Cloud project

Submitted to:

Sir usama musharaf

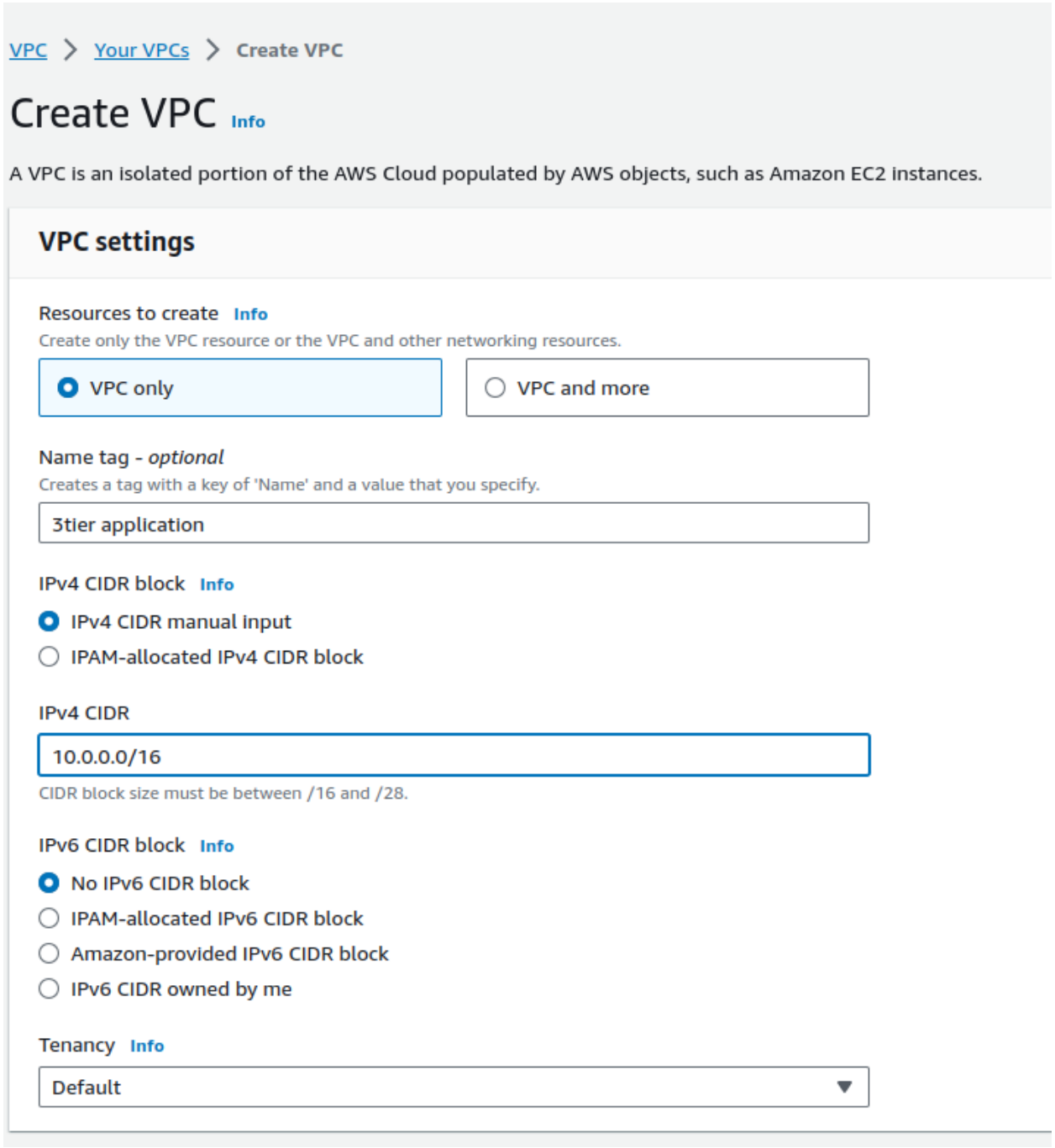
Submitted by :

Shayan khan

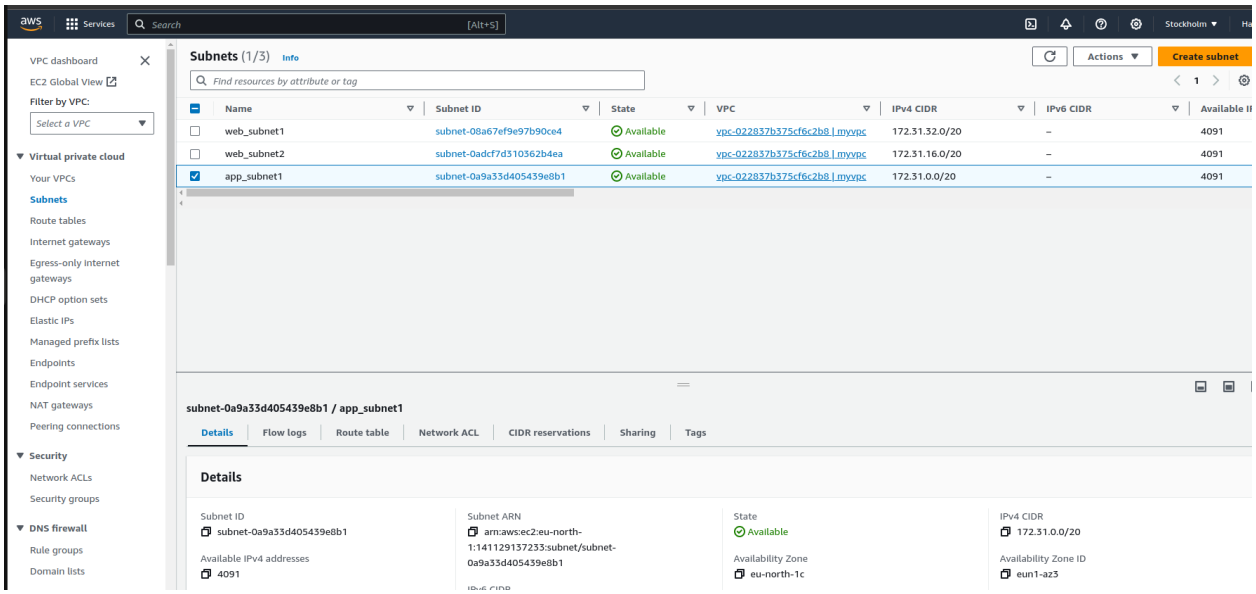
Noman Yousaf

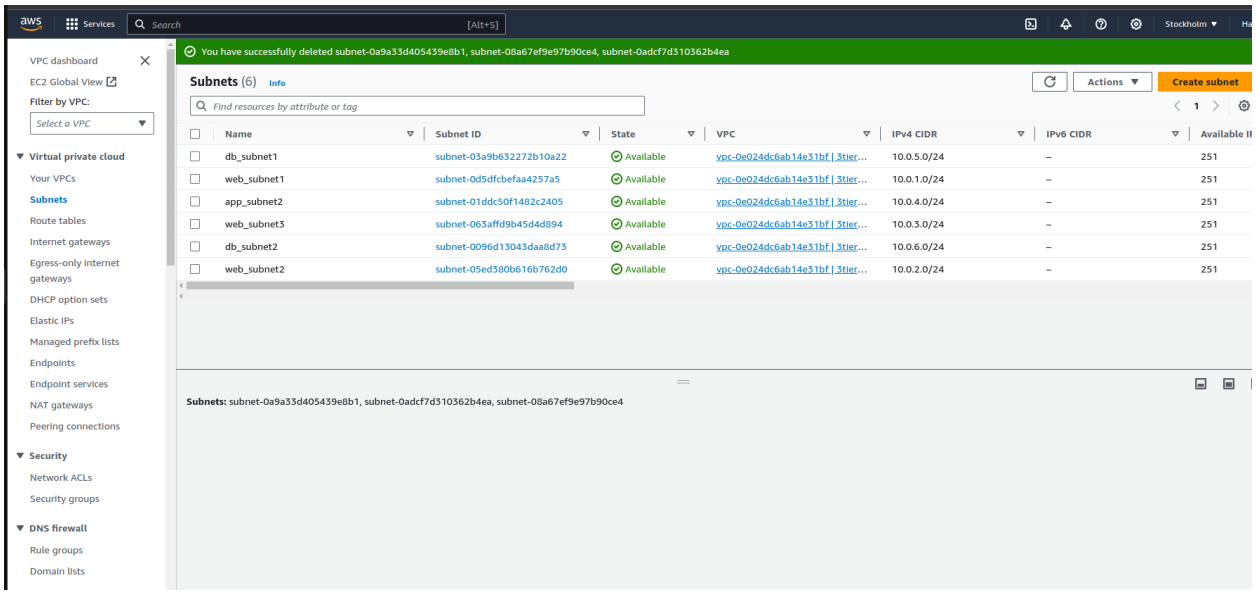
Haq nawaz

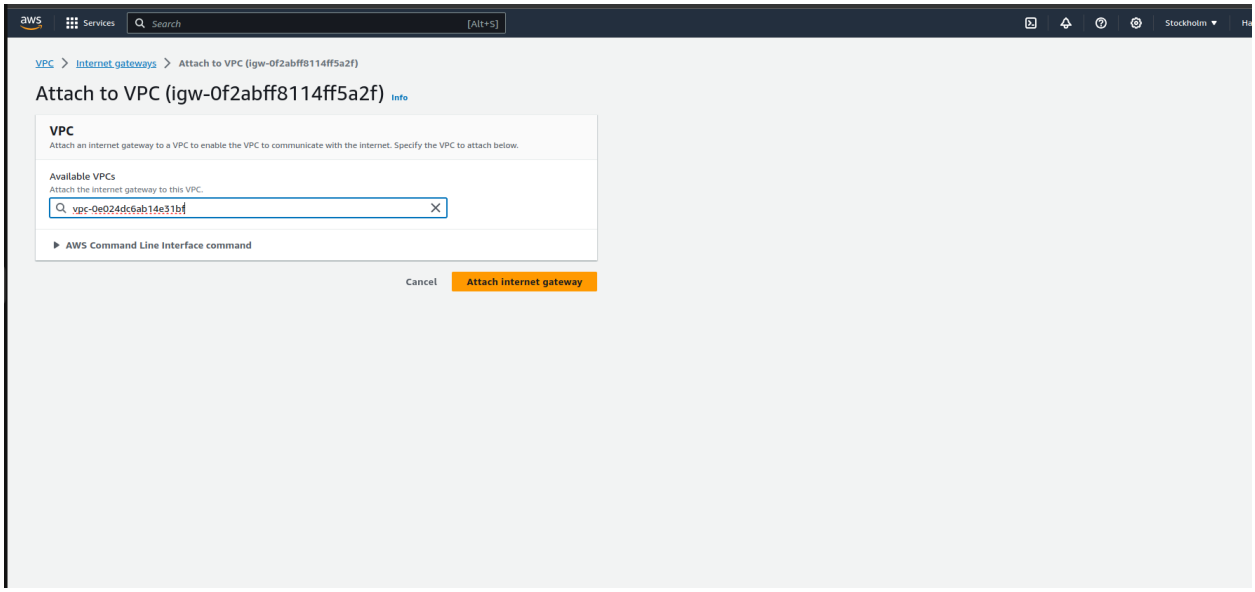
Step 01: creating vpc …



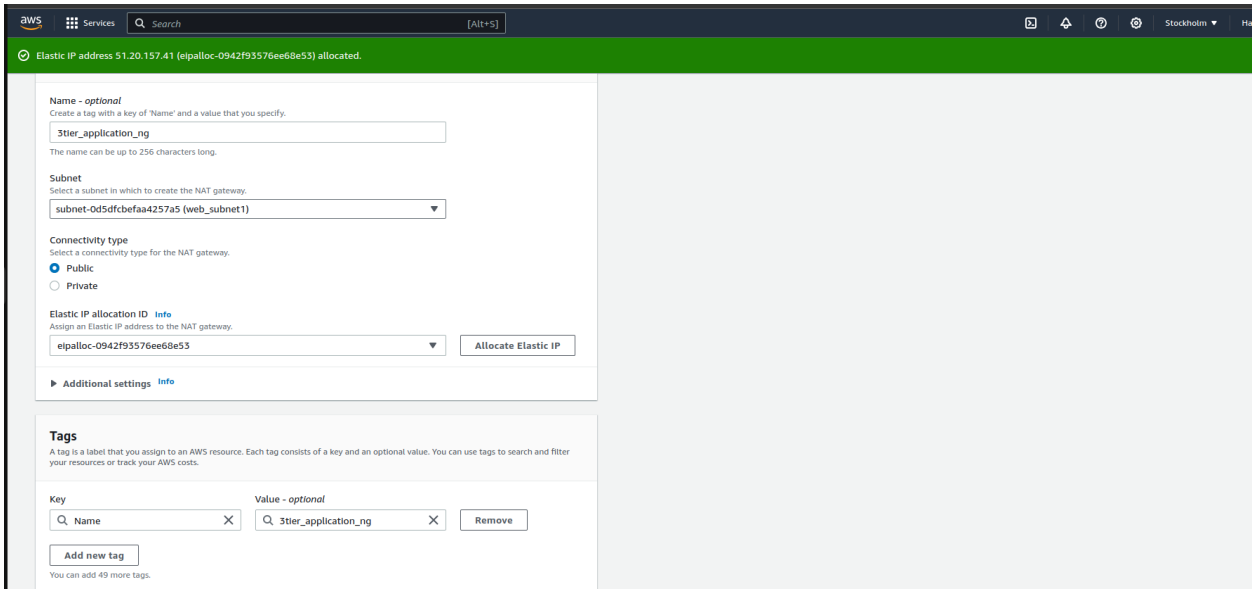
Step 02: creating public and private subnets



