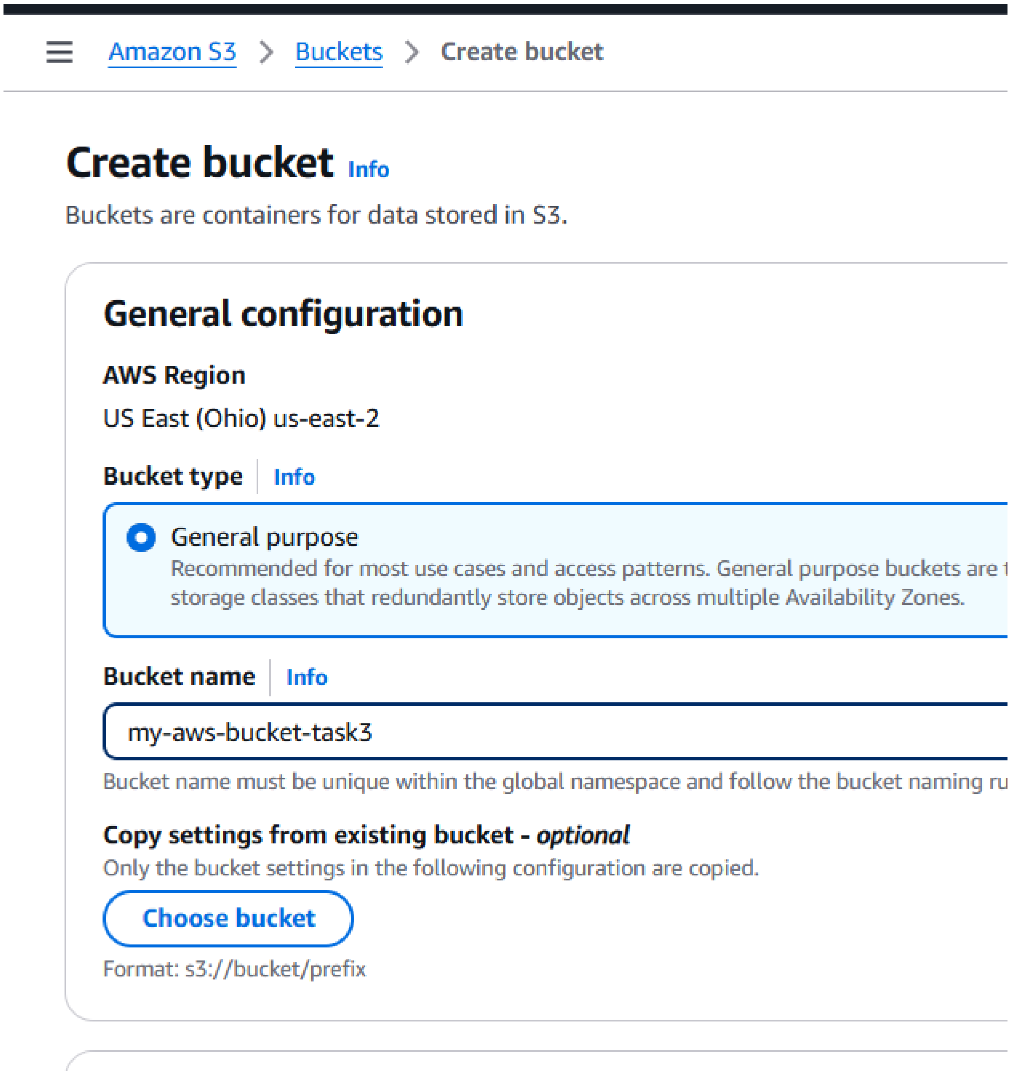
AWS Task-3

Task Description:

1. Create a S3 bucket, with no public access and upload files to the bucket & view the logs using cloudwatch for the uploaded files.

2. Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address



Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (Ohio) us-east-2

Bucket type | Info

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are t
storage classes that redundantly store objects across multiple Availability Zones.

Bucket name | Info

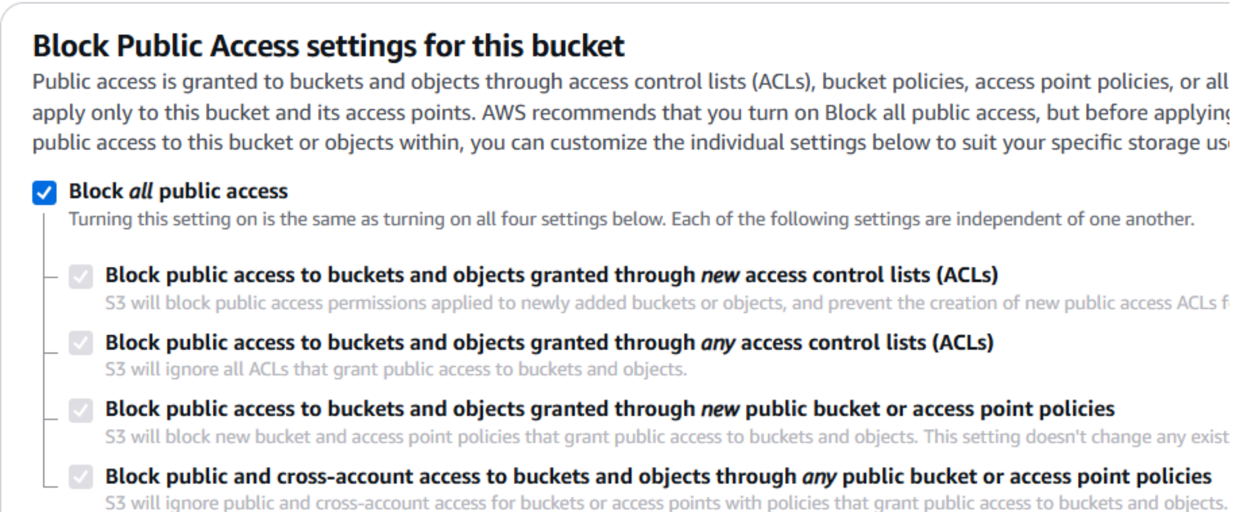
my-aws-bucket-task3

Bucket name must be unique within the global namespace and follow the bucket naming ru

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

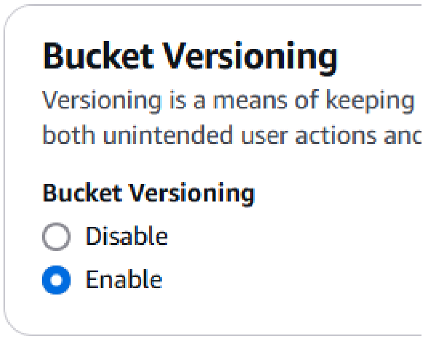


Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all
apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applyin
public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage us

☑ **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 f
- ☑ **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 exist
- ☑ **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.



