



## **Deployment of a Secure and Scalable 3-Tier Web Application on AWS**

**This project was completed by Sarra Soyah and Rania Trabelsi  
Under the supervision of Heithem Abbes**

**Group: IDS3**

**2024/2025**

## **Content**

### **Executive Summary**

### **1 Project Setup**

#### **1.1 Repository Cloning and Initial Setup**

### **2 Networking and Security**

#### **2.1 VPC and Subnet Configuration**

#### **2.2 Routing and Internet Access**

### **3 Security Groups Configuration**

### **4 Database Layer: Amazon RDS**

#### **4.1 Subnet Groups and Configuration**

### **5 Backend Deployment**

### **6 Frontend Deployment**

### **7 External Load Balancer and Auto Scaling**

### **8 Monitoring and Logging**

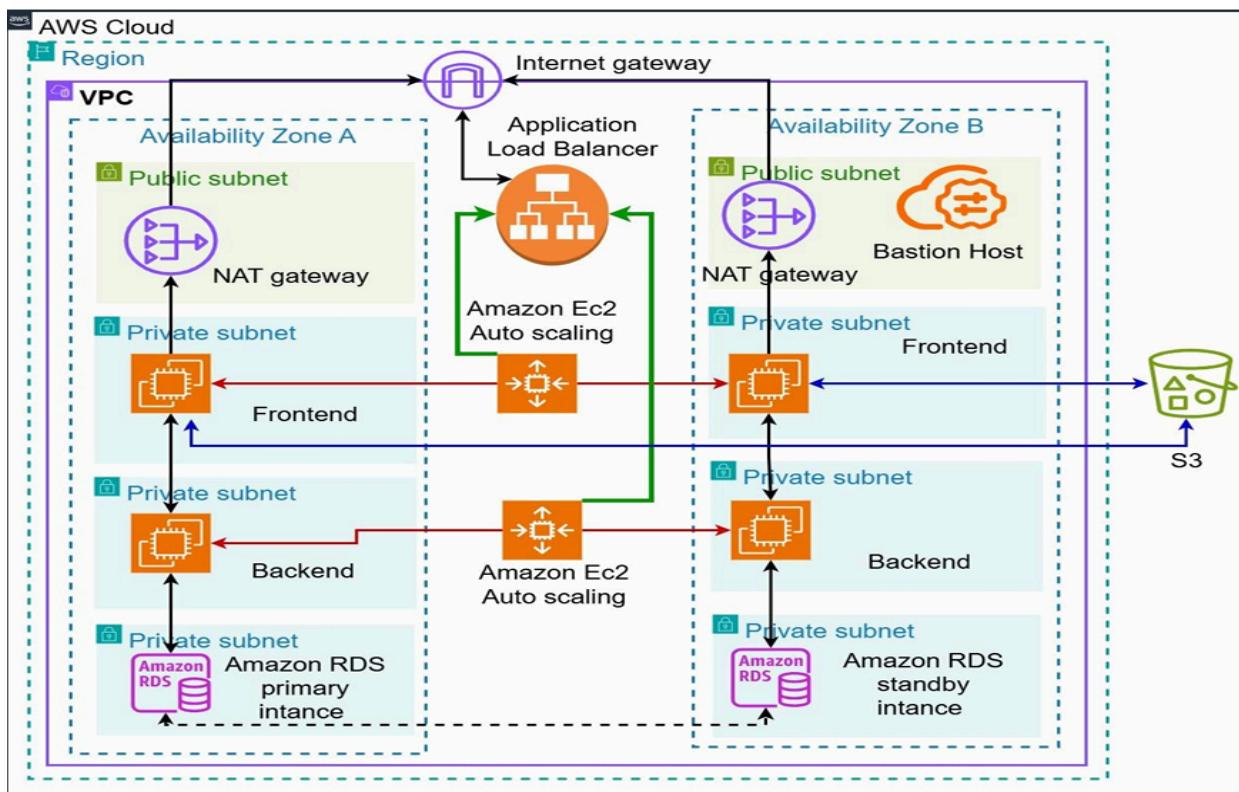
#### **8.1 CloudWatch and CloudTrail**

### **Conclusion**

## Executive Summary

This project focuses on the deployment of a secure, scalable 3-tier web application using Amazon Web Services (AWS). The architecture consists of a web (frontend) layer, an application (backend) layer, and a database layer, all hosted in a Virtual Private Cloud (VPC). We implemented robust security practices, high availability via load balancers and auto scaling groups, and monitoring mechanisms to ensure operational efficiency. This hands-on project enhanced our practical understanding of cloud infrastructure and secure application deployment.

## Architecture:



## Useful\_Link:

<https://catalog.us-east-1.prod.workshops.aws/workshops/85cd2bb2-7f79-4e96-bde-8078e469752a/en-US/cleanup>

## 1. Project Setup

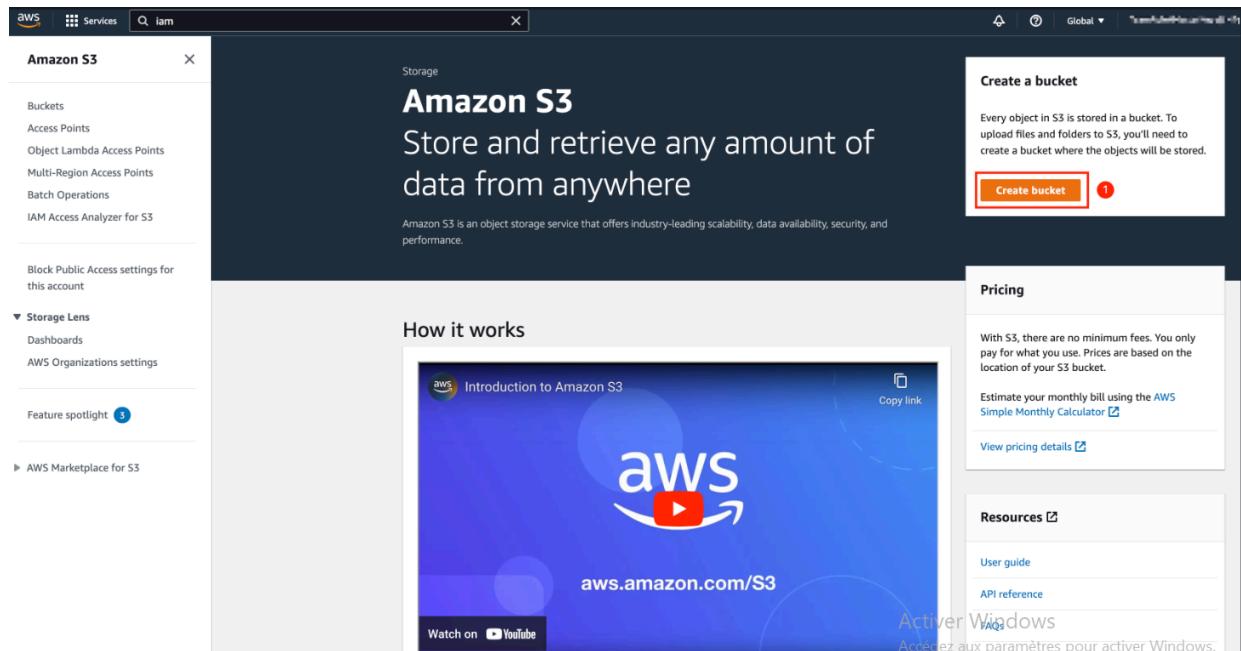
The project began by cloning the official AWS 3-tier web architecture GitHub repository and preparing an S3 bucket for frontend and backend storage. This allowed us to maintain separation of concerns and stage files before deployment.

### Repository:

git clone

<https://github.com/aws-samples/aws-three-tier-web-architecture-workshop>.

git



## 2. Networking and Security

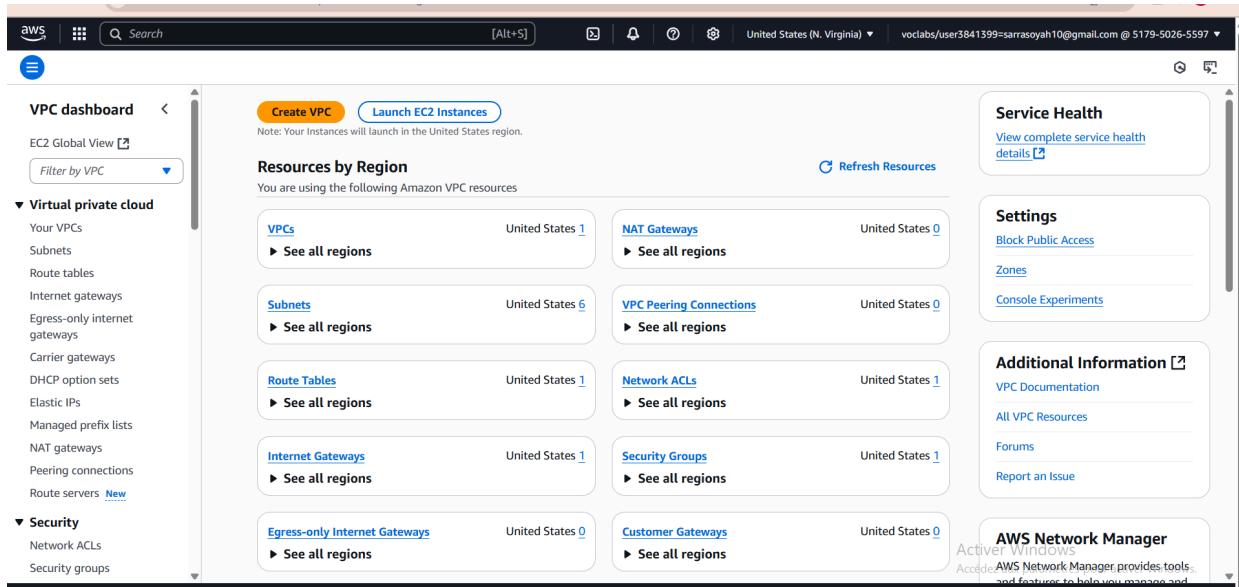
### 2.1 VPC and Subnet Configuration

We created a custom VPC (10.0.0.0/16) with eight subnets across two Availability Zones (AZs) for redundancy.

## 2.2 Internet Access and Routing

We created:

- An Internet Gateway attached to the VPC to allow public subnets to access the internet.
- A NAT Gateway for private instances to access the internet securely (for software updates, etc.).
- Custom route tables for public and private traffic management. For example:
  - Public subnets route internet-bound traffic to the Internet Gateway.
  - Private subnets use the NAT Gateway route.



The screenshot shows the AWS VPC Create VPC workflow. The current step is 'Create S3 endpoint'. The progress bar indicates 11% completion. Below the progress bar, a list of tasks is shown:

- Create VPC: vpc-001e36c180e5b72c0
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: vpc-001e36c180e5b72c0
- Create S3 endpoint
- Create subnet
- Create internet gateway
- Attach internet gateway to the VPC
- Create route table
- Create route
- Associate route table
- Associate route table
- Allocate elastic IP
- Allocate elastic IP
- Create NAT gateway

On the right side of the screen, there is a message in French: "Activer Windows" and "Accédez aux paramètres pour activer Windows."