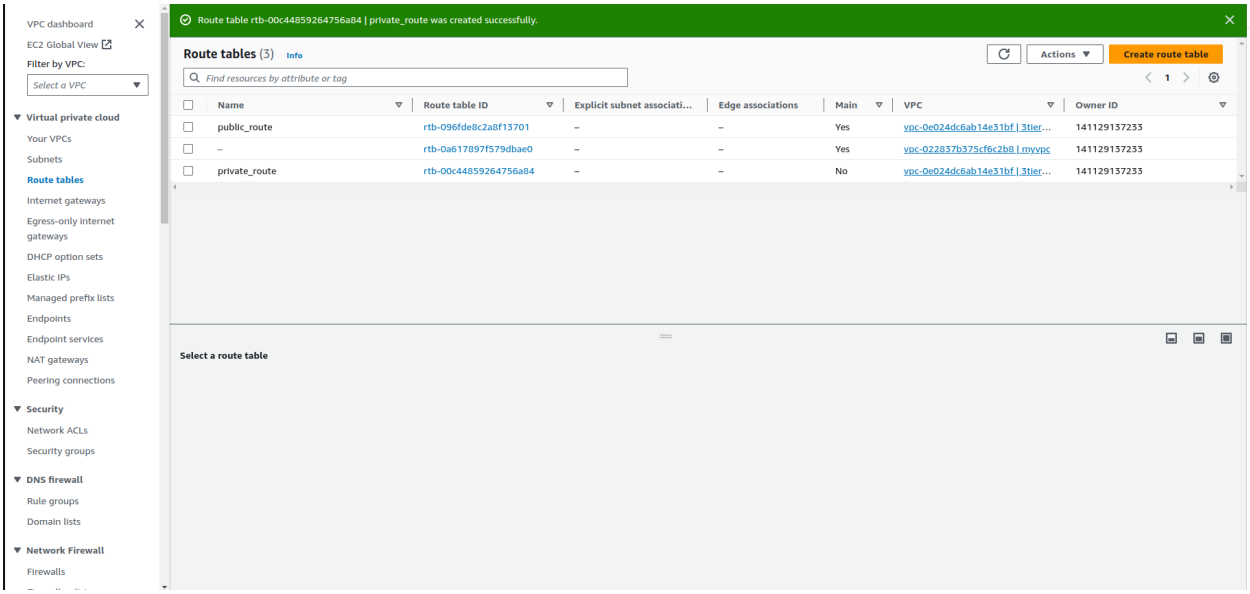


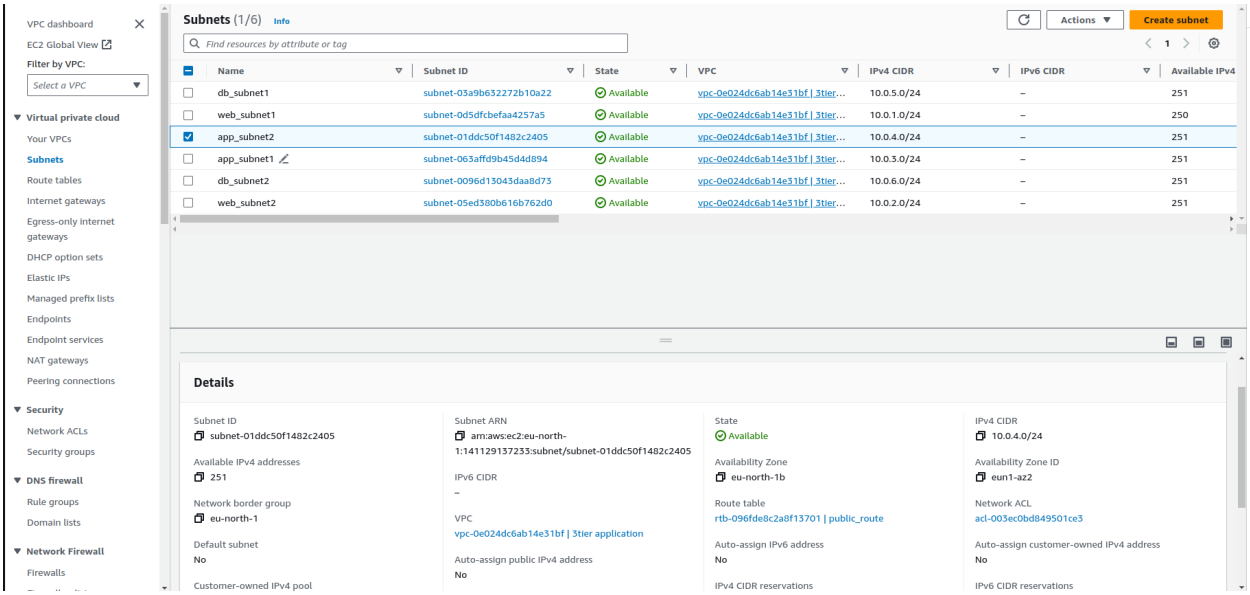


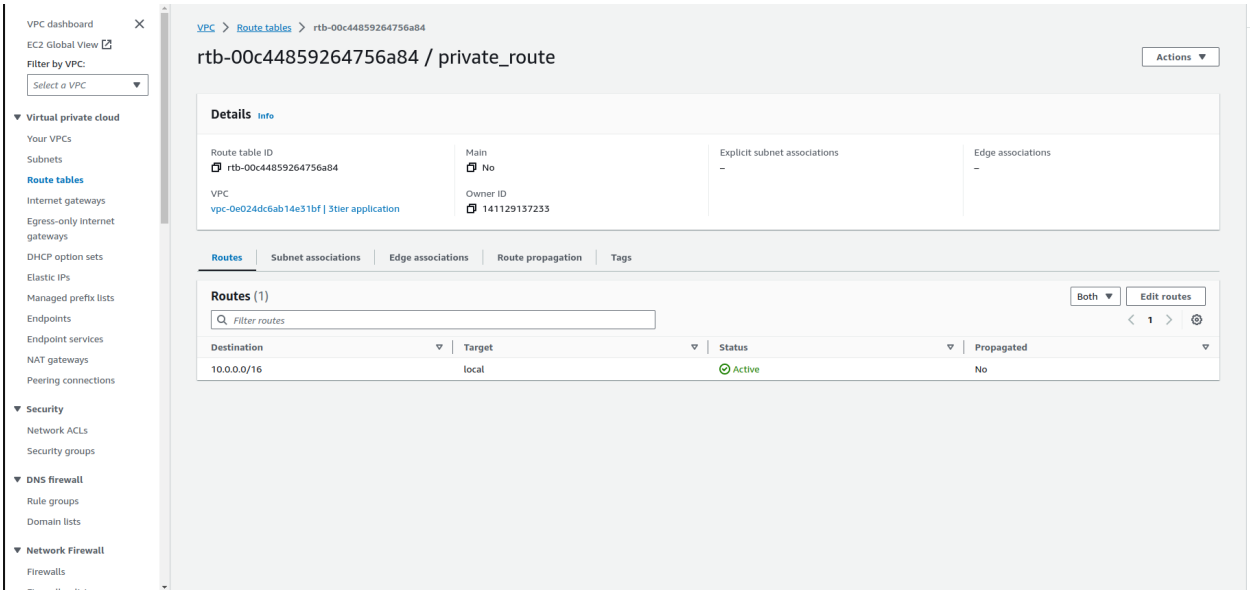
Step 03: creating internet gateway

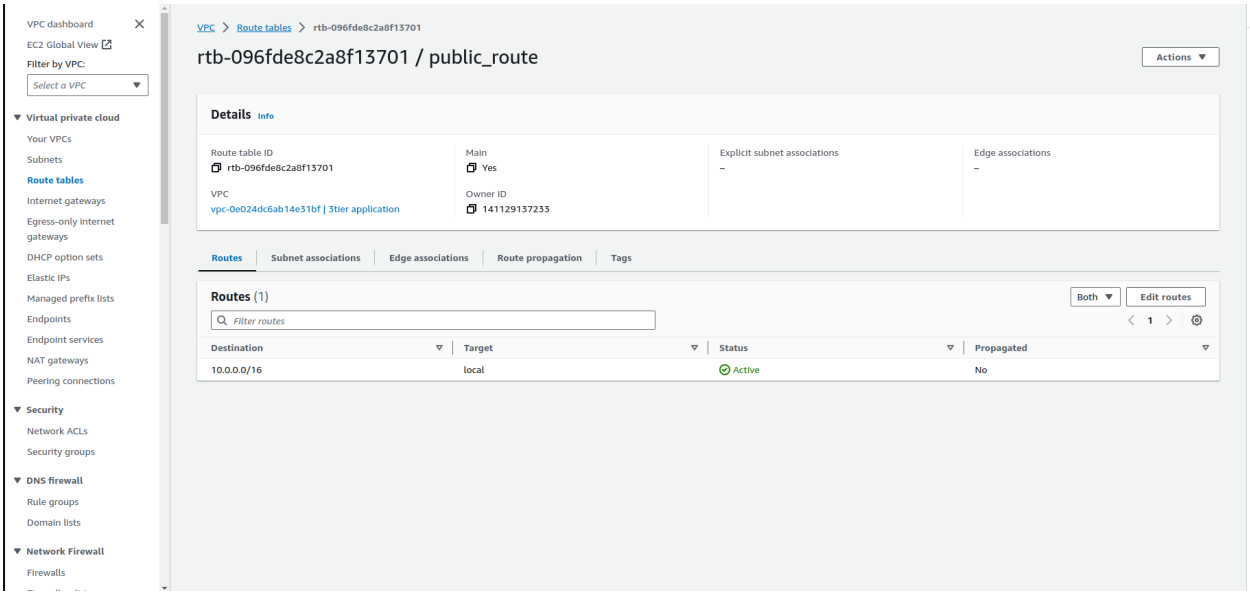


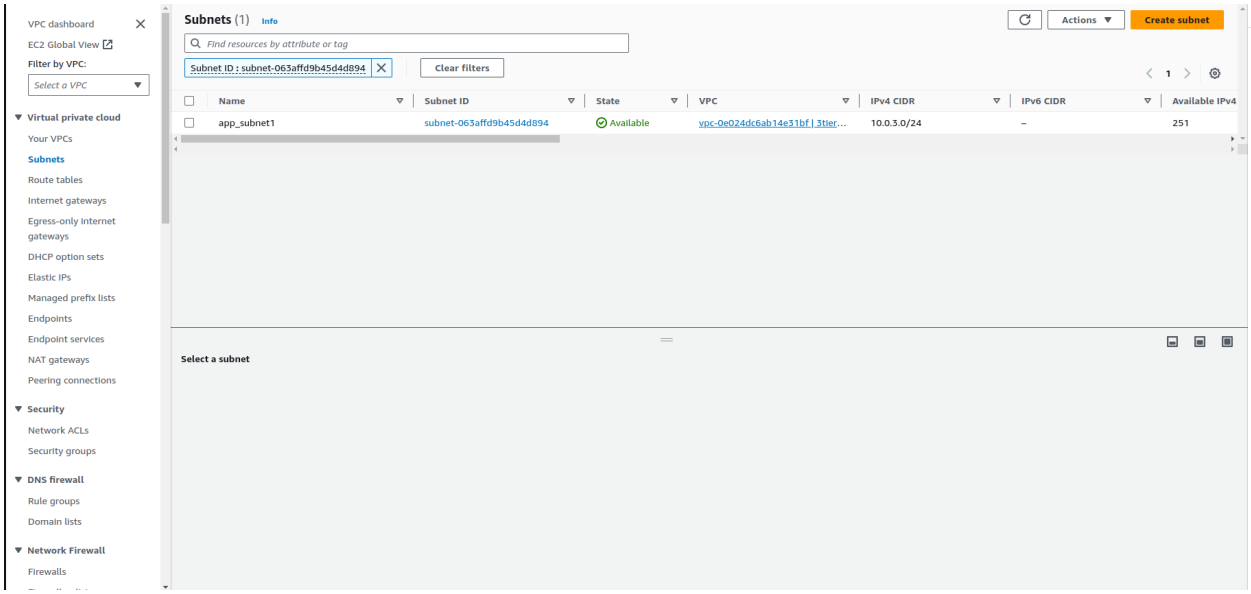
Step 04: Creating route tables


VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Route table rtb-00c44859264756a84 | private_route was created successfully.
Route tables (3) Info
Find resources by attribute or tag
Actions
Create route table
Name
Route table ID
Explicit subnet associati...
Edge associations
Main
VPC
Owner ID
public_route
rtb-096fde8c2a8f13701
–
–
Yes
vpc-0e024dc6ab14e31bf | 3tier...
141129137233
–
rtb-0a617897f579dbae0
–
–
Yes
vpc-022837b375cf6c2b8 | myvpc
141129137233
private_route
rtb-00c44859264756a84
–
–
No
vpc-0e024dc6ab14e31bf | 3tier...
141129137233
Select a route table

