



Name : Ziad Mohamed Ismail Abdelkhalik.

Gmai : ziadmohamd333@gmail.com.

Phone : 01152259562.

Group_Code : GIZ1_SW D8_M1e.

New horizons cairo.

Scenario:

The university is preparing for the new school year. The admissions department has received complaints that their web application for student records is slow or unavailable during peak admissions periods due to high traffic.

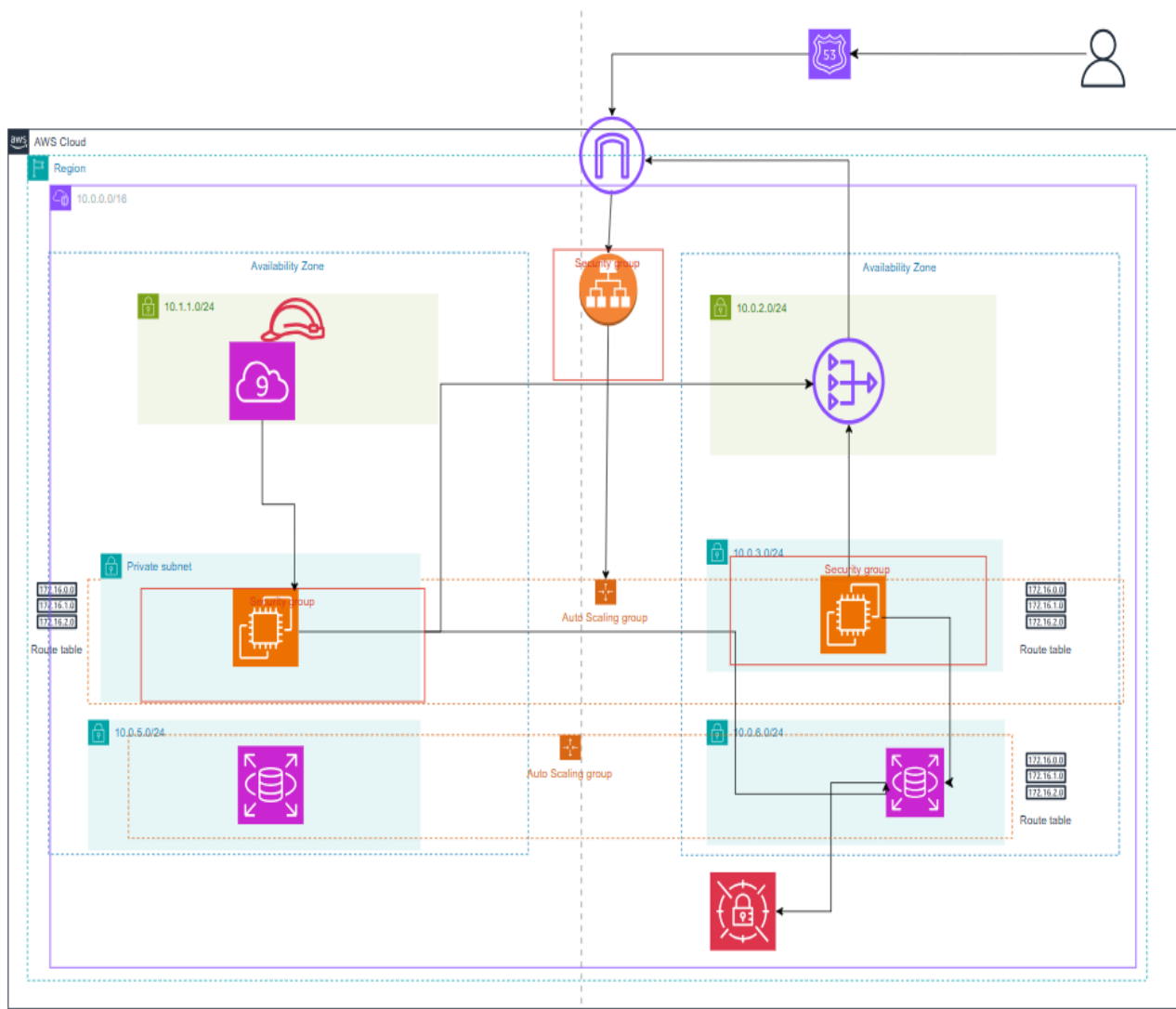
As a cloud engineer, your manager has asked you to create a proof of concept (POC) to host the web application in the AWS Cloud. You are tasked with designing and implementing a new hosting architecture that will improve the user experience for the web application. Your responsibilities include building the infrastructure to host the student records web application in the cloud.