The screenshot shows the AWS VPC Create VPC workflow. The current step is 'Associate S3 endpoint with private subnet route tables: vpce-01501a65373db1961'. The progress bar indicates 11% completion. Below the progress bar, a list of tasks is shown:

- Create internet gateway: igw-0678eca9b8c53904e
- Attach internet gateway to the VPC
- Create route table: rtb-0feec542b27bcfeda
- Create route
- Associate route table
- Associate route table
- Allocate elastic IP: eipalloc-0515cce3b3e71477
- Allocate elastic IP: eipalloc-0d3f92c5db150ebd8
- Create NAT gateway: nat-0eb00de1c381c5075
- Create NAT gateway: nat-0760070c7530464a1
- Wait for NAT Gateways to activate
- Create route table
- Create route
- Associate route table
- Create route table
- Create route
- Associate route table
- Create route table
- Create route
- Associate route table
- Associate route table
- Verifying route table creation
- Associate S3 endpoint with private subnet route tables: vpce-01501a65373db1961

On the right side of the screen, there is a message in French: "Activer Windows" and "Accédez aux paramètres pour activer Windows."

## Adding two more subnets

The screenshot shows the AWS VPC Subnets creation interface. It displays two subnets being created:

- Subnet 1 of 2**: CIDR 10.0.0.0/16, associated with VPC ID vpc-001e36c180e5b72c0 (project-vpc) and Availability Zone us-east-1a.
- Subnet 2 of 2**: CIDR 10.0.32.0/24, associated with VPC ID vpc-001e36c180e5b72c0 (project-vpc) and Availability Zone us-east-1b.

Both subnets have optional tags: rds-A and RDS-B. The interface includes sections for Subnet settings, Subnet name, Availability Zone, IPv4 VPC CIDR block, and IPv4 subnet CIDR block. A note at the bottom right indicates "Activer Windows" (Enable Windows).

## Renaming of route tables

Screenshot of the AWS VPC Route Tables page showing the creation and deletion of route tables.

**Route tables (1/1) Info**

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
project-rtb-private1-us-east-1a	rtb-0fe3202619649389	2 subnets	-	No	vpc-001e36c180e5b72c0   proj...	517950265597

**Edit Name**

project-rtb-private1-us-east-1a

**Details**

Route table ID: rtb-0faeb118cde498d  
Main: No  
Owner ID: 517950265597

**Explicit subnet associations**

subnet-0fe3202619649389 / project-subnet-front-us-east-1a

**Edge associations**

Activer Windows  
Accédez aux paramètres pour activer Windows.

**Route tables (1/5) Info**

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
project-rtb-private2-us-east-1b	rtb-09d2ad988f5080340	3 subnets	-	No	vpc-001e36c180e5b72c0   proj...	517950265597
project-rtb-public	rtb-0a325856bf2833a60	-	-	Yes	vpc-001e36c180e5b72c0   proj...	517950265597
project-rtb-private4-us-east-1b	rtb-0fe3202619649389	3 subnets	-	No	vpc-001e36c180e5b72c0   proj...	517950265597
project-rtb-private3-us-east-1a	rtb-0917267dff0cd23	2 subnets	-	No	vpc-001e36c180e5b72c0   proj...	517950265597
-	rtb-0a88beb699c0b845e5	-	-	Yes	vpc-0df9b29aeafdf8789c	517950265597

**Subnet associations**

You have successfully deleted rtb-02af885abbb8a025 / project-rtb-private4-us-east-1b

**Explicit subnet associations (3)**

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
rds-A	subnet-0e42598e95f50548d	10.0.35.0/24	-
project-subnet-back-us-east-1a	subnet-0917267dff0cd2382	10.0.160.0/20	-
project-subnet-front-us-east-1a	subnet-0fe3202619649389	10.0.128.0/20	-

**Subnets without explicit associations (0)**

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Activer Windows  
Accédez aux paramètres pour activer Windows.

## Final Ressource Map:

### 3. Security Groups Configuration

We adopted a layered security model with multiple Security Groups:

- **SG-Bastion:** allowing ssh from my IP
- **SG-ExternalLB:** allowing http/https from the internet
- **SG-Frontend:** allowing http/https from SG-ExternalLB and ssh from SG-Bastion
- **SG-InternalLB:** allowing http/https from SG-Frontend
- **SG-Backend:** allowing custom TCP on port 4000 from SG-InternalLB and ssh from SG-Bastion
- **SG-DB:** allowing MySQL/Aurora on port 3306 from SG-Backend

#### SG-bastion

**Create security group** [Info](#)

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](#)  
SG-Bastion  
Name cannot be edited after creation.

Description [Info](#)  
acces SSH depuis une IP fixe

VPC info  
vpc-001e36c180e5b72c0 (project-vpc)

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	My IP	196.227.96.81/32

[Add rule](#)

**Outbound rules** [Info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	0.0.0.0/0

[Add rule](#)

⚠️ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

[Activer Windows](#) [Accédez aux paramètres pour activer Windows.](#)

## SG-external-LB:

**Create security group** [Info](#)

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](#)  
SG-LB-internetfacing  
Name cannot be edited after creation.

Description [Info](#)  
acces http et https from internet

VPC info  
vpc-001e36c180e5b72c0 (project-vpc)

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Anywhere	0.0.0.0/0
HTTPS	TCP	443	Anywhere	0.0.0.0/0

[Add rule](#)

⚠️ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

**Outbound rules** [Info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	0.0.0.0/0

[Add rule](#)

[Activer Windows](#) [Accédez aux paramètres pour activer Windows.](#)

## SG-FE

**Create security group** Info

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  
SG-FE  
Name cannot be edited after creation.

Description Info  
acces http https et ssh from external LB

VPC info  
vpc-001e36c180e5b72c0 (project-vpc)

### Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
HTTP	TCP	80	Custom <input type="button" value="Delete"/>	Q sg-0b7f2f82d46b8f50e <input type="button" value="Delete"/> sg-0b7f2f82d46b8f50e <input type="button" value="Delete"/>
HTTPS	TCP	443	Custom <input type="button" value="Delete"/>	Q sg-0b7f2f82d46b8f50e <input type="button" value="Delete"/> sg-0b7f2f82d46b8f50e <input type="button" value="Delete"/>
SSH	TCP	22	Custom <input type="button" value="Delete"/>	Q sg-070dec0e94eaee533a <input type="button" value="Delete"/> sg-070dec0e94eaee533a <input type="button" value="Delete"/>

[Add rule](#)

### Outbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - optional <small>Info</small>
All traffic	All	All	Custom <input type="button" value="Delete"/>	Q 0.0.0.0 <input type="button" value="Delete"/> 0.0.0.0 <input type="button" value="Delete"/>

[Activer Windows](#) (Défaut)  
Accédez aux paramètres pour activer Windows.

## SG-internalLB

[Cloudshell](#) [Feedback](#)

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSecurityGroup:

[aws](#) [Search](#) [Alt+S] United States (N. Virginia) vociabs/user3641399=sarrasoyah10@gmail.com @ S179-5026-5597

[VPC](#) > [Security Groups](#) > Create security group

**Create security group** Info

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  
Internal-LB  
Name cannot be edited after creation.

Description Info  
Http https from FE

VPC info  
vpc-001e36c180e5b72c0 (project-vpc)

### Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
HTTP	TCP	80	Custom <input type="button" value="Delete"/>	Q sg-040634a1d74d93e9d <input type="button" value="Delete"/> sg-040634a1d74d93e9d <input type="button" value="Delete"/>
HTTPS	TCP	443	Custom <input type="button" value="Delete"/>	Q sg-040634a1d74d93e9d <input type="button" value="Delete"/> sg-040634a1d74d93e9d <input type="button" value="Delete"/>

[Add rule](#)

### Outbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - optional <small>Info</small>
All traffic	All	All	Custom <input type="button" value="Delete"/>	Q 0.0.0.0 <input type="button" value="Delete"/> 0.0.0.0 <input type="button" value="Delete"/>

[Activer Windows](#) (Défaut)  
Accédez aux paramètres pour activer Windows.

## SG-BE

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSecurityGroup:

**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](#)  
SG-BE  
Name cannot be edited after creation.

Description [Info](#)  
access custom tcp from internal LB on port 4000 and ssh from bastion

VPC info  
vpc-001e36c180e5b72c0 (project-vpc)

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	4000	Custom	sg-0335de3514f154639 <a href="#">X</a> <a href="#">Delete</a>
SSH	TCP	22	Custom	sg-0335de3514f154639 <a href="#">X</a> sg-070dec0e94eae333a <a href="#">X</a> <a href="#">Delete</a>

[Add rule](#)

**Outbound rules** [Info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	0.0.0.0/0 <a href="#">X</a> <a href="#">Delete</a>

[Add rule](#)

Activer Windows  
Accédez aux paramètres pour activer Windows.

## SG-RDS

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSecurityGroup:

**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](#)  
DB-securitygroup  
Name cannot be edited after creation.

Description [Info](#)  
accept traffic from BE on port 3306

VPC info  
vpc-001e36c180e5b72c0 (project-vpc)

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional
MySQL/Aurora	TCP	3306	Custom	sg-0a9b4ecc5885a7e89 <a href="#">X</a> sg-0a9b4ecc5885a7e89 <a href="#">X</a> <a href="#">Delete</a>

[Add rule](#)

**Outbound rules** [Info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	0.0.0.0/0 <a href="#">X</a> <a href="#">Delete</a>

[Add rule](#)

⚠️ Rules with destination of 0.0.0.0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses. [Learn More](#)

Activer Windows  
Accédez aux paramètres pour activer Windows.

## 4. Database Layer: Amazon RDS

We deployed a MySQL database on Amazon RDS with Multi-AZ support:

- Created RDS Subnet Groups using the two private RDS subnets
- Configured automatic failover with a primary (writer) and secondary (reader) instance

- Enabled automated backups, monitoring, and CloudWatch alarms
- Retrieved the RDS endpoint and updated dbconfig.js in the backend to connect securely using private IPs

## ● Creating Subnet Groups

The screenshot shows the AWS Aurora and RDS Subnet groups page. The left sidebar includes options like Dashboard, Databases, Query editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups (selected), Parameter groups, Option groups, Custom engine versions, Zero-ETL integrations, Events, Event subscriptions, Recommendations, and Certificate update. The main content area displays a table titled 'Subnet groups (0)' with columns for Name, Description, Status, and VPC. A message states 'No db subnet groups' and 'You don't have any db subnet groups.' A blue button labeled 'Create DB subnet group' is visible.

The screenshot shows the 'Create DB subnet group' wizard. Step 1: Create DB subnet group details. It asks for a Name (DB-Subnet-Group) and a Description (subnet group of RDS A and B). It also requires selecting a VPC (project-vpc (vpc-001e36c180e5b72c0)). A note says '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.'

The screenshot shows the 'Create DB subnet group' wizard. Step 2: Add subnets. It lists 'Availability Zones' (us-east-1a, us-east-1b) and 'Subnets' (RDS-B, rds-A). A note says 'Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.' A blue button at the bottom says 'Next Step'.

Subnet groups (1)				
<input type="text"/> Filter by subnet group		Description	Status	VPC
<input type="checkbox"/>	Name	db-subnet-group	subnet group of RDS A and B	Complete

## • Database Configuration

us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:

**Create database** Info

**Choose a database creation method**

- Standard create You set all of the configuration options, including ones for availability, security, backups, and maintenance.
- Easy create Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

**Engine options**

Engine type Info

- Aurora (MySQL Compatible) 
- Aurora (PostgreSQL Compatible) 
- MySQL 
- PostgreSQL 
- MariaDB 
- Oracle 
- Microsoft SQL Server 
- IBM Db2 

Engine version Engine version

Aurora MySQL-Compatible Edition >

Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

Activer Windows Accédez aux paramètres pour activer Windows.

