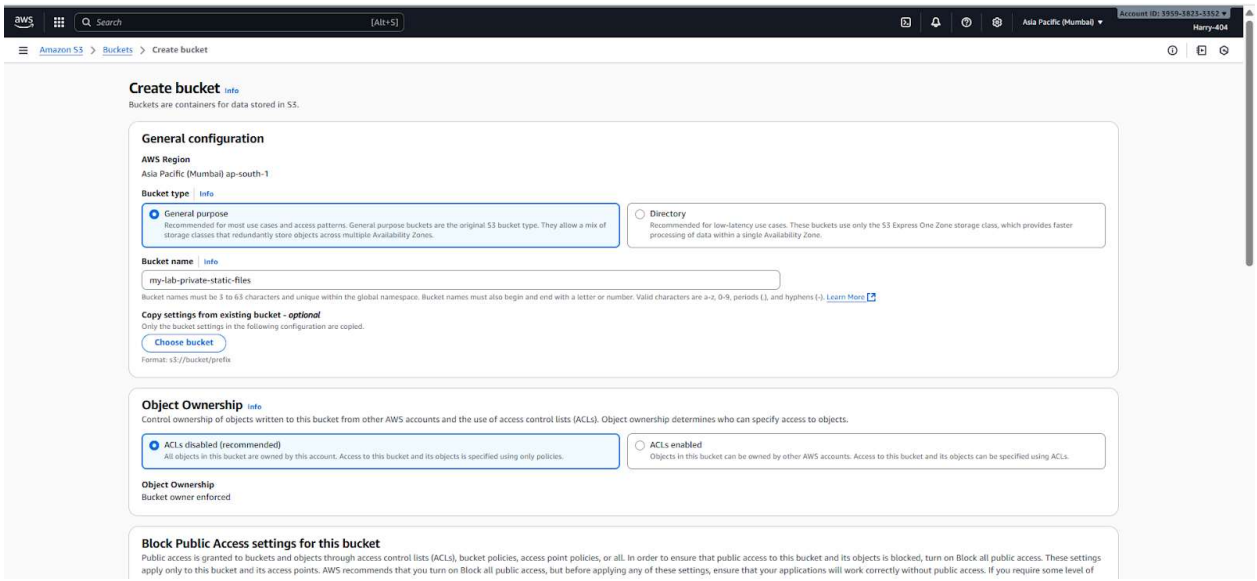
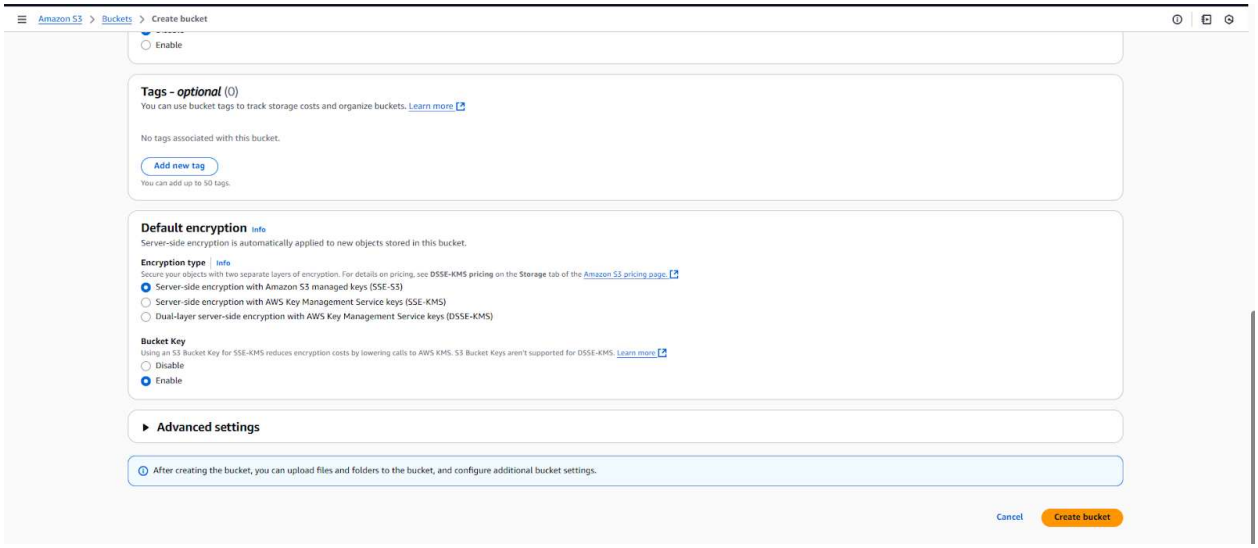
Secure Web Hosting on AWS using EC2, S3, IAM Roles, and Application Load Balancer

S3 Bucket (Static Files: logo.png, style.css)

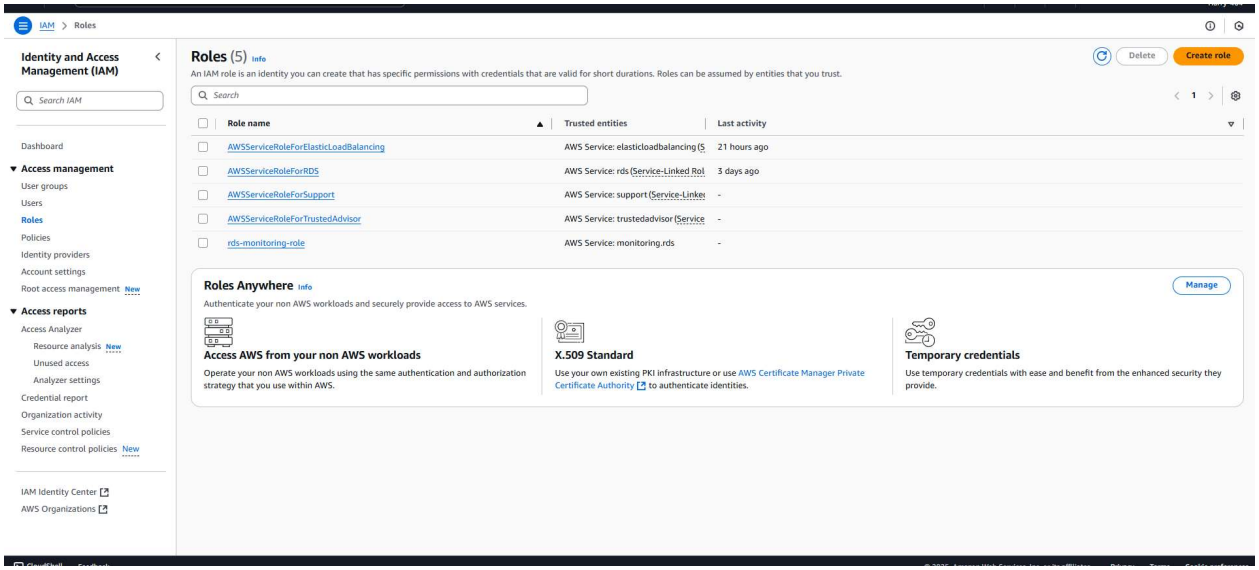
- Go to S3 → Create bucket → Name: `my-lab-private-static-files`
- Region: ap-south-1 (Mumbai)
- Block all public access: ON (recommended)
- ACLs: Disabled, Object Ownership: Bucket owner enforced
- Default encryption: SSE-S3 or SSE-KMS (recommended for production, optional for this lab)
- After creation: Upload your `logo.png` and `style.css` files to the bucket

