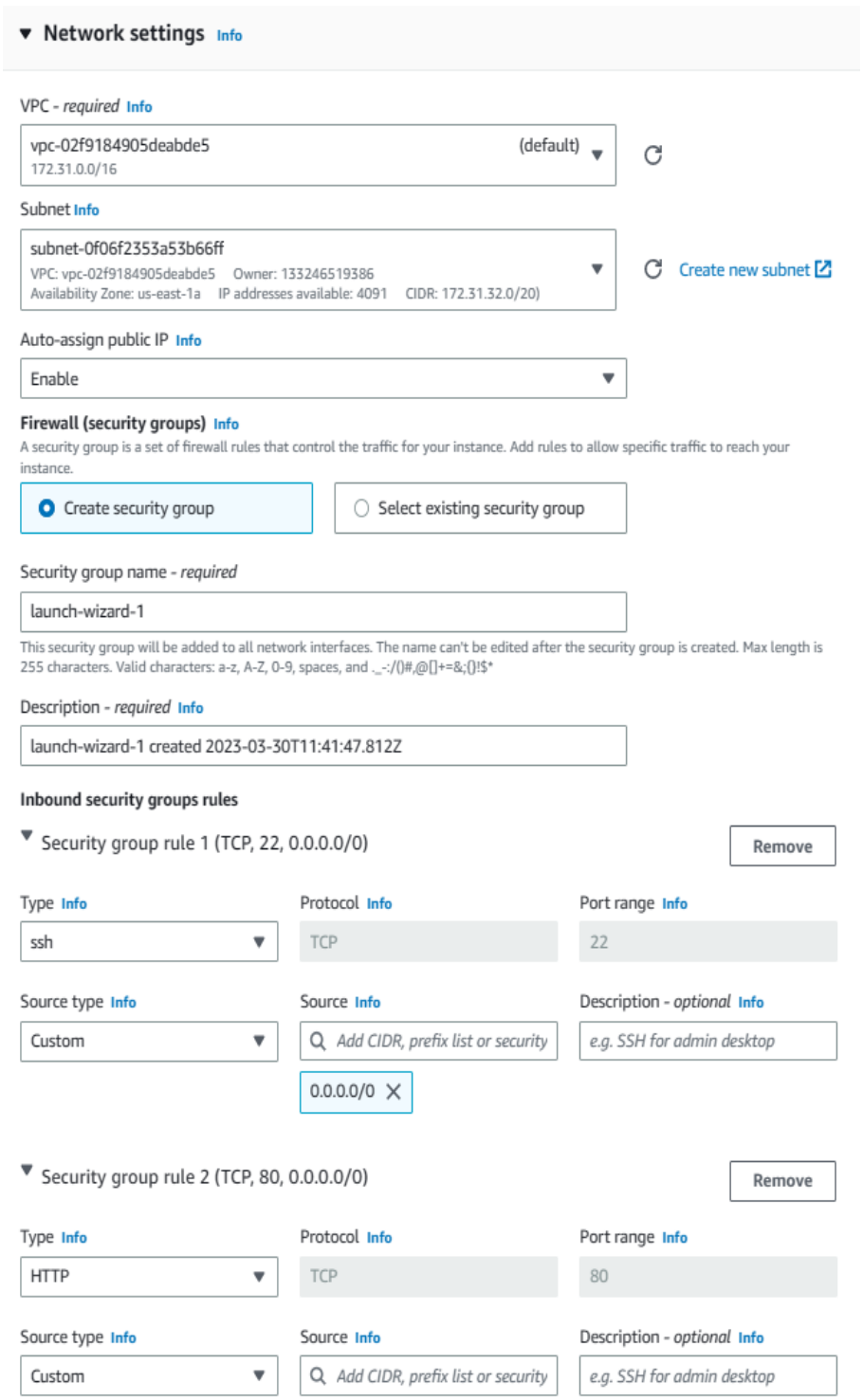
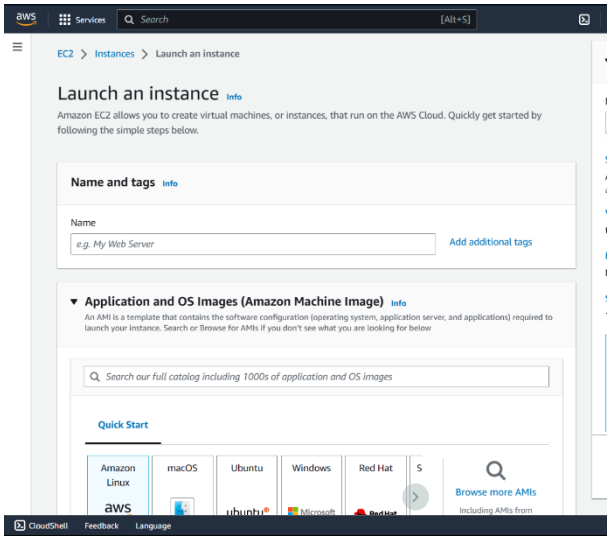
# Configure and connect a MySQL Database Instance with a Web Server

**Step1:** Launching an Amazon EC2 instance (VM) which will mimic the web server.

**Specifications:**

Amazon Linux 2 AMI (HVM)- Kernal 5.10, SSD Type




Network Settings:

Auto-Assign-IP is **enabled**

Subnet: us-east-1a

Inbound Rules:

