



AWS Academy Cloud Foundations: Configuring Elastic Block Store, Relational Database Service, and Elastic Cloud Compute Auto Scaling

Colin J. Faletto, CCNA

Purpose

This write-up is intended to document and explain the fourth, fifth, and sixth in the AWS Academy Cloud Foundations course. These labs are intended to provide additional knowledge in the field of cloud computing, such as block-level file storage for virtual machines, basic relational database configuration, and automatic infrastructure scaling to meet user demand. These concepts are essential for new cloud engineers to provide parallels to more advanced facets of traditional IT. These labs also provide a strong foundation of knowledge for the AWS management console, as they all take place primarily inside this console.

Background

Amazon is a company based in Seattle that runs the biggest e-commerce platform in the world. They were started in 1994 by former CEO Jeff Bezos, and have grown from a small online bookstore to a giant online store offering a wide variety of products. Amazon also has a strong physical retail presence in the grocery space with their Amazon Fresh and Whole Foods chains, and has a strong online media presence through Twitch, Prime Video, and Amazon Music, which provide entertainment in the form of livestreams, movies and television shows, and music respectively. Amazon also has a popular line of e-readers and tablets with their Kindle brand and has a successful brand of artificial intelligence assistants with their Amazon Alexa A.I. and their Amazon Echo line of smart speakers.

Amazon Web Services, or AWS, is Amazon's cloud computing division. It was created in 2002 to provide simple web services to customers and expanded to cloud storage and computing in 2006. It is the leading cloud service provider and is popular for its pay-as-you-go service model. AWS provides services to everyone from small businesses to massive companies like Coca-Cola and Apple, and even provides web infrastructure to government branches. AWS takes the responsibility and cost of managing a data center out of the hands of businesses and maintains a massive global network of Amazon data centers that split customer traffic among them. AWS currently has 34 geographic regions, each of which have multiple availability zones which themselves contain multiple data centers. These data centers are in undisclosed locations for security reasons, though their general position is published. AWS offers services for virtual machines, cloud storage, database management, machine learning, IoT services, cloud networking, and much more.

Amazon Elastic Compute Cloud, or EC2, is an AWS service that allows customers to create virtual machines in the AWS cloud. These machines are very versatile, as they can be allocated as many or as few resources (CPU, RAM, GPU) as needed and can run nearly any operating system. By default, EC2 instances will run Amazon Linux, which is a version of Linux optimized for AWS servers. Amazon's e-commerce platform, its primary source of revenue, has been running on EC2 instances for over a decade. EC2 instances have a variety of different types, which are optimized for different purposes such as memory (R series, X series), compute (C series), and storage (H series, I series, D series).

Amazon Virtual Private Cloud, or VPC, is an AWS service that provides a virtual network inside the AWS cloud. This service allows AWS objects, such as EC2 instances, to communicate with each other. In a VPC, each EC2 machine is assigned a unique private IPv4 address, which is then connected via NAT to a public address on an internet gateway. Using this gateway, machines in the VPC can communicate with other AWS VPCs and other Internet-connected machines. Amazon VPC is provided at no additional charge to customers using EC2 instances.

Amazon Identity and Access Management, or IAM, is an AWS service that provides a layer of security to customers by limiting the resources different users can access. IAM follows the principle of least privilege, meaning that by default, all AWS controls are blocked for users unless they have been explicitly granted permissions. IAM represents a portion of the customer responsibilities in the AWS shared responsibility model, which is a model outlining that AWS is responsible for the physical security of data centers and networks while the customer is responsible for keeping their customer data and configurations safe. One of IAM's unique features is its role feature, which creates identities with elevated permissions that can be temporarily assigned to users. This feature works similarly to the "sudo" command in unix-based operating systems.

Amazon Elastic Block Store, or EBS, is an AWS service that allows virtual block-level storage to be attached to an EC2 instance. These drives can be formatted with any number of different file systems, such as ext3, ext4 (used with Linux), NTFS (used with Windows), and APFS (used with macOS). Depending on the partitioning scheme, EBS drives can be up to 16 tebibytes in size. EBS Volumes come as either solid-state or hard disk storage, with SSDs coming in high-performance IOPS and general-purpose GP variants, and HDDs coming in throughput-optimized (ST) and cold low-cost (SC) variants. EBS volumes are set up in a way that ensures redundancy, meaning that component failure in AWS data centers doesn't result in data loss for the customer.

A relational database is a type of database that stores information in terms of keys and values. A value is a specific data point that can be accessed by referencing its corresponding key. Relational databases can be divided further into any number of different tables. Amazon Relational Database Service, or RDS, is an AWS service that allows relational databases to be created and managed in the AWS cloud. RDS supports several database types, such as MySQL, Oracle Database, MariaDB, PostgreSQL, and Microsoft SQL Server. Amazon also offers their own database type, Aurora, which is compatible with MySQL and optimized for performance and availability. RDS databases can also be deployed across multiple availability zones, which can optionally create multiple instances of an RDS database in different locations.

AWS Elastic Load balancing, or ELB, is an AWS service that automatically balances traffic across multiple devices in the AWS cloud. It is often used in conjunction with EC2 instances. This service creates more consistency in how AWS resources are distributed, which ensures a more stable experience for end users.

AWS Auto Scaling is an AWS service that allows applications to automatically be created or deleted based on a variety of targets, such as CPU utilization or bandwidth. This service facilitates scalability of cloud computing services and adapts AWS

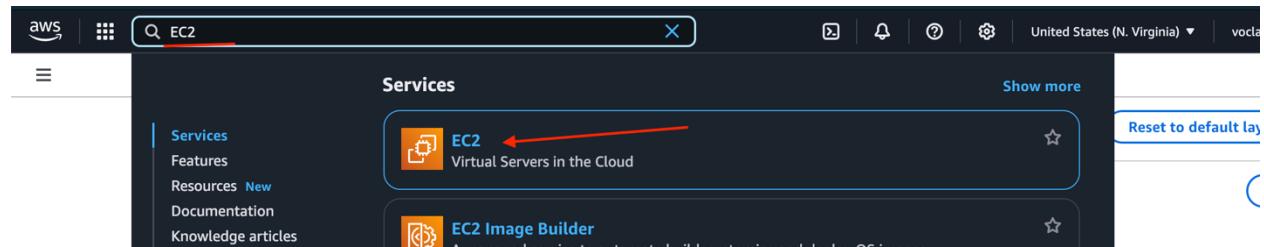
resources to better fit the needs of customers at any given time. This service is also economical for AWS users as it allows them to pay only for resources required for any given moment in time. Auto Scaling can automatically create and delete resources, EC2 instances, DynamoDB databases, and Aurora RDS databases.

Lab Summary

This write-up covers three different AWS labs. The first lab involves creating an EBS volume, attaching it to an EC2 instance, instantiating a new file system on the volume, then creating and restoring a snapshot of the volume. The second lab involves building and launching an RDS address book database, connecting it to a pre-existing web server, then manipulating the database with a web server GUI. The third lab involves creating a load balancer and auto scaling group based on an EC2 instance AMI, then testing the auto scaling feature by simulating excess CPU usage.

Lab Commands (EBS)

From the AWS search bar, type in and launch “EC2”.



From the Instances tab, make sure that the EC2 instance named “Lab” has been created. Make sure to write down the EC2 instance’s availability zone, which is “us-east-1a” in this case.

Instances (1/2) Info							
Name		Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	Lab	i-0efb740a27507c4d8	Running	t2.micro	0/2 checks passed	View alarms +	us-east-1a
<input type="checkbox"/>	Bastion Host	i-0b1eda8fc492c49d0	Running	t2.micro	0/2 checks passed	View alarms +	us-east-1a

Go to the “Volumes” section and click “Create Volume”.

The screenshot shows the AWS EBS Volumes page. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Events, Instances, Images, and Elastic Block Store. Under 'Elastic Block Store', 'Volumes' is selected. The main area displays a table of volumes with columns: Name, Volume ID, Type, Size, IOPS, Throughput, Snapshot ID, and Created. Two volumes are listed: 'vol-09102cbfa618ed794' (gp3, 8 GiB, 3000 IOPS, 125 Throughput, snap-07c32f..., 2025/01/14 15:28 GMT-8) and 'vol-0467495f93c918dc4' (gp3, 9 GiB, 3000 IOPS, 125 Throughput, snap-07c32f..., 2025/01/14 15:28 GMT-8). At the top right, there are 'Actions' and 'Create volume' buttons. A red arrow points from the text above to the 'Create volume' button.

Set the volume type to “gp2”, the size to 1 gigabyte, and the availability zone to the same zone as the Lab instance.

