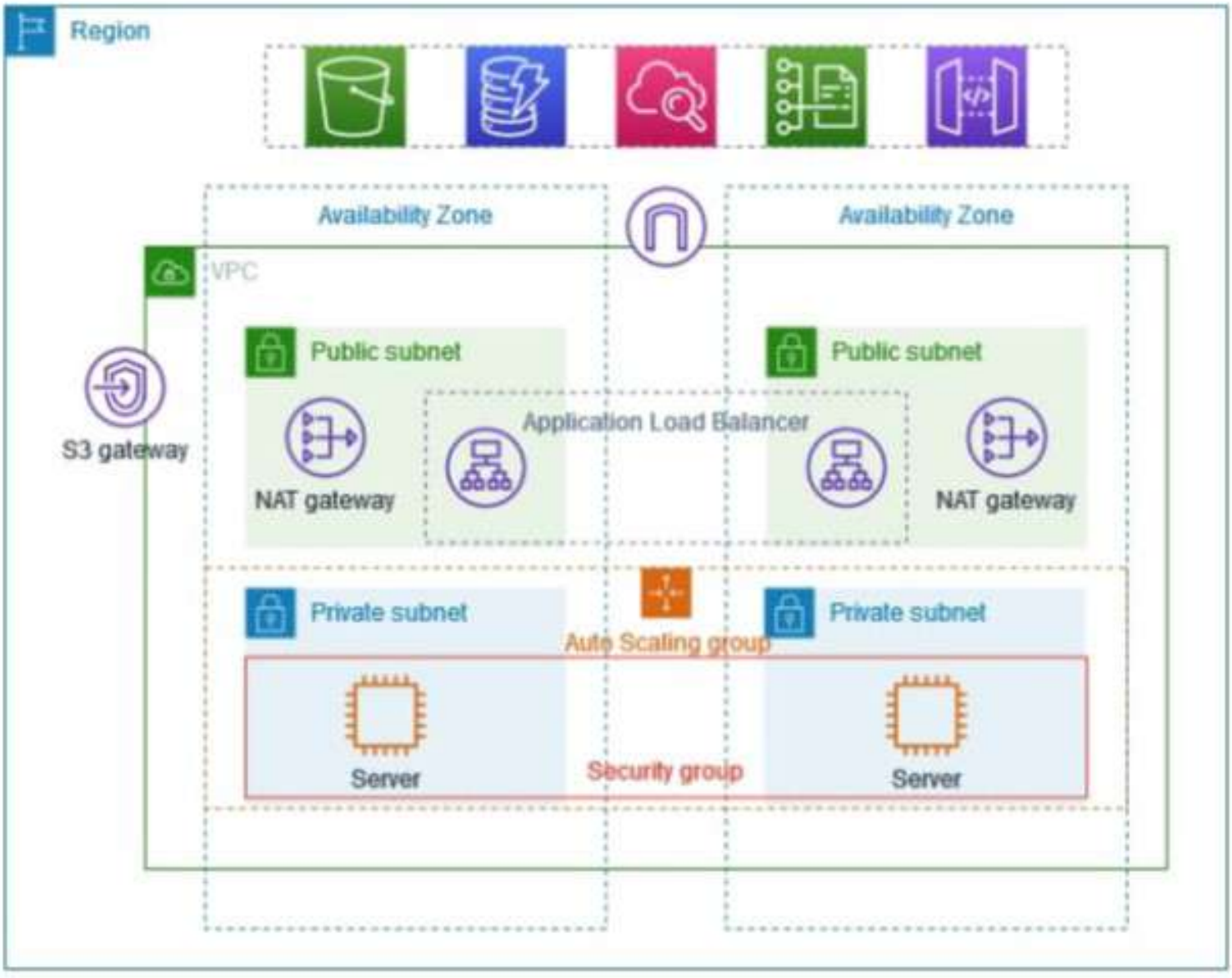
mazon S3 by using a gateway VPC

A VPC with subnets in two Availability Zones.



Close

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, suc

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

aws-prod-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

Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1	**2**	3

▶ **Customize AZs**

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**

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.

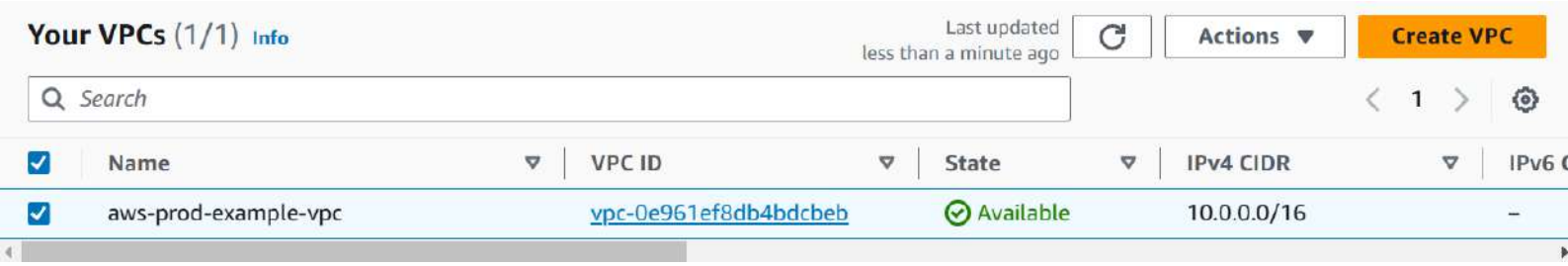
None	S3 Gateway

DNS options Info

- [x] Enable DNS hostnames
- [x] Enable DNS resolution

▶ **Additional tags**

Cancel **Create VPC**


Your VPCs (1/1) Info
Last updated
less than a minute ago
Actions
Create VPC
Search
1
Name
VPC ID
State
IPv4 CIDR
IPv6
aws-prod-example-vpc
vpc-0e961ef8db4bdcbeb
Available
10.0.0.0/16
–

Compute

EC2 launch templates

Streamline, simplify and standardize instance launches

Use launch templates to automate instance launches, simplify permission policies, and enforce best practices across your organization. Save launch parameters in a template that can be used for on-demand launches and with managed services, including EC2 Auto Scaling and EC2 Fleet. Easily update your launch parameters by creating a new launch template version.

New launch template

Create launch template

Create launch template

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

Launch template name and description

Launch template name - *required*

aws-prod-example

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

proof of concept of aws private subnet

Max 255 chars

Auto Scaling guidance | Info

Select this if you intend to use this template with EC2 Auto Scaling

- [x] Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

Application and OS Images (Amazon Machine Image) - required 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

Recently launched

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

al2023-ami-2023.5.20240819.0-kernel-6.1-x86_64
ami-02b49a24cfb95941c
2024-08-15T17:38:24.000Z Architecture: 64-bit (x86) Virtualization: hvm ENA enabled: true
Root device type: ebs Boot mode: uefi-preferred

○ Select existing security group

● Create security group

Security group name - *required*

aws-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 access

VPC | Info

vpc-0e961ef8db4bdcbeb (aws-prod-example-vpc)
10.0.0.0/16

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	Add CIDR, prefix list or secur	e.g. SSH for admin desktop

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

Source type Info	Source Info	Description - *optional* Info
Anywhere ▼	Add CIDR, prefix list or secur	e.g. SSH for admin desktop
	0.0.0.0/0 ✕	

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

Type Info	Protocol Info	Port range Info
Custom TCP ▼	TCP	8000

Source type Info	Source Info	Description - *optional* Info
Anywhere ▼	Add CIDR, prefix list or secur	e.g. SSH for admin desktop

Creating template
Creating security groups

25%

Details

Amazon EC2 Auto Scaling
helps maintain the availability of your applications

Auto Scaling groups are collections of Amazon EC2 instances that enable automatic scaling and fleet management features. These features help you maintain the health and availability of your applications.

Create Auto Scaling group

Get started with EC2 Auto Scaling by creating an Auto Scaling group.

Create Auto Scaling group

Name

Auto Scaling group name

Enter a name to identify the group.

aws-prod-example

Must be unique to this account in the current Region and no more than 255 characters.

