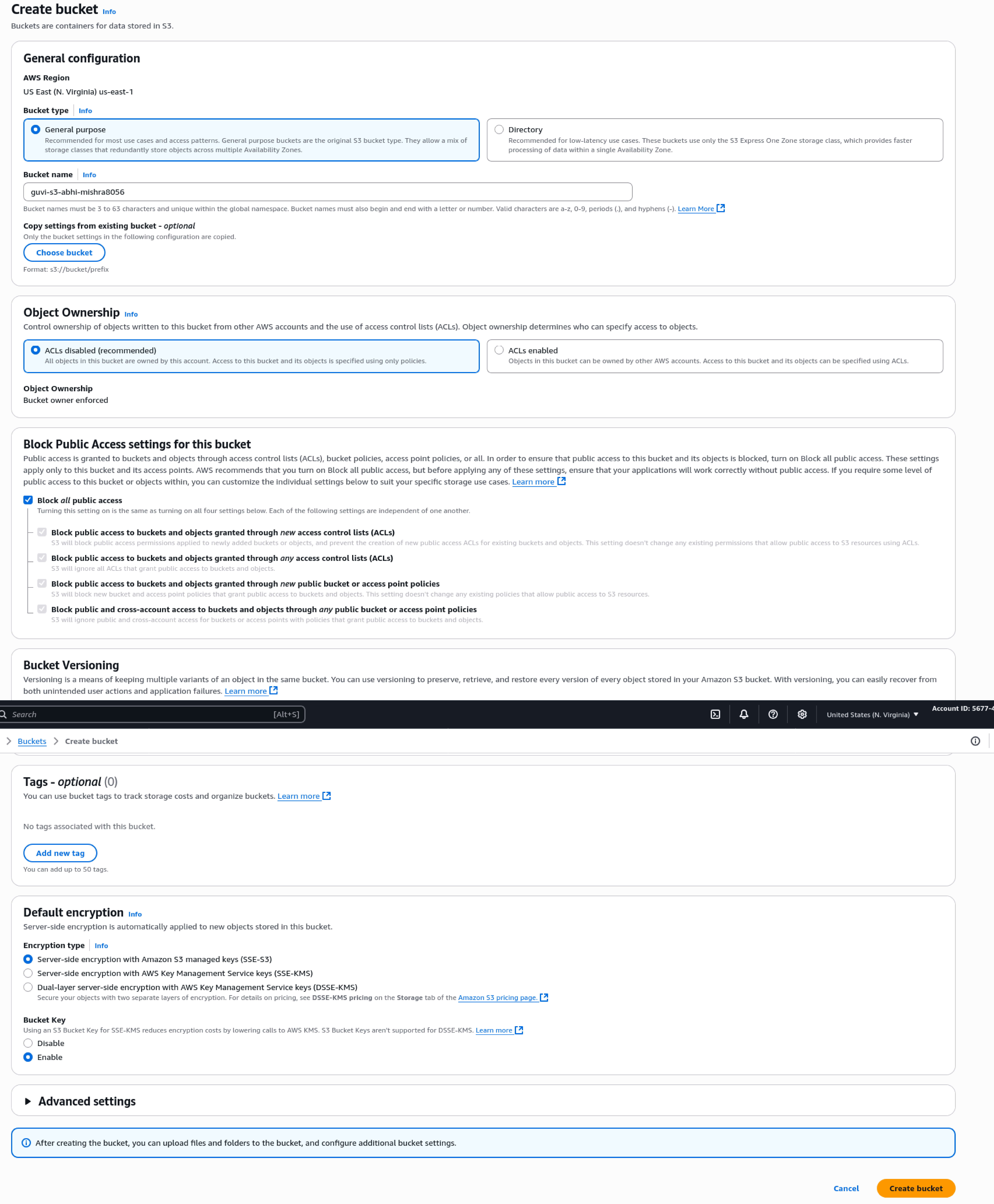


Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type Info

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

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

Bucket name Info

guvi-s3-abhi-mishra8056

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

Object Ownership Info

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

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

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

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

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

☑ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☑ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☑ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☑ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

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

Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

Add new tag

You can add up to 50 tags.

Default encryption Info

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

Encryption type Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

Bucket Key

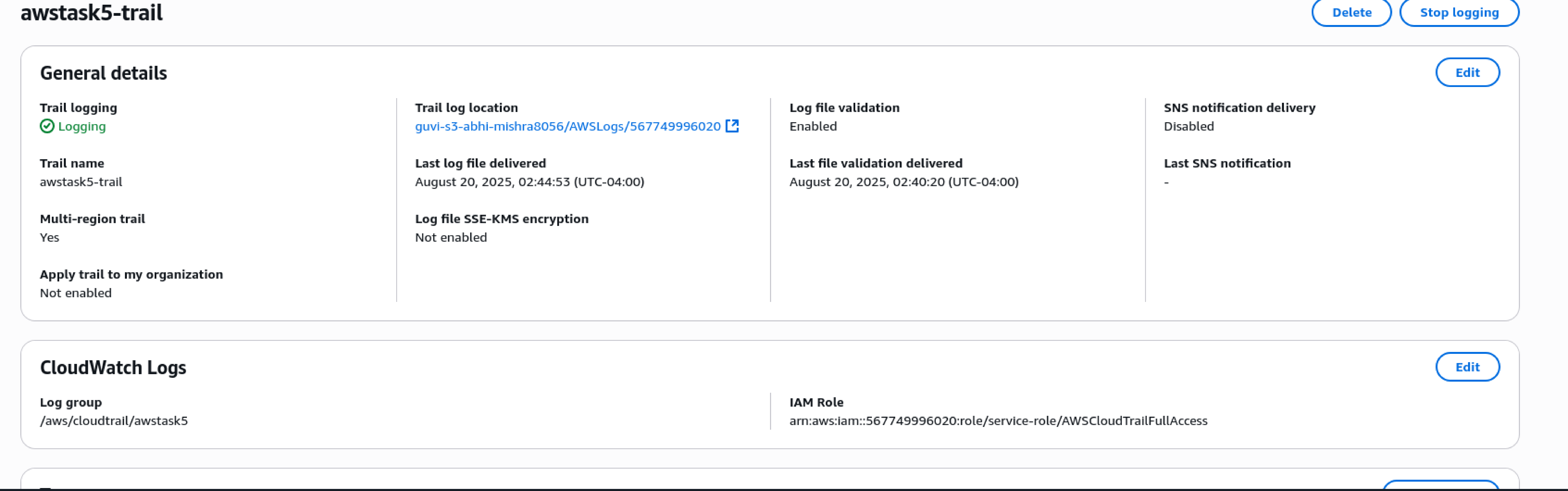
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

○ Disable

● Enable

▶ **Advanced settings**

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



awstask5-trail

General details

Trail logging
Logging

Trail name
awstask5-trail

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
guvi-s3-abhi-mishra8056/AWSLogs/567749996020

Last log file delivered
August 20, 2025, 02:44:53 (UTC-04:00)

Log file SSE-KMS encryption
Not enabled

Log file validation
Enabled

Last file validation delivered
August 20, 2025, 02:40:20 (UTC-04:00)