The screenshot shows the 'Create volume' configuration page. It includes fields for Volume type (General Purpose SSD (gp2)), Size (1 GiB), IOPS (100 / 3000), Throughput (Not applicable), Availability Zone (us-east-1a), and Snapshot ID (Don't create volume from a snapshot). There's also an Encryption section with an 'Encrypt this volume' checkbox. A red arrow points from the text above to the 'Add tag' button in the 'Tags - optional' section.

Under “Tags”, click “Add Tag”.

The screenshot shows the 'Tags - optional' section. It explains what tags are and provides a note about the number of tags. A red arrow points from the text above to the 'Add tag' button. Another red arrow points from the text above to the 'Add tag' button in the 'Tags - optional' section.

Set the key to “Name” and the value to “My Volume”.

Tags - optional Info

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/> X	<input type="text" value="My Volume"/> X
Add tag	

Click “Create Volume”.

Snapshot summary Info

⌚ Click refresh to view backup information
The volume type that you select and the tags that you assign determine whether the volume will be backed up by any Data Lifecycle Manager policies.

Cancel Create volume

You should now be redirected to the Volumes page. Click the checkbox next to My Volume, then under Actions, click Attach Volume.

The screenshot shows the AWS Volumes page with a green success message at the top: "Successfully created volume vol-04310c6ab006881e7." Below it is a table of volumes. The second row, "My Volume" (vol-04310c6ab006881e7), has a checked checkbox. A red arrow points to this checkbox. To the right, a context menu is open over the "Actions" button. The "Attach volume" option is highlighted with a red box and a red arrow pointing to it. Other options in the menu include Modify volume, Create snapshot, Create snapshot lifecycle policy, Delete volume, Detach volume, Force detach volume, Manage auto-enabled I/O, Manage tags, and Fault injection.

Set the instance to the Lab instance and the device name to /dev/sdf, then click Attach volume.

Basic details

Volume ID

Availability Zone
us-east-1a

Instance Info

Device name Info

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

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

Go to the “Instances” section, click the checkbox next to “Lab”, and click “Connect”.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with options like Dashboard, EC2 Global View, Events, Instances (with 'Instances' selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations. The main area is titled 'Instances (1/2) Info' and shows a table with two rows. The first row has a checked checkbox, the name 'Lab', instance ID 'i-0efb740a27507c4d8', state 'Running', type 't2.micro', status check '2/2 checks passed', alarm status 'View alarms +', availability zone 'us-east-1a', and public IP 'ec2-54-19'. The second row is for a 'Bastion Host' with similar details. At the top right, there are buttons for 'Connect', 'Instance state', 'Actions', and 'Launch instances'.

Select “EC2 instance connect”, select “Public IPv4 address”, then click “Connect”.

This screenshot shows the 'EC2 Instance Connect' configuration page. It has tabs for 'EC2 Instance Connect', 'Session Manager', 'SSH client', and 'EC2 serial console'. Under 'Connection Type', the 'Connect using EC2 Instance Connect' option is selected (radio button is checked). Below it, under 'Address', the 'Public IPv4 address' is selected and shows '54.197.37.249'. There's also an option for 'IPv6 address' which is not selected. In the 'Username' field, 'ec2-user' is entered. A note at the bottom says: 'Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' At the bottom right, there are 'Cancel' and 'Connect' buttons, with 'Connect' being highlighted by a red arrow.

Run the command `df -h` to list the mounted volumes; you should see output like this:

```

        #_
        ~\_ #####
        ~\_ #####\ Amazon Linux 2023
        ~~ \###|
        ~~ \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
        ~~ V~' '-->
        ~~~ /
        ~~~ ./
        /m/ /
[ec2-user@ip-10-1-11-198 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M    0   4.0M  0% /dev
tmpfs          475M    0   475M  0% /dev/shm
tmpfs          190M  452K  190M  1% /run
/dev/xvda1      8.0G  1.6G  6.4G 20% /
tmpfs          475M    0   475M  0% /tmp
/dev/xvda128    10M  1.3M  8.7M 13% /boot/efi
tmpfs          95M    0   95M  0% /run/user/1000

```

Run the command `sudo mkfs -t ext3 /dev/sdf` to create an ext3 file system on the volume you created.

```
[ec2-user@ip-10-1-11-198 ~]$ sudo mkfs -t ext3 /dev/sdf
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 262144 4k blocks and 65536 inodes
Filesystem UUID: d545580a-928e-4063-ad5d-bda7ee246ba3
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
```

Run the command `sudo mkdir /mnt/data-store` to create a new folder at `/mnt/data-store`.

```
[ec2-user@ip-10-1-11-198 ~]$ sudo mkdir /mnt/data-store
```

Run the command `sudo mount /dev/sdf /mnt/data-store` to mount your volume at the created folder.

```
[ec2-user@ip-10-1-11-198 ~]$ sudo mount /dev/sdf /mnt/data-store
```

Run the command `echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab` to add this mount binding to `/etc/fstab`, a file that automatically mounts volumes at startup.

```
[ec2-user@ip-10-1-11-198 ~]$ echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab
```

Run the command `cat /etc/fstab` to confirm that the line was added.

```
[ec2-user@ip-10-1-11-198 ~]$ cat /etc/fstab
#
UUID=73e034f4-2887-4ec9-8b40-0d35c0091a37   /
UUID=9F37-3C35       /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
```

Run the command `sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"` to create a file with the text “some text has been written” at the specified location.

```
[ec2-user@ip-10-1-11-50 ~]$ sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
```

Run the command `cat /mnt/data-store/file.txt` to confirm that the file was written.

```
[ec2-user@ip-10-1-11-50 ~]$ cat /mnt/data-store/file.txt
some text has been written
```

Go back to the main AWS console tab. Under Volumes, check My Volume, then click Actions > Create Snapshot.

The screenshot shows the AWS Lambda console with a success message: "Successfully attached volume vol-0918321c092d50b99 to instance i-0e35f74c96c3fce5". Below it is a table of volumes. A red arrow points to the "Actions" menu for the selected volume "My Volume".

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Created	Availability Zone	Status
vol-0918321c092d50b99	gp3	9 GiB	3000	125	snap-055e2a...	2025/01/16 13:55 GMT-8	us-east-1a	In-use	
vol-0938cb0354483571	gp3	8 GiB	3000	125	snap-055e2a...	2025/01/16 13:55 GMT-8	us-east-1a	In-use	
My Volume	vol-0918321c092d50b99	gp2	1 GiB	100	-	-	2025/01/16 13:56 GMT-8	us-east-1a	In-use

Under Tags, click Add Tag, set the key to Name, set the value to My Snapshot, then click Create Snapshot.

Create snapshot info

Create a point-in-time snapshot to back up the data on an Amazon EBS volume to Amazon S3.

Source volume

Volume ID: vol-0918321c092d50b99 (My Volume) Availability Zone: us-east-1a

Snapshot details

Description: Add a description for your snapshot

Encryption Info: Not encrypted

Tags Info

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Q Name	Value - optional: Q My Snapshot	Remove
-------------	---------------------------------	--------

Add tag

You can add 49 more tags.

Cancel Create snapshot

Switch back to the console and run the command `sudo rm /mnt/data-store/file.txt` to remove the file you created earlier.

```
[ec2-user@ip-10-1-11-50 ~]$ sudo rm /mnt/data-store/file.txt
```

Run the command `ls /mnt/data-store` to confirm that the file has been deleted.

```
[ec2-user@ip-10-1-11-50 ~]$ ls /mnt/data-store
lost+found      no mention of file.txt
```

Back in the AWS console, go to Snapshots > Check My Snapshot > Actions > Create volume from snapshot.

Snapshots (1 / 1) Info

Name	Snapshot ID	Volume size	Description	Storage tier	Snapshot status	Started	Progress	Encrypted
<input checked="" type="checkbox"/> My Snapshot	snap-08d374bc52f3d4244	1 GiB	-	Standard	Completed	2025/01/16 14:09 GMT-8	100%	No

Snapshot ID: snap-08d374bc52f3d4244 (My Snapshot)

Details Snapshot settings Storage tier Tags

Snapshot ID <input checked="" type="checkbox"/> snap-08d374bc52f3d4244 (My Snapshot)	Progress 100%	Snapshot status Completed	Owner 652055526343
Started <input checked="" type="checkbox"/> Thu Jan 16 2025 14:09:20 GMT-0800 (Pacific Standard Time)	Product codes	Fast snapshot restore	Description
Source volume <input checked="" type="checkbox"/> Volume ID vol-0918321d092d50b99	Volume size <input checked="" type="checkbox"/> 1 GiB	KMS key alias	KMS key ARN
Encryption Not encrypted	KMS key ID		

Set the volume type to gp2 (everything else should be correct by default), then click Add Tag, set the key to Name, set the value to Restored Volume, then click Create Volume.

