VALAXY TRAINING ASSIGNMENT 3

Pre-Deployment

Customize the application dependencies mentioned below on AWS EC2 instance and create the Golden AMI.

1. AWS CLI
2. Install Apache Web Server
3. Install Git
4. Cloudwatch Agent
5. Push custom memory metrics to Cloudwatch.
6. AWS SSM Agent

Number 1 & 6 are installed by default on AmazonLinux 2, so install the rest.

- Launch an instance in a default VPC and run the following commands

```
sudo su
yum install -y httpd git
yum install amazon-cloudwatch-agent -y
```

- Run this cloudwatch config wizard and select the defaults, but ensure to select the memory option when prompted and the cwagent user

```
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
```

- Start the cloudwatch agent

```
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json -s
```

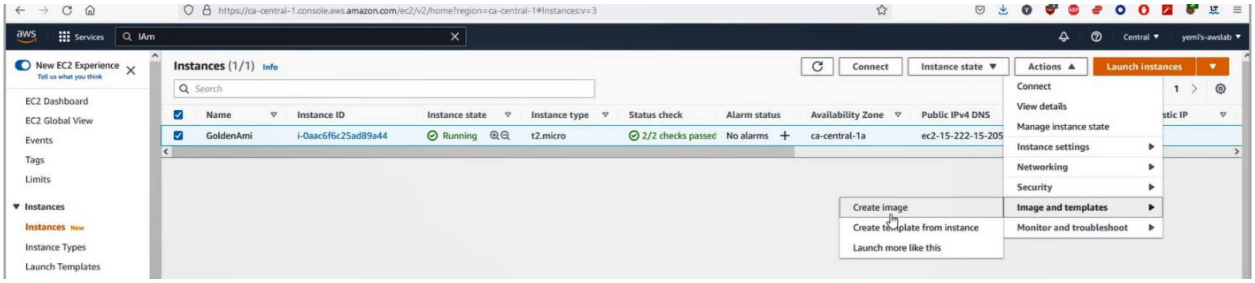
- Verify the cloudwatch agent is running

```
systemctl status amazon-cloudwatch-agent.service
```

- To Push custom memory metrics to Cloudwatch, attach an IAM role to the instance with this AWS managed policy named `CloudWatchFullAccess`

- If you need to test the session manager works also attach `AmazonSSMFullAccess` AWS managed policy to the existing IAM role

Once all dependencies are installed, create the AMI as shown below



Instances (1/1) Info

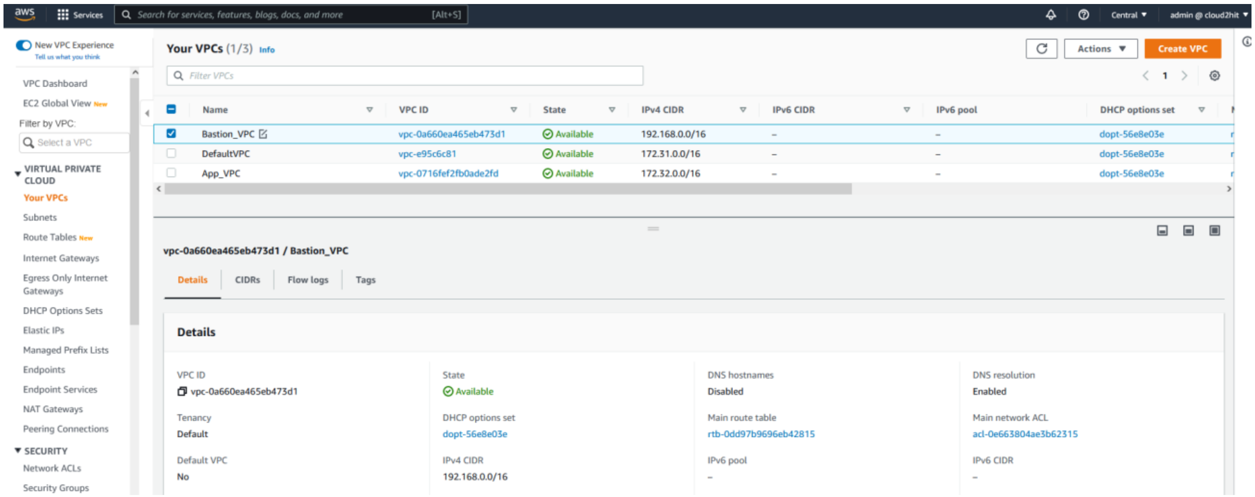
☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	GoldenAmi	i-0aac6f6c25ad89a44	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1a	ec2-15-222-15-205

VPC Deployment

1. Build VPC network (192.168.0.0/16) for Bastion Host deployment as per the architecture shown above.

   `Implemented my whole assignment in Canada (central) region.`

   `Create Bastion VPC with this basic configuration`



Your VPCs (1/3) Info

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP options set
☑	Bastion_VPC	vpc-0a660ea465eb473d1	Available	192.168.0.0/16	–	–	dopt-56e8e03e
□	DefaultVPC	vpc-e95c6c81	Available	172.31.0.0/16	–	–	dopt-56e8e03e
□	App_VPC	vpc-0716fef2fb0ade2fd	Available	172.32.0.0/16	–	–	dopt-56e8e03e

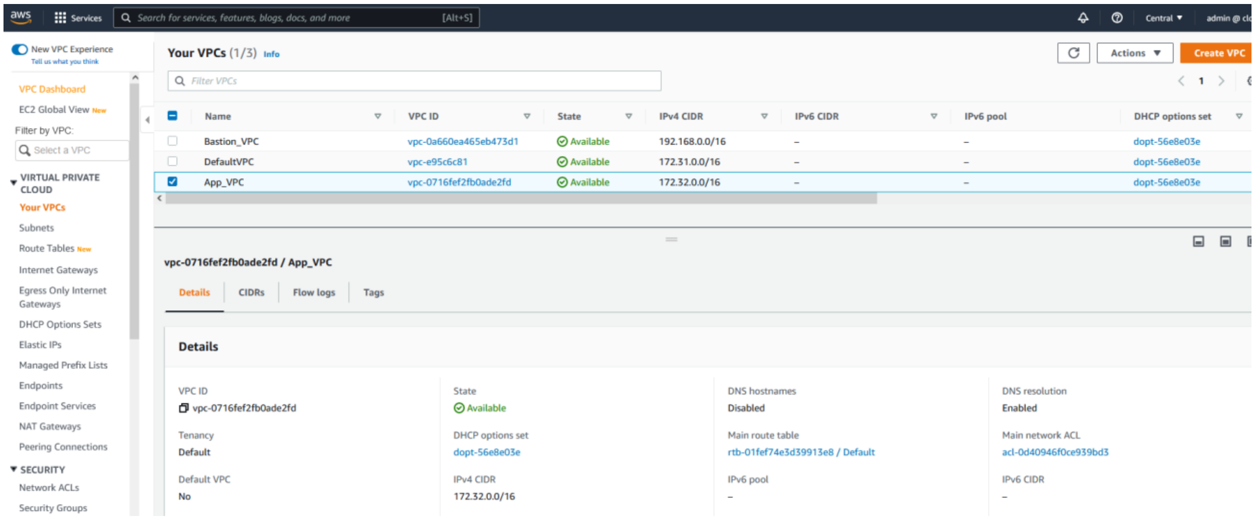
vpc-0a660ea465eb473d1 / Bastion_VPC

Details

VPC ID vpc-0a660ea465eb473d1	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-56e8e03e	Main route table rtb-0dd97b9696eb42815	Main network ACL acl-0e663804ae3b62315
Default VPC No	IPv4 CIDR 192.168.0.0/16	IPv6 pool –	IPv6 CIDR –

2. Build VPC network (172.32.0.0/16) for deploying Highly Available and Auto Scalable application servers as per the architecture shown above.

   `Create App VPC with this basic configuration`



Your VPCs (1/3) Info

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP options set
Bastion_VPC	vpc-0a660ea465eb473d1	Available	192.168.0.0/16	–	–	dopt-56e8e03e
DefaultVPC	vpc-e95c6c81	Available	172.31.0.0/16	–	–	dopt-56e8e03e
App_VPC	vpc-0716fef2fb0ade2fd	Available	172.32.0.0/16	–	–	dopt-56e8e03e

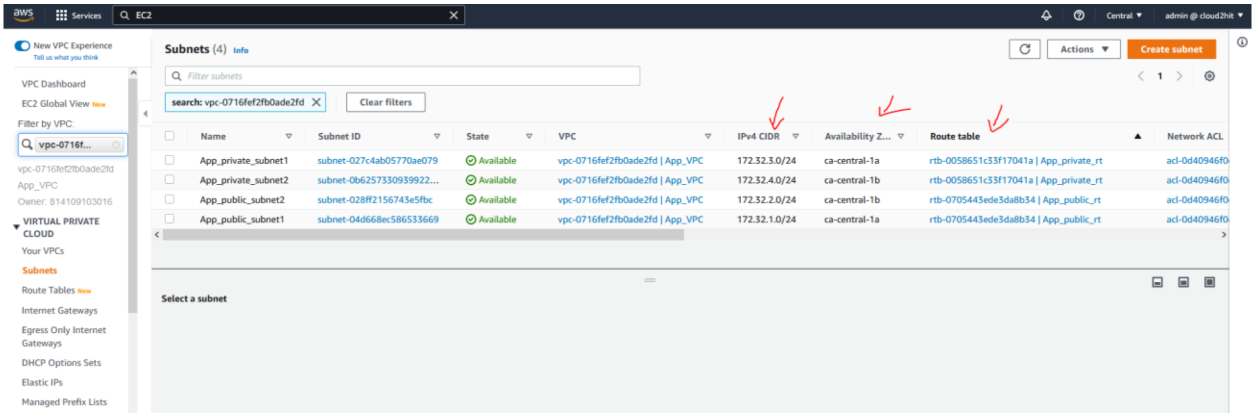
vpc-0716fef2fb0ade2fd / App_VPC

Details

VPC ID vpc-0716fef2fb0ade2fd	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-56e8e03e	Main route table rtb-01fef74e3d39913e8 / Default	Main network ACL acl-0d40946f0ce939bd3
Default VPC No	IPv4 CIDR 172.32.0.0/16	IPv6 pool –	IPv6 CIDR –

3. Create NAT Gateway in Public Subnet and update Private Subnet associated Route Table accordingly to route the default traffic to NAT for outbound internet connection.

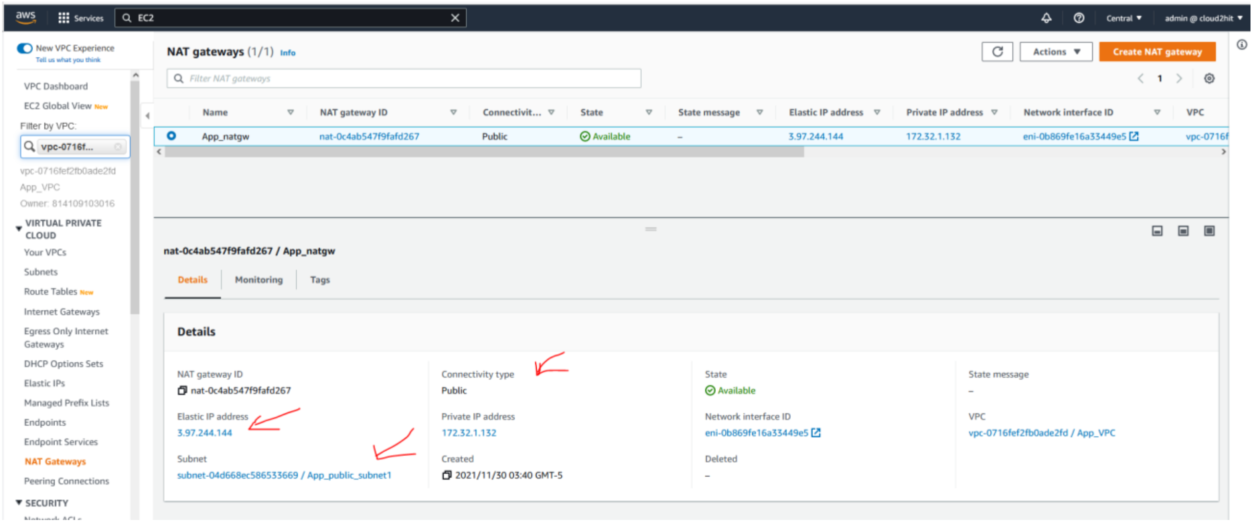
```
Create all 4 subnets shown for APP VPC. Note route table IDs, AZs and
CIDRs
```



Subnets (4) Info

Name	Subnet ID	State	VPC	IPv4 CIDR	Availability Z...	Route table	Network ACL
App_private_subnet1	subnet-027c4ab05770ae079	Available	vpc-0716fef2fb0ade2fd | App_VPC	172.32.3.0/24	ca-central-1a	rtb-0058651c33f17041a | App_private_rt	acl-0d40946f0
App_private_subnet2	subnet-0b6257330939922...	Available	vpc-0716fef2fb0ade2fd | App_VPC	172.32.4.0/24	ca-central-1b	rtb-0058651c33f17041a | App_private_rt	acl-0d40946f0
App_public_subnet2	subnet-028ff2156743e5fbc	Available	vpc-0716fef2fb0ade2fd | App_VPC	172.32.2.0/24	ca-central-1b	rtb-0705443ede3da8b34 | App_public_rt	acl-0d40946f0
App_public_subnet1	subnet-04d668ec586533669	Available	vpc-0716fef2fb0ade2fd | App_VPC	172.32.1.0/24	ca-central-1a	rtb-0705443ede3da8b34 | App_public_rt	acl-0d40946f0

```
Create Nat gateway. Note connectivity type, EIP and public subnet
```



NAT gateways (1/1) Info

	Name	NAT gateway ID	Connectivit...	State	State message	Elastic IP address	Private IP address	Network interface ID	VPC
●	App_natgw	nat-0c4ab547f9fafd267	Public	✓ Available	–	3.97.244.144	172.32.1.132	eni-0b869fe16a33449e5	vpc-0716f

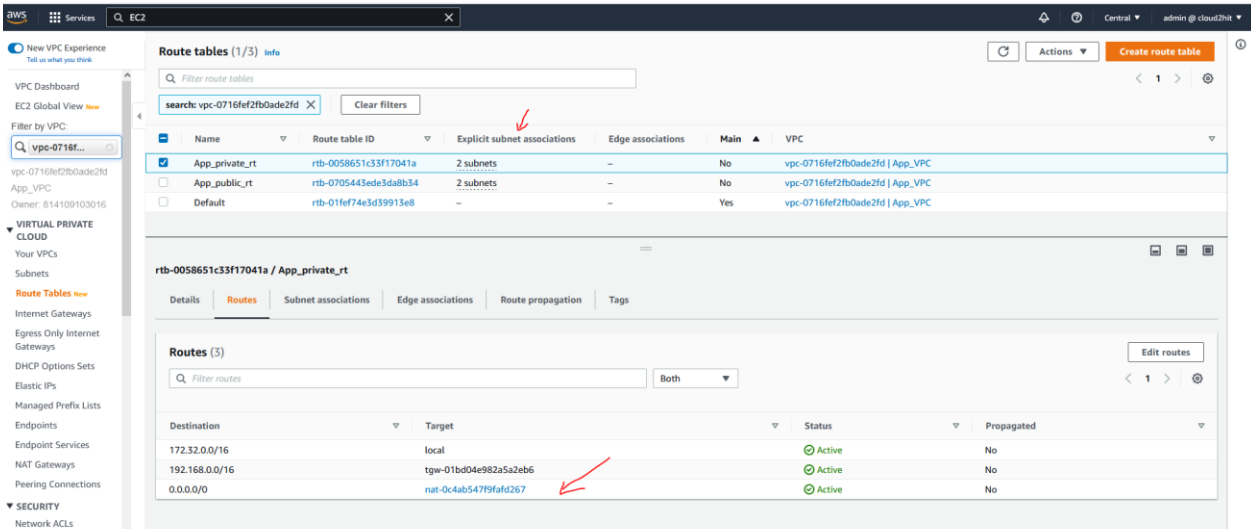
nat-0c4ab547f9fafd267 / App_natgw

Details

NAT gateway ID nat-0c4ab547f9fafd267	Connectivity type Public	State ✓ Available	State message –
Elastic IP address 3.97.244.144	Private IP address 172.32.1.132	Network interface ID eni-0b869fe16a33449e5	VPC vpc-0716fef2fb0ade2fd / App_VPC
Subnet subnet-04d668ec586533669 / App_public_subnet1	Created 2021/11/30 03:40 GMT-5	Deleted –	

See private and public route table rules.

