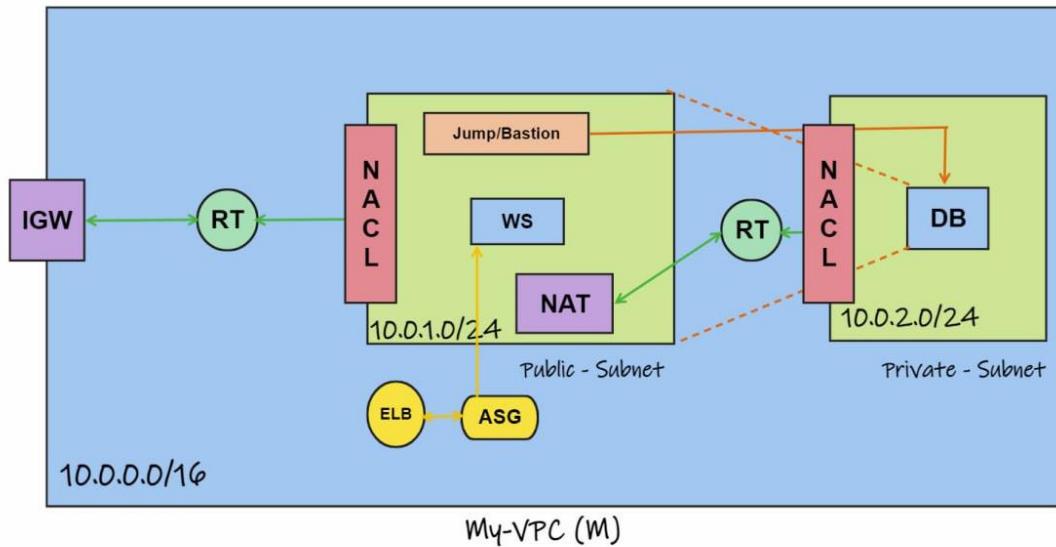


VPC ARCHITECTURE

VPC SERVICE:

VPC means Virtual Private Cloud . It is the service related to Network . Let us see the architecture of this VPC Service.



We have various components in the structure of the VPC, such as:

- Vpc
- Subnets
- IGW
- Route tables
- Web server
- Database Server
- Jump/Bastion Box
- NAT
- ASG
- ELB
- NACL

Let us briefly Understand the components one by one.

1. VPC:

VPC is the main outline of the structure where we create all the components and operate the service.

The CIDR range is 10.0.0.0/16.

2. Subnets:

In VPC we have two kind of subnets they are public and private .By default all the subnets are public at the time of creation .If we have to create a private subnet then first create the public subnet and then

convert the public subnet to the private by enabling the subnet to public IP and then create the Internet Gateway and attach it to the VPC.

3. IGW:

IGW means Internet Gateway .It is used to make the public subnet to private subnet and for internet connection.

4. Route Tables:

We use Route tables to connect one subnet to other and IGW to subnets.

5. Web server:

Web server is the server that produces the services to the user we have 2 ports to the webserver they are ssh and http ports.

6. Database server:

Database server is the private one and have only access to the webserver along with administrator to make the changes in it.

It have only one port called as MYSQL:3306.

7. Jump Box:

Jump box is also called as Bastion box ,it is used to securely connect the webserver to the database server through ssh port.

8. NAT:

NAT means Network Address Translator , It have both public and private IP's and used to get the internet for the Database.

9. ASG:

ASG means Auto Scaling Groups which launches the webserver automatically and attach webservers to Elastic Load Balancer.

To create a ASG we require Launch template, scaling policies and ELB.

10. Elastic Load Balancer:

Elastic load balancer is responsible for creating a valve in the network so that it acts as the common entry point of traffic ,balances the load and routes traffic only to the healthy server.

11. NACL:

NACL means Network Access Control List , we can create a NACL of custom and main .

In this VPC structure we create the elastic load balancer and accommodate it in the launch template of the ASG.

We have given only one server to the ASG along with webserver in the public subnet.

The CIDR ranges of the subnets:

Public subnet – 10.0.1.0/24

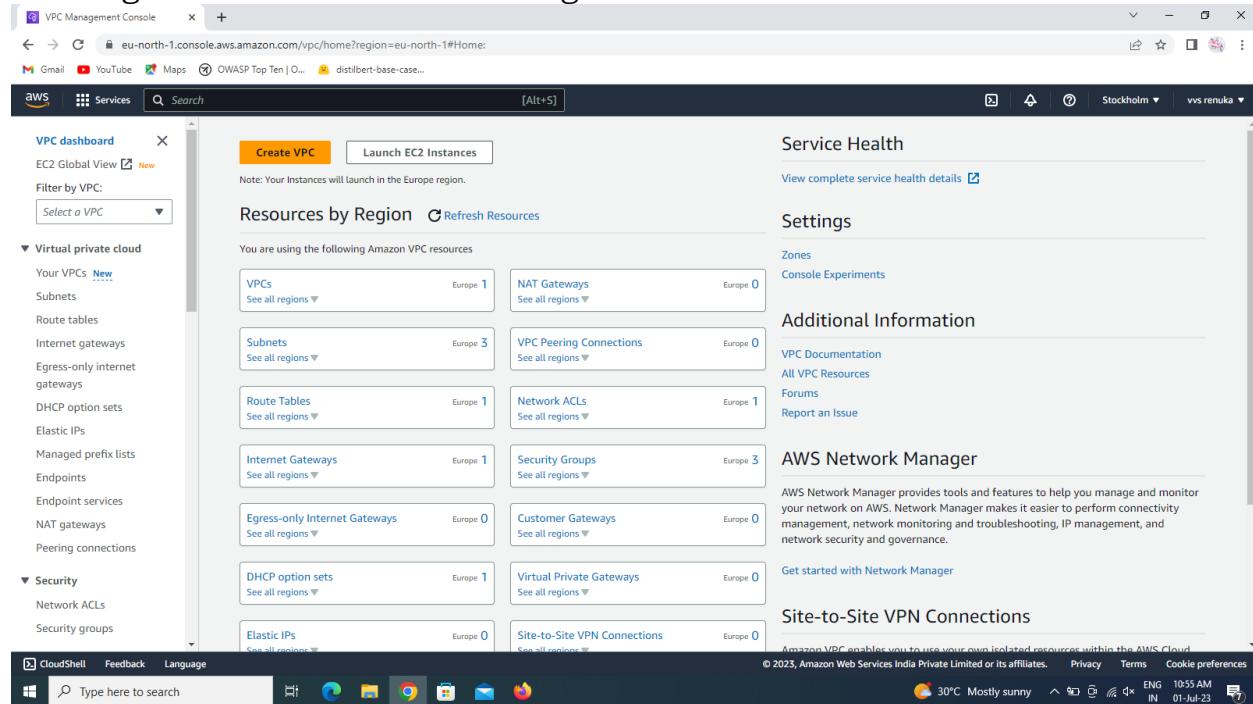
Private subnet – 10.0.2.0/24

CREATION OF VPC STRUCTURE

In creation of the VPC structure there are many steps . Let us see the steps involved in the creation of the VPC structure:

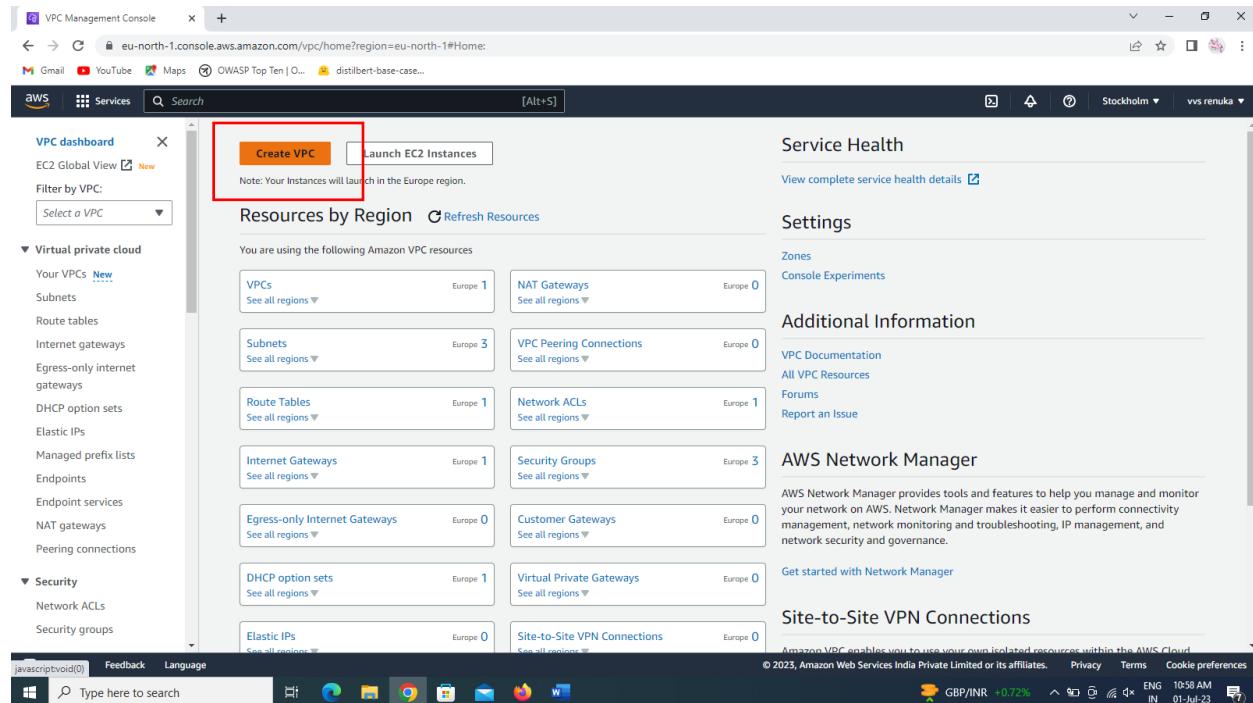
Creation of VPC outer structure

First login to the AWS console and go to VPC service .



The screenshot shows the AWS VPC Management Console dashboard. On the left, a sidebar lists various VPC-related services like EC2 Global View, Virtual private cloud, Security, and CloudShell. The main area displays 'Resources by Region' for the Europe region, showing counts for VPCs (1), Subnets (3), Route Tables (1), Internet Gateways (1), Egress-only Internet Gateways (0), DHCP option sets (1), Elastic IPs (0), NAT Gateways (0), VPC Peering Connections (0), Network ACLs (1), Security Groups (3), Customer Gateways (0), Virtual Private Gateways (0), and Site-to-Site VPN Connections (0). A prominent orange 'Create VPC' button is located at the top center, which is highlighted with a red box.

Select Create VPC to create a new VPC.



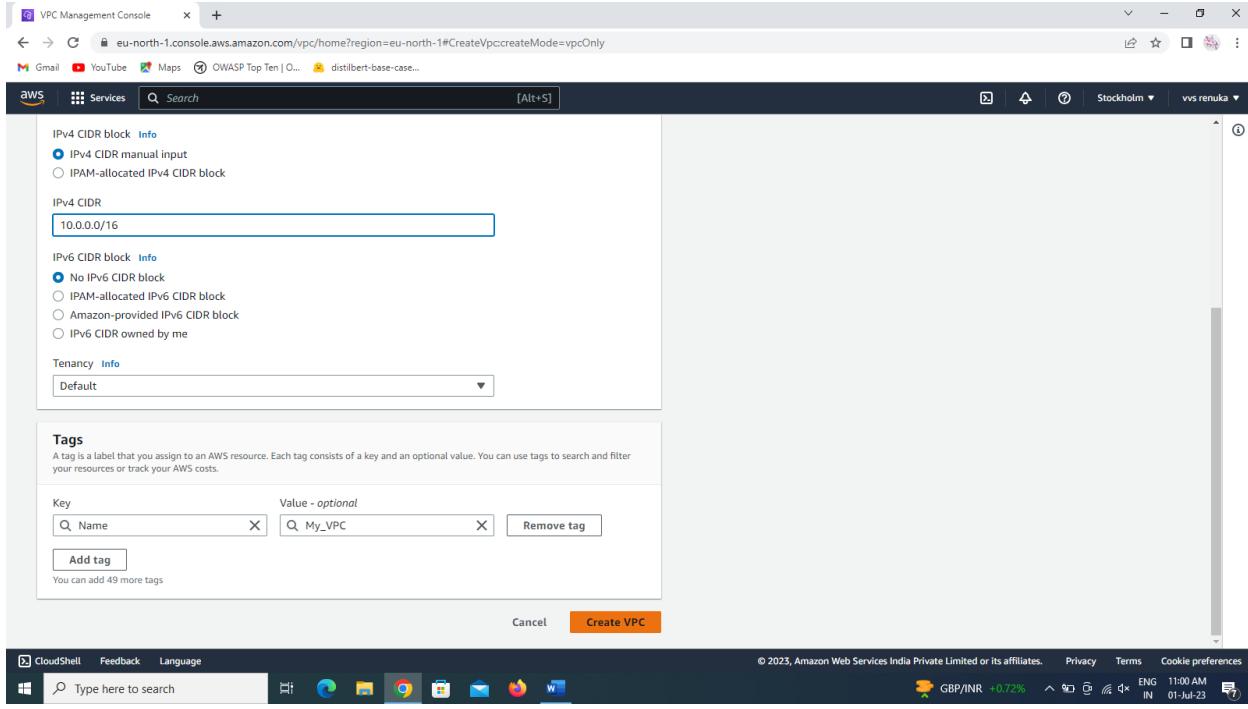
This screenshot shows the 'Create VPC' step in the AWS VPC Management Console. The 'Create VPC' button is highlighted with a red box. The interface includes a search bar, navigation links for EC2 Global View, Services, and a language dropdown set to English (IN). The main content area shows the 'Create VPC' step with a note: 'Note: Your Instances will launch in the Europe region.' Below this, the 'Resources by Region' section for Europe is identical to the one in the previous screenshot, showing 1 VPC, 3 Subnets, etc.

Next click on VPC only because if we select VPC and more it creates the VPC of its own so if we select VPC only we can customize it.

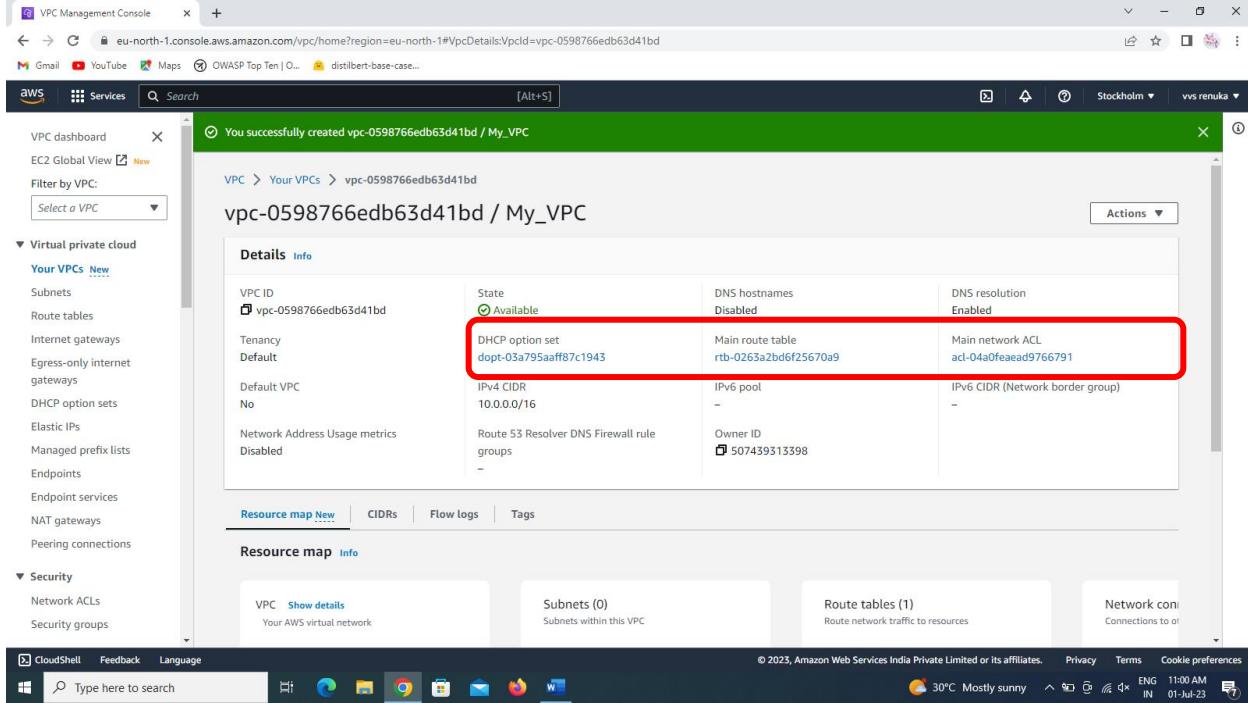
Now give the name to the VPC of your choice here I am giving the name of the VPC as My_VPC.

Also give the CIDR range of the VPC as 10.0.0.0/16 which we have seen earlier in the block diagram of the VPC Structure.

Now select the settings related to IPV6 CIDR as no IPV6 CIDR block because we are creating the VPC only in IPV4.



Now finally all the required columns to create the VPC so click on the create the VPC So we get the VPC created.



When a VPC is created we can see that there are three default things such as DHCP Option Set, Main Route table , Main NACL are created automatically.

Creation of Subnets

To create subnets go to subnets option in the VPC service which is located on the left pane , here we can find that already 3 subnets are created these subnets are related to the default VPC.

The screenshot shows the AWS VPC Management Console with the Subnets page open. The left sidebar shows navigation options like VPC dashboard, EC2 Global View, and various subnets and security settings. The main area displays a table titled "Subnets (3) Info". The table has columns for Name, Subnet ID, State, VPC, IPv4 CIDR, and IPv6 CIDR. The first three rows are highlighted with a red box. The "Actions" button is visible at the top right of the table.

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
-	subnet-039b7aa9516723cdb	Available	vpc-0c805c16989d9ed81	172.31.32.0/20	-
-	subnet-0b4f619a7fb478eca	Available	vpc-0c805c16989d9ed81	172.31.0.0/20	-
-	subnet-06c4f15d42e4feb4	Available	vpc-0c805c16989d9ed81	172.31.16.0/20	-

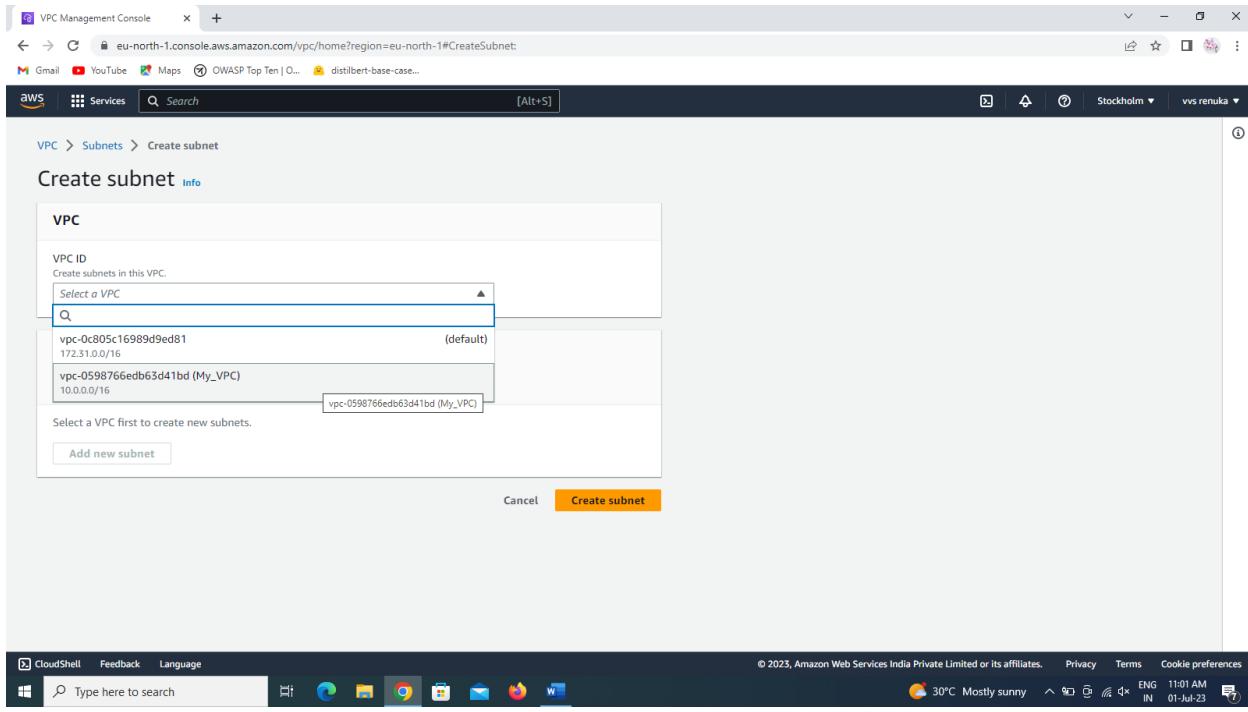
To create the subnets in MY_VPC select create subnet option which is on the top right of the console.

The screenshot shows the AWS VPC Management Console with the Subnets page open. The left sidebar shows navigation options like VPC dashboard, EC2 Global View, and various subnets and security settings. The main area displays a table titled "Subnets (3) Info". The "Create subnet" button is highlighted with a red box at the top right of the table header. The table has columns for Name, Subnet ID, State, VPC, IPv4 CIDR, and IPv6 CIDR. The first three rows are listed below the header.