Your challenge is to plan, design, build, and deploy the application to the AWS Cloud in accordance with AWS Well-Architected Framework best practices. During peak admissions periods, the application must support thousands of users while being highly available, scalable, load-balanced, secure, and high-performing.

The following image shows an example of the student records web application. The site lists records of students who have applied for admission to the university. Users can view, add, delete, and modify student records.

To achieve this, I used the following AWS services:

- **EC2 instances** to deploy the application, with an **Application Load Balancer** and **Auto Scaling Group** to ensure high availability and scalability.
- **Security groups** to provide robust security for the application.
- **Amazon RDS** to store student data, as it is a relational database well-suited for this purpose.
- **Cloud9** to develop and implement the code in my environment.
- **Internet Gateway** to ensure the application is accessible over the internet.



- **Functional:** The solution meets the functional requirements, such as the ability to view, add, delete, or modify the student records, without any perceivable delay.

Application load balancer: The solution can properly balance user traffic to avoid overloaded or underutilized resources. We use **Application Load Balancing** to distribute incoming application traffic across multiple targets, such as EC2 instances, in various Availability Zones. This increases the availability of your application.

You add one or more listeners to your load balancer. A listener checks for connection requests from clients, using the protocol and port that you configure. The rules you define for a listener determine how the load balancer routes requests to its registered targets. Each rule consists of a priority, one or more actions, and one or more conditions. When the conditions for a rule are met, the corresponding actions are performed.

You must define a default rule for each listener, and you can optionally define additional rules.

Scalable: We use an **Auto Scaling group** to achieve high scalability in our web servers. An Auto Scaling group contains a collection of EC2 instances that are treated as a logical grouping for automatic scaling and management purposes. It also allows the use of Amazon EC2 Auto Scaling features, such as health check replacements and scaling policies.

Both maintaining the number of instances in the Auto Scaling group and automatic scaling are core functionalities of the Amazon EC2 Auto Scaling service. The size of an Auto Scaling group depends on the number of instances you set as the desired capacity. You can adjust this capacity to meet demand, either manually or through automatic scaling.

The Auto Scaling group starts by launching enough instances to meet the desired capacity and maintains this number of instances by performing periodic health checks on the group's instances.

Highly available: We use **Multi-Availability Zones (AZs)** to achieve high availability. AZs are isolated locations within a region. Deploying your

infrastructure across multiple AZs helps ensure that your application remains operational if one AZ experiences an outage.

We use an **Auto Scaling group** to achieve high scalability for our web servers, and **Application Load Balancing** to distribute incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones.

We use **RDS Multi-AZ** to ensure that your database has a standby replica in a different AZ. In case of a failure, automatic failover occurs to the standby instance. For read-heavy applications, you can create read replicas of your database in multiple AZs or even across regions.

Security : The database is secured and cannot be accessed directly from public networks. I placed the **RDS DB** in a private subnet and configured the security group's inbound rules to accept **traffic only from the security group of the EC2 instance**. I use **security groups** to ensure high security for my instance.

AWS IAM roles allow you to manage permissions securely by controlling access to AWS resources. We also apply data encryption to encrypt data at rest. Encryption is enabled for databases and storage volumes, and **AWS Key Management Service (KMS)** provides centralized key management.