Note 3 route with targets for local, natgw and transit gw in private route table



Route tables (1/3) Info

search: vpc-0716fef2fb0ade2fd

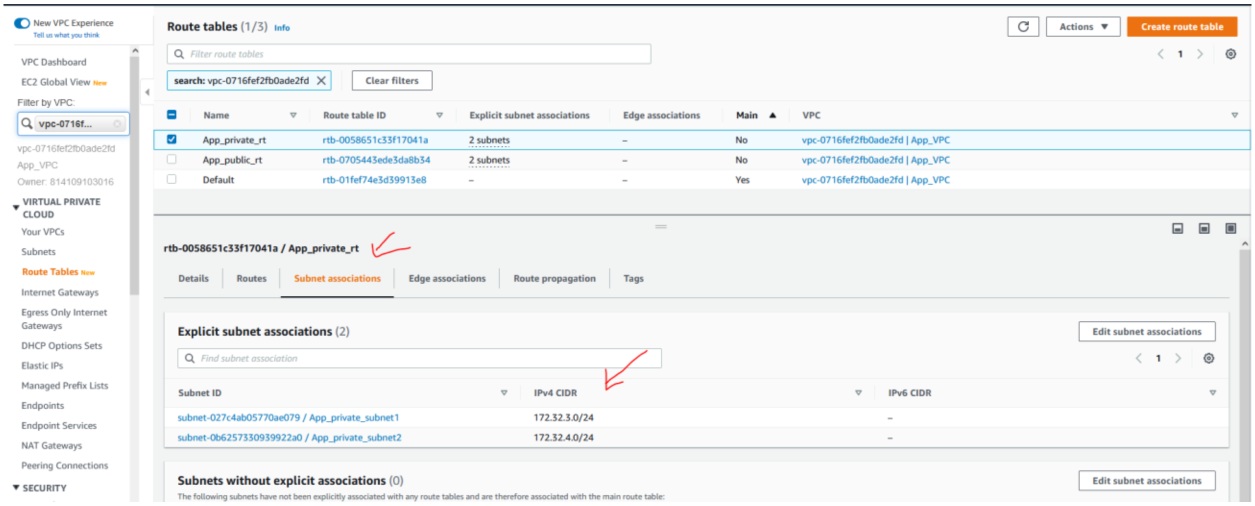
	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
☑	App_private_rt	rtb-0058651c33f17041a	2 subnets	–	No	vpc-0716fef2fb0ade2fd | App_VPC
□	App_public_rt	rtb-0705443ede3da8b34	2 subnets	–	No	vpc-0716fef2fb0ade2fd | App_VPC
□	Default	rtb-01fef74e3d39913e8	–	–	Yes	vpc-0716fef2fb0ade2fd | App_VPC

rtb-0058651c33f17041a / App_private_rt

Routes (3)

Destination	Target	Status	Propagated
172.32.0.0/16	local	✓ Active	No
192.168.0.0/16	tgw-01bd04e982a5a2eb6	✓ Active	No
0.0.0.0/0	nat-0c4ab547f9fafd267	✓ Active	No

Private route table Subnet associations



Route tables (1/3) Info

search: vpc-0716fef2fb0ade2fd

	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
☑	App_private_rt	rtb-0058651c33f17041a	2 subnets	–	No	vpc-0716fef2fb0ade2fd | App_VPC
□	App_public_rt	rtb-0705443ede3da8b34	2 subnets	–	No	vpc-0716fef2fb0ade2fd | App_VPC
□	Default	rtb-01fef74e3d39913e8	–	–	Yes	vpc-0716fef2fb0ade2fd | App_VPC

rtb-0058651c33f17041a / App_private_rt

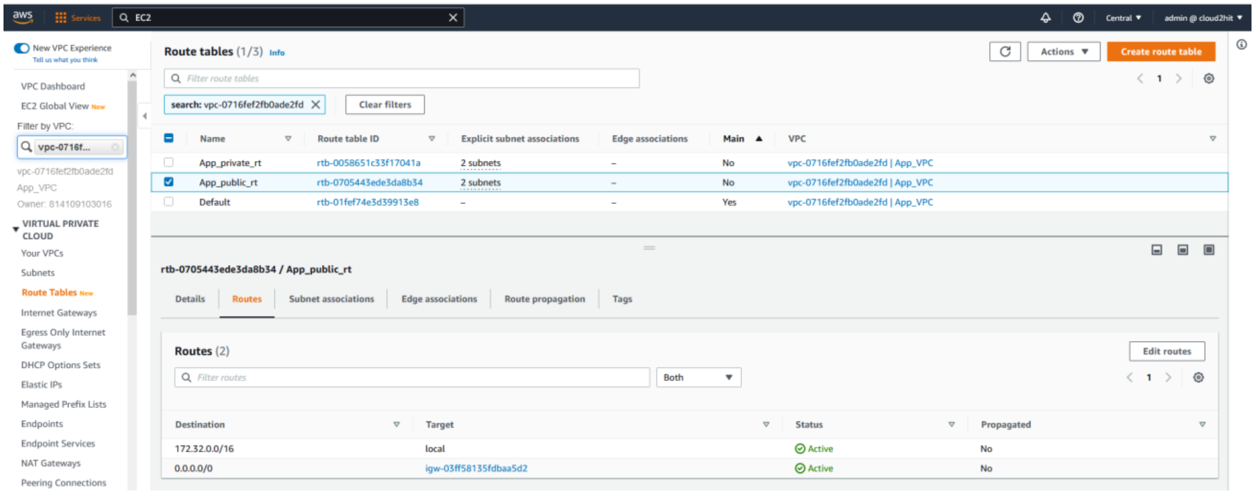
Explicit subnet associations (2)

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-027c4ab05770ae079 / App_private_subnet1	172.32.3.0/24	–
subnet-0b6257330939922a0 / App_private_subnet2	172.32.4.0/24	–

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

```
Public route table in APP VPC with 0.0.0.0/0 route
```



Route tables (1/3) Info

search: vpc-0716fef2fb0ade2fd

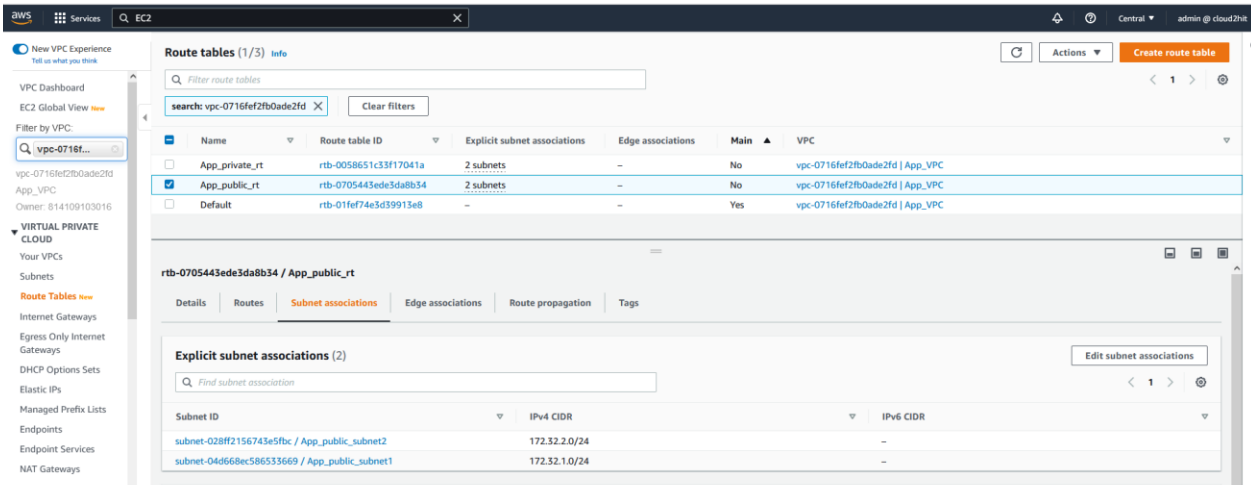
	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
□	App_private_rt	rtb-0058651c33f17041a	2 subnets	–	No	vpc-0716fef2fb0ade2fd | App_VPC
☑	App_public_rt	rtb-0705443ede3da8b34	2 subnets	–	No	vpc-0716fef2fb0ade2fd | App_VPC
□	Default	rtb-01fef74e3d39913e8	–	–	Yes	vpc-0716fef2fb0ade2fd | App_VPC

rtb-0705443ede3da8b34 / App_public_rt

Routes (2)

Destination	Target	Status	Propagated
172.32.0.0/16	local	✓ Active	No
0.0.0.0/0	igw-03ff58135fdbaa5d2	✓ Active	No

```
Public route table Subnet associations
```



Route tables (1/3) Info

search: vpc-0716fef2fb0ade2fd

	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
□	App_private_rt	rtb-0058651c33f17041a	2 subnets	–	No	vpc-0716fef2fb0ade2fd | App_VPC
☑	App_public_rt	rtb-0705443ede3da8b34	2 subnets	–	No	vpc-0716fef2fb0ade2fd | App_VPC
□	Default	rtb-01fef74e3d39913e8	–	–	Yes	vpc-0716fef2fb0ade2fd | App_VPC

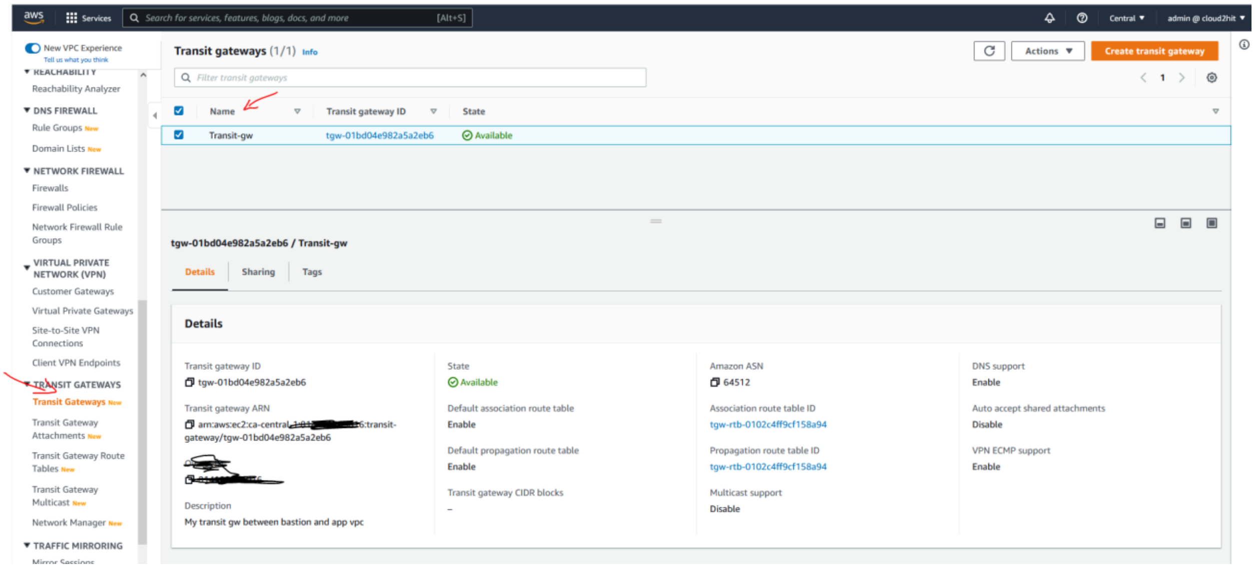
rtb-0705443ede3da8b34 / App_public_rt

Explicit subnet associations (2)

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-028ff2156743e5fbc / App_public_subnet2	172.32.2.0/24	–
subnet-04d668ec586533669 / App_public_subnet1	172.32.1.0/24	–

4. Create Transit Gateway and associate both VPCs to the Transit Gateway for private communication.

   `Click create transit gateway and add only a name`



Transit gateways (1/1)

☑	Name	Transit gateway ID	State
☑	Transit-gw	tgw-01bd04e982a5a2eb6	Available

tgw-01bd04e982a5a2eb6 / Transit-gw

Details | Sharing | Tags

Details

Transit gateway ID
tgw-01bd04e982a5a2eb6

Transit gateway ARN
arn:aws:ec2:ca-central[redacted]6:transit-gateway/tgw-01bd04e982a5a2eb6

[redacted]

Description
My transit gw between bastion and app vpc

State
Available

Default association route table
Enable

Default propagation route table
Enable

Transit gateway CIDR blocks
–

Amazon ASN
64512

Association route table ID
tgw-rtb-0102c4ff9cf158a94

Propagation route table ID
tgw-rtb-0102c4ff9cf158a94

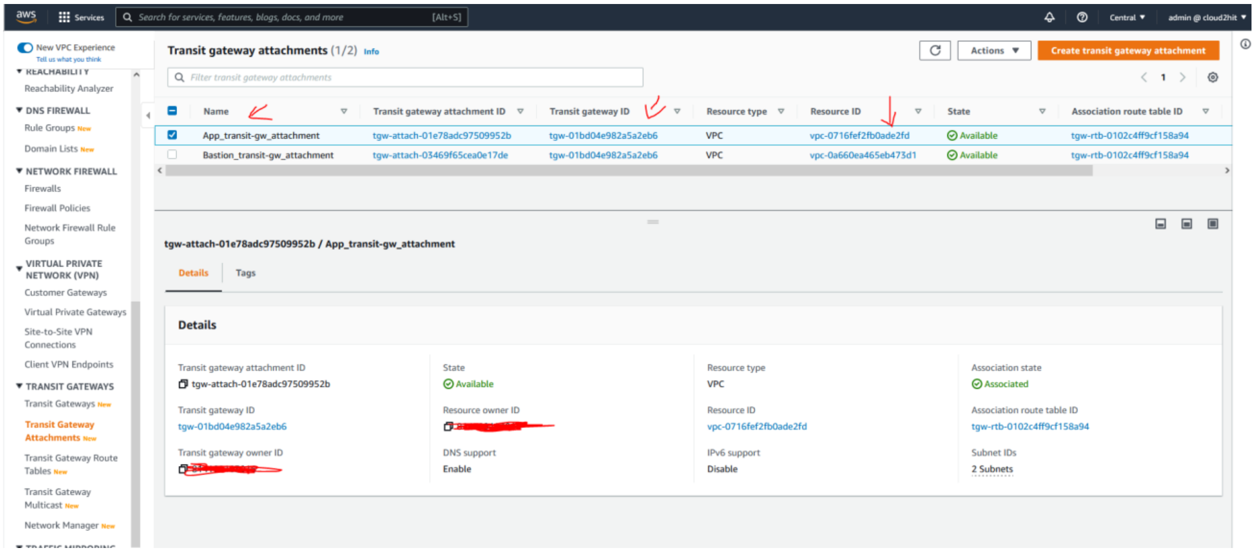
Multicast support
Disable

DNS support
Enable

Auto accept shared attachments
Disable

VPN ECMP support
Enable

   `You need to create 2 transit gw attachment to each VPC. Add name, select existing transit gw ID, select Bastion & App VPC`



