off, backup turned off, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name Info

pooja-db

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group Info

default.mariadb10.11

Option group Info

default:mariadb-10-11

Assign security group

Virtual private cloud (VPC) Info

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

my-vpc (vpc-07bec28b60ac7a91e)
3 Subnets, 3 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group Info

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

rds-security-grp
2 Subnets, 2 Availability Zones

VPC security group (firewall) Info

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

- Choose existing
  Choose existing VPC security groups
- Create new
  Create new VPC security group

New VPC security group name

vpcsg

Availability Zone Info

ap-southeast-1b

In additional configuration disable

Backup

☐ Enable automated backups

Creates a point-in-time snapshot of your database

Encryption

☐ Enable encryption

Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. **Info**

Log exports

Select the log types to publish to Amazon CloudWatch Logs

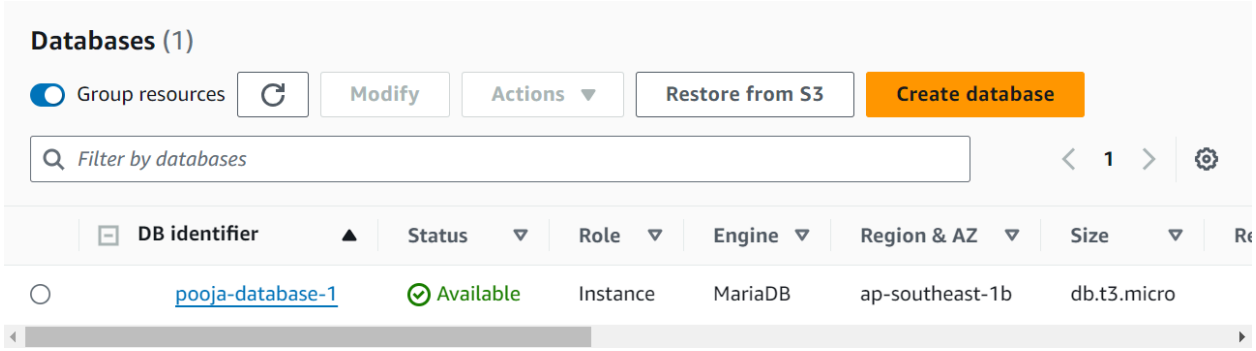
☐ Audit log
☐ Error log
☐ General log
☐ Slow query log

IAM role

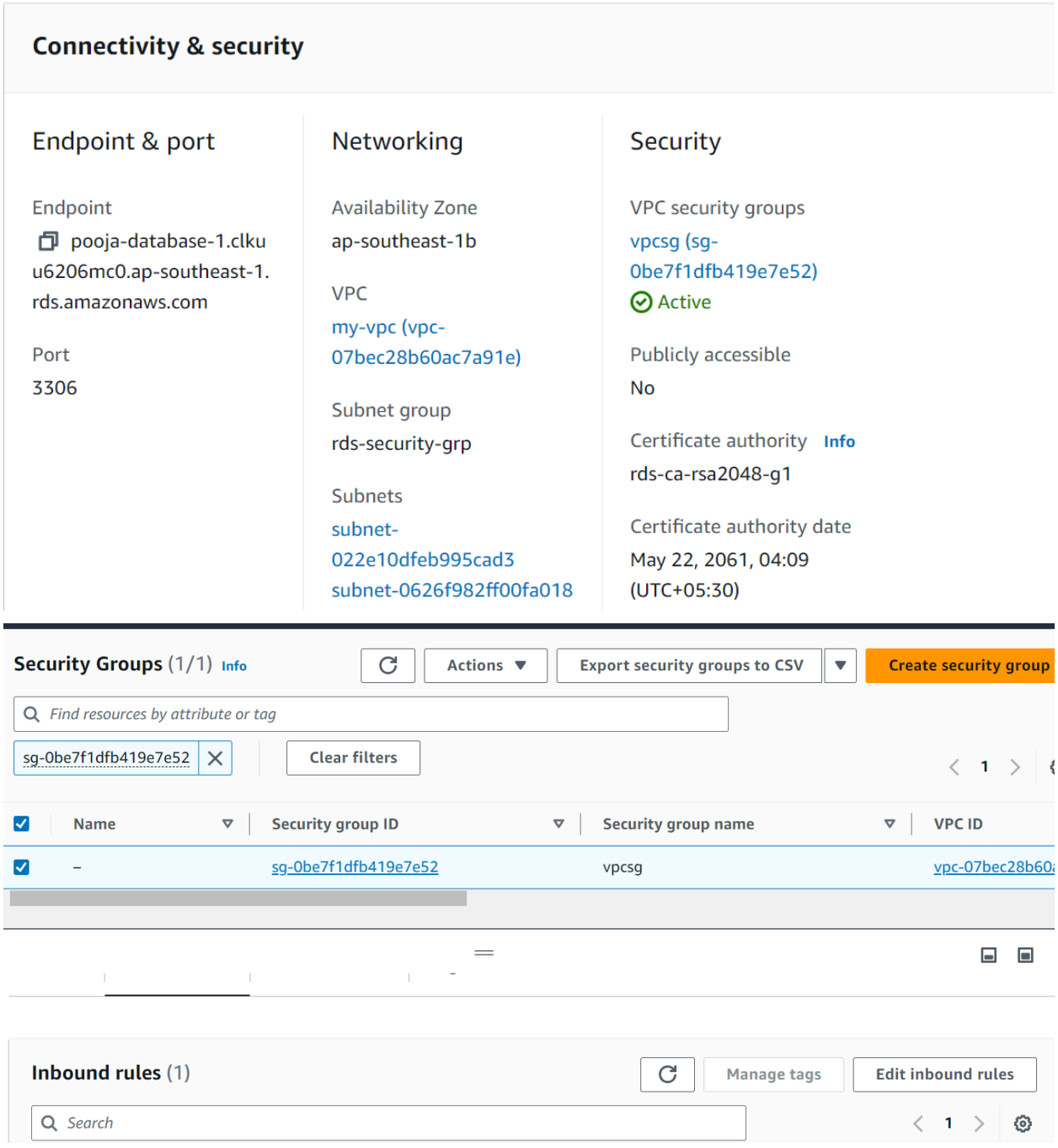
The following service-linked role is used for publishing logs to CloudWatch Logs.

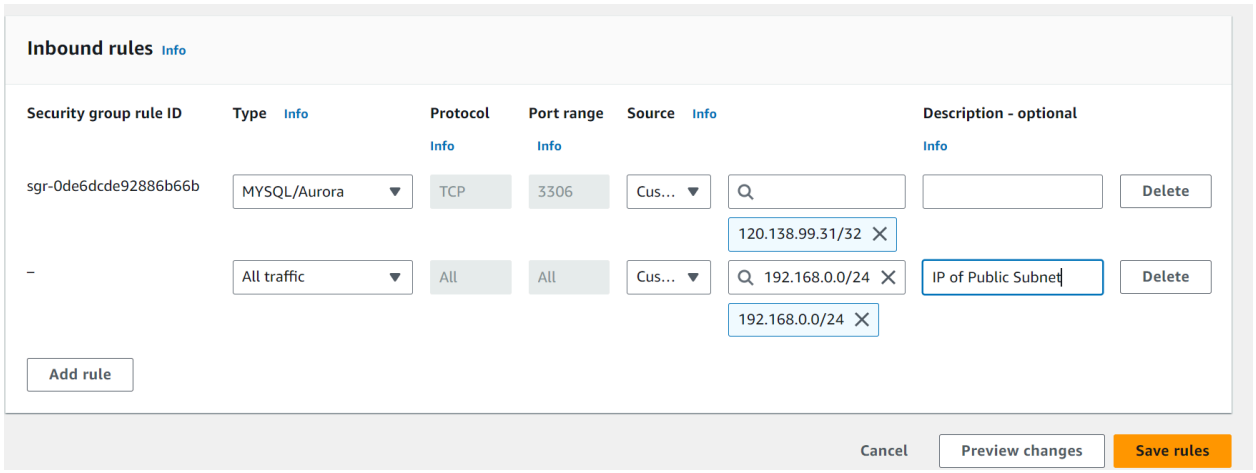
RDS service-linked role

RDS Instance is created :

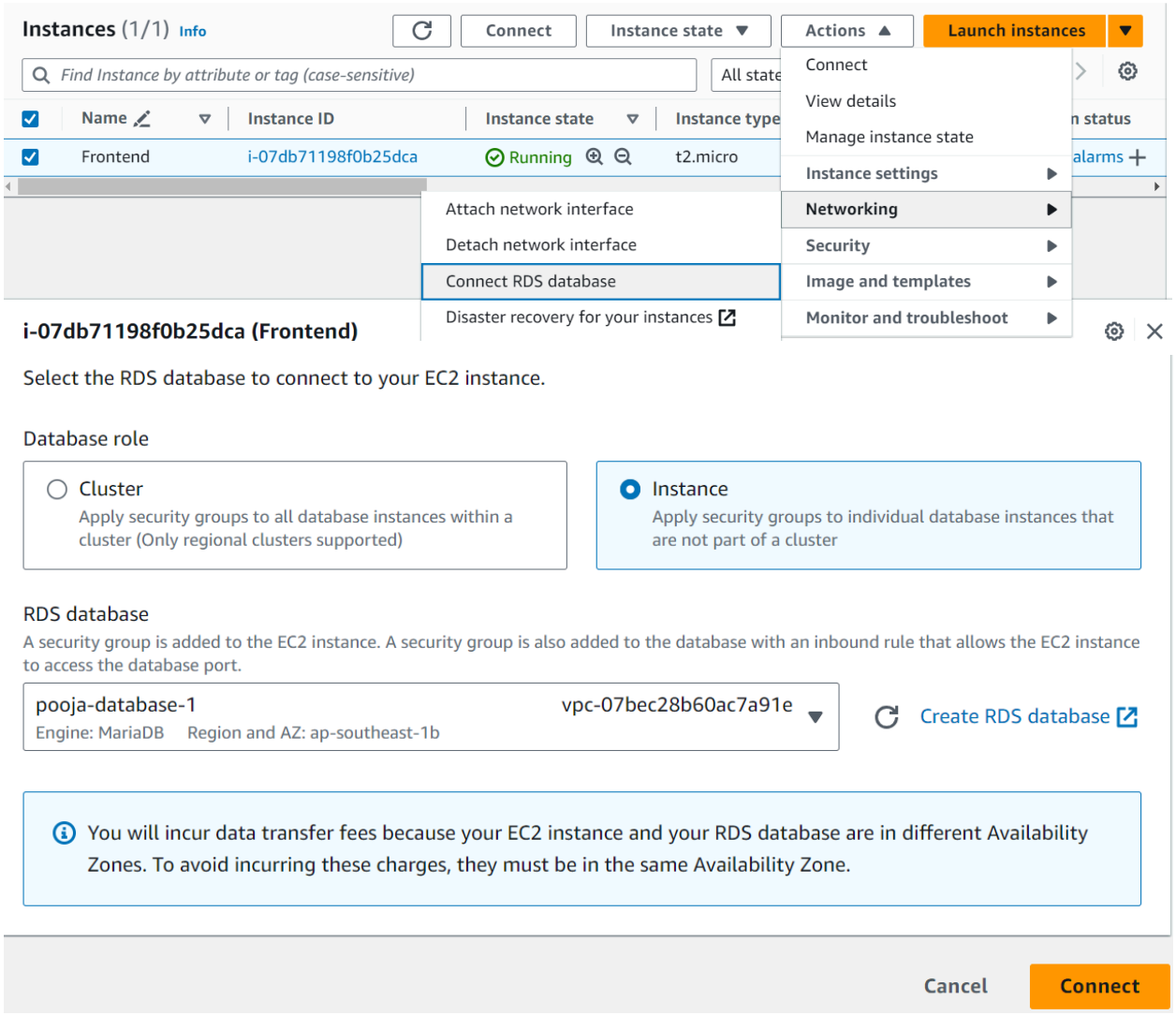


RDS > Security grp > inbound rules > edit



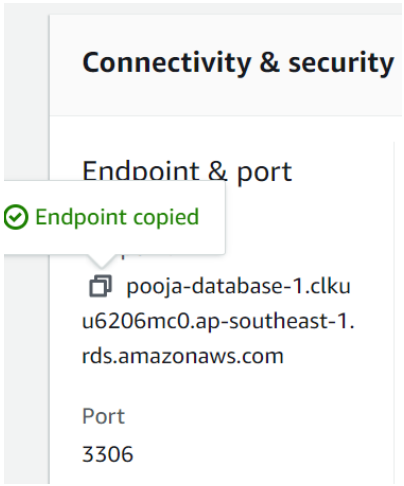

Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
sgr-0de6dcde92886b66b
MYSQL/Aurora
TCP
3306
Cus...
120.138.99.31/32
Delete
-
All traffic
All
All
Cus...
192.168.0.0/24
IP of Public Subnet
192.168.0.0/24
Delete
Add rule
Cancel
Preview changes
Save rules

Connect EC2


Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Frontend
i-07db71198f0b25dca
Running
t2.micro
Connect
View details
Manage instance state
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Attach network interface
Detach network interface
Connect RDS database
Disaster recovery for your instances
i-07db71198f0b25dca (Frontend)
Select the RDS database to connect to your EC2 instance.
Database role
Cluster
Apply security groups to all database instances within a cluster (Only regional clusters supported)
Instance
Apply security groups to individual database instances that are not part of a cluster
RDS database
A security group is added to the EC2 instance. A security group is also added to the database with an inbound rule that allows the EC2 instance to access the database port.
pooja-database-1
vpc-07bec28b60ac7a91e
Engine: MariaDB
Region and AZ: ap-southeast-1b
Create RDS database
You will incur data transfer fees because your EC2 instance and your RDS database are in different Availability Zones. To avoid incurring these charges, they must be in the same Availability Zone.
Cancel
Connect

```
[ec2-user@ip-192-168-0-186 ~]$ sudo su
[root@ip-192-168-0-186 ec2-user]# yum update -y
Last metadata expiration check: 0:39:19 ago on Tue Aug 13 11:06:59 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-192-168-0-186 ec2-user]# yum install mariadb* -y
Last metadata expiration check: 0:39:43 ago on Tue Aug 13 11:06:59 2024.
Dependencies resolved.
```

pooja-database-1.clkuu6206mc0.ap-southeast-1.rds.amazonaws.com




```
[root@ip-192-168-0-186 ec2-user]# mysql -u admin -p -h pooja-database-1.clkuu6206mc0.ap-southeast-1.rds.amazonaws.com
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 49
Server version: 10.11.8-MariaDB managed by https://aws.amazon.com/rds/

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

```
MariaDB [(none)]> create database pooja;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| innodb             |
| mysql              |
| performance_schema |
| pooja              |
| poojadb            |
| sys                |
+--------------------+
7 rows in set (0.001 sec)

MariaDB [(none)]> use database pooja
ERROR 1049 (42000): Unknown database 'database'
MariaDB [(none)]> use pooja
Database changed
```

Syntax for Creating a Table:

create table table1(id int,name varchar(30),salary int);

```
MariaDB [pooja]> create table table1(id int,name varchar(30),salary int);
Query OK, 0 rows affected (0.006 sec)
```

INSERT INTO table1 (id, name, salary) values (2,'Pooja Kharade', 90000), (3, 'Juli Chaurasiya', 55000), (4, 'Sonam Bharti', 60000);

```
MariaDB [pooja]> INSERT INTO table1 (id, name, salary) values (2,'Pooja Kharade', 90000), (3, 'Juli Chaurasiya', 55000), (4, 'Sonam Bhar
ti', 60000);
Query OK, 3 rows affected (0.002 sec)
Records: 3  Duplicates: 0  Warnings: 0
```

SELECT * FROM table1;

```
MariaDB [pooja]> SELECT * FROM table1;
+------+-----------------+--------+
| id   | name            | salary |
+------+-----------------+--------+
|    2 | Pooja Kharade   |  90000 |
|    3 | Juli Chaurasiya |  55000 |
|    4 | Sonam Bharti    |  60000 |
+------+-----------------+--------+
3 rows in set (0.001 sec)
```

UPDATE table1 SET salary = 62000 WHERE id = 2;

```
MariaDB [pooja]> UPDATE table1 SET salary = 62000 WHERE id = 2;
Query OK, 1 row affected (0.002 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

```
MariaDB [pooja]> SELECT * FROM table1;
+------+-----------------+--------+
| id   | name            | salary |
+------+-----------------+--------+
|    2 | Pooja Kharade   |  62000 |
|    3 | Juli Chaurasiya |  55000 |
|    4 | Sonam Bharti    |  60000 |
+------+-----------------+--------+
3 rows in set (0.001 sec)
```

DELETE FROM table1 WHERE id = 4;

```
MariaDB [pooja]> SELECT * FROM table1;
+------+-----------------+--------+
| id   | name            | salary |
+------+-----------------+--------+
|    2 | Pooja Kharade   |  62000 |
|    3 | Juli Chaurasiya |  55000 |
+------+-----------------+--------+
2 rows in set (0.001 sec)
```

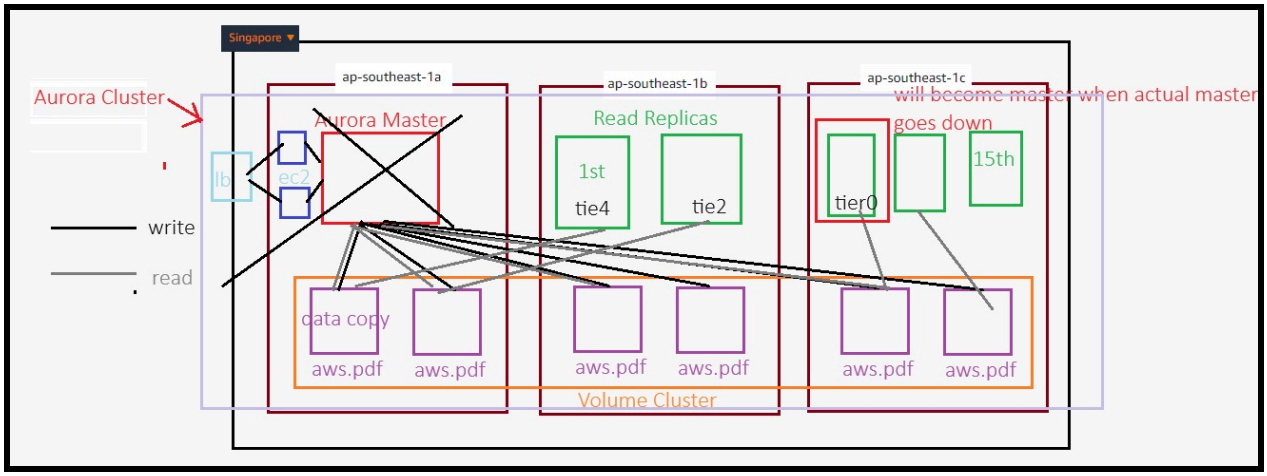
Date : 14-08-2024

AIM : Deploying EC2 with RDS Aurora in Different AZs Using Free Tier

Objective

The objective of this documentation is to guide you through deploying an EC2 instance connected to an RDS Aurora database, both located in different Availability Zones (AZs). The setup will include a read replica for the RDS instance and enabling automated backups. The goal is to ensure high availability, data durability, and efficient read performance while staying within the AWS Free Tier.

Architecture Flow Diagram



1. **VPC Setup**:
    - Create a Virtual Private Cloud (VPC) with multiple subnets in different AZs.
    - Ensure one subnet is designated for the EC2 instance and another for the RDS Aurora instance.
2. **EC2 Instance Configuration**:
    - Launch an EC2 instance in one of the subnets within the VPC.
    - Configure security groups to allow communication between the EC2 instance and the RDS Aurora instance.
3. **RDS Aurora Instance Setup**:
    - Deploy an RDS Aurora instance in a different AZ from the EC2 instance.
    - Create a read replica in another AZ to improve read scalability and availability.
    - Enable automated backups for the RDS Aurora instance.
4. **Data Flow**:

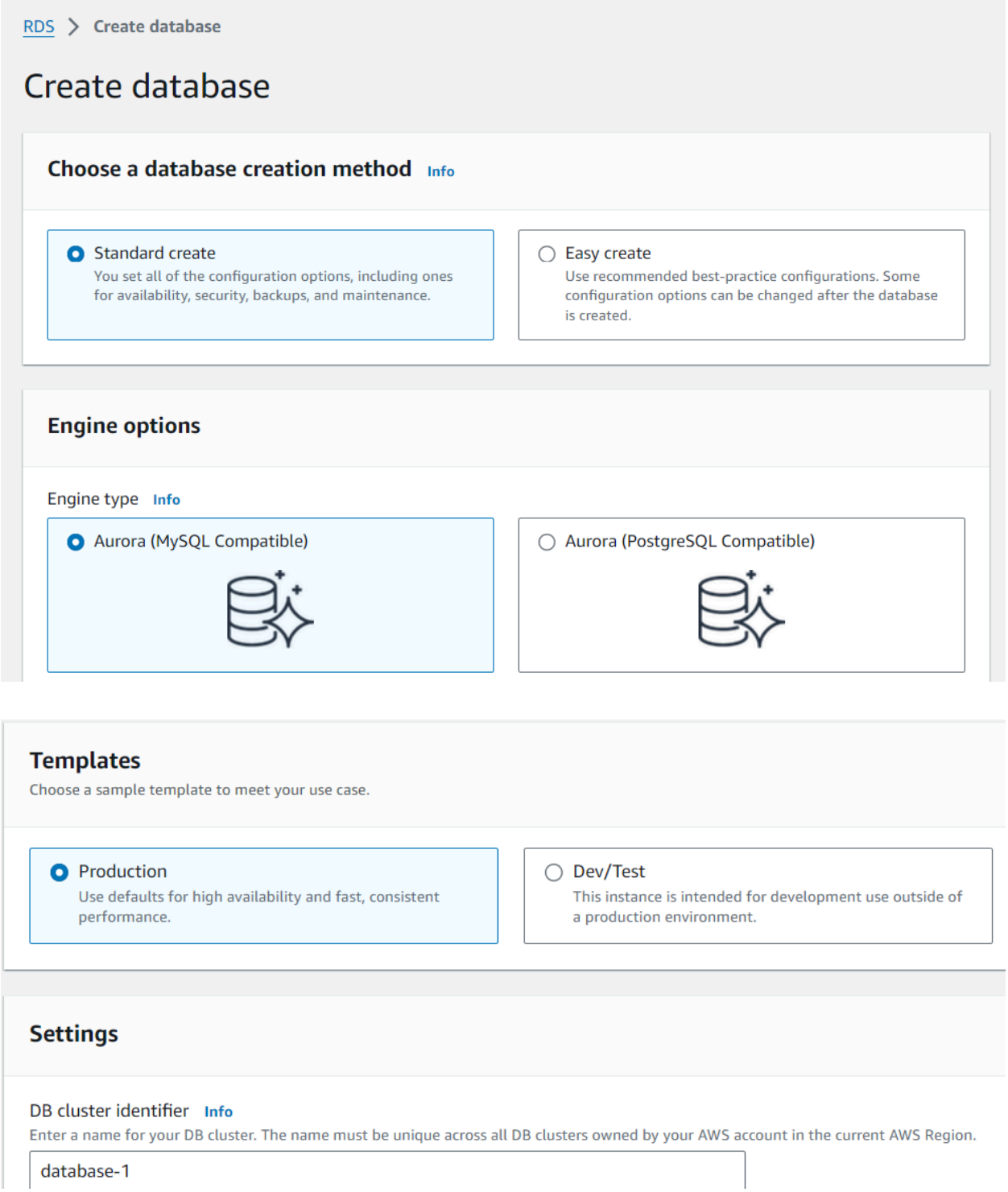
    - The EC2 instance serves as the application server, interacting with the RDS Aurora instance for database operations.
    - The RDS Aurora instance processes write operations, while the read replica handles read queries to offload the main database.
5. **Security and Backup**:
    - Implement IAM roles and policies to manage access.
    - Enable automated backups and Multi-AZ failover for the RDS Aurora instance.

Step-by-Step Implementation

1. **Create a VPC**:
    - Navigate to the VPC dashboard and create a new VPC.
    - Add subnets in different AZs (e.g., us-east-1a, us-east-1b).
    - Create a route table and associate it with the subnets.
2. **Launch EC2 Instance**:
    - Go to the EC2 dashboard and launch a new instance.
    - Choose an AMI that is Free Tier eligible (e.g., Amazon Linux 2).
    - Place the instance in one of the subnets created in your VPC.
    - Configure a security group allowing SSH access and inbound connections from the RDS instance.
3. **Create RDS Aurora Instance**:
    - In the RDS dashboard, create a new Aurora database cluster.

4. Select a different AZ for the RDS instance compared to the EC2 instance.
5. Enable Multi-AZ deployment for high availability.
6. Configure the read replica in a separate AZ to handle read operations.

4. Choose the option for "MySQL-compatible" Aurora.



Master username **Info**

Type a login ID for the master user of your DB instance.

admin

1 to 32 alphanumeric characters. The first character must be a letter.

Credentials management

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

- ○ Managed in AWS Secrets Manager - *most secure*
  RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.
- ◉ Self managed
  Create your own password or have RDS create a password that you manage.

