Project:1 Deploy Scalable VPC Architecture on AWS cloud

TABLE OF CONTENTS

1.Goal

2.Pre-Requisites

3.Pre-Deployment

4.VPC Deployment

5.Validation

6.Solution

1.Pre-Requisites
2.You must be having an AWS account to create infrastructure resources on AWS cloud.
3.Source Code -

Pre-Deployment steps

1.AWS CLI

2.Install Apache Web Server

3.CloudWatch Agent installation

4.AWS logs configuration

5.Push custom memory metrics to Cloud Watch

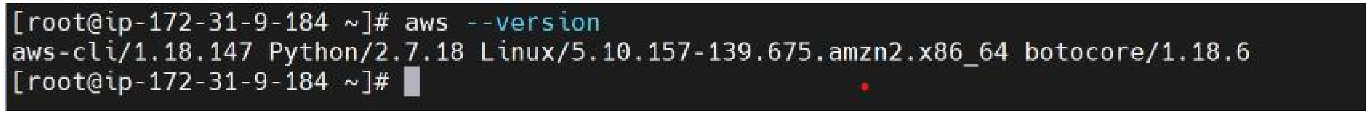
6.AWS SSM Agent

7.Creating Golden AMI

1.AWS CLI

AWS cli comes pre-installed when we use AWS AMI while launching the instance, to validate the version installed we can use #

aws - -version



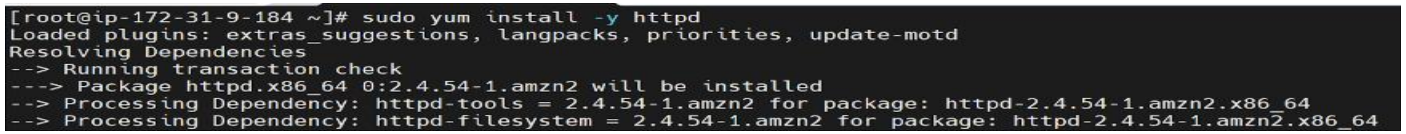
```
[root@ip-172-31-9-184 ~]# aws --version
aws-cli/1.18.147 Python/2.7.18 Linux/5.10.157-139.675.amzn2.x86_64 botocore/1.18.6
[root@ip-172-31-9-184 ~]#
```

2.Install Apache Web Server

To install Apache webserver on Amazon Linux use command #

yum install -y httpd

systemctl enable httpd



```
[root@ip-172-31-9-184 ~]# sudo yum install -y httpd
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
---> Package httpd.x86_64 0:2.4.54-1.amzn2 will be installed
--> Processing Dependency: httpd-tools = 2.4.54-1.amzn2 for package: httpd-2.4.54-1.amzn2.x86_64
--> Processing Dependency: httpd-filesystem = 2.4.54-1.amzn2 for package: httpd-2.4.54-1.amzn2.x86_64
```

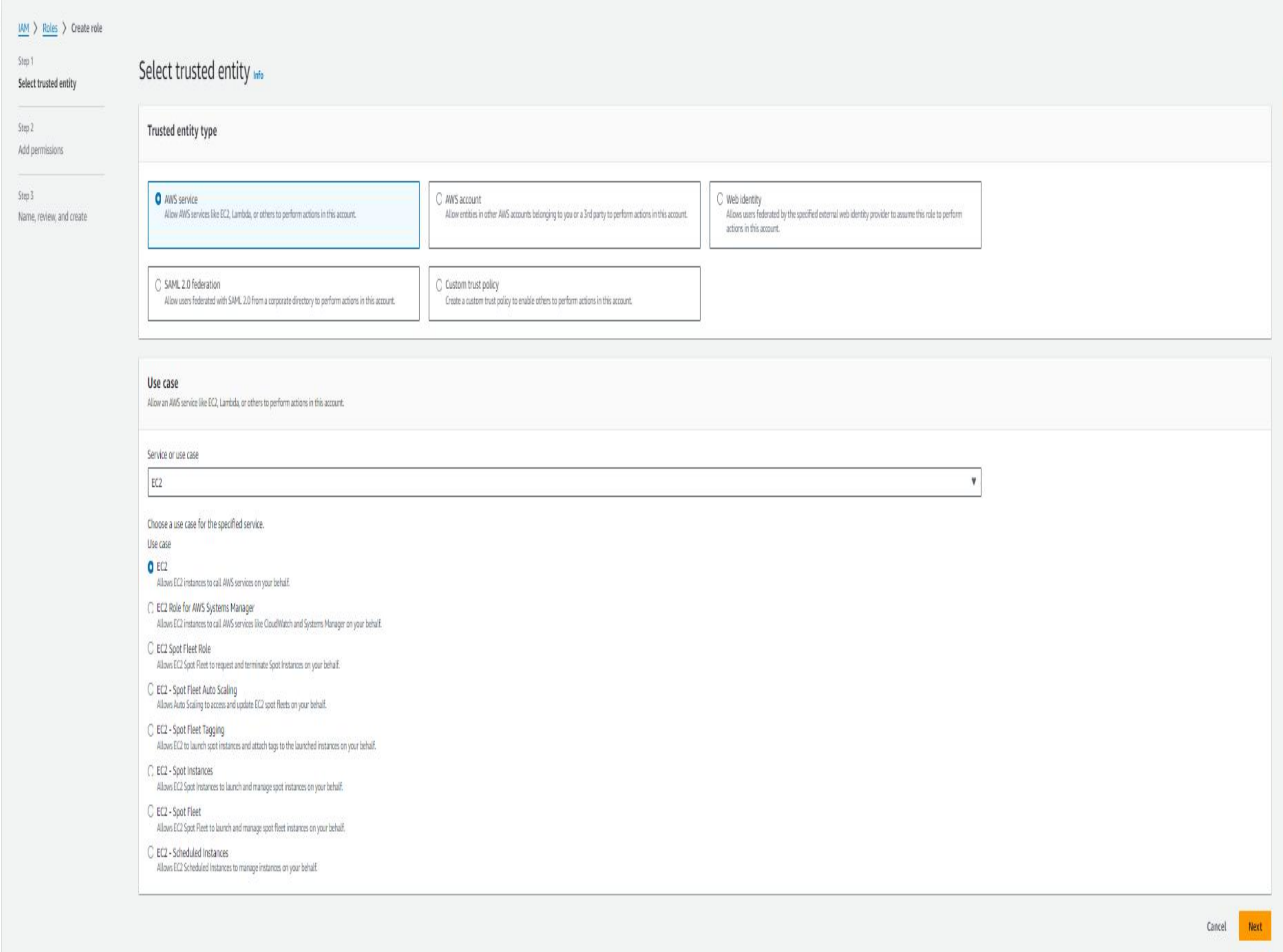
3.CloudWatch Agent

To install CloudWatch Agent on Amazon Linux use command

sudo yum install amazon-cloudwatch-agent
systemctl enable amazon-cloudwatch-agent

4.Create IAM Role for “Launch template” with permmisions

1.Cloudwatchfullaccess 2.sshfullaccess 3.s3fullaccess



Select trusted entity

Trusted entity type

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

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

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

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

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

Use case

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

Service or use case: EC2

Choose a use case for the specified service.

Use case

● EC2
Allows EC2 instances to call AWS services on your behalf.

○ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

○ EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

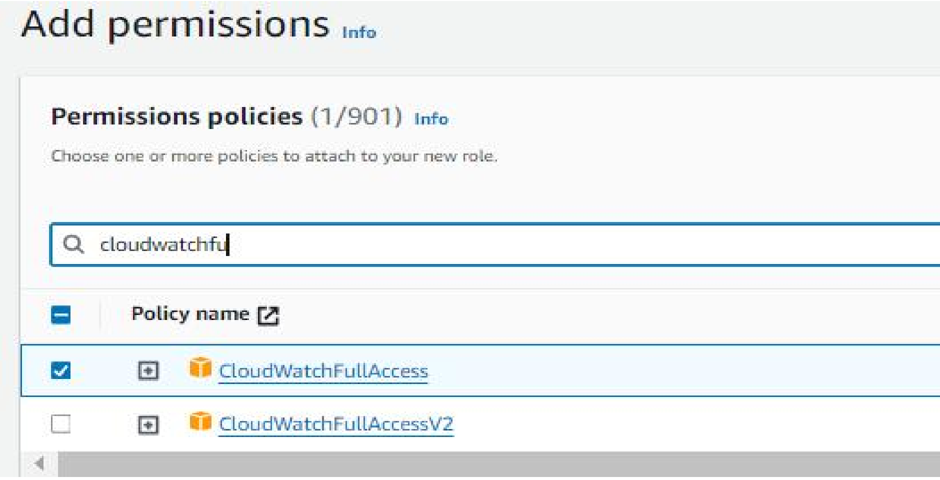
○ EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

○ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

○ EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

○ EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

○ EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.



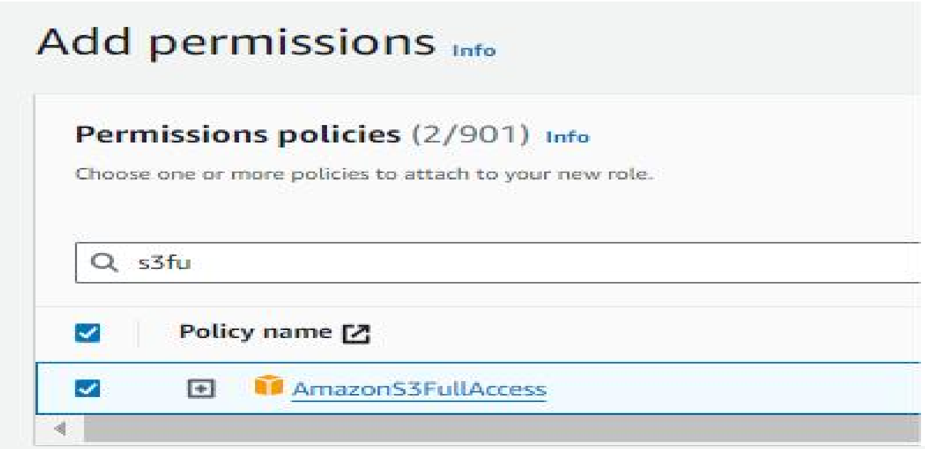
Add permissions

Permissions policies (1/901)

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

cloudwatchfu

	Policy name
☑	CloudWatchFullAccess
□	CloudWatchFullAccessV2



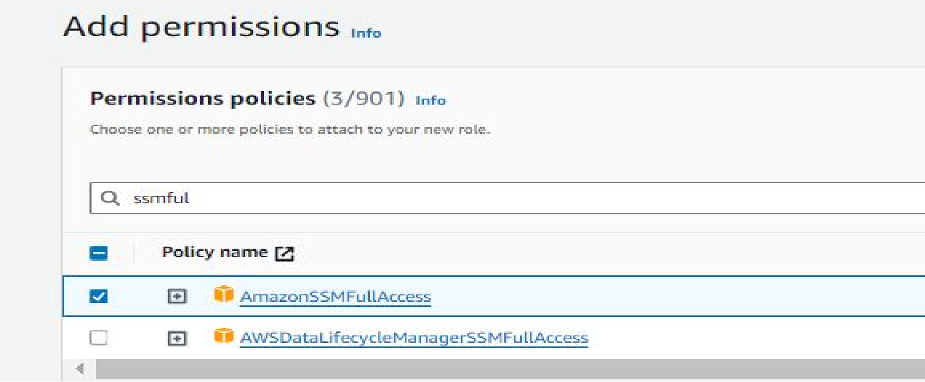
Add permissions

Permissions policies (2/901)

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

s3fu

☑	Policy name
☑	AmazonS3FullAccess



Add permissions

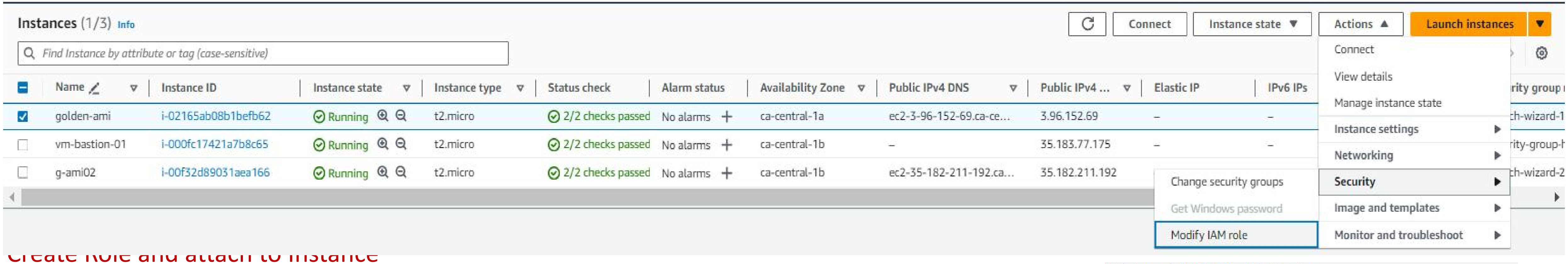
Permissions policies (3/901)

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

ssmful

	Policy name
☑	AmazonSSMFullAccess
□	AWSDataLifecycleManagerSSMFullAccess

5. Attach launch-template role to Golden instance



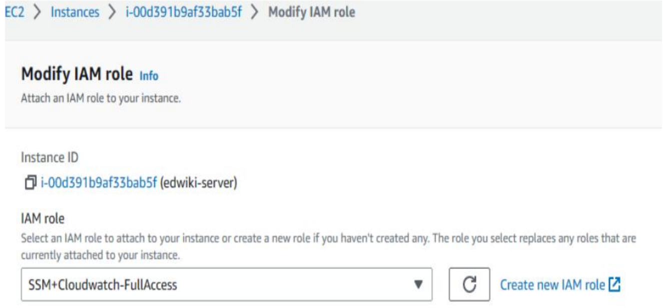
Instances (1/3) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	rity group
☑	golden-ami	i-02165ab08b1befb62	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1a	ec2-3-96-152-69.ca-ce...	3.96.152.69	–	–	ch-wizard-1
□	vm-bastion-01	i-000fc17421a7b8c65	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1b	–	35.183.77.175	–	–	rity-group-l
□	g-ami02	i-00f32d89031aea166	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1b	ec2-35-182-211-192.ca...	35.182.211.192			ch-wizard-2

- Create Role and attach to instance
- After attaching create a .json file
- In Golden-ami creator instance Navigate to “cd /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json”

vi amazon-cloudwatch-agent.json

- paste the following commands of memory-metrics and save it
- click on the link
- https://bitbucket.org/dptrealtime/devops-projects/src/master/VPC%20Architecture/memory_metrics.json



EC2 > Instances > i-00d391b9af33bab5f > Modify IAM role

Modify IAM role Info

Attach an IAM role to your instance.

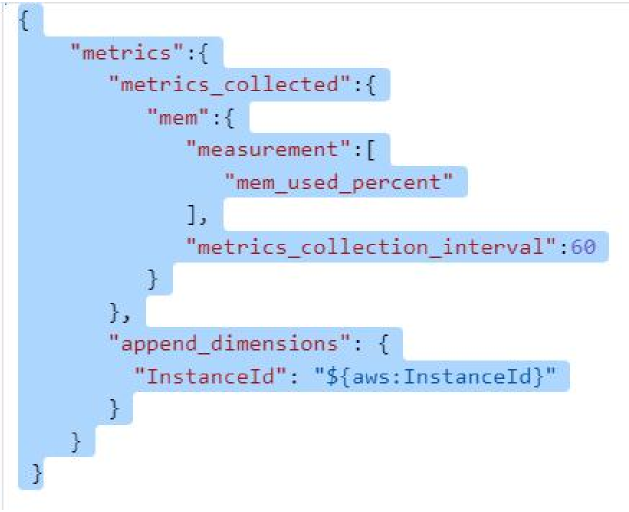
Instance ID

i-00d391b9af33bab5f (edwiki-server)

IAM role

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

SSM+Cloudwatch-FullAccess ▼

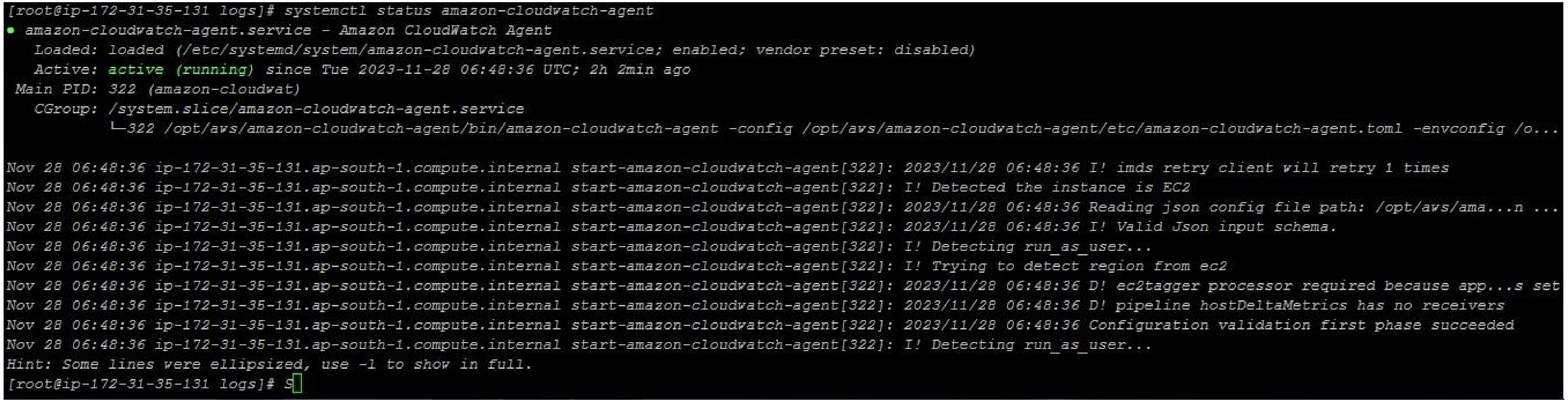


```
{
    "metrics":{
      "metrics_collected":{
        "mem":{
          "measurement":[
            "mem_used_percent"
          ],
          "metrics_collection_interval":60
        }
      },
      "append_dimensions": {
        "InstanceId": "${aws:InstanceId}"
      }
    }
}
```

7.Start CloudWatch Agent

```
systemctl restart amazon-cloudwatch-agent
systemctl status amazon-cloudwatch-agent
```

- output



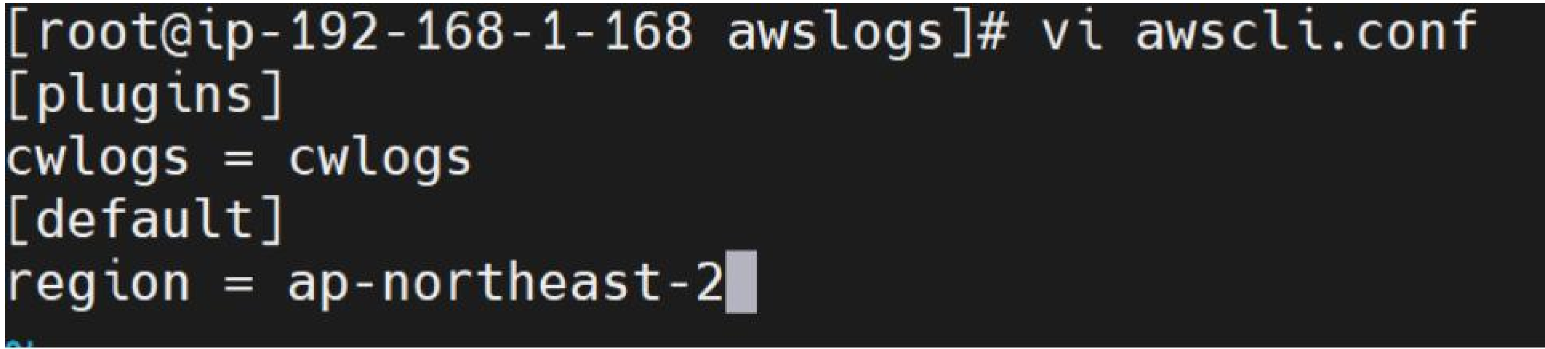
```
[root@ip-172-31-35-131 logs]# systemctl status amazon-cloudwatch-agent
● amazon-cloudwatch-agent.service - Amazon CloudWatch Agent
   Loaded: loaded (/etc/systemd/system/amazon-cloudwatch-agent.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-11-28 06:48:36 UTC; 2h 2min ago
 Main PID: 322 (amazon-cloudwat)
   CGroup: /system.slice/amazon-cloudwatch-agent.service
           └─322 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml -envconfig /o...

Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: 2023/11/28 06:48:36 I! imds retry client will retry 1 times
Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: I! Detected the instance is EC2
Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: 2023/11/28 06:48:36 Reading json config file path: /opt/aws/ama...n ...
Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: 2023/11/28 06:48:36 I! Valid Json input schema.
Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: I! Detecting run_as_user...
Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: I! Trying to detect region from ec2
Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: 2023/11/28 06:48:36 D! ec2tagger processor required because app...s set
Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: 2023/11/28 06:48:36 D! pipeline hostDeltaMetrics has no receivers
Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: 2023/11/28 06:48:36 Configuration validation first phase succeeded
Nov 28 06:48:36 ip-172-31-35-131.ap-south-1.compute.internal start-amazon-cloudwatch-agent[322]: I! Detecting run_as_user...
Hint: Some lines were ellipsized, use -l to show in full.
[root@ip-172-31-35-131 logs]# S
```