We use **VPC** to isolate our network and resources from the public internet. **Secrets Manager** secures sensitive data such as passwords, phone numbers, usernames, database credentials, and more.

High performing: You need to focus on optimizing various aspects of your infrastructure, application design, and resource management. AWS offers a variety of services and tools to help you build scalable, responsive, and high-performing applications. Here's a comprehensive guide on how to optimize for high performance:

- **Choose the right EC2 instance types** for your workload.
- I manage **EC2 instance types, AMIs, storage, networking, security groups, and key pairs** to ensure optimal performance.

Cost optimized : choose the right size EC2 instance to meet my requirements, selecting the best fit for the workload (compute-optimized, memory-optimized, or storage-optimized). Use **AWS Cost Explorer's Resource**

Optimization to identify underutilized instances that can be downsized or terminated.

- **Auto Scaling:** Use Auto Scaling Groups to automatically adjust the number of EC2 instances in response to traffic or load changes. This ensures that you're only paying for the resources you need.
- **Reserved Instances:** I can use reserved instances to save up to 80% of the total cost, which can be 70-90% cheaper than On-Demand instances.
- Ensure your load balancers are efficiently sized and not over-provisioned.
- Use **On-Demand Instances** only when workloads are unpredictable or need short-term scaling.
- Use managed services like **Amazon RDS** that automatically handle operational overhead (patching, scaling, backups), allowing you to focus on cost-efficient use cases.
- Choose the right **database engine** and instance type (On-Demand or Reserved). Scale read-heavy workloads with **RDS Read Replicas** instead of launching larger instances.
- Use **RDS Auto Scaling** to dynamically scale up and down based on demand.
- Continuously monitor resource usage using **Cost Explorer** to track idle or underutilized resources, and set up custom cost and usage alerts.

AWS VPC (Virtual Private Cloud) is a foundational networking service within AWS that allows you to create and manage isolated, secure cloud networks for your AWS resources. It provides full control over your virtual networking environment, including the selection of your own IP address ranges, creation of subnets, routing configurations, and security settings

- **Subnets:**

- A VPC can be divided into subnets (public and private), each residing within an Availability Zone.
- **Public subnets** allow resources (like EC2 instances) to be accessible from the internet, whereas **private subnets** restrict access and are typically used for internal applications or databases.

- **Route Tables:**

- Define how traffic flows within the VPC. You can create custom routes to direct traffic between subnets or to external destinations like the internet or other VPCs.
- **Internet Gateway (IGW):**
 - A VPC component that allows communication between instances in the VPC and the internet. It is typically associated with public subnets.

Pricing : this services that I use and the price

Estimate summary		
Upfront cost	Monthly cost	Total 12 months cost
35.92 USD	1,305.34 USD	15,700.00 USD
		Includes upfront cost

Detailed Estimate

Name	Group	Region	Upfront cost	Monthly cost
AWS Web Application Firewall (WAF)	No group applied	US East (N. Virginia)	0.00 USD	10.00 USD
Status: - Description: Config summary: Number of Web Access Control Lists (Web ACLs) utilized (2 per month)				
Amazon Route 53	No group applied	US East (N. Virginia)	0.00 USD	1.00 USD
Status: - Description: Config summary: Hosted Zones (2), Number of Elastic Network Interfaces ()				
Amazon EC2	No group applied	US East (N. Virginia)	35.92 USD	2.99 USD
Status: - Description: Config summary: Tenancy (Shared Instances), Operating system (Windows Server), Workload (Consistent, Number of instances: 1), Advance EC2 instance (t3.nano), Pricing strategy (Compute Savings Plans 1yr Partial Upfront), Enable monitoring (disabled), DT Inbound: Not selected (0 TB per month), DT Outbound: Not selected (0 TB per month), DT Intra-Region: (0 TB per month)				

Amazon RDS Custom for Oracle	No group applied	US East (N. Virginia)	0.00 USD	419.57 USD
-------------------------------------	------------------	-----------------------	----------	------------

