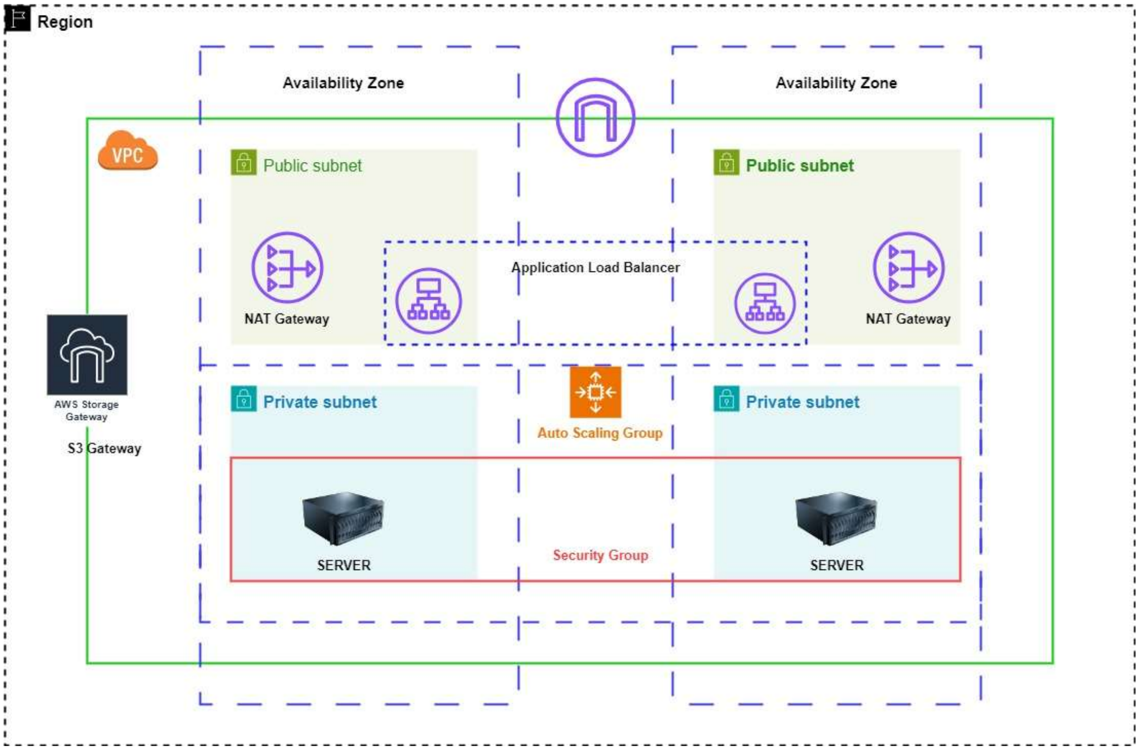
How to create VPC with public-private subnet that you can use for servers in a production environment?

To improve resiliency, you deploy the servers in two Availability Zones, by using an Auto Scaling group and an Application Load Balancer. For additional security, you deploy the servers in private subnets. The servers receive requests through the load balancer. The servers can connect to the internet by using a NAT gateway. To improve resiliency, you deploy the NAT gateway in both Availability Zones.

In a private subnet I have deployed the applications.



Overview -:

The VPC has public subnets and private subnets in two Availability Zones.

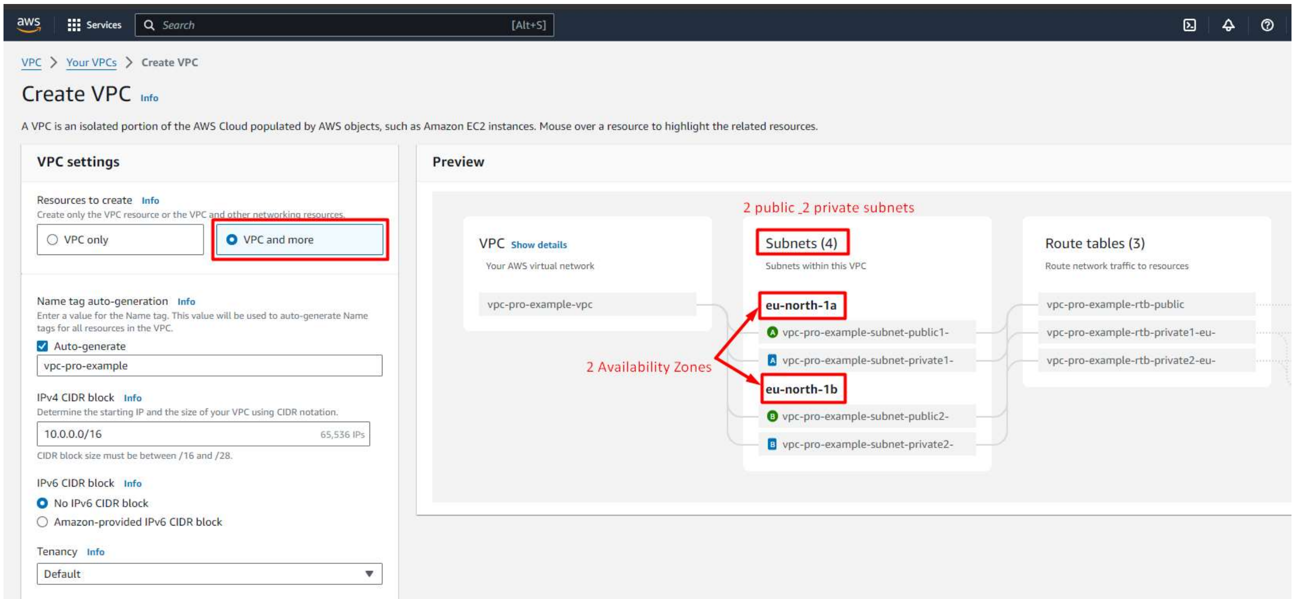
Each public subnet contains a NAT gateway and a load balancer node.

The servers run in the private subnets, are launched and terminated by using an Auto Scaling group, and receive traffic from the load balancer.

The servers can connect to the internet by using the NAT gateway.

Step-1

1. **Create VPC on AWS console.**



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
○ VPC only ● VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
☑ Auto-generate
vpc-pro-example

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

Tenancy Info
Default

Preview

VPC Show details
Your AWS virtual network
vpc-pro-example-vpc

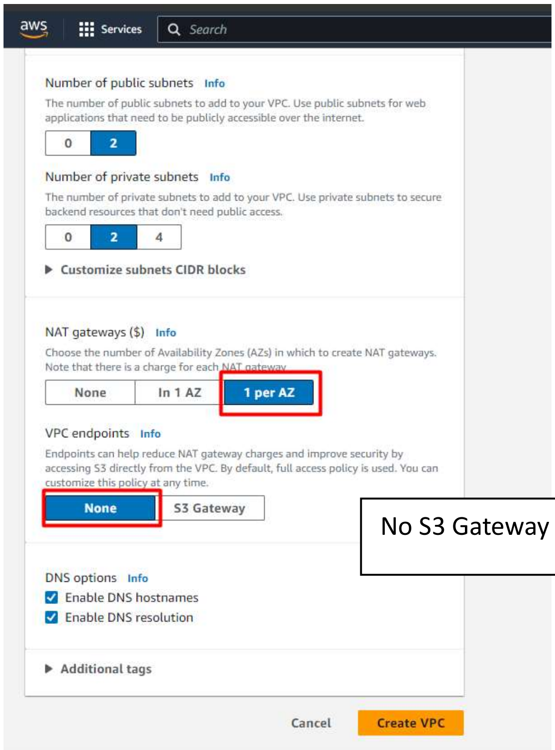
Subnets (4)
Subnets within this VPC
eu-north-1a
vpc-pro-example-subnet-public1-
vpc-pro-example-subnet-private1-
eu-north-1b
vpc-pro-example-subnet-public2-
vpc-pro-example-subnet-private2-

Route tables (3)
Route network traffic to resources
vpc-pro-example-rtb-public
vpc-pro-example-rtb-private1-eu-
vpc-pro-example-rtb-private2-eu-

2 public ,2 private subnets

2 Availability Zones

- Then AWS is going to create
    - Route tables
    - Internet Gateway



Number of public subnets Info
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.
0 | **2**

Number of private subnets Info
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.
0 | **2** | 4

▶ Customize subnets CIDR blocks

NAT gateways ($) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.
None | In 1 AZ | **1 per AZ**

VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.
None | S3 Gateway

DNS options Info
☑ Enable DNS hostnames
☑ Enable DNS resolution

▶ Additional tags

Cancel | Create VPC

No S3 Gateway for VPC

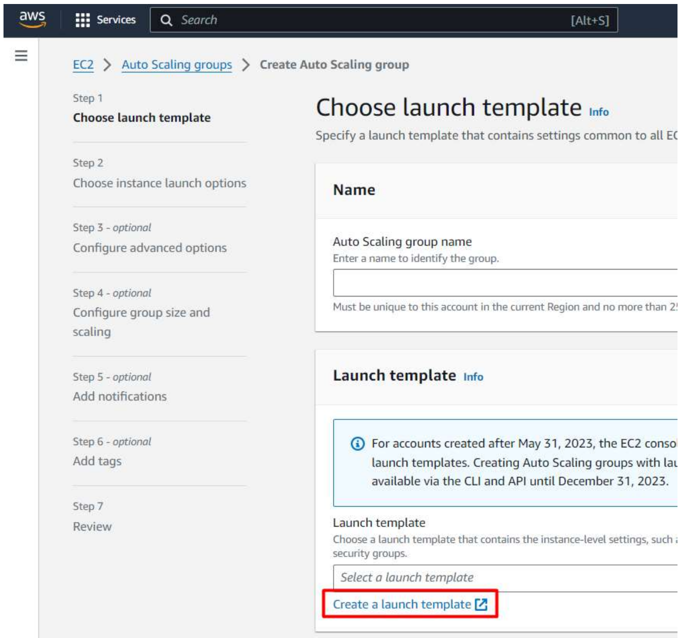
- Now all the configuration is provided.
- Now you can create a VPC.