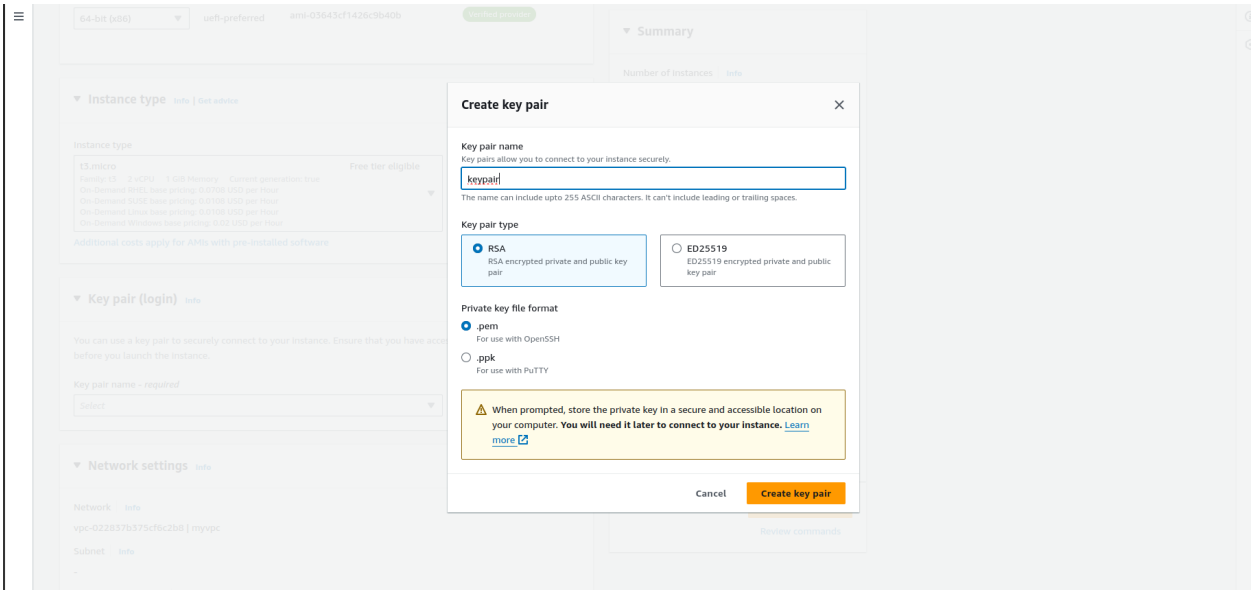

VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Subnets (1/6) Info
Find resources by attribute or tag
Actions
Create subnet
Name
Subnet ID
State
VPC
IPv4 CIDR
IPv6 CIDR
Available IPv4
db_subnet1
subnet-03a9b632272b10a22
Available
vpc-0e024dc6ab14e31bf | 3tier...
10.0.5.0/24
–
251
web_subnet1
subnet-0d5dfcbefaa4257a5
Available
vpc-0e024dc6ab14e31bf | 3tier...
10.0.1.0/24
–
250
app_subnet2
subnet-01ddc50f1482c2405
Available
vpc-0e024dc6ab14e31bf | 3tier...
10.0.4.0/24
–
251
app_subnet1
subnet-063affd9b45d4d894
Available
vpc-0e024dc6ab14e31bf | 3tier...
10.0.3.0/24
–
251
db_subnet2
subnet-0096d13043daa8d73
Available
vpc-0e024dc6ab14e31bf | 3tier...
10.0.6.0/24
–
251
web_subnet2
subnet-05ed380b616b762d0
Available
vpc-0e024dc6ab14e31bf | 3tier...
10.0.2.0/24
–
251
Details
Subnet ID
subnet-01ddc50f1482c2405
Subnet ARN
arn:aws:ec2:eu-north-1:141129137233:subnet/subnet-01ddc50f1482c2405
State
Available
IPv4 CIDR
10.0.4.0/24
Available IPv4 addresses
251
IPv6 CIDR
–
Availability Zone
eu-north-1b
Availability Zone ID
eun1-az2
Network border group
eu-north-1
VPC
vpc-0e024dc6ab14e31bf | 3tier application
Route table
rtb-096fde8c2a8f13701 | public_route
Network ACL
acl-003ec0bd849501ce3
Default subnet
No
Auto-assign public IPv4 address
No
Auto-assign IPv6 address
No
Auto-assign customer-owned IPv4 address
No
Customer-owned IPv4 pool
IPv4 CIDR reservations
IPv6 CIDR reservations

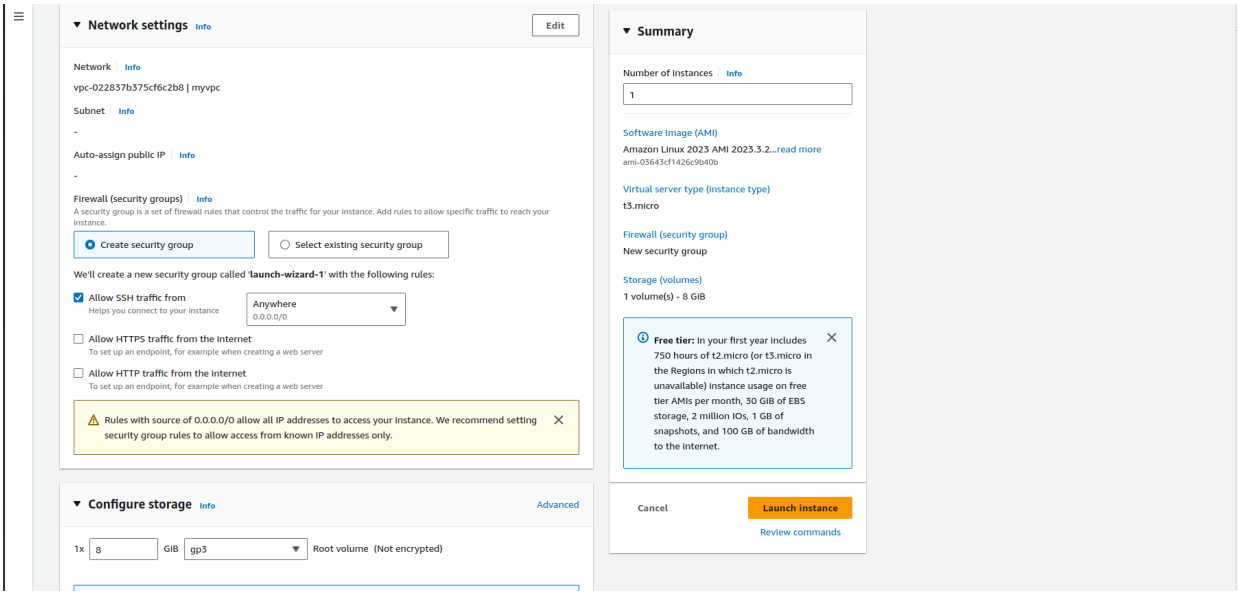

VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
VPC > Route tables > rtb-00c44859264756a84
rtb-00c44859264756a84 / private_route
Actions
Details Info
Route table ID
rtb-00c44859264756a84
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0e024dc6ab14e31bf | 3tier application
Owner ID
141129137233
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No

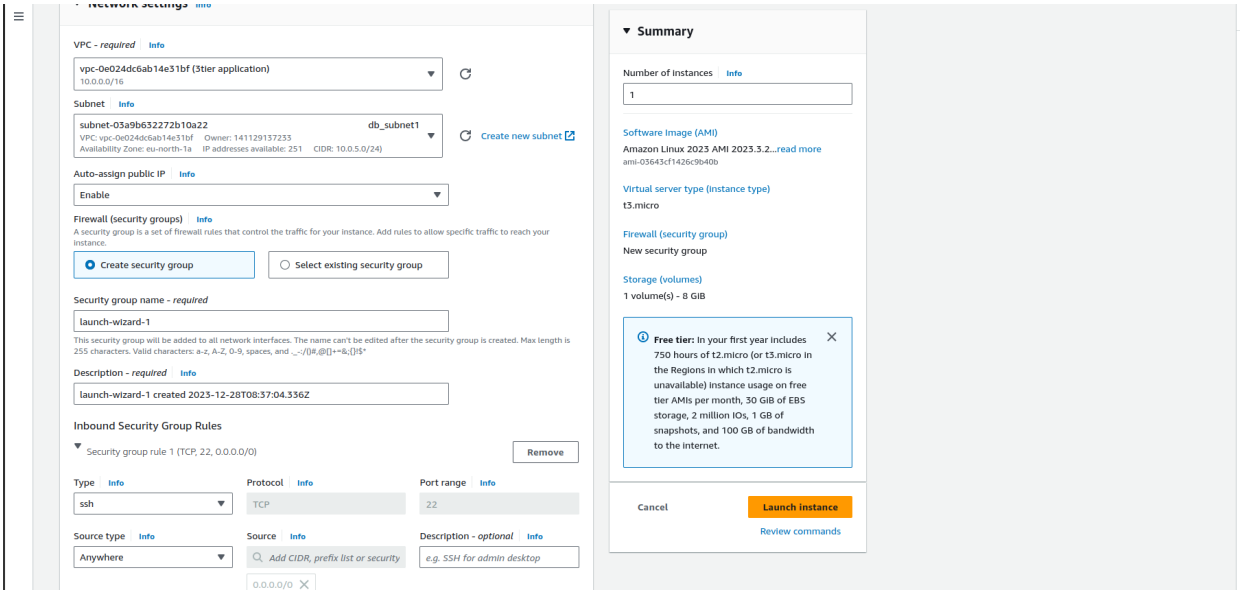

VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
VPC > Route tables > rtb-096fde8c2a8f13701
rtb-096fde8c2a8f13701 / public_route
Actions
Details Info
Route table ID
rtb-096fde8c2a8f13701
Main
Yes
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0e024dc6ab14e31bf | 3tier application
Owner ID
141129137233
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No