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.

aws-prod-example

Create a launch template

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-0e961ef8db4bdcbeb (aws-prod-example-vpc)
10.0.0.0/16

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

ap-south-1a | subnet-052ba93489ad649b4 (aws-prod-example-subnet-private1-ap-south-1a)
10.0.128.0/20

ap-south-1b | subnet-05402edb4c60e69eb (aws-prod-example-subnet-private2-ap-south-1b)
10.0.144.0/20

Create a subnet

Configure group size and scaling - *optional* Info

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

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

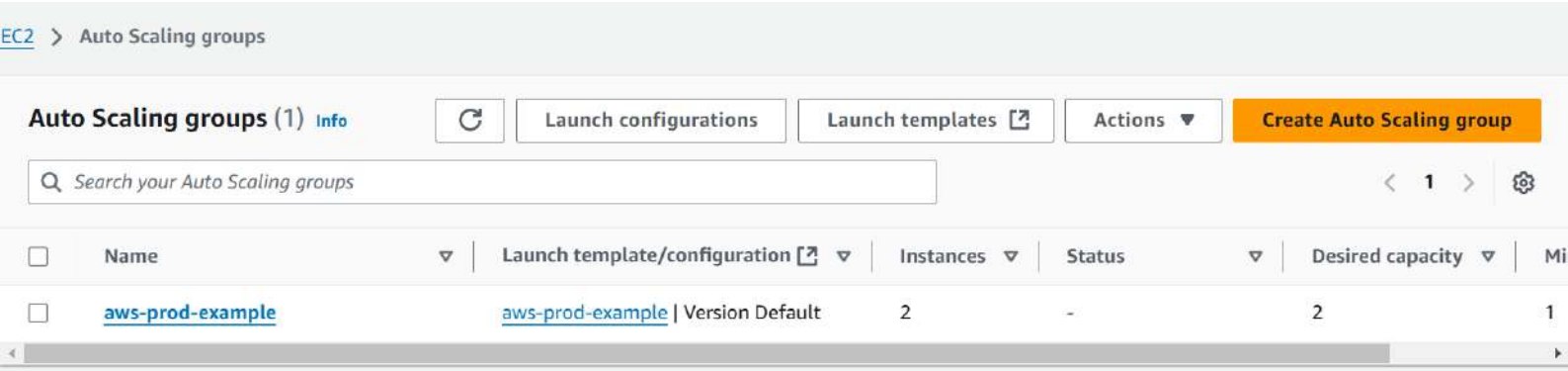
Equal or greater than desired capacity

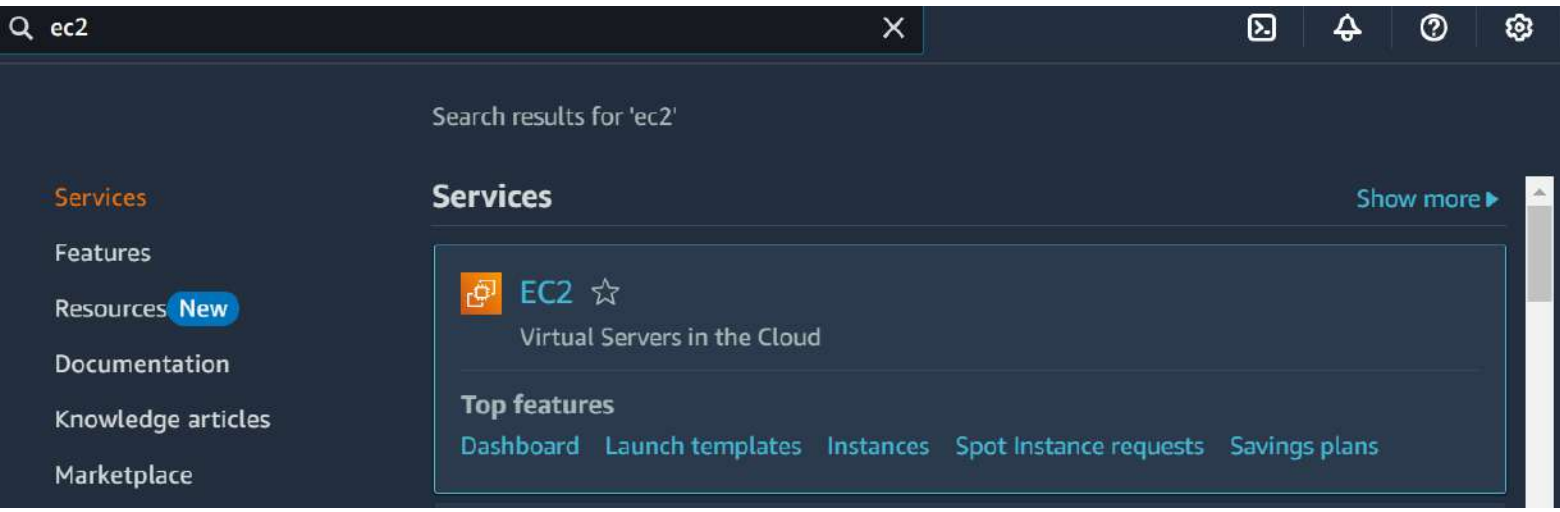
Automatic scaling - *optional*

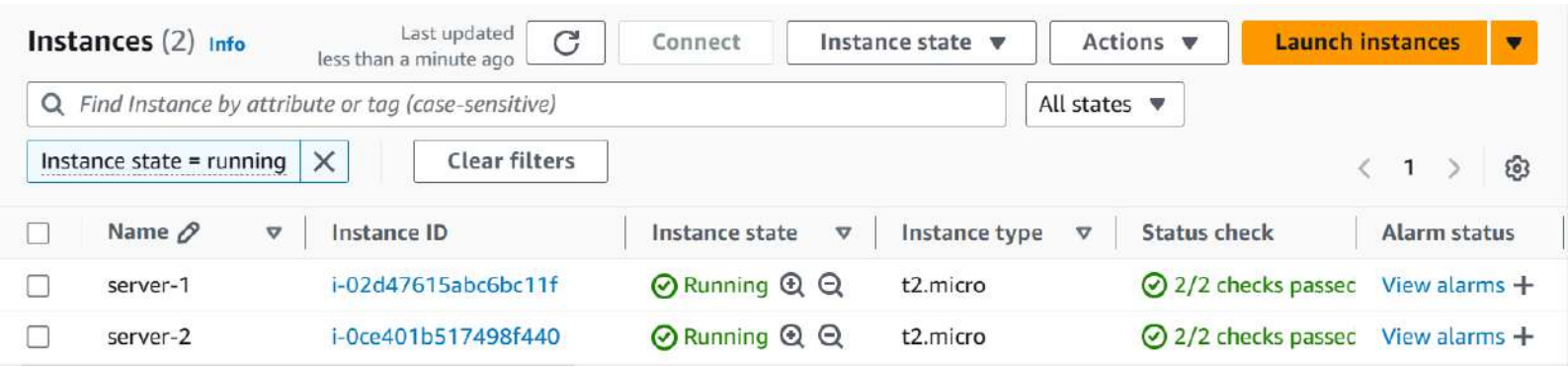
Choose whether to use a target tracking policy | Info

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

- (●) **No scaling policies**
  Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.
- ( ) **Target tracking scaling policy**
  Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.


EC2 > Auto Scaling groups
Auto Scaling groups (1) Info
Launch configurations
Launch templates
Actions
Create Auto Scaling group
Search your Auto Scaling groups
1
Name
Launch template/configuration
Instances
Status
Desired capacity
aws-prod-example
aws-prod-example | Version Default
2
-
2
1


ec2
Search results for 'ec2'
Services
Features
Resources New
Documentation
Knowledge articles
Marketplace
Services
Show more
EC2
Virtual Servers in the Cloud
Top features
Dashboard
Launch templates
Instances
Spot Instance requests
Savings plans


Instances (2) Info
Last updated
less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
server-1
i-02d47615abc6bc11f
Running
t2.micro
2/2 checks passec
View alarms
server-2
i-0ce401b517498f440
Running
t2.micro
2/2 checks passec
View alarms

EC2 > ... > Launch 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

bastion-host

Add additional tags

looking for below

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

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible

ami-0dee22c13ea7a9a67 (64-bit (x86)) / ami-0c8eea98010057bd0 (64-bit (Arm))

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

Instance type Info | Get advice

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Network settings Info

VPC - *required* Info

vpc-0e961ef8db4bdcbeb (aws-prod-example-vpc)
10.0.0.0/16

Subnet Info

subnet-06bbaa16c149f1c77
aws-prod-example-subnet-public1-ap-south-1a
VPC: vpc-0e961ef8db4bdcbeb Owner: 637423560649
Availability Zone: ap-south-1a Zone type: Availability Zone
IP addresses available: 4090 CIDR: 10.0.0.0/20)