8.AWS logs

```
yum install awslogs -y
vi /etc/awslogs/awscli.conf
```

- Replace the existing region with

your preffered region

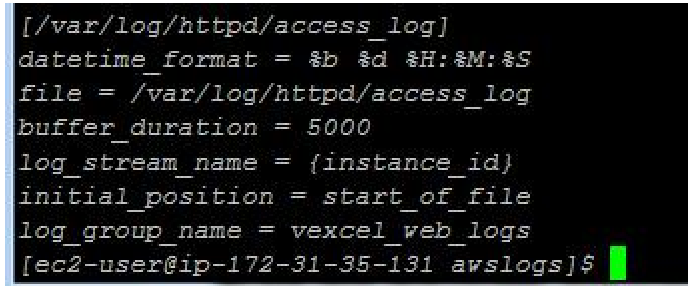


```
[root@ip-192-168-1-168 awslogs]# vi awscli.conf
[plugins]
cwlogs = cwlogs
[default]
region = ap-northeast-2
```

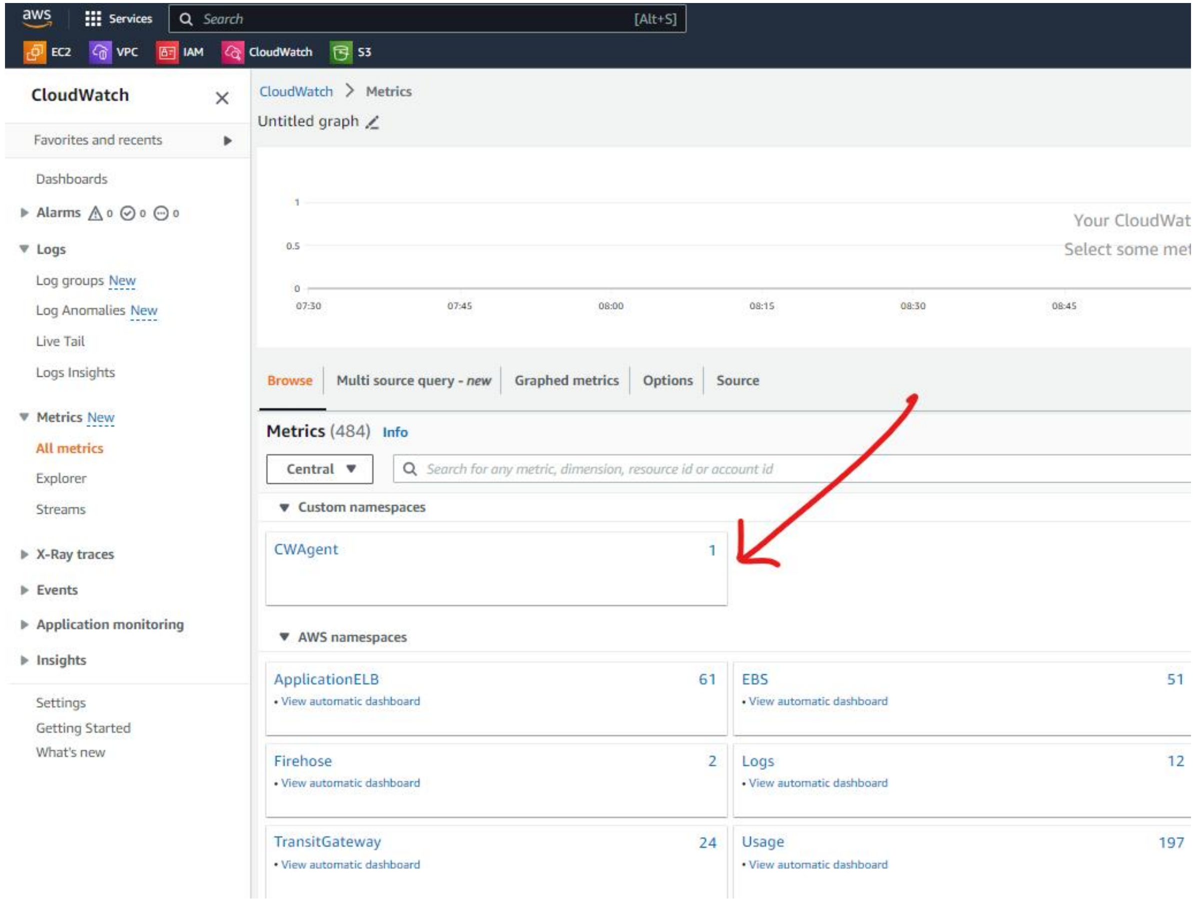
- edit awslogs .conf file and replace
- vi /etc/awslogs/awslogs.conf
- navigate to bottom table

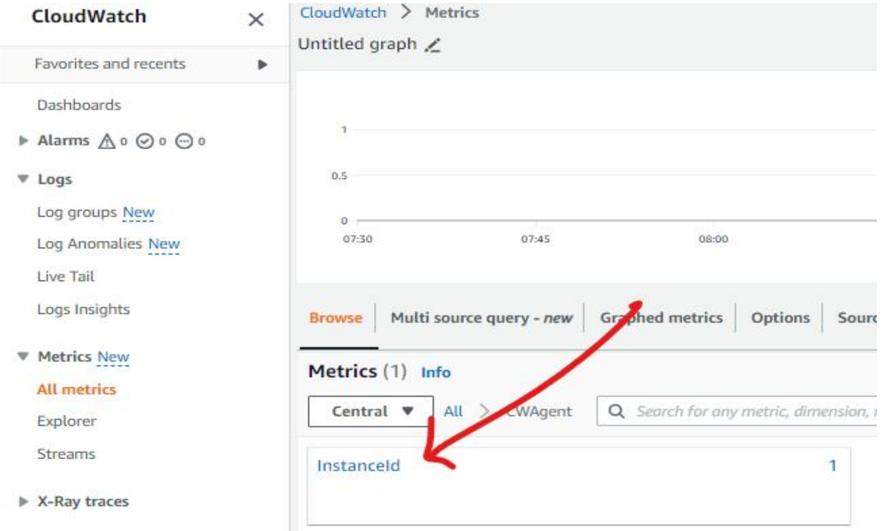
sudo service awslogsd start

or sudo service awslogsd restart



```
[/var/log/httpd/access_log]
datetime_format = %b %d %H:%M:%S
file = /var/log/httpd/access_log
buffer_duration = 5000
log_stream_name = {instance_id}
initial_position = start_of_file
log_group_name = vexcel_web_logs
[ec2-user@ip-172-31-35-131 awslogs]$ 
```





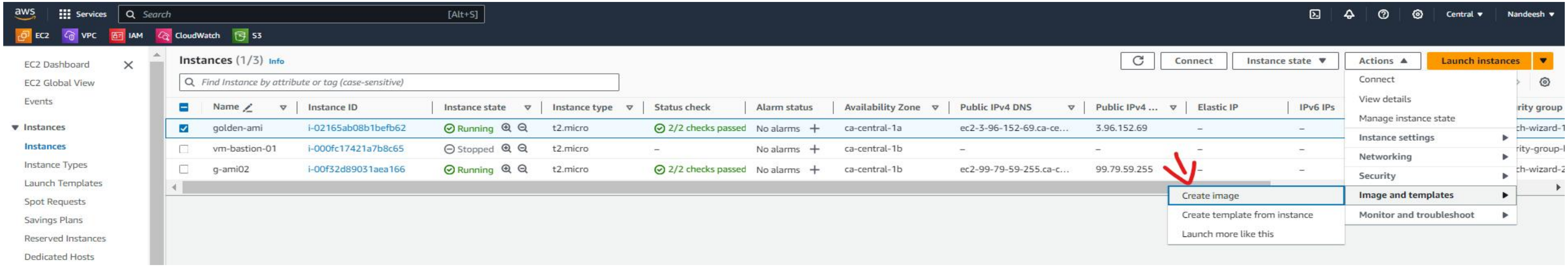
After all of this Configurations we can see that our cloud-watch-agent is pushing the log from instance to cloudwatch service in aws

10. AWS SSM Agent

```
yum install amazon-ssm-agent
systemctl start amazon-ssm-agent
systemctl status amazon-ssm-agent
systemctl enable amazon-ssm-agent
```

11.Creating Golden AMI

- Select you EC2 instance à instance state à stop
- Select you EC2 instance à Actions à image and templates à Create image

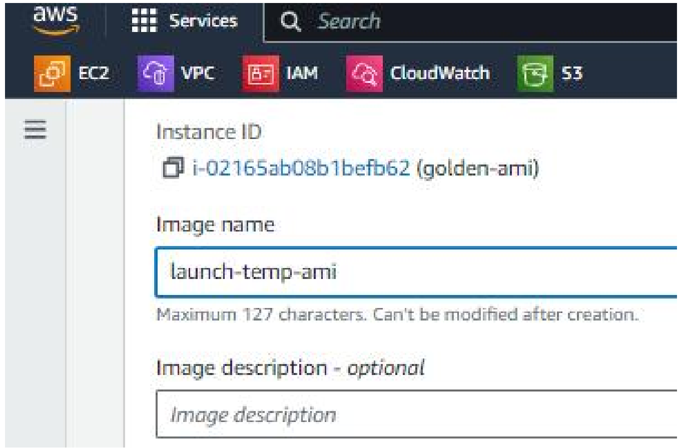


Instances (1/3) Info

Find Instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	...rity group
☑	golden-ami	i-02165ab08b1befb62	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1a	ec2-3-96-152-69.ca-ce...	3.96.152.69	–	–	...h-wizard-1
□	vm-bastion-01	i-000fc17421a7b8c65	Stopped	t2.micro	–	No alarms	ca-central-1b	–	–	–	–	...rity-group-l
□	g-ami02	i-00f32d89031aea166	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1b	ec2-99-79-59-255.ca-c...	99.79.59.255	–	–	...h-wizard-2

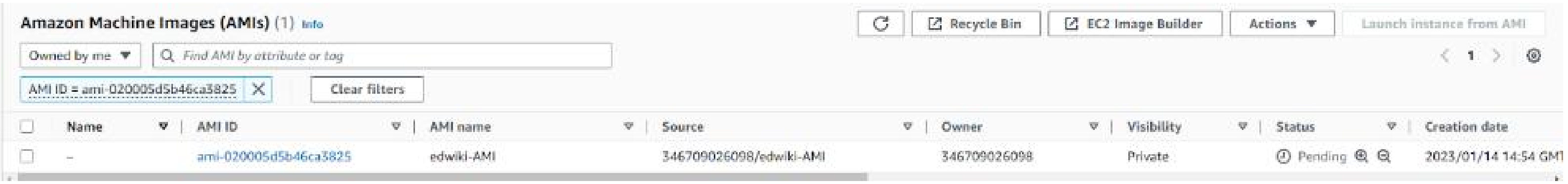
- create the image after configuring all of the pre-requisities with standard name to identify easily.



Instance ID
i-02165ab08b1befb62 (golden-ami)

Image name
launch-temp-ami
Maximum 127 characters. Can't be modified after creation.

Image description - *optional*
Image description



Amazon Machine Images (AMIs) (1) Info

Find AMI by attribute or tag

AMI ID = ami-020005d5b46ca3825

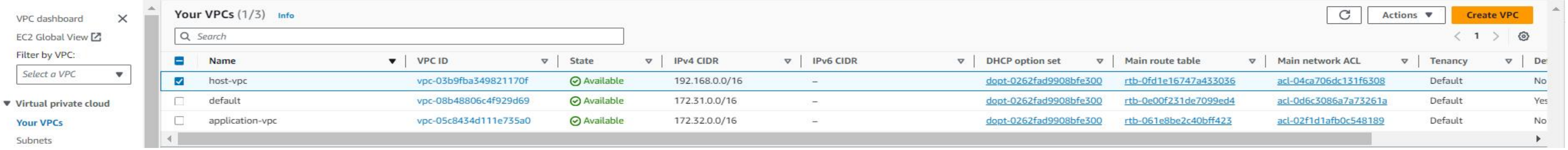
□	Name	AMI ID	AMI name	Source	Owner	Visibility	Status	Creation date
□	–	ami-020005d5b46ca3825	edwiki-AMI	346709026098/edwiki-AMI	346709026098	Private	Pending	2023/01/14 14:54 GMT

- you can now see the AMI’s created

vpc - Deployment

1.Creating VPC : we are creating 2 diff vpc’s as Private vpc or application vpc and Jump-host VPC

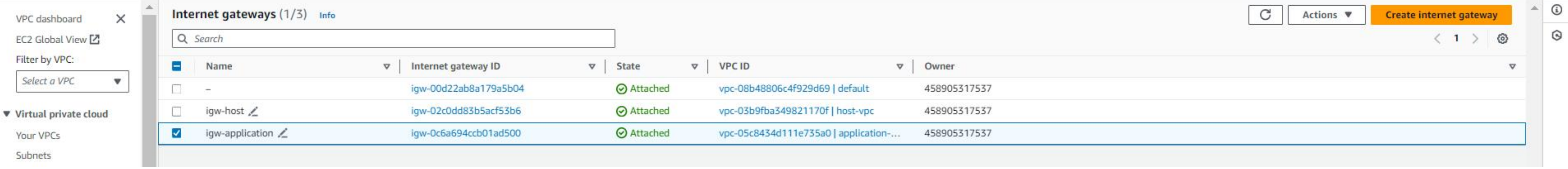
- Navigate to services in aws console and search for VPC and Create a VPC with IP address 192.168.0.0/16 and name “Host-vpc”
- Create another VPC for application server with IP address 172.32.0.0/16 and name “Application vpc”.



Your VPCs (1/3) Info

☐	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network ACL	Tenancy	De
☑	host-vpc	vpc-03b9fba349821170f	Available	192.168.0.0/16	–	dopt-0262fad9908bfe300	rtb-0fd1e16747a433036	acl-04ca706dc131f6308	Default	No
☐	default	vpc-08b48806c4f929d69	Available	172.31.0.0/16	–	dopt-0262fad9908bfe300	rtb-0e00f231de7099ed4	acl-0d6c3086a7a73261a	Default	Yes
☐	application-vpc	vpc-05c8434d111e735a0	Available	172.32.0.0/16	–	dopt-0262fad9908bfe300	rtb-061e8be2c40bff423	acl-02f1d1afb0c548189	Default	No

2.Creating Internet Gateways :Navigate to Internet gateway below your vpc’s toolbar. Create 2 Internet gateways for both Host and application VPC and attach to it them.



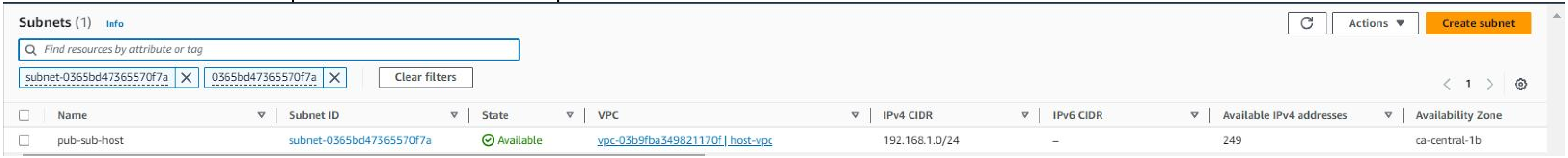
Internet gateways (1/3) Info

☐	Name	Internet gateway ID	State	VPC ID	Owner
☐	–	igw-00d22ab8a179a5b04	Attached	vpc-08b48806c4f929d69 | default	458905317537
☐	igw-host	igw-02c0dd83b5acf53b6	Attached	vpc-03b9fba349821170f | host-vpc	458905317537
☑	igw-application	igw-0c6a694ccb01ad500	Attached	vpc-05c8434d111e735a0 | application-...	458905317537

3.Creating Subnets : Navigate to subnets in Left toolbar and click on create subnets. We are creating 1 subnet for “host-vpc” and 4 subnets for “application-vpc”

- In “application-vpc” we need to create 2 subnets in one Availabilty Zone-1a and another in Availabilty Zone-1b for the High availabilty
- in Availabilty Zone-1a create one public subnet and private subnet, Follow the same for Availabilty Zone-1b

- “Pub-sub-host” is the public subnet for Host-vpc.



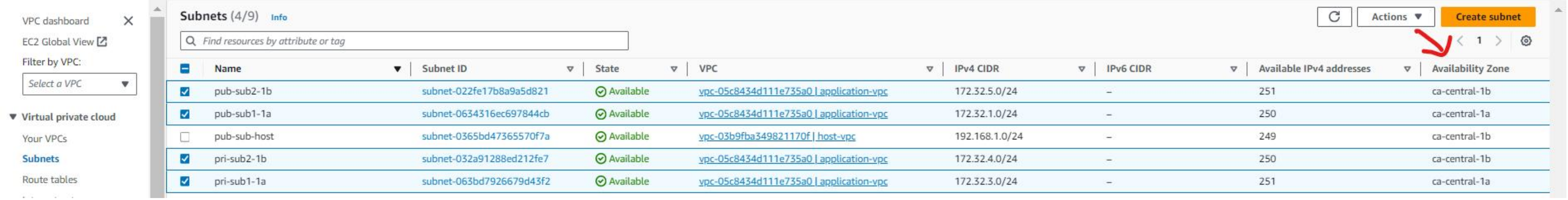
Subnets (1)

Find resources by attribute or tag

subnet-0365bd47365570f7a ✕ 0365bd47365570f7a ✕

□	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone
□	pub-sub-host	subnet-0365bd47365570f7a	✓ Available	vpc-03b9fba349821170f | host-vpc	192.168.1.0/24	–	249	ca-central-1b

- “pub-sub1-1a” and “pri-sub1-1a” is public and private subnets for Availability Zone 1a.