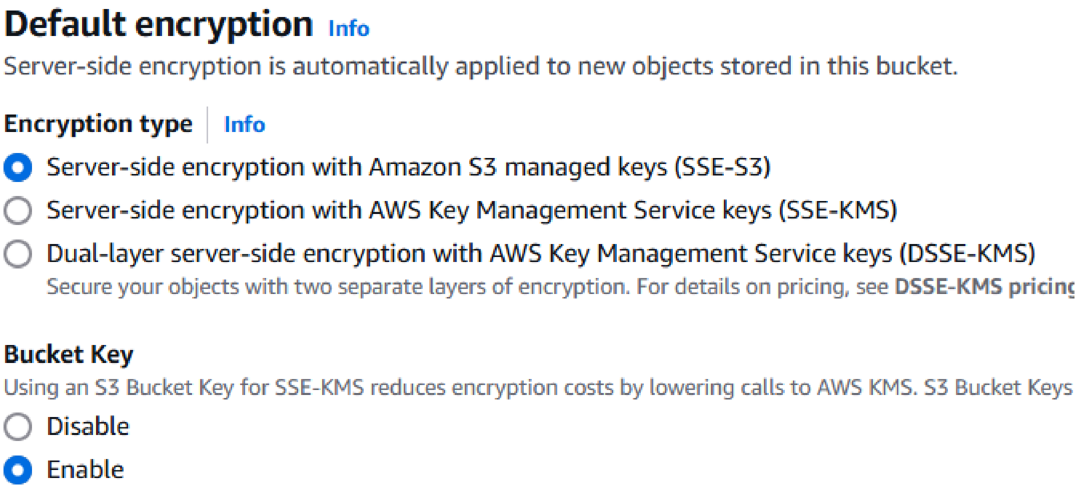
Bucket Versioning

Versioning is a means of keeping
both unintended user actions anc

Bucket Versioning

○ Disable

● Enable



Default encryption Info

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

Encryption type | Info

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

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

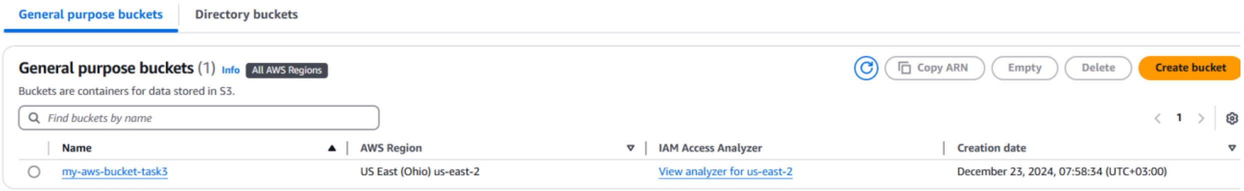
○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing**

Bucket Key

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

○ Disable

● Enable

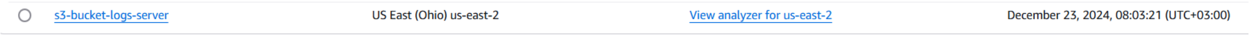


General purpose buckets (1) Info All AWS Regions

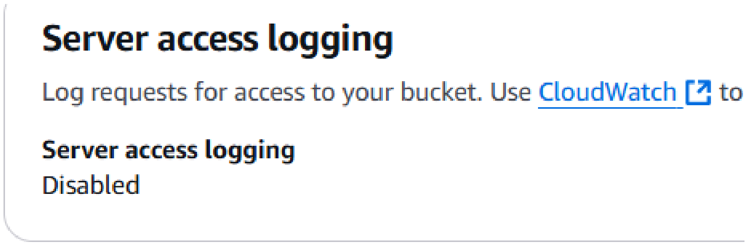
Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	my-aws-bucket-task3	US East (Ohio) us-east-2	View analyzer for us-east-2	December 23, 2024, 07:58:34 (UTC+03:00)

Now create another bucket for logging access



○	s3-bucket-logs-server	US East (Ohio) us-east-2	View analyzer for us-east-2	December 23, 2024, 08:03:21 (UTC+03:00)



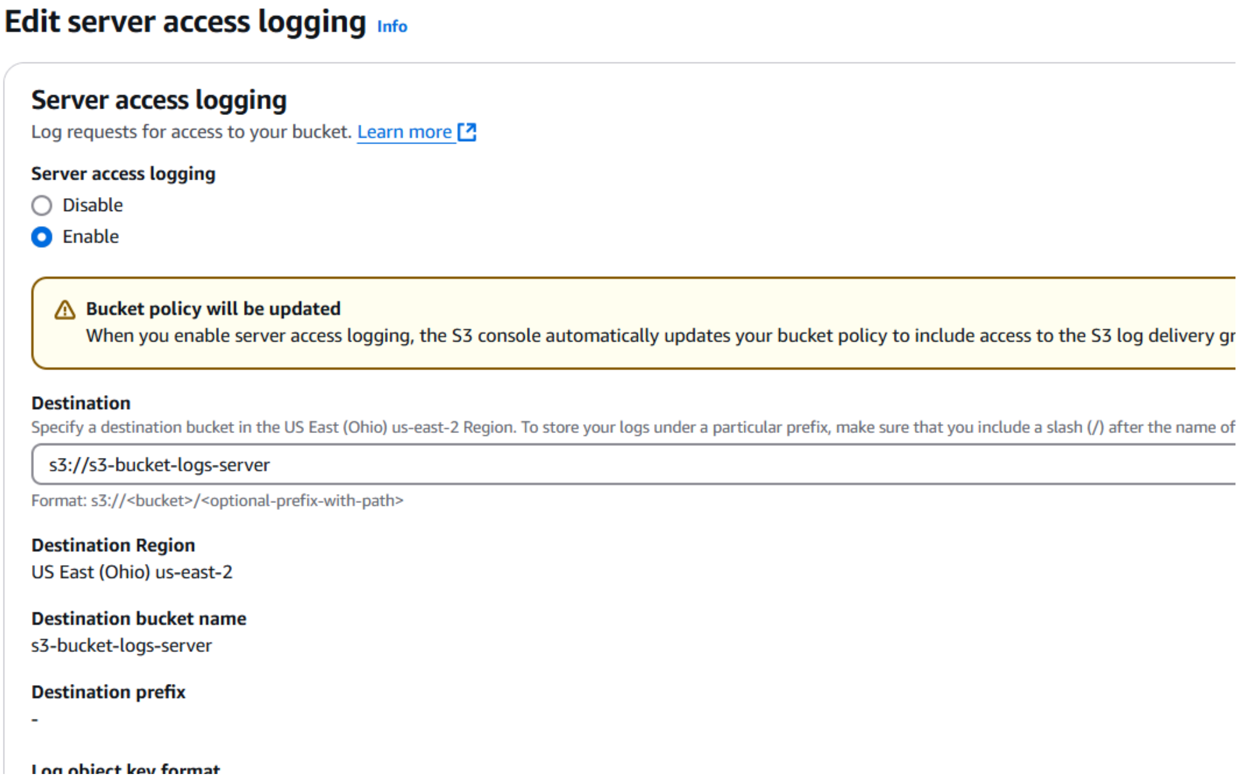
Server access logging

Log requests for access to your bucket. Use CloudWatch to

Server access logging

Disabled

Select the log server for your bucket to store



Edit server access logging Info

Server access logging

Log requests for access to your bucket. Learn more

Server access logging

○ Disable

● Enable

Bucket policy will be updated

When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery gr

Destination

Specify a destination bucket in the US East (Ohio) us-east-2 Region. To store your logs under a particular prefix, make sure that you include a slash (/) after the name of