Volume settings

Snapshot ID
 snap-08d374bc52f3d4244 (My Snapshot)

Volume type [Info](#)
 General Purpose SSD (gp2)

Size (GiB) [Info](#)

Min: 1 GiB, Max: 16384 GiB.

IOPS [Info](#)
100 / 3000
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) [Info](#)
Not applicable

Availability Zone [Info](#)
 us-east-1a

Fast snapshot restore [Info](#)
Not enabled for selected snapshot

Encryption
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
 Encrypt this volume

Tags - optional [Info](#)
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key <input type="text" value="Name"/>	Value - optional <input type="text" value="Restored Volume"/>	Remove
---	---	------------------------

[Add tag](#) 

You can add 49 more tags.

Snapshot summary

[Click refresh to view backup information](#)
The volume type that you select and the tags that you assign determine whether the volume will be backed up by any Data Lifecycle Manager policies.

 [Create volume](#)

Under Volumes, check Restored Volume, then click Actions > Attach Volume

Volumes (1/4) Info

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Created	Availability Zone	Volume state
- Restored Volu...	vol-05032b41f7ecaa218	gp2	1 GiB	100	-	snap-055e2a2...	2025/01/16 13:55 GMT-8	us-east-1a	In-use
-	vol-0f38dbd354483571	gp3	8 GiB	3000	125	snap-066574b...	2025/01/16 14:19 GMT-8	us-east-1a	In-use
My Volume	vol-0918321c092d50b99	gp2	1 GiB	100	-		2025/01/16 13:56 GMT-8	us-east-1a	In-use

Volume ID: vol-05032b41f7ecaa218 (Restored Volume)

Details Status checks Monitoring Tags

Volume ID <input type="checkbox"/> vol-05032b41f7ecaa218 (Restored Volume)	Size <input type="checkbox"/> 1 GiB	Type gp2	Volume status Okay
Volume state <input type="checkbox"/> Available	IOPS 100	Throughput	Multi-Attach enabled No
AWS Compute Optimizer finding <input type="checkbox"/> Opt-in to AWS Compute Optimizer for recommendations. [Learn more]	Availability Zone us-east-1a	Outposts ARN	Operator
Fast snapshot restored No	Attached resources	Created <input type="checkbox"/> Thu Jan 16 2025 14:19:47 GMT-0800 (Pacific Standard Time)	
Instance <input type="checkbox"/> i-0e3f74c96c3f8ce5 (Lab) (running)	Only instances in the same Availability Zone as the selected volume are displayed.	Device name <input type="checkbox"/> /dev/sdg	Recommended device names for Linux: /dev/xvda for root volume. /dev/sdf-f-p for data volumes.
<small> ⓘ 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.</small>			

Set the instance to Lab, the device name to /dev/sdg, then click Attach Volume.

Basic details

Volume ID
 vol-05032b41f7ecaa218 (Restored Volume)

Availability Zone
us-east-1a

Instance
 i-0e3f74c96c3f8ce5
(Lab) (running)

Device name
 /dev/sdg

Attach volume

Run the command `sudo mkdir /mnt/data-store2` to make a new folder for the restored drive.

```
[ec2-user@ip-10-1-11-50 ~]$ sudo mkdir /mnt/data-store2
```

Run the command `sudo mount /dev/sdg /mnt/data-store2` to mount the restored volume at the specified point.

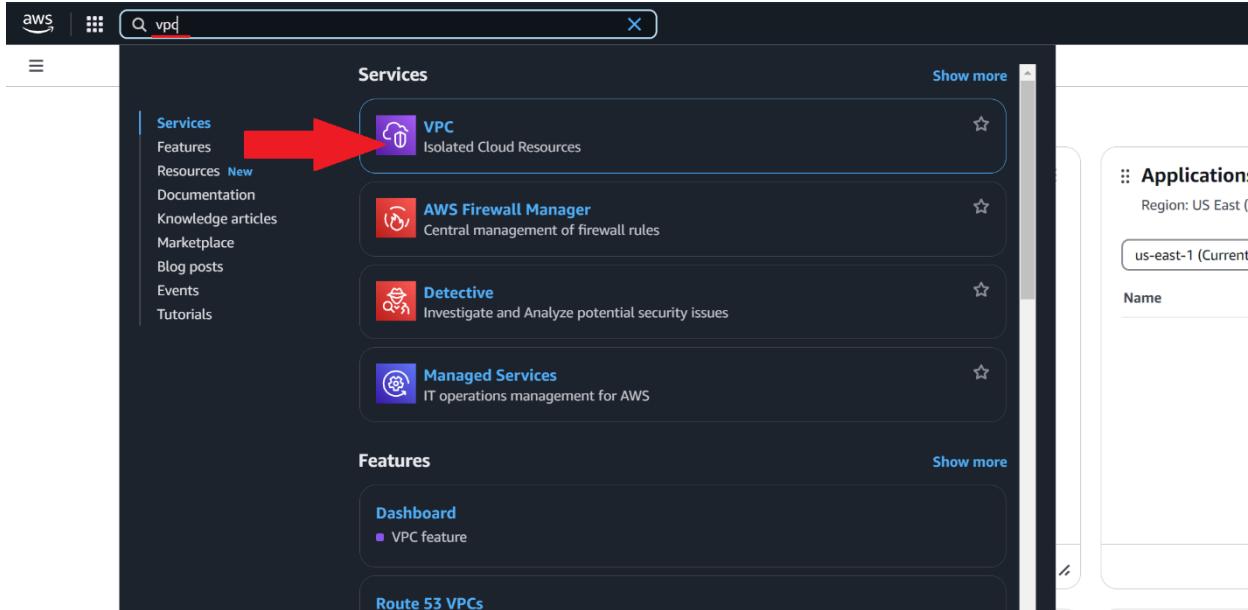
```
[ec2-user@ip-10-1-11-50 ~]$ sudo mount /dev/sdg /mnt/data-store2
```

Run the command `ls /mnt/data-store2/` and ensure that file.txt shows up.

```
[ec2-user@ip-10-1-11-50 ~]$ ls /mnt/data-store2/
file.txt  lost+found
```

Lab Commands (RDS)

From the AWS console search bar, open VPC.



Under Security Groups, click Create Security Group.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rule
-	sg-0fd8bbab053d23d8c	default	vpc-098128e46d33ebc0	default VPC security group	744374891789	1 Permission
Web Security Group	sg-0ae82613fc2f6f787	Web Security Group	vpc-0a8128e46d33ebc0	Enable HTTP access	744374891789	2 Permission
-	sg-0f6a240a72509b331	default	vpc-0ac143cc74bcb0b4	default VPC security group	744374891789	1 Permission
-	sg-022d95aa077ba8fb	WorkEc2SecurityGroup	vpc-0ccad45ce74beddd9	VPC Security Group	744374891789	1 Permission
-	sg-01b248194ab8a7c52	default	vpc-08942d36a0de6cd2	default VPC security group	744374891789	1 Permission

Set the name to DB Security Group, the description to Permit access from Web Security Group, and the VPC to Lab VPC. Under Inbound Rules, click Add Rule, set the type to MySQL/Aurora, and set the source to the Web Security Group. Click Create security group.

Basic details

Security group name [Info](#)
DB Security Group
Name cannot be edited after creation.

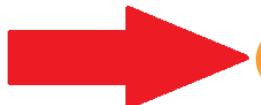
Description [Info](#)
Permit access from Web Security Group

VPC [Info](#)
vpc-0a98128e46d33ebc0 (Lab VPC)

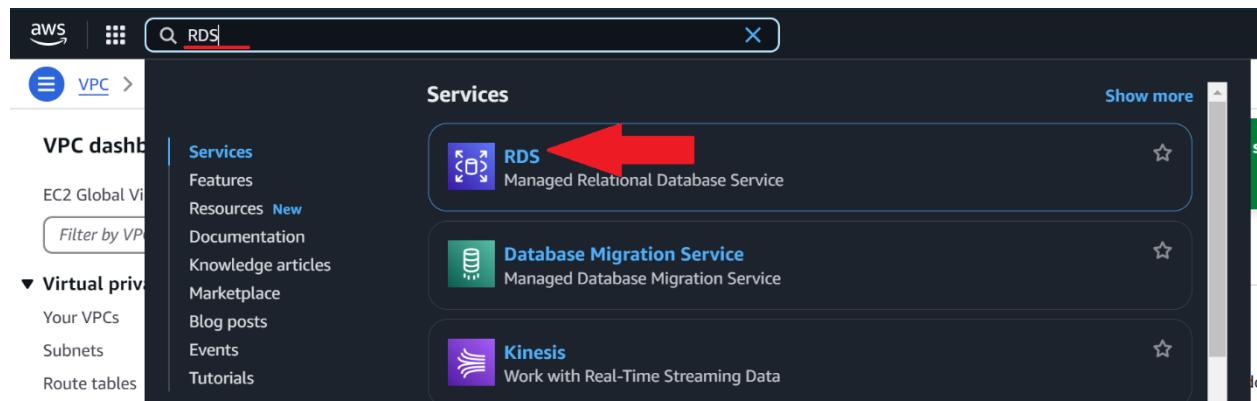
Inbound rules [Info](#)