Step-2

Now you need to create EC2 instance where your applications are deployed, will do them with autoscaling group. In AWS auto scaling cannot created directly you can use launch template.

So, you can use this launch template across multiple groups or this template act as a reference.

Create Auto Scaling Group.



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template

Step 2
Choose instance launch options

Step 3 - *optional*
Configure advanced options

Step 4 - *optional*
Configure group size and scaling

Step 5 - *optional*
Add notifications

Step 6 - *optional*
Add tags

Step 7
Review

Choose launch template Info

Specify a launch template that contains settings common to all EC

Name

Auto Scaling group name
Enter a name to identify the group.

Must be unique to this account in the current Region and no more than 2!

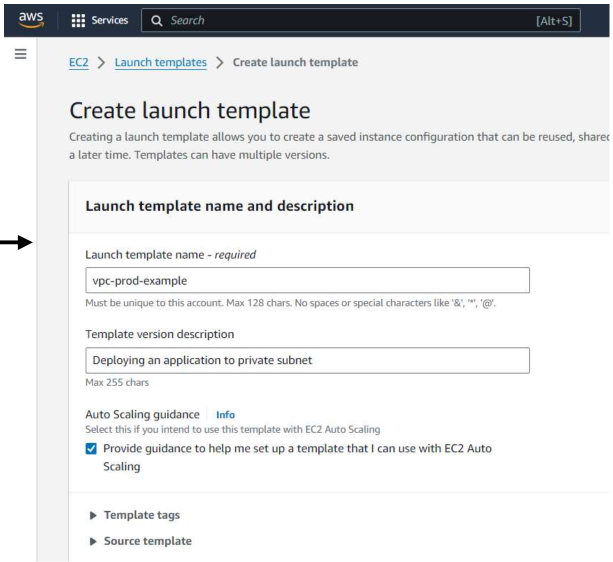
Launch template Info

For accounts created after May 31, 2023, the EC2 conso
launch templates. Creating Auto Scaling groups with lau
available via the CLI and API until December 31, 2023.

Launch template
Choose a launch template that contains the instance-level settings, such a
security groups.

Select a launch template

Create a launch template



EC2 > Launch templates > Create launch template

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, sharec
a later time. Templates can have multiple versions.

Launch template name and description

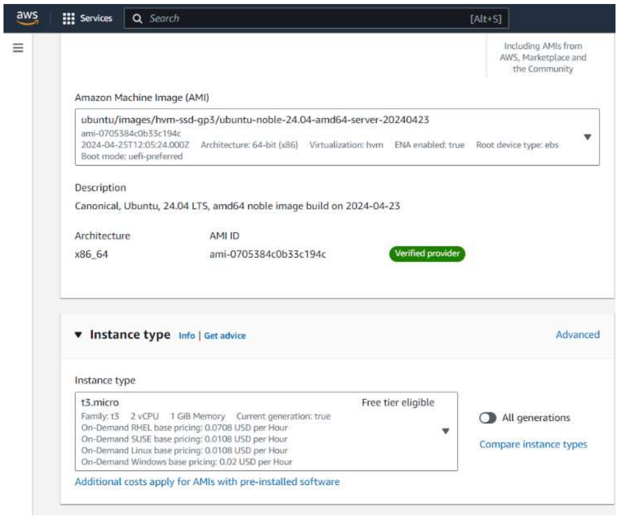
Launch template name - *required*
vpc-prod-example
Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description
Deploying an application to private subnet
Max 255 chars

Auto Scaling guidance Info
Select this if you intend to use this template with EC2 Auto Scaling
☑ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

▶ Template tags
▶ Source template

Then you need to choose operating system and type of instance by your own.



Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)
ubuntu/images/hvm-ssd-gp3/ubuntu-noble-24.04-amd64-server-20240423
ami-0705384c0b33c194c
2024-04-25T12:05:24.000Z Architecture: 64-bit (x86) Virtualization: hvm ENA enabled: true Root device type: ebs
Boot mode: uefi-preferred

Description
Canonical, Ubuntu, 24.04 LTS, amd64 noble image build on 2024-04-23

Architecture	AMI ID
x86_64	ami-0705384c0b33c194c

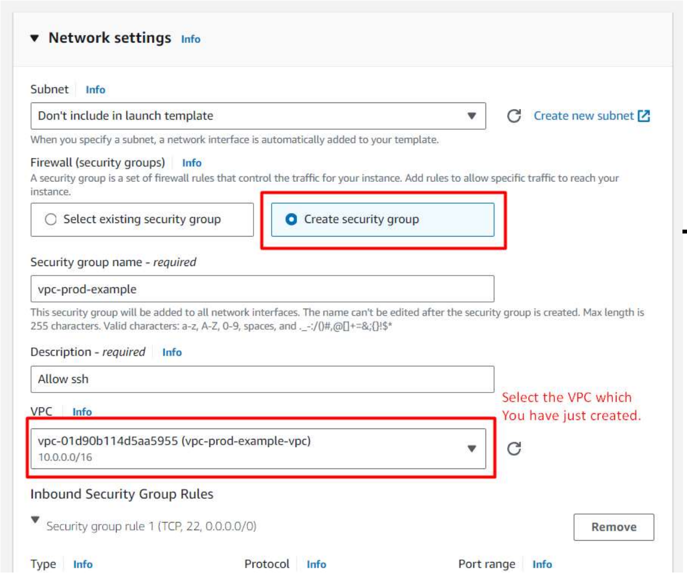
▼ **Instance type** Info | Get advice   Advanced

Instance type
t3.micro   Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.0708 USD per Hour
On-Demand SUSE base pricing: 0.0108 USD per Hour
On-Demand Linux base pricing: 0.0108 USD per Hour
On-Demand Windows base pricing: 0.02 USD per Hour

○ All generations
Compare instance types

Additional costs apply for AMIs with pre-installed software

After that you need to make some changes in network settings as below.



▼ Network settings Info

Subnet Info

Don't include in launch template ▼ — Create new subnet

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

Firewall (security groups) Info

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

○ Select existing security group ● Create security group

Security group name - *required*

vpc-prod-example

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

VPC Info

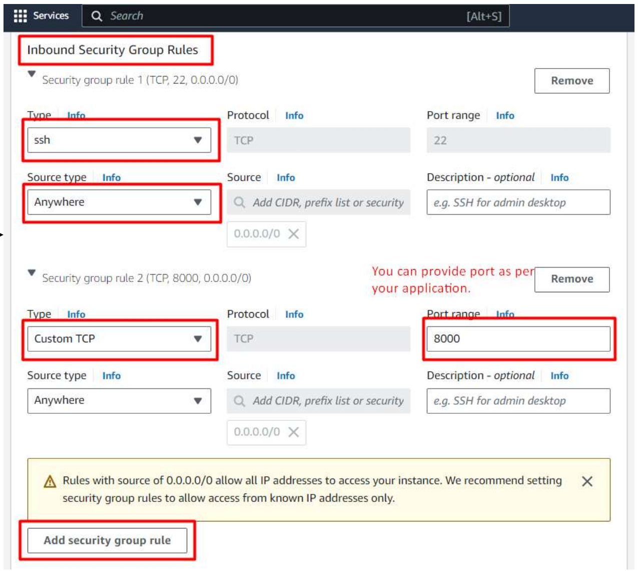
vpc-01d90b114d5aa5955 (vpc-prod-example-vpc)
10.0.0.0/16

Select the VPC which You have just created.

Inbound Security Group Rules

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

Type Info — Protocol Info — Port range Info



Inbound Security Group Rules

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

Type	Protocol	Port range
ssh	TCP	22

Source type	Source	Description - *optional*
Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 8000, 0.0.0.0/0) — Remove

You can provide port as per your application.