s3://s3-bucket-logs-server

Format: s3://<bucket>/<optional-prefix-with-path>

Destination Region

US East (Ohio) us-east-2

Destination bucket name

s3-bucket-logs-server

Destination prefix

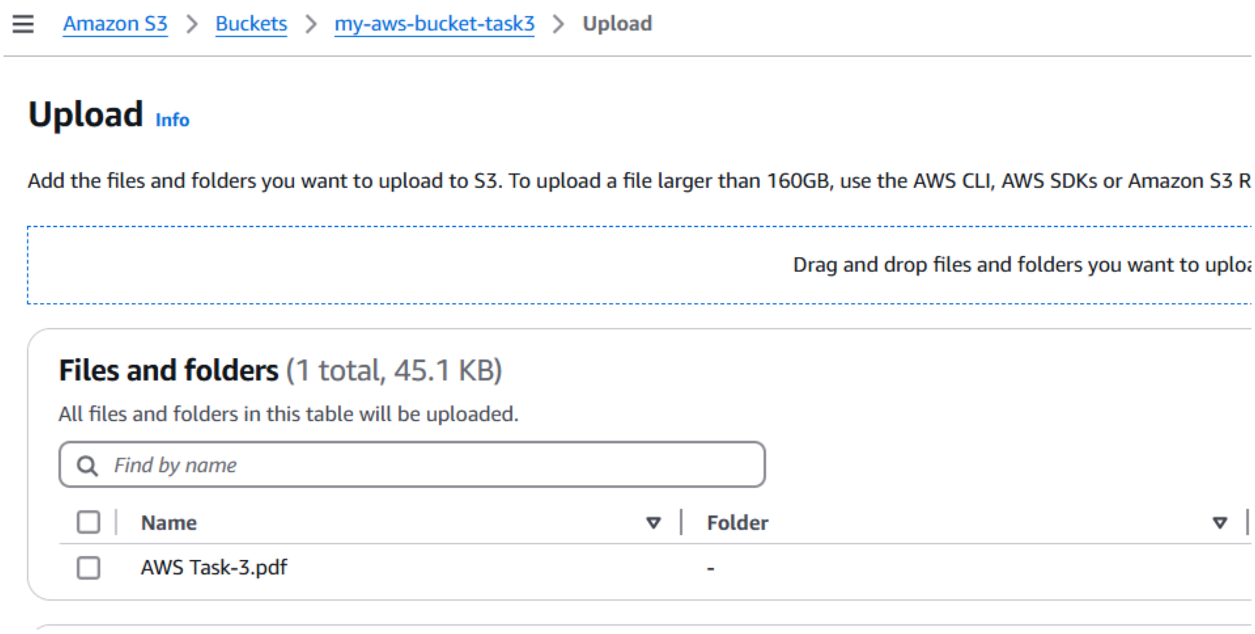
-

Log object key format

Now upload any file into your s3 bucket

It will take few minutes to reflect the logs

Meanwhile we can verify permissions are there on S3 bucket logs



Upload Info

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

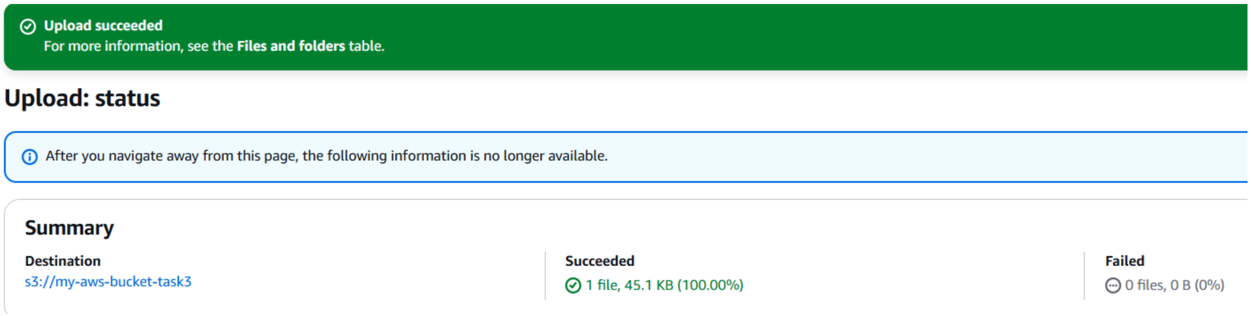
Drag and drop files and folders you want to uploa

Files and folders (1 total, 45.1 KB)

All files and folders in this table will be uploaded.

Find by name

□	Name	Folder
□	AWS Task-3.pdf	-


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

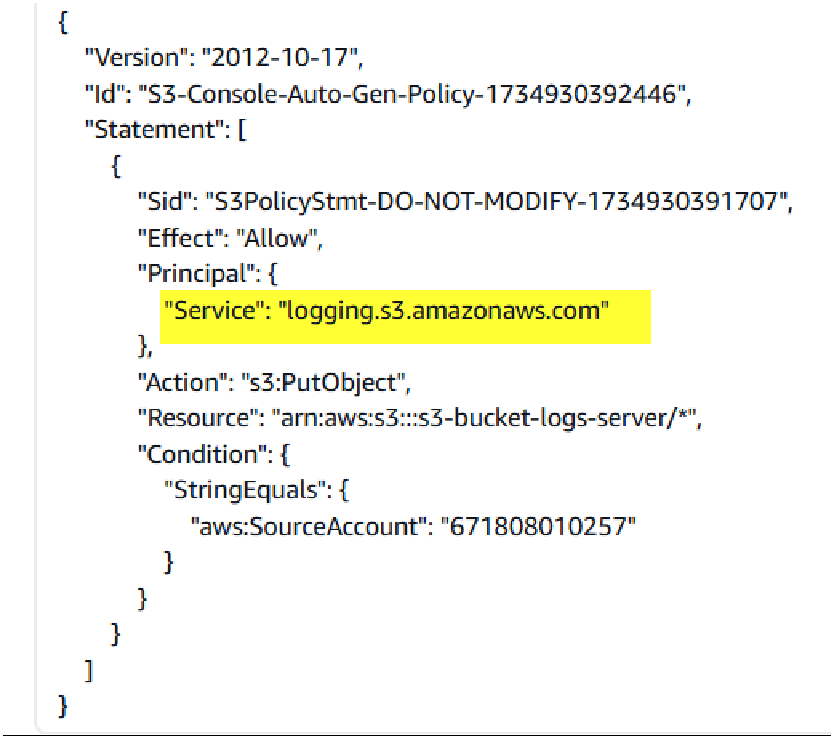
Upload: status

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

Summary

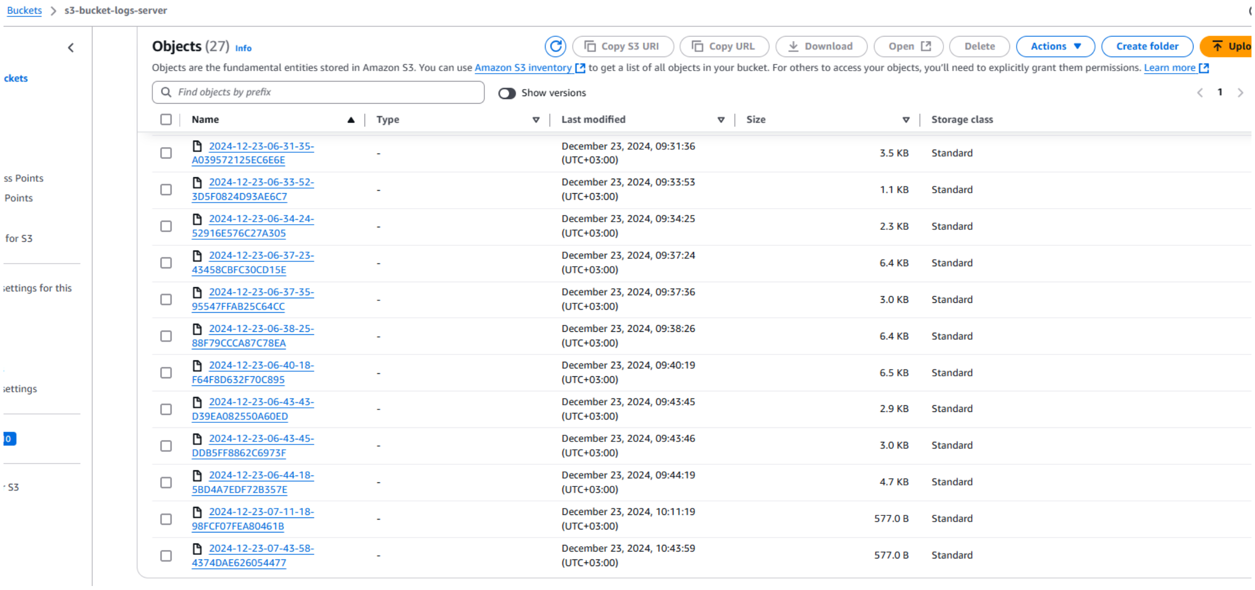
Destination	Succeeded	Failed
s3://my-aws-bucket-task3	1 file, 45.1 KB (100.00%)	0 files, 0 B (0%)