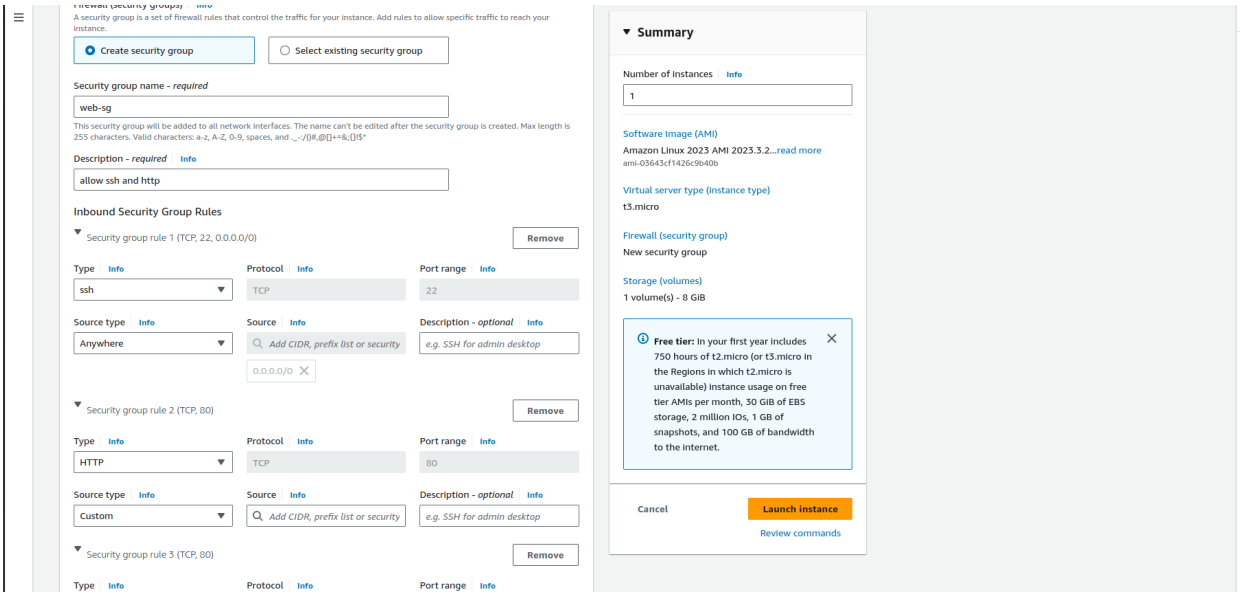


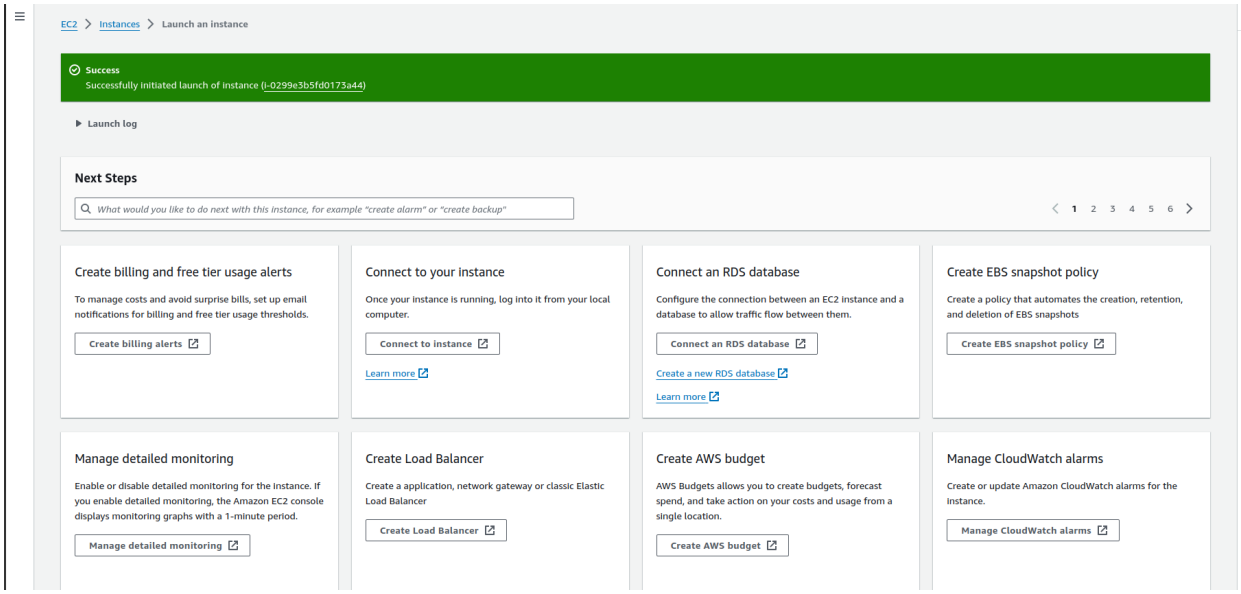
Step 05: Launch EC2 instances

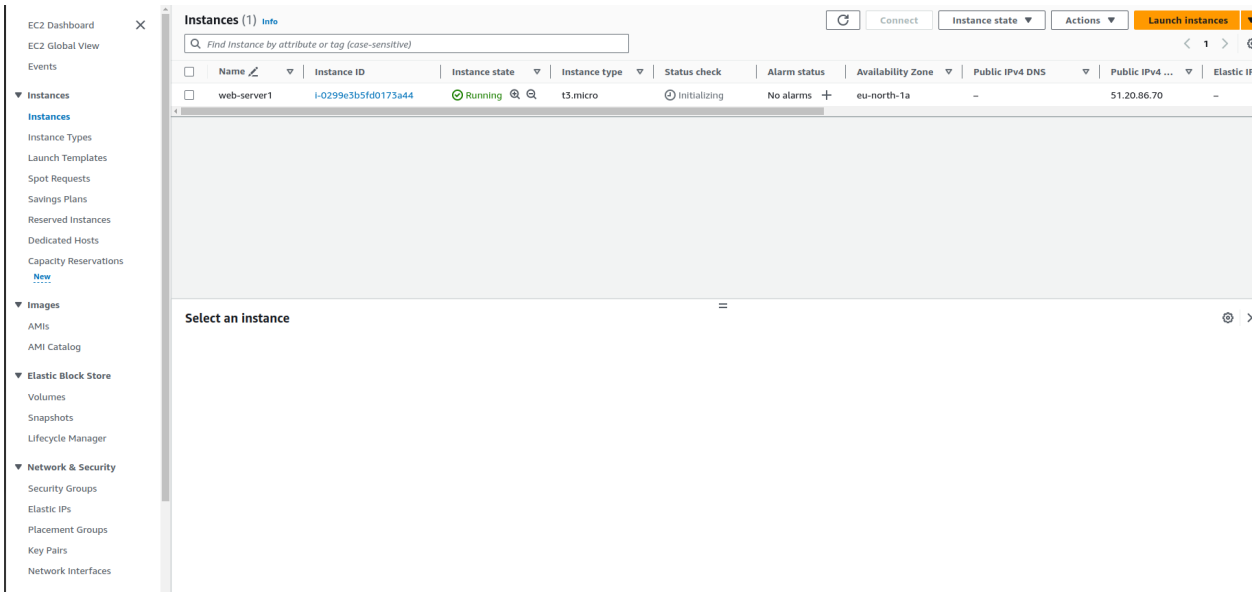

Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
keypair
The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more
Cancel
Create key pair


Network settings
Edit
Network
vpc-022837b375cf6c2b8 | myvpc
Subnet
-
Auto-assign public IP
-
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-1' 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
Advanced
1x
8
GiB
gp3
Root volume (Not encrypted)
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-03643cf1426c9b40b
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands


VPC - required Info
vpc-0e024dc6ab14e31bf (3tier application)
10.0.0.0/16
Subnet Info
subnet-03a9b632272b10a22 db_subnet1
VPC: vpc-0e024dc6ab14e31bf Owner: 141129137233
Availability Zone: eu-north-1a IP addresses available: 251 CIDR: 10.0.5.0/24)
Create new subnet
Auto-assign public IP Info
Enable
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-1
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
launch-wizard-1 created 2023-12-28T08:37:04.336Z
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
0.0.0.0/0
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-03643cf1426c9b40b
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands


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
web-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
allow ssh and http
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
0.0.0.0/0
Security group rule 2 (TCP, 80)
Remove
Type Info
HTTP
Protocol Info
TCP
Port range Info
80
Source type Info
Custom
Source Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
Security group rule 3 (TCP, 80)
Remove
Type Info
Protocol Info
Port range Info
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-03643cf1426c9b40b
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands


EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0299e3b5fd0173a44)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy
Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.
Manage detailed monitoring
Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer
Create Load Balancer
Create AWS budget
AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.
Create AWS budget
Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.
Manage CloudWatch alarms


EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Instances (1) Info
Find Instance by attribute or tag (case-sensitive)
Connect
Instance state
Actions
Launch instances
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
web-server1
i-0299e3b5fd0173a44
Running
t3.micro
Initializing
No alarms
eu-north-1a
–
51.20.86.70
–
Select 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

web-server2

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 the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible

ami-03643cf1426c9b40b (64-bit (x86), uefi-preferred) / ami-0abbdfe8255676ef1 (64-bit (Arm), uefi)

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

Description

Summary

Number of instances Info: 1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-03643cf1426c9b40b

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel | Launch instance | Review commands

Key pair name - *required*

keypair1 | Create new key pair

Network settings Info

VPC - *required* Info

vpc-0e024dc6ab14e31bf (3tier application)
10.0.0.0/16

Subnet Info

subnet-03a9b632272b10a22 — db_subnet1
VPC: vpc-0e024dc6ab14e31bf Owner: 141129137233
Availability Zone: eu-north-1a IP addresses available: 250 CIDR: 10.0.5.0/24)

Create new subnet

Auto-assign public IP Info

Enable

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*

web-subnet2

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

launch-wizard-1 created 2023-12-28T08:49:53.753Z

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

Summary

Number of instances Info: 1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-03643cf1426c9b40b

Virtual server type (instance type)

t3.micro

Firewall (security group)

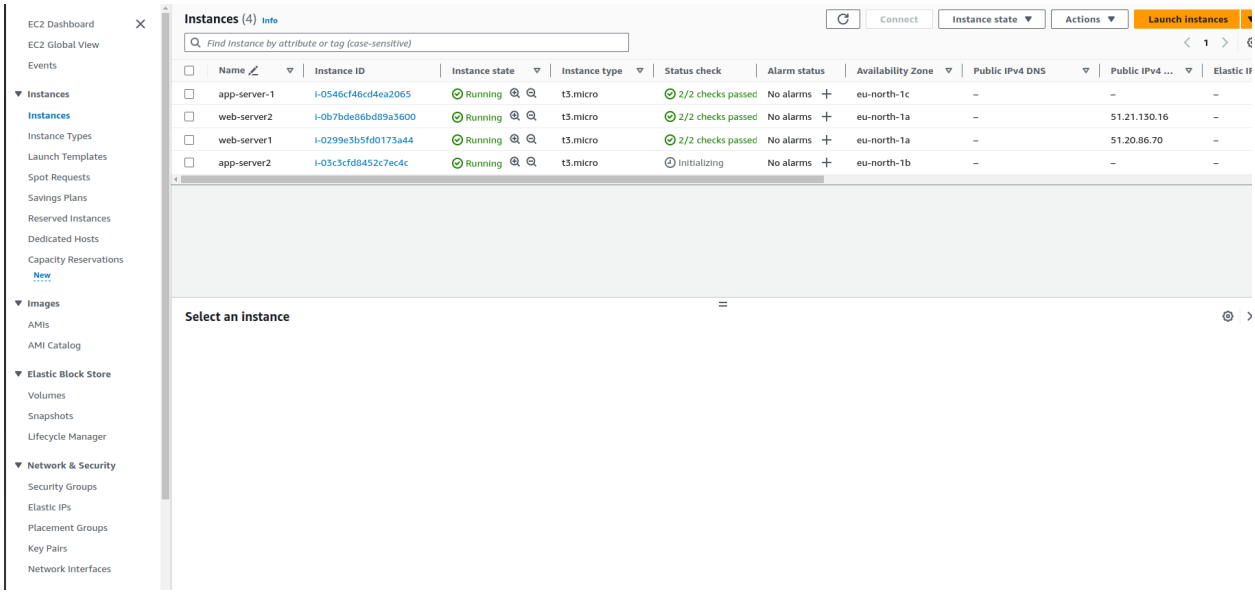
New security group

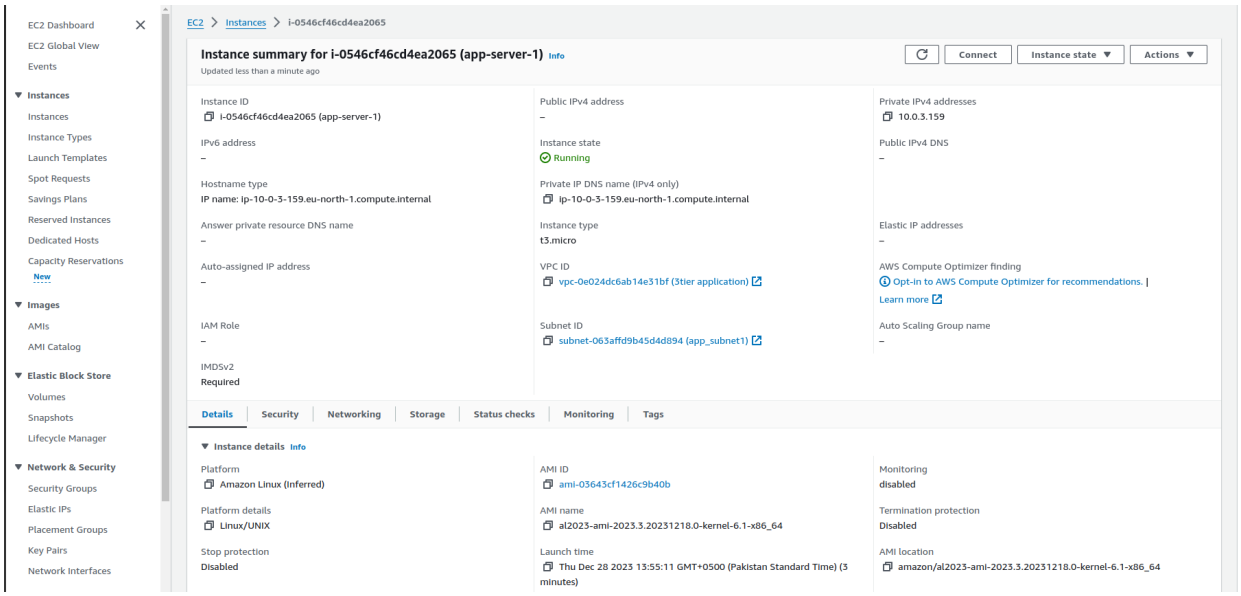
Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