**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.

**Settings**

**DB cluster identifier** Info Enter a name for your DB cluster. The name must be unique across all DB clusters owned by your AWS account in the current AWS Region.

database-1

The DB cluster identifier is case-insensitive, but is stored as all lowercase (as in "mydbcluster"). 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.

admin

1 to 32 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.

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

**Master password** Info

\*\*\*\*\*

Password strength Weak

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

Confirm master password Info

Activer Windows Accédez aux paramètres pour

Aurora MySQL-Compatible Edition >

Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

**Cluster storage configuration** [Info](#)

Choose the storage configuration for the Aurora DB cluster that best fits your application's price predictability and price performance needs.

**Configuration options**

Database instance, storage, and I/O charges vary depending on the configuration. [Learn more](#)

Aurora I/O-Optimized

- Predictable pricing for all applications. Improved price performance for I/O-intensive applications (I/O costs >25% of total database costs).
- No additional charges for read/write I/O operations. DB instance and storage prices include I/O usage.

Aurora Standard

- Cost-effective pricing for many applications with moderate I/O usage (I/O costs <25% of total database costs).
- Pay-per-request I/O charges apply. DB instance and storage prices don't include I/O usage.

Aurora MySQL is Amazon's enterprise-class MySQL database.

**Aurora MySQL offers:**

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling storage
- Six-way replication across Availability Zones
- Up to 15 read replicas with lag under 10-millisecond latency
- Automatic monitoring and failover

**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**

Include previous generation classes

Serverless v2

Memory optimized classes (includes r classes)

Burstable classes (includes t classes)

**db.t3.medium**

2 vCPUs | 4 GiB RAM | Network: Up to 2085 Mbps

**Availability & durability**

**Multi-AZ deployment** [Info](#)

**Availability & durability**

**Multi-AZ deployment** [Info](#)

Create an Aurora Replica or Reader node in a different AZ (recommended for scaled availability)

Creates an Aurora Replica for fast failover and high availability.

Don't create an Aurora Replica

**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 cluster.

**project-vpc (vpc-001e36c180e5b72c0)**

8 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 cluster 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 cluster. Amazon EC2 instances and other resources outside of the VPC can connect to your cluster. Resources inside the VPC can also connect to the cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

No

RDS doesn't assign a public IP address to the cluster. Only Amazon EC2 instances and other resources inside the VPC can connect to your cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

**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

Create new

**Existing VPC security groups**

Choose one or more options

**DB-securitygroup** X

**RDS Proxy**

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

Create an RDS Proxy

RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see [Amazon RDS Proxy pricing](#).

**Certificate authority - optional** [Info](#)

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

**rds-ca-rsa2048-g1 (default)**

Expiry: May 26, 2061

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

**► Additional configuration**

**Monitoring** [Info](#)

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

<input type="radio"/> Database Insights - Advanced <ul style="list-style-type: none"> <li>Retains 15 months of performance history</li> <li>Fleet-level monitoring</li> <li>Integration with CloudWatch Application Signals</li> </ul>	<input checked="" type="radio"/> Database Insights - Standard
--	---

**Additional monitoring settings**  
[Enhanced Monitoring](#), [CloudWatch Logs](#) and [DevOps Guru](#)

**Enhanced Monitoring**

[Enable Enhanced monitoring](#)  
 Enabling Enhanced Monitoring metrics are useful when you want to see how different processes or threads use the CPU.

**Log exports**  
 Select the log types to publish to Amazon CloudWatch Logs

- Audit log
- Error log
- General log
- db-error-log
- instance log
- slow-query-log

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

RDS service-linked role

**Backup**

**Backup retention period** [Info](#)  
 The number of days (1-35) for which automatic backups are kept.  
 day

[Copy tags to snapshots](#)

**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](#)

**Backtrack**

Backtrack lets you quickly rewind the DB cluster to a specific point in time, without having to create another DB cluster. [Info](#)

[Enable Backtrack](#)  
 Enabling Backtrack will charge you for storing the changes you make for backtracking.

**Maintenance**

Auto minor version upgrade [Info](#)

[Enable auto minor version upgrade](#)  
 Enabling auto minor version upgrade will automatically upgrade your database minor version. For limitations and more details, see [Automatically upgrading the minor engine version documentation](#).

**Maintenance window** [Info](#)  
 Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

[Choose a window](#)  
 [No preference](#)

[Enable deletion protection](#)  
 Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

**Compat**

Aurora MySQL enterprise-class database.

- Up to 8 of MySQL
- Up to 1 storage
- Six-way Availability
- Up to 1 lag and
- Automatic failover

**Compatible**

Aurora MySQL is enterprise-class database.

Aurora MySQL off

- Up to five times of MySQL Concurrency
- Up to 128 TB of storage
- Six-way replication
- Up to 15 read replicas
- Up to 10 read lag under 10 ms
- Automatic failover

**Activer Windows**  
[Accédez aux paramètres pour activer](#)

## Database read et write for automatic failover

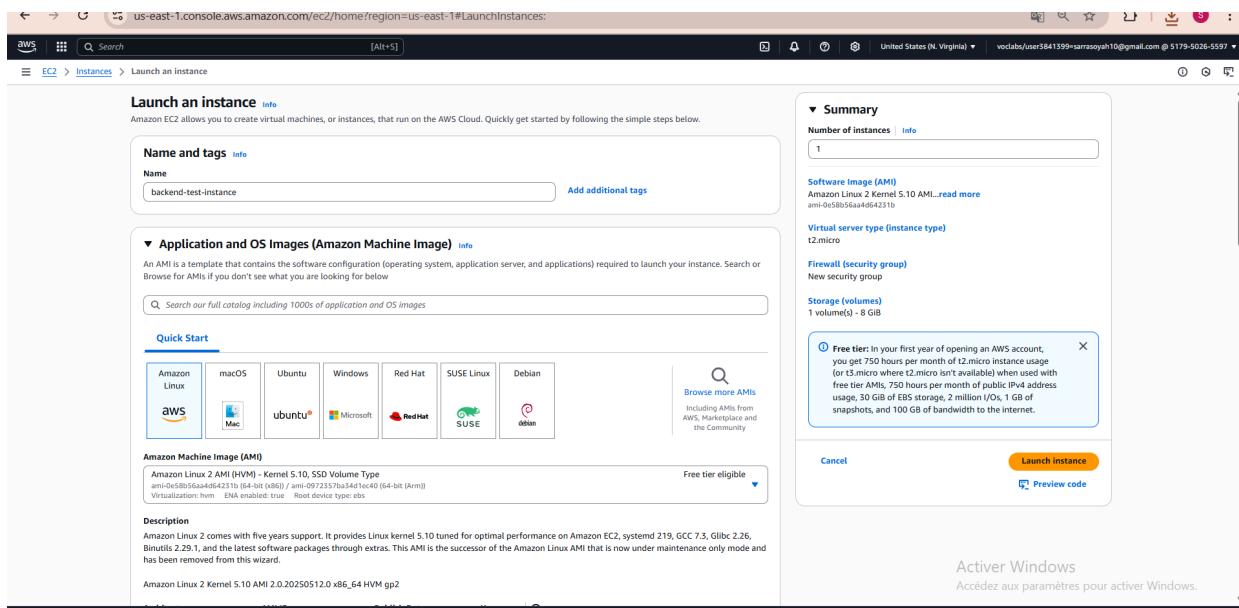
Databases (3)											<a href="#">Create database</a>	
		Status	Role	Engine	Region ...	Size	Recommendations	CPU	Current activity	Ma		
<input type="radio"/>	<input type="checkbox"/> <a href="#">database-1</a>	<a href="#">Creating</a>	Regional cluster	Aurora My...	us-east-1	2 instances	-	-	-	nor		
<input type="radio"/>	<input type="checkbox"/> <a href="#">database-1-instance-1</a>	<a href="#">Creating</a>	Reader instance	Aurora My...	-	db.t3.medium	-	-	-	nor		
<input type="radio"/>	<input type="checkbox"/> <a href="#">database-1-instance-1-us-east-1a</a>	<a href="#">Creating</a>	Reader instance	Aurora My...	us-east-1a	db.t3.medium	-	-	-	nor		

## 5. Backend Deployment

- Launched EC2 instances for the backend in the private application subnets
- Attached the LambdaInstanceProfile IAM role

- Connected via Bastion instance using SSH
- Installed Node.js and other dependencies
- Used the private RDS endpoint and updated configuration in dbconfig.js
- Uploaded backend files to S3
- Configured Internal Load Balancer and Target Group
- Created a Launch Template and Auto Scaling Group for backend servers with health checks enabled

### • Creating Backend Instance



**Amazon Machine Image (AMI)**

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-0e58b56aa4d64231b (64-bit (x86)) / ami-0972357ba34d1ec40 (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Amazon Linux 2 Kernel 5.10 AMI 2.0.20250512.0 x86\_64 HVM gp2

Architecture	AMI ID	Publish Date	Username	Verified provider
64-bit (x86)	ami-0e58b56aa4d64231b	2025-05-10	ec2-user	

**Number of instances** | [Info](#)  
1

**Software Image (AMI)**  
Amazon Linux 2 Kernel 5.10 AMI... [read more](#)  
ami-0e58b56aa4d64231b

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
New security group

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

**Free tier:** In your first year of opening a you get 750 hours per month of t2.micro (or t3.micro where t2.micro isn't available) free tier AMIs, 750 hours per month of usage, 30 GiB of EBS storage, 2 million snapshots, and 100 GB of bandwidth to

[Cancel](#)

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

**Instance type**

t2.micro  
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

All generations

[Compare instance types](#)

**Additional costs apply for AMIs with pre-installed software**

**▼ Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

**Key pair name - required**

sarania

[Create new key pair](#)

[Acti](#)  
[Accé](#)

**▼ Network settings** [Info](#)

**VPC - required** | [Info](#)

vpc-001e36c180e5b72c0 (project-vpc)  
10.0.0.0/16

**Subnet** | [Info](#)

subnet-0917267dff0cd2382 project-subnet-back-us-east-1a  
VPC: vpc-001e36c180e5b72c0 Owner: 517950265597 Availability Zone: us-east-1a  
Zone type: Availability Zone IP addresses available: 4091 CIDR: 10.0.160.0/20

[Create new subnet](#)

**Auto-assign public IP** | [Info](#)

Disable

**Firewall (security groups)** | [Info](#)

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

Create security group  Select existing security group

**Common security groups** | [Info](#)

Select security groups

SG-BE sg-0a9b4ecc5885a7e89 X  
VPC: vpc-001e36c180e5b72c0

[Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

**► Advanced network configuration**

▼ Advanced details [Info](#)

Domain join directory | [Info](#)

Select [Create new directory](#)

IAM instance profile | [Info](#)

LabInstanceProfile [arn:aws:iam::517950265597:instance-profile/LabInstanceProfile](#) [Create new IAM profile](#)

Hostname type | [Info](#)

IP name [Select](#)

DNS Hostname | [Info](#)

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

Instance auto-recovery | [Info](#)

Select [Select](#)

Shutdown behavior | [Info](#)

Stop [Select](#)

Stop - Hibernate behavior | [Info](#)

Select [Select](#)

Termination protection | [Info](#)

Select [Select](#)

Stop protection | [Info](#)

## ● Creating Bastion Instance to connect to the backend one

aws [Search](#) [Alt+S]

EC2 Instances Launch an instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name: bastion-instance [Add additional tags](#)

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS Images

Recent [Quick Start](#)

Amazon Linux [aws](#) macOS [Mac](#) Ubuntu [ubuntu](#) Windows [Microsoft](#) Red Hat [Red Hat](#) SUSE Linux [SUSE](#) Debian [debian](#)

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-09534766d0561c95 (64-bit (x86), uefi-preferred) / ami-05a3e0187917c3e24 (64-bit (Arm), uefi)  
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.7.20250512.0.x86\_64 HVM kernel-6.1

Architecture Boot mode AMI ID Publish Date Username

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.7.2... [read more](#)

ami-09534766d0561c95

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volumet(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro when t2.micro isn't available) when used with free tier AMIs. 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel [Launch instance](#) [Preview code](#)

Activer Windows  
Accédez aux paramètres pour activer Windows.

