

# VPC

## 1. Create VPC

[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.

#### 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 - *optional*  
Creates a tag with a key of 'Name' and a value that you specify.

MY-Mumbai-VPC

IPv4 CIDR block [Info](#)  
☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

IPv4 CIDR

192.168.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)  
☒ No IPv6 CIDR block ☐ IPAM-allocated IPv6 CIDR block ☐ Amazon-provided IPv6 CIDR block ☐ IPv6 CIDR owned by me

Tenancy [Info](#)  
Default

**Your VPCs (2)** [Info](#)

Last updated less than a minute ago

Actions

Create VPC

1

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	-	<a href="#">vpc-0e671aee2ece8f84d</a>	Available	172.31.0.0/16	-
<input type="checkbox"/>	MY-Mumbai-VPC	<a href="#">vpc-0fc5f43b9fa901efd</a>	Available	192.168.0.0/16	-

## 2. Create Internet Gateway (IGW)

[VPC](#) > [Internet gateways](#) > Create internet gateway

### Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

#### Internet gateway settings

##### Name tag

Creates a tag with a key of 'Name' and a value that you specify.

#### Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

Remove

Add new tag

#### Internet gateways (1/2) [Info](#)

Search

	Name	Internet gateway ID	
<input type="checkbox"/>	-	<a href="#">igw-07177315461060f9a</a>	
<input checked="" type="checkbox"/>	My-Mumbai-IGW	<a href="#">igw-01fc5b0357d295ce8</a>	

Actions

Create internet gateway

View details

Attach to VPC

Detach from VPC

Manage tags

Delete internet gateway

[VPC](#) > [Internet gateways](#) > Attach to VPC (igw-01fc5b0357d295ce8)

### Attach to VPC (igw-01fc5b0357d295ce8) [Info](#)

#### VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

##### Available VPCs

Attach the internet gateway to this VPC.

Select a VPC

vpc-0fc5f43b9fa901efd - MY-Mumbai-VPC

AWS Command Line Interface command

Cancel

Attach internet gateway

### 3. Creating Public and Private Subnets

[VPC](#) > [Subnets](#) > Create subnet

## Create subnet [Info](#)

### VPC

#### VPC ID

Create subnets in this VPC.

vpc-0fc5f43b9fa901efd (MY-Mumbai-VPC) ▼

### Associated VPC CIDRs

#### IPv4 CIDRs

192.168.0.0/16

### Subnet 1 of 1

#### Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Public-Subnet-Mumbai

The name can be up to 256 characters long.

#### Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Mumbai) / ap-south-1a ▼

#### IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

192.168.0.0/16 ▼

#### IPv4 subnet CIDR block

192.168.1.0/24

256 IPs

< > ^ v

Subnet 2 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Private-Subnet-Mumbai

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Mumbai) / ap-south-1b

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

192.168.0.0/16

IPv4 subnet CIDR block

192.168.2.0/24

256 IPs

< > ^ v

Subnets (5) [Info](#)

Last updated less than a minute ago

Actions

Create subnet

Find resources by attribute or tag

< 1 >

<input type="checkbox"/>	Name	Subnet ID	State	VPC
<input type="checkbox"/>	-	<a href="#">subnet-05e5889bf6211dee0</a>	Available	<a href="#">vpc-0e671aee2ece8f84d</a>
<input type="checkbox"/>	-	<a href="#">subnet-051c7044b0230918d</a>	Available	<a href="#">vpc-0e671aee2ece8f84d</a>
<input type="checkbox"/>	Private-Subnet-Mumbai	<a href="#">subnet-08c1547242085bd01</a>	Available	<a href="#">vpc-0fc5f43b9fa901efd</a>   MY-
<input type="checkbox"/>	Public-Subnet-Mumbai	<a href="#">subnet-06f243b15b17d806a</a>	Available	<a href="#">vpc-0fc5f43b9fa901efd</a>   MY-

## 4. Creating NAT Gateway

### NAT gateway settings

#### Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

NAT-MUMBAI

The name can be up to 256 characters long.

#### Subnet

Select a subnet in which to create the NAT gateway.

subnet-06f243b15b17d806a (Public-Subnet-Mumbai) ▼

#### Connectivity type

Select a connectivity type for the NAT gateway.

- ☒ Public  
☐ Private

#### Elastic IP allocation ID [Info](#)

Assign an Elastic IP address to the NAT gateway.

eipalloc-0effc5a1ed9797e54 ▼

**Allocate Elastic IP**

[Click on Allocate Elastic IP]

## 5. Create Routing Tables

[VPC](#) > [Route tables](#) > Create route table

### Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

#### Route table settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

VPC

The VPC to use for this route table.

[VPC](#) > [Route tables](#) > Create route table

### Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

#### Route table settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

VPC

The VPC to use for this route table.

