

CLOUD COMPUTING LABS SECTION II

Daniel Ge

Period 678



CISCO

CCNP LAB REPORT

Purpose

These labs continue with more exercises of the AWS concepts covered in later sections of the AWS Cloud Foundations course to train users in familiarity with using the AWS management system in sample corporate scenarios. By going through more mock scenarios with more AWS services, we expand our experience in implementing AWS Cloud solutions to tackle more advanced business goals.

Background Information

When an EC2 (Elastic Compute Cloud) instance is deleted, all the data associated with the instance would typically be deleted. To prevent this from happening, we may use Amazon EBS (Elastic Block Storage) by attaching the instance to Amazon Elastic Block Storage such that data is preserved even when the instance is unexpectedly terminated, such as by a power outage.

The advantage of AWS EBS over normal Object storage would be that block storage allows us to change a small part of a large file without updating the entire file through virtue of dividing the file into many blocks. This advantage significantly reduces the latency and cost if EBS, while improving throughput.

EBS Volumes also offer additional features for resiliency through automatic replication within the Availability Zones and optional backups to Amazon S3. Through snapshots, we may recreate a previous stable version of the volume in case the current version has an error that cannot be recovered.

EBS Volumes are divided into Solid State Drives (SSD) and Hard Disk Drives (HDD) then further subdivided into options such as General Purpose or Provisioned IOPS, each offering different Volume Sizes, Volume Maximums, and Throughputs. Selecting the correct EBS Volume for a given situation is key to saving on costs while achieving the desired result.

Though AWS' storage services like AWS S3 (Simple Storage System) or EBS (Elastic Block Storage) allow us transfer large amounts of unstructured data with high throughput and low latency, organizations may occasionally need to achieve more complex tasks on their data such as filtering or data analytics. For this purpose, AWS provides various Database services, including AWS RDS (Relational Database Service)

AWS RDS allows users to create multiple databases in each DB instance. These instances can be deployed across multiple AZs (availability zones) and are best fit for applications without too much information stored but frequently accessed. RDS offers advantages including high throughput, low-cost, data security, and automatic scaling.

AWS RDS DBs are best used for high durability complex querying with high query and write rates as opposed to use cases with massive read rates or GET requests done without SQL.

After setting up the RDS DB, instances are charged either on-demand or reserved for a multi-year term. The first backup to the storage can be made without additional charge.

Given the fluctuation of traffic for web organizations throughout a given day or year, it is often inefficient to upkeep many EC2 instances, RDS databases, or other applications to account for the maximum spike in traffic usage every year. Instead, AWS allows us to automatically scale many of our services used according to demand.

In our lab, we will be large interacting with EC2 Auto Scaling. Using AWS CloudWatch, we may set alarms to detect when our AWS traffic gets too high or too low. When these alarms are triggered, we may then configure for EC2 Auto Scaling to automatically increase or decrease the number of EC2 instances run.

To distribute traffic across new and old instances in a balanced manner, we use Elastic Load Balancing. During periods of high traffic volume, load balancing automatically assigns each user traffic to some instance such that, overall, each instance is used at a similar level. Load balancing can occur at the Application level (OSI Layer 7) for HTTP/HTTPS traffic, at the network level (OSI Layer 4) for TCP/UDP/TLS traffic, or the classic load balancer to balance traffic across EC2 instances.

Lab Summary

In Lab 4, we practice using Amazon EBS (Elastic Block Storage). We begin by creating a new EBS Volume, then attach the volume to an EC2 instance. After the connection is established, we will then use EBS Snapshots to preserve the current file state. To test EBS Snapshots, we will make changes on our EBS Volume by deleting a file, then use snapshots to restore it.

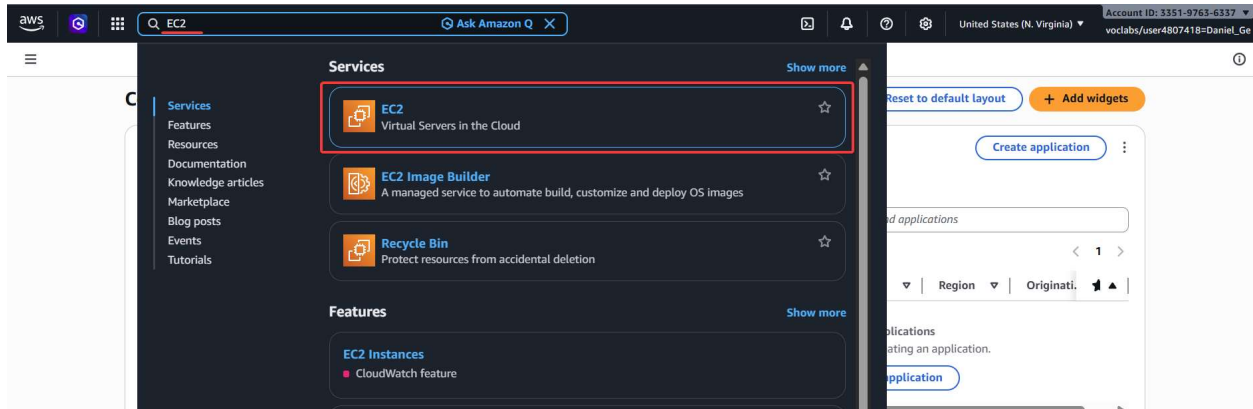
In Lab 5, we practice creating and using an Amazon RDS (Relational Database System) DB instance. We begin by configuring the appropriate security groups and subnet group for the instance, then create the instance itself through the AWS Management Console. We may then test the RDS DB instance by interacting with the database through a browser window.

In Lab 6, we practice with creating load balancers and auto scaling groups. The lab begins with creating a load balancer for the incoming web traffic. Afterwards, we create an Auto-Scaling group with a desired capacity of 2 but max capacity of 6 set to scale at Average CPU Utilization greater than 60%. We test the load balancer by spamming the EC2 instance with traffic, and observing the new instances being added.

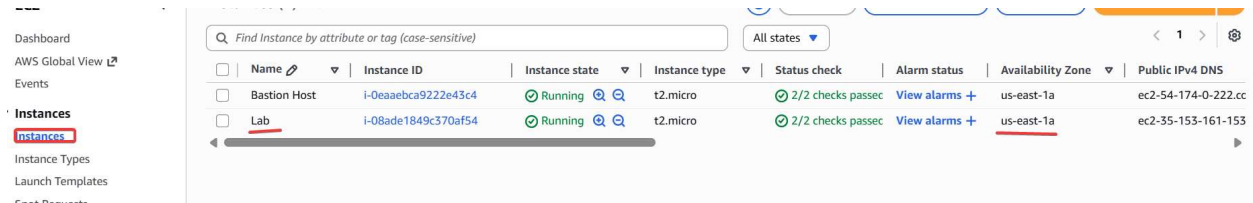
Lab Procedure

Working with EBS (Lab 4)

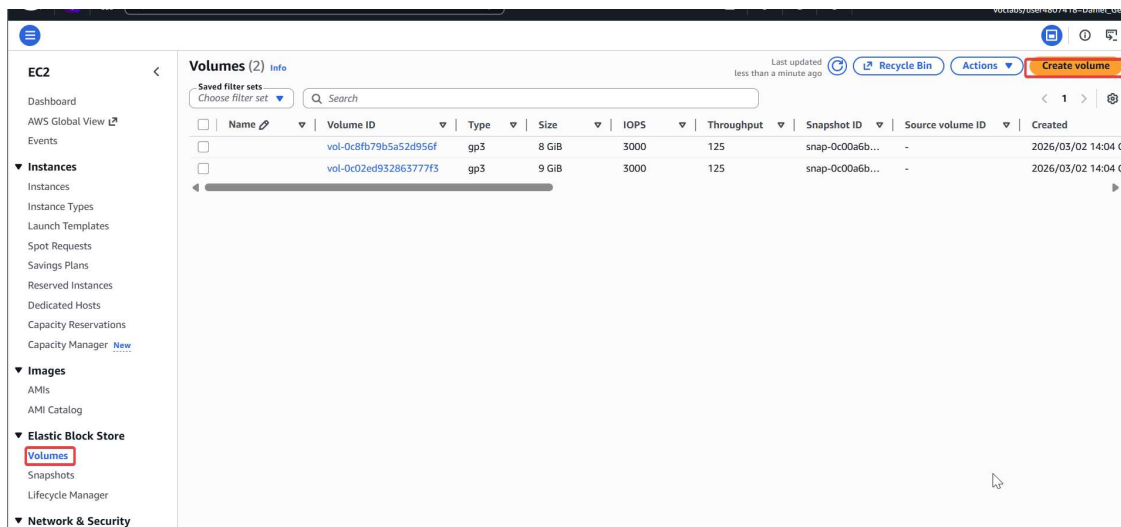
To begin creating a new EBS Volume, using the search bar, open the EC2 menu



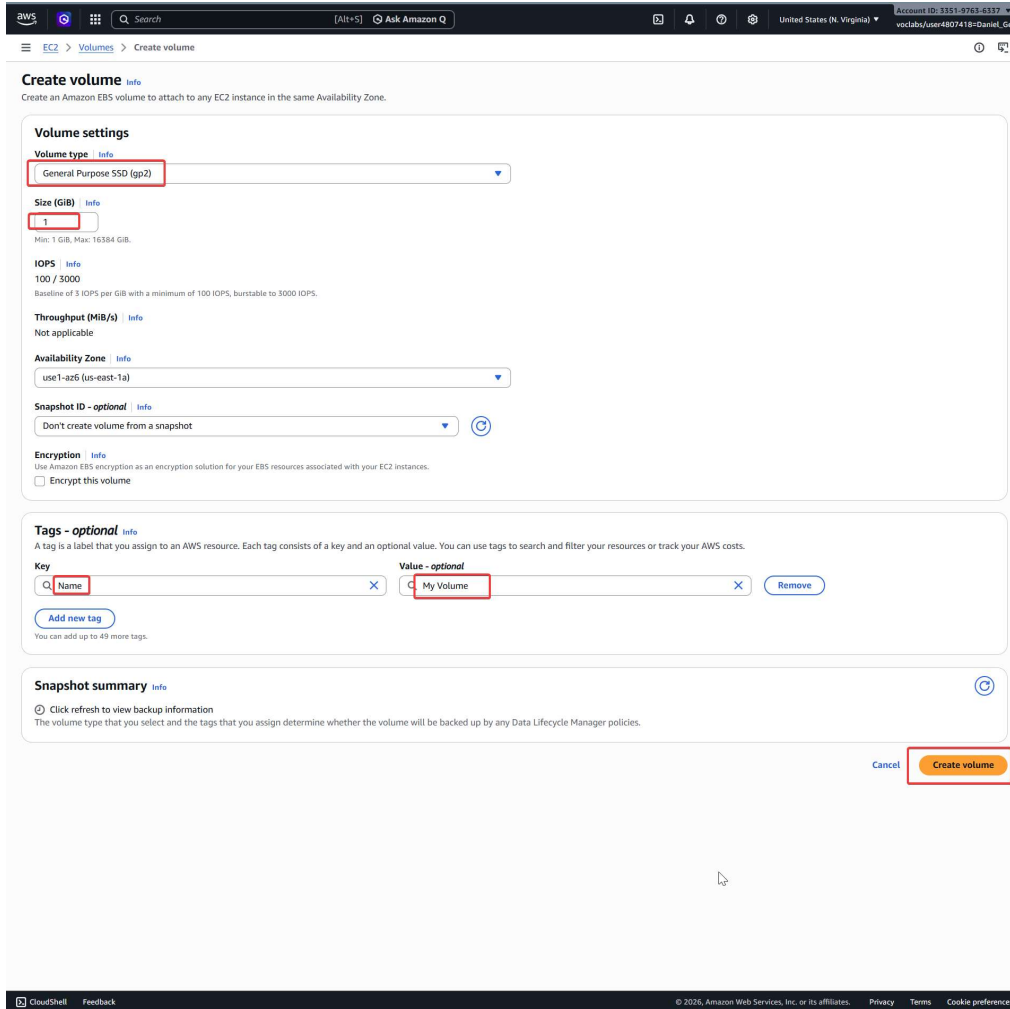
Click the instances tab and verify that there is an instance Lab already started running in us-east-1a



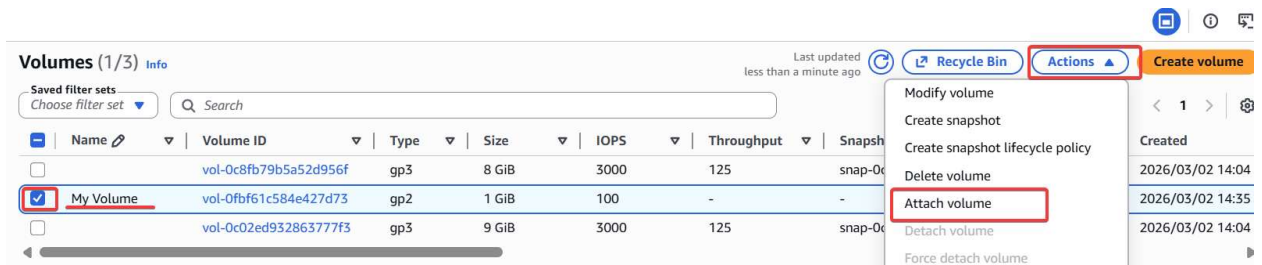
Click the Volumes tab on the left menu, then click “Create Volume”



Confirm the Volume type is set to gp2, set the size to 1 GiB, and add a Tag with key “Name” and Value “My Volume”



Select the checkbox next to the Volume with name “My Volume”, then click the Actions drop bar and click Attach Volume



Configure the instance to the one labeled “Lab” and device name to “/dev/sdf”, then click Attach Volume

Attach volume Info

Attach a volume to an instance to use it as you would a regular physical hard disk drive.