Type	Protocol	Port range
Custom TCP	TCP	8000

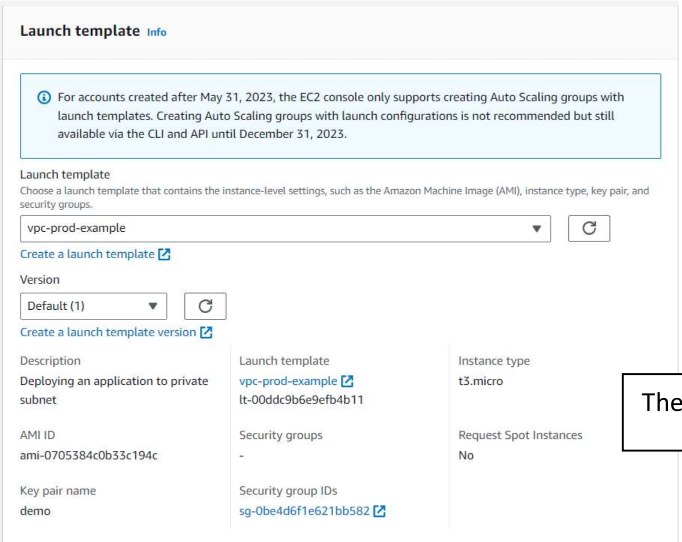
Source type	Source	Description - *optional*
Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

⚠ 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.

Add security group rule

Now, you have done with all configuration. Now you can create launch template.

After that refresh the page and you can see the launch template.



Launch template Info

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

Launch template

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

vpc-prod-example

Create a launch template

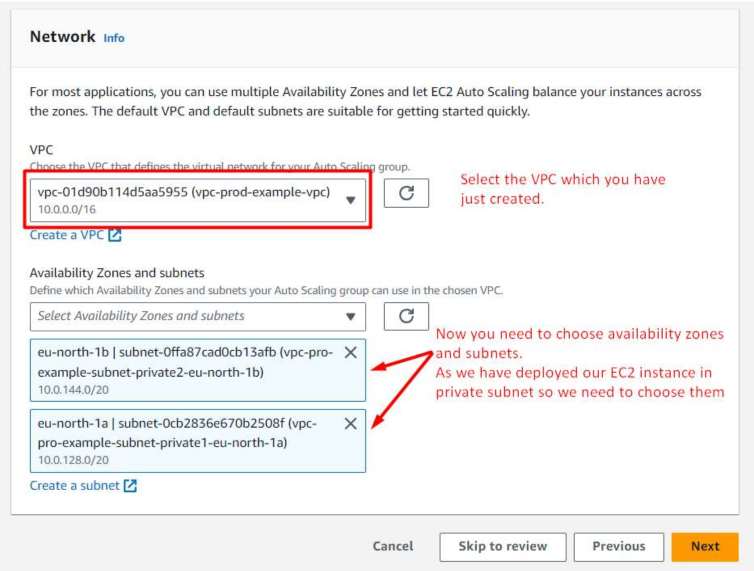
Version

Default (1)

Create a launch template version

Description	Launch template	Instance type
Deploying an application to private subnet	vpc-prod-example lt-00ddc9b6e9efb4b11	t3.micro
AMI ID	**Security groups**	**Request Spot Instances**
ami-0705384c0b33c194c	-	No
Key pair name	**Security group IDs**	
demo	sg-0be4d6f1e621bb582	

Then press next!



Network Info

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

VPC

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

vpc-01d90b114d5aa5955 (vpc-prod-example-vpc)
10.0.0.0/16

Select the VPC which you have just created.

Create a VPC

Availability Zones and subnets

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

Select Availability Zones and subnets

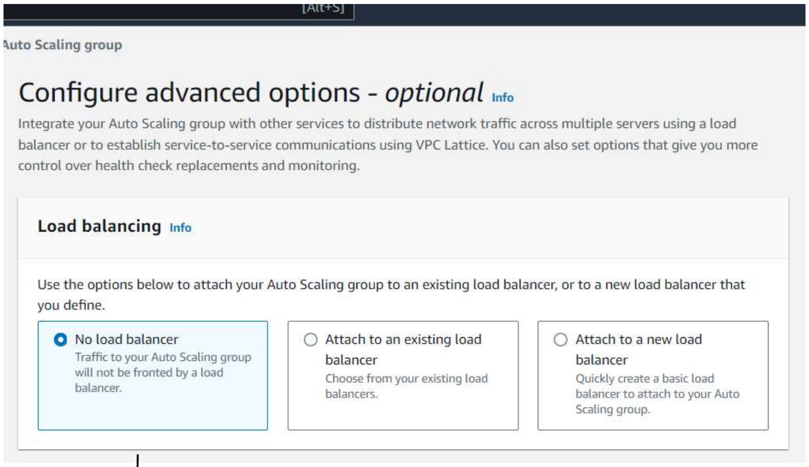
eu-north-1b | subnet-0ffa87cad0cb13afb (vpc-pro-example-subnet-private2-eu-north-1b)
10.0.144.0/20

eu-north-1a | subnet-0cb2836e670b2508f (vpc-pro-example-subnet-private1-eu-north-1a)
10.0.128.0/20

Now you need to choose availability zones and subnets.
As we have deployed our EC2 instance in private subnet so we need to choose them

Create a subnet

Cancel — Skip to review — Previous — Next



Auto Scaling group

Configure advanced options - *optional* Info

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

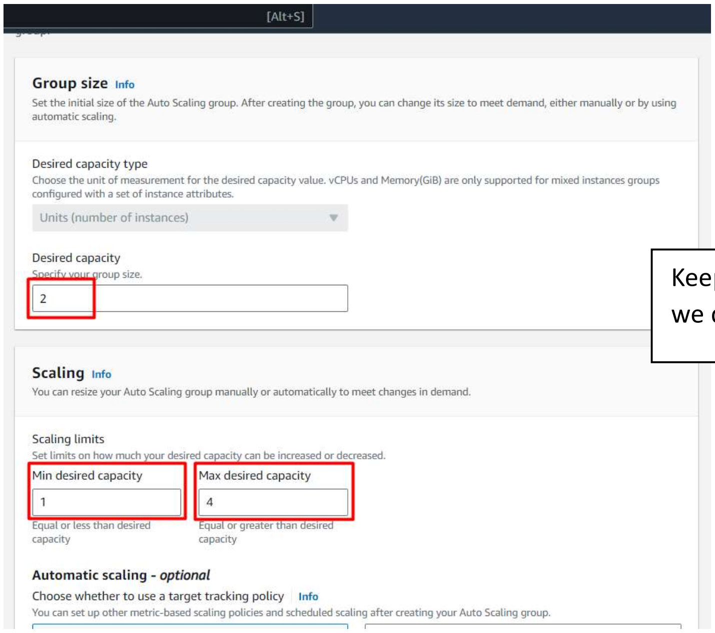
Load balancing Info

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

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

At this moment, we are not going to create any load balancer. We will create load balancer in different context.

We will create load balancer in public subnet.



Group size Info

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

Desired capacity type

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

Units (number of instances)

Desired capacity

Specify your group size.

2

Scaling Info

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

Scaling limits

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

Min desired capacity: 1 — Equal or less than desired capacity

Max desired capacity: 4 — Equal or greater than desired capacity

Automatic scaling - *optional*

Choose whether to use a target tracking policy Info

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

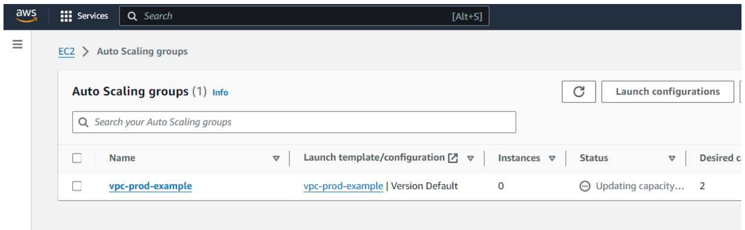
Keep other settings as it is. Which we don't require right now.

We are going to start with two EC2 instance.

But in some of the case if you receive more traffic, then auto scaling group based on CPU monitoring increase the capacity of EC2 instance from n number of size.

Now you have done with all configuration for Auto Scaling Group and now you can lunch or create Auto Scaling Group.

Your Auto Scaling Group looks like below.