Cloudshell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

The screenshot shows the AWS Lambda Create Function wizard. The current step is "Configure instance settings".

**Instance type:** t2.micro (Free tier eligible)

**Key pair (login):** sarania (Create new key pair)

**Network settings:**

- VPC - required:** project-vpc (10.0.0.0/16)
- Subnet:** subnet-Ofeg63438faf736c3 (project-subnet-public1-us-east-1a)
- Auto-assign public IP:** Enable
- Firewall (security groups):** Select existing security group (SG-Bastion)
- Common security groups:** SG-Bastion sg-070dec0e94ae333a

**Summary:**

- Number of instances: 1
- Software Image (AMI): Amazon Linux 2023 AM ami-0953476d60561c955
- Virtual server type (in): t2.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB
- Free tier: In your free tier you get 750 hours (or t3.micro when you start using it).

**PS: Don't forget to always put LambdaProfile in IAM Role**

- Connecting to backend test instance from bastion

```

MINGW64:/c/Users/sarra/Downloads
sarra@DESKTOP-URGH140 MINGW64 ~/Downloads (master)
$ chmod 664 sarania.pem

sarra@DESKTOP-URGH140 MINGW64 ~/Downloads (master)
$ scp -i sarania.pem sarania.pem ec2-user@18.234.227.48:~
The authenticity of host '18.234.227.48 (18.234.227.48)' can't be established.
ED25519 key fingerprint is SHA256:VpNwMMOHknbbZB4B4rvccaHVDAK1wPWrS5fDCx4JA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '18.234.227.48' (ED25519) to the list of known hosts.
sarania.pem                                         100% 1674      8.0KB/s   00:00

sarra@DESKTOP-URGH140 MINGW64 ~/Downloads (master)
$
```

## Pinging the Instance

```

sarra@DESKTOP-URGH140 MINGW64 ~/Downloads (master)
$ ssh -i sarania.pem ec2-user@18.234.227.48
#_###_ Amazon Linux 2023
~~\###\ https://aws.amazon.com/linux/amazon-linux-2023
~~\###\ V~`-->
~~\###\ /`_
~~\###\ /`_
~~\###\ /`_
[ec2-user@ip-10-0-0-210 ~]$ ssh -i sarania.pem ec2-user@10.0.166.110
The authenticity of host '10.0.166.110 (10.0.166.110)' can't be established.
ED25519 key fingerprint is SHA256:s32xQ62AZYj3qb3lL09tz807wWkLRLWxtzJNPd1rjw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.166.110' (ED25519) to the list of known hosts.
@ WARNING: UNPROTECTED PRIVATE KEY FILE!
@ Permissions 0644 for 'sarania.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "sarania.pem": bad permissions
ec2-user@10.0.166.110: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-0-210 ~]$ chmod 400 sarania.pem
[ec2-user@ip-10-0-0-210 ~]$ ssh -i sarania.pem ec2-user@10.0.166.110
#_###_ Amazon Linux 2
~~\###\ AL2 End of Life is 2026-06-30.
~~\###\ V~`-->
~~\###\ /`_
~~\###\ /`_
A newer version of Amazon Linux is available!
~~\###\ /`_
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-166-110 ~]$ sudo -su ec2-user
[ec2-user@ip-10-0-166-110 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=1.48 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=1.61 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=0.992 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=1.27 ms
AC
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.992/1.341/1.617/0.236 ms
[ec2-user@ip-10-0-166-110 ~]$
```

```
[ec2-user@ip-10-0-166-110 ~]$ sudo yum install mysql -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Resolving Dependencies
--> Running transaction check
-->> Package mariadb.x86_64 1:5.5.68-1.amzn2.0.1 will be installed
-->> Finished Dependency Resolution
Dependencies Resolved

=====
| 3.6 kB 00:00:00

=====
Package          Arch      Version           Repository      Size
=====
Installing:
mariadb          x86_64   1:5.5.68-1.amzn2.0.1      amzn2-core      8.8 M
=====
Transaction Summary
=====
Install 1 Package

Total download size: 8.8 M
Installed size: 49 M
Downloading packages:
mariadb-5.5.68-1.amzn2.0.1.x86_64.rpm | 8.8 MB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64
  Verifying  : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64
Installed:
  mariadb.x86_64 1:5.5.68-1.amzn2.0.1
=====
[Complete!]

Active Windows
Accédez aux paramètres pour activer Windows.
```

## • Extracting the endpoint of the writer instance of RDS

Aurora and RDS > Databases > database-1 > database-1-instance-1

DB identifier	Status	Role	Engine	Region ...	Size	Recom...	CPU	Current...	Maintenance	VPC
database-1	Available	Regional...	Aurora My...	us-east-1	2 instances	-	-	-	none	-
database-1-instance-1	Available	Writer ins...	Aurora My...	us-east-1a	db.t3.med...	9.56%	2 Select	none	vpc-001e...	
database-1-instance-1-us-east-1a	Available	Reader ins...	Aurora My...	us-east-1a	db.t3.med...	9.46%	2 Select	none	vpc-001e...	

**Connectivity & security**

**Endpoint & port**

- Endpoint copied: database-1-instance-1.csbharcajjer.us-east-1.rds.amazonaws.com:3306

**Networking**

- Availability Zone: us-east-1a
- VPC: project-vpc (vpc-001e36c180e5b72c0)
- Subnet group: db-subnet-group
- Subnets: subnet-0e42598a95f30248d, subnet-0c5d494265f1f88c4
- Network type: IPv4

**Security**

- VPC security groups: DB-securitygroup (sg-004e5c762da1822ec) (Active)
- Publicly accessible: No
- Certificate authority: rds-ca-rsa2048-g1
- Certificate authority date: May 26, 2061, 00:34 (UTC+01:00)
- DB instance certificate expiration date: May 22, 2026, 23:43 (UTC+01:00)

**Security group rules (2)**

Active Windows

```
[ec2-user@ip-10-0-166-110 ~]$ mysql -h database-1-instance-1.csbharcajjer.us-east-1.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 163
Server version: 8.0.39 8bc99e28

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```

MySQL [(none)]> CREATE DATABASE webappdb;
Query OK, 1 row affected (0.00 sec)

MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| webappdb |
+-----+
5 rows in set (0.01 sec)

MySQL [(none)]>
MySQL [(none)]>
MySQL [(none)]> USE webappdb;
Database changed
MySQL [webappdb]> CREATE TABLE IF NOT EXISTS transactions(id INT NOT NULL
-> AUTO_INCREMENT, amount DECIMAL(10,2), description
-> VARCHAR(100), PRIMARY KEY(id));
Query OK, 0 rows affected (0.02 sec)

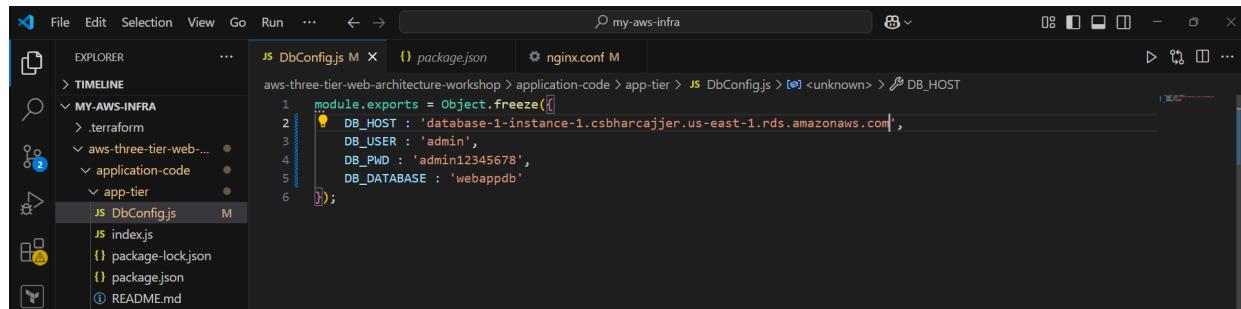
MySQL [webappdb]> SHOW TABLES;
+-----+
| Tables_in_webappdb |
+-----+
| transactions |
+-----+
1 row in set (0.00 sec)

MySQL [webappdb]> INSERT INTO transactions (amount,description) VALUES ('400','groceries');
Query OK, 1 row affected (0.00 sec)

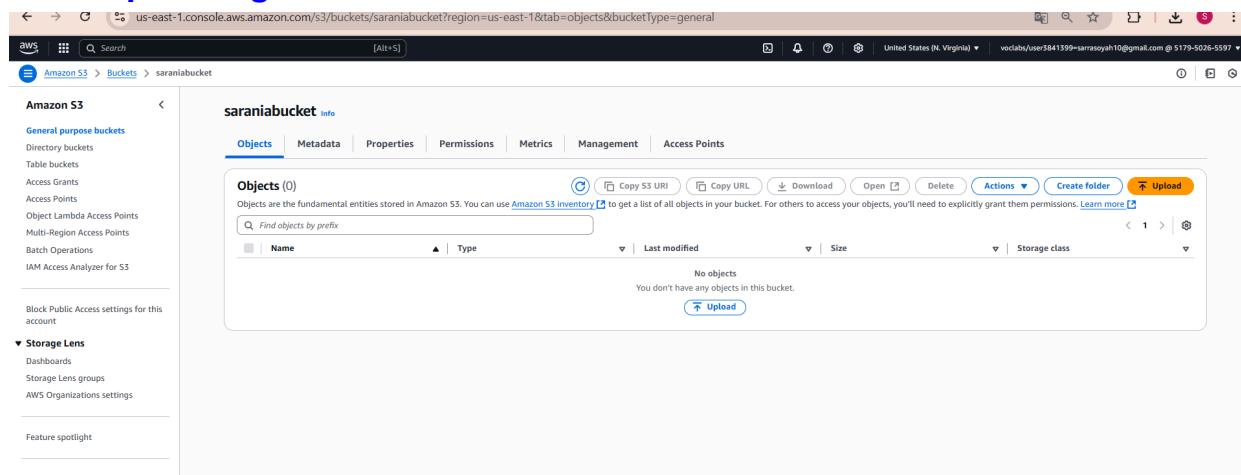
MySQL [webappdb]> SELECT * FROM transactions;
+----+----+----+
| id | amount | description |
+----+----+----+
| 1 | 400.00 | groceries |
+----+----+----+
1 row in set (0.00 sec)

```

- **Changing The DBConfig.js file with RDS credentials:**



- **Uploading backend files to our S3**



Amazon S3 > Buckets > saranabucket > Upload

### Upload info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

**Files and folders (6 total, 48.8 KB)**

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	DbConfig.js	app-tier/	text/javascript	203.0 B
<input type="checkbox"/>	index.js	app-tier/	text/javascript	3.2 kB
<input type="checkbox"/>	package-lock.json	app-tier/	application/json	42.9 kB
<input type="checkbox"/>	package.json	app-tier/	application/json	682.0 B
<input type="checkbox"/>	README.md	app-tier/	-	14.0 B
<input type="checkbox"/>	TransactionService.js	app-tier/	text/javascript	1.8 kB

**Destination info**

Destination [s3://saranabucket](#)

**Destination details**

Bucket settings that impact new objects stored in the specified destination.