Basic details

Volume ID
vol-0fbf61c584e427d73 (My Volume)

Availability Zone
use1-az6 (us-east-1a)

Instance Info
i-08ade1849c370af54 (lab) (running)

Only instances in the same Availability Zone as the selected volume are displayed.

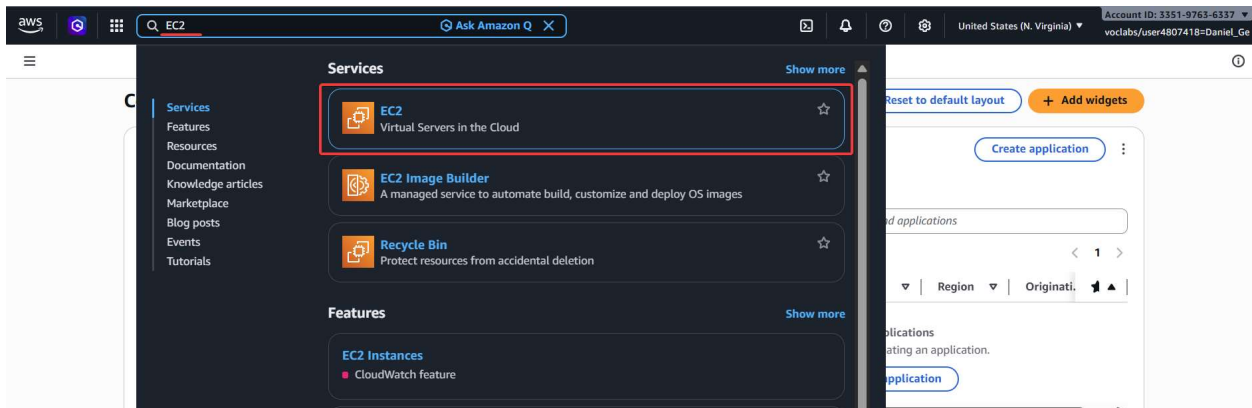
Device name Info
/dev/sdf

Recommended device names for Linux: /dev/xvda for root volume, /dev/sd[f-p] for data volumes.

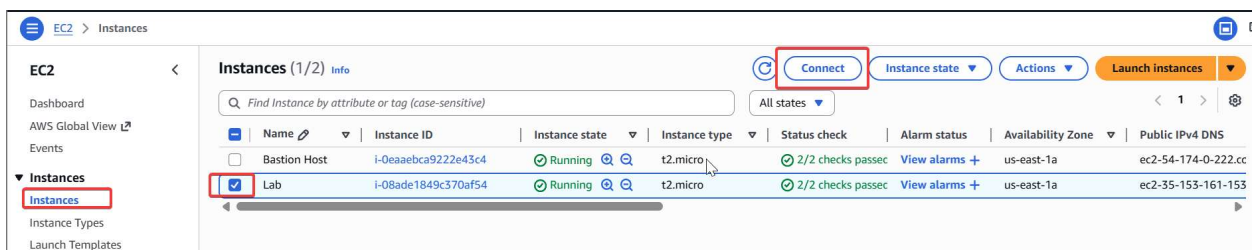
Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

[Cancel](#) [Attach volume](#)

Using the search bar, open the EC2 menu



Open “Instances” from the left menu, then click the checkbox next to “lab”. Click “Connect” on the top



Keep the default settings and click Connect


```
[ec2-user@ip-10-1-11-134 ~]$ sudo mkfs -t ext3 /dev/sdf
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 262144 4k blocks and 65536 inodes
Filesystem UUID: ba09c403-fe6d-4184-8297-baaa9c8287c4
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done
```

Now create a directory for mounting the new volume using the command,

```
sudo mkdir /mnt/data-store
```

```
[ec2-user@ip-10-1-11-134 ~]$ sudo mkdir /mnt/data-store
```

Mount the new volume to the EC2 instance using the command,

```
sudo mount /dev/sdf /mnt/data-store
```

```
[ec2-user@ip-10-1-11-134 ~]$ sudo mount /dev/sdf /mnt/data-store
```

To ensure the instance mounts this volume upon startup, add the following command,

```
echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee
-a /etc/fstab
```

```
[ec2-user@ip-10-1-11-134 ~]$ echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab
/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2
```

View the configuration file using the command,

```
cat /etc/fstab
```

```
[ec2-user@ip-10-1-11-134 ~]$ cat /etc/fstab
#
UUID=96e83033-9c05-4912-8900-93256ded3e51 / xfs defaults,noatime 1 1
UUID=C42B-0705 /boot/efi vfat defaults,noatime,uid=0,gid=0,umask=0077,shortname=winnt,x-systemd.automount 0 2
/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2
```

Verify the changes by typing in “df -h” and click enter. Observe the new /dev/xvdf mounted onto the data store

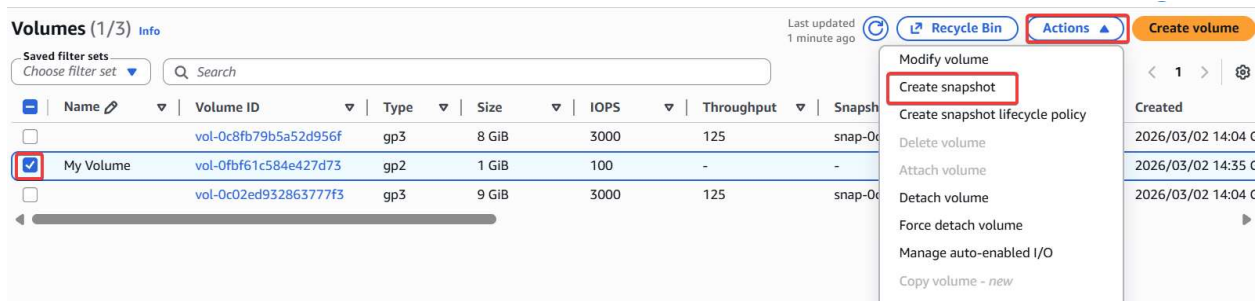
```
[ec2-user@ip-10-1-11-134 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M  0    4.0M  0%  /dev
tmpfs           481M  0    481M  0%  /dev/shm
tmpfs           193M  440K 192M  1%  /run
/dev/xvda1      8.0G  1.7G  6.4G  21%  /
tmpfs           481M  0    481M  0%  /tmp
/dev/xvda128    10M   1.3M  8.7M  13%  /boot/efi
tmpfs           97M   0    97M   0%  /run/user/1000
/dev/xvdf       975M  60K   924M  1%  /mnt/data-store
```

To test, create file.txt on the data-store folder and write a text on there using the command
`sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"`

Then verify the text has been added

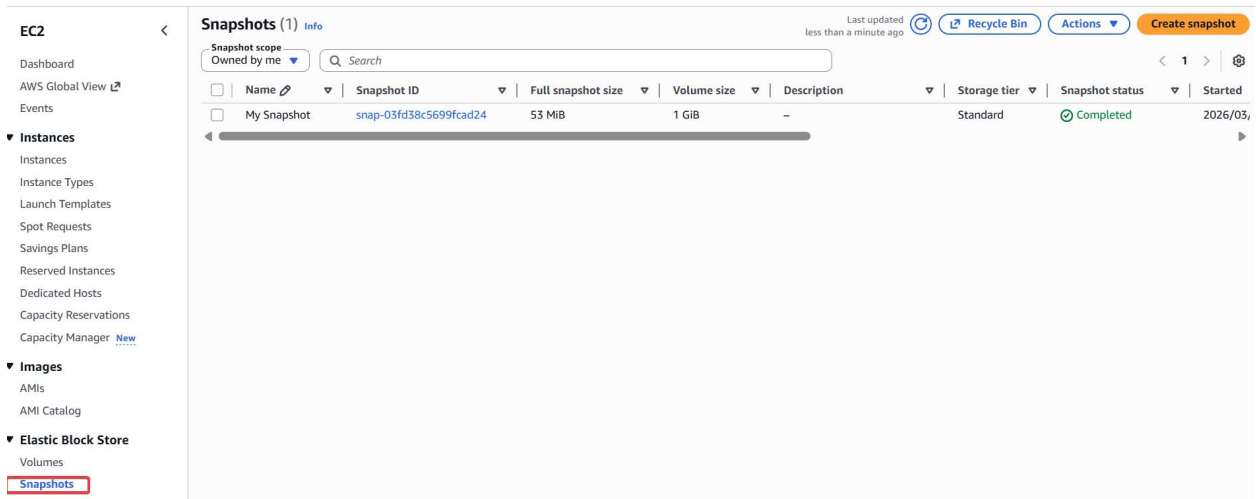
```
[ec2-user@ip-10-1-11-134 ~]$ sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
[ec2-user@ip-10-1-11-134 ~]$ cat /mnt/data-store/file.txt
some text has been written
```

Return to the Volumes tab on EC2 console. Select “My Volumes” then “Create snapshot” under the “Actions” menu



Add a tag with Key “Name” and Value “My Snapshot”, then click Create Snapshot

Open Snapshots using the left menu and verify that a new snapshot has been created



Return to EC2 Connect Console and delete the file.txt file using the command,

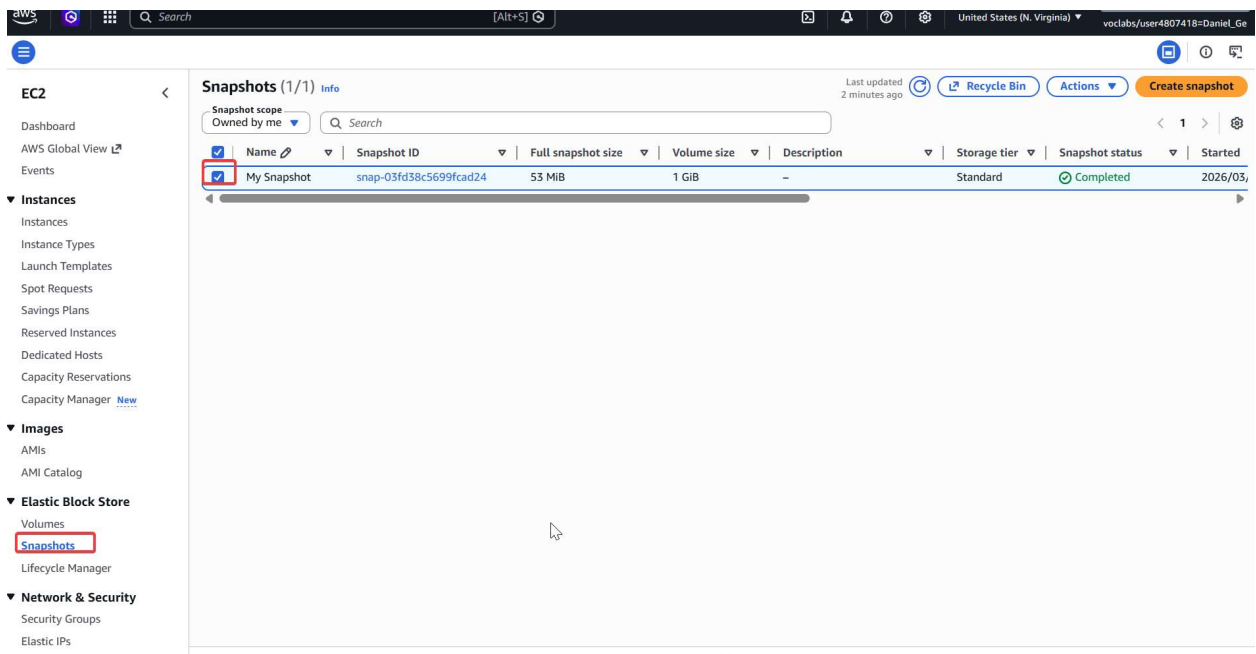
```
sudo rm /mnt/data-store/file.txt
```