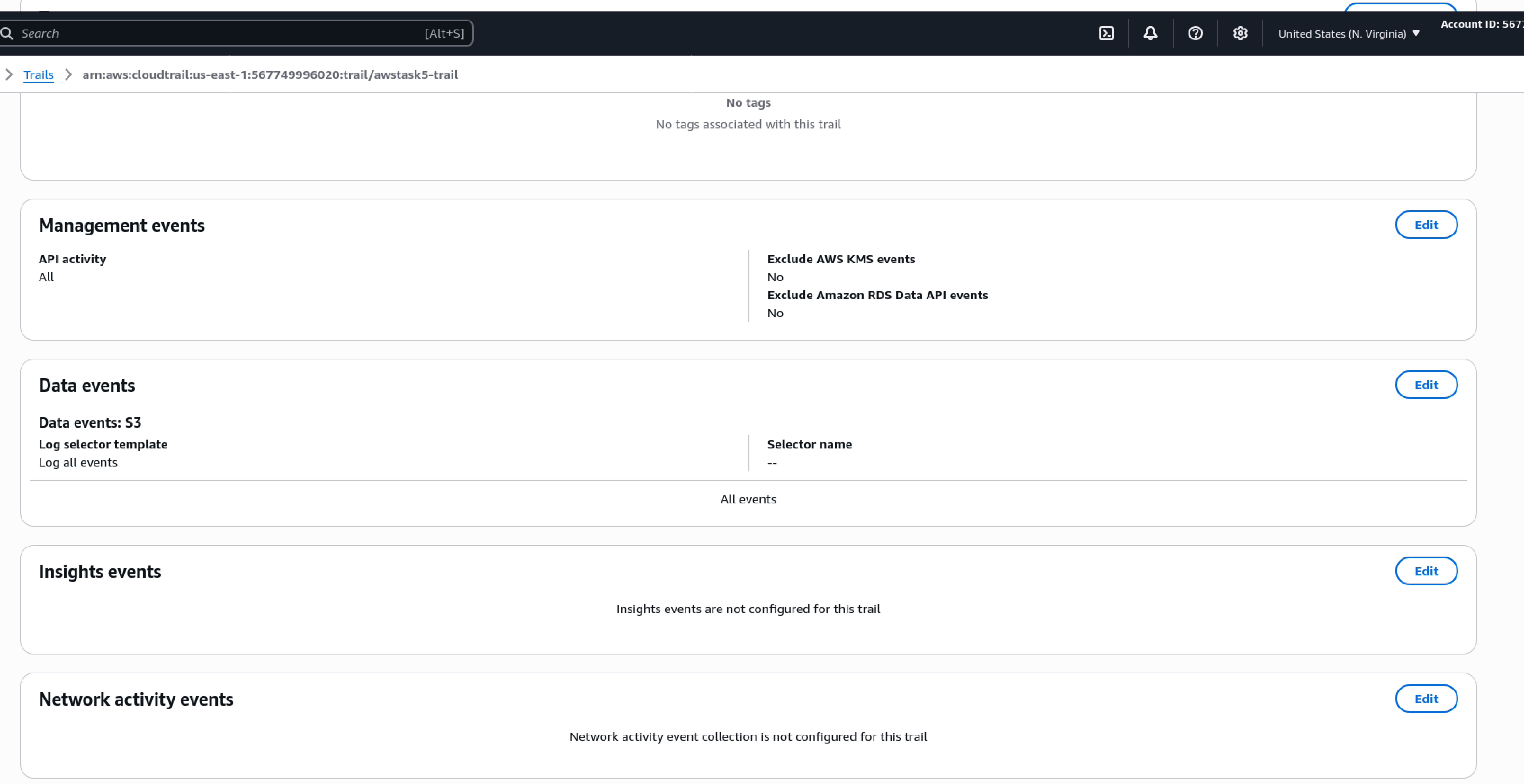
SNS notification delivery
Disabled

Last SNS notification
-

CloudWatch Logs

Log group
/aws/cloudtrail/awstask5

IAM Role
arn:aws:iam::567749996020:role/service-role/AWSCloudTrailFullAccess



Trails > arn:aws:cloudtrail:us-east-1:567749996020:trail/awstask5-trail

No tags
No tags associated with this trail

Management events

API activity
All

Exclude AWS KMS events
No

Exclude Amazon RDS Data API events
No

Data events

Data events: S3

Log selector template
Log all events

Selector name
--

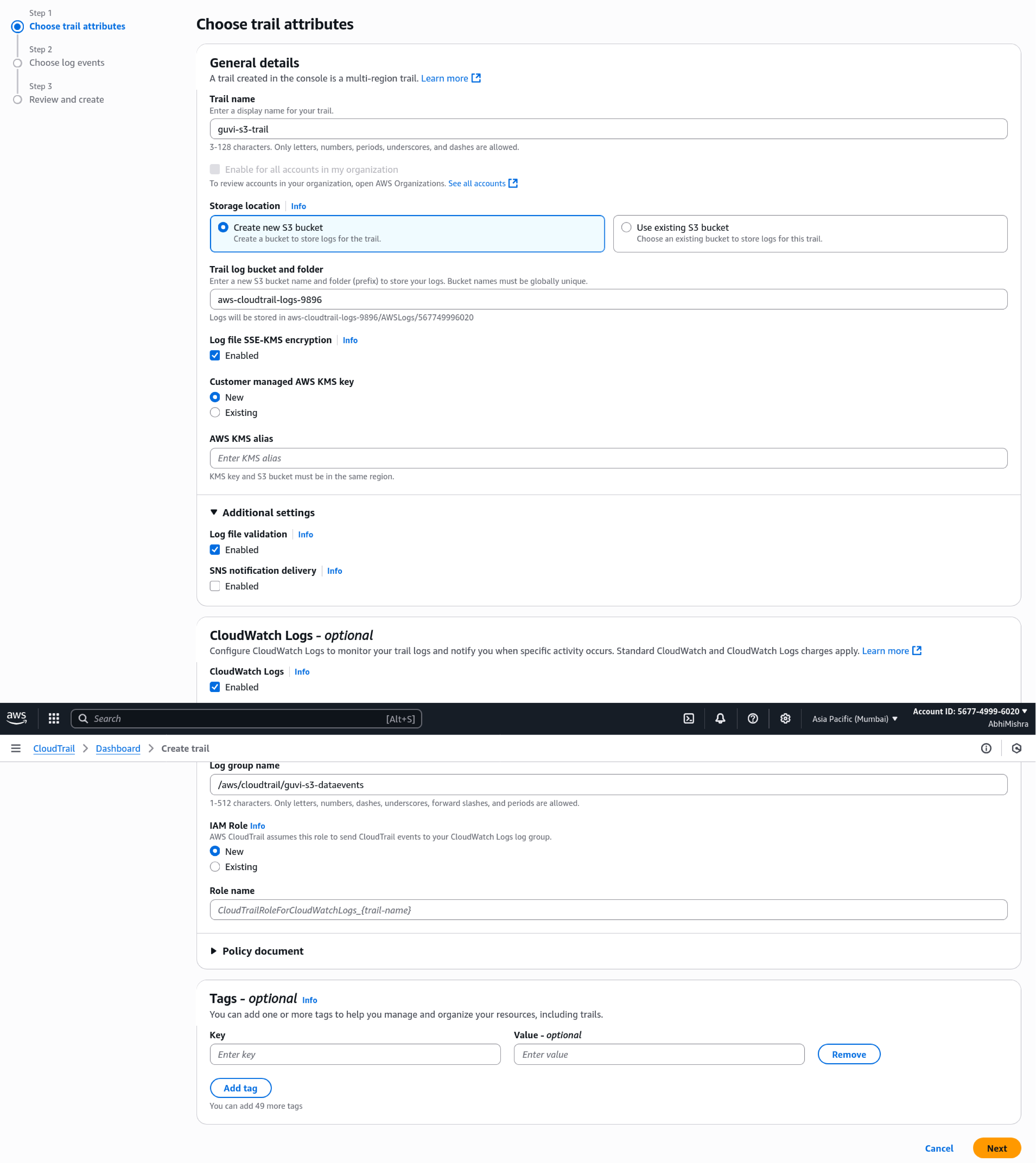
All events

Insights events

Insights events are not configured for this trail

Network activity events

Network activity event collection is not configured for this trail



Step 1
● Choose trail attributes

Step 2
○ Choose log events

Step 3
○ Review and create

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.
guvi-s3-trail
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-9896
Logs will be stored in aws-cloudtrail-logs-9896/AWSLogs/567749996020

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

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

aws
Search
[Alt+S]
Asia Pacific (Mumbai) ▼
Account ID: 5677-4999-6020 ▼
AbhiMishra
CloudTrail > Dashboard > Create trail

Log group name
/aws/cloudtrail/guvi-s3-dataevents
1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

IAM Role Info
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.
● New
○ Existing

Role name
CloudTrailRoleForCloudWatchLogs_{trail-name}

▶ **Policy document**

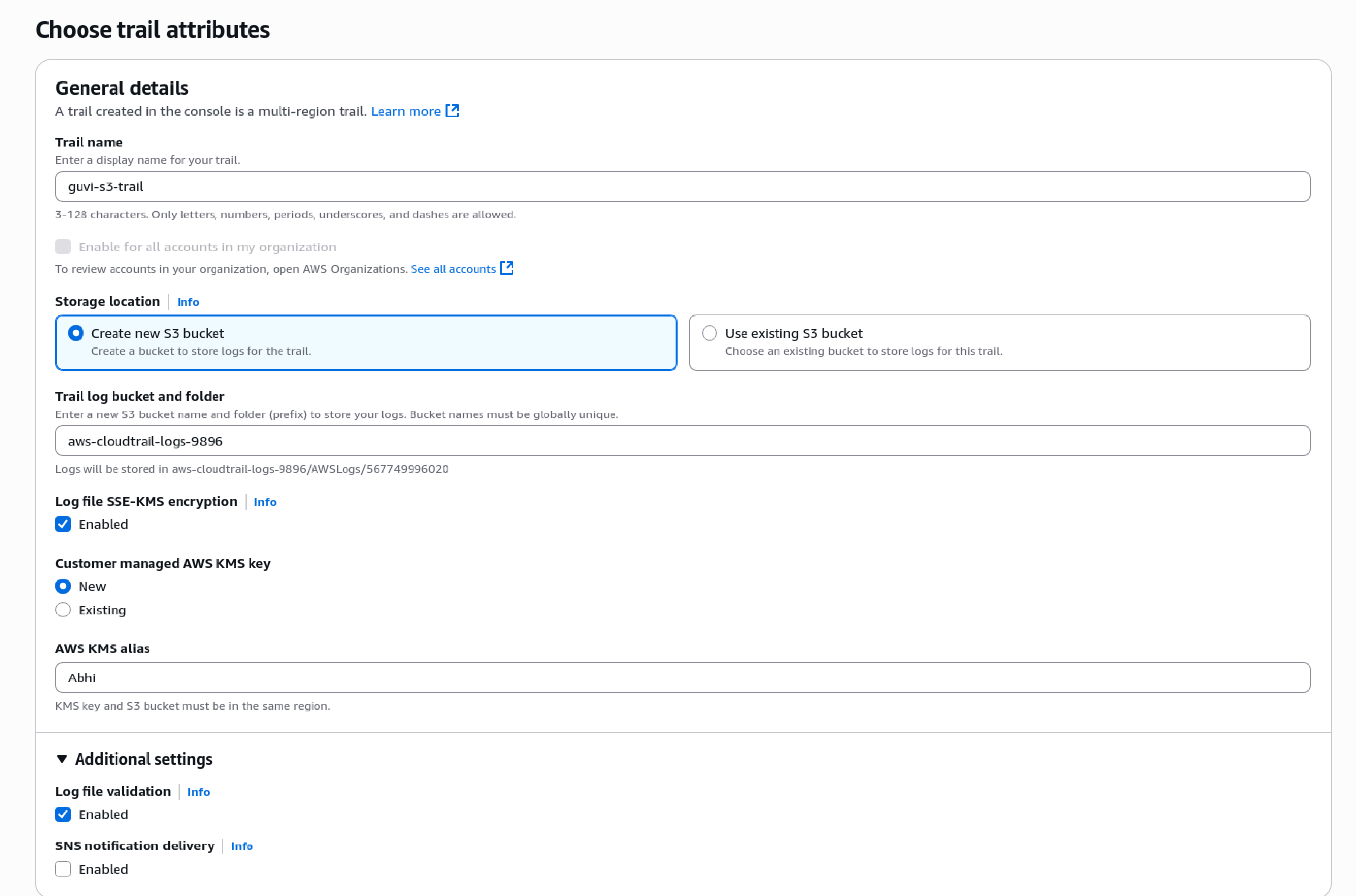
Tags - *optional* Info

You can add one or more tags to help you manage and organize your resources, including trails.

Key	Value - *optional*	
Enter key	*Enter value*	Remove

Add tag
You can add 49 more tags

Cancel Next



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.

