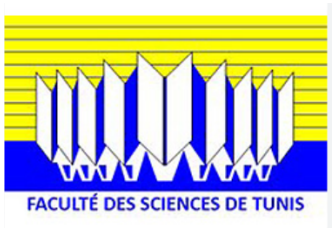




# Deployment of a Secure and Scalable 3-Tier Web Application on AWS

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

**Group: IDS3**

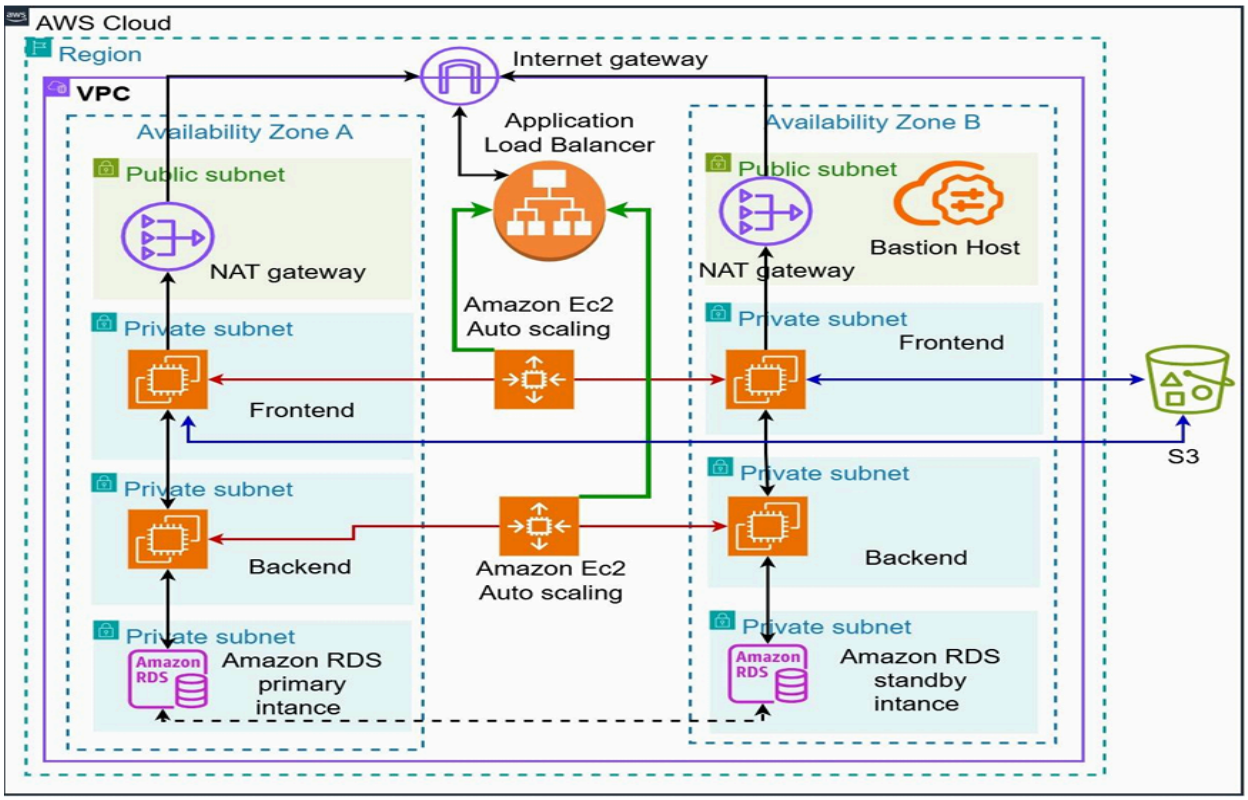
**2024/2025**

## Content

## Executive Summary

**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:

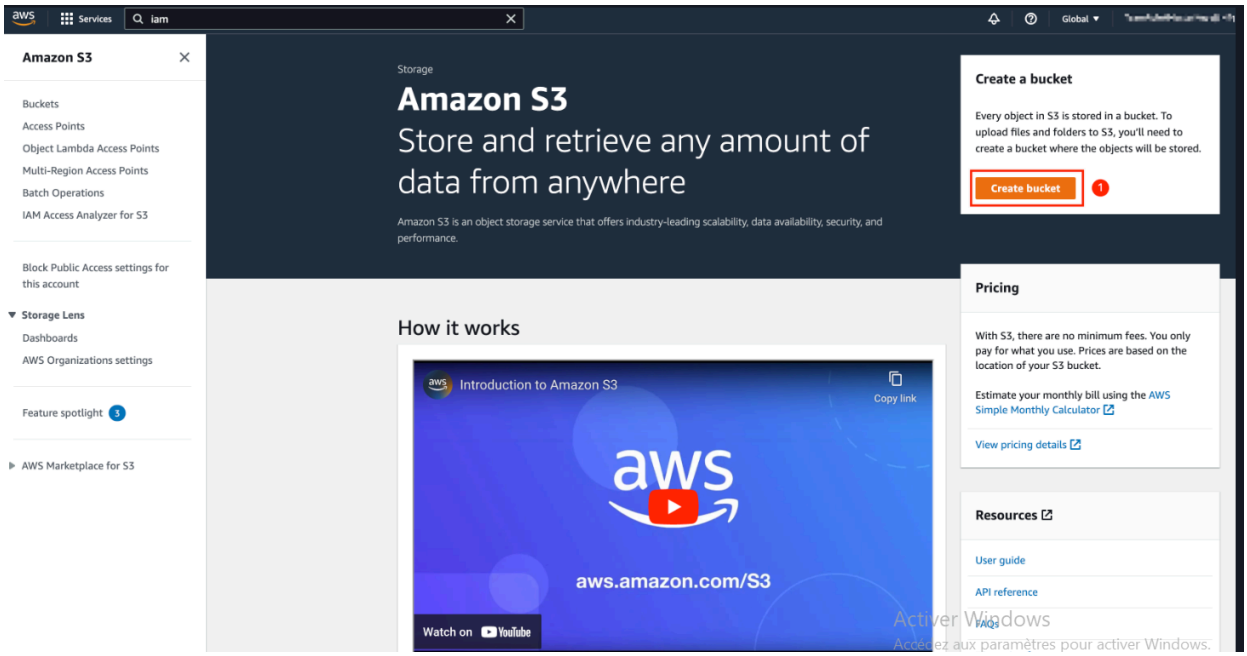


**Useful_Link:**
https://catalog.us-east-1.prod.workshops.aws/workshops/85cd2bb2-7f79-4e96-bdee-8078e469752a/en-US/cleanup

## 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

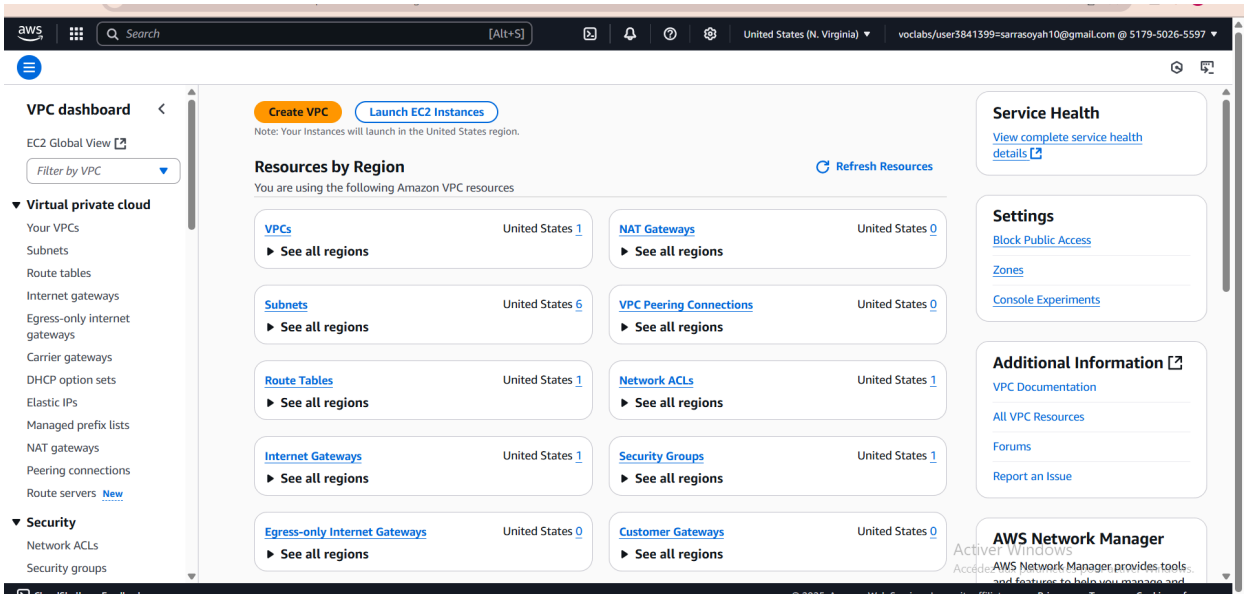
### 2.1 VPC and Subnet Configuration

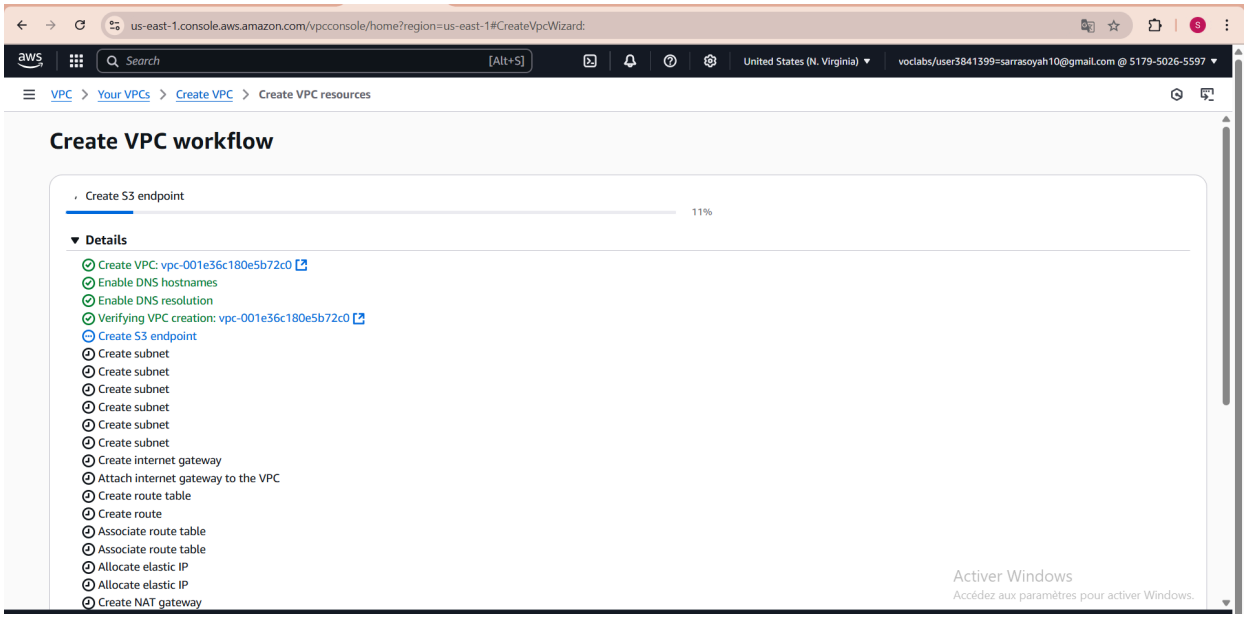
**We created a custom VPC (10.0.0.0/16) with eight subnets across two Availability Zones (AZs) for redundancy.**

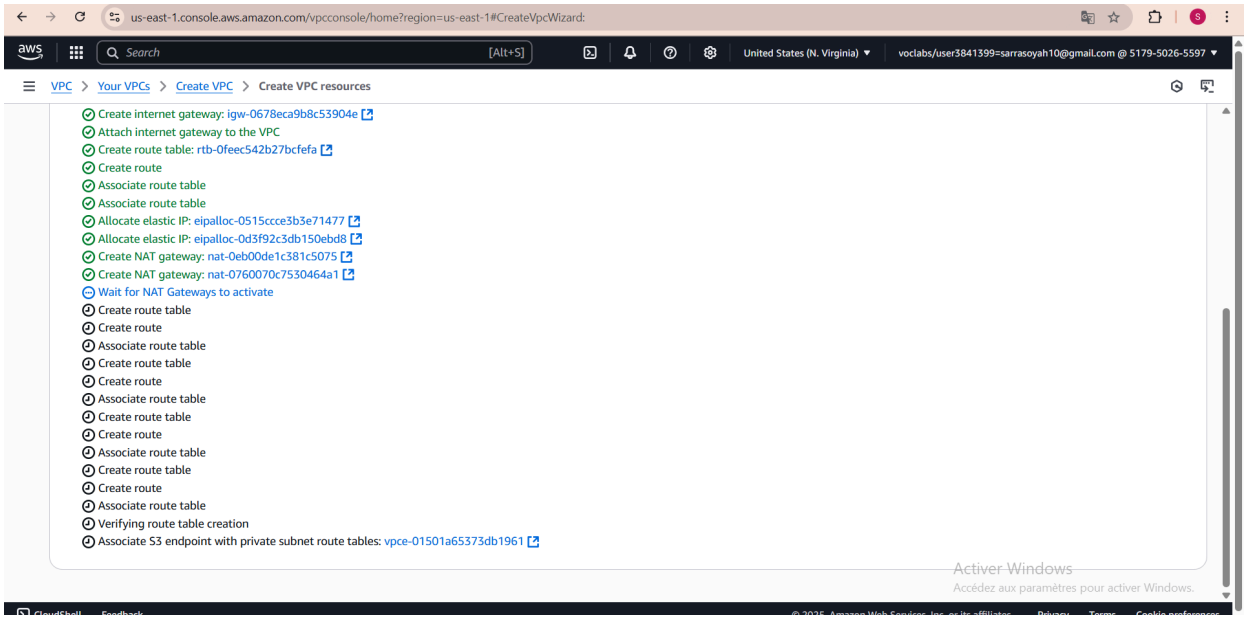
## 2.2 Internet Access and Routing

**We created:**

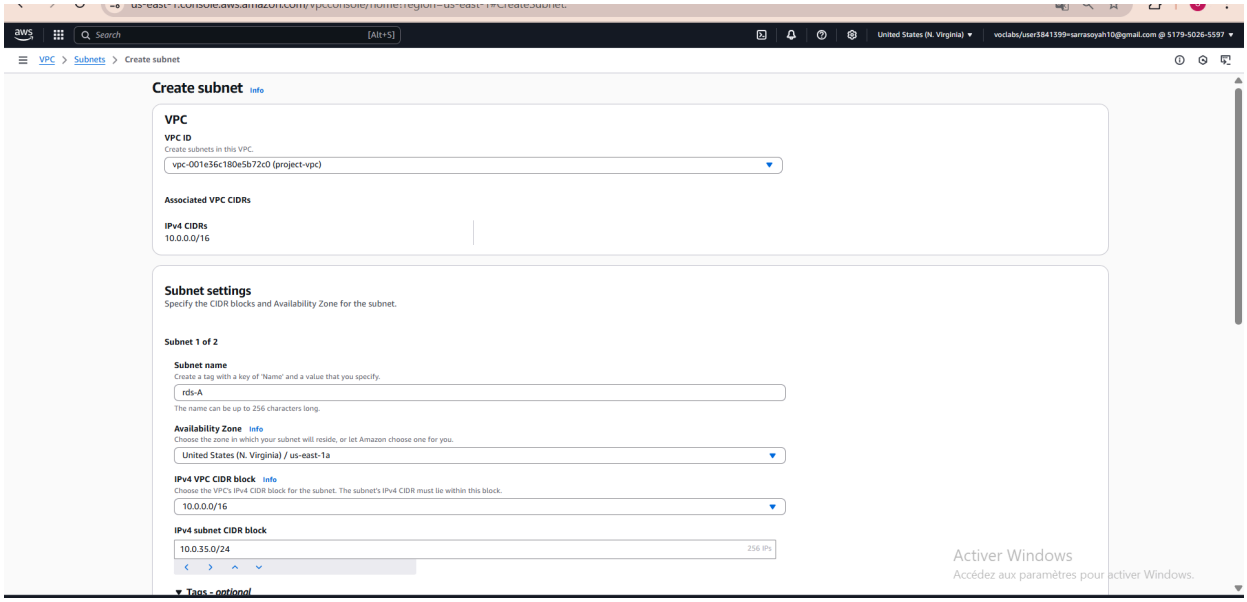
- **An Internet Gateway attached to the VPC to allow public subnets to access the internet.**
- **A NAT Gateway for private instances to access the internet securely (for software updates, etc.).**
- **Custom route tables for public and private traffic management. For example:**
    - **Public subnets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