Verify the deletion using the command,

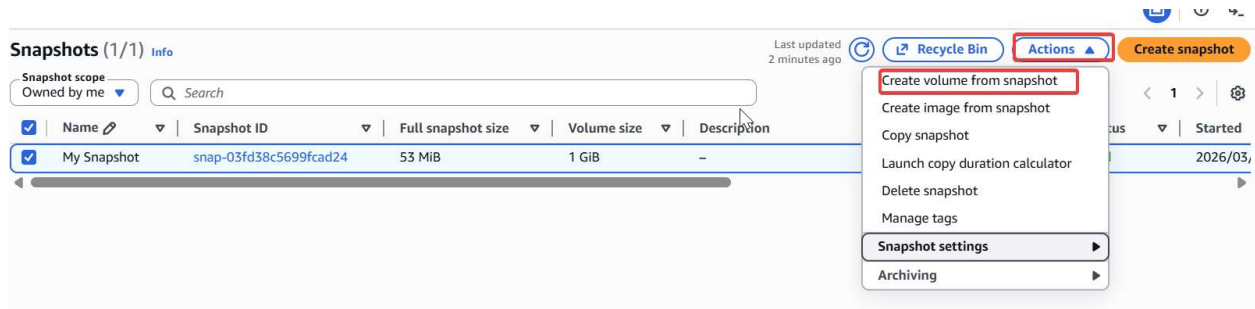
```
ls /mnt/data-store/
```

```
[ec2-user@ip-10-1-11-134 ~]$ sudo rm /mnt/data-store/file.txt
[ec2-user@ip-10-1-11-134 ~]$ ls /mnt/data-store/
lost+found
```

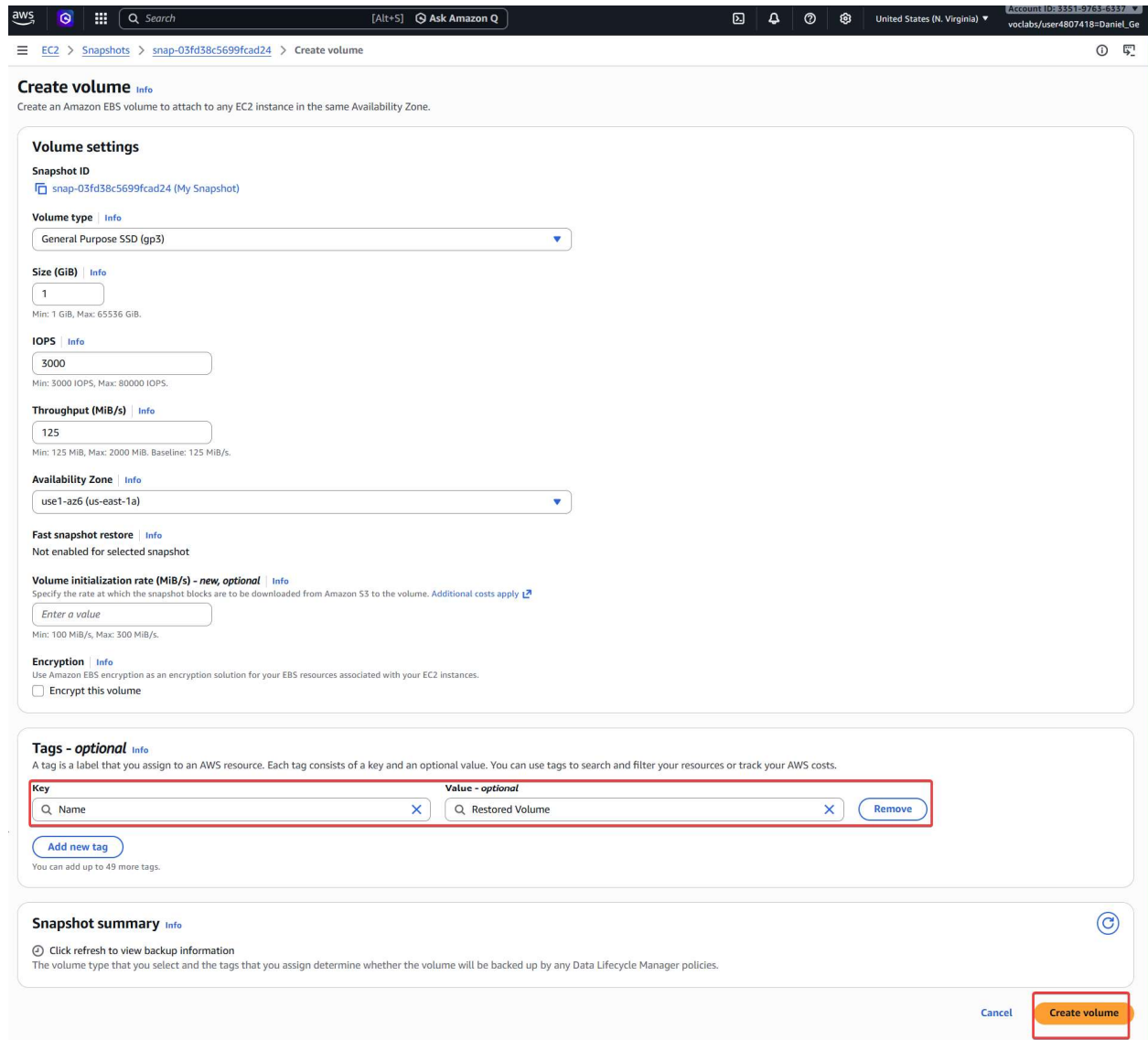
To restore this file using the snapshot, return to the Snapshots tab and click “My Snapshot”



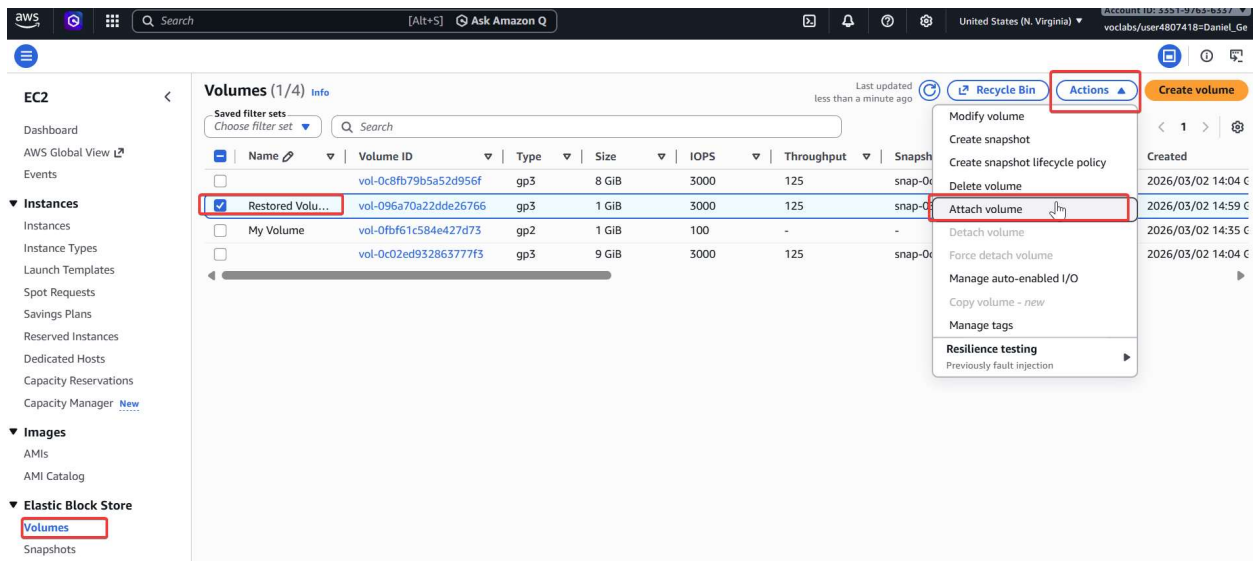
Under the Actions drop down, click “Create volume from snapshot”



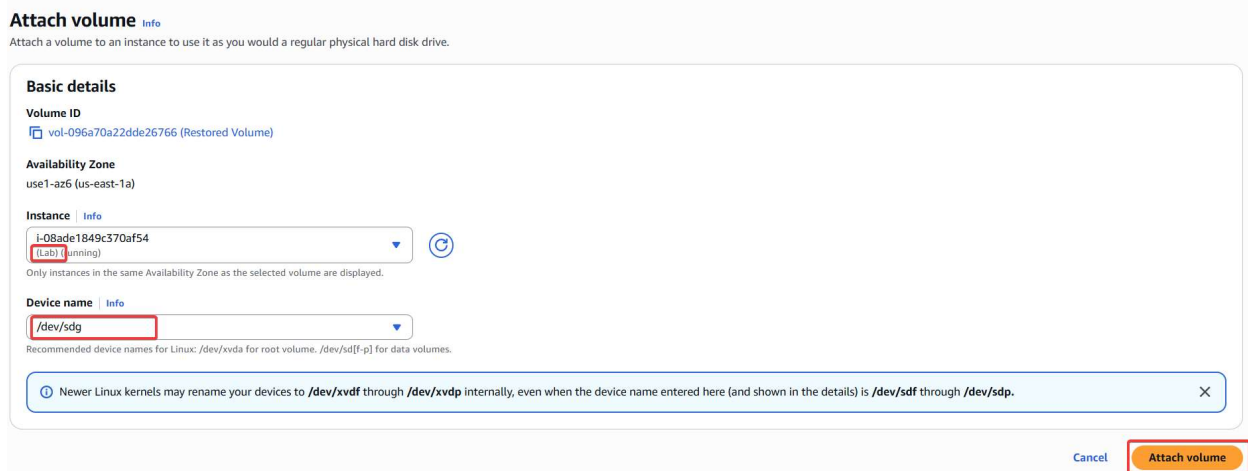
Configure the Tag as follows, then “Create volume”



Navigate to the Volumes tab, click checkbox next to the Restored Volume, and click “Attach Volume” under the Actions drop down



Configure the Instance to lab and Device name to “/dev/sdg”, then click “Attach volume”



Mount the backup using the console through the commands,

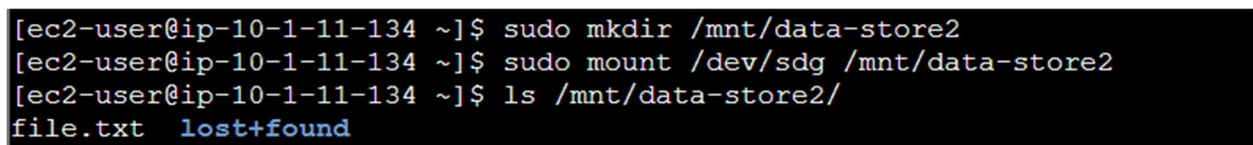
```
sudo mkdir /mnt/data-store2
```

```
sudo mount /dev/sdg /mnt/data-store2
```

Confirm the volume has been mounted using,

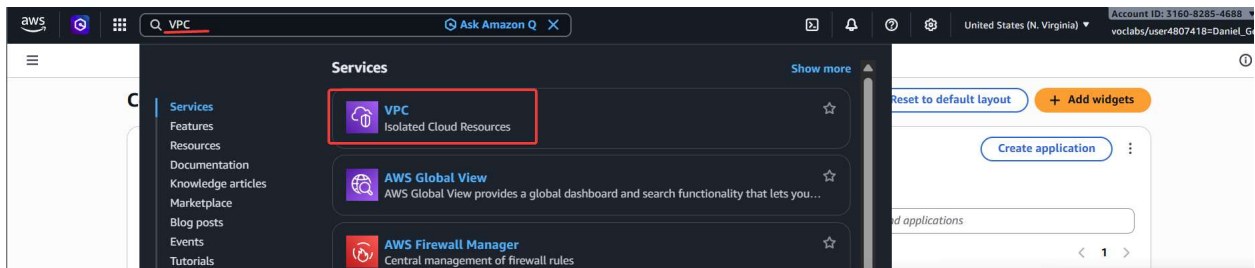
```
sudo mount /dev/sdg /mnt/data-store2
```

file.txt has been restored.