☐ Auto generate password

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

Master password **Info**

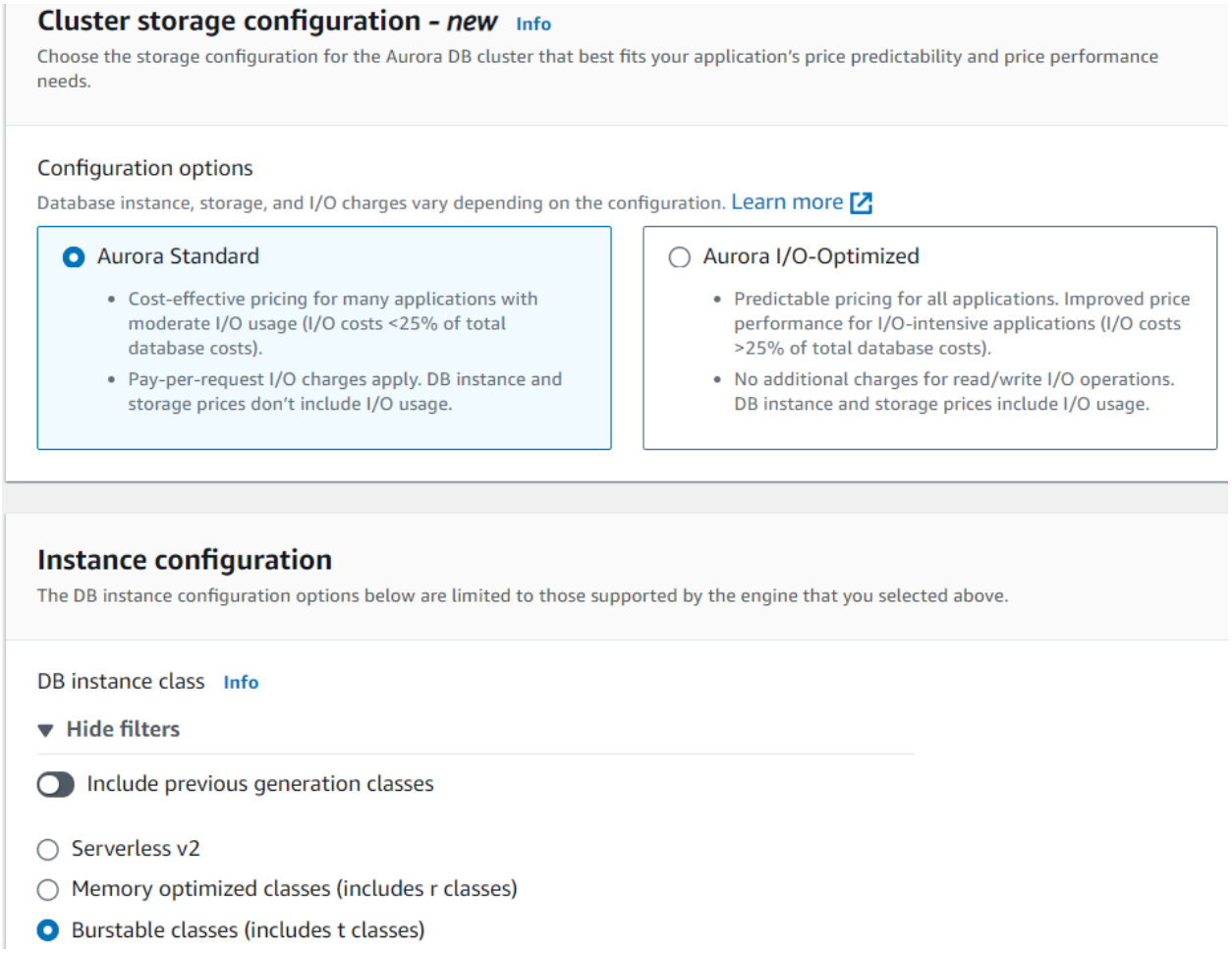
••••••••••

Password strength **Strong**

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

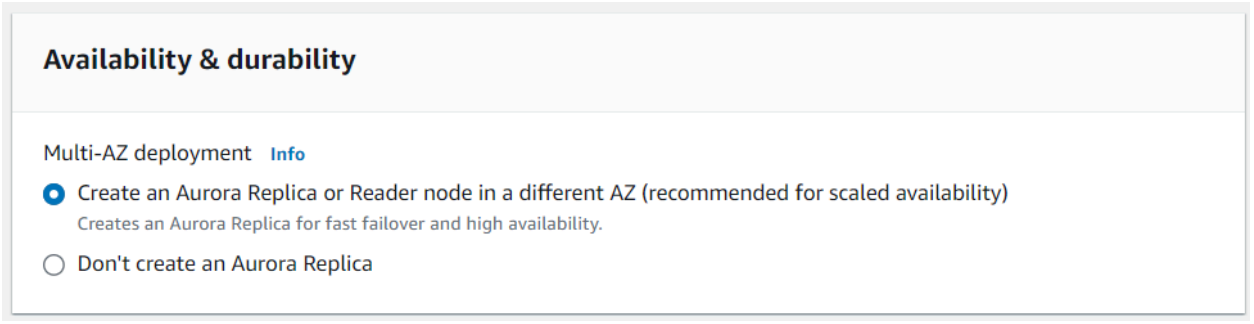
Confirm master password **Info**

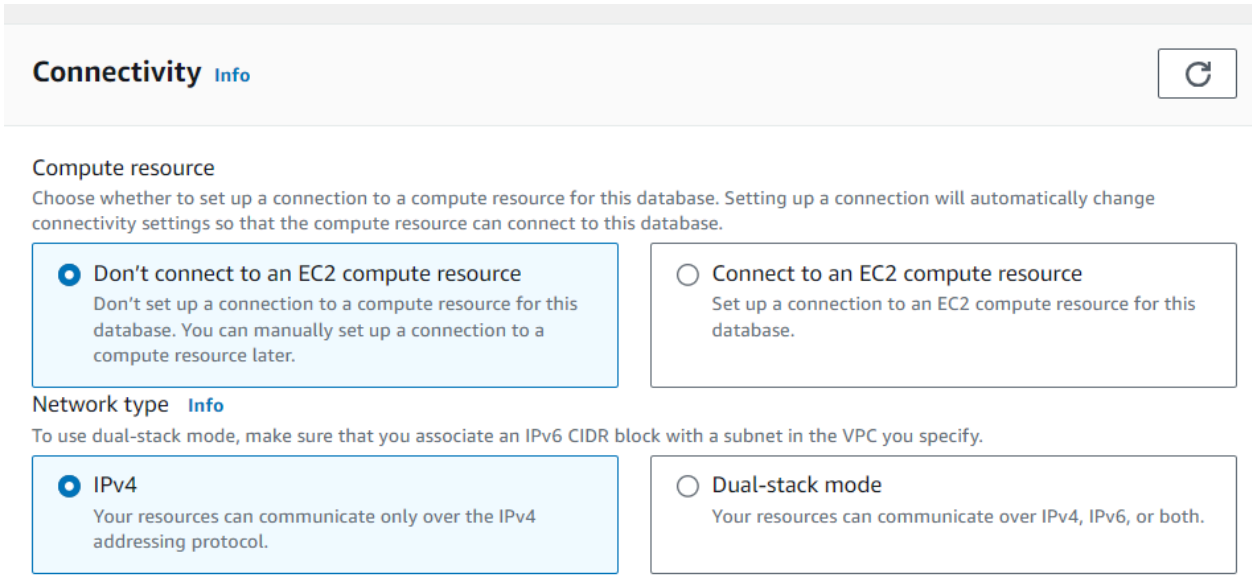
••••••••••



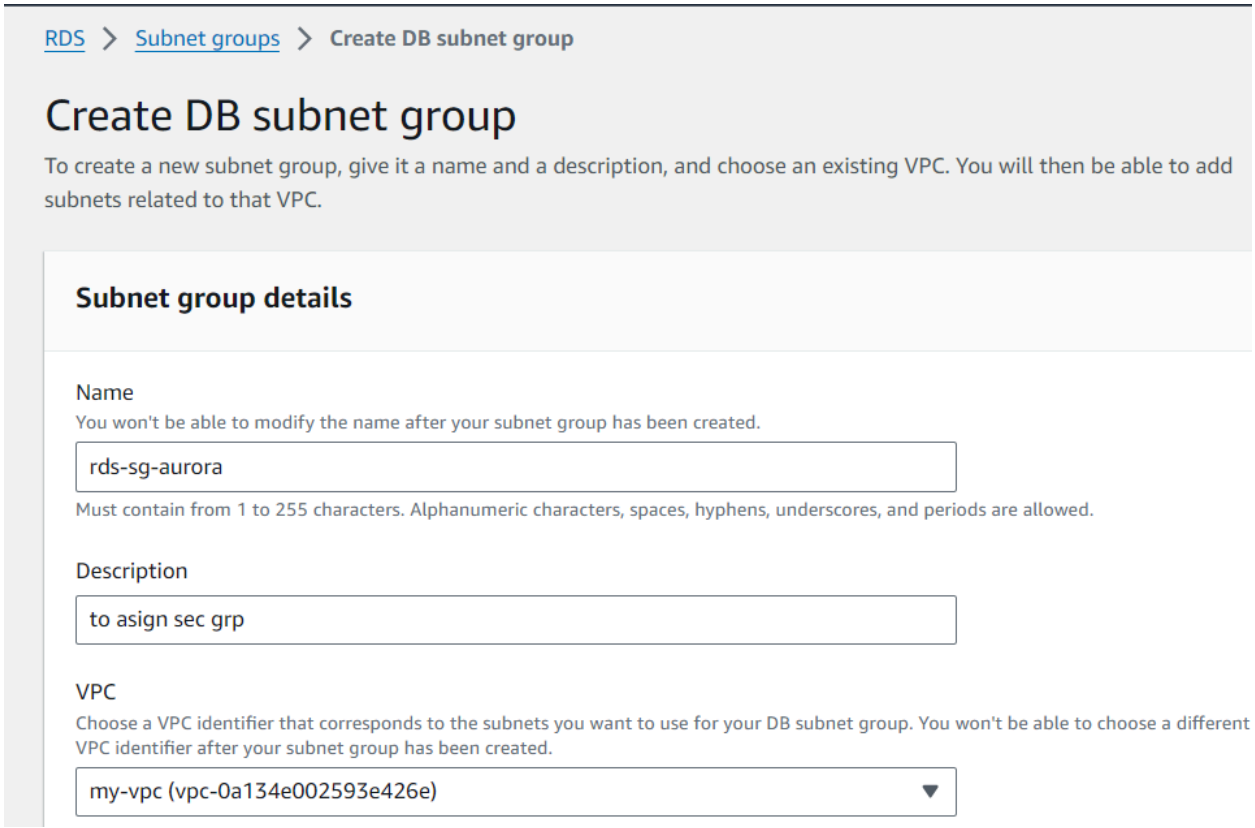
Configure the read replica in a separate AZ to handle read operations.

Enable Multi-AZ deployment for high availability.





Create new DB subnet group



Add subnets

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone

ap-southeast-1b ✕ ap-southeast-1c ✕

Subnets

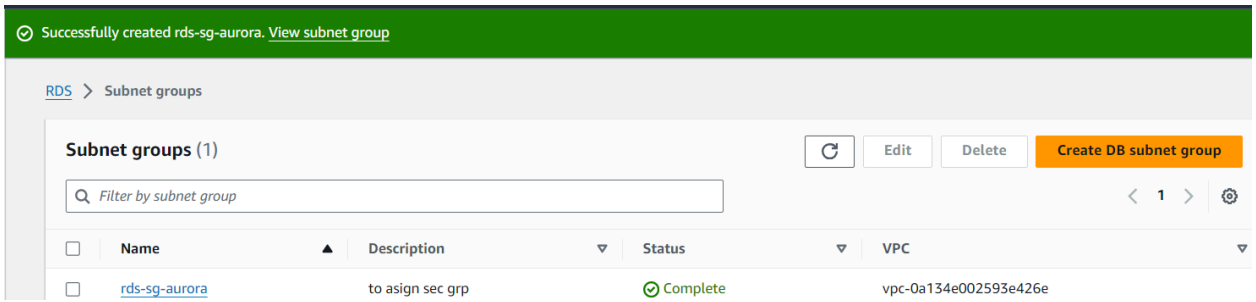
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets

subnet-05d55a186a58e5a35 (192.168.1.0/24) ✕

subnet-00e8865c7f8eb4146 (192.168.2.0/24) ✕

For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.



Virtual private cloud (VPC) **Info**

Choose the VPC. The VPC defines the virtual networking environment for this DB cluster.

my-vpc (vpc-0a134e002593e426e)
3 Subnets, 3 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group **Info**

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB cluster can use in the VPC that you selected.

rds-sg-aurora
2 Subnets, 2 Availability Zones

Public access **Info**

- Yes
  RDS assigns a public IP address to the cluster. Amazon EC2 instances and other resources outside of the VPC can connect to your cluster. Resources inside the VPC can also connect to the cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.
- No
  RDS doesn't assign a public IP address to the cluster. Only Amazon EC2 instances and other resources inside the VPC can connect to your cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

New VPC security group name

vpc-sg

Availability Zone **Info**

ap-southeast-1b

Additional configuration

Database options, encryption turned on, failover, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name Info

database-1

If you do not specify a database name, Amazon RDS does not create a database.

DB cluster parameter group Info

default.aurora-mysql8.0

DB parameter group Info

default.aurora-mysql8.0

Backup

Backup retention period Info

The number of days (1-35) for which automatic backups are kept.

1 day

Copy tags to snapshots

Encryption

Enable encryption

Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. Info

Backtrack

Backtrack lets you quickly rewind the DB cluster to a specific point in time, without having to create another DB cluster. Info

Enable Backtrack

Enabling Backtrack will charge you for storing the changes you make for backtracking.

Log exports

Select the log types to publish to Amazon CloudWatch Logs

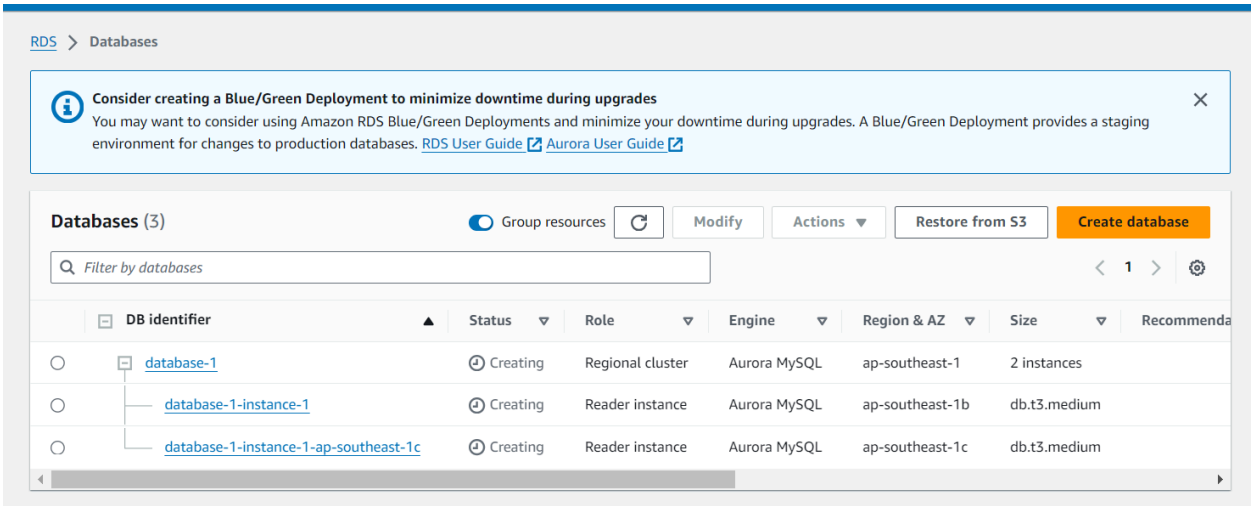
Audit log

Error log

General log

Slow query log

IAM role



Launch An Instance

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

frontend

Add additional tags

Application and OS Images (Amazon Machine Image) Info

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

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

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Li

Browse more AMIs

Including AMIs from AWS, Marketplace and

Instance type Info | Get advice

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0146 USD per Hour
On-Demand Windows base pricing: 0.0192 USD per Hour
On-Demand RHEL base pricing: 0.029 USD per Hour
On-Demand SUSE base pricing: 0.0146 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

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

Key pair name - *required*

mykey

Create new key pair

Network settings Info

VPC - *required* Info

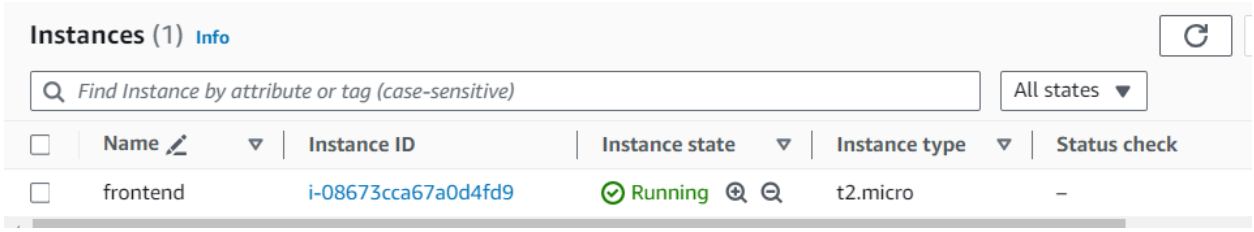
vpc-0a134e002593e426e (my-vpc)
192.168.0.0/16

Inbound Security Group Rules

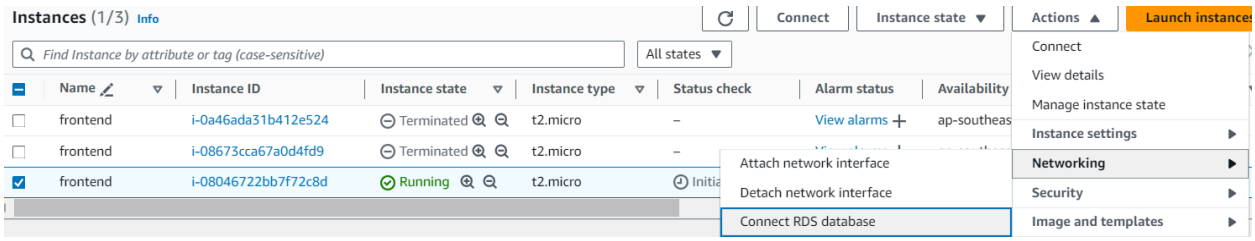
Security group rule 1 (TCP, 22, 0.0.0.0/0) — Remove

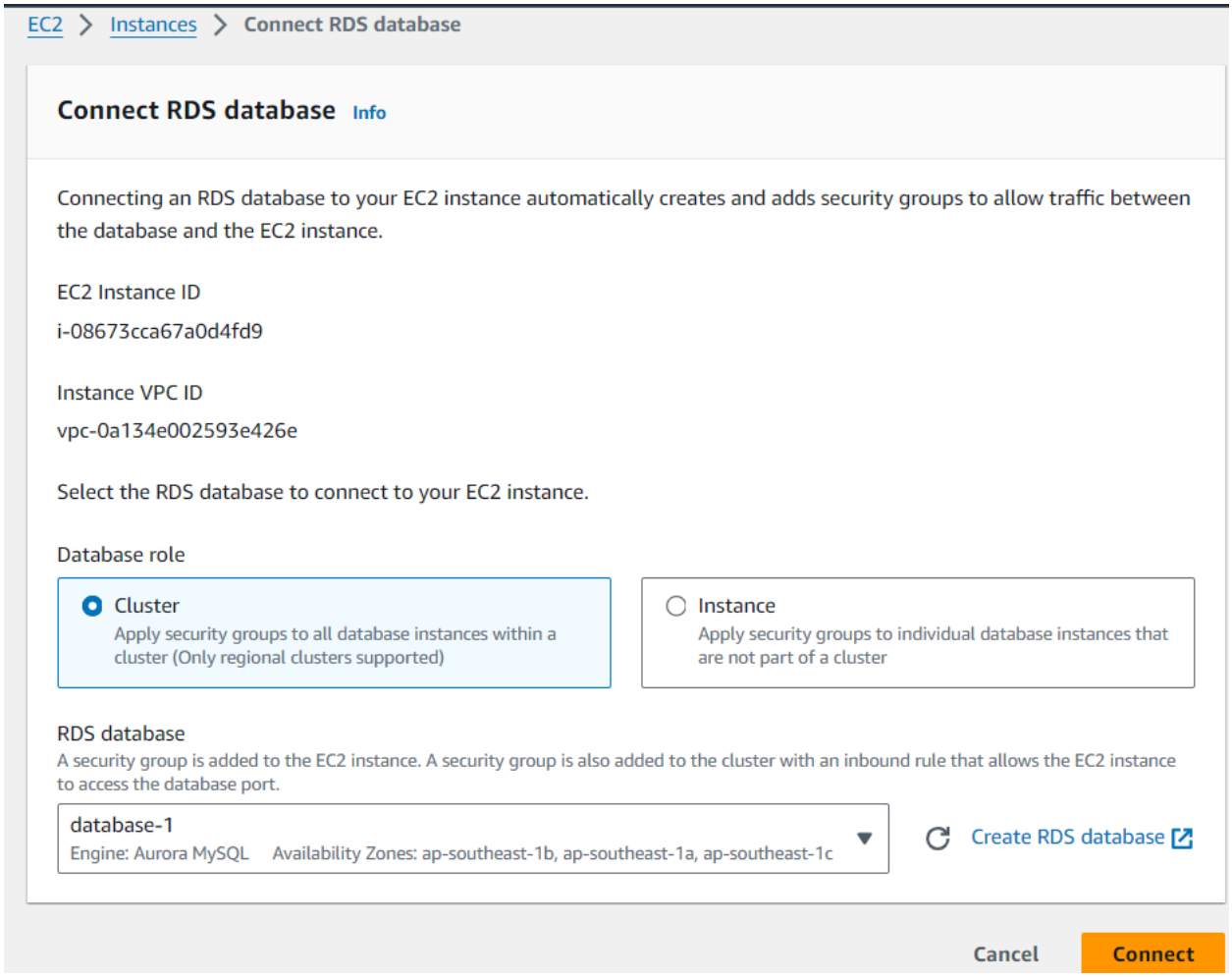
Type Info	Protocol Info	Port range Info
ssh	TCP	22

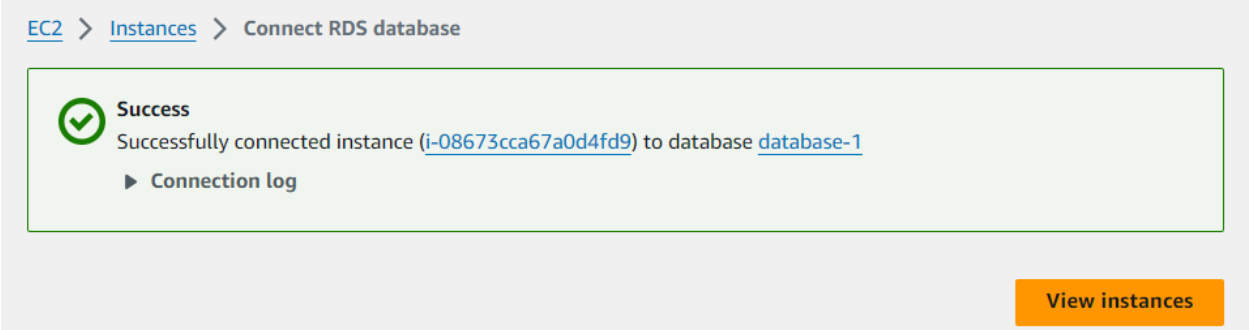
Source type Info	Source Info	Description - *optional* Info
Anywhere	*Add CIDR, prefix list or security* — 0.0.0.0/0	*e.g. SSH for admin desktop*



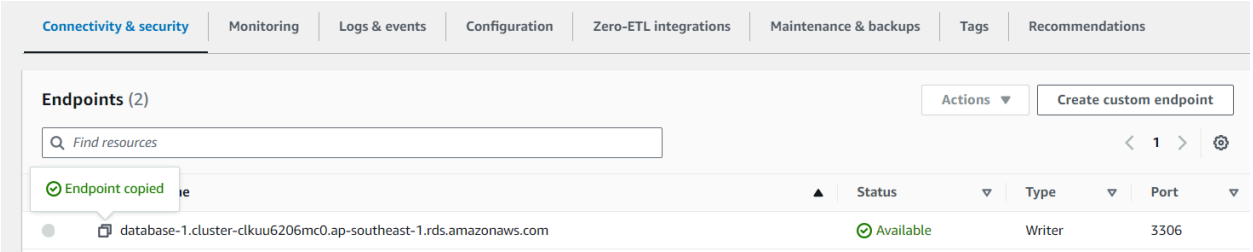
Connect EC2 with RDS







Update the application's configuration to point to the RDS Aurora endpoint.