Subnets (4/9)

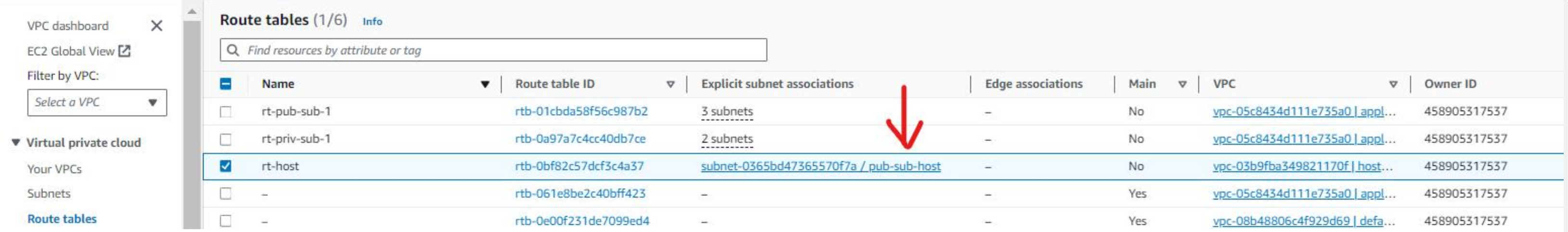
Find resources by attribute or tag

☐	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone
☑	pub-sub2-1b	subnet-022fe17b8a9a5d821	✓ Available	vpc-05c8434d111e735a0 | application-vpc	172.32.5.0/24	–	251	ca-central-1b
☑	pub-sub1-1a	subnet-0634316ec697844cb	✓ Available	vpc-05c8434d111e735a0 | application-vpc	172.32.1.0/24	–	250	ca-central-1a
□	pub-sub-host	subnet-0365bd47365570f7a	✓ Available	vpc-03b9fba349821170f | host-vpc	192.168.1.0/24	–	249	ca-central-1b
☑	pri-sub2-1b	subnet-032a91288ed212fe7	✓ Available	vpc-05c8434d111e735a0 | application-vpc	172.32.4.0/24	–	250	ca-central-1b
☑	pri-sub1-1a	subnet-063bd7926679d43f2	✓ Available	vpc-05c8434d111e735a0 | application-vpc	172.32.3.0/24	–	251	ca-central-1a

- “pub-sub2-1b” and “pri-sub2-1b” is public and private subnets for Availability Zone 1b

4. Creating Route Tables : Navigate to Route tables section in left side of vpc toolbar and create 3 Route Tables

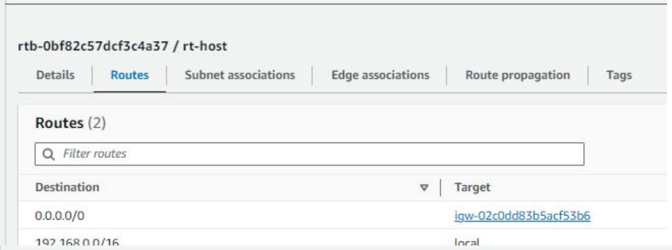
- “Rt-host” is for “host-vpc” and associate subnet “Pub-sub-host”.



Route tables (1/6)

Find resources by attribute or tag

☐	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
□	rt-pub-sub-1	rtb-01cbda58f56c987b2	3 subnets	–	No	vpc-05c8434d111e735a0 | appl...	458905317537
□	rt-priv-sub-1	rtb-0a97a7c4cc40db7ce	2 subnets	–	No	vpc-05c8434d111e735a0 | appl...	458905317537
☑	rt-host	rtb-0bf82c57dcf3c4a37	subnet-0365bd47365570f7a / pub-sub-host	–	No	vpc-03b9fba349821170f | host...	458905317537
□	–	rtb-061e8be2c40bff423	–	–	Yes	vpc-05c8434d111e735a0 | appl...	458905317537
□	–	rtb-0e00f231de7099ed4	–	–	Yes	vpc-08b48806c4f929d69 | defa...	458905317537



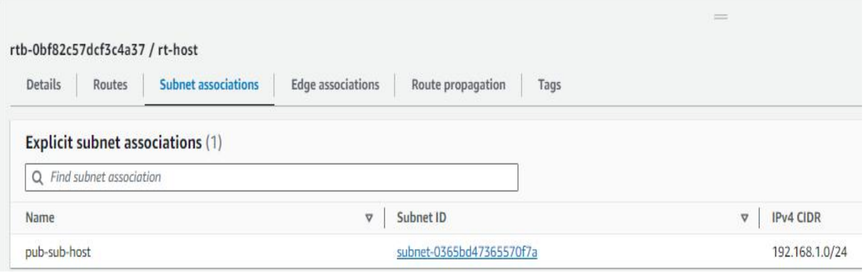
rtb-0bf82c57dcf3c4a37 / rt-host

Routes (2)

Filter routes

Destination	Target
0.0.0.0/0	igw-02c0dd83b5acf53b6
192.168.0.0/16	local

- Routes->edit routes and attach “rt-host” to internet gateway destination-0.0.0.0/0
- Subnet association-> edit associations attach->”pub-sub-host”



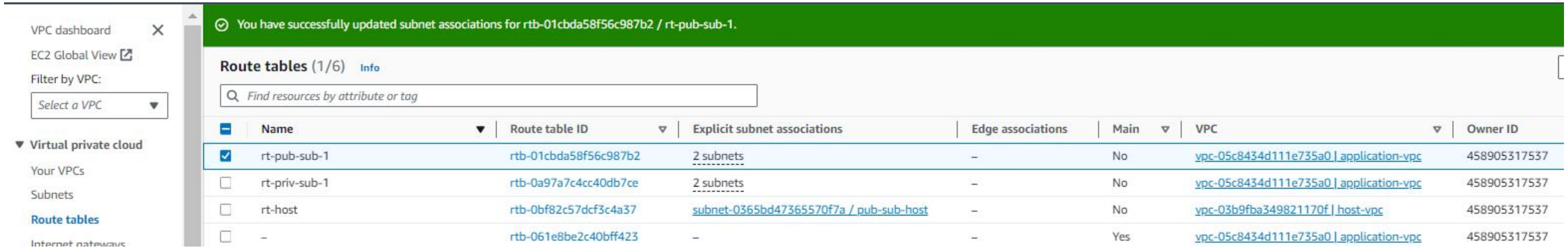
rtb-0bf82c57dcf3c4a37 / rt-host

Explicit subnet associations (1)

Find subnet association

Name	Subnet ID	IPv4 CIDR
pub-sub-host	subnet-0365bd47365570f7a	192.168.1.0/24

- create 2 route tables for “application-vpc”
- “rt-pub-application” is for Public subnet “pub-sub1-1a” and “pub-sub2-1b”.



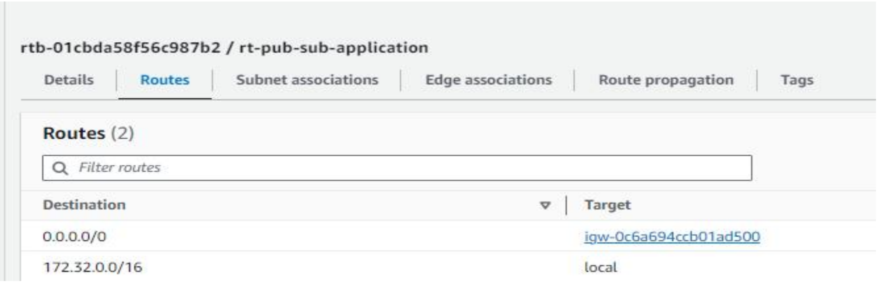
You have successfully updated subnet associations for rtb-01cbda58f56c987b2 / rt-pub-sub-1.

Route tables (1/6) Info

Find resources by attribute or tag

☐	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
☑	rt-pub-sub-1	rtb-01cbda58f56c987b2	2 subnets	–	No	vpc-05c8434d111e735a0 | application-vpc	458905317537
☐	rt-priv-sub-1	rtb-0a97a7c4cc40db7ce	2 subnets	–	No	vpc-05c8434d111e735a0 | application-vpc	458905317537
☐	rt-host	rtb-0bf82c57dcf3c4a37	subnet-0365bd47365570f7a / pub-sub-host	–	No	vpc-03b9fba349821170f | host-vpc	458905317537
☐	–	rtb-061e8be2c40bff423	–	–	Yes	vpc-05c8434d111e735a0 | application-vpc	458905317537

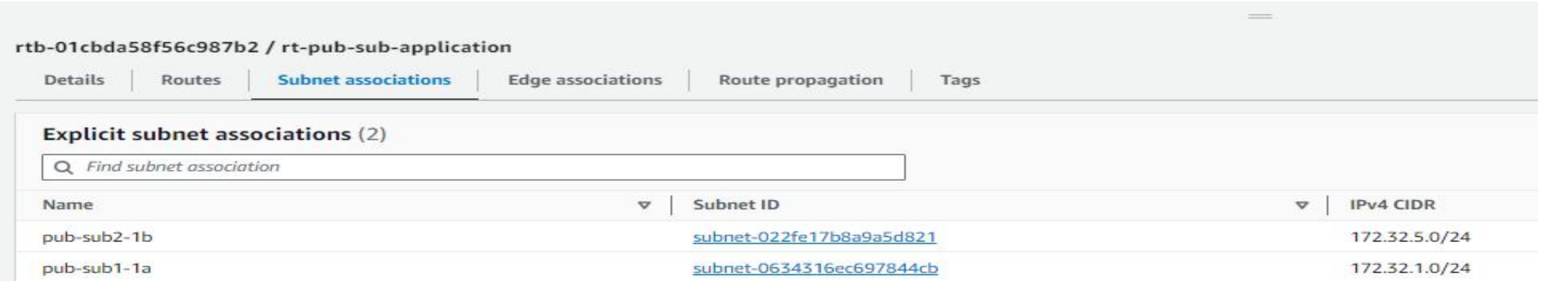
- Routes->edit routes and attach “rt-pub-application” to internet gateway --> destination 0.0.0.0/0


rtb-01cbda58f56c987b2 / rt-pub-sub-application

Routes (2)

Filter routes

Destination	Target
0.0.0.0/0	igw-0c6a694ccb01ad500
172.32.0.0/16	local

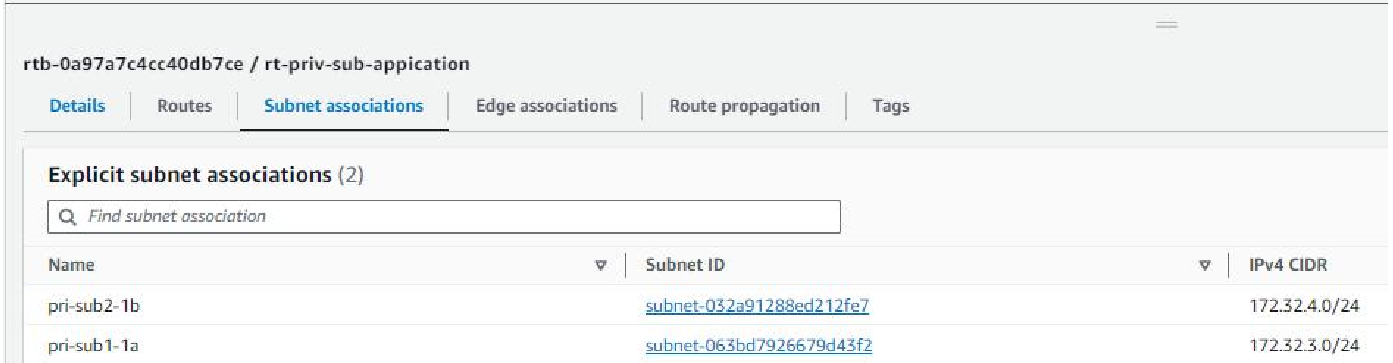

rtb-01cbda58f56c987b2 / rt-pub-sub-application

Explicit subnet associations (2)

Find subnet association

Name	Subnet ID	IPv4 CIDR
pub-sub2-1b	subnet-022fe17b8a9a5d821	172.32.5.0/24
pub-sub1-1a	subnet-0634316ec697844cb	172.32.1.0/24

- “rt-pri-application” is for Private subnet “pri-sub1-1a” and “pri-sub2-1b”.


rtb-0a97a7c4cc40db7ce / rt-priv-sub-appication

Explicit subnet associations (2)

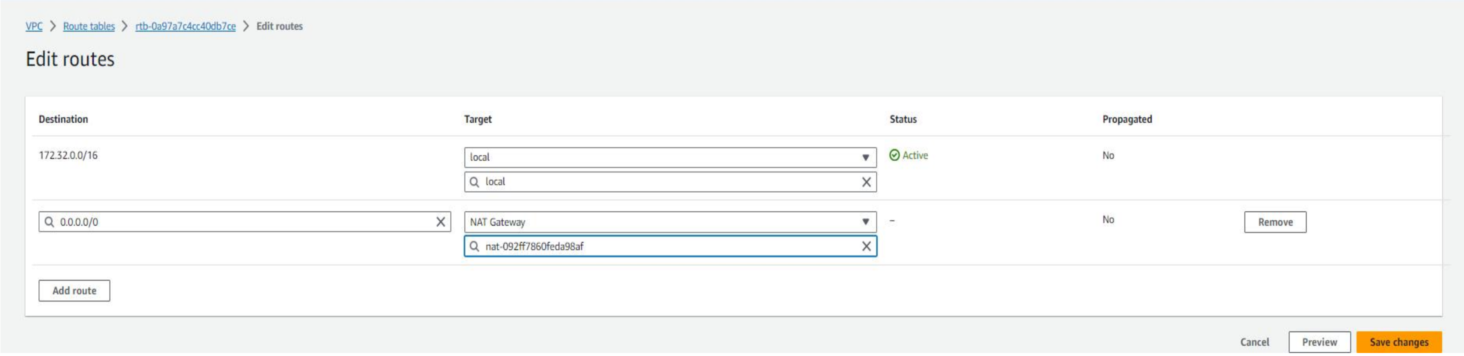
Find subnet association

Name	Subnet ID	IPv4 CIDR
pri-sub2-1b	subnet-032a91288ed212fe7	172.32.4.0/24
pri-sub1-1a	subnet-063bd7926679d43f2	172.32.3.0/24

- Note: internet access for private subnet should be redirected to Nat-Gateway- It allows only outbound rules and blocks all inbound traffic in order to safeguard the data from when exposed to internet.

5.NAT-Gateway: VPC -> Nat gateways -> Create NAT gateway-> Provide Name -> Subnet details and allocate elastic ip

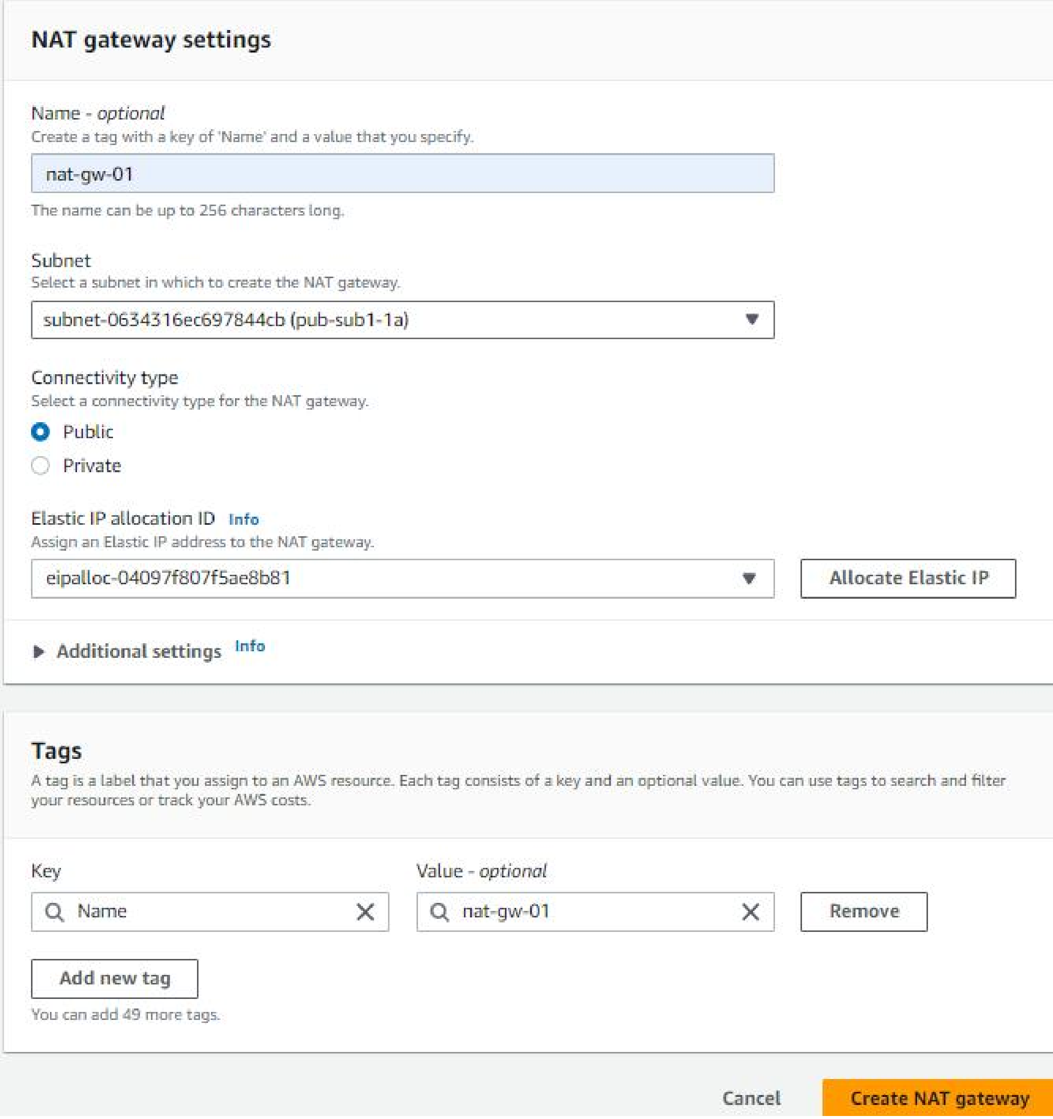
- Select any public-subnet-application
- Edit Route table- “rt-pri-application” and attach “nat-gw-01”



VPC > Route tables > rtb-0a97a7c4cc40db7ce > Edit routes

Edit routes

Destination	Target	Status	Propagated	
172.32.0.0/16	local local	✓ Active	No	
0.0.0.0/0	NAT Gateway nat-092ff7860feda98af	-	No	Remove



NAT gateway settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
nat-gw-01
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0634316ec697844cb (pub-sub1-1a)

Connectivity type
Select a connectivity type for the NAT gateway.
● Public
○ Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-04097f807f5ae8b81

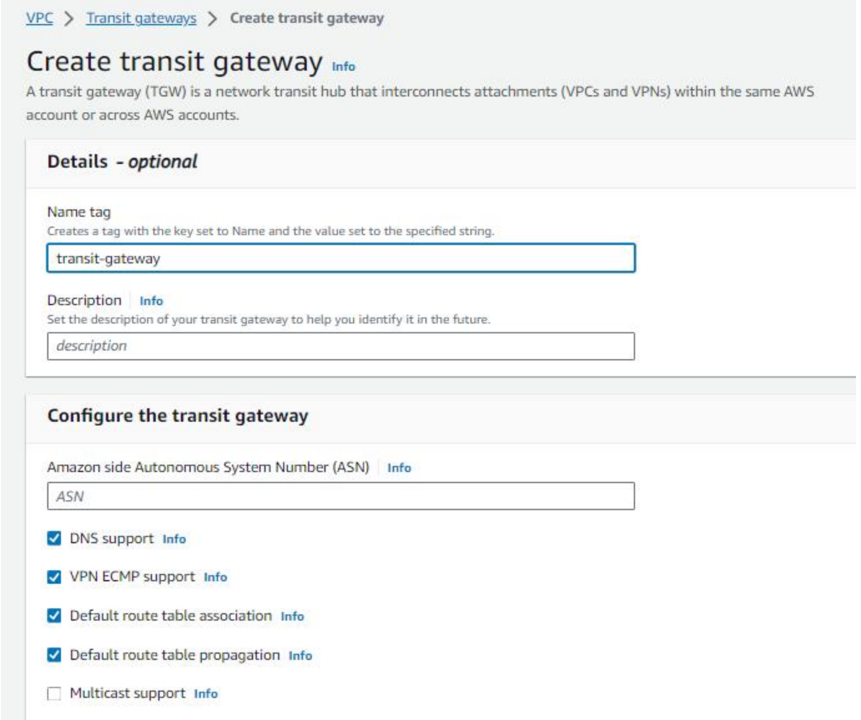
Tags

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 - *optional*	
Name	nat-gw-01	Remove

You can add 49 more tags.