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
-	subnet-039b7aa9516723cdb	Available	vpc-0c805c16989d9ed81	172.31.32.0/20	-
-	subnet-0b4f619a7fb478eca	Available	vpc-0c805c16989d9ed81	172.31.0.0/20	-
-	subnet-06c4f15d42e4feb4	Available	vpc-0c805c16989d9ed81	172.31.16.0/20	-

After clicking on the create subnet we get the page asking to select the VPC in which we have to create the subnets.

Now select the VPC in which we have to create the subnets to complete the VPC Structure.



CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

30°C Mostly sunny ENG IN 11:01 AM 01-Jul-23

After the selection of the VPC we get the columns to select the qualities required in our subnets that we are going to be created in the VPC . Here we create the 2 subnets one is public subnet and other one is private subnet but by default both the subnets are private later we make the required subnet as public subnet.

First subnet is Public Subnet

For this first give the name of the subnet as 10.0.1.0/24-1a-PUB

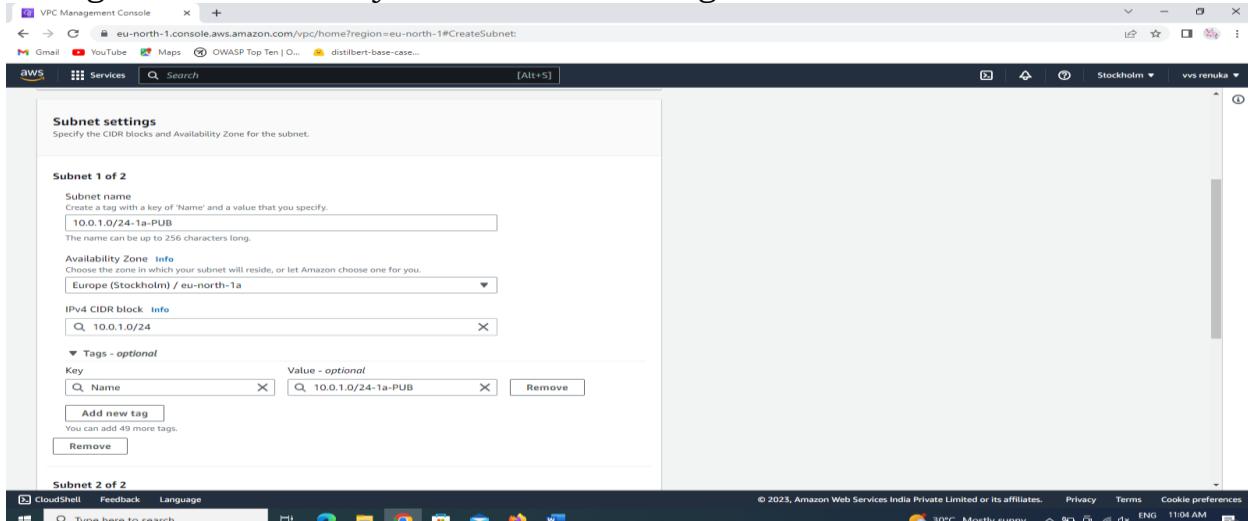
This is the format to easily identify the subnet , in the name of the subnet there are three regions they are CIDR range, Availability zone , type of the subnet.

CIDR range = 10.0.1.0/24

Availability zone = 1a

Type of the subnet = Public

Next give the Availability zone and CIDR range.



CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

30°C Mostly sunny ENG IN 11:04 AM 01-Jul-23

As we have created the public subnet like wise we have create the private subnet

The screenshot shows the AWS VPC Management Console with a modal window titled "Subnet 2 of 2". The form fields include:

- Subnet name:** 10.0.2.0/24-1b-PVT
- Availability Zone:** Europe (Stockholm) / eu-north-1b
- IPv4 CIDR block:** 10.0.2.0/24
- Tags - optional:** A single tag named "Name" with value "10.0.2.0/24-1b-PVT".

At the bottom right of the modal is a yellow "Create subnet" button.

We can see that the 2 subnets are created successfully but the subnet that we have created as public is really not a public subnet it is just a public subnet for name .To make this subnet as public we have to enable the public and then create a IGW and connect it to the subnet.

The screenshot shows the AWS VPC Management Console with a green success message at the top: "You have successfully created 2 subnets: subnet-0123c7f44c7a91533, subnet-0f723c804d4eca1a3". Below this is a table titled "Subnets (2) Info" showing the following data:

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
10.0.2.0/24-1b-PVT	subnet-0f723c804d4eca1a3	Available	vpc-0598766edb63d41bd M...	10.0.2.0/24	-
10.0.1.0/24-1a-PUB	subnet-0123c7f44c7a91533	Available	vpc-0598766edb63d41bd M...	10.0.1.0/24	-

At the bottom left, there is a "Select a subnet" dropdown menu.

Making the public subnet as public

Select the public subnet and then go to actions and select edit subnet associations and then enable the ipv4 ,save changes.

You have successfully created 2 subnets: subnet-0123c7f44c7a91533, subnet-0f723c804d4eca1a3

Subnets (1/2) Info

Name	Subnet ID	State	VPC	IPv4 CIDR
10.0.2.0/24-1b-PVT	subnet-0f723c804d4eca1a3	Available	vpc-0598766edb63d41bd M...	10.0.2.0/24
10.0.1.0/24-1a-PUB	subnet-0123c7f44c7a91533	Available	vpc-0598766edb63d41bd M...	10.0.1.0/24

subnet-0123c7f44c7a91533 / 10.0.1.0/24-1a-PUB

Details

Subnet ID	Subnet ARN	State	IPv4 CIDR
subnet-0123c7f44c7a91533	arn:aws:ec2:eu-north-	Available	10.0.1.0/24

Edit subnet settings

Subnet

Subnet ID	Name
subnet-0123c7f44c7a91533	10.0.1.0/24-1a-PUB

Auto-assign IP settings

Enable the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

Enable auto-assign public IPv4 address

Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch Info

Enable resource name DNS AAAA record on launch Info

Hostname type

Resource name
 IP name

To create an Internet Gateway select the internet gateway option.

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

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-0d9b42d91ff2a34c3	Attached	vpc-0c805c16989d9ed81	507439313398

igw-0d9b42d91ff2a34c3

[Details](#) [Tags](#)

Details

Internet gateway ID igw-0d9b42d91ff2a34c3	State Attached	VPC ID vpc-0c805c16989d9ed81	Owner 507439313398
--	-------------------	---------------------------------	-----------------------

Give name to Internet gateway as IGW and click on create.

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.
IGW

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 Name	Value - optional IGW
-------------	-------------------------

Add new tag
You can add 49 more tags.

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

Now we can see that the IGW is created.

VPC Management Console

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#InternetGateway:internetGatewayId=igw-04ffb2475d8ea1b77

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

The following internet gateway was created: igw-04ffb2475d8ea1b77 - IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC

VPC dashboard

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs New Subnets Route tables

Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections

Security Network ACLs Security groups

CloudShell Feedback Language

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

30°C Mostly sunny ENG IN 11:07 AM 01-Jul-23

igw-04ffb2475d8ea1b77 / IGW

Details Info

Internet gateway ID: igw-04ffb2475d8ea1b77 State: Detached VPC ID: - Owner: 507439313398

Tags

Search tags

Key Value

Name: IGW

Manage tags

Now attach the IGW to the VPC .

Internet gateways | VPC Manager

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#igws:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Internet gateways (1/2) Info

Filter internet gateways

Name	Internet gateway ID	State	VPC ID
IGW	igw-04ffb2475d8ea1b77	Detached	-
-	igw-0d9b42d91ff2a34c3	Attached	vpc-0c805c16989d9ed81

Actions ▾ Create internet gateway

View details

Attach to VPC

Detach from VPC

Manage tags

Delete internet gateway

igw-04ffb2475d8ea1b77 / IGW

Details Tags

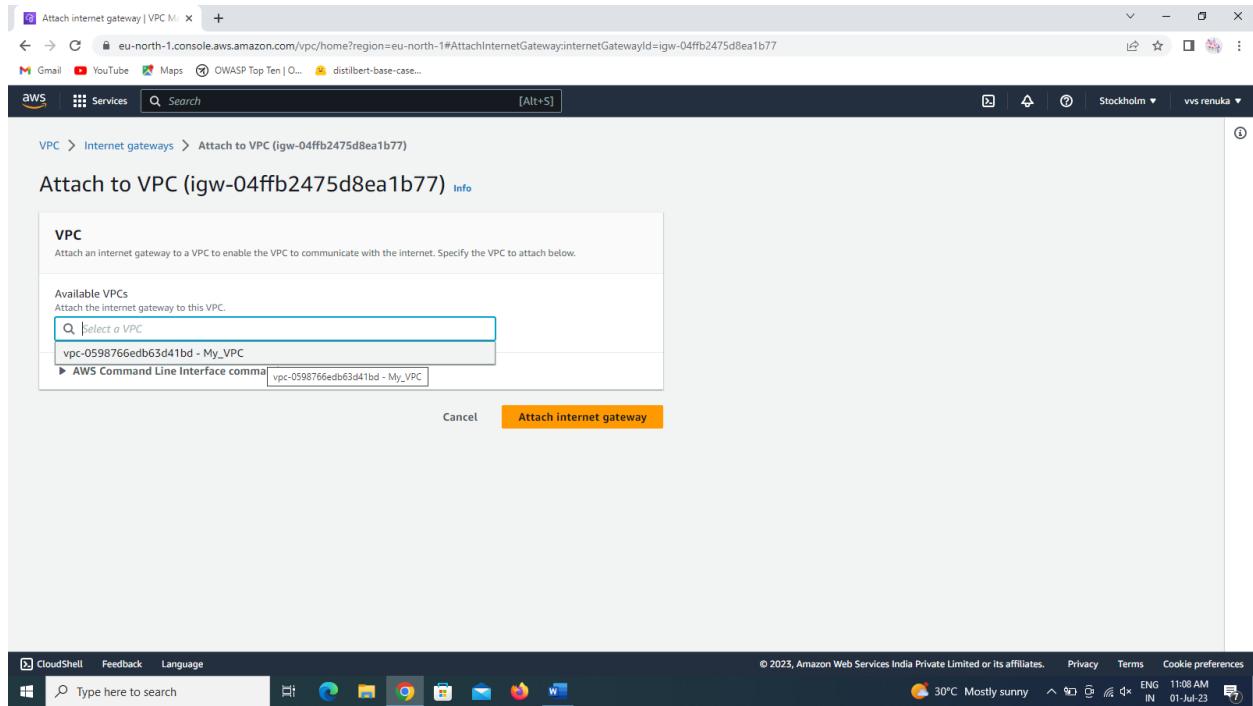
Internet gateway ID: igw-04ffb2475d8ea1b77 State: Detached VPC ID: - Owner: 507439313398

CloudShell Feedback Language

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

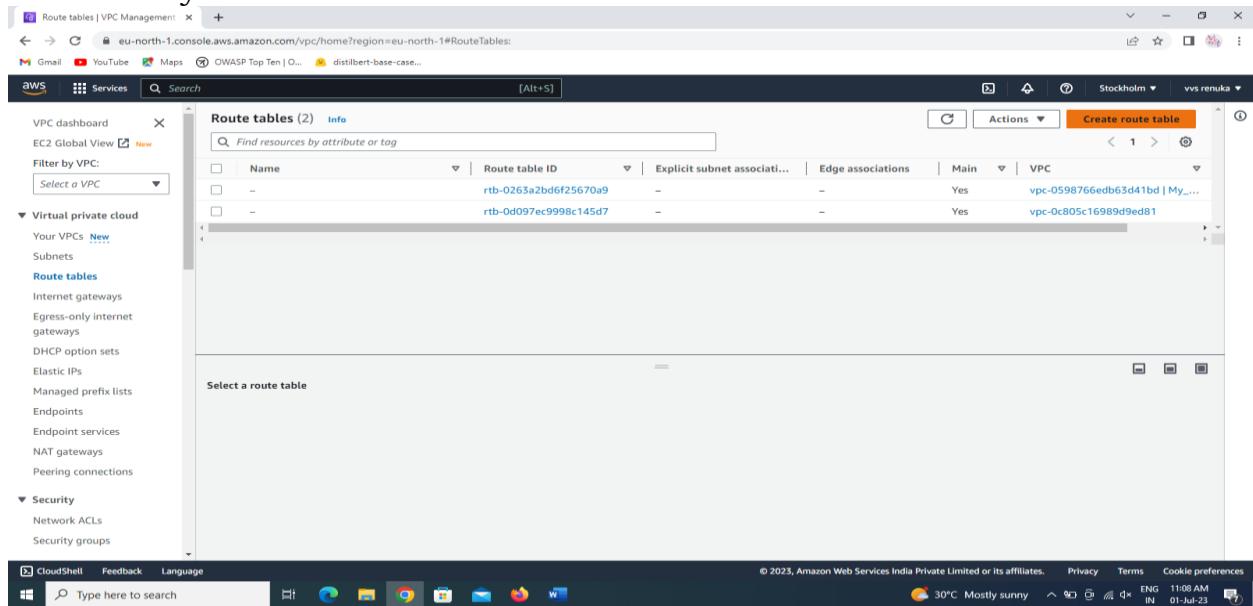
30°C Mostly sunny ENG IN 11:07 AM 01-Jul-23



We have successfully created the internet gate way and attached it to the subnet to make it public for this we require to create a route table when a VPC is created a Route table is created which is main route table but to connect IGW to the public subnet we require a custom route table.

After creating the route table edit the subnet associations and add the public subnet to it but other end of the route table is not connected for this we require to the route of the IGW to the route table.

Now the connection between the subnet and IGW through RT was established successfully.



VPC Management Console

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-08c7634dd89ad9a92

Services Search [Alt+S]

VPC > Route tables > rtb-08c7634dd89ad9a92 > 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
10.0.2.0/24-1b-PVT	subnet-0f723c804d4eca1a3	10.0.2.0/24	-	Main (rtb-0263a2bd6f25670a9)
10.0.1.0/24-1a-PUB	subnet-0123c7f44c7a91533	10.0.1.0/24	-	Main (rtb-0263a2bd6f25670a9)

Selected subnets

subnet-0123c7f44c7a91533 / 10.0.1.0/24-1a-PUB X

Cancel Save associations

VPC Management Console

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#EditRoutes:RouteTableId=rtb-08c7634dd89ad9a92

Services Search [Alt+S]

VPC > Route tables > rtb-08c7634dd89ad9a92 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-04ffb2475d8ea1b77	-	No

Add route Remove

Cancel Preview Save changes

Creation of webserver

We have to create the webserver in the public subnet for this we have go to ec2 service and then create an instance named as webserver having the linux os , t3.micro as instance type . here I have created a new keypair named as ws and the security group is also named as ws for easy identification. Until we have

seen only selection of security groups, security group rules but here we can see the selection of VPC and subnet in which we are going to create the webserver.

The screenshot shows the AWS EC2 Management Console Home page. On the left, there's a navigation sidebar with sections like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area displays 'Resources' with counts for Instances (running), Auto Scaling Groups, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes. To the right, there's a panel for 'Account attributes' showing supported platforms (VPC), Default VPC (vpc-0c805c16989d9ed81), and other settings like EBS encryption and EC2 Serial Console. Below that is an 'Explore AWS' section with links to cost reduction tips and GuardDuty Malware Protection.

The screenshot shows the 'Launch an instance' wizard. It starts with a summary step where you can enter the number of instances (set to 1). Then it moves to the 'Name and tags' step, where you can provide a name (e.g., 'webserver') and add tags. Next is the 'Application and OS Images (Amazon Machine Image)' step, where you can search for AMIs or use the 'Quick Start' feature. Finally, it reaches the 'Summary' step, which includes a note about the free tier (750 hours of t2.micro usage) and a prominent 'Launch instance' button. The bottom of the screen shows the standard AWS navigation bar with CloudShell, Feedback, Language, and search.

Launch an instance | EC2 Manager

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

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

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

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-0c858d4d1feca5370 (64-bit (x86), uefi-preferred) / ami-066feb9d7da9ba4b3 (64-bit (Arm), uefi) Virtualization: hvm ENA enabled: true Root device type: ebs Free tier eligible

Description

Amazon Linux 2023 AMI 2023.1.20230629.0 x86_64 HVM kernel-6.1

Architecture Boot mode AMI ID Verified provider

64-bit (x86) uefi-preferred ami-0c858d4d1feca5370

Summary

Number of instances Info 1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.1.2...read more ami-0c858d4d1feca5370

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Cancel Launch instance Review commands

Launch an instance | EC2 Manager

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

Instance type

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

All generations Compare instance types

Key pair (login)

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

Key pair name - required Select Create new key pair

Network settings

Network Info vpc-0c805c16989d9ed81 Subnet Info

Edit

Summary

Number of instances Info 1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.1.2...read more ami-0c858d4d1feca5370

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Cancel Launch instance Review commands

The screenshot shows the AWS EC2 Launch Instance wizard. On the left, under 'Network settings', a VPC is selected (vpc-0598766edb63d41bd (My_VPC) 10.0.0.0/16). A subnet is chosen (subnet-0123c7f44c7a91533), and 'Auto-assign public IP' is set to 'Enable'. Under 'Firewall (security groups)', a new security group named 'ws' is being created. The 'Description' field contains 'ws'. On the right, the 'Summary' section shows 1 instance, the AMI (Amazon Linux 2023 AMI 2023.1.2...), the instance type (t3.micro), and storage (1 volume(s) - 8 GiB). Buttons for 'Launch instance' and 'Review commands' are at the bottom.

The screenshot shows the continuation of the EC2 Launch Instance wizard. On the left, under 'Inbound Security Group Rules', a rule is defined: 'Security group rule 1 (TCP, 22, 49.37.154.210/32, admin)'. The 'Type' is 'ssh', 'Protocol' is 'TCP', and 'Port range' is '22'. The 'Source type' is 'My IP'. The 'Name' is 'Add CDR, prefix list or security' and the 'Description' is 'admin'. On the right, the 'Summary' section remains the same, showing 1 instance, the AMI, instance type, and storage. Buttons for 'Launch instance' and 'Review commands' are at the bottom.

Here we create the webserver statically so we have to paste the bin bash commands.