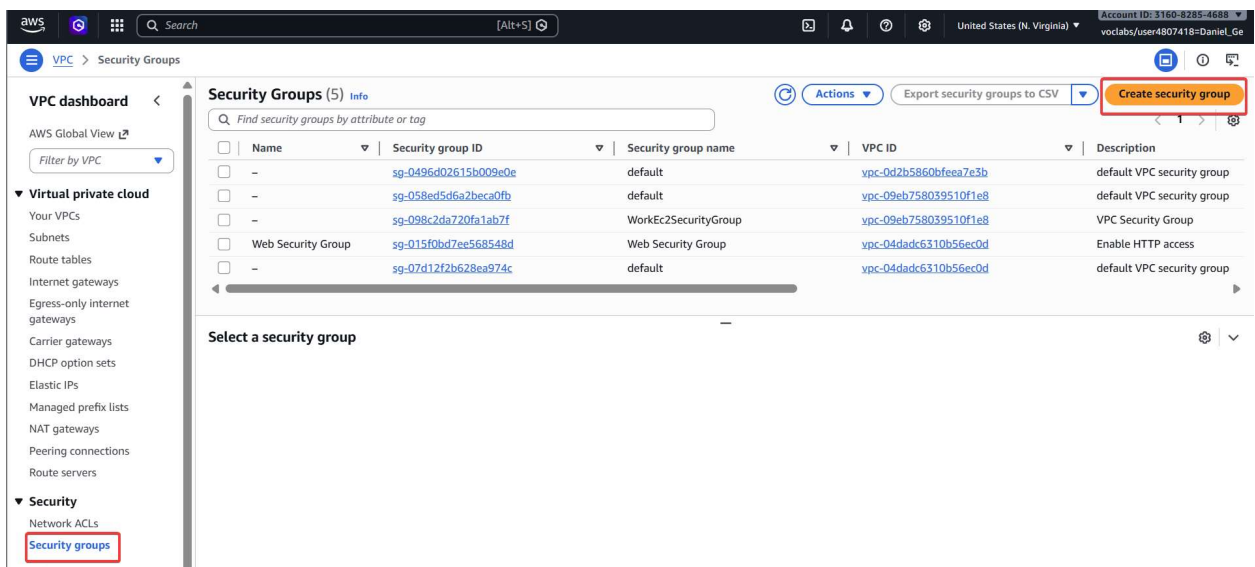


Build a Database Server (Lab 5)

Using the search bar, open search for and open the VPC console



Click “Security groups” on the left menu, then the “Create security group” button



Configure the security group name and description as follows, then set the VPC to the pre-made Lab VPC

Basic details

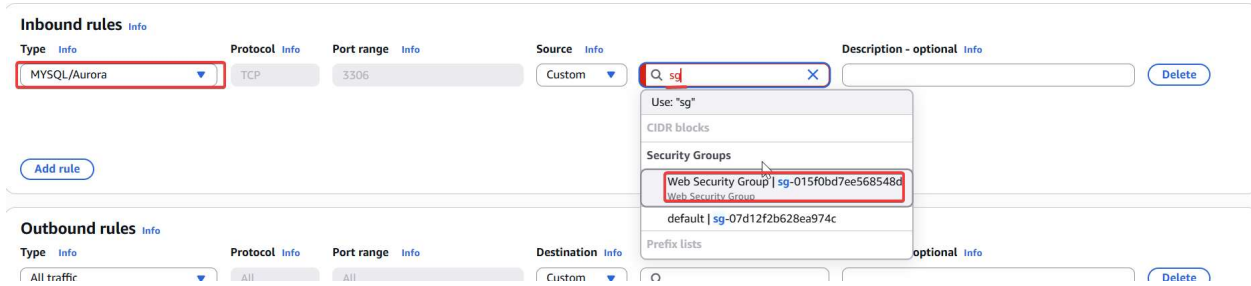
Security group name [Info](#)

Name cannot be edited after creation.

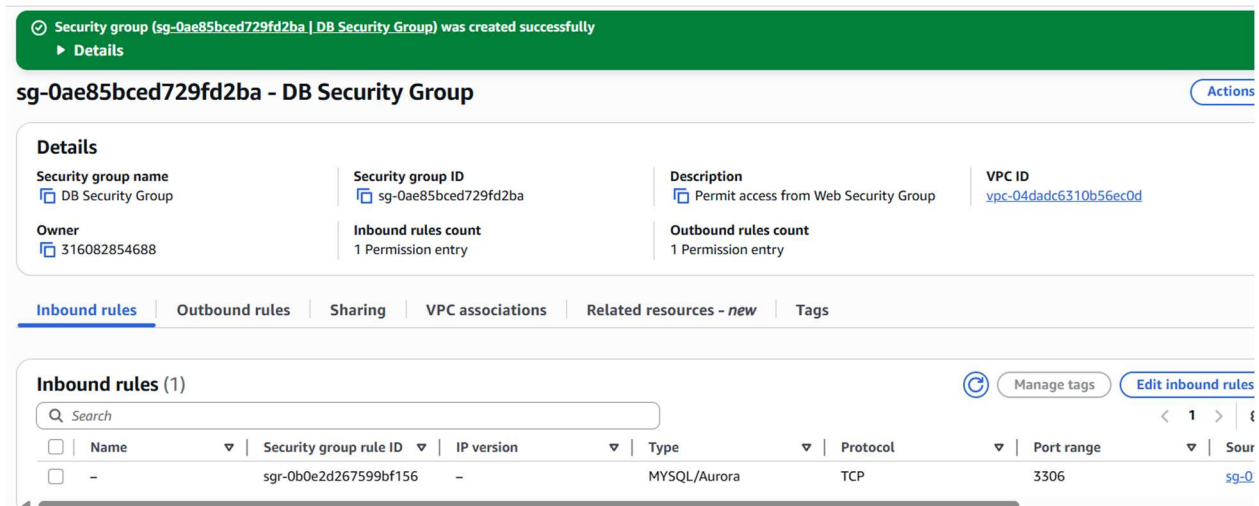
Description [Info](#)

VPC [Info](#)

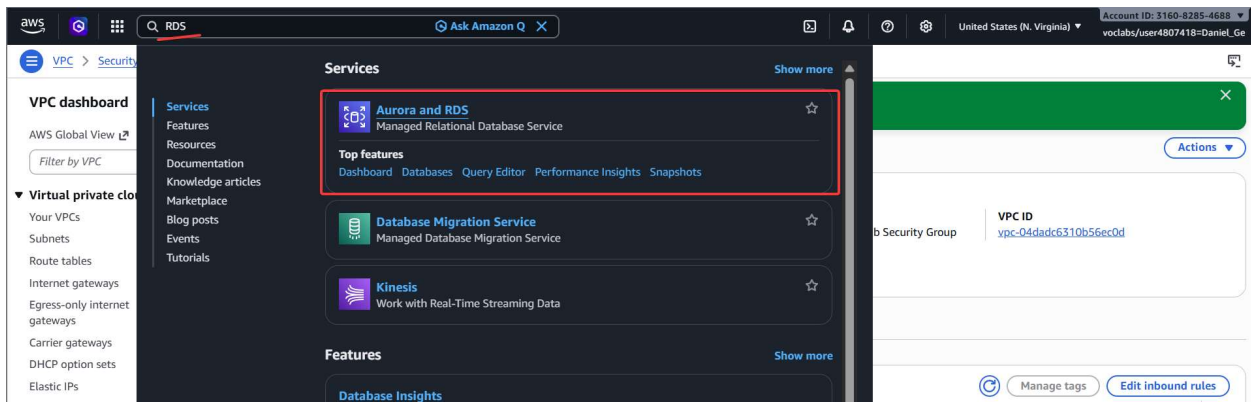
Set the type to MySQL/Aurora, then type sg in the search bar to the right of Source to find security group “Web Security Group”



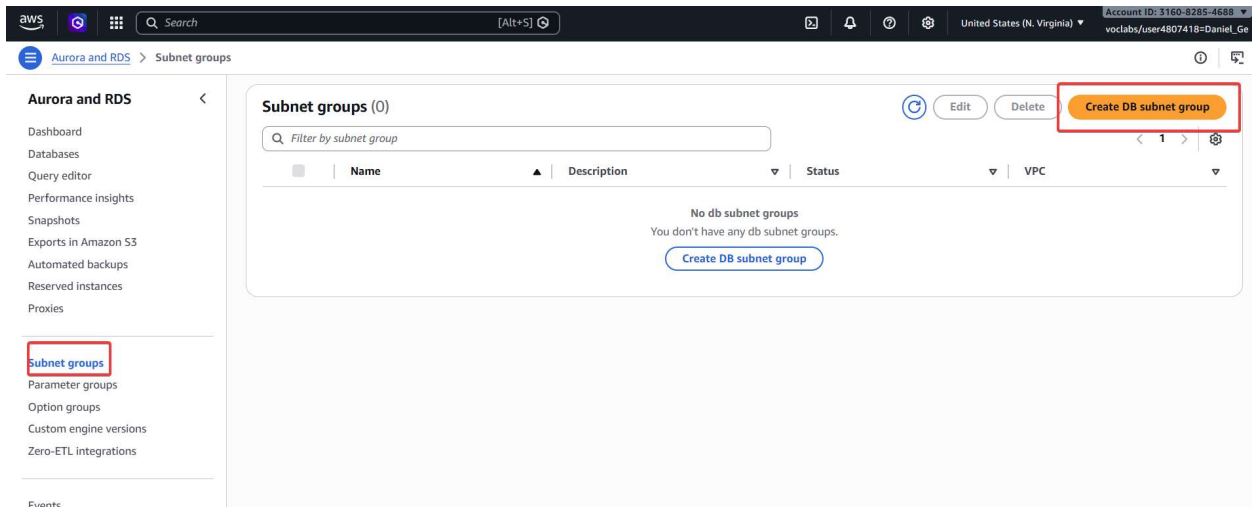
Click Create Security Group



Using the search bar, navigate to the Aurora and RDS console



Click “Subnet groups”, then “Create DB subnet group”



Configure the Name and Description as follows, then choose Lab VPC

Subnet group details

Name
You won't be able to modify the name after your subnet group has been created.

DB-Subnet-Group

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

DB Subnet Group

VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

Lab VPC (vpc-04dad6310b56ec0d)
4 Subnets, 2 Availability Zones

Add Availability zones “us-east-1a” and “us-east-1b” and subnets “Private Subnet 1” and “Private Subnet 2”, then click Create

Add subnets

Availability Zones
Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone

us-east-1a x us-east-1b x

Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets

Private Subnet 1 x Subnet ID: subnet-0b5b0960ff279064b CIDR: 10.0.1.0/24

Private Subnet 2 x Subnet ID: subnet-0b202db01bfd8cd7f CIDR: 10.0.3.0/24

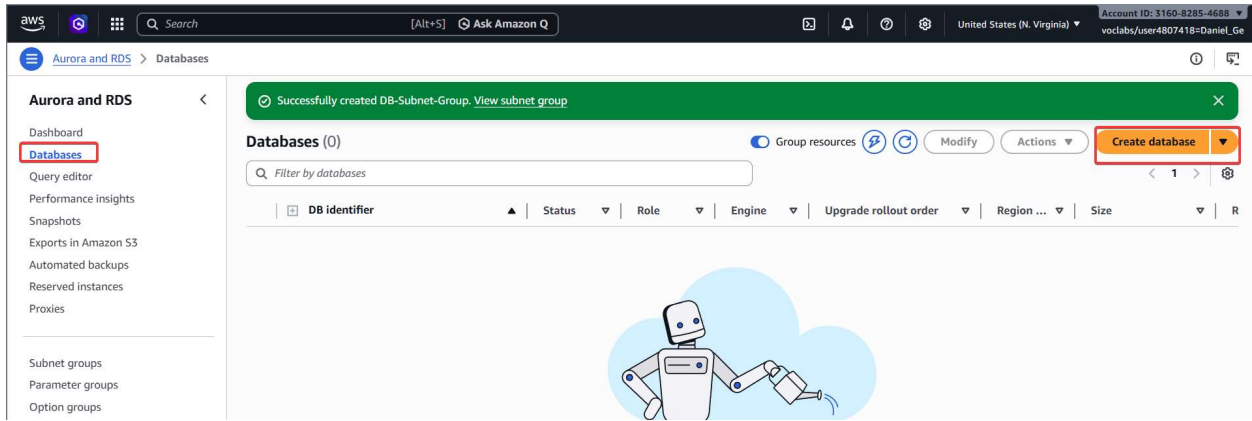
For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.