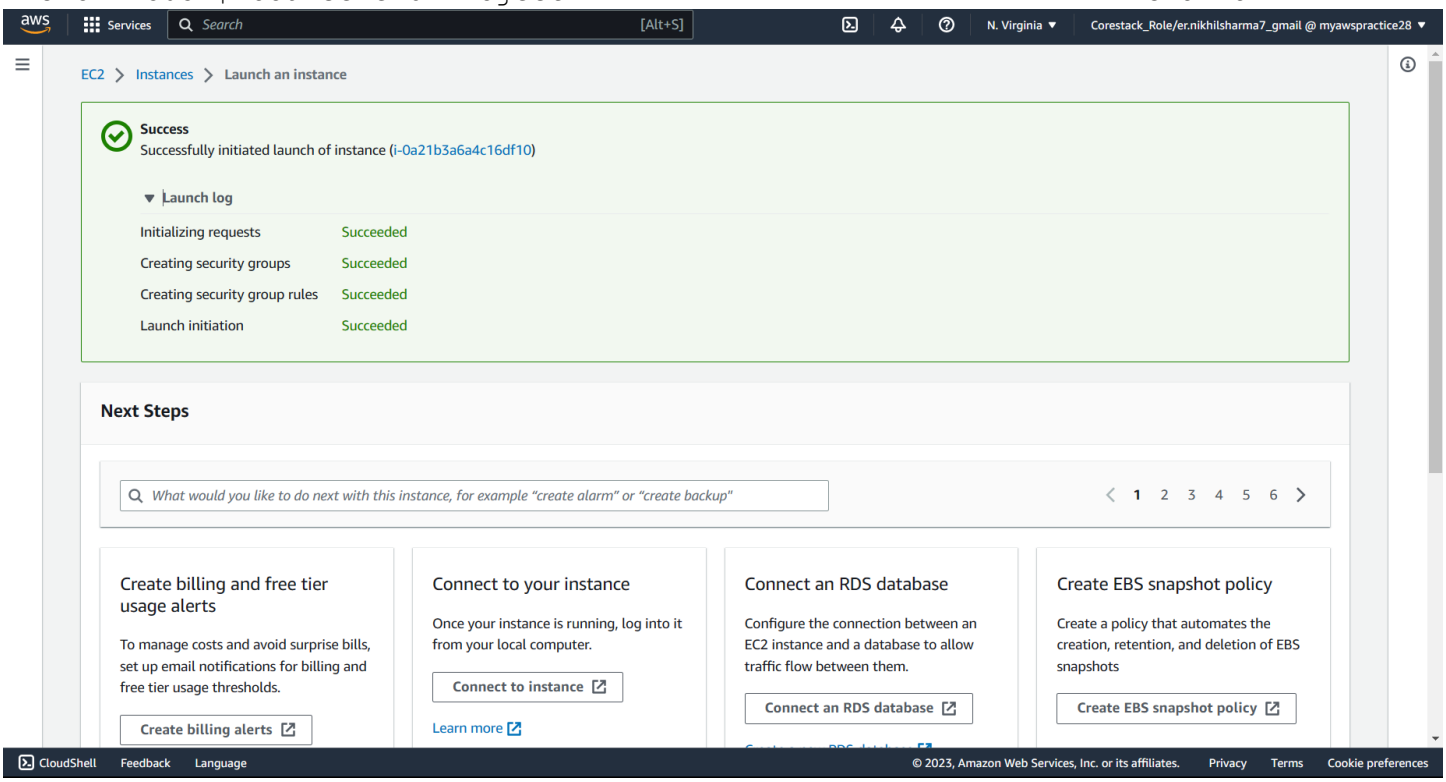
SSH

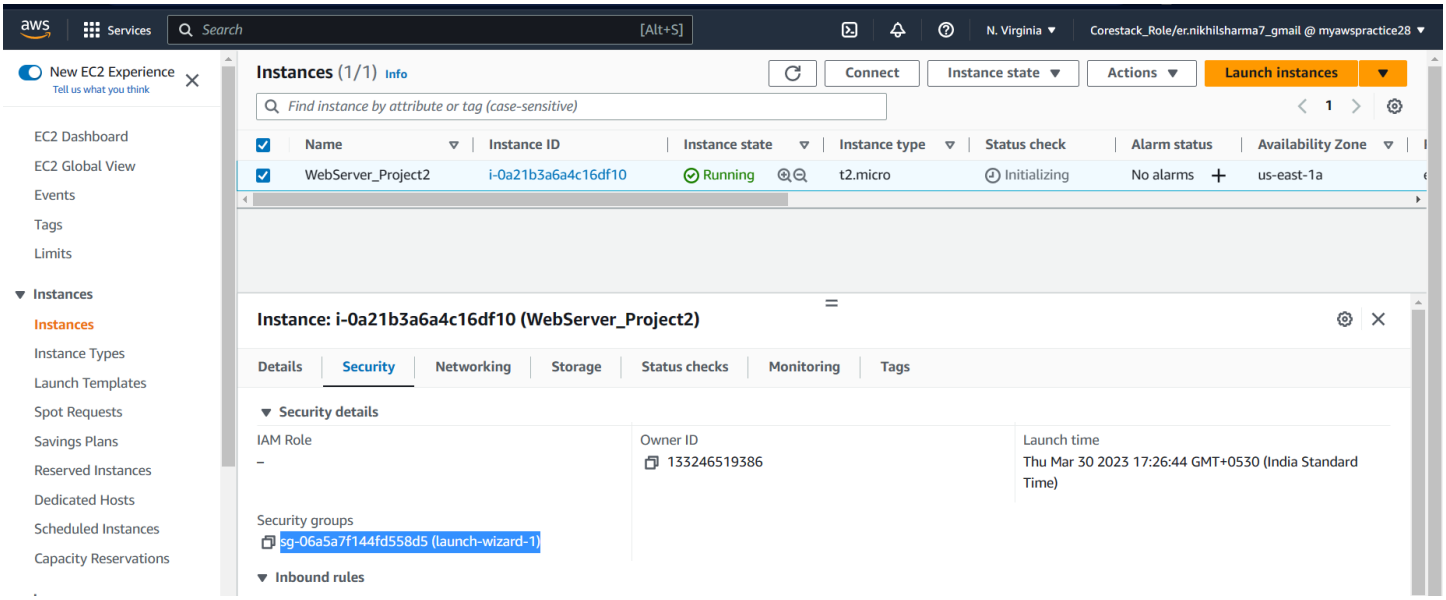
HTTP

HTTPS

Storage type:

EBS volume:8gib gp2




After the successful launch of VM. Note down its Security Group:

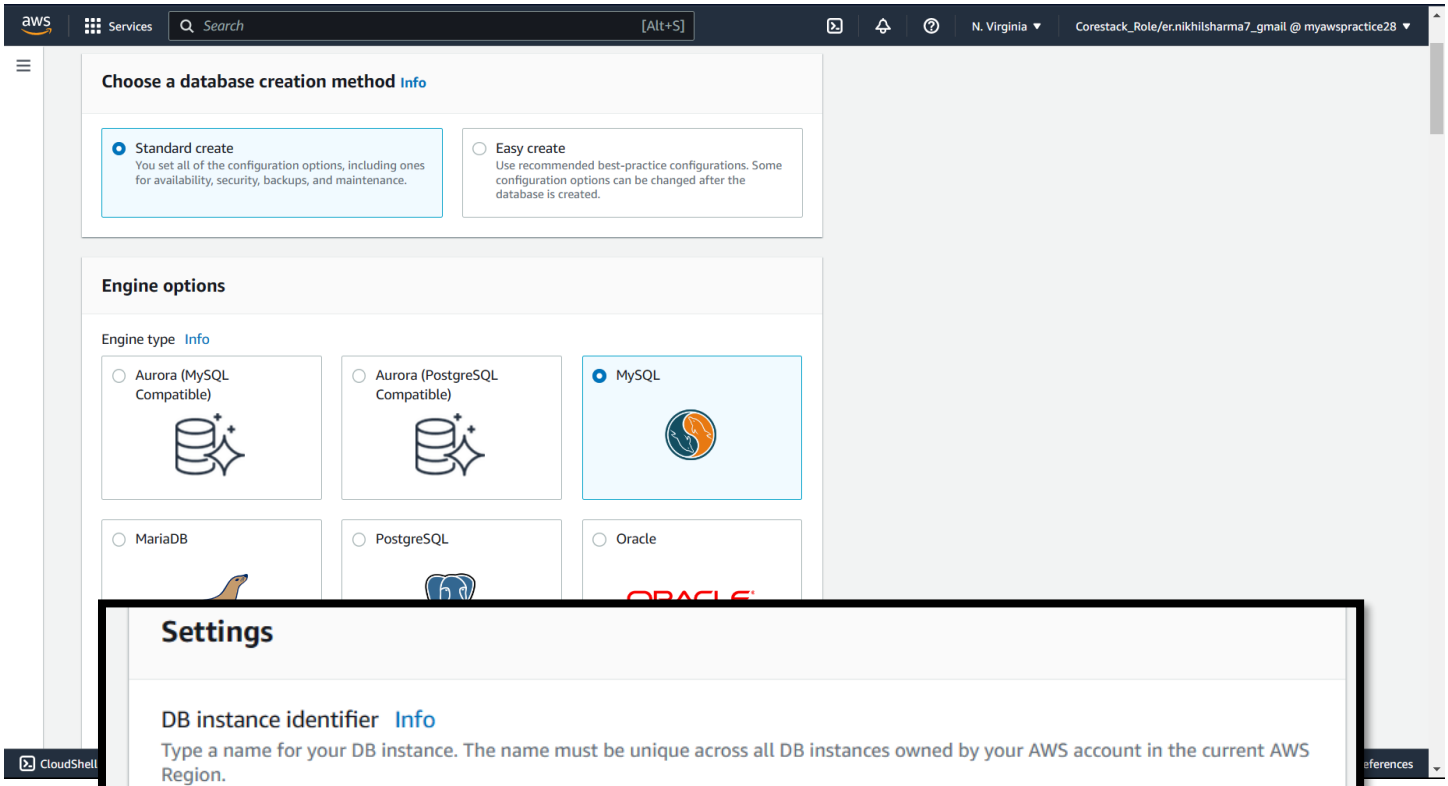
sg-06a5a7f144fd558d5 (launch-wizard-1)

**Step2:**

Launching the RDS, MySQL server instance with t2.micro instance type.

Selected Free-tier.

And MySQL version 8.0.28




## Settings

DB instance identifier Info

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

MySQLDBForWebServer

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

### Credentials Settings

Master username Info

Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. First character must be a letter.

☐ Manage master credentials in AWS Secrets Manager

Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
Learn more

☐ Auto generate a password

Amazon RDS can generate a password for you, or you can specify your own password.