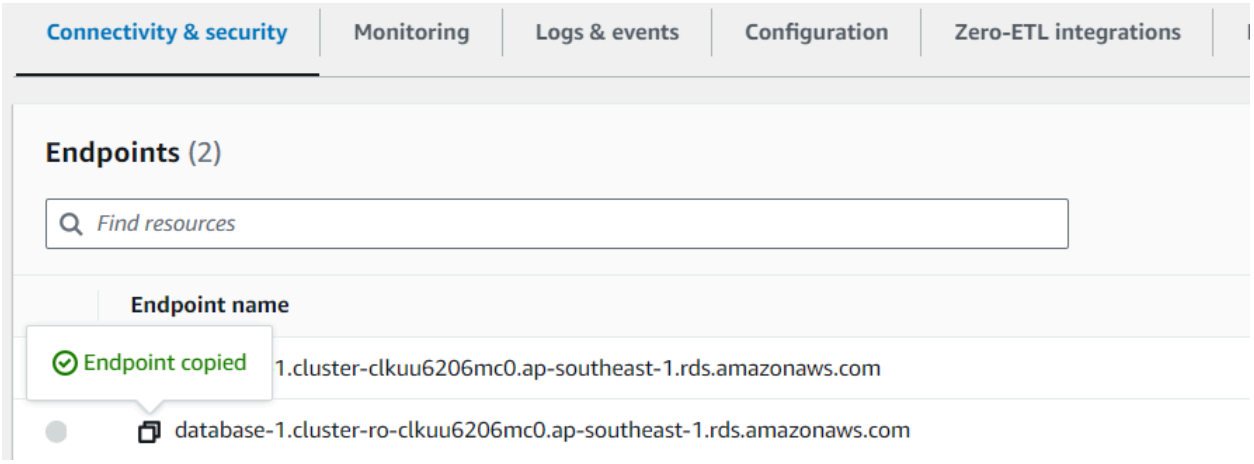



```
       _/m/'
Last login: Sat Aug 17 15:26:53 2024 from 3.0.5.35
[ec2-user@ip-192-168-0-66 ~]$ sudo su
[root@ip-192-168-0-66 ec2-user]# yum update -y
Last metadata expiration check: 0:13:13 ago on Sat Aug 17 15:26:12 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-192-168-0-66 ec2-user]# yum upgrade -y
Last metadata expiration check: 0:13:21 ago on Sat Aug 17 15:26:12 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-192-168-0-66 ec2-user]# yum install mariadb* -y
Last metadata expiration check: 0:13:46 ago on Sat Aug 17 15:26:12 2024.
Package mariadb-connector-c-3.1.13-1.amzn2023.0.3.x86_64 is already installed.
Package mariadb-connector-c-config-3.1.13-1.amzn2023.0.3.noarch is already installed.
Package mariadb-connector-c-devel-3.1.13-1.amzn2023.0.3.x86_64 is already installed.
Package mariadb-connector-c-test-3.1.13-1.amzn2023.0.3.x86_64 is already installed.
Package mariadb105-3:10.5.25-1.amzn2023.0.1.x86_64 is already installed.
Package mariadb105-backup-3:10.5.25-1.amzn2023.0.1.x86_64 is already installed.
Package mariadb105-common-3:10.5.25-1.amzn2023.0.1.x86_64 is already installed.
```

```
[root@ip-192-168-0-66 ec2-user]# mysql -u admin -p -h database-1.cluster-clkuu6206mc0.ap-southeast-1.rds.amazonaws.com
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 218
Server version: 8.0.32 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| database1          |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.004 sec)
```

```
MySQL [(none)]> create database auradb;
Query OK, 1 row affected (0.004 sec)

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| auradb             |
| database1          |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
6 rows in set (0.002 sec)
```

For read operations, configure the application to use the read replica endpoint.




```
MySQL [(none)]> exit
Bye
[root@ip-192-168-0-66 ec2-user]# mysql -u admin -p -h database-1.cluster-ro-clkuu6206mc0.ap-southeast-1.rds.amazonaws.com
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 204
Server version: 8.0.32 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| auradb             |
| database1          |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
6 rows in set (0.002 sec)

MySQL [(none)]> create database auroradb;
ERROR 1836 (HY000): Running in read-only mode
MySQL [(none)]>
```

Testing:

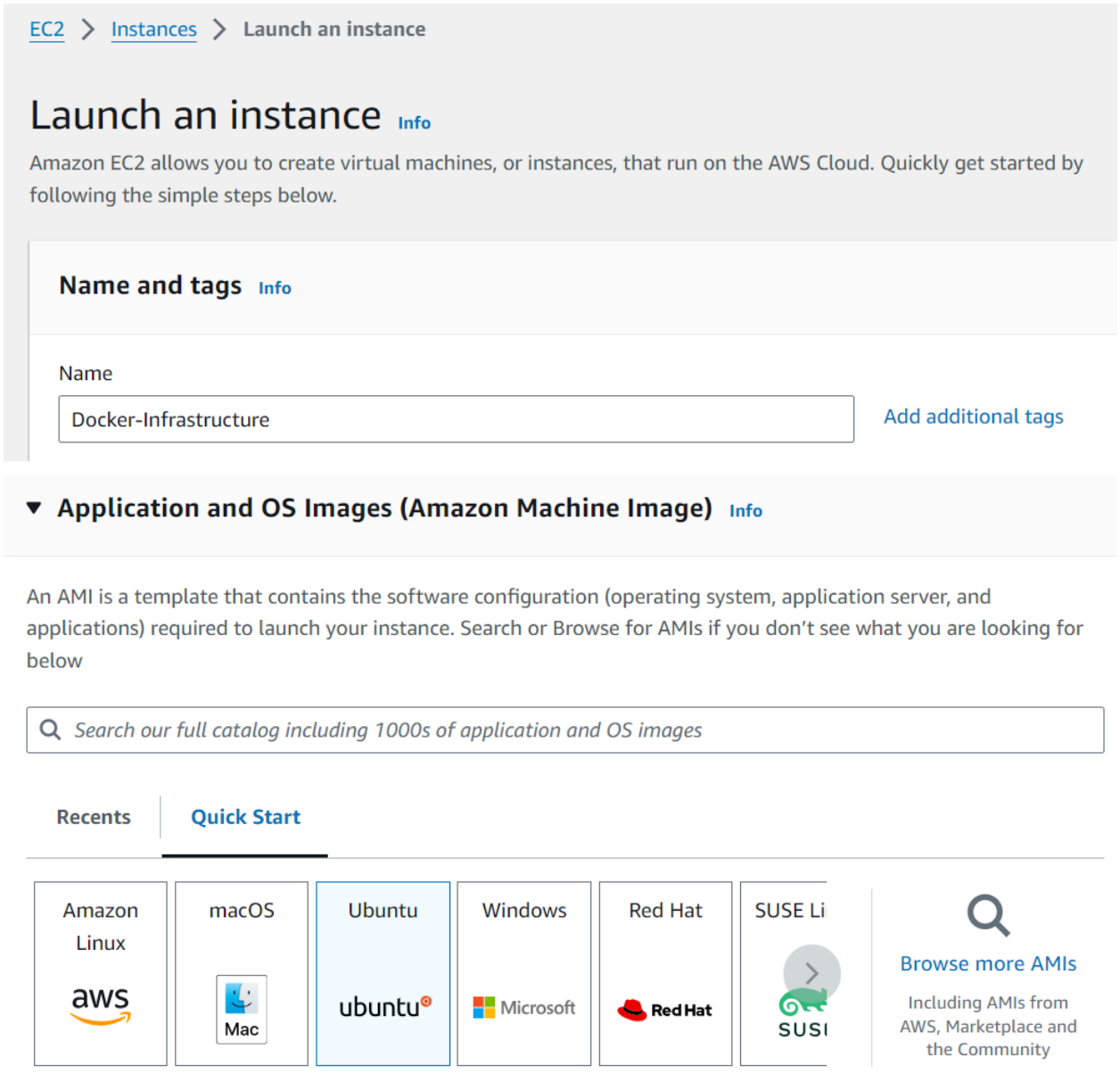
- Perform some read and write operations to ensure everything is set up correctly.
- Test the failover by temporarily stopping the primary RDS instance and checking if the application switches to the replica or the secondary AZ.

Conclusion

By following this guide, you have successfully deployed an EC2 instance and an RDS Aurora database in different AZs, complete with a read replica and automated backups. This architecture ensures high availability, better performance, and cost-effective use of AWS resources under the Free Tier. The use of different AZs for the EC2 instance and the RDS database helps enhance the fault tolerance of the application, while the read replica improves the read performance.

Date : 20/08/24

AIM : DevOps (Development Operations)



Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Li

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible

ami-060e277c0d4cce553 (64-bit (x86)) / ami-09b5c6390225b29cc (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Architecture: 64-bit (x86)

AMI ID: ami-060e277c0d4cce553 Verified provider

Instance type

c3.large

Family: c3 2 vCPU 3.75 GiB Memory Current generation: false

On-Demand RHEL base pricing: 0.161 USD per Hour

On-Demand Linux base pricing: 0.132 USD per Hour

On-Demand Windows base pricing: 0.238 USD per Hour

On-Demand SUSE base pricing: 0.232 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Instance type Info | Get advice

Instance type

t2.medium
Family: t2 2 vCPU 4 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.0872 USD per Hour
On-Demand Windows base pricing: 0.0764 USD per Hour
On-Demand SUSE base pricing: 0.1584 USD per Hour
On-Demand Linux base pricing: 0.0584 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

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

Key pair name - *required*

mykey

Create new key pair

Network settings Info

VPC - *required* Info

vpc-046539f8fe281e626 (my-vpc)
10.10.0.0/24

Subnet Info

subnet-008a806d543a9ae43 Pub-sub
VPC: vpc-046539f8fe281e626 Owner: 637423493890
Availability Zone: ap-southeast-1a Zone type: Availability Zone
IP addresses available: 11 CIDR: 10.10.0.0/28)

Create new subnet

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - *required*

launch-wizard-5

Step 1 : Installing Docker

The Docker installation package available in the official Ubuntu repository may not be the latest version. To ensure we get the latest version, we'll install Docker from the official Docker repository. To do that, we'll add a new package source, add the GPG key from Docker to ensure the downloads are valid, and then install the package.

First, update your existing list of packages:

> sudo apt update

```
ubuntu@ip-10-10-0-4:~$ sudo su
root@ip-10-10-0-4:/home/ubuntu# sudo apt update
Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:8 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:9 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:10 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:11 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:12 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:13 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [349 kB]
Get:14 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [89.1 kB]
Get:15 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [5948 B]
Get:16 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [323 kB]
Get:17 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [136 kB]
```

Next, install a few prerequisite packages which let apt use packages over HTTPS:

sudo apt install apt-transport-https ca-certificates curl software-properties-common

```
root@ip-10-10-0-4:/home/ubuntu# sudo apt install apt-transport-https ca-certificates curl software-properties-common
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20240203).
ca-certificates set to manually installed.
software-properties-common is already the newest version (0.99.48).
software-properties-common set to manually installed.
The following NEW packages will be installed:
  apt-transport-https
The following packages will be upgraded:
  curl libcurl3t64-gnutls libcurl4t64
3 upgraded, 1 newly installed, 0 to remove and 52 not upgraded.
Need to get 904 kB of archives.
After this operation, 35.8 kB of additional disk space will be used.
Get:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all 2.7.14build2 [3974 B]
Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 curl amd64 8.5.0-2ubuntu10.2 [227 kB]
Get:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libcurl4t64 amd64 8.5.0-2ubuntu10.2 [341 kB]
Get:4 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libcurl3t64-gnutls amd64 8.5.0-2ubuntu10.2 [333 kB]
Fetched 904 kB in 0s (17.9 MB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 67739 files and directories currently installed.)
```

Then add the GPG key for the official Docker repository to your system:

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

```
root@ip-10-10-0-4:/home/ubuntu# curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
root@ip-10-10-0-4:/home/ubuntu# sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable"
Repository: 'deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable'
Description:
Archive for codename: focal components: stable
More info: https://download.docker.com/linux/ubuntu
Adding repository.
Press [ENTER] to continue or Ctrl-c to cancel.
Adding deb entry to /etc/apt/sources.list.d/archive_uri-https_download_docker_com_linux_ubuntu-noble.list
Adding disabled deb-src entry to /etc/apt/sources.list.d/archive_uri-https_download_docker_com_linux_ubuntu-noble.list
Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:4 https://download.docker.com/linux/ubuntu focal InRelease [57.7 kB]
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:6 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages [48.8 kB]
Fetched 106 kB in 1s (199 kB/s)
Reading package lists... Done
```

Add the Docker repository to APT sources:

sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable"

```
root@ip-10-10-0-4:/home/ubuntu# sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable"
Repository: 'deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable'
Description:
Archive for codename: focal components: stable
More info: https://download.docker.com/linux/ubuntu
Adding repository.
Press [ENTER] to continue or Ctrl-c to cancel.
Adding deb entry to /etc/apt/sources.list.d/archive_uri-https_download_docker_com_linux_ubuntu-noble.list
Adding disabled deb-src entry to /etc/apt/sources.list.d/archive_uri-https_download_docker_com_linux_ubuntu-noble.list
Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:4 https://download.docker.com/linux/ubuntu focal InRelease [57.7 kB]
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:6 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages [48.8 kB]
Fetched 106 kB in 1s (199 kB/s)
Reading package lists... Done
W: https://download.docker.com/linux/ubuntu/dists/focal/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECAT
ION section in apt-key(8) for details.
```

This will also update our package database with the Docker packages from the newly added repo.

Make sure you are about to install from the Docker repo instead of the default Ubuntu repo:

apt-cache policy docker-ce

```
root@ip-10-10-0-4:/home/ubuntu# sudo apt install docker-ce
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  containerd.io docker-buildx-plugin docker-ce-cli docker-ce-rootless-extras docker-compose-plugin libltdl7 libslirp0 pigz slirp4netns
Suggested packages:
  aufs-tools cgroupfs-mount | cgroup-lite
The following NEW packages will be installed:
  containerd.io docker-buildx-plugin docker-ce docker-ce-cli docker-ce-rootless-extras docker-compose-plugin libltdl7 libslirp0 pigz slirp4netns
0 upgraded, 10 newly installed, 0 to remove and 52 not upgraded.
Need to get 122 MB of archives.
After this operation, 437 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Finally, install Docker:

```
root@ip-10-10-0-4:/home/ubuntu# sudo apt install docker-ce
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
docker-ce is already the newest version (5:27.1.2-1~ubuntu.20.04~focal).
0 upgraded, 0 newly installed, 0 to remove and 52 not upgraded.
root@ip-10-10-0-4:/home/ubuntu#
```

Docker should now be installed, the daemon started, and the process enabled to start on boot. Check that it's running:
sudo systemctl status docker

```
root@ip-10-10-0-4:/home/ubuntu# sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-08-20 15:44:26 UTC; 9min ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 3442 (dockerd)
      Tasks: 14
     Memory: 25.2M (peak: 26.8M)
        CPU: 511ms
     CGroup: /system.slice/docker.service
             └─3442 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
```

```
...skipping...
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-08-20 15:44:26 UTC; 9min ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 3442 (dockerd)
      Tasks: 14
     Memory: 25.2M (peak: 26.8M)
        CPU: 511ms
     CGroup: /system.slice/docker.service
             └─3442 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

Aug 20 15:44:26 ip-10-10-0-4 dockerd[3442]: time="2024-08-20T15:44:26.279173077Z" level=info msg="Starting up"
Aug 20 15:44:26 ip-10-10-0-4 dockerd[3442]: time="2024-08-20T15:44:26.279767801Z" level=info msg="detected 127.0.0.53 nameserver, assuming systemd-res>
Aug 20 15:44:26 ip-10-10-0-4 dockerd[3442]: time="2024-08-20T15:44:26.466473194Z" level=info msg="Loading containers: start."
Aug 20 15:44:26 ip-10-10-0-4 dockerd[3442]: time="2024-08-20T15:44:26.889023392Z" level=info msg="Loading containers: done."
Aug 20 15:44:26 ip-10-10-0-4 dockerd[3442]: time="2024-08-20T15:44:26.919305776Z" level=info msg="Docker daemon" commit=f9522e5 containerd-snapshotter>
Aug 20 15:44:26 ip-10-10-0-4 dockerd[3442]: time="2024-08-20T15:44:26.919414989Z" level=info msg="Daemon has completed initialization"
Aug 20 15:44:26 ip-10-10-0-4 dockerd[3442]: time="2024-08-20T15:44:26.996773962Z" level=info msg="API listen on /run/docker.sock"
Aug 20 15:44:26 ip-10-10-0-4 systemd[1]: Started docker.service - Docker Application Container Engine.
Aug 20 15:52:04 ip-10-10-0-4 dockerd[3442]: time="2024-08-20T15:52:04.827406577Z" level=error msg="Not continuing with pull after error: errors:\ndeni>
Aug 20 15:52:04 ip-10-10-0-4 dockerd[3442]: time="2024-08-20T15:52:04.827445798Z" level=info msg="Ignoring extra error returned from registry" error="
~
```

```
root@ip-10-10-0-4:/home/ubuntu# sudo apt install docker-ce
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
docker-ce is already the newest version (5:27.1.2-1~ubuntu.20.04~focal).
0 upgraded, 0 newly installed, 0 to remove and 52 not upgraded.
root@ip-10-10-0-4:/home/ubuntu# docker --version
Docker version 27.1.2, build d01f264
root@ip-10-10-0-4:/home/ubuntu# systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-08-20 15:44:26 UTC; 16min ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 3442 (dockerd)
      Tasks: 14
     Memory: 23.2M (peak: 26.8M)
        CPU: 601ms
     CGroup: /system.slice/docker.service
             └─3442 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
```

 # Use Ubuntu 22.04 as the base image
FROM ubuntu:22.04

 # Update installed packages and install Apache
**RUN apt update && **
**apt install -y apache2 && **
**rm -rf /var/lib/apt/lists/* && **
service apache2 start

 # Write hello world message

RUN echo 'Hello World' > /var/www/html/index.html

 # Create a custom Apache configuration file to set the ServerName
**RUN echo 'ServerName localhost' > /etc/apache2/conf-available/servername.conf && **
a2enconf servername

 # Configure Apache
**RUN mkdir -p /var/run/apache2 /var/lock/apache2 && **
**echo '#!/bin/bash\n' **
'service apache2 start && /usr/sbin/apachectl -D FOREGROUND' >
**/usr/local/bin/run_apache.sh && **
chmod +x /usr/local/bin/run_apache.sh

EXPOSE 80

CMD ["/usr/local/bin/run_apache.sh"]

```
root@ip-172-31-33-135:/home/ubuntu# history
    1  sudo apt install apt-transport-https ca-certificates curl software-properties-common -y
    2  sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
    3  echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/ubuntu
$(. /etc/os-release && echo "$VERSION_CODENAME") stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
    4  sudo apt update
    5  sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
    6  sudo docker --version
    7  sudo systemctl enable docker
    8  sudo systemctl status docker
    9  sudo docker pull nginx:latest
   10  $ sudo docker images
   11  docker images
   12  docker pull nginx
   13  docker container run -it nginx:latest /bin/bash
   14  vi dockerfile
   15  ls
   16  docker images
   17  docker build -t pooja-image
   18  docker images
   19  docker container build -f
   20  docker container build -f dockerfile
   21  docker container build -f dockerfile -it pooja-image .
   22  ls
   23  docker images
   24  docker container build -it pooja-image .
   25  ls
```

```
root@ip-172-31-33-135:/home/ubuntu# docker container run -it pooja-image /bin/bash
root@3c2f7f596e49:/# service apache2 status
 * apache2 is not running
root@3c2f7f596e49:/# service apache2 start
 * Starting Apache httpd web server apache2
 *
root@3c2f7f596e49:/# service apache2 status
 * apache2 is running
root@3c2f7f596e49:/#
```

In another session

```
root@ip-172-31-33-135:/home/ubuntu# curl http://172.17.0.2
Hello World
root@ip-172-31-33-135:/home/ubuntu# history
    1  docker container inspect 3c2f7f596e49
    2  curl http://172.17.0.2
    3  history
root@ip-172-31-33-135:/home/ubuntu#
```

Vi dockerfile

```
# Write hello world message
RUN echo 'Hello Pooja' > /var/www/html/index.html

# Create a custom Apache configuration file to set the ServerName
RUN echo 'ServerName localhost' > /etc/apache2/conf-available/servername.conf && \
    a2enconf servername

# Configure Apache
RUN mkdir -p /var/run/apache2 /var/lock/apache2 && \
    echo '#!/bin/bash\n' \
    'service apache2 start && /usr/sbin/apachectl -D FOREGROUND' > /usr/local/bin/run_apache.sh && \
    chmod +x /usr/local/bin/run_apache.sh

EXPOSE 80

CMD ["/usr/local/bin/run_apache.sh"]

6%
-- INSERT --
op
```

```
root@ip-172-31-33-135:/home/ubuntu# docker images
REPOSITORY    TAG       IMAGE ID       CREATED          SIZE
pooja-image   latest    7e3e631339ef   24 minutes ago   186MB
nginx         latest    5ef79149e0ec   6 days ago       188MB
root@ip-172-31-33-135:/home/ubuntu#
```

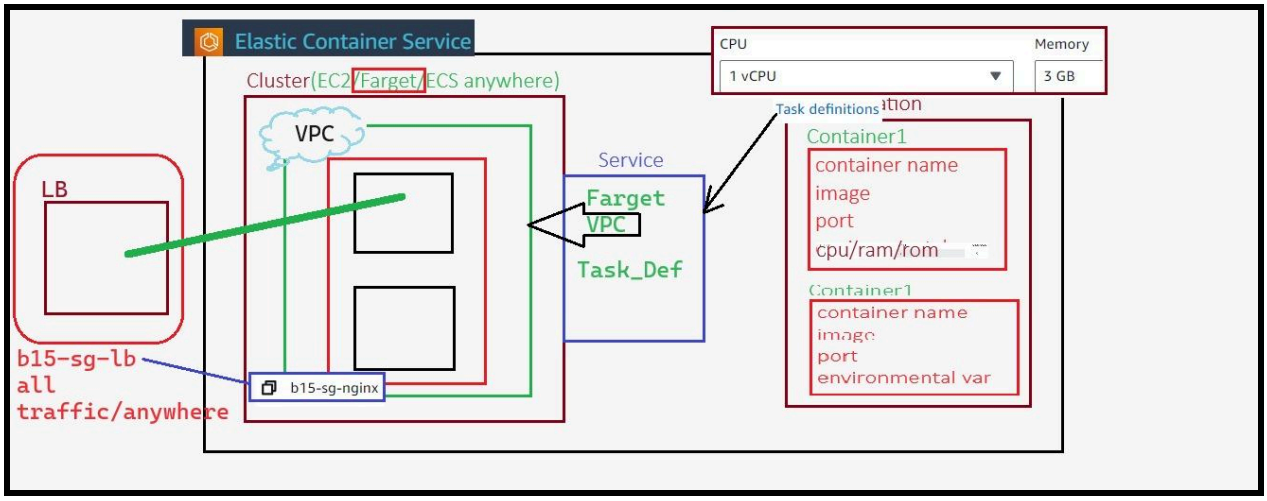
```
root@ip-172-31-33-135:/home/ubuntu# docker build -t pooja-image:version1
ERROR: "docker buildx build" requires exactly 1 argument.
See 'docker buildx build --help'.