**Permissions**

Grant public access and access to other AWS accounts.

**Properties**

Specify storage class, encryption settings, tags, and more.

Activer Windows  
Accédez aux paramètres pour activer Windows.

## • Creating the target group of the backend

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateTargetGroup:

aws [Alt+S]

EC2 > Target groups > Create target group

**Step 1**

**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.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

**Target group name**

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

**Protocol : Port**

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation.

HTTP  80

Activer Windows  
Accédez aux paramètres pour activer Windows.

cloudShell Feedback 20°C Ciel couvert Rechercher © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 00:18 23/05/2025

**Target group name**

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

**Protocol : Port**

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation.

HTTP

80

1-65535

**IP address type**

Only targets with the indicated IP address type can be registered to this target group.

**IPv4**  
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

**IPv6**  
Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

**VPC**

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

project-vpc  
 vpc-001e16c180e5b72d0  
 IPv4 VPC CIDR: 10.0.0.0/16

**Protocol version**

**HTTP1**  
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

**HTTP2**  
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

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

[Activer Windows](#)  
 Accédez aux paramètres pour activer Windows.

---

**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

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**

[Restore defaults](#)

**Health check port**

The port the load balancer uses when performing health checks on targets. By default, the health check port is the same as the target group's traffic port. However, you can specify a different port as an override.

Traffic port

Override

4001

1-65535

**Healthy threshold**

The number of consecutive health checks successes required before considering an unhealthy target healthy.

5

2-10

**Unhealthy threshold**

The number of consecutive health check failures required before considering a target unhealthy.

2

[Activer Windows](#)  
 Accédez aux paramètres pour activer Windows.

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

## ● creating internal LB:

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LoadBalancers:

**Load balancers**

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

**Create Application Load Balancer**

**Application Load Balancers now support public IPv4 IP Address Management (IPAM)**

You can get started with this feature by configuring IP pools in the Network mapping section.

**Create Application Load Balancer**

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

**How Application Load Balancers work**

**Basic configuration**

**Load balancer name**

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

**Internal-LB**

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

**Scheme**

Scheme can't be changed after the load balancer is created.

**Internet-facing**

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

**Internal**

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

**Load balancer IP address type**

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

**IPv4** (selected)

Includes only IPv4 addresses.

**Dualstack**

Includes IPv4 and IPv6 addresses.

**Network mapping**

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

**VPC**

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.

vpc-001e16c180e5b7z0  
IPv4 VPC CIDR: 10.0.0.0/16

**IP pools - new**

You can optionally choose to configure an IPAM pool as the preferred source for your load balancer's IP addresses. Create or view Pools in the Amazon VPC IP Address Manager console.

**Availability Zones and subnets**

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

**us-east-1a (use1-az2)**

Subnet

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

subnet-0917267dff0cc2382  
IPv4 subnet CIDR: 10.0.160.0/20

**project-subnet-back-us-east-1a**

**us-east-1b (use1-az4)**

Subnet

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

subnet-00e3e64dcfca7497  
IPv4 subnet CIDR: 10.0.176.0/20

**Security groups**

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Capture d'écran copié dans le Presse-papiers  
Enregistrement automatique dans le dossier des captures d'écran.  
Activer Windows

**Security groups** [Info](#)  
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

**Select up to 5 security groups**

**Internal-LB** sg-0335de3514f154639 VPC: vpc-001e36c180e5b72c0

**Listeners and routing** [Info](#)  
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

**Listener: HTTP:80**

Protocol: <b>HTTP</b>	Port: <b>80</b>
Default action: <a href="#">Info</a>	
Forward to: <b>tg-backend</b>	Target type: Instance, IPv4
<a href="#">Create target group</a>	

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

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

[Add listener](#)

## ● Launching the template of our backend

**Create launch template**  
Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

**Launch template name and description**

Launch template name - **required**  
  
Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '\*', '@'.

Template version description  
  
Max 255 chars

**Auto Scaling guidance** [Info](#)  
Select this if you intend to use this template with EC2 Auto Scaling  
 Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

**► Template tags**  
**► Source template**

**Launch template contents**  
Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

**▼ Application and OS Images (Amazon Machine Image) - required** [Info](#)  
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

**Recents** **Quick Start**

Amazon Linux	macOS	Ubuntu	Windows	Red Hat	SUSE Linux	Debian
--------------	-------	--------	---------	---------	------------	--------

[Browse more AMIs](#)

**Summary**

**Software Image (AMI)**  
Amazon Linux 2 Kernel 5.10 AMI...  
ami-0e58b56aa4d64231b

**Virtual server type (instance type)**  
-

**Firewall (security group)**  
-

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

**Free tier:** In your first year of per month of t2.micro instances available when used with free IPv4 address usage, 30 GiB of snapshots, and 100 GB of bandwidth.

[Cancel](#)

Search our full catalog including 1000s of application and OS images

**Recents**    **Quick Start**

**Amazon Machine Image (AMI)**

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-0e58b56aa4d64231b (64-bit (x86)) / ami-0972357ba34d1ec40 (64-bit (Arm))  
Virtualization: hvm   ENA enabled: true   Root device type: ebs   Free tier eligible

**Description**  
Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Amazon Linux 2 Kernel 5.10 AMI 2.0.20250512.0.x86\_64 HVM gp2

Architecture	AMI ID	Publish Date	Username	Verified provider
64-bit (x86)	ami-0e58b56aa4d64231b	2025-05-10	ec2-user	Verified provider

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

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

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

**Key pair (login)** [Info](#)  
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

**Key pair name**  [Create new key pair](#)

**Network settings** [Info](#)

**Subnet** [Info](#)  
Don't include in launch template [Create new subnet](#)

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

**Firewall (security groups)** [Info](#)  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Select existing security group    Create security group

**Security groups** [Info](#)  
Select security groups

SG-BE sg-0a9b4ecc5885a7e89 [X](#)  
VPC: vpc-001e56c180e5b72c0   [Compare security group rules](#)

▼ Advanced details [Info](#)

IAM instance profile [Info](#)  
LabInstanceProfile  
arn:aws:iam::517950265597:instance-profile/LabInstanceProfile

Create new IAM profile

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

- Configuring user data for the backend EC2 image

V1 for instance metadata access will break.

Metadata response hop limit [Info](#)  
2

Allow tags in metadata [Info](#)  
Don't include in launch template

User data - optional [Info](#)  
Upload a file with your user data or enter it in the field.

```
#!/bin/bash
# Switch to ec2-user
cd /home/ec2-user
export HOME=/home/ec2-user

# Update and install MySQL client
sudo yum update -y
sudo yum install -y mysql

# Install Node.js via NVM
curl -o https://raw.githubusercontent.com/nvm-sh/nvm/v0.38.0/install.sh | bash
export NVM_DIR="/home/ec2-user/.nvm"
source "$NVM_DIR/nvm.sh"
```

User data has already been base64 encoded

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
SG-BE

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

Free tier: In your first year of usage, you get 1 free hour per month of t2.micro instances (up to 10 instances available) when used with free Amazon VPC traffic, up to 100 IPv4 address usage, 30 GiB of storage usage per month, and 100 GB of bandwidth usage per month.

- AutoScaling Group of the Backend

aws [Alt+S] Search United States (N. Virginia) vodabas/user\$41399@sarrasoyah10@gmail.com @ 5179-5026-5597 ▾

EC2 > Auto Scaling groups > Create Auto Scaling group

**Step 1**

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

**Choose launch template or configuration** Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

**Name**

**Auto Scaling group name**

Enter a name to identify the group.

**ASG-backend**

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

**Launch template** Info

**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.

**backendTemplate**

**Create a launch template**

**Version**

**Default (1)**

**Description**

Template for backend EC2s

**AMI ID**

ami-0e58b56aa4d64231b

**Key pair name**

sarania

**Launch template**

**backendTemplate**

lt-0680dc792f515aca0

**Instance type**

t2.micro

**Security groups**

-

**Request Spot Instances**

No

**Security group IDs**

sg-0a9b4ecc5885a7e89

**Additional details**

**Storage (volumes)**

**Date created**

**Activer Windows**

Accédez aux paramètres pour activer Windows.

Switch to Launch configuration

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateAutoScalingGroup:

aws [Alt+S] Search United States (N. Virginia) vodabas/user\$41399@sarrasoyah10@gmail.com @ 5179-5026-5597 ▾

EC2 > Auto Scaling groups > Create Auto Scaling group

**Step 1**

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

**Choose instance launch options** Info

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

**Instance type requirements** Info

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

**Launch template**

**backendTemplate**

lt-0680dc792f515aca0

**Version**

Default

**Description**

Template for backend EC2s

**Instance type**

t2.micro

**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-001e36c180e5b72c0 (project-vpc)

10.0.0.0/16

**Select Availability Zones and subnets**

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

**Create a VPC**

**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**

10.0.176.0/20

10.0.176.0/20

10.0.176.0/20

**Create a subnet**

**Activer Windows**

Accédez aux paramètres pour activer Windows.

Availability Zone distribution - new

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateAutoScalingGroup:

**Integrate with other services - optional** Info

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

**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

tg-backend | HTTP X

**VPC Lattice integration options** Info

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

Select VPC Lattice service to attach

No VPC Lattice service

Attach to VPC Lattice service

**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.

EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing. To avoid unexpected terminations, first verify the settings of these health checks in the [Load Balancer console](#) [2]

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

Activer Windows  
Accédez aux paramètres pour activer Windows.

Add tags

Step 7

Review

**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**

**Instance warmup** Info

300 seconds

Disable scale in to create only a scale-out policy

**Instance maintenance policy** Info

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Rechercher

00:28 23/05/2025

**Instance maintenance policy** [Info](#)

Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.

Choose a replacement behavior depending on your availability requirements

**Mixed behavior**

No policy

For rebalancing events, new instances will launch before terminating others. For all other events, instances terminate and launch at the same time.

**Prioritize availability**

Launch before terminating

Launch new instances and wait for them to be ready before terminating others. This allows you to go above your desired capacity by a given percentage and may temporarily increase costs.

**Control costs**

Terminate and launch

Terminate and launch instances at the same time. This allows you to go below your desired capacity by a given percentage and may temporarily reduce availability.

**Flexible**

Custom behavior

Set custom values for the minimum and maximum amount of available capacity. This gives you greater flexibility in setting how far below and over your desired capacity EC2 Auto Scaling goes when replacing instances.

**Set healthy percentage**

Set the minimum and maximum percentage of your desired capacity that must be healthy and ready for use for EC2 Auto Scaling to proceed with replacing instances.