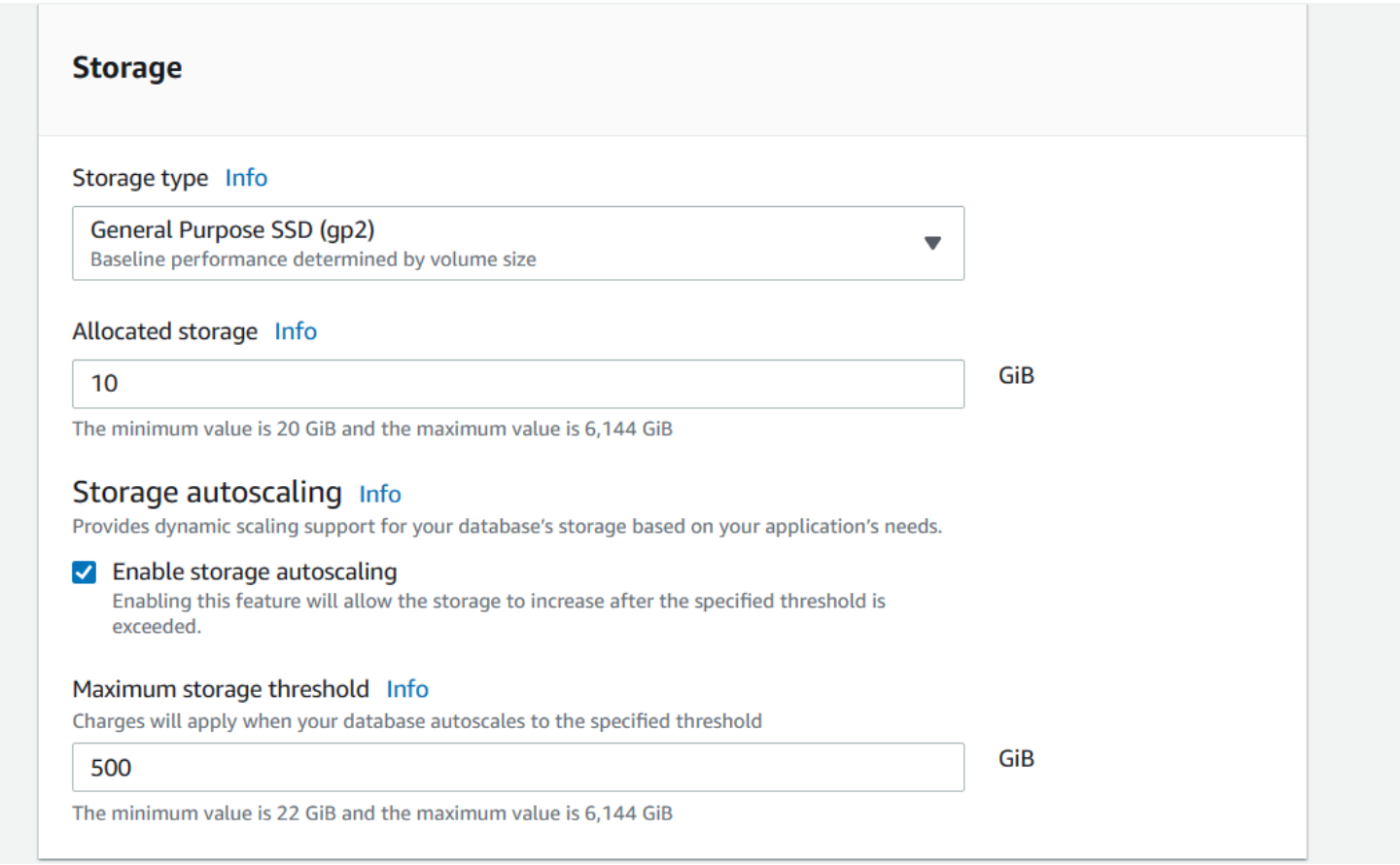
Master password Info

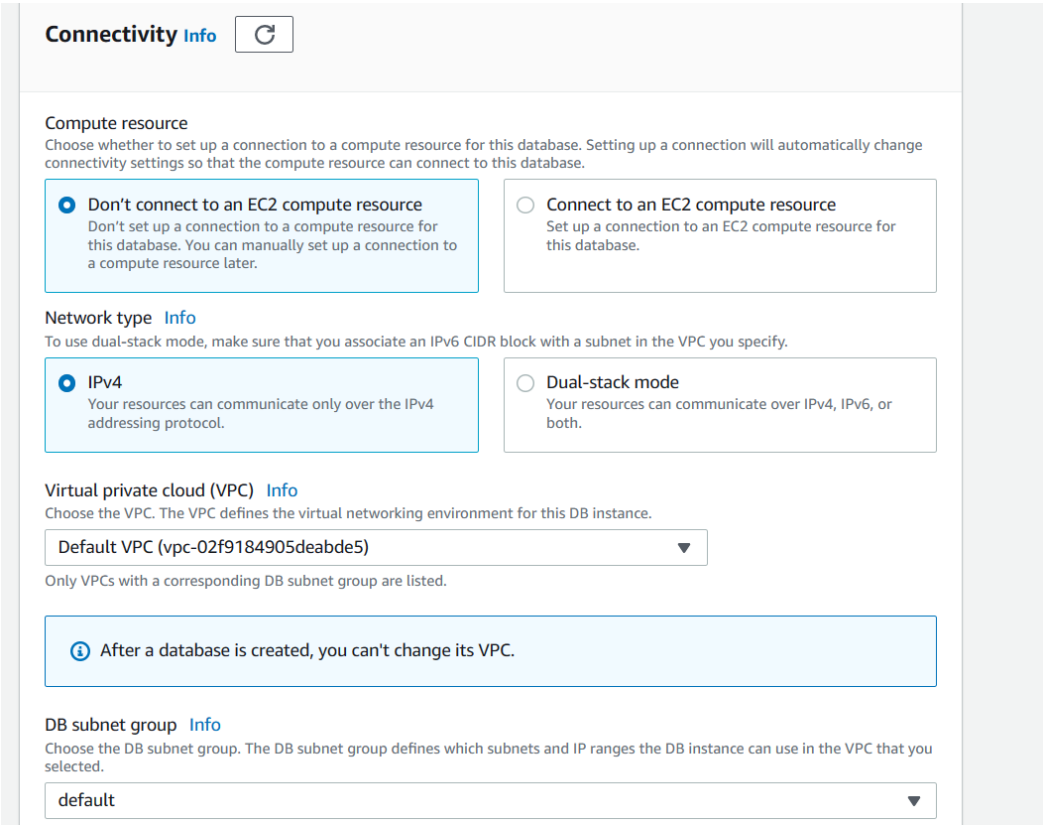
••••••••

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

Confirm master password Info

Instance Configuration: t2.micro



Public access Info

- Yes
  RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
- No
  RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) Info

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

- Choose existing
  Choose existing VPC security groups
- Create new
  Create new VPC security group

Existing VPC security groups

*Choose one or more options*

launch-wizard-1 ×

Availability Zone Info

us-east-1a

RDS Proxy

RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

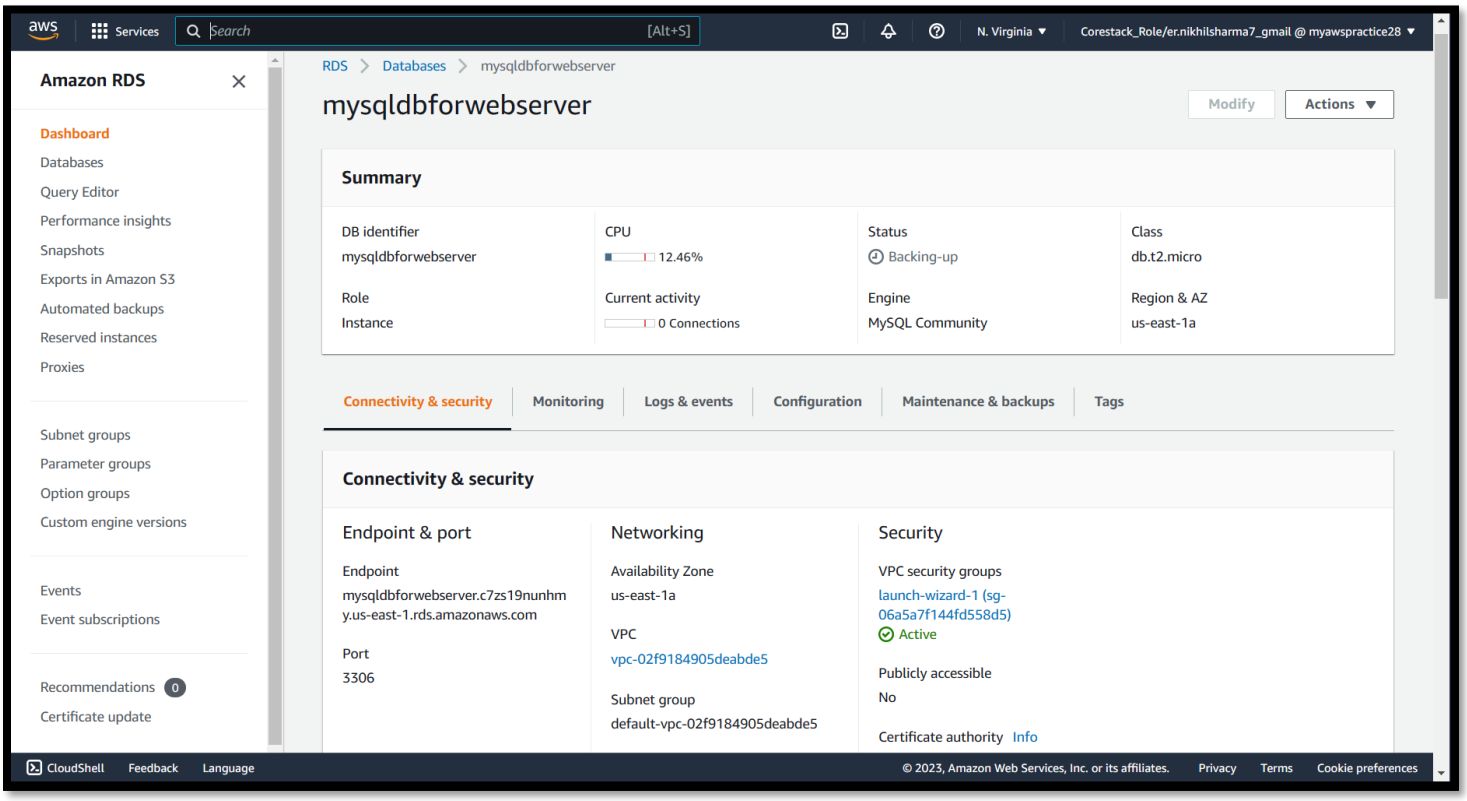
- Create an RDS Proxy Info
  RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see Amazon RDS Proxy pricing.

Certificate authority - *optional* Info

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-2019 (default)

If you don't select a certificate authority, RDS chooses one for you.

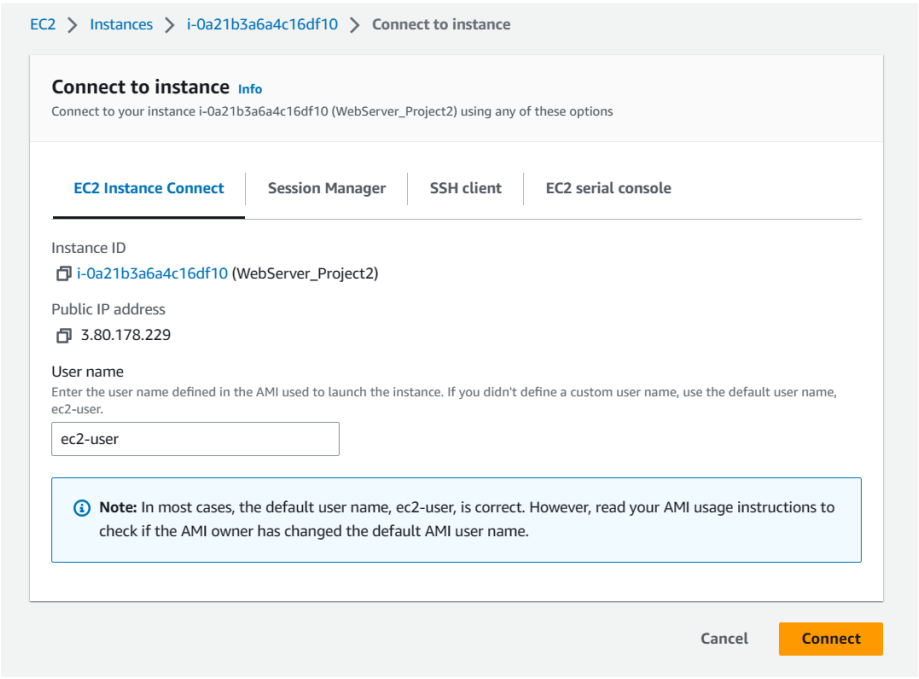



Endpoint: It is required to connect the VM with the Database instance.