Status: -

Description:

Config summary: Storage for each RDS Custom instance (General Purpose SSD (gp2)), Storage amount (100 GB), Instance type (db.r5.xlarge), Number of RDS Custom for Oracle instances (1), Utilization (On-Demand only) (100 %Utilized/Month), License (Customer-provided), Database edition (Enterprise), Deployment option (Single-AZ)


Amazon Virtual Private Cloud (VPC)	No group applied	US East (N. Virginia)	0.00 USD	871.78 USD
---	------------------	-----------------------	----------	------------

Status: -

Description:

Config summary: Working days per month (22) Number of NAT Gateways (1) Number of Availability Zones that Gateway Load Balancer is deployed to (1), Number of Gateway Load Balancer Endpoints (1), Total processed bytes (100 GB per hour)

Acknowledgement

AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services. [Learn more](#) 

VPC :

Is a foundational networking service within AWS that allows you to create and manage isolated, secure cloud networks for your AWS resources.

☐ VPC only

☒ VPC and more

Name tag auto-generation [Info](#)

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate

IPv4 CIDR block [Info](#)

Determine the starting IP and the size of your VPC using CIDR notation.

65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

VPC [Show details](#)

Your AWS virtual network

project-vpc

Subnets (4)

Subnets within this VPC

us-east-1a

☒ project-subnet-public1-us-east-1a

☒ project-subnet-private1-us-east-1a

us-east-1b

☒ project-subnet-public2-us-east-1b

☒ project-subnet-private2-us-east-1b

Route tables (3)

Route network traffic to resources

☒ project-rtb-public

☒ project-rtb-private1-us-east-1a

☒ project-rtb-private2-us-east-1b

Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

Customize subnets CIDR blocks

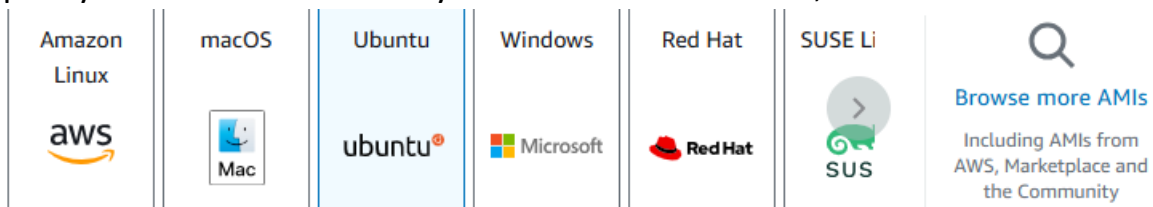
NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

Ec2 Instance : is a web service that provides resizable compute capacity in the cloud. It allows you to run virtual servers, known as EC2 instances



Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

Free tier eligible

ami-0866a3c8686eaeeba (64-bit (x86)) / ami-0325498274077fac5 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture

64-bit (x86)

AMI ID

ami-0866a3c8686eaeeba

Username

ubuntu



Verified provider

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

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Windows base pricing: 0.0162 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

☐ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

Security group of Instance

I use **security groups** to ensure high security for my instance , in this case I use **SSH** to SSH is commonly used to securely connect to and manage your EC2 instances. By allowing inbound traffic on port 22, you enable secure remote access to your Instances , I use **MySQL/Aurora** is a popular relational database management system, and it typically uses port 3306 for communication.

sg-09954387a4d1d436e - project-secgroup Actions ▾

Details

Security group name project-secgroup	Security group ID sg-09954387a4d1d436e	Description ec2 secgroup	VPC ID vpc-02fd1190906a826f3
Owner 767997536243	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