Subnets selected (2)

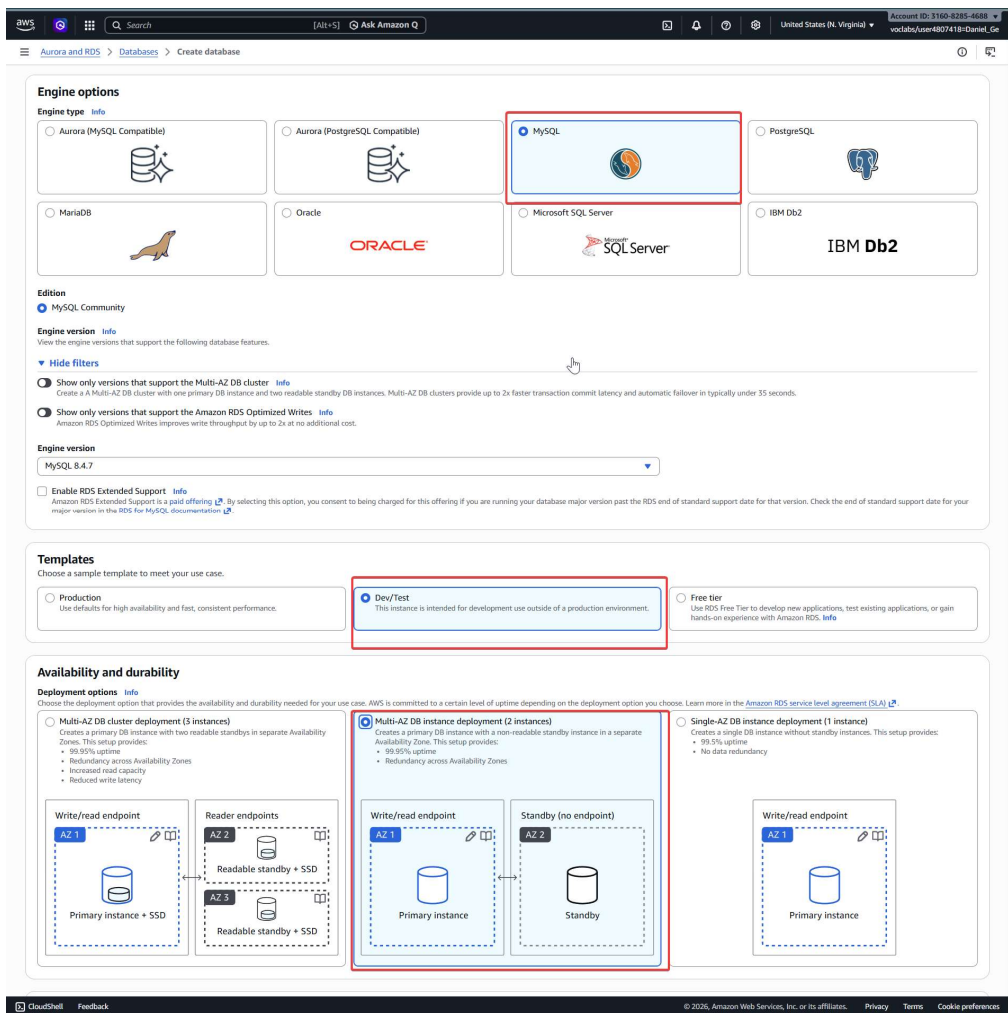
Availability zone	Subnet name	Subnet ID	CIDR block
us-east-1a	Private Subnet 1	subnet-0b5b0960ff279064b	10.0.1.0/24
us-east-1b	Private Subnet 2	subnet-0b202db01bfd8cd7f	10.0.3.0/24

Cancel Create

Click the “Databases” tab, then “Create database”



Choose MySQL, Dev/Test, and 2 instances



Configure the DB instance identifier and Master username as follows, then select “Self managed” and set the Master password to “lab-password”

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.

lab-db

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 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.

main

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

Managed in AWS Secrets Manager - *most secure*
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

Self managed
Create your own password or have RDS create a password that you manage.

Auto generate password

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

Master password [Info](#)

Password strength **Average**

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' * @

Confirm master password [Info](#)

Select Burstable classes under Instance configuration

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)

▼ Hide filters

- Show instance classes that support Amazon RDS Optimized Writes [Info](#)**
Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.
- Include previous generation classes
- Standard classes (includes m classes)
- Memory optimized classes (includes r and x classes)
- Burstable classes (includes t classes)**

Instance type

db.t3.micro

2 vCPUs 1 GiB RAM EBS Bandwidth: Up to 2,085 Mbps Network: Up to 5 Gbps

Change the Allocated storage to 20

Storage

Storage type [Info](#)

Provisioned IOPS SSD (io2) storage volumes are now available.

General Purpose SSD (gp3)

Performance scales independently from storage

Allocated storage [Info](#)

20

GiB

Minimum: 20 GiB. Maximum: 6,144 GiB

Provisioned IOPS [Info](#)

3000

IOPS

Baseline IOPS of 3,000 IOPS is included for allocated storage less than 400 GiB.

Storage throughput [Info](#)

125

MiBps

Baseline storage throughput of 125 MiBps is included for allocated storage less than 400 GiB.

To provision additional IOPS and throughput, increase the allocated storage to 400 GiB or greater.

► Additional storage configuration

Select “Lab VPC” for the Virtual private cloud, and configure the Existing VPC security group to only DB Security Group

Connectivity [Info](#)

Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

Virtual private cloud (VPC) [Info](#)
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Lab VPC (vpc-04dad6310b56ec0d)
4 Subnets, 2 Availability Zones

After a database is created, you can't change its VPC. Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group [Info](#)
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

db-subnet-group
2 Subnets, 2 Availability Zones

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

DB Security Group

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-rsa2048-g1 (default)
Expiry: May 25, 2061

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

► Additional configuration

Under monitoring, uncheck “Enable Enhanced monitoring”, uncheck “Enable automated backup”, and uncheck “Enable encryption”

Monitoring [Info](#)

Choose monitoring tools for this database. Database Insights provides a combined view of Performance Insights and Enhanced Monitoring for your fleet of databases. Database Insights pricing is separate from RDS monthly estimates. See [Amazon CloudWatch pricing](#).

Database Insights - Advanced

- Retains 15 months of performance history
- Fleet-level monitoring
- Integration with CloudWatch Application Signals

Database Insights - Standard

Additional monitoring settings

Enhanced Monitoring, CloudWatch Logs and DevOps Guru

Enhanced Monitoring

Enable Enhanced monitoring

Enabling Enhanced Monitoring metrics are useful when you want to see how different processes or threads use the CPU.

Log exports

Select the log types to publish to Amazon CloudWatch Logs

- Audit log
- Error log
- General log
- iam-db-auth-error log
- Slow query log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

Additional configuration

Database options, encryption turned off, backup turned off, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name [Info](#)

lab

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

default.mysql8.4

Option group [Info](#)

default:mysql-8-4

Backup

Enable automated backup

Creates a point-in-time snapshot of your database

Backup tags [Info](#)

Copies tags from the source database to the automated backup and snapshots respectively.

Copy tags to automated backup

This is a one-time setting. Future tag modifications need manual updates.

Enable encryption

Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

Click “Create database” and wait approximately 5 minutes for the database to deploy

Creating database lab-db [View connection details](#) ✕

Your database might take a few minutes to launch. You can use settings from lab-db to simplify configuration of suggested database add-ons while we finish creating your DB for you.

0 0 1 0 1

Databases (1) Group resources Modify Actions Create database

Filter by databases

DB identifier	Status	Role	Engine	Upgrade rollout order	Region ...	Size
lab-db	Creating	Instance	MySQL Co...	SECOND	us-east-1b	db.t3.micro

Click the blue lab-db link to open the lab-db page

Databases (1) Group resources Modify Actions

Filter by databases

DB identifier	Status	Role	Engine	Upgrade rollout order	Region ...	Size
lab-db	Available	Instance	MySQL Co...	SECOND	us-east-1b	db.t3.micro

Under the connectivity & security tab, click “Endpoints” and copy the Endpoint URL

Connectivity & security | Monitoring | Logs & events | Configuration | Zero-ETL integrations | Maintenance & backups | Data migration

Connect using [Info](#)

Code snippets
 Use when connecting through SDK, APIs, or third-party tools including agents.

CloudShell
 Use for a quick access to AWS CLI that launches directly from the AWS Management Console.

Endpoints
 Use when connecting through any IDE interface.

Database name: lab
 Master username: main
 Internet access gateway: Disabled
 Port: 3306

Endpoint type: Instance endpoint

Additional configurations

Connectivity & security

Endpoint & port

Endpoint: lab-db.clgth76x5lza.us-east-1.rds.amazonaws.com

Port: 3306

Networking

Availability Zone: us-east-1b

VPC: Lab VPC (vpc-04dad6310b56ec0d)

Subnet group: db-subnet-group

Subnets: subnet-0b202db01bfd8cd7f, subnet-0b5b0960ff279064b

Network type: IPv4

Security

VPC security groups: DB Security Group (sg-0ae85bced729fd2ba) Active

Publicly accessible: No

Certificate authority: rds-ca-rsa2048-g1

Certificate authority date: May 25, 2061, 16:34 (UTC-07:00)

DB instance certificate expiration date: March 04, 2027, 11:45 (UTC-08:00)

Return to the lab instruction page used to start the lab. Click “AWS Details” at the top right, then paste the WebServer IP into the browser

00:46 Start Lab End Lab **AWS Details** Details

Submit Submission Report Grades

Cloud Access Close

AWS CLI: Show

Cloud Labs
Remaining session time: 00:45:03(46 minutes)
Session started at: 2026-03-04T11:11:45-0800
Session to end at: 2026-03-04T12:41:45-0800

Accumulated lab time: 00:44:00 (44 minutes)

(1) ips -- public:54.80.94.157, private:10.0.2.30 (2) ips -- public:35.175.217.253, private:10.0.0.231

SSH key Show Download PEM Download PPK

AWS SSO Download URL

SecretKey	MYnkyOA9AKvig38EH0tXcH8ek/gUpZqGtTswC
WebServer	54.80.94.157
BastionHost	35.175.217.253
Region	us-east-1
AccessKey	AKIAUT...

Copy Ctrl+C
Copy link to highlight
Go to 54.80.94.157
Print... Ctrl+P
Open in reading mode
Translate selection to English
Inspect

The page displays information about the EC2 instance. Click the RDS link

aws Load Test **RDS**

Meta-Data	Value
InstanceId	i-07c2c0d55de87fc37
Availability Zone	us-east-1b

Current CPU Load: 7%

Paste the previously copied URL into Endpoint, enter “lab” for Database, “main” for Username, and “lab-password” for Password. Click Submit.

aws Load Test RDS

Endpoint

Database

Username

Password

The page will now display an address book from the App, which can be edited. The changes will be reflected in the RDS database across multiple regions

aws Load Test RDS

Address Book




Last name	First name	Phone	Email	Admin
Doe	Jane	010-110-1101	janed@someotheraddress.org	Add Contact Edit Remove
Johnson	Roberto	123-456-7890	roberto@someaddress.com	Edit Remove

Load Balancing (Lab 6)

Using the search bar, navigate to AWS EC2 menu

aws Ask Amazon Q

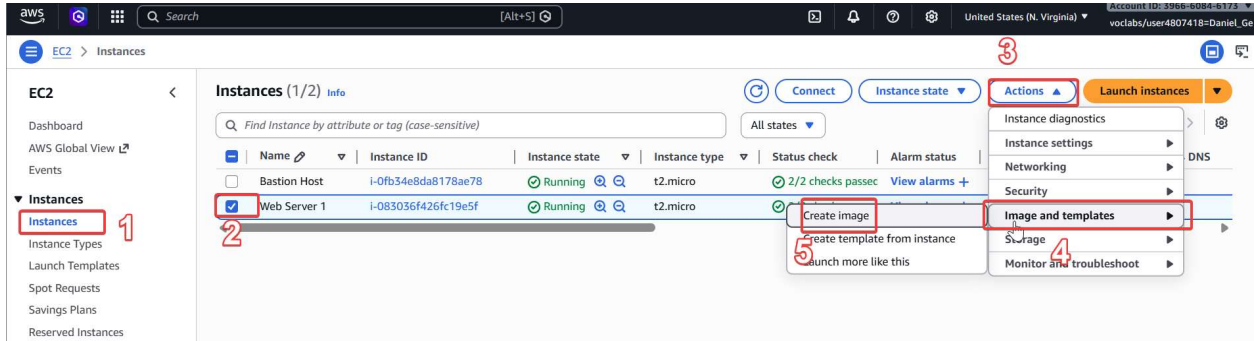
Services [Show more](#)

-  **EC2**
Virtual Servers in the Cloud ☆
-  **EC2 Image Builder**
A managed service to automate build, customize and deploy OS images ☆
-  **Recycle Bin**
Protect resources from accidental deletion ☆

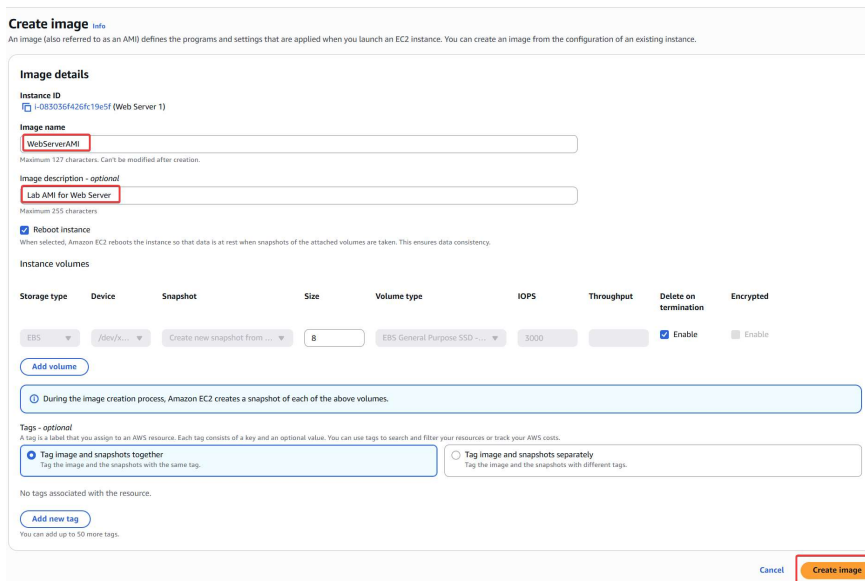
Features [Show more](#)