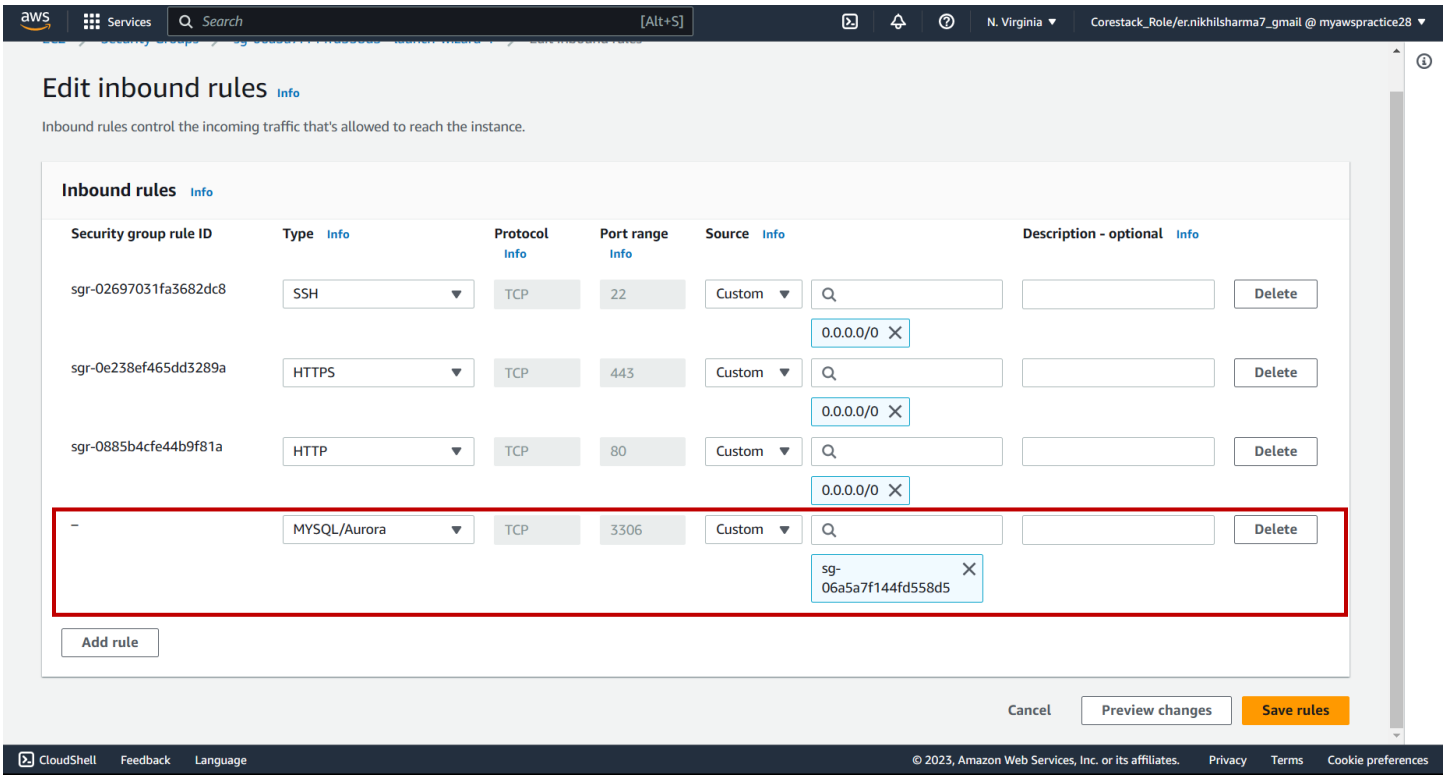
```
mysqldbforwebserver.c7zs19nunhmy.us-east-1.rds.amazonaws.com
```

**STEP-3:**

Instance connect:



**Editing the inbound rule of the RDS.**

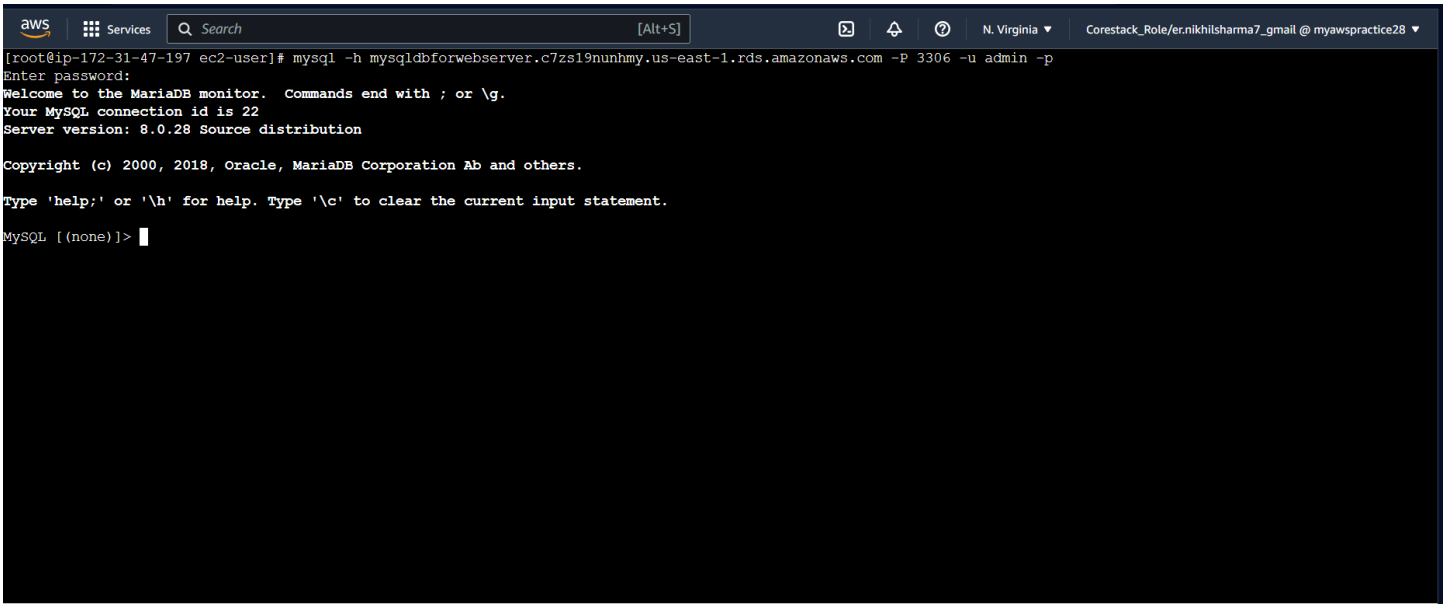



After connecting to the instance, installing the MySQL on it.

```
sudo su
yum install mysql
```

When MySQL client is installed on the VM, we can easily connect the RDS and VM using the following command.

```
mysql -h mysqldbforwebserver.c7zs19nunhmy.us-east-1.rds.amazonaws.com -P 3306 -u admin -p
```



## Requirements/Deliverables

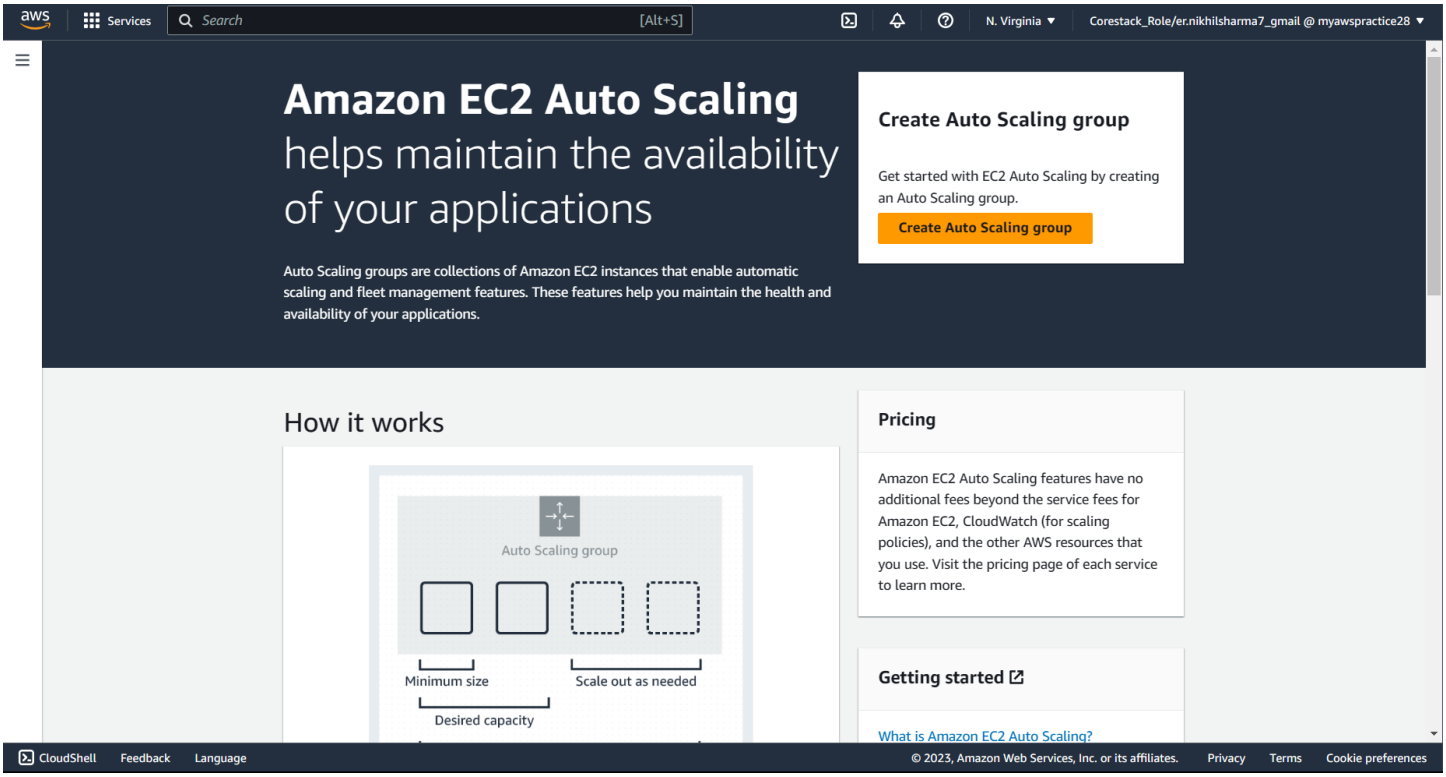
**You must use the following:**
Create a Database Instance with the following specifications:
Database creation method: Standard Create
Engine: MySQL
Database Instance size: db.t2.micro