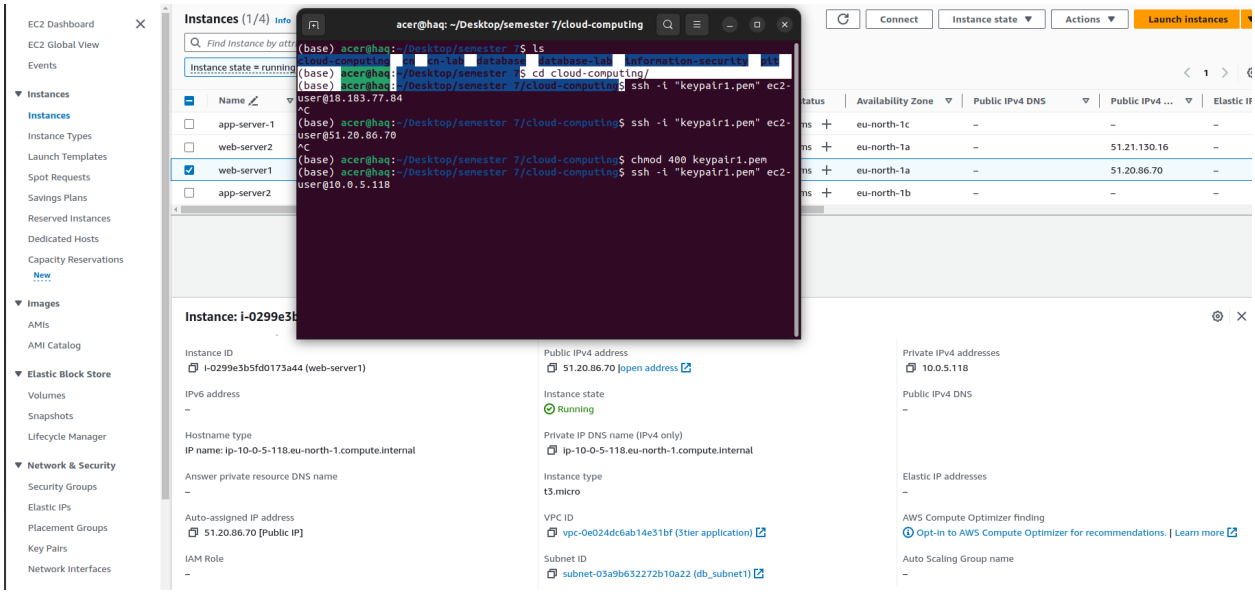
Cancel | Launch instance | Review commands

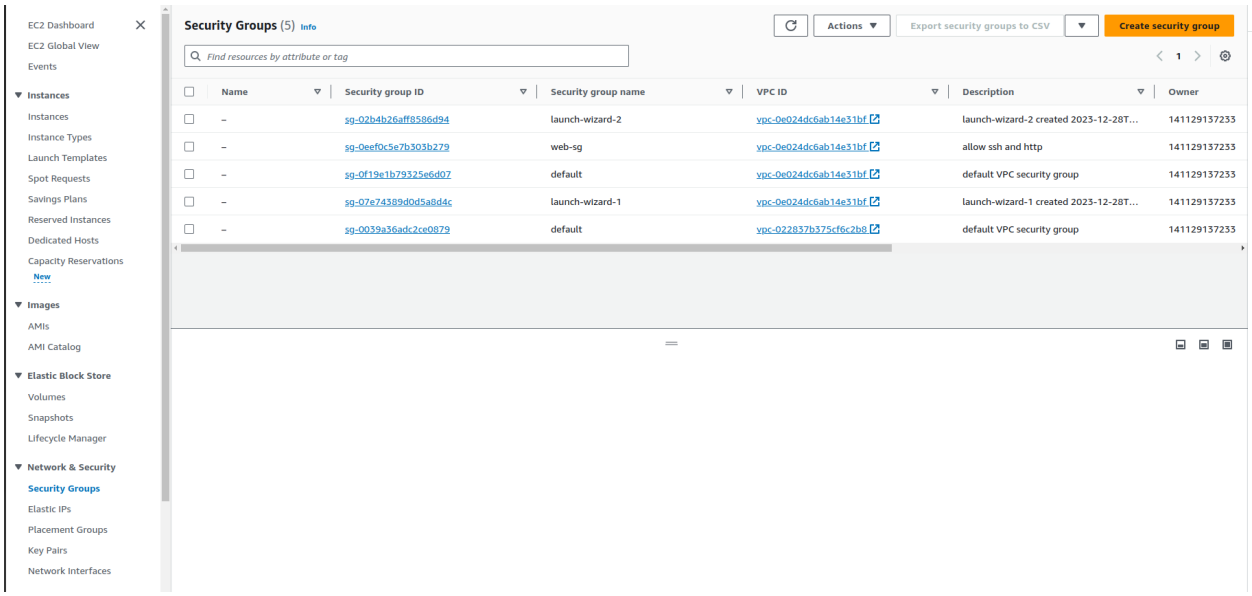


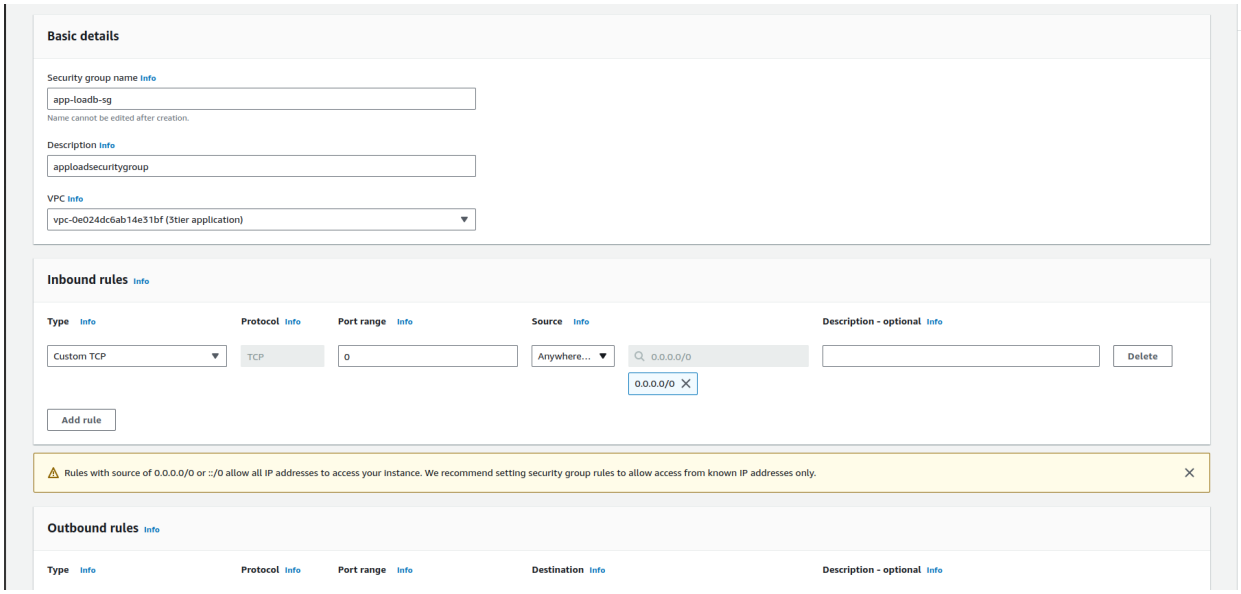


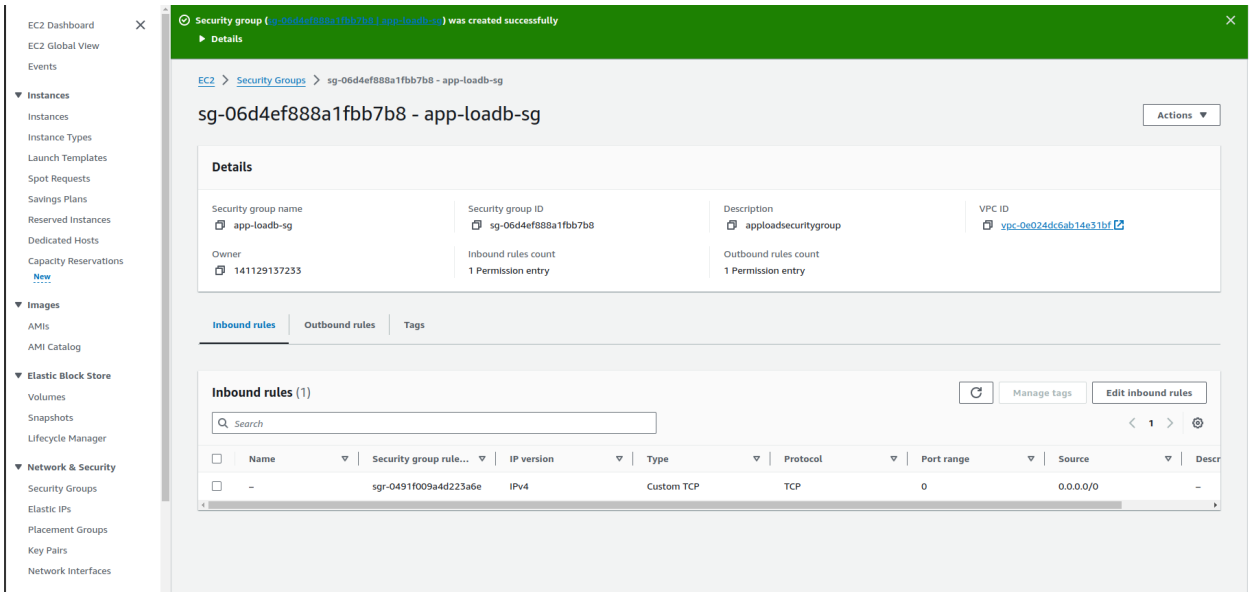
Step 06: Connecting with EC2 instance web server 1 through terminal