Usage:  docker buildx build [OPTIONS] PATH | URL | -

Start a build
root@ip-172-31-33-135:/home/ubuntu#
```

```
root@ip-172-31-33-135:/home/ubuntu# docker images
REPOSITORY    TAG       IMAGE ID       CREATED          SIZE
pooja-image   latest    7e3e631339ef   33 minutes ago   186MB
pooja-image   ver1      7e3e631339ef   33 minutes ago   186MB
nginx         latest    5ef79149e0ec   6 days ago       188MB
root@ip-172-31-33-135:/home/ubuntu#
```

Date : 23/08/2024

Aim : configuring AWS Elastic Container Service (ECS)

Architecture

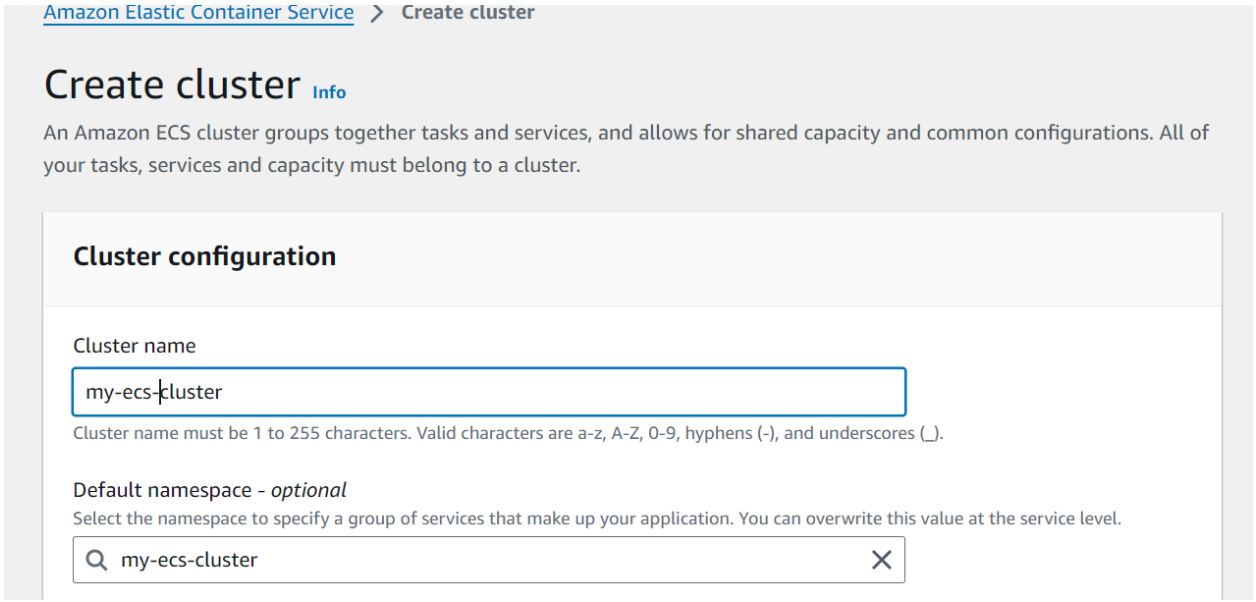


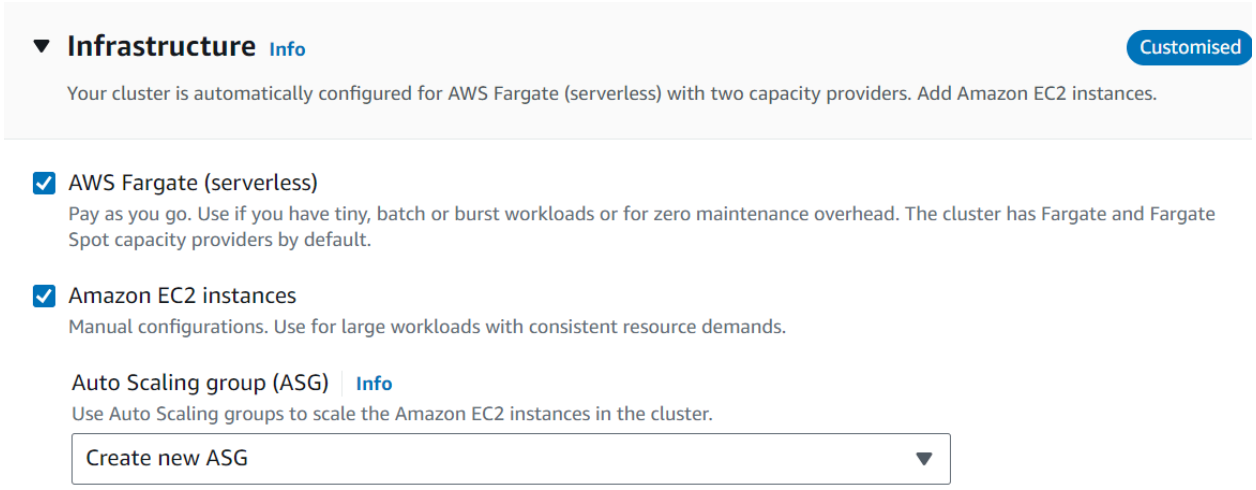
1. Set Up the AWS Environment

- **Log in to AWS Console: Log in to your AWS account.**
- **Navigate to ECS: Go to the AWS Management Console and search for "Elastic Container Service" (ECS).**

2. Create a Cluster

- **Launch ECS Cluster:**
  - **Select "Clusters" from the ECS menu.**
  - **Click on "Create Cluster."**


Amazon Elastic Container Service
Create cluster
Create cluster Info
An Amazon ECS cluster groups together tasks and services, and allows for shared capacity and common configurations. All of your tasks, services and capacity must belong to a cluster.
Cluster configuration
Cluster name
my-ecs-cluster
Cluster name must be 1 to 255 characters. Valid characters are a-z, A-Z, 0-9, hyphens (-), and underscores (_).
Default namespace - optional
Select the namespace to specify a group of services that make up your application. You can overwrite this value at the service level.
my-ecs-cluster


Infrastructure Info
Customised
Your cluster is automatically configured for AWS Fargate (serverless) with two capacity providers. Add Amazon EC2 instances.
AWS Fargate (serverless)
Pay as you go. Use if you have tiny, batch or burst workloads or for zero maintenance overhead. The cluster has Fargate and Fargate Spot capacity providers by default.
Amazon EC2 instances
Manual configurations. Use for large workloads with consistent resource demands.
Auto Scaling group (ASG) Info
Use Auto Scaling groups to scale the Amazon EC2 instances in the cluster.
Create new ASG

Provisioning model

Select a provisioning model for your instances

(•) On-demand
With on-demand instances, you pay for compute capacity by the hour, with no long-term commitments or upfront payments.

( ) Spot
Amazon EC2 Spot instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot instances are available at up to a 90% discount compared to on-demand prices.

Container instance Amazon Machine Image (AMI)

Choose the Amazon ECS-optimised AMI for your instance.

Amazon Linux 2 (kernel 5.10) ▼

EC2 instance type

Choose based on the workloads you plan to run on this cluster.

t2.micro — Free tier eligible ▼
i386, x86_64
1 vCPU 1 GiB memory

Desired capacity

Specify the number of instances to launch in your cluster.

Minimum: 1

Maximum: 2

SSH Key pair

If you do not specify a key pair, you can't connect to the instances via SSH unless you choose an AMI that is configured to allow users another way to log in.

mykey ▼ [↻] Create a new key pair

Root EBS volume size

You can increase the size of the root EBS volume to allow for greater image and container storage.

30

VPC

Use a VPC with public and private subnets. By default, VPCs are created for your AWS account. To create a new VPC, go to the VPC Console.

vpc-0129db4aa535d446a
default

Subnets

Select the subnets where your tasks run. We recommend that you use three subnets for production.

Choose subnets | Clear current selection

subnet-07732c2a81779aa5a
ap-southeast-1a 172.31.32.0/20

subnet-0f0af9cb9f16212c2
ap-southeast-1c 172.31.0.0/20

subnet-00bf90a0af8d6fdc6 public
ap-southeast-1b 172.31.16.0/20

Security group Info

Choose an existing security group or create a new security group.

- (•) Use an existing security group
- ( ) Create a new security group

Security group name

Choose an existing security group.

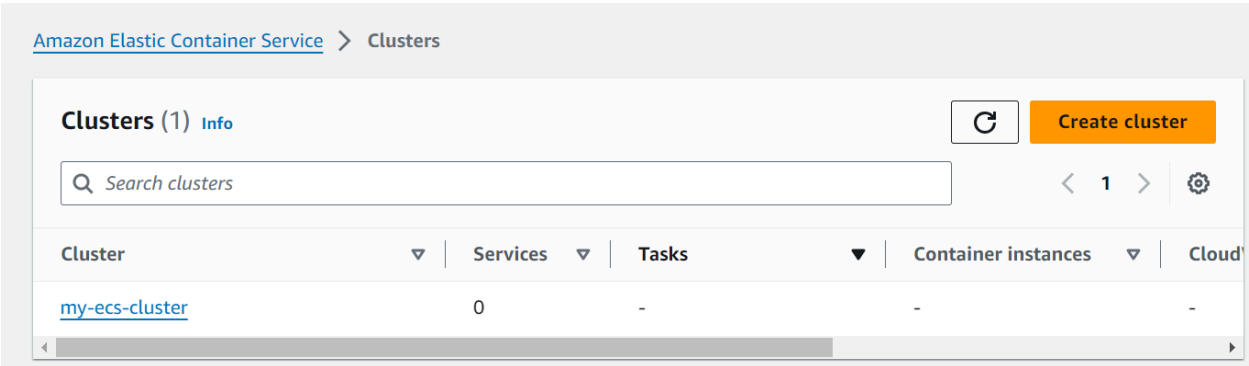
Choose security groups

sg-046c30df1ba69023d
default

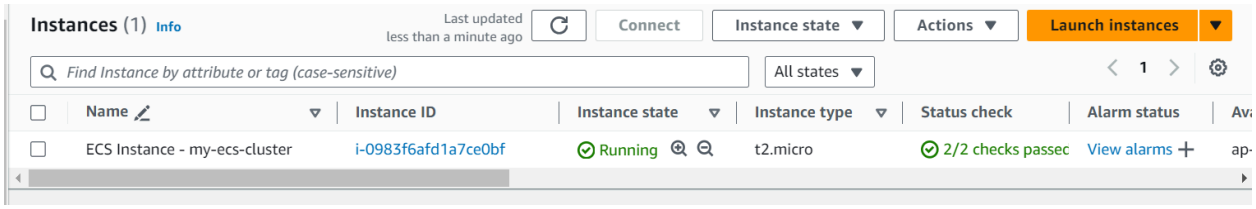
Auto-assign public IP Info

Choose whether to auto-assign a public IP to the Amazon EC2 instances

Turn on

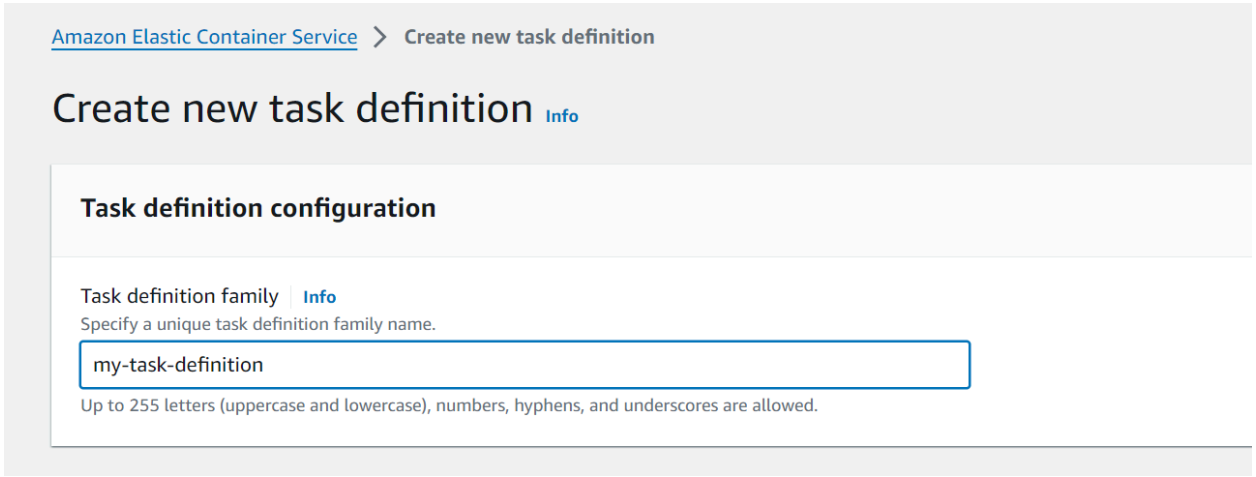


An EC2 instance will be created

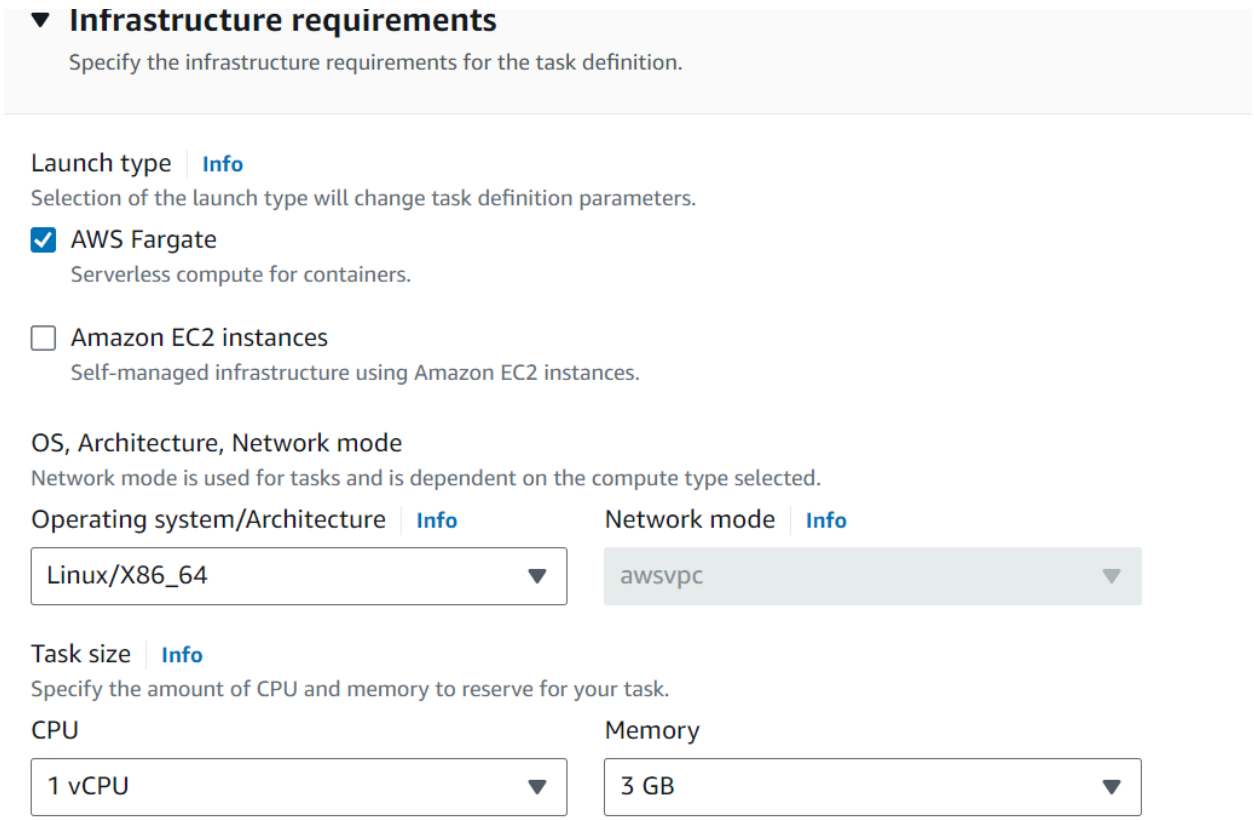


3. Define a Task Definition

- **Create a New Task Definition**:
    - In the ECS menu, select "Task Definitions."