Now go to logs bucket and view the logs



```
{
  "Version": "2012-10-17",
  "Id": "S3-Console-Auto-Gen-Policy-1734930392446",
  "Statement": [
    {
      "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1734930391707",
      "Effect": "Allow",
      "Principal": {
        "Service": "logging.s3.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::s3-bucket-logs-server/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "671808010257"
        }
      }
    }
  ]
}
```

Note: logs take 30 min to 1 hour to reflect



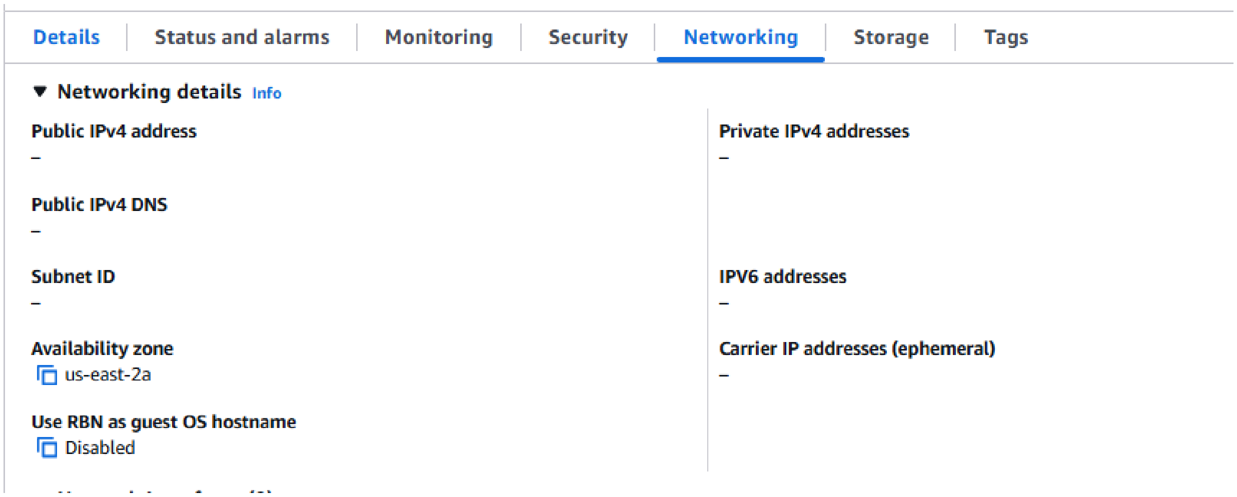
Objects (27) Info

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

□	Name	Type	Last modified	Size	Storage class
□	2024-12-23-06-31-35-A039572125EC6E6E	-	December 23, 2024, 09:31:36 (UTC+03:00)	3.5 KB	Standard
□	2024-12-23-06-33-52-3D5F0824D93AE6C7	-	December 23, 2024, 09:33:53 (UTC+03:00)	1.1 KB	Standard
□	2024-12-23-06-34-24-52916E576C27A305	-	December 23, 2024, 09:34:25 (UTC+03:00)	2.3 KB	Standard
□	2024-12-23-06-37-23-43458CBFC30CD15E	-	December 23, 2024, 09:37:24 (UTC+03:00)	6.4 KB	Standard
□	2024-12-23-06-37-35-95547FFAB25C64CC	-	December 23, 2024, 09:37:36 (UTC+03:00)	3.0 KB	Standard
□	2024-12-23-06-38-25-88F79CCCA87C78EA	-	December 23, 2024, 09:38:26 (UTC+03:00)	6.4 KB	Standard
□	2024-12-23-06-40-18-F64F8D632F70C895	-	December 23, 2024, 09:40:19 (UTC+03:00)	6.5 KB	Standard
□	2024-12-23-06-43-43-D39EA082550A60ED	-	December 23, 2024, 09:43:45 (UTC+03:00)	2.9 KB	Standard
□	2024-12-23-06-43-45-DDB5FF8862C6973F	-	December 23, 2024, 09:43:46 (UTC+03:00)	3.0 KB	Standard
□	2024-12-23-06-44-18-5BD4A7EDF72B357E	-	December 23, 2024, 09:44:19 (UTC+03:00)	4.7 KB	Standard
□	2024-12-23-07-11-18-98FCF07FEA80461B	-	December 23, 2024, 10:11:19 (UTC+03:00)	577.0 B	Standard
□	2024-12-23-07-43-58-4374DAE626054477	-	December 23, 2024, 10:43:59 (UTC+03:00)	577.0 B	Standard