- EC2 Instances**
● CloudWatch feature
- EC2 Resource Health**
● CloudWatch feature

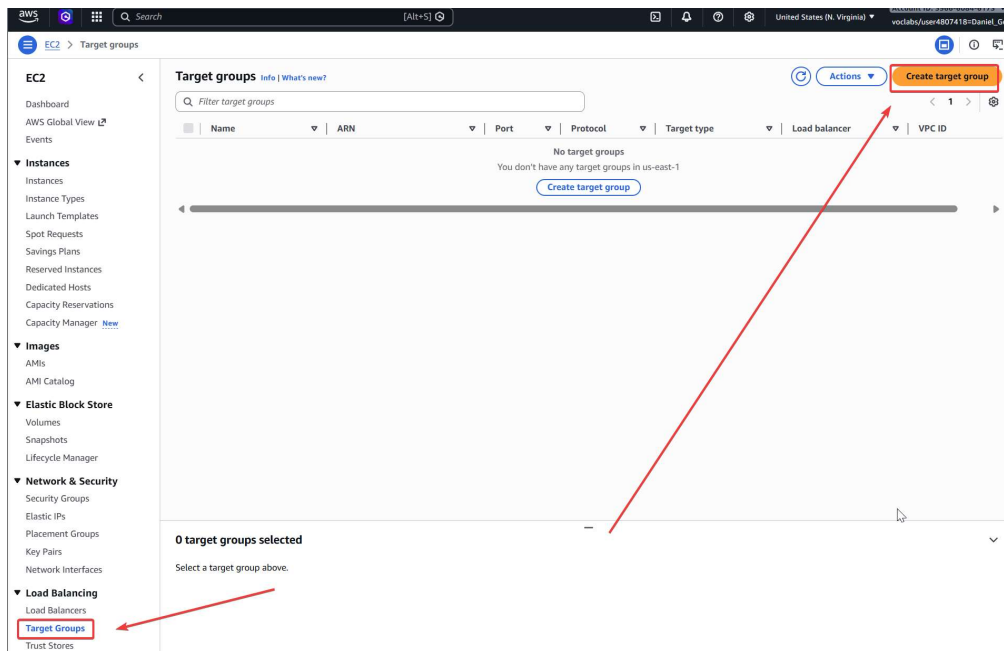
Go to the Instances tab using the left menu. Click Web Server 1, Actions > Images and templates > Create image



Name the image “WebServerAMI” and configure description “Lab AMI for Web Server”, then click Create Image



We now create a Load Balancer. In the left menu, go to the Target Groups tab. Then, click “Create target group”



Enter group name “LabGroup”; select Lab VPC. Then, click “Next” at bottom of the screen to proceed.

Step 1 **Create target group**

Step 2 - recommended Register targets

Step 3 Review and create

Create target group

A target group can be made up of one or more targets. Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Settings - immutable
Choose a target type and the load balancer and listener will route traffic to your target. These settings can't be modified after target group creation.

Target type
Indicate what resource type you want to target. Only the selected resource type can be registered to this target group.

- Instances**
Supports load balancing to instances in a VPC. Integrate with Auto Scaling Groups or ECS services for automatic management.
Suitable for: ALB | NLB | GWLB
- IP addresses**
Supports load balancing to VPC and on-premises resources. Facilitates routing to IP addresses and network interfaces on the same instance. Supports IPv6 targets.
Suitable for: ALB | NLB | GWLB
- Lambda function**
Supports load balancing to a single Lambda function. ALB required as traffic source.
Suitable for: ALB
- Application Load Balancer**
Allows use of static IP addresses and PrivateLink with an Application Load Balancer. NLB required as traffic source.
Suitable for: NLB

Target group name
Name must be unique per Region per AWS account.

Accepts: a-z, A-Z, 0-9, and hyphen (-). Can't begin or end with hyphen. 1-32 total characters; Count: 8/32

Protocol
Protocol for communication between the load balancer and targets.

Port
Port number where targets receive traffic. Can be overridden for individual targets during registration.

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.

10.0.0.0/16 [Create VPC](#)

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.
- gRPC**
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Click “Next” and skip the Register targets step, then click “Create target group”

EC2 > Target groups > Create target group

Step 1 Create target group

Step 2 - recommended Register targets

Step 3 **Review and create**

Review and create

Review your target group configuration before creating

Step 1: Target group details [Edit](#)

Target group details

Name LabGroup	Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1
VPC vpc-0e3d175806df201d1 ↗	IP address type IPv4		

Health check details

Health check protocol HTTP	Health check path /	Health check port traffic-port	Interval 30 seconds
Timeout 5 seconds	Healthy threshold 5	Unhealthy threshold 2	Success codes 200

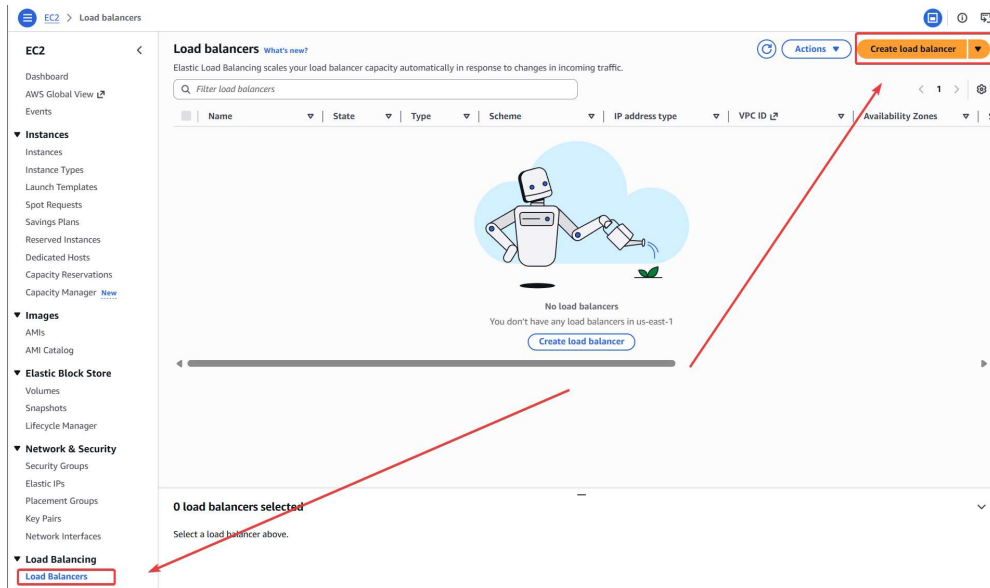
Step 2: Register targets [Edit](#)

Targets (0)

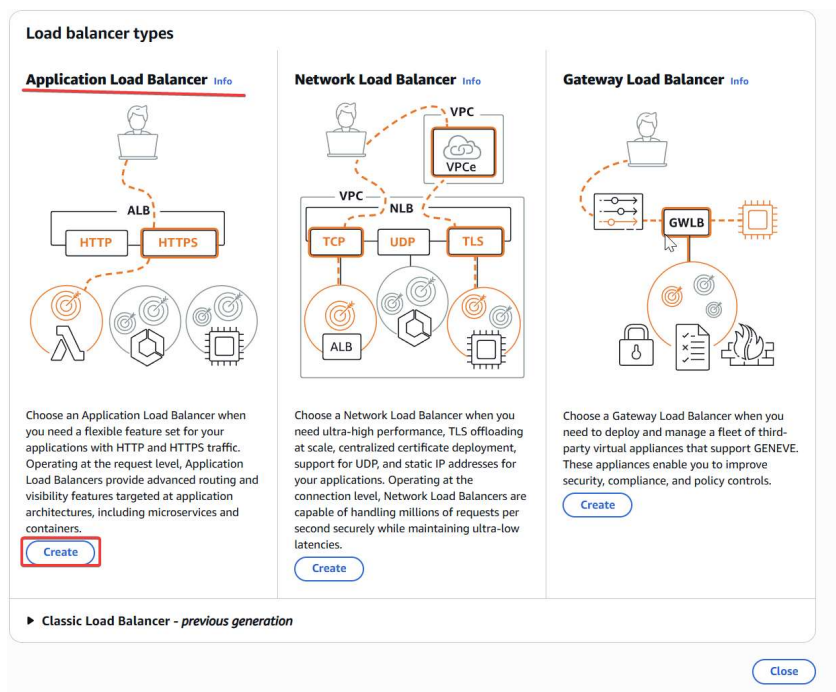
Instance ID	Name	Port	Zone
No targets added			

[Cancel](#) [Previous](#) [Create target group](#)

Now click the “Load Balancers” tab on the left sidebar, then click “Create load balancer”



Click Create under Application Load Balancer



Name the Load balancer “LabELB”, select Lab VPC, then select Public Subnet 1 and Public Subnet 2 under the two Availability zones

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.

LabELB

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

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type | Info
Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

IPv4
Includes only IPv4 addresses.

Dualstack
Includes IPv4 and IPv6 addresses.

Dualstack without public IPv4
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **Internet-facing** load balancers only.

Network mapping

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

VPC | Info
The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#).

vpc-0e3d175806df201d1 (Lab VPC)
10.0.0.0/16

[Create VPC](#)

IP pools | Info
You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view Pools in the [Amazon VPC IP Address Manager console](#).

Use IPAM pool for public IPv4 addresses
The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets | Info
Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

us-east-1a (use1-a2z)

Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-09d68f7f50518e54b (Public Subnet 1)
10.0.0.0/24

us-east-1b (use1-a24)

Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0ec6fa7e1d0a8e870 (Public Subnet 2)
10.0.2.0/24

Under Security groups, deselect Default and select Web Security Group; under “Target group” for Default action of forward to target groups, select LabGroup

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

Web Security Group (sg-0d7b53402882a13f6)

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 [Remove]

Protocol HTTP **Port** 80
1-65535

Default action | Info
The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Routing action

Forward to target groups Redirect to URL Return fixed response

Forward to target group | Info
Choose a target group and specify routing weight or [create target group](#).

Target group	Protocol	Weight	Percent
LabGroup Target type: Instance, IPv4 Target stickiness: OFF	HTTP	1 0-999	100%

[+ Add target group](#)
You can add up to 4 more target groups.

Target group stickiness | Info
Enables the load balancer to bind a user's session to a specific target group. To use stickiness the client must support cookies. If you want to bind a user's session to a specific target, turn on the Target Group attribute Stickiness.

Turn on target group stickiness

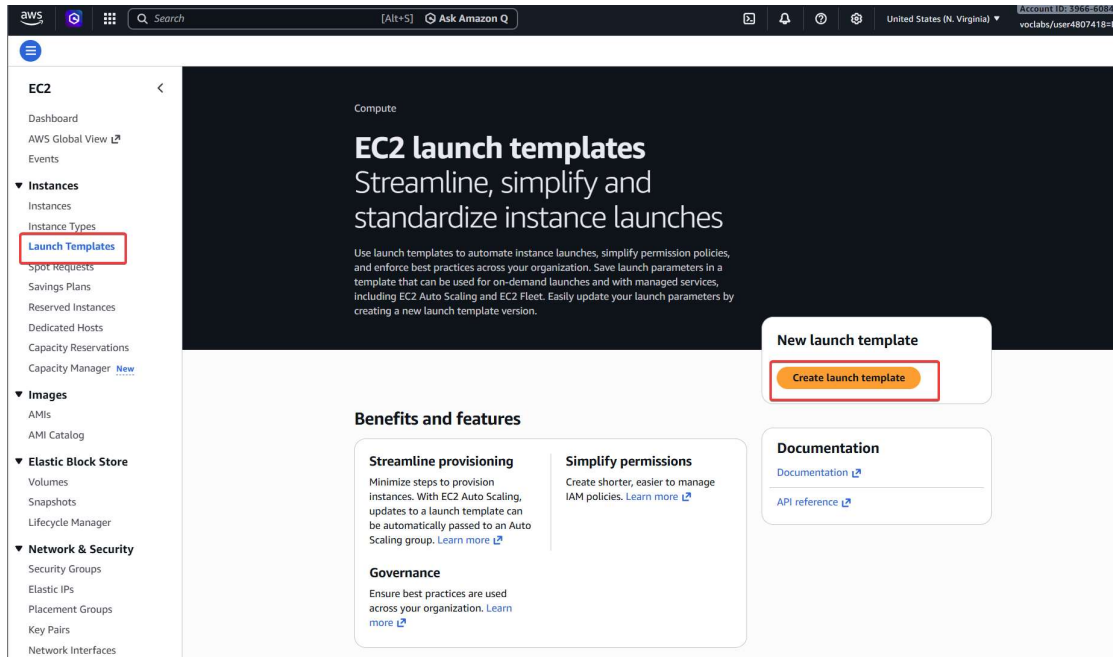
Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)
You can add up to 50 more tags.