Min  Max  % of 2 instances

This range is currently within your group's scaling limits.

**View capacity during replacements based on your desired capacity**

**Additional capacity settings**

**enabling cloudwatch**

**Additional capacity settings**

**Capacity Reservation preference** [Info](#)

Select whether you want Auto Scaling to launch instances into an existing Capacity Reservation or Capacity Reservation resource group.

Default

Auto Scaling uses the Capacity Reservation preference from your launch template.

None

Instances will not be launched into a Capacity Reservation.

Capacity Reservations only

Instances will only be launched into a Capacity Reservation. If capacity isn't available, the instances fail to launch.

Capacity Reservations first

Instances will attempt to launch into a Capacity Reservation first. If capacity isn't available, instances will run in On-Demand capacity.

**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

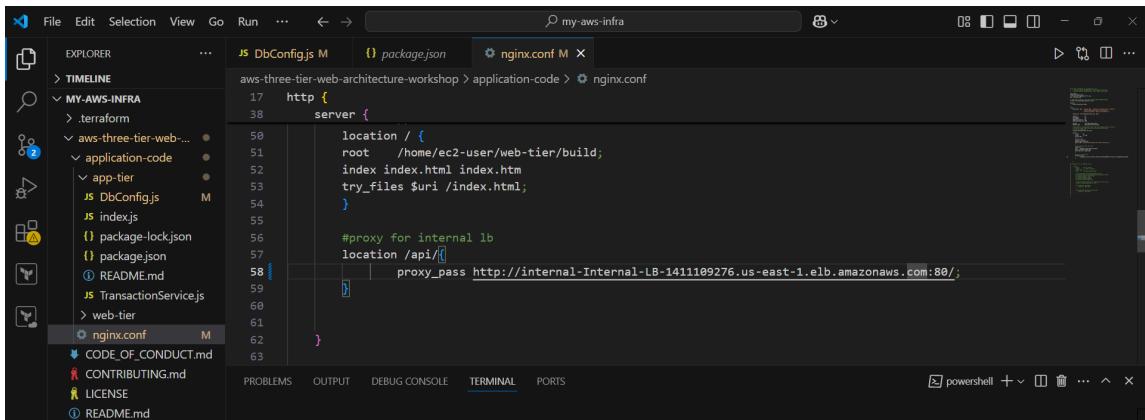
[Cancel](#) [Skip to review](#) [Previous](#) [Next](#)

## 6. Frontend Deployment

- Built the React application locally and uploaded to S3
- Launched frontend EC2 instances in private subnets
- Used a Launch Template with User Data to install NGINX and deploy the frontend build automatically
- Set up a Target Group for frontend instances

- Deployed an Internet-Facing Load Balancer and mapped frontend traffic to it
- Configured Auto Scaling for frontend servers based on CPU utilization

- Update the configuration file

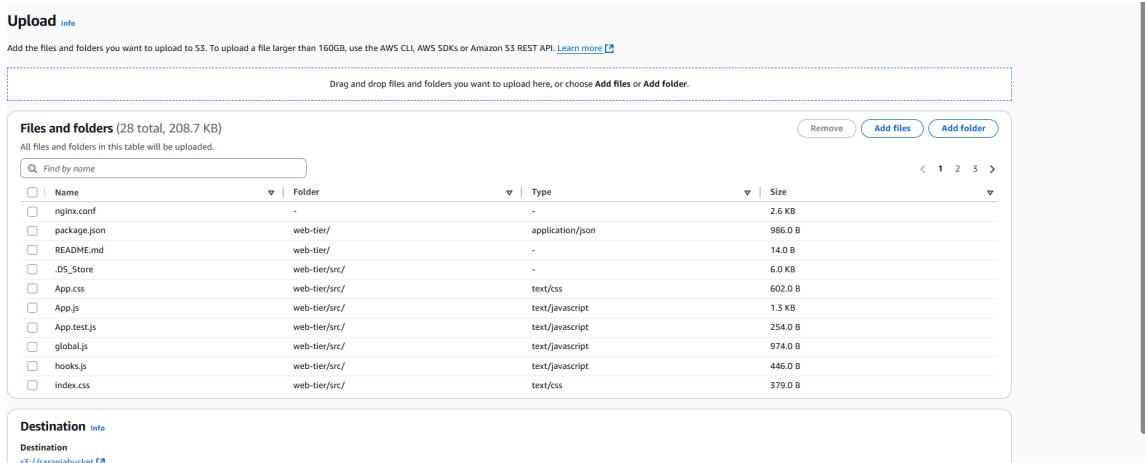


```

17 http {
38     server {
50         location / {
51             root /home/ec2-user/web-tier/build;
52             index index.html index.htm;
53             try_files $uri /index.html;
54         }
55
56         #proxy for internal lb
57         location /api/ {
58             proxy_pass http://internal-Internal-LB-1411109276.us-east-1.elb.amazonaws.com:80/;
59         }
60
61     }
62 }
63

```

- Deploy the frontend code to S3



Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	nginx.conf	-	-	2.6 KB
<input type="checkbox"/>	package.json	web-tier/	application/json	986.0 B
<input type="checkbox"/>	README.md	web-tier/	-	14.0 B
<input type="checkbox"/>	.DS_Store	web-tier/src/	-	6.0 KB
<input type="checkbox"/>	App.css	web-tier/src/	text/css	602.0 B
<input type="checkbox"/>	App.js	web-tier/src/	text/javascript	1.3 KB
<input type="checkbox"/>	App.test.js	web-tier/src/	text/javascript	254.0 B
<input type="checkbox"/>	global.js	web-tier/src/	text/javascript	974.0 B
<input type="checkbox"/>	hooks.js	web-tier/src/	text/javascript	446.0 B
<input type="checkbox"/>	index.css	web-tier/src/	text/css	379.0 B

Destination [Info](#)

Destination [s3://saraniabucket](#)

- Create a target group

Screenshot of the AWS EC2 Target Groups page showing a single target group named "tg-backend".

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
tg-backend	arn:aws:elasticloadbalancin...	80	HTTP	Instance	Internal-LB	vpc-001e36c180e5b72c0

**Create target group**

**Specify group details**

**Basic configuration**

**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.
- IP addresses
  - Supports load balancing to VPC and on-premises resources.
  - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
  - Offers flexibility with microservice based architectures, simplifying inter-application communication.
  - Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
- Lambda function
  - Facilitates routing to a single Lambda function.
  - Accessible to Application Load Balancers only.
- Application Load Balancer
  - Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
  - Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

**Target group name**  
frontend-tg

**Protocol & Port**  
HTTP  
80

**Health checks**

**Health check protocol**  
HTTP

**Health check path**  
/

**Advanced health check settings**

**Health check port**  
Traffic port

**Healthy threshold**  
5

**Activer Windows**  
Accédez aux paramètres pour activer Windows.

## 7. External Load Balancer & Auto Scaling

- External ALB (Application Load Balancer) was deployed with listeners on HTTP/HTTPS.
- Mapped to frontend EC2 target group
- Configured with two public subnets

- Set up an internet-facing load balancer

**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](#).

**project-vpc**  
vpc-001e35c180a5b72c  
IPv4 CIDR: 10.0.0.0/16

**IP pools - new** Info

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

Use IPAM pool for public IPv4 addresses

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

**Availability Zones and subnets** Info

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

us-east-1a (use1-az1)

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

subnet-0f663438bfaf736c  
IPv4 subnet CIDR: 10.0.0.0/20

project-subnet-public1-us-east-1a

us-east-1b (use1-az2)

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

subnet-08821f2640300065  
IPv4 subnet CIDR: 10.0.16.0/20

project-subnet-public2-us-east-1b

**Security groups** Info

- Setting its subnets to public

**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](#).

**project-vpc**  
vpc-001e35c180a5b72c  
IPv4 CIDR: 10.0.0.0/16

**IP pools - new** Info

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

Use IPAM pool for public IPv4 addresses

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

**Availability Zones and subnets** Info

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

us-east-1a (use1-az1)

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

subnet-0f663438bfaf736c  
IPv4 subnet CIDR: 10.0.0.0/20

project-subnet-public1-us-east-1a

us-east-1b (use1-az2)

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

subnet-08821f2640300065  
IPv4 subnet CIDR: 10.0.16.0/20

project-subnet-public2-us-east-1b

**Security groups** Info

**Security groups** [Info](#)  
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

**Listeners and routing** [Info](#)  
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

**Listener HTTP:80**

Protocol	Port	Default action	Target type
HTTP	:80	Forward to frontend-tg	HTTP

[Create target group](#)

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

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

## ● Template for frontend EC2s

Sandbox | Database | AWS Thread | Create lau... | Document | Launch AW... | Workben... | Distributio... | SecurityGr... | Security Groups

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateTemplate:

aws Search [Alt+S] United States (N. Virginia)

EC2 > Launch templates > Create launch template

**Create launch template**

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

**Launch template name and description**

Launch template name - required  
 Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '"', '@'.

Template version description  
 Max 255 chars

Auto Scaling guidance | [Info](#)  
Select this if you intend to use this template with EC2 Auto Scaling  
 Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

▶ Template tags  
▶ Source template

**Launch template contents**  
Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

**Application and OS Images (Amazon Machine Image) - required** [Info](#)  
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Q Search our full catalog including 1000s of application and OS images

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Linux | Debian

Browse more AMIs

**Summary**

Software image (AMI)  
Amazon Linux 2 Kernel 5.10 AMI... [read ami-e58b56aa4d64231b](#)

Virtual server type (instance type)  
-

Firewall (security group)  
-

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

Free tier: In your first year of operation per month of t2.micro instance usage available when used with free tier IPv4 address usage, 30 GiB of EBS snapshots, and 100 GB of bandwidth

Cancel

Out  
Capture  
Enregis...  
capture  
Activ...  
Accédi...

**Launch template contents**  
Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

**▼ Application and OS Images (Amazon Machine Image) - required [Info](#)**  
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

**Recent** **Quick Start**

**Amazon Machine Image (AMI)**

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-0e58b56aa4d64231b (64-bit (x86)) / ami-0972357ba34d1ec40 (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**  
Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Amazon Linux 2 Kernel 5.10 AMI 2.0.20250512.0 x86\_64 HVM gp2

Architecture	AMI ID	Publish Date	Username
64-bit (x86)	ami-0e58b56aa4d64231b	2025-05-10	ec2-user 

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

**Instance type**

Don't include in launch template  [Compare instance types](#)

**▼ Key pair (login) [Info](#)**  
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

**Key pair name**

sarania 

**▼ Network settings [Info](#)**

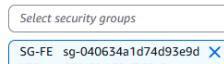
**Subnet** 

Don't include in launch template 

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

**Firewall (security groups) [Info](#)**  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Select existing security group  Create security group

**Security groups**  

SG-FE sg-040634a1d74d95e9d   
VPC: vpc-001e36c180e5b72c0

**EC2 > Launch templates > Create launch template**

Metadata version: V2 only (token required)

Metadata response hop limit: 2

Allow tags in metadata: Don't include in launch template

User data - optional:

```
#!/bin/bash
# Set home directory for ec2-user
cd /home/ec2-user
export HOME=/home/ec2-user

# Install dependencies
sudo yum update -y
sudo yum install -y git curl unzip awscli

# Install NVM and Node.js 16
curl -o https://raw.githubusercontent.com/nvm-sh/nvm/v0.38.0/install.sh | bash
export NVM_DIR="/home/ec2-user/.nvm"
source "$NVM_DIR/nvm.sh"
nvm install 16
```

User data has already been base64 encoded

**Summary**

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more  
ami-0e58b056aa4664231b

Virtual server type (instance type): SG-1E

Firewall (security group): SG-1E

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs. 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

**Create launch template**

Activer Windows  
Accédez aux paramètres pour activer Wi-Fi

## ● Configure auto scaling

**EC2 > Auto Scaling groups > Create Auto Scaling group**

Step 1: Choose launch template or configuration

Step 2: Choose instance launch options

Step 3: optional

Step 4: optional

Step 5: optional

Step 6: optional

Step 7: optional

**Choose launch template or configuration**

Name: autoscaling-frontend

Launch template: frontend-template

Description: ami-0955476d60561c955

Key pair name: saranya

AMIs: ami-0955476d60561c955

Security groups: -

Security group IDs: sg-040634a1d74d93e9d

Instance type: Request Spot Instances No

**Create Auto Scaling group**

Activer Windows  
Accédez aux paramètres pour activer Windows.