Transit gateway attachments (1/2)

	Name	Transit gateway attachment ID	Transit gateway ID	Resource type	Resource ID	State	Association route table ID
☑	App_transit-gw_attachment	tgw-attach-01e78adc97509952b	tgw-01bd04e982a5a2eb6	VPC	vpc-0716fef2fb0ade2fd	Available	tgw-rtb-0102c4ff9cf158a94
☐	Bastion_transit-gw_attachment	tgw-attach-03469f65cea0e17de	tgw-01bd04e982a5a2eb6	VPC	vpc-0a660ea465eb473d1	Available	tgw-rtb-0102c4ff9cf158a94

tgw-attach-01e78adc97509952b / App_transit-gw_attachment

Details | Tags

Details

Transit gateway attachment ID
tgw-attach-01e78adc97509952b

Transit gateway ID
tgw-01bd04e982a5a2eb6

Transit gateway owner ID
[redacted]

State
Available

Resource owner ID
[redacted]

DNS support
Enable

Resource type
VPC

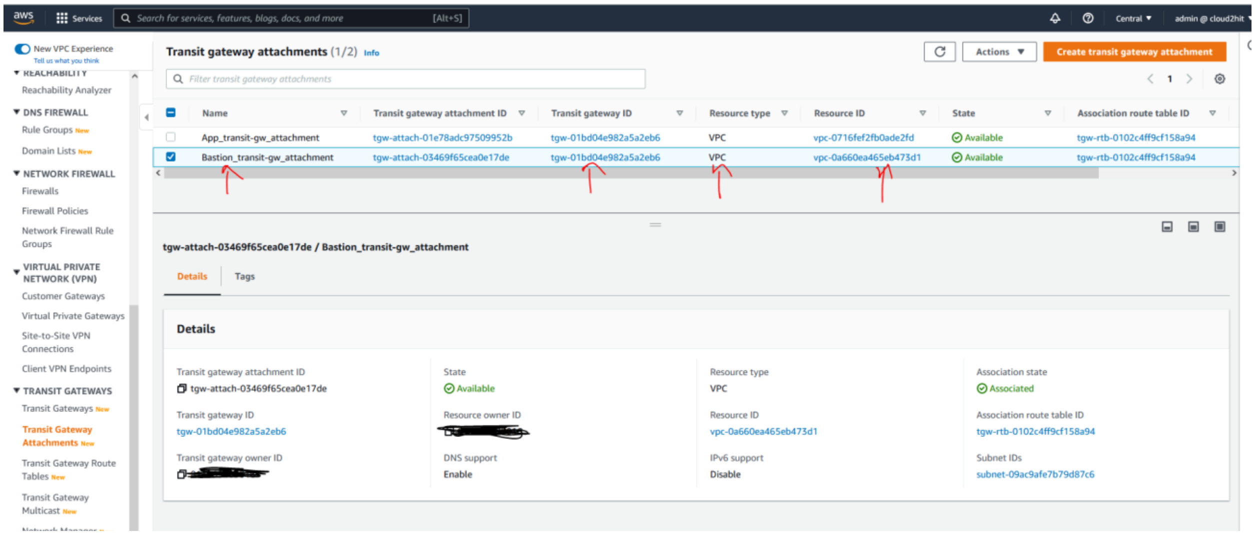
Resource ID
vpc-0716fef2fb0ade2fd

IPv6 support
Disable

Association state
Associated

Association route table ID
tgw-rtb-0102c4ff9cf158a94

Subnet IDs
2 Subnets



Transit gateway attachments (1/2) Info

	Name	Transit gateway attachment ID	Transit gateway ID	Resource type	Resource ID	State	Association route table ID
□	App_transit-gw_attachment	tgw-attach-01e78adc97509952b	tgw-01bd04e982a5a2eb6	VPC	vpc-0716fef2fb0ade2fd	✓ Available	tgw-rtb-0102c4ff9cf158a94
☑	Bastion_transit-gw_attachment	tgw-attach-03469f65cea0e17de	tgw-01bd04e982a5a2eb6	VPC	vpc-0a660ea465eb473d1	✓ Available	tgw-rtb-0102c4ff9cf158a94

tgw-attach-03469f65cea0e17de / Bastion_transit-gw_attachment

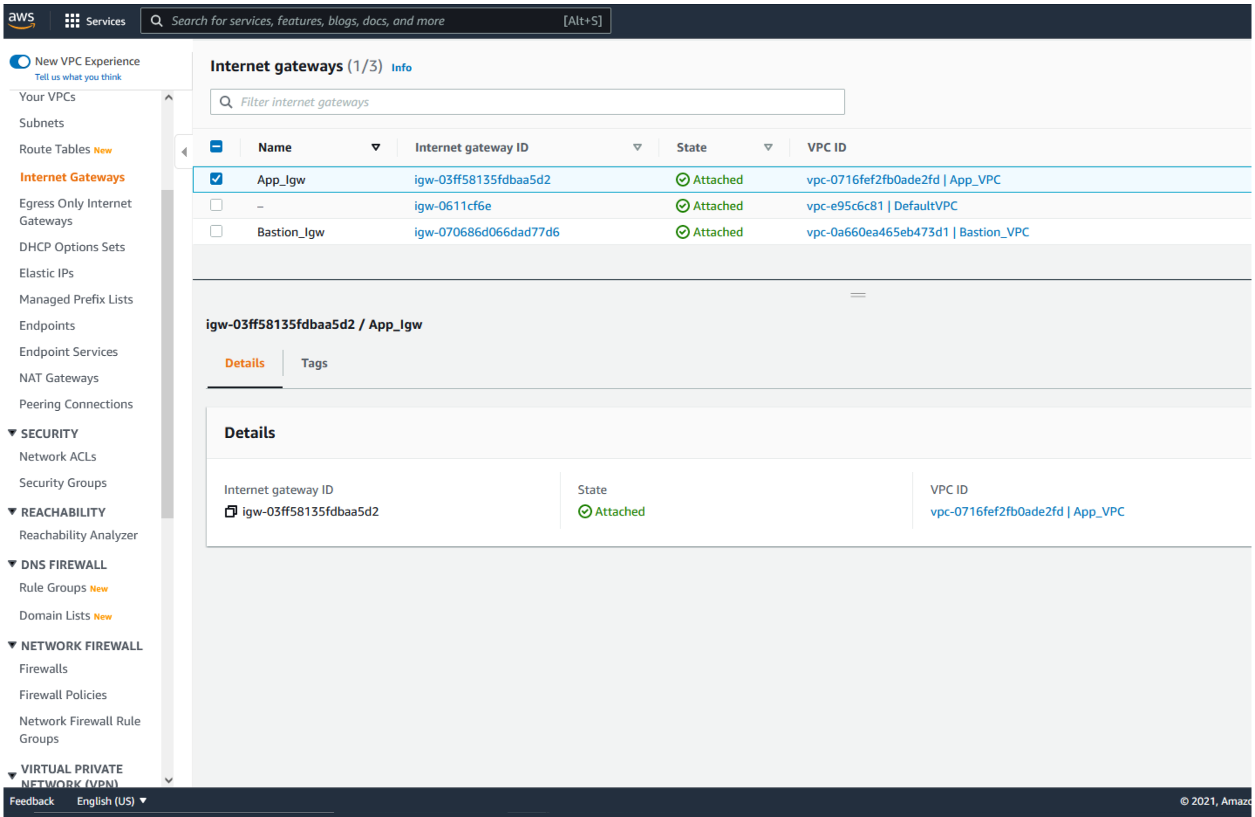
Details | Tags

Details

Transit gateway attachment ID tgw-attach-03469f65cea0e17de	State ✓ Available	Resource type VPC	Association state ✓ Associated
Transit gateway ID tgw-01bd04e982a5a2eb6	Resource owner ID [redacted]	Resource ID vpc-0a660ea465eb473d1	Association route table ID tgw-rtb-0102c4ff9cf158a94
Transit gateway owner ID [redacted]	DNS support Enable	IPv6 support Disable	Subnet IDs subnet-09ac9afe7b79d87c6

5. Create Internet Gateway for each VPC and Public Subnet associated Route Table accordingly to route the default traffic to IGW for inbound/outbound internet connection.

   Create 2 Internet GWz and attach to each VPC. Routes are shown with 0.0.0.0/0 in previous step snapshot



Internet gateways (1/3) Info

Filter internet gateways

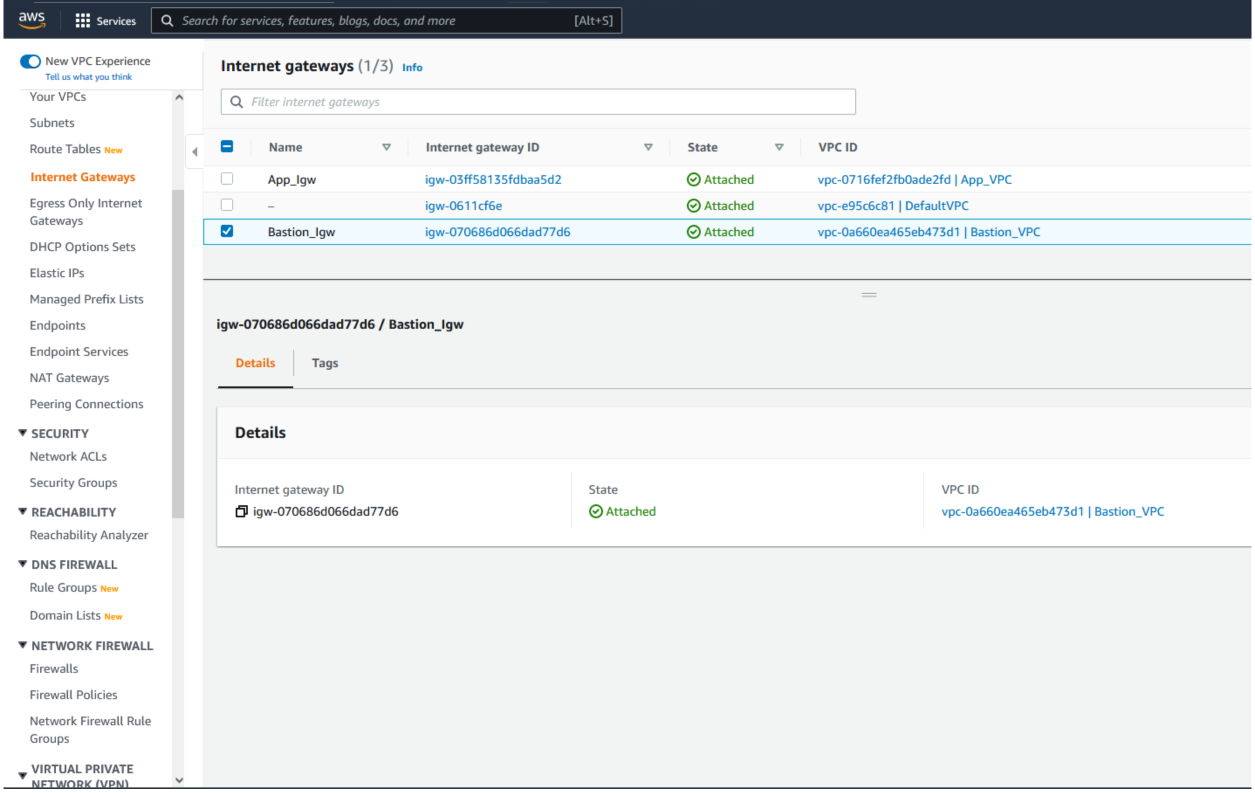
	Name	Internet gateway ID	State	VPC ID
☑	App_Igw	igw-03ff58135fdbaa5d2	Attached	vpc-0716fef2fb0ade2fd | App_VPC
□	–	igw-0611cf6e	Attached	vpc-e95c6c81 | DefaultVPC
□	Bastion_Igw	igw-070686d066dad77d6	Attached	vpc-0a660ea465eb473d1 | Bastion_VPC

igw-03ff58135fdbaa5d2 / App_Igw

Details | Tags

Details

Internet gateway ID	State	VPC ID
igw-03ff58135fdbaa5d2	Attached	vpc-0716fef2fb0ade2fd | App_VPC



Internet gateways (1/3) Info

Filter internet gateways

	Name	Internet gateway ID	State	VPC ID
□	App_Igw	igw-03ff58135fdbaa5d2	Attached	vpc-0716fef2fb0ade2fd | App_VPC
□	–	igw-0611cf6e	Attached	vpc-e95c6c81 | DefaultVPC
☑	Bastion_Igw	igw-070686d066dad77d6	Attached	vpc-0a660ea465eb473d1 | Bastion_VPC

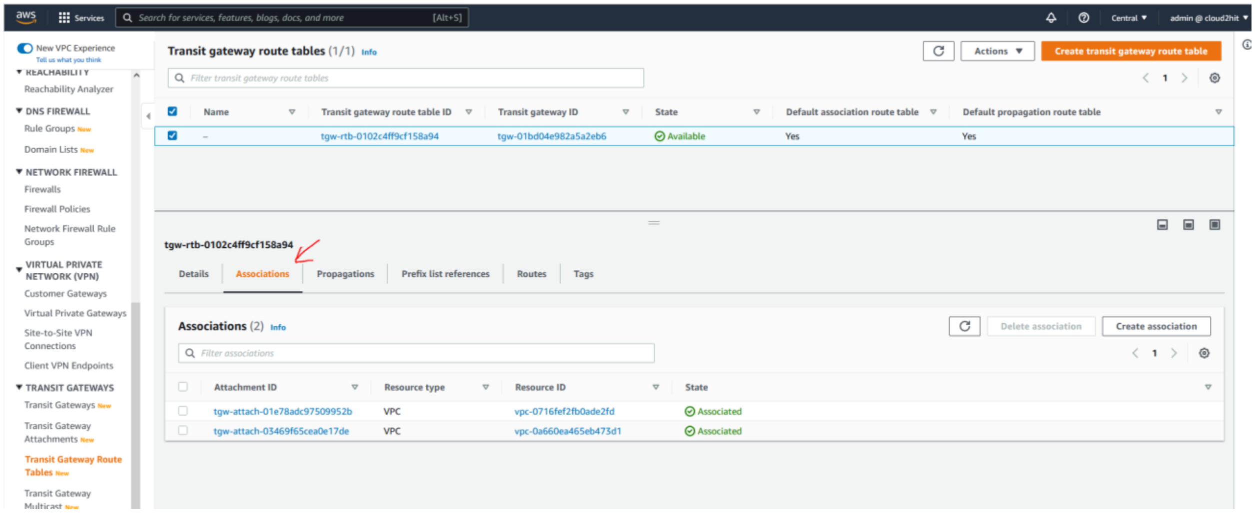
igw-070686d066dad77d6 / Bastion_Igw

Details | Tags

Details

Internet gateway ID	State	VPC ID
igw-070686d066dad77d6	Attached	vpc-0a660ea465eb473d1 | Bastion_VPC