Scroll to bottom and click Create load balancer

☑ **Successfully created load balancer: LabELB**
It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.

In the left menu, choose the Launch Templates tab. Then, click “Create launch template”



Name the template “LabConfig” and select Auto Scaling guidance

Launch template name and description

Launch template name - *required*

LabConfig

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**

▶ **Source template**

Select t2.micro for instance type, vockey for key pair name, and “Web Security Group” for security group

Instance type [Info](#) | [Get advice](#) Advanced

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0116 USD per Hour On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour

All generations [Compare instance types](#)

[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

vockey

[Create new key pair](#)

Network settings [Info](#)

Subnet [Info](#)

Don't include in launch template

[Create new subnet](#)

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

Availability Zone [Info](#)

Don't include in launch template

[Enable additional zones](#)

Not applicable for EC2 Auto Scaling

Firewall (security groups) [Info](#)

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

Select existing security group Create security group

Security groups [Info](#)

Select security groups

[Compare security group rules](#)

Web Security Group sg-0d7b53402882a13f6 ✕
VPC: vpc-0e3d175806df201d1

Advanced network configuration

Enable Detailed CloudWatch monitoring and Create Launch template

▼ Advanced details [Info](#)

IAM instance profile [Info](#)
 [Create new IAM profile](#)

Hostname type [Info](#)

DNS Hostname [Info](#)
 Enable resource-based IPv4 (A record) DNS requests
 Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery [Info](#)

Shutdown behavior [Info](#)

Not applicable for EC2 Auto Scaling

Stop - Hibernate behavior [Info](#)

Not applicable for Amazon EC2 Auto Scaling.

Termination protection [Info](#)

Stop protection [Info](#)

Detailed CloudWatch monitoring [Info](#)

Additional charges apply

Credit specification [Info](#)

▼ Summary

Software Image (AMI)
 Lab AMI for Web Server
 ami-0740b9d27dcaa130f

Virtual server type (instance type)
 t2.micro

Firewall (security group)
 Web Security Group

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance. Charges may apply depending on your account's free tier status.

[Cancel](#) [Create launch template](#)

Click LabConfig in the success message



Under Actions, click “Create Auto Scaling Group”

LabConfig (lt-04418448c00c38449) [Actions](#) [Delete template](#)

Launch template details

Launch template ID
lt-04418448c00c38449

Launch template name
LabConfig

Default version
1

[Details](#)
[Versions](#)
[Template tags](#)

Launch template version details

Version
1 (Default)

Description
-

Date created
2026-03-10T21:24:51.000Z

Created by
arn:aws:sts::396660846173:assumed-rol...=Daniel_Ge

[Actions](#) [Delete template version](#)

- Launch instance from template
- Modify template (Create new version)
- Delete template version
- Set default version
- Manage tags
- Create Spot Fleet
- Create Auto Scaling group

Name the group “Lab Auto Scaling Group”, then click “Next”

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.

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#)

i 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.

[Create a launch template](#)

Version

[Create a launch template version](#)

Description

-

Launch template

[LabConfig](#)
lt-04418448c00c38449

Instance type

t2.micro

AMI ID

ami-0740b9d27dcaa130f

Security groups

-

Request Spot Instances

No

Key pair name

vockey

Security group IDs

[sg-0d7b53402882a13f6](#)

Additional details

Storage (volumes)

-

Date created

Tue Mar 10 2026 14:24:51 GMT-0700 (Pacific Daylight Time)

[Cancel](#)

[Next](#)

Choose Lab VPC for VPC. Choose Private Subnet 1 and Private Subnet 2 for Availability Zones and subnets, then click Next.

The screenshot shows the 'Choose instance launch options' step in the AWS console. The left sidebar lists steps from 'Choose launch template' to 'Review'. The main content area is divided into three sections:

- Instance type requirements:** Includes a table with columns for Launch template, Version, and Description. The selected launch template is 'LabConfig' with ID 'lt-04418448c00c38449' and version 'Default'. The instance type is 't2.micro'. An 'Override launch template' button is present.
- Network:** Includes a 'VPC' dropdown menu with 'vpc-0e3d175806df201d1 (Lab VPC)' selected. Below it, an 'Availability Zones and subnets' dropdown menu shows two selected subnets: 'use1-az2 (us-east-1a) | subnet-0b7bb6429a4e704ba (Private Subnet 1)' and 'use1-az4 (us-east-1b) | subnet-0c8c5996657e6b51a (Private Subnet 2)'. A 'Create a VPC' link is visible below the VPC dropdown.
- Availability Zone distribution - new:** Two radio button options are shown: 'Balanced best effort' (selected) and 'Balanced only'.

At the bottom right, there are four buttons: 'Cancel', 'Skip to review', 'Previous', and 'Next'.

Choose “Attach to an existing load balancer” and select LabGroup as the target group. Click “Next” to continue

EC2 > Auto Scaling groups > Create Auto Scaling group

Use a load balancer to distribute network traffic across multiple servers. Enable service-to-service communications with VPC Lattice. Shift resources away from impaired Availability Zones with zonal shift. You can also customize health check replacements and monitoring.

Step 2: Choose instance launch options
 Step 3 - optional: Integrate with other services
 Step 4 - optional: Configure group size and scaling
 Step 5 - optional: Add notifications
 Step 6 - optional: Add tags
 Step 7: Review

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.

Select Load balancing options

- 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 to attach

- 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

LabGroup | HTTP
 Application Load Balancer: LabELB

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](#)

Application Recovery Controller (ARC) zonal shift - new Info
 During an Availability Zone impairment, target instance launches towards other healthy Availability Zones.

Enable zonal shift
 New instance launches will be retargeted towards healthy Availability Zones until the zonal shift is canceled.

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

EC2 health checks
 Always enabled

Additional health check types - optional Info

- Turn on Elastic Load Balancing health checks Recommended
Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.
- Turn on VPC Lattice health checks
VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.
- Turn on Amazon EBS health checks
EBS monitors whether an instance's root volume or attached volume stalls. When it reports an unhealthy volume, EC2 Auto Scaling can replace the instance on its next periodic health check.

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

300 seconds

Cancel Skip to review Previous **Next**

Make the following configurations

- Desired capacity: 2
- Min desired capacity: 2
- Max desired capacity: 6

Select "Target tracking scaling policy", name the policy "LabScalingPolicy", then set Metric type to Average CPU utilization with target value 60

Configure group size and scaling - optional [Info](#)

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

Group size [Info](#)

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances) ▼

Desired capacity

Specify your group size.

2

Scaling [Info](#)

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

2

Equal or less than desired capacity

Max desired capacity

6

Equal or greater than desired capacity

Automatic scaling - optional

Choose whether to use a target tracking policy [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies

Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling policy

Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

LabScalingPolicy

Metric type [Info](#)

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization ▼

Target value

60

Instance warmup [Info](#)

300

seconds

Disable scale in to create only a scale-out policy

Enable group metrics collection within CloudWatch, then click Next

Additional settings

Instance scale-in protection

If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

Enable instance scale-in protection

Monitoring [Info](#)

Enable group metrics collection within CloudWatch

Default instance warmup [Info](#)

The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

Enable default instance warmup

Auto Scaling group deletion protection - new [Info](#)

Configure how this Auto Scaling group can be deleted.

None (default)

The Auto Scaling group can be deleted.

Prevent force deletion

The Auto Scaling group cannot be force deleted. To delete the group, all instances must be detached or terminated, and all warm pools must be deleted.

Prevent all deletion

The Auto Scaling group cannot be deleted.

Cancel

Skip to review

Previous

Next

Click Next to skip Step 5, then click “Add tag” with Key “Name” and Value “Lab Instance” in Step 6. Click Next.

Add tags - optional [Info](#)

Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched.

i You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group. ✕

Tags (1)

Key

Value - optional

Tag new instances

Name

Lab Instance

Remove

Add tag

49 remaining

Cancel

Previous

Next

Review the configuration, then click “Create Auto Scaling group”

Take the action
Add or remove capacity units as required

Instances need
300 seconds to warm up before including in metric

Scale in
Enabled

Instance maintenance policy

Replacement behavior
No policy

Min healthy percentage
-

Max healthy percentage
-

Additional settings

Instance scale-in protection
Disabled

Monitoring
Enabled

Default instance warmup
Disabled

Auto Scaling group deletion protection
None (default)

Capacity Reservation preference

Preference
Default

Capacity Reservation IDs
-

Resource Groups
-

Step 5: Add notifications Edit

Notifications
No notifications

Step 6: Add tags Edit

Tags (1)

Key	Value	Tag new instances
Name	Lab Instance	Yes

[Preview code](#) Cancel Previous Create Auto Scaling group

Go to the Instances tab using the left menu to check there are now two instances named “Lab Instance” launched by Auto Scaling

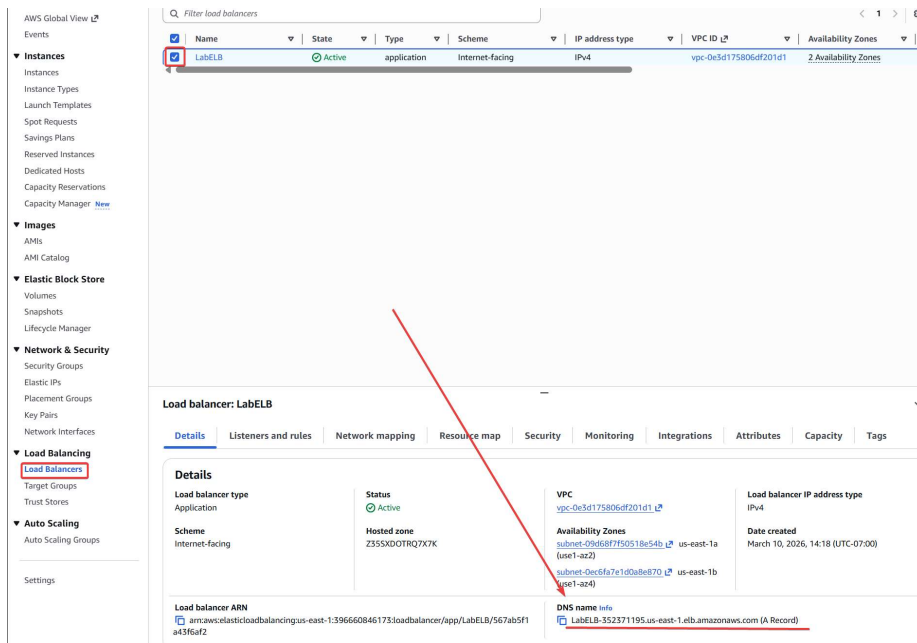
EC2 > Instances

EC2 < **Instances (4) Info** Connect Instance state Actions Launch instances

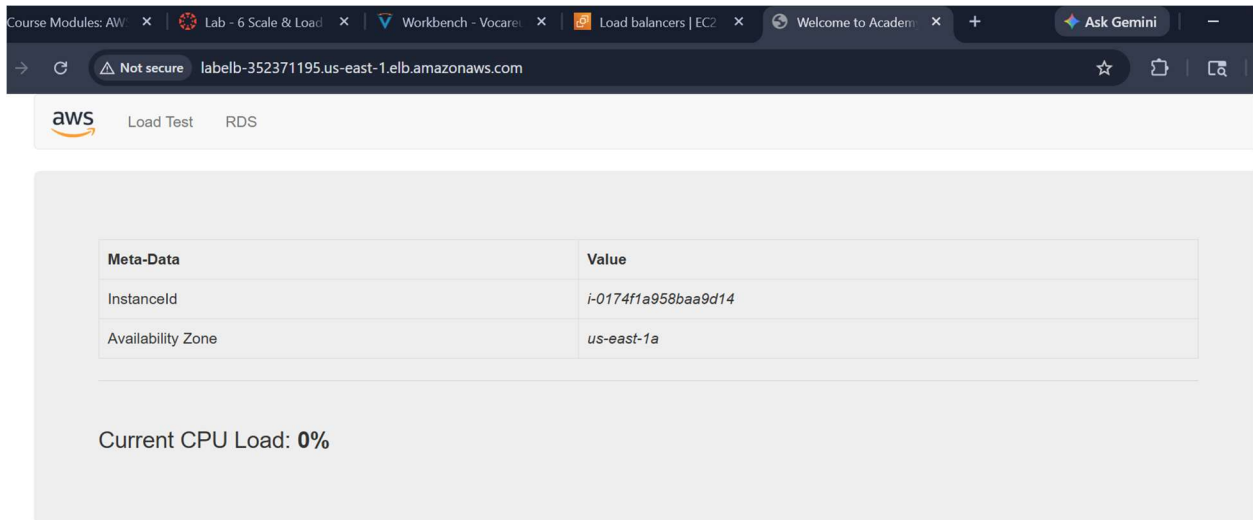
Find Instance by attribute or tag (case-sensitive) All states