Inbound rules (3) Manage tags Edit inbound rules

Q Search

<input type="checkbox"/>	Name ▾	Security group rule... ▾	IP version ▾	Type ▾	Protocol ▾	Port range ▾	Source ▾	Description
<input type="checkbox"/>	-	sgr-081bfd633955325...	IPv4	SSH	TCP	22	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-0f98ca36feca8dce6	IPv4	HTTP	TCP	80	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-0e6f7360bb2ceaa02	IPv4	MySQL/Aurora	TCP	3306	0.0.0.0/0	-

Security group of RDS

in the inbound I identify the source is the security group of the ec2 instance to insure no request connect RDS unless the ec2 instance

sg-0577ad2bb86be2c68 - rds-secgroup Actions ▾

Details

Security group name rds-secgroup	Security group ID sg-0577ad2bb86be2c68	Description RDS security group .	VPC ID vpc-02fd1190906a826f3
Owner 767997536243	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags







Inbound rules (1) Manage tags Edit inbound rules

Q Search

<input type="checkbox"/>	Name ▾	Security group rule... ▾	IP version ▾	Type ▾	Protocol ▾	Port range ▾	Source ▾	Description
<input type="checkbox"/>	-	sgr-065c82e4d59aff865	-	SSH	TCP	22	sg-09954387a4d1d43...	-

RDS :

Is a managed database service provided by AWS that simplifies the setup, operation, and scaling of relational databases in the cloud. RDS supports several database engines,

<input checked="" type="radio"/> MySQL 	<input type="radio"/> MariaDB 
<input type="radio"/> PostgreSQL 	<input type="radio"/> Oracle 
<input type="radio"/> Microsoft SQL Server 	<input type="radio"/> IBM Db2 

Edition

☒ MySQL Community

Engine version [Info](#)

View the engine versions that support the following database features.

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.

EC2 instance [Info](#)

Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

i-0b5443be950767550
ec22-project-lab22

Some VPC settings can't be changed when a compute resource is added
Adding an EC2 compute resource automatically selects the VPC, DB subnet group, and public access settings for this database. To allow the EC2 instance to access the database, a VPC security group rds-ec2-X is added to the database and another called ec2-rds-X to the EC2 instance. You can remove the new security group for the database only by removing the compute resource.

Virtual private cloud (VPC) [Info](#)

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

project-lab-vpc (vpc-02fd1190906a826f3)
9 Subnets, 5 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.

- ☒ **Choose existing**
Choose existing DB subnet group
- ☐ **Automatic setup**
RDS creates a new subnet group for you or reuses an existing subnet group

Cloud9 :

Is a cloud-based integrated development environment (IDE) that allows you to write, run, and debug your code using just a web browser. It provides a rich set of tools and features to streamline the development process, making it easier for developers to collaborate and manage their applications in the cloud. Here's a detailed overview of AWS Cloud9, including its features, benefits, and use cases.

Determines what the Cloud9 IDE will run on.

☒ **New EC2 instance**

Cloud9 creates an EC2 instance in your account. The configuration of your EC2 instance cannot be changed by Cloud9 after creation.

☐ **Existing compute**

You have an existing instance or server that you'd like to use.

New EC2 instance

Instance type [Info](#)

The memory and CPU of the EC2 instance that will be created for Cloud9 to run on.

☐ **t2.micro (1 GiB RAM + 1 vCPU)**

Free-tier eligible. Ideal for educational users and exploration.

☐ **t3.small (2 GiB RAM + 2 vCPU)**

Recommended for small web projects.

☐ **m5.large (8 GiB RAM + 2 vCPU)**

Recommended for production and most general-purpose development.

☒ **Additional instance types**

Explore additional instances to fit your need.

Additional instance types

t3.large

Platform [Info](#)

This will be installed on your EC2 instance. We recommend Amazon Linux 2023.

Amazon Linux 2023

Timeout

How long Cloud9 can be inactive (no user input) before auto-hibernating. This helps prevent unnecessary charges.

30 minutes

Application load balancer :

Is a service that automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances

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 or 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 [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 1 using VPC peering. To confirm the VPC for your targets, view [target groups](#). For a new VPC, [create a VPC](#).

project-lab-vpc
vpc-02fd1190906a826f3
IPv4 VPC 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, the load balancer or the VPC are not available for selection.