Type	Protocol	Port range	Source	Description - optional
MySQL/Aurora	TCP	3306	Custom	Q sg-0a8263c6e2f6fe79 X sg-0a8263c6e2f6fe797 X Web Security Group

[Add rule](#) 

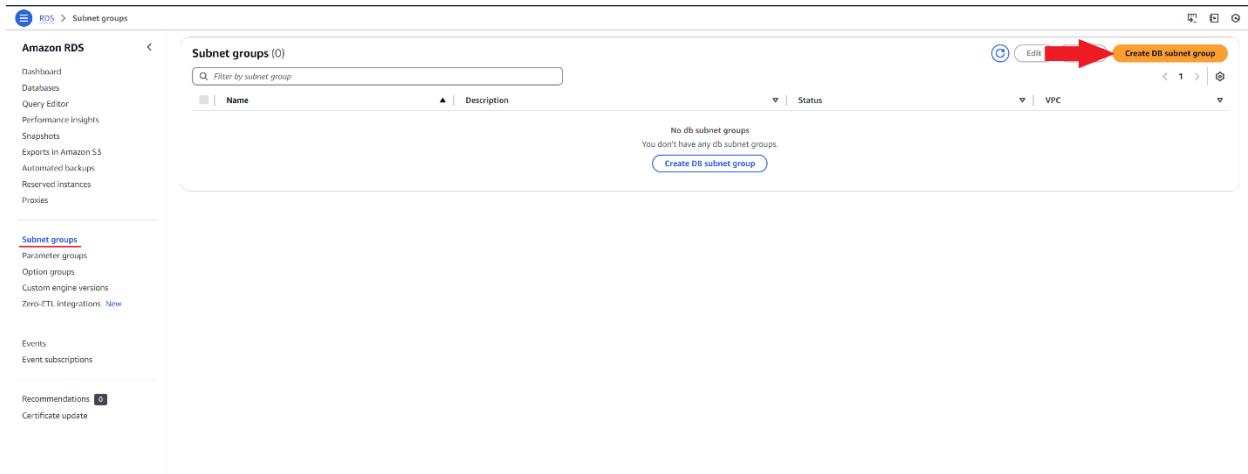
 **Create security group**

Go to RDS from the search bar.



The screenshot shows the AWS CloudSearch interface. In the top navigation bar, the search bar contains the text "RDS". Below the search bar, the "Services" section is displayed, featuring several service cards. The "RDS" card, which includes the text "Managed Relational Database Service", is highlighted with a large red arrow pointing to it. Other visible services include "Database Migration Service" and "Kinesis". On the left side, there is a sidebar with links for "VPC dashboard", "Virtual private clouds", and other AWS services.

Go to Subnet groups > Create DB Subnet Group.



Set the name to DB-Subnet-Group, the description to DB Subnet Group, and the VPC to Lab VPC. Set the availability zones to us-east-1a and us-east-1b, and set the subnets to Private Subnet 1 and Private Subnet 2. Click Create.

Subnet group details

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

Description

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.

Add subnets

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

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

Private Subnet 2	X
Subnet ID: subnet-0b6d2f04e4b4ef8b2	CIDR: 10.0.3.0/24
Private Subnet 1	X
Subnet ID: subnet-089f0ad02ef871ca8	CIDR: 10.0.1.0/24

(i) 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-1b	Private Subnet 2	subnet-0b6d2f04e4b4ef8b2	10.0.3.0/24
us-east-1a	Private Subnet 1	subnet-089f0ad02ef871ca8	10.0.1.0/24

Go to Databases > Create Database.

Successfully created DB-Subnet-Group. View subnet group

Databases (0)

Create database

Set the engine type to MySQL.

Engine options

Engine type [Info](#)

- Aurora (MySQL Compatible)
- Aurora (PostgreSQL Compatible)
- MySQL
- PostgreSQL

Set the template to Dev/Test.

Templates

Choose a sample template to meet your use case.

- Production
Use defaults for high availability and fast, consistent performance.
- Dev/Test
This instance is intended for development use outside of a production environment.
- Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

Set the deployment options to Multi-AZ DB instance.

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

- Multi-AZ DB Cluster
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.
- Multi-AZ DB instance
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- Single DB instance
Creates a single DB instance with no standby DB instances.

Set the DB instance identifier to lab-db, the master username to main, the credentials management to self-managed, and 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.
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.
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 let RDS generate one for you and manage it.

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

Master password [Info](#)
Password strength: **Neutral**
Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / \ ^ @

Confirm master password [Info](#)



Under Instance configuration, set the instance class to Burstable classes, and select db.t3.micro.

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)

db.t3.micro
2 vCPUs 1 GiB RAM Network: Up to 2,085 Mbps



Under storage, set the storage type to General Purpose SSD and the allocated storage to 20 GiB.

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](#)
 GiB
Minimum: 20 GiB, Maximum: 6,144 GiB

Provisioned IOPS [Info](#)
3000 IOPS

Storage throughput [Info](#)
125 MiBps

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

Additional storage configuration

Under connectivity, set the VPC to Lab VPC and set the existing security groups to 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-098128e46d35ebc0)
4 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

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 [X](#)

Under monitoring, disable Enhanced monitoring.

Monitoring

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

Under additional configuration, set the initial database name to lab, and disable automated backups and encryption.

▼ 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.mysql8.0

Option group [Info](#)
default:mysql-8.0

Backup
 Enable automated backups
Creates a point-in-time snapshot of your database

Encryption
 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.

ⓘ You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

 **Create database**

Click on lab-db.

	DB identifier	Status	Role	Engine
	lab-db	Creating	Instance	MySQL Co

Wait until the status says Modifying or Available

Scroll down to the Connectivity and security section and copy the Endpoint value.

Connect to the Lab's web server IP, and click on RDS.

Paste the endpoint URL, and enter the database name, username, and password from earlier.

If done correctly, you should see an address book database. Click “Remove” to remove an entry.

Address Book

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

You should see a message saying that the entry has been removed. Next, click the “Edit” button next to the remaining entry.

Address Book

Entry has been removed

Last name	First name	Phone	Email	Admin
Add Contact				
Doe	Jane	010-110-1101	janed@someotheraddress.org	Edit Remove



Change the details of the entry and click “Submit”.

Address Book

Edit Contact

Last name:

First name:

Phone:

Email:



Last name	First name	Phone	Email	Admin
Add Contact				
Doe	Jane	010-110-1101	janed@someotheraddress.org	Edit Remove

You should see a success message. Click “Add contact” to add a new contact.

Address Book

Data Updated!

Last name	First name	Phone	Email	Admin
Mason	Jeffrey	010-110-1101	janed@someotheraddress.org	Edit Remove

Add some information for the new contact and click “Submit”.

Address Book

Add Contact

Last Name: Hansen

First Name: Michael

Phone: 4254561111

Email: realemail@email.com

Submit

Last name	First name	Phone	Email	Admin
Mason	Jeffrey	010-110-1101	janed@someotheraddress.org	Edit Remove

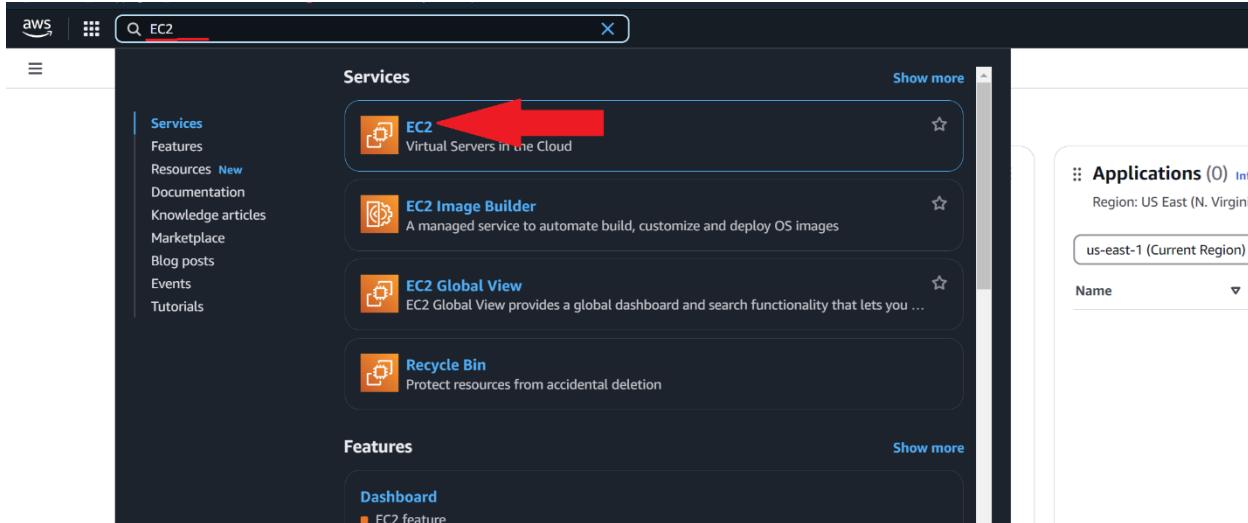
You should see both your newly created and newly modified entry in the address book.