Create new subnet

Auto-assign public IP Info

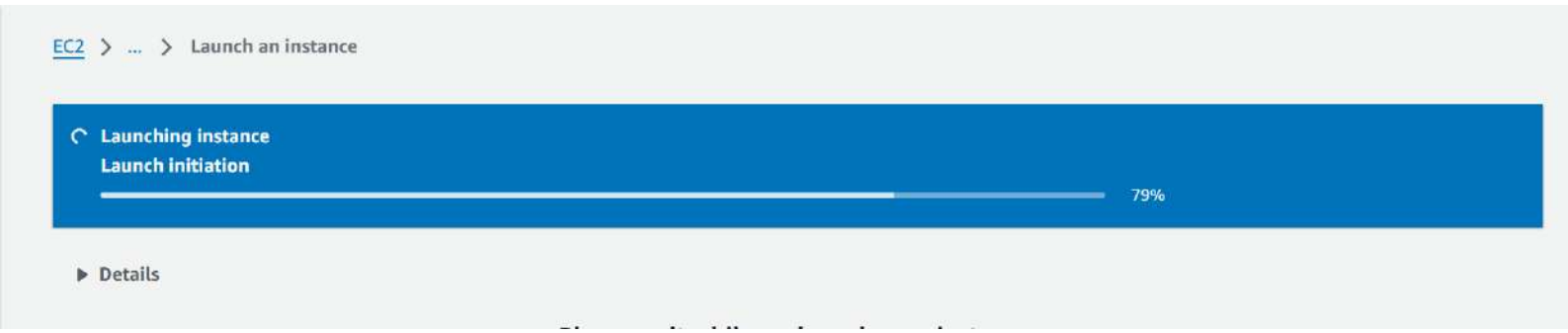
Enable

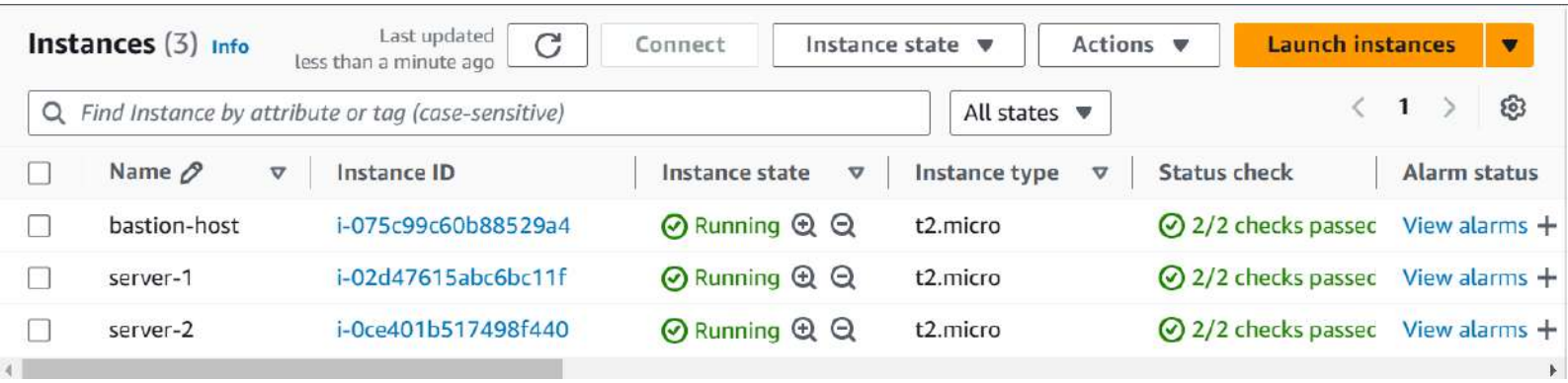
Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

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

- (•) Create security group
- ( ) Select existing security group


EC2 > ... > Launch an instance
Launching instance
Launch initiation
79%
Details


Instances (3) Info
Last updated
less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
bastion-host
i-075c99c60b88529a4
Running
t2.micro
2/2 checks passec
View alarms
server-1
i-02d47615abc6bc11f
Running
t2.micro
2/2 checks passec
View alarms
server-2
i-0ce401b517498f440
Running
t2.micro
2/2 checks passec
View alarms

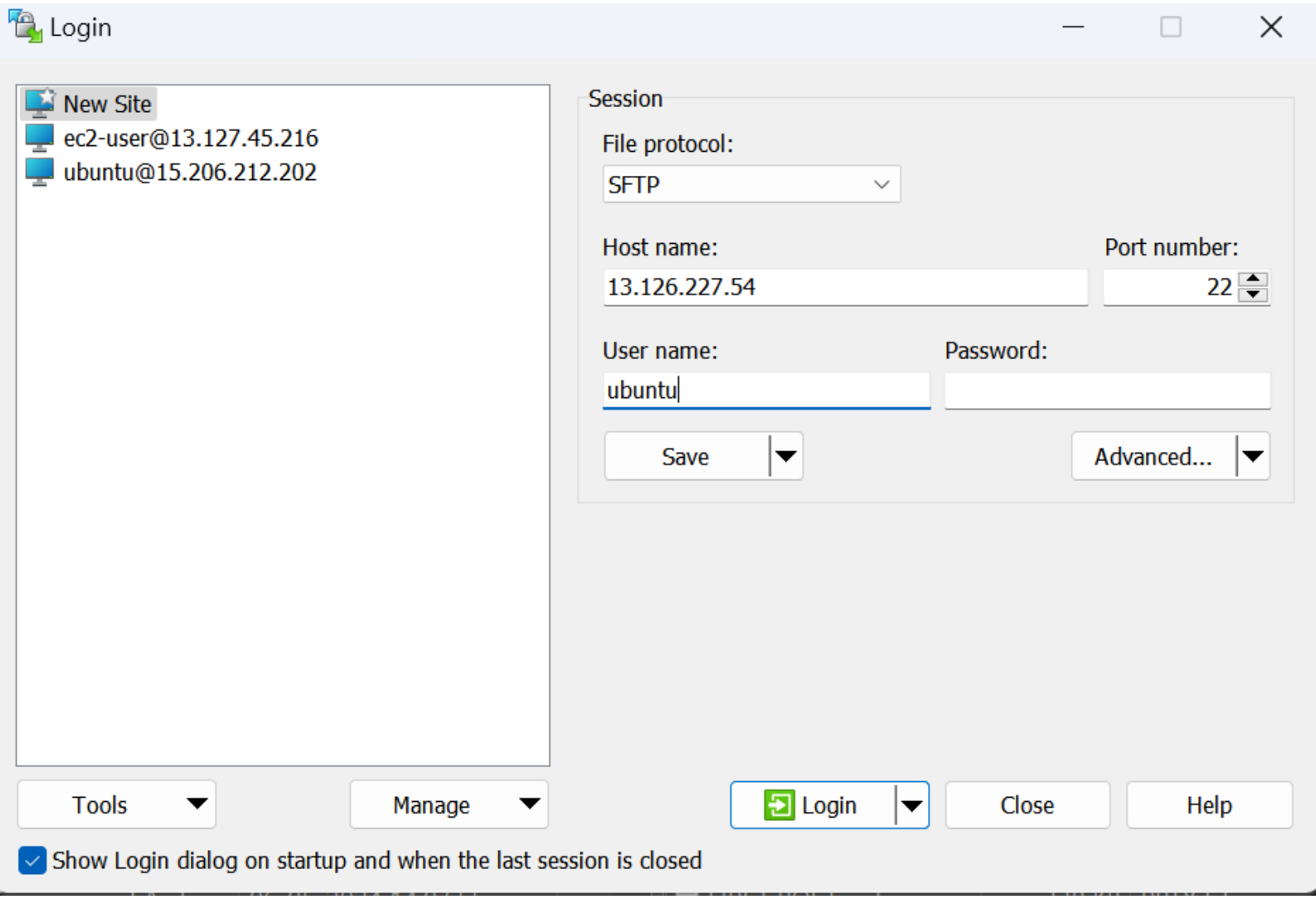
Instance summary for i-0f4df9ed5a61d62e8 (bastion-host) Info