Launch an instance | EC2 Manager

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Source type Info Name Info Description - optional Info
My IP Add CIDR, prefix list or security admin
49.37.154.210/32

▼ Security group rule 2 (TCP, 80, Multiple sources, public) Remove

Type Info Protocol Info Port range Info
HTTP TCP 80

Source type Info Source Info Description - optional Info
Anywhere Add CIDR, prefix list or security public
0.0.0.0/0 ::/0

⚠ 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 Advanced network configuration

▼ Configure storage Info Advanced

CloudShell Feedback Language ws.pem

Type here to search Show all

30°C Mostly sunny ENG IN 11:24 AM 01-Jul-23

Launch instance Review commands

Launch an instance | EC2 Manager

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

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 Advanced network configuration

▼ Configure storage Info Advanced

CloudShell Feedback Language ws.pem

Type here to search Show all

30°C Mostly sunny ENG IN 11:24 AM 01-Jul-23

1x 8 GiB gp3 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

0 x File systems Edit

► Advanced details Info

Number of instances Info 1

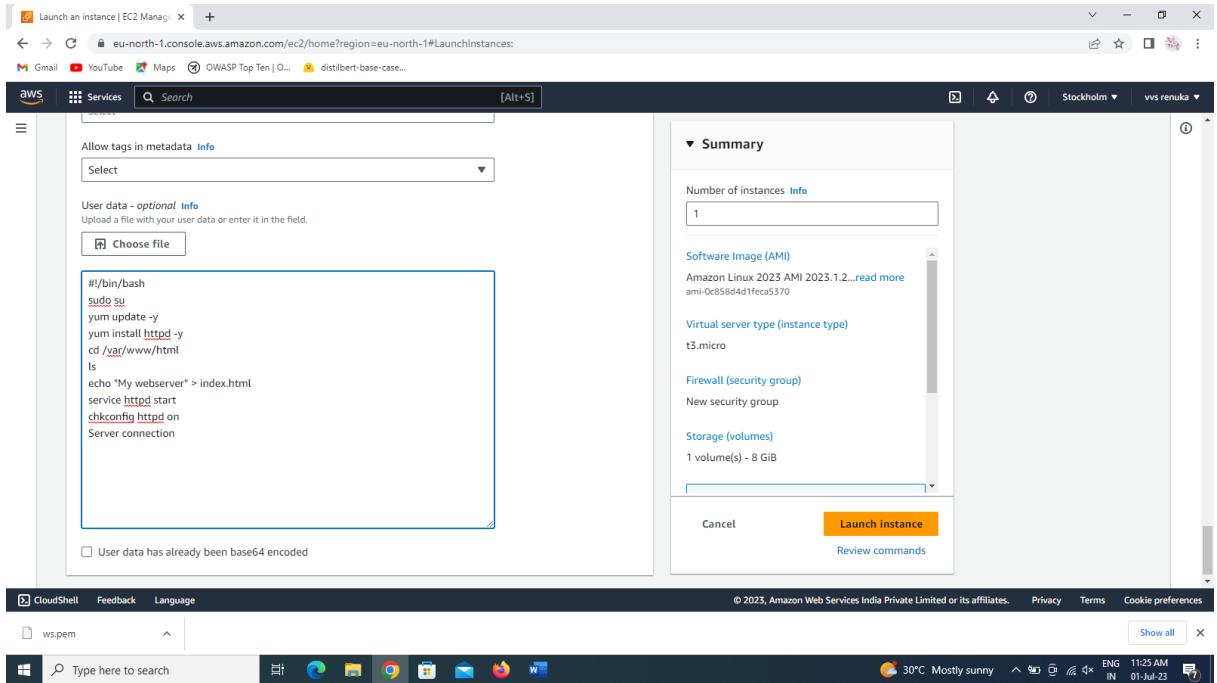
Software Image (AMI) Amazon Linux 2023 AMI 2023.1.2...read more ami-0c858d4dfceca5370

Virtual server type (instance type) t3.micro

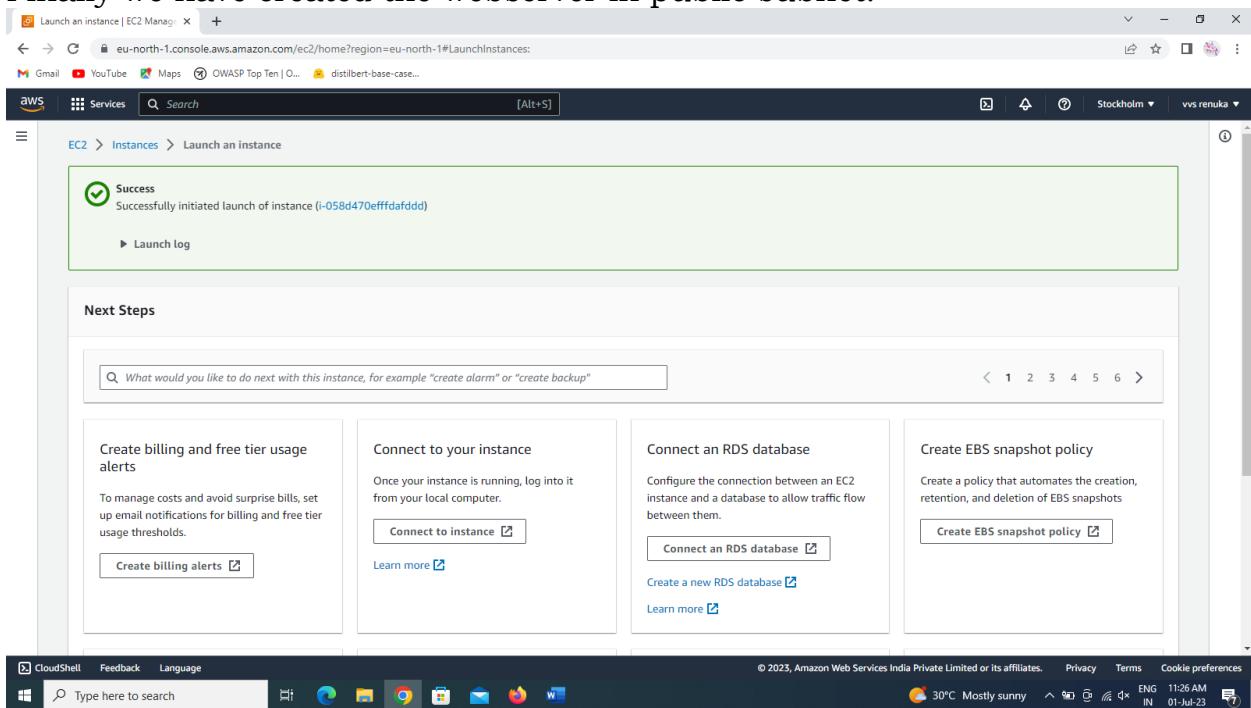
Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 8 GiB

Cancel Launch instance Review commands



Finally we have created the webserver in public subnet.



Now we also have to create the Data base server in the private subnet. Data base subnet also have same specifications related to os and type but name ,vpc ,subnet ,security group and security group rules are changed.

EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

following the simple steps below.

Name and tags [Info](#)

Name Add additional tags

Application and OS Images (Amazon Machine Image) [Info](#)

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

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

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Li [Browse more AMIs](#)

Amazon Machine Image (AMI)

CloudShell Feedback Language Type here to search © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 30°C Mostly sunny ENG IN 11:27 AM 01-Jul-23

Number of instances [Info](#) 1

Software Image (AMI) Amazon Linux 2023 AMI 2023.1.2... [read more](#) ami-0c858d4d1feca5370

Virtual server type (instance type) t3.micro

Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Cancel Launch instance Review commands

EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-0c858d4d1feca5370 (64-bit (x86), uefi-preferred) / ami-066feb9d7da9ba4b3 (64-bit (Arm), uefi) Free tier eligible Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.1.20230629.0 x86_64 HVM kernel-6.1

Architecture 64-bit (x86) Boot mode uefi-preferred AMI ID ami-0c858d4d1feca5370 Verified provider

Instance type [Info](#)

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

All generations Compare instance types

Number of instances [Info](#) 1

Software Image (AMI) Amazon Linux 2023 AMI 2023.1.2... [read more](#) ami-0c858d4d1feca5370

Virtual server type (instance type) t3.micro

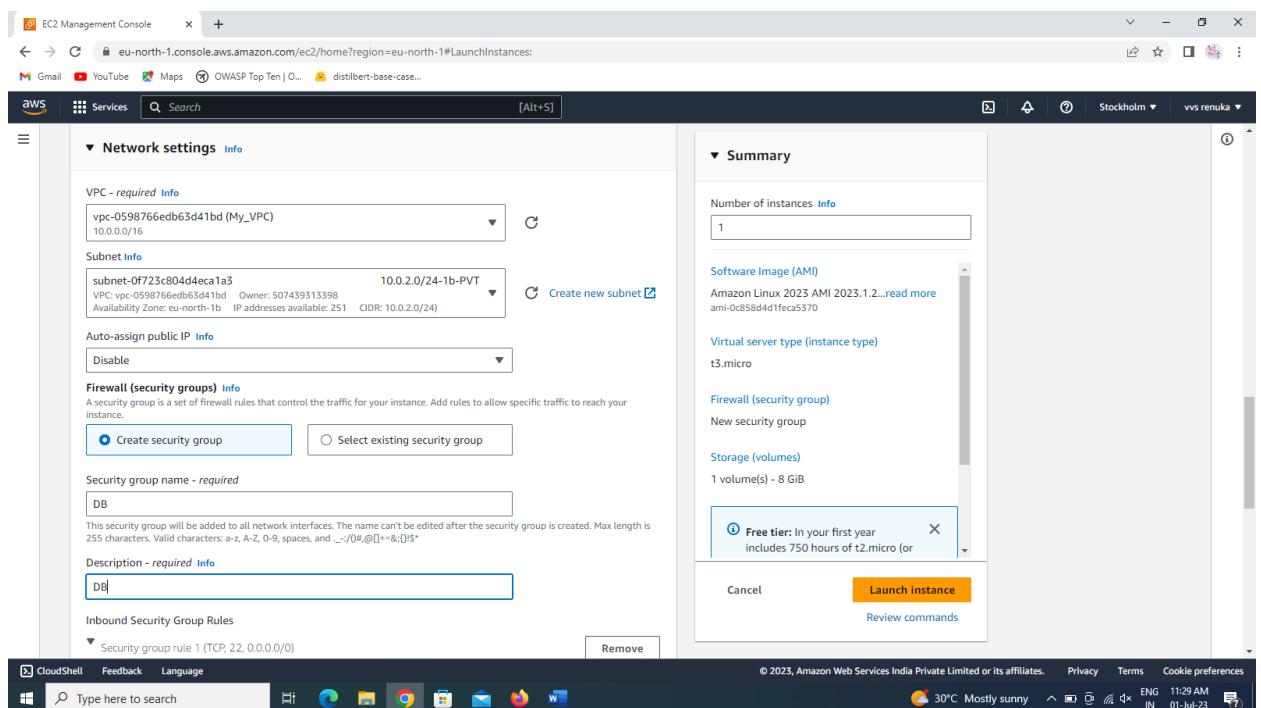
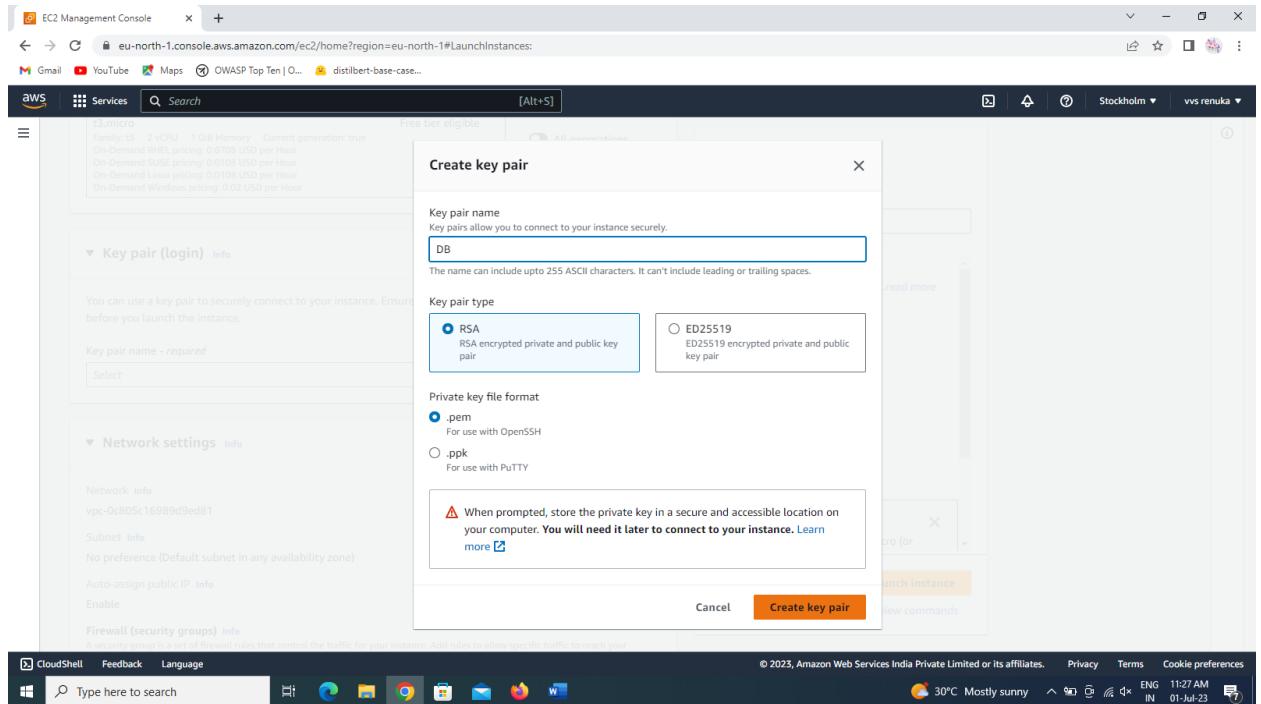
Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Cancel Launch instance Review commands

CloudShell Feedback Language Type here to search © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 30°C Mostly sunny ENG IN 11:27 AM 01-Jul-23



EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

aws Services Search [Alt+S]

Security group name - required
DB

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
DB

Inbound Security Group Rules

Security group rule 1 (TCP, 3306, 10.0.1.0/24, PUB-SN-CIDR)

Type Info Protocol Info Port range Info
MySQL/Aurora TCP 3306

Source type Info Source Info Description - optional Info
Custom Add CIDR, prefix list or security PUB-SN-CIDR
10.0.1.0/24 X

Add security group rule Advanced network configuration

Configure storage Info Advanced

CloudShell Feedback Language Type here to search

Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023.1.2...read more
ami-0c858d4dfeca5370

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Cancel Launch instance Review commands

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences
30°C Mostly sunny ENG IN 11:32 AM 01-Jul-23

EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

aws Services Search [Alt+S]

Description - required Info
DB

Inbound Security Group Rules

Security group rule 1 (TCP, 3306, 10.0.1.0/24, PUB-SN-CIDR)

Type Info Protocol Info Port range Info
MySQL/Aurora TCP 3306

Source type Info Source Info Description - optional Info
Custom Add CIDR, prefix list or security PUB-SN-CIDR
10.0.1.0/24 X

Security group rule 2 (TCP, 22, 49.37.154.210/32, admin)

Type Info Protocol Info Port range Info
ssh TCP 22

Source type Info Name Info Description - optional Info
My IP Add CIDR, prefix list or security admin
49.37.154.210/32 X

Add security group rule Advanced network configuration

CloudShell Feedback Language Type here to search

Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023.1.2...read more
ami-0c858d4dfeca5370

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Cancel Launch instance Review commands

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences
30°C Mostly sunny ENG IN 11:33 AM 01-Jul-23

After creation of servers in the let us check whether the webserver is working or not.

Instances | EC2 Management Con

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#instances:

New EC2 Experience Tell us what you think

aws Services Search [Alt+S]

Instances (1/2) Info

Find instance by attribute or tag (case-sensitive)

Name Instance ID Instance state Instance type Status check Alarm status Availability Zone Public IPv4 DNS

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
webserver	i-058d470efffdafddd	Running	t3.micro	2/2 checks passed	No alarms	+ eu-north-1a	-
Database	i-06a7c263aa5e3adce	Running	t3.micro	Initializing	No alarms	+ eu-north-1b	-

Instance: i-058d470efffdafddd (webserver)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary Info

Instance ID i-058d470efffdafddd (webserver)	Public IPv4 address 149.223.7 open address	Private IPv4 addresses 10.0.1.160
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-10-0-1-160.eu-north-1.compute.internal	Private IP DNS name (IPv4 only) ip-10-0-1-160.eu-north-1.compute.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t3.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address 149.223.7 [Public IP]	VPC ID vpc-0598766edb63d41bd (My_VPC)	

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

30°C Mostly sunny ENG IN 11:35 AM 01-Jul-23

Instances | EC2 Management Con

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#instances:

New EC2 Experience Tell us what you think

aws Services Search [Alt+S]

Instances (1/2) Info

Find instance by attribute or tag (case-sensitive)

Name Instance ID Instance state Instance type Status check Alarm status Availability Zone Public IPv4 DNS

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
webserver	i-058d470efffdafddd	Running	t3.micro	2/2 checks passed	No alarms	+ eu-north-1a	-
Database	i-06a7c263aa5e3adce	Running	t3.micro	Initializing	No alarms	+ eu-north-1b	-

Instance: i-058d470efffdafddd (webserver)

Details Security Networking Storage Status checks Monitoring Tags

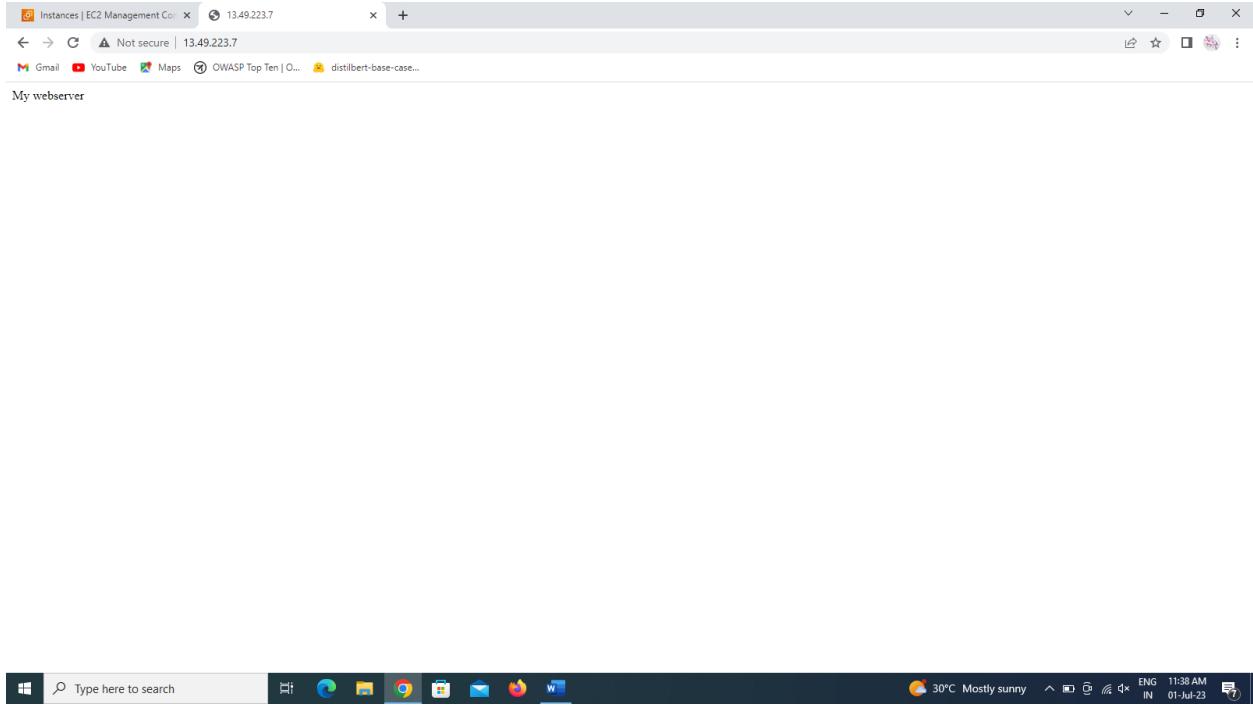
Instance summary Info

Instance ID i-058d470efffdafddd (webserver)	Public IPv4 address copied 149.223.7 open address	Private IPv4 addresses 10.0.1.160
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-10-0-1-160.eu-north-1.compute.internal	Private IP DNS name (IPv4 only) ip-10-0-1-160.eu-north-1.compute.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t3.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address 149.223.7 [Public IP]	VPC ID vpc-0598766edb63d41bd (My_VPC)	

CloudShell Feedback Language

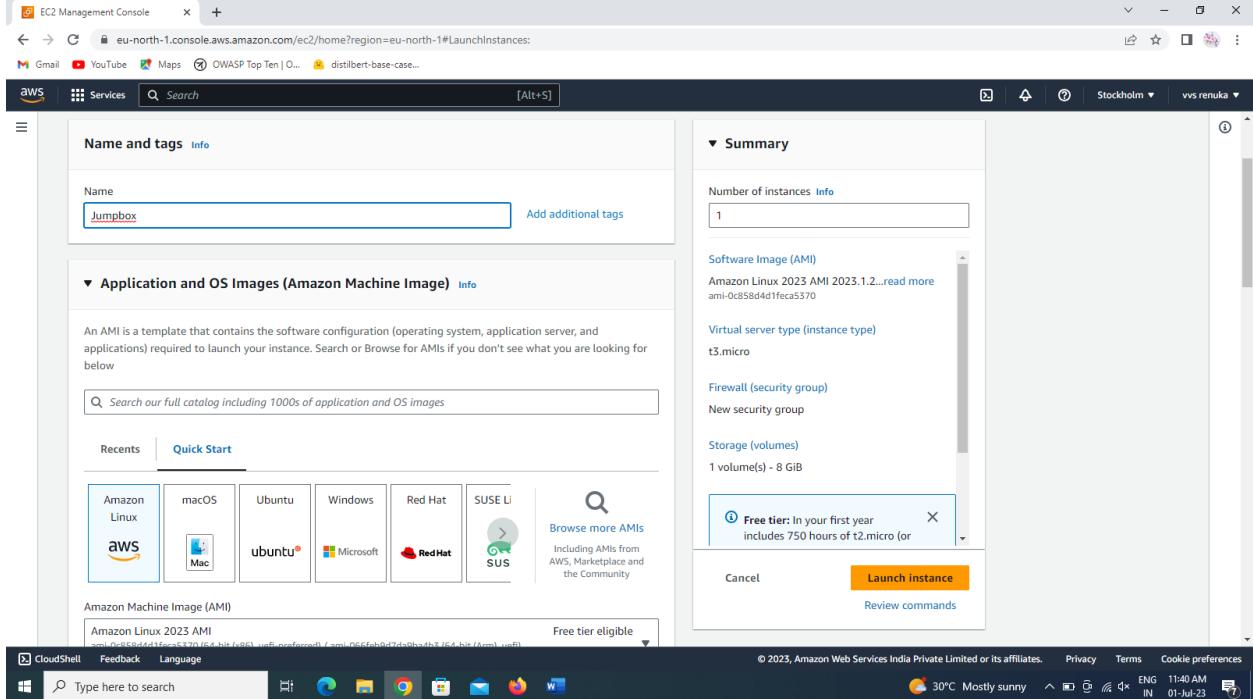
© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

30°C Mostly sunny ENG IN 11:38 AM 01-Jul-23



We can see here that the webserver is working so we have to connect the database and webserver for this we have to create the jump or bastion box so that the connection is secured.

For creation of jump box we have to create an instance named as jump box and linux os with t3.micro as instance type same as webserver instance but only the security group rules are changed.



EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI
ami-0c858d4d1feca5370 (64-bit (x86), uefi-preferred) / ami-066feb9d7da9ba4b3 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.1.20230629.0 x86_64 HVM kernel-6.1

Architecture: 64-bit (x86) Boot mode: uefi-preferred AMI ID: ami-0c858d4d1feca5370 Verified provider

Instance type

t3.micro Family: t3 2 vCPU 1 GiB Memory Current generation: true Free tier eligible All generations Compare instance types

Key pair (login)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair

CloudShell Feedback Language Type here to search

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.1.2... read more
ami-0c858d4d1feca5370

Virtual server type (instance type): t3.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Cancel Launch instance Review commands

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 30°C Mostly sunny ENG IN 11:40 AM 01-Jul-23

EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Instance type

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

Key pair (login)

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

Key pair name - required Select

Create key pair

Key pair name: jump Key pairs allow you to connect to your instance securely. The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type: RSA RSA encrypted private and public key pair ED25519 ED25519 encrypted private and public key pair

Private key file format: .pem For use with OpenSSH .ppk For use with PuTTY

When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more

Cancel Create key pair

CloudShell Feedback Language Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 30°C Mostly sunny ENG IN 11:40 AM 01-Jul-23

The screenshot shows the AWS EC2 Management Console interface. On the left, the 'Network settings' section is visible, showing a selected VPC (vpc-0598766edb63d41bd) and a subnet (subnet-0123cf44c7a91533). The 'Security group' section is expanded, showing a new security group named 'jump'. In the 'Inbound Security Group Rules' section, there is one rule defined: 'Security group rule 1 (TCP, 22, 49.37.154.210/32, admin)'. The 'Configure storage' section shows a 1x 8 GiB gp3 volume. On the right, the 'Summary' panel shows 'Number of instances' set to 1, using the 'Amazon Linux 2023 AMI 2023.1.2...' software image, and the 'Virtual server type' is t3.micro. The 'Launch instance' button is highlighted in orange.

Now copy the private ip address of the jump box and paste in the security groups inbound rules of the database server.

EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#instances:

New EC2 Experience

Instances (1/3) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
webserver	i-058d470efffdafddd	Running	t3.micro	2/2 checks passed	No alarms	+ eu-north-1a	-
Jumpbox	i-0074e708acea3ce9c	Running	t3.micro	Initializing	No alarms	+ eu-north-1a	-
Database	i-06a7c263aa5e3adce	Running	t3.micro	2/2 checks passed	No alarms	+ eu-north-1b	-

Instance: i-0074e708acea3ce9c (Jumpbox)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary Info

Instance ID i-0074e708acea3ce9c (Jumpbox)	Public IPv4 address 13.53.182.58 open address	Instance state Running	Private IP DNS name (IPv4 only) ip-10-0-1-223.eu-north-1.compute.internal	Instance type t3.micro	Elastic IP addresses -
IPv6 address -	Instance state Running	Private IP DNS name (IPv4 only) ip-10-0-1-223.eu-north-1.compute.internal	VPC ID vpc-0598766edb63d41bd (My_VPC)	VPC ID vpc-0598766edb63d41bd (My_VPC)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Hostname type IP name: ip-10-0-1-223.eu-north-1.compute.internal	Answer private resource DNS name -	Instance type t3.micro	VPC ID vpc-0598766edb63d41bd (My_VPC)	VPC ID vpc-0598766edb63d41bd (My_VPC)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address 13.53.182.58 [Public IP]	Public IPv4 address 13.53.182.58 open address	Private IP DNS name (IPv4 only) ip-10-0-1-223.eu-north-1.compute.internal	Public IPv4 DNS -	Public IPv4 DNS -	Public IPv4 DNS -

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

30°C Mostly sunny ENG IN 11:44 AM 01-Jul-23

EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#instances:

New EC2 Experience

Instances (1/3) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
webserver	i-058d470efffdafddd	Running	t3.micro	2/2 checks passed	No alarms	+ eu-north-1a	-
Jumpbox	i-0074e708acea3ce9c	Running	t3.micro	Initializing	No alarms	+ eu-north-1a	-
Database	i-06a7c263aa5e3adce	Running	t3.micro	2/2 checks passed	No alarms	+ eu-north-1b	-

Instance: i-06a7c263aa5e3adce (Database)

Details Security Networking Storage Status checks Monitoring Tags

Security details

IAM Role -	Owner ID 507439313398	Launch time Sat Jul 01 2023 11:34:21 GMT+0530 (India Standard Time)
Security groups sg-053004dd67273125f (DB)		

Inbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0a4acf15e2544db01	22	TCP	49.37.154.210/32	DB
-	-	7700	TCP	10.0.1.0/1	DB

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

30°C Mostly sunny ENG IN 11:44 AM 01-Jul-23

EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#SecurityGroup:securityGroupId=sg-053004dd67273125f

aws Services Search [Alt+S]

EC2 > Security Groups > sg-053004dd67273125f - DB

sg-053004dd67273125f - DB

Details

Security group name	sg	Description	VPC ID
DB	sg-053004dd67273125f	DB	vpc-0598766edb63d41bd
Owner	507439313398	Inbound rules count	2 Permission entries
			Outbound rules count 1 Permission entry

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range
sg-0a4ac1f3e2544db01	SSH	TCP	22	Custom	10.0.1.223/32
sgr-07ef4db1b27c67c76	MySQL/Aurora	TCP	3306	Custom	10.0.1.0/24

EC2 Management Console

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-053004dd67273125f

aws Services Search [Alt+S]

EC2 > Security Groups > sg-053004dd67273125f - DB > Edit inbound rules

Edit inbound rules [Info](#)

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

Inbound rules [Info](#)

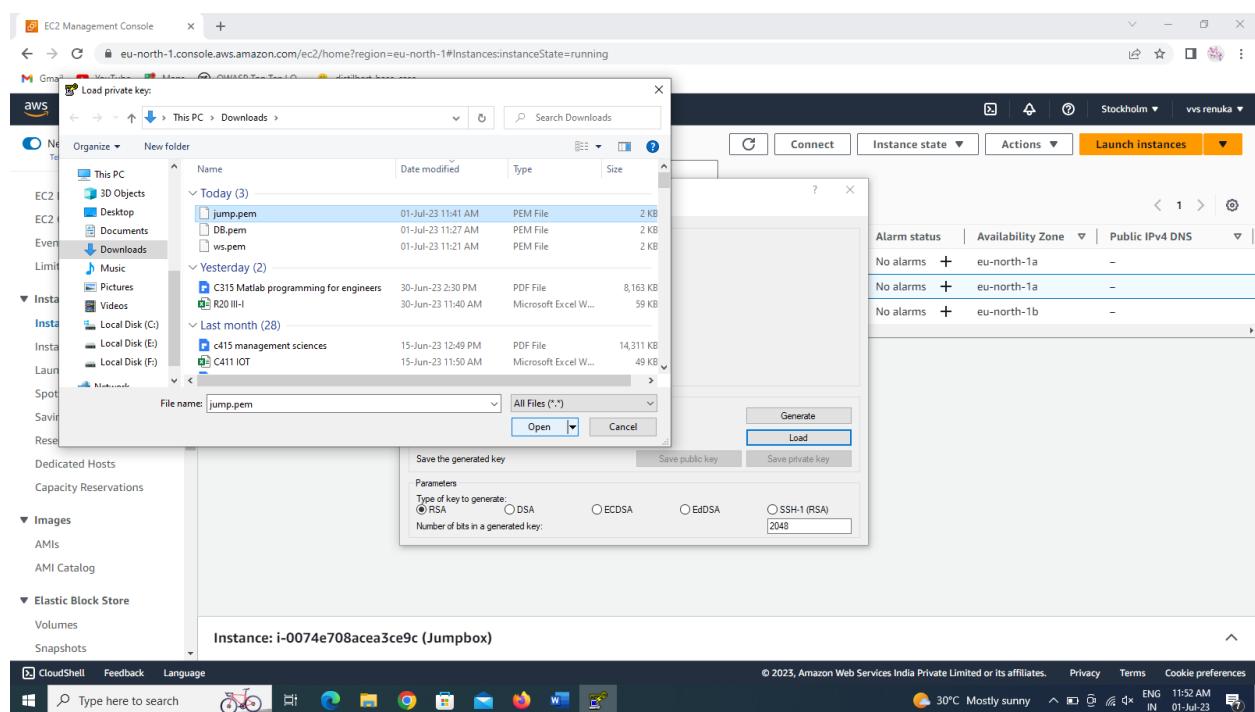
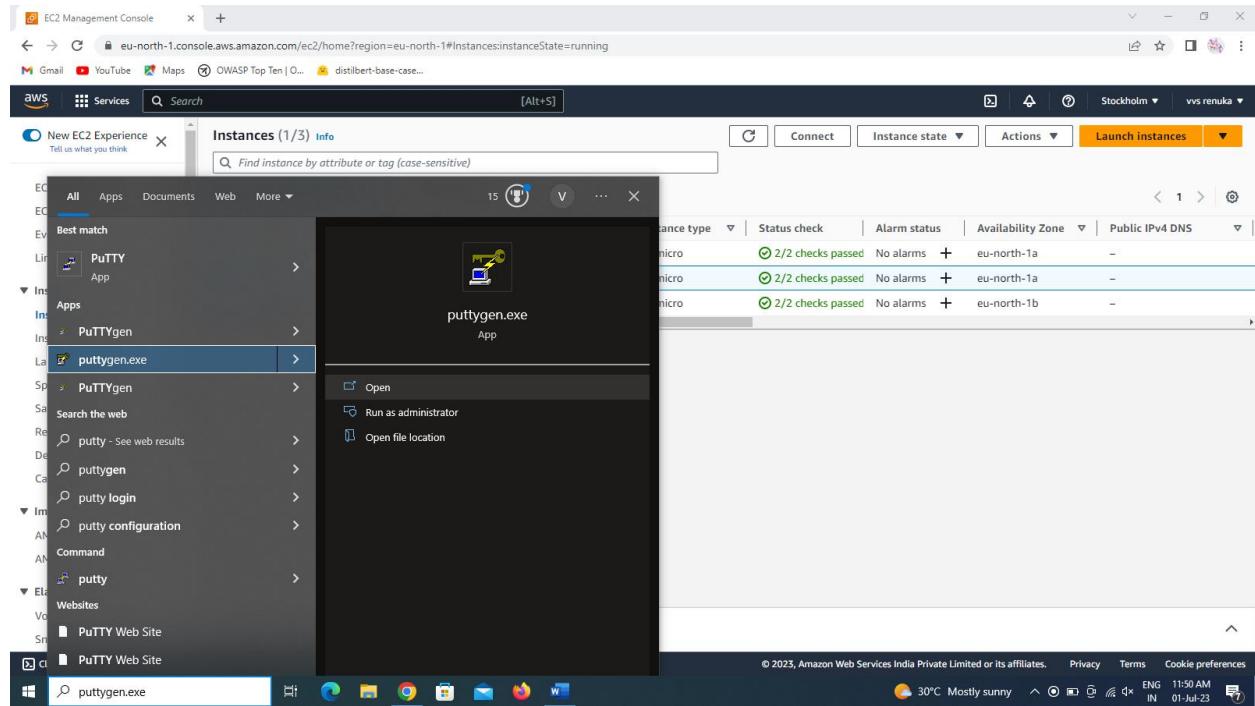
Security group rule ID	Type	Info	Protocol	Info	Port range	Source	Info	Description - optional	Info
sg-0a4ac1f3e2544db01	SSH		TCP		22	Custom		admin-JUMP-Pvt	
sgr-07ef4db1b27c67c76	MySQL/Aurora		TCP		3306	Custom		PUB-SN-CIDR	

Add rule

Cancel Preview changes Save rules

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 30°C Mostly sunny ENG IN 11:45 AM 01-Jul-23

To connect jump box to the data base server in private subnet securely first open the putty generator and generate a .ppk file to the keypair of the jumpbox, Also save the ppk file to the computer.



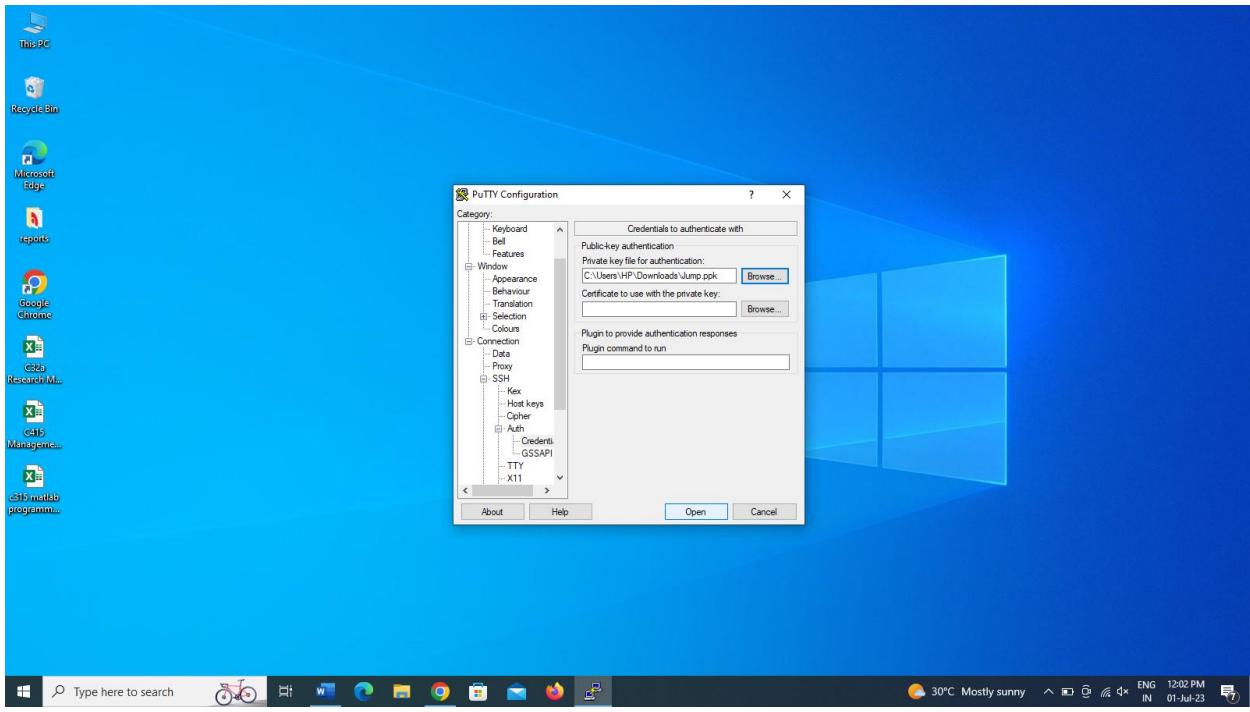
The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with options like EC2 Dashboard, EC2 Global View, Events, Limits, Instances (selected), Images, and Elastic Block Store. The main area displays a list of instances: webservice (i-058d), Jumpbox (i-0074e), and Database (i-06a7c). A modal window titled "Putty Key Generator" is open, showing a public key fingerprint and options for generating or loading private keys. The instance "Jumpbox" is selected in the list.

Now select the jumpbox , select the connect option so that we can connect with the jumpbox and access the files and perform operations on it.

This screenshot shows the same EC2 Management Console interface as the previous one, but with the "Connect" button highlighted in orange for the "Jumpbox" instance in the list. The instance details pane at the bottom is still showing information for the "Jumpbox" instance.

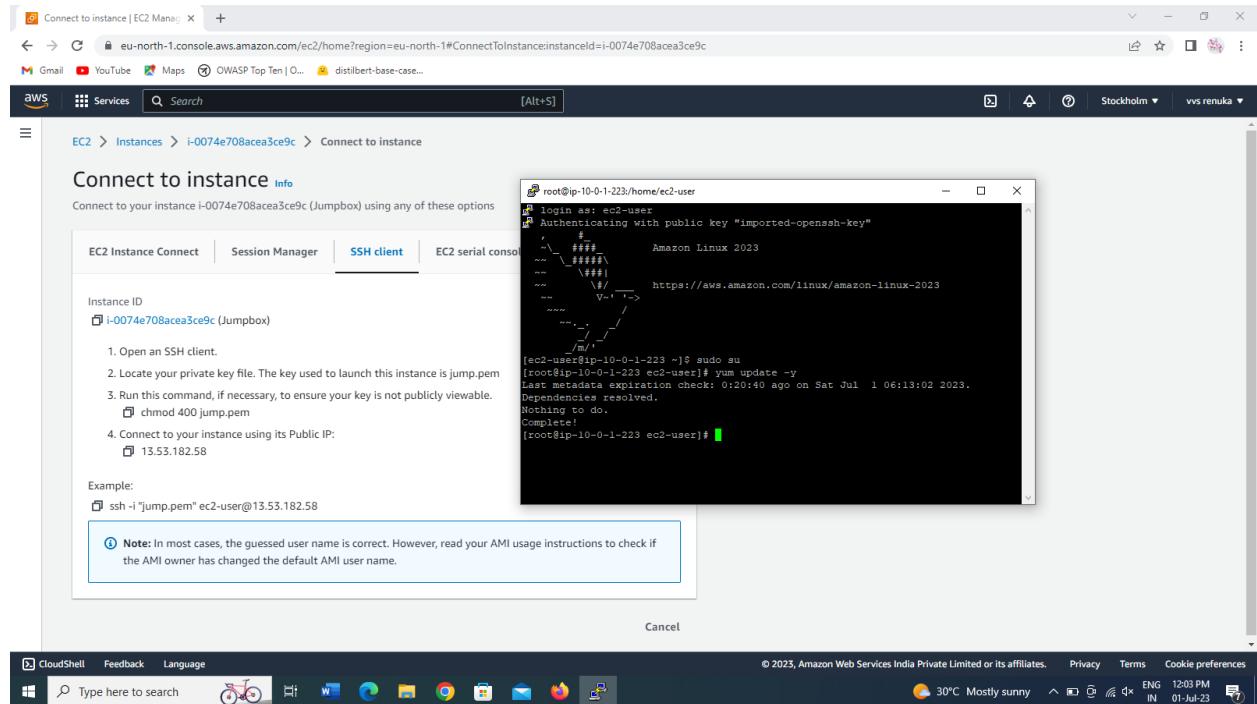
Copy the public ip address of the jumpbox and place it as the hostname in the putty and give the ppk file in the credentials which is present under auth tab of ssh.

The screenshot shows two windows side-by-side. The left window is the 'Connect to instance' dialog from the AWS Management Console, specifically for an EC2 instance with ID i-0074e708acea3ce9c. It displays instructions for connecting via SSH, including the copied public IP (13.53.182.58) and an example command (ssh -i "jump.pem" ec2-user@13.53.182.58). A note at the bottom cautions about the guessed user name. The right window is the 'Putty Configuration' dialog, showing the 'Session' category with the host name set to 13.53.182.58 and port set to 22. The 'SSH' radio button is selected. Both windows are overlaid on a Windows desktop background.

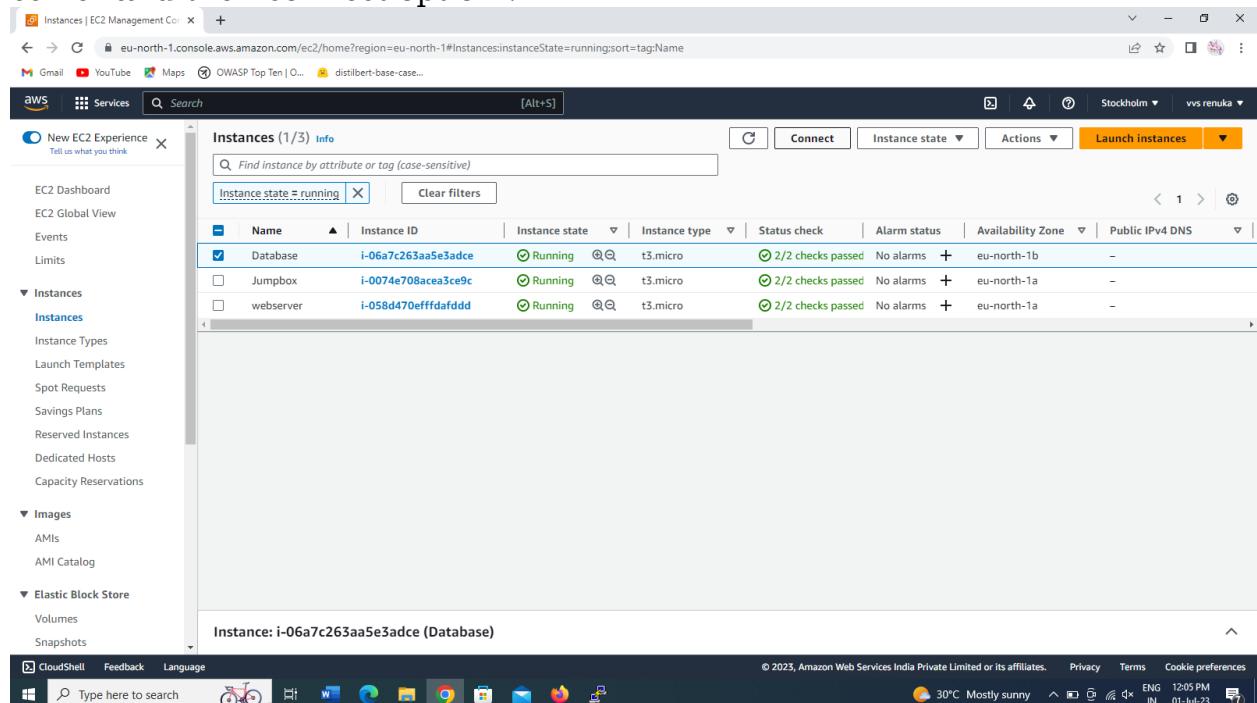


Now select open option and give the login as ec2-user and enter.
We will get access to the jumpbox.