☒ Public-RouteTable [rtb-0553451d21e03ccd1](#) - -

Details | **routes** | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

Both Edit routes

Filter routes

Destination

Target

Status

Propagated

192.168.0.0/16

local

Active

No

VPC > Route tables > [rtb-0553451d21e03ccd1](#) > Edit routes

### Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
<input type="text" value="0.0.0.0/0"/>	Internet Gateway	-	No
	<input type="text" value="igw-01fc5b0357d295ce8"/>		

VPC > Route tables > [rtb-0553451d21e03ccd1](#) > Edit subnet associations

### Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	Private-Subnet-Mumbai	<a href="#">subnet-08c1547242085bd01</a>	192.168.2.0/24	-	<a href="#">Main (rtb-00720390260cad90)</a>
<input checked="" type="checkbox"/>	Public-Subnet-Mumbai	<a href="#">subnet-06f243b15b17d806a</a>	192.168.1.0/24	-	<a href="#">Main (rtb-00720390260cad90)</a>

[Added Public subnet association to Public Route table]

<input checked="" type="checkbox"/>	Private-RouteTable	<a href="#">rtb-093582ad5c000612e</a>	-	-
<input type="checkbox"/>	-	<a href="#">rtb-00720390260cad90b</a>	-	-
<input type="checkbox"/>	Public-RouteTable	<a href="#">rtb-0553451d21e03ccd1</a>	<a href="#">subnet-06f243b15b17d8...</a>	-

**rtb-093582ad5c000612e / Private-RouteTable**

Details | **Routes** | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

Destination	Target	Status	Propagated
-------------	--------	--------	------------

### Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
<input type="text" value="0.0.0.0/0"/>	NAT Gateway	-	No
	<input type="text" value="nat-09fea314d0c3fca55"/>		

VPC > Route tables > rtb-093582ad5c000612e > Edit subnet associations

## Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	Private-Subnet-Mumbai	<a href="#">subnet-08c1547242085bd01</a>	192.168.2.0/24	–	<a href="#">Main (rtb-00720390260cad90</a>
<input type="checkbox"/>	Public-Subnet-Mumbai	<a href="#">subnet-06f243b15b17d806a</a>	192.168.1.0/24	–	<a href="#">rtb-0553451d21e03ccd1 / Pul</a>

## 6. Creating Security Group

EC2 > Security Groups > Create security group

## Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

### Basic details

Security group name [Info](#)

Mumbai-SG

Name cannot be edited after creation.

Description [Info](#)

New-SG-Mumbai

VPC [Info](#)

vpc-0fc5f43b9fa901efd (MY-Mumbai-VPC)

– All traffic All All Cu...  Delete

Add rule

[Inbound rule must be self also]



## 7. Creating EC2 Instances – Boston/ Jump Instance + Private 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. Quickly get started by following the simple steps below.

#### Name and tags [Info](#)

Name

Bastion Server

[Add additional tags](#)

#### Amazon Machine Image (AMI)

Red Hat Enterprise Linux 9 (HVM), SSD Volume Type

Free tier eligible ▼

ami-022ce6f32988af5fa (64-bit (x86)) / ami-0b0ec21d6b2ce310b (64-bit (Arm))

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

#### Description

Red Hat Enterprise Linux version 9 (HVM), EBS General Purpose (SSD) Volume Type

Architecture

64-bit (x86) ▼

AMI ID

ami-022ce6f32988af5fa

Verified provider

## ▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0fc5f43b9fa901efd (MY-Mumbai-VPC)  
192.168.0.0/16



Subnet [Info](#)

subnet-06f243b15b17d806a Public-Subnet-Mumbai  
VPC: vpc-0fc5f43b9fa901efd Owner: 966481983228  
Availability Zone: ap-south-1a Zone type: Availability Zone  
IP addresses available: 250 CIDR: 192.168.1.0/24



[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

Common security groups [Info](#)

Select security groups



[Compare security group rules](#)

Mumbai-SG sg-09b9119c0e257f510 ✕  
VPC: vpc-0fc5f43b9fa901efd

Security groups that you add or remove here will be added to or removed from all your network interfaces.

[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. Quickly get started by following the simple steps below.

### Name and tags [Info](#)

Name

Private Server

[Add additional tags](#)

### Amazon Machine Image (AMI)

Red Hat Enterprise Linux 9 (HVM), SSD Volume Type

Free tier eligible

ami-022ce6f32988af5fa (64-bit (x86)) / ami-0b0ec21d6b2ce310b (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

### Description

Red Hat Enterprise Linux version 9 (HVM), EBS General Purpose (SSD) Volume Type

### Architecture

64-bit (x86)

### AMI ID

ami-022ce6f32988af5fa

Verified provider

### VPC - required [Info](#)

vpc-0fc5f43b9fa901efd (MY-Mumbai-VPC)  
192.168.0.0/16



### Subnet [Info](#)

subnet-08c1547242085bd01 Private-Subnet-Mumbai  
VPC: vpc-0fc5f43b9fa901efd Owner: 966481983228  
Availability Zone: ap-south-1b Zone type: Availability Zone  
IP addresses available: 251 CIDR: 192.168.2.0/24



[Create new subnet](#)