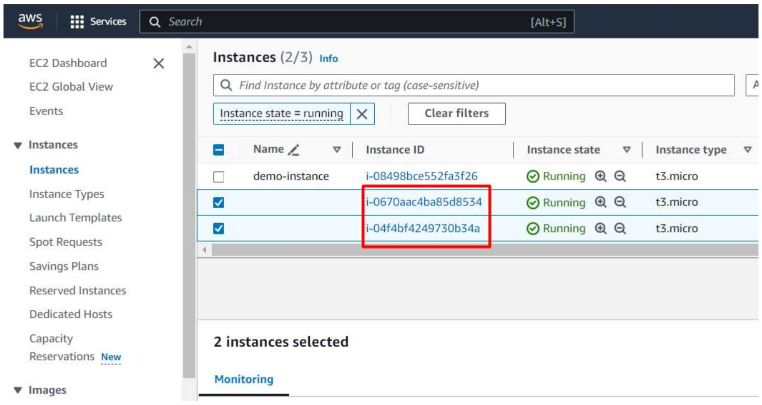


Auto Scaling groups (1) Info

Search your Auto Scaling groups

Name	Launch template/configuration	Instances	Status	Desired c
vpc-prod-example	vpc-prod-example | Version Default	0	Updating capacity...	2

As you can see our both EC2 instance is created by Auto Scaling Group is running fine.



Instances (2/3) Info

Find Instance by attribute or tag (case-sensitive)

Instance state = running ✕ | Clear filters

☑	Name	Instance ID	Instance state	Instance type
□	demo-instance	i-08498bce552fa3f26	Running	t3.micro
☑		i-0670aac4ba85d8534	Running	t3.micro
☑		i-04f4bf4249730b34a	Running	t3.micro

2 instances selected

Step-3

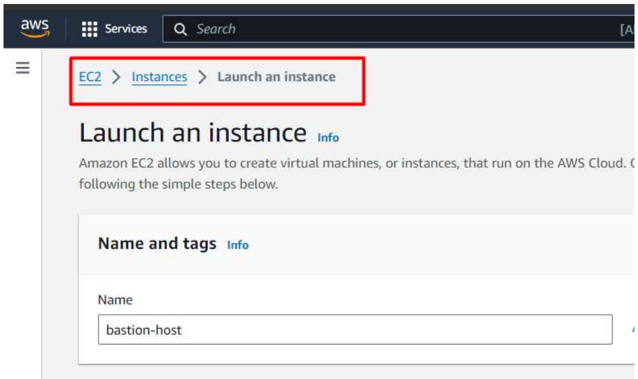
You can clearly see your EC2 instance does not have public IP address. If you want to login into EC2 instance which is in private subnet. Then you must use bastion Host or Jump server.

Bastion Host or Jump server -: It act as a mediator between your private subnet and public subnet or external person.

So, you need to create bastion host.

Go to

Instance → Launch an Instance



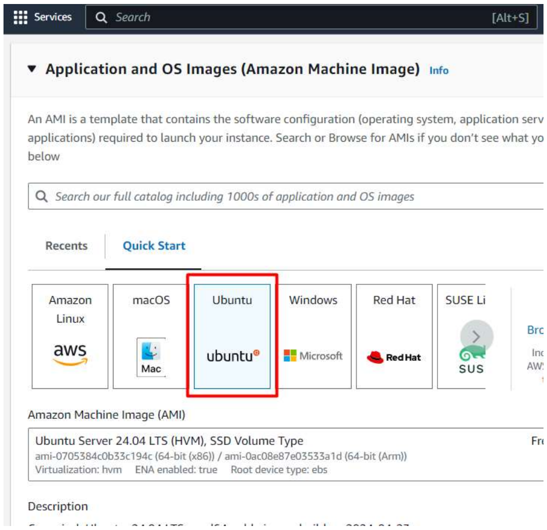
EC2 > Instances > Launch an instance

Launch an instance Info

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

Name and tags Info

Name: bastion-host



Application and OS Images (Amazon Machine Image) Info

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

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

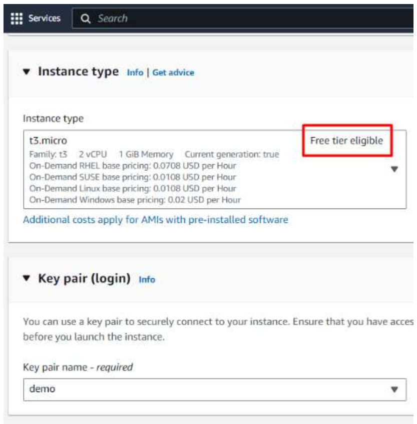
Recents | Quick Start

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

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0705384c0b33c194c (64-bit (x86)) / ami-0ac08e87e03533a1d (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description



Instance type Info | Get advice

Instance type

t3.micro Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.0708 USD per Hour
On-Demand SUSE base pricing: 0.0108 USD per Hour
On-Demand Linux base pricing: 0.0108 USD per Hour
On-Demand Windows base pricing: 0.02 USD per Hour

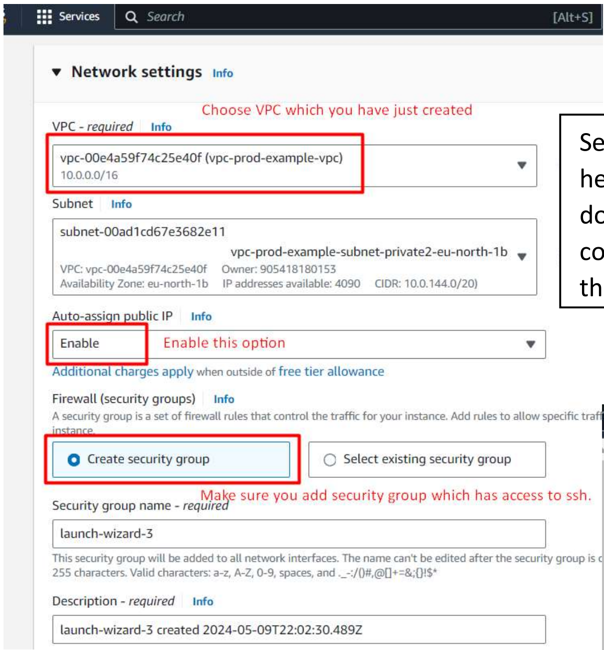
Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

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

Key pair name - required: demo

You need to edit network settings.



▼ Network settings Info

Choose VPC which you have just created

VPC - *required* Info

vpc-00e4a59f74c25e40f (vpc-prod-example-vpc)
10.0.0.0/16

Subnet Info

subnet-00ad1cd67e3682e11
vpc-prod-example-subnet-private2-eu-north-1b
VPC: vpc-00e4a59f74c25e40f Owner: 905418180153
Availability Zone: eu-north-1b IP addresses available: 4090 CIDR: 10.0.144.0/20)

Auto-assign public IP Info

Enable — Enable this option

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

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

● Create security group ○ Select existing security group

Make sure you add security group which has access to ssh.

Security group name - *required*

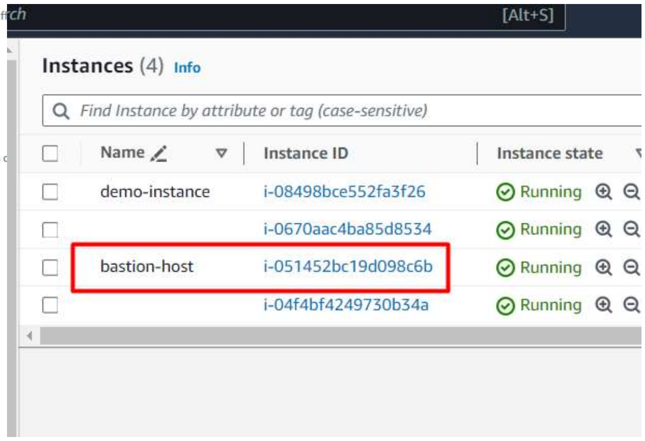
launch-wizard-3

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

Description - *required* Info

launch-wizard-3 created 2024-05-09T22:02:30.489Z

Select public subnet here then you have done with all configuration. Leave all the setting as it is and



Instances (4) Info

□	Name	Instance ID	Instance state
□	demo-instance	i-08498bce552fa3f26	Running
□		i-0670aac4ba85d8534	Running
□	bastion-host	i-051452bc19d098c6b	Running
□		i-04f4bf4249730b34a	Running

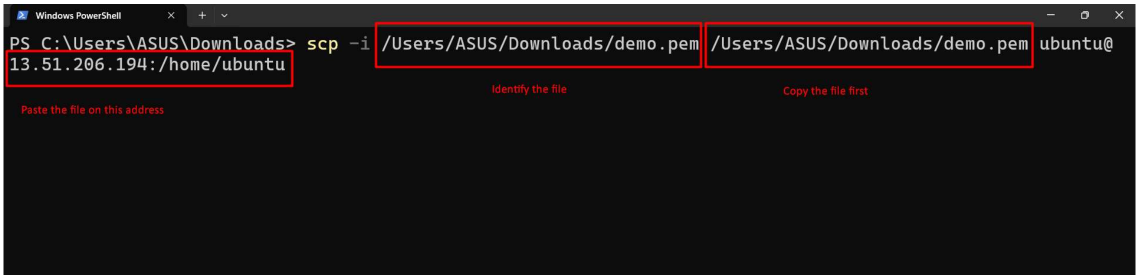
Once the instance is launched you can SSH from public subnet to private subnet.