    - Click on "Create new Task Definition."



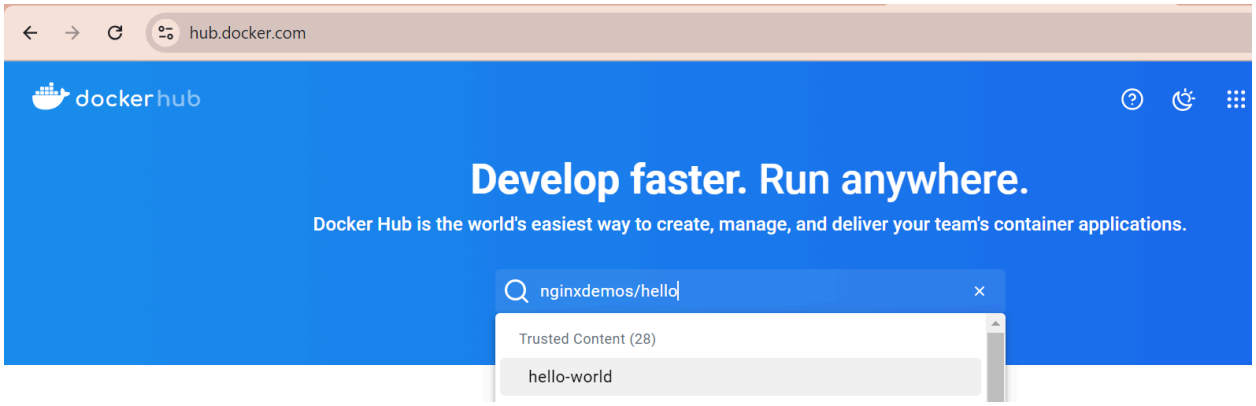
    - Choose "Fargate" as the launch type.



Configure Task Settings:

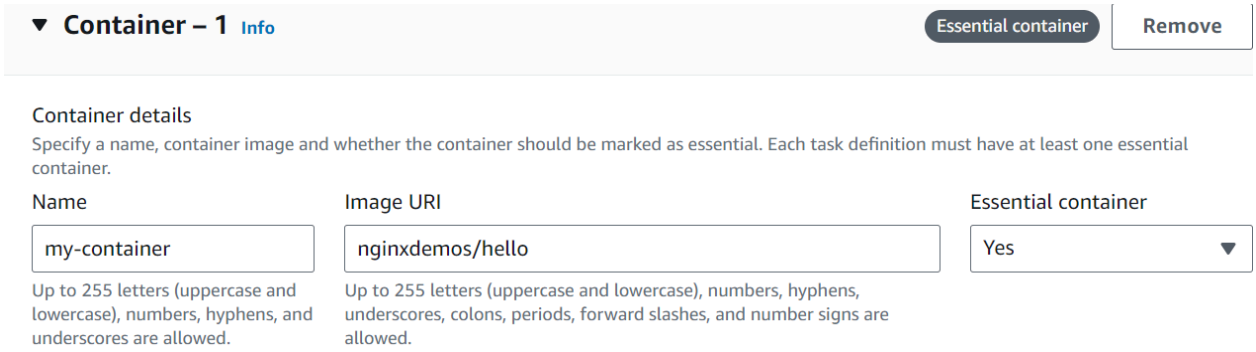
- Specify the task definition name (e.g., Task_Def).
- Set the vCPU and memory according to your requirements. In the diagram, it's shown as 1 vCPU and 3 GB memory.

Docker Hub >

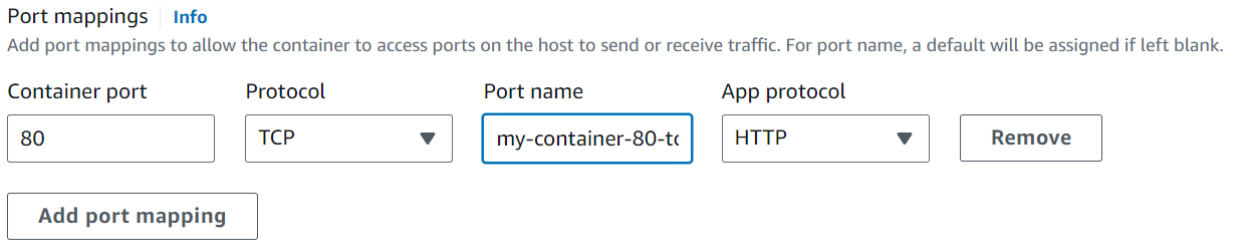


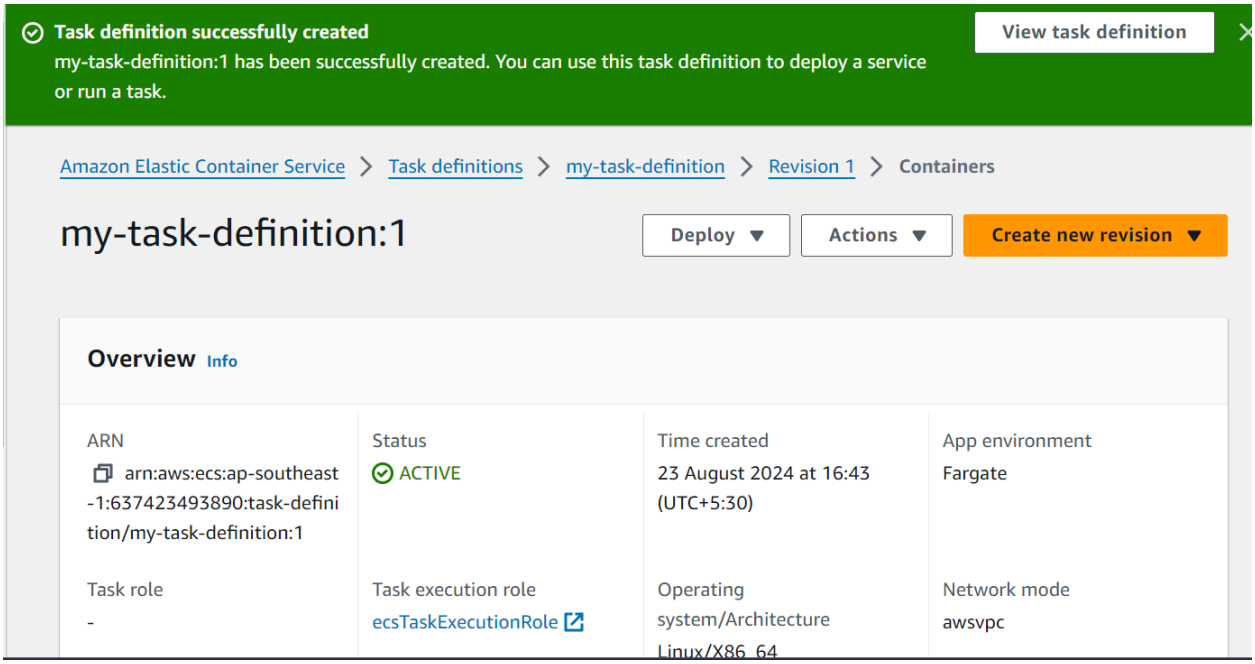
Add Container Definitions:

- Add a container (e.g., Container1) by providing the container name, image (e.g., nginx), and port mapping. Include any environmental variables if necessary.
- Repeat for additional containers if needed.



my-container-80-tcp





4. Create and Configure a Service

- **Service Creation**:
  - Go back to the ECS dashboard and select "Clusters."
  - Choose the cluster you created earlier.
  - Click on "Create" under "Services."

Existing cluster

my-ecs-cluster

▼ **Compute configuration *(advanced)***

Compute options | Info

To ensure task distribution across your compute types, use appropriate compute options.

- ○ Capacity provider strategy
  Specify a launch strategy to distribute your tasks across one or more capacity providers.
- ◉ Launch type
  Launch tasks directly without the use of a capacity provider strategy.

Launch type | Info

Select either managed capacity (Fargate), or custom capacity (EC2 or user-managed, External instances). External instances are registered to your cluster using the ECS Anywhere capability.

FARGATE ▼

Platform version | Info

Specify the platform version on which to run your service.

LATEST ▼

Deployment configuration

Application type | Info

Specify what type of application you want to run.

- ◉ Service
  Launch a group of tasks handling a long-running computing work that can be stopped and restarted. For example, a web application.
- ○ Task
  Launch a standalone task that runs and terminates. For example, a batch job.

Task definition

Select an existing task definition. To create a new task definition, go to Task definitions.

☐ Specify the revision manually

Manually input the revision instead of choosing from the 100 most recent revisions for the selected task definition family.

Family

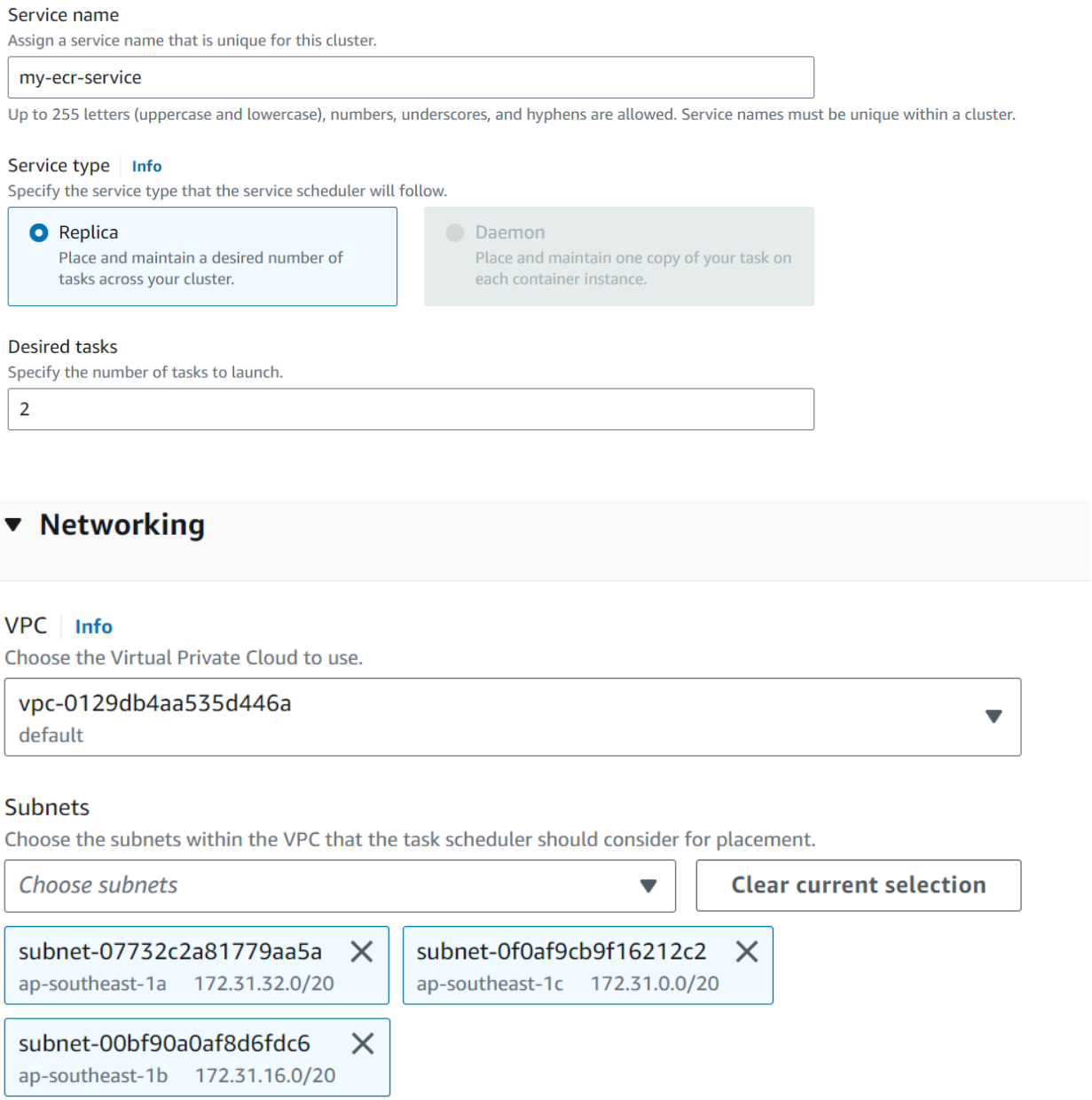
my-task-definition ▼

Revision

1 (LATEST) ▼

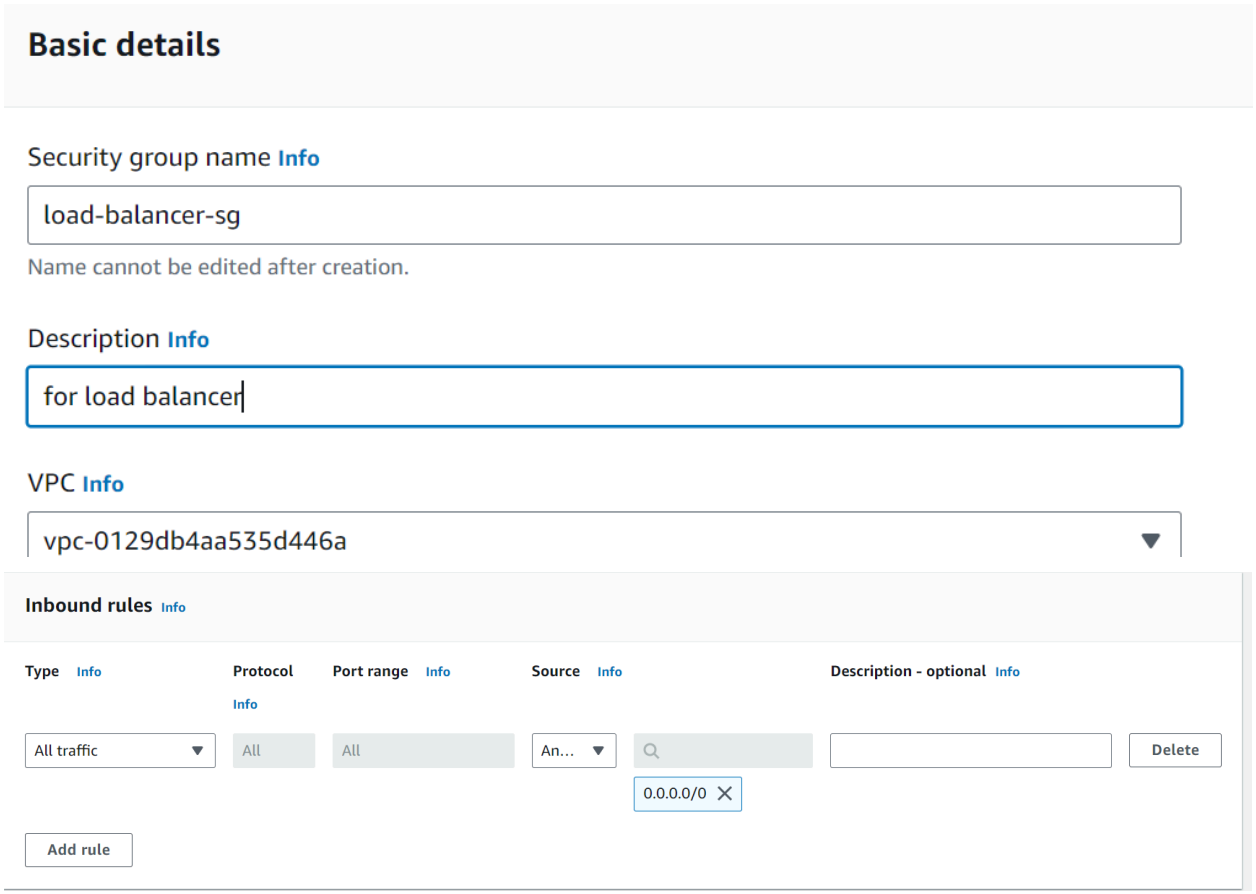
Service Settings:

- **Select the launch type as "Fargate."**
- **Use the task definition created in the previous step (e.g., Task_Def).**
- **Set the number of tasks (for high availability, set at least 2 tasks).**
- **Assign a VPC (Virtual Private Cloud) and subnets as per the diagram.**
- **Choose a load balancer configuration. The diagram shows a load balancer (LB) associated with security group b15-sg-lb**



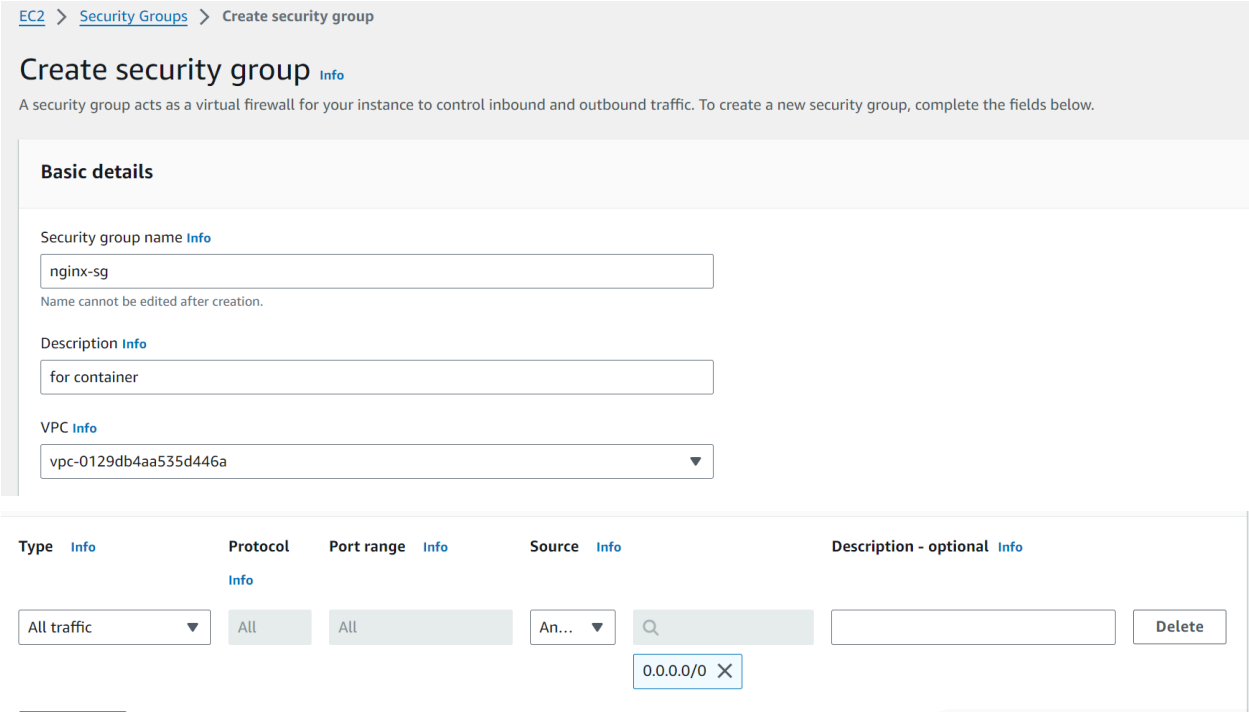
5. Configure Security Groups

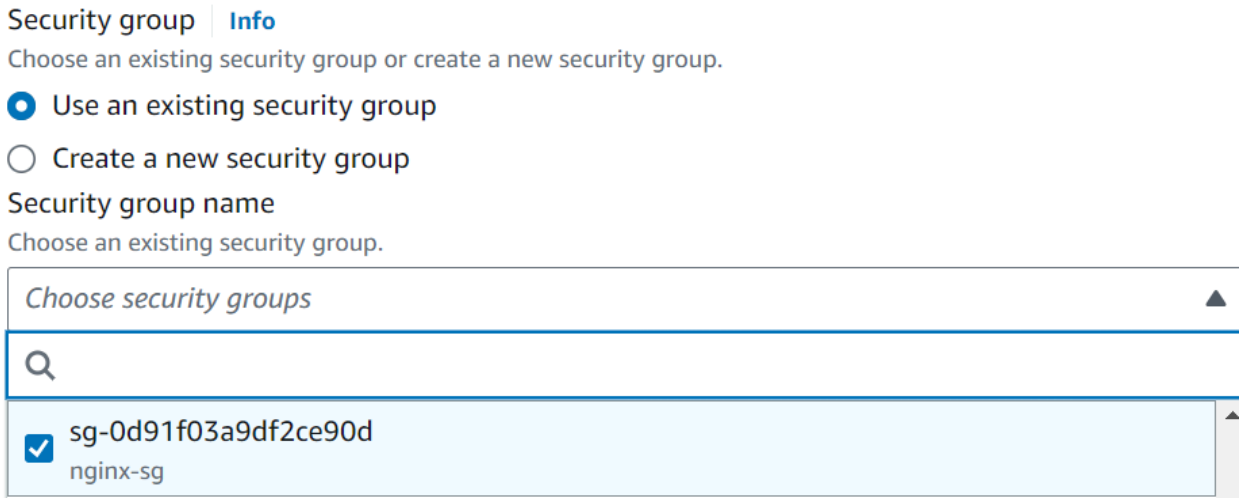
- **Load Balancer Security Group**:
  - Navigate to the "EC2" dashboard and select "Security Groups."
  - Create a new security group (e.g., b15-sg-lb) allowing inbound traffic on necessary ports (e.g., HTTP/HTTPS).
- **Container Security Group**:
  - Create a new security group (e.g., b15-sg-nginx) for your ECS tasks, allowing inbound traffic only from the load balancer.



6. Attach Load Balancer to Service

- **Register Load Balancer with ECS**:
    - In the service creation wizard, select "Application Load Balancer."
    - Choose the load balancer you set up earlier.
    - Define listeners for the ports and target groups as per your ECS service requirements.





Load balancer type | Info

Configure a load balancer to distribute incoming traffic across the tasks running in your service.

Application Load Balancer

Container

The container and port to load balance the incoming traffic to

my-container 80:80

Host port:Container port

Application Load Balancer

Specify whether to create a new load balancer or choose an existing one.

- (•) Create a new load balancer
- ( ) Use an existing load balancer

Load balancer name

Assign a unique name for the load balancer.

my-load-balancer

Health check grace period | Info

1

Listener | Info

Specify the port and protocol that the load balancer will listen for connection requests on.

- (•) Create new listener
- ( ) Use an existing listener
  You need to select an existing load balancer.

Port

80

Protocol

HTTP