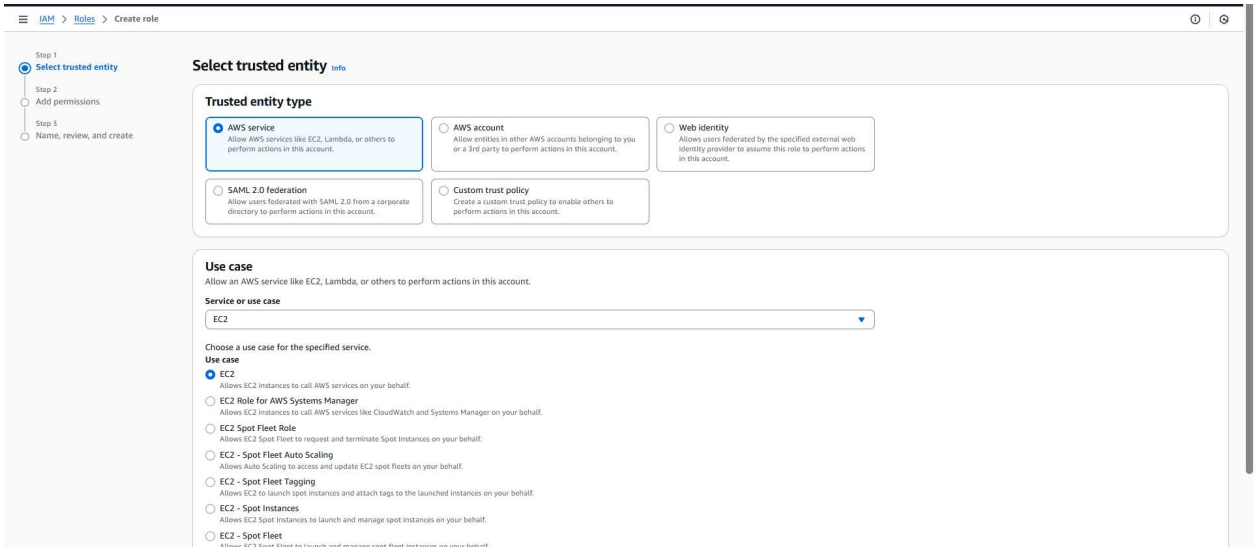


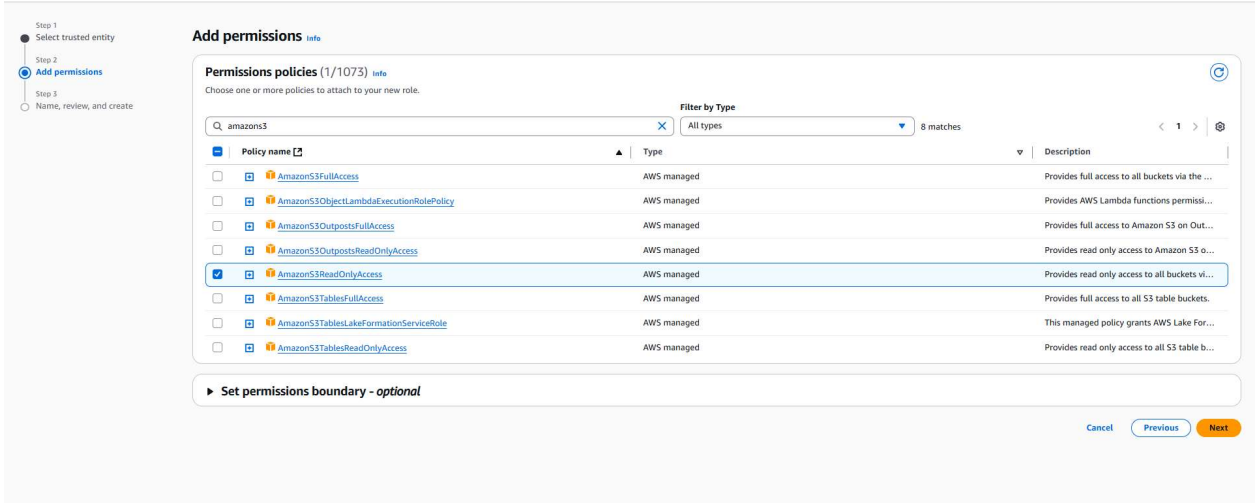


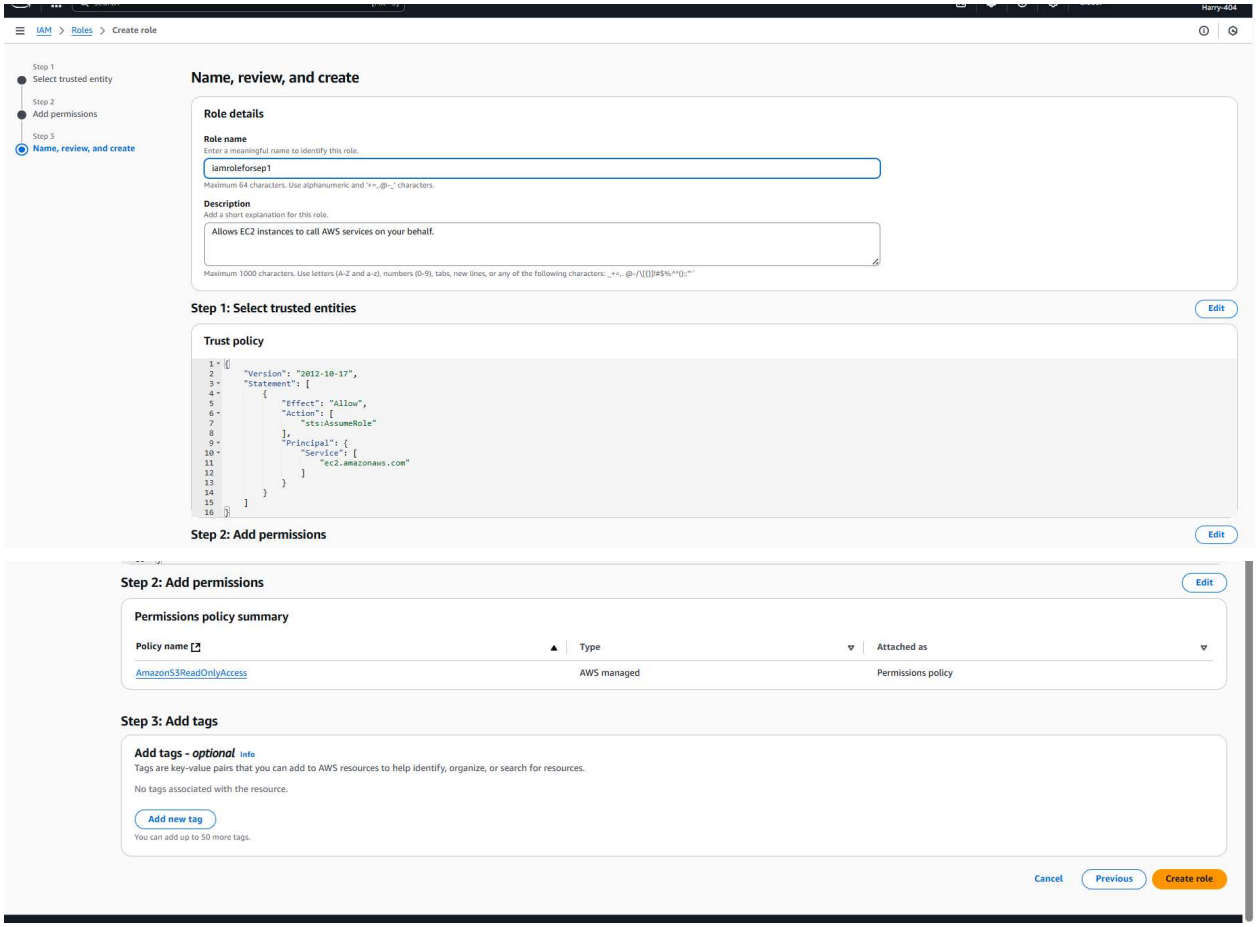
IAM Role (EC2 Instance Profile with S3 Read Permissions)

- Go to IAM → Roles → Create Role
- Trusted Entity: AWS Service → EC2
- Attach policy:
    - For full S3 read (lab/demo): `AmazonS3ReadOnlyAccess`
- Name: `iamroleforsep1` (or similar)
- Save role and assign to EC2 at launch


IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Roles (5) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Search
Role name
Trusted entities
Last activity
AWSServiceRoleForElasticLoadBalancing
AWS Service: elasticloadbalancing (S
21 hours ago
AWSServiceRoleForRDS
AWS Service: rds (Service-Linked Rol
3 days ago
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
-
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
-
rds-monitoring-role
AWS Service: monitoring.rds
-
Roles Anywhere Info
Manage
Authenticate your non AWS workloads and securely provide access to AWS services.
Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.
X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.
Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.


IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
EC2
Choose a use case for the specified service.
Use case
EC2
Allows EC2 instances to call AWS services on your behalf.
EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
EC2 - Spot Fleet


Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1/1073) Info
Choose one or more policies to attach to your new role.
Filter by Type
amazons3
All types
8 matches
Policy name
Type
Description
AmazonS3FullAccess
AWS managed
Provides full access to all buckets via the ...
AmazonS3ObjectLambdaExecutionRolePolicy
AWS managed
Provides AWS Lambda functions permissi...
AmazonS3OutpostsFullAccess
AWS managed
Provides full access to Amazon S3 on Out...
AmazonS3OutpostsReadOnlyAccess
AWS managed
Provides read only access to Amazon S3 o...
AmazonS3ReadOnlyAccess
AWS managed
Provides read only access to all buckets vi...
AmazonS3TablesFullAccess
AWS managed
Provides full access to all S3 table buckets.
AmazonS3TablesLakeFormationServiceRole
AWS managed
This managed policy grants AWS Lake For...
AmazonS3TablesReadOnlyAccess
AWS managed
Provides read only access to all S3 table b...
Set permissions boundary - optional
Cancel
Previous
Next