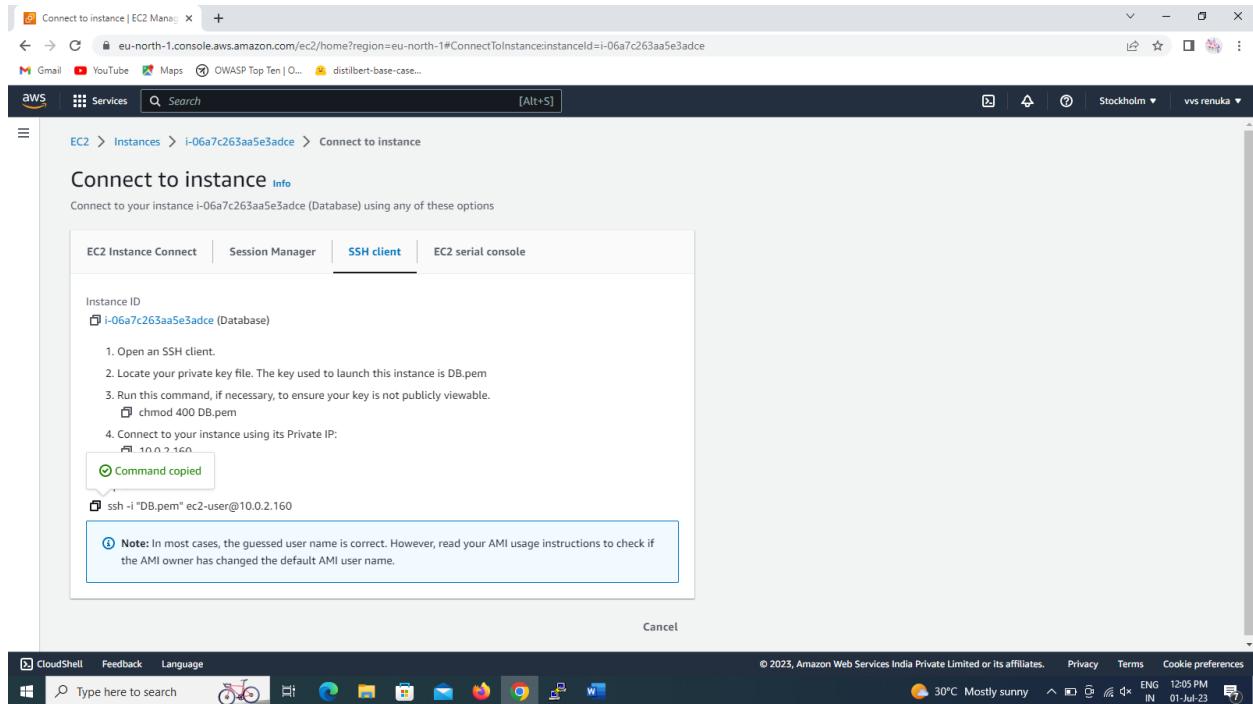
Now type the commands as sudo su ,yum update -y so that we can check whether our linux instance is upto date and lets us to know that if it have any updates.



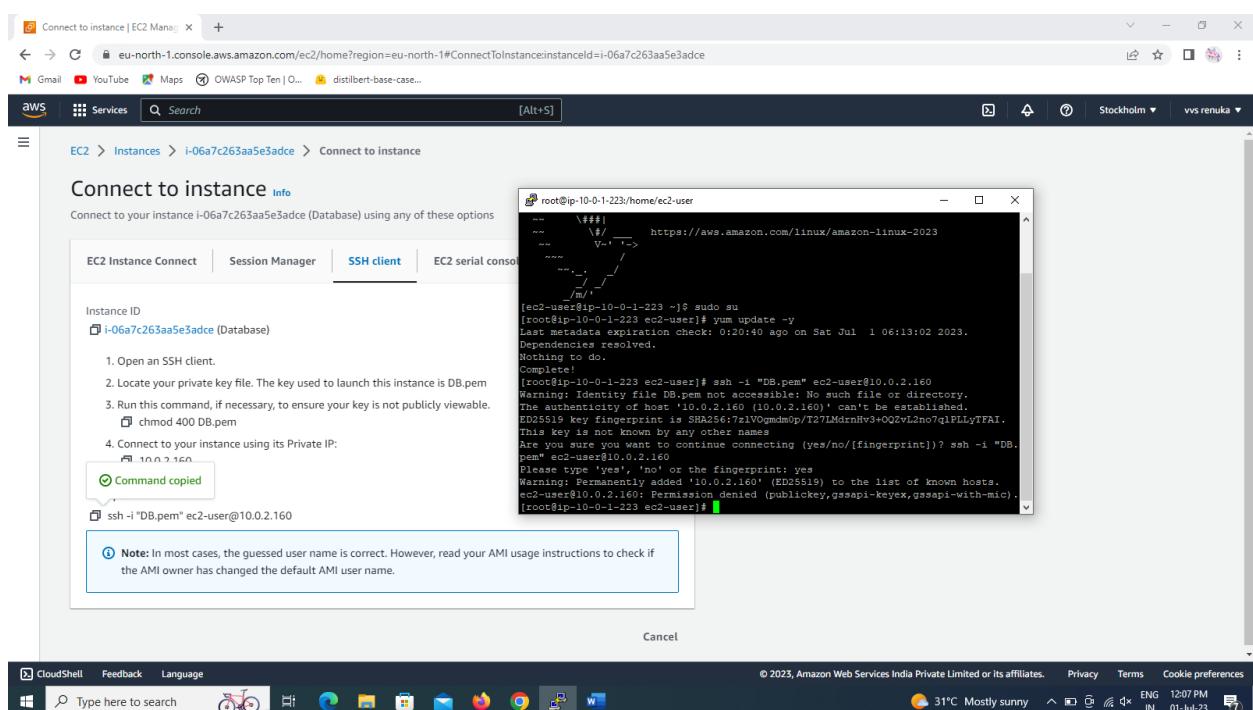
Here we can see that the instance is up to date and there are no updates to be made , Now to connect the database to jump box copy ,select the database server and then connect option .



After that copy the command which allows us to get connected i.e. ssh.....



Paste the command in the linux instance.



Now we can see that it throughs an error that the pem file named as DB is not found.so, we have to move the DB file from database to the jumpbox . To perform this action we require a software named as winscp. So first download and install the software in our computer.

The screenshot shows a web browser window with the address bar containing "WinSCP : Official Site : Download". The main content is the "WinSCP 6.1 Download" page. At the top, there's a navigation bar with links for Home, News, Introduction, Download, Install, Documentation, and Forum. Below the navigation bar, there are two advertisements: one for "Download Free Source Code" from PieceX and another for "Download Free Source Code" from WinSCP. The main text on the page discusses the features of WinSCP 6.1, including Local file manager mode, Windows 11 flat style graphics, SSH core upgraded to PuTTY 0.78, ongoing delete operation moved to background queue, and showing directory size in file panel.

After installing we have to login to the new session to transfer the file .
Logging in to the WINSCP is similar to the logging process of the putty.
First give the host name which is the public ip of the jump box.

The screenshot shows the WinSCP application running on a Windows desktop. A session setup dialog box is open in the center of the screen, titled "New Site". It contains fields for "Name" (set to "New Site"), "File protocol" (set to "SFTP"), "Host name" (empty), "Port number" (set to "22"), "User name" (empty), and "Password" (empty). There are "Save" and "Advanced..." buttons at the bottom. In the background, the Windows taskbar is visible with various icons like Microsoft Edge, Google Chrome, and File Explorer. The desktop background is blue.

Instances | EC2 Management Con

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#instancesv=3:\$case=true%5Cclient:false\$regex=tags:false%5Cclient:false;sort=tagName

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Instances (1/3) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Database	i-06a7c263aa5e3adce	Running	t3.micro	2/2 checks passed	No alarms	+ eu-north-1b	-
Jumpbox	i-0074e708acea3ce9c	Running	t3.micro	2/2 checks passed	No alarms	+ eu-north-1a	-
webserver	i-058d470efffdafddd	Running	t3.micro	2/2 checks passed	No alarms	+ eu-north-1a	-

EC2 Dashboard
EC2 Global View
Events
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots

CloudShell Feedback Language

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

31°C Mostly sunny 12:12 PM 01-Jul-23 ENG IN

Connect to instance | EC2 Manag

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#ConnectToInstanceinstanceId=i-0074e708acea3ce9c

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

EC2 > Instances > i-0074e708acea3ce9c > Connect to instance

Connect to instance Info

Connect to your instance i-0074e708acea3ce9c (Jumpbox) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 serial console

Instance ID
i-0074e708acea3ce9c (Jumpbox)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is jump.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.

Public IP copied 10 jump.pem

Connect to your instance using its Public IP:
13.53.182.58

Example:
ssh -i "jump.pem" ec2-user@13.53.182.58

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

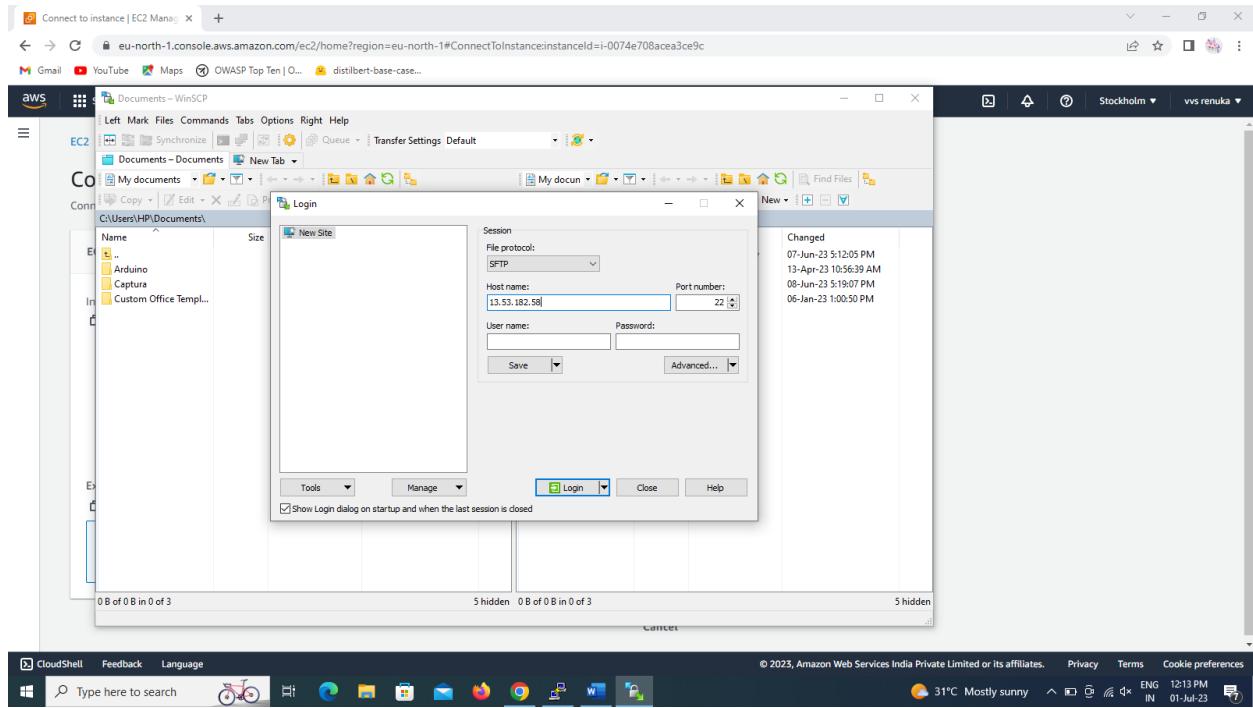
Cancel

CloudShell Feedback Language

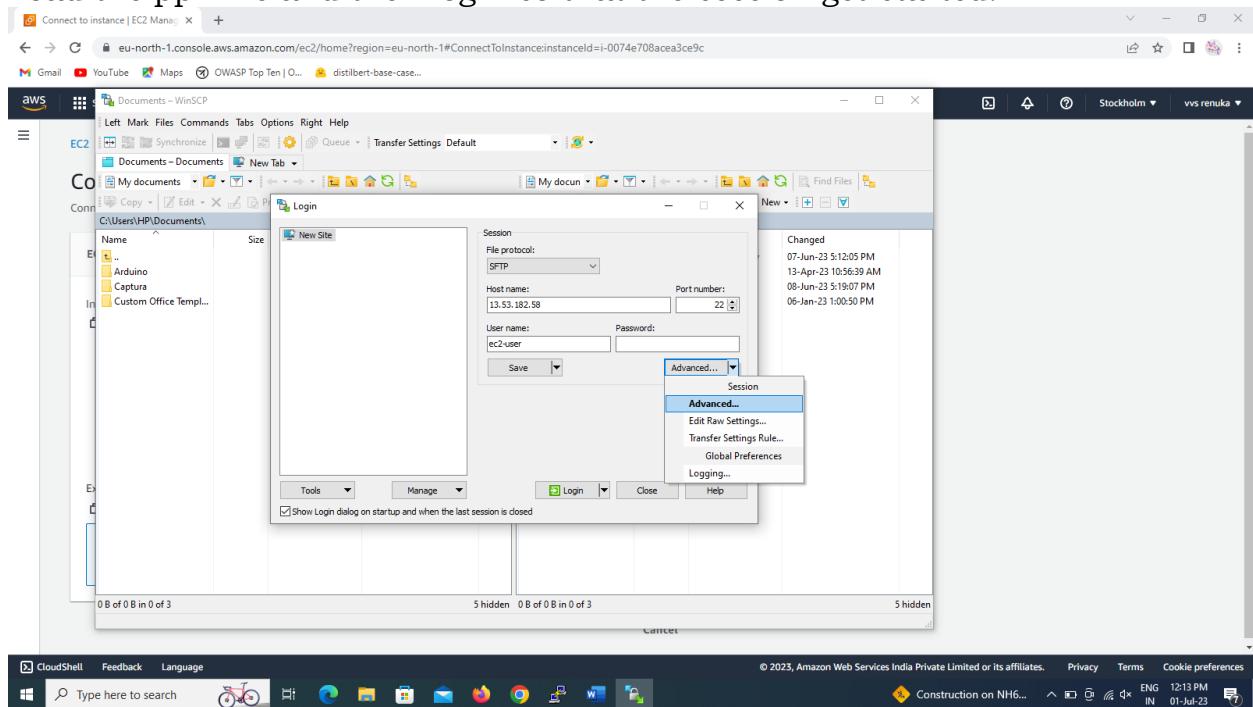
Type here to search

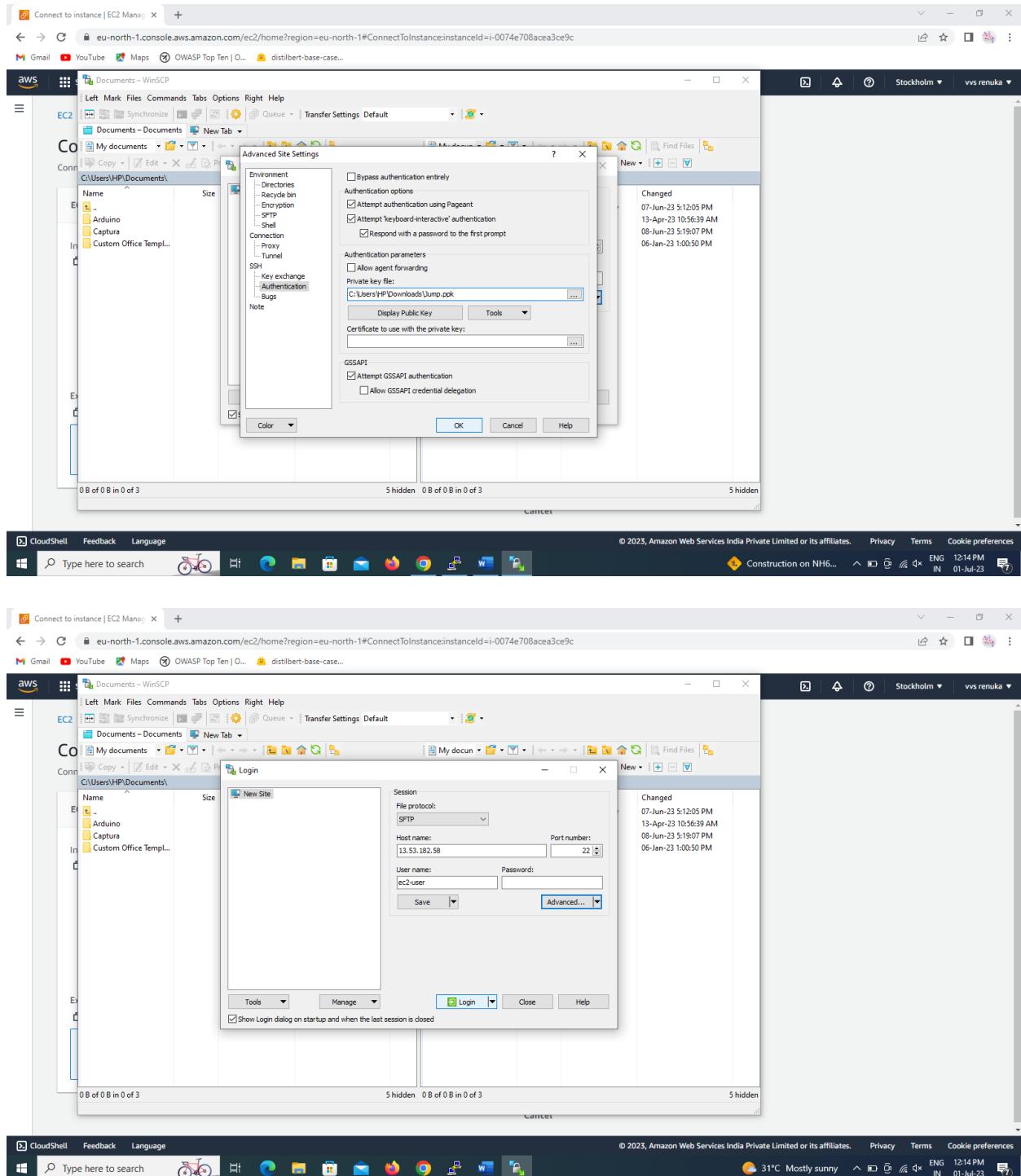
© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

31°C Mostly sunny 12:12 PM 01-Jul-23 ENG IN

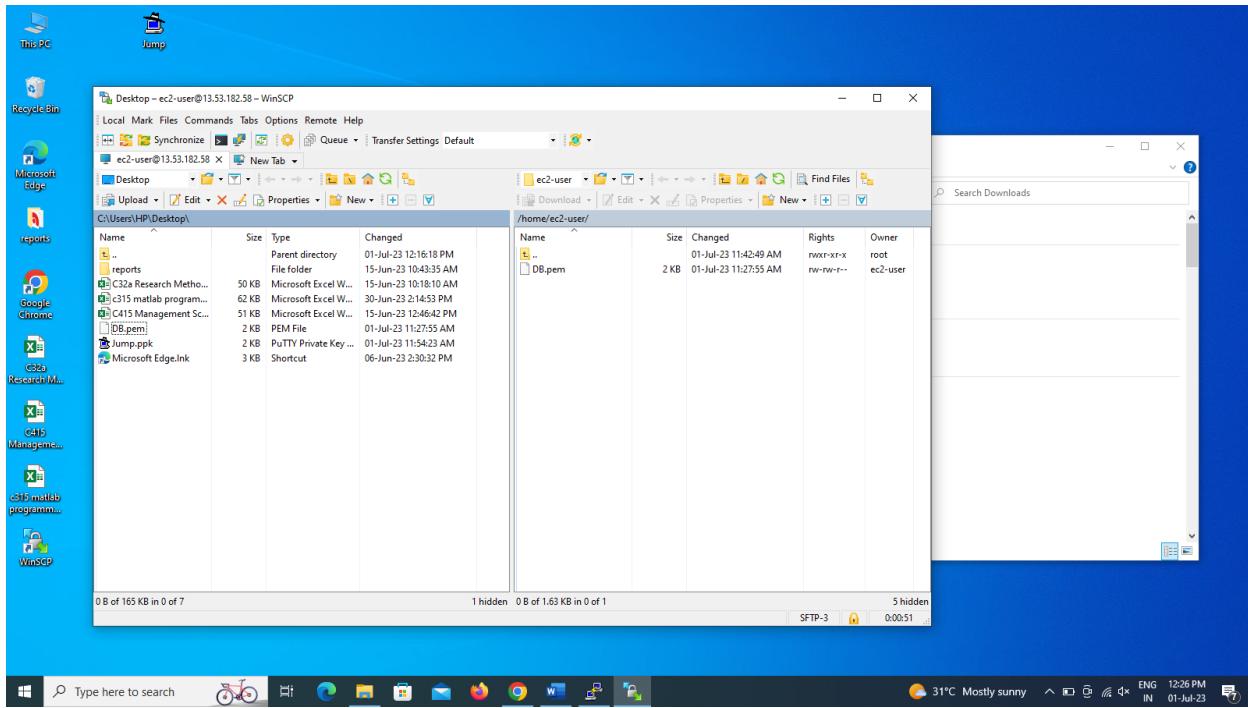


Next give the username and go to advanced settings.
Load the ppk file and then login so that the session get started.





As the session is created now copy the DB file to the jump box instance .