### Auto-assign public IP [Info](#)

Disable

### 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

### Common security groups [Info](#)

Select security groups



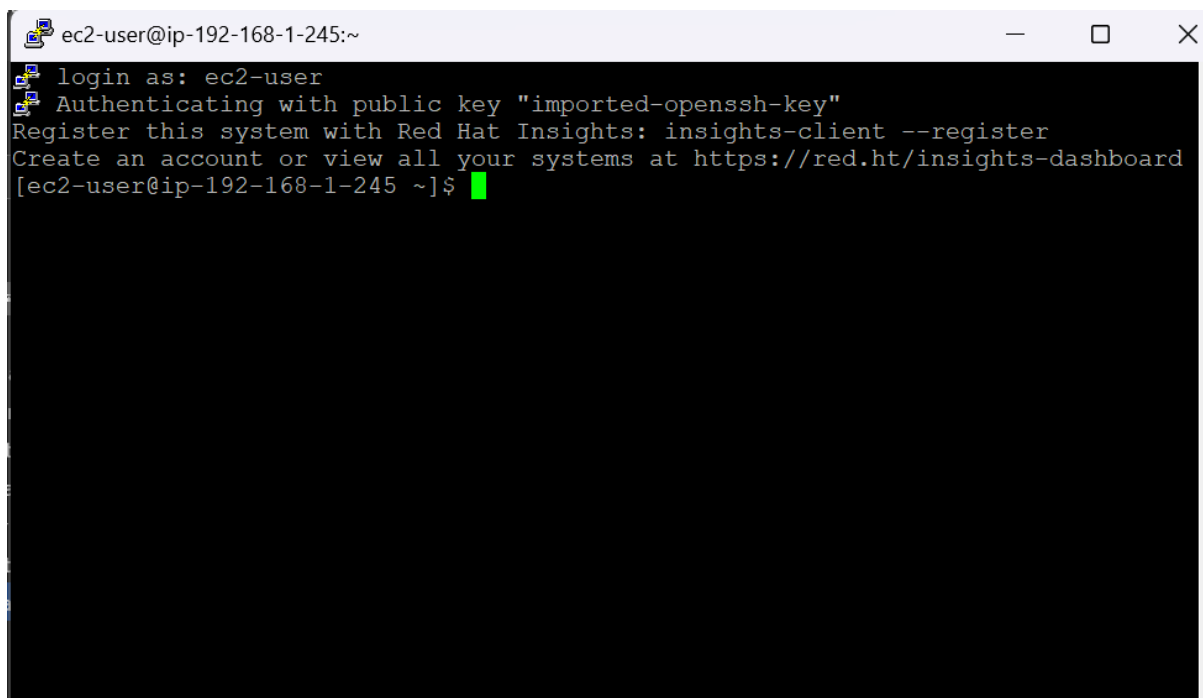
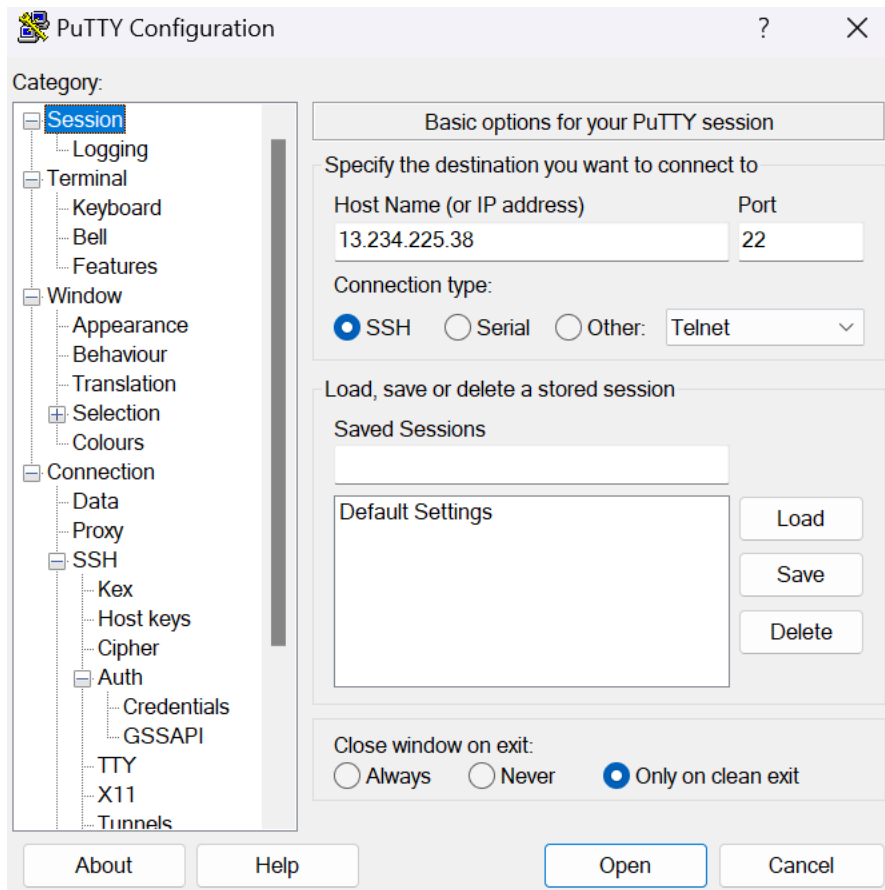
[Compare security group rules](#)

Mumbai-SG sg-09b9119c0e257f510 X  
VPC: vpc-0fc5f43b9fa901efd

Security groups that you add or remove here will be added to or removed from all your network interfaces.