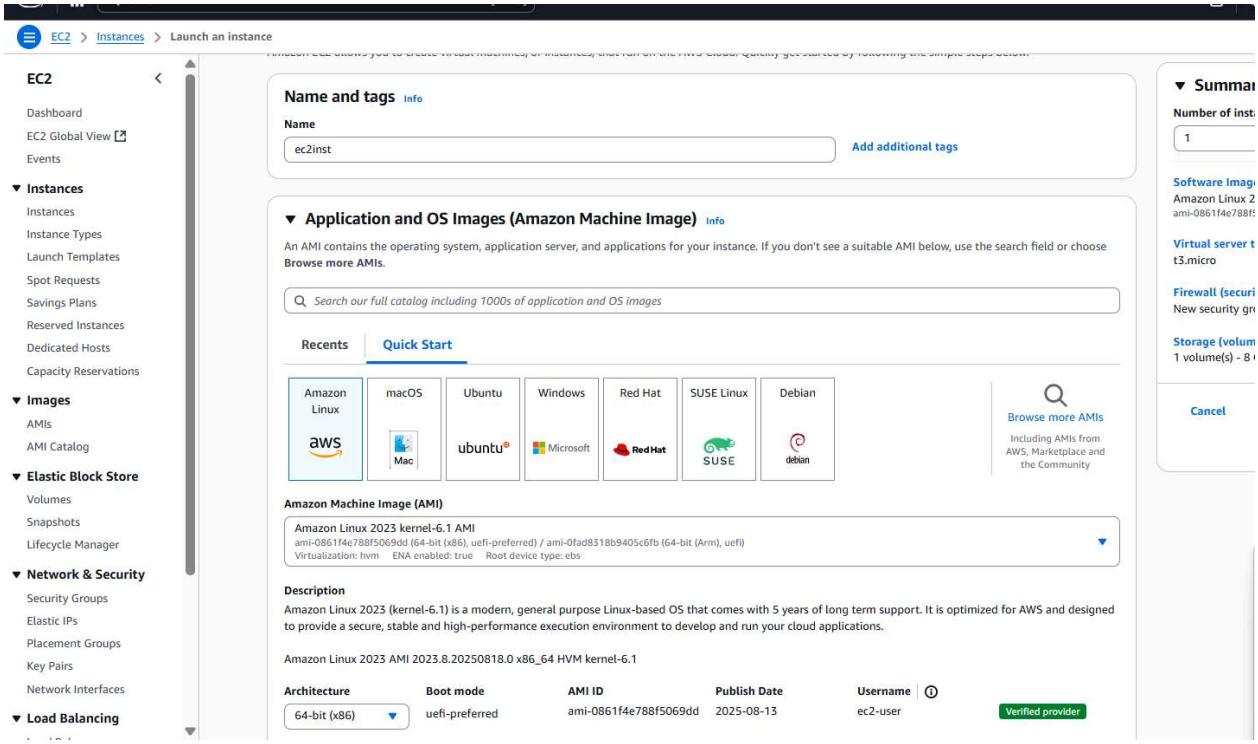

IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
iamroleforsep1
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, .@-/\[{}]!#$%^*();:"'
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
"Service": [
"ec2.amazonaws.com"
]
}
}
]
}
Step 2: Add permissions
Edit

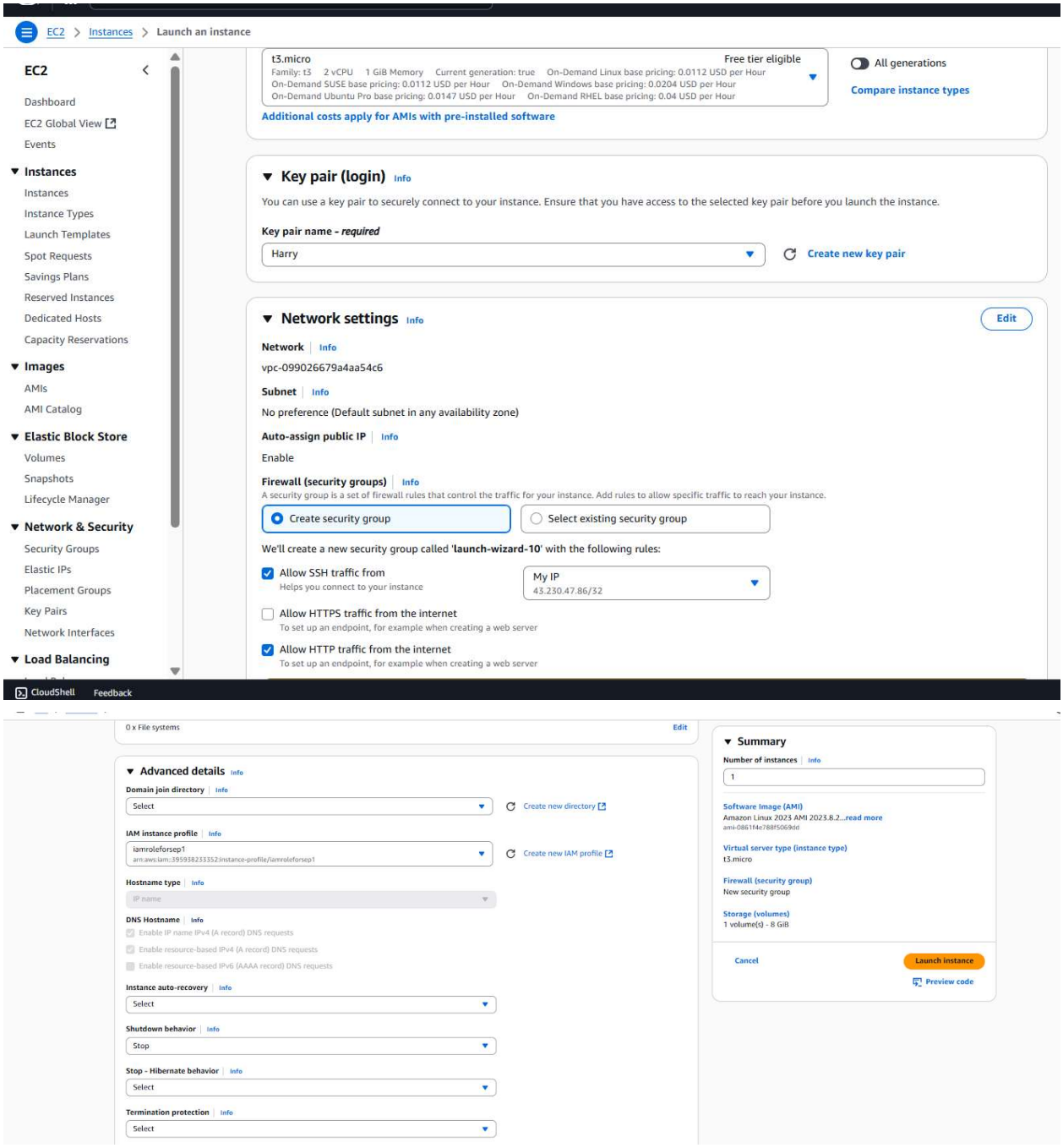
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
AmazonS3ReadOnlyAccess
AWS managed
Permissions policy
Step 3: Add tags
Add tags - optional
Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create role

EC2 Instance Setup (Linux + Nginx + AWS CLI)

Launch two EC2 instances with:

- AMI: Amazon Linux 2/2023
- Instance Type: t3.micro (free tier/demo)
- Security Group: Allow TCP 80 (HTTP), 22 (SSH)
- IAM Role: Choose the one created above (e.g. `iamroleforsep1` as in screenshot)





- User Data (Paste during launch):

```
#!/bin/bash
yum update -y
yum install -y nginx awscli
systemctl enable --now nginx

# Create web root
```

```
mkdir -p /usr/share/nginx/html

# Download static assets from S3
aws s3 cp s3://my-lab-private-static-files/logo.png /usr/share/nginx/html/
aws s3 cp s3://my-lab-private-static-files/style.css /usr/share/nginx/html/

# Create dynamic index.html using hostname
cat <<EOF > /usr/share/nginx/html/index.html
<!doctype html>
<html>
 <head>
  <title>EC2 + S3 + IAM Lab</title>
  <link rel="stylesheet" href="style.css">
 </head>
 <body>
  <h1>Hello from $(hostname)</h1>
  <img src="logo.png" width="200">
  <p>Static files securely served from S3 using IAM Role</p>
 </body>
</html>
EOF
```

- Launch both instances in the same VPC/public subnet

Metadata version | Info

V2 only (token required)

⚠ For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.