6.Create Transit Gateway : Navigate to Transit-gateway and create



VPC > Transit gateways > Create transit gateway

Create transit gateway Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details - *optional*

Name tag
Creates a tag with the key set to Name and the value set to the specified string.
transit-gateway

Description Info
Set the description of your transit gateway to help you identify it in the future.
description

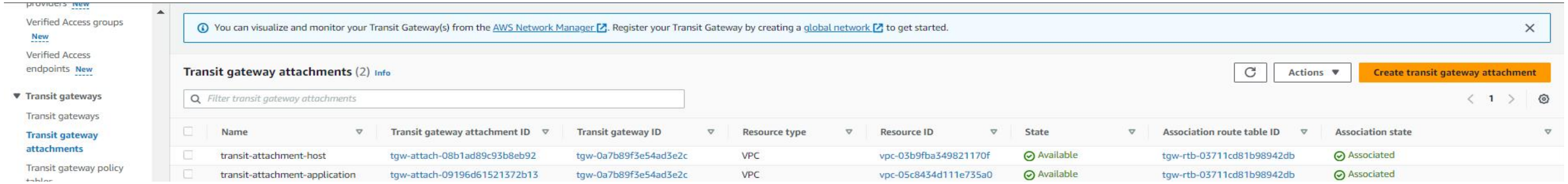
Configure the transit gateway

Amazon side Autonomous System Number (ASN) Info
ASN

☑ DNS support Info
☑ VPN ECMP support Info
☑ Default route table association Info
☑ Default route table propagation Info
□ Multicast support Info

7.Transit-gateway attachments : Navigate to transit gateway attachments-->create

- Create 2 transit gateways -


providers New
Verified Access groups New
Verified Access endpoints New
▼ Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Actions ▼
Create transit gateway attachment
Filter transit gateway attachments
< 1 >

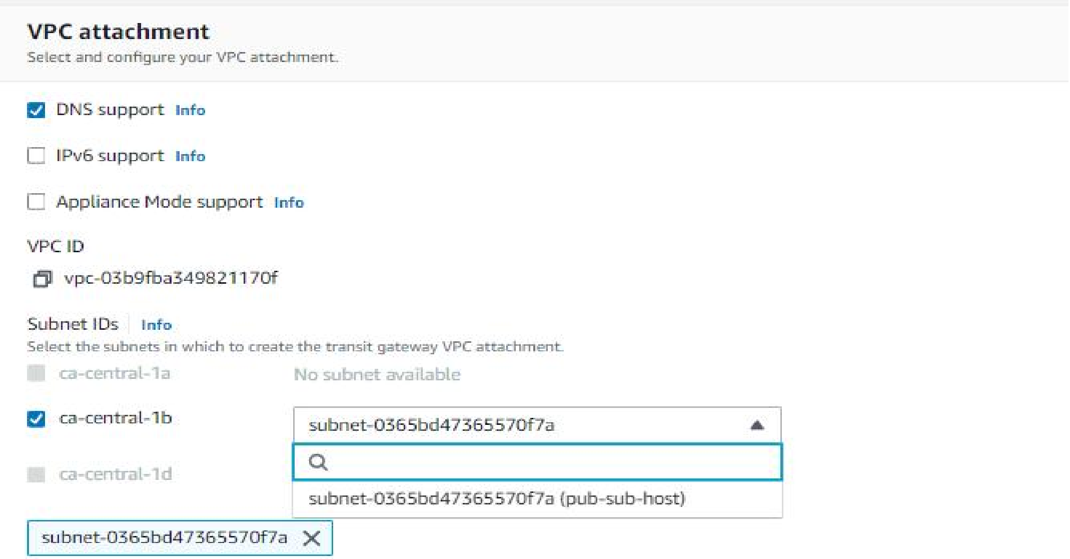
You can visualize and monitor your Transit Gateway(s) from the AWS Network Manager. Register your Transit Gateway by creating a global network to get started.

Transit gateway attachments (2) Info

	Name	Transit gateway attachment ID	Transit gateway ID	Resource type	Resource ID	State	Association route table ID	Association state
□	transit-attachment-host	tgw-attach-08b1ad89c93b8eb92	tgw-0a7b89f3e54ad3e2c	VPC	vpc-03b9fba349821170f	✓ Available	tgw-rtb-03711cd81b98942db	✓ Associated
□	transit-attachment-application	tgw-attach-09196d61521372b13	tgw-0a7b89f3e54ad3e2c	VPC	vpc-05c8434d111e735a0	✓ Available	tgw-rtb-03711cd81b98942db	✓ Associated

- 1.transit-attachment-host = Select to “host-vpc” and subnet “Pub-sub-host”
- 2.transit-attachment-application = Select to ““application-vpc” and private subnets “pri-sub1-1a” and “pri-sub2-1b”.

transit-attachment-host



VPC attachment

Select and configure your VPC attachment.

☑ DNS support Info

□ IPv6 support Info

□ Appliance Mode support Info

VPC ID

vpc-03b9fba349821170f

Subnet IDs Info

Select the subnets in which to create the transit gateway VPC attachment.

□ ca-central-1a No subnet available

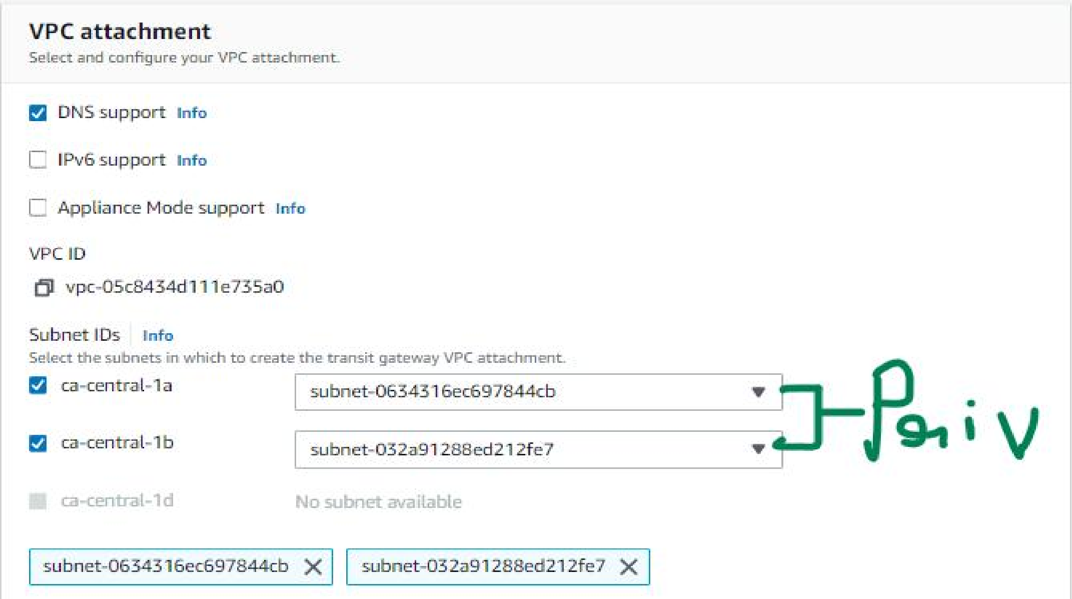
☑ ca-central-1b subnet-0365bd47365570f7a ▲

subnet-0365bd47365570f7a (pub-sub-host)

□ ca-central-1d

subnet-0365bd47365570f7a ✕

transit-attachment-application



VPC attachment

Select and configure your VPC attachment.

☑ DNS support Info

□ IPv6 support Info

□ Appliance Mode support Info

VPC ID

vpc-05c8434d111e735a0

Subnet IDs Info

Select the subnets in which to create the transit gateway VPC attachment.

☑ ca-central-1a subnet-0634316ec697844cb ▼

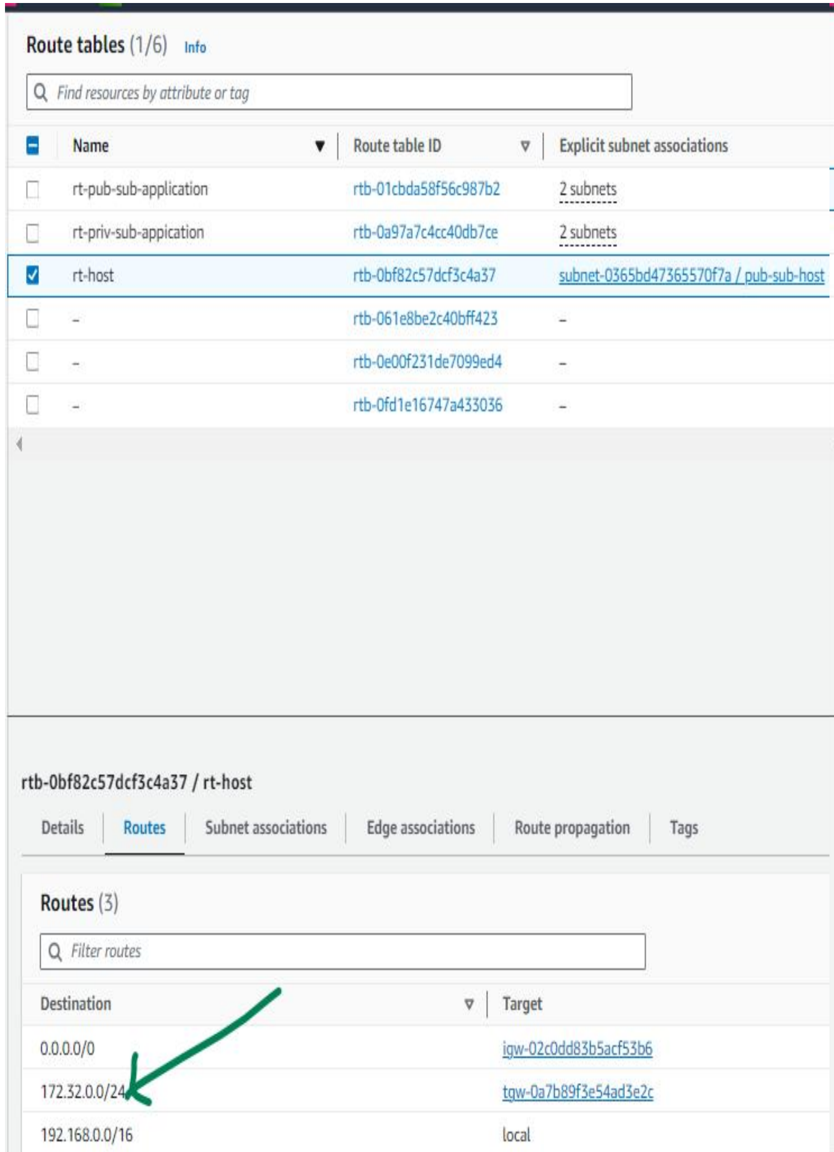
☑ ca-central-1b subnet-032a91288ed212fe7 ▼

□ ca-central-1d No subnet available

subnet-0634316ec697844cb ✕ subnet-032a91288ed212fe7 ✕

- after Creating 2 attachments wait for a moment and cross check Transit gateway route tables it will automatically create Associations and propagations.

- Navigate to route tables --> Edit route tables --> Modify route tables of both the VPCs to route traffic to Transit Gateway



Route tables (1/6) Info

Find resources by attribute or tag

▬	Name	Route table ID	Explicit subnet associations
☐	rt-pub-sub-application	rtb-01cbda58f56c987b2	2 subnets
☐	rt-priv-sub-appication	rtb-0a97a7c4cc40db7ce	2 subnets
☑	rt-host	rtb-0bf82c57dcf3c4a37	subnet-0365bd47365570f7a / pub-sub-host
☐	–	rtb-061e8be2c40bff423	–
☐	–	rtb-0e00f231de7099ed4	–
☐	–	rtb-0fd1e16747a433036	–

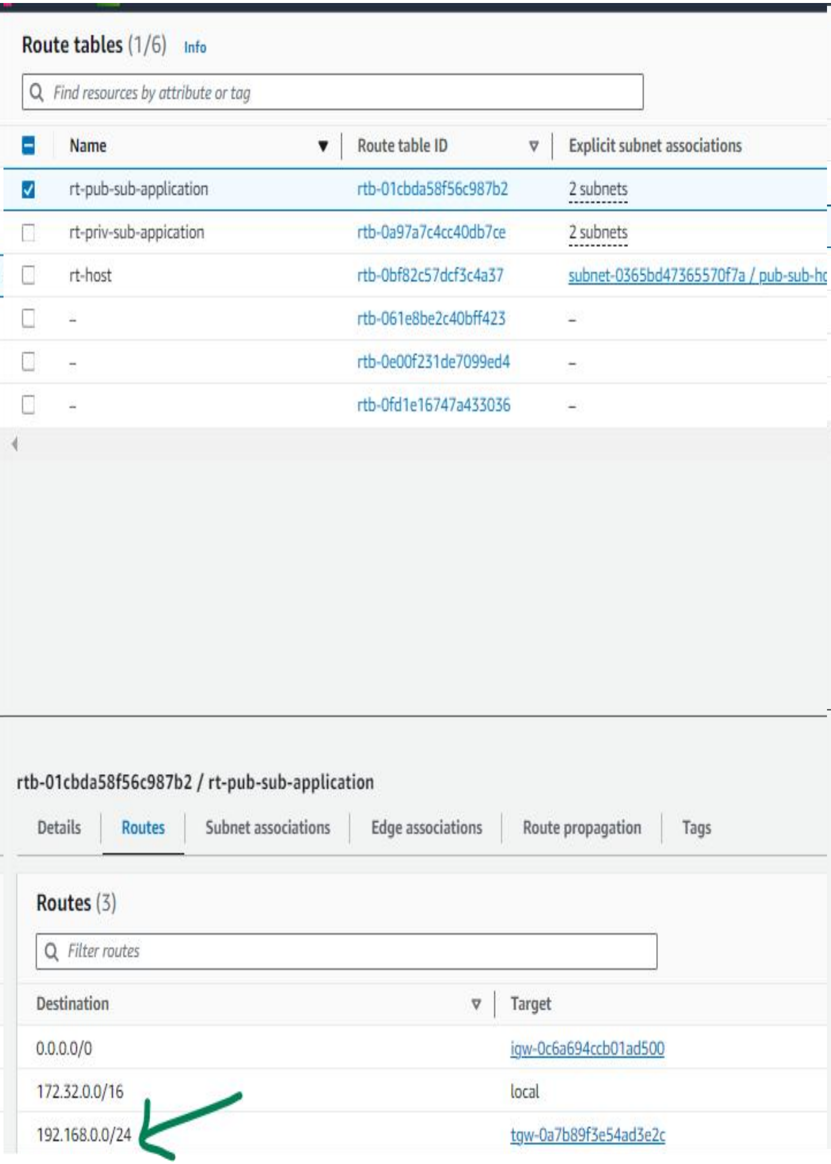
rtb-0bf82c57dcf3c4a37 / rt-host

Routes (3)

Filter routes

Destination	Target
0.0.0.0/0	igw-02c0dd83b5acf53b6
172.32.0.0/24	tgw-0a7b89f3e54ad3e2c
192.168.0.0/16	local

copy Ip address of “application-vpc” and attach it to “rt-host” rote table



Route tables (1/6) Info

Find resources by attribute or tag

▬	Name	Route table ID	Explicit subnet associations
☑	rt-pub-sub-application	rtb-01cbda58f56c987b2	2 subnets
☐	rt-priv-sub-appication	rtb-0a97a7c4cc40db7ce	2 subnets
☐	rt-host	rtb-0bf82c57dcf3c4a37	subnet-0365bd47365570f7a / pub-sub-hc
☐	–	rtb-061e8be2c40bff423	–
☐	–	rtb-0e00f231de7099ed4	–
☐	–	rtb-0fd1e16747a433036	–

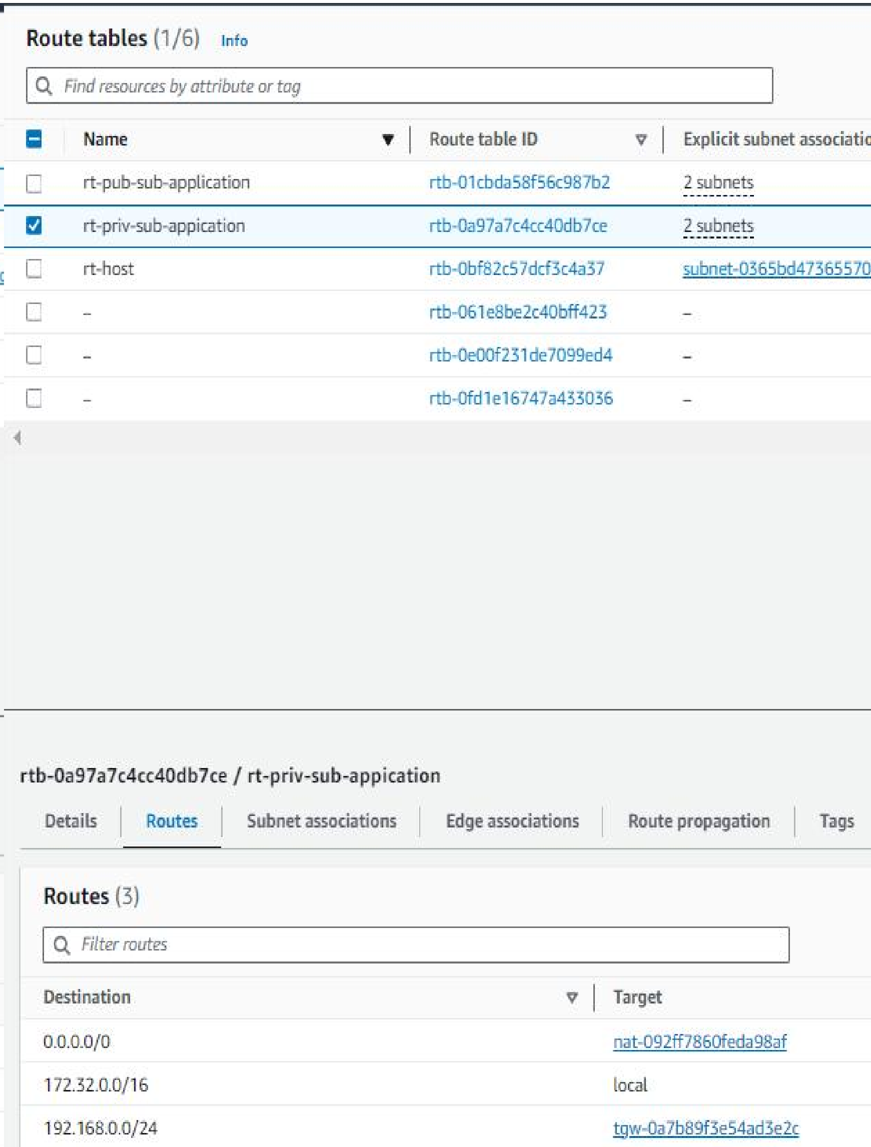
rtb-01cbda58f56c987b2 / rt-pub-sub-application

Routes (3)

Filter routes

Destination	Target
0.0.0.0/0	igw-0c6a694ccb01ad500
172.32.0.0/16	local
192.168.0.0/24	tgw-0a7b89f3e54ad3e2c

copy Ip address of “host-vpc” and attach it to “rt-pub-sub-application” rote table