## 8. Connecting to Bastion Server

If our VPC is successful then only our bastion server will work



[We can see our IP is started with 192.168.1.---] that means public subnet.

// Now we will try to connect to Private server using Boston server

<input type="checkbox"/>	Bastion Server-2	i-03a21884beef7cb15	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	ap-south-1a
<input type="checkbox"/>	Bastion Server	i-0d80aa6a256a3ed8e	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	ap-south-1a
<input checked="" type="checkbox"/>	Private Server	i-044fa15bae9303a9e	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	ap-south-1b

[Press Connect]

EC2 > Instances > i-044fa15bae9303a9e > Connect to instance

## Connect to instance [Info](#)

Connect to your instance i-044fa15bae9303a9e (Private Server) using any of these options

EC2 Instance Connect	Session Manager	SSH client	EC2 serial console
<p>Instance ID</p> <p> i-044fa15bae9303a9e (Private Server)</p> <ol style="list-style-type: none"> <li>1. Open an SSH client.</li> <li>2. Locate your private key file. The key used to launch this instance is LearnAWS-1.pem</li> <li>3. Run this command, if necessary, to ensure your key is not publicly viewable. <ul style="list-style-type: none"> <li> <code>chmod 400 "LearnAWS-1.pem"</code></li> </ul> </li> <li>4. Connect to your instance using its Private IP: <ul style="list-style-type: none"> <li> 192.168.2.26</li> </ul> </li> </ol> <p>Example:</p> <p> <code>ssh -i "LearnAWS-1.pem" ec2-user@192.168.2.26</code></p>			

[Copy Example Line & paste in Bastion server]

[Permission Denied → we need to have the pem file inside the Bastion server]

For that simple way is to copy the complete pemfile data and create a new file in the bastion server and then use the command again → It will work]

```
ec2-user@ip-192-168-2-26:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[ec2-user@ip-192-168-1-90 ~]$ sudo -s
[root@ip-192-168-1-90 ec2-user]# vi LearnAWS-1.pem
[root@ip-192-168-1-90 ec2-user]# chmod 400 LearnAWS-1.pem
[root@ip-192-168-1-90 ec2-user]# ls
LearnAWS-1.pem
[root@ip-192-168-1-90 ec2-user]# ssh -i "LearnAWS-1.pem" ec2-user@192.168.2.26
The authenticity of host '192.168.2.26 (192.168.2.26)' can't be established.
ED25519 key fingerprint is SHA256:nQWLLZak/sNa0xfVkr/i7DoOmInx4eUDzOcvtX4tjmY8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.26' (ED25519) to the list of known hosts.
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[ec2-user@ip-192-168-2-26 ~]$
```

## Connected to Private Server Using Bostion server

We have attached NAT gateway to the Private Route table which is connected to Private subnets and we are in private server which is located in private subnet.

NAT is present that means we have internet access, to test it will download a sample in the ec2

```
root@ip-192-168-2-26:/home/ec2-user
[ec2-user@ip-192-168-2-26 ~]$ sudo -s
[root@ip-192-168-2-26 ec2-user]# yum install -y wget
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to register.

Red Hat Enterprise Linux 9 for x86_64 - AppStream from RHUI (RPMs) 57 MB/s | 40 MB 00:00
Red Hat Enterprise Linux 9 for x86_64 - BaseOS from RHUI (RPMs) 58 MB/s | 30 MB 00:00
Red Hat Enterprise Linux 9 Client Configuration 33 kB/s | 3.0 kB 00:00
Dependencies resolved.

Package Architecture Version Repository Size
Installing:
wget x86_64 1.21.1-8.el9_4 rhel-9-appstream-rhui-rpms 789 k

Transaction Summary
Install 1 Package

Total download size: 789 k
Installed size: 3.1 M
Downloading Packages:
wget-1.21.1-8.el9_4.x86_64.rpm 14 MB/s | 789 kB 00:00
Total 9.5 MB/s | 789 kB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing :
Installing : wget-1.21.1-8.el9_4.x86_64 1/1
Running scriptlet: wget-1.21.1-8.el9_4.x86_64 1/1
Verifying : wget-1.21.1-8.el9_4.x86_64 1/1
Installed products updated.

Installed:
wget-1.21.1-8.el9_4.x86_64

Complete!
[root@ip-192-168-2-26 ec2-user]#
```

Now we try to stop the internet access, for that we need to remove the routes access (NAT) from private route table.

Route tables (1/4) Info

Last updated about 1 hour ago

Actions

Create route table

Find resources by attribute or tag

	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-0b93c86ed7e0000b1	-	-	Yes	vpc-0e...
<input checked="" type="checkbox"/>	Private-RouteTable	rtb-093582ad5c000612e	subnet-08c1547242085b...	-	No	vpc-0fc...
<input type="checkbox"/>	-	rtb-00720390260cad90b	-	-	Yes	vpc-0fc...
<input type="checkbox"/>	Public-RouteTable	rtb-0553451d21e03ccr1	subnet-06f243h15h17d8	-	No	vpc-0fr...

rtb-093582ad5c000612e / Private-RouteTable

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Both Edit routes

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	nat-09fea314d0c3fca55	Active	No
192.168.0.0/16	local	Active	No