B) **<u>step 1: create separate Instances with different availability zone</u>**

Apache Server 1 , Apache Server 2



▼ Networking details

Public IPv4 address
–

Public IPv4 DNS
–

Subnet ID
–

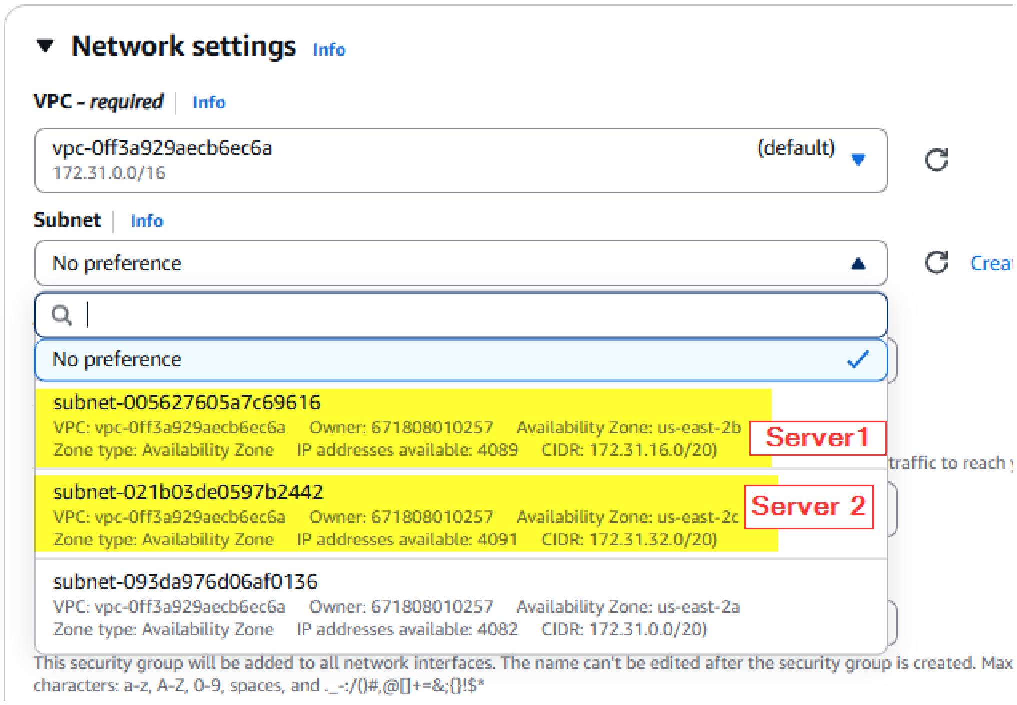
Availability zone
us-east-2a

Use RBN as guest OS hostname
Disabled

Private IPv4 addresses
–

IPV6 addresses
–

Carrier IP addresses (ephemeral)
–



▼ Network settings

VPC - *required*

vpc-0ff3a929aecb6ec6a (default)
172.31.0.0/16

Subnet

No preference ▲

No preference ✓

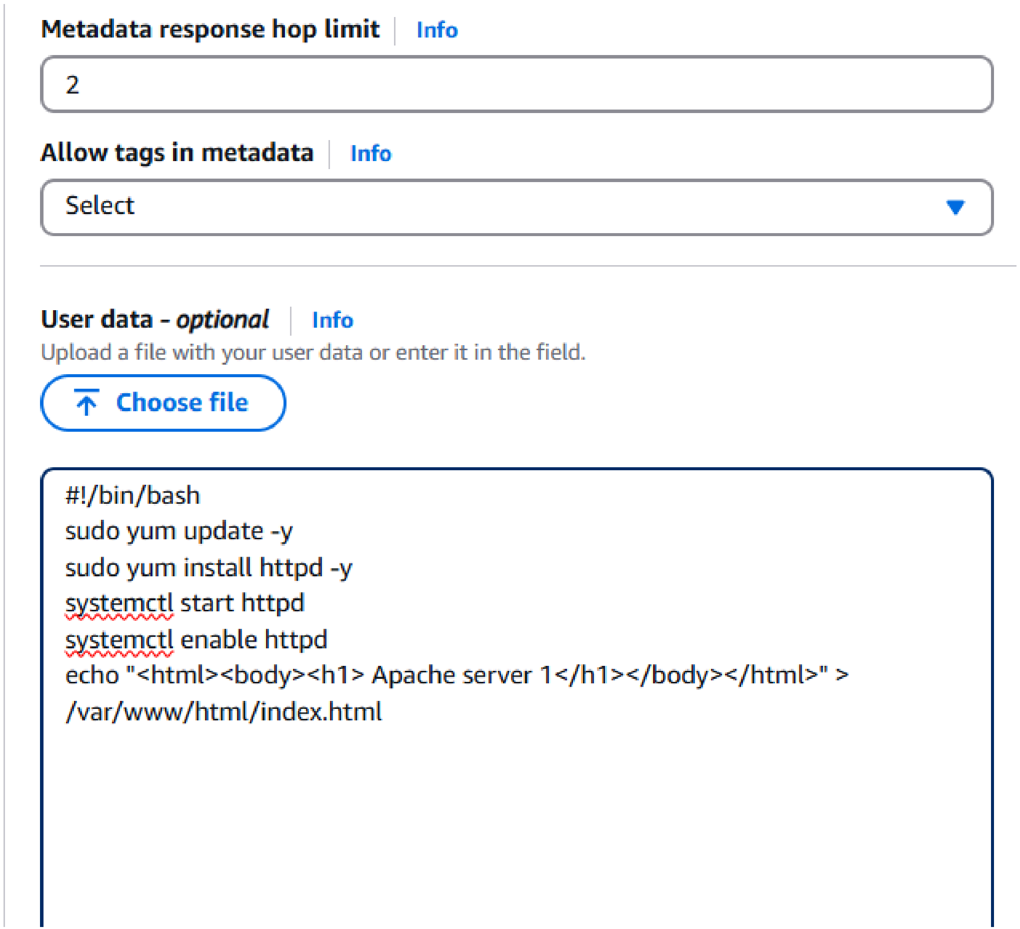
subnet-005627605a7c69616
VPC: vpc-0ff3a929aecb6ec6a Owner: 671808010257 Availability Zone: us-east-2b
Zone type: Availability Zone IP addresses available: 4089 CIDR: 172.31.16.0/20)

subnet-021b03de0597b2442
VPC: vpc-0ff3a929aecb6ec6a Owner: 671808010257 Availability Zone: us-east-2c
Zone type: Availability Zone IP addresses available: 4091 CIDR: 172.31.32.0/20)

subnet-093da976d06af0136
VPC: vpc-0ff3a929aecb6ec6a Owner: 671808010257 Availability Zone: us-east-2a
Zone type: Availability Zone IP addresses available: 4082 CIDR: 172.31.0.0/20)

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

Metadata to be use inside



Metadata response hop limit

2

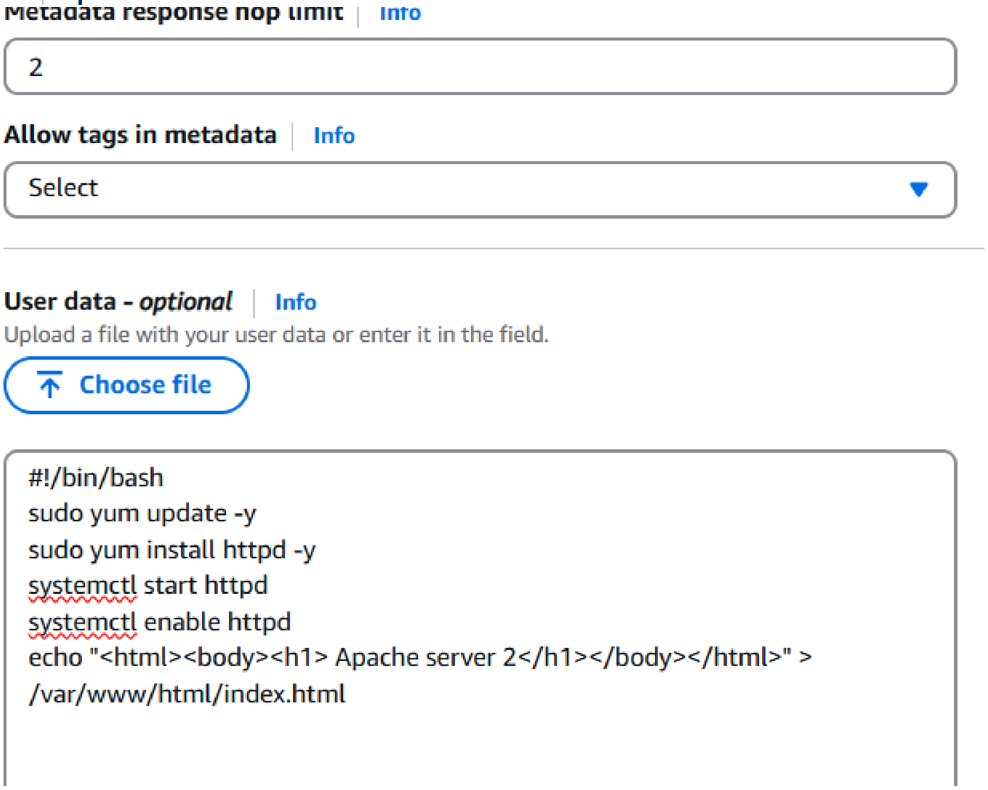
Allow tags in metadata

Select

User data - *optional*

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

```
#!/bin/bash
sudo yum update -y
sudo yum install httpd -y
systemctl start httpd
systemctl enable httpd
echo "<html><body><h1> Apache server 1</h1></body></html>" >
/var/www/html/index.html
```