Address Book

Last name	First name	Phone	Email	Admin
Hansen	Michael	4254561111	realemail@email.com	Edit Remove
Mason	Jeffrey	010-110-1101	janed@someotheraddress.org	Edit Remove

Lab Commands (Auto Scaling)

Go to the AWS management console and select “EC2”.



Go to Instances, ensure that Web Server 1's status is 2/2 checks passed, then click on the checkbox next to the web server and click Actions > Image and Templates > Create Image.

The screenshot shows the AWS Instances page. On the left, there's a sidebar with 'Instances' selected. In the main area, a table lists two instances: 'Bastion Host' and 'Web Server 1'. A red arrow points to the checkbox next to 'Web Server 1'. To the right, under the 'Actions' dropdown menu, a sub-menu is open with a red arrow pointing to the 'Create image' option. The 'Create image' option is highlighted with a yellow box.

Set the image name to WebServerAMI and the image description to Lab AMI for Web Server, then click Create image.

The screenshot shows the 'Create Image' configuration dialog. It includes fields for 'Instance ID' (i-0ae9535acc8323e8d), 'Image name' (WebServerAMI), 'Image description - optional' (Lab AMI for Web Server), and a 'Reboot instance' checkbox. Under 'Instance volumes', there's a table with columns for Storage type, Device, Snapshot, Size, Volume type, IOPS, Throughput, Delete on termination, and Encrypted. A note says 'During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.' At the bottom, there are sections for 'Tags - optional' (with options for 'Tag image and snapshots together' and 'Tag image and snapshots separately') and a 'Create image' button highlighted with a red arrow.

Go to Target Groups > Create target group.

The screenshot shows the AWS EC2 Target Groups page. On the left, there's a navigation sidebar with various EC2-related options like Dashboard, EC2 Global View, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. Under Load Balancing, 'Target Groups' is selected and highlighted with a red arrow. At the top right, there's a 'Create target group' button. Below it, a message says 'No target groups' and 'You don't have any target groups in us-east-1'. There's also a 'Create target group' link.

Set the target type to Instances and the target group name to LabGroup.

The screenshot shows the 'Basic configuration' step of the 'Create target group' wizard. It has a heading 'Basic configuration' and a note 'Settings in this section can't be changed after the target group is created.' Below this, there's a section titled 'Choose a target type' with four options: 'Instances' (selected), 'IP addresses', 'Lambda function', and 'Application Load Balancer'. Each option has a list of benefits. At the bottom, there's a 'Target group name' field containing 'LabGroup' and a note about character restrictions.

Set the VPC to Lab VPC, then click Next.

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.

Lab VPC
vpc-0000000000000000
IPv4 VPC CIDR: 10.0.0.0/16

Protocol

- 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.

Health checks
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol
 HTTP

Health check path
Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.

Up to 1024 characters allowed.

Advanced health check settings

Attributes
Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

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

 **Next**

Click “Create target group”.

Review targets

Targets (0)

Show only pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
No instances added yet Specify instances above, or leave the group empty if you prefer to add targets later.								

0 pending

 **Create target group**

Go to Load Balancers > Create load balancer.

EC2 > Load balancers

Load balancers
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
No load balancers You don't have any load balancers in us-east-1						

Create load balancer

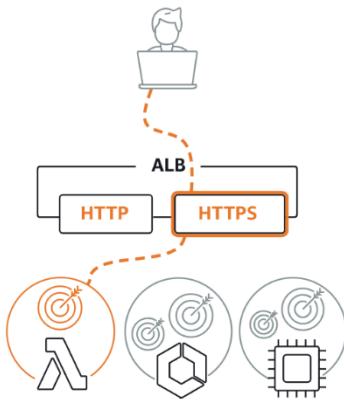
0 load balancers selected
Select a load balancer above.

 **Create load balancer**

Under Application Load Balancer, click Create.

Load balancer types

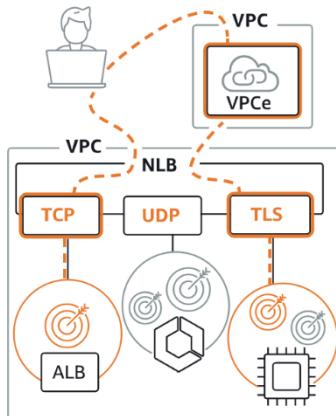
Application Load Balancer [Info](#)



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

[Create](#)

Network Load Balancer [Info](#)



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

[Create](#)

Gateway Load Balancer [Info](#)



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

[Create](#)

Under Basic configuration, set the load balancer name to LabELB.

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.

Under Network mapping, set the VPC to Lab VPC, check both availability zones, and set them to Public Subnets 1 and 2 respectively.

Network mapping [Info](#)

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](#). For a new VPC, create a VPC.

Lab VPC
vpc-008b28f7a7c4a4266
IPv4 CIDR: 10.0.0.0/16



Mappings [Info](#)

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

Availability Zones

us-east-1a (use1-az2)

Subnet

subnet-0168f37adddecfa2b0
IPv4 subnet CIDR: 10.0.0.0/24

Public Subnet 1



IPV4 address

Assigned by AWS

us-east-1b (use1-az4)

Subnet

subnet-09ee7b908570d1175
IPv4 subnet CIDR: 10.0.2.0/24

Public Subnet 2



IPV6 address

Assigned by AWS

Under Security groups, select Web Security Group and unselect default.

The screenshot shows the AWS Security Groups page. At the top, it says "Select up to 5 security groups". Below is a search bar with a magnifying glass icon. A list of security groups is shown, with one group highlighted in blue:

- ~~Default~~ sg-00fbf0c02422c58c9 VPC: vpc-008b28f7a7c4a4266
- DB Security Group sg-0464bf7e75572f3ec VPC: vpc-008b28f7a7c4a4266
- Web Security Group** sg-06dc1ae2846dc7037 VPC: vpc-008b28f7a7c4a4266
- c138865a355074919004965t1w110584150310-BastionSecurityGroup-nEzkE28fhoGv sg-088aaad175bb951f5 VPC: vpc-008b28f7a7c4a4266

Under Listeners and routing, set the default action to LabGroup

The screenshot shows the AWS Listeners and routing configuration page. It displays a single listener entry:

Protocol	Port	Default action
HTTP	80	Forward to LabGroup (Info) Target type: Instance, IPv4

Below the table, there are sections for "Listener tags - optional" and a "Create target group" button.

Click Create load balancer.

The screenshot shows the "Creation workflow and status" section of the AWS Create load balancer page. It includes a "Server-side tasks and status" table:

Task	Status
After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.	Not Started

A large red arrow points to the "Create load balancer" button at the bottom right of the screen.

Go to Launch Templates > Create launch template.

The screenshot shows the AWS EC2 Launch Templates page. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The 'Launch Templates' section is currently selected. The main content area has a title 'EC2 launch templates' and a subtitle 'Streamline, simplify and standardize instance launches'. Below this, there's a brief description of what launch templates do. To the right, there's a 'New launch template' button with a red arrow pointing to it. Below the button, there's a 'Benefits and features' section with three items: Streamline provisioning, Simplify permissions, and Governance. To the right of the benefits section is a 'Documentation' box with links to Documentation and API reference.

Set the launch template name to LabConfig and click the checkbox under Auto Scaling Guidance.

The screenshot shows the 'Launch template name and description' form. It includes fields for 'Launch template name - required' (containing 'LabConfig'), 'Template version description' (containing 'A prod webserver for MyApp'), and 'Auto Scaling guidance' (with a checked checkbox). Below these are sections for 'Template tags' and 'Source template'.

Under the Application and OS images section, click My AMIs and select the AMI you created earlier.

