

Lab 05

CLOUD COMPUTING

CS-4075

Course Instructor:

Sir Zaheer Sani

Name: Zeeshan Ali

Roll No: 20i-2465

Section: SE-A

Due Date: Nov 15, 2023



Lab 5

Accessing the AWS Management Console:

1. At the top of these instructions, choose Start Lab to launch your lab.

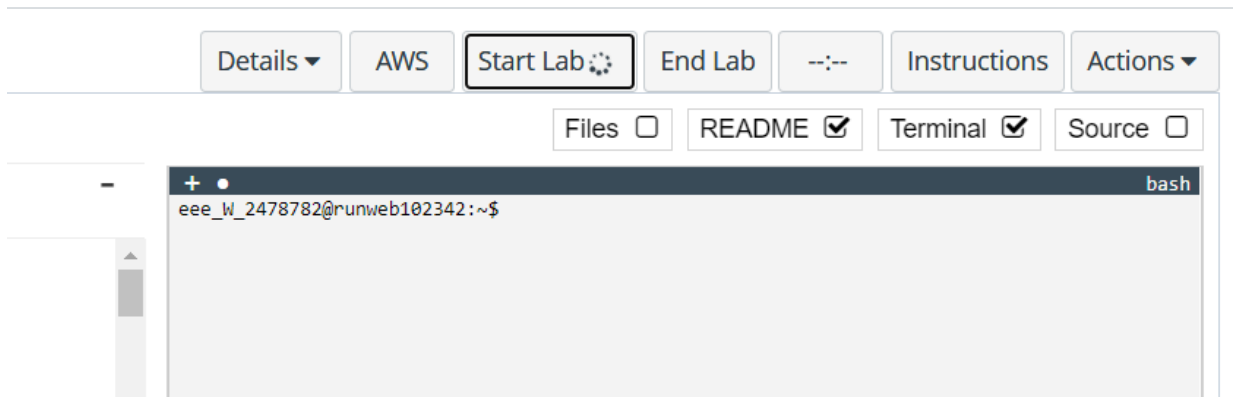


Figure 1: start the lab.

A Start Lab panel opens displaying the lab status.

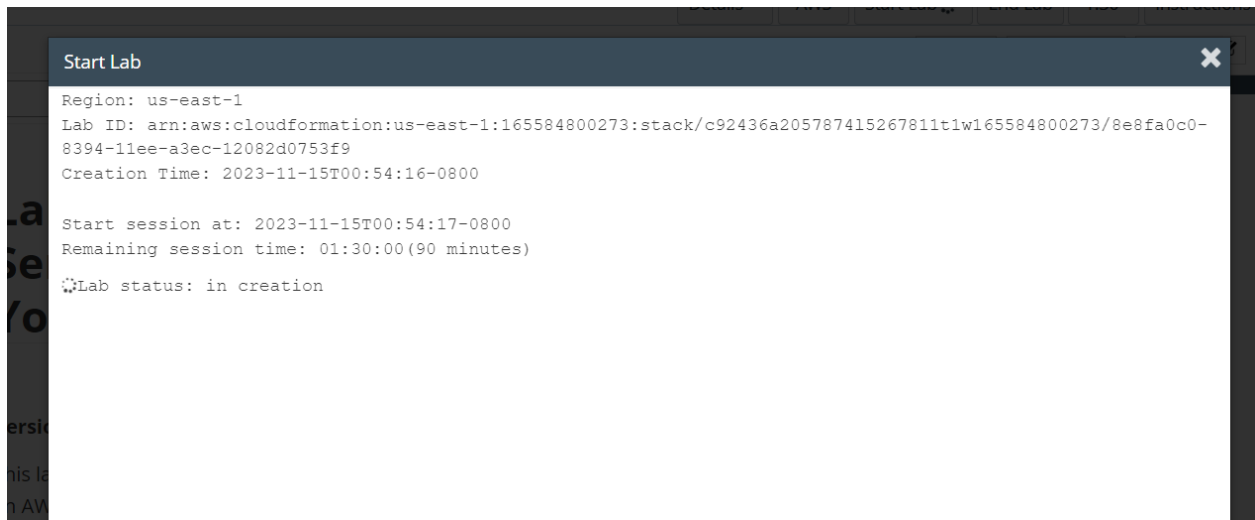


Figure 2: lab is in creation stge.

2. Wait until you see the message "**Lab status: ready**", then choose the **X** to close the Start Lab panel.

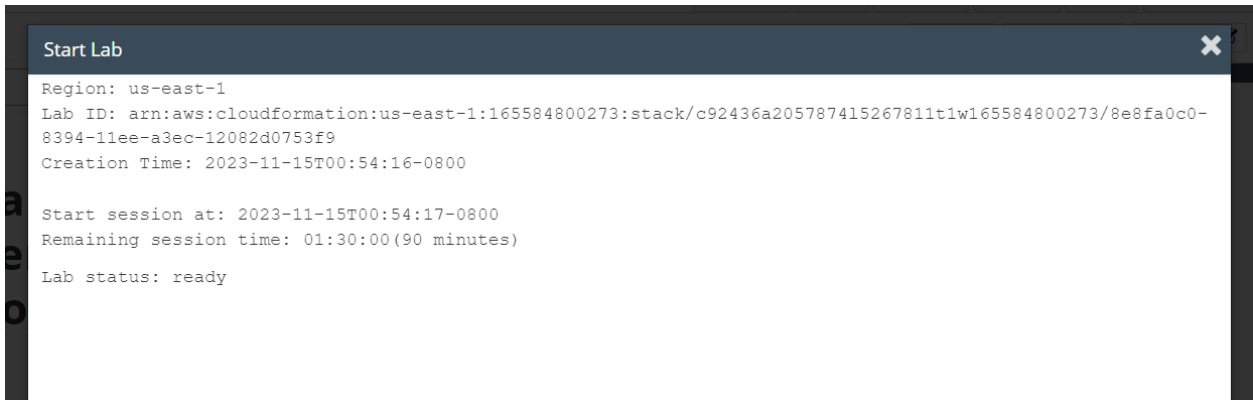


Figure 3: Lab is ready to use.