Target group | Info

Specify whether to create a new target group or choose an existing one that the load balancer will use to route requests to the tasks in your service.

- (•) Create new target group
- ( ) Use an existing target group

Target group name

ecs-my-ecs-my-ecr-service

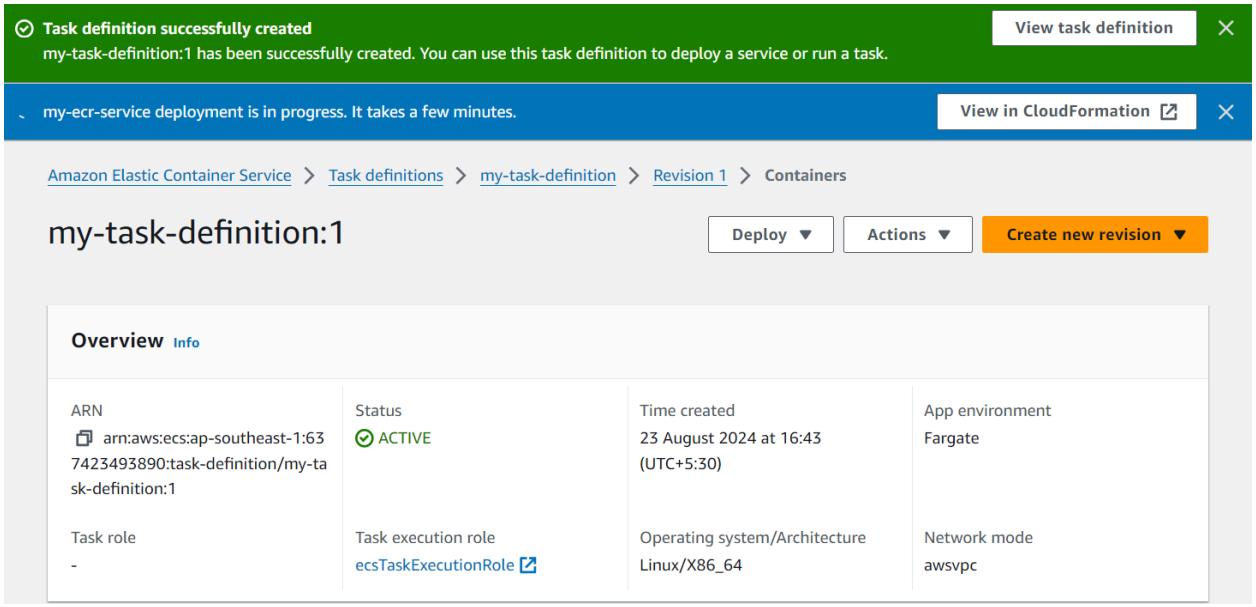
Protocol

HTTP

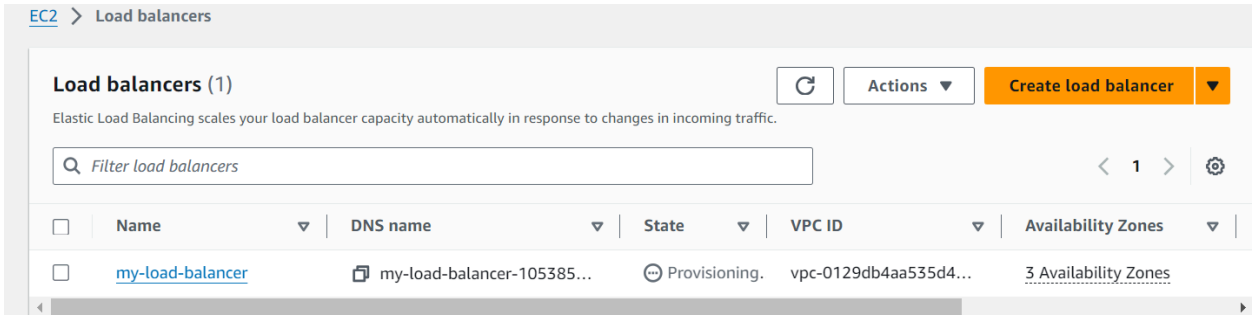
Deregistration delay

The amount of time to wait before the state of a deregistering target changes from draining to unused.

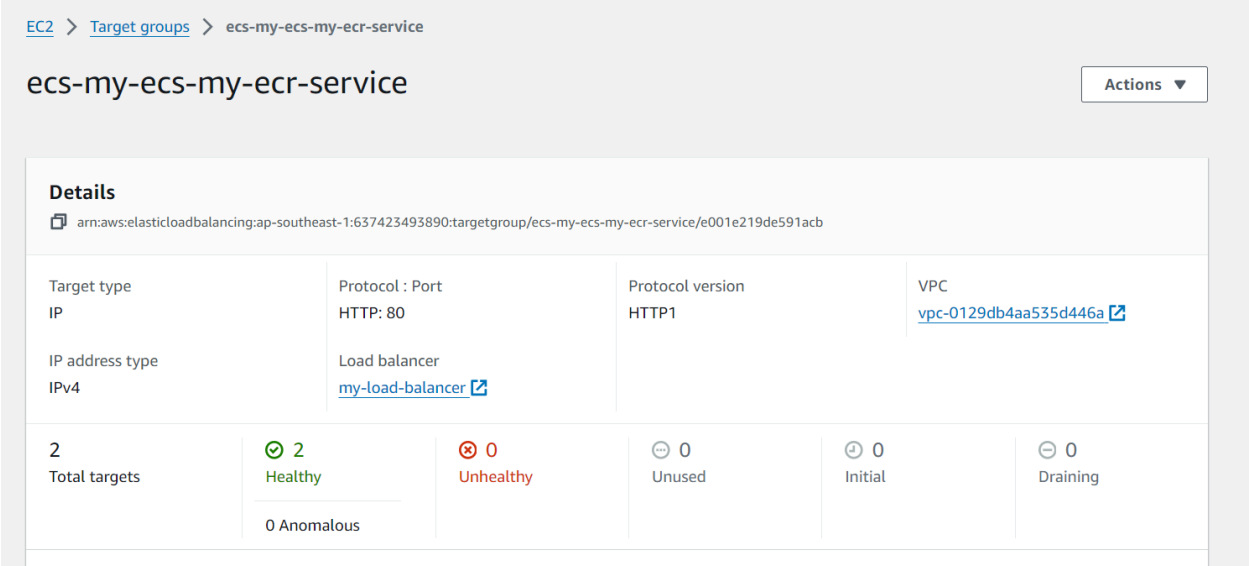
300

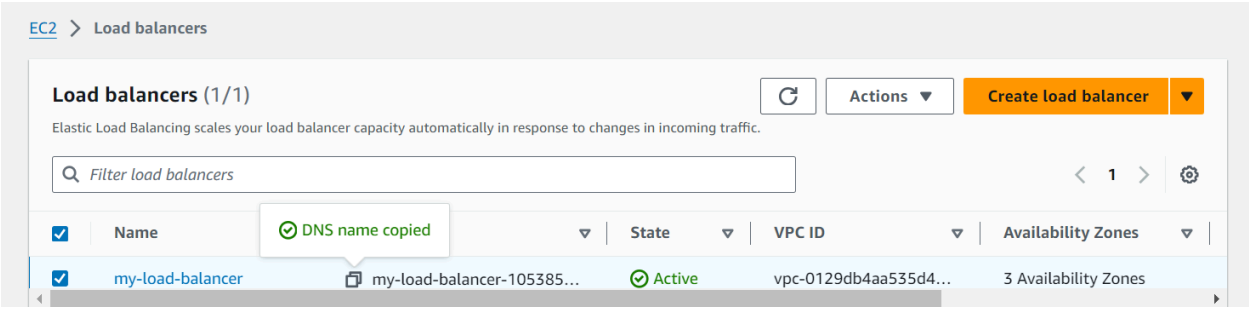


Load balancer will be created



Loadbalancer > Targets > check if the load-balancer is healthy or not





8. Test and Monitor

- **Access the Application**:
  - Once the service is up, you can access the application using the DNS name of the load balancer.
- **Monitor ECS**:
  - Use the ECS dashboard to monitor the health of tasks, scaling, and other metrics.

NGINX
Part of F5

Server address:	172.31.26.85:80
Server name:	ip-172-31-26-85.ap-southeast-1.compute.internal
Date:	23/Aug/2024:11:36:23 +0000
URI:	/

Auto Refresh

Request ID: 37eceb98cf9e02c983206a172082e5df
© F5, Inc. 2020 - 2024

NGINX
Part of F5

Server address:	172.31.32.4:80
Server name:	ip-172-31-32-4.ap-southeast-1.compute.internal
Date:	23/Aug/2024:11:38:25 +0000
URI:	/

Auto Refresh

Request ID: 1ca4234d8d0d0ce111091ef89fa4b67d
© F5, Inc. 2020 - 2024

Date : 30/08/2024

DynamoDB

Date : 02/09/2024

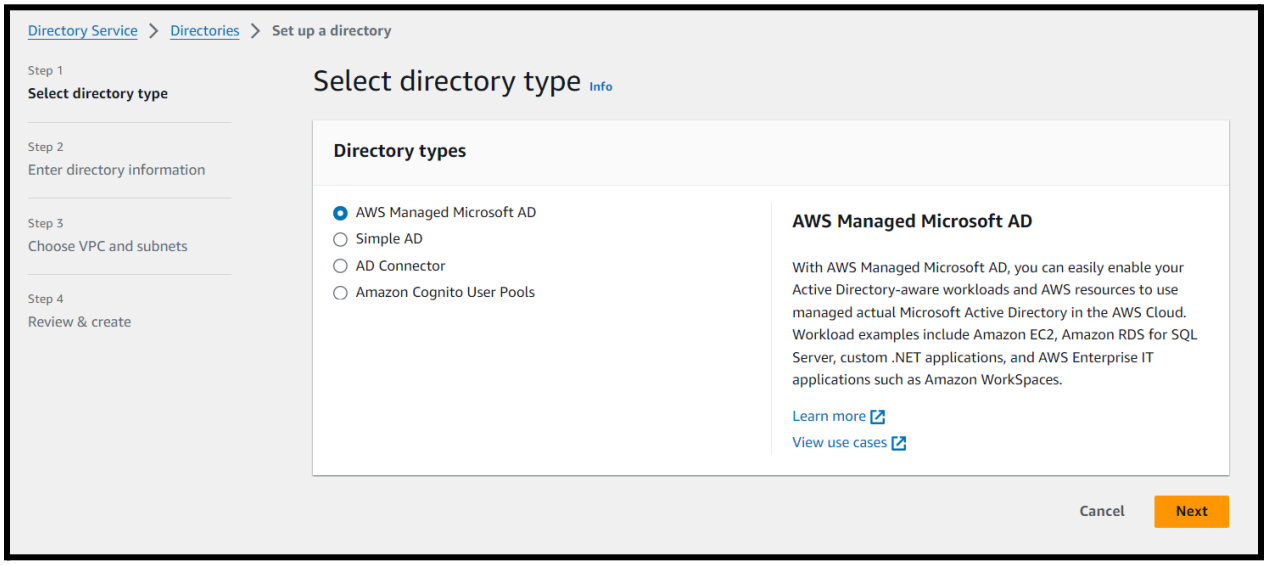
DIRECTORY SERVICES

1. **Navigate to Directory Service:**

- In the AWS Management Console, type **"Directory Service"** in the search bar and select it from the results.

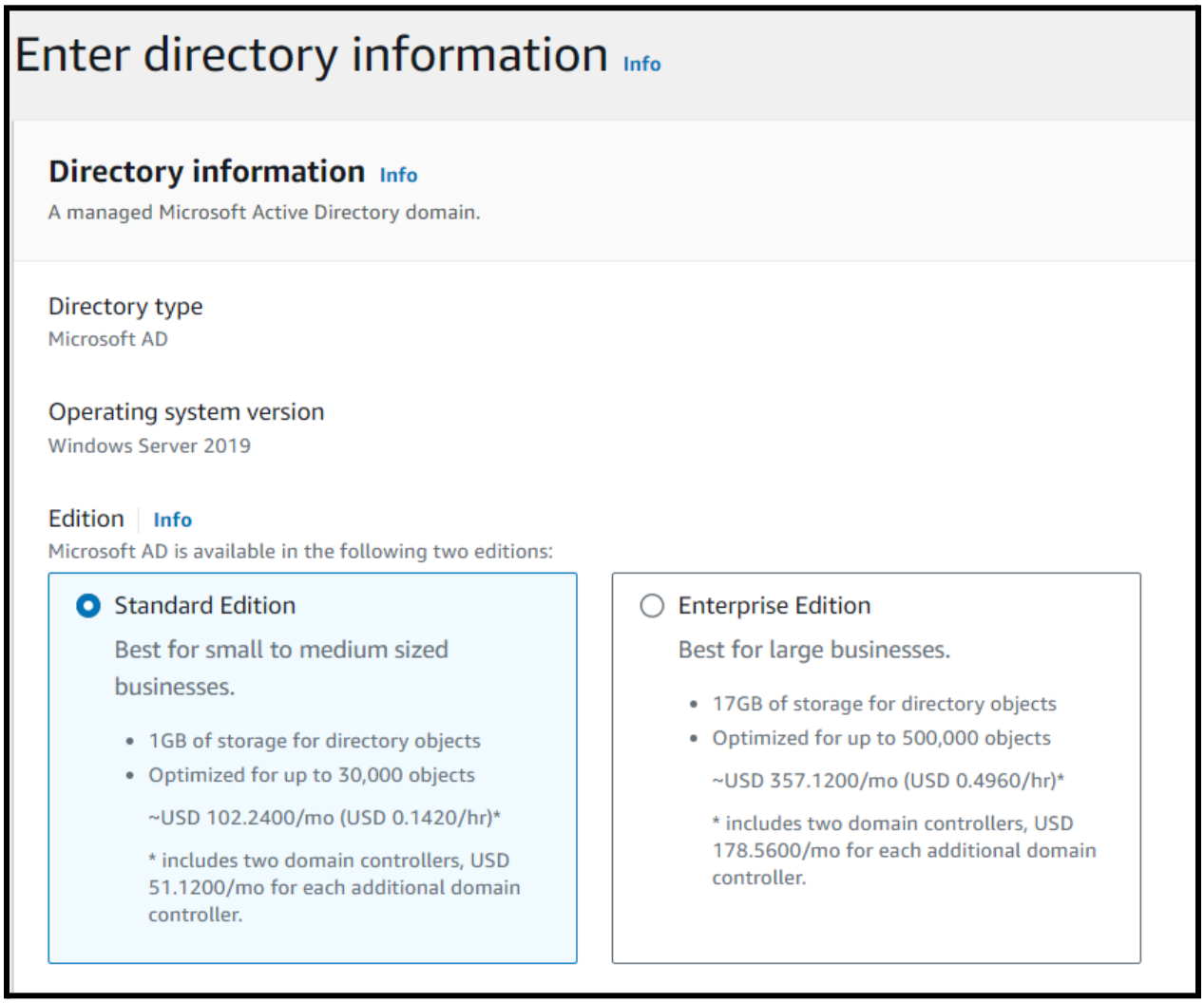
2. **Select Directory Type:**

- Click **"Set up Directory"**.
- AWS offers different types of directories:
    - **AWS Managed Microsoft AD**: A fully managed Microsoft Active Directory.
    - **Simple AD**: A managed directory compatible with Microsoft Active Directory.
    - **AD Connector**: A proxy that connects your existing on-premises Active Directory to AWS.
    - **Cognito User Pools**: For managing users in your applications.
- For most basic use cases, **Microsoft AD** might be suitable.



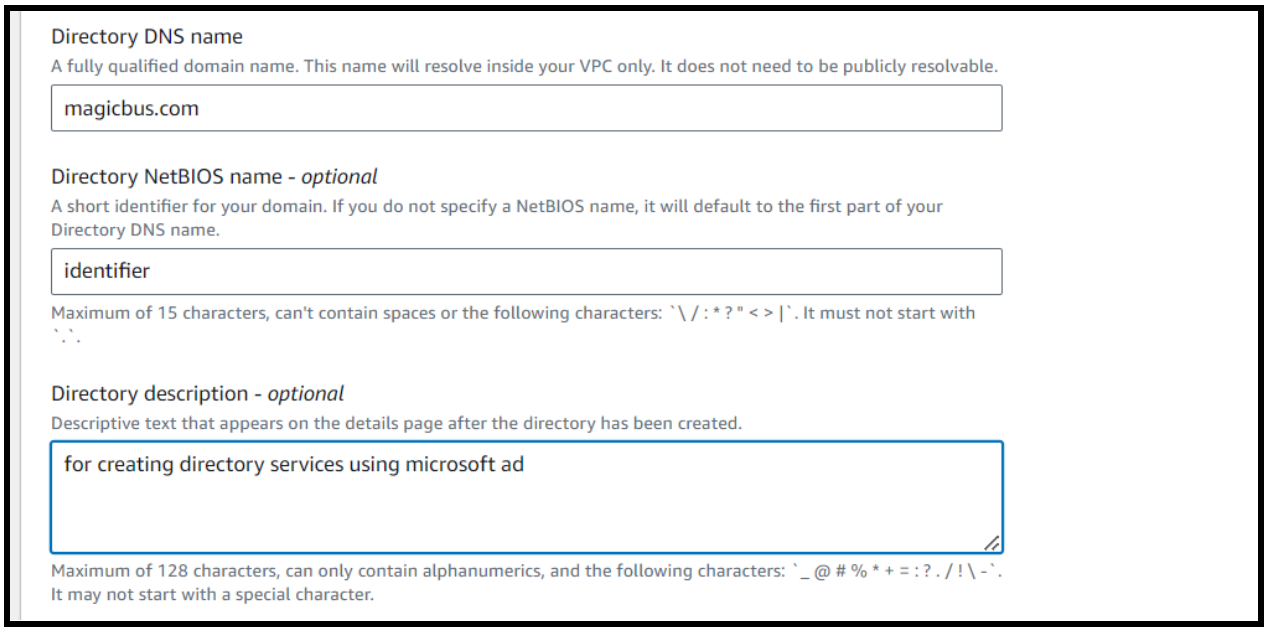
3.Select Edition:

- You can choose between the **Standard Edition** and **Enterprise Edition**. However, be aware that the **Free Tier** offers only limited usage, so check if the edition you select fits within your budget.
- For smaller environments or testing, the **Standard Edition** is usually sufficient.



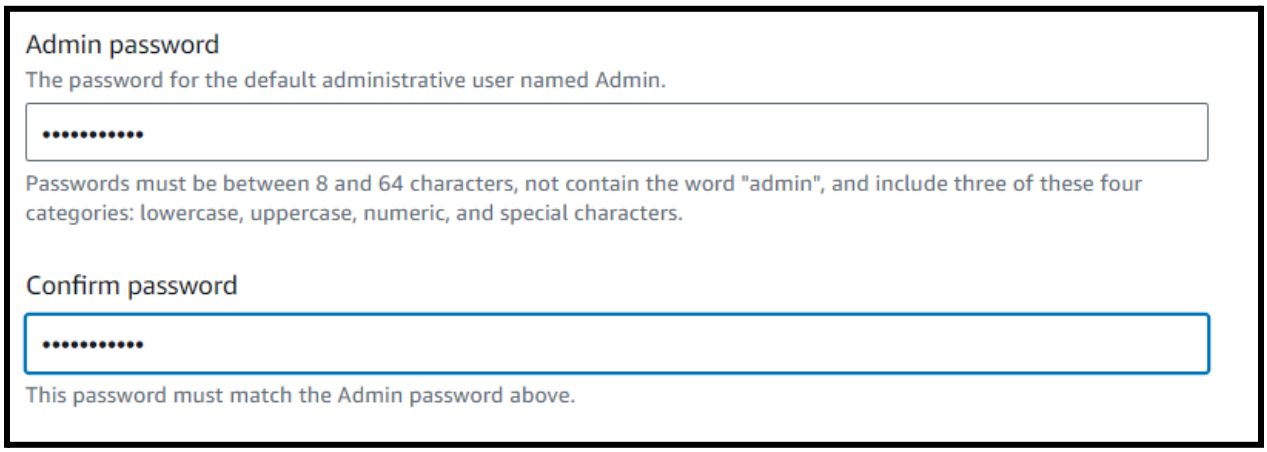
4.Provide Directory Details:

- **Directory DNS name:** This is the fully qualified domain name (FQDN) for your directory, like `example.com`.
- **NetBIOS name:** A shorter name for legacy systems that might not support the full DNS name.
- **Description:** A brief description of your directory.



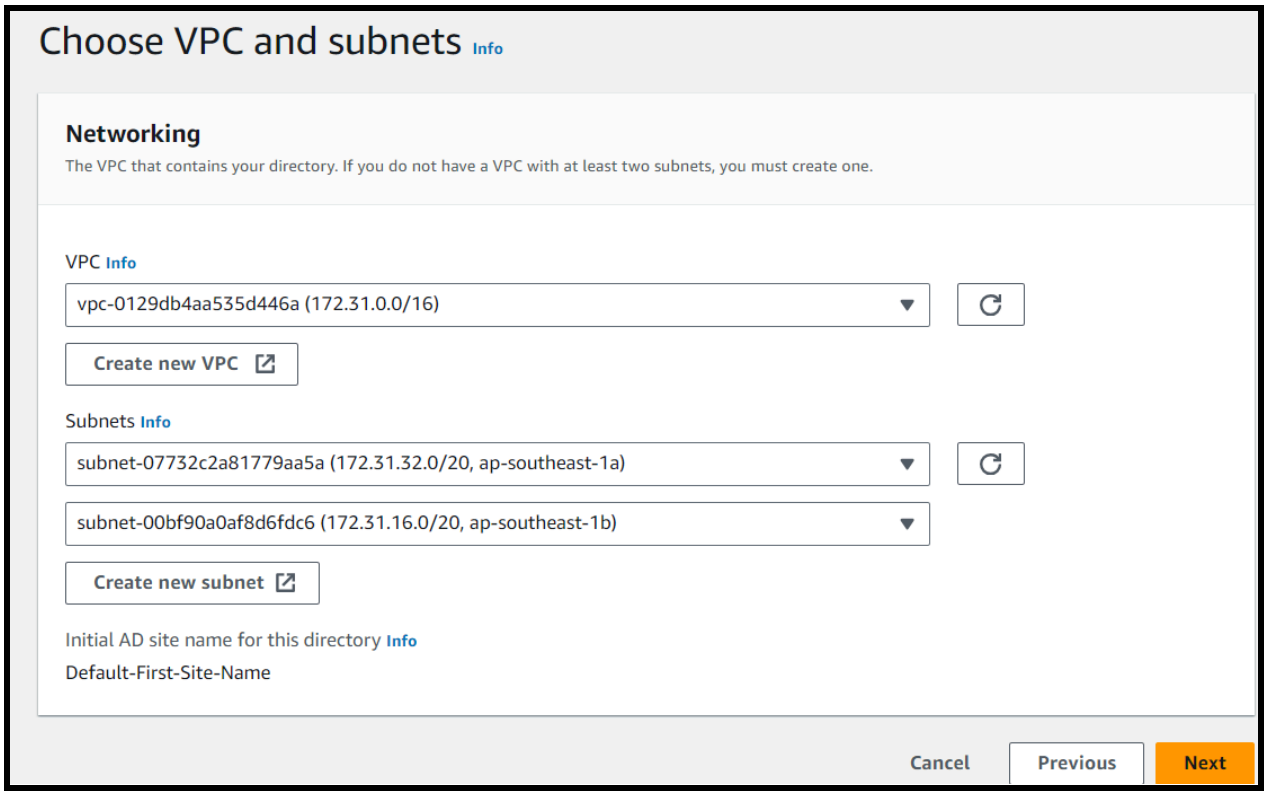
5.Set up Admin Credentials:

- Provide a password for the `Admin` account. This is the account you'll use to manage the directory. Magicbus@123



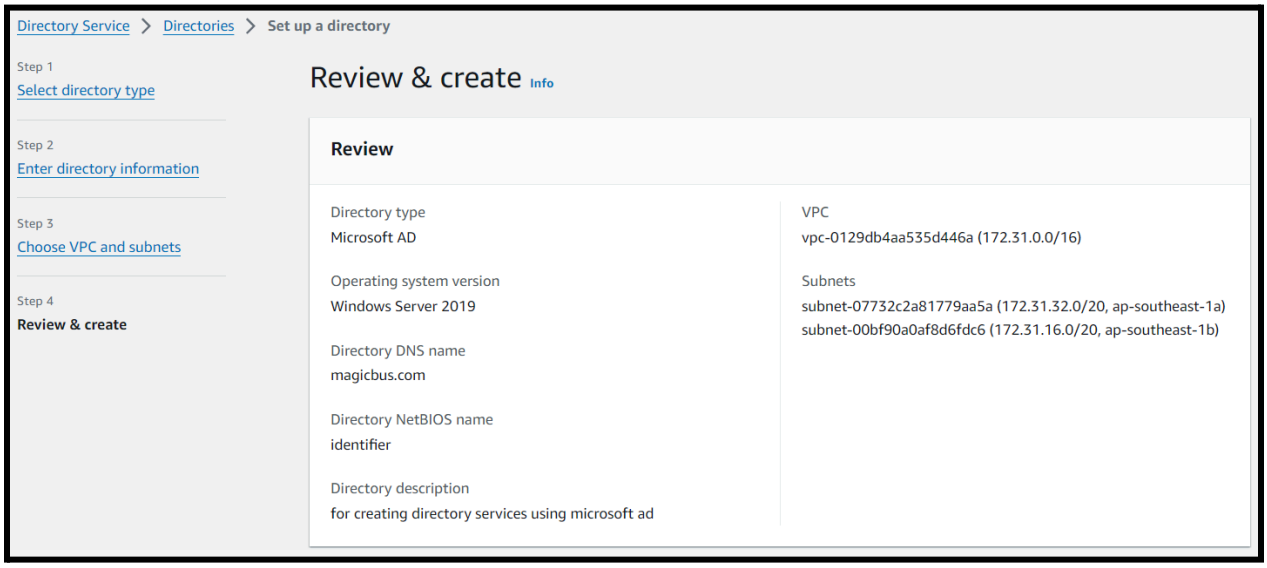
6. VPC and Subnets Selection:

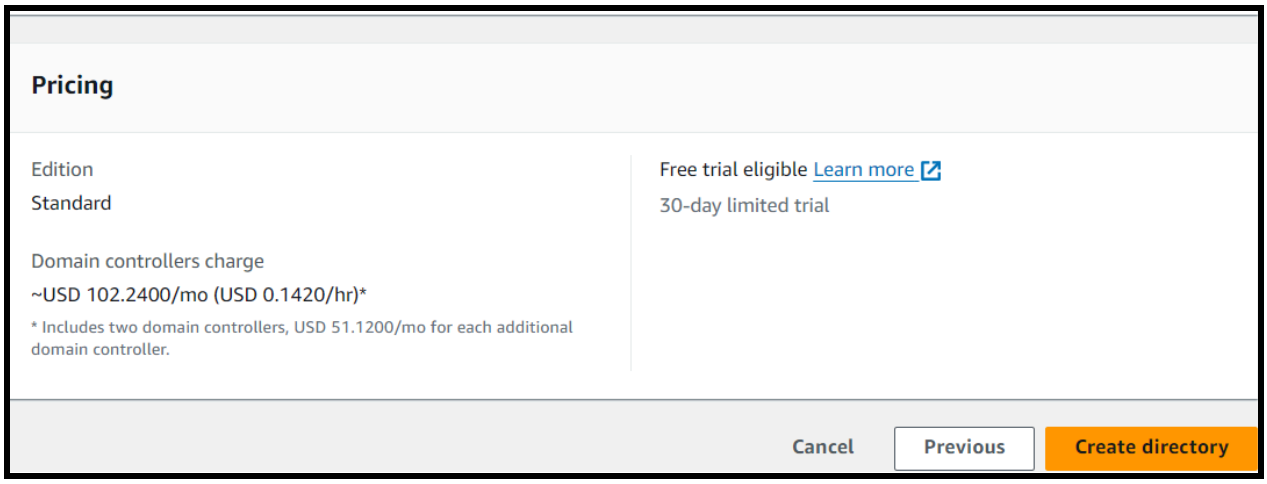
- Select the **Virtual Private Cloud (VPC)** where you want to deploy the directory.
- Choose two subnets in different Availability Zones (AZs) within that VPC. This ensures high availability.

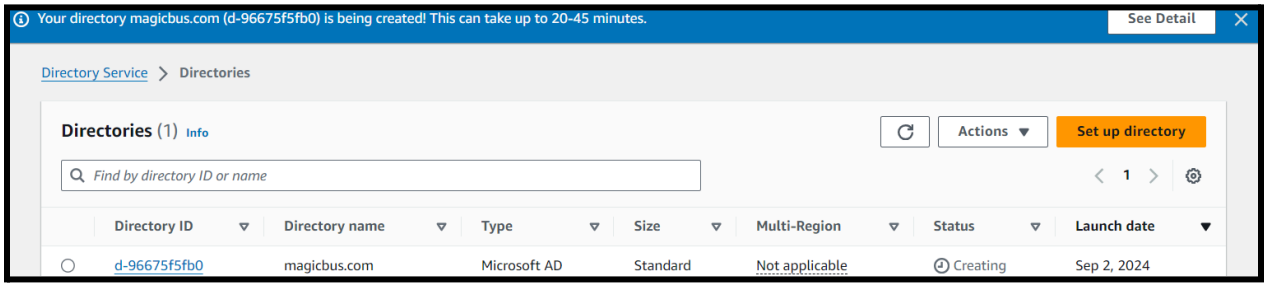


7. Review and Create:

- Review your settings, and then click **"Create Directory"**.
- It may take some time for the directory to be created.

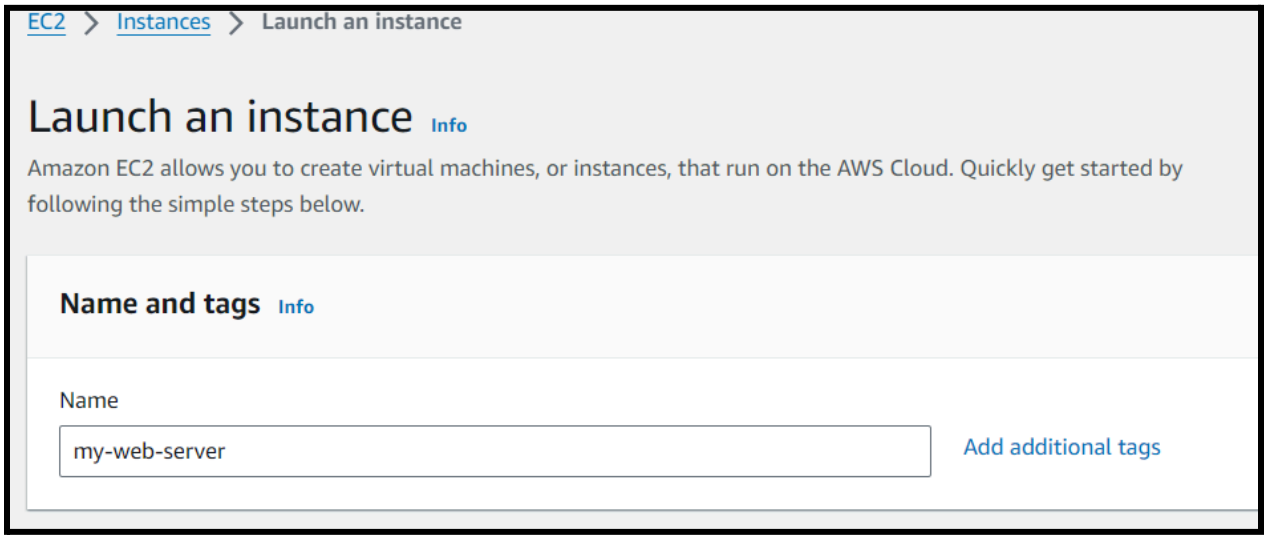






9. Integrate with EC2 Instances (Optional):

- Once the directory is created, you can join Amazon EC2 instances to this directory, enabling them to authenticate using AD credentials.



Application and OS Images (Amazon Machine Image) Info

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

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

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Li

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base — Free tier eligible
ami-09927fda4a30717cd (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Network settings Info

VPC - *required* Info

vpc-0129db4aa535d446a (default)
172.31.0.0/16

Subnet Info

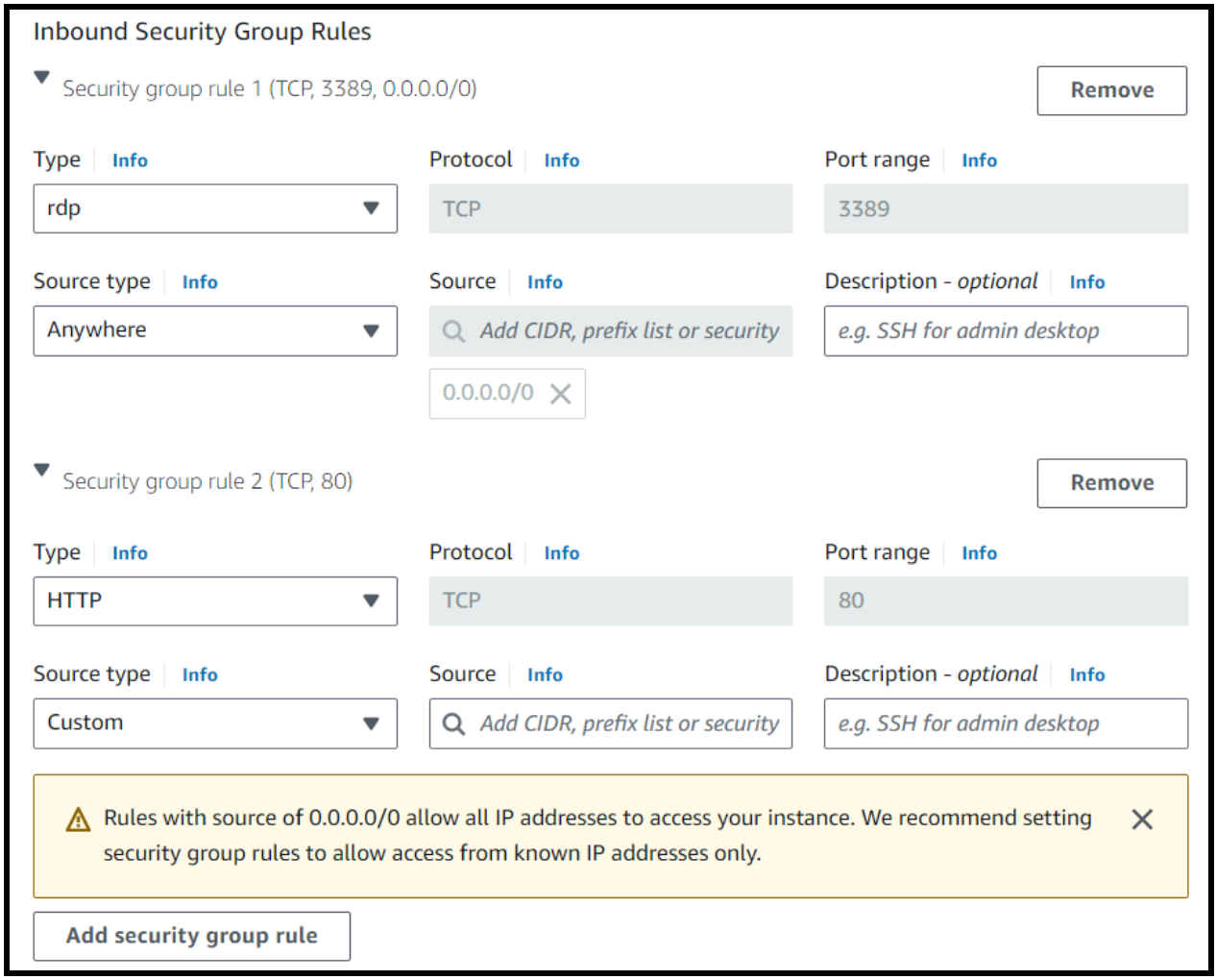
subnet-07732c2a81779aa5a