guvi-s3-trail

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-9896

Logs will be stored in aws-cloudtrail-logs-9896/AWSLogs/567749996020

Log file SSE-KMS encryption | Info

☑ Enabled

Customer managed AWS KMS key

● New

○ Existing

AWS KMS alias

Abhi

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

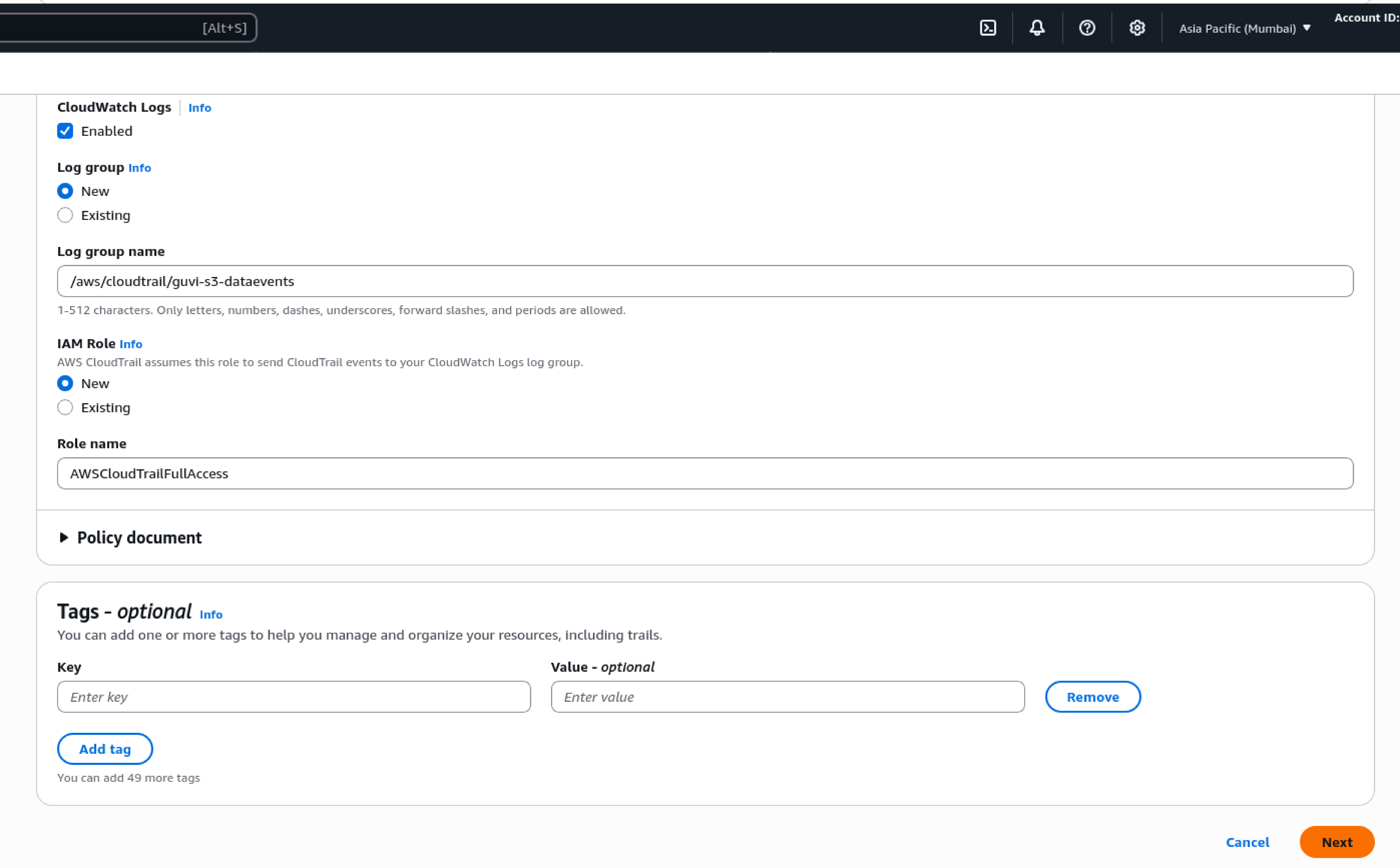
▼ Additional settings

Log file validation | Info

☑ Enabled

SNS notification delivery | Info

□ Enabled



CloudWatch Logs | Info

☑ Enabled

Log group Info

● New

○ Existing

Log group name

/aws/cloudtrail/guvi-s3-dataevents

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

IAM Role Info

AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

● New

○ Existing

Role name

AWSCloudTrailFullAccess

▶ **Policy document**

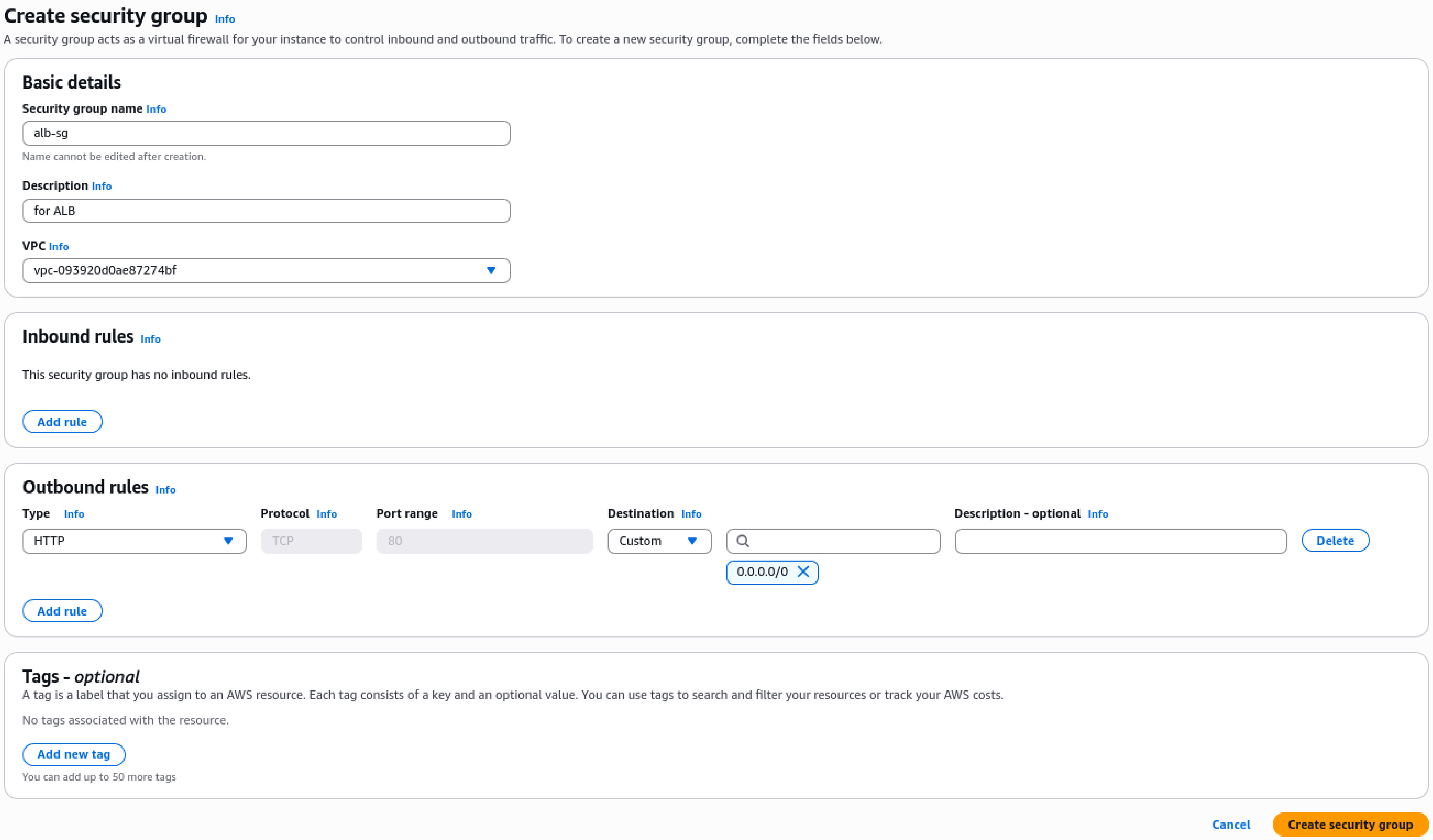
Tags - *optional* Info

You can add one or more tags to help you manage and organize your resources, including trails.

Key	Value - *optional*	
Enter key	*Enter value*	Remove

Add tag

You can add 49 more tags



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

alb-sg

Name cannot be edited after creation.

Description Info

for ALB

VPC Info

vpc-093920d0ae87274bf ▼

Inbound rules Info

This security group has no inbound rules.

Outbound rules Info

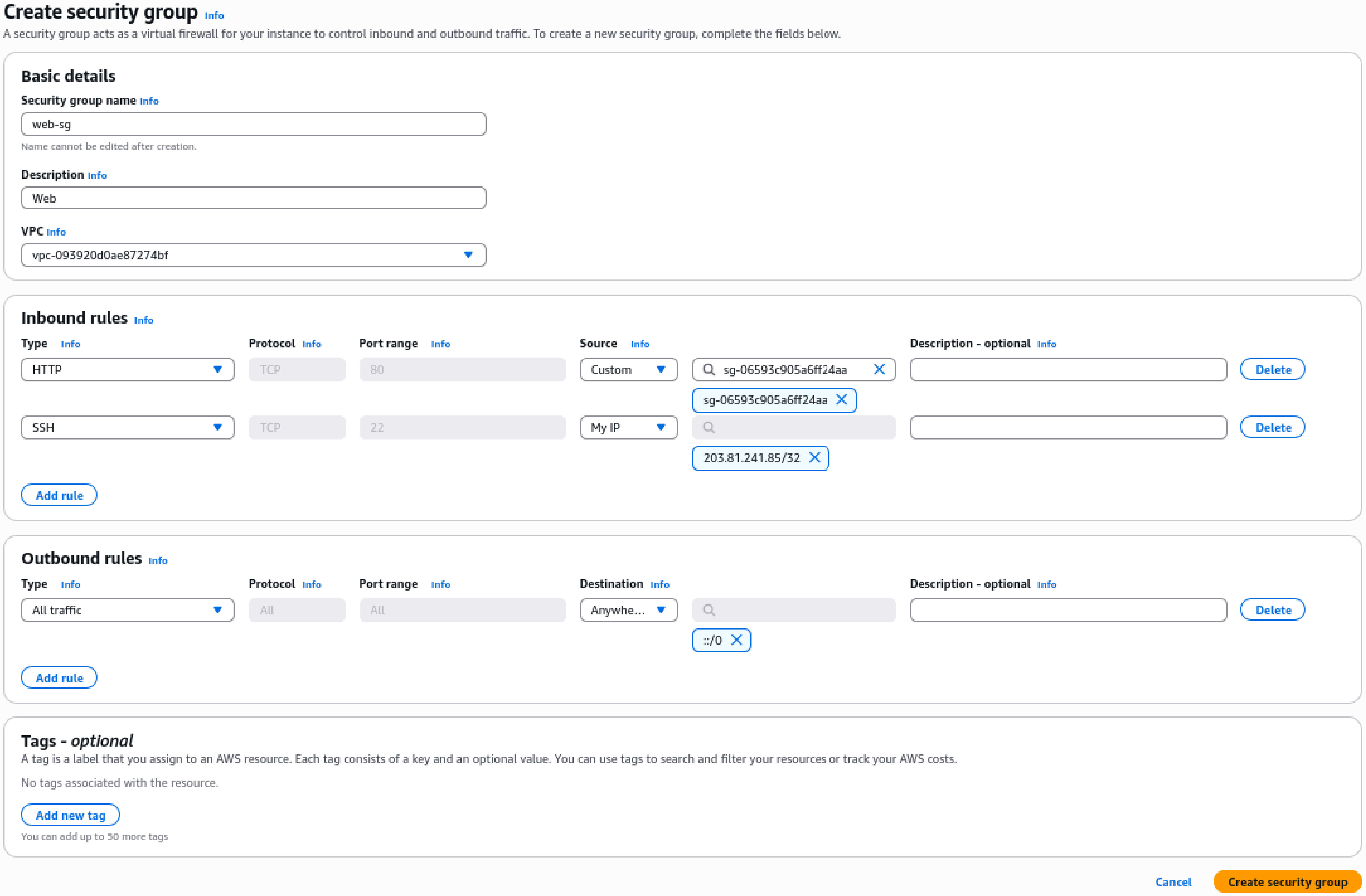
Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info	
HTTP ▼	TCP	80	Custom ▼	0.0.0.0/0 ✕		Delete

Tags - *optional*

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

No tags associated with the resource.

You can add up to 50 more tags



Create security group

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

Basic details

Security group name: web-sg

Name cannot be edited after creation.