Step 07: Connecting with EC2 instance app server 1 through terminal

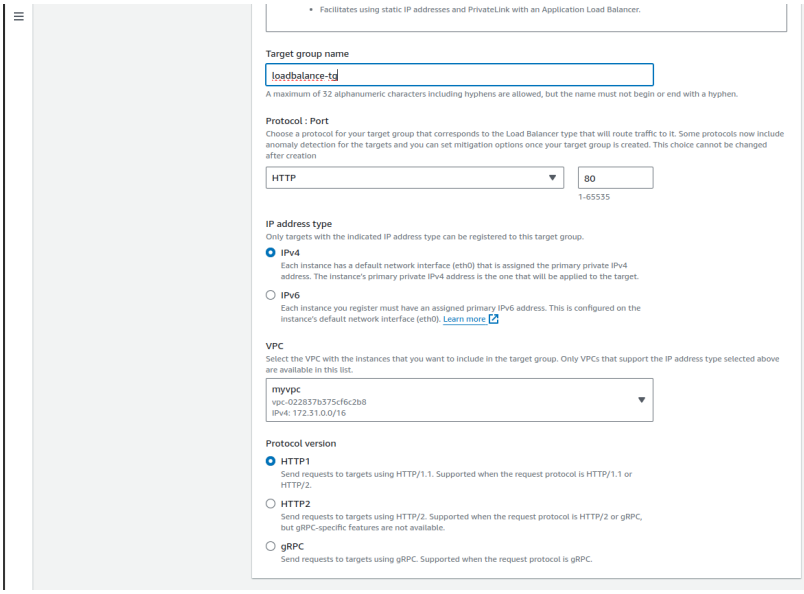

EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Instances (1/4) Info
Connect
Instance state
Actions
Launch instances
Instance state = running
Name
Availability Zone
Public IPv4 DNS
Public IPv4 ...
app-server-1
eu-north-1c
web-server2
eu-north-1a
51.21.130.16
web-server1
eu-north-1a
51.20.86.70
app-server2
eu-north-1b
acer@haq: ~/Desktop/semester 7/cloud-computing
(base) acer@haq:~/Desktop/semester 7$ ls
cloud-computing cn-lab database databaselab information-security os
(base) acer@haq:~/Desktop/semester 7$ cd cloud-computing/
(base) acer@haq:~/Desktop/semester 7/cloud-computing$ ssh -i "keypair1.pem" ec2-user@18.183.77.84
^C
(base) acer@haq:~/Desktop/semester 7/cloud-computing$ ssh -i "keypair1.pem" ec2-user@51.20.86.70
^C
(base) acer@haq:~/Desktop/semester 7/cloud-computing$ chmod 400 keypair1.pem
(base) acer@haq:~/Desktop/semester 7/cloud-computing$ ssh -i "keypair1.pem" ec2-user@10.0.5.118
Instance: i-0299e3b
Instance ID
i-0299e3b5fd0173a44 (web-server1)
Public IPv4 address
51.20.86.70 |open address
Private IPv4 addresses
10.0.5.118
IPv6 address
–
Instance state
Running
Public IPv4 DNS
–
Hostname type
IP name: ip-10-0-5-118.eu-north-1.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-5-118.eu-north-1.compute.internal
Answer private resource DNS name
–
Instance type
t3.micro
Elastic IP addresses
–
Auto-assigned IP address
51.20.86.70 [Public IP]
VPC ID
vpc-0e024dc6ab14e31bf (3tier application)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role
–
Subnet ID
subnet-03a9b632272b10a22 (db_subnet1)
Auto Scaling Group name
–

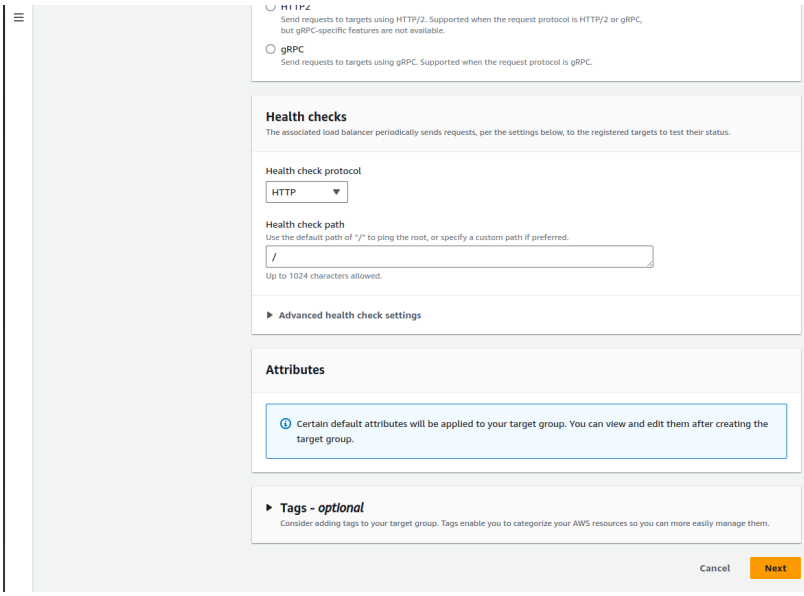

EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Security Groups (5) Info
Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
Name
Security group ID
Security group name
VPC ID
Description
Owner
sg-02b4b26aff8586d94
launch-wizard-2
vpc-0e024dc6ab14e31bf
launch-wizard-2 created 2023-12-28T...
141129137233
sg-0eef0c5e7b303b279
web-sg
allow ssh and http
sg-0f19e1b79325e6d07
default
default VPC security group
sg-07e74389d0d5a8d4c
launch-wizard-1
launch-wizard-1 created 2023-12-28T...
sg-0039a36adc2ce0879
vpc-022837b375cf6c2b8

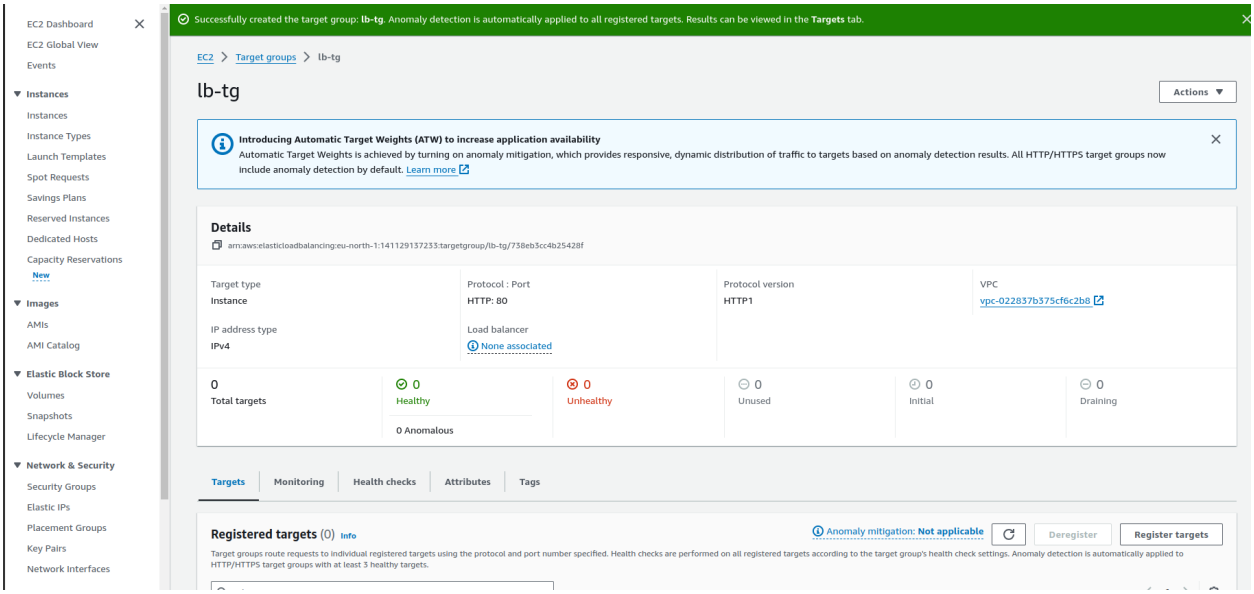


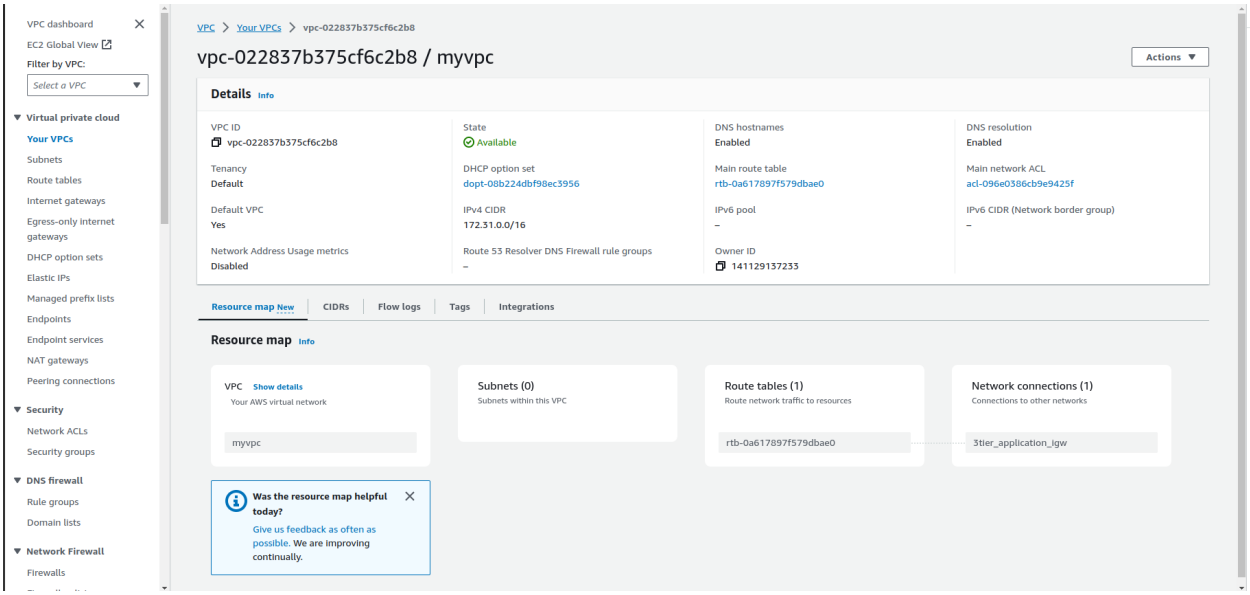


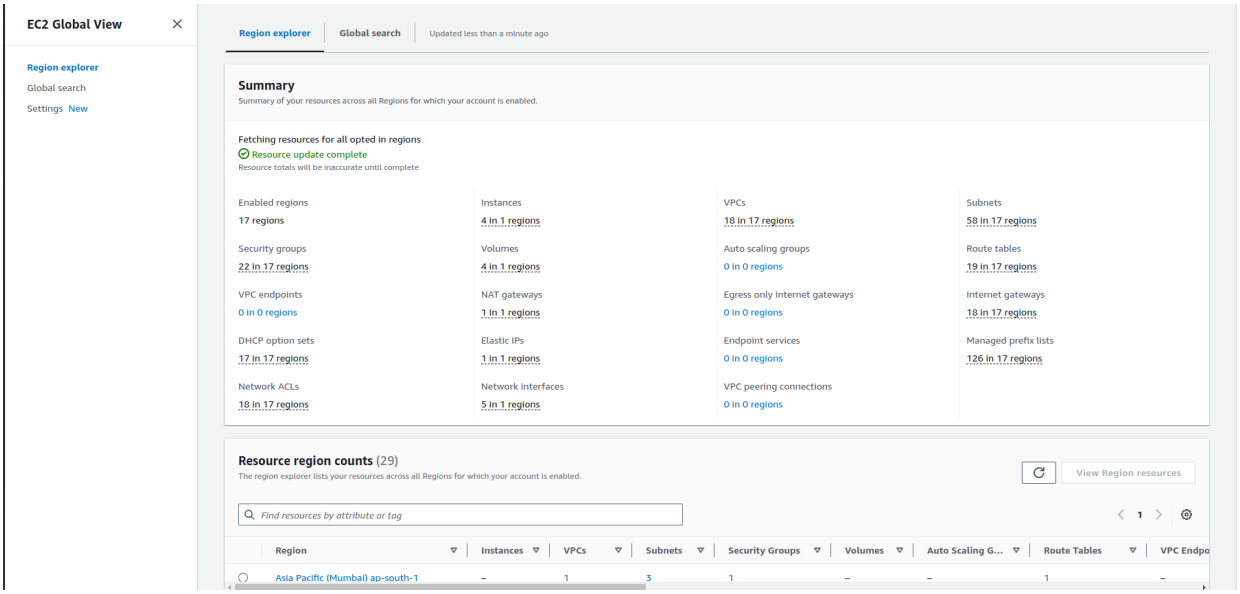
Step 08: Creating application load balancer