VPC: vpc-0129db4aa535d446a Owner: 637423493890
Availability Zone: ap-southeast-1a Zone type: Availability Zone
IP addresses available: 4089 CIDR: 172.31.32.0/20)

Create new subnet

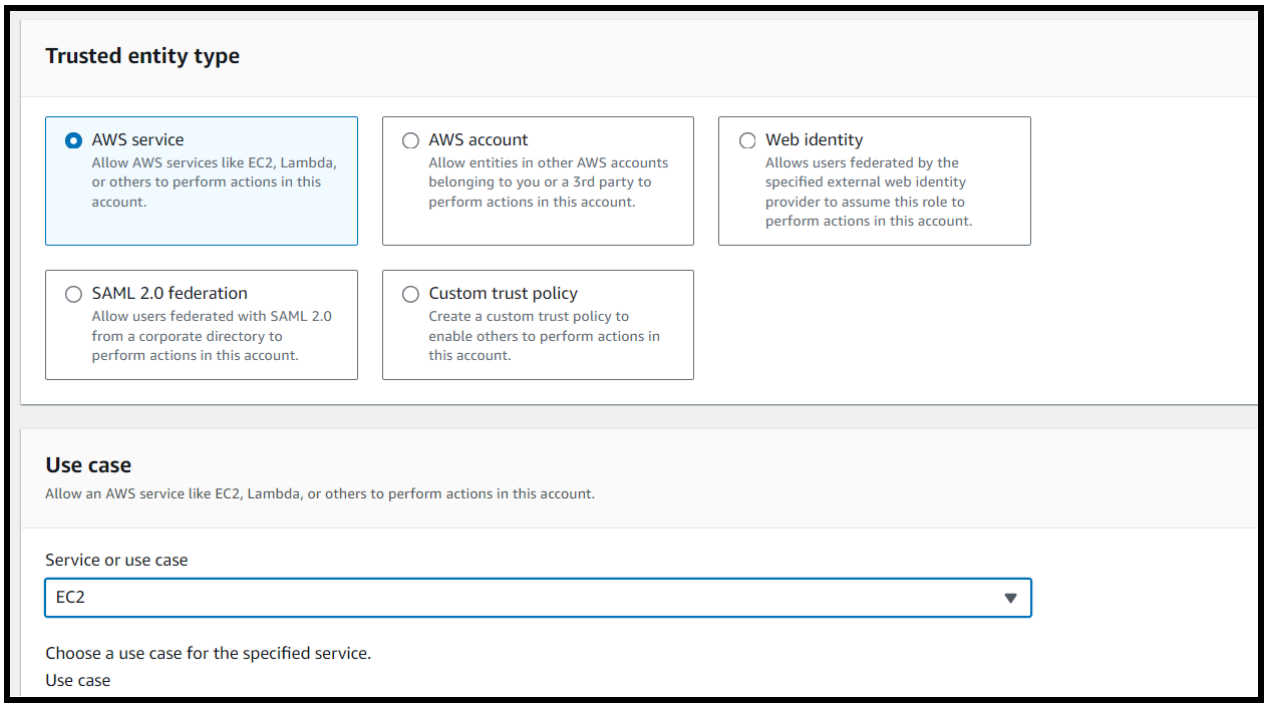
Auto-assign public IP Info

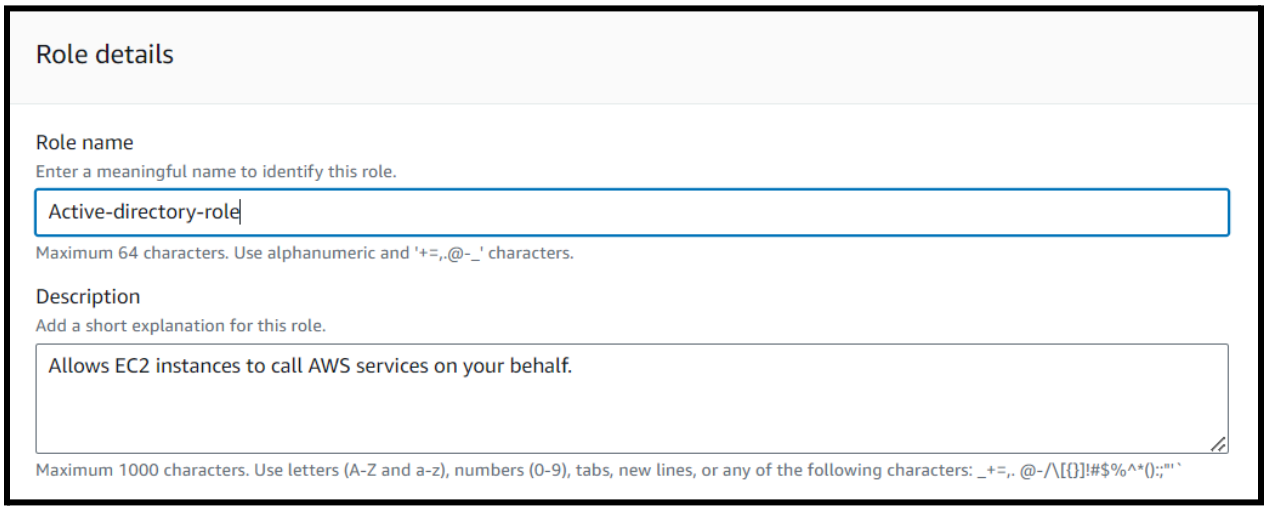
Enable

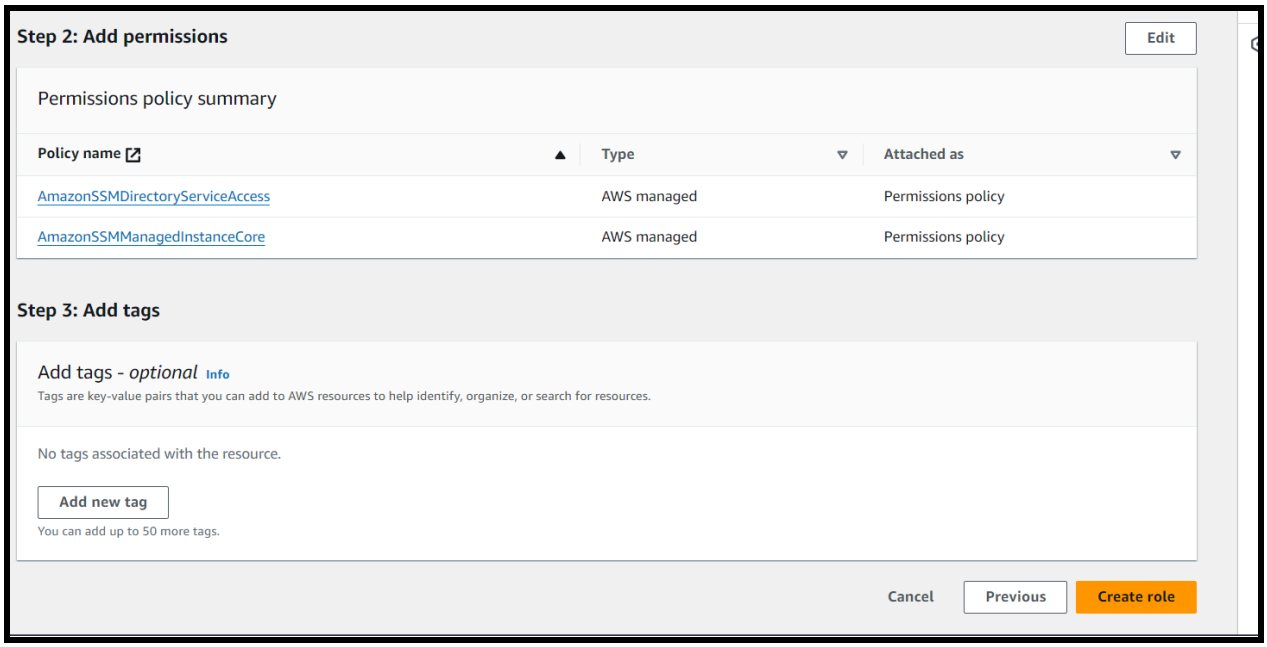
Additional charges apply when outside of free tier allowance

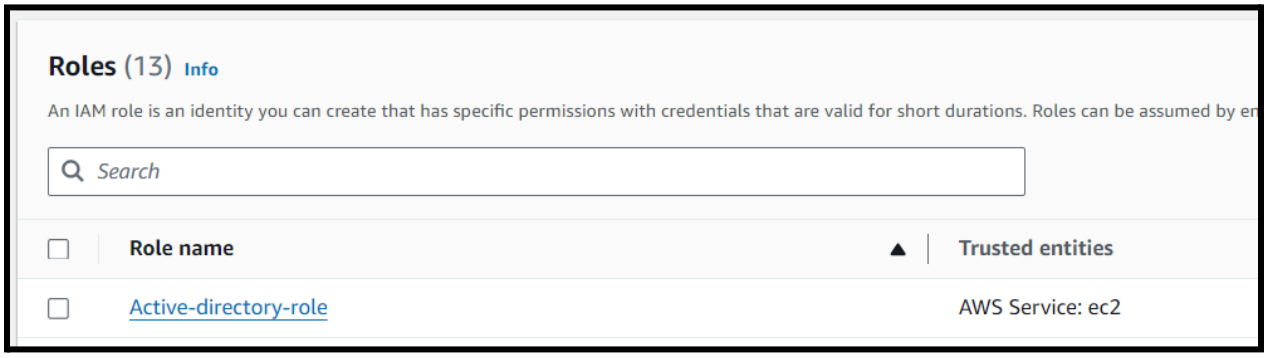


Create role for EC2


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


Role details
Role name
Enter a meaningful name to identify this role.
Active-directory-role
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: _+=,. @-/\[{}]!#$%^*();:"'`

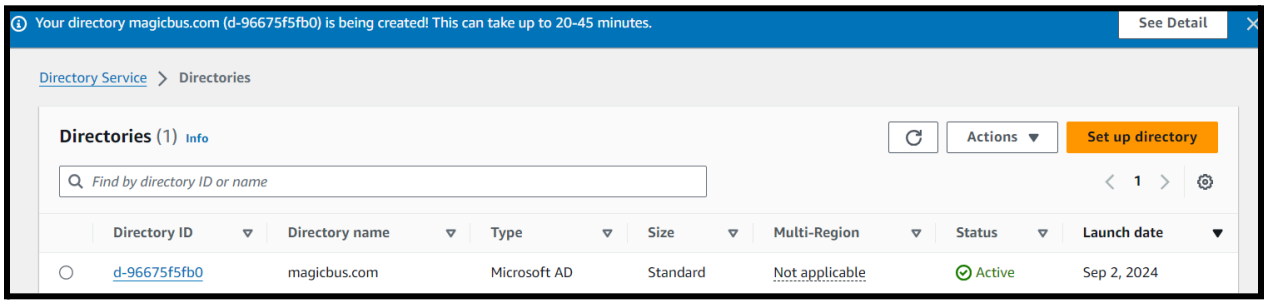




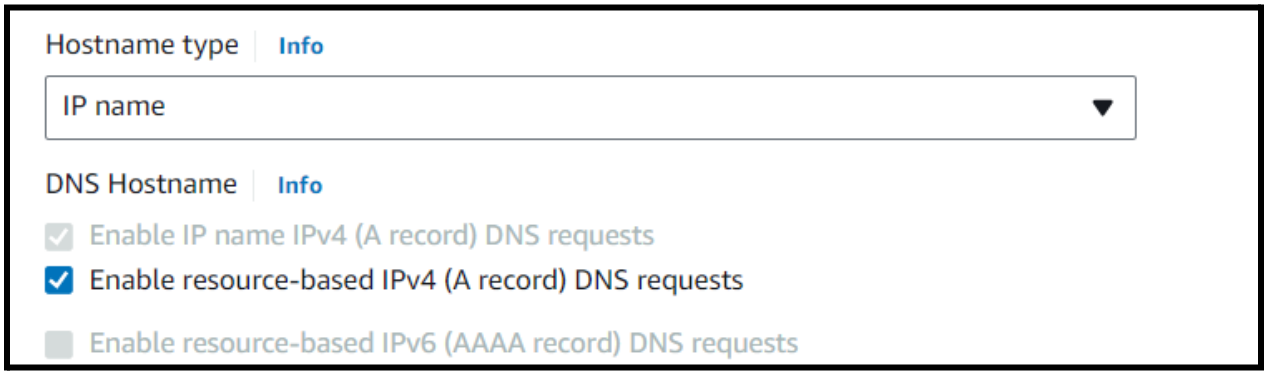
In additional settings of EC2 > attach created IAM role

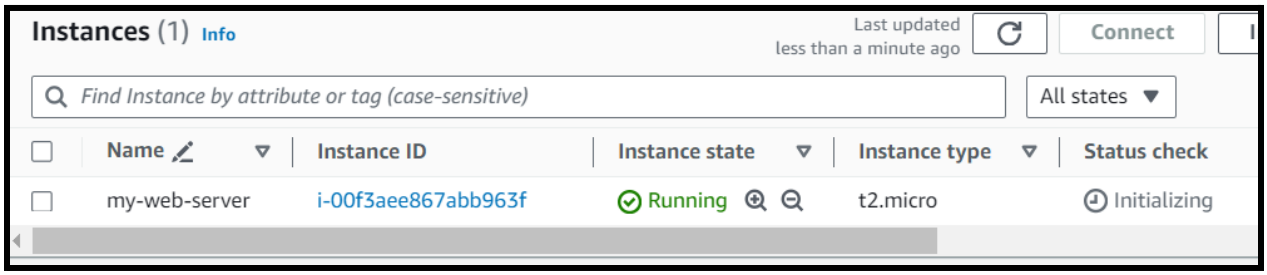
Wait for directory to be created once done > attach it to Domain join directory

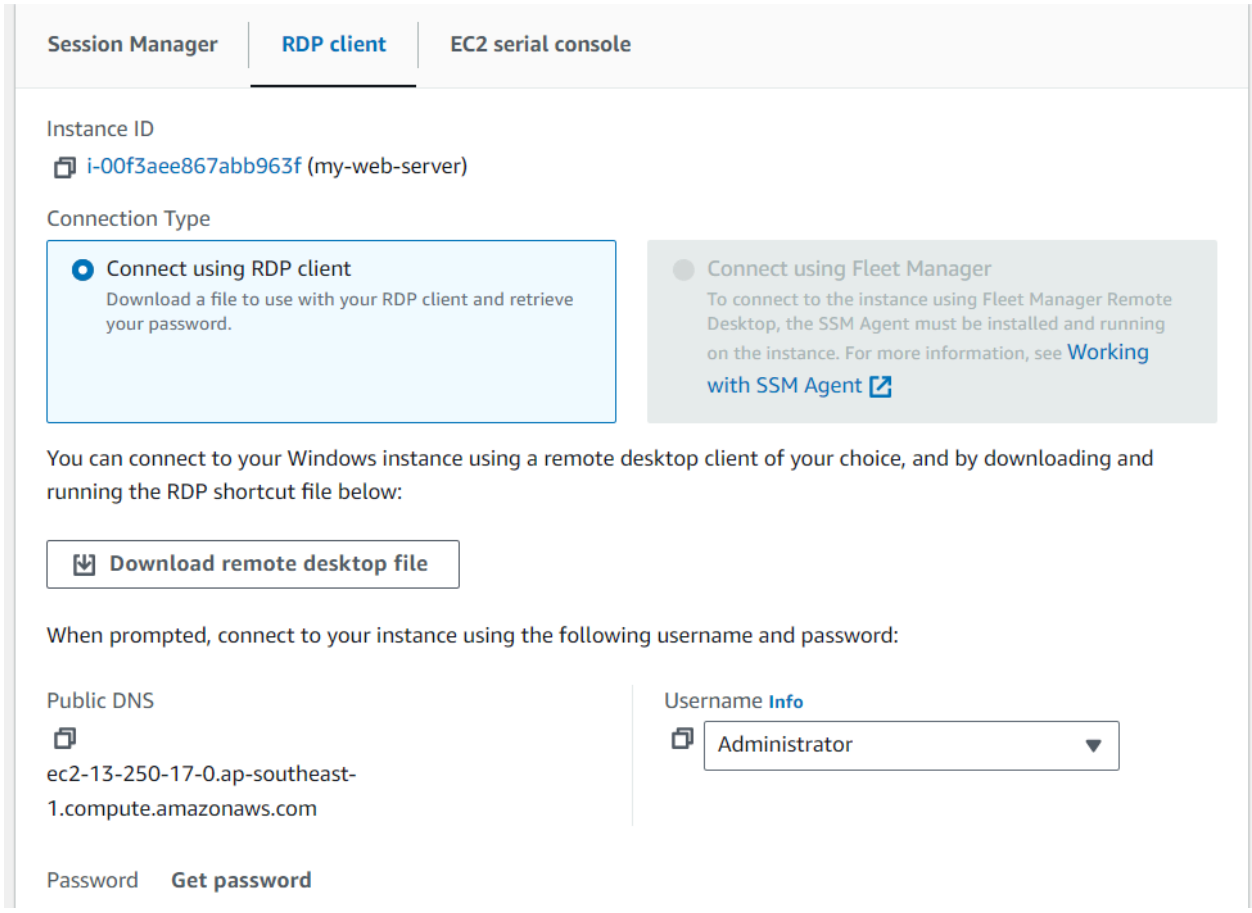
Directory is active now

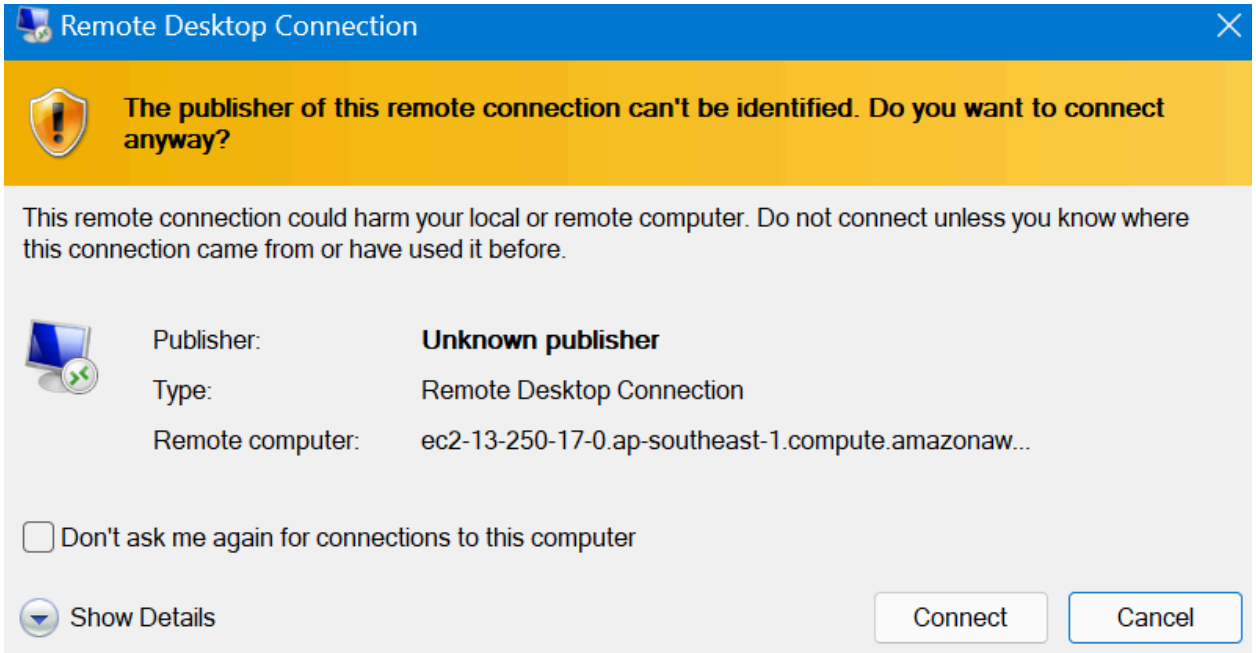


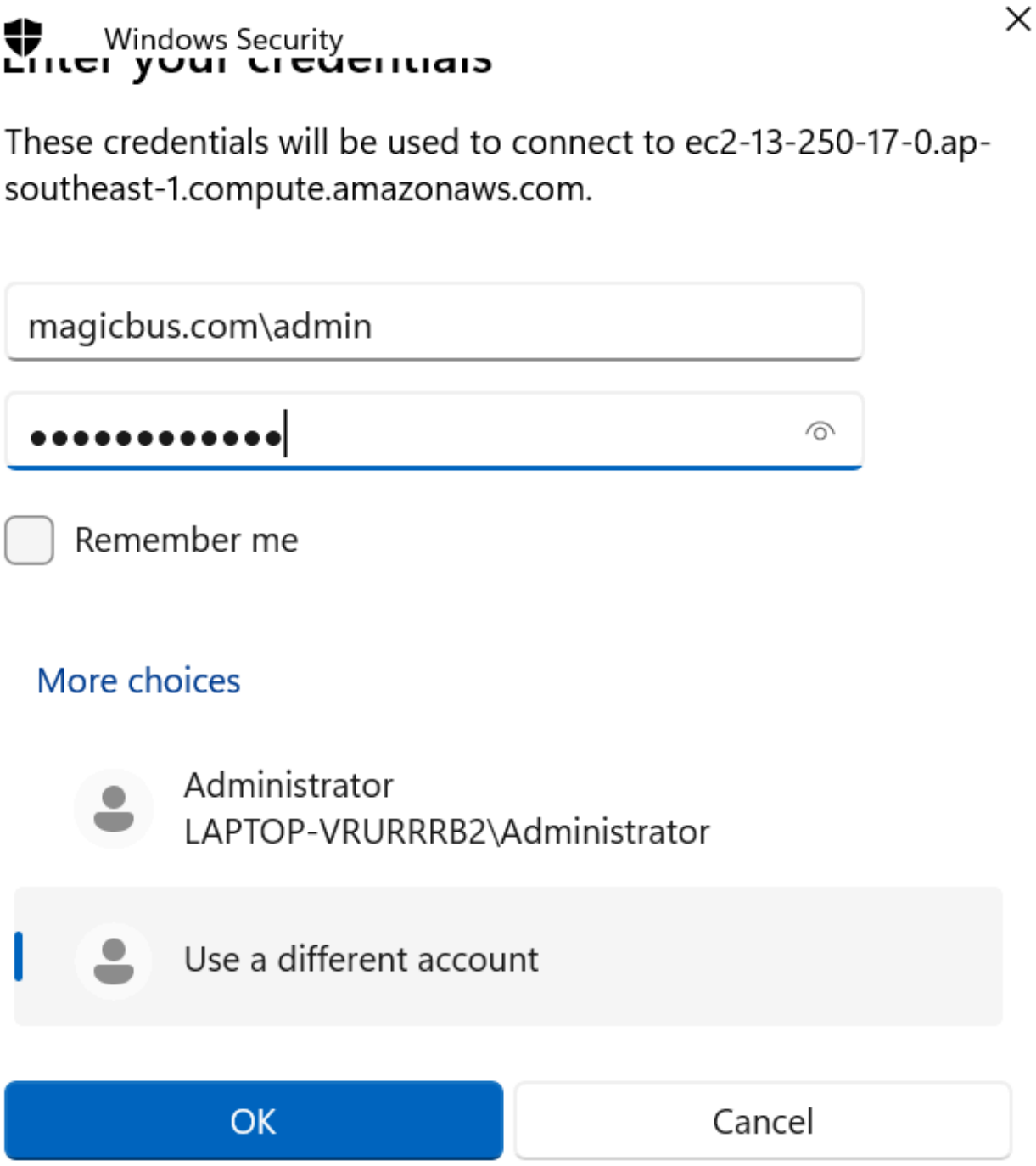
Select directory





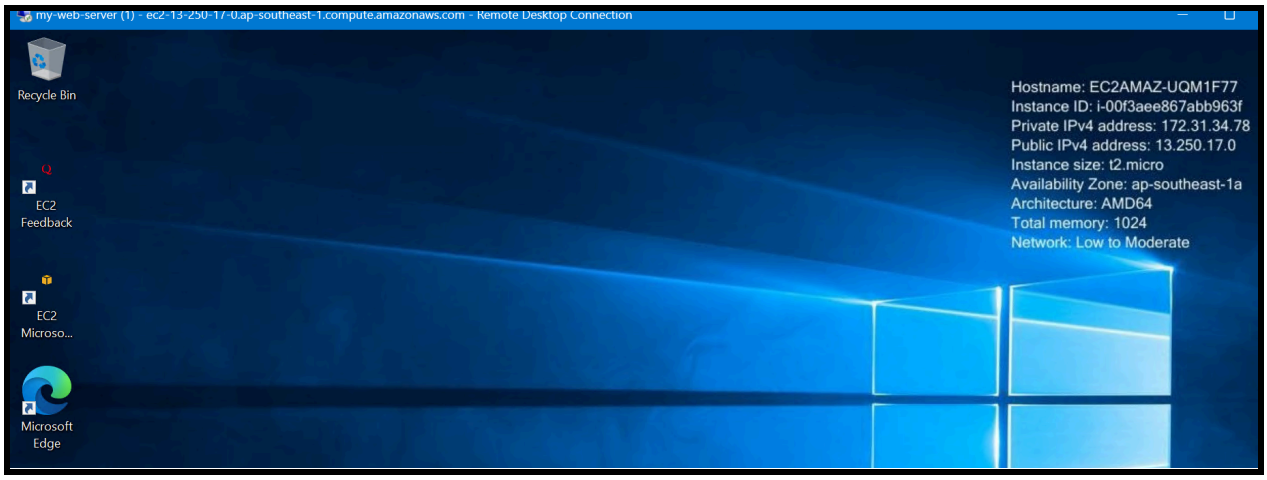

Session Manager
RDP client
EC2 serial console
Instance ID
i-00f3aee867abb963f (my-web-server)
Connection Type
Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see Working with SSM Agent
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:
Download remote desktop file
When prompted, connect to your instance using the following username and password:
Public DNS
ec2-13-250-17-0.ap-southeast-1.compute.amazonaws.com
Username Info
Administrator
Password
Get password

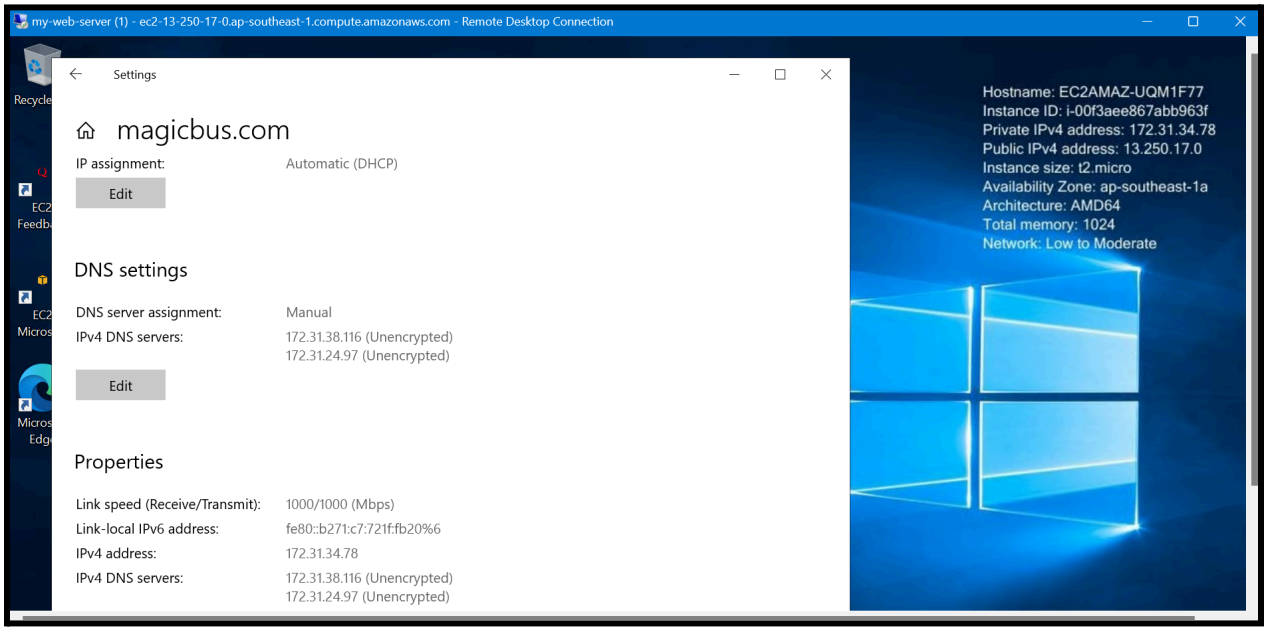

Remote Desktop Connection
The publisher of this remote connection can't be identified. Do you want to connect anyway?
This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.
Publisher:
Unknown publisher
Type:
Remote Desktop Connection
Remote computer:
ec2-13-250-17-0.ap-southeast-1.compute.amazonaw...
Don't ask me again for connections to this computer
Show Details
Connect
Cancel



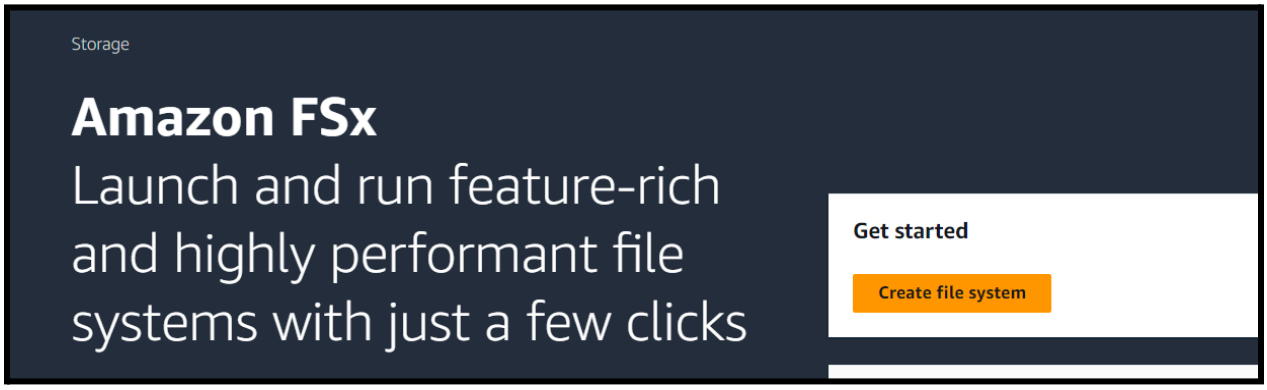
10. Use AWS Managed Microsoft AD:

- With the directory set up, you can manage it through standard AD tools such as the **Active Directory Users and Computers (ADUC)** or **Group Policy Management Console (GPMC)**, by connecting through a domain-joined EC2 instance.


my-web-server (1) - ec2-13-250-17-0.ap-southeast-1.compute.amazonaws.com - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Microso...
Microsoft Edge
Hostname: EC2AMAZ-UQM1F77
Instance ID: i-00f3aee867abb963f
Private IPv4 address: 172.31.34.78
Public IPv4 address: 13.250.17.0
Instance size: t2.micro
Availability Zone: ap-southeast-1a
Architecture: AMD64
Total memory: 1024
Network: Low to Moderate


my-web-server (1) - ec2-13-250-17-0.ap-southeast-1.compute.amazonaws.com - Remote Desktop Connection
Settings
magicbus.com
IP assignment:
Automatic (DHCP)
Edit
DNS settings
DNS server assignment:
Manual
IPv4 DNS servers:
172.31.38.116 (Unencrypted)
172.31.24.97 (Unencrypted)
Edit
Properties
Link speed (Receive/Transmit):
1000/1000 (Mbps)
Link-local IPv6 address:
fe80::b271:c7:721f:fb20%6
IPv4 address:
172.31.34.78
IPv4 DNS servers:
172.31.38.116 (Unencrypted)
172.31.24.97 (Unencrypted)
Hostname: EC2AMAZ-UQM1F77
Instance ID: i-00f3aee867abb963f
Private IPv4 address: 172.31.34.78
Public IPv4 address: 13.250.17.0
Instance size: t2.micro
Availability Zone: ap-southeast-1a
Architecture: AMD64
Total memory: 1024
Network: Low to Moderate

FILE STORAGE EXTENSION (FSx)

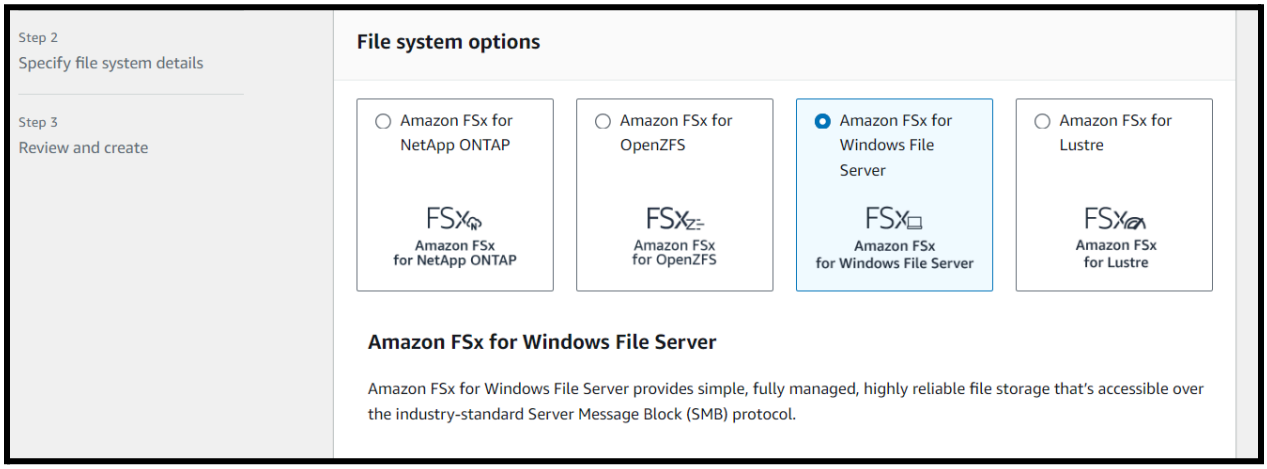


Choose Your File System:

- Click **"Create file system"**..

4. Choose File System Type:

- Select **"Amazon FSx for Windows File Server"**.



5. Configure File System Settings:

File System Deployment:

- **Deployment Type:** Choose between **Multi-AZ** (high availability across two Availability Zones) or **Single-AZ** (lower cost, but with single AZ redundancy). For cost savings, you may prefer **Single-AZ**.

Storage Capacity:

- **Storage Capacity:** Choose the minimum storage capacity that meets your needs (starting from 32 GiB). Smaller capacity helps manage costs.

Throughput Capacity:

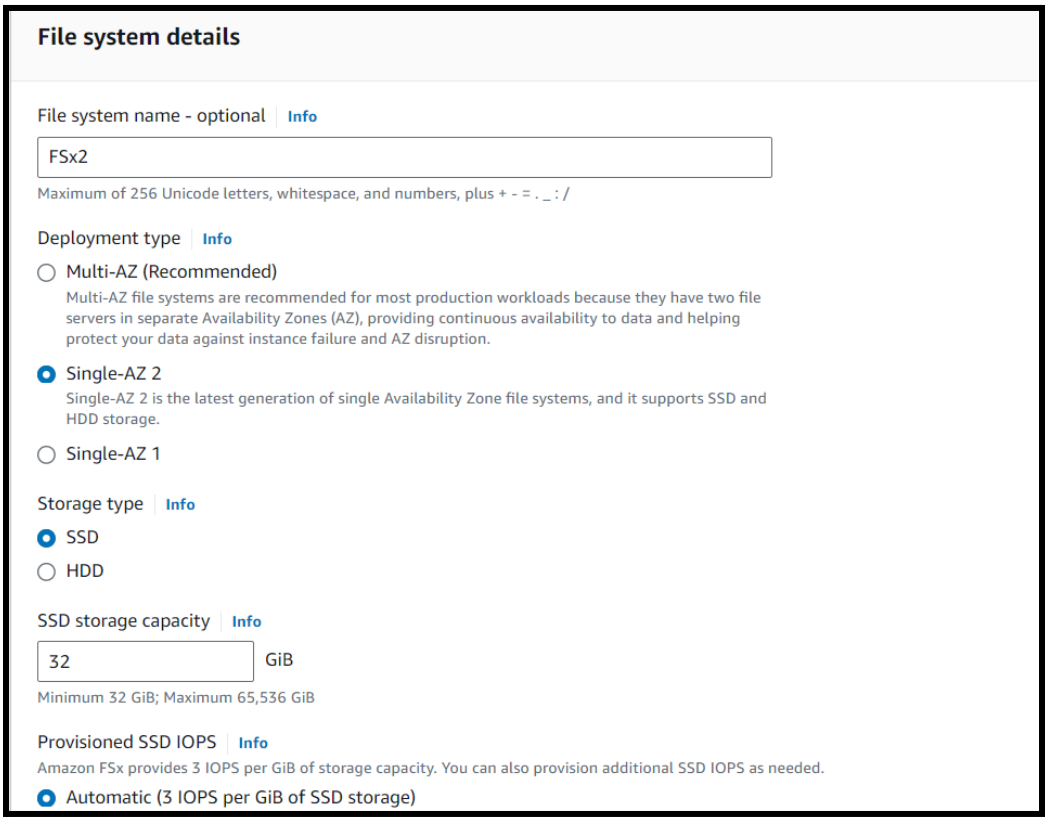
- **Throughput Capacity:** Select the throughput level. The default is often sufficient, but you can choose lower throughput to save costs.