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input type="checkbox"/>	Bastion Host	i-0fb34e8da8178ae78	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-
<input type="checkbox"/>	Web Server 1	i-083036f426fc19e5f	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-
<input type="checkbox"/>	Lab Instance	i-0174f1a958baa9d14	Running	t2.micro	Initializing	View alarms +	us-east-1a	-
<input type="checkbox"/>	Lab Instance	i-0925248acc5a03df2	Running	t2.micro	Initializing	View alarms +	us-east-1b	-

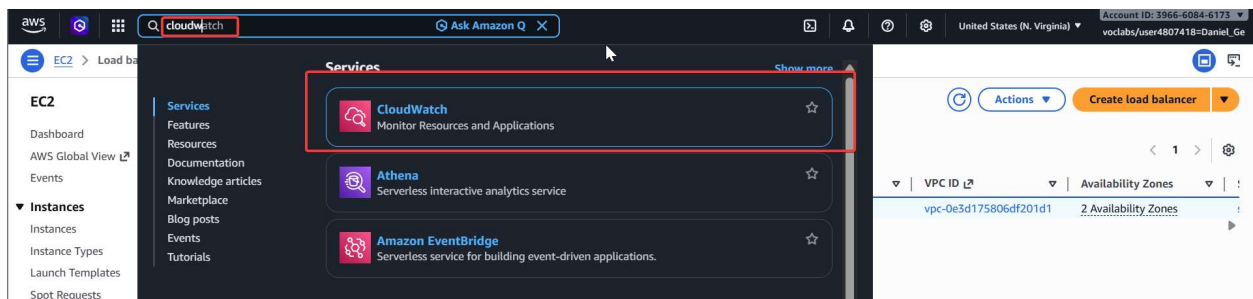
Select the Load Balancers tab on the left menu, then select the LabELB load balancer. Find and copy the DNS name



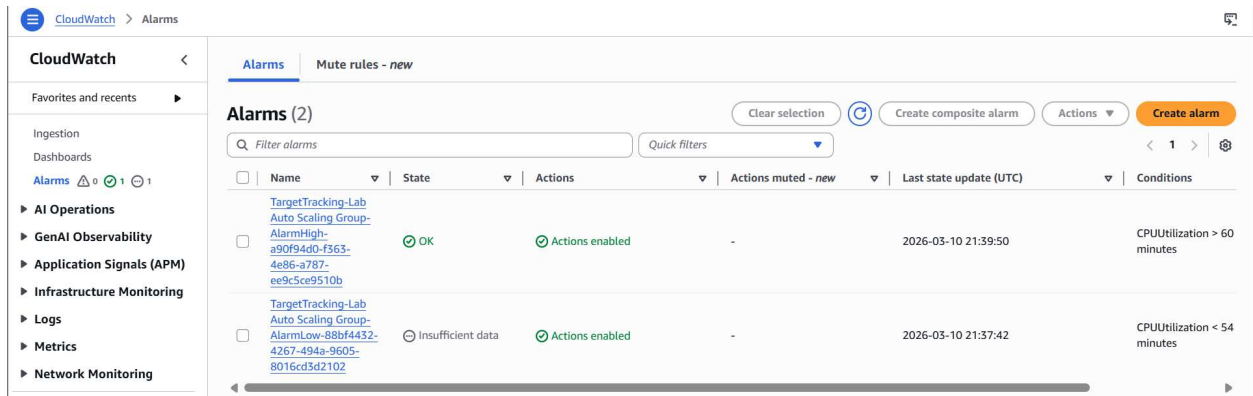
Paste the DNS name into a browser. It will display the CPU Load



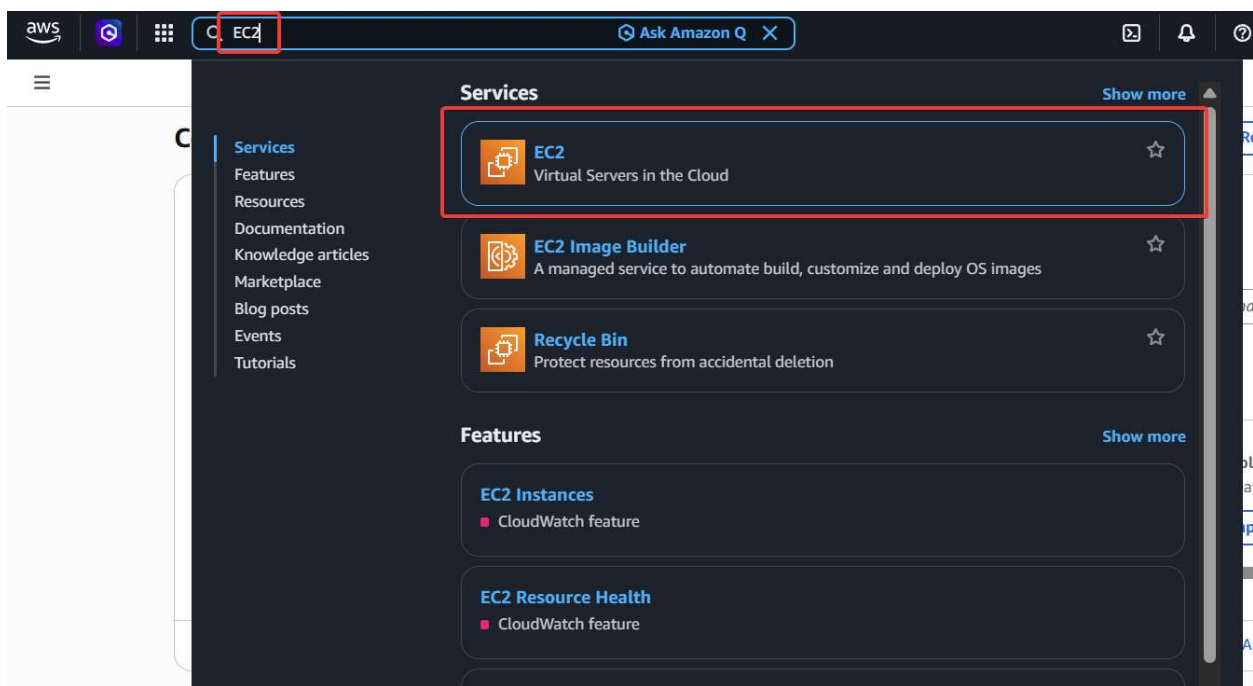
Using the search bar, go to "CloudWatch"



In the Alarms tab, we may find two alarms



Using the search bar, go to the EC2 Console



Go to the Auto Scaling Group, check the Lab Auto Scaling Group, and follow the steps below to edit the LabScalingPolicy

The screenshot shows the AWS Management Console interface for configuring an Auto Scaling group. The left-hand navigation pane has 'Auto Scaling Groups' highlighted with a red box and the number 1. The main content area shows a table of Auto Scaling groups with 'Lab Auto Scaling Group' selected, indicated by a red box and the number 2. Below the table, the 'Automatic scaling' tab is selected, marked with a red box and the number 3. The 'Dynamic scaling policies' section shows a policy named 'LabScalingPolicy' with its details expanded, highlighted by a red box and the number 4. An 'Actions' dropdown menu is open, with the 'Edit' option selected, highlighted by a red box and the number 6. The 'Target tracking scaling' policy type is visible, and the 'Target value' is set to 50.

Set the Target value to 50, then click “Update”

Edit dynamic scaling policy

Policy type

Target tracking scaling

Scaling policy name

LabScalingPolicy

Metric type | Info

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization

Target value

50

Instance warmup | Info

300 seconds

Disable scale in to create only a scale-out policy

Cancel
Update

Return to the CloudWatch alarms page and select the alarm displaying “OK”

Alarms (1/2)

Filter alarms Quick filters

Clear selection Create composite alarm Actions Create alarm

Name	State	Actions	Actions muted - new	Last state update (UTC)	Conditions
<input checked="" type="checkbox"/> TargetTracking-Lab Auto Scaling Group-AlarmHigh-2514c57b-8b3a-4d93-8e95-c357714c60623	OK	Actions enabled	-	2026-03-10 21:50:03	CPUUtilization > 50 minutes
<input type="checkbox"/> TargetTracking-Lab Auto Scaling Group-AlarmLow-7a816318-3756-49b6-aca5-c3fb41a424f9	Insufficient data	Actions enabled	-	2026-03-10 21:49:05	CPUUtilization < 45 minutes

Return to the web browser tab from earlier, then click “Load Test”

aws Load Test RDS

Meta-Data	Value
InstanceId	i-0174f1a958baa9d14
Availability Zone	us-east-1a

Current CPU Load: 0%

Return to the CloudWatch console tab and wait until the state change to “Alarm High”. We can see that additional instances are getting launched in response

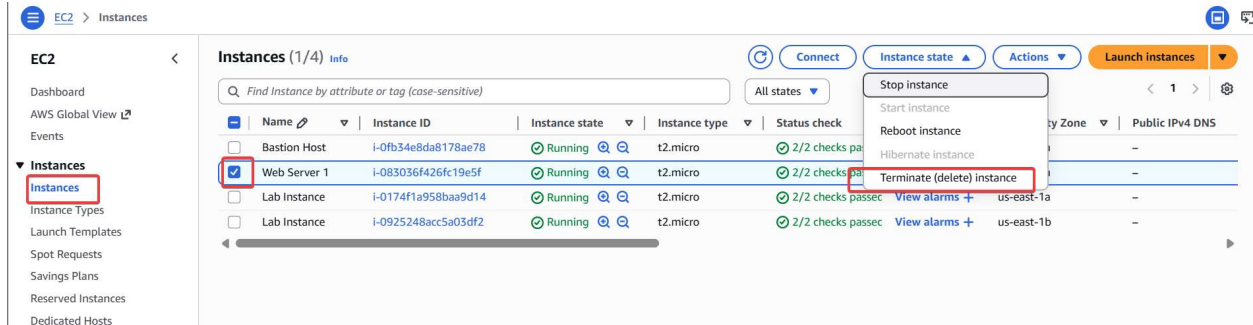
Alarms (1/2)

Filter alarms Quick filters

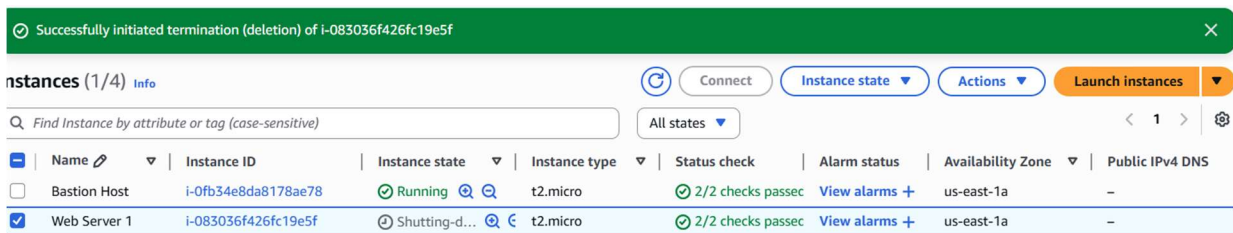
Clear selection Create composite alarm Actions Create alarm

Name	State	Actions	Actions muted - new	Last state update (UTC)	Conditions
<input checked="" type="checkbox"/> TargetTracking-Lab Auto Scaling Group-AlarmHigh-2514c57b-8b3a-4d93-8e95-c357714c60623	In alarm	Actions enabled	-	2026-03-10 21:56:03	CPUUtilization > 50 minutes
<input type="checkbox"/> TargetTracking-Lab Auto Scaling Group-AlarmLow-7a816318-3756-49b6-aca5-c3fb41a424f9	OK	Actions enabled	-	2026-03-10 21:53:26	CPUUtilization < 45 minutes

Return to the EC2 tab and go to Instances. Click Web Server 1, Instance state > Terminate



Choose Terminate to terminate the instance



Conclusion

Through completing the two parts of the Cloud Computing AWS mock activities, including 6 labs and 2 activities, we have experienced setting up different cloud computing solutions on AWS through a variety of AWS features. In the future, we are prepared to apply the AWS services appropriately through our training in the videos, then replicate these steps through our experience in the above labs.