But SSH to private subnet again you need the key value pair which is available on your system. So, you need to copy the key value pair to bastion host.

Along with log into bastion host you also need to login into instances for that this bastion host should the SSh access for these instances.

Using this command you can copy your key value for from your local system to bastion host. You need to provide your bastion host instance's IP address.

> scp - i scp securley copy the file from one host machine to other host machine.

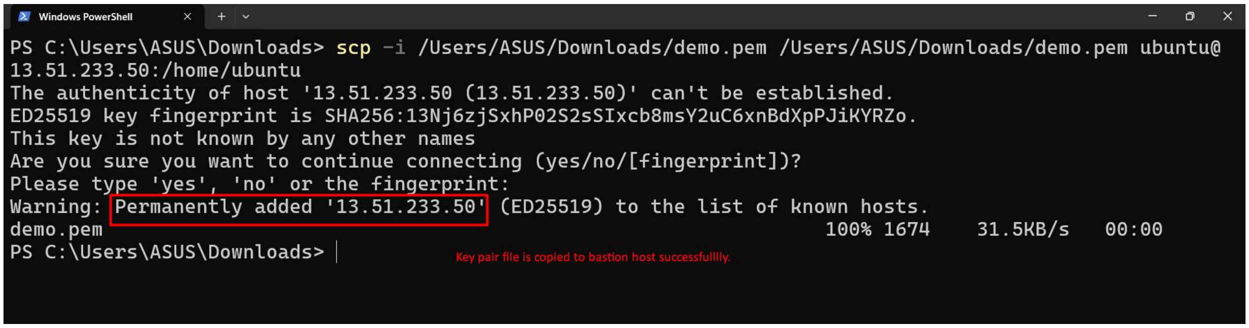


```
PS C:\Users\ASUS\Downloads> scp -i /Users/ASUS/Downloads/demo.pem /Users/ASUS/Downloads/demo.pem ubuntu@
13.51.206.194:/home/ubuntu
```

Identify the file

Copy the file first

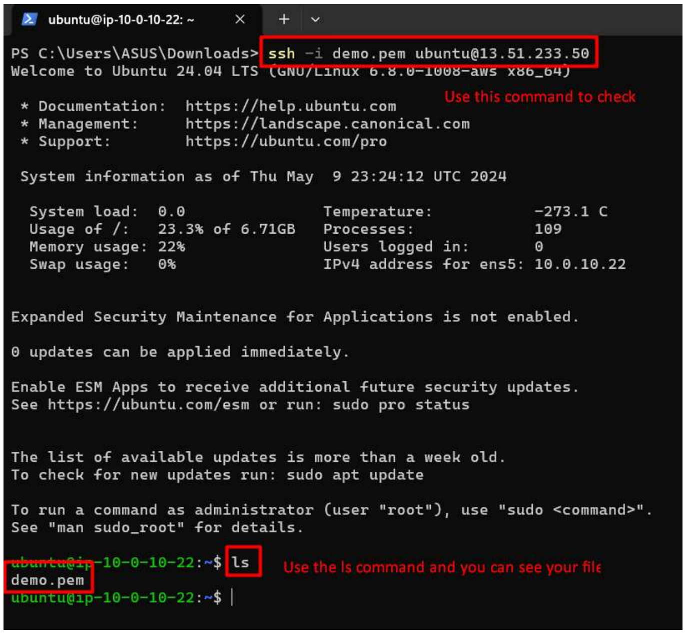
Paste the file on this address



```
PS C:\Users\ASUS\Downloads> scp -i /Users/ASUS/Downloads/demo.pem /Users/ASUS/Downloads/demo.pem ubuntu@
13.51.233.50:/home/ubuntu
The authenticity of host '13.51.233.50 (13.51.233.50)' can't be established.
ED25519 key fingerprint is SHA256:13Nj6zjSxhP02S2sSIxcb8msY2uC6xnBdXpPJiKYRZo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Please type 'yes', 'no' or the fingerprint:
Warning: Permanently added '13.51.233.50' (ED25519) to the list of known hosts.
demo.pem                                                                      100% 1674    31.5KB/s   00:00
PS C:\Users\ASUS\Downloads> |
```

Key pair file is copied to bastion host successfulllly.

You can login to the bastion host and see whether the file is copied or not.



```
PS C:\Users\ASUS\Downloads> ssh -i demo.pem ubuntu@13.51.233.50
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1008-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu May  9 23:24:12 UTC 2024

  System load:  0.0               Temperature:           -273.1 C
  Usage of /:   23.3% of 6.71GB   Processes:             109
  Memory usage: 22%               Users logged in:       0
  Swap usage:   0%                IPv4 address for ens5: 10.0.10.22


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-10-22:~$ ls
demo.pem
ubuntu@ip-10-0-10-22:~$ |
```

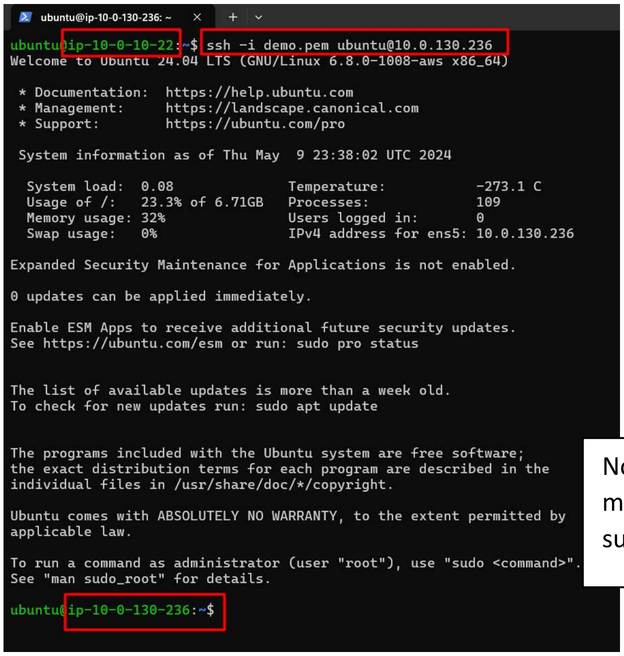
Use this command to check

Use the ls command and you can see your file

If your key pair file is not there then you cannot login to any instances which are available in private subnet.

Step-4

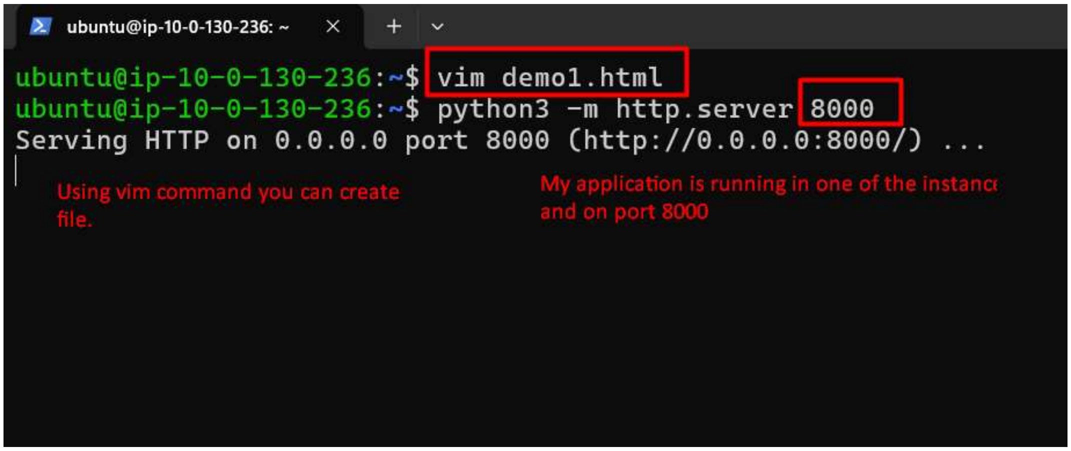
Now you need to login into your one of the instances and install the application.



```
ubuntu@ip-10-0-10-22:~$ ssh -i demo.pem ubuntu@10.0.130.236
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1008-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu May  9 23:38:02 UTC 2024

  System load:  0.08               Temperature:           -273.1 C
  Usage of /:   23.3% of 6.71GB    Processes:             109
  Memory usage: 32%                Users logged in:       0
  Swap usage:   0%                 IPv4 address for ens5: 10.0.130.236

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-130-236:~$
```

Now you can see I'm able to login to my instance which is in private subnet.