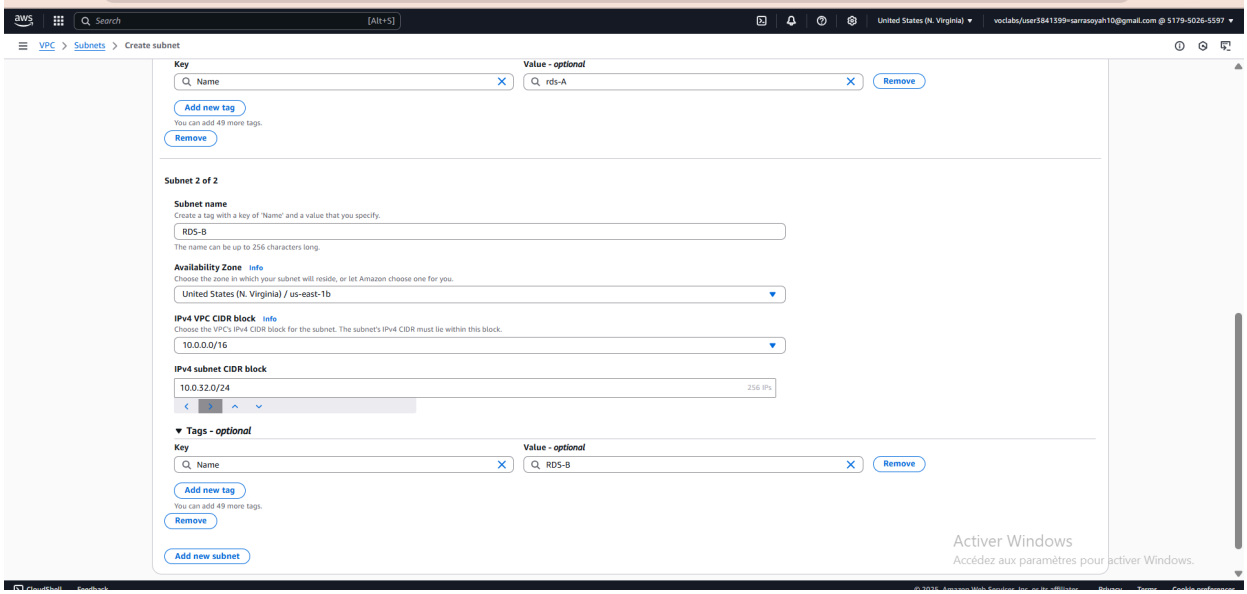




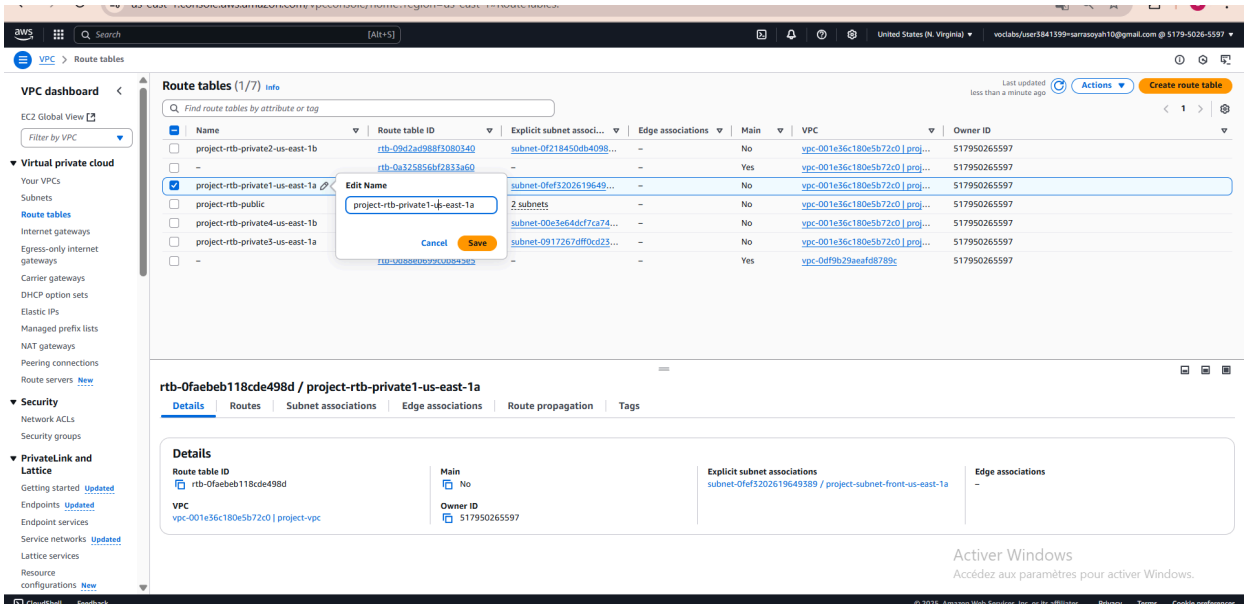



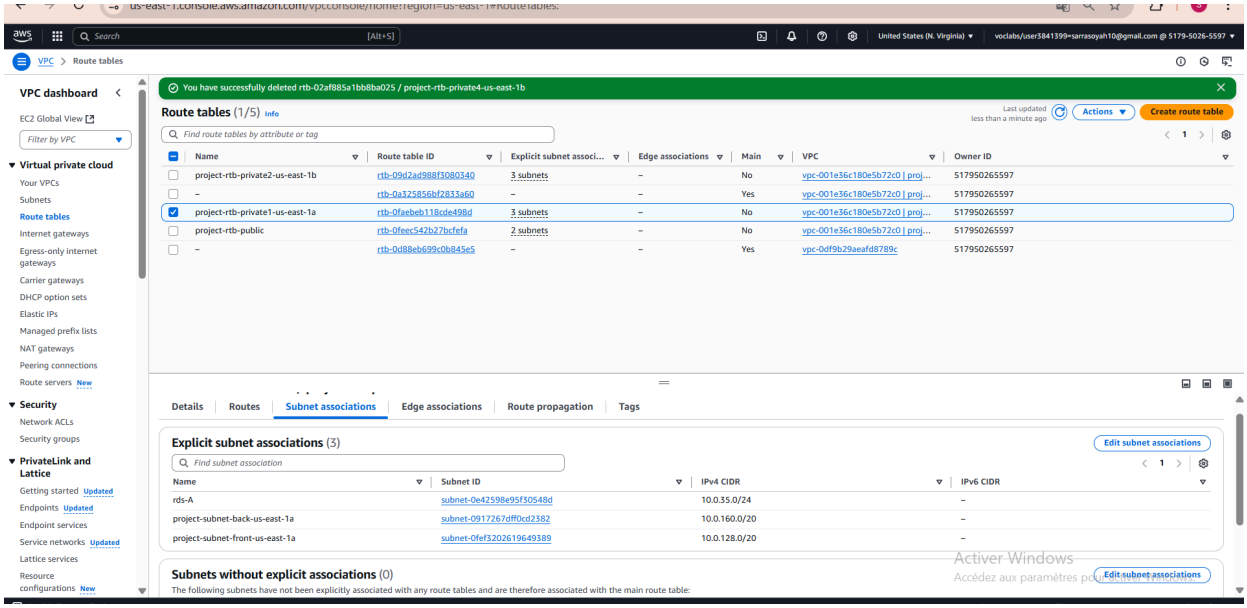

## Adding two more subnets



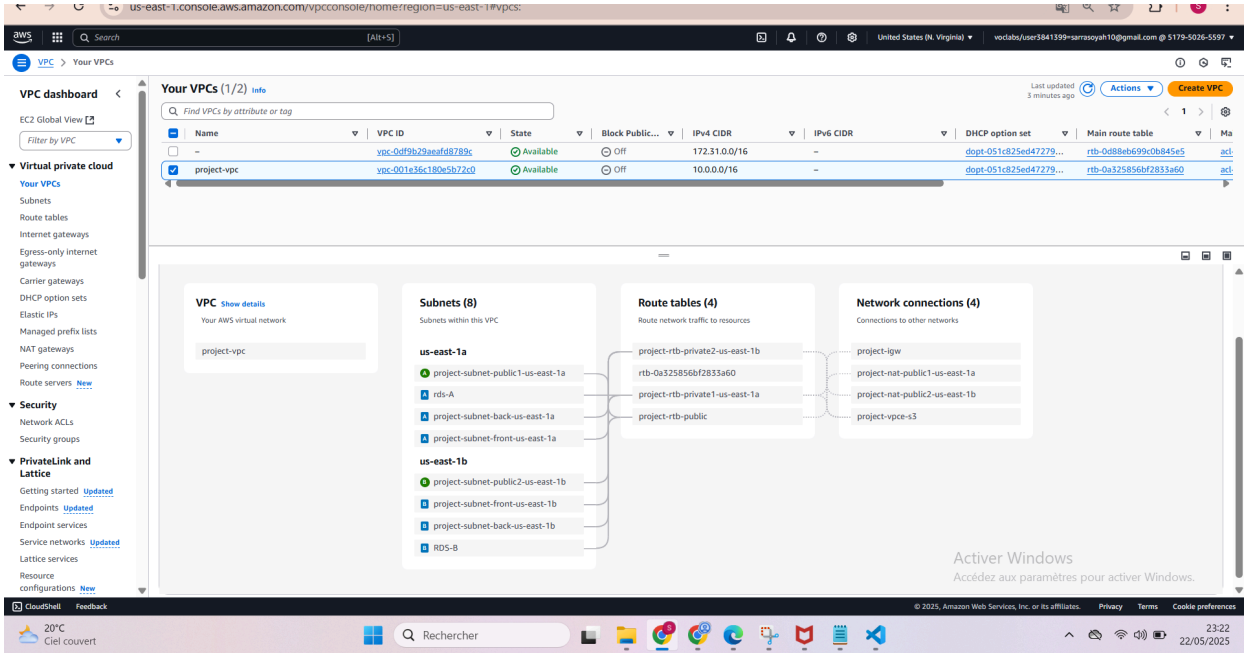




# Renaming of route tables




# Final Ressource Map:

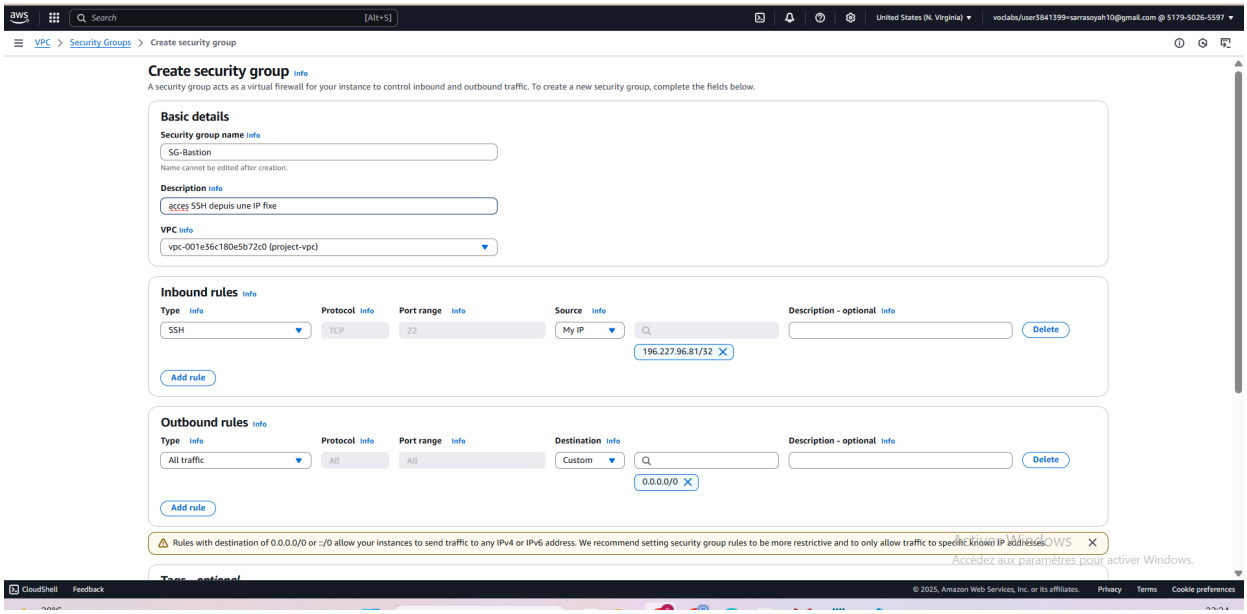



## 3. Security Groups Configuration

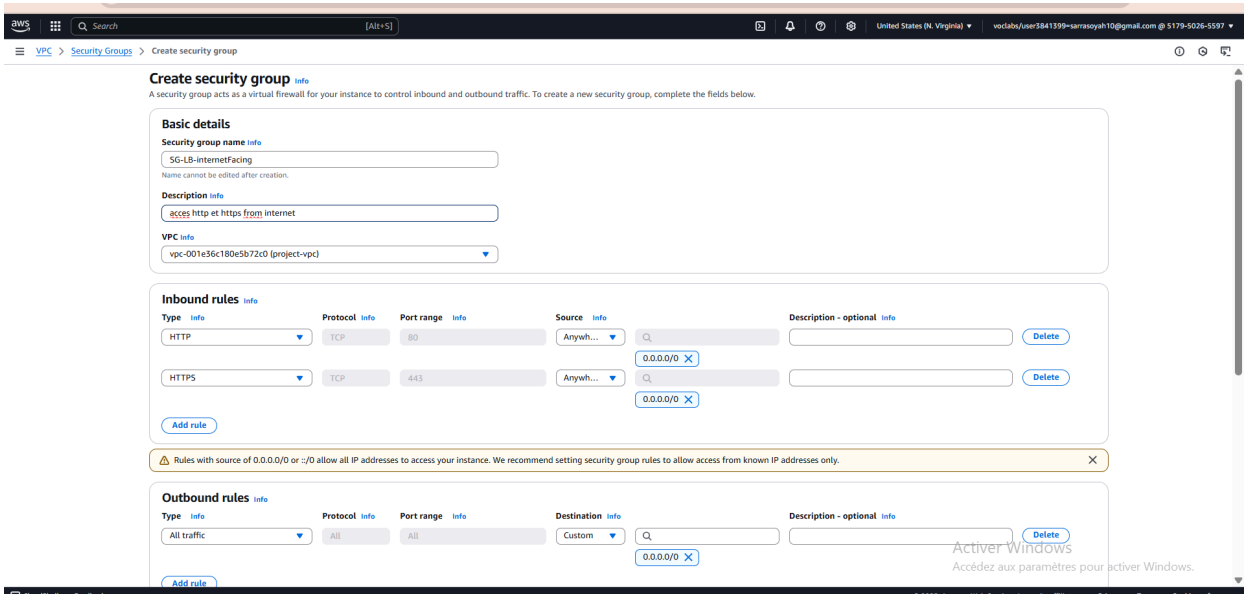
**We adopted a layered security model with multiple Security Groups:**