VPC > Route tables > rtb-093582ad5c000612e > Edit routes

Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	NAT Gateway	Active	No

Add route

Remove

[Remove NAT Gateway]

Updated routes for rtb-093582ad5c000612e / Private-RouteTable successfully

rtb-093582ad5c000612e / Private-RouteTable

Details Info

Route table ID

rtb-093582ad5c000612e

VPC

vpc-0fc5f43b9fa901efd | MY-Mumbai-VPC

Main

No

Owner ID

966481983228

Explicit subnet associations

subnet-08c1547242085bd01 / Private-Subnet-Mumbai

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Both Edit routes

Filter routes

1

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No

Now we will test the Private server internet access

```
Running script: wget -1.21.1-8.el9_4.x86_64
Verifying : wget-1.21.1-8.el9_4.x86_64
Installed products updated.
Installed:
  wget-1.21.1-8.el9_4.x86_64

Complete!
[root@ip-192-168-2-26 ec2-user]# yum install -y httpd
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to register.
Last metadata expiration check: 0:04:56 ago on Wed 04 Sep 2024 10:55:45 AM UTC.
Dependencies resolved.
=====
Package                                Architecture      Version            Repository          Size
-----
Installing:
httpd                                  x86_64            2.4.57-11.el9_4.1  rhel-9-appstream-rhui-rpms 51 k
Installing dependencies:
apr                                    x86_64            1.7.0-12.el9_3    rhel-9-appstream-rhui-rpms 126 k
apr-util                              x86_64            1.6.1-23.el9      rhel-9-appstream-rhui-rpms 97 k
apr-util-bdb                          x86_64            1.6.1-23.el9      rhel-9-appstream-rhui-rpms 14 k
httpd-core                            x86_64            2.4.57-11.el9_4.1 rhel-9-appstream-rhui-rpms 1.5 M
httpd-filesystem                     noarch            2.4.57-11.el9_4.1 rhel-9-appstream-rhui-rpms 14 k
httpd-tools                          x86_64            2.4.57-11.el9_4.1 rhel-9-appstream-rhui-rpms 86 k
mailcap                              noarch            2.1.49-5.el9      rhel-9-baseos-rhui-rpms 35 k
redhat-logos-httpd                  noarch            90.4-2.el9        rhel-9-appstream-rhui-rpms 18 k
Installing weak dependencies:
apr-util-openssl                     x86_64            1.6.1-23.el9      rhel-9-appstream-rhui-rpms 17 k
mod_http2                           x86_64            2.0.26-2.el9_4    rhel-9-appstream-rhui-rpms 167 k
mod_lua                             x86_64            2.4.57-11.el9_4.1 rhel-9-appstream-rhui-rpms 60 k
Transaction Summary
-----
Install 12 Packages

Total download size: 2.2 M
Installed size: 6.1 M
Downloading Packages:
^[[D      [      ===      ] --- B/s | 0 B  --:-- E
[      [      ===      ] --- B/s | 0 B  --:-- ETA
```

```
Total download size: 2.2 M
Installed size: 6.1 M
Downloading Packages:
^[[D
[====]
] --- B/s | 0 B --:-- E
] --- B/s | 0 B --:-- ETAA
^C
[====]
] --- B/s | 0 B --:-- ET
A
The downloaded packages were saved in cache until the next successful transaction.
You can remove cached packages by executing 'yum clean packages'.
Error: Error downloading packages:
  Interrupted by a SIGINT signal
[root@ip-192-168-2-26 ec2-user]#
```

To get internet access again just add the NAT gateway again in the routes

VPC > Route tables > [rtb-093582ad5c000612e](#) > Edit routes

### Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
<input type="text" value="0.0.0.0/0"/>	NAT Gateway	-	No
	<input type="text" value="nat-09fea314d0c3fca55"/>		

Updated routes for [rtb-093582ad5c000612e](#) / Private-RouteTable successfully

Details Info

Route table ID

rtb-093582ad5c000612e

VPC

vpc-0fc5f43b9fa901efd | MY-Mumbai-VPC

Main

No

Owner ID

966481983228

Explicit subnet associations

[subnet-08c1547242085bd01](#) / [Private-Subnet-Mumbai](#)

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both Edit routes

< 1 > ⚙

Destination	Target	Status	Propagated
0.0.0.0/0	<a href="#">nat-09fea314d0c3fca55</a>	Active	No
192.168.0.0/16	local	Active	No