Metadata response hop limit | Info

2

Allow tags in metadata | Info

Select

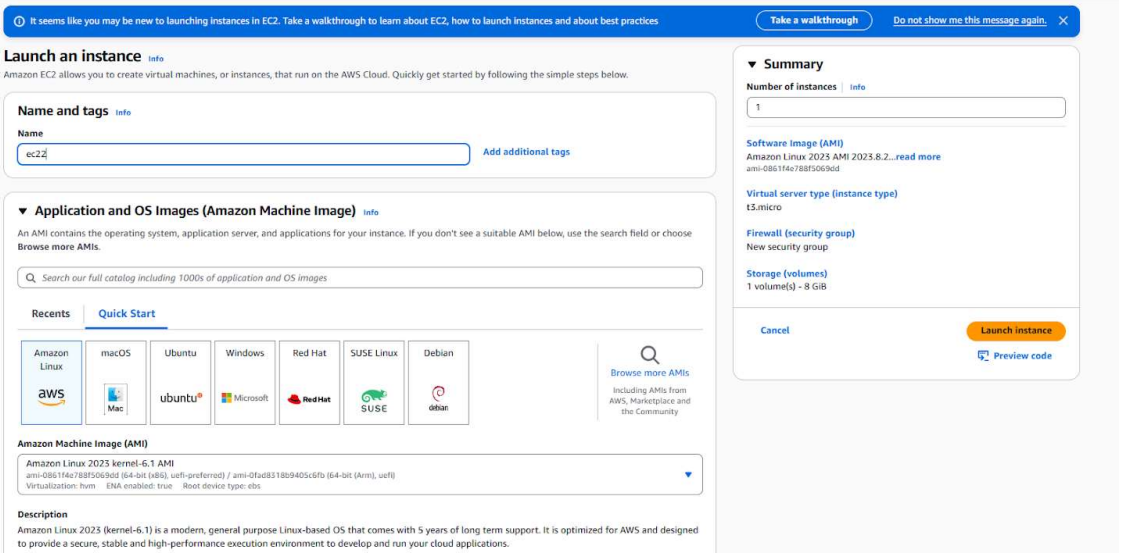
User data - *optional* | Info

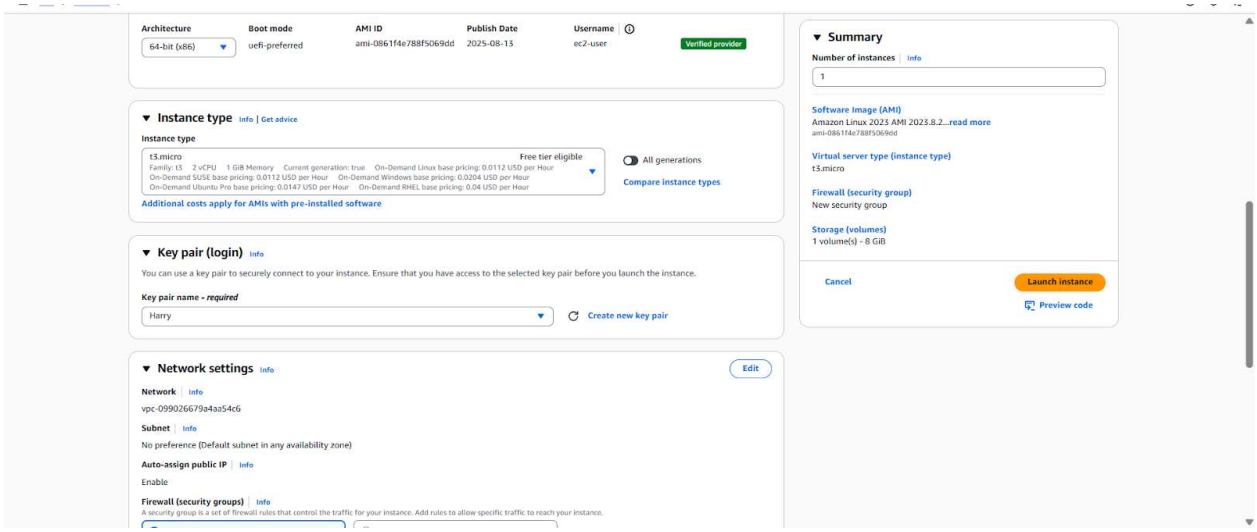
Upload a file with your user data or enter it in the field.

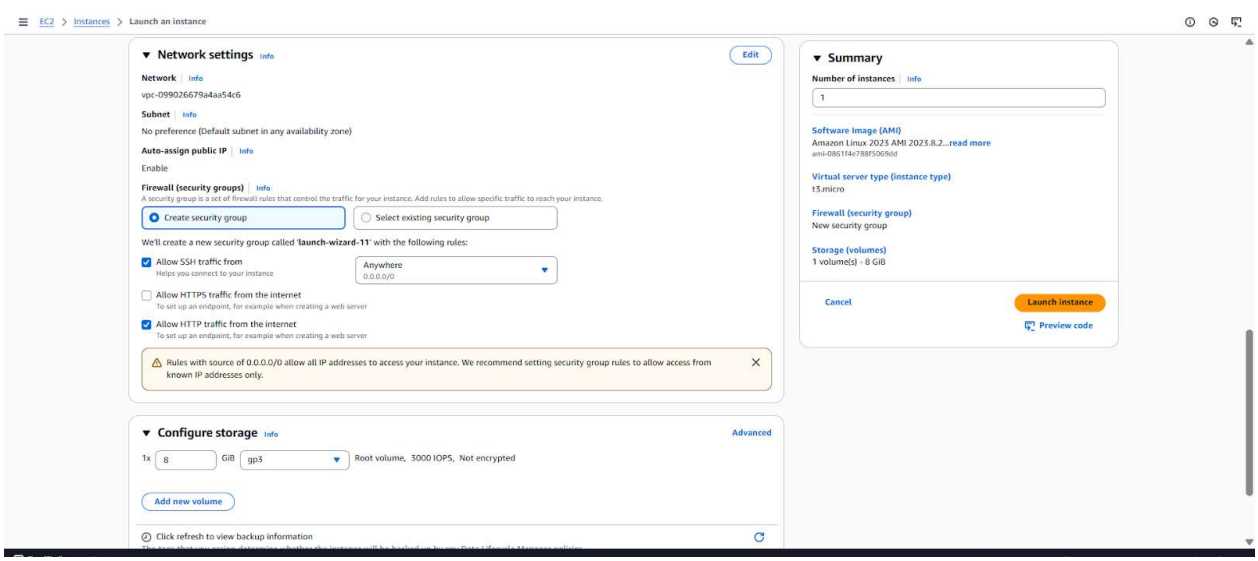
Choose file

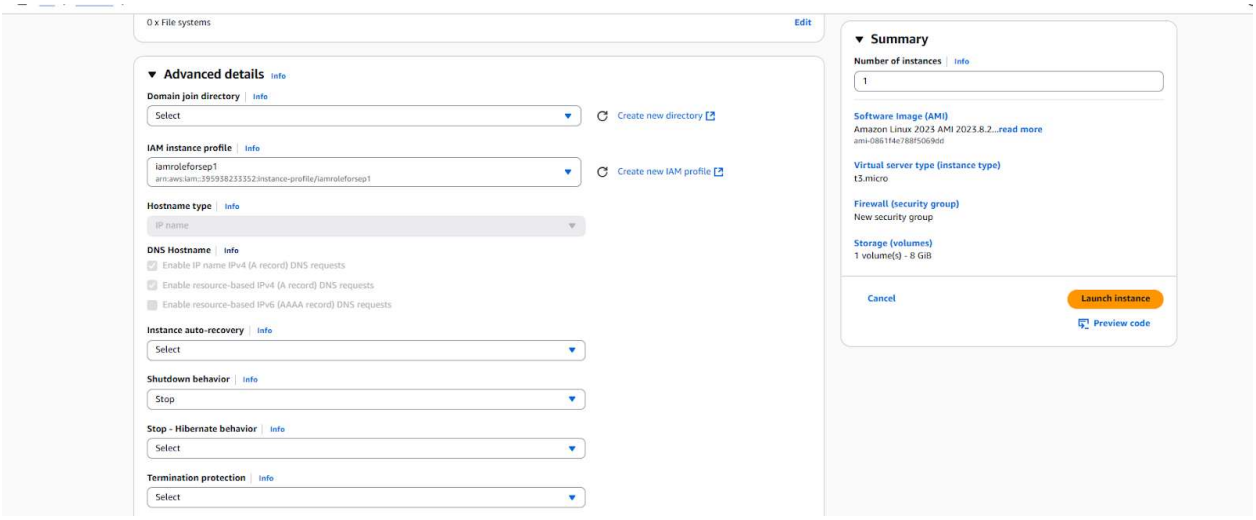
```
yum update -y
yum install -y nginx awscli
systemctl enable --now nginx
mkdir -p /usr/share/nginx/html
aws s3 cp s3://my-lab-private-static-files1/logo.png /usr/share/nginx/html/
aws s3 cp s3://my-lab-private-static-files1/style.css /usr/share/nginx/html/
cat <<EOF > /usr/share/nginx/html/index.html
<!doctype html>
<html>
 <head>
  <title>EC2 + S3 + IAM Lab</title>
  <link rel="stylesheet" href="style.css">
 </head>
 <body>
  <h1>Hello from $(hostname)</h1>
```