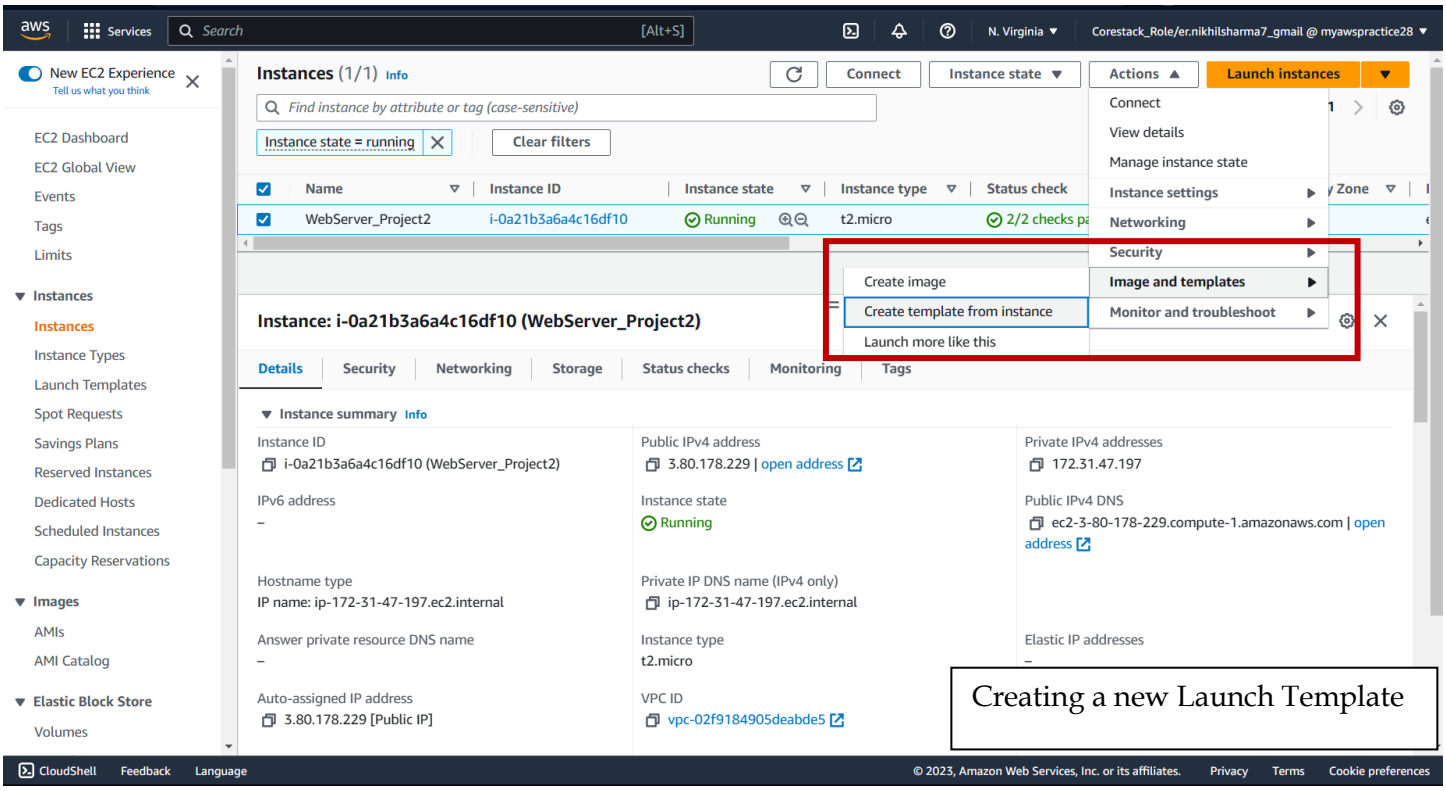
**Create an EC2 Instance with the following specifications:**
AMI: Amazon Linux
Region: Use only US East (N Virginia), us-east-1, and us-east-2
Instance types: t2.micro and t3.micro
Allowed EBS types: GP2 and Standard

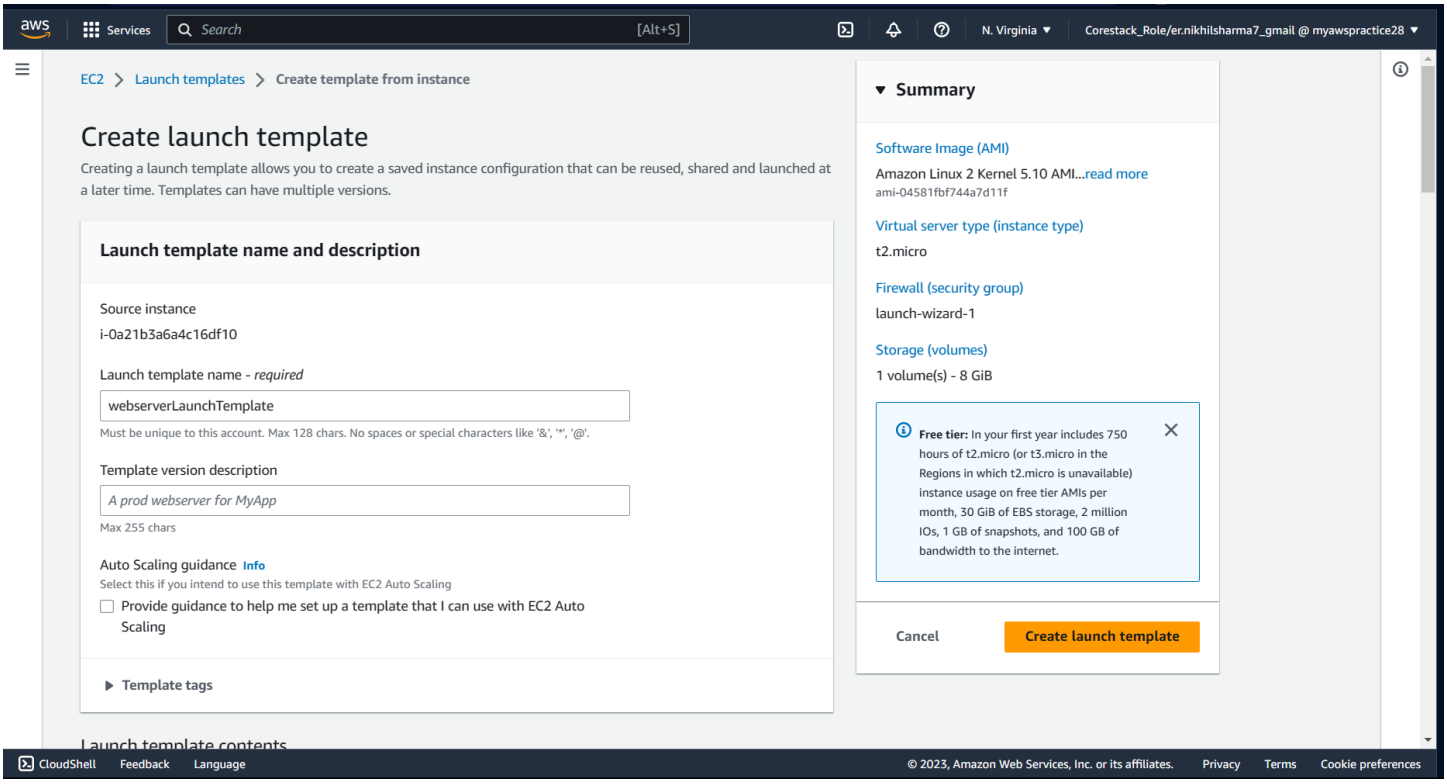
- Make sure that the Availability Zone is similar throughout the instances and volumes
- Ensure that the server scales automatically and the traffic is optimally routed among the scaled servers

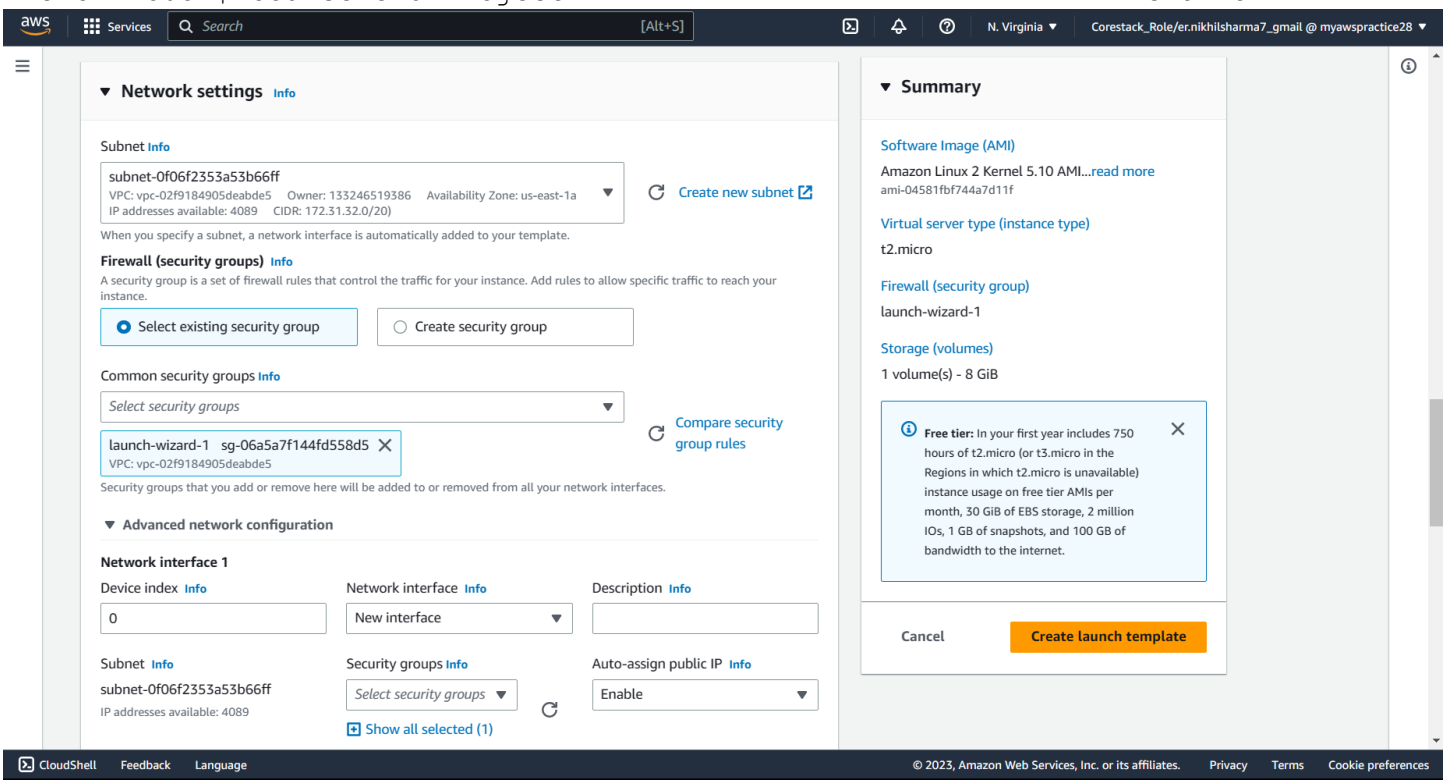
Adding the High-Availability to the webserver by leveraging the Auto Scaling Group (ASG) feature and handling-traffic using the Load Balancer.