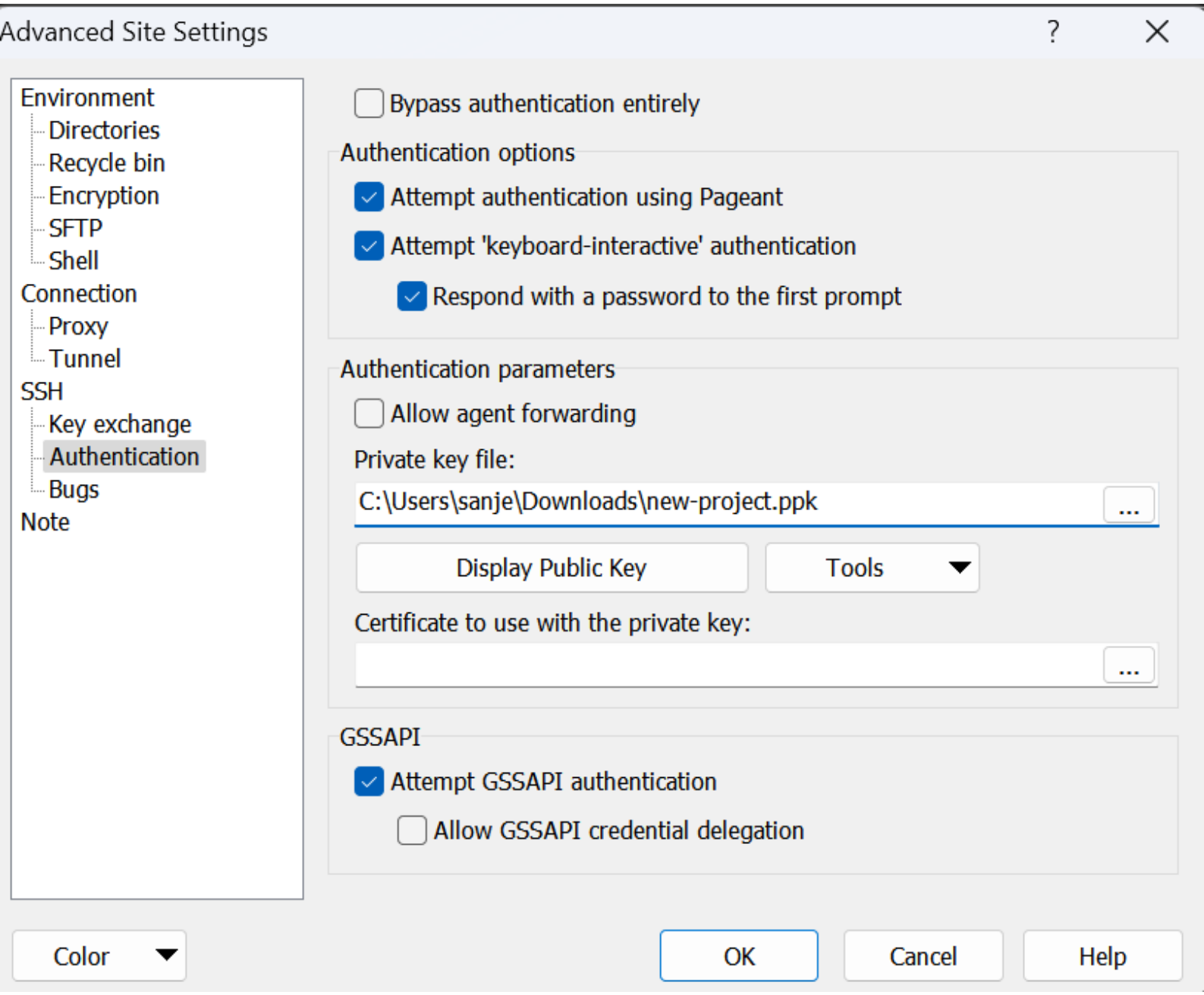
Connect | Instance state | Actions

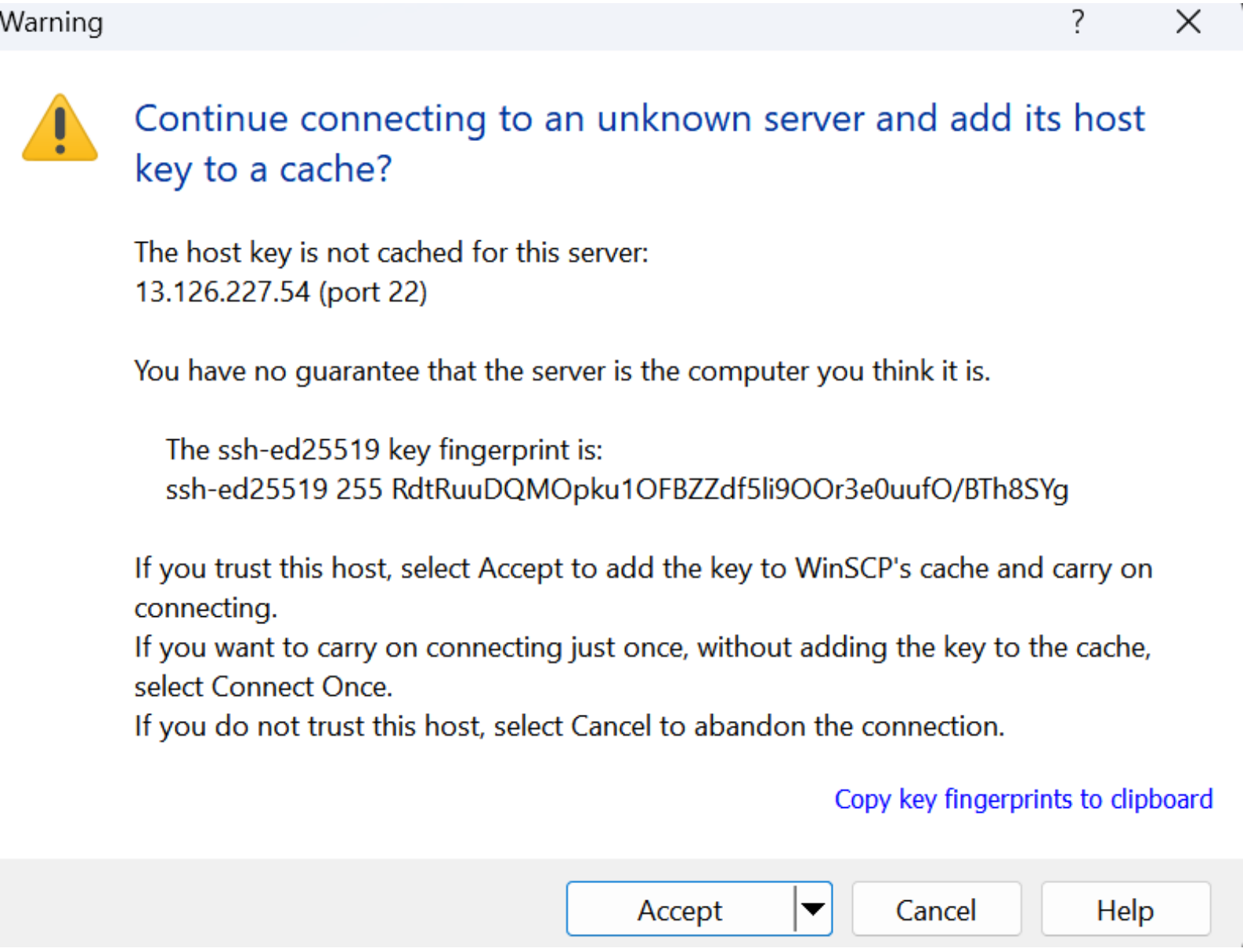
Updated less than a minute ago

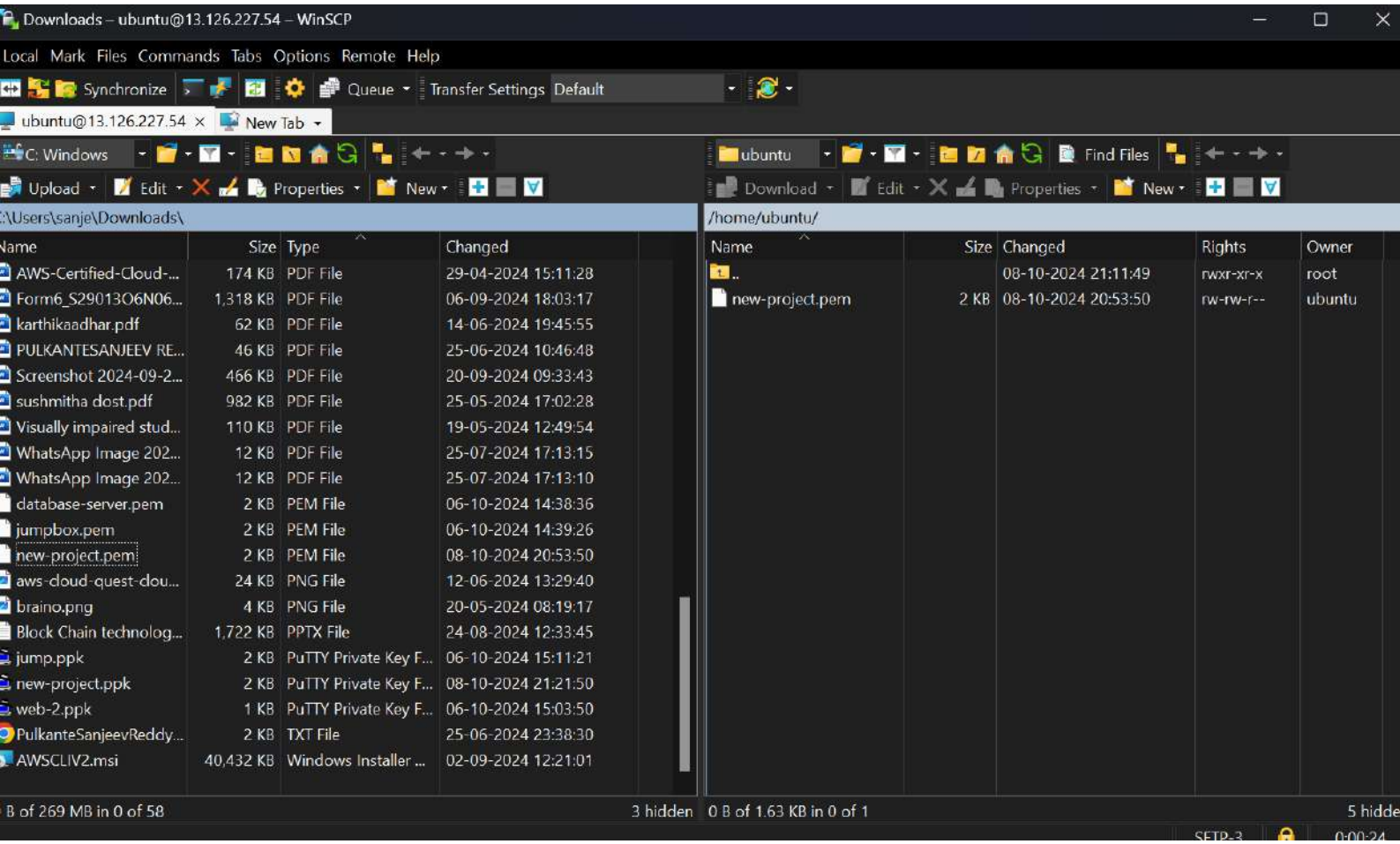
Public IPv4 address copied

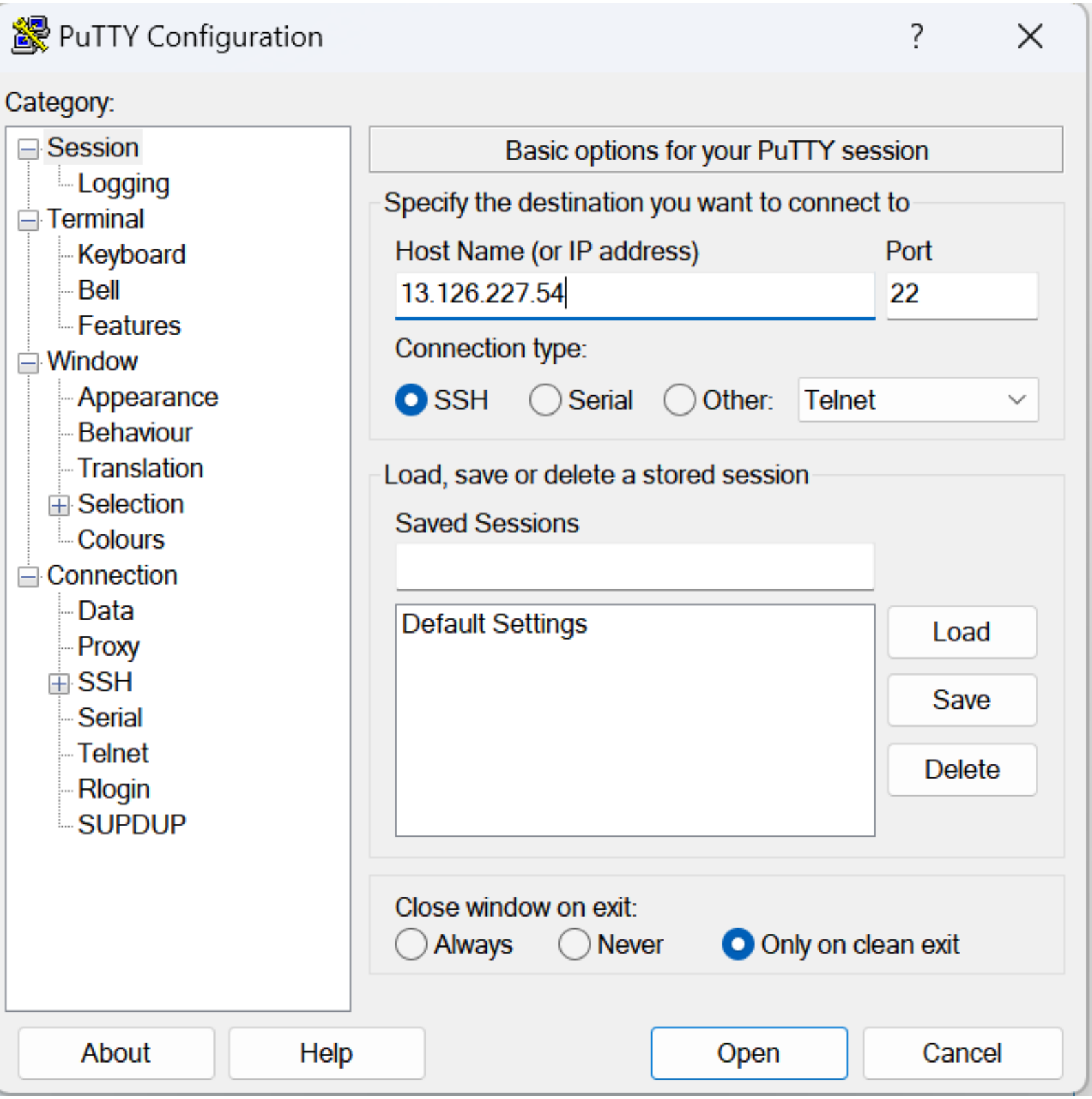
Instance ID	Public IPv4 address	Private IPv4 addresses
i-0f4df9ed5a61d62e8 (bastion-host)	13.126.227.54 | open address	10.0.3.157
IPv6 address	**Instance state**	**Public IPv4 DNS**
–	Running	ec2-13-126-227-54.ap-south-1.compute.amazonaws.com | open address

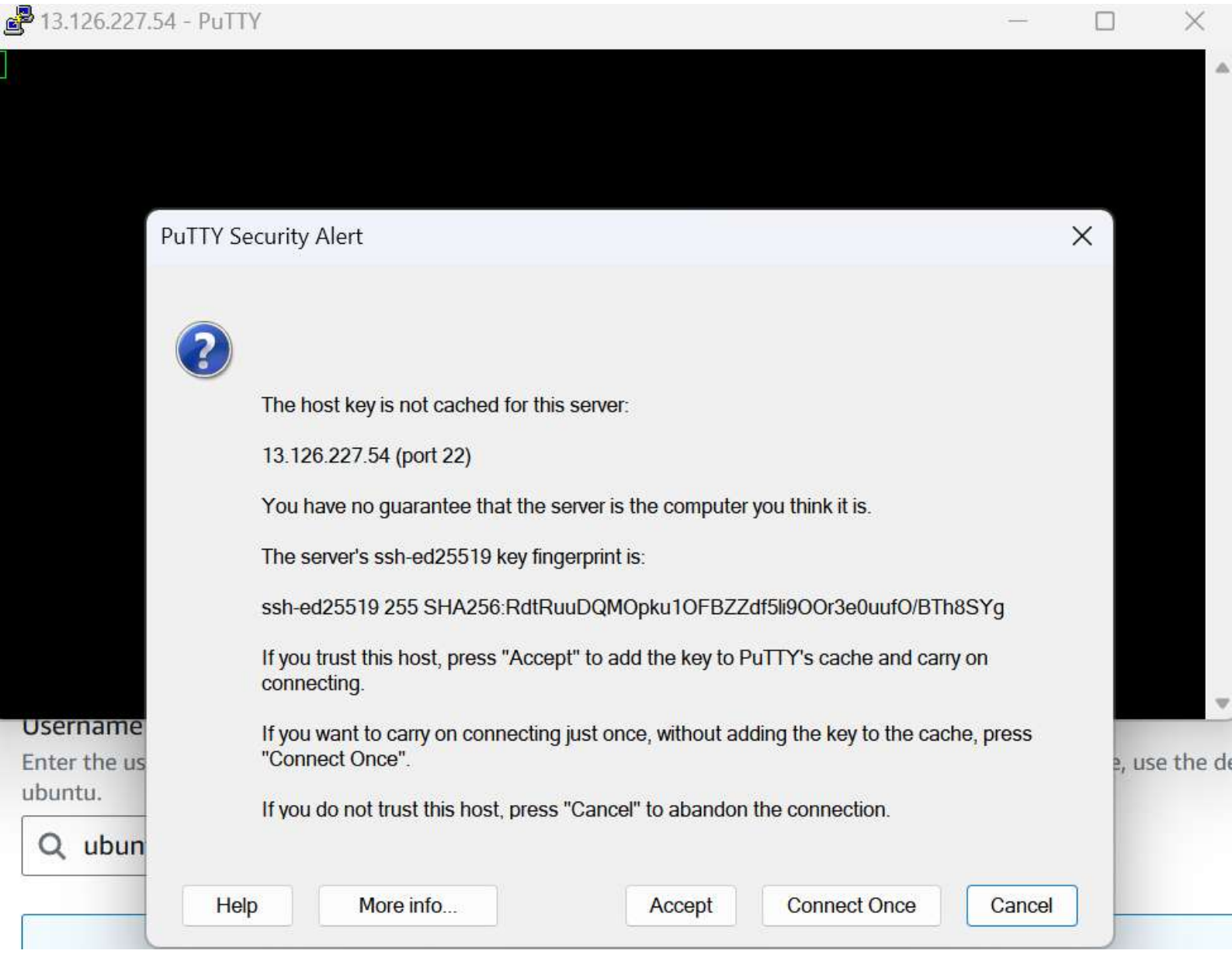

Login
New Site
ec2-user@13.127.45.216
ubuntu@15.206.212.202
Session
File protocol:
SFTP
Host name:
13.126.227.54
Port number:
22
User name:
ubuntu
Password:
Save
Advanced...