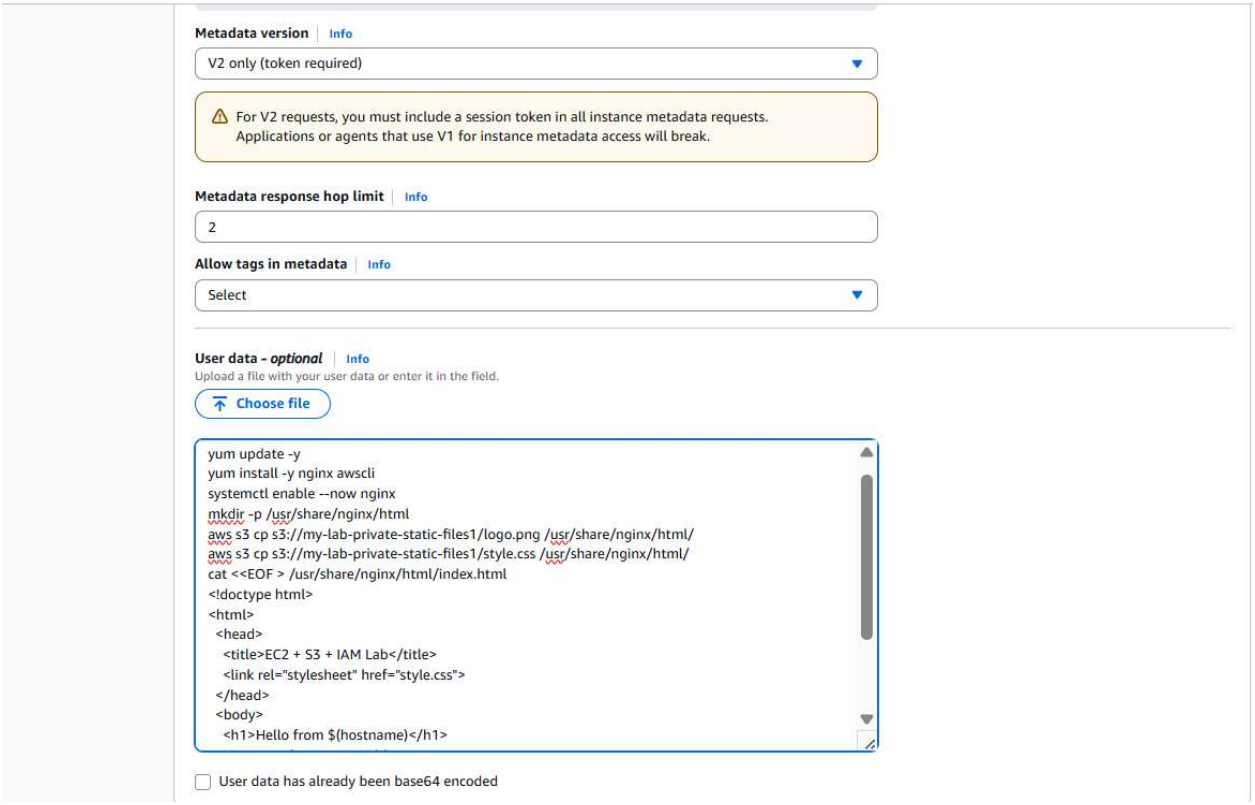
☐ User data has already been base64 encoded




Architecture
64-bit (x86)
Boot mode
uefi-preferred
AMI ID
ami-0861f4e788f5069dd
Publish Date
2025-08-13
Username
ec2-user
Verified provider
Instance type
Info | Get advice
Instance type
t3.micro
Free tier eligible
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
Harry
Create new key pair
Network settings
Info
Edit
Network
vpc-099026679a4aa54c6
Subnet
No preference (Default subnet in any availability zone)
Auto-assign public IP
Enable
Firewall (security groups)
A security group is a set of firewall rules that control the traffic for your instance.
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code


EC2
Instances
Launch an instance
Network settings
Info
Edit
Network
vpc-099026679a4aa54c6
Subnet
No preference (Default subnet in any availability zone)
Auto-assign public IP
Enable
Firewall (security groups)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-11' with the following rules:
Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0
Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server
Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Configure storage
Info
Advanced
1x
8
GiB
gp3
Root volume, 3000 IOPS, Not encrypted
Add new volume
Click refresh to view backup information
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code