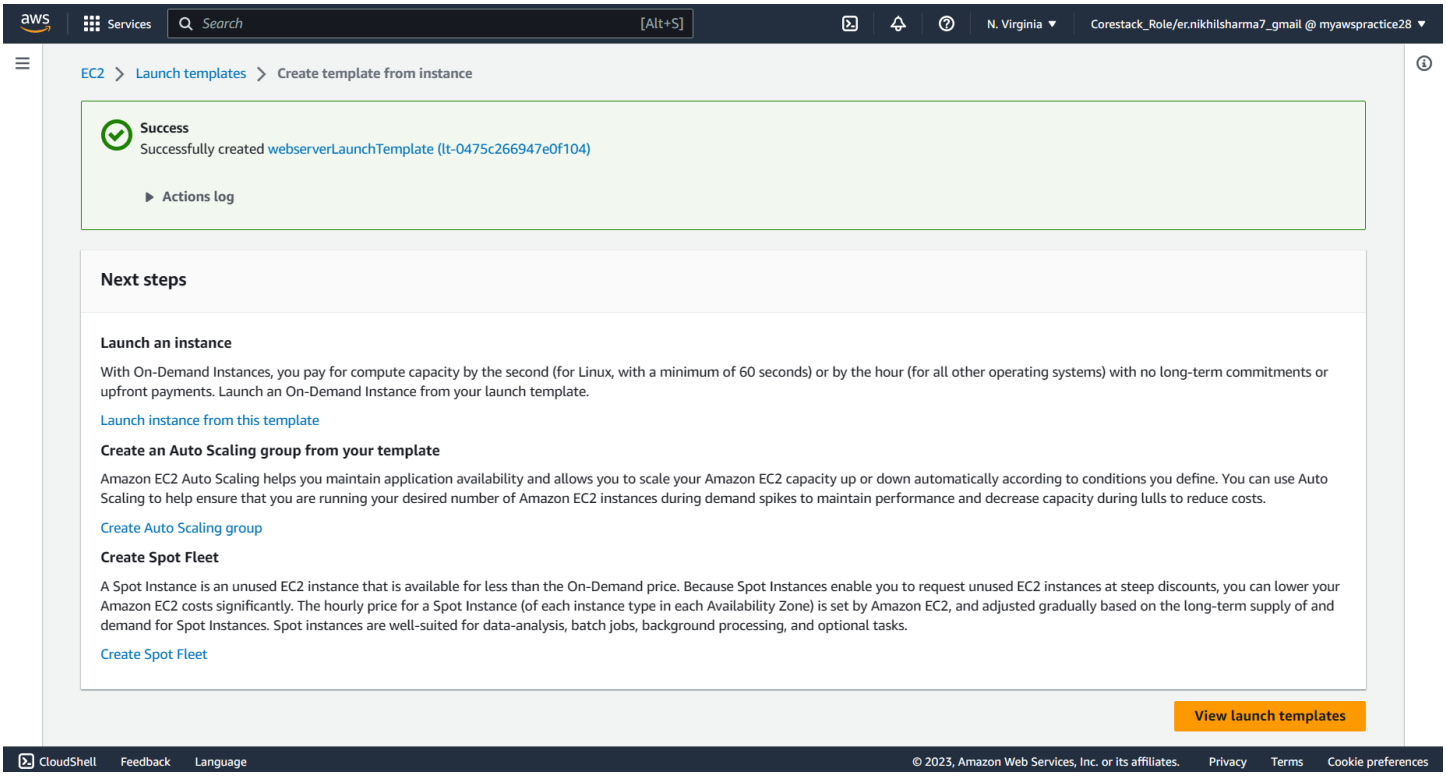
# ASG and Application Load Balancer



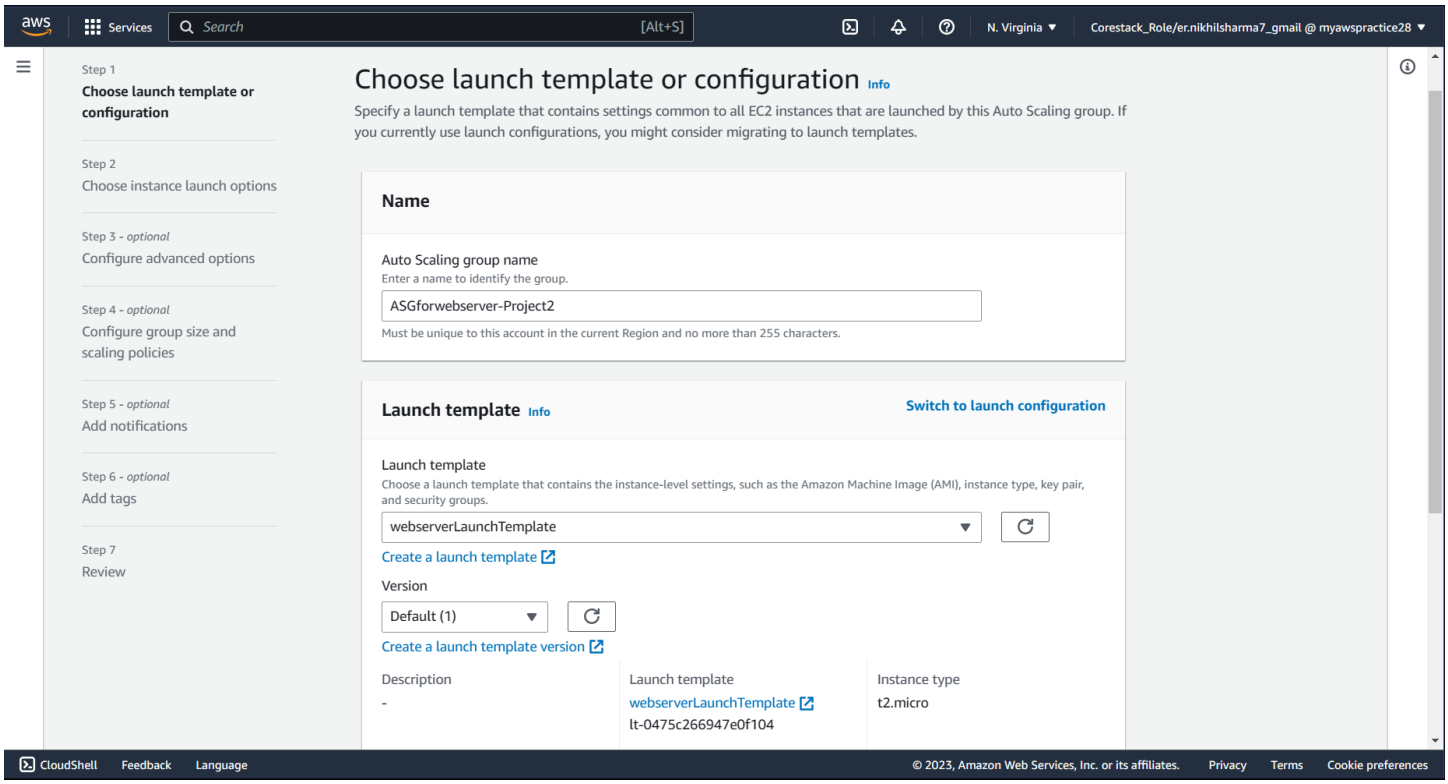

Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Connect
View details
Manage instance state
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Create image
Create template from instance
Launch more like this
WebServer_Project2
i-0a21b3a6a4c16df10
Running
t2.micro
Instance: i-0a21b3a6a4c16df10 (WebServer_Project2)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance summary Info
Instance ID
i-0a21b3a6a4c16df10 (WebServer_Project2)
Public IPv4 address
3.80.178.229 | open address
Private IPv4 addresses
172.31.47.197
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-3-80-178-229.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-172-31-47-197.ec2.internal
Private IP DNS name (IPv4 only)
ip-172-31-47-197.ec2.internal
Answer private resource DNS name
–
Instance type
t2.micro
Elastic IP addresses
–
Auto-assigned IP address
3.80.178.229 [Public IP]
VPC ID
vpc-02f9184905deabde5
Creating a new Launch Template