Install the python application and create HTML page as well for demo.



```
ubuntu@ip-10-0-130-236:~$ vim demo1.html
ubuntu@ip-10-0-130-236:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Using vim command you can create file.

My application is running in one of the instanc and on port 8000

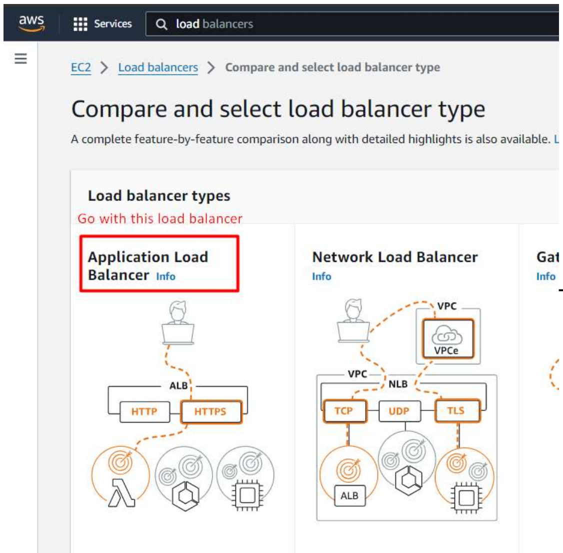
Why we have logged into only one of the instances because while using load balancer I want to demonstrate that traffic is going to one particular instance, it is hitting and giving you back the response.

Whereas it goes to other particular application in a different subnet it is giving you an error response because this page is not available or the application is not available.

So, for that purpose I've installed python application in one EC2 instance and did not install in other EC2 instance.

Step-5

Create the load balancer and attach these instances as target group that will be our final stage.



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. L

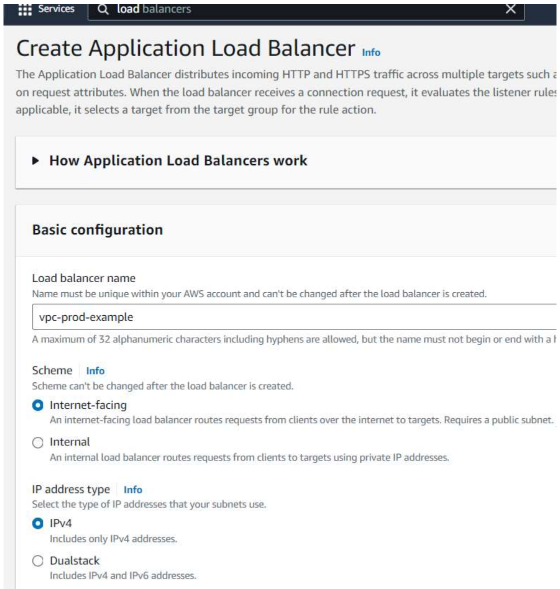
Load balancer types

Go with this load balancer

Application Load Balancer Info

Network Load Balancer Info

Gat Info



Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such a on request attributes. When the load balancer receives a connection request, it evaluates the listener rules applicable, it selects a target from the target group for the rule action.

▸ How Application Load Balancers work

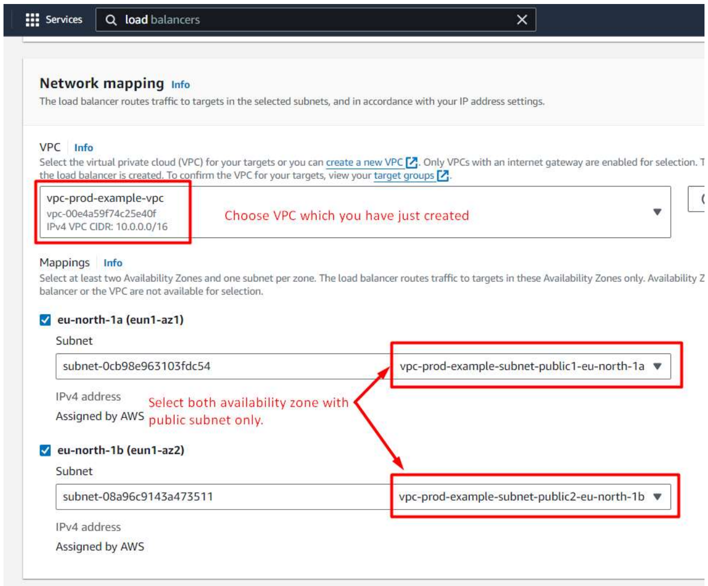
Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
vpc-prod-example
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a h

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.
○ 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
Includes only IPv4 addresses.
○ Dualstack
Includes IPv4 and IPv6 addresses.

Load balancer should be in public subnet and it should be directly connected with internet gateway.



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. T the load balancer is created. To confirm the VPC for your targets, view your target groups.

vpc-prod-example-vpc
vpc-00e4a59f74c25e40f
IPv4 VPC CIDR: 10.0.0.0/16

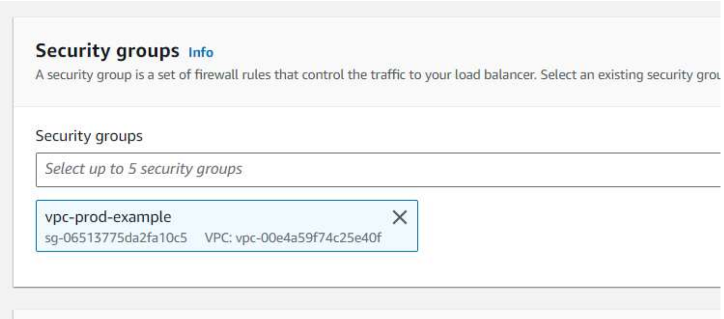
Choose VPC which you have just created

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 Z balancer or the VPC are not available for selection.

☑ eu-north-1a (eun1-az1)
Subnet
subnet-0cb98e963103fdc54 | vpc-prod-example-subnet-public1-eu-north-1a ▼
IPv4 address
Assigned by AWS

Select both availability zone with public subnet only.

☑ eu-north-1b (eun1-az2)
Subnet
subnet-08a96c9143a473511 | vpc-prod-example-subnet-public2-eu-north-1b ▼
IPv4 address
Assigned by AWS



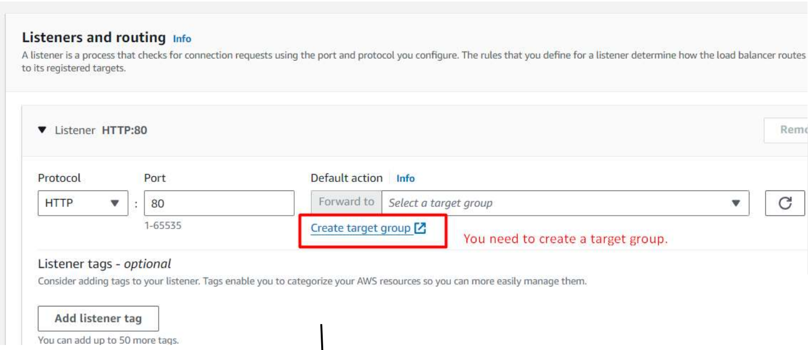
Security groups Info
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security grou

Security groups
Select up to 5 security groups

vpc-prod-example ✕
sg-06513775da2fa10c5 VPC: vpc-00e4a59f74c25e40f

You can select any security group or create new security group as well.

What you ae trying to do in security group is for the load balancer are you allowing all the traffic or not.



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 to its registered targets.

▼ Listener **HTTP:80**

Protocol	Port	Default action