This transit gateway route table will be created by default with these associations to each VPC



Transit gateway route tables (1/1) Info

☑	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table	Default propagation route table
☑	–	tgw-rtb-0102c4ff9cf158a94	tgw-01bd04e982a5a2eb6	✓ Available	Yes	Yes

tgw-rtb-0102c4ff9cf158a94

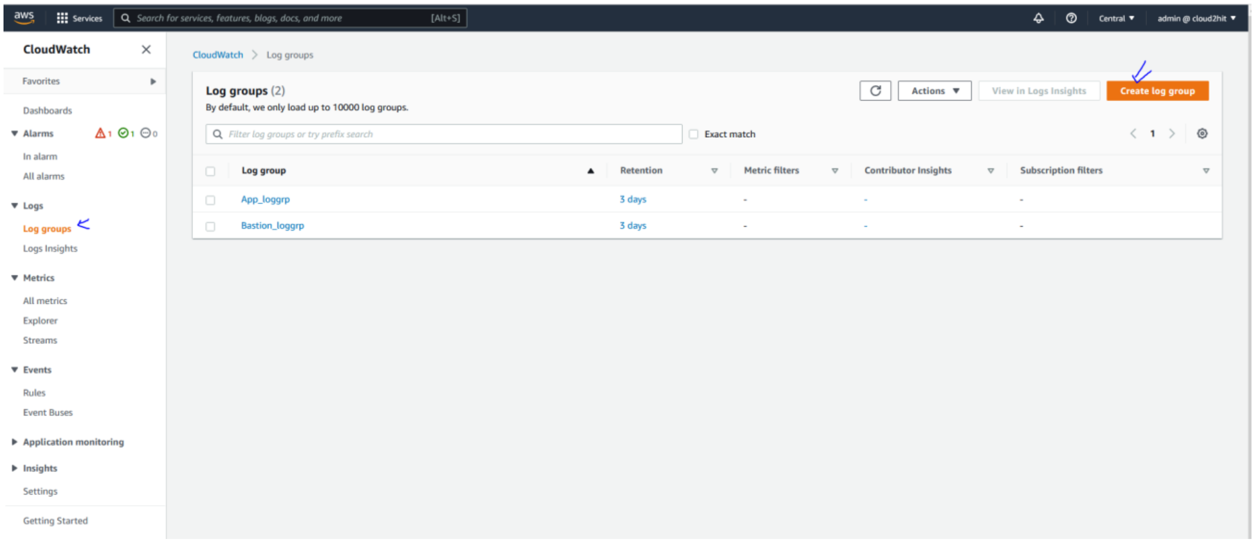
Associations (2) Info

□	Attachment ID	Resource type	Resource ID	State
□	tgw-attach-01e78adc97509952b	VPC	vpc-0716fef2fb0ade2fd	✓ Associated
□	tgw-attach-03469f65cea0e17de	VPC	vpc-0a660ea465eb473d1	✓ Associated

Afterwards update the private route table in ApP vpc and public route table in Bastion VPC, with the routes shown in previous snapshot

6. Create Cloudwatch Log Group with two Log Streams to store the VPC Flow Logs of both VPCs.

   To create 2 logroups, Click logroup in cloudwatch and click create log group. These 2 for Bastion and App VPCs were created with a retention 3 days. No logs streams will be seen until next step

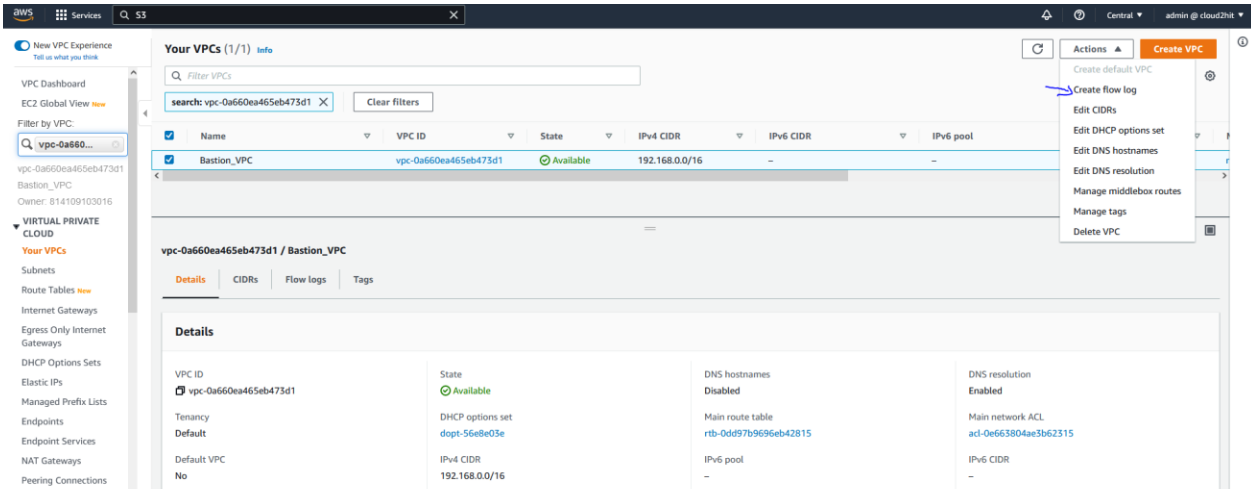


Log groups (2)
By default, we only load up to 10000 log groups.

□	Log group	Retention	Metric filters	Contributor Insights	Subscription filters
□	App_loggrp	3 days	-	-	-
□	Bastion_loggrp	3 days	-	-	-

7. Enable Flow Logs for both VPCs and push the Flow Logs to Cloudwatch Log Groups and store the logs in the respective Log Stream for each VPC.

   To enable flow logs, click Actions and Create flow logs. Repeat for each VPC



Your VPCs (1/1) Info

search: vpc-0a660ea465eb473d1 | Clear filters

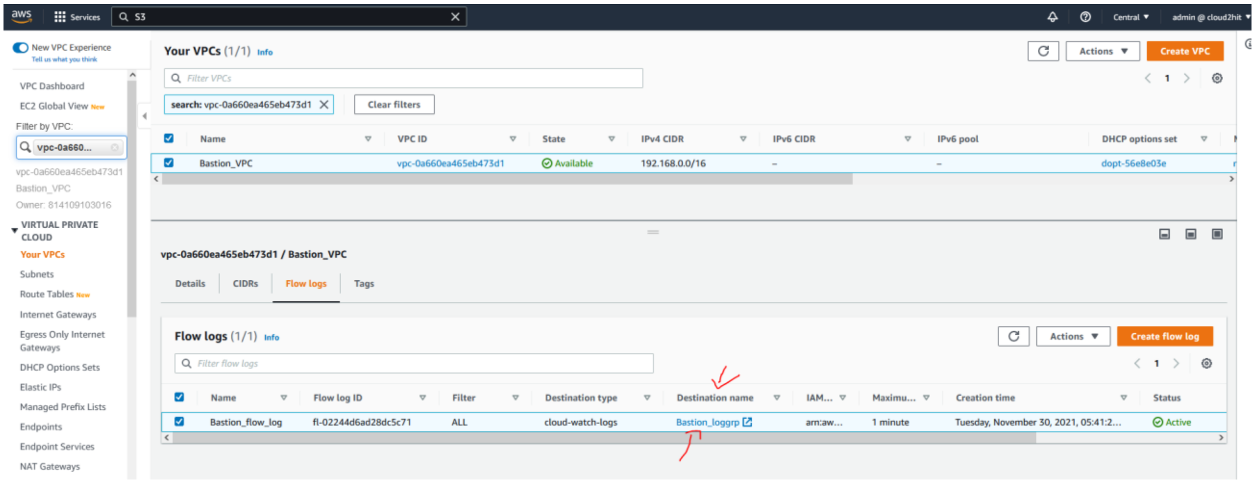
☑	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool
☑	Bastion_VPC	vpc-0a660ea465eb473d1	Available	192.168.0.0/16	–	–

vpc-0a660ea465eb473d1 / Bastion_VPC

Details

VPC ID vpc-0a660ea465eb473d1	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-56e8e03e	Main route table rtb-0dd97b9696eb42815	Main network ACL acl-0e663804ae3b62315
Default VPC No	IPv4 CIDR 192.168.0.0/16	IPv6 pool –	IPv6 CIDR –

This is bastion VPC flow log settings after creation. Note the destination Name from previous step



Your VPCs (1/1) Info

search: vpc-0a660ea465eb473d1 | Clear filters

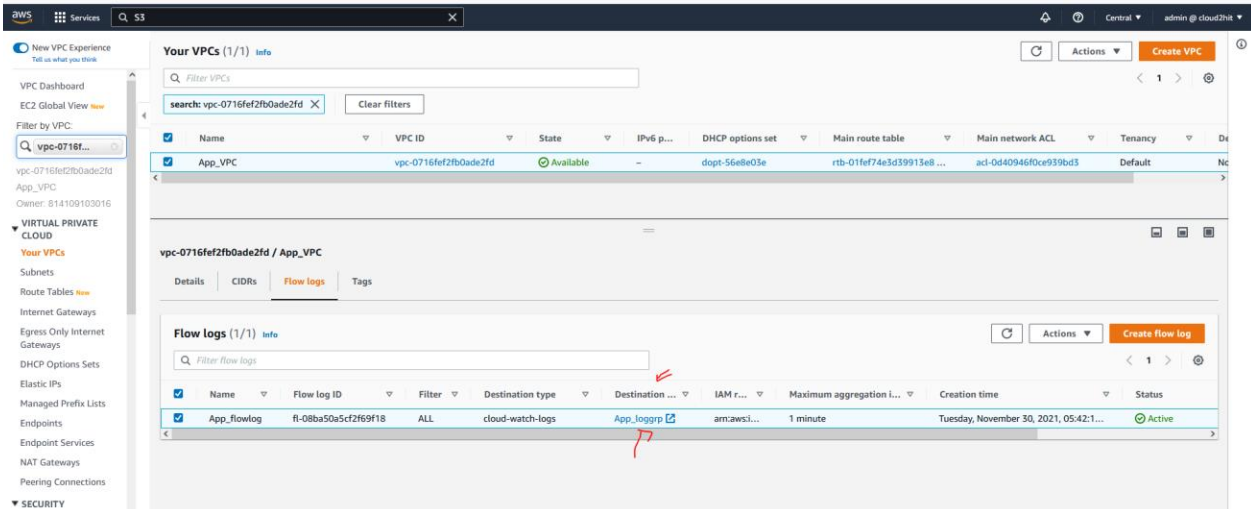
☑	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP options set
☑	Bastion_VPC	vpc-0a660ea465eb473d1	Available	192.168.0.0/16	–	–	dopt-56e8e03e

vpc-0a660ea465eb473d1 / Bastion_VPC

Flow logs (1/1) Info

☑	Name	Flow log ID	Filter	Destination type	Destination name	IAM...	Maximu...	Creation time	Status
☑	Bastion_flow_log	fl-02244d6ad28dc5c71	ALL	cloud-watch-logs	Bastion_loggrp	arn:aw...	1 minute	Tuesday, November 30, 2021, 05:41:2...	Active

Similar config for APP vpc flow log



Your VPCs (1/1) Info

search: vpc-0716fef2fb0ade2fd | Clear filters

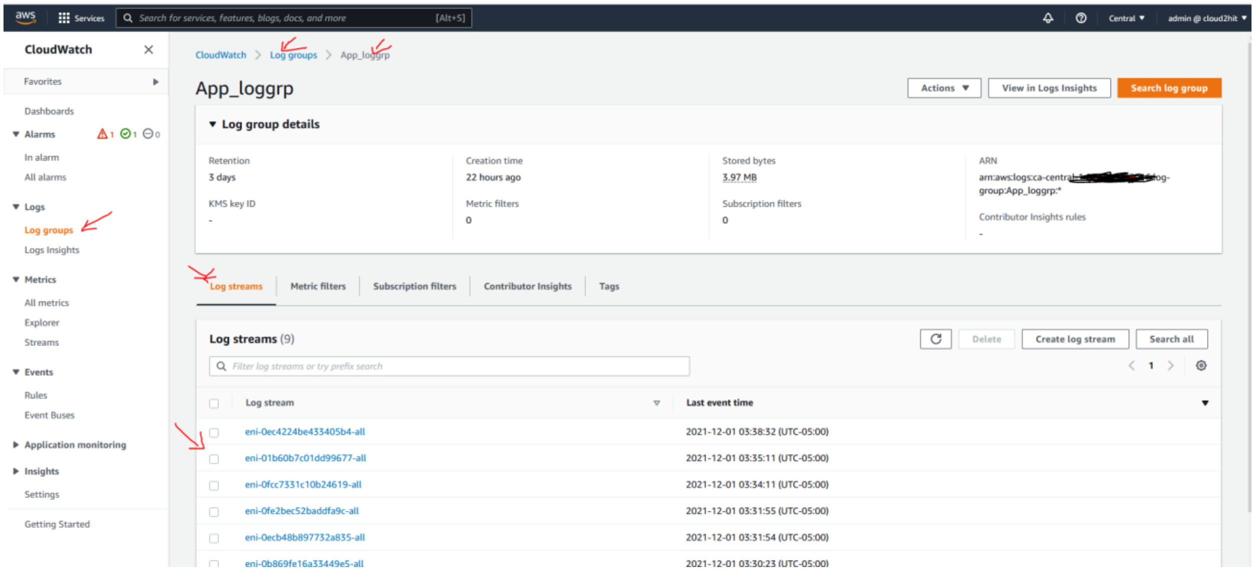
☑	Name	VPC ID	State	IPv6 p...	DHCP options set	Main route table	Main network ACL	Tenancy	De
☑	App_VPC	vpc-0716fef2fb0ade2fd	Available	–	dopt-56e8e03e	rtb-01fef74e3d39913e8 ...	acl-0d40946f0ce939bd3	Default	Nc

vpc-0716fef2fb0ade2fd / App_VPC

Flow logs (1/1) Info

☑	Name	Flow log ID	Filter	Destination type	Destination ...	IAM r...	Maximum aggregation i...	Creation time	Status
☑	App_flowlog	fl-08ba50a5cf2f69f18	ALL	cloud-watch-logs	App_loggrp	arn:aws:i...	1 minute	Tuesday, November 30, 2021, 05:42:1...	Active

These log streams will auto stream once steps above are completed. APP vpc sample flow logs are Shown below