Route tables (1/6) Info

Find resources by attribute or tag

▬	Name	Route table ID	Explicit subnet associatio
☐	rt-pub-sub-application	rtb-01cbda58f56c987b2	2 subnets
☑	rt-priv-sub-appication	rtb-0a97a7c4cc40db7ce	2 subnets
☐	rt-host	rtb-0bf82c57dcf3c4a37	subnet-0365bd47365570
☐	–	rtb-061e8be2c40bff423	–
☐	–	rtb-0e00f231de7099ed4	–
☐	–	rtb-0fd1e16747a433036	–

rtb-0a97a7c4cc40db7ce / rt-priv-sub-appication

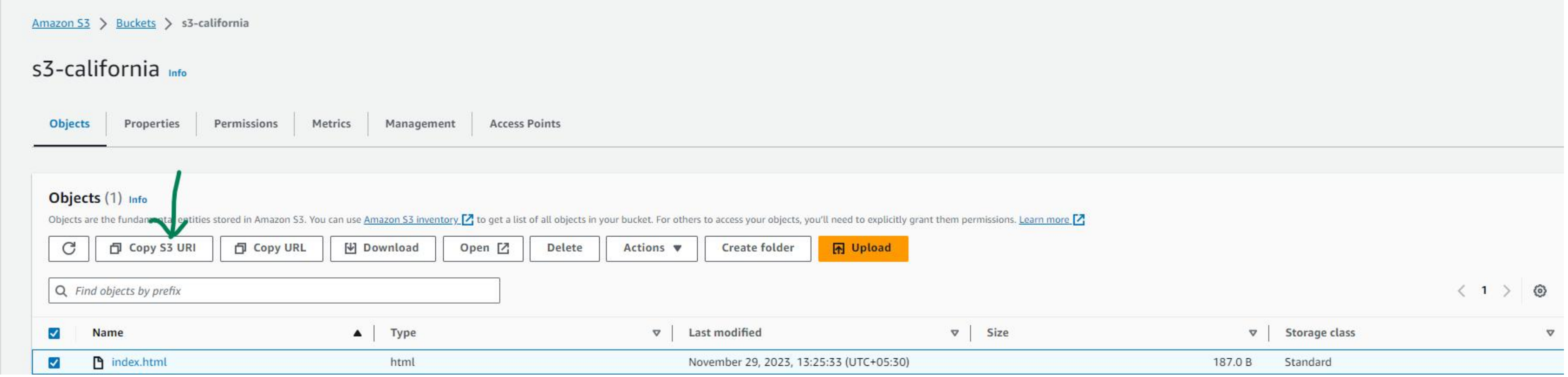
Routes (3)

Filter routes

Destination	Target
0.0.0.0/0	nat-092ff7860feda98af
172.32.0.0/16	local
192.168.0.0/24	tgw-0a7b89f3e54ad3e2c

copy Ip address of “host-vpc” and attach it to “rt-pri-sub-application” rote table

9.Create S3 Bucket : Navigate to services-->S3-->create a Bucket and upload your Index.html File and copy s3 url.



s3-california

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name	Type	Last modified	Size	Storage class
☑	index.html	html	November 29, 2023, 13:25:33 (UTC+05:30)	187.0 B	Standard

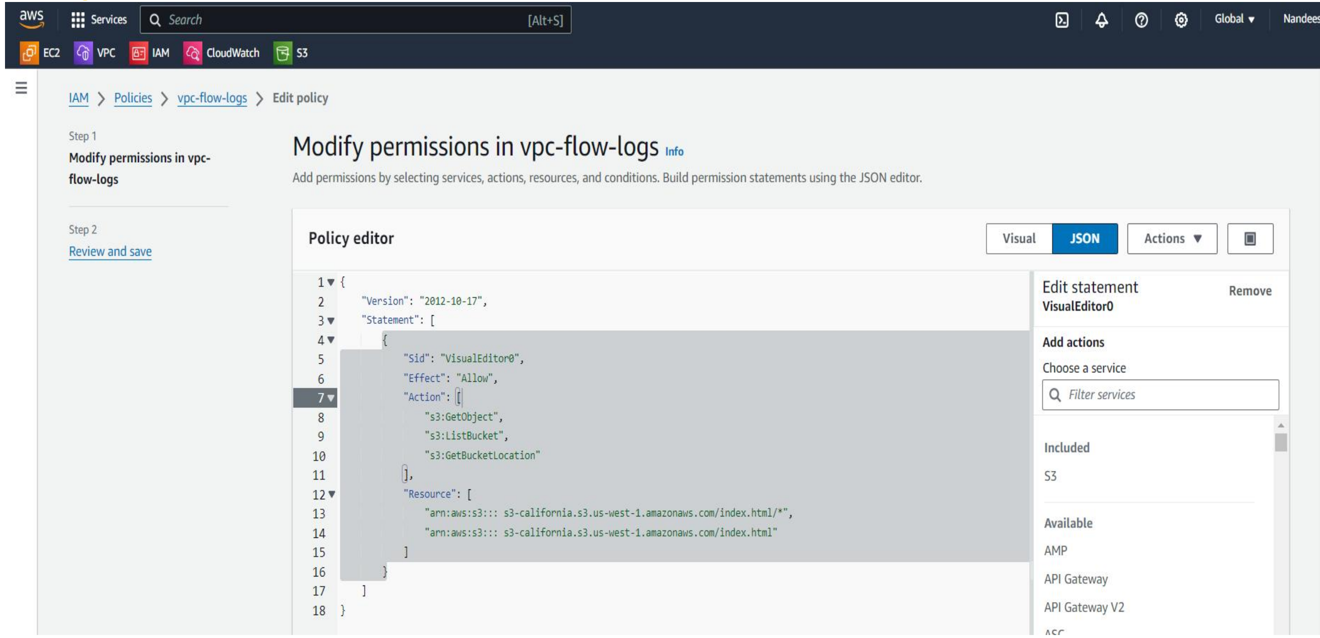
copy s3 Url -- **https://s3-california.s3.us-west-1.amazonaws.com/index.html**