Description: Web

VPC: vpc-093920d0ae87274bf

Inbound rules

Type	Protocol	Port range	Source		Description - optional
HTTP	TCP	80	Custom	sg-06593c905a6ff24aa sg-06593c905a6ff24aa	
SSH	TCP	22	My IP	203.81.241.85/32	

Outbound rules

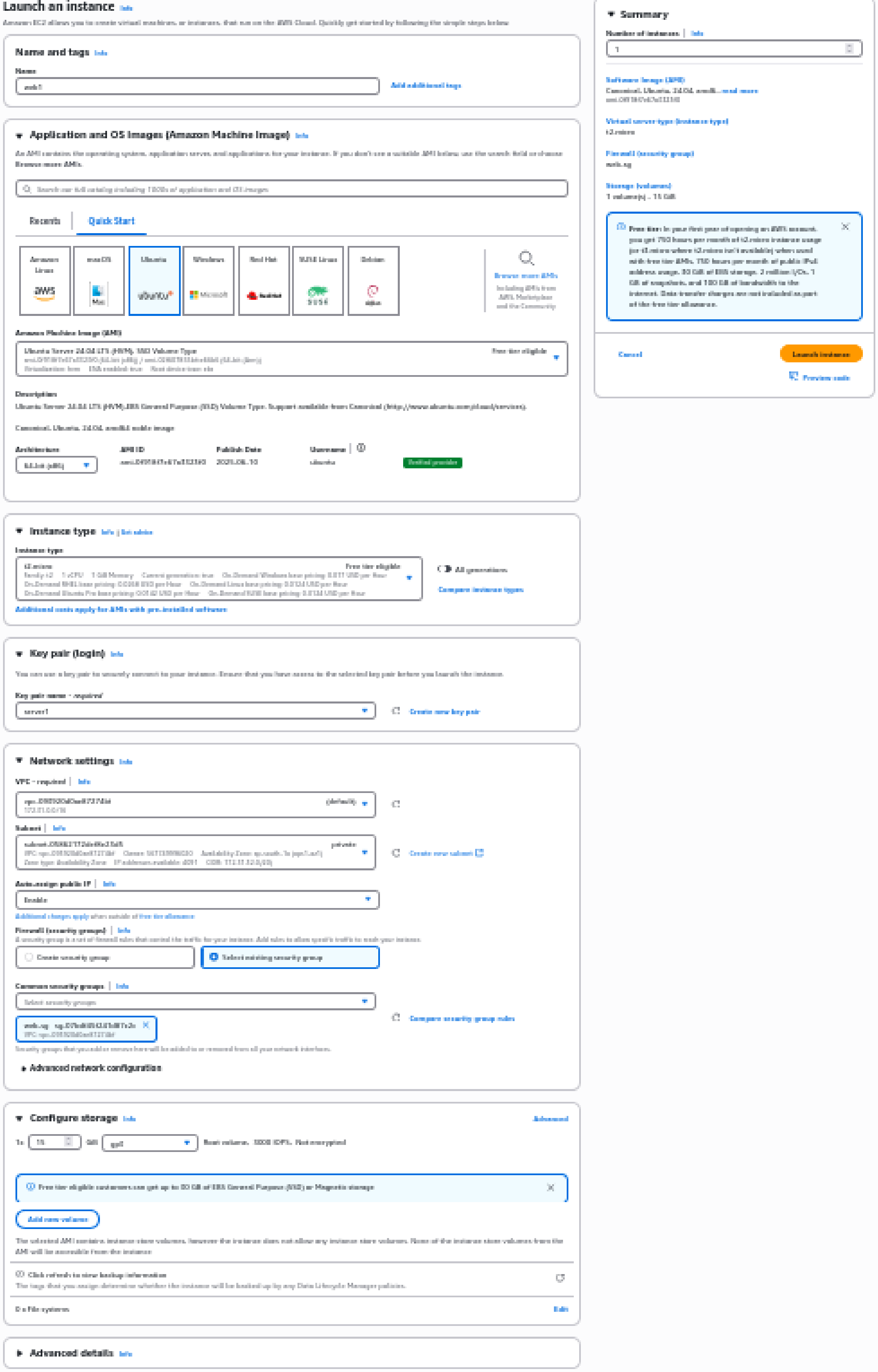
Type	Protocol	Port range	Destination		Description - optional
All traffic	All	All	Anywhe...	::/0	

Tags - *optional*

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

No tags associated with the resource.

You can add up to 50 more tags



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
web1
Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

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

Recents | Quick Start

Amazon Machine Image (AMI)
Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-0f918f7e67a3323f0 (64-bit (x86)) / ami-[illegible] (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).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture: 64-bit (x86)
AMI ID: ami-0f918f7e67a3323f0
Publish Date: 2025-06-10
Username: ubuntu
Verified provider

▼ Instance type Info | Get advice

Instance type
t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 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 - required
server1
Create new key pair

▼ Network settings Info

VPC - required | Info
vpc-[illegible] (default)
172.31.0.0/16

Subnet | Info
subnet-[illegible] private
VPC: vpc-[illegible] Owner: [illegible] Availability Zone: ap-south-1a (aps1-az1)
Zone type: Availability Zone IP addresses available: 4091 CIDR: 172.31.32.0/20
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

Common security groups | Info
Select security groups
web-sg sg-[illegible]
VPC: vpc-[illegible]
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.

▸ Advanced network configuration

▼ Configure storage Info — Advanced

1x 15 GiB gp3 Root volume, 3000 IOPS, Not encrypted

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

Add new volume

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

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

0 x File systems — Edit

▸ Advanced details Info

▼ Summary

Number of instances | Info
1

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

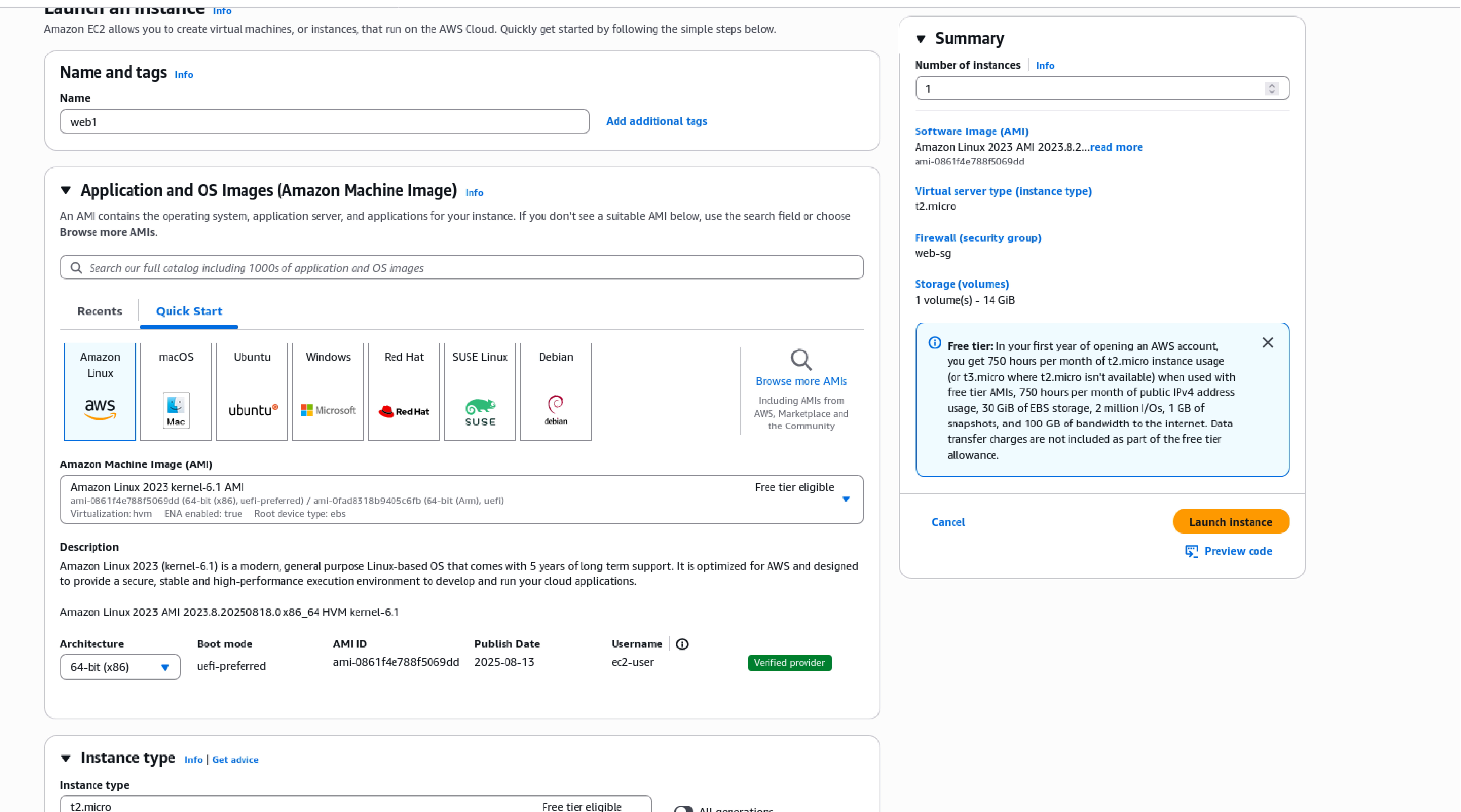
Virtual server type (instance type)
t2.micro

Firewall (security group)
web-sg

Storage (volumes)
1 volume(s) - 15 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.

Cancel
Launch instance
Preview code



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: web1

▼ Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose **Browse more AMIs**.