Check Internet access is working or not..



```
(12/12): httpd-core-2.4.57-11.el9_4.1.x86_64.rpm 31 MB/s | 1.5 MB 00:00
-----
Total 13 MB/s | 2.2 MB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : 1/1
  Installing     : apr-1.7.0-12.el9_3.x86_64 1/12
  Installing     : apr-util-bdb-1.6.1-23.el9.x86_64 2/12
  Installing     : apr-util-openssl-1.6.1-23.el9.x86_64 3/12
  Installing     : apr-util-1.6.1-23.el9.x86_64 4/12
  Installing     : httpd-tools-2.4.57-11.el9_4.1.x86_64 5/12
  Installing     : mailcap-2.1.49-5.el9.noarch 6/12
  Running scriptlet: httpd-filesystem-2.4.57-11.el9_4.1.noarch 7/12
  Installing     : httpd-filesystem-2.4.57-11.el9_4.1.noarch 7/12
  Installing     : httpd-core-2.4.57-11.el9_4.1.x86_64 8/12
  Installing     : mod_lua-2.4.57-11.el9_4.1.x86_64 9/12
  Installing     : redhat-logos-httpd-90.4-2.el9.noarch 10/12
  Installing     : mod_http2-2.0.26-2.el9_4.x86_64 11/12
  Installing     : httpd-2.4.57-11.el9_4.1.x86_64 12/12
  Running scriptlet: httpd-2.4.57-11.el9_4.1.x86_64 12/12
  Verifying      : apr-util-1.6.1-23.el9.x86_64 1/12
  Verifying      : apr-util-bdb-1.6.1-23.el9.x86_64 2/12
  Verifying      : apr-util-openssl-1.6.1-23.el9.x86_64 3/12
  Verifying      : redhat-logos-httpd-90.4-2.el9.noarch 4/12
  Verifying      : apr-1.7.0-12.el9_3.x86_64 5/12
  Verifying      : mod_http2-2.0.26-2.el9_4.x86_64 6/12
  Verifying      : httpd-2.4.57-11.el9_4.1.x86_64 7/12
  Verifying      : httpd-core-2.4.57-11.el9_4.1.x86_64 8/12
  Verifying      : httpd-filesystem-2.4.57-11.el9_4.1.noarch 9/12
  Verifying      : httpd-tools-2.4.57-11.el9_4.1.x86_64 10/12
  Verifying      : mod_lua-2.4.57-11.el9_4.1.x86_64 11/12
  Verifying      : mailcap-2.1.49-5.el9.noarch 12/12
Installed products updated.

Installed:
apr-1.7.0-12.el9_3.x86_64      apr-util-1.6.1-23.el9.x86_64      apr-util-bdb-1.6.1-23.el9.x86_64      apr-util-openssl-1.6.1-23.el9.x86_64
httpd-2.4.57-11.el9_4.1.x86_64  httpd-core-2.4.57-11.el9_4.1.x86_64  httpd-filesystem-2.4.57-11.el9_4.1.noarch  httpd-tools-2.4.57-11.el9_4.1.x86_64
mailcap-2.1.49-5.el9.noarch    mod_http2-2.0.26-2.el9_4.x86_64    mod_lua-2.4.57-11.el9_4.1.x86_64      redhat-logos-httpd-90.4-2.el9.noarch

Complete!
[root@ip-192-168-2-26 ec2-user]#
```

# VPC - END POINTS

## 9. Install AWS cli in EC2

**(Optional)** The following command block downloads and installs the AWS CLI without first verifying the integrity of your download. To verify the integrity of your download, use the below step by step instructions.

To install the AWS CLI, run the following commands.

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

To update your current installation of the AWS CLI, add your existing symlink and installer information to construct the `install` command using the `--bin-dir`, `--install-dir`, and `--update` parameters. The following

```
root@ip-192-168-2-26:/home/ec2-user
[root@ip-192-168-2-26 ec2-user]# curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 58.0M  100 58.0M    0     0  92.5M      0 --:--:-- --:--:-- --:--:--  92.5M
[root@ip-192-168-2-26 ec2-user]# yum install -y unzip
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhnc" or "subscription-manager" to register.
Last metadata expiration check: 0:03:03 ago on Wed 04 Sep 2024 11:05:47 AM UTC.
Dependencies resolved.
=====
Package                        Architecture      Version           Repository        Size
=====
Installing:
unzip                          x86_64            6.0-56.el9       rhel-9-baseos-rhui-rpms 186 k
Transaction Summary
=====
Install 1 Package
Total download size: 186 k
Installed size: 392 k
Downloading Packages:
unzip-6.0-56.el9.x86_64.rpm                                           4.7 MB/s | 186 kB  00:00
-----
Total                                                                    2.9 MB/s | 186 kB  00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : unzip-6.0-56.el9.x86_64                               1/1
  Installing     : unzip-6.0-56.el9.x86_64                               1/1
  Running scriptlet: unzip-6.0-56.el9.x86_64                               1/1
  Verifying      : unzip-6.0-56.el9.x86_64                               1/1
Installed products updated.

Installed:
  unzip-6.0-56.el9.x86_64

Complete!
[root@ip-192-168-2-26 ec2-user]#
```

[unzip awscliv2.zip]

```
[root@ip-192-168-2-26 ec2-user]# ls
aws  awscliv2.zip
[root@ip-192-168-2-26 ec2-user]#

[root@ip-192-168-2-26 ec2-user]# sudo ./aws/install
You can now run: /usr/local/bin/aws --version
[root@ip-192-168-2-26 ec2-user]# ^C
[root@ip-192-168-2-26 ec2-user]# /usr/local/bin/aws --version
aws-cli/2.17.43 Python/3.11.9 Linux/5.14.0-427.20.1.el9_4.x86_64 exe/x86_64.rhel.9
[root@ip-192-168-2-26 ec2-user]#
```

I want to access the AWS, for that we have ways

1. Access Key and super Key (Security Concerns)
2. Using IAM Roles (High Security)

So lets attach a IAM role to the private server[bcz we are accessing the private server]

Select trusted entity

Step 2  
Add permissions

Step 3  
Name, review, and create

Select trusted entity [Info](#)

Trusted entity type

☒ AWS service  
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ AWS account  
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ Web identity  
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ SAML 2.0 federation  
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy  
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case  
EC2

Choose a use case for the specified service.  
Use case  
☒ EC2

[IAM](#) > [Roles](#) > Create role

Step 1  
[Select trusted entity](#)

Step 2  
Add permissions

Step 3  
Name, review, and create

Add permissions [Info](#)

Permissions policies (1/950) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type

s3fu

All types

1 match

<input checked="" type="checkbox"/>	Policy name	Type	Description
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the ...