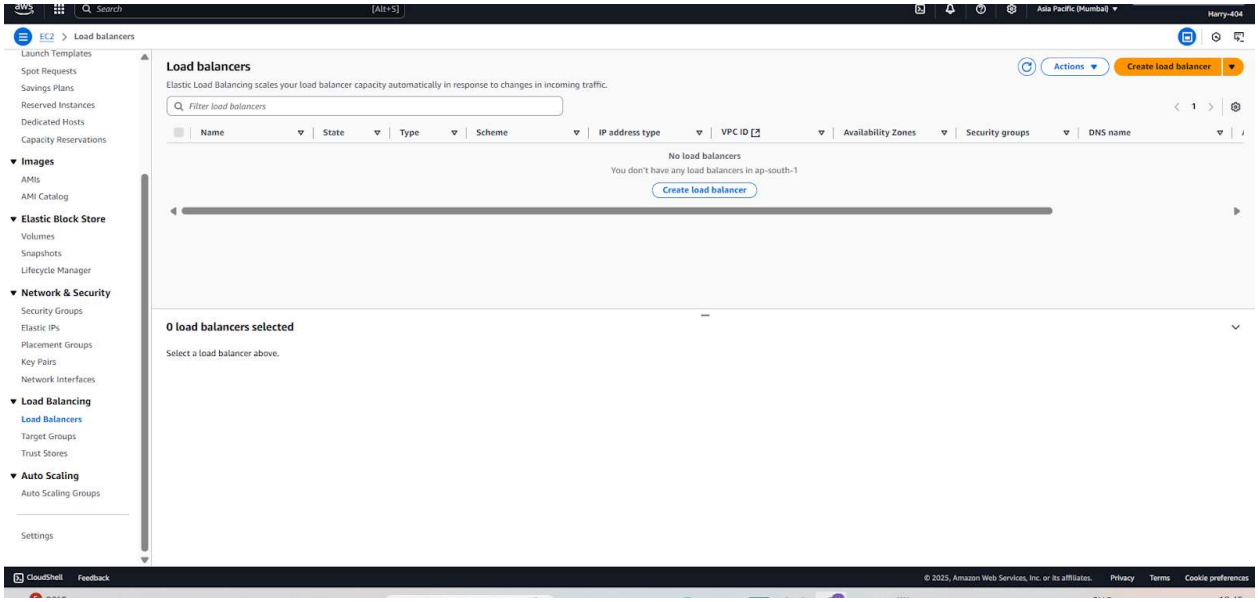


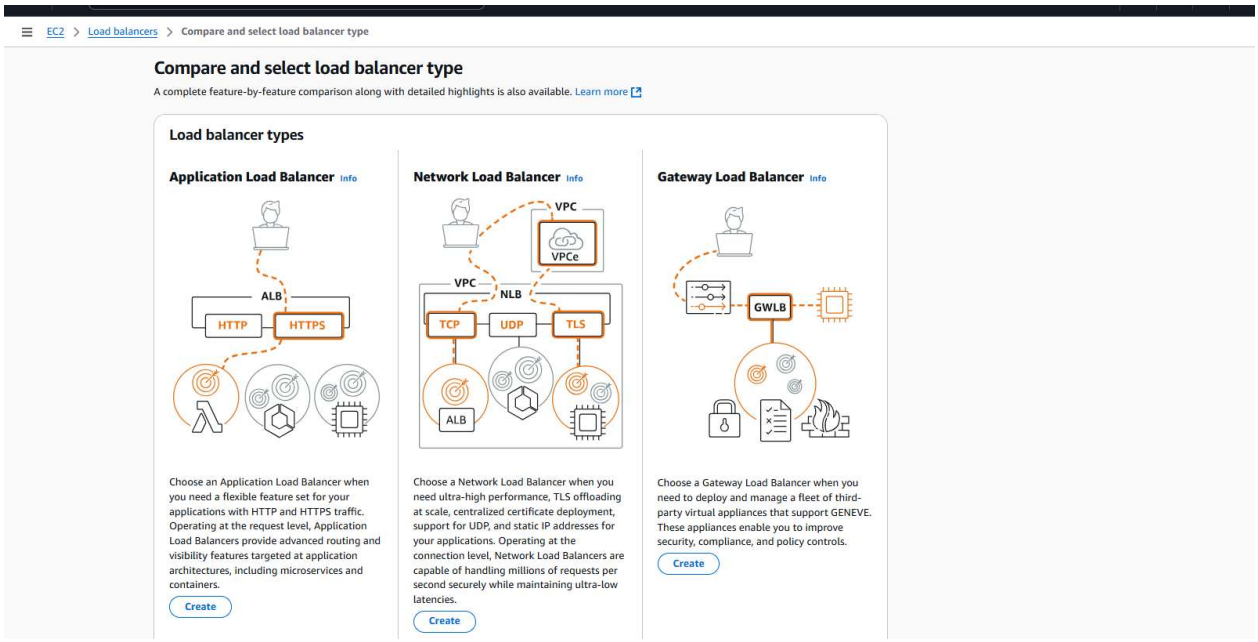


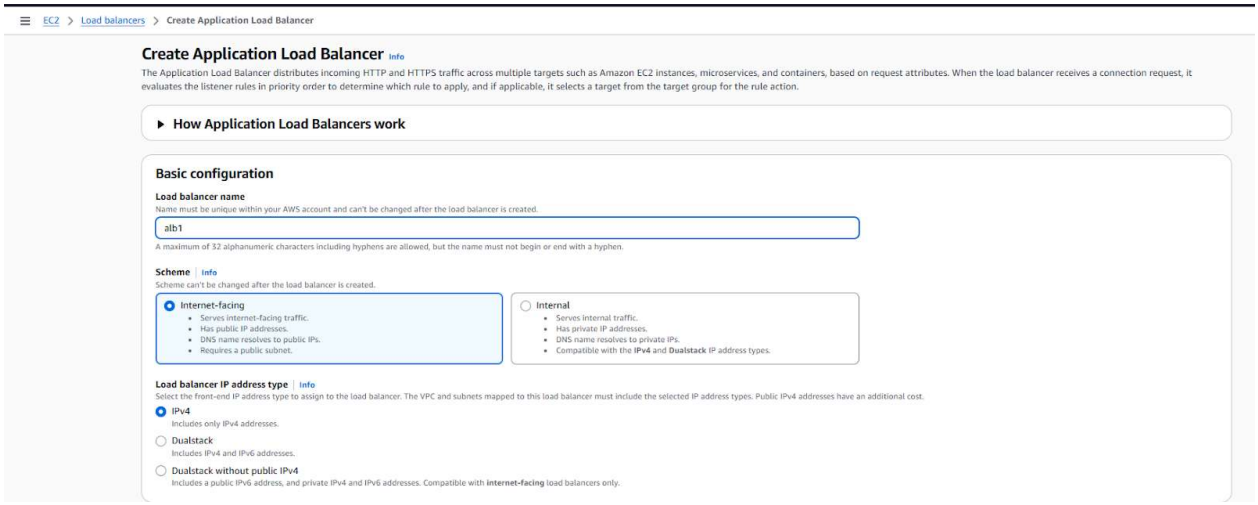
Application Load Balancer (ALB)

- Go to EC2 → Load Balancers → Create Load Balancer
- Type: Application Load Balancer
- Scheme: Internet-facing
- Listener: HTTP (port 80)
- Network mapping: Select at least two subnets in different AZs for HA (as shown in your screenshot)

- Security Groups: Open port 80 inbound
- Target Group: New, Type: Instance, Protocol: HTTP, Port: 80
- Register both EC2 instances as targets
- After creation: Get the DNS name of the ALB (e.g., `alb1-xxxx.ap-south-1.elb.amazonaws.com`)







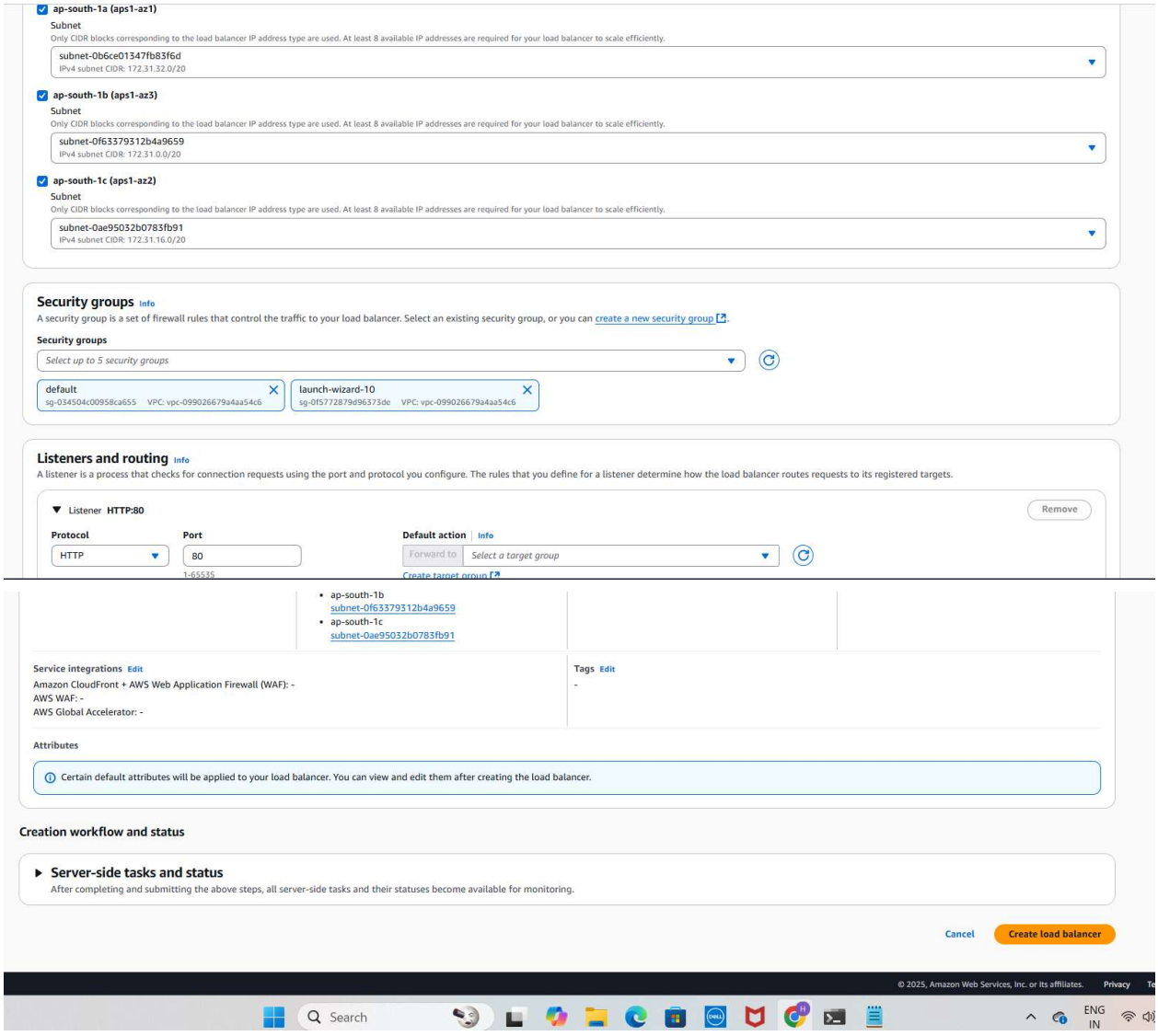
Create Application Load Balancer Info
The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a
evaluates the listener rules in priority 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.
alb1
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