HTTP ▼	80 (1-65535)	Forward to: Select a target group ▼

Create target group

You need to create a target group.

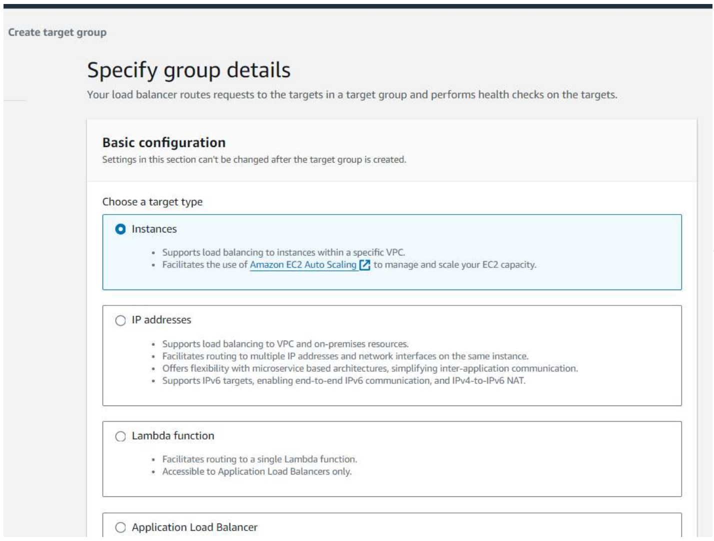
Listener tags - *optional*

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.

Here you can define which instance is accessible



Create target group

Specify group details

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

Basic configuration

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

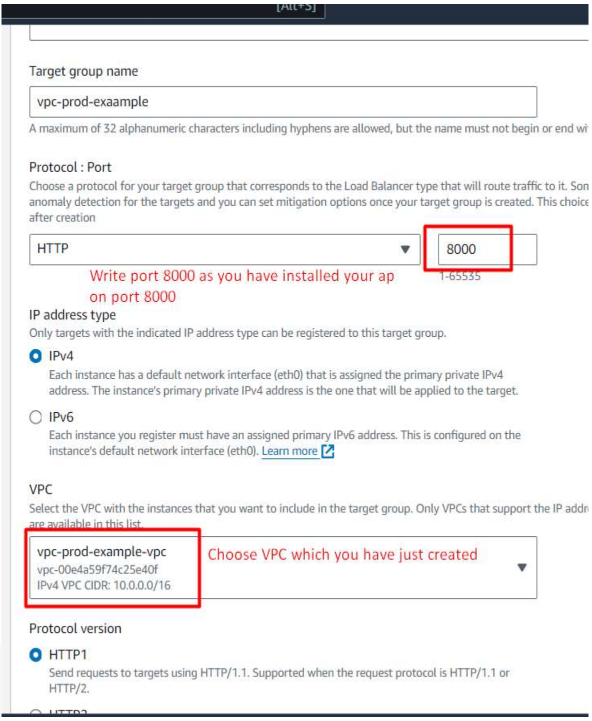
Choose a target type

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

○ 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



Target group name

vpc-prod-exaample

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end wi

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Son anomaly detection for the targets and you can set mitigation options once your target group is created. This choice after creation

HTTP ▼ : 8000 (1-65535)

Write port 8000 as you have installed your ap on port 8000

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 addr are available in this list.

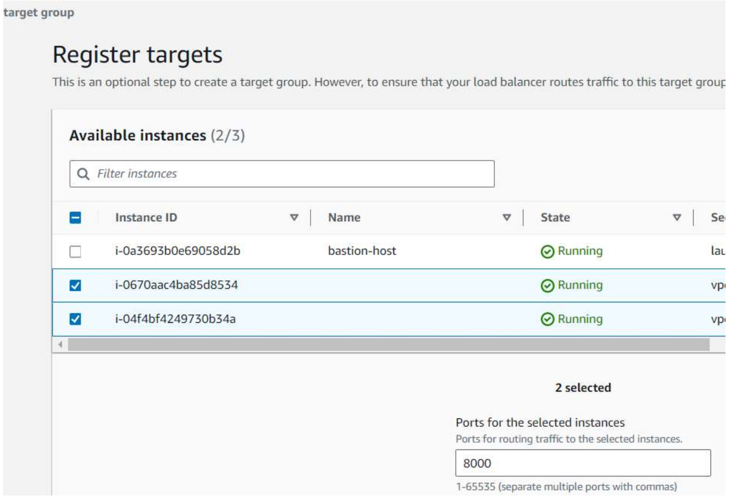
vpc-prod-example-vpc
vpc-00e4a59f74c25e40f
IPv4 VPC CIDR: 10.0.0.0/16

Choose VPC which you have just created

Protocol version

● HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

Then click on next.



target group

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

Available instances (2/3)

Filter instances

	Instance ID	Name	State	Se
□	i-0a3693b0e69058d2b	bastion-host	✓ Running	lau
☑	i-0670aac4ba85d8534		✓ Running	vp
☑	i-04f4bf4249730b34a		✓ Running	vp

2 selected

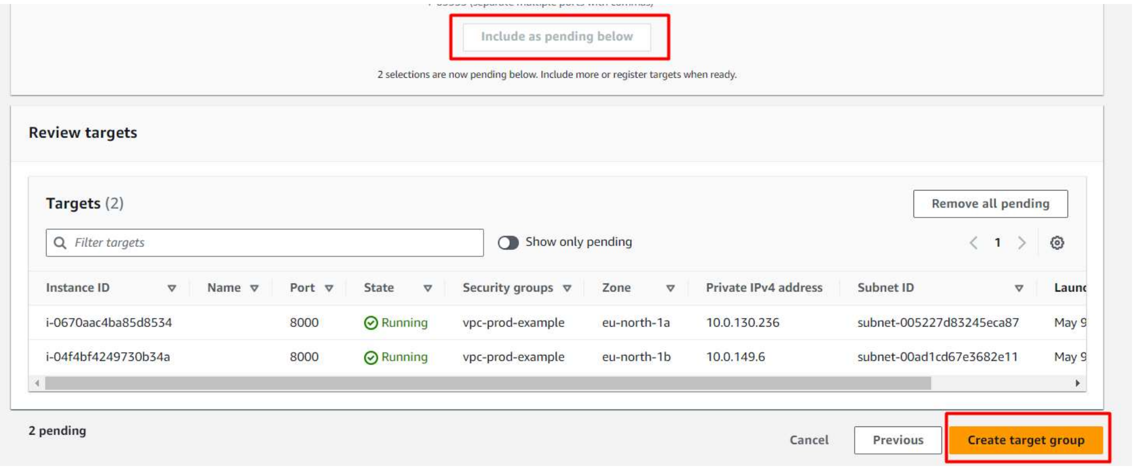
Ports for the selected instances

Ports for routing traffic to the selected instances.

8000

1-65535 (separate multiple ports with commas)

Here one instance has the application and other instance does not have the application. Later you can install the application to the other instance and see how is the traffic flowing.



Include as pending below

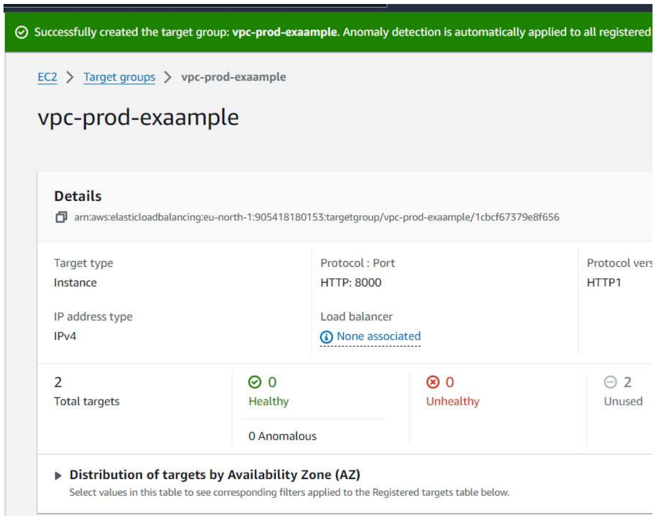
2 selections are now pending below. Include more or register targets when ready.

Review targets

Targets (2)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launc
i-0670aac4ba85d8534		8000	✓ Running	vpc-prod-example	eu-north-1a	10.0.130.236	subnet-005227d83245eca87	May 9
i-04f4bf4249730b34a		8000	✓ Running	vpc-prod-example	eu-north-1b	10.0.149.6	subnet-00ad1cd67e3682e11	May 9

2 pending



Successfully created the target group: **vpc-prod-exaample**. Anomaly detection is automatically applied to all registered

EC2 > Target groups > vpc-prod-exaample

vpc-prod-exaample

Details

arn:aws:elasticloadbalancing:eu-north-1:905418180153:targetgroup/vpc-prod-exaample/1cbcf67379e8f656

Target type: Instance

Protocol : Port: HTTP: 8000

Protocol vers: HTTP1

IP address type: IPv4

Load balancer: None associated

2 Total targets

0 Healthy

0 Anomalous

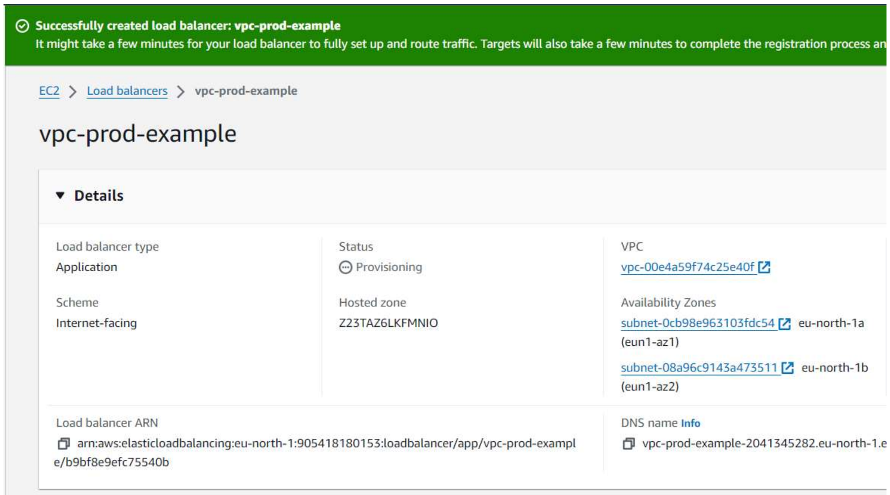
0 Unhealthy

2 Unused

Distribution of targets by Availability Zone (AZ)

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

Now you need to attach this target group to load balancer and you can launch load balancer.