Metadata response hop limit

2

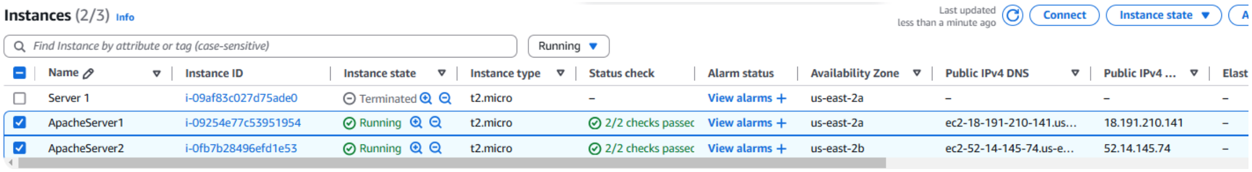
Allow tags in metadata

Select

User data - *optional*

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

```
#!/bin/bash
sudo yum update -y
sudo yum install httpd -y
systemctl start httpd
systemctl enable httpd
echo "<html><body><h1> Apache server 2</h1></body></html>" >
/var/www/html/index.html
```



Instances (2/3) Info

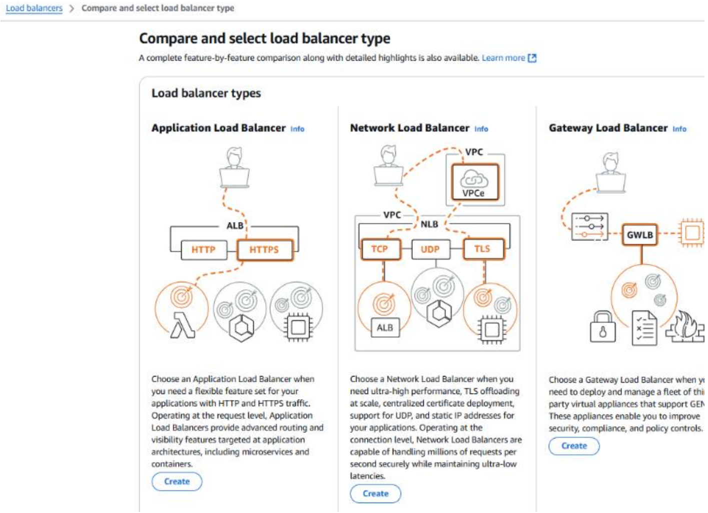
Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

Running ▼

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elast
□	Server 1	i-09af83c027d75ade0	Terminated	t2.micro	–	View alarms +	us-east-2a	–	–	–
☑	ApacheServer1	i-09254e77c53951954	Running	t2.micro	2/2 checks passec	View alarms +	us-east-2a	ec2-18-191-210-141.us...	18.191.210.141	–
☑	ApacheServer2	i-0fb7b28496efd1e53	Running	t2.micro	2/2 checks passec	View alarms +	us-east-2b	ec2-52-14-145-74.us-e...	52.14.145.74	–

step 2: create Application Loadbalancer with listner port 80 HTTP and add Servers into it



Load balancers > Compare and select load balancer type

Compare and select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. Learn more

Load balancer types

Application Load Balancer Info

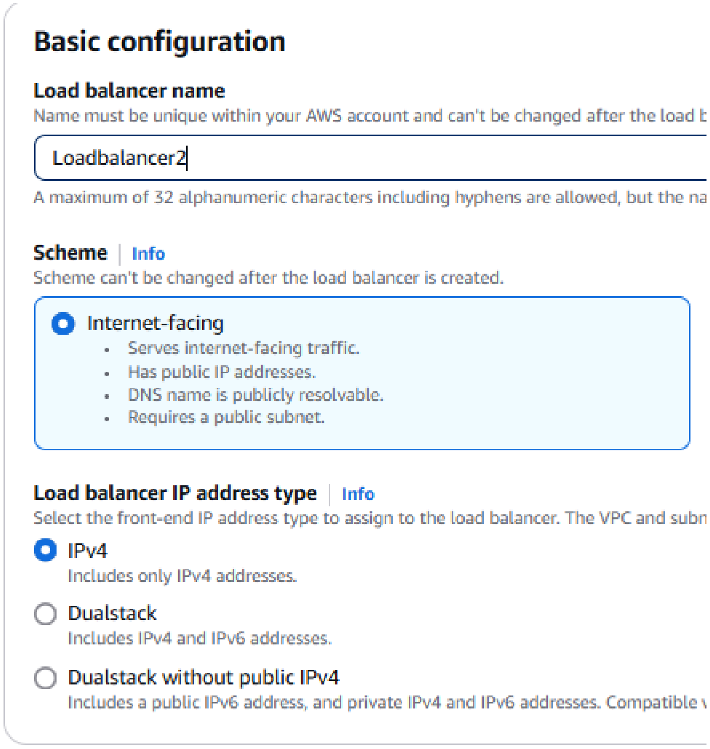
Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Network Load Balancer Info

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Gateway Load Balancer Info

Choose a Gateway Load Balancer when y need to deploy and manage a fleet of thi party virtual appliances that support GEN These appliances enable you to improve security, compliance, and policy controls.



Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load b

Loadbalancer2

A maximum of 32 alphanumeric characters including hyphens are allowed, but the na

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 is publicly resolvable.
- Requires a public subnet.

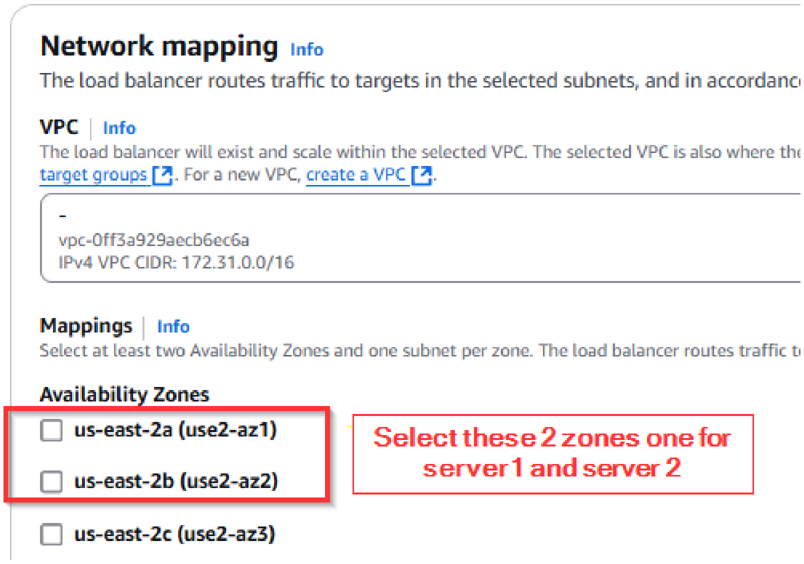
Load balancer IP address type | Info

Select the front-end IP address type to assign to the load balancer. The VPC and subn

● 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 w



Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordanc

VPC | Info

The load balancer will exist and scale within the selected VPC. The selected VPC is also where th target groups. For a new VPC, create a VPC.