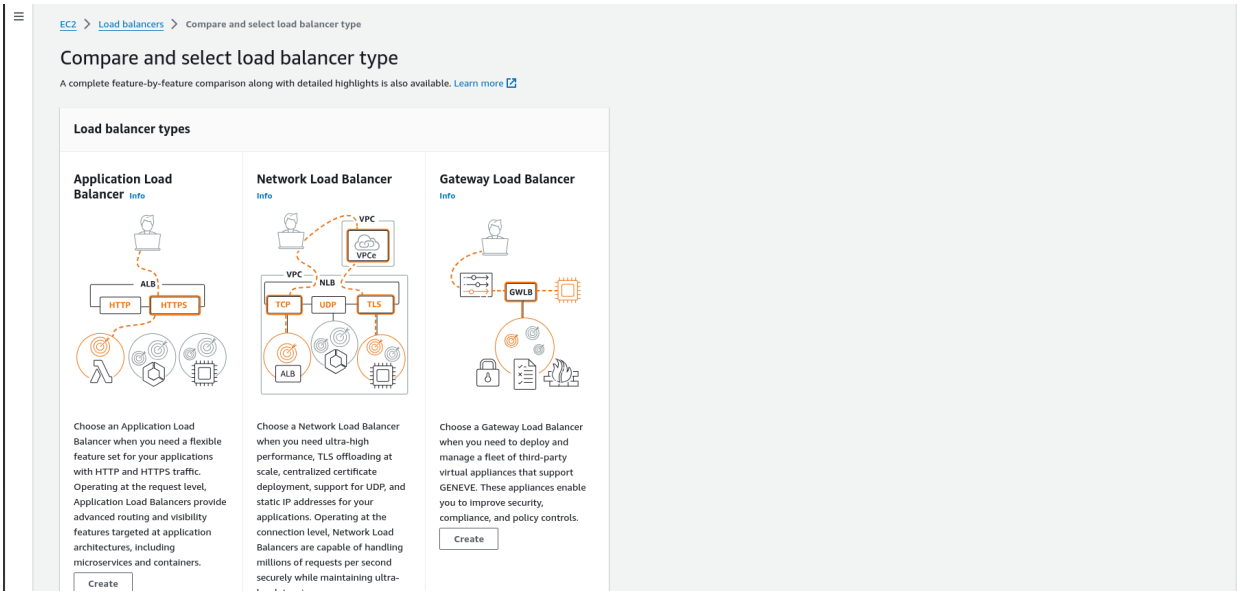

• Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.
Target group name
loadbalance-tg
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.
Protocol : Port
Choose a protocol for your target group 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.
myvpc
vpc-022837b375cf6c2b8
IPv4: 172.31.0.0/16
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.


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 ping the root, or specify a custom path if preferred.
/
Up to 1024 characters allowed.
Advanced health check settings
Attributes
Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.
Tags - optional
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.
Cancel
Next


EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Successfully created the target group: lb-tg. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab.
EC2 > Target groups > lb-tg
lb-tg
Actions
Introducing Automatic Target Weights (ATW) to increase application availability
Automatic Target Weights is achieved by turning on anomaly mitigation, which provides responsive, dynamic distribution of traffic to targets based on anomaly detection results. All HTTP/HTTPS target groups now include anomaly detection by default. Learn more
Details
arn:aws:elasticloadbalancing:eu-north-1:141129137233:targetgroup/lb-tg/738eb3cc4b25428f
Target type
Instance
Protocol : Port
HTTP: 80
Protocol version
HTTP1
VPC
vpc-022837b375cf6c2b8
IP address type
IPv4
Load balancer
None associated
0
Total targets
0
Healthy
0 Anomalous
0
Unhealthy
0
Unused
0
Initial
0
Draining
Targets
Monitoring
Health checks
Attributes
Tags
Registered targets (0) 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.


VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
VPC > Your VPCs > vpc-022837b375cf6c2b8
vpc-022837b375cf6c2b8 / myvpc
Actions
Details Info
VPC ID
vpc-022837b375cf6c2b8
State
Available
DNS hostnames
Enabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-08b224dbf98ec3956
Main route table
rtb-0a617897f579dbae0
Main network ACL
acl-096e0386cb9e9425f
Default VPC
Yes
IPv4 CIDR
172.31.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
–
Owner ID
141129137233
Resource map New
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Your AWS virtual network
myvpc
Subnets (0)
Subnets within this VPC
Route tables (1)
Route network traffic to resources
rtb-0a617897f579dbae0
Network connections (1)
Connections to other networks
3tier_application_igw
Was the resource map helpful today?
Give us feedback as often as possible. We are improving continually.


EC2 Global View
Region explorer
Global search
Settings New
Region explorer
Global search
Updated less than a minute ago
Summary
Summary of your resources across all Regions for which your account is enabled.
Fetching resources for all opted in regions
Resource update complete
Resource totals will be inaccurate until complete
Enabled regions
17 regions
Instances
4 in 1 regions
VPCs
18 in 17 regions
Subnets
58 in 17 regions
Security groups
22 in 17 regions
Volumes
4 in 1 regions
Auto scaling groups
0 in 0 regions
Route tables
19 in 17 regions
VPC endpoints
0 in 0 regions
NAT gateways
1 in 1 regions
Egress only internet gateways
0 in 0 regions
Internet gateways
18 in 17 regions
DHCP option sets
17 in 17 regions
Elastic IPs
1 in 1 regions
Endpoint services
0 in 0 regions
Managed prefix lists
126 in 17 regions
Network ACLs
18 in 17 regions
Network interfaces
5 in 1 regions
VPC peering connections
0 in 0 regions
Resource region counts (29)
The region explorer lists your resources across all Regions for which your account is enabled.
View Region resources
Find resources by attribute or tag
Region
Instances
VPCs
Subnets
Security Groups
Volumes
Auto Scaling G...
Route Tables
VPC Endpo
Asia Pacific (Mumbai) ap-south-1


EC2
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
ALB
HTTP
HTTPS
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.
Create
Network Load Balancer Info
VPC
VPCe
VPC
NLB
TCP
UDP
TLS
ALB
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-
Gateway Load Balancer Info
GWLB
Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.
Create

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 Elastic Load Balancing works**

Basic configuration

Load balancer name

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

3-tier-app-loadbalancer

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
  An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more
- ( ) Internal
  An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type Info

Select the type of IP addresses that your subnets use.

- (•) IPv4
  Recommended for internal load balancers.
- ( ) Dualstack
  Includes IPv4 and IPv6 addresses.

Network mapping Info

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

VPC Info

Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.

-

( ) Dualstack
Includes IPv4 and IPv6 addresses.

Network mapping Info

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

VPC Info

Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.

-
vpc-0accb0e05907b4023
IPv4: 172.31.0.0/16

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 are not supported by the load balancer or the VPC are not available for selection.

- [ ] **us-east-1a (use1-az2)**
- [ ] **us-east-1b (use1-az4)**
- [ ] **us-east-1c (use1-az6)**
- [ ] **us-east-1d (use1-az1)**
- [ ] **us-east-1e (use1-az3)**
- [ ] **us-east-1f (use1-az5)**

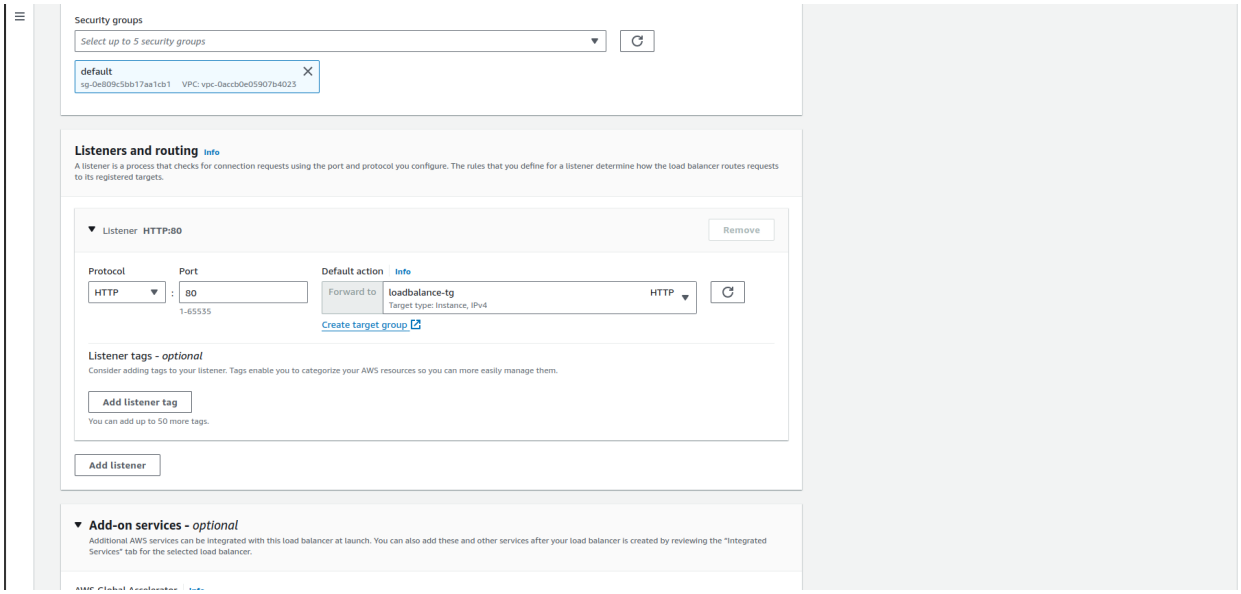
Security groups Info

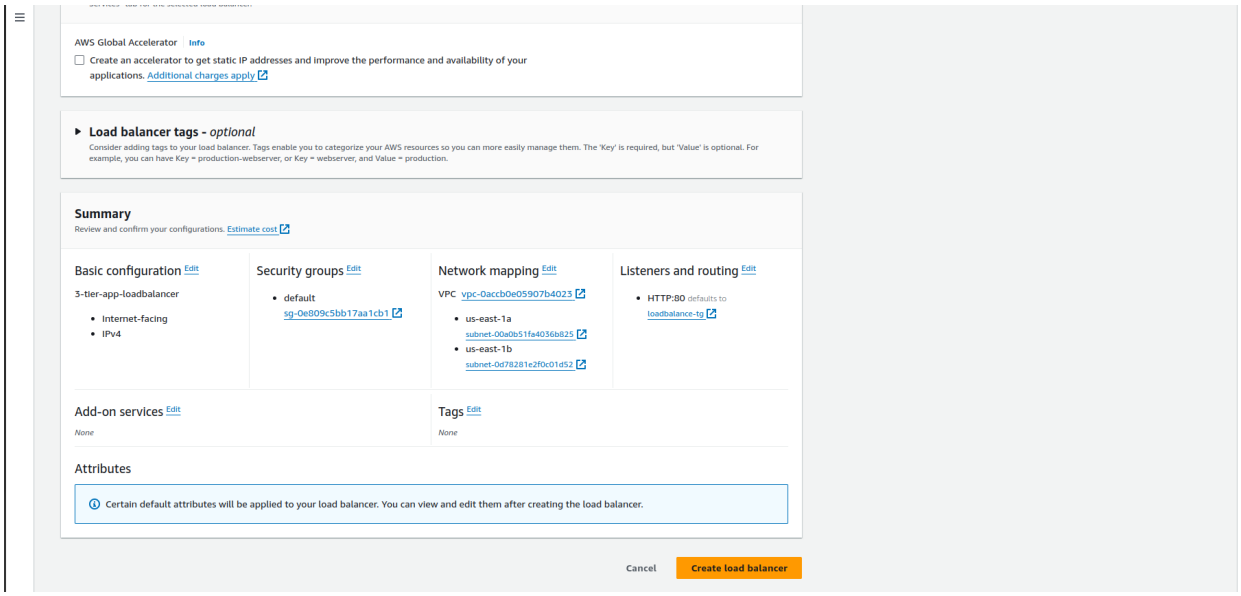
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