3. At the top of these instructions, choose AWS.

This will open the AWS Management Console in a new browser tab. The system will automatically log you in.

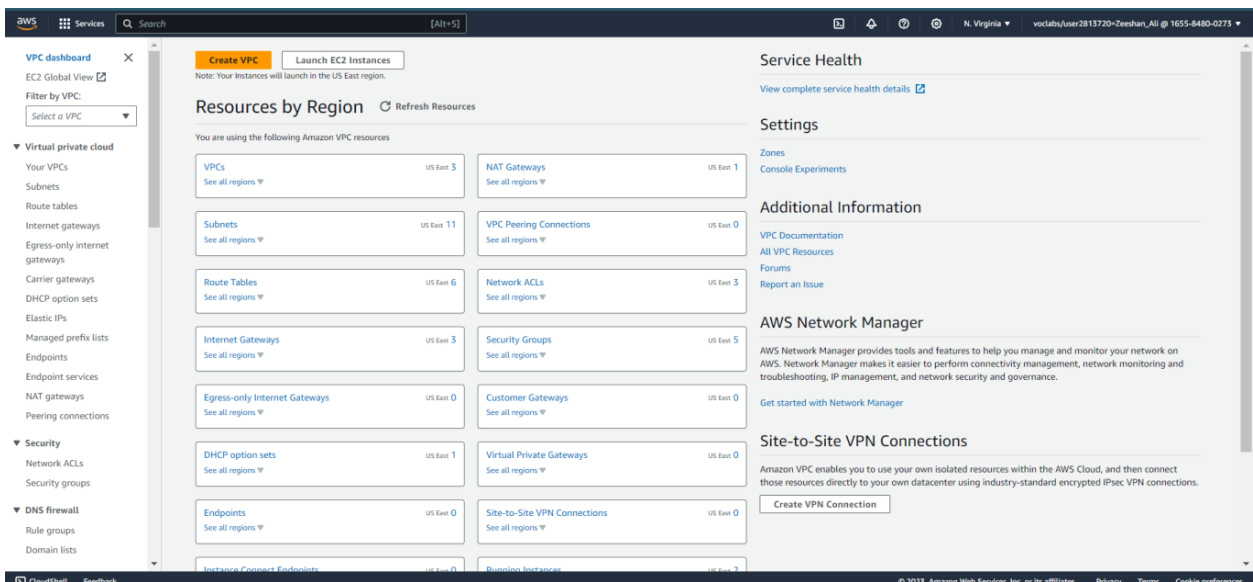


Figure 4: AWS DASHBOARD

Task 1: Create a Security Group for the RDS DB Instance

5. In the **AWS Management Console**, on the Services menu, choose **VPC**.

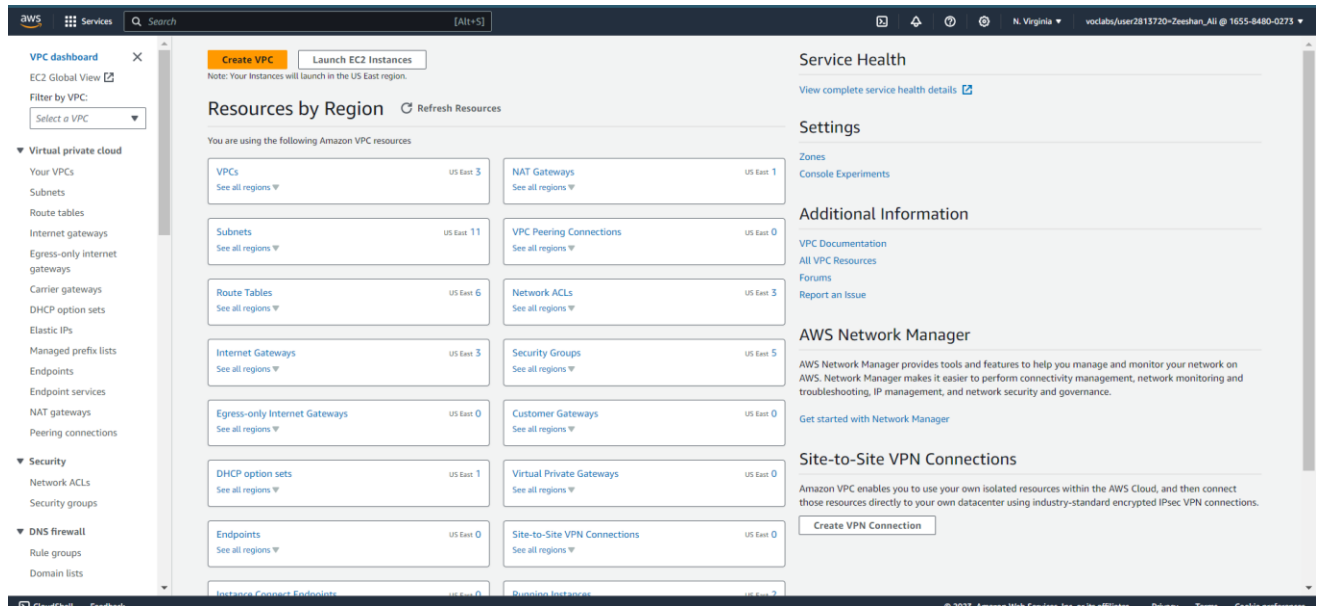


Figure 5: VPC DASHBOARD

6. In the left navigation pane, choose **Security Groups**.
7. Choose Create security group and then configure:
 - **Security group name:** DB Security Group
 - **Description:** Permit access from Web Security Group
 - **VPC:** Lab VPC
8. In the **Inbound rules** pane, choose Add rule.

The security group currently has no rules. You will add a rule to permit access from the *Web Security Group*.

9. Configure the following settings:
 - **Type:** MySQL/Aurora (3306)
 - **CIDR, IP, Security Group or Prefix List:** Type `sg` and then select *Web Security Group*.