-
vpc-0ff3a929aecb6ec6a
IPv4 VPC CIDR: 172.31.0.0/16

Mappings | Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic t

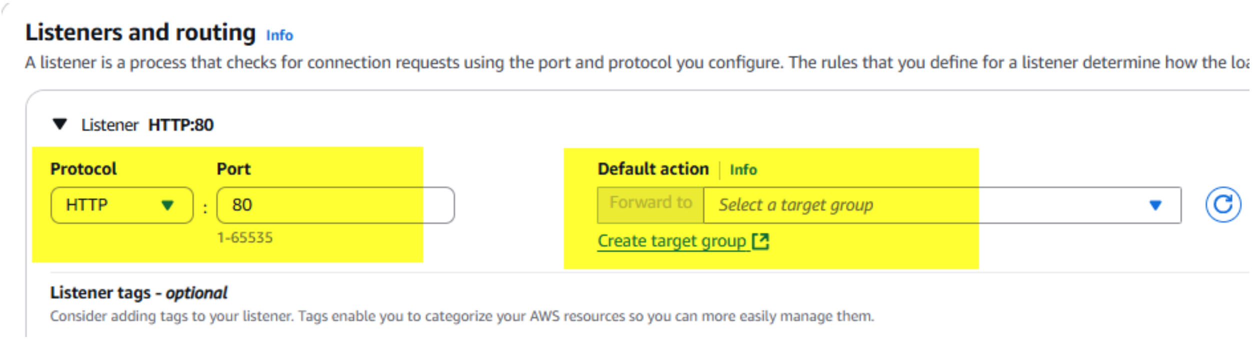
Availability Zones

□ **us-east-2a (use2-az1)**

□ **us-east-2b (use2-az2)**

□ **us-east-2c (use2-az3)**

Select these 2 zones one for server1 and server 2



Listeners and routing Info

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 loa

▼ Listener **HTTP:80**

Protocol: HTTP ▼

Port: 80

1-65535

Default action | Info

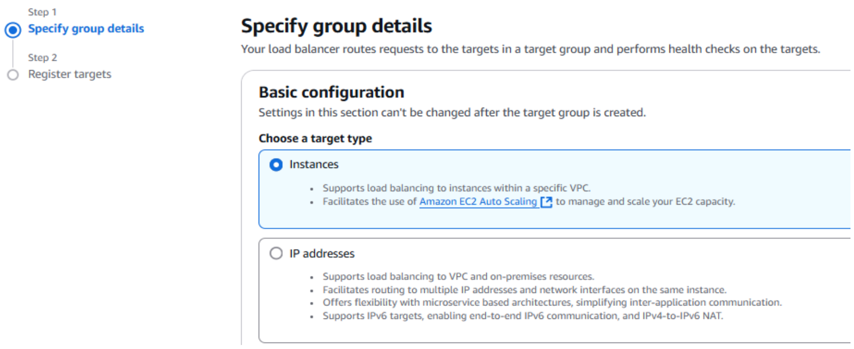
Forward to: *Select a target group* ▼

Create target group

Listener tags - *optional*

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Create Target Group



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.

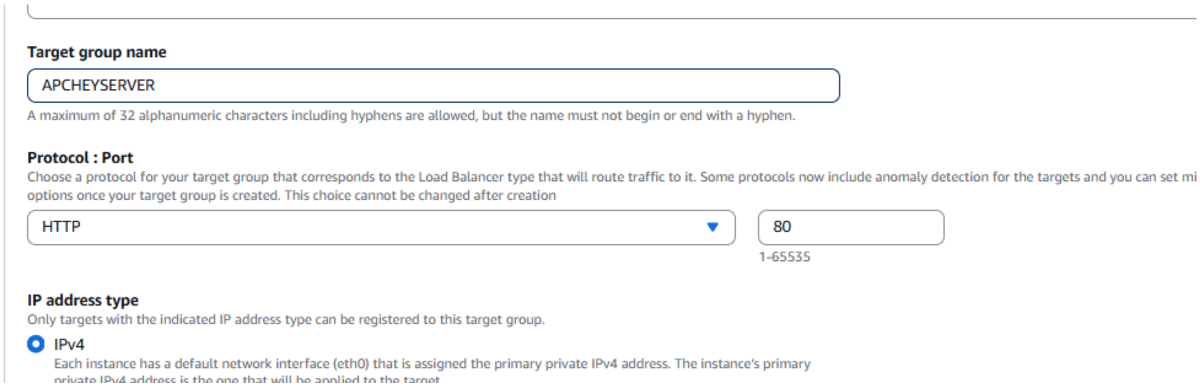
Choose a target type

● 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.



Target group name

APCHEYSERVER

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 mi options once your target group is created. This choice cannot be changed after creation

HTTP ▼ 80

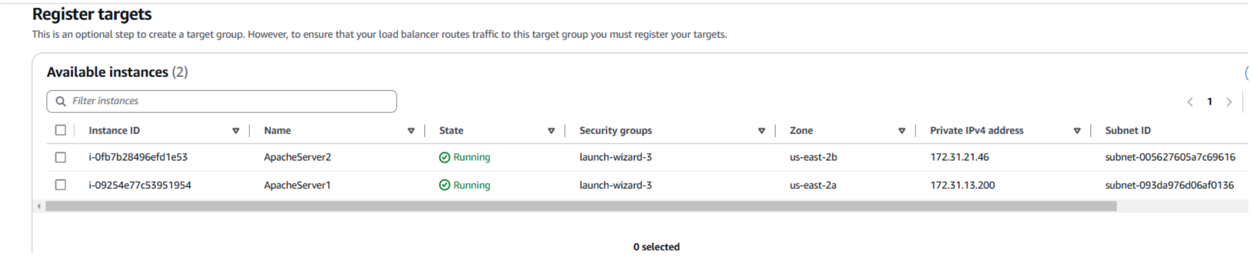
1-65535

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



Register targets

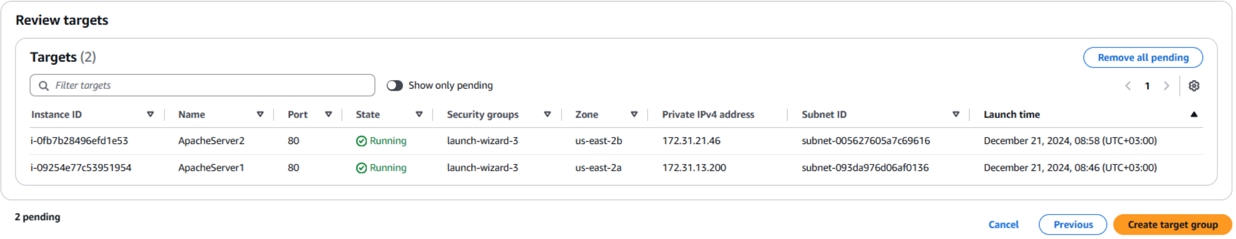
This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2)

Filter instances

□	Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID
□	i-0fb7b28496efd1e53	ApacheServer2	✓ Running	launch-wizard-3	us-east-2b	172.31.21.46	subnet-005627605a7c69616
□	i-09254e77c53951954	ApacheServer1	✓ Running	launch-wizard-3	us-east-2a	172.31.13.200	subnet-093da976d06af0136