Screenshot of the AWS CloudWatch Metrics console showing the creation of a new Auto Scaling group. The current step is "Integrate with other services - optional".

**Integrate with other services - optional**

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

**Load balancing**

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
- Attach to an existing load balancer
- Attach to a new load balancer

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
- Choose from Classic Load Balancers

Existing load balancer target groups

Select target groups

frontend-tg1 HTTP Application Load Balancer: externalLB

**VPC Lattice integration options**

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

Select VPC Lattice service to attach

- No VPC Lattice service
- Attach to VPC Lattice service

Create new VPC Lattice service

Screenshot of the AWS CloudWatch Metrics console showing the creation of a new Auto Scaling group. The current step is "Configure group size and scaling - optional".

**Configure group size and scaling - optional**

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

**Group size**

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

Desired capacity type

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

Units (number of instances)

Desired capacity

Specify your group size.

2

**Scaling**

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

Scaling limits

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

Min desired capacity

2

Max desired capacity

3

Equal or less than desired capacity

Equal or greater than desired capacity

**Automatic scaling - optional**

Choose whether to use a target tracking policy

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 proportionally to the metric's value.

Scaling policy name

Target Tracking Policy

**Target Tracking Policy**

**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:** 70

**Instance warmup:** [Info](#)  
300 seconds

Disable scale in to create only a scale-out policy

**Instance maintenance policy:** [Info](#)  
Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.

**Choose a replacement behavior depending on your availability requirements:**

- Mixed behavior**: For rebalancing events, new instances will launch before terminating others. For all other events, instances terminate and launch at the same time.
- Prioritize availability**: Launch new instances and wait for them to be ready before terminating others. This allows you to go above your desired capacity by a given percentage and may temporarily increase costs.
- Control costs**: Terminate and launch instances at the same time. This allows you to go below your desired capacity by a given percentage and may temporarily reduce availability.
- Flexible**: Set custom values for the minimum and maximum amount of available capacity. This gives you greater flexibility in setting how far below and over your desired capacity EC2 Auto Scaling goes when replacing instances.

**Set healthy percentage:**  
Set the minimum and maximum percentage of your desired capacity that must be healthy and ready for use for EC2 Auto Scaling to proceed with replacing instances.

Min	Max
90	% to 110
% of 2 instances	

This range is currently within your group's scaling limits.

**Activator Windows**  
Accédez aux paramètres pour activer Windows.

**Additional capacity settings**

**Capacity Reservation preference:** [Info](#)  
Select whether you want Auto Scaling to launch instances into an existing Capacity Reservation or Capacity Reservation resource group.

- Default**: Auto Scaling uses the Capacity Reservation preference from your launch template.
- None**: Instances will not be launched into a Capacity Reservation.
- Capacity Reservations only**: Instances will only be launched into a Capacity Reservation. If capacity isn't available, the instances fail to launch.
- Capacity Reservations first**: Instances will attempt to launch into a Capacity Reservation first. If capacity isn't available, instances will run in On-Demand capacity.

**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](#) [Previous](#) **Next** [Activator Windows](#)

Accédez aux paramètres pour activer Windows.

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

**Final App:**

The screenshot shows a web browser window with the URL [external-1b-1982367368.us-east-1.elb.amazonaws.com/#/db](https://external-1b-1982367368.us-east-1.elb.amazonaws.com/#/db). The page title is "AURORA DATABASE DEMO PAGE". On the left sidebar, there are two items: "HOME" and "DB DEMO". The main content area displays a table with three columns: ID, AMOUNT, and DESC. The table has three rows. The first row is a header with the column names. The second row contains data: ID 1, AMOUNT 400, and DESC groceries. The third row contains data: ID 2, AMOUNT 0, and DESC soyah. There is a "DEL" button at the top right of the table. At the bottom right of the page, there is a message: "Activer Windows" and "Accédez aux paramètres pour activer Windows.".

ID	AMOUNT	DESC
ADD		
1	400	groceries
2	0	soyah

Activer Windows  
Accédez aux paramètres pour activer Windows.

## 8. Monitoring and Logging

### 8.1 CloudWatch and CloudTrail

- Enabled Amazon CloudWatch Logs for application and system logging
- Created CloudWatch Alarms:
  - Alert when CPU > 70%
  - Email notifications via SNS Topic and Subscription
- Enabled AWS CloudTrail to log all API activities, access attempts, and resource changes

### 8.2 RDS Backups and Snapshots

- Enabled automated RDS backups (daily snapshots retained for 7 days)
- Multi-AZ configuration provides high availability and durability

- Backups can be restored to a point-in-time

The image displays two screenshots of the AWS CloudWatch Alarms interface, illustrating the creation and state transition of alarms.

**Screenshot 1 (Top): Alarms (2)**

Name	State	Last state update (UTC)	Conditions	Actions
TargetTracking-asg-front-AlarmLow-0cbea2a3-172a-4e19-8c70-8dbe8347174a	⚠️ In alarm	2025-05-23 00:55:58	CPUUtilization < 49 for 15 datapoints within 15 minutes	Actions enabled
TargetTracking-ASG-backend-AlarmLow-f9b8f919-7e73-4019-a643-5df7212a0827	⚠️ In alarm	2025-05-22 23:45:57	CPUUtilization < 49 for 15 datapoints within 15 minutes	Actions enabled

**Screenshot 2 (Bottom): Alarms (4)**

Name	State	Last state update (UTC)	Conditions	Actions
TargetTracking-asg-front-AlarmLow-0cbea2a3-172a-4e19-8c70-8dbe8347174a	⚠️ In alarm	2025-05-23 00:55:58	CPUUtilization < 49 for 15 datapoints within 15 minutes	Actions enabled
TargetTracking-asg-front-AlarmHigh-3670a346-b575-42ca-9338-d9849d0f79da	🟢 OK	2025-05-23 00:44:50	CPUUtilization > 70 for 3 datapoints within 3 minutes	Actions enabled
TargetTracking-ASG-backend-AlarmLow-f9b8f919-7e73-4019-a643-5df7212a0827	⚠️ In alarm	2025-05-22 23:45:57	CPUUtilization < 49 for 15 datapoints within 15 minutes	Actions enabled
TargetTracking-ASG-backend-AlarmHigh-9112174a-06c7-4789-81ef-7a11869329e2	🟢 OK	2025-05-22 23:31:49	CPUUtilization > 70 for 3 datapoints within 3 minutes	Actions enabled

## Send notifications via Amazon SNS to a specified email address

- Topic Creation

**New Feature**

Amazon SNS now supports High Throughput FIFO topics. [Learn more](#)



## Create topic

### Details

Type | [Info](#)

Topic type cannot be modified after topic is created

FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- Subscription protocols: SQS

Standard

- Best-effort message ordering
- At-least once message delivery
- Subscription protocols: SQS, Lambda, Data Firehose, HTTP, SMS, email, mobile application endpoints

### Name

cloudwatch-alerts

Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (\_).

Display name - optional | [Info](#)

To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.

My Topic

- Subscription Creation

us-east-1.console.aws.amazon.com/sns/v3/home?region=us-e...

AWS | United State vclabs/user3841399=sarrasoyah10@

Amazon SNS > Subscriptions > Create subscription

**New Feature**  
Amazon SNS now supports High Throughput FIFO topics. [Learn more](#)

## Create subscription

### Details

**Topic ARN**

**Protocol**  
The type of endpoint to subscribe

Email

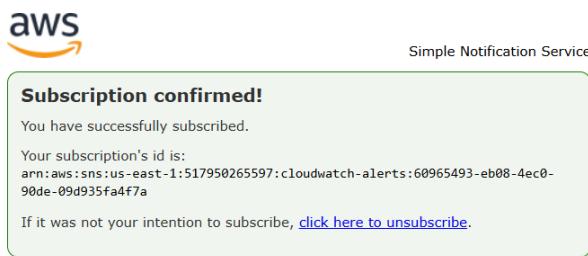
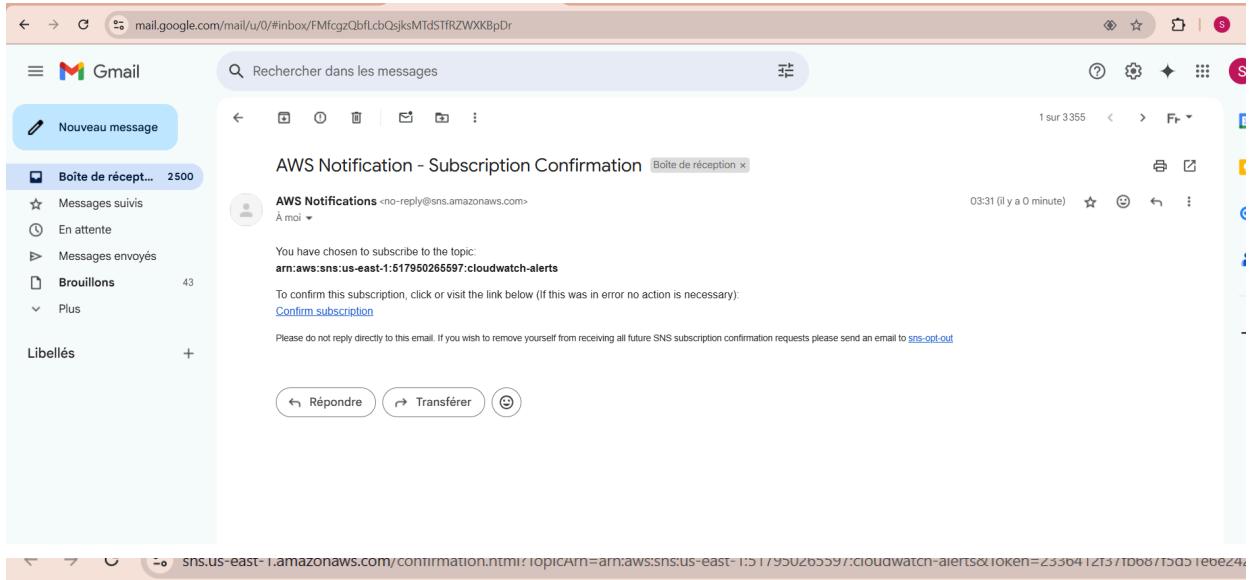
**Endpoint**  
An email address that can receive notifications from Amazon SNS.