The screenshot shows the 'Application and OS Images (Amazon Machine Image) - required' section. It includes a search bar, filters for 'Recents', 'My AMIs' (which is selected and highlighted in blue), and 'Quick Start'. There are also filters for 'Owned by me' and 'Shared with me'. To the right, there's a 'Browse more AMIs' section with a note about including AMIs from AWS, Marketplace, and the Community. Below this is a detailed view of a specific AMI named 'WebServerAMI'.

Set the instance type to t2.micro, the Key pair name to vockey, the Firewall (security groups) section to Select existing security group, and the Security groups dropdown to Web Security Group.

The screenshot shows the AWS CloudFormation Launch Configuration settings page. It includes the following sections:

- Instance type**: Set to t2.micro. Details: Family: t2, 1 vCPU, 1 GiB Memory, Current generation: true, 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, On-Demand Linux base pricing: 0.0116 USD per Hour. Free tier eligible. Advanced button.
- Key pair (login)**: Set to vockey. Create new key pair button.
- Network settings**: Subnet dropdown set to "Don't include in launch template". Create new subnet button. Firewall (security groups) dropdown set to "Select existing security group". Create security group button. Security groups dropdown set to "Web Security Group sg-06dc1ae2846dc7037". Compare security group rules button.
- Advanced**: Detailed CloudWatch monitoring button.

Under Advanced details, enable Detailed CloudWatch monitoring.

▼ Advanced details [Info](#)

IAM instance profile [Info](#)

Don't include in launch template

Hostname type [Info](#)

Don't include in launch template

▼

DNS Hostname [Info](#)

- Enable resource-based IPv4 (A record) DNS requests
- Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery [Info](#)

Don't include in launch template

▼

Shutdown behavior [Info](#)

Don't include in launch template

▼

Not applicable for EC2 Auto Scaling

Stop - Hibernate behavior [Info](#)

Don't include in launch template

▼

Not applicable for Amazon EC2 Auto Scaling.

Termination protection [Info](#)

Don't include in launch template

▼

Stop protection [Info](#)

Don't include in launch template

▼

Detailed CloudWatch monitoring [Info](#)

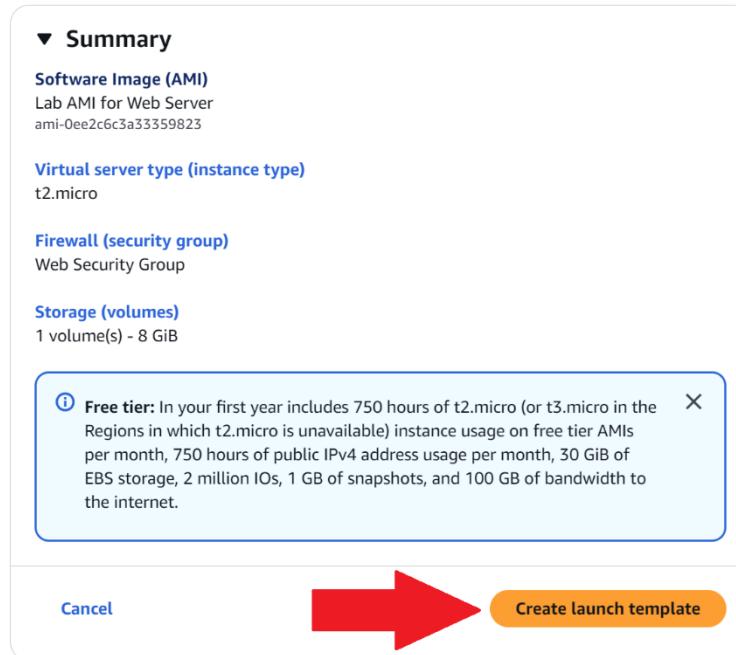
Enable

▼

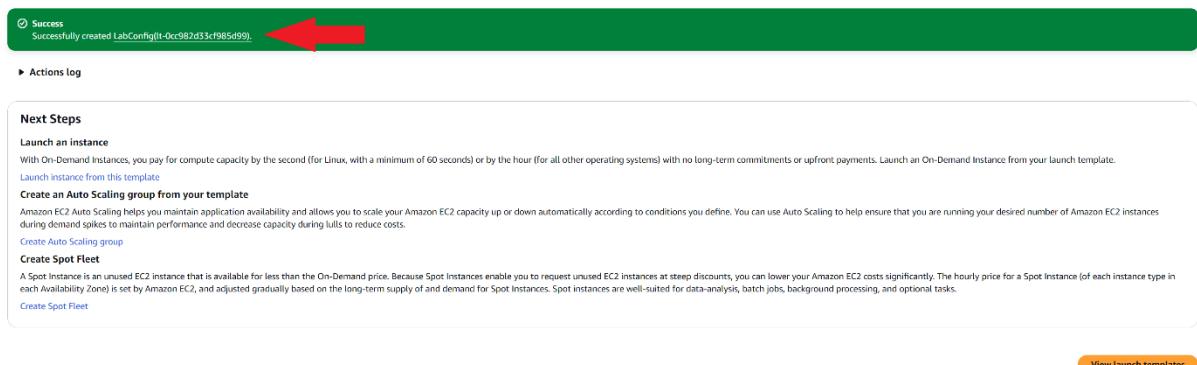
Additional charges apply

Elastic GPU [Info](#)

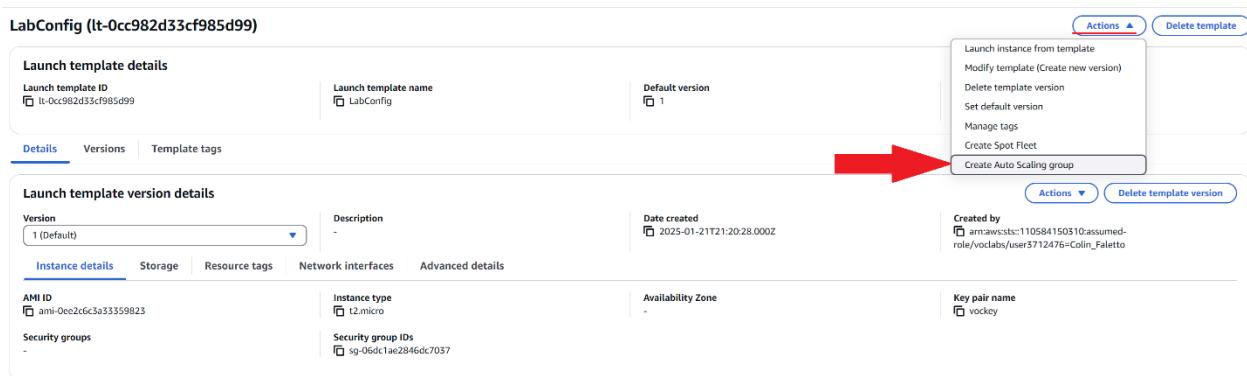
Under Summary, click Create launch template.



Click the hyperlink in the success dialog.



Click Actions > Create auto scaling group.



Set the name to Lab Auto Scaling Group, ensure that the Launch template is set to LabConfig, and click Next.

Name

Auto Scaling group name
Enter a name to identify the group.
Lab Auto Scaling Group

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

Launch template Info

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

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

Create a launch template (C)

Version
Default (1) (C)

Create a launch template version (C)

Description -	Launch template <u>LabConfig</u> <small>(C)</small> lt-0cc982d33cf985d99	Instance type t2.micro
AMI ID ami-0ee2c6c3a33359823	Security groups -	Request Spot Instances No
Key pair name vockey	Security group IDs <u>sg-06dc1ae2846dc7037</u> <small>(C)</small>	

Additional details

Storage (volumes)
-

Date created
Tue Jan 21 2025 13:20:28 GMT-0800 (Pacific Standard Time)



Set the VPC to Lab VPC, select both private subnets under Availability Zones and subnets, then click Next.

Network Info

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

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.
vpc-008b28f7a7c4a4266 (Lab VPC) (C)
10.0.0.0/16

Create a VPC (C)

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

Select Availability Zones and subnets (C)

us-east-1a | subnet-0cf4fa3635252d474 (Private Subnet 1) (C)
10.0.1.0/24

us-east-1b | subnet-00857cd0f2678a98f (Private Subnet 2) (C)
10.0.3.0/24

Create a subnet (C)

Availability Zone distribution - new
Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

Balanced best effort
If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.

Balanced only
If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.



Under load balancing, select attach to an existing load balancer, and under existing load balancer target groups, select LabGroup

Load balancing Info

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

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

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

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

Attach to an existing load balancer

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

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

Choose from Classic Load Balancers

Existing load balancer target groups

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

Select target groups ▼

LabGroup | HTTP X

Application Load Balancer: LabELB

Click Next.