0 selected



Review targets

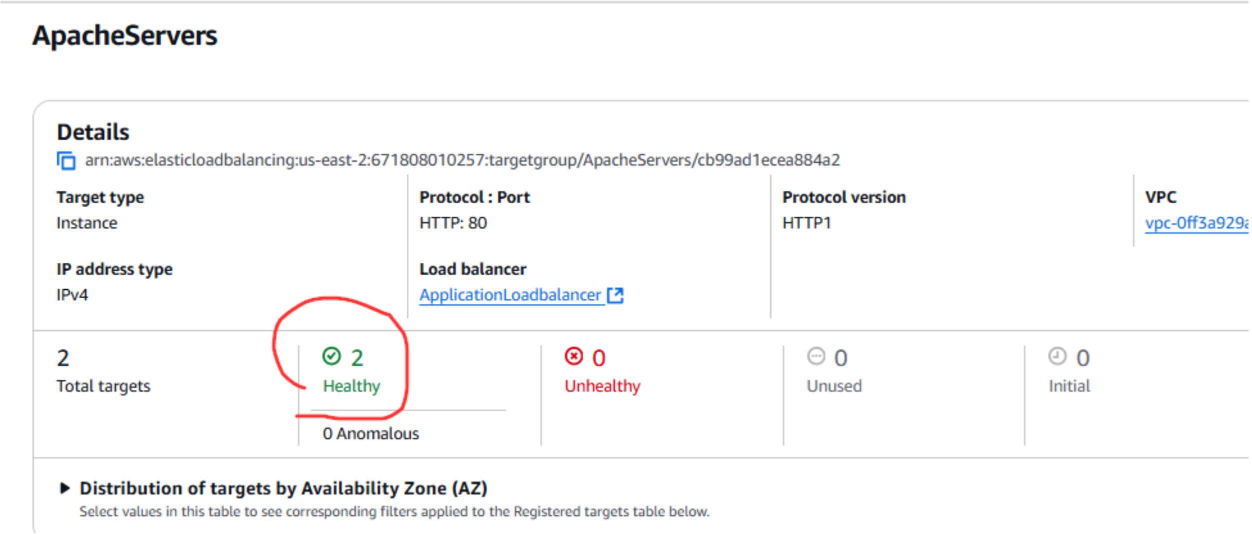
Targets (2)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-0fb7b28496efd1e53	ApacheServer2	80	✓ Running	launch-wizard-3	us-east-2b	172.31.21.46	subnet-005627605a7c69616	December 21, 2024, 08:58 (UTC+03:00)
i-09254e77c53951954	ApacheServer1	80	✓ Running	launch-wizard-3	us-east-2a	172.31.13.200	subnet-093da976d06af0136	December 21, 2024, 08:46 (UTC+03:00)

2 pending

Once created then select inside Create group

and backend server are healthy if ports and everything is fine



ApacheServers

Details

arn:aws:elasticloadbalancing:us-east-2:671808010257:targetgroup/ApacheServers/cb99ad1ecea884a2

Target type
Instance

Protocol : Port
HTTP: 80

Protocol version
HTTP1

VPC
vpc-0ff3a929a

IP address type
IPv4

Load balancer
ApplicationLoadbalancer

2
Total targets

✓ 2
Healthy

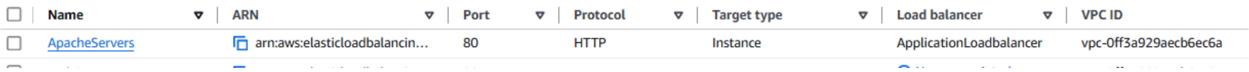
0 Anomalous

⊗ 0
Unhealthy

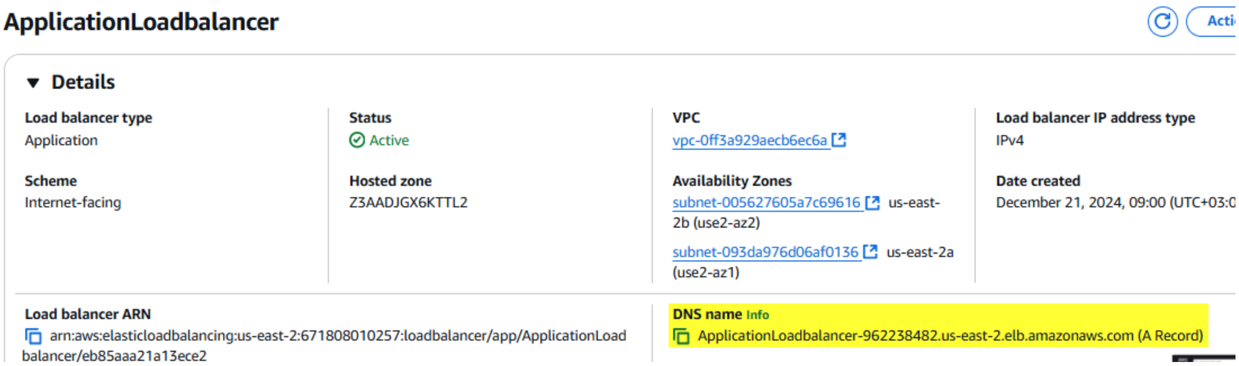
0
Unused

0
Initial

Select values in this table to see corresponding filters applied to the Registered targets table below.



□	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
□	ApacheServers	arn:aws:elasticloadbalancin...	80	HTTP	Instance	ApplicationLoadbalancer	vpc-0ff3a929aecb6ec6a



ApplicationLoadbalancer

▼ Details

Load balancer type
Application

Scheme
Internet-facing

Status
Active

Hosted zone
Z3AADJGX6KTTL2

VPC
vpc-0ff3a929aecb6ec6a

Availability Zones
subnet-005627605a7c69616 us-east-2b (use2-az2)
subnet-093da976d06af0136 us-east-2a (use2-az1)

Load balancer IP address type
IPv4

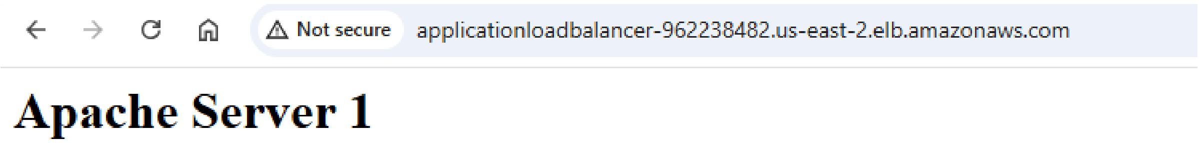
Date created
December 21, 2024, 09:00 (UTC+03:0

Load balancer ARN
arn:aws:elasticloadbalancing:us-east-2:671808010257:loadbalancer/app/ApplicationLoadbalancer/eb85aaa21a13ece2

DNS name Info
ApplicationLoadbalancer-962238482.us-east-2.elb.amazonaws.com (A Record)

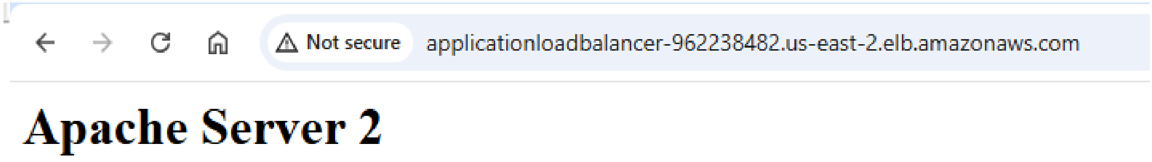
The above URL loadbalancer accesses from your browser , in case not working then edit security group and add Inbound RULE

Loadbalancer URL: http://applicationloadbalancer-962238482.us-east-2.elb.amazonaws.com/



Not secure applicationloadbalancer-962238482.us-east-2.elb.amazonaws.com

Apache Server 1



Not secure applicationloadbalancer-962238482.us-east-2.elb.amazonaws.com

Apache Server 2