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI — Free tier eligible
ami-0861f4e788f5069dd (64-bit (x86), uefi-preferred) / ami-0fad8318b9405c6fb (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

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

Amazon Linux 2023 AMI 2023.8.20250818.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username	
64-bit (x86)	uefi-preferred	ami-0861f4e788f5069dd	2025-08-13	ec2-user	Verified provider

▼ Instance type Info | Get advice

Instance type: t2.micro — Free tier eligible

▼ Summary

Number of instances Info: 1

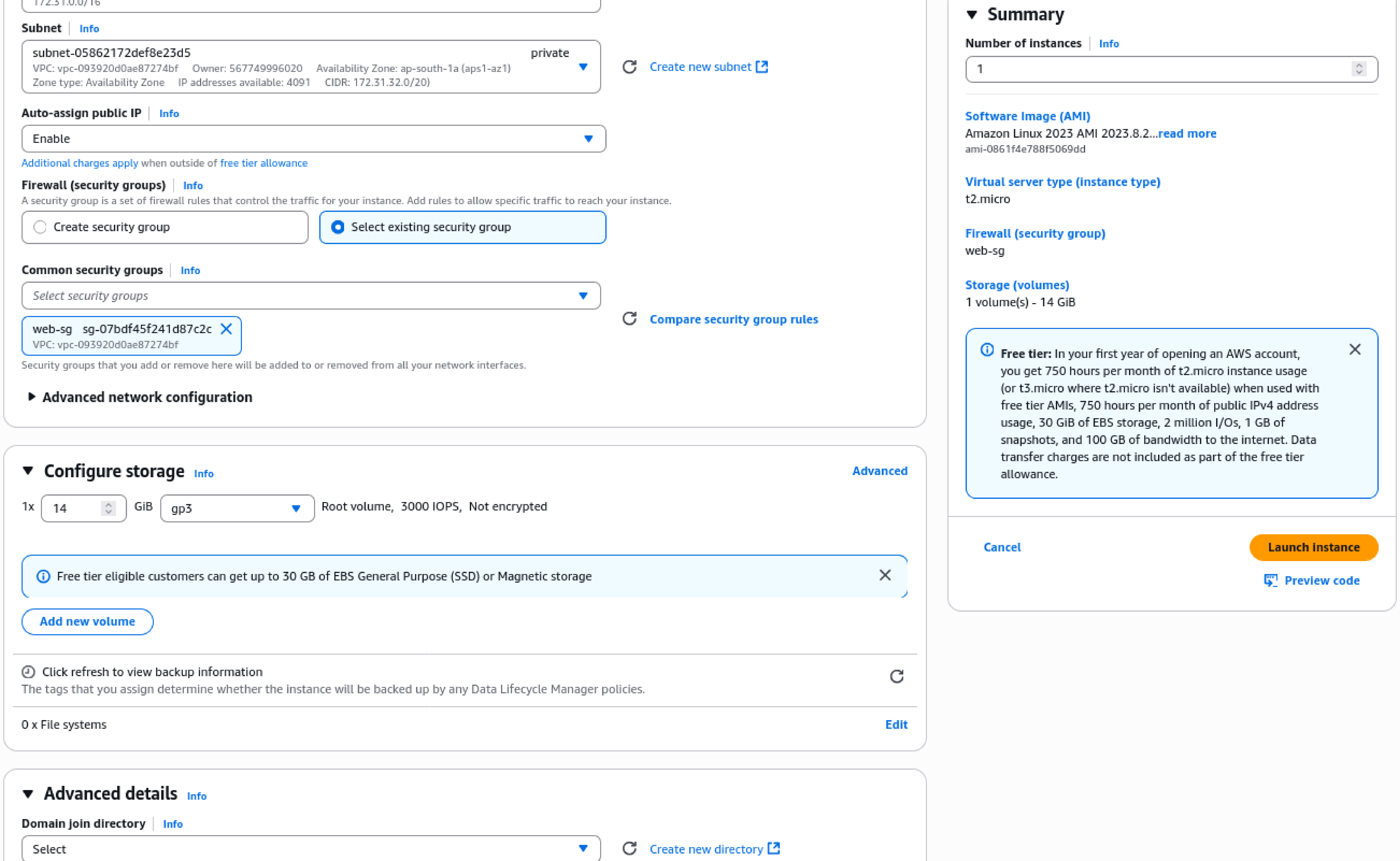
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0861f4e788f5069dd

Virtual server type (instance type)
t2.micro

Firewall (security group)
web-sg

Storage (volumes)
1 volume(s) - 14 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.



172.31.0.0/16

Subnet | Info

subnet-05862172def8e23d5 private
VPC: vpc-093920d0ae87274bf Owner: 567749996020 Availability Zone: ap-south-1a (aps1-az1)
Zone type: Availability Zone IP addresses available: 4091 CIDR: 172.31.32.0/20)

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

Common security groups | Info

Select security groups

web-sg sg-07bdf45f241d87c2c
VPC: vpc-093920d0ae87274bf

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▸ **Advanced network configuration**

▾ Configure storage

Info

Advanced

1x 14 GiB gp3 Root volume, 3000 IOPS, Not encrypted

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

Add new volume

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

▾ Advanced details

Info

Domain join directory | Info

Select

Create new directory

▾ Summary

Number of instances | Info

1

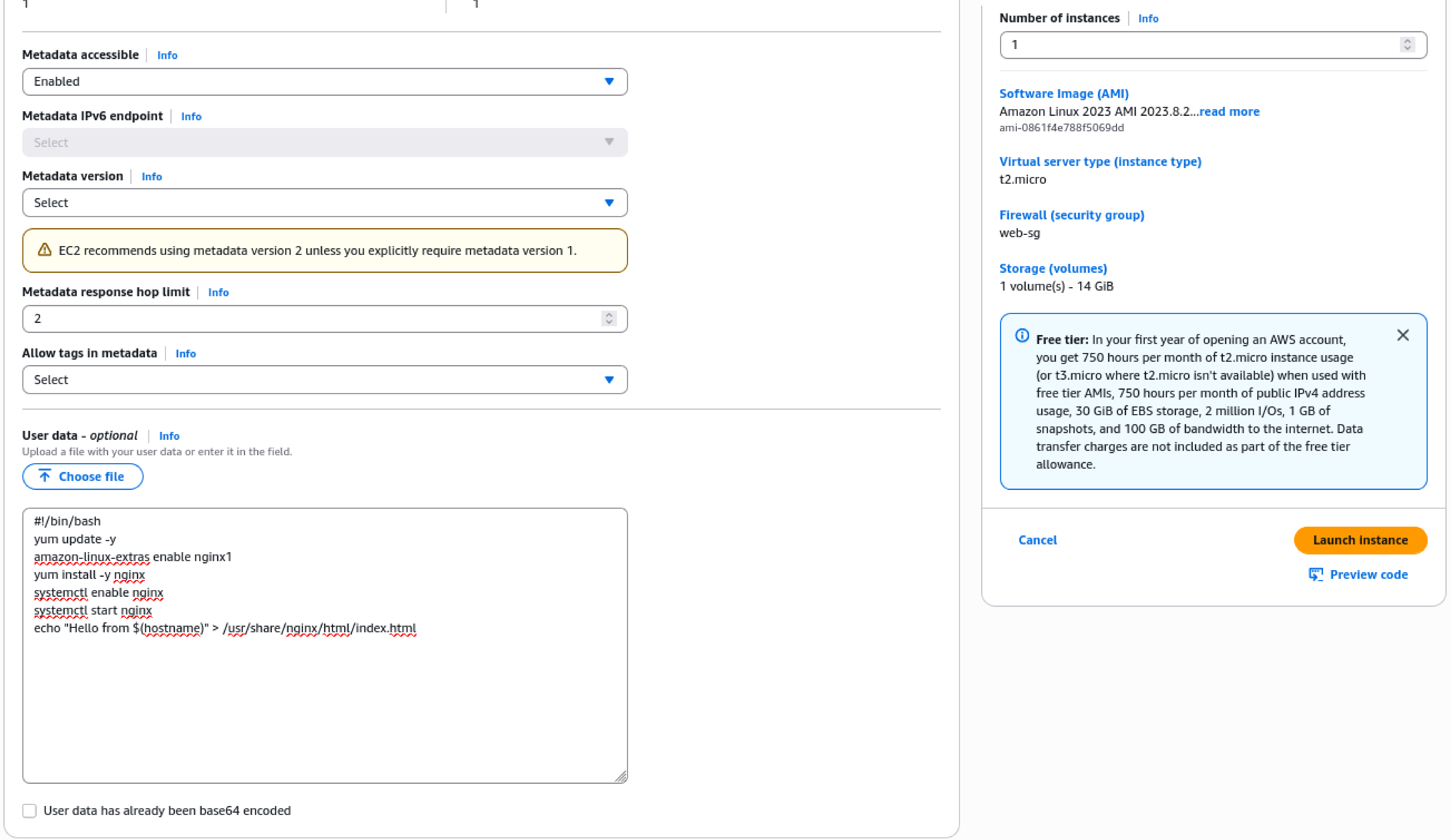
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0861f4e788f5069dd

Virtual server type (instance type)
t2.micro

Firewall (security group)
web-sg

Storage (volumes)
1 volume(s) - 14 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.



1 1

Metadata accessible | Info

Enabled ▼

Metadata IPv6 endpoint | Info

Select ▼

Metadata version | Info

Select ▼

⚠ EC2 recommends using metadata version 2 unless you explicitly require metadata version 1.

Metadata response hop limit | Info

2

Allow tags in metadata | Info

Select ▼

User data - *optional* | Info

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

```
#!/bin/bash
yum update -y
amazon-linux-extras enable nginx1
yum install -y nginx
systemctl enable nginx
systemctl start nginx
echo "Hello from $(hostname)" > /usr/share/nginx/html/index.html
```

□ User data has already been base64 encoded

Number of instances | Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.8.2...read more

ami-0861f4e788f5069dd

Virtual server type (instance type)

t2.micro

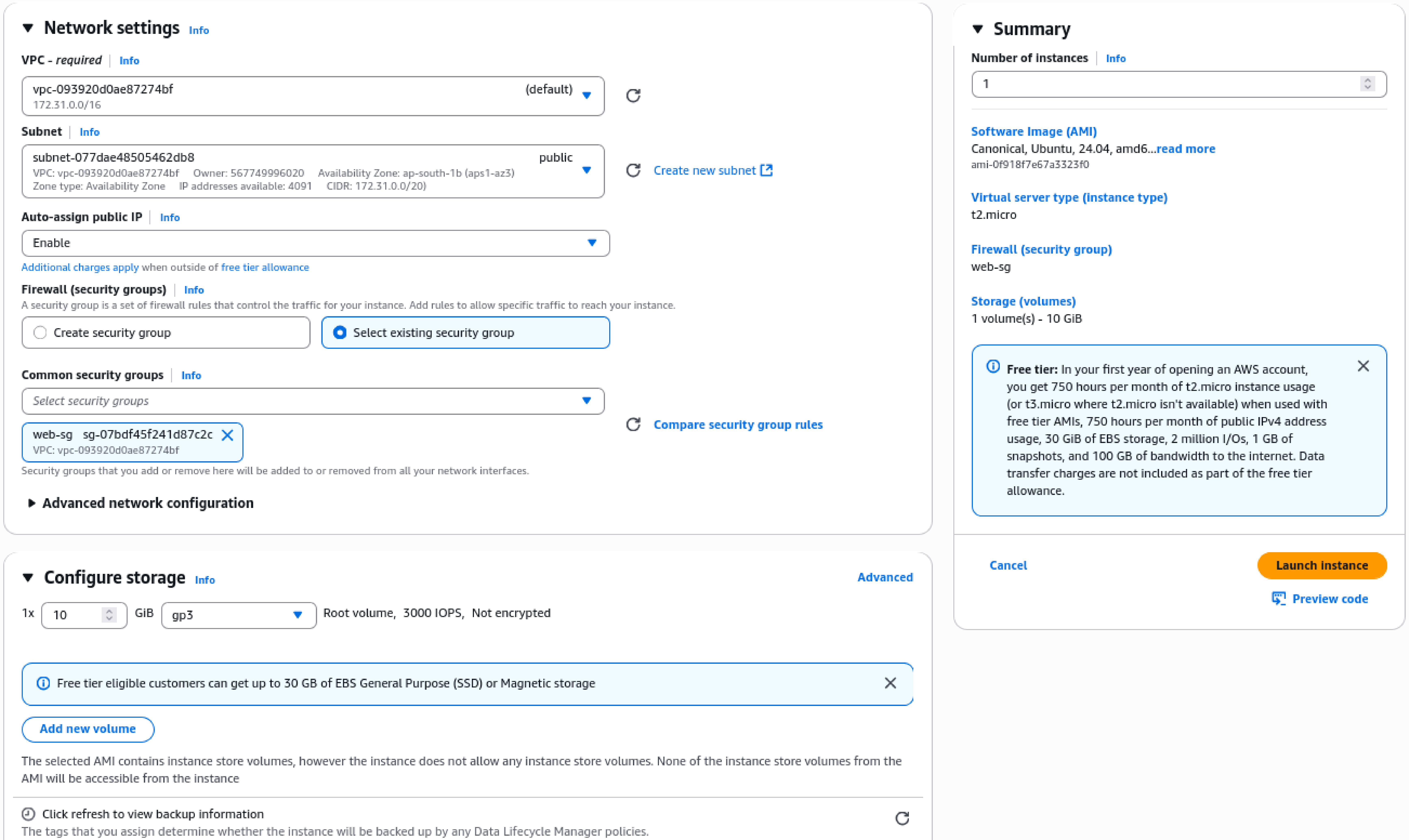
Firewall (security group)

web-sg

Storage (volumes)

1 volume(s) - 14 GiB

ⓘ **Free tier:** In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.