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 Next

Set the Desired capacity to 2, the minimum capacity to 2, and the maximum capacity to 6. Set the automatic scaling policy to target tracking scaling policy, set the name to LabScalingPolicy, the metric type to Average CPU utilization, and the target value to 60. This setting will automatically scale the number of EC2 instances to maintain an average of 60% CPU utilization across instances.

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.

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 Equal or less than desired capacity

Max desired capacity 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

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

Under Additional settings, click 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

Cancel [Skip to review](#)  **Next** 

Under Add notifications, click Next.

Add notifications - optional [Info](#)

Send notifications to SNS topics whenever Amazon EC2 Auto Scaling launches or terminates the EC2 instances in your Auto Scaling group.

[Add notification](#)

Cancel [Skip to review](#)  **Next** 

Under Add tags, click Add tag, set the key to Name, an

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.

ⓘ 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	<input checked="" type="checkbox"/>

Add tag ←

49 remaining

→ **Next**

Click Create Auto Scaling Group.

Step 6: Add tags

Tags (1)

Key	Value	Tag new instances
Name	Lab Instance	Yes

Preview code ← **Create Auto Scaling group** →

Click Instances and ensure that two copies of Lab Instance have been launched.

Instances (1/4) ← **Create Auto Scaling group** →

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs	Monitorin
Bastion Host	i-0ba738e0bc06e7d64b	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	52.207.87.231	-	-	disabled
Lab Instance	i-079e3039caed93dbff	Running	t2.micro	...	View alarms +	us-east-1a	-	-	-	-	enabled
Lab Instance	i-0244d114457306953	Running	t2.micro	...	View alarms +	us-east-1b	-	-	-	-	enabled
Web Server 1	i-0ae9535acc8323e8d	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	34.205.77.105	-	-	disabled

Go to Target Groups, check LabGroup, and ensure that both targets are healthy.

Target groups (1/1) ←

Actions ← **Create target group** →

Target group: LabGroup

Details	Targets	Monitoring	Health checks	Attributes	Tags
Details	2 Total targets	0 Healthy	0 Unhealthy	0 Unused	0 Initial
Target type Instance	Protocol: Port HTTP: 80	Protocol version HTTP/1	VPC vpc-000b28f7a7c4a4266		
IP address type IPv4	Load balancer LabELB				

Distribution of targets by Availability Zone (AZ)

Go to Load balancers, select LabELB, then copy the DNS name.

Load balancers (1/1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Name	DNS name	Status	VPC ID	Availability Zones	Type	Date created
LabELB	LabELB-1904038358.us... (Active) vpc-008b28f7a7cfa4266 2 Availability Zones application January 21, 2025, 13:10 (UTC-08:00)					

Load balancer: LabELB

Details Listeners and rules Network mapping Resource map - new Security Monitoring Integrations Attributes Capacity - new Tags

Details

Load balancer type	Status	Load balancer IP address type
Application	Active	IPv4
Scheme	Hosted zone	Availability Zones
Internet-facing	Z55SXDOOTRQ7XK	subnet-0168f737add6ef2b0 (us-east-1a (use1-az2)) subnet-09ec07908570d1175 (us-eu01-1b (use1-az4))
Load balancer ARN	DNS name info	
arn:aws:elasticloadbalancing:us-east-1:110584150310:loadbalancer/app/LabELB/2f1b12fe2d2a5da	LabELB-1904038358.us-east-1.elb.amazonaws.com (A Record)	

Open the DNS server in a new browser tab and ensure that you see the EC2 instance web server as shown below.

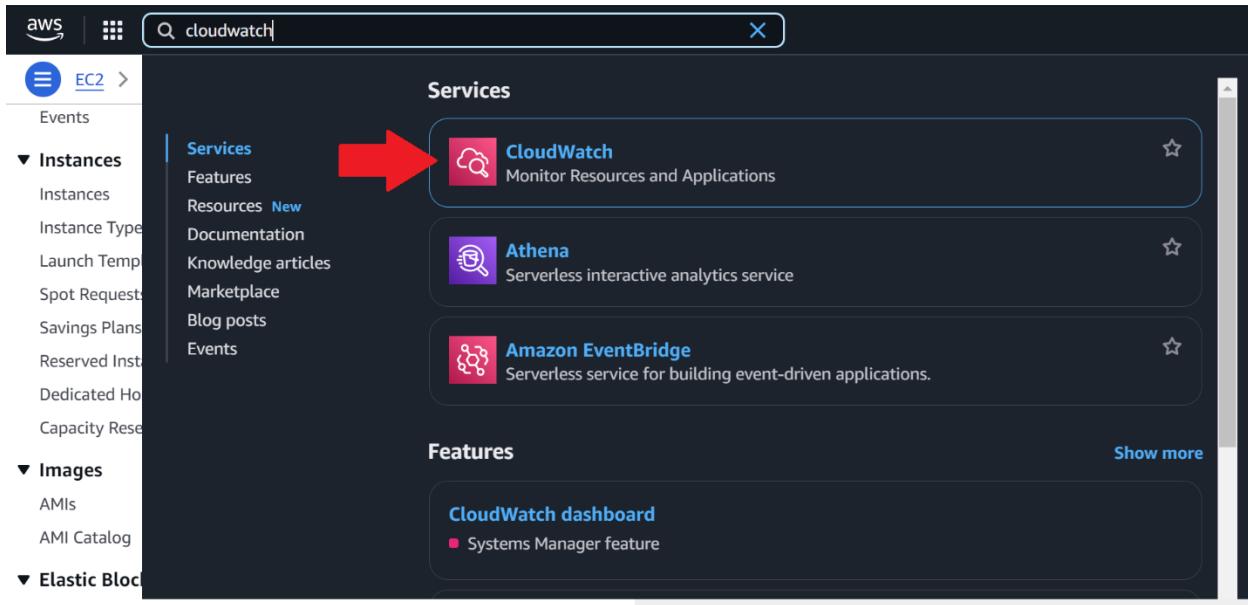
Lab - 6 Scale & Load Balancer | Workbench - Vocareum | Load balancers | EC2 | us-east-1 | Welcome to Academy Cloud!

Load Test RDS

Meta-Data	Value
InstanceId	i-079b3039cae93dbff
Availability Zone	us-east-1a

Current CPU Load: 2%

In the search bar, search for and open Cloudwatch.



Click Alarms > All alarms, and ensure that the AlarmHigh alarm reports OK.

The screenshot shows the 'Alarms' section of the CloudWatch interface. It lists two alarms under the 'All alarms' tab:

- TargetTracking-Lab Auto Scaling Group-AlarmHigh**: Status: OK, Last state update: 2025-01-21 22:21:56, Condition: CPUUtilization > 60 for 3 datapoints within 3 minutes, Actions enabled.
- TargetTracking-Lab Auto Scaling Group-AlarmLow**: Status: Insufficient data, Last state update: 2025-01-21 22:19:51, Condition: CPUUtilization < 54 for 15 datapoints within 15 minutes, Actions enabled.

Go back to EC2 from the search bar.

The screenshot shows the AWS EC2 search results. The sidebar on the left includes sections for CloudWatch, Favorites and recent, Dashboards, AI Operations, Alarms, In alarm, All alarms, and Billing. The main area displays services. A red arrow points to the 'EC2' service card, which is highlighted with a blue border. The card contains the EC2 logo, the text 'Virtual Servers in the Cloud', and a star icon.

Select Auto Scaling groups, select Lab Auto Scaling group, click the Automatic Scaling tab, select LabScalingPolicy, then click Actions > Edit.

The screenshot shows the AWS Auto Scaling groups page. On the left, there's a sidebar with various navigation options like Dashboard, EC2 Global View, Events, Instances, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. Under Auto Scaling, 'Auto Scaling Groups' is selected. In the main content area, it says 'Auto Scaling groups (1/1) info'. There's a search bar and a table with one row: 'Lab Auto Scaling Group' (LaunchConfig | Version Default), 2 instances, Status -, Desired capacity 2, Min 2, Max 6, Availability Zones us-east-1a, us-east-1b. Below this, there's a tab bar with 'Automatic scaling' selected, followed by Details, Integrations - new, Instance management, Instance refresh, Activity, and Monitoring. A note about scaling policies follows. Under 'Dynamic scaling policies (1/1) info', there's a section for 'LabScalingPolicy' with a 'Policy type' dropdown set to 'Target tracking scaling', 'Enabled or disabled' set to 'Enabled', and 'Execute policy when' set to 'As required to maintain Average CPU utilization at 60'. To the right of this section is a 'Actions' dropdown with options: Enable, Disable, Execute, Edit, and Delete.

Set the target value to 50 and click Update.