Successfully created load balancer: vpc-prod-example

It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process an

EC2 > Load balancers > vpc-prod-example

vpc-prod-example

Details

Load balancer type: Application

Status: Provisioning

VPC: vpc-00e4a59f74c25e40f

Scheme: Internet-facing

Hosted zone: Z23TAZ6LKFMNIO

Availability Zones: subnet-0cb98e963103fdc54 eu-north-1a (eun1-az1)
subnet-08a96c9143a473511 eu-north-1b (eun1-az2)

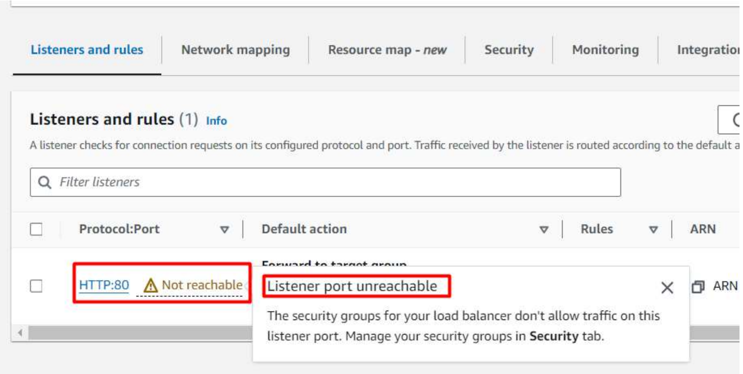
Load balancer ARN: arn:aws:elasticloadbalancing:eu-north-1:905418180153:loadbalancer/app/vpc-prod-example/b9bf8e9efc75540b

DNS name Info: vpc-prod-example-2041345282.eu-north-1.e

Once Load balancer is provisioned let’s try to access it from outside.

The expectation is when you access the application the load balancer should give you response for application.

Now try to access load balancer. You will see that the load balancer is not accessible because the subnet you have attached to the load balancer does not expose port 80.



Listeners and rules (1) Info

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

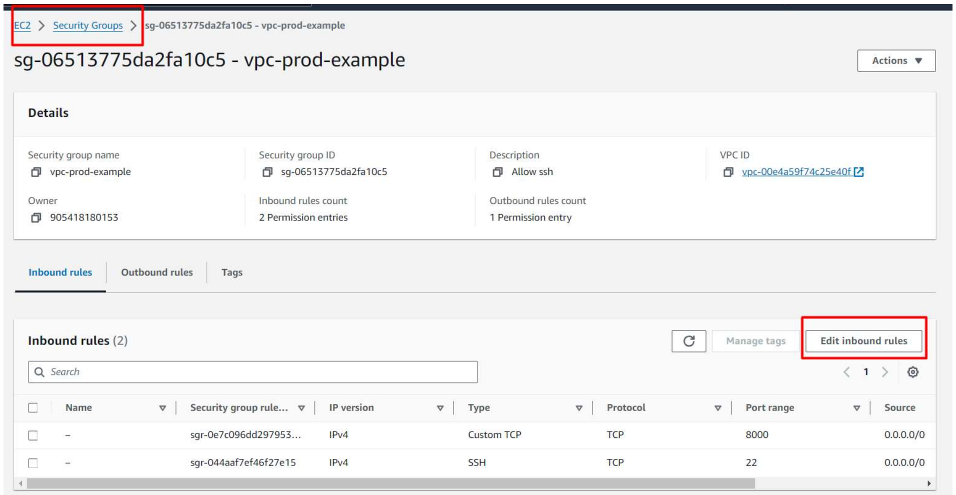
Filter listeners

□	Protocol:Port	Default action	Rules	ARN
□	HTTP:80 ⚠ Not reachable	Forward to target group		ARN

Listener port unreachable

The security groups for your load balancer don't allow traffic on this listener port. Manage your security groups in **Security** tab.

What you need to do now is go to security group and allow HTTP traffic on it.



EC2 > Security Groups > sg-06513775da2fa10c5 - vpc-prod-example
Actions ▼

sg-06513775da2fa10c5 - vpc-prod-example

Details

Security group name: vpc-prod-example

Security group ID: sg-06513775da2fa10c5

Description: Allow ssh

VPC ID: vpc-00e4a59f74c25e40f

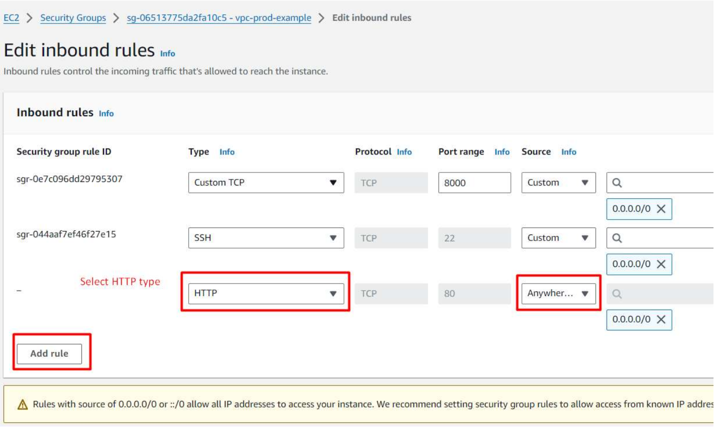
Owner: 905418180153

Inbound rules count: 2 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules (2)

□	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
□	–	sgr-0e7c096dd297953...	IPv4	Custom TCP	TCP	8000	0.0.0.0/0
□	–	sgr-044aaf7ef46f27e15	IPv4	SSH	TCP	22	0.0.0.0/0



EC2 > Security Groups > sg-06513775da2fa10c5 - vpc-prod-example > Edit inbound rules
Add rule

Edit inbound rules Info

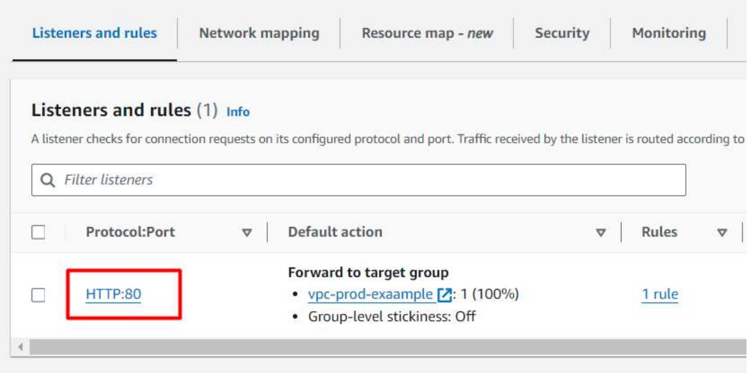
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	
sgr-0e7c096dd29795307	Custom TCP	TCP	8000	Custom	0.0.0.0/0
sgr-044aaf7ef46f27e15	SSH	TCP	22	Custom	0.0.0.0/0
–	HTTP	TCP	80	Anywher...	0.0.0.0/0

Select HTTP type

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addres



Listeners and rules (1) Info

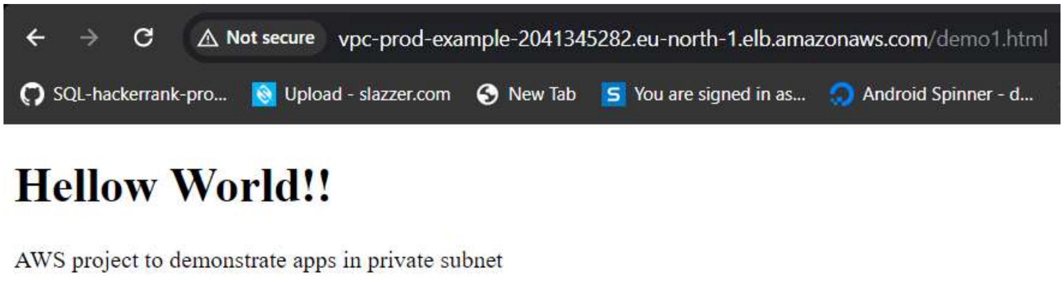
A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to

Filter listeners

□	Protocol:Port	Default action	Rules
□	HTTP:80	Forward to target group • vpc-prod-exaample : 1 (100%) • Group-level stickiness: Off	1 rule

Now you can see error is gone.

Now you can see you are able to access your deployed application.



Hellow World!!

AWS project to demonstrate apps in private subnet

As you can see, we have successfully deployed an application into private subnet and you can access it from outside as well.

So, now you can try to install an application into other instance and can see how is the traffic flow is going.