App_loggrp

Log group details

Retention: 3 days

KMS key ID: -

Creation time: 22 hours ago

Metric filters: 0

Stored bytes: 3.97 MB

Subscription filters: 0

ARN: arn:aws:logs:ca-central[redacted]og-group:App_loggrp:*

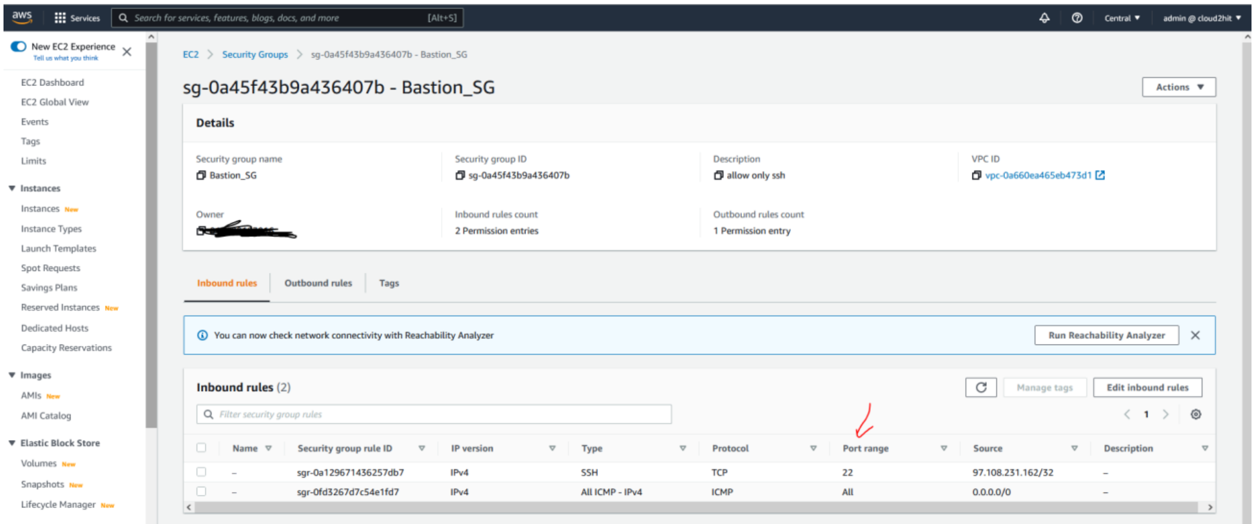
Contributor Insights rules: -

Log streams (9)

Log stream	Last event time
eni-0ec4224be433405b4-all	2021-12-01 03:38:32 (UTC-05:00)
eni-01b60b7c01dd99677-all	2021-12-01 03:35:11 (UTC-05:00)
eni-0fcc7331c10b24619-all	2021-12-01 03:34:11 (UTC-05:00)
eni-0fe2bec52baddfa9c-all	2021-12-01 03:31:55 (UTC-05:00)
eni-0ecb48b897732a835-all	2021-12-01 03:31:54 (UTC-05:00)
eni-0b869fe16a33449e5-all	2021-12-01 03:30:23 (UTC-05:00)

8. Create Security Group for bastion host allowing port 22 from public.

Open port 22 and icmp (optional for ping tests)



sg-0a45f43b9a436407b - Bastion_SG

Details

Security group name: Bastion_SG

Security group ID: sg-0a45f43b9a436407b

Description: allow only ssh

VPC ID: vpc-0a660ea465eb473d1

Owner: [redacted]

Inbound rules count: 2 Permission entries

Outbound rules count: 1 Permission entry

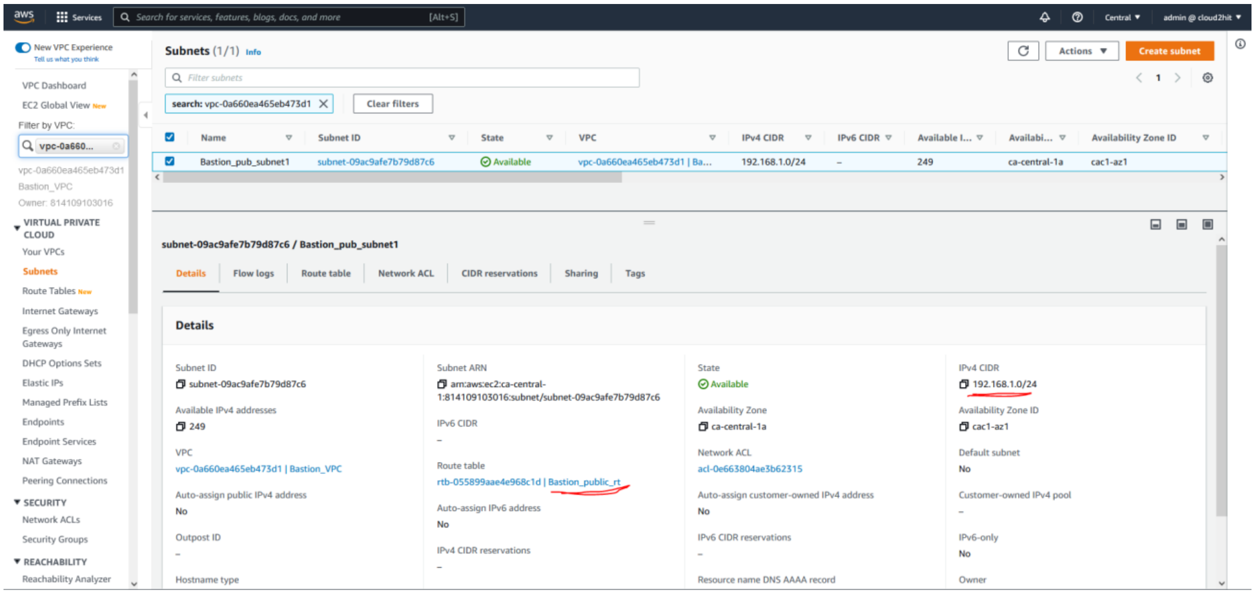
You can now check network connectivity with Reachability Analyzer

Inbound rules (2)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
–	sgr-0a129671436257db7	IPv4	SSH	TCP	22	97.108.231.162/32	–
–	sgr-0fd3267d7c54e1fd7	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	–

9. Deploy Bastion Host EC2 instance in the Public Subnet with EIP associated.

Create Bastion subnet and public route table. Note the CIDR and linked route table



Subnets (1/1) Info

search: vpc-0a660ea465eb473d1

☑	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available I...	Availabi...	Availability Zone ID
☑	Bastion_pub_subnet1	subnet-09ac9afe7b79d87c6	✓ Available	vpc-0a660ea465eb473d1 | Ba...	192.168.1.0/24	–	249	ca-central-1a	cac1-az1

subnet-09ac9afe7b79d87c6 / Bastion_pub_subnet1

Details

Subnet ID: subnet-09ac9afe7b79d87c6

Available IPv4 addresses: 249

VPC: vpc-0a660ea465eb473d1 | Bastion_VPC

Auto-assign public IPv4 address: No

Outpost ID: –

Hostname type

Subnet ARN: arn:aws:ec2:ca-central-1:814109103016:subnet/subnet-09ac9afe7b79d87c6

IPv6 CIDR: –

Route table: rtb-055899aae4e968c1d | Bastion_public_rt

Auto-assign IPv6 address: No

IPv4 CIDR reservations: –

State: ✓ Available

Availability Zone: ca-central-1a

Network ACL: acl-0e663804ae3b62315

Auto-assign customer-owned IPv4 address: No

IPv6 CIDR reservations: –

Resource name DNS AAAA record

IPv4 CIDR: 192.168.1.0/24

Availability Zone ID: cac1-az1

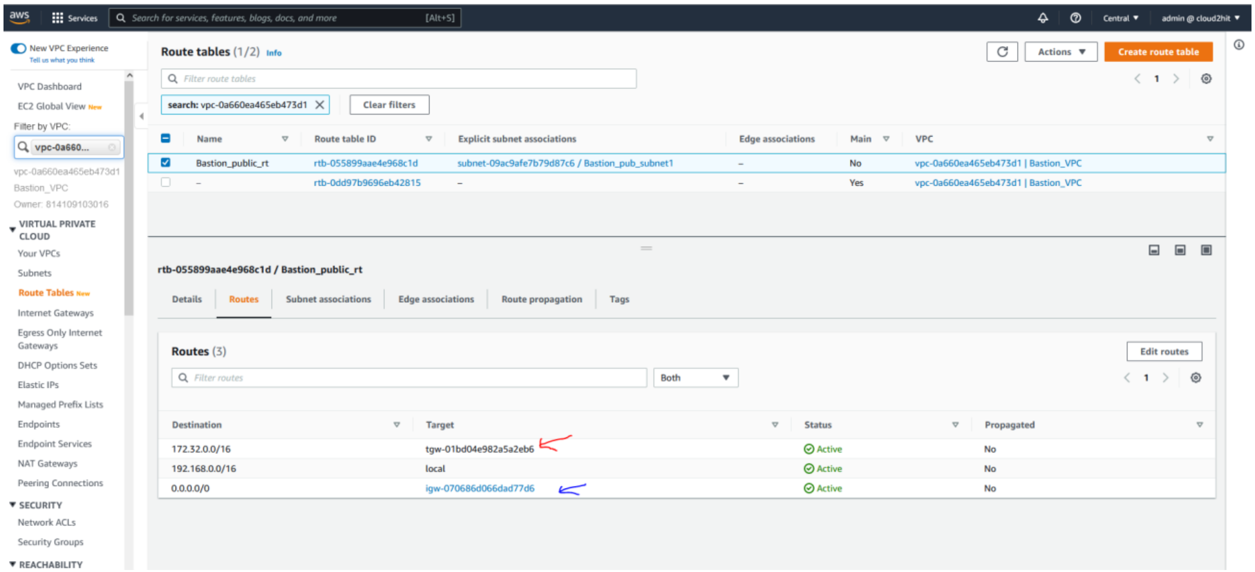
Default subnet: No

Customer-owned IPv4 pool: –

IPv6-only: No

Owner

Public route table of the bastion subnet is shown here. The red route is for a route via the transit gateway to the App VPC and the blue route is for a route for Internet access in and out of the bastion subnet. The tgw ID will only appear after setting up the transit gateway



Route tables (1/2) Info

search: vpc-0a660ea465eb473d1

	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
☑	Bastion_public_rt	rtb-055899aae4e968c1d	subnet-09ac9afe7b79d87c6 / Bastion_pub_subnet1	–	No	vpc-0a660ea465eb473d1 | Bastion_VPC
□	–	rtb-0dd97b9696eb42815	–	–	Yes	vpc-0a660ea465eb473d1 | Bastion_VPC

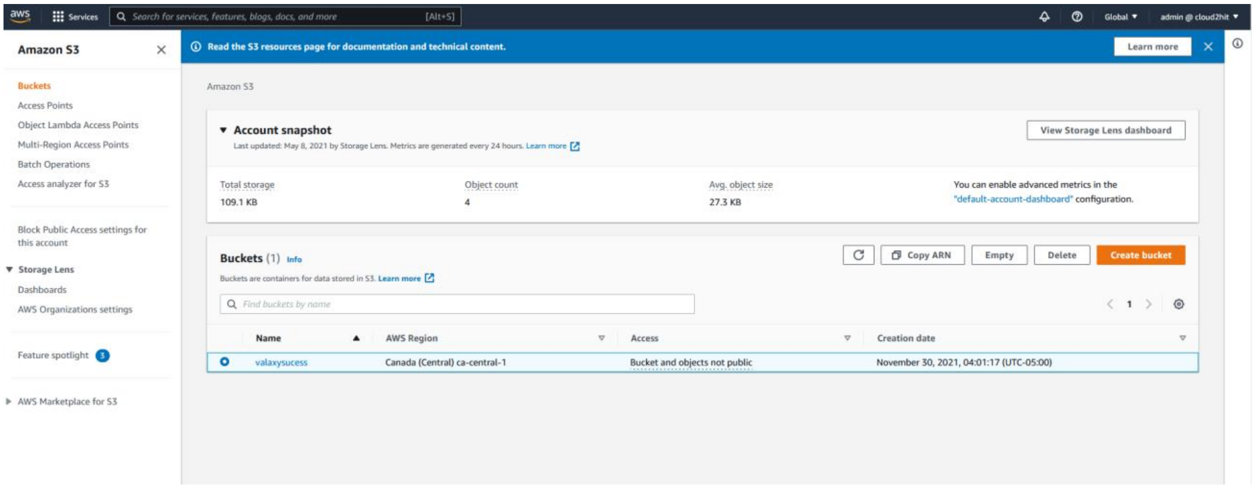
rtb-055899aae4e968c1d / Bastion_public_rt

Routes (3)

Destination	Target	Status	Propagated
172.32.0.0/16	tgw-01bd04e982a5a2eb6	✓ Active	No
192.168.0.0/16	local	✓ Active	No
0.0.0.0/0	igw-070686d066dad77d6	✓ Active	No

10. Create S3 Bucket to store application specific configuration.

This bucket was created in Canada region with default settings



Read the S3 resources page for documentation and technical content.

Account snapshot

Last updated: May 8, 2021 by Storage Lens. Metrics are generated every 24 hours. Learn more

Total storage	Object count	Avg. object size	
109.1 KB	4	27.3 KB	You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets (1) Info

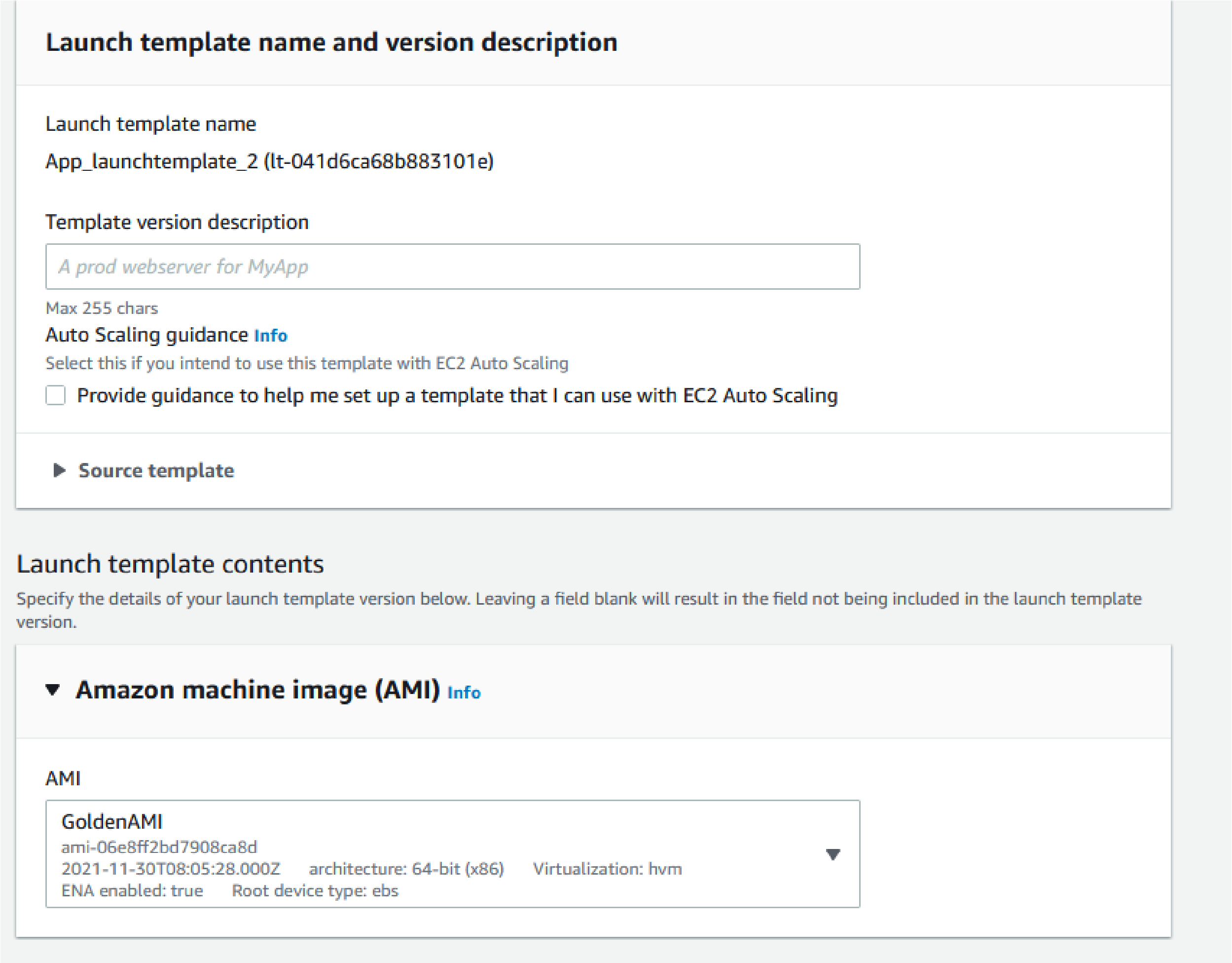
Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
●	valaxysucess	Canada (Central) ca-central-1	Bucket and objects not public	November 30, 2021, 04:01:17 (UTC-05:00)