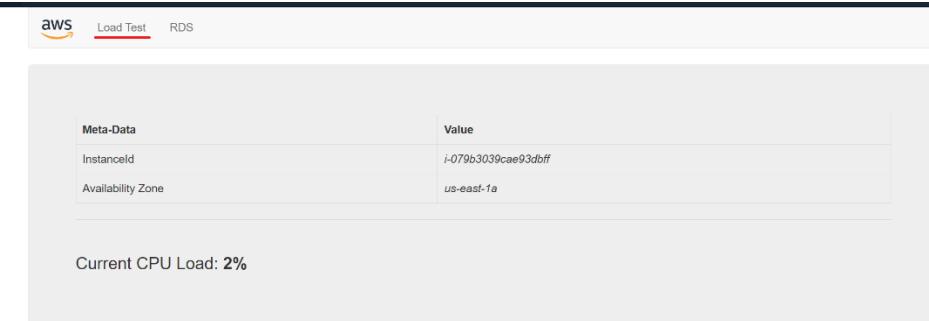
Edit dynamic scaling policy

The screenshot shows the 'Edit dynamic scaling policy' dialog. It has sections for 'Policy type' (Target tracking scaling), 'Scaling policy name' (LabScalingPolicy), 'Metric type' (Info: Average CPU utilization), 'Target value' (50), and 'Instance warmup' (300 seconds). There's also a checkbox for 'Disable scale in to create only a scale-out policy'. At the bottom right is a large orange 'Update' button with a red arrow pointing to it.

Return to Cloudwatch > Alarms > All alarms and ensure the updated AlarmHigh alarm still reports OK.

The screenshot shows the CloudWatch Alarms page with two alarms listed: 'TargetTracking-Lab Auto Scaling Group-AlarmHigh-889540cb-69cc-4c61-89cc-f6c8208964b3' and 'TargetTracking-Lab Auto Scaling Group-AlarmLow-bacd6bae-7e5c-4494-b1fa-c50c6ae63bae'. The first alarm is in the 'OK' state, last updated on 2025-01-21 22:35:22. The second alarm is in the 'Insufficient data' state, last updated on 2025-01-21 22:31:58. Both alarms have their 'Actions' status as 'Actions enabled'. A red arrow points to the 'Actions' column.

Return to the EC2 web server tab and click Load Test.



Return to the AWS console and continually press the refresh button on the alarms page. Eventually, the AlarmHigh will report that it is in alarm.

The screenshot shows the 'Alarms (2)' page in the AWS CloudWatch Metrics Alarms section. It lists two alarms:

- TargetTracking-Lab Auto Scaling Group-AlarmHigh-889540cb-69cc-4c61-89ce-f6c8208964b3**: State: **In alarm**, Last state update: 2025-01-21 22:37:22, Condition: CPUUtilization > 50 for 3 datapoints within 3 minutes, Actions: Actions enabled.
- TargetTracking-Lab Auto Scaling Group-AlarmLow-bacd6bae-7e3c-4494-b1fa-c50c6ae63bae**: State: **OK**, Last state update: 2025-01-21 22:36:47, Condition: CPUUtilization < 37.5 for 15 datapoints within 15 minutes, Actions: Actions enabled.

Return to EC2 > Instances. You should see that the Auto Scaling Group has automatically created more instances of the Lab Instance AMI.

The screenshot shows the 'Instances (6) Info' page in the AWS EC2 Instances section. It lists six instances, all of which are 'Running' and have a Public IPv4 DNS ending in .us-east-1a. The instances are categorized under 'Lab Instance' and include 'Bastion Host' and 'Web Server 1'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv6 DNS	Elastic IP	IPv6 IPs	Monitoring
Bastion Host	i-0ba738e0bce67d64b	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	-	52.207.87.231	-	-	disabled
Lab Instance	i-079b5039cae93dbff	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	-	-	-	-	enabled
Lab Instance	i-0244d314437306933	Running	t2.micro	2/2 checks passed	View alarms	us-east-1b	-	-	-	-	enabled
Lab Instance	i-0aa31259d68950f2	Running	t2.micro	0/2 initializing	View alarms	us-east-1b	-	-	-	-	enabled
Web Server 1	i-0ae9535acc8323e8d	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	-	34.205.77.105	-	-	disabled
Lab Instance	i-02360934f11c0e16c	Running	t2.micro	0/2 initializing	View alarms	us-east-1a	-	-	-	-	enabled

Next, to clean up, select Web Server 1 and click Actions > Terminate (delete) instance.

The screenshot shows the 'Instances (1/6) Info' page in the AWS EC2 Instances section. It lists the same six instances. A red arrow points to the 'Actions' dropdown menu for the 'Web Server 1' instance, specifically highlighting the 'Terminate (delete) instance' option.

Click Terminate.

Terminate (delete) instance?

X

⚠️ On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?

Instance ID	Termination protection
<input type="checkbox"/> i-0ae9535acc8323e8d (Web Server 1)	<input checked="" type="checkbox"/> Disabled

To confirm that you want to delete the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.

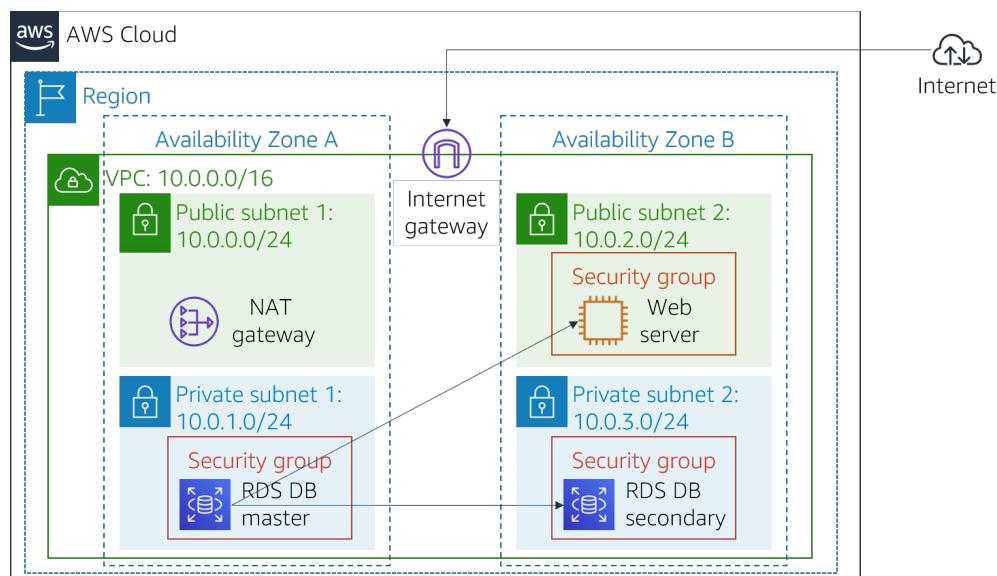
Terminate (delete)



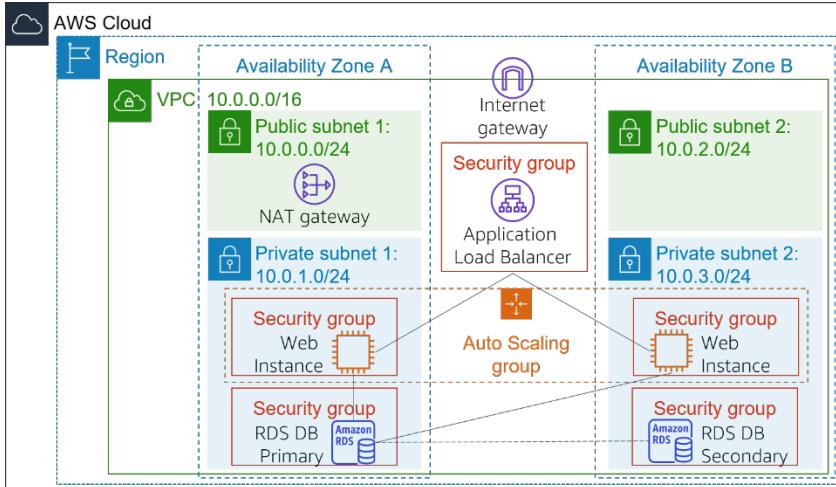
Topology (EBS)



Topology (RDS)



Topology (Auto Scaling)



Problems

No problems were encountered in this lab.

Conclusion

To wrap up, these three labs were a great addition to my understanding of the AWS cloud and management console. Through learning about Elastic Block store, I now have a deeper understanding of the inner workings of Elastic Compute Cloud. Through learning about RDS, I now have a solid foundation of knowledge about how large amounts of data with a consistent structure are stored. Through learning about auto scaling, I'm now confident that I could scale AWS services for use at a company with heavy reliance on cloud resources.