▼ Network settings Info

VPC - *required* | Info

vpc-093920d0ae87274bf (default) ▼
172.31.0.0/16

Subnet | Info

subnet-077dae48505462db8 public ▼
VPC: vpc-093920d0ae87274bf Owner: 567749996020 Availability Zone: ap-south-1b (aps1-az3)
Zone type: Availability Zone IP addresses available: 4091 CIDR: 172.31.0.0/20)

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

Common security groups | Info

Select security groups ▼

web-sg sg-07bdf45f241d87c2c ✕
VPC: vpc-093920d0ae87274bf

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ Advanced network configuration

▼ Configure storage Info

Advanced

1x 10 GiB gp3 ▼ Root volume, 3000 IOPS, Not encrypted

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

Add new volume

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

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

▼ Summary

Number of instances | Info

1

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

Virtual server type (instance type)
t2.micro

Firewall (security group)
web-sg

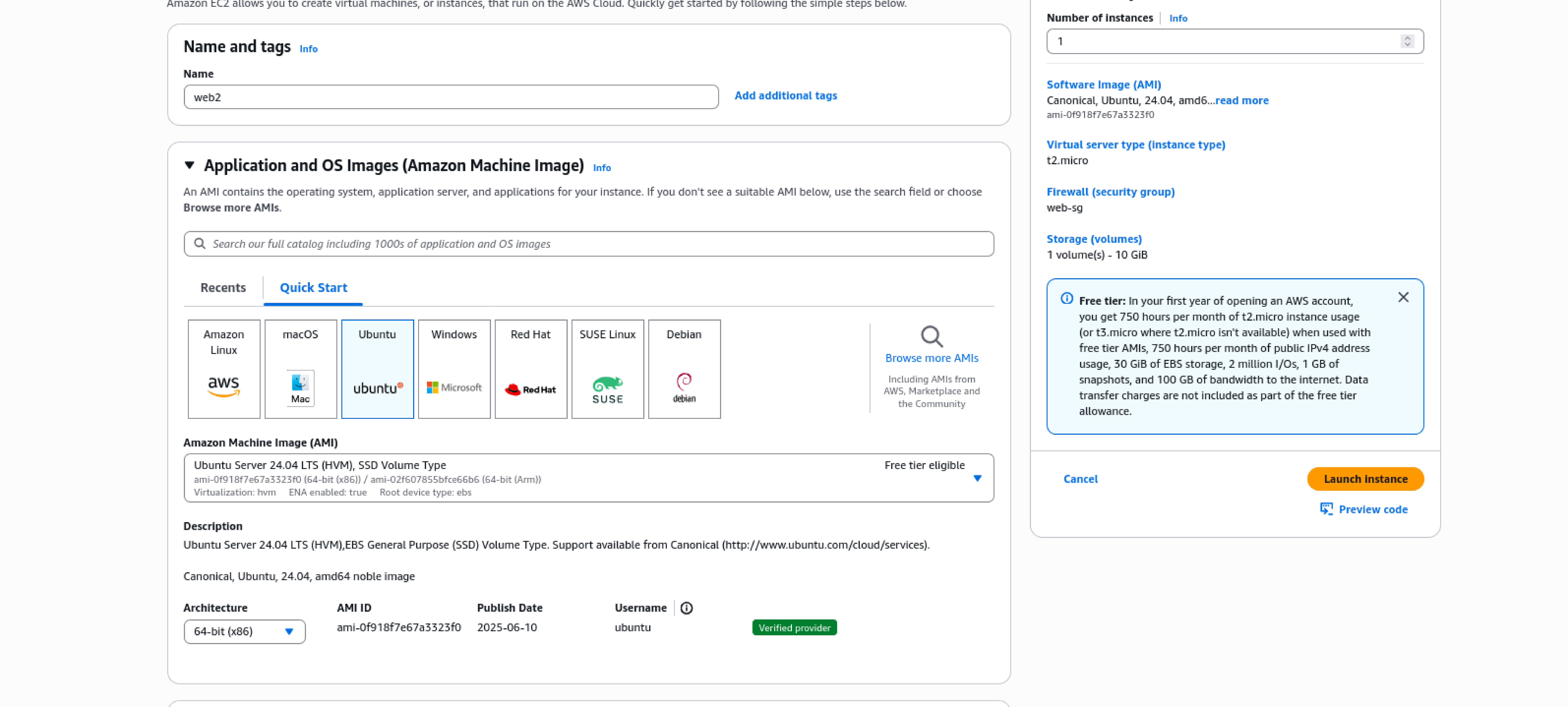
Storage (volumes)
1 volume(s) - 10 GiB

ⓘ **Free tier:** In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance. ✕

Cancel

Launch instance

Preview code



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

Name and tags

Name: web2

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose **Browse more AMIs**.

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

Amazon Machine Image (AMI)

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

Description

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

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture	AMI ID	Publish Date	Username	
64-bit (x86)	ami-0f918f7e67a3323f0	2025-06-10	ubuntu	Verified provider

Number of instances: 1

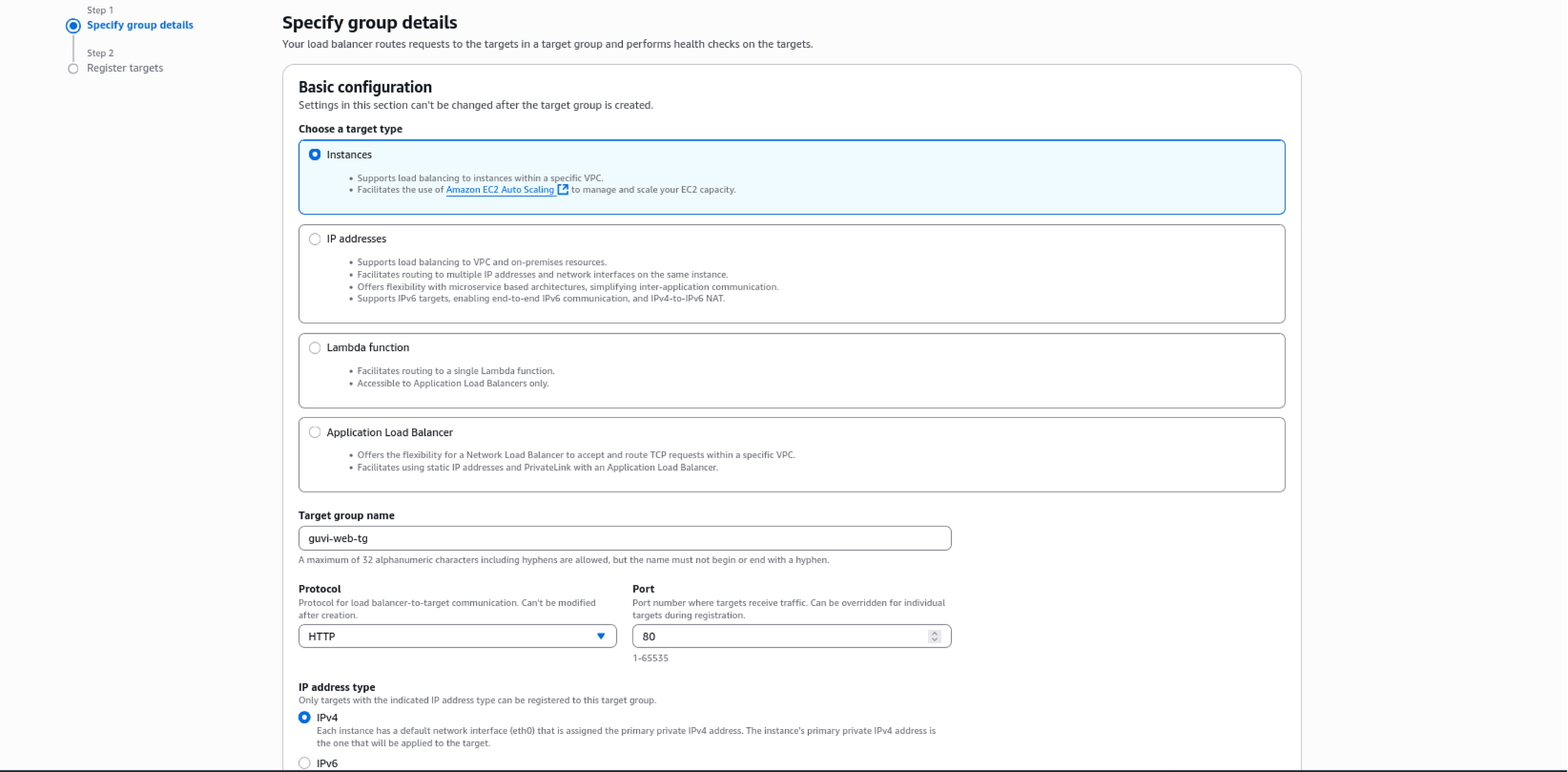
Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-0f918f7e67a3323f0

Virtual server type (instance type)
t2.micro

Firewall (security group)
web-sg

Storage (volumes)
1 volume(s) - 10 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.



Step 1

● Specify group details

Step 2

○ Register targets

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.

○ IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

○ Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

○ Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

guvi-web-tg

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

Protocol

Protocol for load balancer-to-target communication. Can't be modified after creation.

HTTP ▼

Port

Port number where targets receive traffic. Can be overridden for individual targets during registration.