11. Create Launch Configuration with below configuration.
    1. Golden AMI
    2. Instance Type – t2.micro
    3. Userdata to pull the code from Bitbucket Repository to document root folder of webserver and start the httpd service.
    4. IAM Role granting access to Session Manager and to S3 bucket created in the previous step to pull the configuration. (Do not grant S3 Full Access)
    5. Security Group allowing port 22 from Bastion Host and Port 80 from Public.
    6. Key Pair

```
Specification shown here. Create a launch template
```

Referenced previously taken golden ami



Launch template name and version description

Launch template name

App_launchtemplate_2 (lt-041d6ca68b883101e)

Template version description

A prod webserver for MyApp

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

▶ **Source template**

Launch template contents

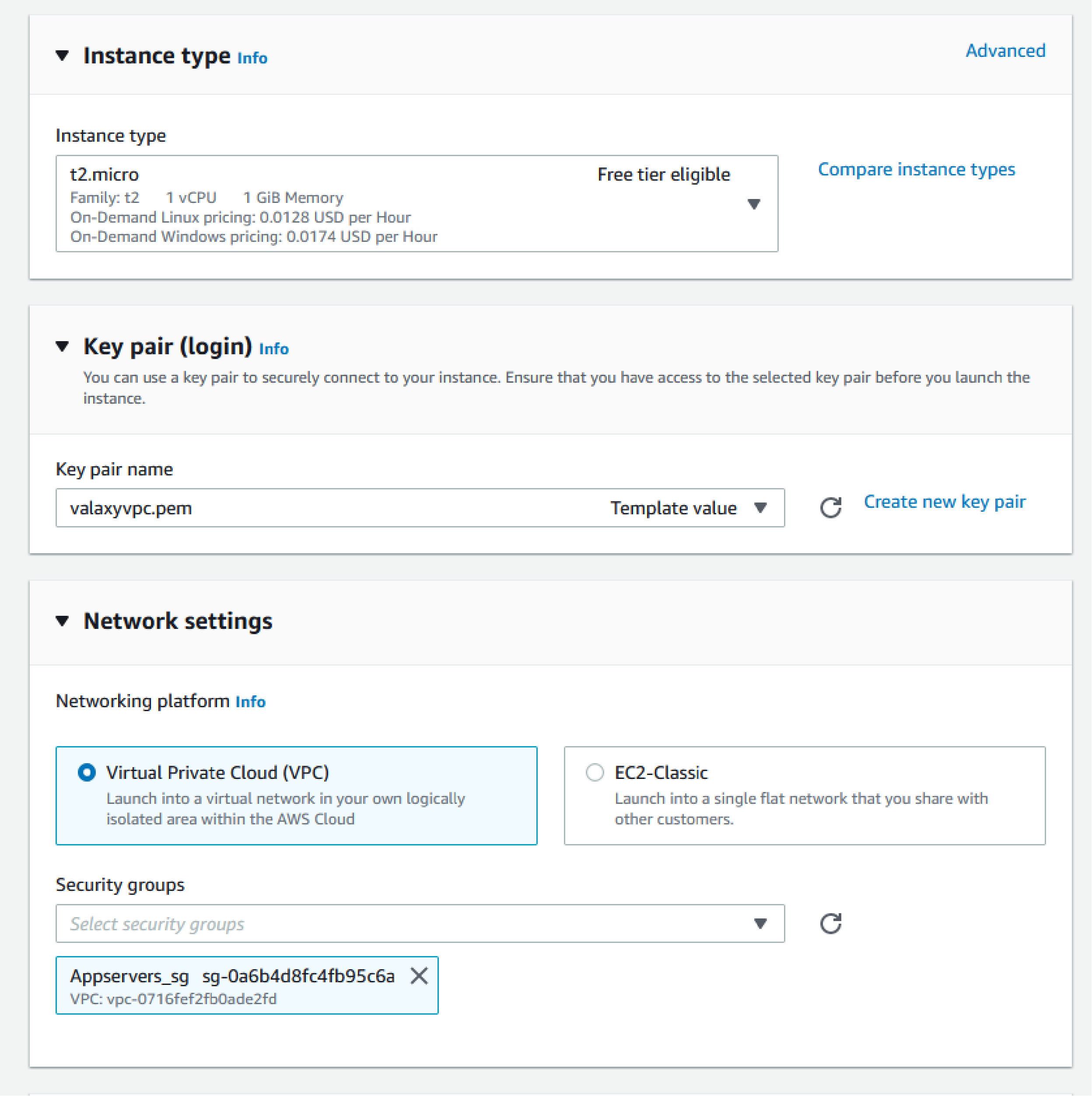
Specify the details of your launch template version below. Leaving a field blank will result in the field not being included in the launch template version.

▼ **Amazon machine image (AMI)** Info

AMI

GoldenAMI
ami-06e8ff2bd7908ca8d
2021-11-30T08:05:28.000Z architecture: 64-bit (x86) Virtualization: hvm
ENA enabled: true Root device type: ebs

Launch template security group,



▼ Instance type Info

Instance type

t2.micro — Free tier eligible ▼
Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0128 USD per Hour
On-Demand Windows pricing: 0.0174 USD per Hour

▼ 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

valaxyvpc.pem — Template value ▼

▼ Network settings

Networking platform Info

● Virtual Private Cloud (VPC)
Launch into a virtual network in your own logically isolated area within the AWS Cloud

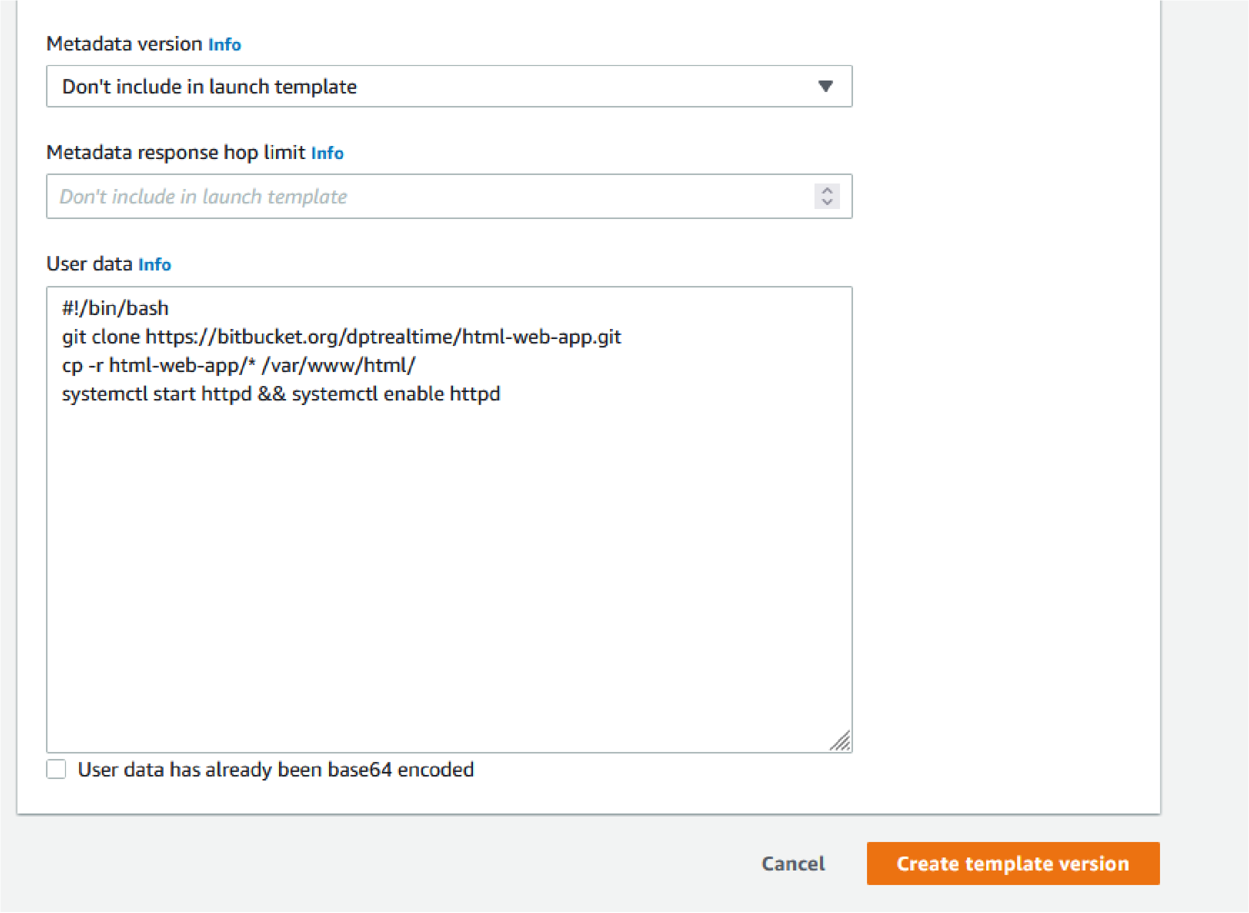
○ EC2-Classic
Launch into a single flat network that you share with other customers.

Security groups

Select security groups ▼

Appservers_sg sg-0a6b4d8fc4fb95c6a ✕
VPC: vpc-0716fef2fb0ade2fd

Userdata clones repo and starts apache



Metadata version Info

Don't include in launch template

Metadata response hop limit Info

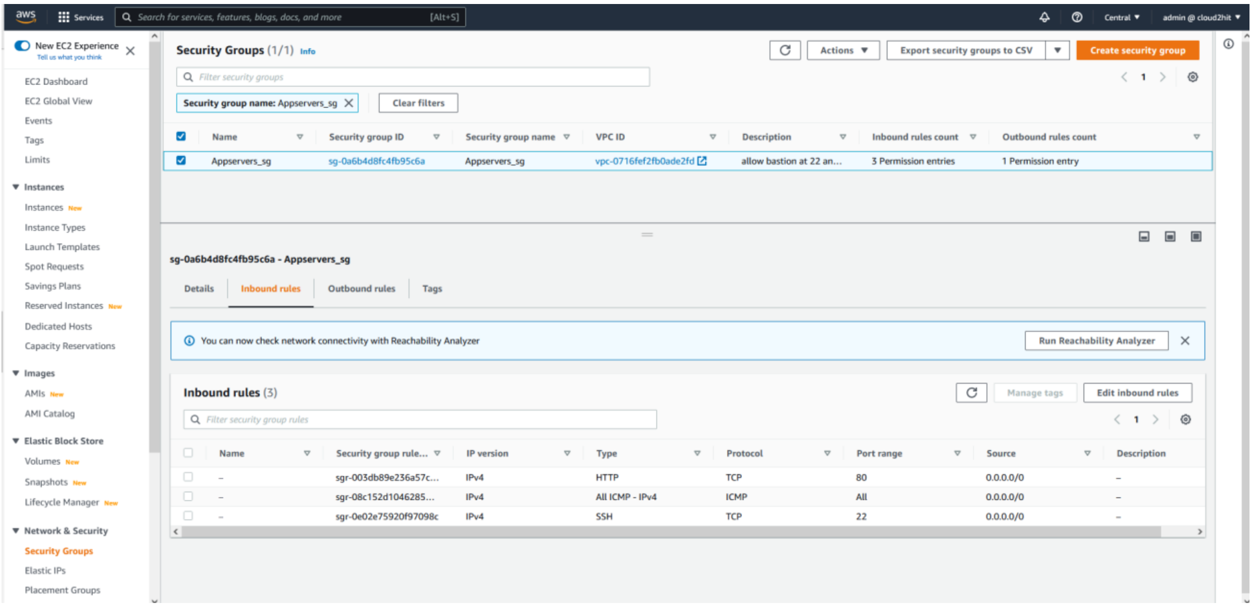
Don't include in launch template

User data Info

```
#!/bin/bash
git clone https://bitbucket.org/dptrealtime/html-web-app.git
cp -r html-web-app/* /var/www/html/
systemctl start httpd && systemctl enable httpd
```

□ User data has already been base64 encoded

This is the security group rules for launcg template for reference



Security Groups (1/1) Info

Security group name: Appservers_sg

☑	Name	Security group ID	Security group name	VPC ID	Description	Inbound rules count	Outbound rules count
☑	Appservers_sg	sg-0a6b4d8fc4fb95c6a	Appservers_sg	vpc-0716fef2fb0ade2fd	allow bastion at 22 an...	3 Permission entries	1 Permission entry

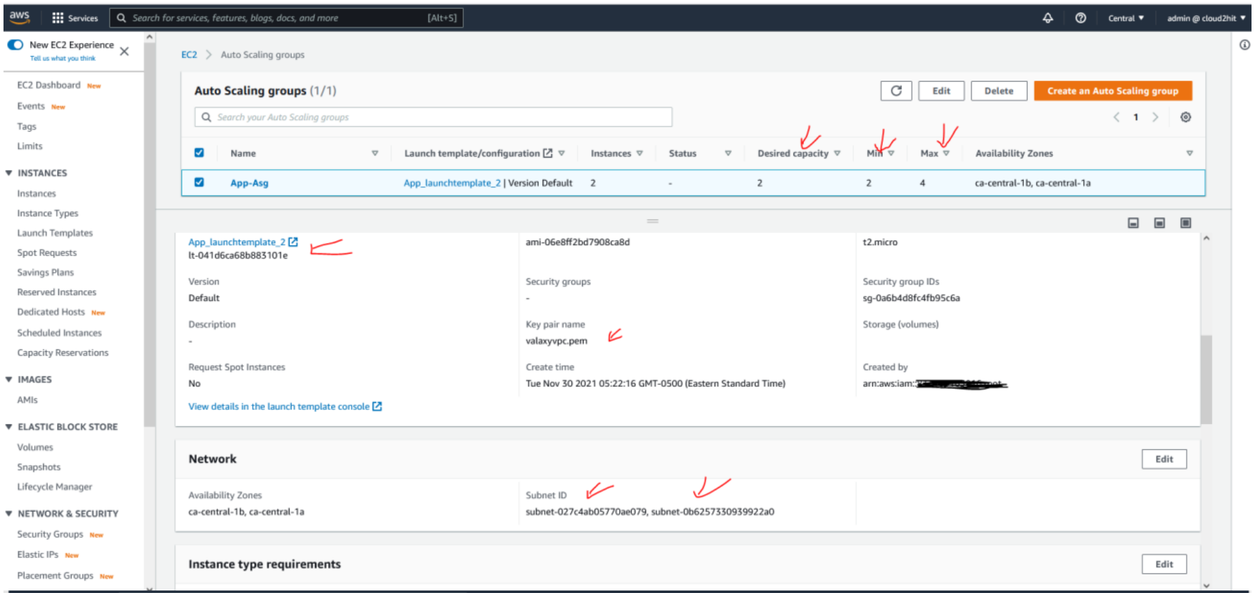
sg-0a6b4d8fc4fb95c6a - Appservers_sg

You can now check network connectivity with Reachability Analyzer

Inbound rules (3)