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

Inbound rules Info

Type	Protocol	Port range	Source	Description - optional
MySQL/Aurora	TCP	3306	Custom	

Figure 6: Security Groups

This configures the Database security group to permit inbound traffic on port 3306 from any EC2 instance that is associated with the *Web Security Group*.

10. Choose Create security group.

Security group (sg-Odd8a6488ff6c6277 - DB Security Group) was created successfully

Details

sg-Odd8a6488ff6c6277 - DB Security Group

Security group name DB Security Group	Security group ID sg-Odd8a6488ff6c6277	Description Permit access from Web Security Group	VPC ID vpc-05031a2e467f769f4
Owner 165584800273	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules (1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sg-027de5ee3398688...	-	MySQL/Aurora	TCP	3306	sg-0687aaa4140bd5f6...	-

Figure 7: Success Create security group.

You will use this security group when launching the Amazon RDS database.

Task 2: Create a DB Subnet Group

11. On the Services menu, choose **RDS**.

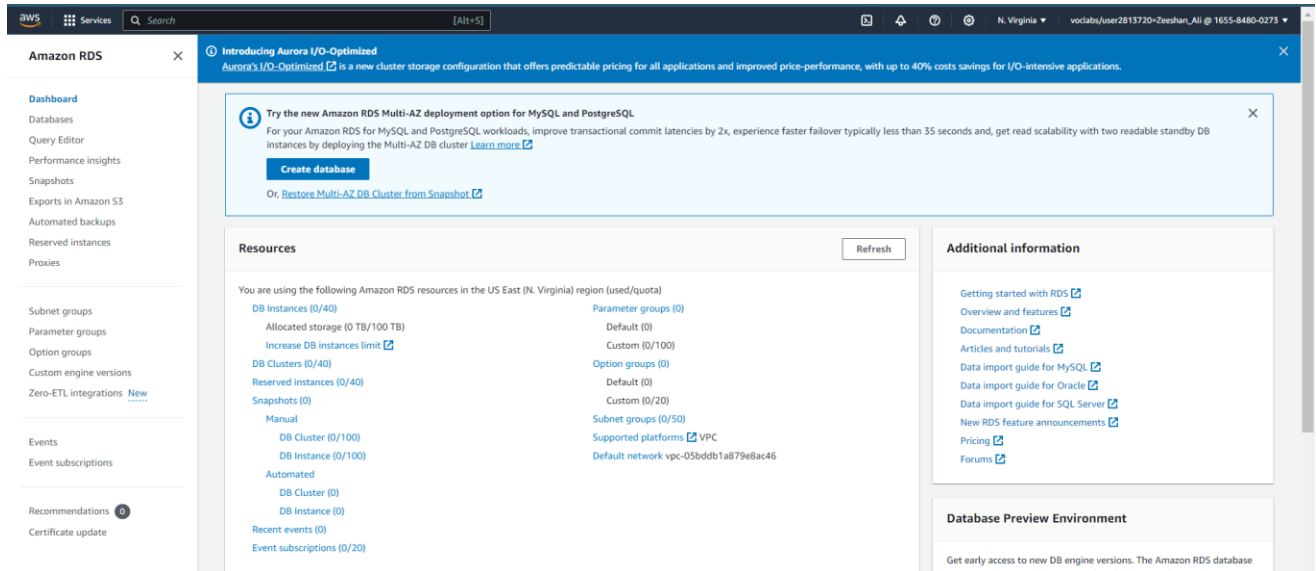


Figure 8: RDS

12. In the left navigation pane, choose **Subnet groups**.

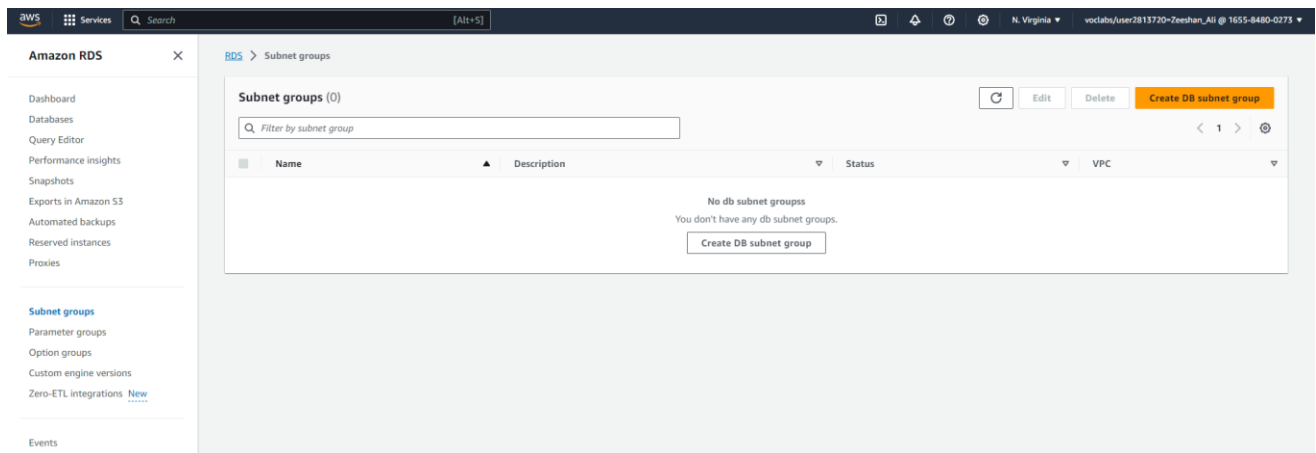


Figure 9: Subnet groups

13. Choose Create DB Subnet Group then configure:

- **Name:** DB-Subnet-Group
- **Description:** DB Subnet Group
- **VPC:** Lab VPC

aws Services Search [Alt+S]

Amazon RDS X

- Dashboard
- Databases
- Query Editor
- Performance insights
- Snapshots
- Exports in Amazon S3
- Automated backups
- Reserved instances
- Proxies