80

1-65535

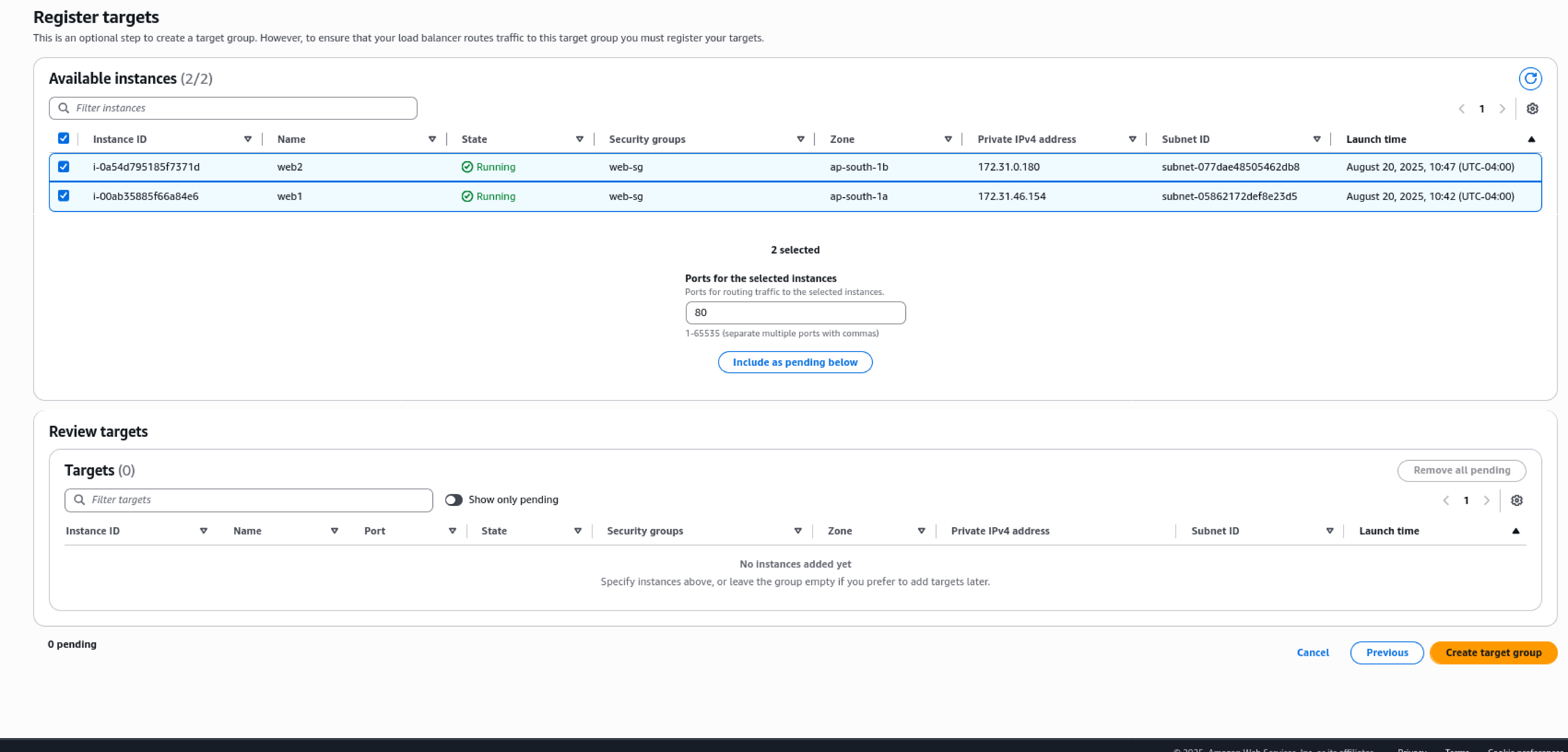
IP address type

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



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 (2/2)

☑	Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
☑	i-0a54d795185f7371d	web2	✓ Running	web-sg	ap-south-1b	172.31.0.180	subnet-077dae48505462db8	August 20, 2025, 10:47 (UTC-04:00)
☑	i-00ab35885f66a84e6	web1	✓ Running	web-sg	ap-south-1a	172.31.46.154	subnet-05862172def8e23d5	August 20, 2025, 10:42 (UTC-04:00)

2 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Review targets

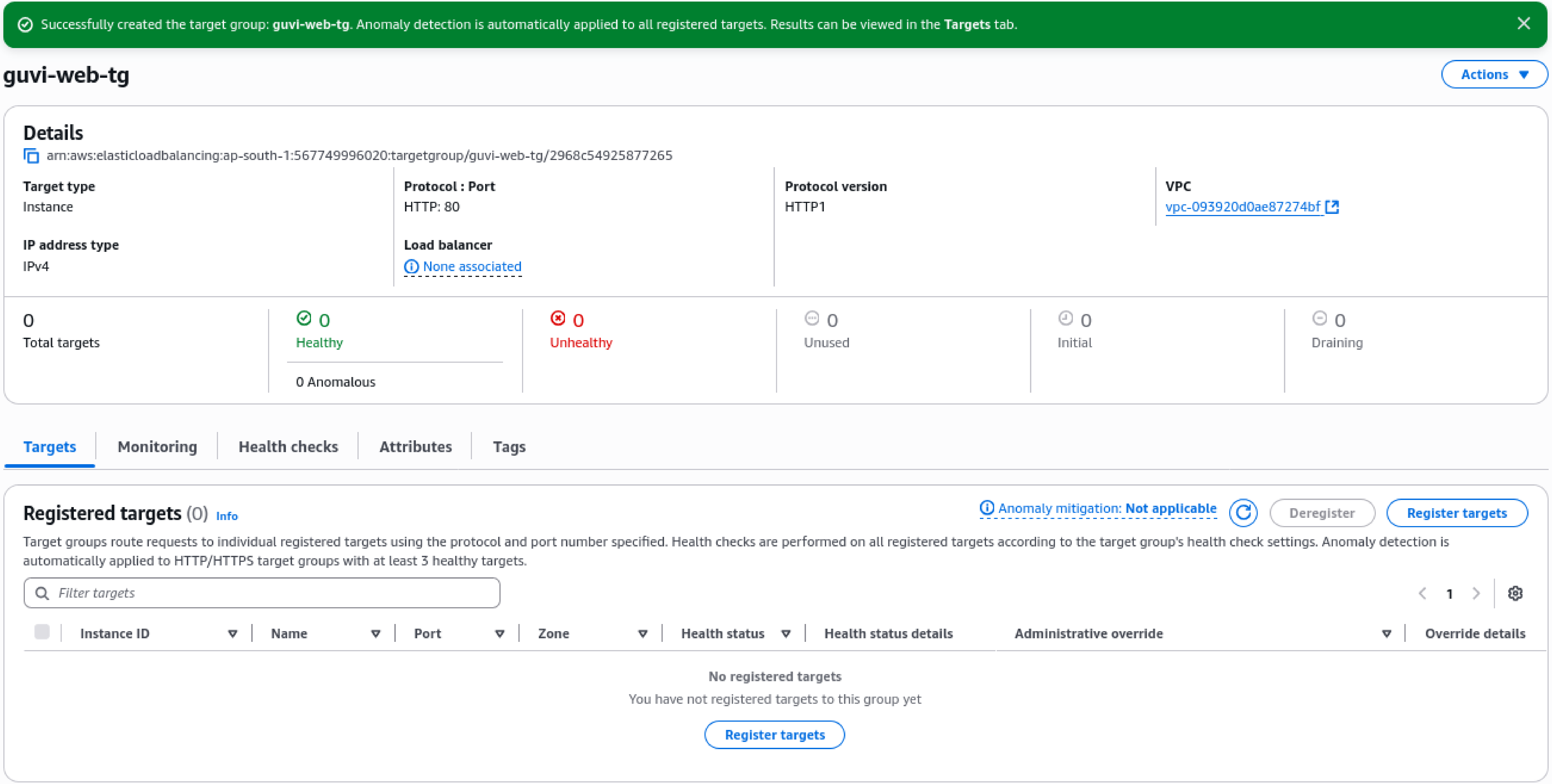
Targets (0)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time

No instances added yet

Specify instances above, or leave the group empty if you prefer to add targets later.

0 pending



Successfully created the target group: **guvi-web-tg**. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the **Targets** tab.

guvi-web-tg

Details

arn:aws:elasticloadbalancing:ap-south-1:567749996020:targetgroup/guvi-web-tg/2968c54925877265

Target type
Instance

Protocol : Port
HTTP: 80

Protocol version
HTTP1

VPC
vpc-093920d0ae87274bf

IP address type
IPv4

Load balancer
None associated

0 Total targets	✓ 0 Healthy 0 Anomalous	✗ 0 Unhealthy	0 Unused	0 Initial	0 Draining

Registered targets (0) Info

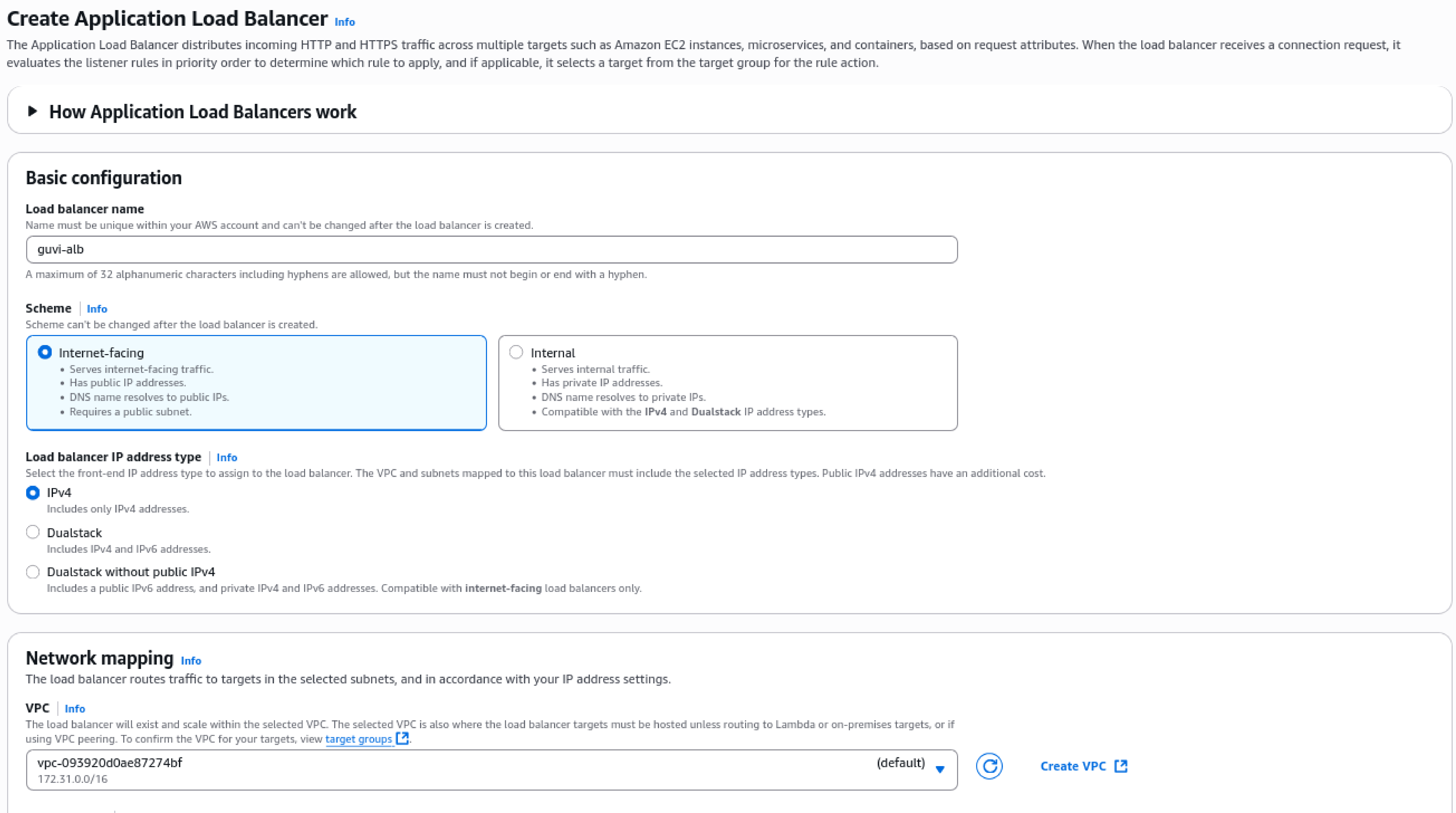
Anomaly mitigation: **Not applicable**

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

□	Instance ID	Name	Port	Zone	Health status	Health status details	Administrative override	Override details

No registered targets

You have not registered targets to this group yet



Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▶ How Application Load Balancers work

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

guvi-alb

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

Scheme | Info

Scheme can't be changed after the load balancer is created.