□	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-003db89e236a57c...	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-08c152d1046285...	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	–
□	–	sgr-0e02e75920f97098c	IPv4	SSH	TCP	22	0.0.0.0/0	–

12. Create Auto Scaling Group with Min: 2 Max: 4 with two Private Subnets associated to 1a and 1b zones.



Auto Scaling groups (1/1)

☑	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
☑	App-Asg	App_launchtemplate_2 | Version Default	2	-	2	2	4	ca-central-1b, ca-central-1a

App_launchtemplate_2
lt-041d6ca68b883101e

ami-06e8ff2bd7908ca8d

t2.micro

Version
Default

Security groups
-

Security group IDs
sg-0a6b4d8fc4fb95c6a

Description
-

Key pair name
valaxyvpc.pem

Storage (volumes)

Request Spot Instances
No

Create time
Tue Nov 30 2021 05:22:16 GMT-0500 (Eastern Standard Time)

Created by
arn:aws:iam:[redacted]

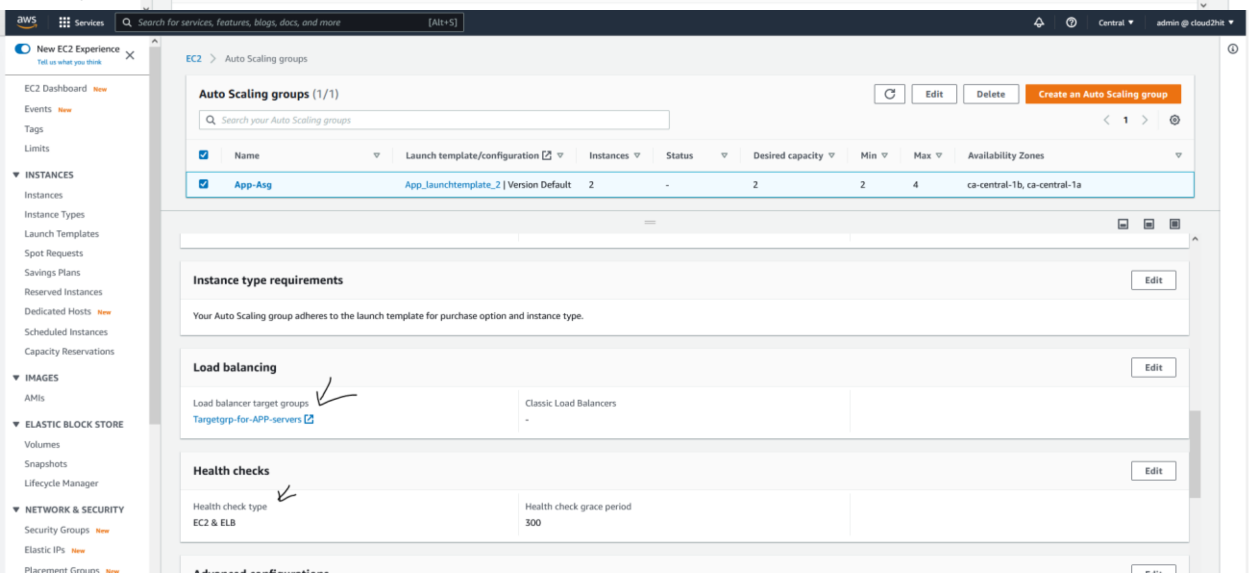
View details in the launch template console

Network

Availability Zones
ca-central-1b, ca-central-1a

Subnet ID
subnet-027c4ab05770ae079, subnet-0b6257330939922a0

Instance type requirements



Auto Scaling groups (1/1)

☑	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
☑	App-Asg	App_launchtemplate_2 | Version Default	2	-	2	2	4	ca-central-1b, ca-central-1a

Instance type requirements

Your Auto Scaling group adheres to the launch template for purchase option and instance type.

Load balancing

Load balancer target groups
Targetgrp-for-APP-servers

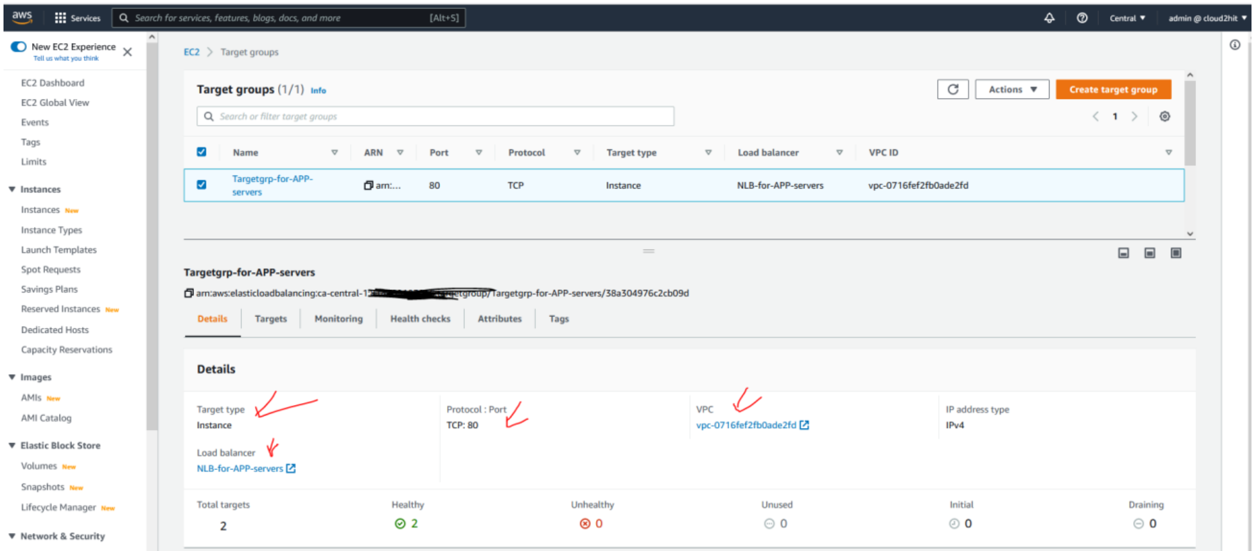
Classic Load Balancers
-

Health checks

Health check type
EC2 & ELB

Health check grace period
300

13. Create Target Group and associate it with ASG.



Target groups (1/1) Info

☑	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
☑	Targetgrp-for-APP-servers	arn:...	80	TCP	Instance	NLB-for-APP-servers	vpc-0716fef2fb0ade2fd

Targetgrp-for-APP-servers

arn:aws:elasticloadbalancing:ca-central-1[redacted]Targetgrp-for-APP-servers/38a304976c2cb09d

Details

Target type
Instance

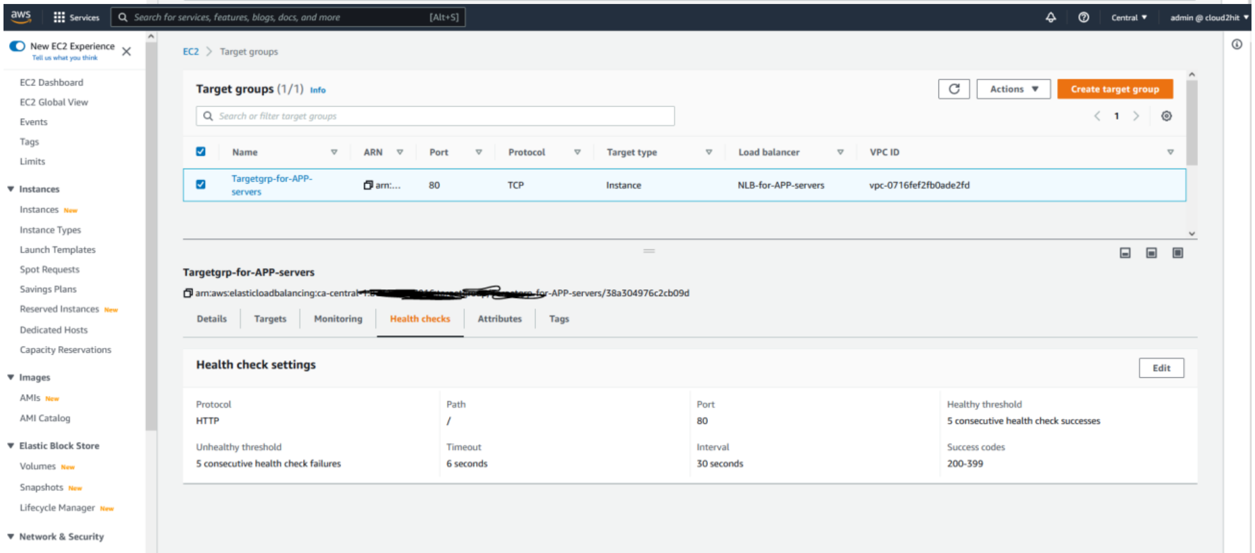
Protocol : Port
TCP: 80

VPC
vpc-0716fef2fb0ade2fd

IP address type
IPv4

Load balancer
NLB-for-APP-servers

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
2	2	0	0	0	0



Target groups (1/1) Info

☑	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
☑	Targetgrp-for-APP-servers	arn:...	80	TCP	Instance	NLB-for-APP-servers	vpc-0716fef2fb0ade2fd

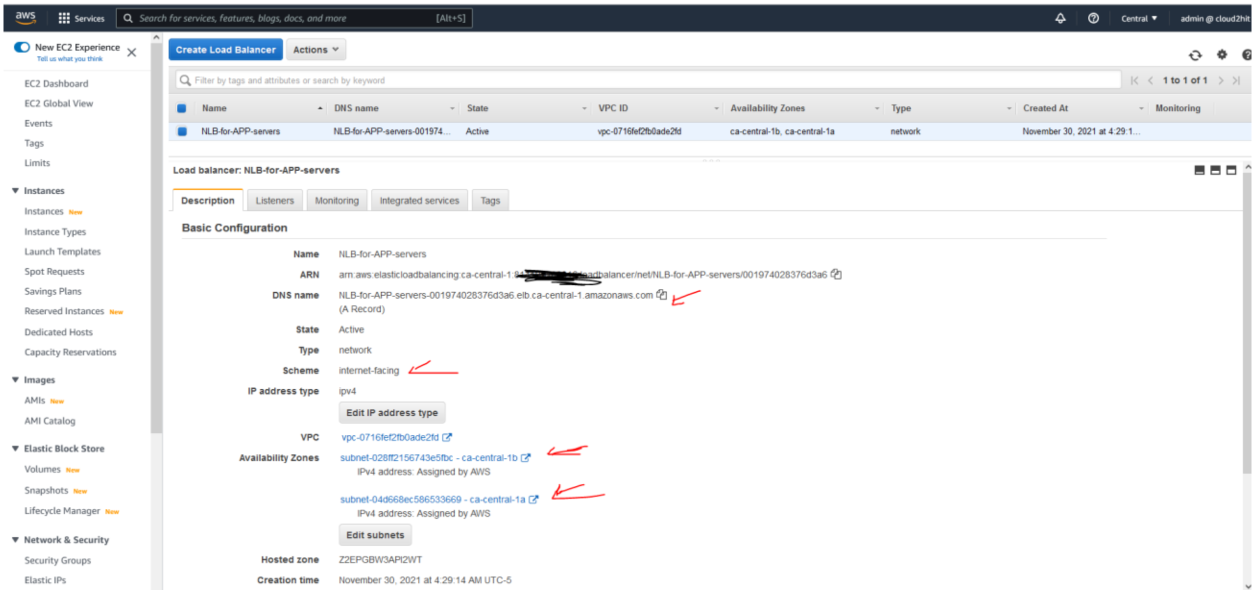
Targetgrp-for-APP-servers

arn:aws:elasticloadbalancing:ca-central[redacted]r-APP-servers/38a304976c2cb09d

Health check settings

Protocol	Path	Port	Healthy threshold
HTTP	/	80	5 consecutive health check successes
Unhealthy threshold	**Timeout**	**Interval**	**Success codes**
5 consecutive health check failures	6 seconds	30 seconds	200-399

14. Create Network Load balancer in Public Subnet and add Target Group as target.

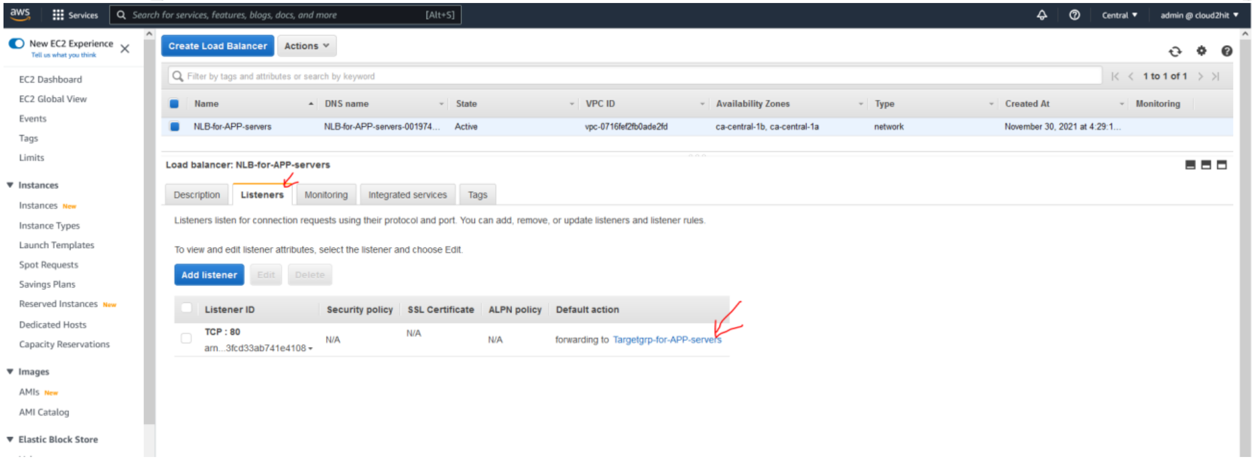


■	Name	DNS name	State	VPC ID	Availability Zones	Type	Created At	Monitoring
■	NLB-for-APP-servers	NLB-for-APP-servers-001974...	Active	vpc-0716fef2fb0ade2fd	ca-central-1b, ca-central-1a	network	November 30, 2021 at 4:29:1...	

Load balancer: NLB-for-APP-servers

Basic Configuration

Name	NLB-for-APP-servers
ARN	arn:aws:elasticloadbalancing:ca-central-1:[redacted]adbalancer/net/NLB-for-APP-servers/001974028376d3a6
DNS name	NLB-for-APP-servers-001974028376d3a6.elb.ca-central-1.amazonaws.com (A Record)
State	Active
Type	network
Scheme	internet-facing
IP address type	ipv4
VPC	vpc-0716fef2fb0ade2fd
Availability Zones	subnet-028ff2156743e5fbc - ca-central-1b IPv4 address: Assigned by AWS subnet-04d668ec586533669 - ca-central-1a IPv4 address: Assigned by AWS
Hosted zone	Z2EPGBW3API2WT
Creation time	November 30, 2021 at 4:29:14 AM UTC-5



■	Name	DNS name	State	VPC ID	Availability Zones	Type	Created At	Monitoring
■	NLB-for-APP-servers	NLB-for-APP-servers-001974...	Active	vpc-0716fef2fb0ade2fd	ca-central-1b, ca-central-1a	network	November 30, 2021 at 4:29:1...	