Subnet groups

- Parameter groups
- Option groups
- Custom engine versions
- Zero-ETL integrations [New](#)

RDS > Subnet groups > Create DB subnet group

Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that 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-05031a2e467f769f4)

Figure 10: Create DB Subnet Group

14. Scroll down to the **Add Subnets** section.
15. Expand the list of values under **Availability Zones** and select the first two zones: **us-east-1a** and **us-east-1b**.
16. Expand the list of values under **Subnets** and select the subnets associated with the CIDR ranges **10.0.1.0/24** and **10.0.3.0/24**. These subnets should now be shown in the **Subnets selected** table.
17. Choose Create

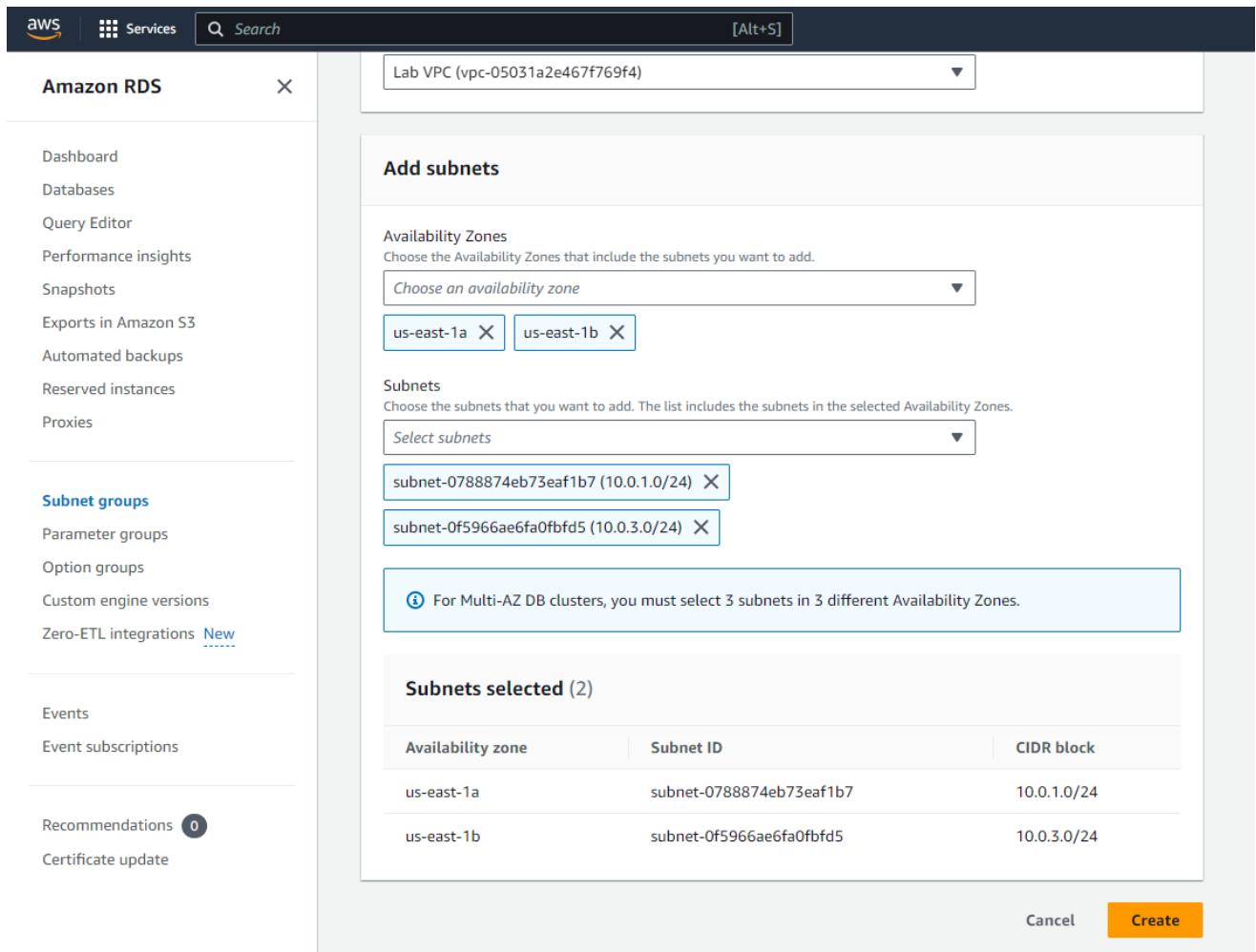


Figure 11: Choose Create

You will use this DB subnet group when creating the database in the next task.

Task 3: Create an Amazon RDS DB Instance

18. In the left navigation pane, choose **Databases**.
19. Choose Create database.

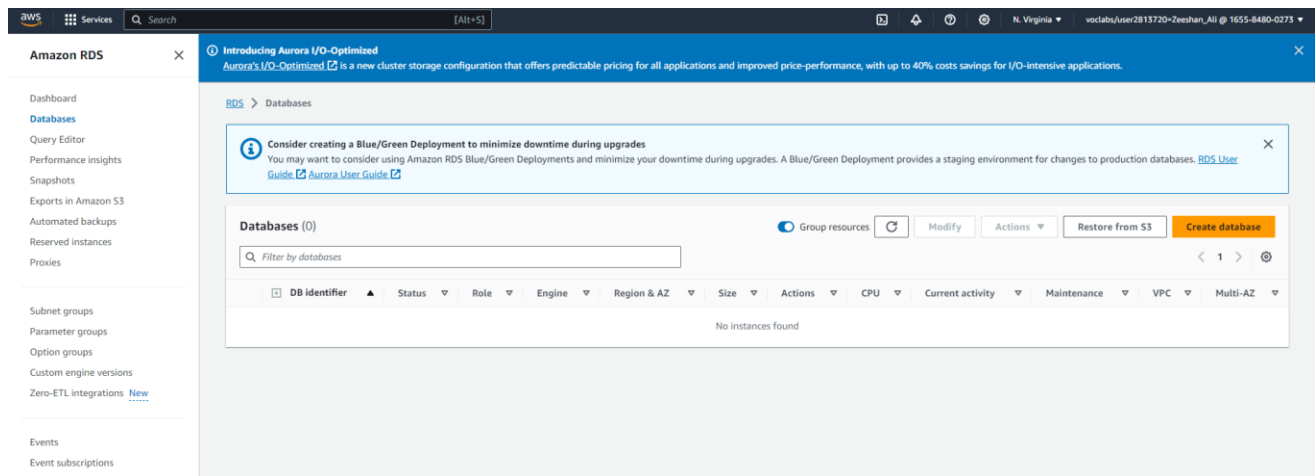


Figure 12: choose Databases.