- **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**

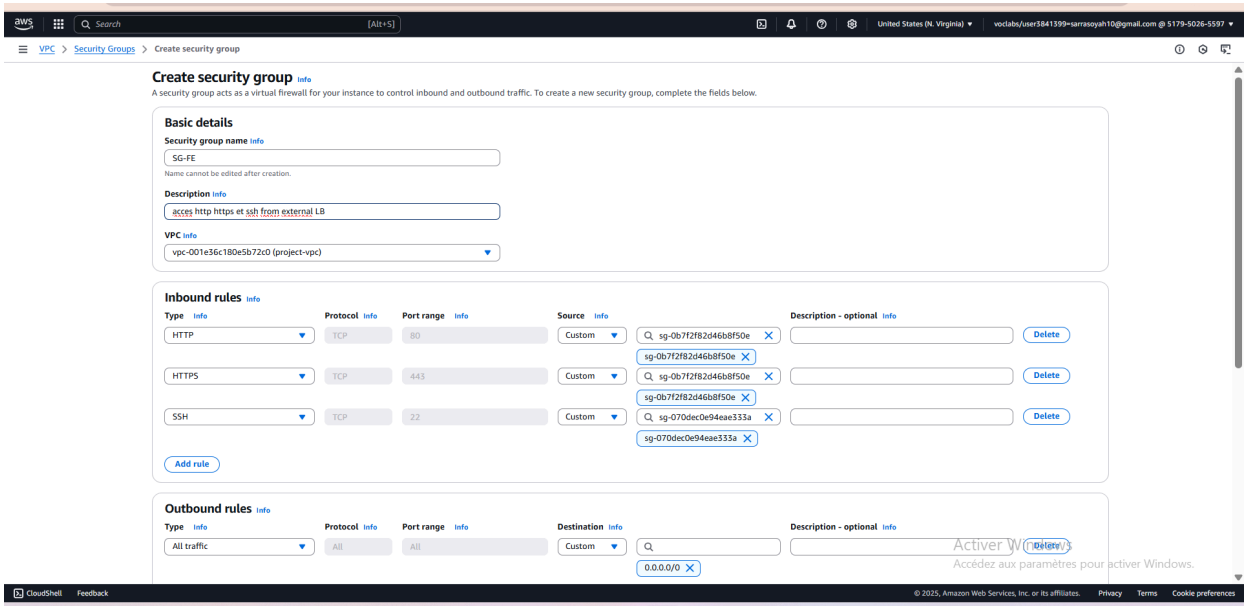
### SG-bastion



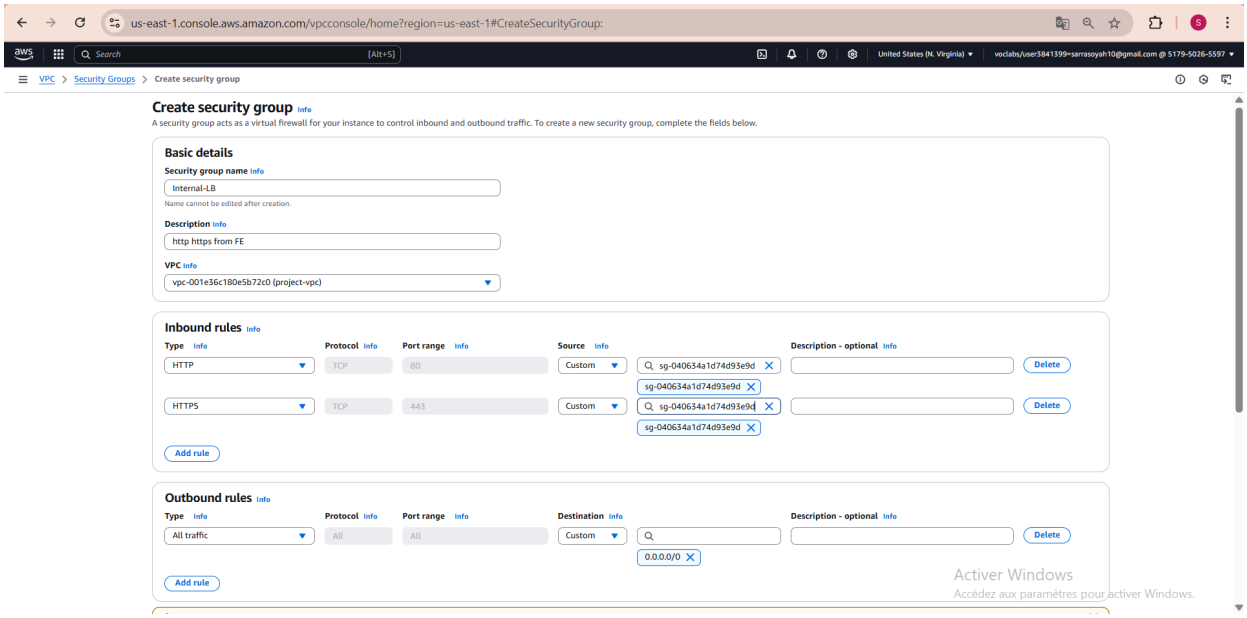

## SG-external-LB:



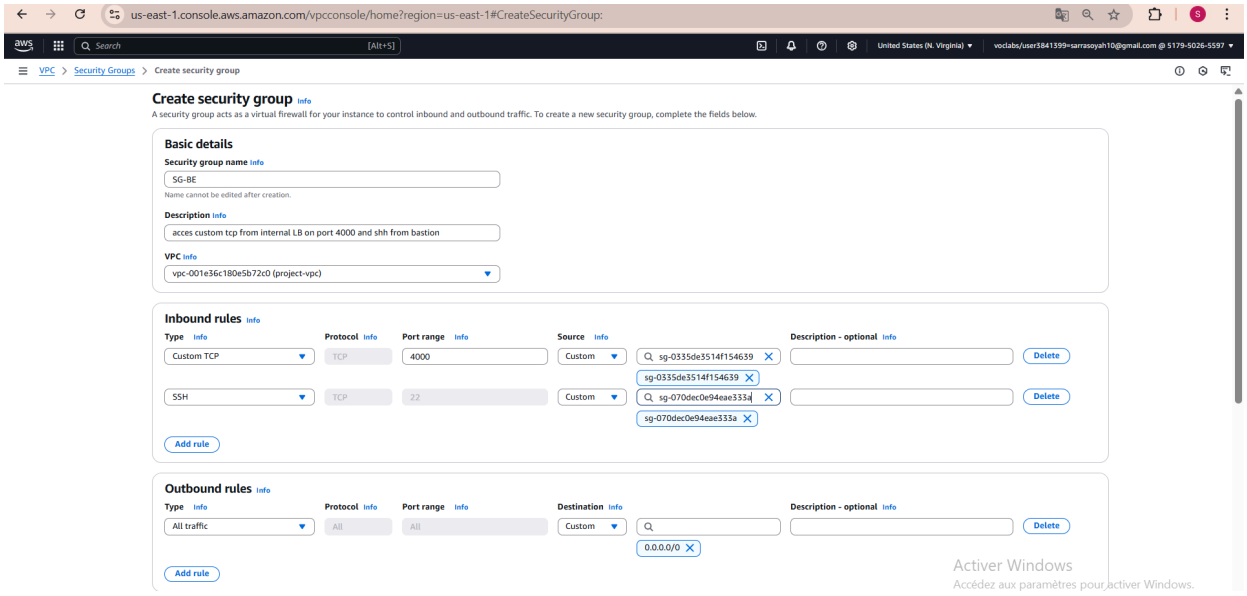

## SG-FE



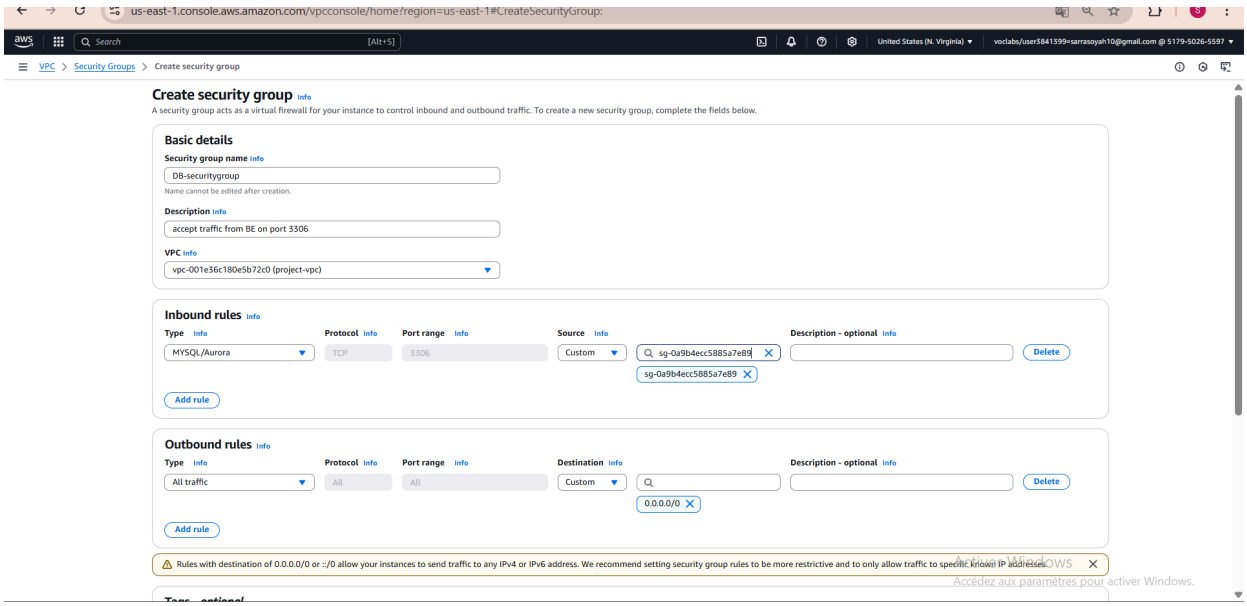

# SG-internalLB




# SG-BE




## SG-RDS




## 4. Database Layer: Amazon RDS

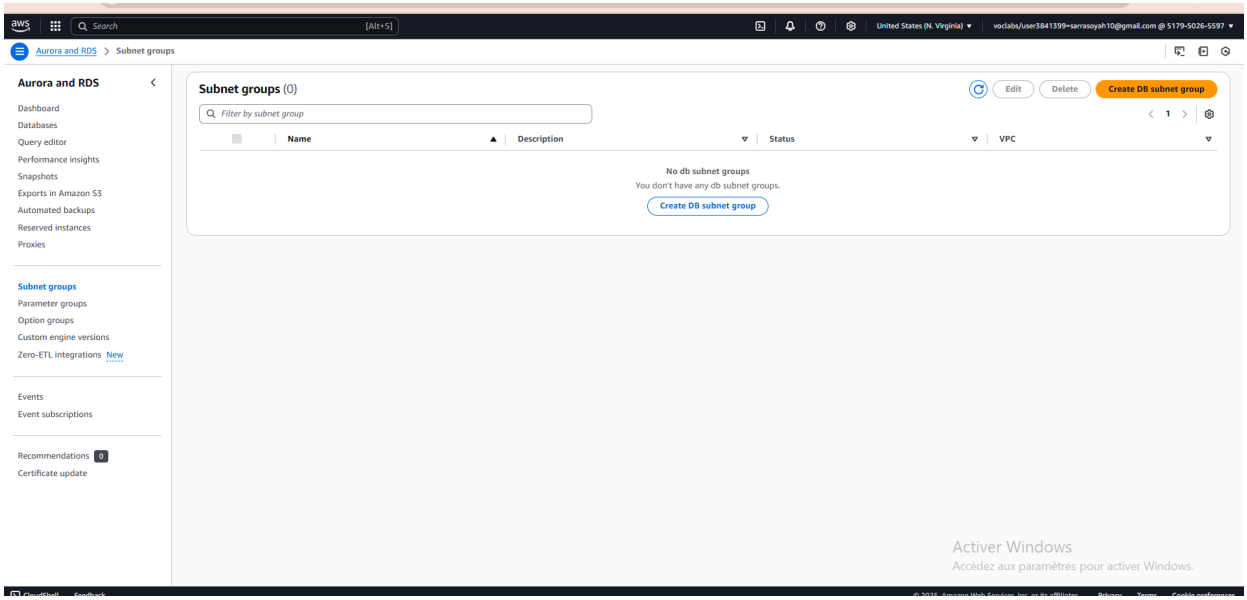
**We deployed a MySQL database on Amazon RDS with Multi-AZ support:**

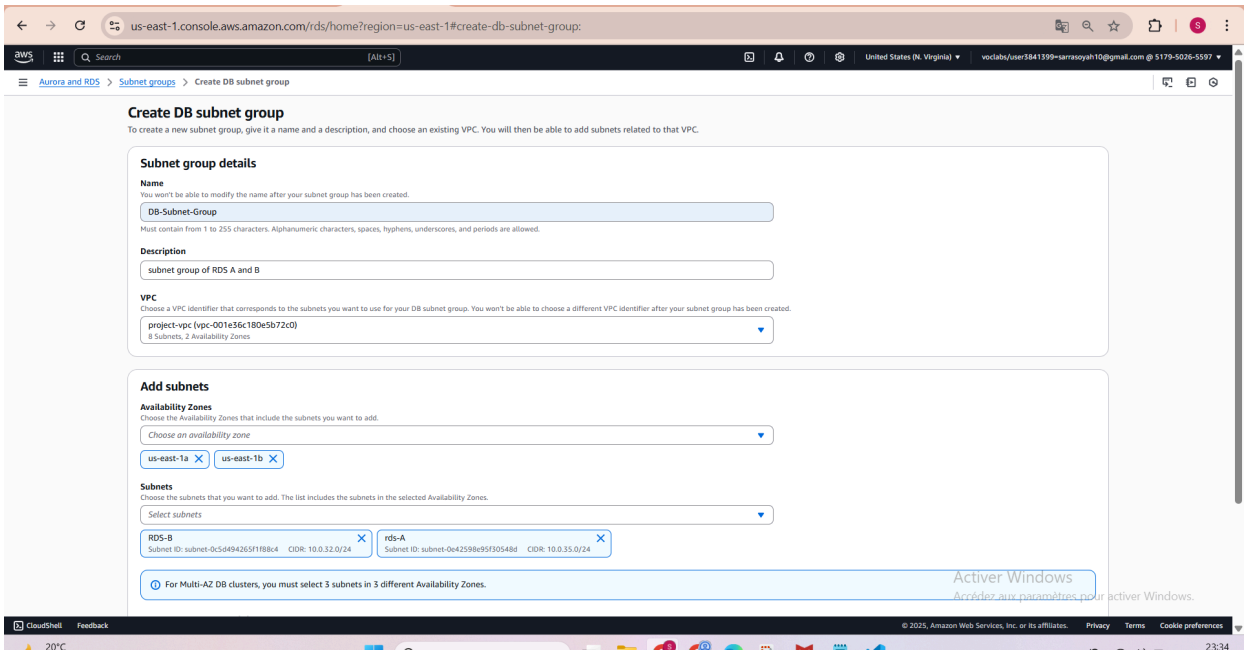
- **Created RDS Subnet Groups using the two private RDS subnets**
- **Configured automatic failover with a primary (writer) and secondary (reader) instance**

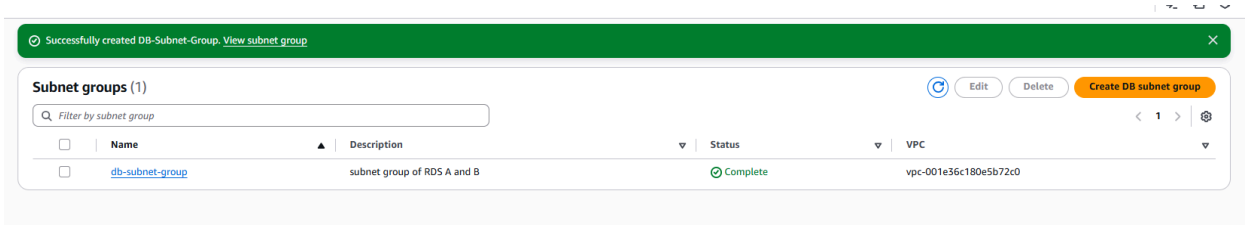
- **Enabled automated backups, monitoring, and CloudWatch alarms**

- **Retrieved the RDS endpoint and updated `dbconfig.js` in the backend to connect securely using private IPs**

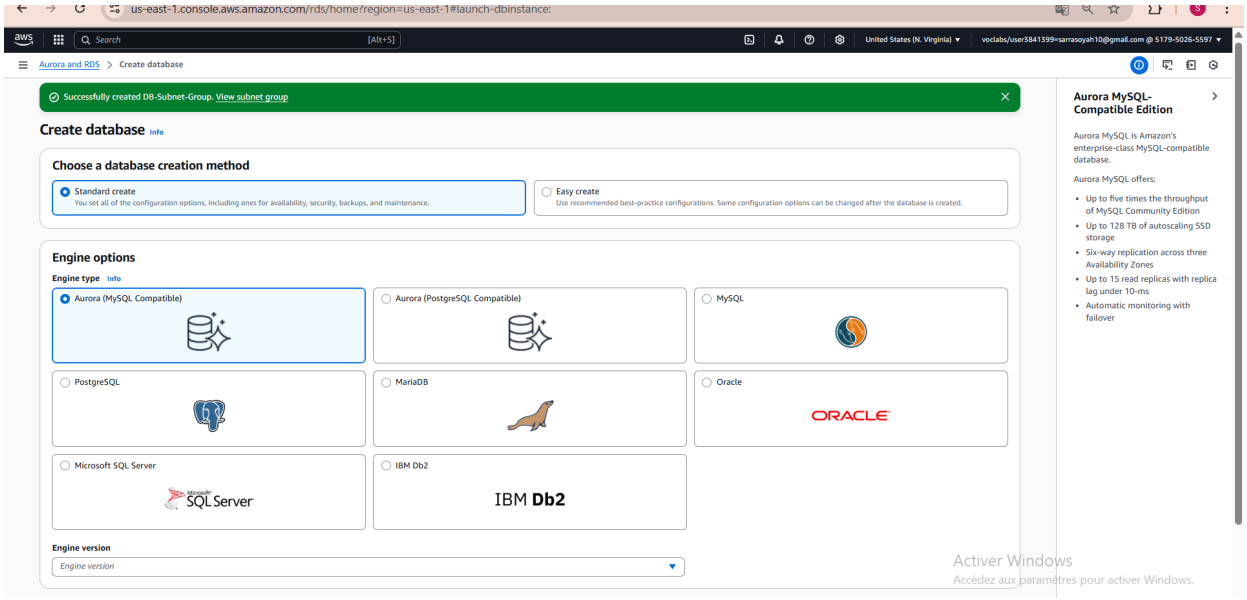
- **Creating Subnet Groups**

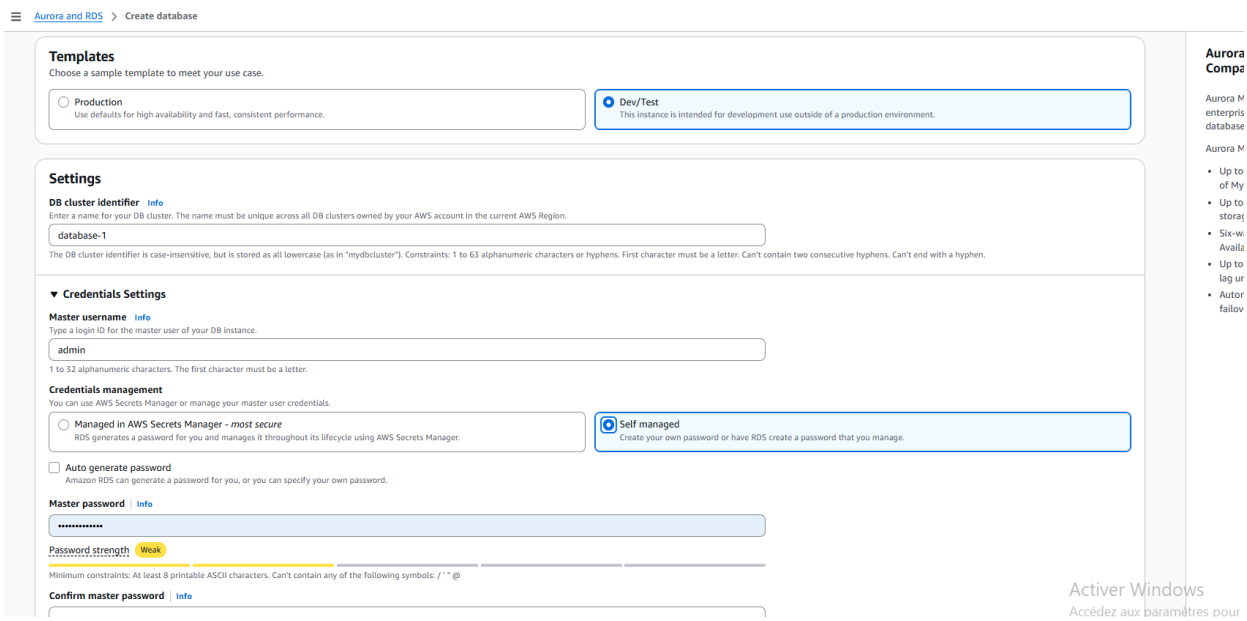





- **Database Configuration**



## 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.

## 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 2.085 Mbps

## Availability & durability

**Multi-AZ deployment** Info

Aurora MySQL is A enterprise-class M database.