Availability Zones

☒ **us-east-1a (use1-az1)**

Subnet

subnet-03b2481875dde5b30
IPv4 subnet CIDR: 10.0.32.0/25

RDS-Pvt-subnet-1

Target Group :

Is a logical grouping of resources (such as EC2 instances, IP addresses, or AWS Lambda functions) that you want the load balancer to route traffic to.

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

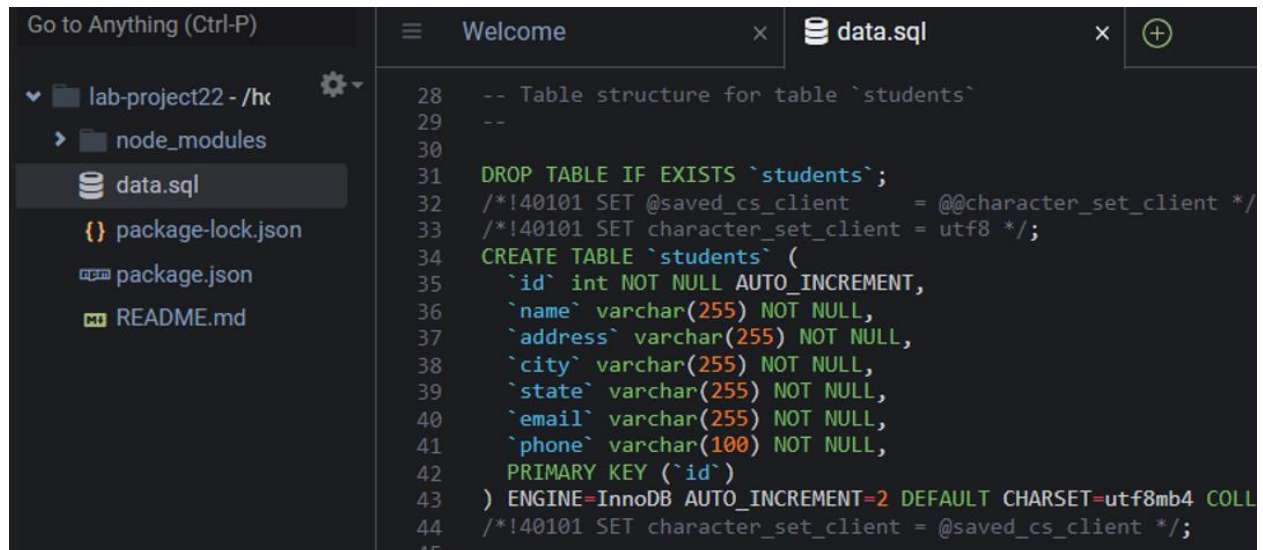
Basic configuration
Settings in this section can't be changed after the target group is created.

Choose a target type

☒ **Instances**

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

DB authentication with CLOUD9 IDE :