► Set permissions boundary - optional

Cancel

Previous

Next

[IAM](#) > [Roles](#) > Create role

Step 1  
[Select trusted entity](#)

Step 2  
[Add permissions](#)

Step 3  
**Name, review, and create**

## Name, review, and create

### Role details

**Role name**  
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+=, @- /[]!#\$%^&\*~`' characters.

**Description**  
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: \_+=, @- /[]!#\$%^&\*~`'.

Now Attach the IAM role to EC2 [private server]

Successfully initiated termination (deletion) of i-0d80aa6a256a3ed8e

Instances (1/4) [Info](#) Last updated 27 minutes ago [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

[All states](#)

	Name	Instance ID	Instance state	Instance type	Status checks
<input type="checkbox"/>	Bastion Server-1	i-0a943ad84ee99dbc7	Terminated	t2.micro	-
<input type="checkbox"/>	Bastion Server-2	i-03a21884beef7cb15	Running	t2.micro	2/2 checks passed
<input type="checkbox"/>	Bastion Server	i-0d80aa6a256a3ed8e	Terminated	t2.micro	-
<input checked="" type="checkbox"/>	Private Server	i-044fa15bae9303a9e	Running	t2.micro	2/2 checks passed

Actions for Private Server (i-044fa15bae9303a9e):

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

[EC2](#) > [Instances](#) > [i-044fa15bae9303a9e](#) > [Modify IAM role](#)

## Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

[i-044fa15bae9303a9e](#) (Private Server)

**IAM role**  
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

[Refresh](#) [Create new IAM role](#)

[Cancel](#) [Update IAM role](#)

// Now we have the complete S3 access in Private server.

// Creating a Bucket using EC2

```
[root@ip-192-168-2-26 ec2-user]# /usr/local/bin/aws s3 mb s3://2024-test-vpcendpoint-demo --region ap-south-1
make_bucket: 2024-test-vpcendpoint-demo
[root@ip-192-168-2-26 ec2-user]#
```

[Bucket Created]

Bucket Name: 2024-test-vpcendpoint-demo

Region : ap-south-1 [Mumbai]

Amazon S3

► Account snapshot - updated every 24 hours

All AWS Regions

View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets

Directory buckets

General purpose buckets (1)

Info

All AWS Regions

↻

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 > ⚙

	Name	▲	AWS Region	▼	IAM Access Analyzer	Creation date	▼
<input type="radio"/>	<a href="#">2024-test-vpcendpoint-demo</a>		Asia Pacific (Mumbai)	ap-south-1	<a href="#">View analyzer for ap-south-1</a>	September 4, 2024, 16:51:51 (UTC+05:30)	

// I want to access the S3 with out internet

For this I have to create a END Point in VPC and attach it to the private sever

[Remove the NAT route from private routes]

Route tables (1/4)

Info

Last updated 35 minutes ago

↻

Actions

Create route table

Find resources by attribute or tag

< 1 > ⚙

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input type="checkbox"/>	-	<a href="#">rtb-0b93c86ed7e0000b1</a>	-	-	Yes	<a href="#">vpc-0ef...</a>
<input checked="" type="checkbox"/>	Private-RouteTable	<a href="#">rtb-093582ad5c000612e</a>	<a href="#">subnet-08c1547242085b...</a>	-	No	<a href="#">vpc-0fc...</a>
<input type="checkbox"/>	-	<a href="#">rtb-00720390260cad90b</a>	-	-	Yes	<a href="#">vpc-0fc...</a>

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both

Edit routes

Filter routes

< 1 > ⚙

Destination	Target	Status	Propagated
0.0.0.0/0	<a href="#">nat-09fea314d0c3fca55</a>	Active	No
192.168.0.0/16	local	Active	No

Updated routes for rtb-093582ad5c000612e / Private-RouteTable successfully

Details

rtb-093582ad5c000612e / Private-RouteTable

DetailsInfo

Route table ID

rtb-093582ad5c000612e

VPC

vpc-0fc5f43b9fa901efd | MY-Mumbai-VPC

Main

No

Owner ID

966481983228

Explicit subnet associations

subnet-08c1547242085bd01 / Private-Subnet-Mumbai

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Both

Edit routes

Filter routes

< 1 >

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No

## CREATE END POINTS

VPC > Endpoints > Create endpoint

Create endpointInfo

There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and Gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an Elastic Network Interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while Gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