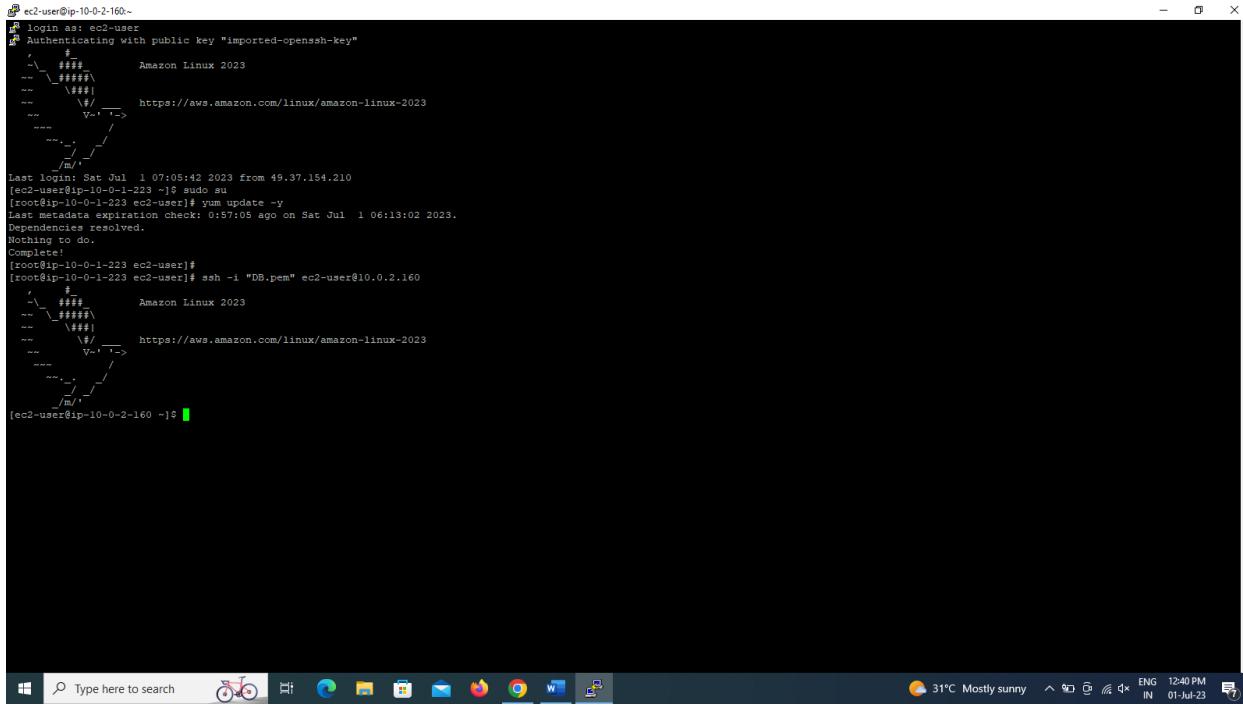


Now go to jumpbox and copy paste the previous command and we get them connected.

```

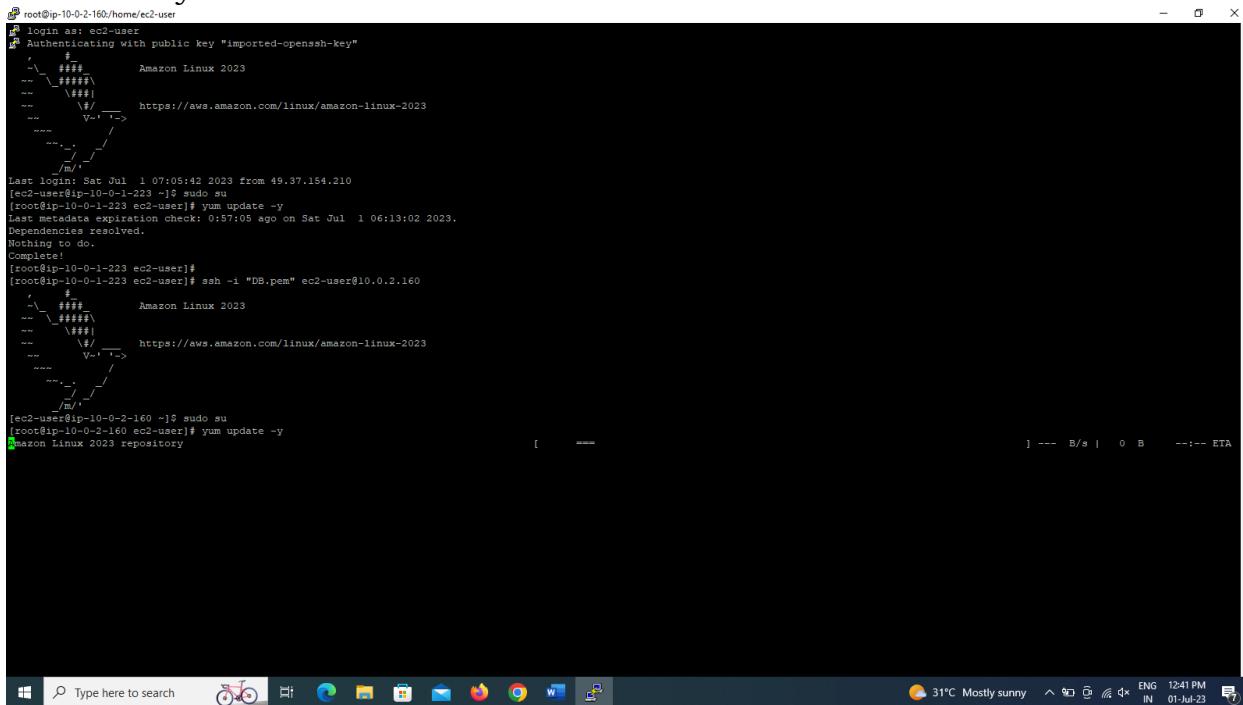
[ec2-user@ip-10-0-1-223 ~]
[ec2-user@ip-10-0-1-223 ~] login as: ec2-user
[ec2-user@ip-10-0-1-223 ~] Authenticating with public key "imported-openssh-key"
[ec2-user@ip-10-0-1-223 ~] Last login: Sat Jul 1 06:51:47 2023 from 49.37.154.210
[ec2-user@ip-10-0-1-223 ~] ls -l "DB.pem" ec2-user@10.0.2.160
[ec2-user@ip-10-0-1-223 ~] Warning: Identity file DB.pem not accessible: No such file or directory.
[ec2-user@ip-10-0-1-223 ~] The authenticity of host '10.0.2.160 (10.0.2.160)' can't be established.
[ec2-user@ip-10-0-1-223 ~] ED25519 key fingerprint is SHA256:7z1VOgmdmOp/T27LMdrnHv3+O2vL2no7qlPLlyTFAI.
[ec2-user@ip-10-0-1-223 ~] This key is not known by any other names
[ec2-user@ip-10-0-1-223 ~] Are you sure you want to continue connecting (yes/no/[fingerprint])?
[ec2-user@ip-10-0-1-223 ~] Host key verification failed.
[ec2-user@ip-10-0-1-223 ~] ssh -i "DB.pem" ec2-user@10.0.2.160
[ec2-user@ip-10-0-1-223 ~] Warning: Identity file DB.pem not accessible: No such file or directory.
[ec2-user@ip-10-0-1-223 ~] The authenticity of host '10.0.2.160 (10.0.2.160)' can't be established.
[ec2-user@ip-10-0-1-223 ~] ED25519 key fingerprint is SHA256:7z1VOgmdmOp/T27LMdrnHv3+O2vL2no7qlPLlyTFAI.
[ec2-user@ip-10-0-1-223 ~] This key is not known by any other names
[ec2-user@ip-10-0-1-223 ~] Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
[ec2-user@ip-10-0-1-223 ~] Warning: Permanently added '10.0.2.160' (ED25519) to the list of known hosts.
[ec2-user@ip-10-0-1-223 ~] Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-1-223 ~] ls
[ec2-user@ip-10-0-1-223 ~] ls

```



```
ec2-user@ip-10-0-2-160:~  
[ec2-user@ip-10-0-2-160 ~]$ login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
[ec2-user@ip-10-0-2-160 ~]$  
[ec2-user@ip-10-0-2-160 ~]$ sudo su  
[root@ip-10-0-2-160 ~]# yum update -y  
Last metadata expiration check: 0:57:05 ago on Sat Jul 1 06:13:02 2023.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@ip-10-0-2-160 ~]# [root@ip-10-0-2-160 ~]# ssh -i "DB.pem" ec2-user@10.0.2.160  
[ec2-user@ip-10-0-2-160 ~]$
```

Now check whether there are any updates and if there is any internet connectivity or not.

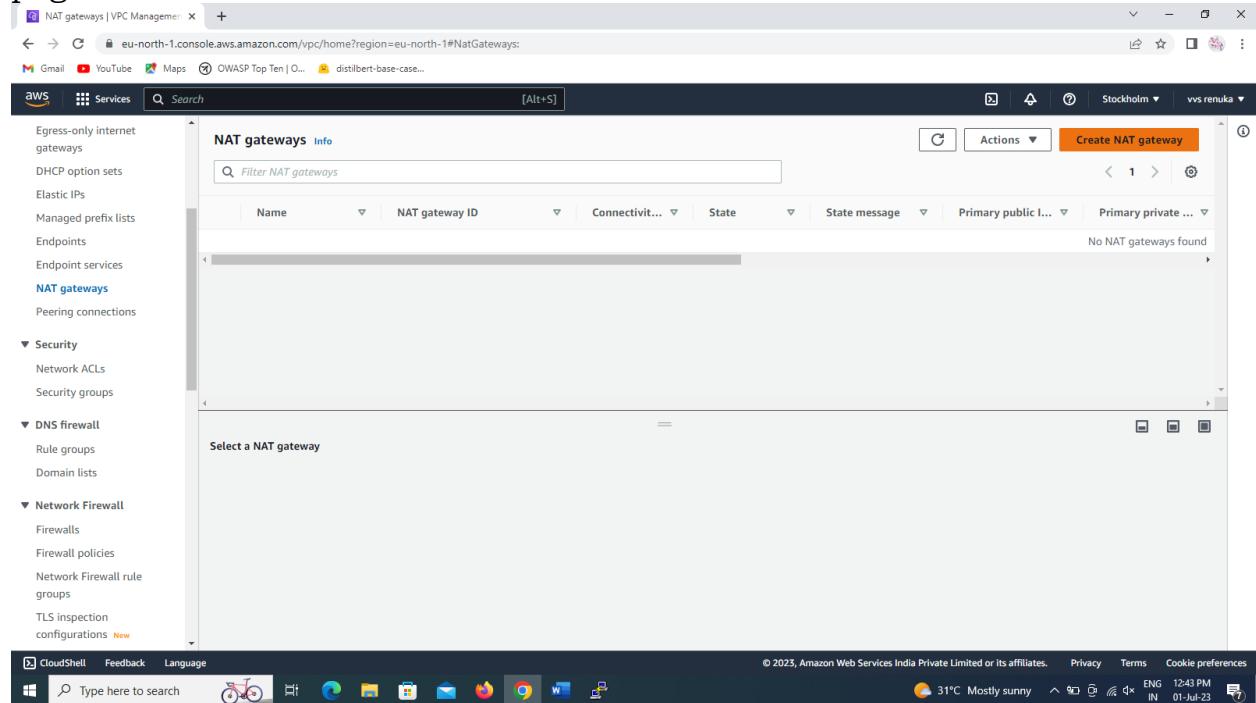


```
root@ip-10-0-2-160:~  
[root@ip-10-0-2-160 ~]$ login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
[root@ip-10-0-2-160 ~]$  
[root@ip-10-0-2-160 ~]$ sudo su  
[root@ip-10-0-2-160 ~]# yum update -y  
Last metadata expiration check: 0:57:05 ago on Sat Jul 1 06:13:02 2023.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@ip-10-0-2-160 ~]# [root@ip-10-0-2-160 ~]# ssh -i "DB.pem" ec2-user@10.0.2.160  
[ec2-user@ip-10-0-2-160 ~]$ sudo su  
[root@ip-10-0-2-160 ~]# yum update -y  
Amazon Linux 2023 repository [      == ] --- B/s | 0 B --:-- ETA
```

We find that there is no internet connectivity for this we have to create the NAT.

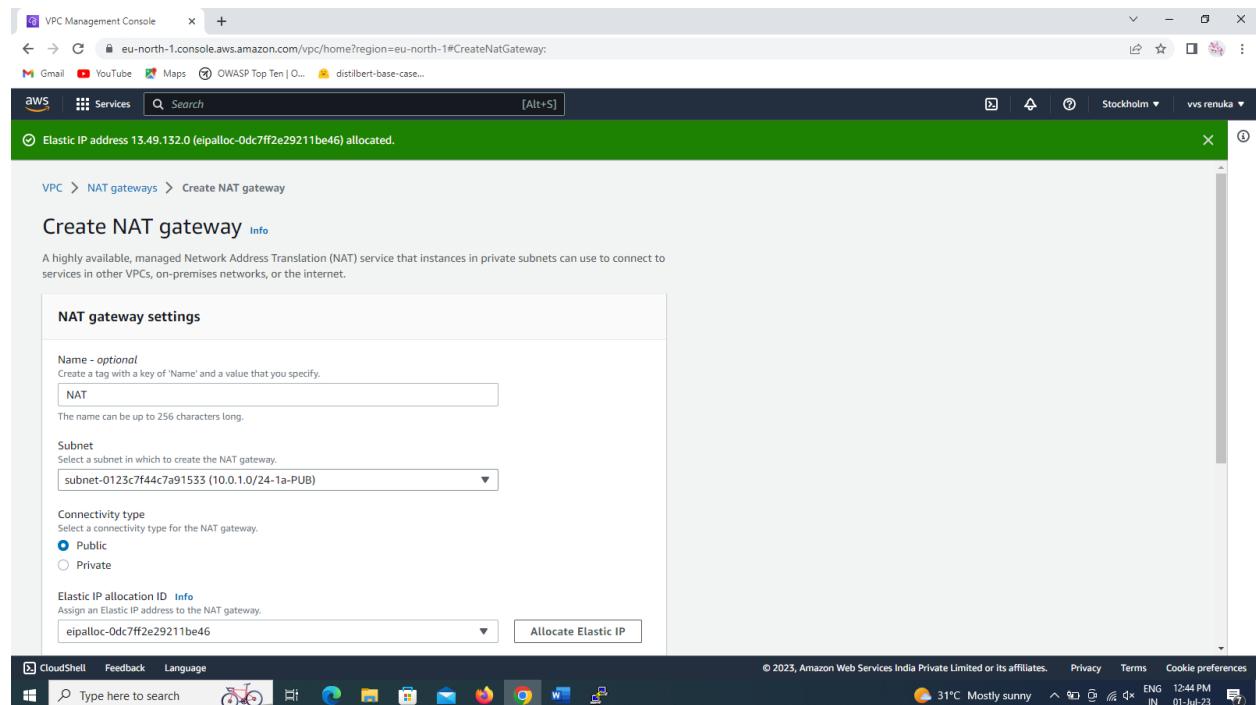
Creation of NAT

First go to VPC service and select the NAT option which is on the left side of the page.



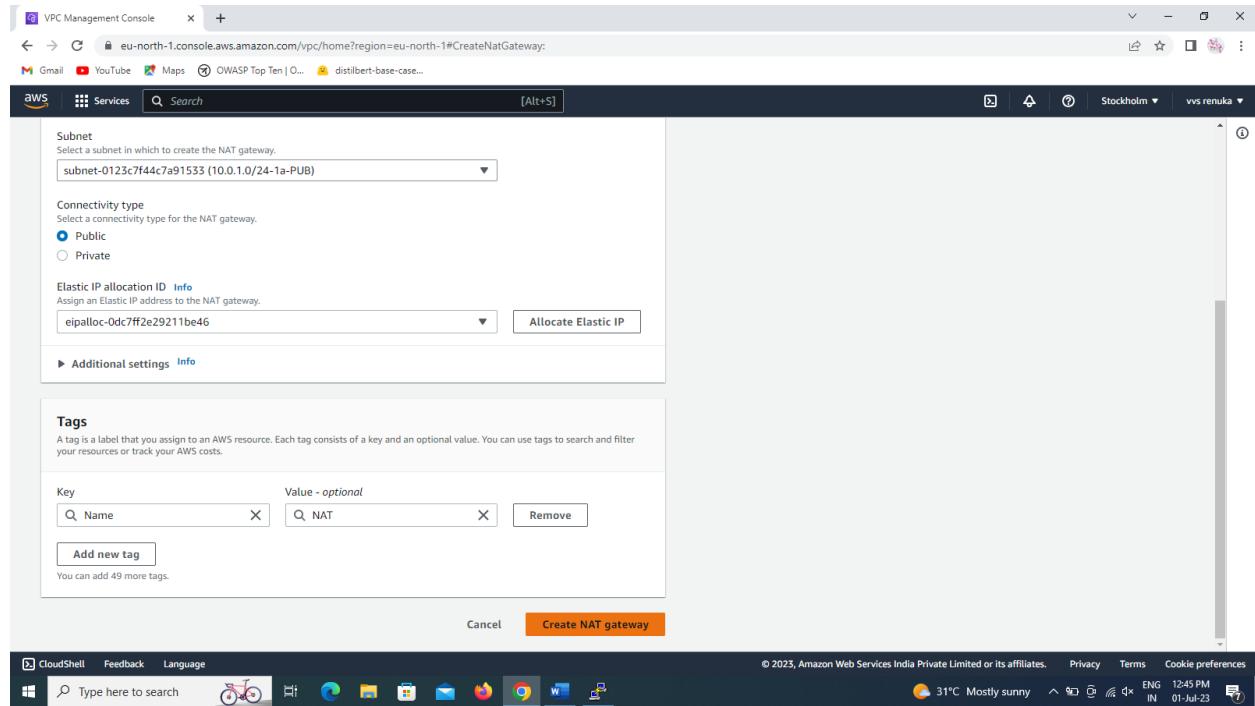
The screenshot shows the AWS VPC Management Console. On the left, a navigation pane lists various services under 'Services', with 'NAT gateways' selected. The main area is titled 'NAT gateways Info' and contains a table header with columns: Name, NAT gateway ID, Connectivity..., State, State message, Primary public I..., and Primary private ...'. A message at the bottom says 'No NAT gateways found'. At the top right, there is a 'Create NAT gateway' button.

Give the name of the NAT and other settings required.



The screenshot shows the 'Create NAT gateway' wizard. Step 1 is 'NAT gateway settings'. It includes fields for 'Name - optional' (containing 'NAT'), 'Subnet' (set to 'subnet-0123c7f44c7a91533 (10.0.1.0/24-1a-PUB)'), 'Connectivity type' (set to 'Public'), and 'Elastic IP allocation ID' (containing 'eipalloc-0dc7ff2e29211be46'). An 'Allocate Elastic IP' button is visible at the bottom right. A green banner at the top indicates 'Elastic IP address 13.49.132.0 (eipalloc-0dc7ff2e29211be46) allocated.'

We also have to allocate the elastic IP.



By using the main route table we can connect the NAT to the database to get internet connectivity.

For this go to route table and edit the subnet associations .

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnet associations			

VPC Management Console

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#RouteTableDetails:RouteTableId=rtb-0263a2bd6f25670a9

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

VPC dashboard EC2 Global View New Filter by VPC: Select a VPC

Virtual private cloud Your VPCs New Subnets Route tables Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections Security Network ACLs Security groups

CloudShell Feedback Language Type here to search 31°C Mostly sunny 12:48 PM 01-Jul-23

Route tables > rtb-0263a2bd6f25670a9 / RT_Main

rtb-0263a2bd6f25670a9 / RT_Main

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

Details Info

Route table ID: rtb-0263a2bd6f25670a9 Main: Yes Explicit subnet associations: - Edge associations: -

VPC: vpc-0598766edb63d41bd | My_VPC Owner ID: 507439313398

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (0) Edit subnet associations

Name Subnet ID IPv4 CIDR IPv6 CIDR

No subnet associations You do not have any subnet associations.

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 12:48 PM 01-Jul-23

Select the private subnet.

VPC Management Console

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1>EditRouteTableSubnetAssociations:RouteTableId=rtb-0263a2bd6f25670a9

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

VPC > Route tables > rtb-0263a2bd6f25670a9 > 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
10.0.2.0/24-1b-PVT	subnet-0f723c804d4eca1a3	10.0.2.0/24	-	Main (rtb-0263a2bd6f25670a9 / RT_M...
10.0.1.0/24-1a-PUB	subnet-0123c7f44c7a91533	10.0.1.0/24	-	rtb-08c7634dd89ad9a92 / RT_Custom

Selected subnets

subnet-0f723c804d4eca1a3 / 10.0.2.0/24-1b-PVT X

Cancel Save associations

CloudShell Feedback Language Type here to search 31°C Mostly sunny 12:49 PM 01-Jul-23

The screenshot shows the AWS VPC Management Console. A success message at the top states: "You have successfully updated subnet associations for rtb-0263a2bd6f25670a9 / RT_Main." Below this, the route table details for "rtb-0263a2bd6f25670a9 / RT_Main" are displayed. The "Routes" tab is selected, showing one route entry:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

At the bottom right of the main content area, there is a "Run Reachability Analyzer" button.

Now add the route to the route table.

The screenshot shows the "Edit routes" interface for the route table "rtb-0263a2bd6f25670a9". The table lists two routes:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-0ab22aa02701c62cb	-	No

A "Remove" button is visible next to the second route entry. At the bottom of the interface are "Cancel", "Preview", and "Save changes" buttons. The status bar at the bottom indicates it's 31°C, Mostly sunny, and the time is 12:49 PM on 01-Jul-23.