Aurora MySQL offe

- Up to five time of MySQL Com
- Up to 128 TB o storage
- Six-way replica Availability Zor
- Up to 15 read r lag under 10-m
- Automatic mor failover

## 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.

Activer Windows

**Aurora MySQL-Compatible Edition**

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

Aurora MySQL offers:

- Up to five times the throu of MySQL Community Ed
- Up to 128 TB of autoscali storage
- Six-way replication across Availability Zones
- Up to 15 read replicas wi lag under 10-ms
- Automatic monitoring wi failover

**VPC security group (firewall)** Info

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

- Choose existing
  Choose existing VPC security groups
- Create new
  Create new VPC security group

**Existing VPC security groups**

*Choose one or more options*

DB-securitygroup

**RDS Proxy**

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

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

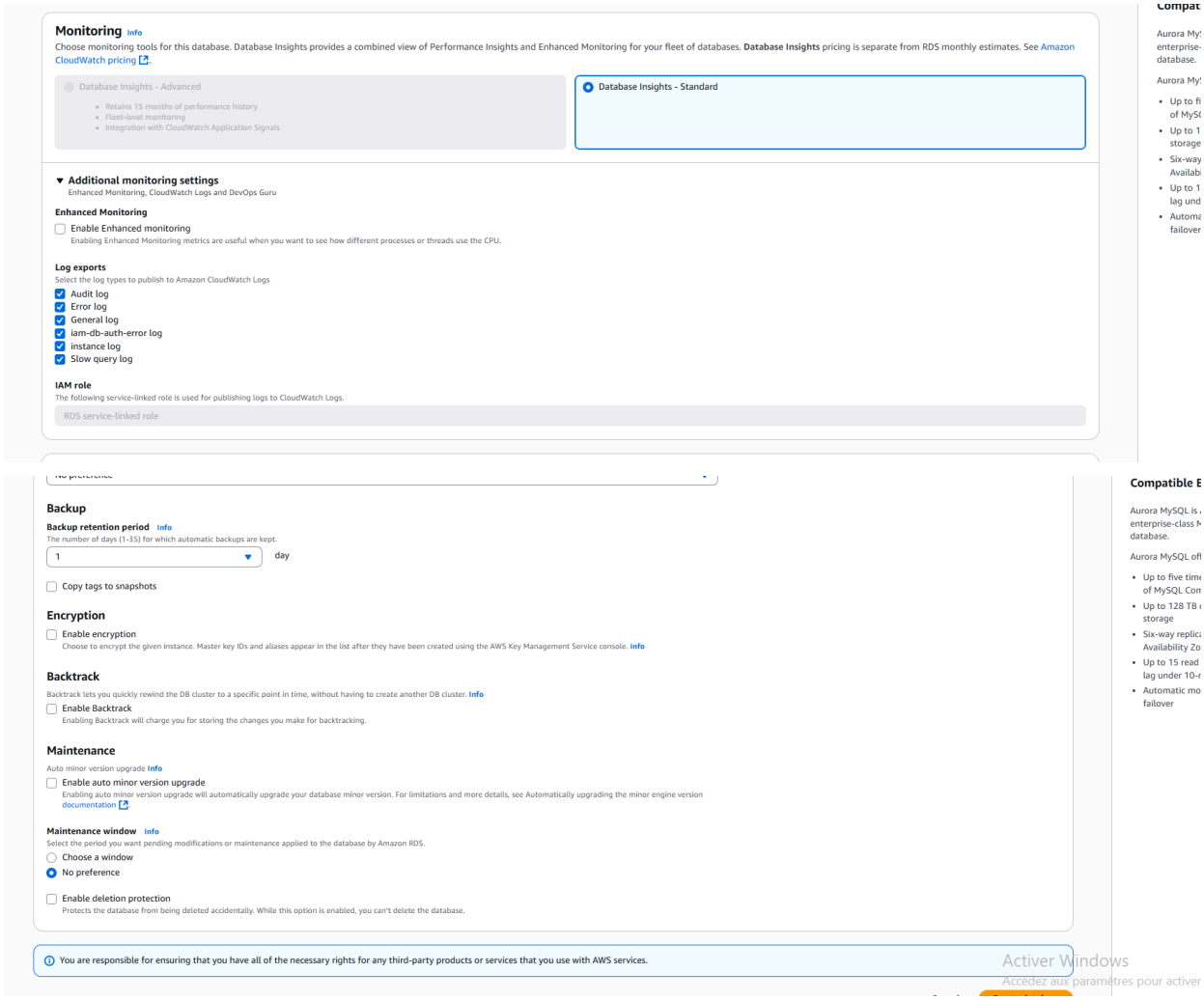
**Certificate authority - *optional*** Info

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

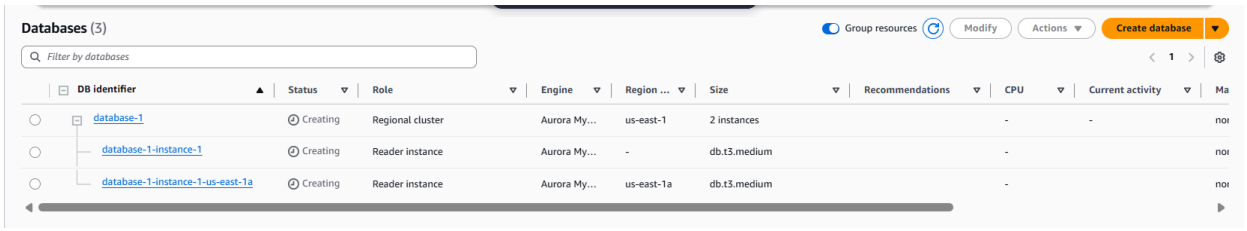
rds-ca-rsa2048-g1 (default)
Expiry: May 26, 2061

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

▶ **Additional configuration**




## Database read et write for automatic failover



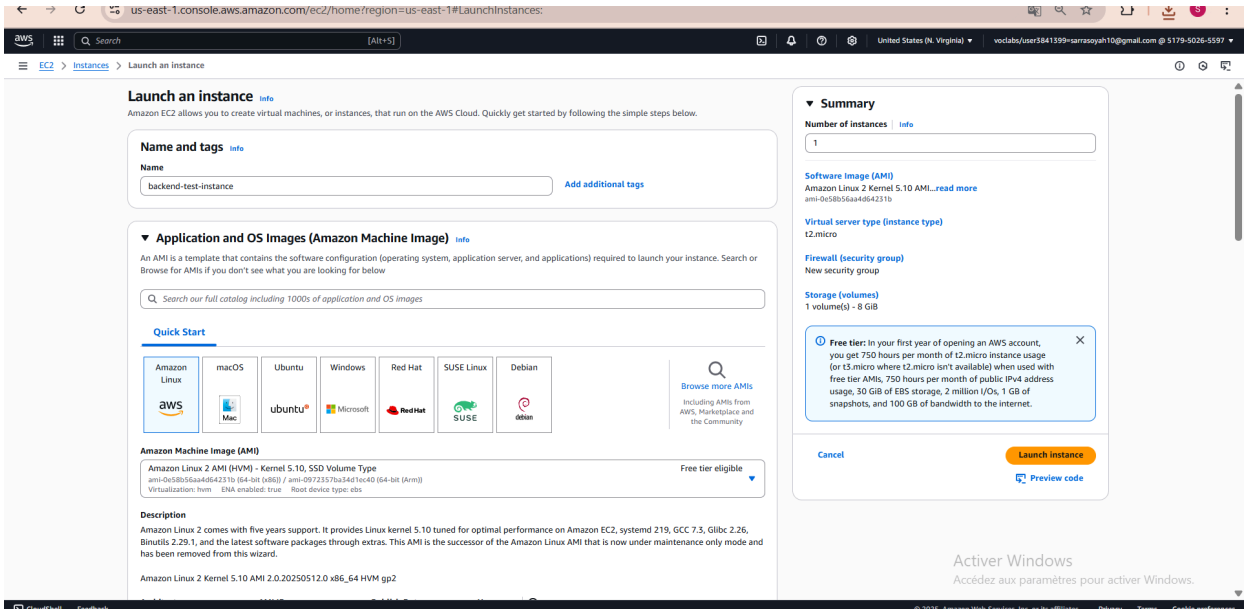

## 5. Backend Deployment

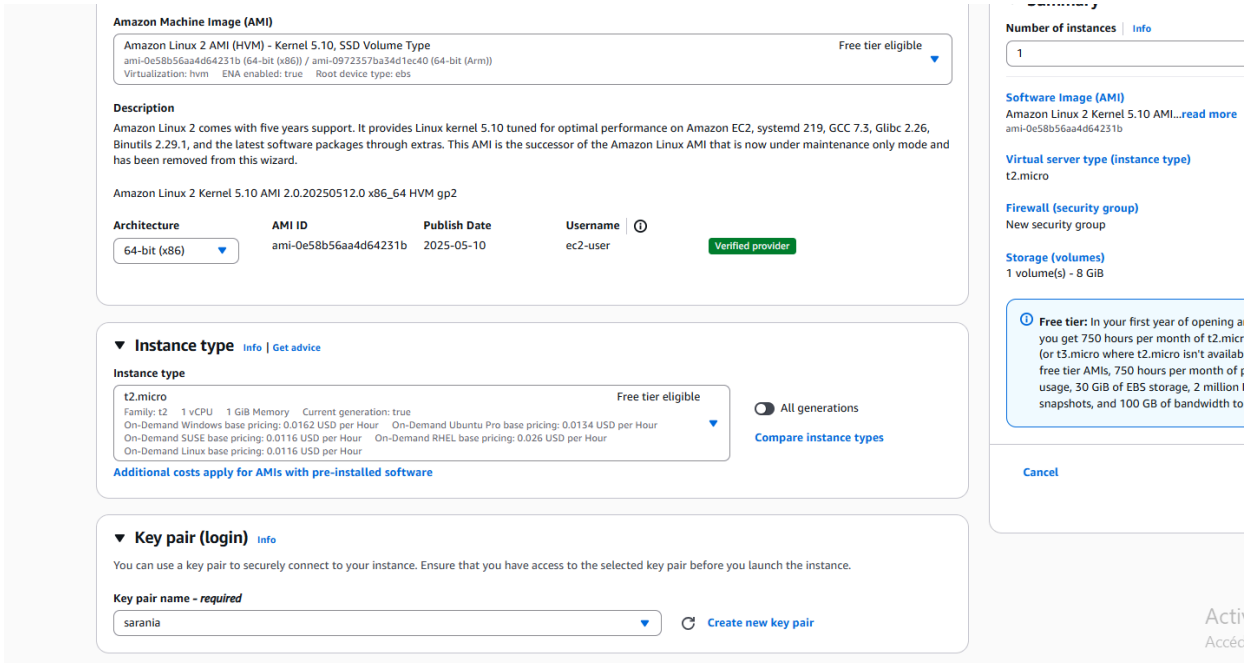
- **Launched EC2 instances for the backend in the private application subnets**

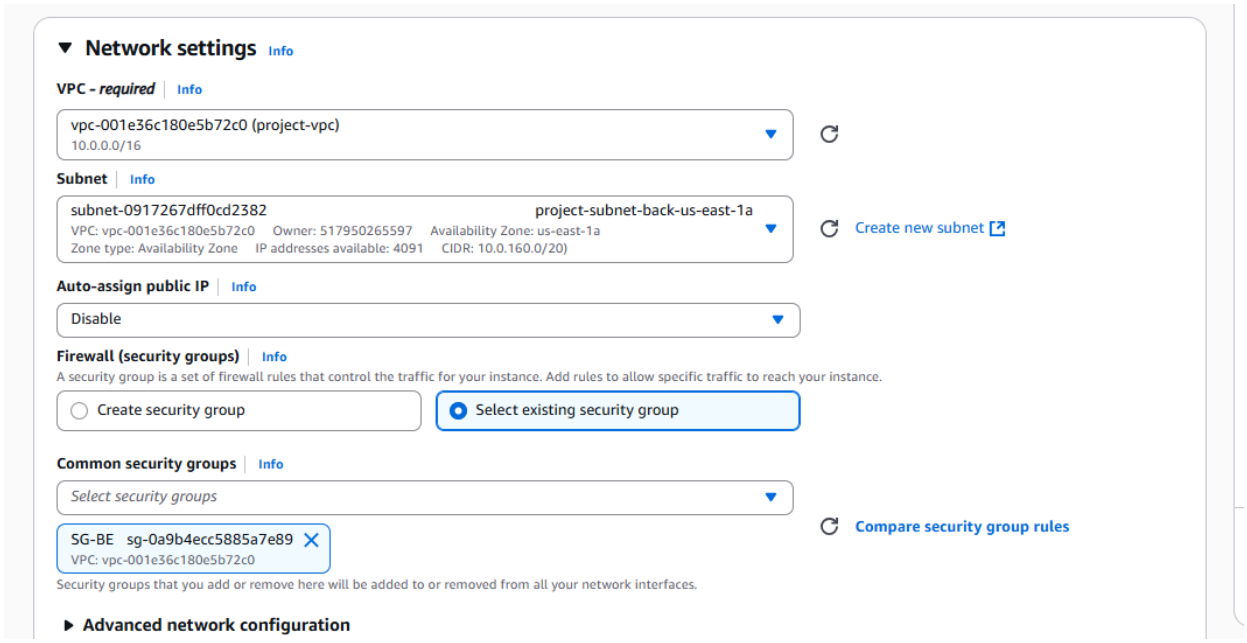
- **Attached the LabInstanceProfile IAM role**

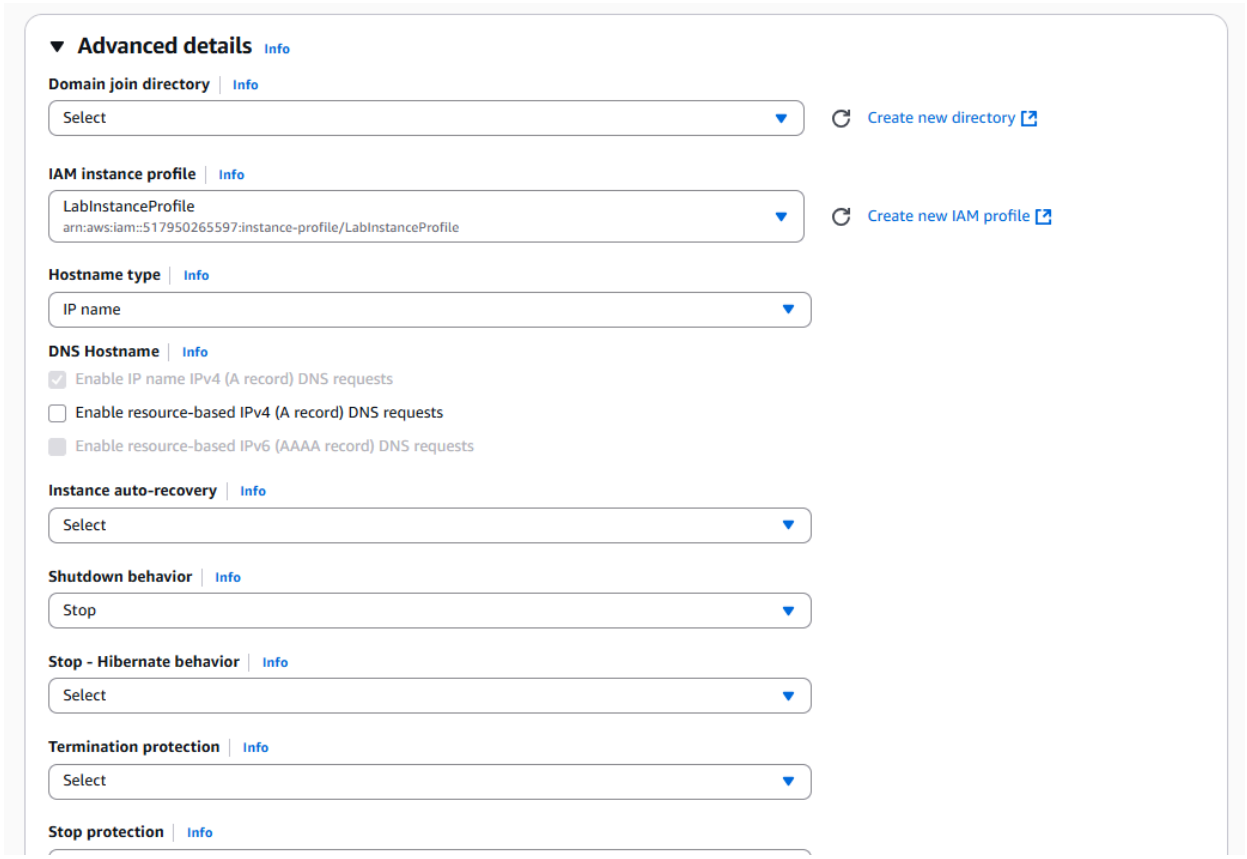
- **Connected via Bastion instance using SSH**
- **Installed Node.js and other dependencies**
- **Used the private RDS endpoint and updated configuration in dbconfig.js**
- **Uploaded backend files to S3**
- **Configured Internal Load Balancer and Target Group**
- **Created a Launch Template and Auto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