Tools
Manage
Login
Close
Help
Show Login dialog on startup and when the last session is closed

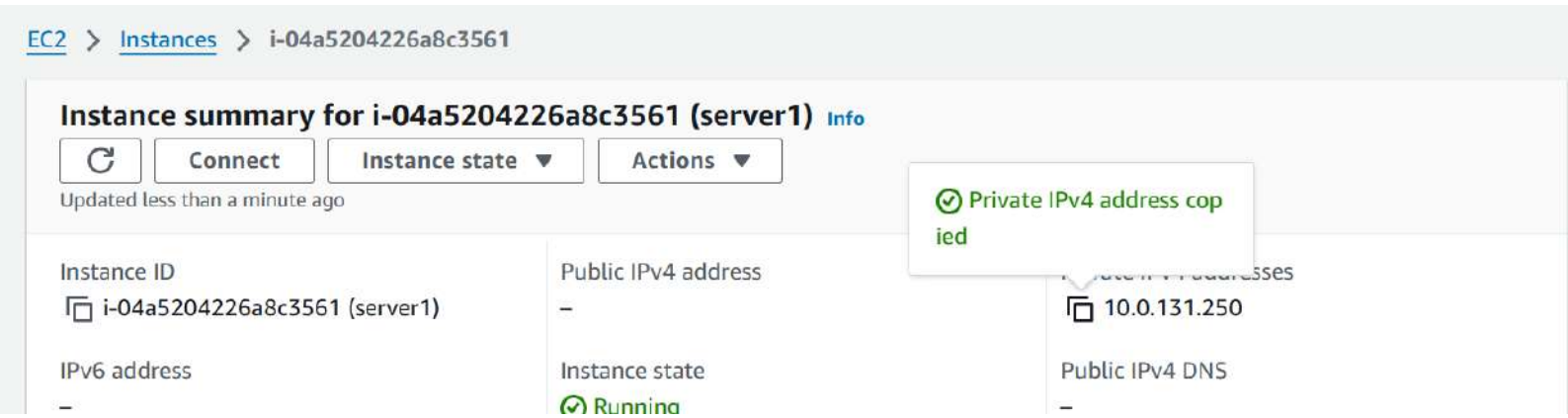

Advanced Site Settings
Environment
Directories
Recycle bin
Encryption
SFTP
Shell
Connection
Proxy
Tunnel
SSH
Key exchange
Authentication
Bugs
Note
Bypass authentication entirely
Authentication options
Attempt authentication using Pageant
Attempt 'keyboard-interactive' authentication
Respond with a password to the first prompt
Authentication parameters
Allow agent forwarding
Private key file:
C:\Users\sanje\Downloads\new-project.ppk
Display Public Key
Tools
Certificate to use with the private key:
GSSAPI
Attempt GSSAPI authentication
Allow GSSAPI credential delegation
Color
OK
Cancel
Help