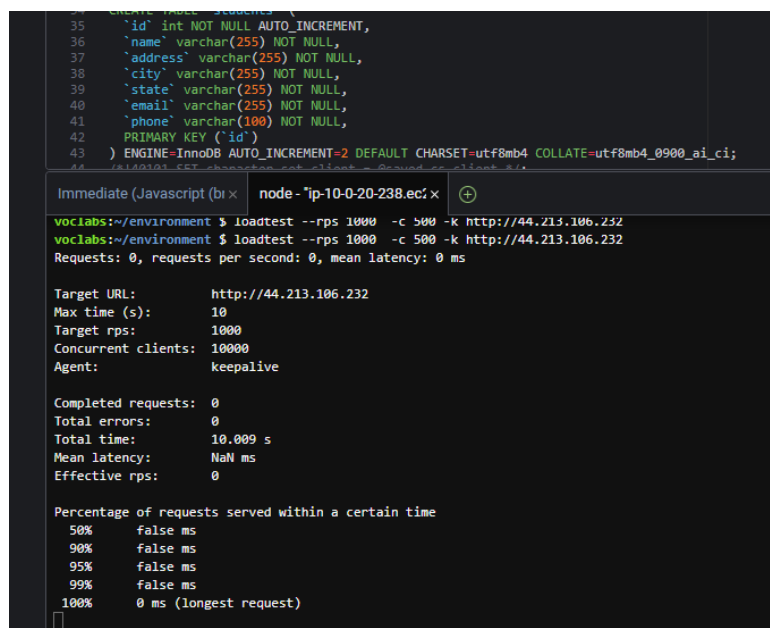


```
28 -- Table structure for table `students`
29 --
30
31 DROP TABLE IF EXISTS `students`;
32 /*!40101 SET @saved_cs_client      = @@character_set_client */;
33 /*!40101 SET character_set_client = utf8 */;
34 CREATE TABLE `students` (
35   `id` int NOT NULL AUTO_INCREMENT,
36   `name` varchar(255) NOT NULL,
37   `address` varchar(255) NOT NULL,
38   `city` varchar(255) NOT NULL,
39   `state` varchar(255) NOT NULL,
40   `email` varchar(255) NOT NULL,
41   `phone` varchar(100) NOT NULL,
42   PRIMARY KEY (`id`)
43 ) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=utf8mb4 COLL
44 /*!40101 SET character_set_client = @saved_cs_client */;
45
```



```
--
-- Dumping data for table `students`
--
--
LOCK TABLES `students` WRITE;
/*!40000 ALTER TABLE `students` DISABLE KEYS */;
INSERT INTO `students` VALUES (1,'ziad mohamed ismail','giza','Giza','giza','ziadmohamd333@gmail.com','01152259562');
/*!40000 ALTER TABLE `students` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

Cloud9 with load test :



```
35 CREATE TABLE `students` (
36   `id` int NOT NULL AUTO_INCREMENT,
37   `name` varchar(255) NOT NULL,
38   `address` varchar(255) NOT NULL,
39   `city` varchar(255) NOT NULL,
40   `state` varchar(255) NOT NULL,
41   `email` varchar(255) NOT NULL,
42   `phone` varchar(100) NOT NULL,
43   PRIMARY KEY (`id`)
44 ) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
45

Immediate (Javascript (bi x) node- 'ip-10-0-20-238.ec2.x' +
voclabs:~/environment $ loadtest --rps 1000 -c 500 -k http://44.213.106.232
voclabs:~/environment $ loadtest --rps 1000 -c 500 -k http://44.213.106.232
Requests: 0, requests per second: 0, mean latency: 0 ms

Target URL:      http://44.213.106.232
Max time (s):    10
Target rps:      1000
Concurrent clients: 10000
Agent:           keepalive

Completed requests: 0
Total errors:      0
Total time:        10.009 s
Mean latency:      NaN ms
Effective rps:     0


Percentage of requests served within a certain time
50%    false ms
90%    false ms
95%    false ms
99%    false ms
100%   0 ms (longest request)
```

Finally, I tested the output of the application and inserted my data into the application. :

Lab Instructions: Buildir x Load balancer details | x VpcDetails | VPC Conso x EC2 Instance Connect x Students x lab-project22 - AWS Cl x

44.213.106.232/students

CS2 term 2 - Googl... Harver تصميم تجربة المستخدم Backend Developer... Task List edabit - Search Day 7: Regular Expr... Introduction to Nod... ChatGPT



XYZ University

[Home](#)[Students list](#)

All students

Name	Address	City	State	Email	Phone	
ziad mohamed ismail	giza	Giza	giza	ziadmohamd333@gmail.com	01152259562	edit
mohamed mmmm	giza	Giza	giza	ziadmohamd333@gmail.com	01152259562	edit

[Add a new student](#)