10. Create an IAM Policy: To allow access to this bucket only

Replace resource s3 path with your s3

bucket url

click - link for s3 policy



Step 1
Modify permissions in vpc-flow-logs

Step 2
Review and save

Modify permissions in vpc-flow-logs

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3::: s3-california.s3.us-west-1.amazonaws.com/index.html/*",
                "arn:aws:s3::: s3-california.s3.us-west-1.amazonaws.com/index.html"
            ]
        }
    ]
}
```

Edit statement
VisualEditor0

Add actions

Choose a service

Included

S3

Available

AMP

API Gateway

API Gateway V2

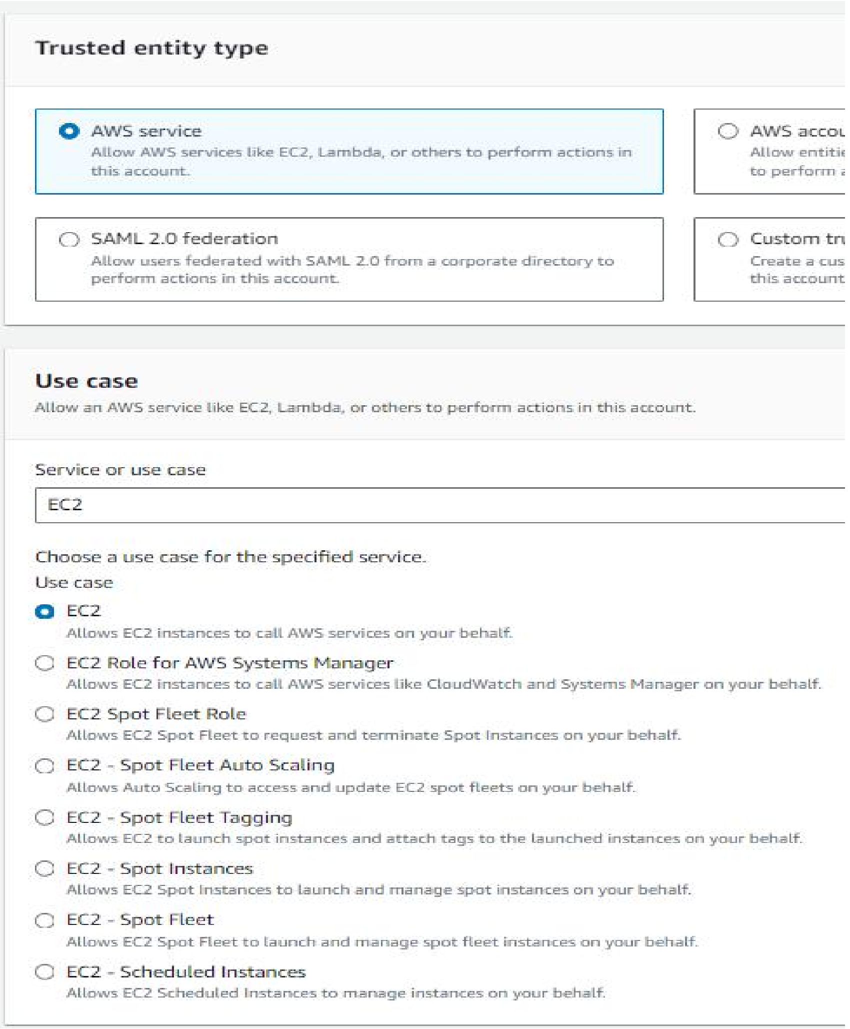
ASC

11. Create a IAM Role : Role name = SSM+Cloudwatch-FullAccess with “cloudwatcfullaccess” policy and “vpc-flow-logs”.

Note : Edit JSON is not permitted while creating Role we can modify after creating.

- Replace ec2 with your policy name

and save it.



Trusted entity type

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

○ AWS accou
Allow entitie
to perform a

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

○ Custom tru
Create a cus
this account

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

Service or use case
EC2

Choose a use case for the specified service.
Use case

● EC2
Allows EC2 instances to call AWS services on your behalf.

○ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

○ EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

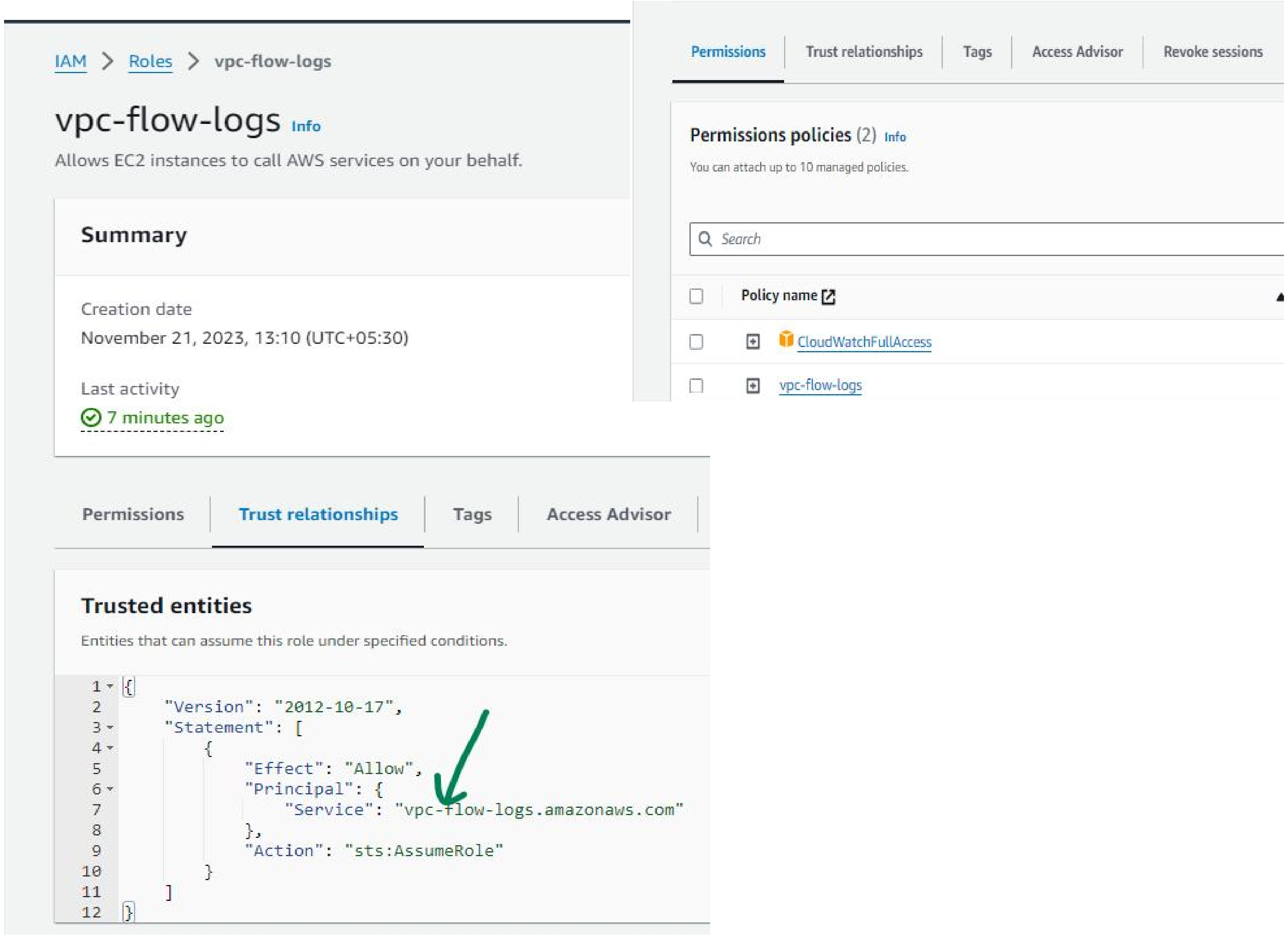
○ EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

○ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

○ EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

○ EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

○ EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.



IAM > Roles > vpc-flow-logs

vpc-flow-logs Info
Allows EC2 instances to call AWS services on your behalf.

Summary

Creation date
November 21, 2023, 13:10 (UTC+05:30)

Last activity
7 minutes ago

Trusted entities
Entities that can assume this role under specified conditions.

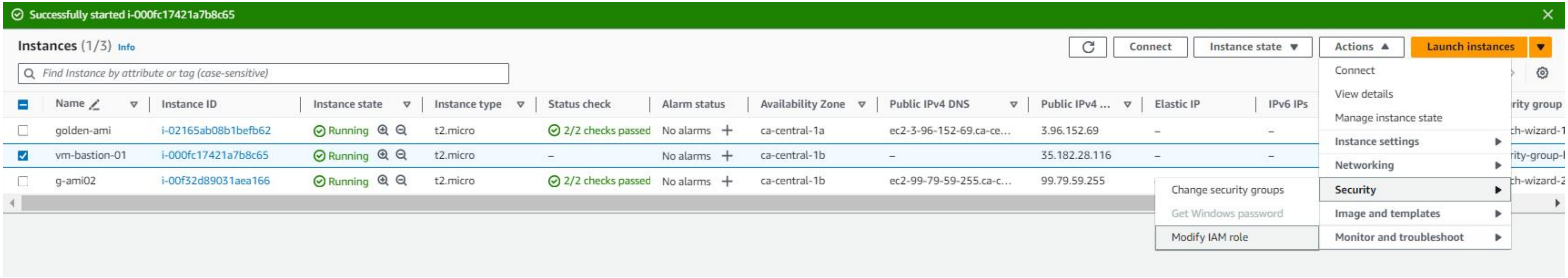
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpc-flow-logs.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Permissions policies (2) Info
You can attach up to 10 managed policies.

□	Policy name
□	CloudWatchFullAccess
□	vpc-flow-logs

12. Create an EC2 Instance : Spinup an Ec2 Instance name = VM_Bastion in “host-vpc” with public subnet “pub-sub-host”

With Security group having access to port 80 HTTP and 20 SSH



Successfully started i-000fc17421a7b8c65

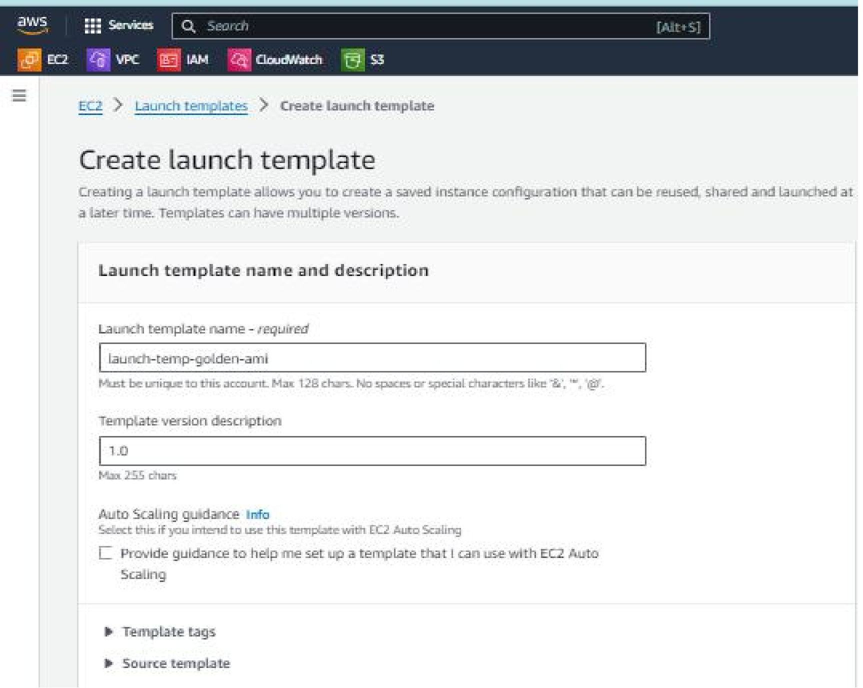
Instances (1/3) Info

Find Instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	rity group
□	golden-ami	i-02165ab08b1befb62	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1a	ec2-3-96-152-69.ca-ce...	3.96.152.69	–	–	ch-wizard-1
☑	vm-bastion-01	i-000fc17421a7b8c65	Running	t2.micro	–	No alarms	ca-central-1b	–	35.182.28.116	–	–	rity-group-l
□	g-ami02	i-00f32d89031aea166	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1b	ec2-99-79-59-255.ca-c...	99.79.59.255			ch-wizard-2

Attach created IAM Role “SSM+Cloudwatch-FullAccess”

13. Launch Template : Create A Launch Template Using Golden-AMI or AMI Created



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*

launch-temp-golden-ami

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

Template version description

1.0

Max 255 chars

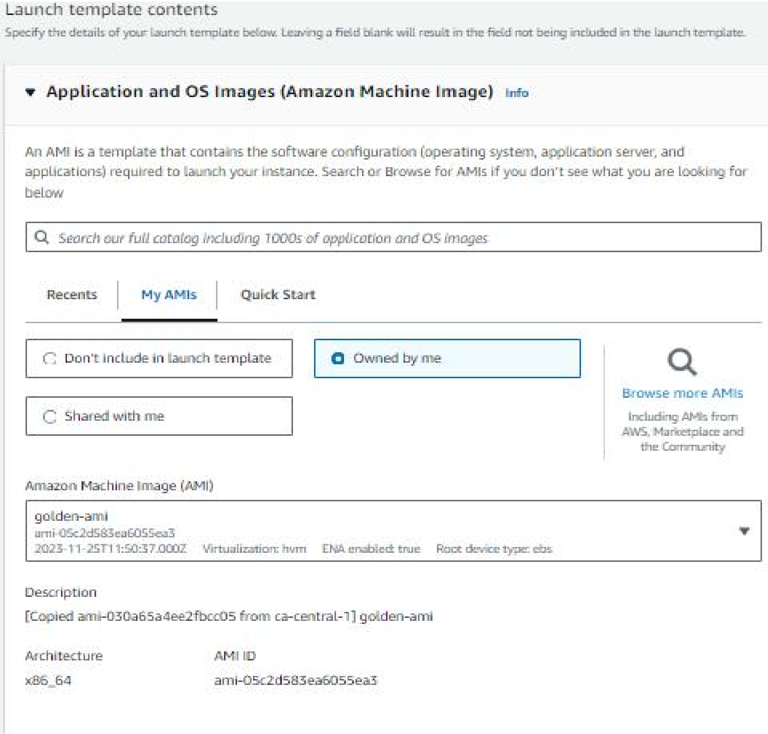
Auto Scaling guidance Info

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



Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▾ 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

○ Don't include in launch template

● Owned by me

○ Shared with me

Amazon Machine Image (AMI)

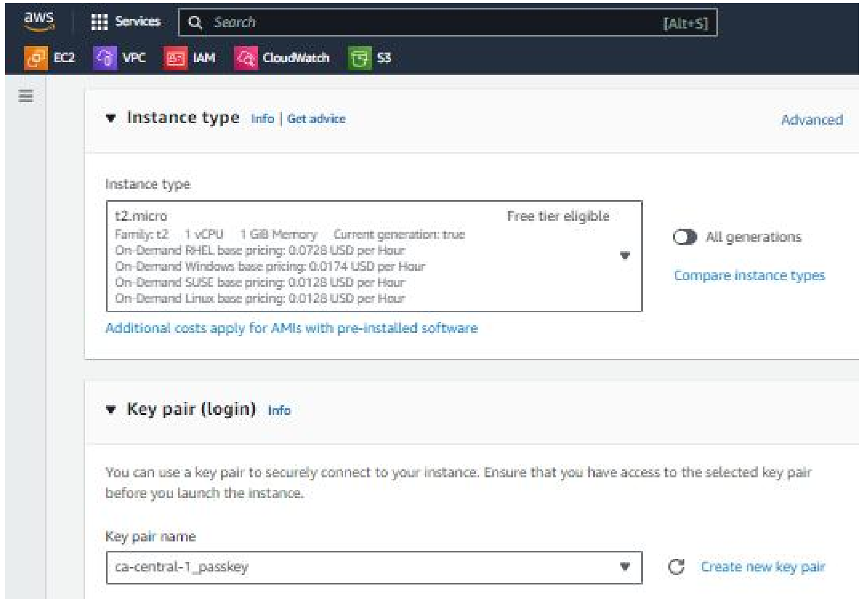
golden-ami
ami-05c2d583ea6055ea3
2023-11-25T11:50:37.000Z Virtualization: hvm ENA enabled: true Root device type: ebs

Description

[Copied ami-030a65a4ee2fbcc05 from ca-central-1] golden-ami

Architecture: x86_64

AMI ID: ami-05c2d583ea6055ea3



▾ Instance type Info | Get advice

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.0728 USD per Hour
On-Demand Windows base pricing: 0.0174 USD per Hour
On-Demand SUSE base pricing: 0.0128 USD per Hour
On-Demand Linux base pricing: 0.0128 USD per Hour

All generations

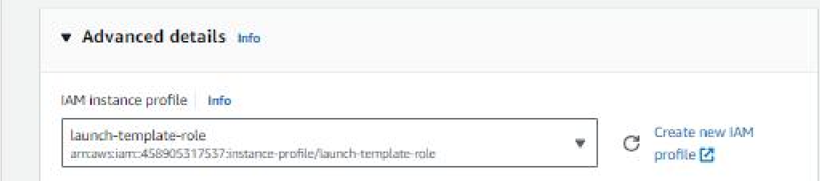
Additional costs apply for AMIs with pre-installed software

▾ Key pair (login) Info

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

Key pair name

ca-central-1_passkey



▾ Advanced details Info

IAM instance profile Info

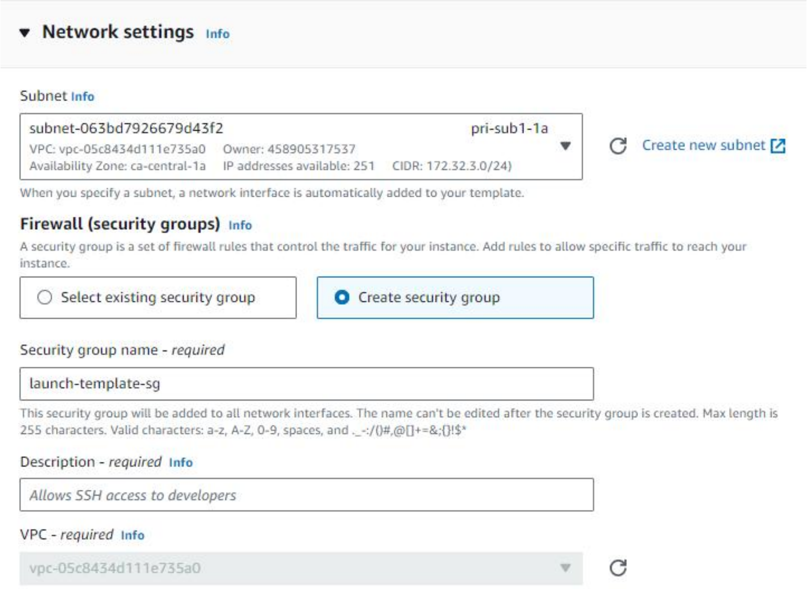
launch-template-role
arn:aws:iam::458905317537:instance-profile/launch-template-role

- Provide a standard name to identify and provide the Template Version according to modification.
- Select My-ami's and select Created AMI (Golden-AMI) and Instance type can selected.
- Select Keypair as ypur current working region.
- select advanced Details dropdown and in IAM Instance profile choose and attach "launch-temp-role"

Create Launch Template

13. Launch Template

- In Network settings Choose Private Subnet “pri-sub1-1a”
- Choose security group allowing with SSH-22 and HTTP-80
- Edit User data and add Commands
- link to get user data
- Note Don’t Include sudo yum install awslogs -y Because We have already configured the AWS logs on our Golden AMI



Network settings

Subnet

subnet-063bd7926679d43f2 pri-sub1-1a
VPC: vpc-05c8434d111e735a0 Owner: 458905317537
Availability Zone: ca-central-1a IP addresses available: 251 CIDR: 172.32.3.0/24)

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

Firewall (security groups)

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

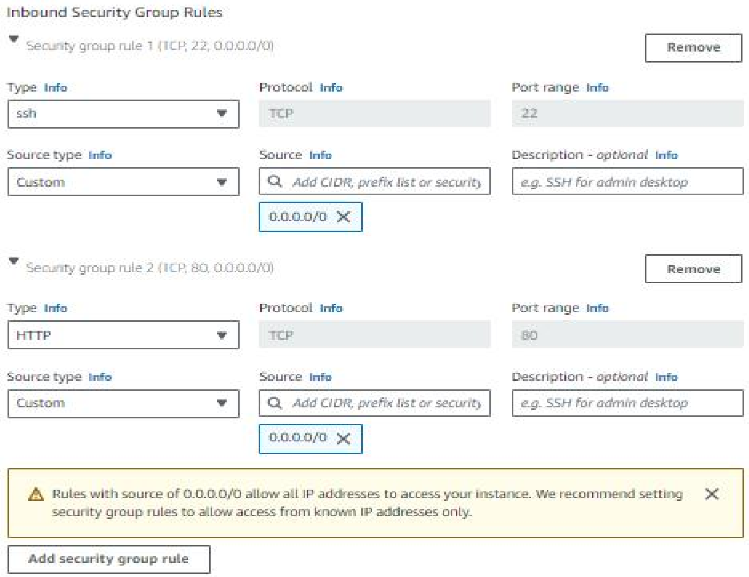
○ Select existing security group ● Create security group

Security group name - *required*: launch-template-sg

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

Description - *required*: *Allows SSH access to developers*

VPC - *required*: vpc-05c8434d111e735a0



Inbound Security Group Rules

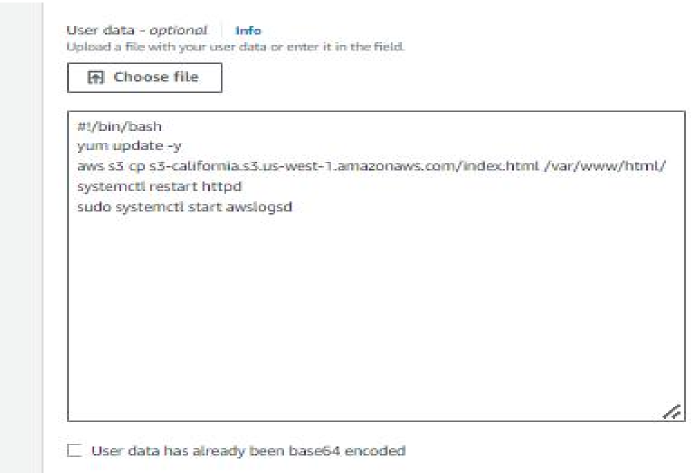
Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type: ssh	Protocol: TCP	Port range: 22
Source type: Custom	Source: *Add CIDR, prefix list or security* 0.0.0.0/0	Description - *optional*: *e.g. SSH for admin desktop*

Security group rule 2 (TCP, 80, 0.0.0.0/0)

Type: HTTP	Protocol: TCP	Port range: 80
Source type: Custom	Source: *Add CIDR, prefix list or security* 0.0.0.0/0	Description - *optional*: *e.g. SSH for admin desktop*

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



User data - *optional*

Upload a file with your user data or enter it in the field.

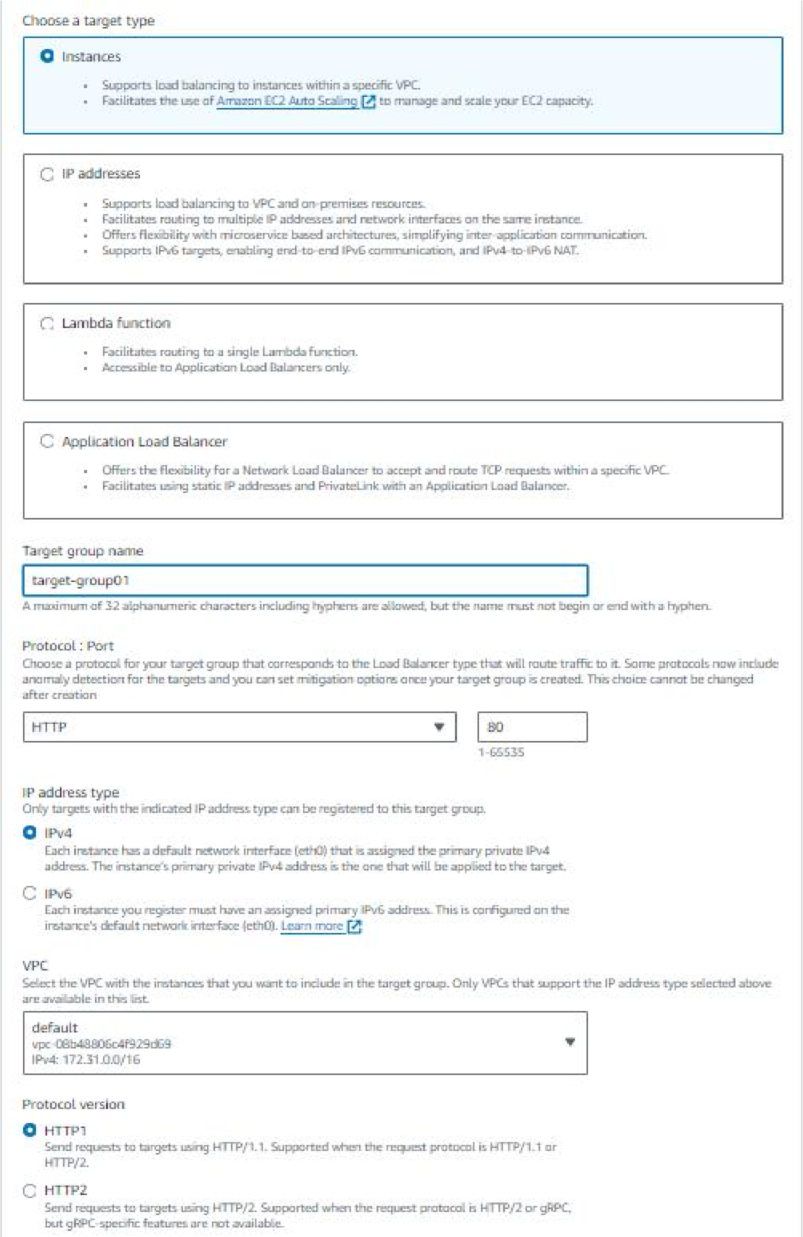
```
#!/bin/bash
yum update -y
aws s3 cp s3-california.s3.us-west-1.amazonaws.com/index.html /var/www/html/
systemctl restart httpd
sudo systemctl start awslogsd
```

□ User data has already been base64 encoded

Create Launch Template

14.Target Groups : Navigate to target group in the Ec2 Section and create with name “Target_Group-01”

Don’t Change Any default values and create a Target Group



Choose a target type

● Instances

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

○ IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

○ Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

○ Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

target-group01

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP ▼ 80

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

● IPv4

Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

○ IPv6

Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). Learn more

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

default
vpc-08b48806c4f929d69
IPv4: 172.31.0.0/16 ▼

Protocol version

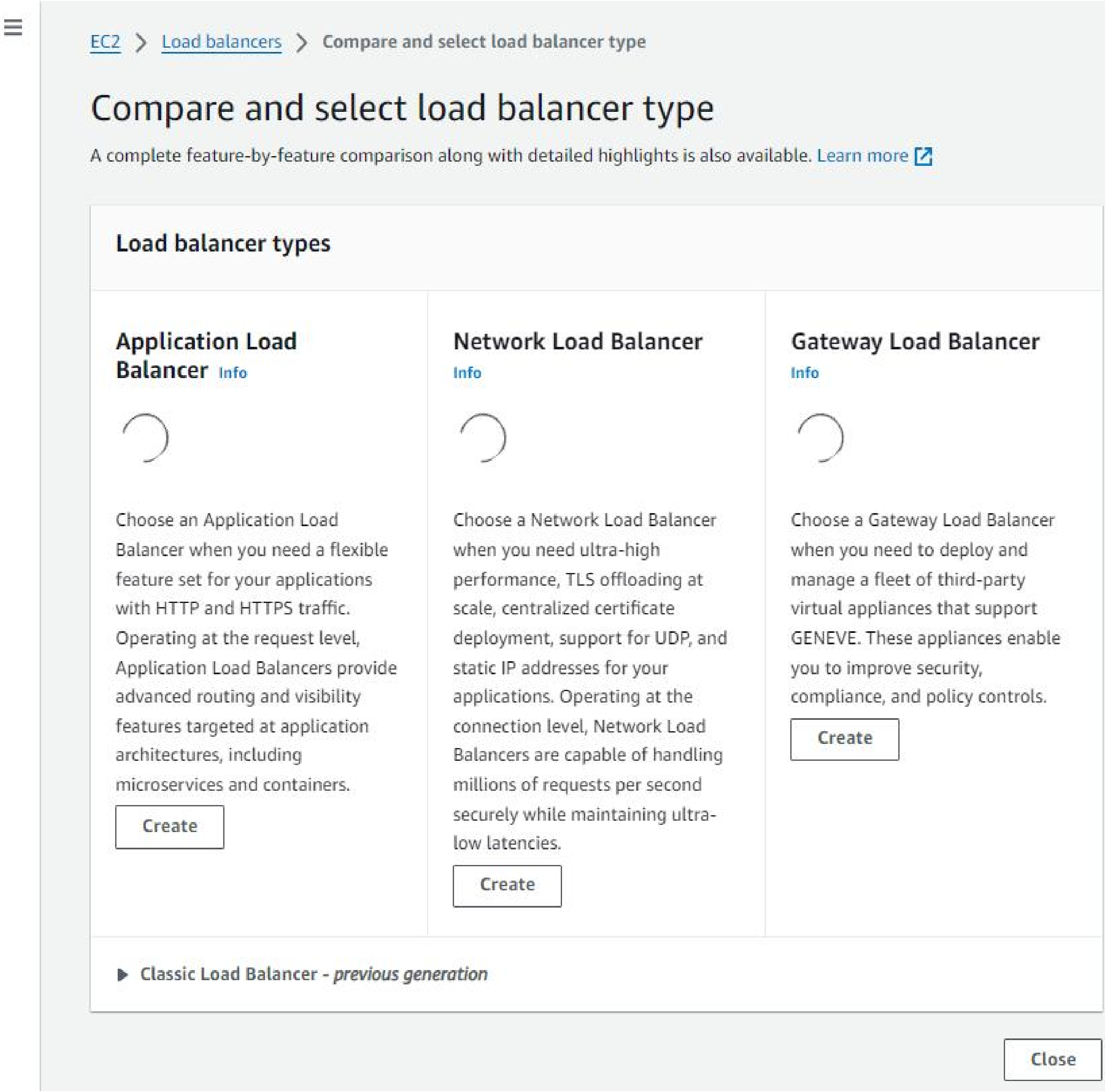
● HTTP1

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

○ HTTP2

Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

15. Load Balancers : Create Load balancer for Public Subnets.



EC2 > Load balancers > Compare and select load balancer type

Compare and select load balancer type

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

Load balancer types

Application Load Balancer Info

Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

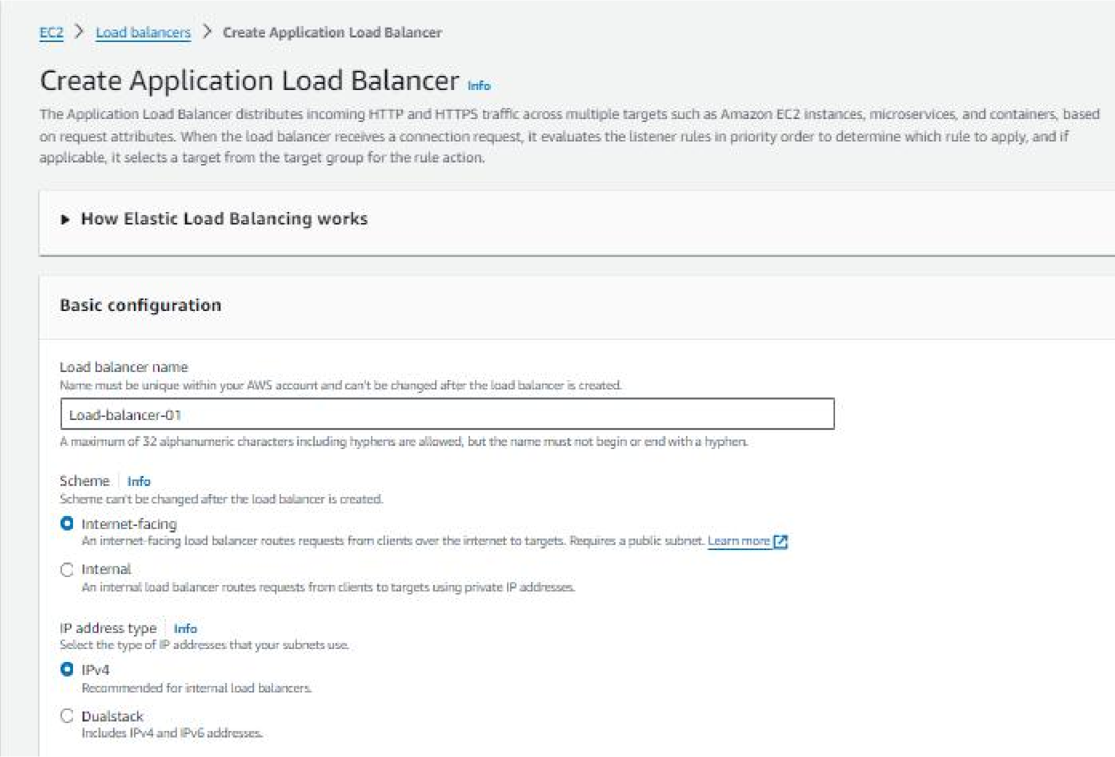
Network Load Balancer Info

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Gateway Load Balancer Info

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

▸ Classic Load Balancer - *previous generation*



EC2 > Load balancers > Create Application Load Balancer

Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▸ How Elastic Load Balancing works

Basic configuration

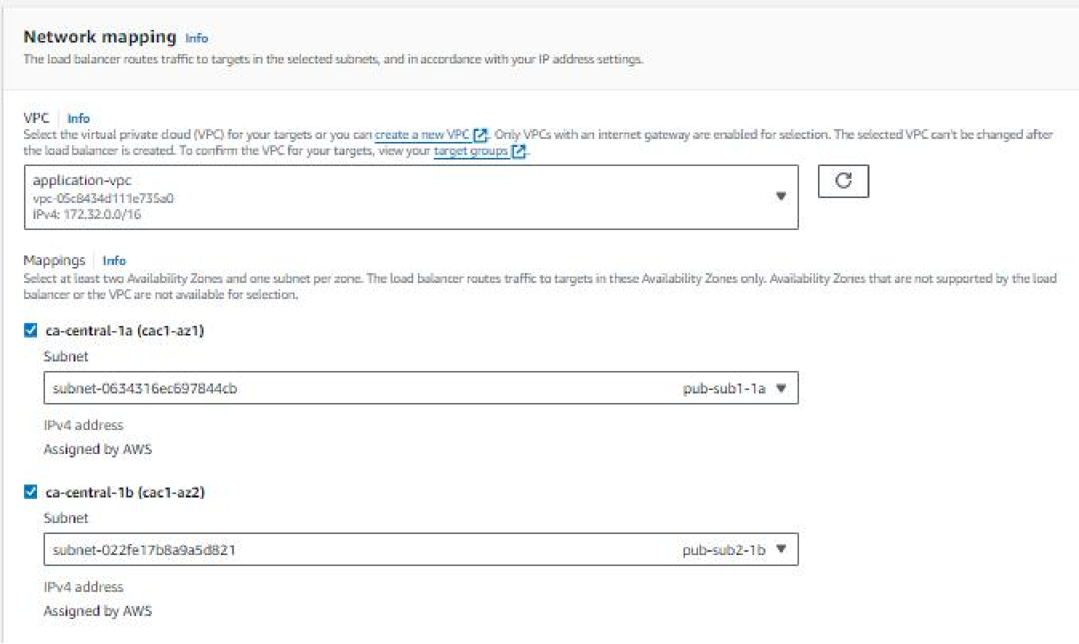
Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
Load-balancer-01
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme | Info
Scheme can't be changed after the load balancer is created.
● Internet-facing
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more
○ Internal
An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type | Info
Select the type of IP addresses that your subnets use.
● IPv4
Recommended for internal load balancers.
○ Dualstack
Includes IPv4 and IPv6 addresses.

We can Choose the Load Balancer according our requirements.

15. Load Balancers



Network mapping Info

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

VPC | Info

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

application-vpc
vpc-05c8434d111e735a0
IPv4: 172.32.0.0/16

Mappings | Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☑ ca-central-1a (cac1-az1)

Subnet: subnet-0634316ec697844cb pub-sub1-1a

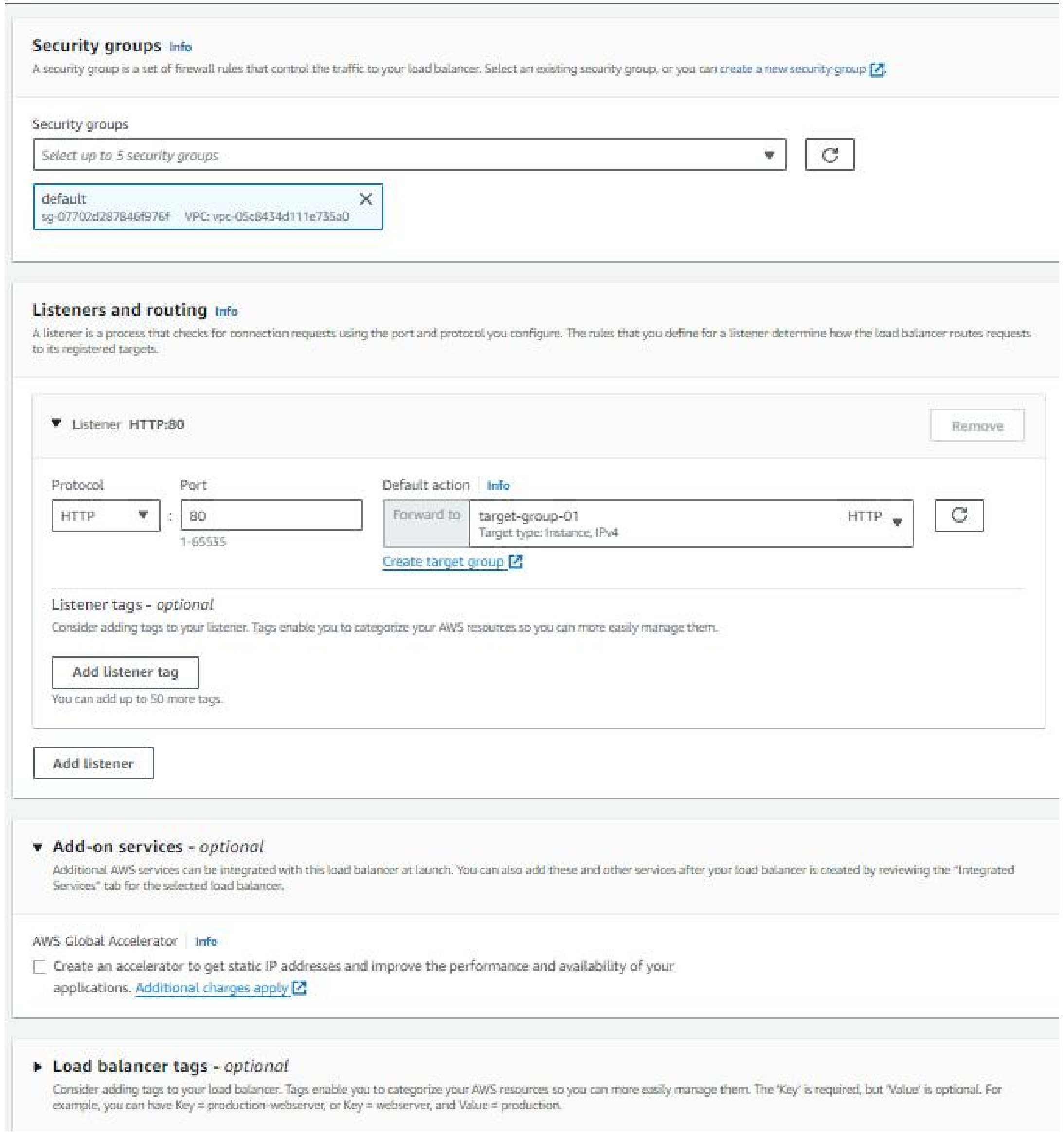
IPv4 address: Assigned by AWS

☑ ca-central-1b (cac1-az2)

Subnet: subnet-022fe17b8a9a5d821 pub-sub2-1b

IPv4 address: Assigned by AWS

- Select “application-vpc”
- select 2 diff AZ and select “pub-sub-1a” and “pub-sub-1b”
- Security Groups with port 22 SSh and port 80 HTTP
- Select Listerners and routing as Target-Group-01
- and Create the Load Balancers.



Security groups Info

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

Security groups: *Select up to 5 security groups*

default
sg-07702d287846f976f VPC: vpc-05c8434d111e735a0

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Listener HTTP:80

Protocol: HTTP

Port: 80 (1-65535)

Default action | Info: Forward to target-group-01 HTTP
Target type: Instance, IPv4

Create target group

Listener tags - *optional*

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

You can add up to 50 more tags.

Add-on services - *optional*

Additional AWS services can be integrated with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the "Integrated Services" tab for the selected load balancer.

AWS Global Accelerator | Info

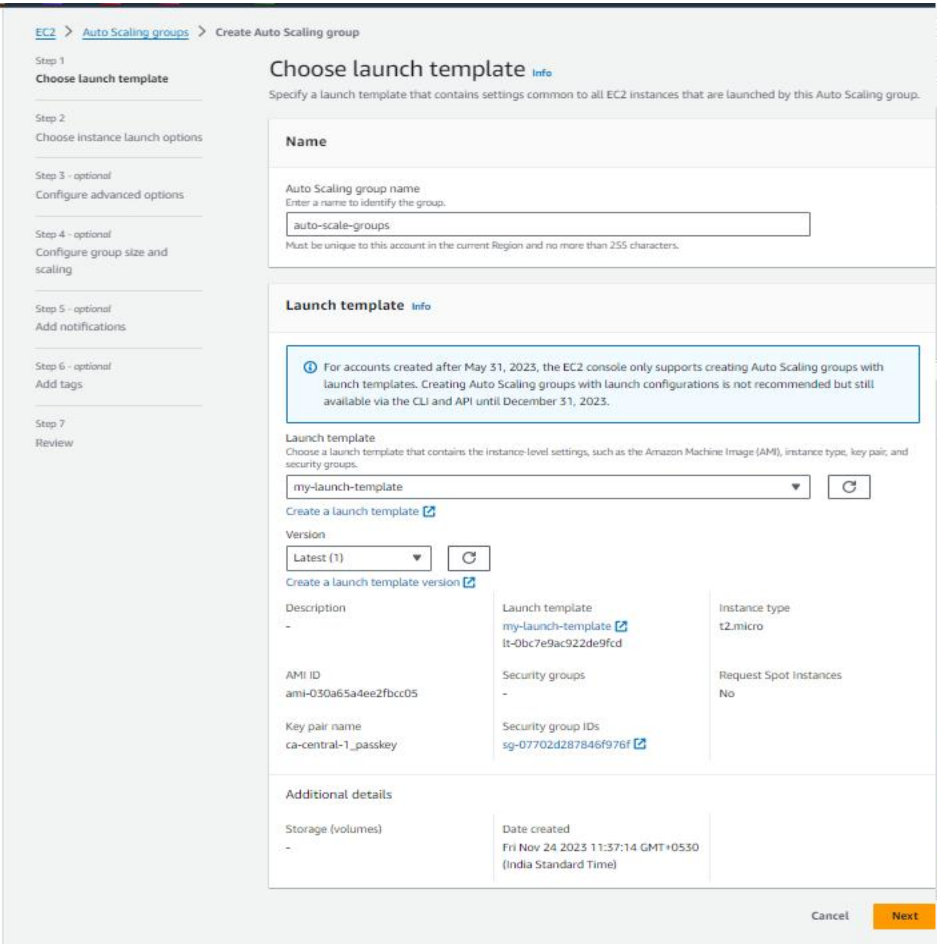
□ Create an accelerator to get static IP addresses and improve the performance and availability of your applications. Additional charges apply

Load balancer tags - *optional*

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

16. Auto Scalling Groups: Navigate to Auto scalling groupps in Ec2 and Create a ASG

- Enter a Standard and identifiable Name, and Select “Launch-template -01” and in versio dropdown select latest -in case if any changes has been made it will take the latest template.
- Choose “application-vpc” and private subnets “pri-sub-1a” and pri-sub-1b”, Attach it to existing load balancer “load-balancer-01” and choose “Target-Group-01”.
- In capacity Providers [desired capacity = 1] [mim capacity = 1] [max capacity = 3] as per documentation, dont change anything create a ASG and verify in ec2 instance (Automatically a instance will be launched by ASG)



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template

Step 2
Choose instance launch options

Step 3 - optional
Configure advanced options

Step 4 - optional
Configure group size and scaling

Step 5 - optional
Add notifications

Step 6 - optional
Add tags

Step 7
Review

Choose launch template Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name
Enter a name to identify the group.
auto-scale-groups
Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info

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

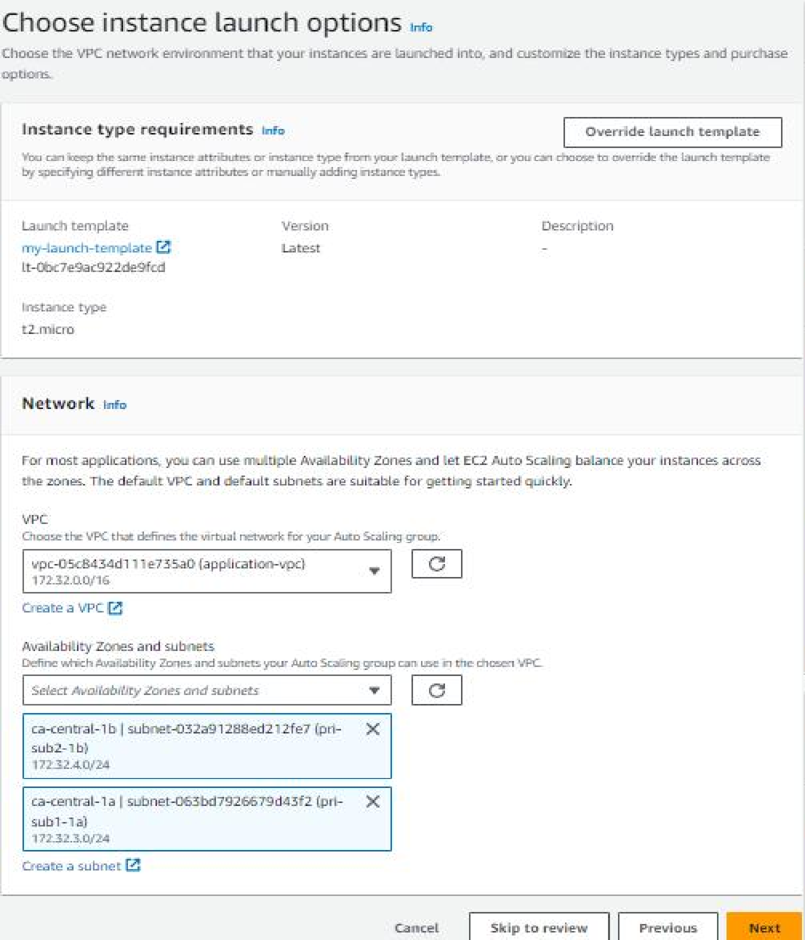
Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.
my-launch-template
Create a launch template

Version
Latest (1)
Create a launch template version

Description	Launch template	Instance type
-	my-launch-template lt-0bc7e9ac922de9fcd	t2.micro
AMI ID	Security groups	Request Spot Instances
ami-030a65a4ee2fbcc05	-	No
Key pair name	Security group IDs	
ca-central-1_passkey	sg-07702d287846f976f	

Additional details

Storage (volumes)	Date created
-	Fri Nov 24 2023 11:37:14 GMT+0530 (India Standard Time)



Choose instance launch options Info

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

Instance type requirements Info

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
my-launch-template lt-0bc7e9ac922de9fcd	Latest	-

Instance type
t2.micro

Network Info

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

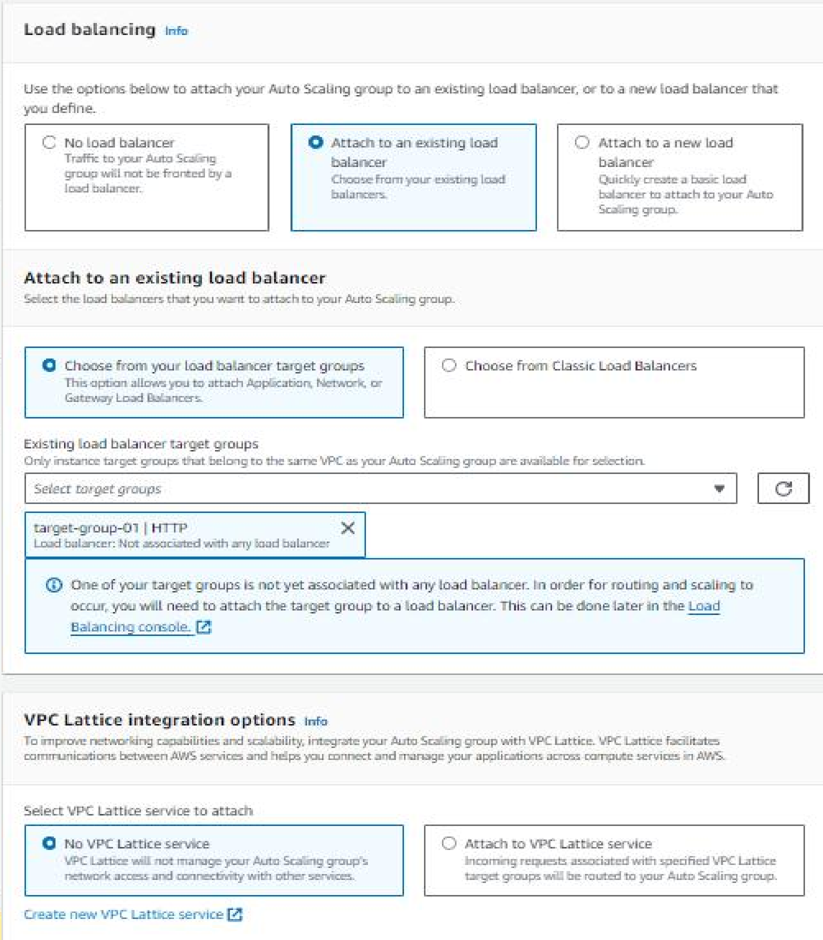
VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.
vpc-05c8434d111e735a0 (application-vpc)
172.32.0.0/16
Create a VPC

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

ca-central-1b | subnet-032a91288ed212fe7 (pri-sub2-1b)
172.32.4.0/24

ca-central-1a | subnet-063bd7926679d43f2 (pri-sub1-1a)
172.32.3.0/24

Create a subnet



Load balancing Info

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

○ No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.

● Attach to an existing load balancer
Choose from your existing load balancers.

○ Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

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

Existing load balancer target groups
Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.
Select target groups

target-group-01 | HTTP
Load balancer: Not associated with any load balancer

One of your target groups is not yet associated with any load balancer. In order for routing and scaling to occur, you will need to attach the target group to a load balancer. This can be done later in the Load Balancing console.

VPC Lattice integration options Info

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

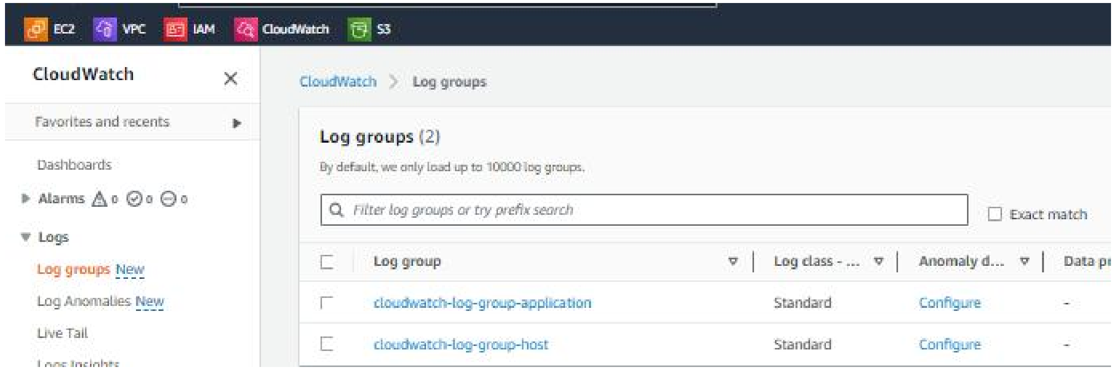
Select VPC Lattice service to attach

● No VPC Lattice service
VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.

○ Attach to VPC Lattice service
Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.

Create new VPC Lattice service

17.Cloudwatch: Navigate to Cloudwatch services --> Logs --> log group --> Create 2 Log groups for host and application.



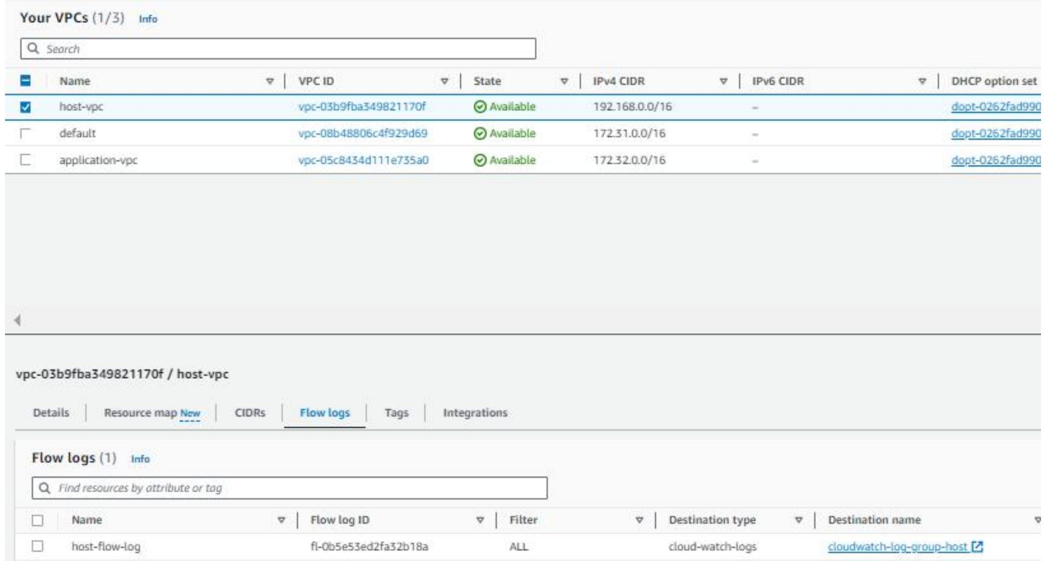
Log groups (2)

By default, we only load up to 10000 log groups.

Filter log groups or try prefix search

□	Log group	Log class - ...	Anomaly d...	Data pr
□	cloudwatch-log-group-application	Standard	Configure	-
□	cloudwatch-log-group-host	Standard	Configure	-

- Navigate to VPC -host --> Flow Logs --> Create Flow-logs


Your VPCs (1/3) Info

Search

■	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set
☑	host-vpc	vpc-03b9fba349821170f	Available	192.168.0.0/16	–	dopt-0262fad990
□	default	vpc-08b48806c4f929d69	Available	172.31.0.0/16	–	dopt-0262fad990
□	application-vpc	vpc-05c8434d111e735a0	Available	172.32.0.0/16	–	dopt-0262fad990

vpc-03b9fba349821170f / host-vpc

Flow logs (1) Info

Find resources by attribute or tag

□	Name	Flow log ID	Filter	Destination type	Destination name
□	host-flow-log	fl-0b5e53ed2fa32b18a	ALL	cloud-watch-logs	cloudwatch-log-group-host

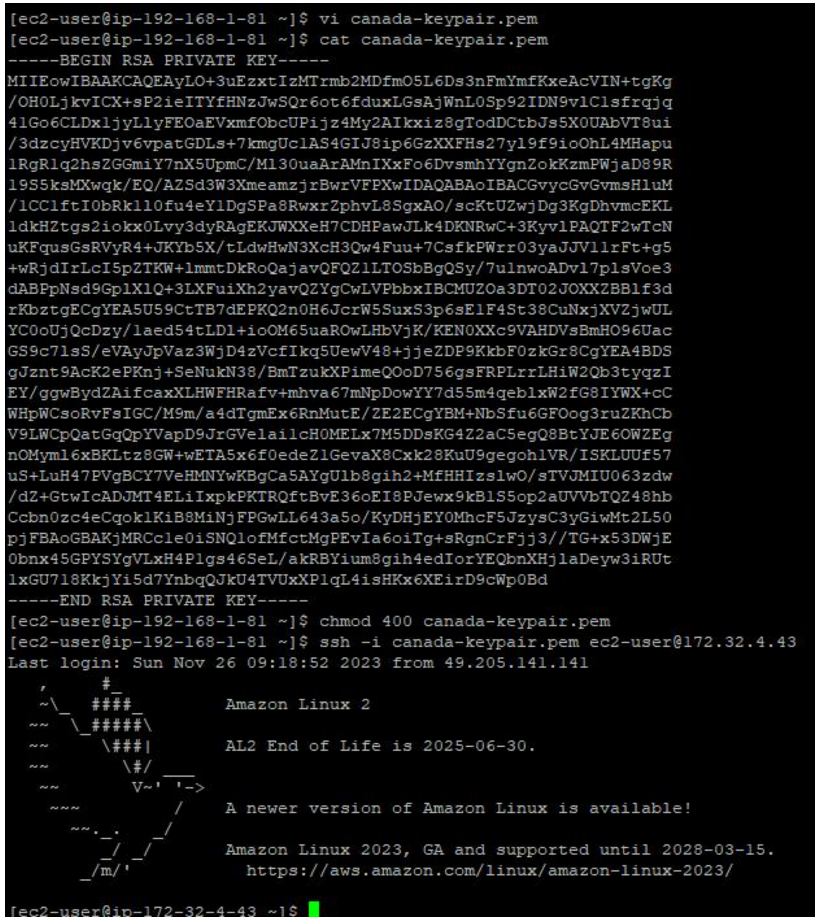
Repeat the same step for Application VPC

Navigate to application-vpc --> Flow Logs --> Create Flow-logs

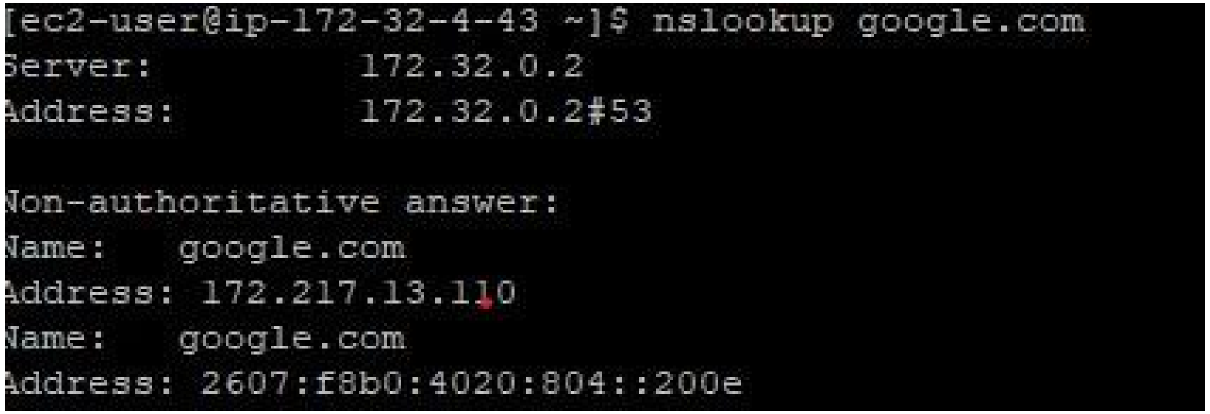
Validation

1.As DevOps Engineer login to Private Instances via Bastion Host.

- Result : Successfully Logged In to bastion server



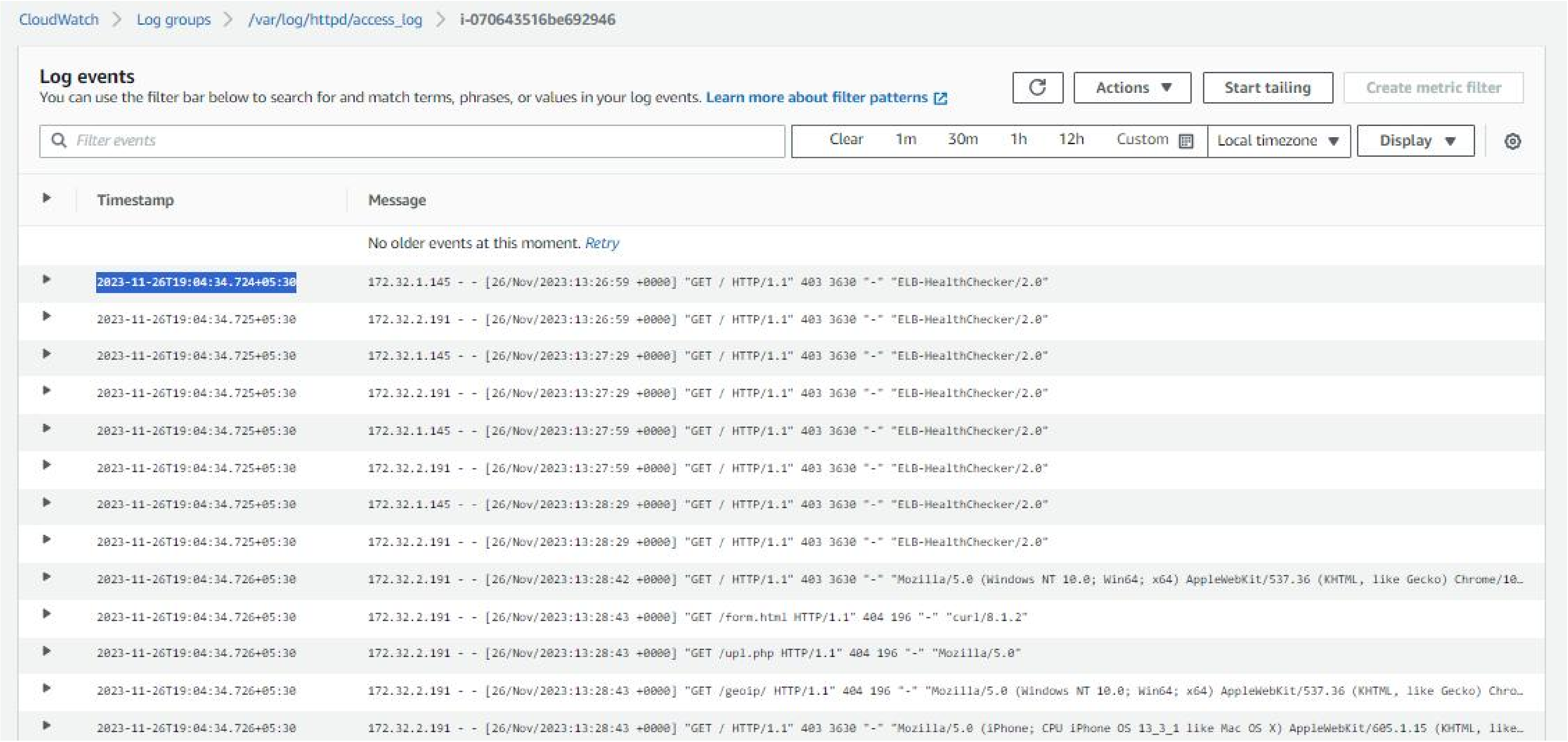
```
[ec2-user@ip-192-168-1-81 ~]$ vi canada-keypair.pem
[ec2-user@ip-192-168-1-81 ~]$ cat canada-keypair.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAyLO+3uEzxtIzMTrmb2MDfmO5L6Ds3nFmYmfKxeAcVIN+tgKg
/OH0LjkvICX+sP2ieITYfHNzJwSQr6ot6fduxLGsAjWnL0Sp92IDN9vlClsfrqjq
41Go6CLDxljyLlyFEOaEVxmfObcUPijz4My2AIkxiz8gTodDCtbJs5X0UAbVT8ui
/3dzcyHVKDjv6vpatGDLs+7kmgUclAS4GIJ8ip6GzXXFHs27yl9f9ioOhL4MHapu
lRgRlq2hsZGGmiY7nX5UpmC/Ml30uaArAMnIXxFo6DvsmhYYgnZokKzmPWjaD89R
l9S5ksMXwqk/EQ/AZSd3W3XmeamzjrBwrVFPXwIDAQABAoIBACGvycGvGvmsHluM
/lCClftI0bRkll0fu4eYlDgSPa8RwxrZphvL8SgxAO/scKtUZwjDg3KgDhvmcEKL
ldkHZtgs2iokx0Lvy3dyRAgEKJWXXeH7CDHPawJLk4DKNRwC+3KyvlPAQTF2wTcN
uKFqusGsRVyR4+JKYb5X/tLdwHwN3XcH3Qw4Fuu+7CsfkPWrr03yaJJVllrFt+g5
+wRjdIrLcI5pZTKW+lmmtDkRoQajavQFQZlLTOSbBgQSy/7ulnwoADvl7plsVoe3
dABPpNsd9GplXlQ+3LXFuiXh2yavQZYgCwLVPbbxIBCMUZOa3DT02JOXXZBBlf3d
rKbztgECgYEA5U59CtTB7dEPKQ2n0H6JcrW5SuxS3p6sElF4St38CuNxjXVZjwUL
YC0oUjQcDzy/laed54tLDl+ioOM65uaROwLHbVjK/KEN0XXc9VAHDVsBmHO96Uac
GS9c7lsS/eVAyJpVaz3WjD4zVcfIkq5UewV48+jjeZDP9KkbF0zkGr8CgYEA4BDS
gJznt9AcK2ePKnj+SeNukN38/BmTzukXPimeQOoD756gsFRPLrrLHiW2Qb3tyqzI
EY/ggwBydZAifcaxXLHWFHRafv+mhva67mNpDowYY7d55m4qeblxW2fG8IYWX+cC
WHpWCsoRvFsIGC/M9m/a4dTgmEx6RnMutE/ZE2ECgYBM+NbSfu6GFOog3ruZKhCb
V9LWCpQatGqQpYVapD9JrGVelailcH0MELx7M5DDsKG4Z2aC5egQ8BtYJE6OWZEg
nOMyml6xBKLtz8GW+wETA5x6f0edeZlGevaX8Cxk28KuU9gegohlVR/ISKLUUf57
uS+LuH47PVgBCY7VeHMNYwKBgCa5AYgUlb8gih2+MfHHIzslwO/sTVJMIU063zdw
/dZ+GtwIcADJMT4ELiIxpkPKTRQftBvE36oEI8PJewx9kBlS5op2aUVVbTQZ48hb
Ccbn0zc4eCqoklKiB8MiNjFPGwLL643a5o/KyDHjEY0MhcF5JzysC3yGiwMt2L50
pjFBAoGBAKjMRCcle0iSNQlofMfctMgPEvIa6oiTg+sRgnCrFjj3//TG+x53DWjE
0bnx45GPYSYgVLxH4Plgs46SeL/akRBYium8gih4edIorYEQbnXHjlaDeyw3iRUt
lxGU7l8KkjYi5d7YnbqQJkU4TVUxXPlqL4isHKx6XEirD9cWp0Bd
-----END RSA PRIVATE KEY-----
[ec2-user@ip-192-168-1-81 ~]$ chmod 400 canada-keypair.pem
[ec2-user@ip-192-168-1-81 ~]$ ssh -i canada-keypair.pem ec2-user@172.32.4.43
Last login: Sun Nov 26 09:18:52 2023 from 49.205.141.141
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2025-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-172-32-4-43 ~]$
```