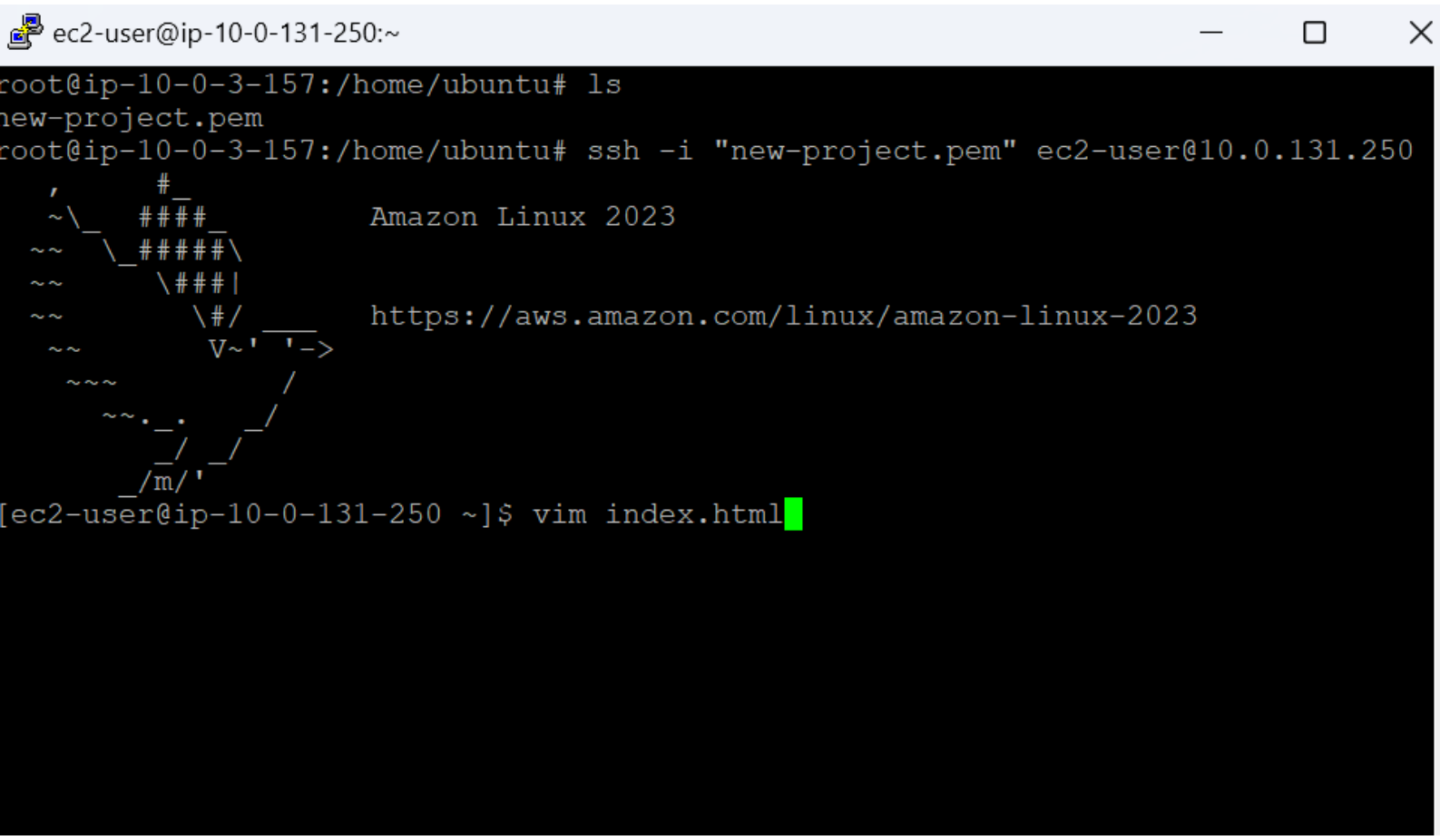

Warning
Continue connecting to an unknown server and add its host key to a cache?
The host key is not cached for this server:
13.126.227.54 (port 22)
You have no guarantee that the server is the computer you think it is.
The ssh-ed25519 key fingerprint is:
ssh-ed25519 255 RdtRuuDQMOpku1OFBZZdf5li9OOr3e0uufO/BTh8SYg
If you trust this host, select Accept to add the key to WinSCP's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, select Connect Once.
If you do not trust this host, select Cancel to abandon the connection.
Copy key fingerprints to clipboard
Accept
Cancel
Help


Downloads – ubuntu@13.126.227.54 – WinSCP
Local Mark Files Commands Tabs Options Remote Help
Synchronize Queue Transfer Settings Default
ubuntu@13.126.227.54 New Tab
C: Windows
Upload Edit Properties New
C:\Users\sanje\Downloads\
Name Size Type Changed
AWS-Certified-Cloud-... 174 KB PDF File 29-04-2024 15:11:28
Form6_S29013O6N06... 1,318 KB PDF File 06-09-2024 18:03:17
karthikaadhar.pdf 62 KB PDF File 14-06-2024 19:45:55
PULKANTESANJEEV RE... 46 KB PDF File 25-06-2024 10:46:48
Screenshot 2024-09-2... 466 KB PDF File 20-09-2024 09:33:43
sushmitha dost.pdf 982 KB PDF File 25-05-2024 17:02:28
Visually impaired stud... 110 KB PDF File 19-05-2024 12:49:54
WhatsApp Image 202... 12 KB PDF File 25-07-2024 17:13:15
WhatsApp Image 202... 12 KB PDF File 25-07-2024 17:13:10
database-server.pem 2 KB PEM File 06-10-2024 14:38:36
jumpbox.pem 2 KB PEM File 06-10-2024 14:39:26
new-project.pem 2 KB PEM File 08-10-2024 20:53:50
aws-cloud-quest-clou... 24 KB PNG File 12-06-2024 13:29:40
braino.png 4 KB PNG File 20-05-2024 08:19:17
Block Chain technolog... 1,722 KB PPTX File 24-08-2024 12:33:45
jump.ppk 2 KB PuTTY Private Key F... 06-10-2024 15:11:21
new-project.ppk 2 KB PuTTY Private Key F... 08-10-2024 21:21:50
web-2.ppk 1 KB PuTTY Private Key F... 06-10-2024 15:03:50
PulkanteSanjeevReddy... 2 KB TXT File 25-06-2024 23:38:30
AWSCLIV2.msi 40,432 KB Windows Installer ... 02-09-2024 12:21:01
B of 269 MB in 0 of 58
3 hidden
ubuntu Find Files
Download Edit Properties New
/home/ubuntu/
Name Size Changed Rights Owner
.. 08-10-2024 21:11:49 rwxr-xr-x root
new-project.pem 2 KB 08-10-2024 20:53:50 rw-rw-r-- ubuntu
0 B of 1.63 KB in 0 of 1
5 hidde


PuTTY Configuration
?
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
13.126.227.54
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel


13.126.227.54 - PuTTY
PuTTY Security Alert
The host key is not cached for this server:
13.126.227.54 (port 22)
You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:RdtRuuDQMOpku1OFBZZdf5li9OOr3e0uufO/BTh8SYg
If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".
If you do not trust this host, press "Cancel" to abandon the connection.
Help
More info...
Accept
Connect Once
Cancel