20. Select **MySQL** under **Engine Options**.

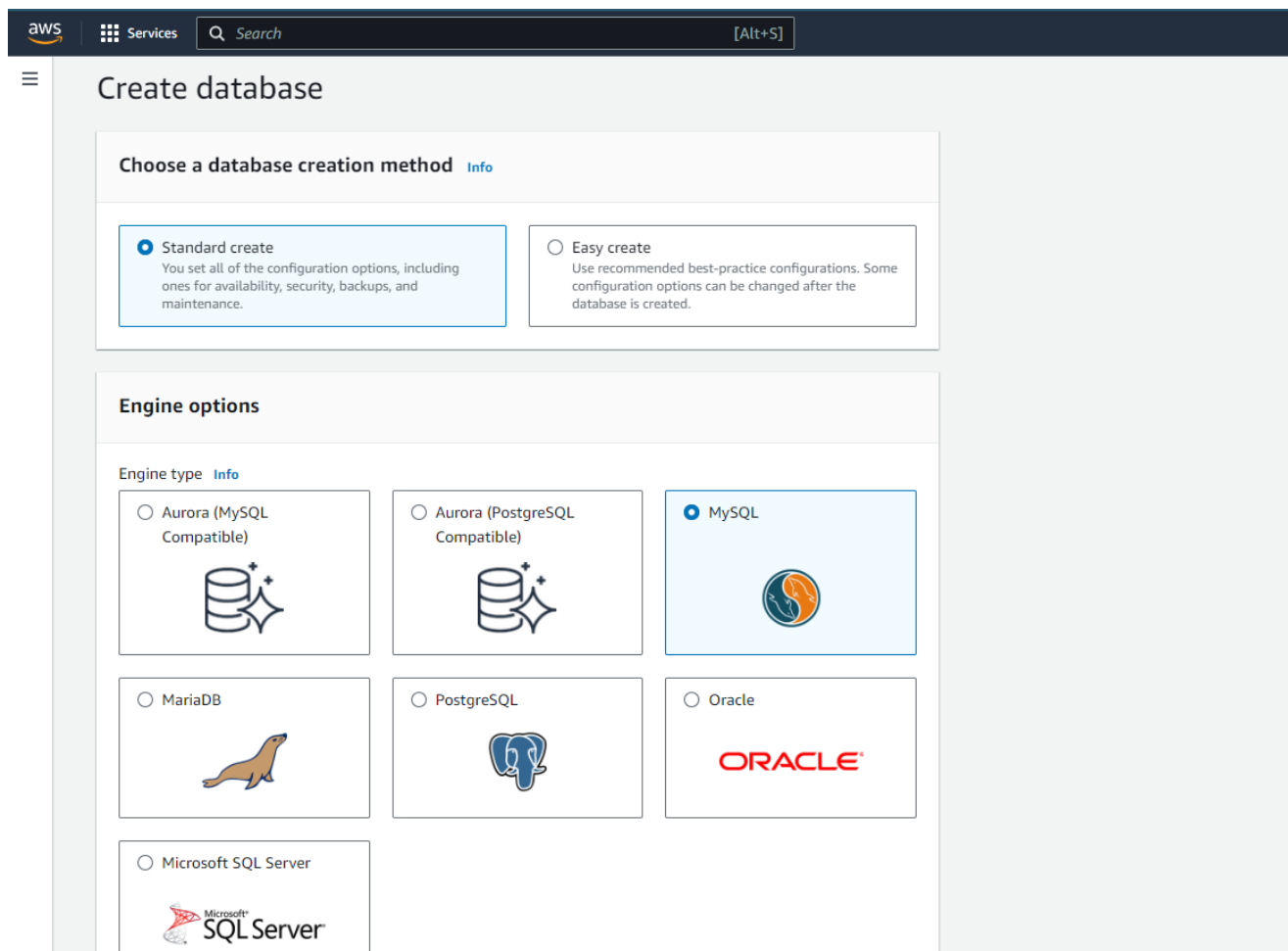


Figure 13: Select MySQL

21. Under **Templates** choose **Dev/Test**.

22. Under **Availability and durability** choose **multi-AZ DB instance**.

The screenshot displays the Amazon RDS console configuration page. At the top, the 'Engine Version' dropdown is set to 'MySQL 8.0.33'. Below this, the 'Templates' section is active, showing three options: 'Production', 'Dev/Test' (which is selected with a blue radio button and highlighted with a blue border), and 'Free tier'. Each option includes a brief description of its use case. The 'Dev/Test' option states: 'This instance is intended for development use outside of a production environment.' Below the templates, the 'Availability and durability' section is visible, showing 'Deployment options' with an 'Info' link. It lists three options: 'Multi-AZ DB Cluster - new', 'Multi-AZ DB instance' (selected with a blue radio button), and 'Single DB instance'. Each option includes a description of its configuration and availability features. The 'Multi-AZ DB instance' option states: '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.'

Figure 14: choose them.

23. Under **Settings**, configure:

- **DB instance identifier:** lab-db
- **Master username:** main
- **Master password:** lab-password
- **Confirm password:** 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 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

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

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

☐ **Manage master credentials in AWS Secrets Manager**

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

[i](#) If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
[Learn more](#) [↗](#)

☐ **Auto generate a password**

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

Master password [Info](#)

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

Confirm master password [Info](#)

Figure 15: configure.