● Internet-facing
- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

○ Internal
- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the **IPv4** and **Dualstack** IP address types.

Load balancer IP address type | Info

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

● IPv4
Includes only IPv4 addresses.

○ Dualstack
Includes IPv4 and IPv6 addresses.

○ Dualstack without public IPv4
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

Network mapping Info

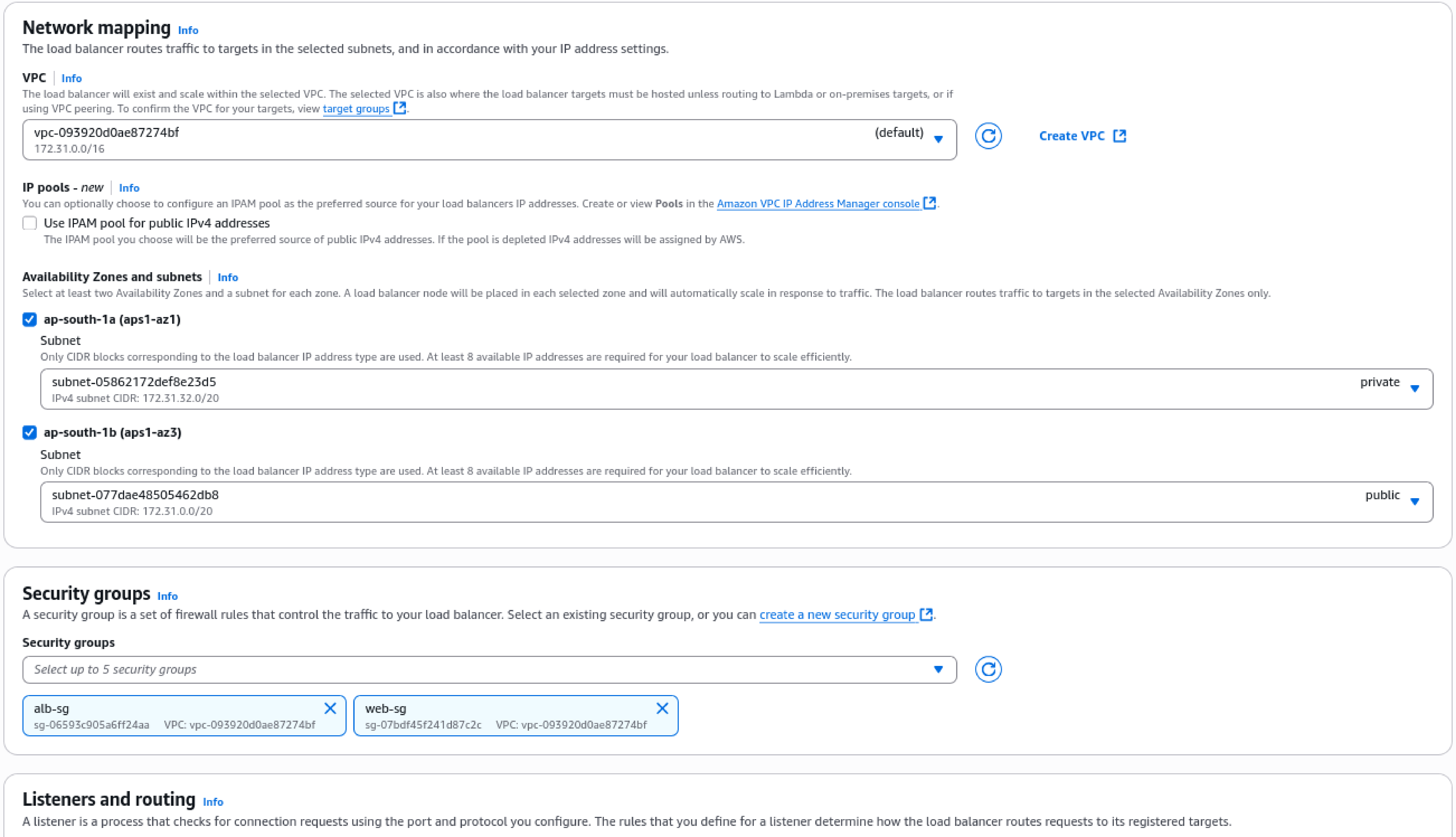
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

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 or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view target groups.

vpc-093920d0ae87274bf (default) ▼
172.31.0.0/16

Create VPC



Network mapping

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

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 or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view target groups.

vpc-093920d0ae87274bf (default) ▼
172.31.0.0/16

IP pools - *new* | Info

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view **Pools** in the Amazon VPC IP Address Manager console.

☐ Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets | Info

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

☑ **ap-south-1a (aps1-az1)**

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-05862172def8e23d5 private ▼
IPv4 subnet CIDR: 172.31.32.0/20

☑ **ap-south-1b (aps1-az3)**

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-077dae48505462db8 public ▼
IPv4 subnet CIDR: 172.31.0.0/20

Security groups

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

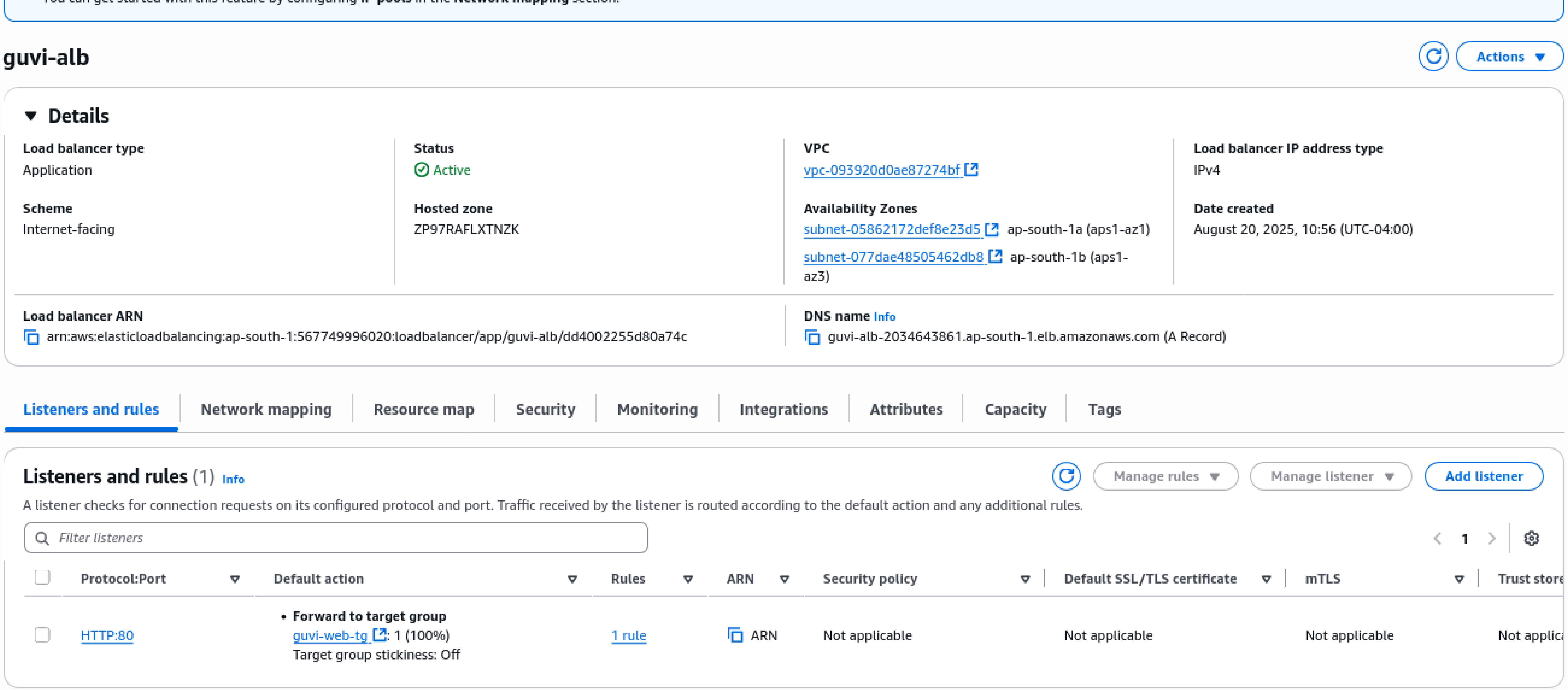
Select up to 5 security groups ▼

alb-sg
sg-06593c905a6ff24aa VPC: vpc-093920d0ae87274bf

web-sg
sg-07bdf45f241d87c2c VPC: vpc-093920d0ae87274bf

Listeners and routing

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.



You can get started with this feature by configuring IP pools in the Network mapping section.

guvi-alb

Details

Load balancer type
Application

Status
Active

VPC
vpc-093920d0ae87274bf

Load balancer IP address type
IPv4

Scheme
Internet-facing

Hosted zone
ZP97RAFLXTNZK

Availability Zones
subnet-05862172def8e23d5 ap-south-1a (aps1-az1)
subnet-077dae48505462db8 ap-south-1b (aps1-az3)

Date created
August 20, 2025, 10:56 (UTC-04:00)

Load balancer ARN
arn:aws:elasticloadbalancing:ap-south-1:567749996020:loadbalancer/app/guvi-alb/dd4002255d80a74c

DNS name Info
guvi-alb-2034643861.ap-south-1.elb.amazonaws.com (A Record)

Listeners and rules (1) Info

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

□	Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS	Trust store
□	HTTP:80	• Forward to target group guvi-web-tg: 1 (100%) Target group stickiness: Off	1 rule	ARN	Not applicable	Not applicable	Not applicable	Not applica