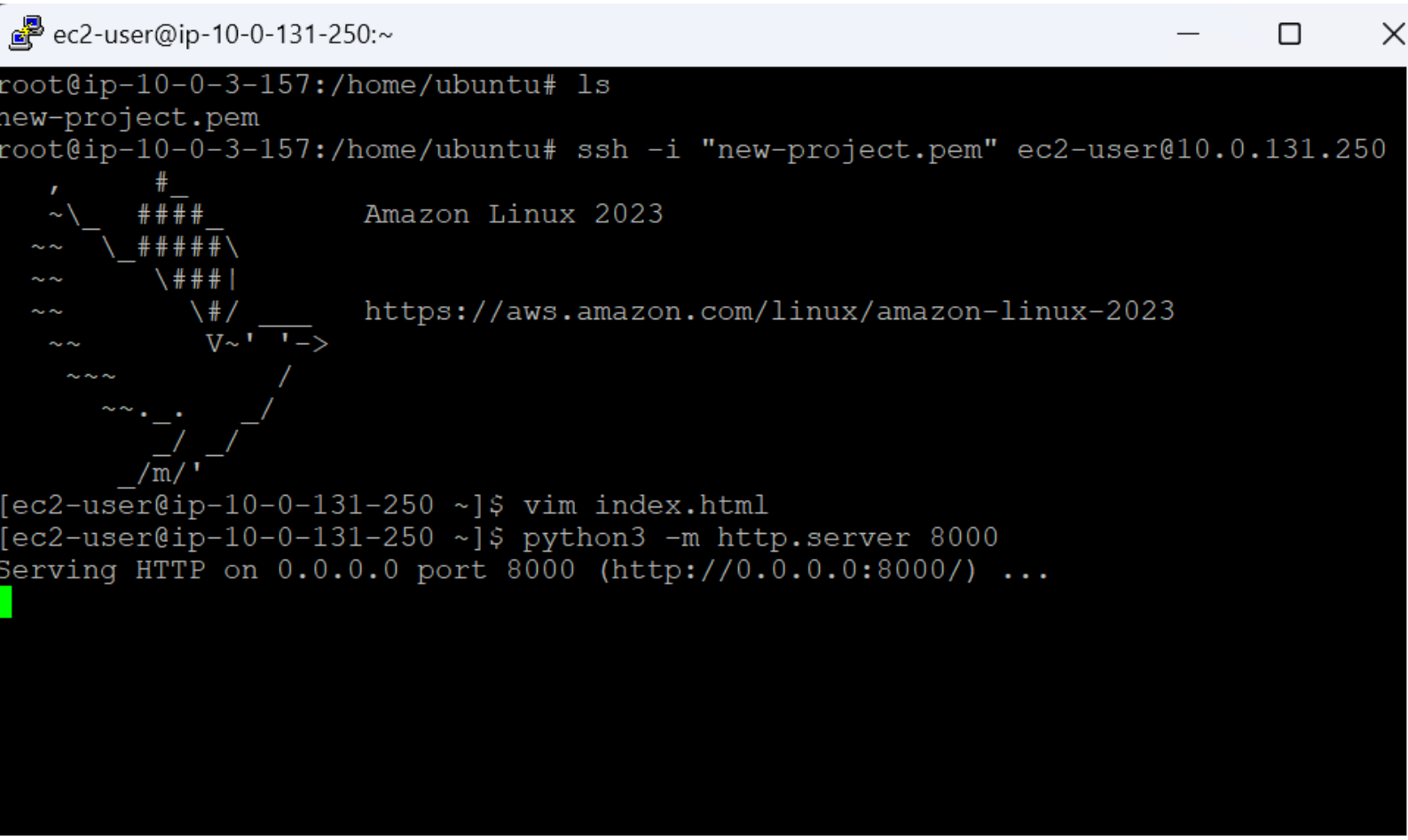

EC2 > Instances > i-04a5204226a8c3561
Instance summary for i-04a5204226a8c3561 (server1) Info
Connect
Instance state
Actions
Updated less than a minute ago
Private IPv4 address cop
ied
Instance ID
i-04a5204226a8c3561 (server1)
Public IPv4 address
–
10.0.131.250
IPv6 address
–
Instance state
Running
Public IPv4 DNS
–


ec2-user@ip-10-0-131-250:~
root@ip-10-0-3-157:/home/ubuntu# ls
new-project.pem
root@ip-10-0-3-157:/home/ubuntu# ssh -i "new-project.pem" ec2-user@10.0.131.250
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-131-250 ~]$ vim index.html

```
<!DOCTYPE html>
<html>
<body>

<h1>my first aws project demonastrate apps in private subnet</h1>
<p>thank you abhishek.veeramalla sir.</p>

</body>
</html>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                                    6,37          All
```

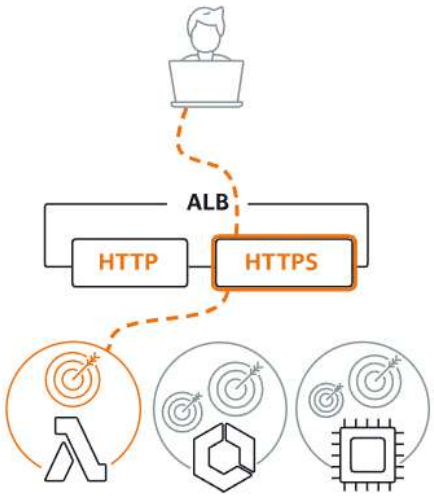

ec2-user@ip-10-0-131-250:~
root@ip-10-0-3-157:/home/ubuntu# ls
new-project.pem
root@ip-10-0-3-157:/home/ubuntu# ssh -i "new-project.pem" ec2-user@10.0.131.250
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-131-250 ~]$ vim index.html
[ec2-user@ip-10-0-131-250 ~]$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

Compare and select load balancer type

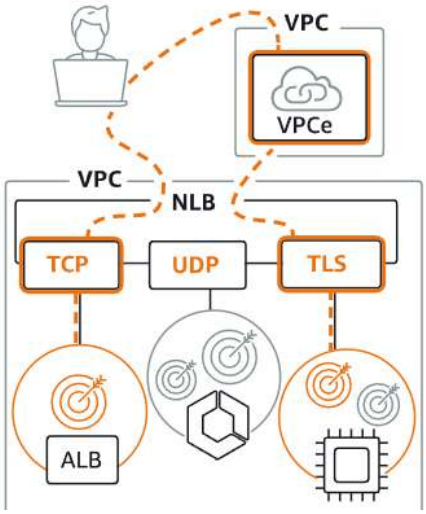
A complete feature-by-feature comparison along with detailed highlights is also available. Learn more

Load balancer types

Application Load Balancer Info



Network Load Balancer Info



Gateway Load Balancer Info

Load balancer name

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

prod-example

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. 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.

VPC Info

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view target groups. For a new VPC, create a VPC.

aws-prod-example-vpc
vpc-0637186099594ec40
IPv4 VPC CIDR: 10.0.0.0/16

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.

Availability Zones

ap-south-1a (aps1-az1)

Subnet

subnet-08f08b223827cb92b aws-prod-example-subnet-public1-ap-south-1a
IPv4 subnet CIDR: 10.0.0.0/20

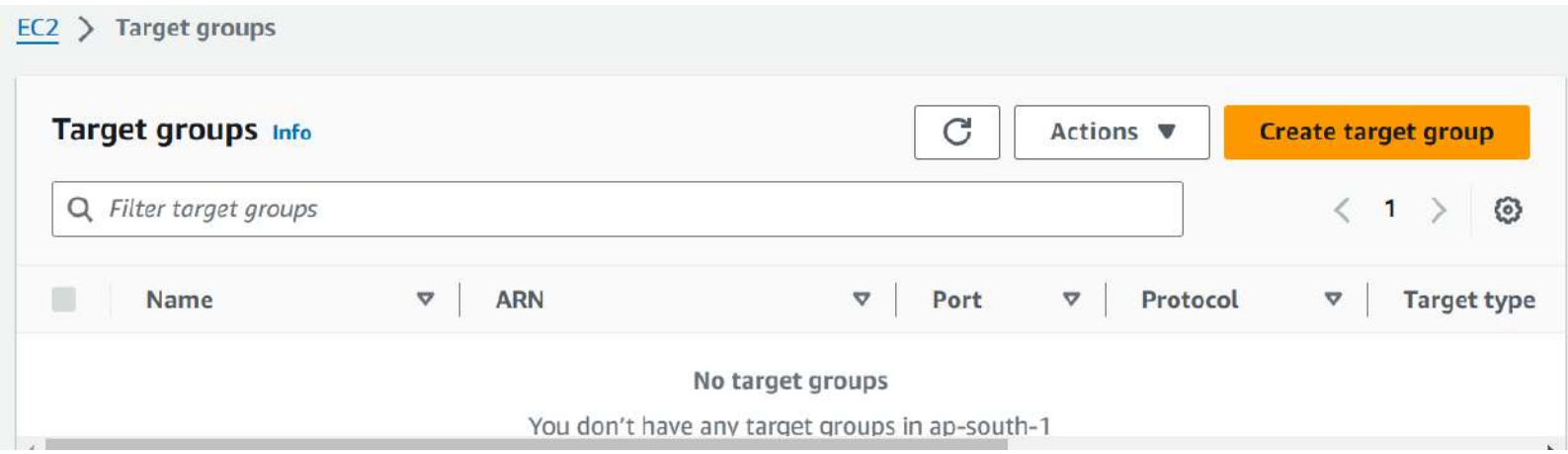
IPv4 address

Assigned by AWS

ap-south-1b (aps1-az3)