24. Under **DB instance class**, configure:

- Select **Burstable classes (includes t classes)**.
- Select *db.t3.micro*

25. Under **Storage**, configure:

- **Storage type:** *General Purpose (SSD)*
- **Allocated storage:** *20*

Instance configuration

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

DB instance class [Info](#)

► Show filters

- ☐ 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: 2,085 Mbps

Storage

Storage type [Info](#)

General Purpose SSD (gp3)

Performance scales independently from storage

Allocated storage [Info](#)

20

GiB

Minimum: 20 GiB. Maximum: 6,144 GiB

i After you modify the storage for a DB instance, the status of the DB instance will be in storage-optimization. Your instance will remain available as the storage-optimization operation completes.
[Learn more](#) [↗](#)

Figure 16: choose them.

26. Under **Connectivity**, configure:

- **Virtual Private Cloud (VPC):** *Lab VPC*

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-05031a2e467f769f4)

4 Subnets, 2 Availability Zones

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

Figure 17: choose them.

27. Under **Existing VPC security groups**, from the dropdown list:

- Choose *DB Security Group*.
- Deselect *default*.

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-2019 (default)
Expiry: Aug 22, 2024 ▼

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

▼ Additional configuration

Database port [Info](#)

TCP/IP port that the database will use for application connections.

3306

Figure 18: choose them.

28. Expand **Additional configuration**, then configure:

- **Initial database name:** lab
- Uncheck **Enable automatic backups.**
- Uncheck **Enable encryption.**
- Uncheck **Enable Enhanced monitoring.**

▼ 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](#)

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

DB parameter group [Info](#)

Option group [Info](#)

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](#)

Log exports

Select the log types to publish to Amazon CloudWatch Logs

☐ Audit log

☐ Error log

☐ General log

Figure 19: configure.

IAM role

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

RDS service-linked role

Maintenance

Auto minor version upgrade [Info](#)

☐ Enable auto minor version upgrade

Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

☐ Choose a window

☒ No preference

Deletion protection

☐ Enable deletion protection

Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

i 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.

Cancel

Create database

Figure 20: Create database.

29. Choose Create database. Your database will now be launched.

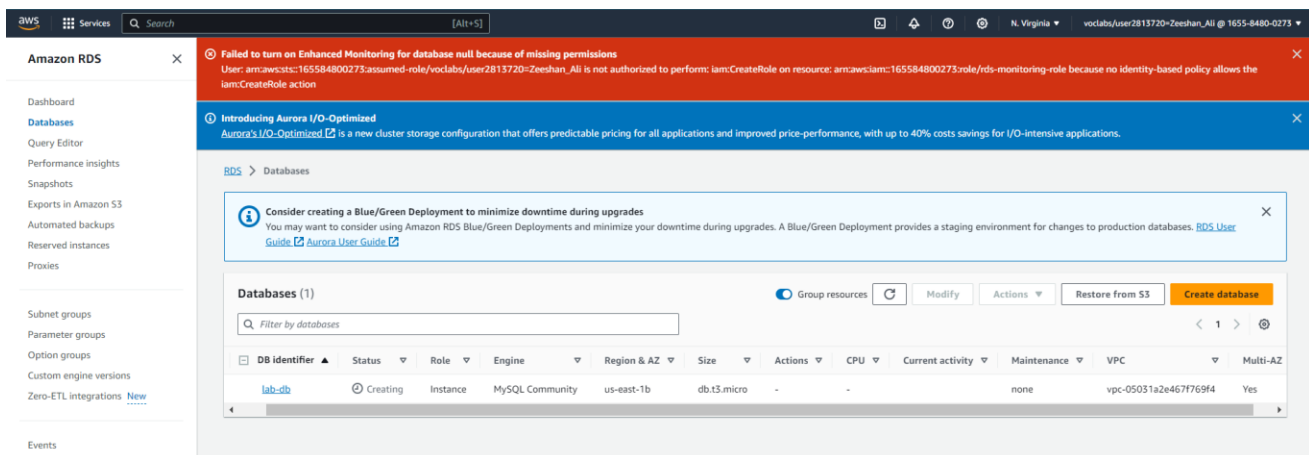


Figure 21: database will launch.

If you receive an error that mentions "not authorized to perform: iam:CreateRole", make sure you unchecked *Enable Enhanced monitoring* in the previous step.