- **Creating Backend Instance**

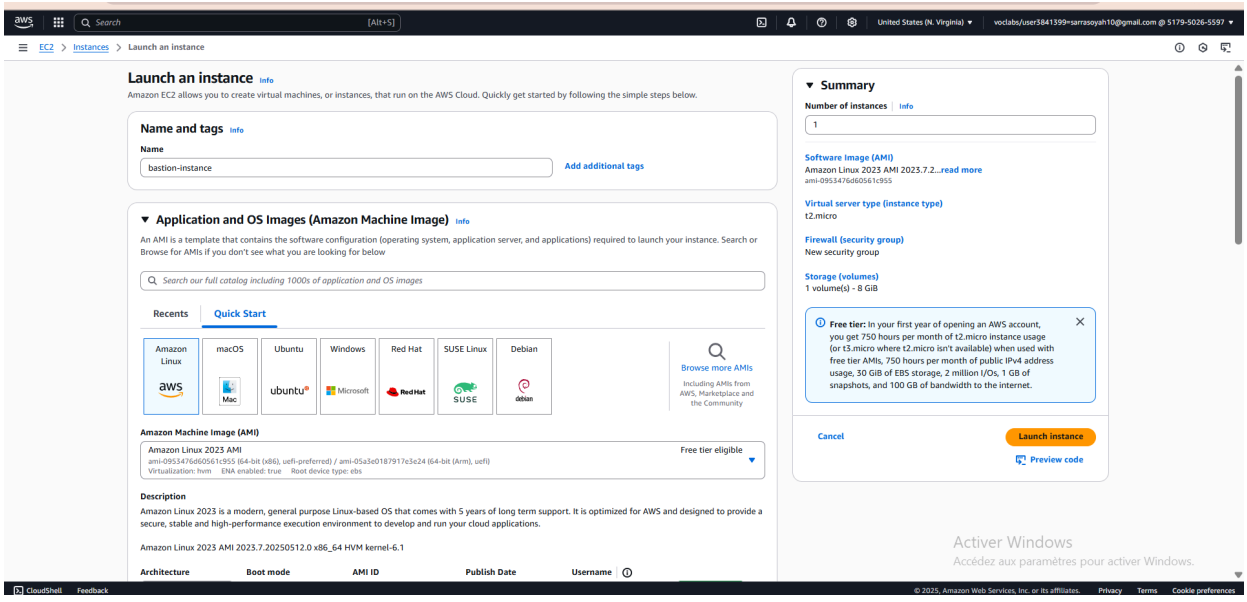


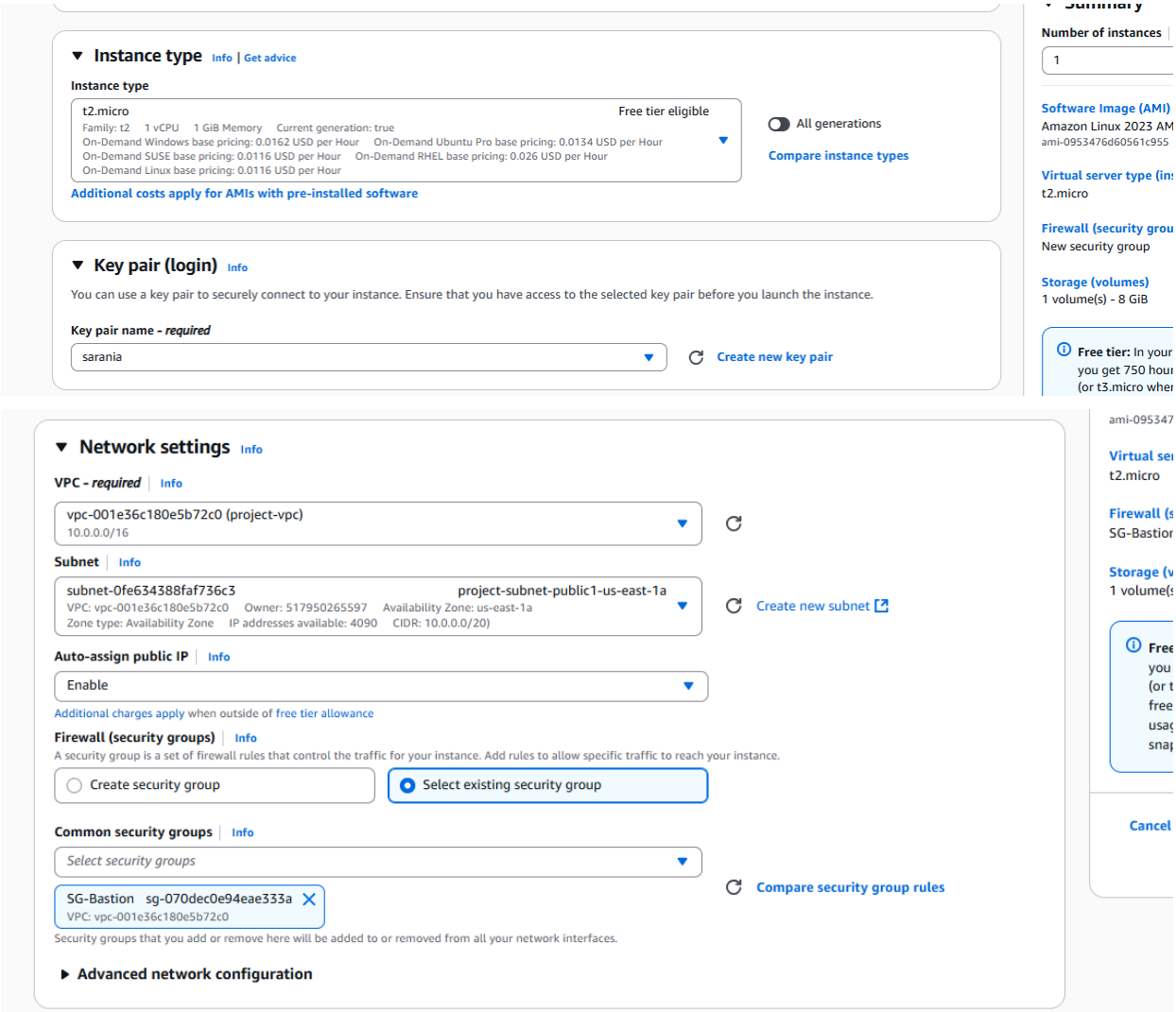

Amazon Machine Image (AMI)
Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
Free tier eligible
ami-0e58b56aa4d64231b (64-bit (x86)) / ami-0972357ba34d1ec40 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs
Description
Amazon Linux 2 comes with five years support. It provides 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
64-bit (x86)
AMI ID
ami-0e58b56aa4d64231b
Publish Date
2025-05-10
Username
ec2-user
Verified provider
Instance type Info | Get advice
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour On-Demand 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
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
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.micr
(or t3.micro where t2.micro isn't availab
free tier AMIs, 750 hours per month of
usage, 30 GiB of EBS storage, 2 million
snapshots, and 100 GB of bandwidth to
Cancel


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
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




- **Creating Bastion Instance to connect to the backend one**









**PS: Don't' forget to always put LabInstanceProfile 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:VpNwWMMOHknbbZB4B4rvccaHVDARK1WPWrS5fDCx4JA.
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)
$
```

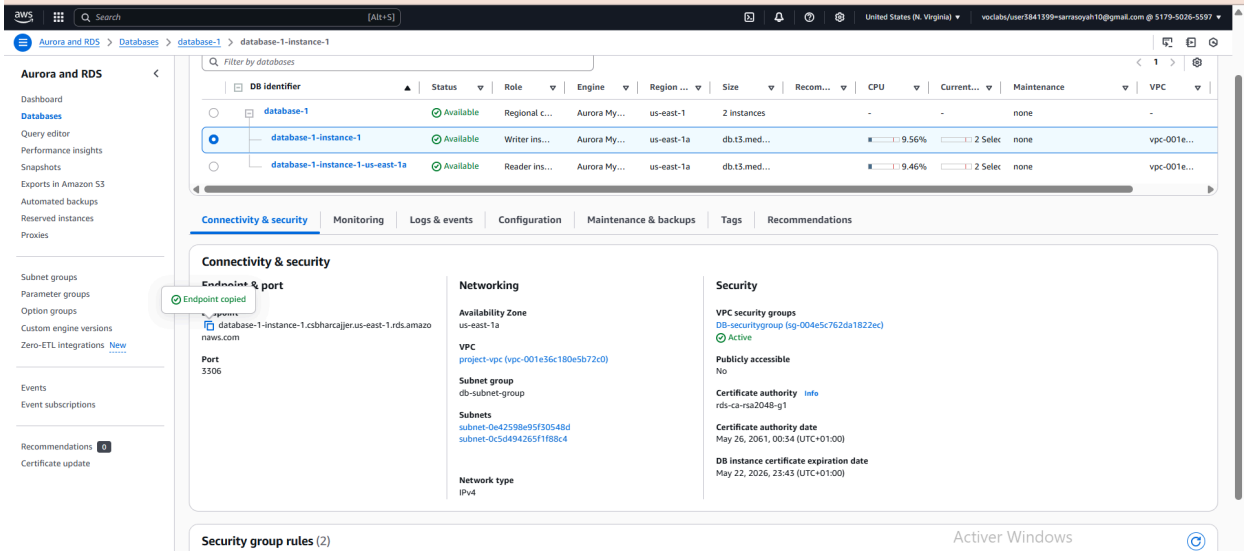
## Pinging the Instance

```
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~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[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:s3ZxQ62AZYj3qb31LQ9tz8O7wWkLRLWtxtzJNPdlrjw.
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.
       _/m/'           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
^C
--- 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                                                                                                                                                | 3.6 kB  00:00:00
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

================================================================================================================================================================================
 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                                                                                                                         1/1
  Verifying  : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64                                                                                                                         1/1

Installed:
  mariadb.x86_64 1:5.5.68-1.amzn2.0.1

Complete!
```



- **Extracting the endpoint of the writer instance of RDS**

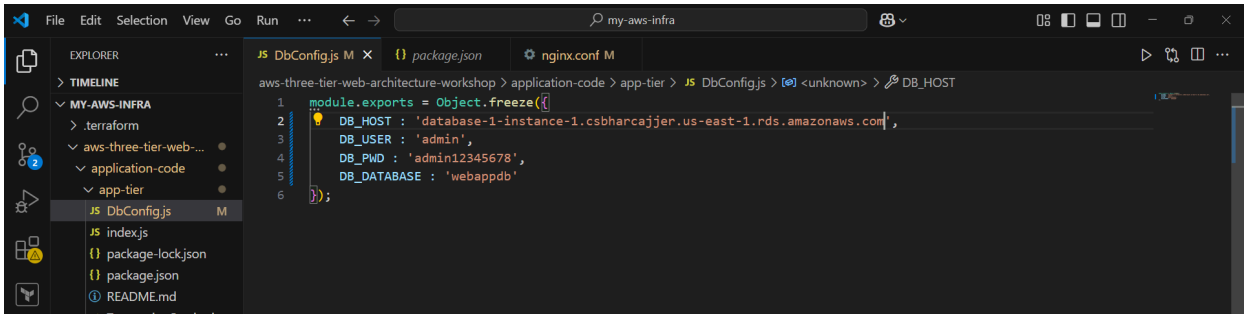




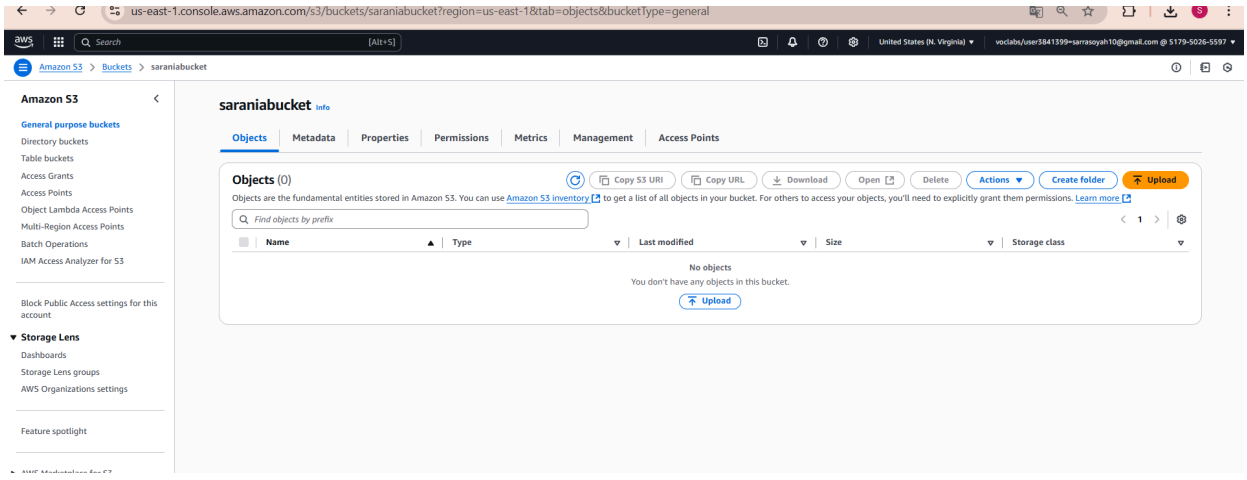

```
Complete!
[ec2-user@ip-10-0-166-110 ~]$ mysql -h database-1-instance-1.csbharcajjer.us-east-1.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 163
Server version: 8.0.39 8bc99e28