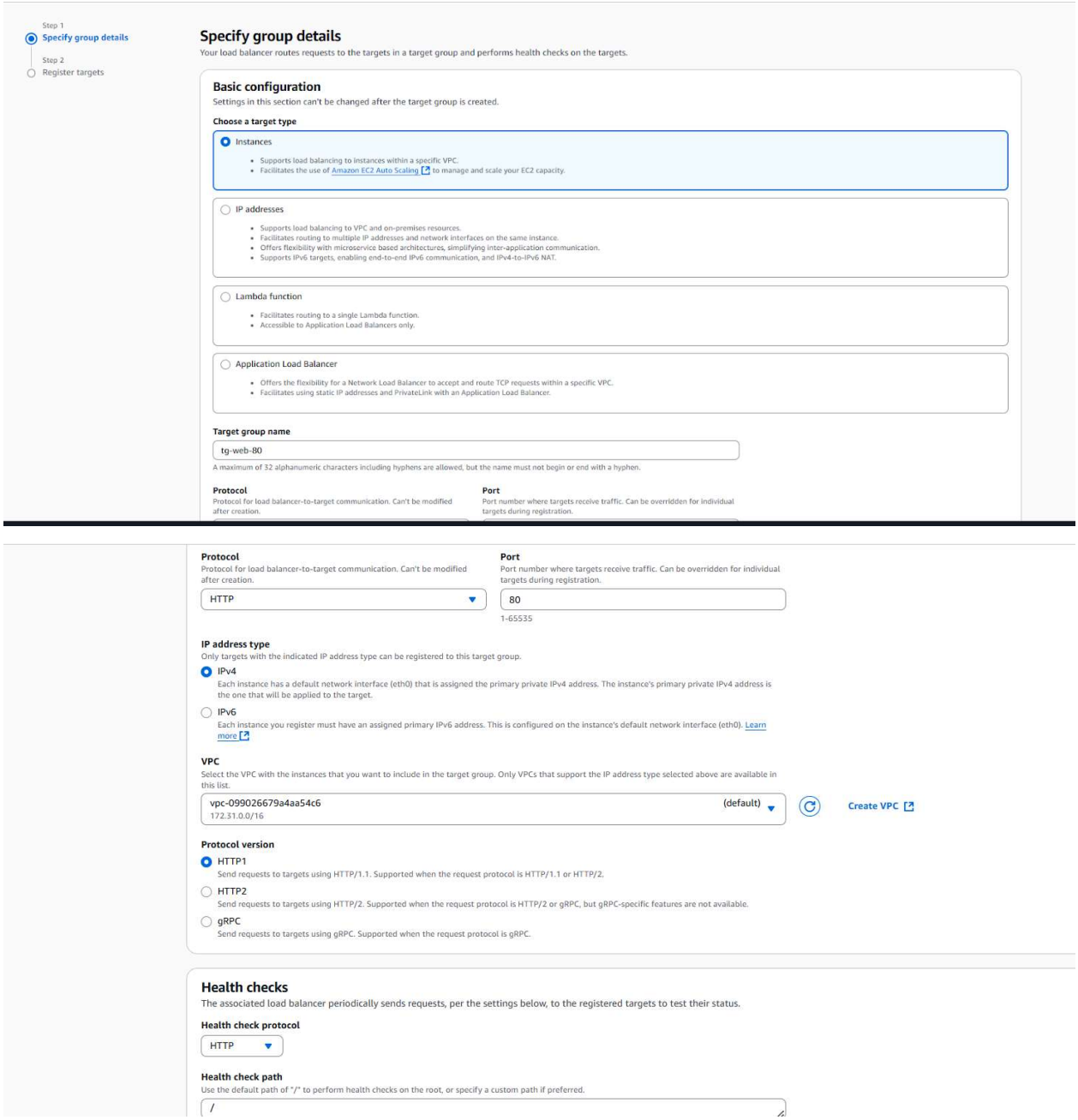
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

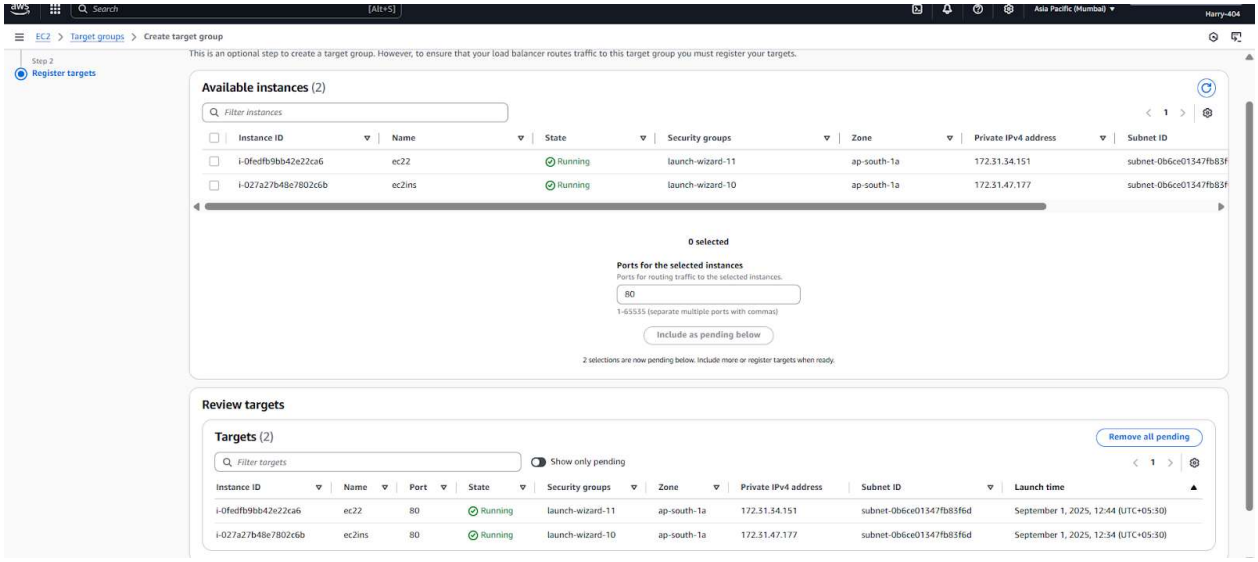
VPC | Info

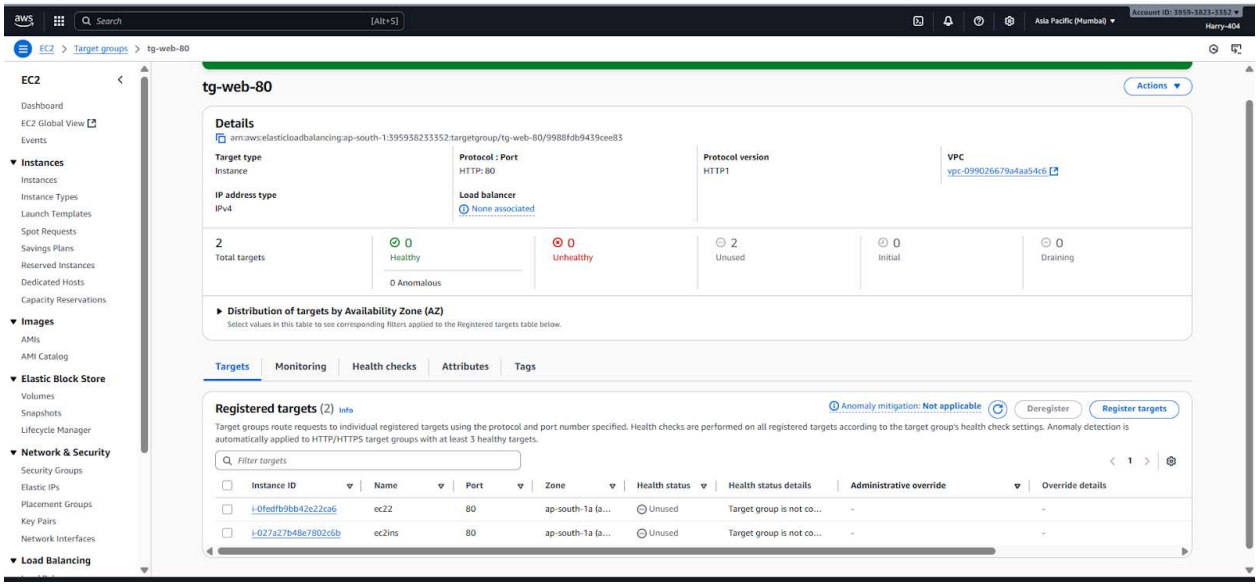
The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if

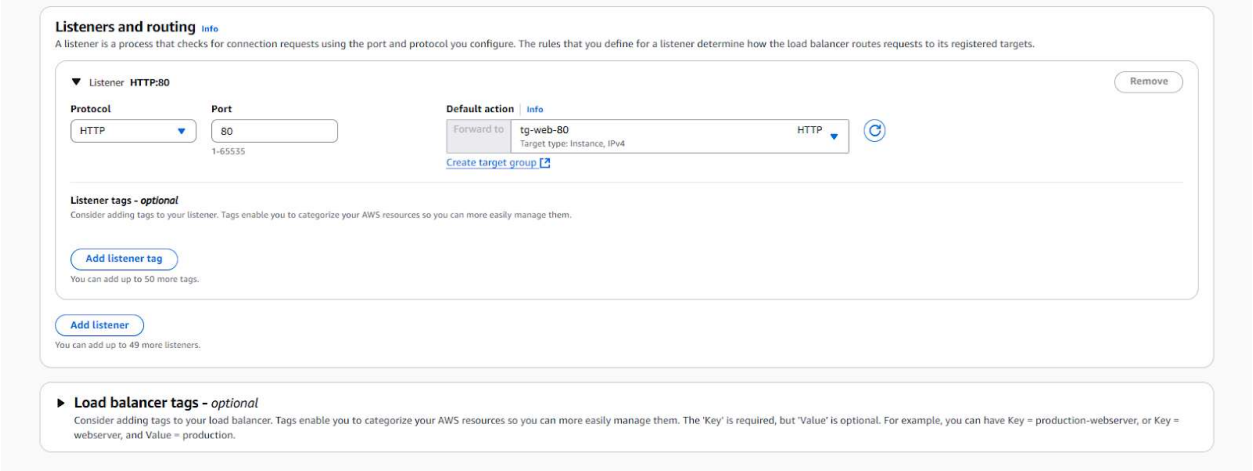

ap-south-1a (aps1-az1)
Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.
subnet-0b6ce01347fb83f6d
IPv4 subnet CIDR: 172.31.32.0/20
ap-south-1b (aps1-az3)
Subnet
Only CIDR blocks 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-0f63379312b4a9659
IPv4 subnet CIDR: 172.31.0.0/20
ap-south-1c (aps1-az2)
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-0ae95032b0783fb91
IPv4 subnet CIDR: 172.31.16.0/20
Security groups Info
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
default
sg-034504c00958ca655 VPC: vpc-099026679a4aa54c6
launch-wizard-10
sg-0f5772879d96373de VPC: vpc-099026679a4aa54c6
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 load balancer routes requests to its registered targets.
Listener HTTP:80
Remove
Protocol
HTTP
Port
80
1-65535
Default action Info
Forward to
Select a target group
Create target group