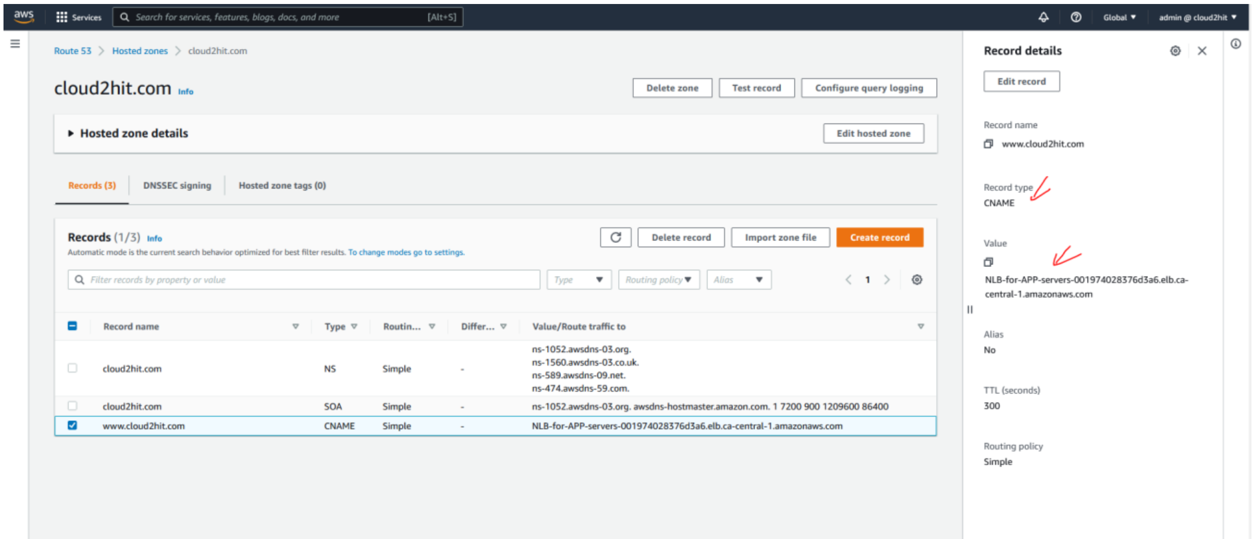
Load balancer: NLB-for-APP-servers

Listeners listen for connection requests using their protocol and port. You can add, remove, or update listeners and listener rules.

To view and edit listener attributes, select the listener and choose Edit.

□	Listener ID	Security policy	SSL Certificate	ALPN policy	Default action
□	TCP : 80 arn...3fcd33ab741e4108	N/A	N/A	N/A	forwarding to Targetgrp-for-APP-servers

15. Update route53 hosted zone with CNAME record routing the traffic to NLB.



cloud2hit.com

Records (1/3)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

■	Record name	Type	Routin...	Differ...	Value/Route traffic to
□	cloud2hit.com	NS	Simple	-	ns-1052.awsdns-03.org. ns-1560.awsdns-03.co.uk. ns-589.awsdns-09.net. ns-474.awsdns-59.com.
□	cloud2hit.com	SOA	Simple	-	ns-1052.awsdns-03.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
☑	www.cloud2hit.com	CNAME	Simple	-	NLB-for-APP-servers-001974028376d3a6.elb.ca-central-1.amazonaws.com

Record details

Record name
www.cloud2hit.com

Record type
CNAME

Value
NLB-for-APP-servers-001974028376d3a6.elb.ca-central-1.amazonaws.com

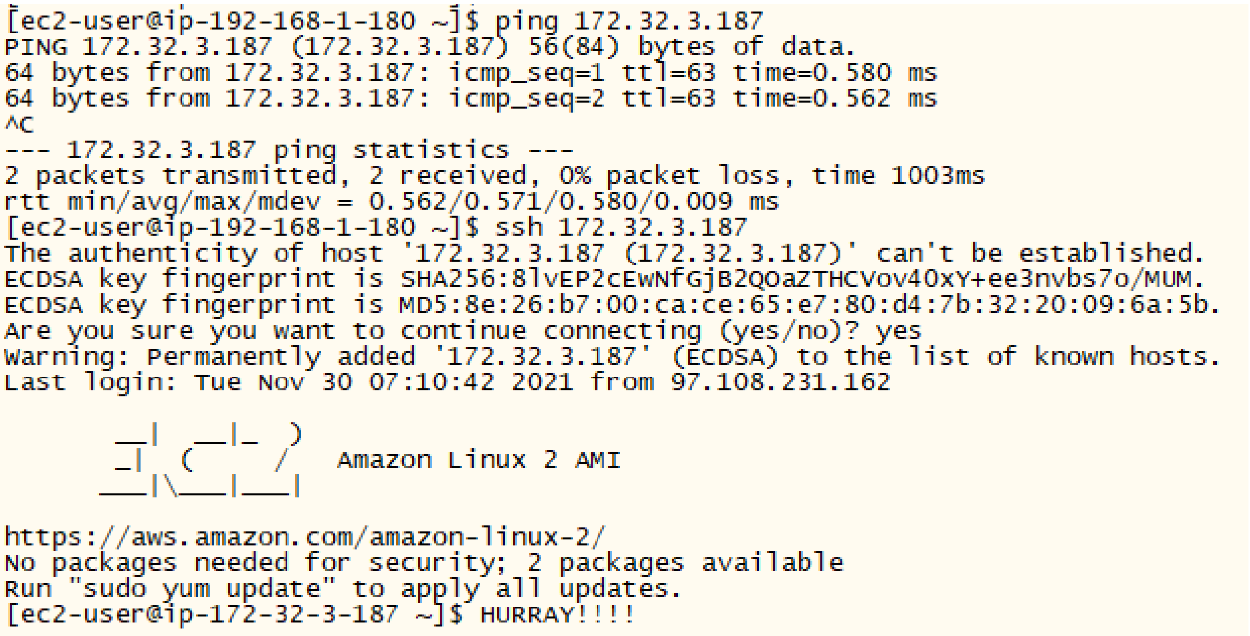
Alias
No

TTL (seconds)
300

Routing policy
Simple

Validation

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

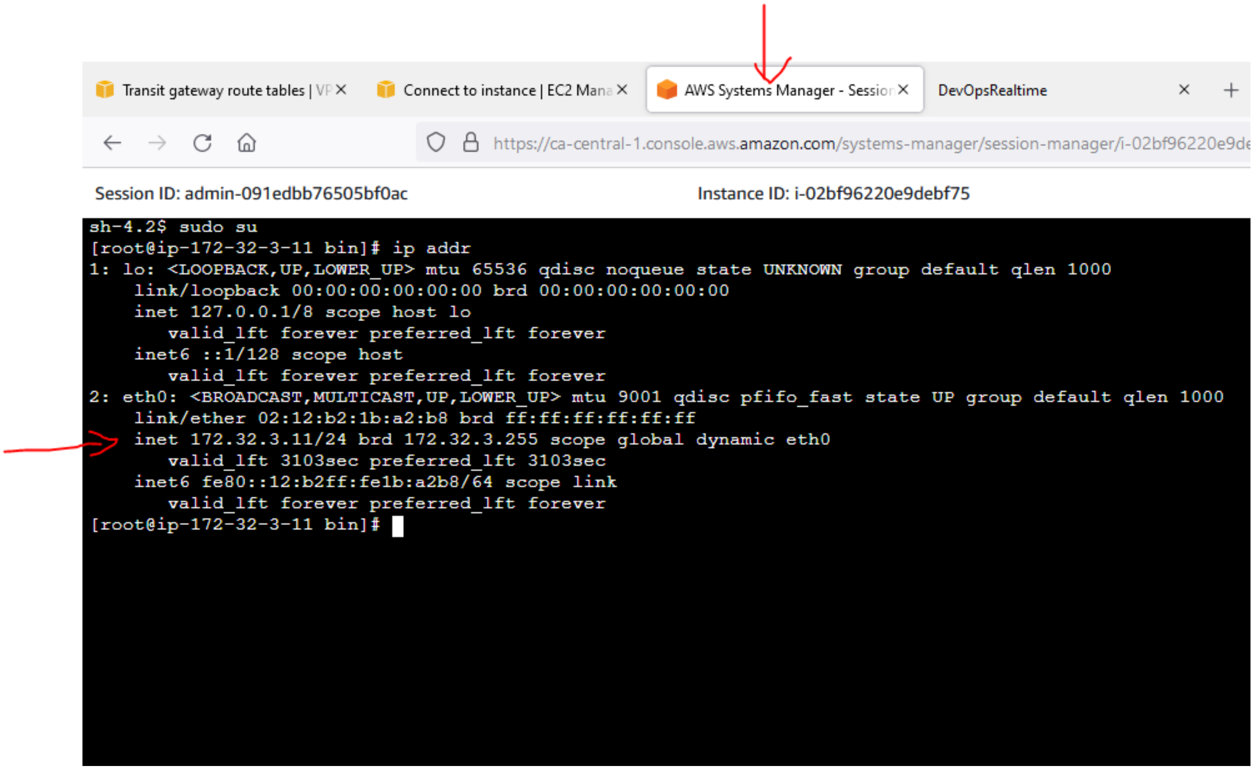


```
[ec2-user@ip-192-168-1-180 ~]$ ping 172.32.3.187
PING 172.32.3.187 (172.32.3.187) 56(84) bytes of data.
64 bytes from 172.32.3.187: icmp_seq=1 ttl=63 time=0.580 ms
64 bytes from 172.32.3.187: icmp_seq=2 ttl=63 time=0.562 ms
^C
--- 172.32.3.187 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.562/0.571/0.580/0.009 ms
[ec2-user@ip-192-168-1-180 ~]$ ssh 172.32.3.187
The authenticity of host '172.32.3.187 (172.32.3.187)' can't be established.
ECDSA key fingerprint is SHA256:8lvEP2cEwNfGjB2QOaZTHCVov40xY+ee3nvbs7o/MUM.
ECDSA key fingerprint is MD5:8e:26:b7:00:ca:ce:65:e7:80:d4:7b:32:20:09:6a:5b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.32.3.187' (ECDSA) to the list of known hosts.
Last login: Tue Nov 30 07:10:42 2021 from 97.108.231.162

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
No packages needed for security; 2 packages available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-32-3-187 ~]$ HURRAY!!!!
```

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



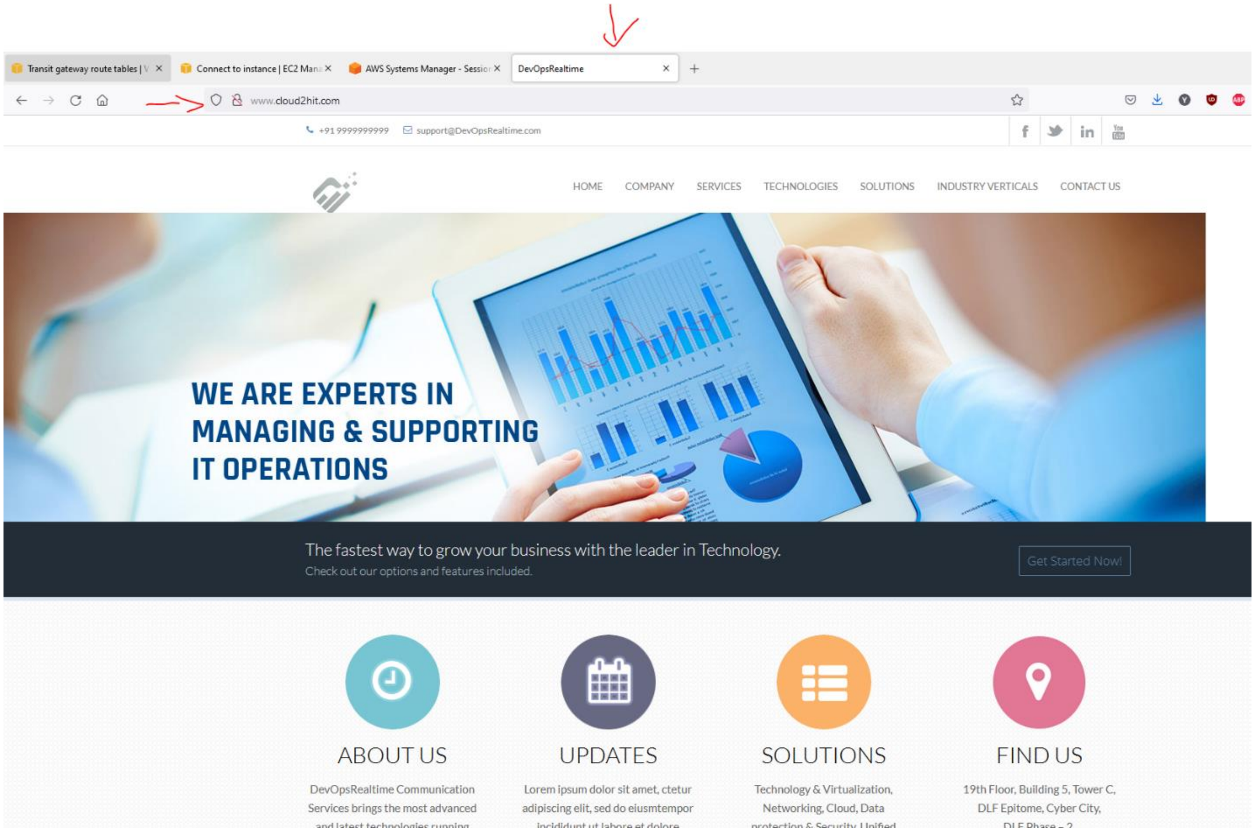
Transit gateway route tables | VP
Connect to instance | EC2 Mana
AWS Systems Manager - Session
DevOpsRealtime
https://ca-central-1.console.aws.amazon.com/systems-manager/session-manager/i-02bf96220e9de

Session ID: admin-091edbb76505bf0ac

Instance ID: i-02bf96220e9debf75

```
sh-4.2$ sudo su
[root@ip-172-32-3-11 bin]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:12:b2:1b:a2:b8 brd ff:ff:ff:ff:ff:ff
    inet 172.32.3.11/24 brd 172.32.3.255 scope global dynamic eth0
       valid_lft 3103sec preferred_lft 3103sec
    inet6 fe80::12:b2ff:fe1b:a2b8/64 scope link
       valid_lft forever preferred_lft forever
[root@ip-172-32-3-11 bin]#
```

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



WE ARE EXPERTS IN
MANAGING & SUPPORTING
IT OPERATIONS

The fastest way to grow your business with the leader in Technology.
Check out our options and features included.

ABOUT US

DevOpsRealtime Communication Services brings the most advanced and latest technologies running

UPDATES

Lorem ipsum dolor sit amet, ctetur adipiscing elit, sed do eiusmtempor incididunt ut labore et dolore

SOLUTIONS

Technology & Virtualization, Networking, Cloud, Data protection & Security, Unified

FIND US

19th Floor, Building 5, Tower C,
DLF Epitome, Cyber City,
DLF Phase – 2