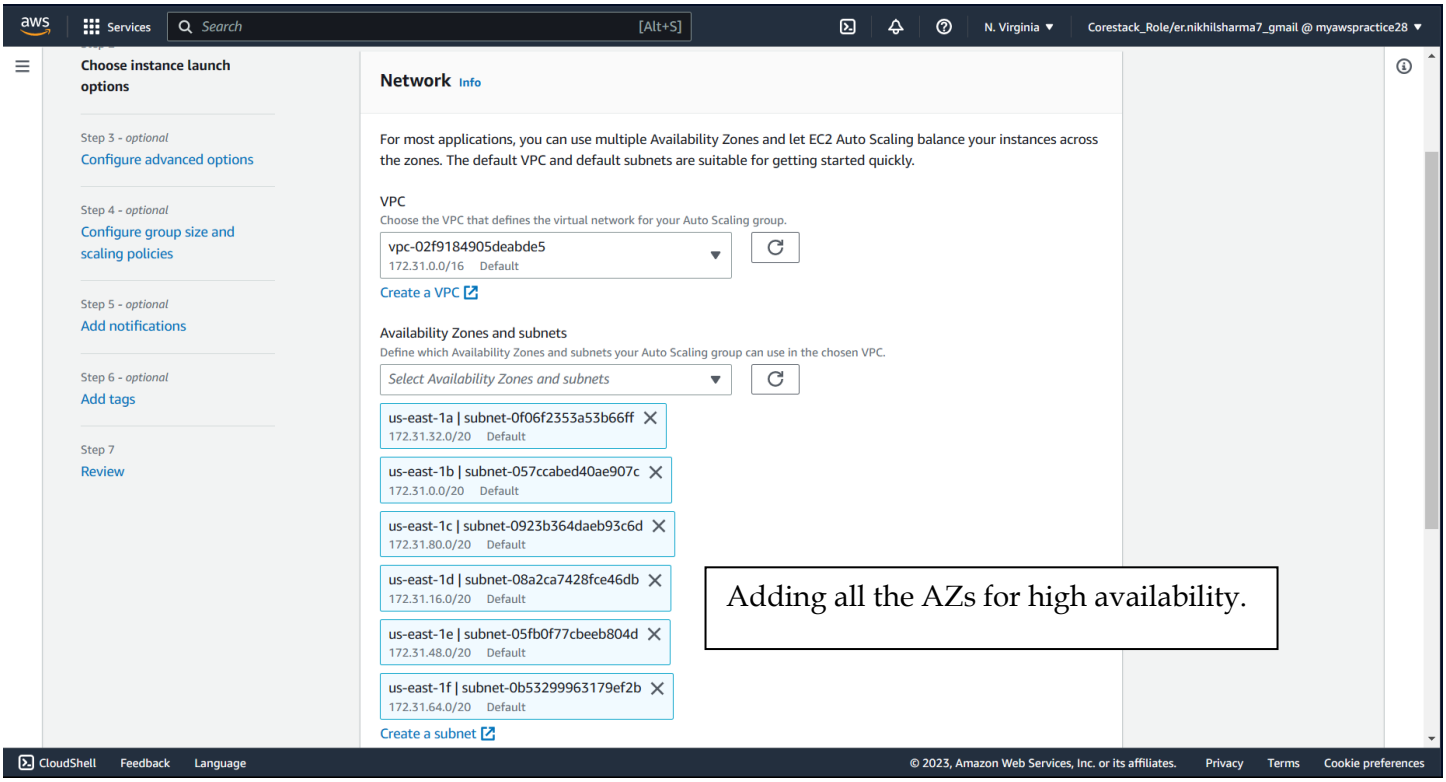

EC2 > Launch templates > Create template from instance
Create launch template
Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.
Launch template name and description
Source instance
i-0a21b3a6a4c16df10
Launch template name - required
webserverLaunchTemplate
Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.
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
Template tags
Summary
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-04581fbf744a7d11f
Virtual server type (instance type)
t2.micro
Firewall (security group)
launch-wizard-1
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Create launch template


Services
Search
[Alt+S]
N. Virginia
Corestack_Role/er.nikhilsharma7_gmail @ myawspractice28
Network settings Info
Subnet Info
subnet-0f06f2353a53b66ff
VPC: vpc-02f9184905deabde5 Owner: 133246519386 Availability Zone: us-east-1a
IP addresses available: 4089 CIDR: 172.31.32.0/20)
Create new subnet
When you specify a subnet, a network interface is automatically added to your template.
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Select existing security group
Create security group
Common security groups Info
Select security groups
launch-wizard-1 sg-06a5a7f144fd558d5
VPC: vpc-02f9184905deabde5
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Advanced network configuration
Network interface 1
Device index Info
0
Network interface Info
New interface
Description Info
Subnet Info
subnet-0f06f2353a53b66ff
IP addresses available: 4089
Security groups Info
Select security groups
Show all selected (1)
Auto-assign public IP Info
Enable
Summary
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-04581fbf744a7d11f
Virtual server type (instance type)
t2.micro
Firewall (security group)
launch-wizard-1
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Create launch template
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

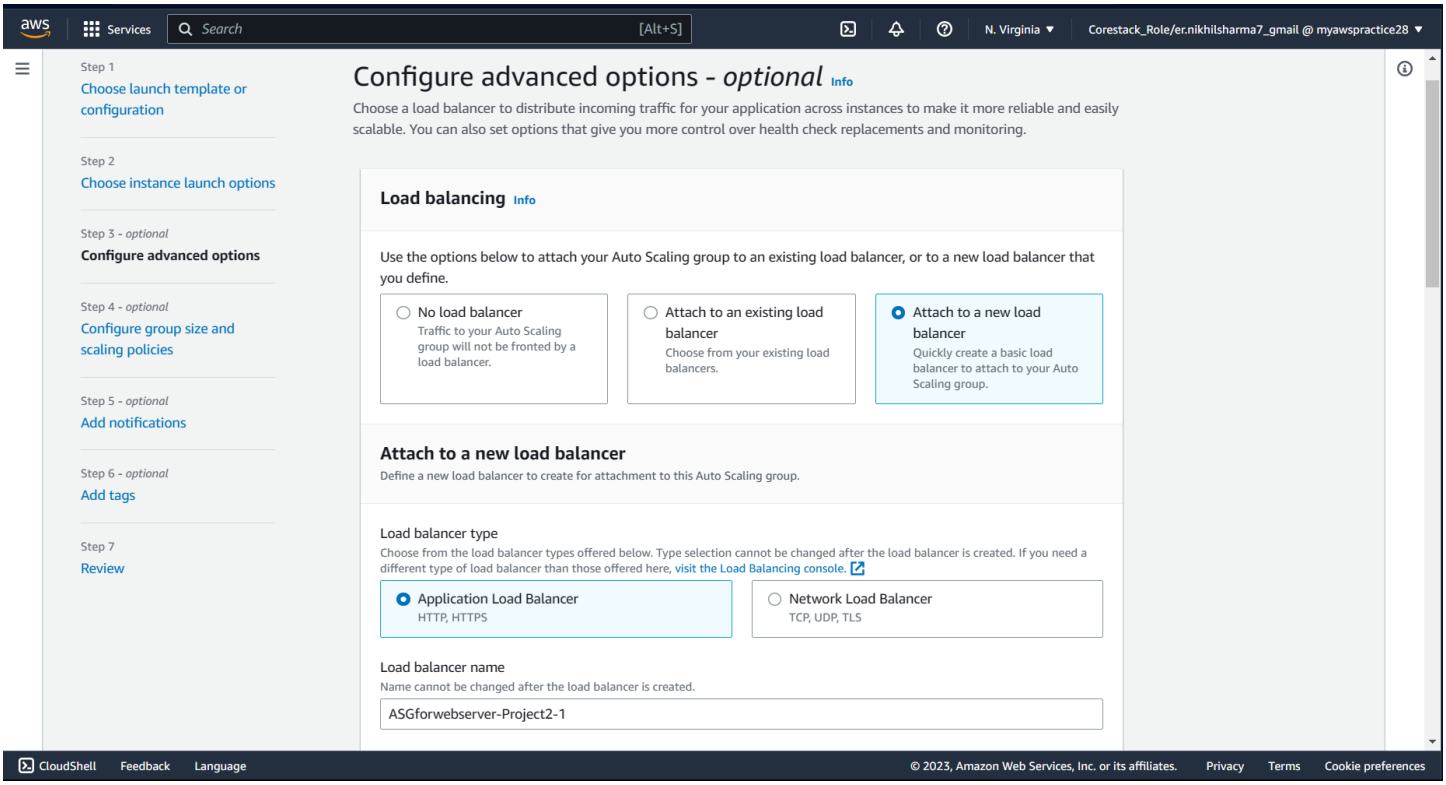

Services
Search
[Alt+S]
N. Virginia
Corestack_Role/er.nikhilsharma7_gmail @ myawspractice28
EC2 > Launch templates > Create template from instance
Success
Successfully created webserverLaunchTemplate (lt-0475c266947e0f104)
Actions log
Next steps
Launch an instance
With On-Demand Instances, you pay for compute capacity by the second (for Linux, with a minimum of 60 seconds) or by the hour (for all other operating systems) with no long-term commitments or upfront payments. Launch an On-Demand Instance from your launch template.
Launch instance from this template
Create an Auto Scaling group from your template
Amazon EC2 Auto Scaling helps you maintain application availability and allows you to scale your Amazon EC2 capacity up or down automatically according to conditions you define. You can use Auto Scaling to help ensure that you are running your desired number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
Create Auto Scaling group
Create Spot Fleet
A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance (of each instance type in each Availability Zone) is set by Amazon EC2, and adjusted gradually based on the long-term supply of and demand for Spot Instances. Spot instances are well-suited for data-analysis, batch jobs, background processing, and optional tasks.
Create Spot Fleet
View launch templates
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