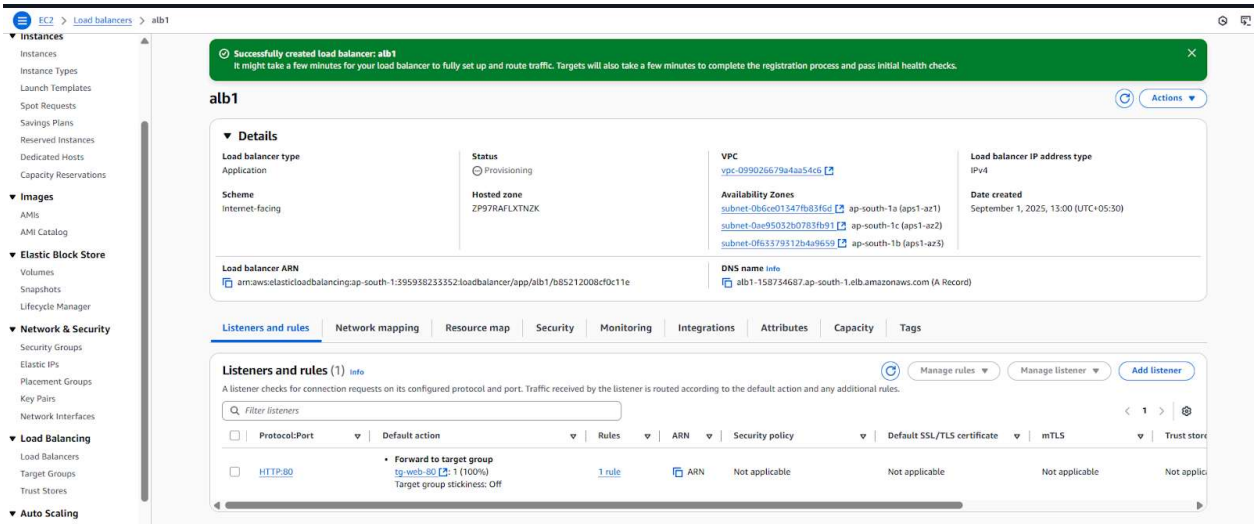
ap-south-1b
subnet-0f63379312b4a9659
ap-south-1c
subnet-0ae95032b0783fb91
Service integrations Edit
Amazon CloudFront + AWS Web Application Firewall (WAF): -
AWS WAF: -
AWS Global Accelerator: -
Tags Edit
-
Attributes
Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.
Creation workflow and status
Server-side tasks and status
After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.
Cancel
Create load balancer
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Search
ENG
IN


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
tg-web-80
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.
Port
Port number where targets receive traffic. Can be overridden for individual targets during registration.
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
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-099026679a4aa54c6
172.31.0.0/16
(default)
Create VPC
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.
/


EC2 > Target groups > Create target group
Step 2
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-0fedfb9bb42e22ca6 | ec22 | Running | launch-wizard-11 | ap-south-1a | 172.31.34.151 | subnet-0b6ce01347fb83f
i-027a27b48e7802c6b | ec2ins | Running | launch-wizard-10 | ap-south-1a | 172.31.47.177 | subnet-0b6ce01347fb83f
0 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
2 selections are now pending below. Include more or register targets when ready.
Review targets
Targets (2)
Remove all pending
Filter targets
Show only pending
Instance ID | Name | Port | State | Security groups | Zone | Private IPv4 address | Subnet ID | Launch time
i-0fedfb9bb42e22ca6 | ec22 | 80 | Running | launch-wizard-11 | ap-south-1a | 172.31.34.151 | subnet-0b6ce01347fb83f6d | September 1, 2025, 12:44 (UTC+05:30)
i-027a27b48e7802c6b | ec2ins | 80 | Running | launch-wizard-10 | ap-south-1a | 172.31.47.177 | subnet-0b6ce01347fb83f6d | September 1, 2025, 12:34 (UTC+05:30)

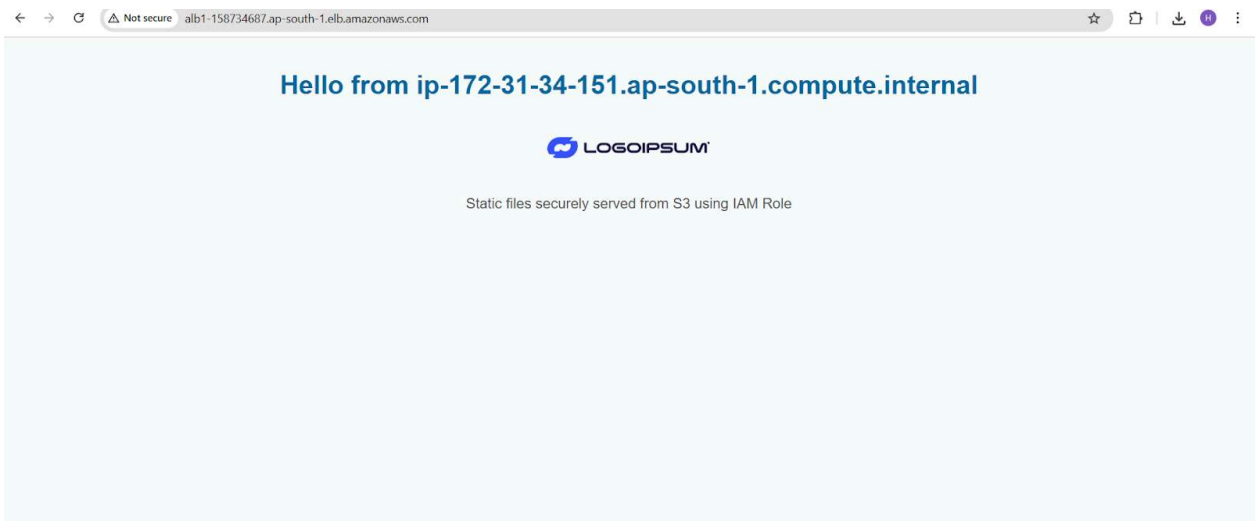

EC2 > Target groups > tg-web-80
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
tg-web-80
Actions
Details
arn:aws:elasticloadbalancing:ap-south-1:395938233352:targetgroup/tg-web-80/9988fdb9439cee83
Target type
Instance
Protocol : Port
HTTP: 80
Protocol version
HTTP1
VPC
vpc-099026679a4aa54c6
IP address type
IPv4
Load balancer
None associated
2
Total targets
0
Healthy
0 Anomalous
0
Unhealthy
2
Unused
0
Initial
0
Draining
Distribution of targets by Availability Zone (AZ)
Select values in this table to see corresponding filters applied to the Registered targets table below.
Targets
Monitoring
Health checks
Attributes
Tags
Registered targets (2) Info
Anomaly mitigation: Not applicable
Deregister
Register targets
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.
Filter targets
Instance ID | Name | Port | Zone | Health status | Health status details | Administrative override | Override details
i-0fedfb9bb42e22ca6 | ec22 | 80 | ap-south-1a (a... | Unused | Target group is not co... | - | -
i-027a27b48e7802c6b | ec2ins | 80 | ap-south-1a (a... | Unused | Target group is not co... | - | -





Test

- Open the ALB DNS in your browser:
  - Should display "Hello from ..." with each EC2 instance's hostname when refreshed
  - `logo.png` and styling should load (fetched from S3 privately, thanks to EC2 IAM role)—no public S3 access!


Not secure
alb1-158734687.ap-south-1.elb.amazonaws.com
Hello from ip-172-31-34-151.ap-south-1.compute.internal
LOGOIPSUM
Static files securely served from S3 using IAM Role

Summary Table: Location and Usage

Step	File Needed	AWS Service	Config/Code	Purpose
S3 Storage	logo.png, style.css	S3	Upload to bucket, block public	Secure static assets
IAM Role	None	IAM	S3 GetObject policy	Least-privilege EC2 S3 access
EC2 UserData	logo.png, style.css	EC2	aws s3 cp, HTML snippet	Serve dynamic/static web content
HTML Output	logo.png	Nginx	`<img src="logo.png" ...>`	Display image on index.html