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

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

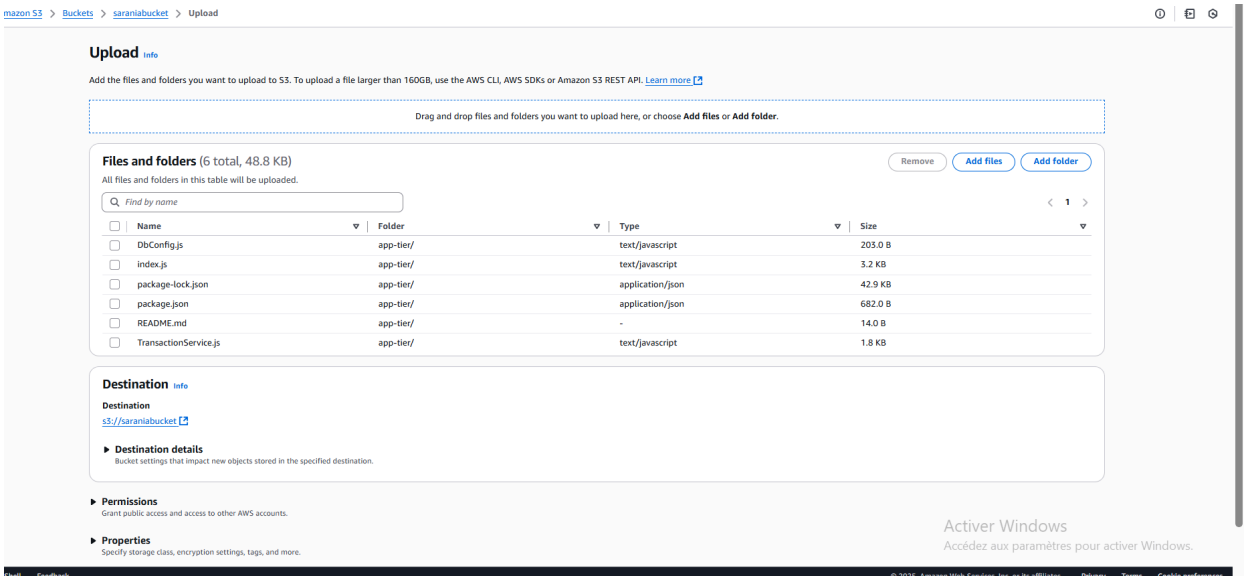
```
MySQL [(none)]> CREATE DATABASE webappdb;
Query OK, 1 row affected (0.00 sec)

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:**

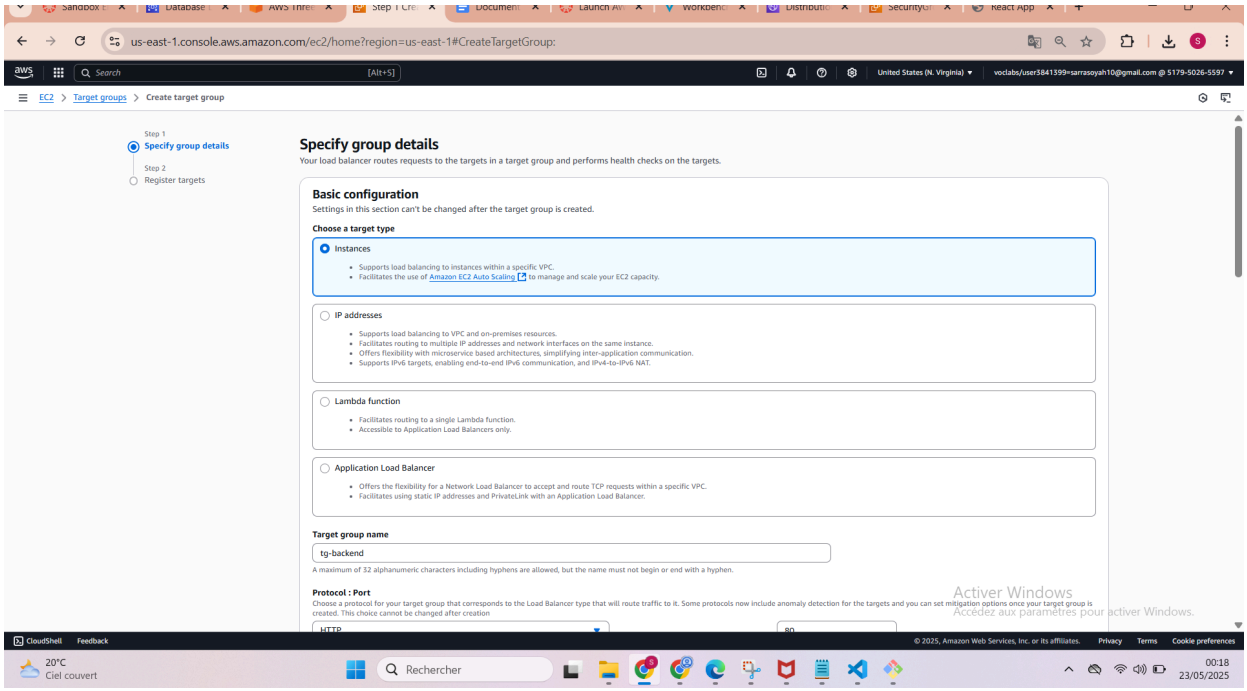


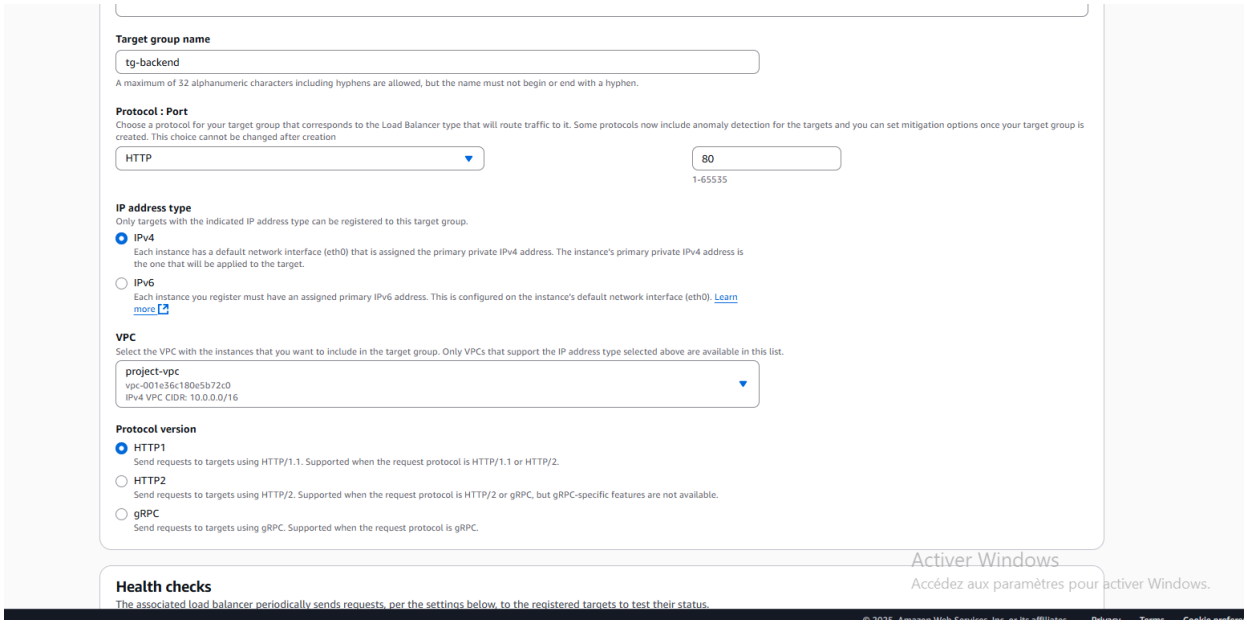

- **Uploading backend files to our S3**

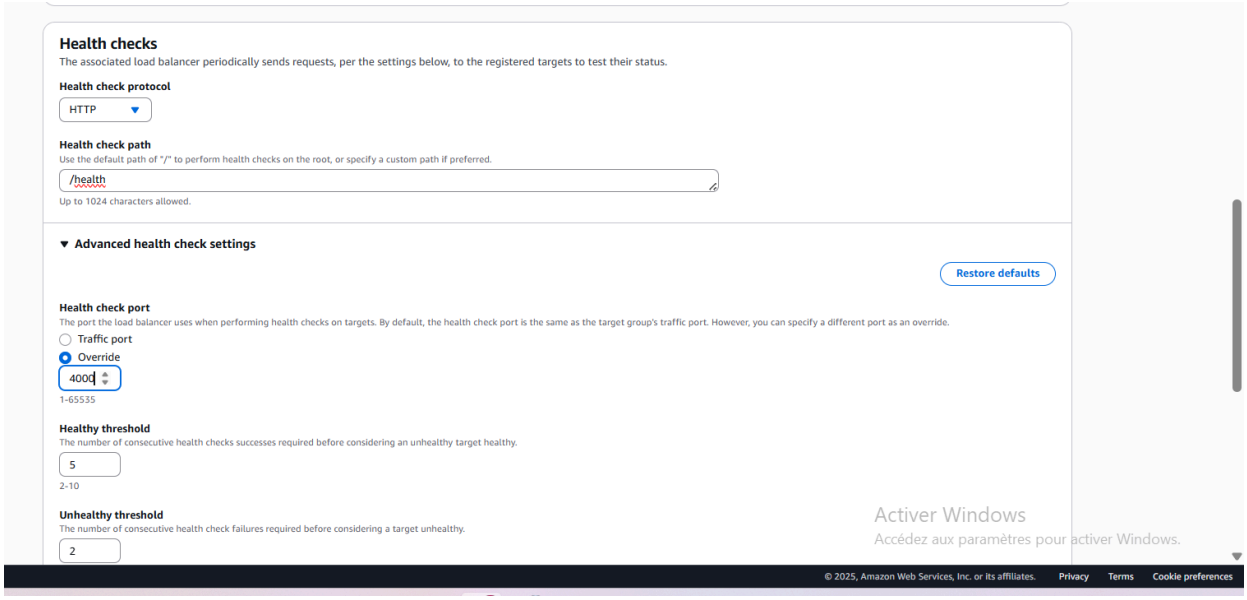




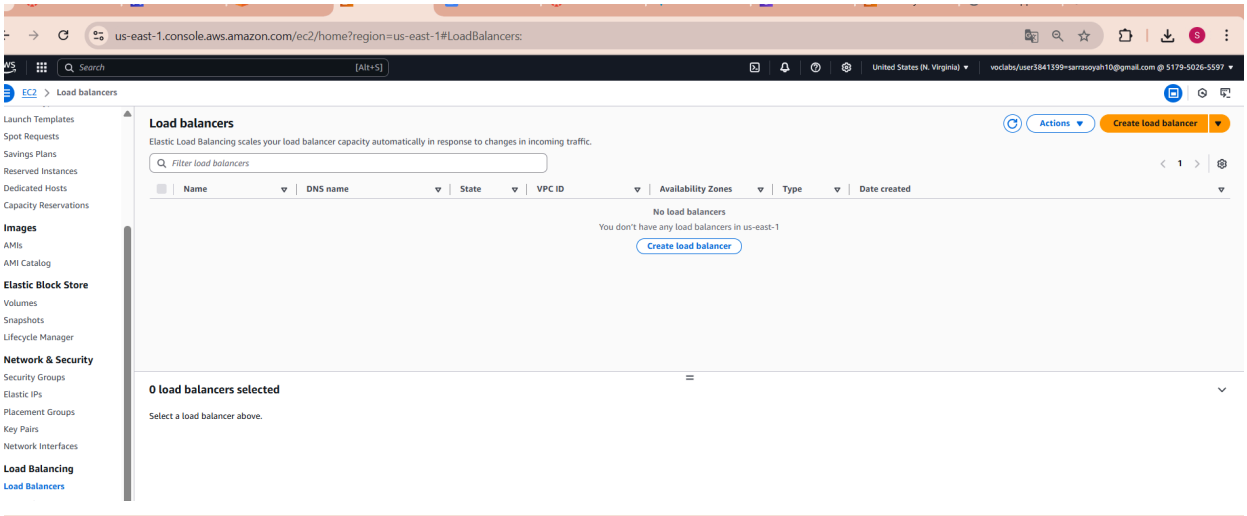

- **Creating the target group of the backend**

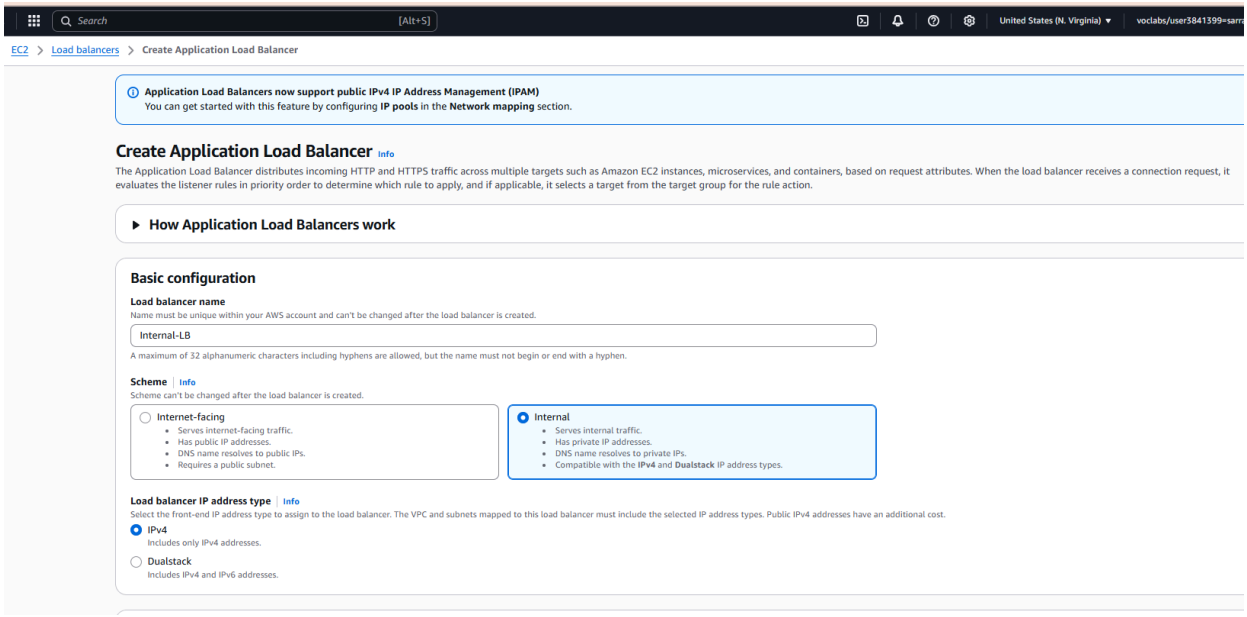


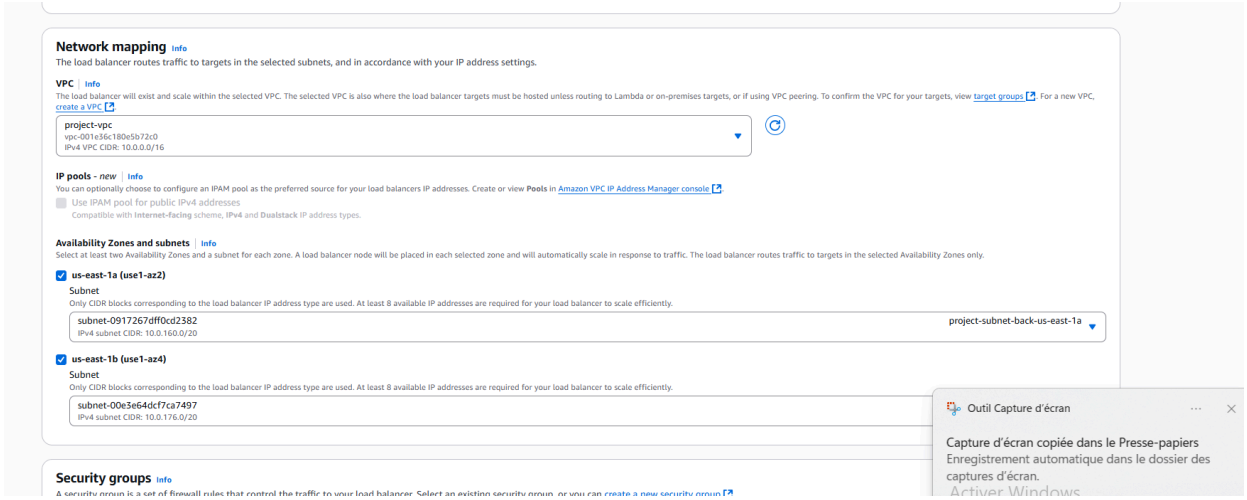


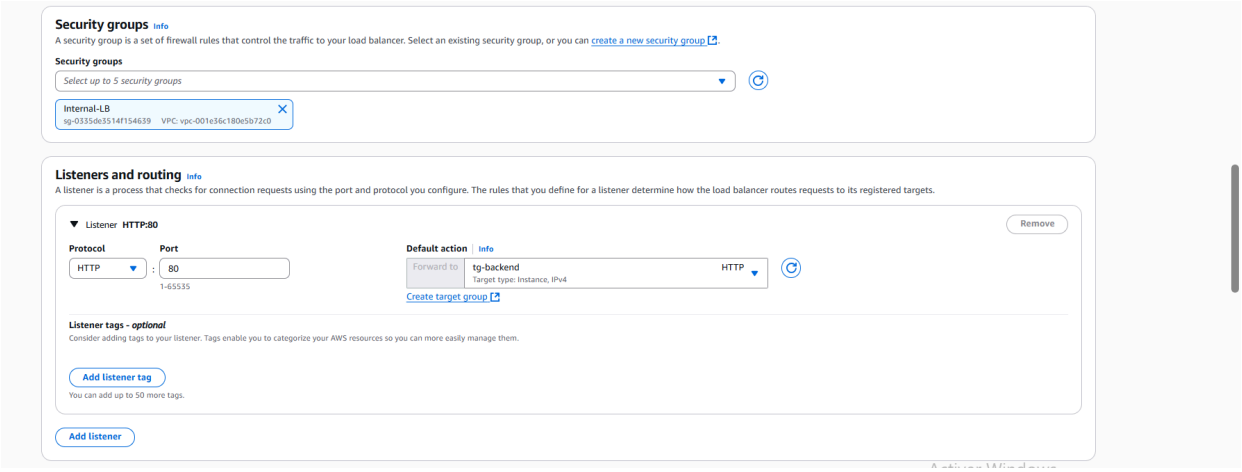




- **creating internal LB:**

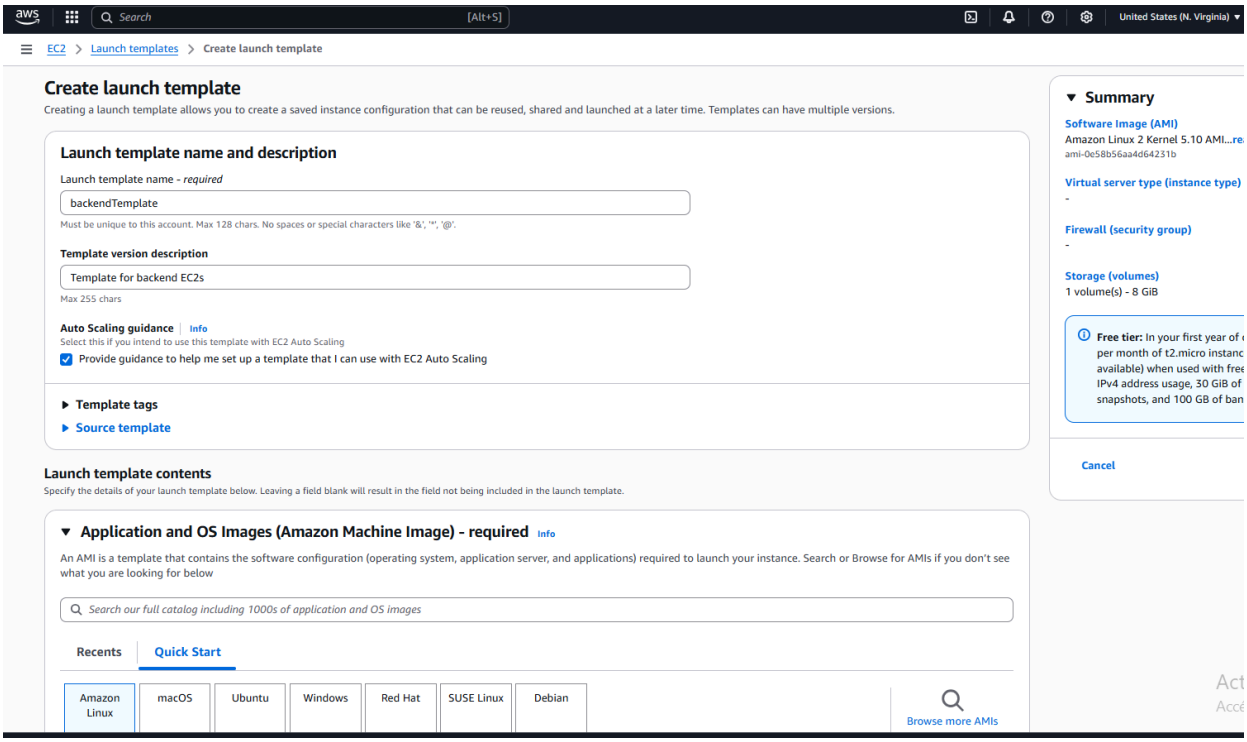

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LoadBalancers:
Search [Alt+S]
United States (N. Virginia)
EC2 > Load balancers
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
Load Balancers
Load balancers
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.
Actions
Create load balancer
Filter load balancers
Name
DNS name
State
VPC ID
Availability Zones
Type
Date created
No load balancers
You don't have any load balancers in us-east-1
Create load balancer
0 load balancers selected
Select a load balancer above.


Search [Alt+S]
United States (N. Virginia)
EC2 > Load balancers > 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 Info
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 Info
Scheme can't be changed after the load balancer is created.
Internet-facing
Serves internet-facing traffic.
Has public IP addresses.
DNS name resolves to public IPs.
Requires a public subnet.
Internal
Serves internal traffic.
Has private IP addresses.
DNS name resolves to private IPs.
Compatible with the IPv4 and Dualstack IP address types.
Load balancer IP address type Info
Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.
IPv4
Includes only IPv4 addresses.
Dualstack
Includes IPv4 and IPv6 addresses.


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-001e16c180e5b72c0
IPv4 VPC 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 balancers IP addresses. Create or view Pools in Amazon VPC IP Address Manager console.
Use IPAM pool for public IPv4 addresses
Compatible with Internet-facing scheme, IPv4 and Dualstack IP address types.
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-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-0917267dff0cd2382
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-00e3e64dcf7ca7497