After your subscription is created, you must confirm it. [Info](#)

► **Subscription filter policy - optional** [Info](#)  
This policy filters the messages that a subscriber receives.

CloudShell [Feedback](#) [Privacy](#) [Terms](#) [Cookie preferences](#)

- **Output**



## ● Alarm Creation

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~MetricSelection~AlarmType~MetricAlarm~AlarmData~(Metrics~(~)~AlarmName~'~A...)

CloudWatch > Alarms > Create alarm

Step 1 Specify metric and conditions

Step 2 Configure actions

Step 3 Add alarm details

Step 4 Preview and create

**Metric**

**Graph**

Preview of the metric or metric expression and the alarm threshold.

Select metric

Cancel Next

Activer Windows  
Accédez aux paramètres pour activer Windows.

CloudShell Feedback 18°C Barberbar 03:36

aws CloudWatch Alarms Create alarm

Step 1 Specify metric and conditions

Step 2 Configure actions

Step 3 Add alarm details

Step 4 Preview and create

**Metric**

**Graph**

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Percent

70

56.9

43.9

00:00 00:30 01:00 01:30 02:00 02:30

CPUUtilization

**Namespace** AWS/EC2

**Metric name** CPUUtilization

**InstanceId** i-03c69574eb7b0e99f

**Instance name** No name specified

**Statistic** Average

**Period** 5 minutes Activer Windows  
Accédez aux paramètres pour activer Windows.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**Conditions**

**Threshold type**

**Static**  
Use a value as a threshold

**Anomaly detection**  
Use a band as a threshold

**Whenever CPUUtilization is...**  
Define the alarm condition.

**Greater**  
> threshold

**Greater/Equal**  
>= threshold

**Lower/Equal**  
<= threshold

**Lower**  
< threshold

**than...**  
Define the threshold value.

70

Must be a number

**▼ Additional configuration**

**Datapoints to alarm**  
Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.

1 out of 1

**Missing data treatment**  
How to treat missing data when evaluating the alarm.

Treat missing data as missing

**Activer Windows**  
Accédez aux paramètres pour activer Windows.

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsv2:create/~(Page~Actions~AlarmType~MetricAlarm~AlarmData~Namespace~AWS~ZTECZ~Metric...)

CloudWatch > Alarms > Create alarm

Turn on Recommendations to pre-populate the wizard with the recommended alarms.

Step 1 Specify metric and conditions

Step 2 **Configure actions**

Step 3 Add alarm details

Step 4 Preview and create

**Configure actions**

**Notification**

**Alarm state trigger**  
Define the alarm state that will trigger this action.

**In alarm**  
The metric or expression is outside of the defined threshold.

**OK**  
The metric or expression is within the defined threshold.

**Insufficient data**  
The alarm has just started or not enough data is available.

**Send a notification to the following SNS topic**  
Define the SNS (Simple Notification Service) topic that will receive the notification.

**Select an existing SNS topic**

Create new topic

Use topic ARN to notify other accounts

**Send a notification to...**

cloudwatch-alerts

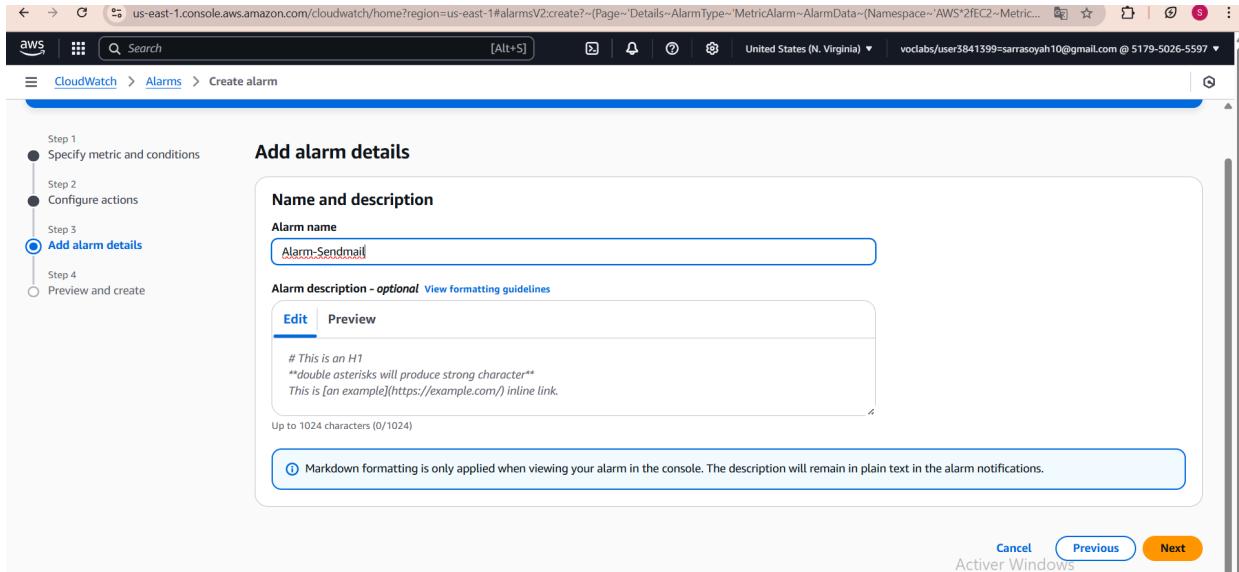
Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.

Email (endpoints)

sarrasoyah10@gmail.com - View in SNS Console

Add notification

**Activer Windows**  
Accédez aux paramètres pour activer Windows.



## ● Enable backup in RDS :

### Backup

#### Backup retention period Info

The number of days (1-35) for which automatic backups are kept.

 days

#### Start time

 :  UTC

#### Duration

 hours

Copy tags to snapshots

### Maintenance

#### Auto minor version upgrade Info

Enable auto minor version upgrade

Enabling auto minor version upgrade will automatically upgrade your database minor version. For limitations and more details, see Automatically upgrading the minor engine version [documentation](#).

## ● Cloutrail creation:

us-east-1.console.aws.amazon.com/cloudtrailv2/home?region...     

aws |  |  |  |  |  | United State ▾ | vclabs/user3841399=sarrasoyah10@ ▾

☰ CloudTrail > Dashboard > Create trail  

Step 1  
**Choose trail attributes**

Step 2  
Choose log events

Step 3  
Review and create

## Choose trail attributes

### General details

A trail created in the console is a multi-region trail. [Learn more](#)

**Trail name**  
Enter a display name for your trail.  
  
3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization  
To review accounts in your organization, open AWS Organizations.  
[See all accounts](#)

**Storage location** [Info](#)

Create new S3 bucket  
Create a bucket to store logs for the trail.

Use existing S3 bucket  
Choose an existing bucket to store logs for this trail.

**Trail log bucket name**  
Enter a new S3 bucket name and folder (prefix) to store your logs.  
Bucket names must be globally unique.

us-east-1.console.aws.amazon.com/cloudtrailv2/home?region=us-east-1#/create

CloudTrail > Dashboard > Create trail

Step 1 Choose trail attributes

Step 2 Choose log events

Step 3 Review and create

## Choose trail attributes

**General details**  
A trail created in the console is a multi-region trail. [Learn more](#)

**Trail name**  
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization  
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

**Storage location** [Info](#)

Create new S3 bucket  
Create a bucket to store logs for the trail.

Use existing S3 bucket  
Choose an existing bucket to store logs for this trail.

**Trail log bucket name**  
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

[X](#) [Browse](#)

**Prefix - optional**

Logs will be stored in saranibucket/AWSLogs/517950265597

**Log file SSE-KMS encryption** [Info](#)

Enabled

**Additional settings**

**Log file validation** [Info](#)

Enabled

**SNS notification delivery** [Info](#)

Enabled

**CloudWatch Logs - optional**  
Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. [Learn more](#)

[CloudWatch Logs](#) [Info](#)

Activer Windows

Accédez aux paramètres pour activer Windows.

Screenshot of the AWS CloudTrail 'Create trail' wizard Step 2: Choose log events.

**Events** Info  
Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

**Event type**  
Choose the type of events that you want to log.

**Management events**  
Capture management operations performed on your AWS resources.

**Data events**  
Log the resource operations performed on or within a resource.

**Insights events**  
Identify unusual activity, errors, or user behavior in your account.

**Network activity events**  
Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.

**Management events** Info  
Management events show information about management operations performed on resources in your AWS account.

**API activity**  
Choose the activities you want to log.

**Read**       **Write**

**Exclude AWS KMS events**

**Activer Windows**  
Accédez aux paramètres pour activer Windows.

**Step 1** Choose trail attributes  
**Step 2** Choose log events  
**Step 3** Review and create

**Review and create**

**Step 1: Choose trail attributes**

**General details**

Trail name management-trail	Trail log location saraniabucket/AWSLogs/517950265597	Log file validation Enabled
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled	SNS notification delivery Disabled
Apply trail to my organization Not enabled		

**CloudWatch Logs**

No CloudWatch Logs log groups  
CloudWatch Logs is not configured for this trail

**Tags**

**Activer Windows**  
Accédez aux paramètres pour activer Windows.

**Trails**

Trail successfully created

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
management-trail	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:517950265597:trail/management-trail	Disabled	No	saraniabucket	-	-	Logging

The screenshot shows the AWS CloudTrail Event history interface. On the left, there's a navigation sidebar with options like Dashboard, Event history, Insights, Lake, Settings, Pricing, Documentation, Forums, and FAQs. The main area is titled "Event history (50+)" and includes a search bar and filter buttons for date and time, and a "Clear filter" button. A table lists 50 events, each with a checkbox, event name, event time, user name, event source, resource type, and resource name. Most events are from "ssm.amazonaws.com" and involve "UpdateInstanceInfor...". At the bottom of the table, it says "0 / 5 events selected". Below the table, there's a section titled "Compare event details" with a note to "Select 2-5 events to compare their details." To the right, there's a link to "Activer Windows" with the sub-note "Accédez aux paramètres pour activer Windows."

	Event name	Event time	User name	Event source	Resource type	Resource name
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	May 23, 2025, 04:00:27 (UTC+0...)	i-0b84ee3064655...	ssm.amazonaws.com	-	-
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	May 23, 2025, 03:59:00 (UTC+0...)	i-08ea7d65b0da0...	ssm.amazonaws.com	-	-
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	May 23, 2025, 03:58:25 (UTC+0...)	i-06de932737e17f...	ssm.amazonaws.com	-	-
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	May 23, 2025, 03:57:00 (UTC+0...)	i-00e249dae27dfc...	ssm.amazonaws.com	-	-
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	May 23, 2025, 03:56:56 (UTC+0...)	i-0286d31d1c5b0...	ssm.amazonaws.com	-	-
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	May 23, 2025, 03:55:27 (UTC+0...)	i-0b84ee3064655...	ssm.amazonaws.com	-	-
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	May 23, 2025, 03:54:00 (UTC+0...)	i-08ea7d65b0da0...	ssm.amazonaws.com	-	-

## Conclusion

**This project gave us practical experience in deploying a secure and scalable 3-tier web application on AWS. We designed a custom VPC, configured routing and security groups, deployed EC2 instances for the frontend and backend, set up Auto Scaling and Load Balancers, and launched a Multi-AZ RDS database.**

**We also enabled monitoring with CloudWatch and CloudTrail and hosted static content on S3. This project strengthened our skills in cloud infrastructure, security, and high availability.**