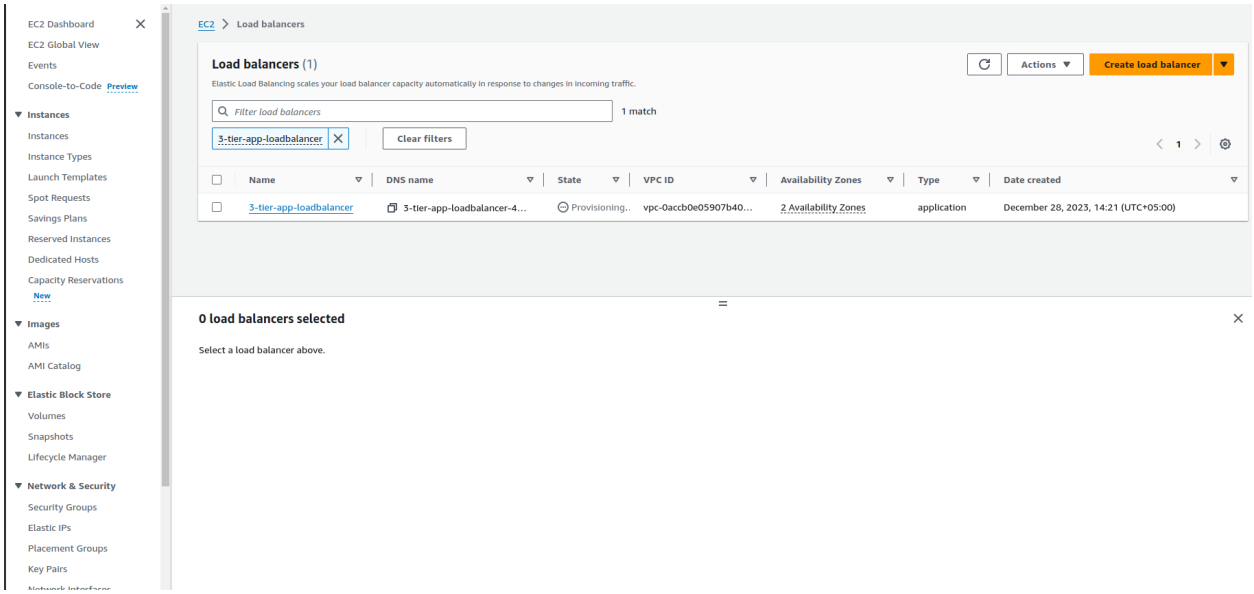
Security groups

Select up to 5 security groups

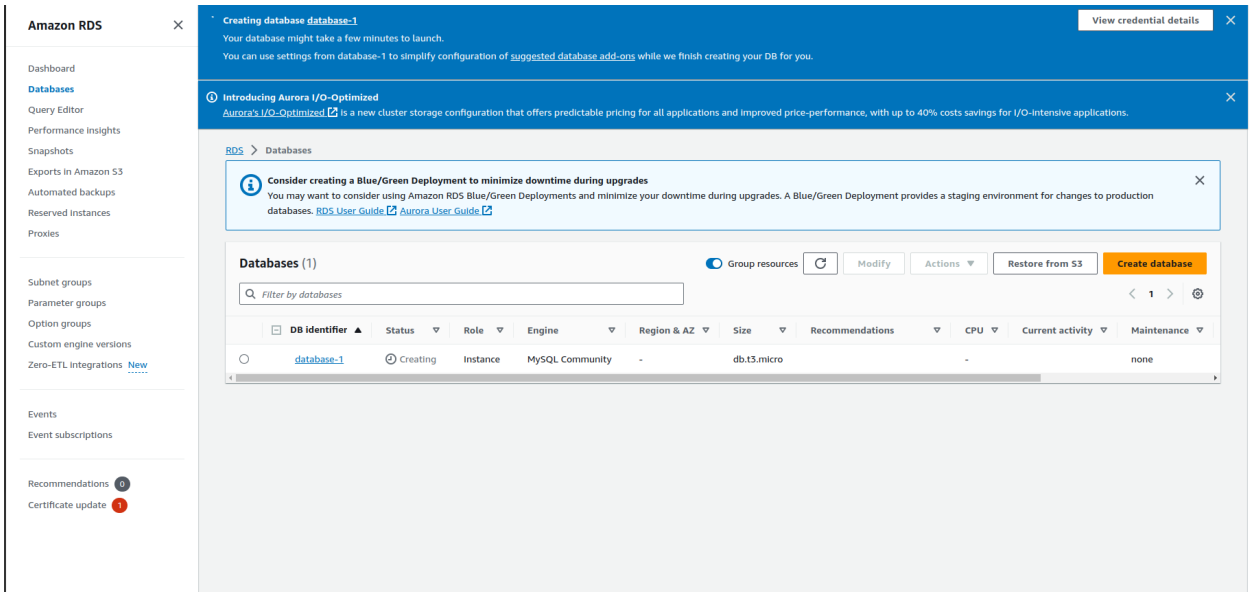
default

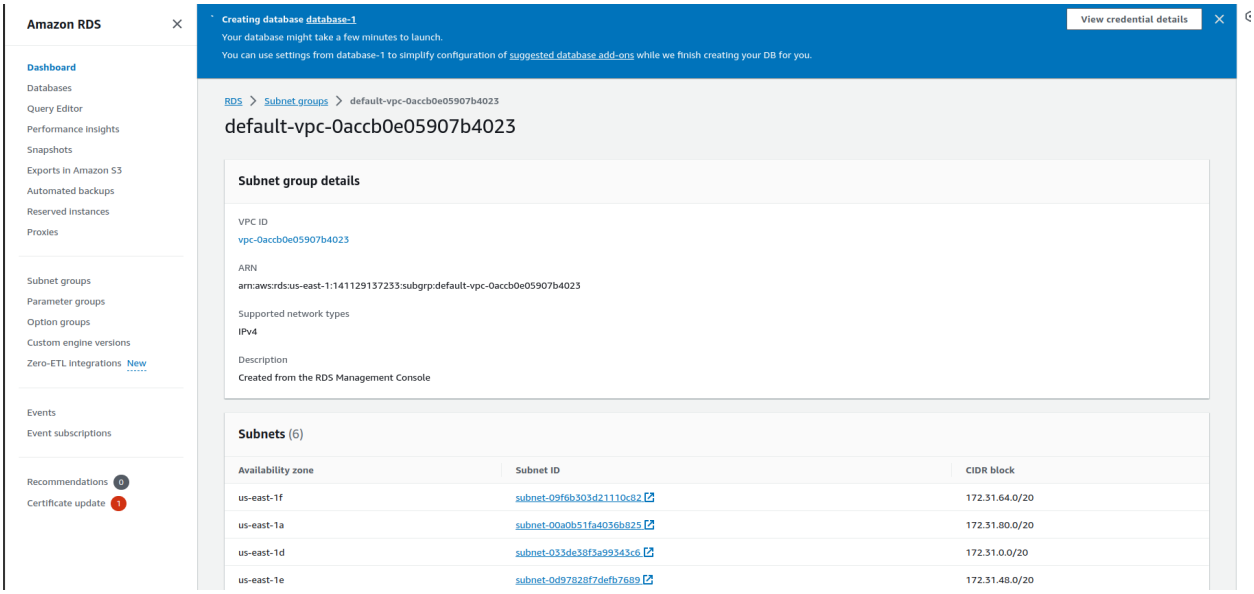

Security groups
Select up to 5 security groups
default
sg-0e809c5bb17aa1cb1 VPC: vpc-0accb0e05907b4023
Listeners and routing Info
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.
Listener HTTP:80
Remove
Protocol
Port
Default action Info
HTTP
80
1-65535
Forward to
loadbalance-tg
Target type: Instance, IPv4
HTTP
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.
Add listener tag
You can add up to 50 more tags.
Add listener
Add-on services - optional
Additional AWS services can be integrated with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the "Integrated Services" tab for the selected load balancer.

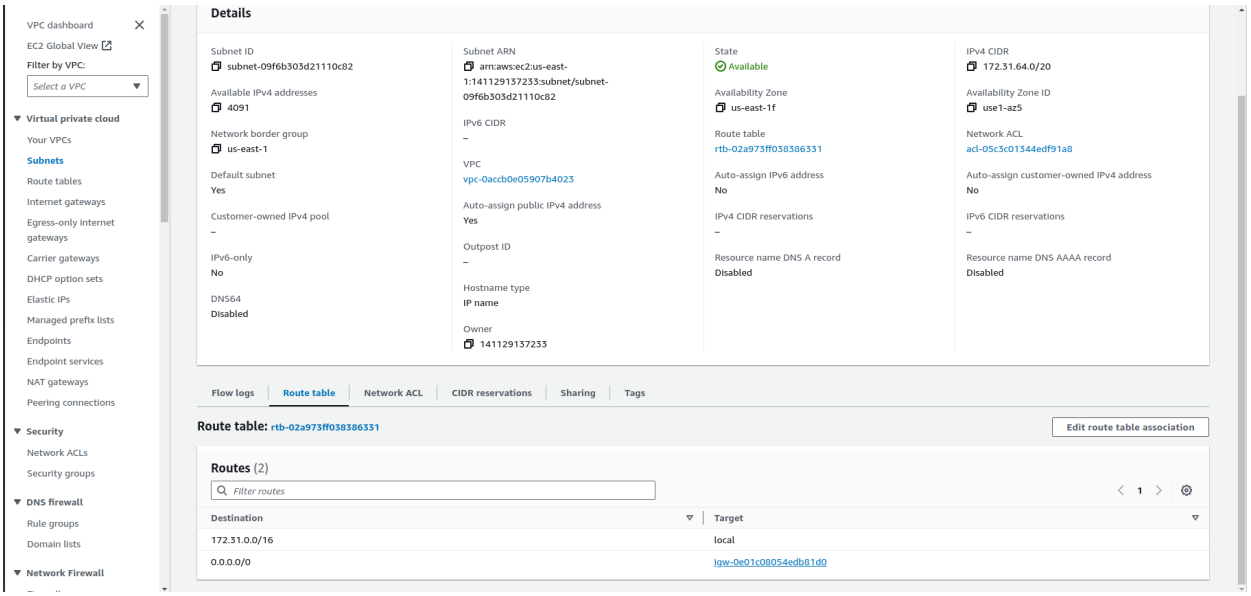

AWS Global Accelerator Info
Create an accelerator to get static IP addresses and improve the performance and availability of your applications. Additional charges apply
Load balancer tags - optional
Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.
Summary
Review and confirm your configurations. Estimate cost
Basic configuration Edit
3-tier-app-loadbalancer
Internet-facing
IPv4
Security groups Edit
default
sg-0e809c5bb17aa1cb1
Network mapping Edit
VPC vpc-0accb0e05907b4023
us-east-1a
subnet-00a0b51fa4036b825
us-east-1b
subnet-0d78281e2f0c01d52
Listeners and routing Edit
HTTP:80 defaults to
loadbalance-tg
Add-on services Edit
None
Tags Edit
None
Attributes
Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.
Cancel
Create load balancer



Step 9: Launching RDS instances (db-1 , db2)




Amazon RDS
Dashboard
Databases
Query Editor
Performance Insights
Snapshots
Exports in Amazon S3
Automated backups
Reserved instances
Proxies
Subnet groups
Parameter groups
Option groups
Custom engine versions
Zero-ETL integrations New
Events
Event subscriptions
Recommendations 0
Certificate update 1
Creating database database-1
Your database might take a few minutes to launch.
You can use settings from database-1 to simplify configuration of suggested database add-ons while we finish creating your DB for you.
View credential details
RDS > Subnet groups > default-vpc-0accb0e05907b4023
default-vpc-0accb0e05907b4023
Subnet group details
VPC ID
vpc-0accb0e05907b4023
ARN
arn:aws:rds:us-east-1:141129137233:subgrp:default-vpc-0accb0e05907b4023
Supported network types
IPv4
Description
Created from the RDS Management Console
Subnets (6)
Availability zone
Subnet ID
CIDR block
us-east-1f
subnet-09f6b303d21110c82
172.31.64.0/20
us-east-1a
subnet-00a0b51fa4036b825
172.31.80.0/20
us-east-1d
subnet-033de38f3a99343c6
172.31.0.0/20
us-east-1e
subnet-0d97828f7defb7689
172.31.48.0/20


VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Details
Subnet ID
subnet-09f6b303d21110c82
Available IPv4 addresses
4091
Network border group
us-east-1
Default subnet
Yes
Customer-owned IPv4 pool
–
IPv6-only
No
DNS64
Disabled
Subnet ARN
arn:aws:ec2:us-east-1:141129137233:subnet/subnet-09f6b303d21110c82
IPv6 CIDR
–
VPC
vpc-0accb0e05907b4023
Auto-assign public IPv4 address
Yes
Outpost ID
–
Hostname type
IP name
Owner
141129137233
State
Available
Availability Zone
us-east-1f
Route table
rtb-02a973ff038386331
Auto-assign IPv6 address
No
IPv4 CIDR reservations
–
Resource name DNS A record
Disabled
IPv4 CIDR
172.31.64.0/20
Availability Zone ID
use1-az5
Network ACL
acl-05c3c01344edf91a8
Auto-assign customer-owned IPv4 address
No
IPv6 CIDR reservations
–
Resource name DNS AAAA record
Disabled
Flow logs
Route table
Network ACL
CIDR reservations
Sharing
Tags
Route table: rtb-02a973ff038386331
Edit route table association
Routes (2)
Filter routes
Destination
Target
172.31.0.0/16
local
0.0.0.0/0
igw-0e01c08054edb81d0