IPv4 subnet CIDR: 10.0.176.0/20
Security groups Info
Outil Capture d'écran
Capture d'écran copiée dans le Presse-papiers
Enregistrement automatique dans le dossier des captures d'écran.




- **Launching the template of our backend**



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
Including AMIs from AWS, Marketplace and the Community

**Amazon Machine Image (AMI)**

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type — Free tier eligible
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 | Verified provider |

## Instance type Info | Get advice

Advanced

## Instance type Info | Get advice

Advanced

**Instance type**

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand 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

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**

sarania

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.

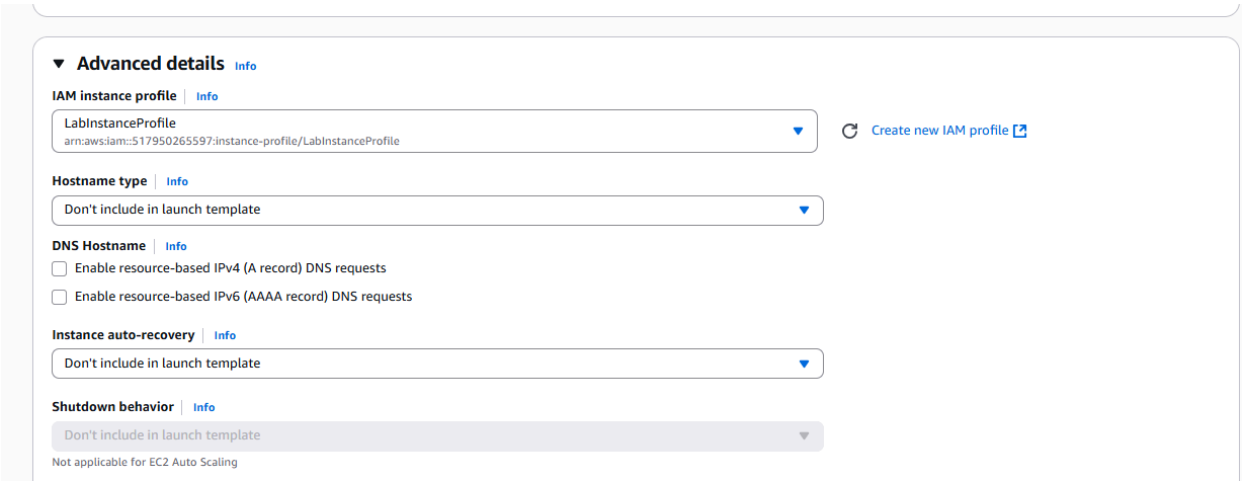
Select existing security group | Create security group

**Security groups** Info

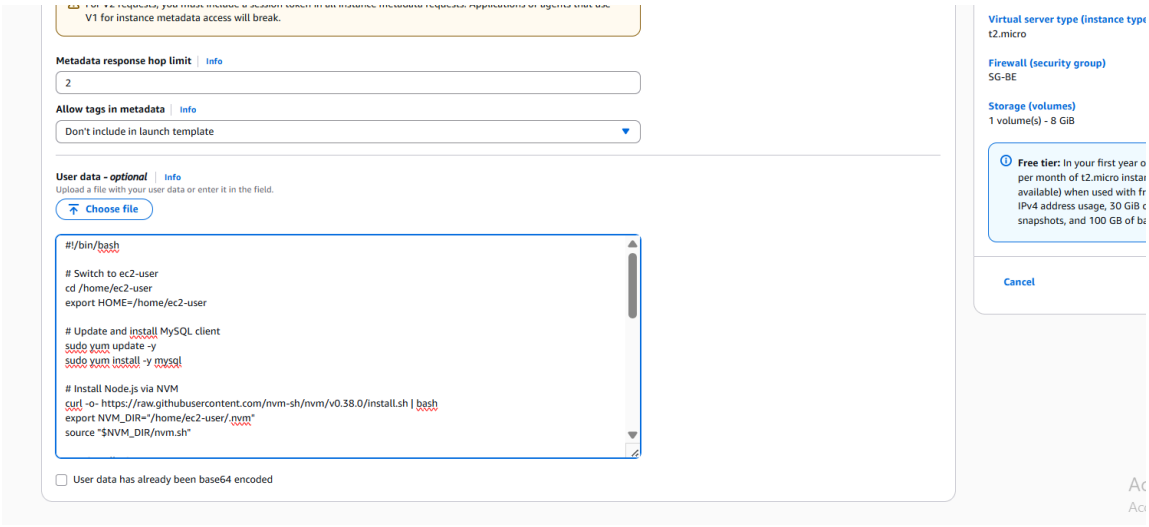
Select security groups

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

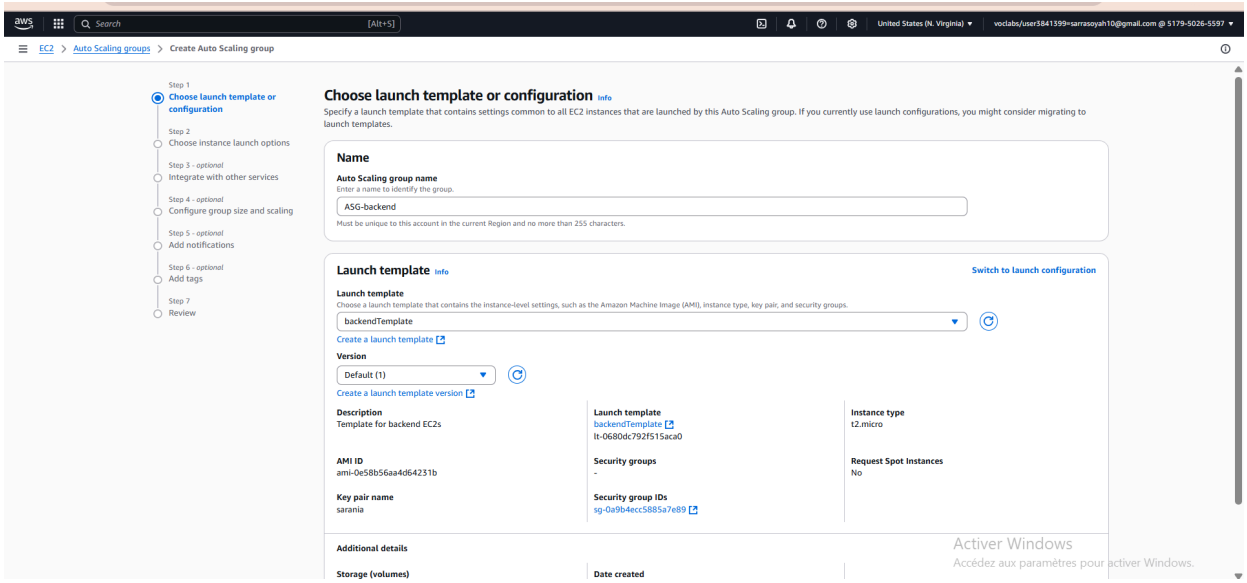
Compare security group rules

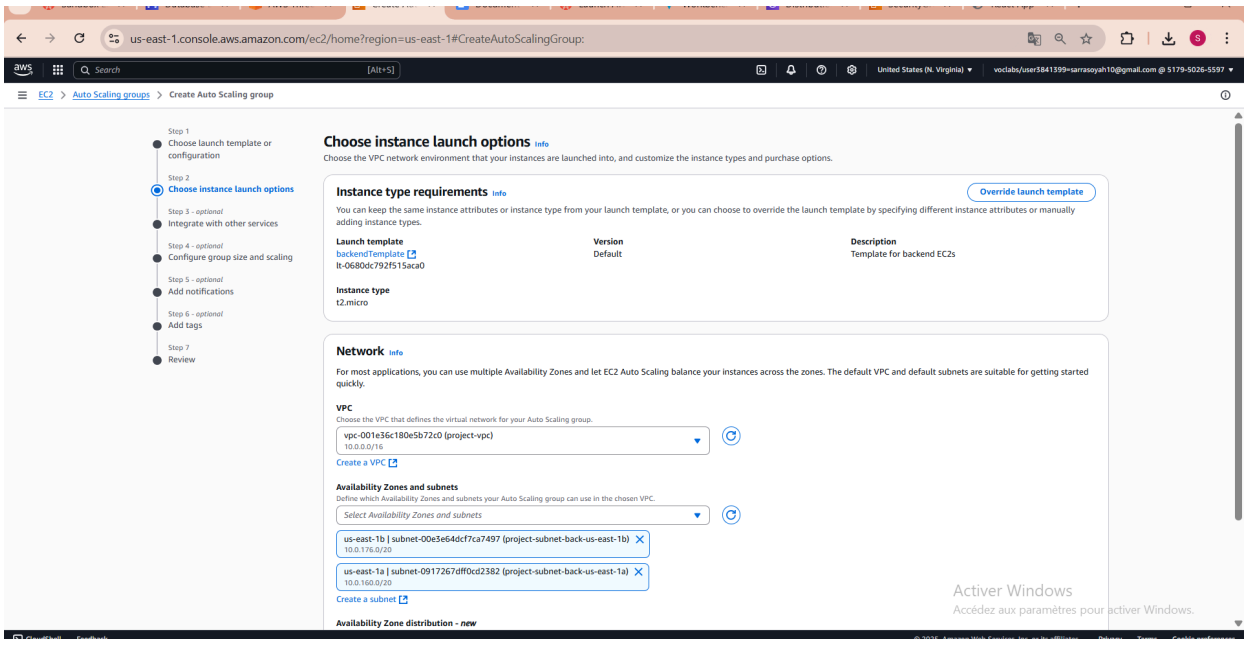


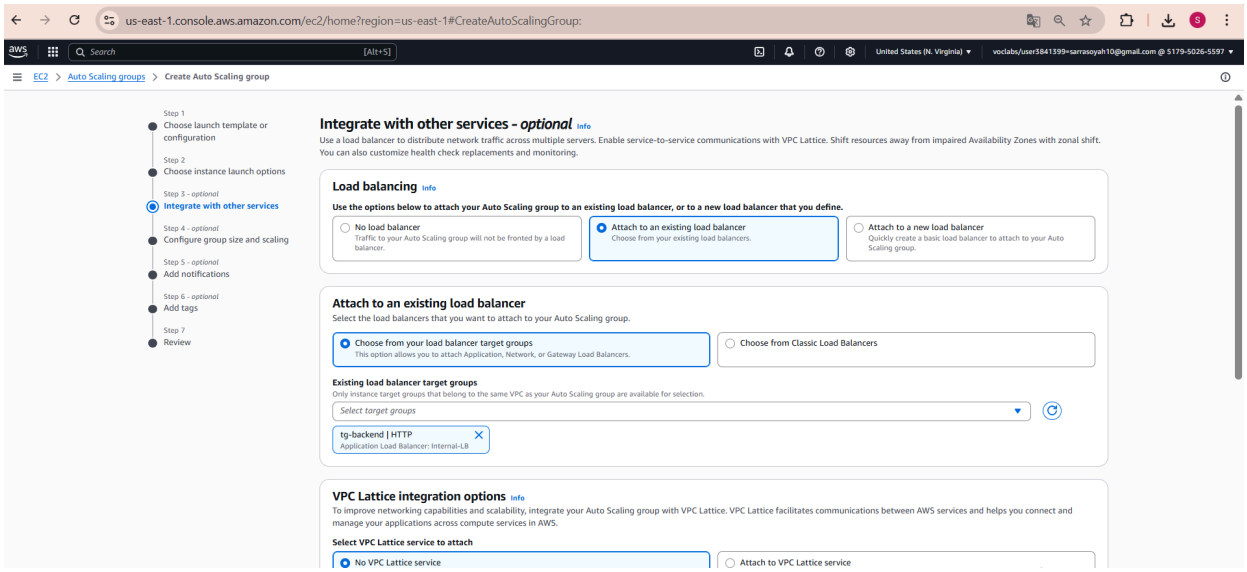

- **Configuring user data for the backend EC2 image**

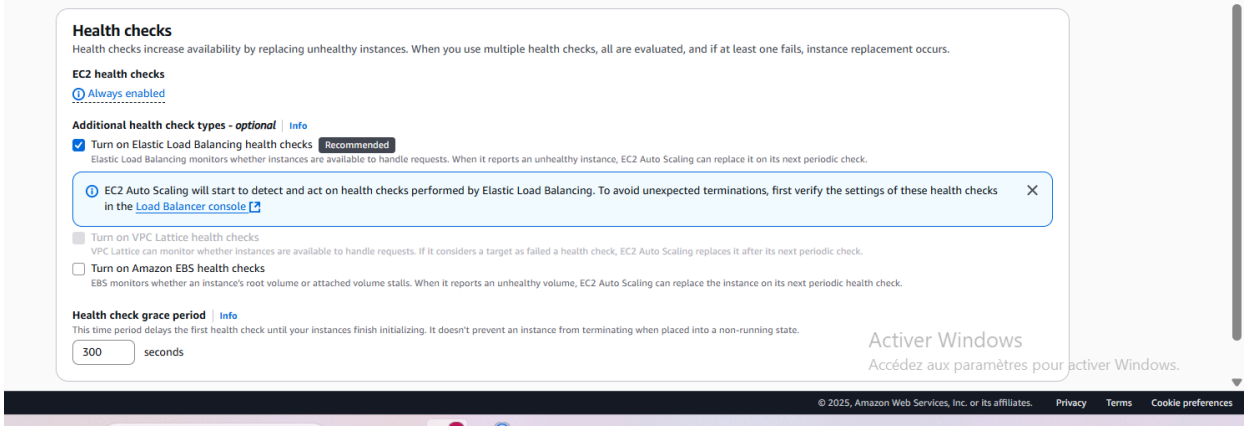


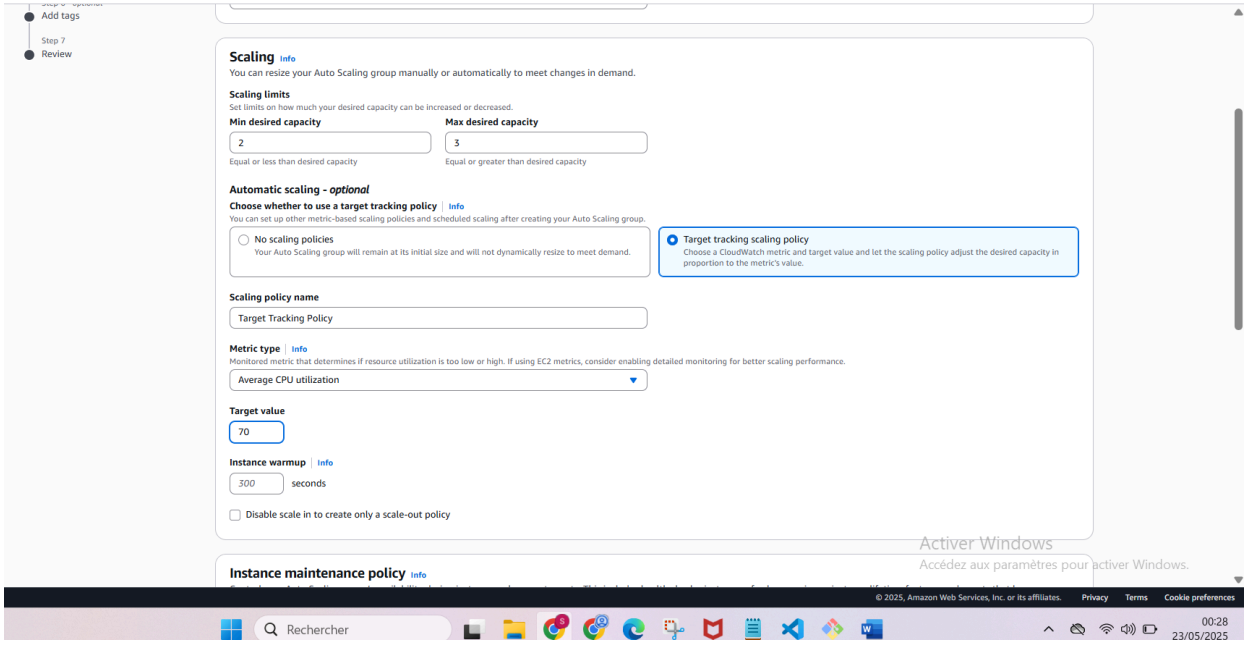

- **AutoScaling Group of the Backend**

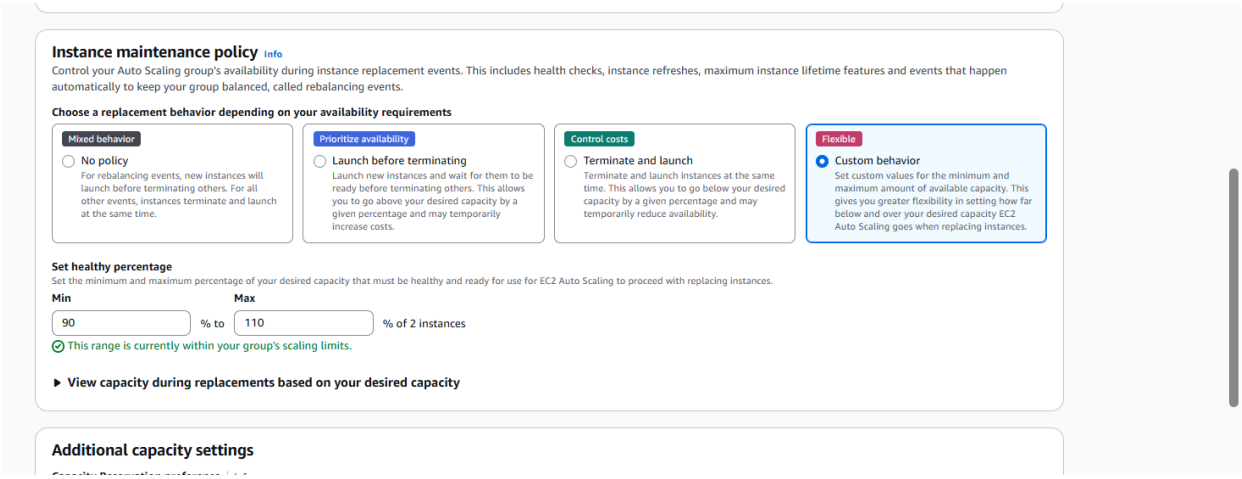

Search [Alt+S]
United States (N. Virginia)
voclabs/user3841399=sarrasoyah10@gmail.com @ 5179-5026-5597
EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template or configuration
Step 2
Choose instance launch options
Step 3 - optional
Integrate with other services
Step 4 - optional
Configure group size and scaling
Step 5 - optional
Add notifications
Step 6 - optional
Add tags
Step 7
Review
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
Switch to launch configuration
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)
Create a launch template version
Description
Template for backend EC2s
Launch template
backendTemplate
lt-0680dc792f515aca0
Instance type
t2.micro
AMI ID
ami-0e58b56aa4d64231b
Security groups
-
Request Spot Instances
No
Key pair name
sarania
Security group IDs
sg-0a9b4ecc5885a7e89
Additional details
Storage (volumes)
Date created
Activer Windows
Accédez aux paramètres pour activer Windows.


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateAutoScalingGroup:
Search [Alt+S]
United States (N. Virginia)