```
[ec2-user@ip-172-32-4-43 ~]$ nslookup google.com
Server:         172.32.0.2
Address:        172.32.0.2#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.13.110
Name:   google.com
Address: 2607:f8b0:4020:804::200e
```

Validation

2.Cloudwatch agent is pushing logs from instance to Cloudwatch monitoring



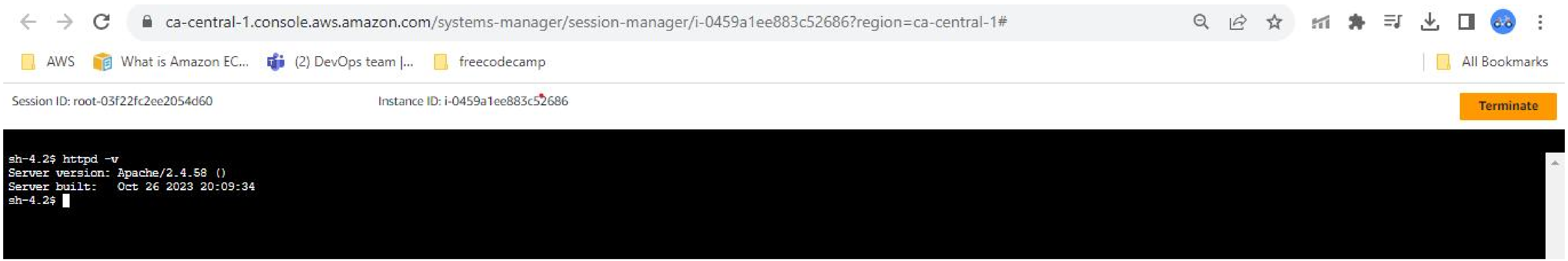
Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