Finally we get the internet connectivity.

```

root@ip-10-0-2-160:/home/ec2-user
[ec2-user@ip-10-0-2-160 ~]$ login as: ec2-user
Authenticating with public key "imported-openssh-key"
[ec2-user@ip-10-0-2-160 ~]$ Amazon Linux 2023
[ec2-user@ip-10-0-2-160 ~]$ https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-2-160 ~]$ 
[ec2-user@ip-10-0-2-160 ~]$ Last login: Sat Jul  1 07:05:12 2023 from 49.37.154.210
[ec2-user@ip-10-0-1-223 ~]$ sudo su
[ec2-user@ip-10-0-1-223 ec2-user]# yum update -y
Last metadata expiration check: 0:57:05 ago on Sat Jul  1 06:13:02 2023.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-10-0-1-223 ec2-user]# ssh -i "DB.pem" ec2-user@10.0.2.160
[ec2-user@ip-10-0-1-223 ec2-user]# Amazon Linux 2023
[ec2-user@ip-10-0-1-223 ec2-user]# https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-1-223 ec2-user]# 
[ec2-user@ip-10-0-2-160 ~]$ sudo su
[ec2-user@ip-10-0-2-160 ec2-user]# yum update -y
Amazon Linux 2023 repository
Errors during downloading metadata for repository 'amazonlinux':
 - Curl error (28): Timeout was reached for https://al2023-repos-eu-north-1-dee612dc2.s3.dualstack.eu-north-1.amazonaws.com/core/mirrors/2023.1.20230629/x86_64/mirror.list [Failed to connect to al2023-repos-eu-north-1-dee612dc2.s3.dualstack.eu-north-1.amazonaws.com port 443 after 30000 ms: Timeout was reached]
Error: Failed to download metadata for repo 'amazonlinux': Cannot prepare internal mirrorlist: Curl error (28): Timeout was reached for https://al2023-repos-eu-north-1-dee612dc2.s3.dualstack.eu-north-1.amazonaws.com/core/mirrors/2023.1.20230629/x86_64/mirror.list [Failed to connect to al2023-repos-eu-north-1-dee612dc2.s3.dualstack.eu-north-1.amazonaws.com port 443 after 30000 ms: Timeout was reached]
Amazon Linux 2023 Kernel Livepatch repository
Ignoring repositories: amazonlinux
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-10-0-2-160 ec2-user]# yum update -y
Amazon Linux 2023 repository
Last metadata expiration check: 0:00:04 ago on Sat Jul  1 07:24:32 2023.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-10-0-2-160 ec2-user]# 

```

Once check whether the webserver is running or not.



We have to create the NACL to the subnets.

For public subnet we have to create custom NACL.

Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#acl:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Network ACLs (1/2) Info

Find resources by attribute or tag

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules
NACL_Main	acl-04a0feae9766791	2 Subnets	Yes	vpc-0598766edb63d41bd / My_VPC	2 Inbound r...
-	acl-05abef16d727836e4	3 Subnets	Yes	vpc-0805c16989d9ed81	2 Inbound r...

Details Inbound rules Outbound rules Subnet associations Tags

Details

Network ACL ID acl-04a0feae9766791	Associated with 2 Subnets	Default Yes	VPC ID vpc-0598766edb63d41bd / My_VPC
Owner 507439313398			

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 31°C Mostly sunny ENG IN 12:58 PM 01-Jul-23

Create network ACL | VPC Management

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#CreateNetworkAcl:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

VPC > Network ACLs > Create network ACL

Create network ACL Info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

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

VPC
VPC to use for this network ACL.
VPC: vpc-0598766edb63d41bd (My_VPC)

Tags

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 - <i>optional</i>
Q Name	Q NACL_custom
Add tag	Remove tag

You can add 49 more tags

Cancel Create network ACL

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 31°C Mostly sunny ENG IN 12:58 PM 01-Jul-23

The screenshot shows the AWS VPC Management console with the URL eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#acls. The left sidebar is collapsed, and the main area displays the 'Network ACLs' table. A green success message at the top states: 'You successfully created acl-00f870771c3da13c8 / NACL_custom.' The table lists three entries:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rule
NACL_Main	acl-04a0feae9d9766791	2 Subnets	Yes	vpc-0598766edb63d41bd / My_VPC	2 Inbound r.
-	acl-05abef16d727836e4	3 Subnets	Yes	vpc-0c805c16989d9ed81	2 Inbound r.
NACL_custom	acl-00f870771c3da13c8	-	No	vpc-0598766edb63d41bd / My_VPC	1 Inbound r.

Below the table, a section titled 'Select a network ACL' contains a dropdown menu with the option 'acl-00f870771c3da13c8 / NACL_custom' selected. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time as 01-Jul-23.

Now we have to assign the NAACL to the subnet.

The screenshot shows the same AWS VPC Management console interface. The 'Subnet associations' tab is now active, displaying a table of subnet associations for the 'NACL_custom' ACL. The table has columns: Name, Subnet ID, Associated with, Availability Zone, IPv4 CIDR, and IPv6 CIDR. There are no visible rows in the table.

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR

The bottom of the screen shows the Windows taskbar and system tray, identical to the previous screenshot.

The screenshot shows the AWS VPC Management Console with the URL eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#EditNetworkAclSubnetAssociations:networkAclId=acl-00f870771c3da13c8. The page displays the 'Edit subnet associations' section for a custom Network ACL. It lists two available subnets: '10.0.2.0/24-1b-PVT' and '10.0.1.0/24-1a-PUB'. The '10.0.1.0/24-1a-PUB' subnet is selected and associated with the custom Network ACL. The 'Selected subnets' section contains the same entry. At the bottom right are 'Cancel' and 'Save changes' buttons.

Now go and check whether the webserver is working or not.
We find that the server is not working.

The screenshot shows a browser window with the URL 13.49.223.7. The page displays an error message: 'This site can't be reached' with the sub-message '13.49.223.7 took too long to respond.' Below this, there are troubleshooting steps: 'Try:' followed by a bulleted list: '• Checking the connection', '• Checking the proxy and the firewall', and '• Running Windows Network Diagnostics'. At the bottom of the error page are 'Reload' and 'Details' buttons. The browser's taskbar at the bottom shows various open tabs and system icons.

Now go to NACL custom and edit the inbound rules and check the website.

VPC > Network ACLs > acl-00f870771c3da13c8 / NAACL_custom > Edit inbound rules

Edit inbound rules [Info](#)

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

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info
100	SSH (22)	TCP (6)	22	32.0.0.0/3	Allow
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Add new rule Sort by rule number

Cancel Preview changes Save changes

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

31°C Mostly sunny ENG IN 1:09 PM 01-Jul-23

EC2 Management Console | Network ACLs | VPC Management | 13.49.223.7

This site can't be reached

13.49.223.7 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Reload Details

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

31°C Mostly sunny ENG IN 1:09 PM 01-Jul-23

EC2 Management Console | Network ACLs | VPC Management | 13.49.223.7

This site can't be reached

13.49.223.7 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Reload Details

Even though we have edited the inbound rules there is a rule which is denied so here comes the role of the ephemeral ports.

EC2 Management Console | Network ACLs | VPC Management | 13.49.223.7 | ephemeral ports - Google Search

About 24,80,000 results (0.27 seconds)

Ephemeral port

An **ephemeral port** is a communications endpoint (port) of a transport layer protocol of the Internet protocol suite that is used for only a short period of ...

People also ask :

- What ports are ephemeral?
- What are ephemeral and non ephemeral ports?
- What is dynamic vs ephemeral ports?
- What are ephemeral ports in TCP header?

What is an Ephemeral Port? - Definition from Techopedia

11-Apr-2014 — An **ephemeral port** is a temporary communication hub used for Internet Protocol (IP) communications. It is created from a set range of port.

EC2 Management Console | VPC Management Console | 13.49.223.7 | eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#EditInboundRules:networkAclId=acl-00f870771c3da13c8

VPC > Network ACLs > acl-00f870771c3da13c8 / NAACL_custom > Edit inbound rules

Edit inbound rules

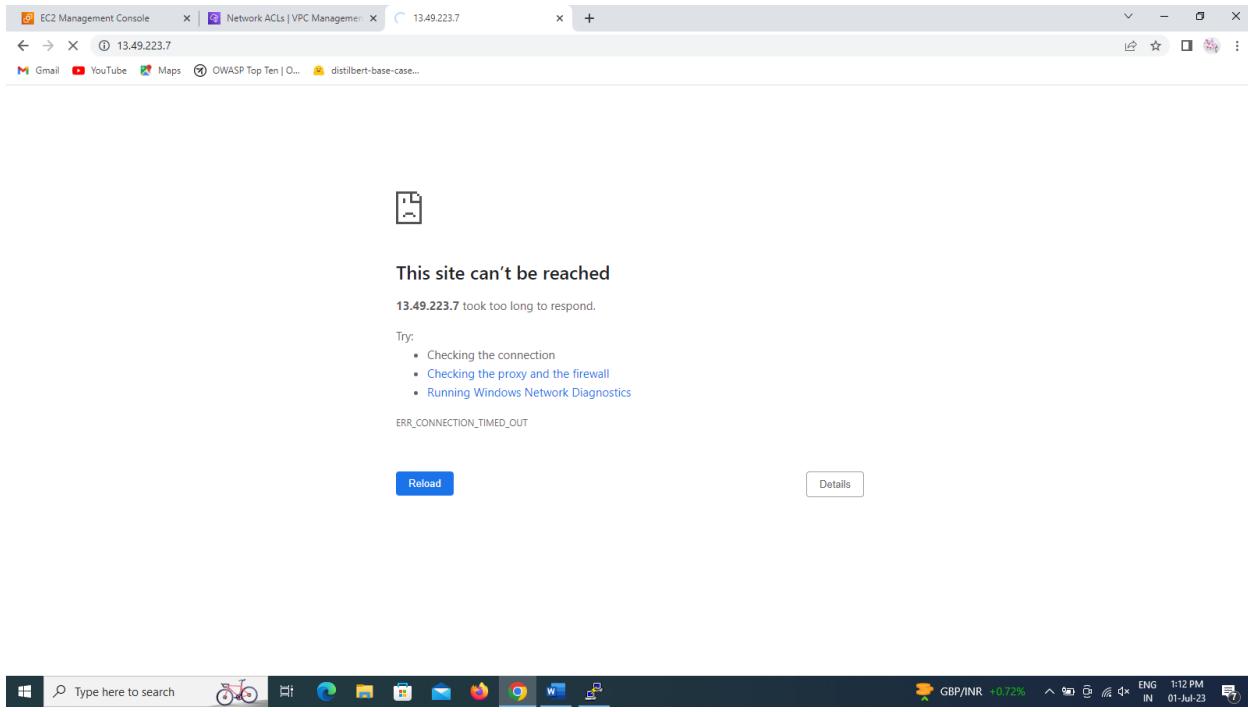
Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	SSH (22)	TCP (6)	22	32.0.0.0/3	Allow
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
300	Custom TCP	TCP (6)	1024-65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Add new rule | Sort by rule number | Cancel | Preview changes | Save changes

CloudShell | Feedback | Language | Type here to search | © 2023, Amazon Web Services India Private Limited or its affiliates. | Privacy | Terms | Cookie preferences | GBP/INR +0.72% | ENG IN | 1:10 PM 01-Jul-23

Even though the changes made we don't get the website worked.



So to solve this not only inbound rules outbound rules also to be edited.

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	SSH (22)	TCP (6)	22	49.37.154.210/32	Allow
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
300	Custom TCP	TCP (6)	1024-65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Add new rule Sort by rule number Cancel Preview changes Save changes

Now we can see that the server is running successfully and securely.



Windows taskbar:

- Type here to search
- High UV
- 1:14 PM
- 01-Jul-23

Browser tabs:

- EC2 Management Console
- VPC Management Console
- 13.49.223.7

Address bar:

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1#EditInboundRules:networkAcld=acl-00f870771c3da13c8

Content area:

VPC > Network ACLs > acl-00f870771c3da13c8 / NAACL_custom > Edit inbound rules

Edit inbound rules Info

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

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	SSH (22)	TCP (6)	22	32.0.0.0/3	Allow
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
300	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
400	Custom TCP	TCP (6)	1024-65535	49.37.154.210/32	Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Add new rule Sort by rule number

Buttons: Cancel, Preview changes, Save changes

Bottom navigation:

- CloudShell
- Feedback
- Language
- © 2023, Amazon Web Services India Private Limited or its affiliates.
- Privacy
- Terms
- Cookie preferences

System tray:

- Construction on NH6...
- 1:18 PM
- 01-Jul-23

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	SSH (22)	TCP (6)	22	49.37.154.210/32	Allow
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
300	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
400	Custom TCP	TCP (6)	1024 - 65535	49.37.154.210/32	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

If we have to make a particular user denied from this access to the website then we can add that particular users Ip address and make him blocked .

EC2 Management Console VPC Management Console 13.49.223.7

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1>EditInboundRules:networkAclId=acl-00f870771c3da13c8

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

VPC > Network ACLs > acl-00f870771c3da13c8 / NAACL_custom > Edit inbound rules

Edit inbound rules [Info](#)

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

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info	Action
100	SSH (22)	TCP (6)	22	49.37.154.210/32	Allow	Remove
180	Custom TCP	TCP (6)	1024 - 65535	49.37.154.210/32	Deny	Remove
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow	Remove
300	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

[Add new rule](#) [Sort by rule number](#)

Cancel [Preview changes](#) [Save changes](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 31°C Mostly sunny ENG IN 1:22 PM 01-Jul-23

EC2 Management Console VPC Management Console 13.49.223.7

eu-north-1.console.aws.amazon.com/vpc/home?region=eu-north-1>EditOutboundRules:networkAclId=acl-00f870771c3da13c8

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

VPC > Network ACLs > acl-00f870771c3da13c8 / NAACL_custom > Edit outbound rules

Edit outbound rules [Info](#)

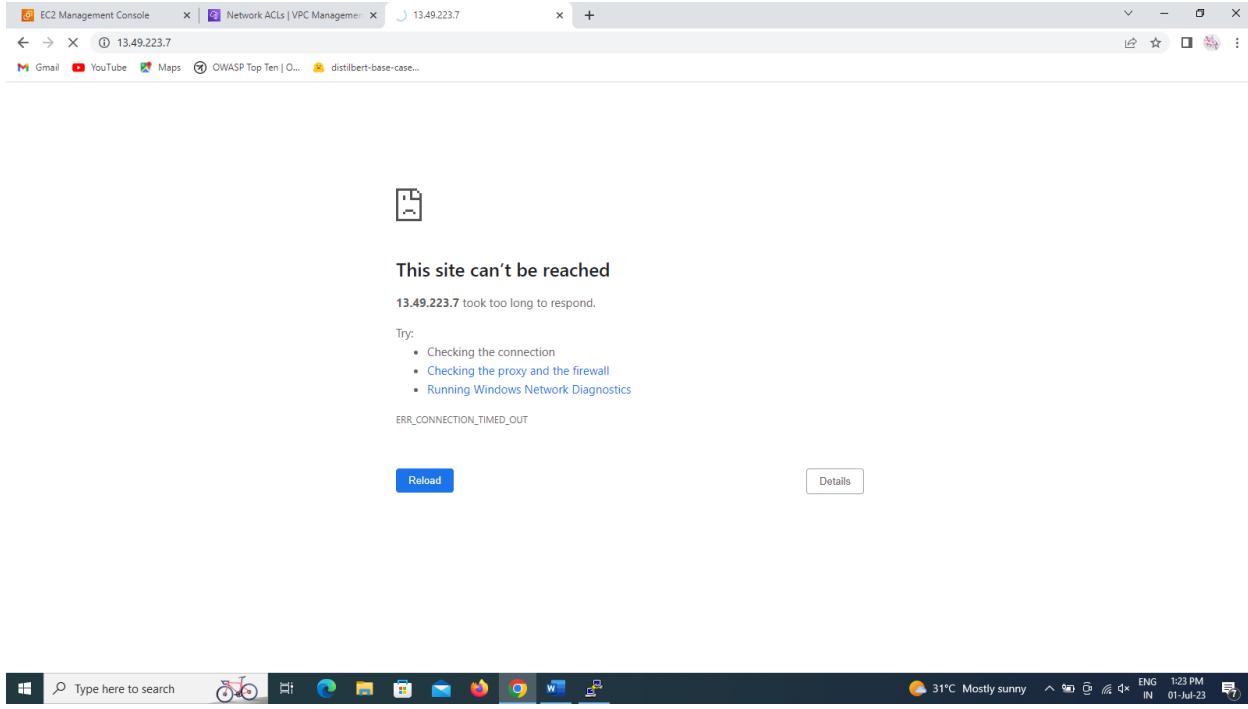
Outbound rules control the outgoing traffic that's allowed to leave the VPC.

Rule number Info	Type Info	Protocol Info	Port range Info	Destination Info	Allow/Deny Info	Action
100	SSH (22)	TCP (6)	22	49.37.154.210/32	Allow	Remove
180	Custom TCP	TCP (6)	1024 - 65535	49.37.154.210/32	Deny	Remove
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow	Remove
300	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

[Add new rule](#) [Sort by rule number](#)

Cancel [Preview changes](#) [Save changes](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 31°C Mostly sunny ENG IN 1:22 PM 01-Jul-23



Finally to balance the traffic between the servers we have to create an elastic load balancer along with the ASG.

For this first we have to create the launch template.

Creation of Launch Template.

The screenshot shows the AWS EC2 Management Console interface. On the left, a sidebar menu is open with 'Launch Templates' selected under 'Instances'. The main content area displays a success message 'Delete Launch Template Request Succeeded'. Below it, the 'EC2 launch templates' page is shown with the sub-headline 'Streamline, simplify and standardize instance launches'. It features a 'New launch template' button and sections for 'Benefits and features' (Streamline provisioning, Simplify permissions) and 'Documentation'.

Name the launch template and give the settings required such as keypair, security group, subnet in which it is going to be created , VPC etc...

Create launch template | EC2 Manager | Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateTemplate:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

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, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

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

Template version description
new asg
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

Summary

Software Image (AMI)

Virtual server type (instance type)

Firewall (security group)

Storage (volumes)

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

Cancel **Create launch template**

Create launch template | EC2 Manager | Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateTemplate:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

Launch template contents

Type here to search

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Mostly sunny ENG IN 1:27 PM 01-Jul-23

Amazon linux

AMI from catalog Recents Quick Start

Amazon Machine Image (AMI)
al2023-ami-2023.1.20230629.0-kernel-6.1-x86_64
ami-0c858d4d1feca5370

Catalog Published Architecture Virtualization Root device type ENA Enabled
Quickstart AMIs 2023-06-28T15:47:15.00Z x86_64 hvm ebs Yes

Browse more AMIs Including AMIs from AWS, Marketplace and the Community

Instance type [Info](#) Advanced

Instance type
Don't include in launch template All generations Compare instance types

Summary

Software Image (AMI)
Amazon Linux 2023 AMI
ami-0c858d4d1feca5370

Virtual server type (instance type)

Firewall (security group)

Storage (volumes)
1 volume(s) - 8 GiB

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

Cancel **Create launch template**

Create launch template | EC2 Manager | Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateTemplate:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Quickstart AMIs 2023-06-28T15:47:15.00 x86_64 hvm ebs Yes

Instance type **t3.micro** Info Advanced

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

All generations Compare instance types

Key pair (login) **Info**

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

Key pair name Create new key pair

Network settings **Info**

CloudShell Feedback Language

Type here to search

Summary

Software Image (AMI)
Amazon Linux 2023 AMI
ami-0c858d4d1fec5370

Virtual server type (instance type)
t3.micro

Firewall (security group)
-

Storage (volumes)
1 volume(s) - 8 GiB

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

Create launch template

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Mostly sunny 1:28 PM 01-Jul-23 ENG IN

Create launch template | EC2 Manager | Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateTemplate:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Quickstart AMIs 2023-06-28T15:47:15.00 x86_64 hvm ebs Yes

Instance type **t3.micro** Info Advanced

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

All generations Compare instance types

Key pair (login) **Info**

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

Key pair name Create new key pair

Network settings **Info**

Subnet info

subnet-0123c7f44c7a91533 10.0.1.0/24-1a-PUB
VPC: vpc-02976edeb5d4fb1 Owner: 507433313398 Availability Zone: eu-north-1a IP addresses available: 248 CIDR: 10.0.1.0/24

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

CloudShell Feedback Language

Type here to search

Summary

Software Image (AMI)
Amazon Linux 2023 AMI
ami-0c858d4d1fec5370

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

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

Create launch template

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Mostly sunny 1:35 PM 01-Jul-23 ENG IN

Create launch template | EC2 Management | Network ACLs | VPC Management | + eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateTemplate: Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

Subnet info

subnet-0123cf7f44c7a91533 10.0.1.0/24-1a-PUB
VPC: vpc-0598766edb63d41bd Owner: 507439313388 Availability Zone: eu-north-1a IP addresses available: 248 CIDR: 10.0.1.0/24

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 asg

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 asg

VPC - required vpc-0598766edb63d41bd

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 49.37.154.210/32)

Type Info Protocol Info Port range Info
ssh TCP 22

Source type Info Name Info Description - optional e.g. SSH for admin desktop

Remove

Cancel Create launch template

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Mostly sunny ENG IN 1:35 PM 01-Jul-23

Create launch template | EC2 Management | Network ACLs | VPC Management | + eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateTemplate: Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

Security group rule 1 (TCP, 22, 49.37.154.210/32)

Type Info Protocol Info Port range Info
ssh TCP 22

Source type Info Name Info Description - optional e.g. SSH for admin desktop

My IP 49.37.154.210/32

Remove

Security group rule 2 (TCP, 80, Multiple sources)