Automatic Backups:

- **Automatic Backups:** Enable or disable automatic daily backups. If backups aren't essential, disabling them can reduce costs.
- **Backup Retention Period:** Set the retention period for your backups (e.g., 7 days).

Windows Authentication:

- **Self-Managed AD or AWS Managed AD:** Choose your authentication method. For integration with an existing AD environment, choose **Self-managed**. If you don't have an AD, you can opt for **AWS Managed AD** (additional cost) or use the built-in simple AD (limited in functionality).



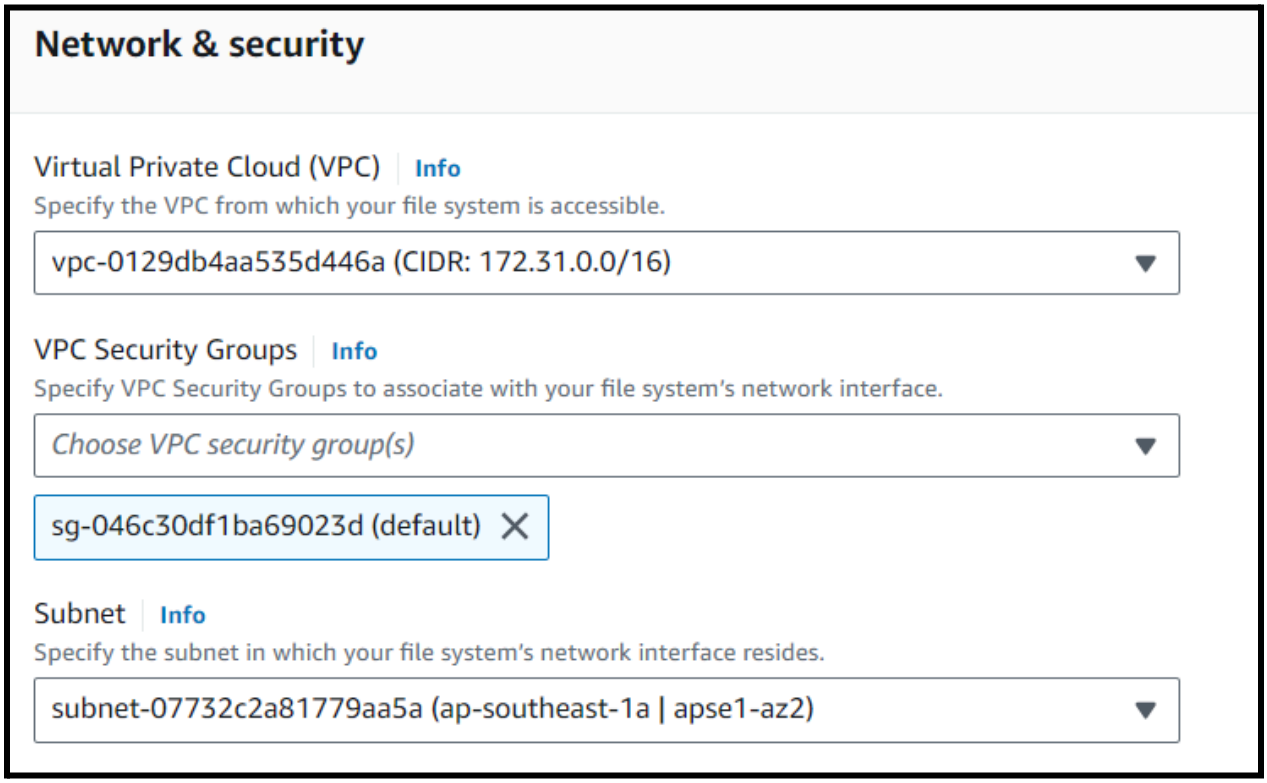
Network & Security:

VPC and Subnet:

- **VPC:** Choose the VPC where your file system will be deployed.
- **Subnets:** Select a subnet in the VPC. For Single-AZ, select one subnet. For Multi-AZ, select two subnets across different AZs.

Security Groups:

- **Security Groups:** Choose or create a security group that allows inbound and outbound traffic for SMB (port 445).



Windows authentication

Choose an Active Directory to provide user authentication and access control for your file system | Info

- (•) AWS Managed Microsoft Active Directory
- ( ) Self-managed Microsoft Active Directory

AWS Managed Microsoft Active Directory | Info

magicbus.com | d-96675f5fb0 ▼ 

Create new directory 

Encryption

Encryption key | Info

aws/fsx (default) ▼

Description	Account	KMS key ID
Default key that protects my FSx resources when no other key is defined	637423493890	45f0b11a-2168-455e-bf28-59bbd440d458

Log access to file shares | Info

Disable logs

Access - *optional*

Backup and maintenance - *optional*

Daily automatic backup | Info

Amazon FSx can protect your data through daily backups

- ○ Enabled
- ◉ Disabled

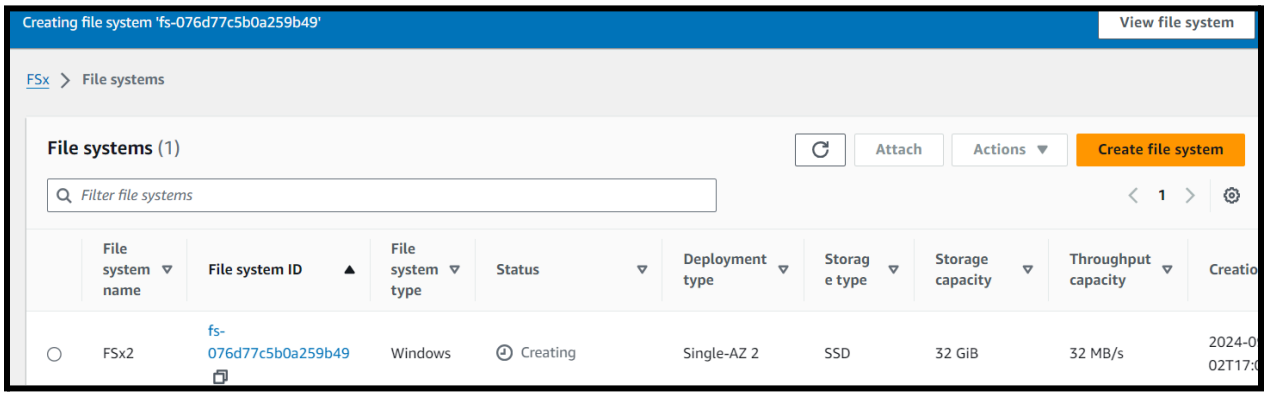
Weekly maintenance window | Info

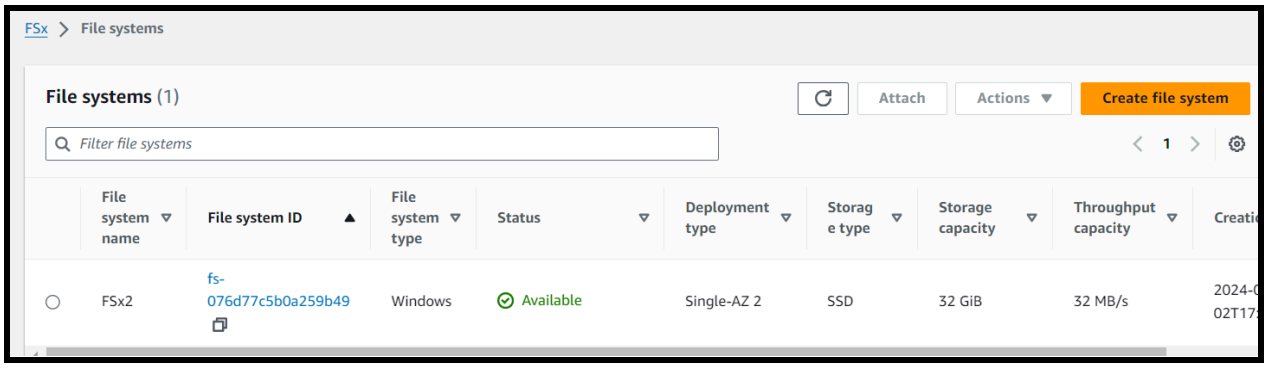
When patching needs to be performed, Amazon FSx performs maintenance on your file system only during this window.

- ◉ No preference
- ○ Select start time for 30-minute weekly maintenance window

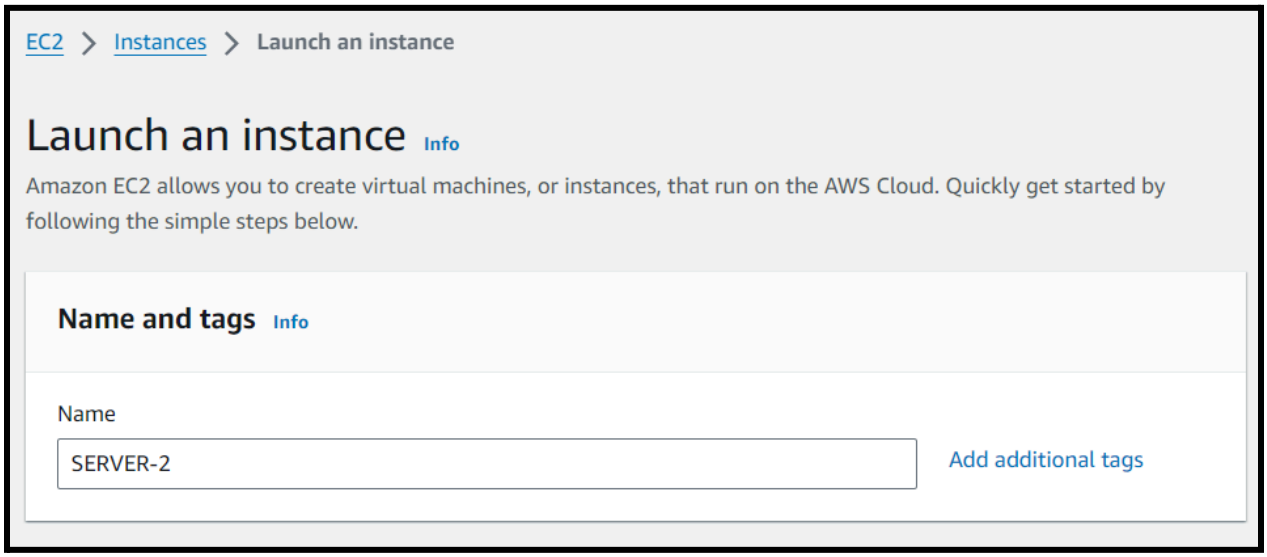
Tags - *optional*

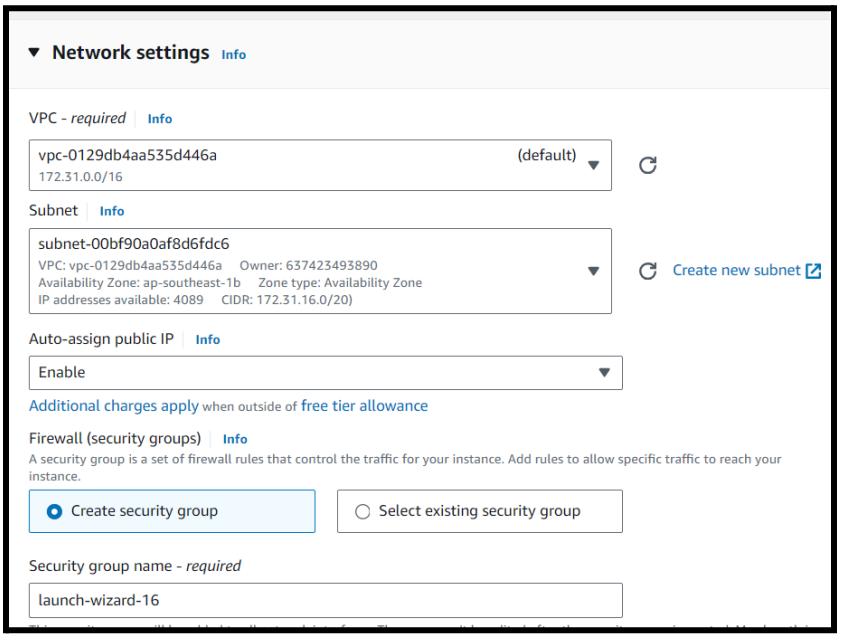
Cancel | Back | Next

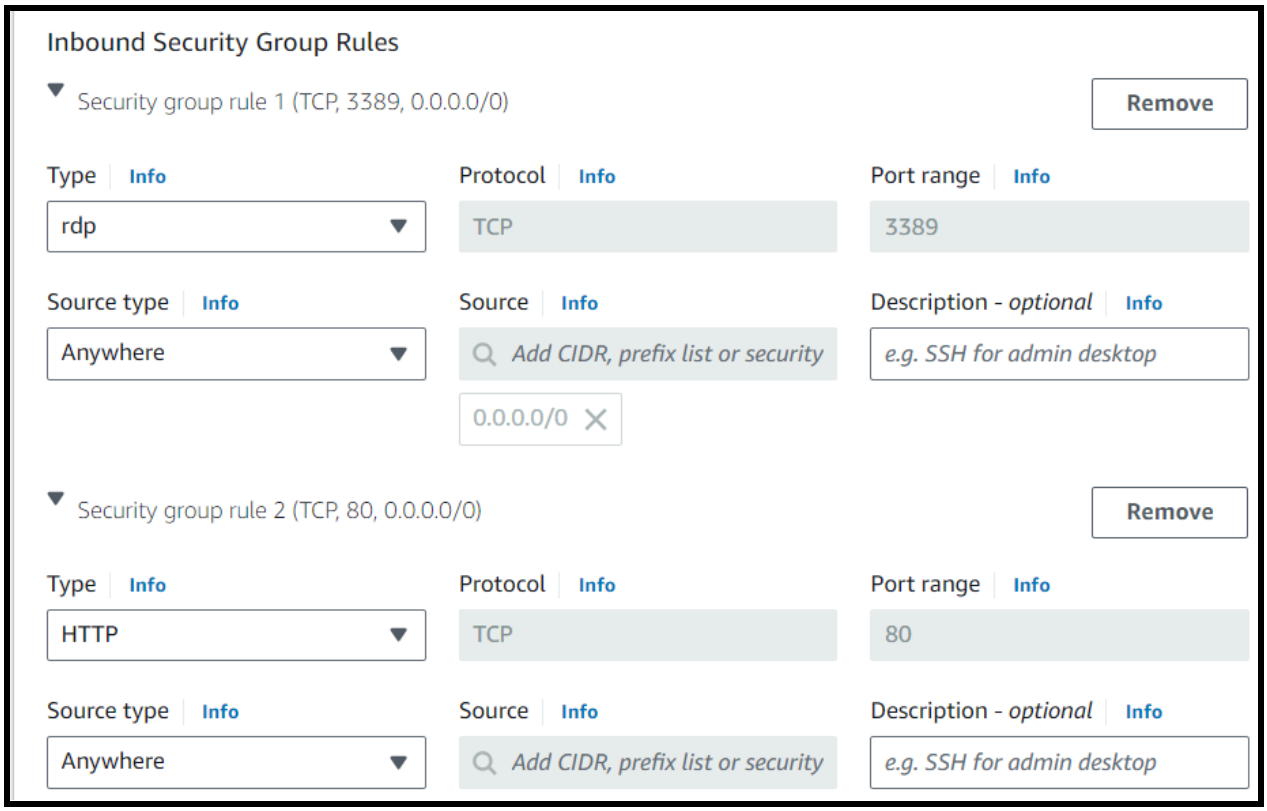


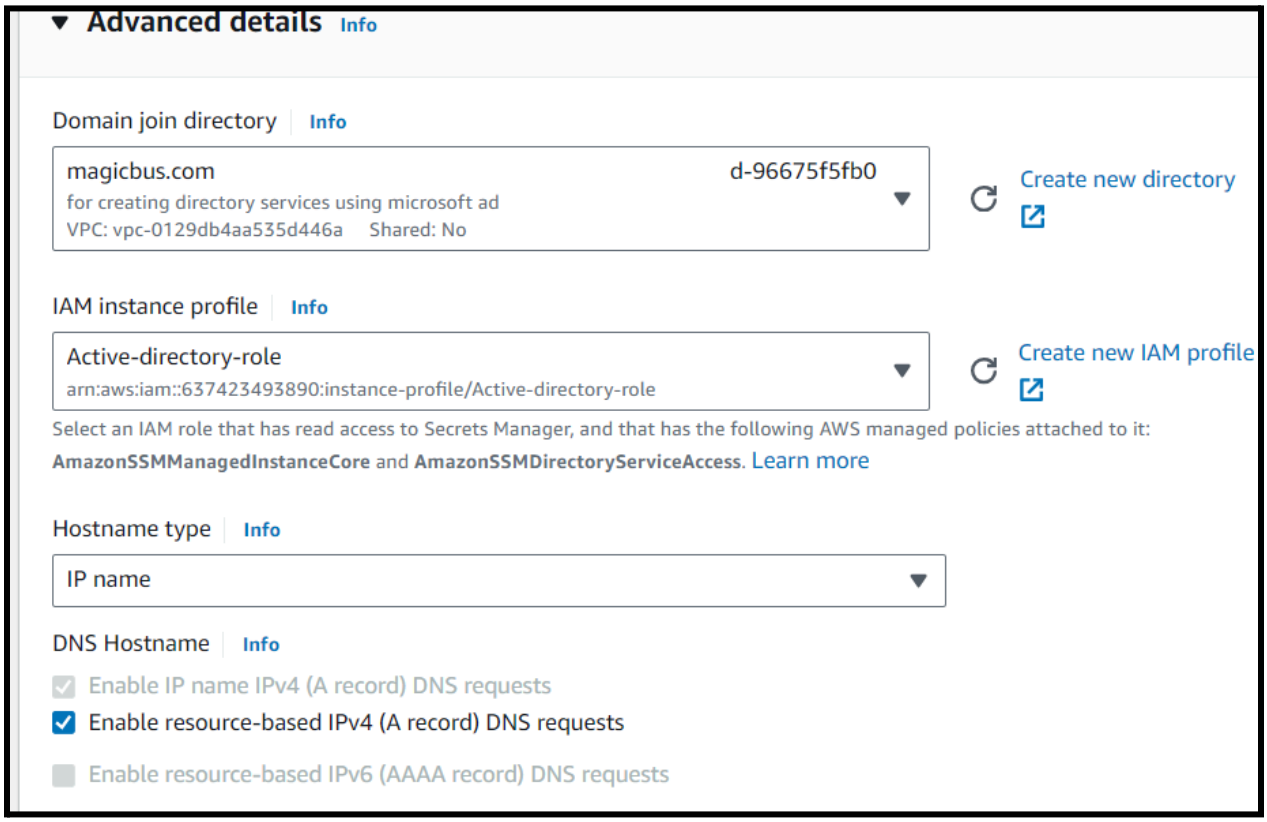


Create another instance






Inbound Security Group Rules
Security group rule 1 (TCP, 3389, 0.0.0.0/0)
Remove
Type Info
rdp
Protocol Info
TCP
Port range Info
3389
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Security group rule 2 (TCP, 80, 0.0.0.0/0)
Remove
Type Info
HTTP
Protocol Info
TCP
Port range Info
80
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop


Advanced details Info
Domain join directory Info
magicbus.com
d-96675f5fb0
for creating directory services using microsoft ad
VPC: vpc-0129db4aa535d446a Shared: No
Create new directory
IAM instance profile Info
Active-directory-role
arn:aws:iam::637423493890:instance-profile/Active-directory-role
Create new IAM profile
Select an IAM role that has read access to Secrets Manager, and that has the following AWS managed policies attached to it:
AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess. Learn more
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

Connect to the File System:

Mounting: From a Windows-based EC2 instance, use the file system's DNS name to mount the file system:
shell
Copy code

```
\\[file-system-dns-name]\[share-name]
```

-
- **Active Directory:** If integrated with AD, ensure that proper permissions are set for users and groups to access the file system.
- `net use Z: \\amznfsxlwi0dd8z.magicbus.com\share`

Attach file system

From Windows instances (Amazon EC2, Amazon WorkSpaces, VMware Cloud on AWS)

Prerequisites

1. Join an EC2 Windows instance to your Active Directory d-96675f5fb0
   - Launch new EC2 Windows instance joined to ActiveDirectory
   - Manually join an existing EC2 Windows instance to ActiveDirectory
2. Connect to EC2 Windows instance

Attach instruction - using the default DNS name

1. Open a command prompt.
2. Execute the following command (you can replace "Z:" with any other available drive letter):

```
net use Z: \\amznfsxlwi0dd8z.magicbus.com\share
```

Attach instruction - using DNS aliases

1. If you have not yet already, create Service Principal Names (SPNs) and DNS CNAME records for the DNS alias
2. Open a command prompt.
3. Execute the following command (you can replace "Z:" with any other

Close