```
Timestamp                      Message
                               No older events at this moment. Retry
2023-11-26T19:04:34.724+05:30  172.32.1.145 - - [26/Nov/2023:13:26:59 +0000] "GET / HTTP/1.1" 403 3630 "-" "ELB-HealthChecker/2.0"
2023-11-26T19:04:34.725+05:30  172.32.2.191 - - [26/Nov/2023:13:26:59 +0000] "GET / HTTP/1.1" 403 3630 "-" "ELB-HealthChecker/2.0"
2023-11-26T19:04:34.725+05:30  172.32.1.145 - - [26/Nov/2023:13:27:29 +0000] "GET / HTTP/1.1" 403 3630 "-" "ELB-HealthChecker/2.0"
2023-11-26T19:04:34.725+05:30  172.32.2.191 - - [26/Nov/2023:13:27:29 +0000] "GET / HTTP/1.1" 403 3630 "-" "ELB-HealthChecker/2.0"
2023-11-26T19:04:34.725+05:30  172.32.1.145 - - [26/Nov/2023:13:27:59 +0000] "GET / HTTP/1.1" 403 3630 "-" "ELB-HealthChecker/2.0"
2023-11-26T19:04:34.725+05:30  172.32.2.191 - - [26/Nov/2023:13:27:59 +0000] "GET / HTTP/1.1" 403 3630 "-" "ELB-HealthChecker/2.0"
2023-11-26T19:04:34.725+05:30  172.32.1.145 - - [26/Nov/2023:13:28:29 +0000] "GET / HTTP/1.1" 403 3630 "-" "ELB-HealthChecker/2.0"
2023-11-26T19:04:34.725+05:30  172.32.2.191 - - [26/Nov/2023:13:28:29 +0000] "GET / HTTP/1.1" 403 3630 "-" "ELB-HealthChecker/2.0"
2023-11-26T19:04:34.726+05:30  172.32.2.191 - - [26/Nov/2023:13:28:42 +0000] "GET / HTTP/1.1" 403 3630 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/10…
2023-11-26T19:04:34.726+05:30  172.32.2.191 - - [26/Nov/2023:13:28:43 +0000] "GET /form.html HTTP/1.1" 404 196 "-" "curl/8.1.2"
2023-11-26T19:04:34.726+05:30  172.32.2.191 - - [26/Nov/2023:13:28:43 +0000] "GET /upl.php HTTP/1.1" 404 196 "-" "Mozilla/5.0"
2023-11-26T19:04:34.726+05:30  172.32.2.191 - - [26/Nov/2023:13:28:43 +0000] "GET /geoip/ HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro…
2023-11-26T19:04:34.726+05:30  172.32.2.191 - - [26/Nov/2023:13:28:43 +0000] "GET / HTTP/1.1" 403 3630 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 13_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like…
```

Validation

3.Login to AWS Session Manager and access the EC2 shell from console.



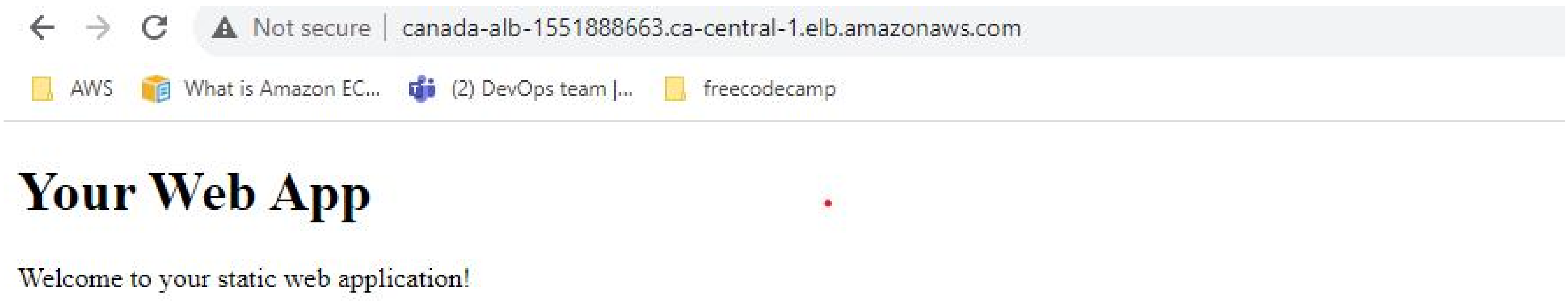
ca-central-1.console.aws.amazon.com/systems-manager/session-manager/i-0459a1ee883c52686?region=ca-central-1#

Session ID: root-03f22fc2ee2054d60

Instance ID: i-0459a1ee883c52686

```
sh-4.2$ httpd -v
Server version: Apache/2.4.58 ()
Server built:   Oct 26 2023 20:09:34
sh-4.2$
```

4.Browse web application from public internet browser using domain name and verify that page loaded.



Not secure | canada-alb-1551888663.ca-central-1.elb.amazonaws.com

Your Web App

Welcome to your static web application!

THANK
YOU