30. Choose **lab-db** (choose the link itself).

31. Wait until **Info** changes to **Modifying** or **Available**.

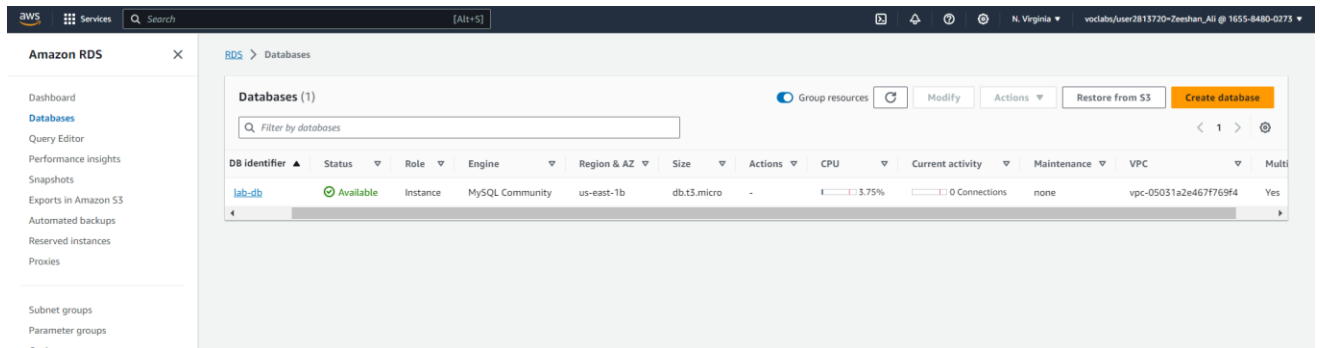


Figure 22: Info changes

32. Scroll down to the **Connectivity & security** section and copy the **Endpoint** field.

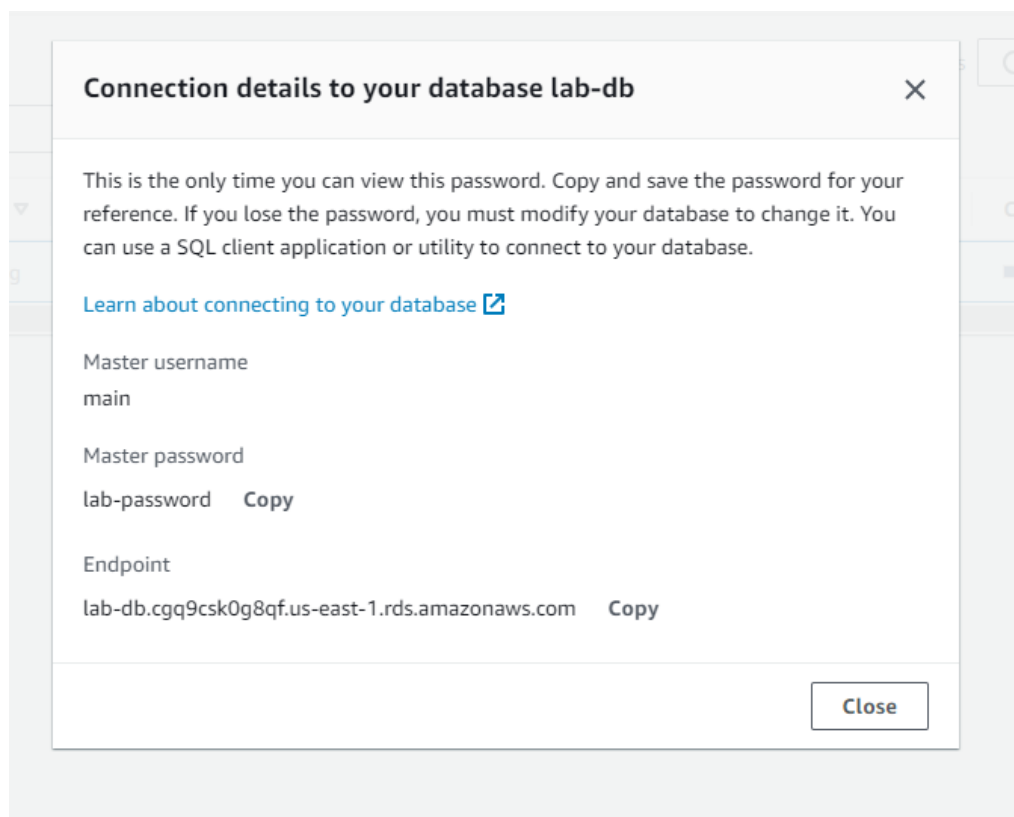


Figure 23: copy the Endpoint.

Task 4: Interact with Your Database

34. To copy the **WebServer** IP address, choose on the Details drop down menu above these instructions, and then choose Show.

Lab 4 - Working with EBS

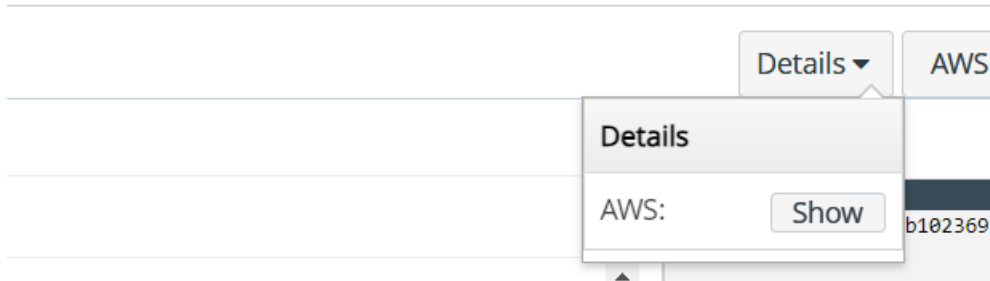


Figure 24: Details drop down menu.

35. Open a new web browser tab, paste the *WebServer* IP address and press Enter.



Figure 25: Webserver IP address



Figure 26: Webserver IP address

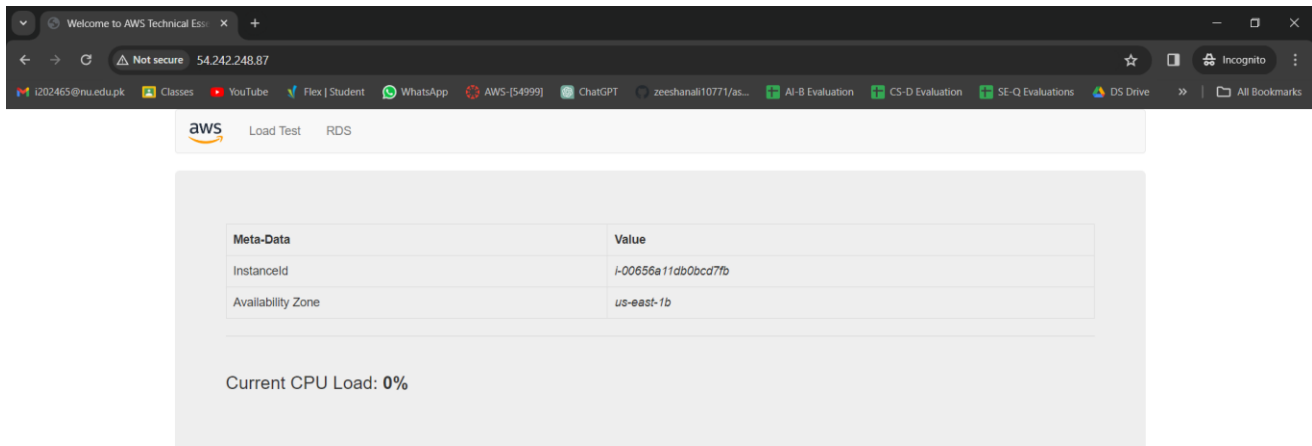


Figure 27: Webserver

36. Choose the **RDS** link at the top of the page.

37. Configure the following settings:

- **Endpoint:** Paste the Endpoint you copied to a text editor earlier
- **Database:** lab
- **Username:** main
- **Password:** lab-password
- Choose **Submit**



Endpoint lab-db.cgq9csk0g8qf.us-east-1.rds.amazonaws.com

Database lab

Username main

Password

Submit

Figure 28: Configure RDS

A message will appear explaining that the application is running a command to copy information to the database. After a few seconds the application will display an **Address Book**.