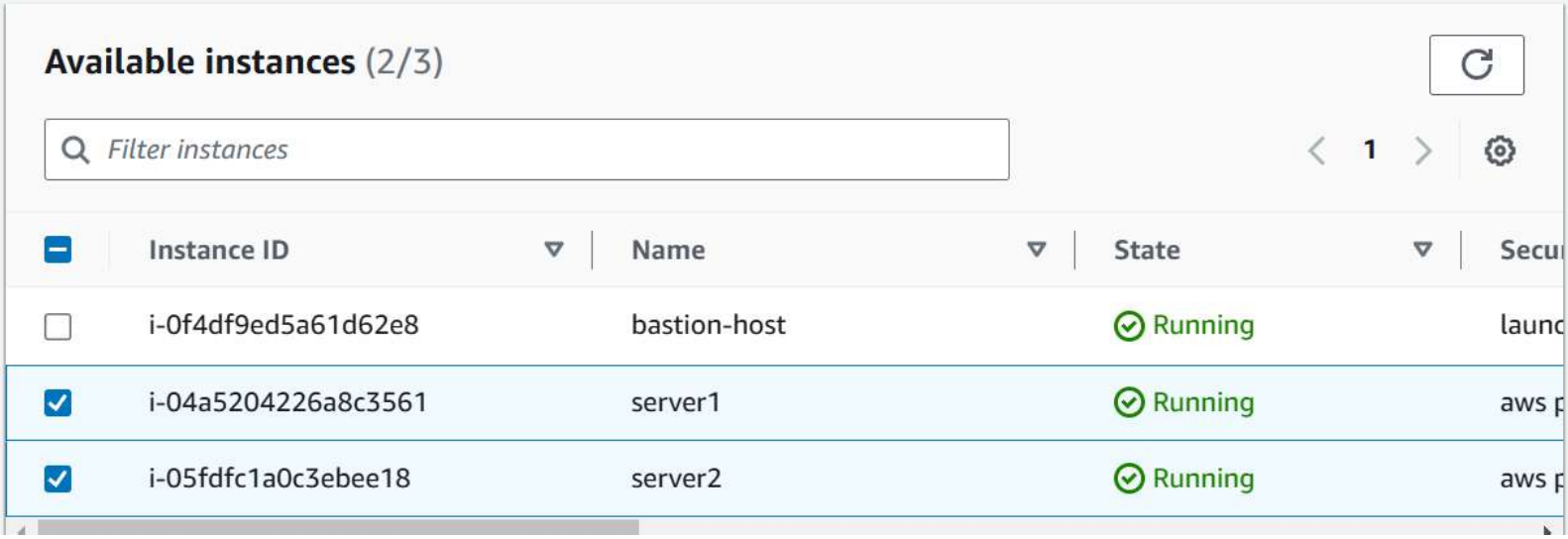
Subnet

subnet-035e7cdd0e0c84d71 aws-prod-example-subnet-public2-ap-south-1b
IPv4 subnet CIDR: 10.0.16.0/20


EC2
Target groups
Target groups Info
Actions
Create target group
Filter target groups
1
Name
ARN
Port
Protocol
Target type
No target groups
You don't have any target groups in ap-south-1

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.



Target group name

aws-prod-example

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

8000

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.

aws-prod-example-vpc
vpc-0637186099594ec40
IPv4 VPC CIDR: 10.0.0.0/16

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.

Ports for the selected instances

Ports for routing traffic to the selected instances.

8000

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

1

Instance ID	Name	Port	State	Security groups	Zone
i-04a5204226a8c3561	server1	8000	Running	aws prod example	ap-south-1a
i-05fdfc1a0c3ebee18	server2	8000	Running	aws prod example	ap-south-1b

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: aws-prod-example — Target type: Instance, IPv4 — HTTP

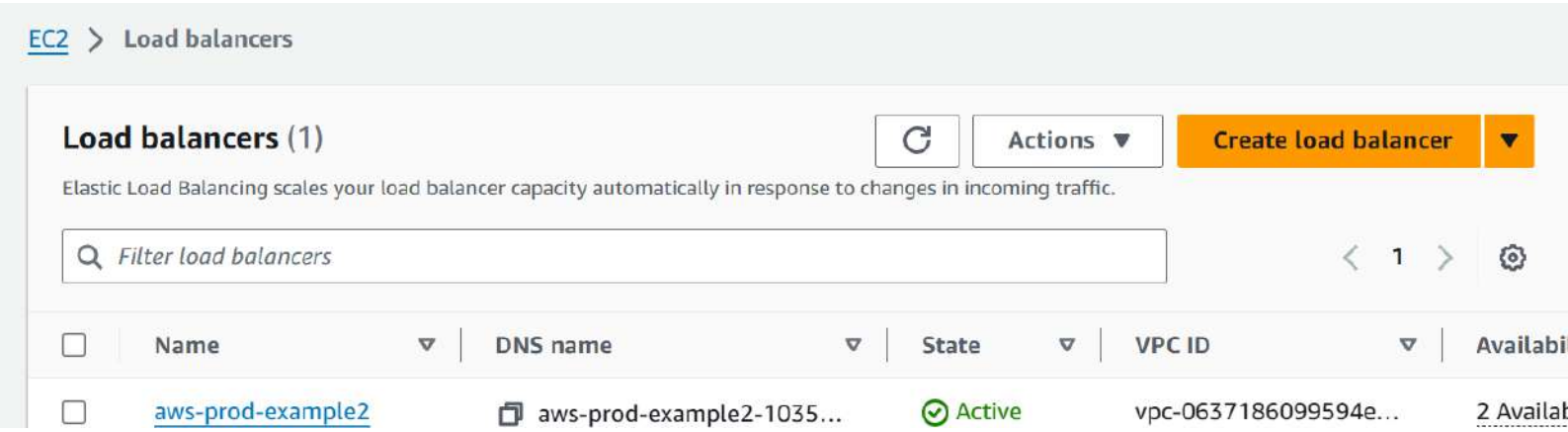
Create target group

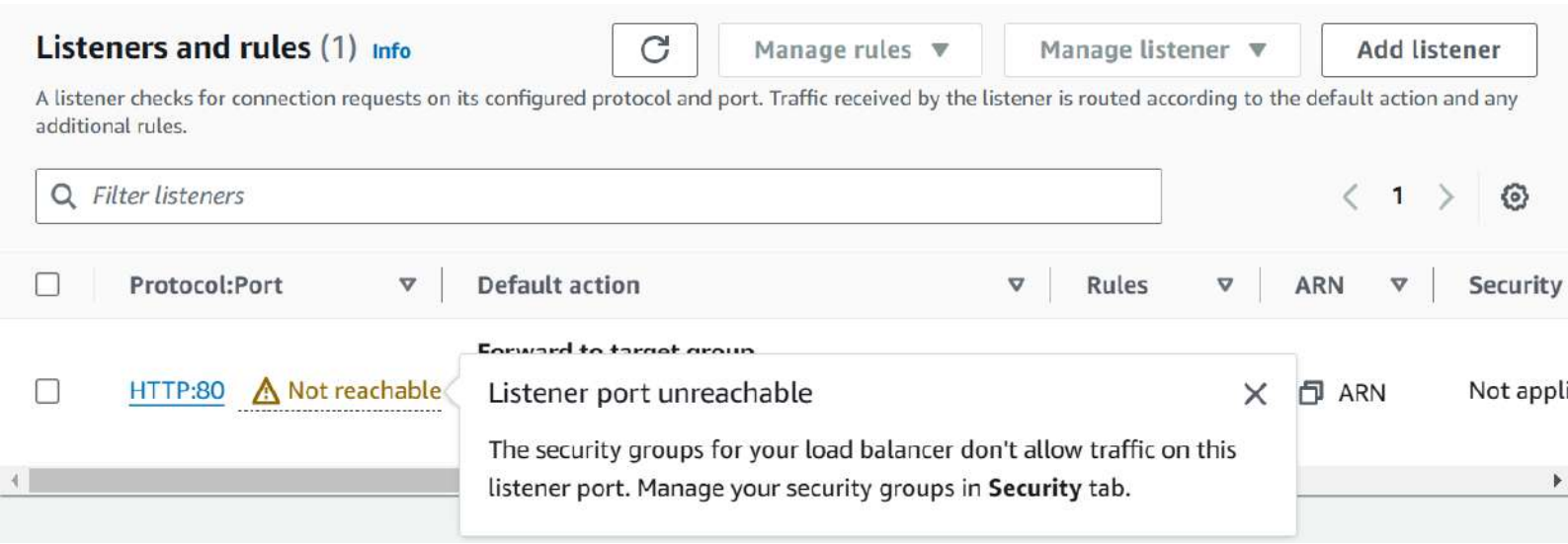
Listener tags - *optional*

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.


EC2 > Load balancers
Load balancers (1)
Actions
Create load balancer
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.
Filter load balancers
1
Name
DNS name
State
VPC ID
Availabi
aws-prod-example2
aws-prod-example2-1035...
Active
vpc-0637186099594e...
2 Availab


Listeners and rules (1) Info
Manage rules
Manage listener
Add listener
A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.
Filter listeners
1
Protocol:Port
Default action
Rules
ARN
Security
HTTP:80
Not reachable
Forward to target group
ARN
Not appli
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.

EC2 > Security Groups > sg-0061fc7173ed54c65 - aws prod example > Edit inbound rules

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		Description - optional Info	
sgr-0be225a0128ee3275	HTTP	TCP	80	Cus...	0.0.0.0/0		Delete
sgr-03abe9c077c794bf4	SSH	TCP	22	Cus...	0.0.0.0/0		Delete
sgr-0ef868bab20ff2845	Custom TCP	TCP	8000	Cus...	0.0.0.0/0		Delete

my first aws project demonastrate apps in private subnet

thank you abhishek.veeramalla sir