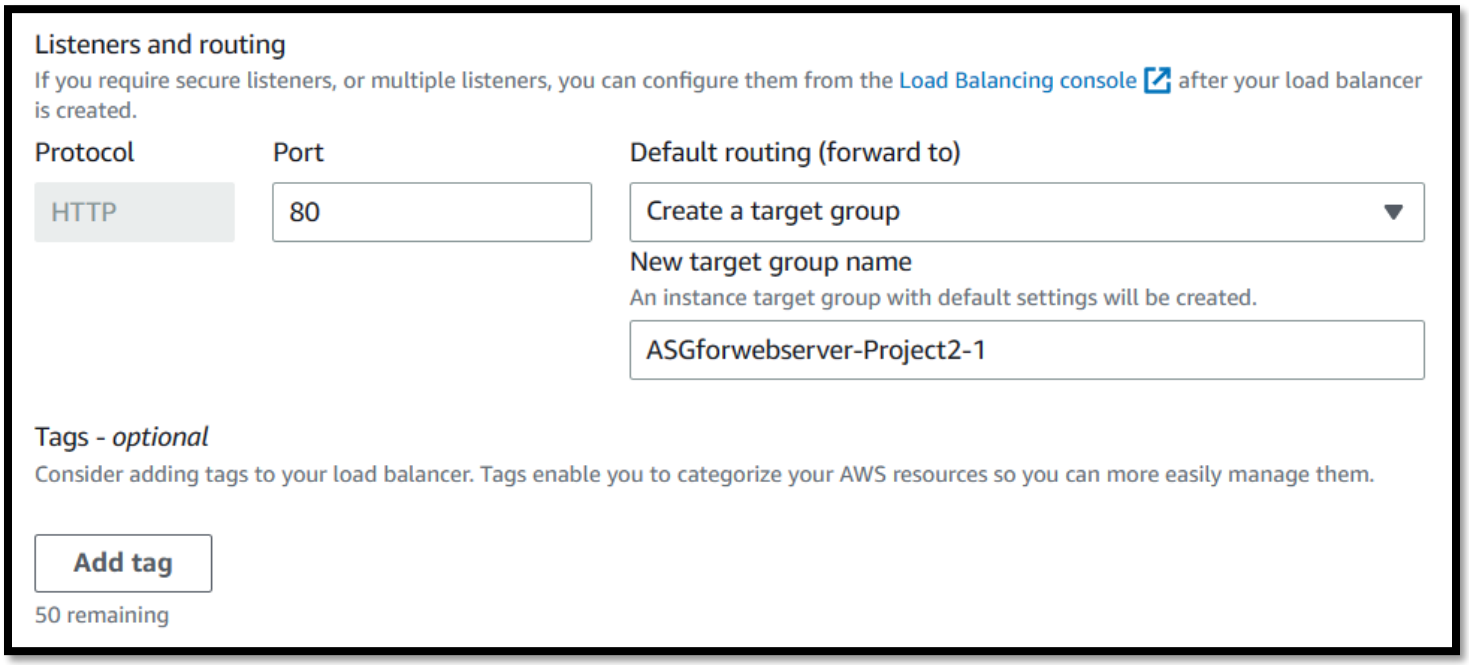
Creating the ASG using the created Template.

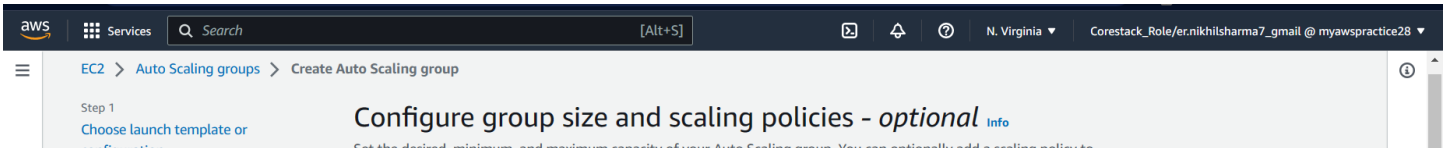


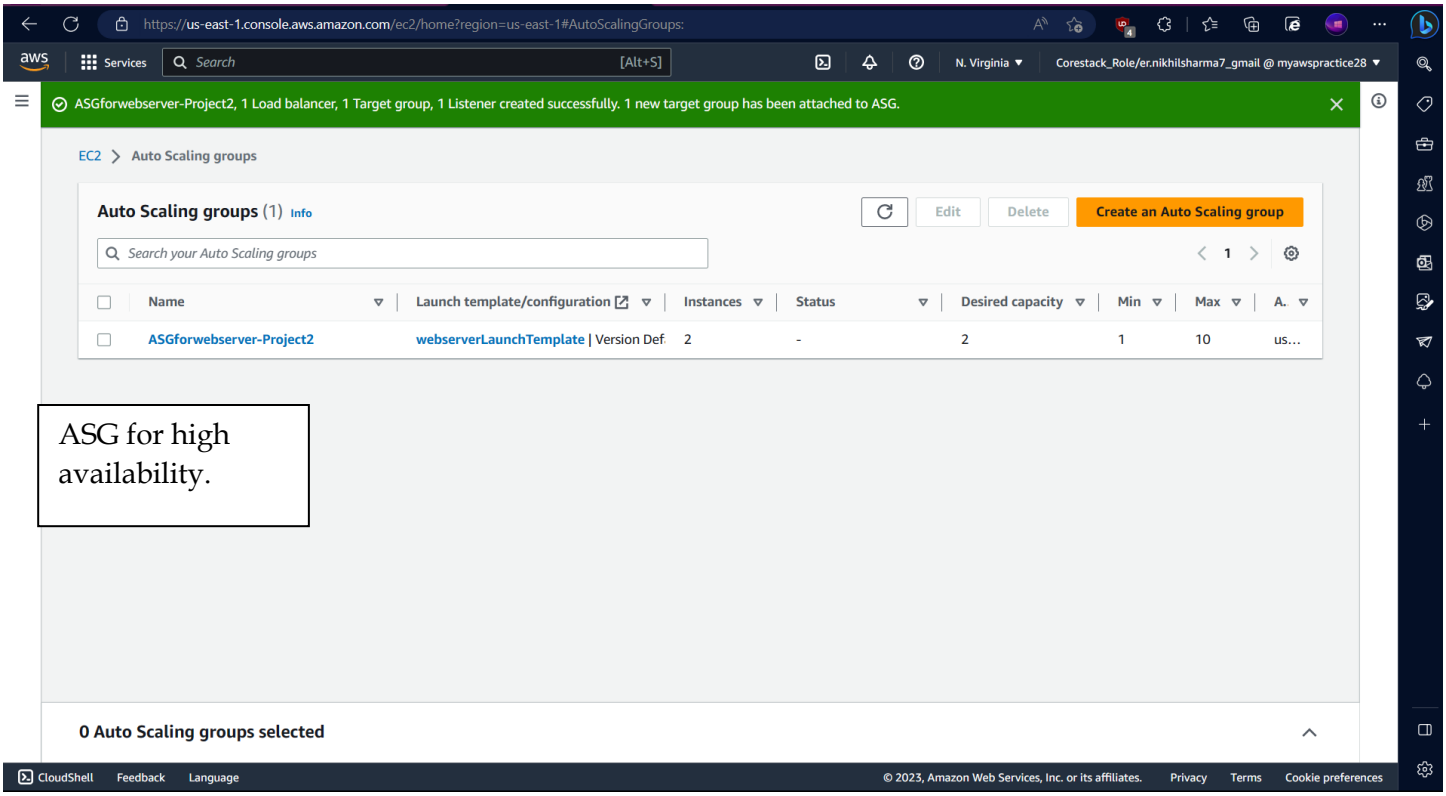



Creating the Internet facing Application Load Balancer(HTTP, HTTPS):

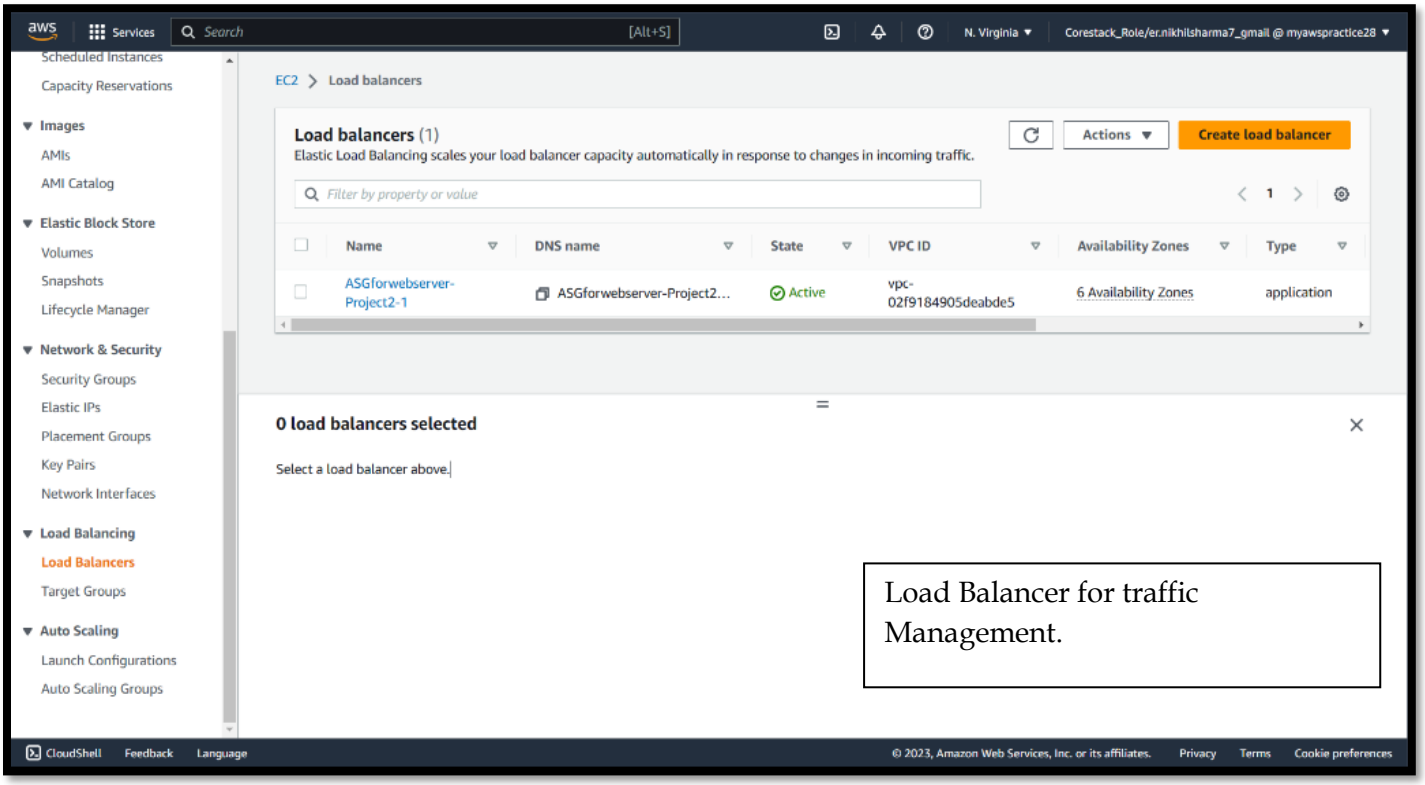





ASG for high availability.




Load Balancer for traffic Management.