The Address Book application uses the RDS database to store information.

38. Test the web application by adding, editing and removing contacts.



Address Book

Last name	First name	Phone	Email	Admin	
				Add Contact	
Ali	Zeeshan	03107048506	i202465@nu.edu.pk	Edit	Remove
Hammad	Aslam	03090559250	20I-2465@nu.edu.pk	Edit	Remove
Johnson	Roberto	123-456-7890	robertoj@someaddress.com	Edit	Remove

Figure 29: Address Book

Lab Complete

39. Choose End Lab at the top of this page and then choose Yes to confirm that you want to end the lab.

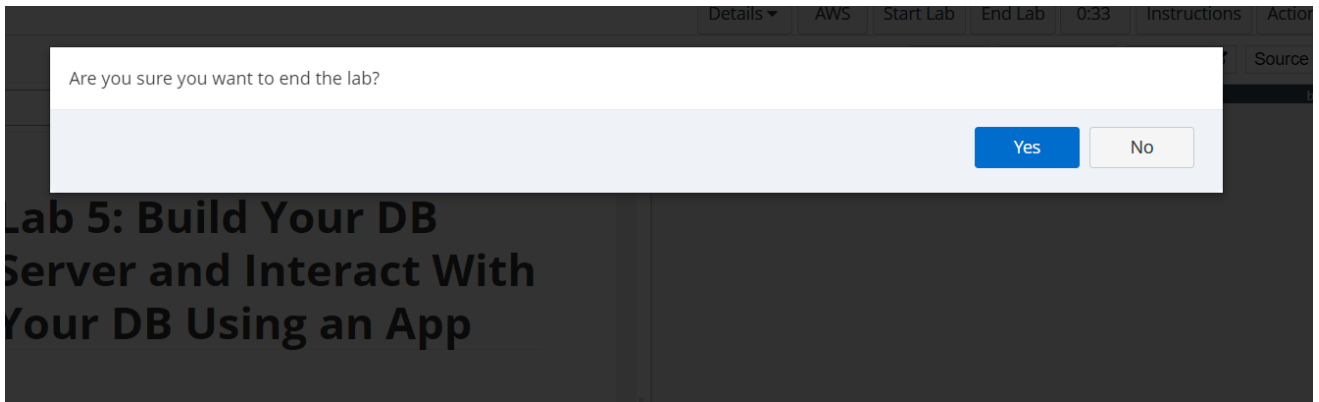


Figure 30: end the lab.

A panel will appear, indicating that "DELETE has been initiated... You may close this message box now."

40. Choose the **X** in the top right corner to close the panel.

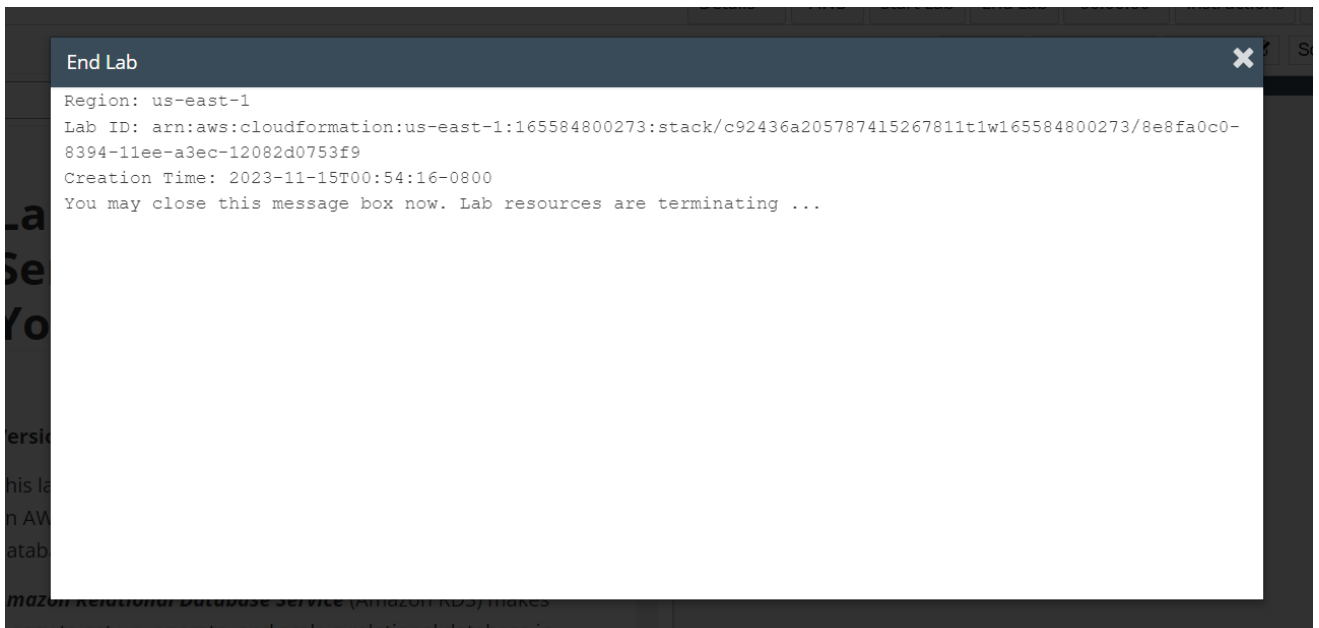


Figure 31: close the panel.