Endpoint settings

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

S3-VPC-ENDPOINT

Service category

Select the service category

AWS services

Services provided by Amazon

PrivateLink Ready partner services

Services with an AWS Service Ready designation

AWS Marketplace services

Services that you've purchased through AWS Marketplace

EC2 Instance Connect Endpoint

Endpoint for the EC2 Instance Connect service

Other endpoint services

Endpoint services that are not part of the AWS managed services

## Using only Gateway Interface

Services (1/4)

Search

s3

Clear filters

< 1 >

Service Name	Owner	Type
com.amazonaws.ap-south-1.s3	amazon	Gateway
com.amazonaws.ap-south-1.s3	amazon	Interface
com.amazonaws.ap-south-1.s3-outposts	amazon	Interface
com.amazonaws.s3-global.accesspoint	amazon	Interface

**VPC**  
Select the VPC in which to create the endpoint

VPC  
The VPC in which to create your endpoint.

vpc-0fc5f43b9fa901efd (MY-Mumbai-VPC)

**Route tables (1/3)** Info

Search

Name	Route Table ID	Main	Associated Id
<input checked="" type="checkbox"/> Private-RouteTable	rtb-093582ad5c000612e (Private-Rout...	No	subnet-08c1547242085bd01 (Private-Subnet-...
<input type="checkbox"/> -	rtb-00720390260cad90b	Yes	-
<input type="checkbox"/> Public-RouteTable	rtb-0553451d21e03ccd1 (Public-Route...	No	subnet-06f243b15b17d806a (Public-Subnet-M...

**Endpoints (1/1)** Info

Search

Create endpoint

Name	VPC endpoint ID	VPC ID	Service name
<input checked="" type="checkbox"/> S3-VPC-ENDPOINT	vpce-07359e19c973b1025	vpc-0fc5f43b9fa901efd   MY-Mumbai-V...	com.amazonaws.ap-south-1.s3

## Internet Access is removed

```
[root@ip-192-168-2-26 ec2-user]# yum install -y httpd
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhnc" or "subscription-manager" to register.

^ARed Hat Enterprise Linux 9 for x86_64 - AppStream from RHUI [
Red Hat Enterprise Linux 9 for x86_64 - AppStream from RHUI [
^CRed Hat Enterprise Linux 9 for x86_64 - AppStream from RHUI [
Red Hat Enterprise Linux 9 for x86_64 - AppStream from RHUI (RPMs) [
Error: Failed to download metadata for repo 'rhel-9-appstream-rhui-rpms': Cannot prepare internal mirrorlist: Interrupted by signal
[root@ip-192-168-2-26 ec2-user]#
```

// But we can access the s3 because of VPC Endpoint [AWS Internet]

**Route tables (1/4)** Info

Find resources by attribute or tag

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input checked="" type="checkbox"/> Private-RouteTable	rtb-093582ad5c000612e	subnet-08c1547242085b...	-	No	vpc-0fc
<input type="checkbox"/> -	rtb-00720390260cad90b	-	-	Yes	vpc-0fc
<input type="checkbox"/> Public-RouteTable	rtb-0553451d21e03ccd1	subnet-06f243b15b17d8...	-	No	vpc-0fc
<input type="checkbox"/> -	rtb-0b93c86ed7e0000b1	-	-	Yes	vpc-0et

**rtb-093582ad5c000612e / Private-RouteTable**

Details | **Routes** | Subnet associations | Edge associations | Route propagation | Tags

**Routes (2)**

Filter routes

Destination	Target	Status	Propagated
pl-78a54011	vpce-07359e19c973b1025	Active	No
192.168.0.0/16	local	Active	No

[Automatically assigned the Prefix List]

Now we will access the S3 bucket from EC2

```
[root@ip-192-168-2-26 ec2-user]# /usr/local/bin/aws s3 ls
2024-09-04 11:21:52 2024-test-vpcendpoint-demo
[root@ip-192-168-2-26 ec2-user]#
```

## 10. DISMANTLE

**Terminate (delete) instances?**

⚠ On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?

Instance ID	Termination protection
i-044fa15bae9303a9e (Private Server)	❌ Disabled
i-03a21884beef7cb15 (Bastion Server-2)	❌ Disabled

To confirm that you want to delete the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.

Cancel Terminate (delete)

**Delete NAT gateway**

**Will be deleted**  
The following NAT gateway will be deleted permanently and can't be recovered later.

Name	NAT gateway ID	State
NAT-MUMBAI	nat-09fea314d0c3fca55	✅ Available

To confirm deletion, type *delete* in the field:

delete

Cancel Delete

**Delete VPC**

This VPC will be deleted permanently and cannot be recovered later:

Name	VPC ID	State
MY-Mumbai-VPC	vpc-0fc5f43b9fa901efd	✅ Available

**Will also be deleted**  
The following 7 resources will also be deleted permanently and cannot be recovered later:

Name	Resource ID	State
My-Mumbai-IGW	igw-01fc5b0357d295ce8	✅ Available
Private-RouteTable	rtb-093582ad5c000612e	-
Public-RouteTable	rtb-0553451d21e03ccd1	-
-	sg-09b9119c0e257f510	-
Private-Subnet-Mumbai	subnet-08c1547242085bd01	✅ Available

To confirm deletion, type *delete* in the field:

delete

Cancel Delete