Type Info Protocol Info Port range Info
HTTP TCP 80

Source type Info Source Info Description - optional e.g. SSH for admin desktop

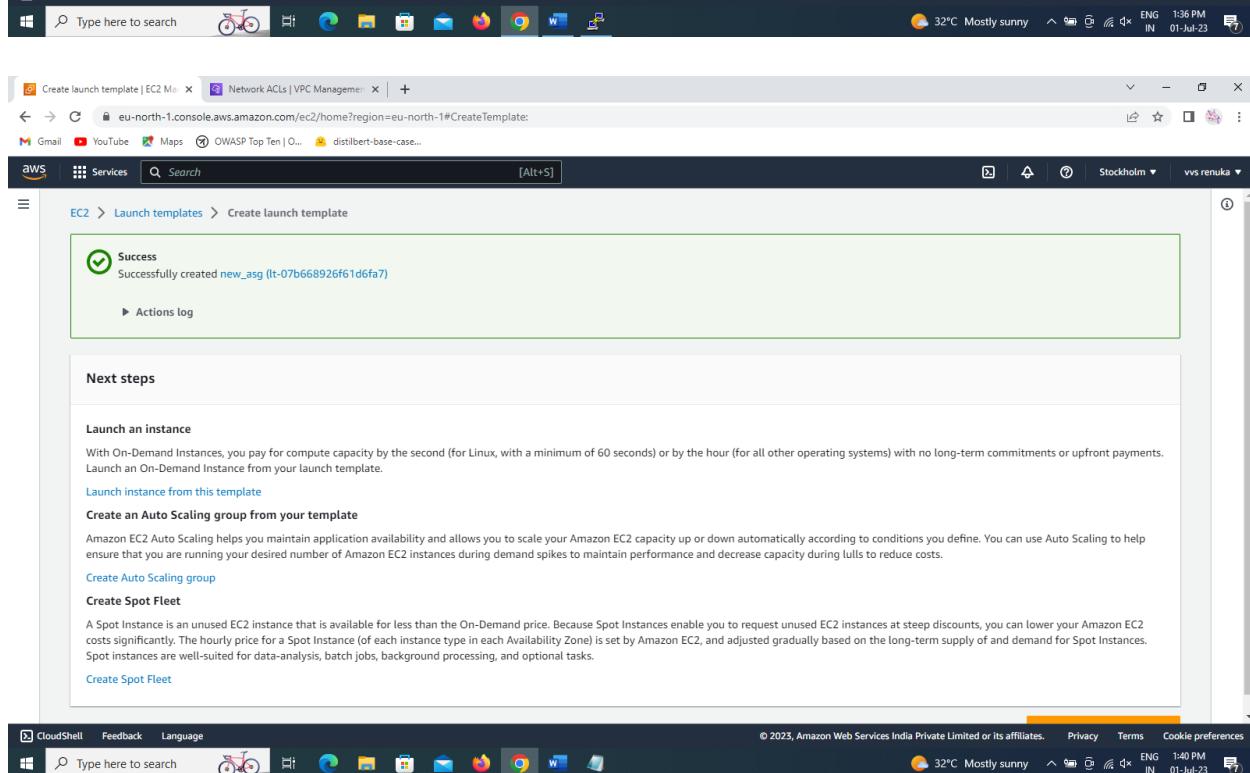
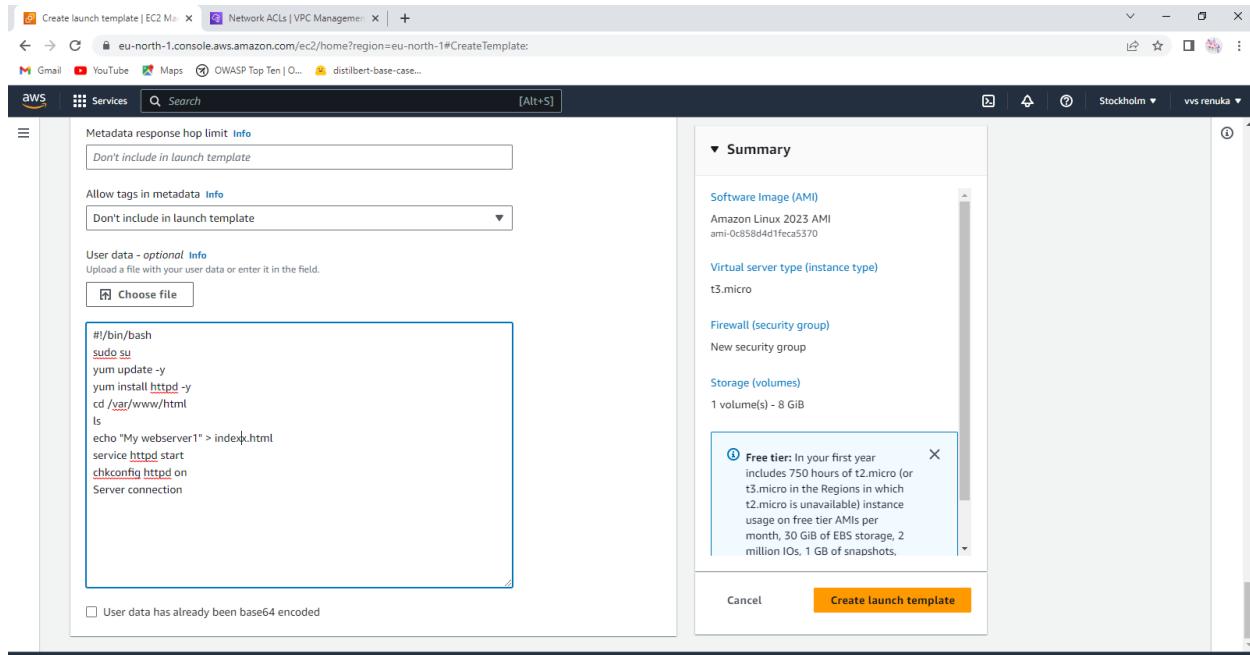
Anywhere 0.0.0.0/0 0.0.0.0/0

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 Advanced network configuration

Cancel Create launch template

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Mostly sunny ENG IN 1:35 PM 01-Jul-23



Next we have to create the classic elastic load balancer.

Screenshot of the AWS EC2 Management Console showing the Load Balancing section. The left sidebar lists services like Capacity Reservations, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. Under Load Balancing, the 'Load Balancers' tab is selected. A message states, "You do not have any load balancers in this region." Below this, a section titled "Select a load balancer" is shown.

Screenshot of the "Create Load Balancer" wizard. The first step, "Select CreateELBWizard:", shows three options: "Classic Load Balancer" (selected), "Network Load Balancer", and "Application Load Balancer". Each option has a brief description and a "Learn more >" link. The "Classic Load Balancer" section includes a "Create" button and a note about choosing it for existing EC2-Classic applications.

Screenshot of the Windows taskbar at the bottom of the screen, showing various pinned icons and the system tray.

Create Load Balancer | EC2 Manager | **Network ACLs | VPC Management** | + eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateELBWizard:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name: My_asg_elb
 Create LB Inside: vpc-0598766edb63d41bd (10.0.0.0/16) | My_VPC
 Create an internal load balancer: (what's this?)
 Enable advanced VPC configuration:

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

Add

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

VPC vpc-0598766edb63d41bd (10.0.0.0/16) | My_VPC

Please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

[Cancel](#) [Next: Assign Security Groups](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Partly sunny ENG IN 1:42 PM 01-Jul-23

Create Load Balancer | EC2 Manager | **Network ACLs | VPC Management** | + eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateELBWizard:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 1: Define Load Balancer

Basic Configuration

Create an internal load balancer: (what's this?)
 Enable advanced VPC configuration:

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

Add

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

VPC vpc-0598766edb63d41bd (10.0.0.0/16) | My_VPC

Available subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
eu-north-1a	subnet-0123c7f44c7e91533	10.0.1.0/24	10.0.1.0/24-1a-PUB	
eu-north-1b	subnet-0f723c804d4eca1a3	10.0.2.0/24	10.0.2.0/24-1b-PVT	

Selected subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
eu-north-1a	subnet-0123c7f44c7e91533	10.0.1.0/24	10.0.1.0/24-1a-PUB	
eu-north-1b	subnet-0f723c804d4eca1a3	10.0.2.0/24	10.0.2.0/24-1b-PVT	

[Cancel](#) [Next: Assign Security Groups](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Partly sunny ENG IN 1:43 PM 01-Jul-23

Create Load Balancer | EC2 Manager Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateELBWizard:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Ping Protocol: HTTP
Ping Port: 80
Ping Path: /indexxx.html

Advanced Details

Response Timeout: 2 seconds
Interval: 5 seconds
Unhealthy threshold: 2
Healthy threshold: 2

Cancel Previous Next: Add EC2 Instances

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

32°C Partly sunny ENG IN 1:45 PM 01-Jul-23

Create Load Balancer | EC2 Manager Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateELBWizard:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-0598766edb63d41bd (10.0.0.0/16) | My_VPC

Select	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-058d470efffdafddd	webserver	running	ws	eu-north-1a	subnet-0123c7f4...	10.0.1.0/24
<input type="checkbox"/>	i-06a7c263aa5e3adce	Database	running	DB	eu-north-1b	subnet-0f723c80...	10.0.2.0/24

Availability Zone Distribution
1 instance in eu-north-1a

Enable Cross-Zone Load Balancing
 Enable Connection Draining 300 seconds

Cancel Previous Next: Add Tags

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

32°C Partly sunny ENG IN 1:45 PM 01-Jul-23

Create Load Balancer | EC2 Manager Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateELBWizard:

Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S]

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Cancel Previous Next: Add Tags

Step 7: Review

Please review the load balancer details before continuing.

Define Load Balancer

Load Balancer name: My-asg-elb
Scheme: internet-facing
Port Configuration: 80 (HTTP) forwarding to 80 (HTTP)

Configure Health Check

Ping Target: HTTP 80/indexxx.html
Timeout: 2 seconds
Interval: 5 seconds
Unhealthy threshold: 2
Healthy threshold: 2

Add EC2 Instances

Cross-zone load balancing: Enabled
Connection Draining: Enabled, 300 seconds
Instances: i-058d470effffadddd (webserver)

VPC Information

VPC: [vpc-0598766edb63d41bd \(My_VPC\)](#)
Subnets: [subnet-0123c7f44c7a91533 \(10.0.1.0/24-1a-PUB\)](#), [subnet-0f723c804d4eca1a3 \(10.0.2.0/24-1b-PVT\)](#)

Security groups

Cancel Previous Create

Finally create an ASG and connect it the webserver in the public subnet to control the traffic.

Auto Scaling groups | EC2 Manager | Network ACLs | VPC Management | +

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#AutoScalingGroups:

CloudShell Feedback Language Type here to search 32°C Partly sunny 1:46 PM 01-Jul-23

Services Search [Alt+S]

aws Stockholm vvs renuka

Capacity Reservations

Images AMIs AMI Catalog

Elastic Block Store Volumes Snapshots Lifecycle Manager

Network & Security Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces

Load Balancing Load Balancers Target Groups

Auto Scaling Auto Scaling Groups

Amazon EC2 Auto Scaling helps maintain the availability of your applications

Create Auto Scaling group

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

Create Auto Scaling group

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.

How it works

Auto Scaling group

Pricing

Amazon EC2 Auto Scaling features have no additional fees beyond the service fees for Amazon EC2, CloudWatch (for scaling policies), and the other AWS resources that you use. Visit the pricing page of each service to learn more.

CloudShell Feedback Language Type here to search 32°C Partly sunny 1:46 PM 01-Jul-23

Select the launch template that we have created earlier.

Create Auto Scaling group | EC2 Network ACLs | VPC Management | + eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateAutoScalingGroup: Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S] Stockholm vvs renuka

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1 Choose launch template or configuration

Step 2 Choose instance launch options

Step 3 - optional Configure advanced options

Step 4 - optional Configure group size and scaling policies

Step 5 - optional Add notifications

Step 6 - optional Add tags

Step 7 Review

Choose launch template or configuration [Info](#)

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

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 255 characters.

Launch template [Info](#) **Switch to launch configuration**

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.
 [Create a launch template](#) [C](#)

Version
 [C](#) [Create a launch template version](#) [C](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Partly sunny ENG IN 1:47 PM 01-Jul-23

Create Auto Scaling group | EC2 Network ACLs | VPC Management | + eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateAutoScalingGroup: Gmail YouTube Maps OWASP Top Ten | O... distilbert-base-case...

aws Services Search [Alt+S] Stockholm vvs renuka

Configure advanced options

Step 4 - optional Configure group size and scaling policies

Step 5 - optional Add notifications

Step 6 - optional Add tags

Step 7 Review

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.
 [C](#) [Create a VPC](#) [C](#)

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.
 [C](#)

eu-north-1a | subnet-0123c7f44c7a91533 (10.0.1.0/24-1a-PUB)
10.0.1.0/24

eu-north-1b | subnet-0F723c804d4eca1a3 (10.0.2.0/24-1b-PVT)
10.0.2.0/24

[Create a subnet](#) [C](#)

Instance type requirements [Info](#) **Override launch template**

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Launch template	Version	Description
<input type="text" value="new_asg"/> C	Default	asg
lt-07b668926f61d6fa7		

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Partly sunny ENG IN 1:47 PM 01-Jul-23

Create Auto Scaling group | EC2 Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateAutoScalingGroup:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Choose instance launch options

Load balancing Info

Step 3 - optional

Configure advanced options

Step 4 - optional

Configure group size and scaling policies

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

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 from 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.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

Choose from your load balancer target groups
This option allows you to attach Application, Network, or Gateway Load Balancers.

Choose from Classic Load Balancers

Classic Load Balancers

Select Classic Load Balancers

My-asg-elb X

Classic Load Balancer

Health checks

Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback Language

Type here to search

32°C Partly sunny 1:48 PM 01-Jul-23 ENG IN

Create Auto Scaling group | EC2 Network ACLs | VPC Management

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateAutoScalingGroup:

Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Health checks

Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.

EC2 health checks

Always enabled

Additional health check types - optional

Turn on Elastic Load Balancing health checks Recommended
Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.

EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing.
To avoid unexpected terminations, first verify the settings of these health checks in the Load Balancer console.

Health check grace period Info
This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.

300 seconds

Additional settings

Monitoring Info

Enable group metrics collection within CloudWatch

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback Language

Type here to search

32°C Partly sunny 1:48 PM 01-Jul-23 ENG IN

Create Auto Scaling group | EC2 Network ACLs | VPC Management | + eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateAutoScalingGroup: Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1 Choose launch template or configuration

Step 2 Choose instance launch options

Step 3 - optional Configure advanced options

Step 4 - optional Configure group size and scaling policies

Step 5 - optional Add notifications

Step 6 - optional Add tags

Step 7 Review

Configure group size and scaling policies - optional Info

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

Group size - optional Info

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity

Minimum capacity

Maximum capacity

Scaling policies - optional

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. Info

Target tracking scaling policy Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

None

Scaling policy name

Metric type

Target value

Instances need seconds warm up before including in metric

Disable scale in to create only a scale-out policy

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Partly sunny ENG IN 1:49 PM 01-Jul-23

Create Auto Scaling group | EC2 Network ACLs | VPC Management | + eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateAutoScalingGroup: Gmail YouTube Maps OWASP Top Ten | O... distibert-base-case...

aws Services Search [Alt+S]

Scaling policies - optional

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. Info

Target tracking scaling policy Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

None

Scaling policy name

Metric type

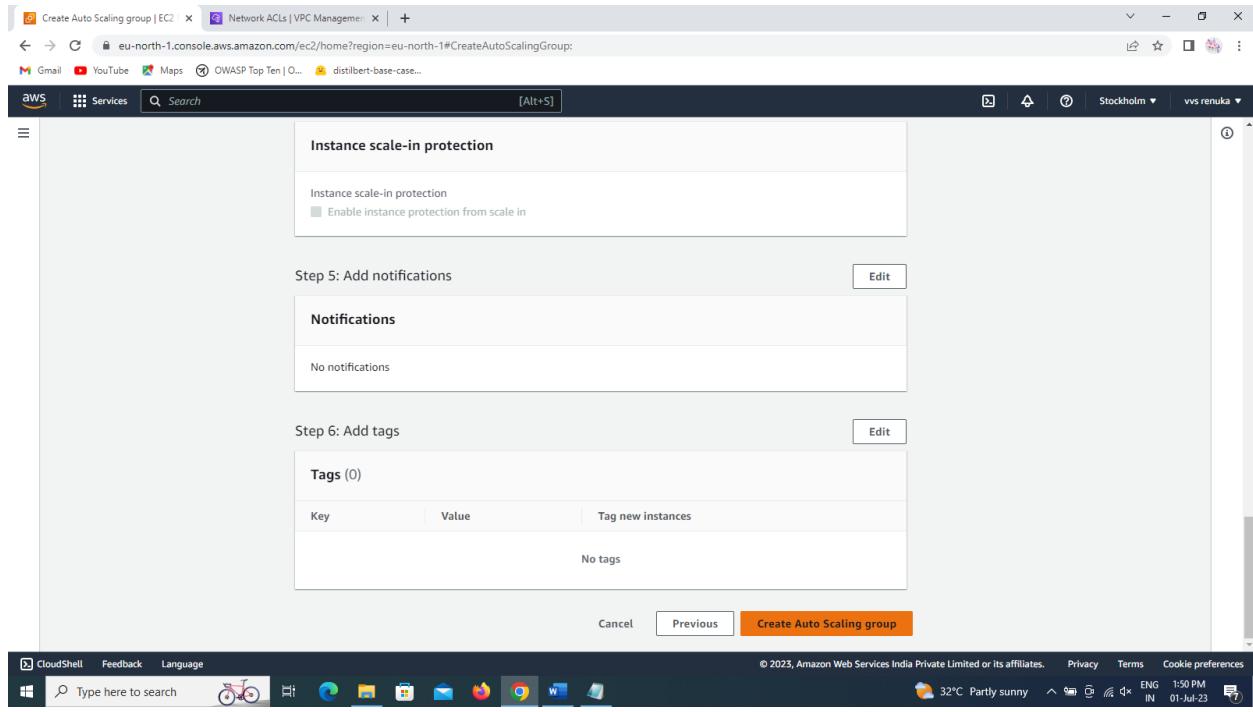
Target value

Instances need seconds warm up before including in metric

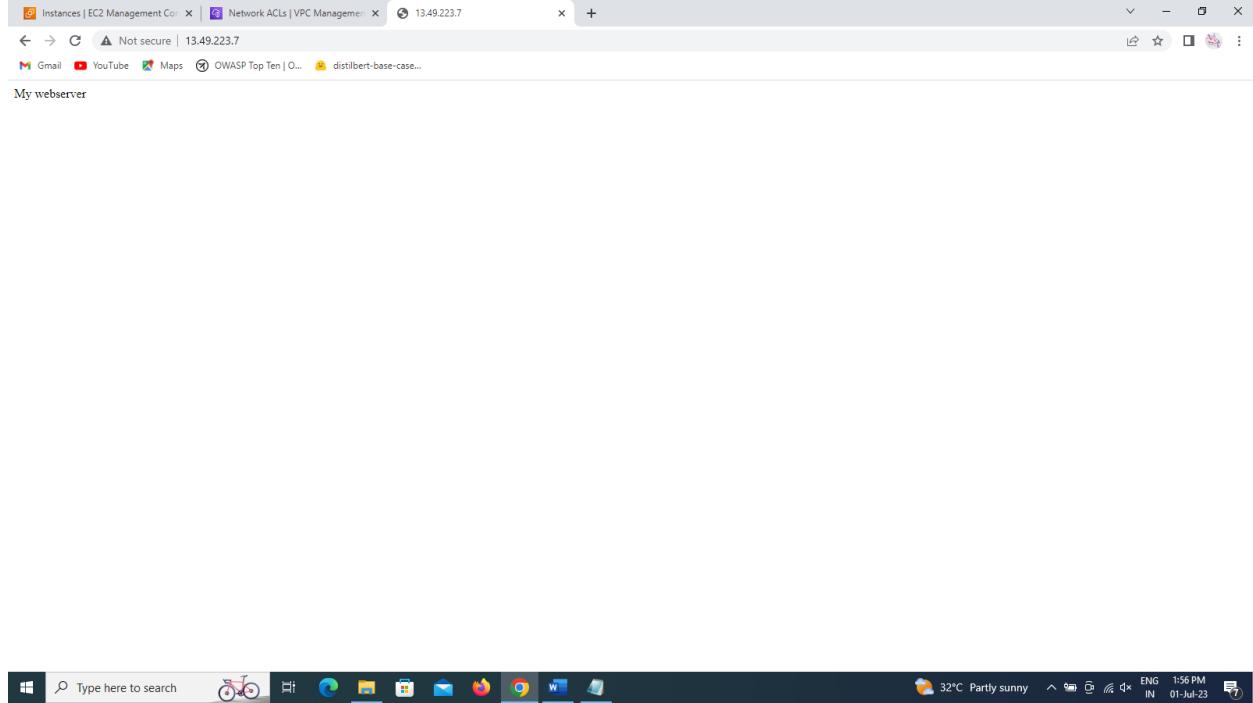
Disable scale in to create only a scale-out policy

Instance scale-in protection - optional

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Partly sunny ENG IN 1:50 PM 01-Jul-23



Now check the whether the webserver is working properly or not.



Finally we have successfully created the VPC Strucure.

Velampalli Venkata SushmaRenuka
Roll No:20JN1A05I2
AWS intern at Brainovision