voclabs/user3841399=sarrasoyah10@gmail.com @ 5179-5026-5597
EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template or configuration
Step 2
Choose instance launch options
Step 3 - optional
Integrate with other services
Step 4 - optional
Configure group size and scaling
Step 5 - optional
Add notifications
Step 6 - optional
Add tags
Step 7
Review
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
Override launch template
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
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
us-east-1b | subnet-00e3e64dcf7ca7497 (project-subnet-back-us-east-1b)
10.0.176.0/20
us-east-1a | subnet-0917267dff0cd2382 (project-subnet-back-us-east-1a)
10.0.160.0/20
Create a subnet
Availability Zone distribution - new
Activer Windows
Accédez aux paramètres pour activer Windows.

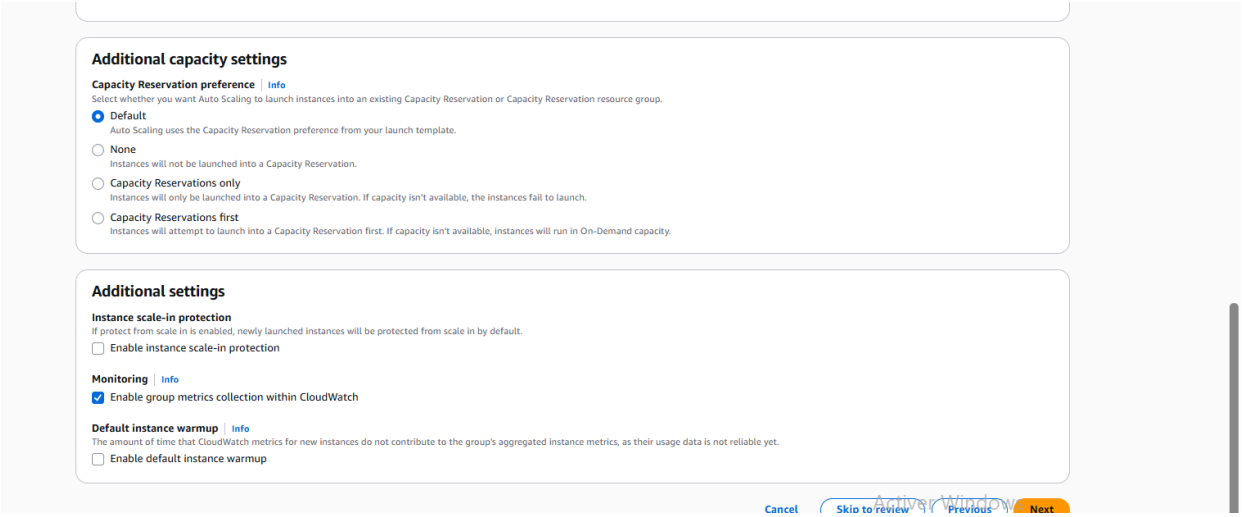

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateAutoScalingGroup:
EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1 Choose launch template or configuration
Step 2 Choose instance launch options
Step 3 - optional Integrate with other services
Step 4 - optional Configure group size and scaling
Step 5 - optional Add notifications
Step 6 - optional Add tags
Step 7 Review
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
Application Load Balancer: Internal-LB
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
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.
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences


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
2
Equal or less than desired capacity
Max desired capacity
3
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
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
Activer Windows
Accédez aux paramètres pour activer Windows.
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
Rechercher
00:28
23/05/2025




- **enabling cloudwatch**



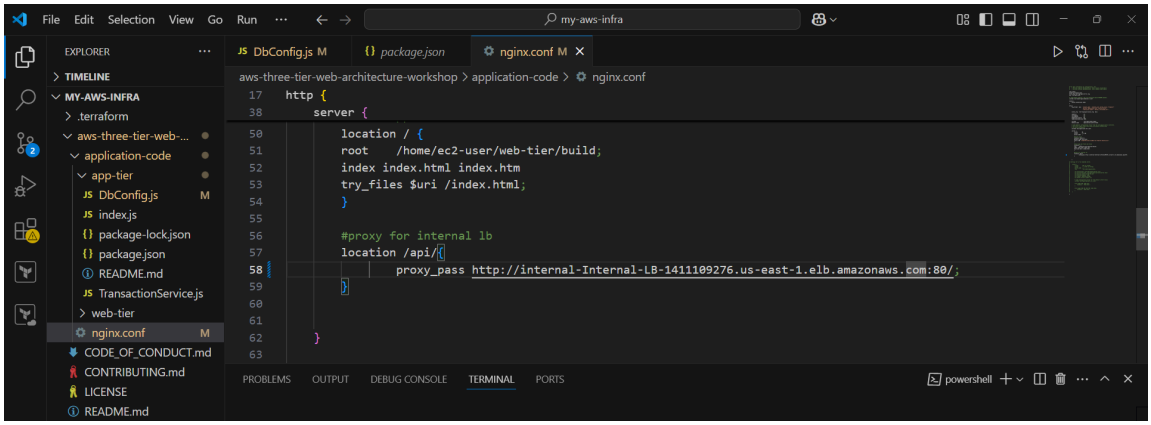

## 6. Frontend Deployment

- **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**

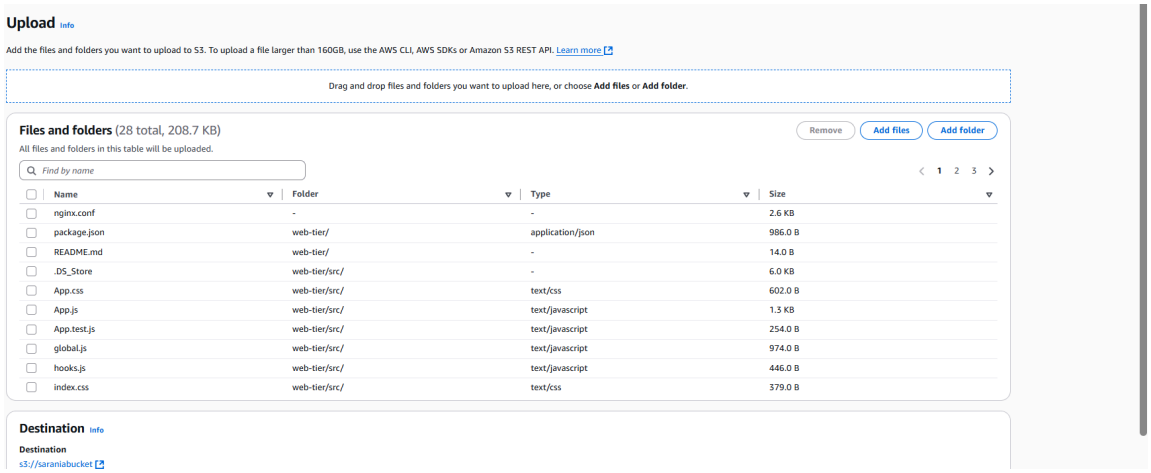
- **Deployed an Internet-Facing Load Balancer and mapped frontend traffic to it**

- **Configured Auto Scaling for frontend servers based on CPU utilization**

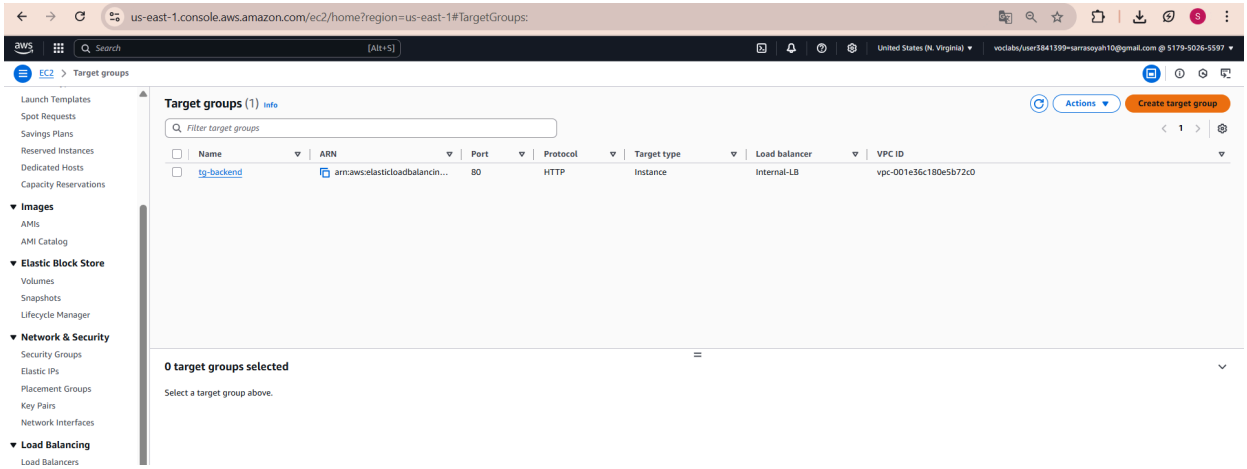
- **Update the configuration file**

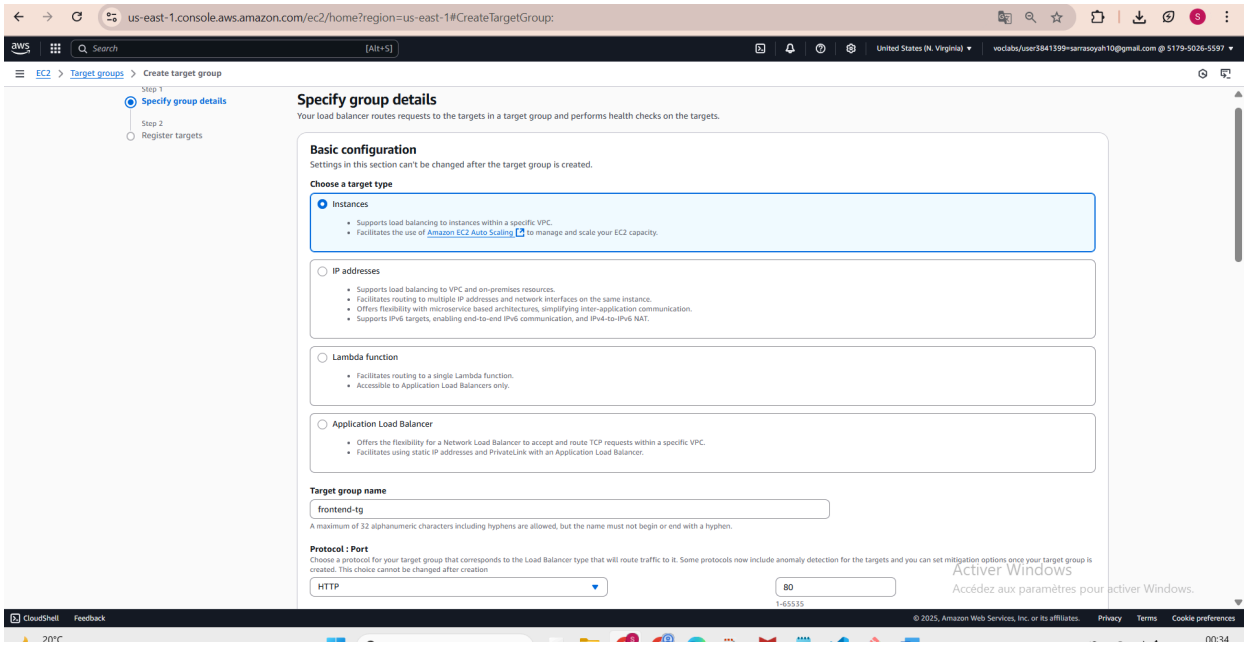


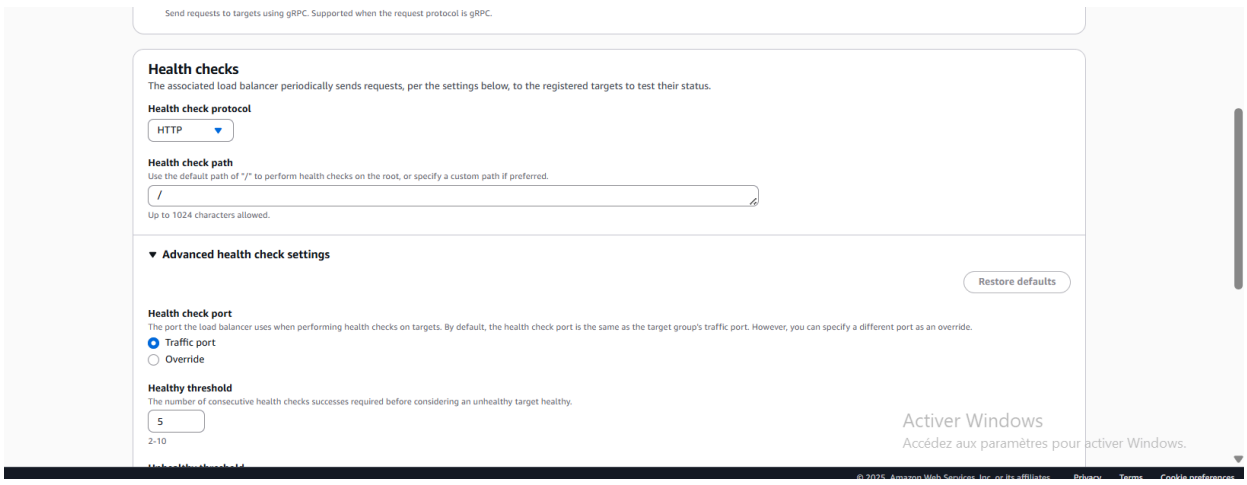

- **Deploy the frontend code to S3**




- **Create a target group**



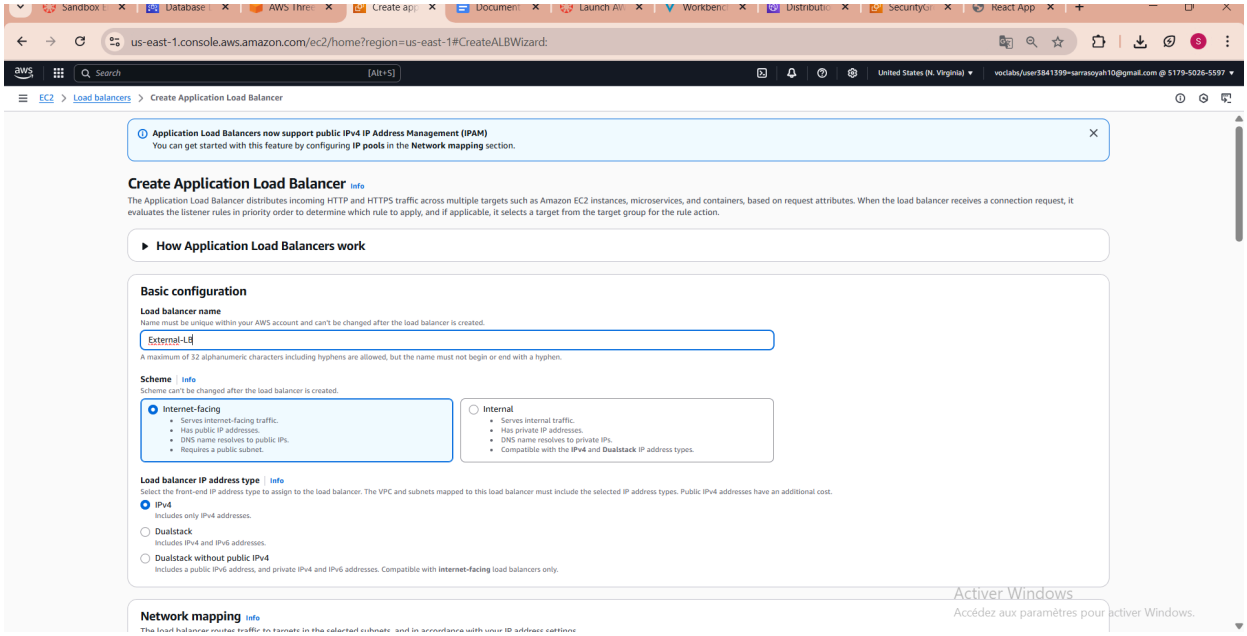



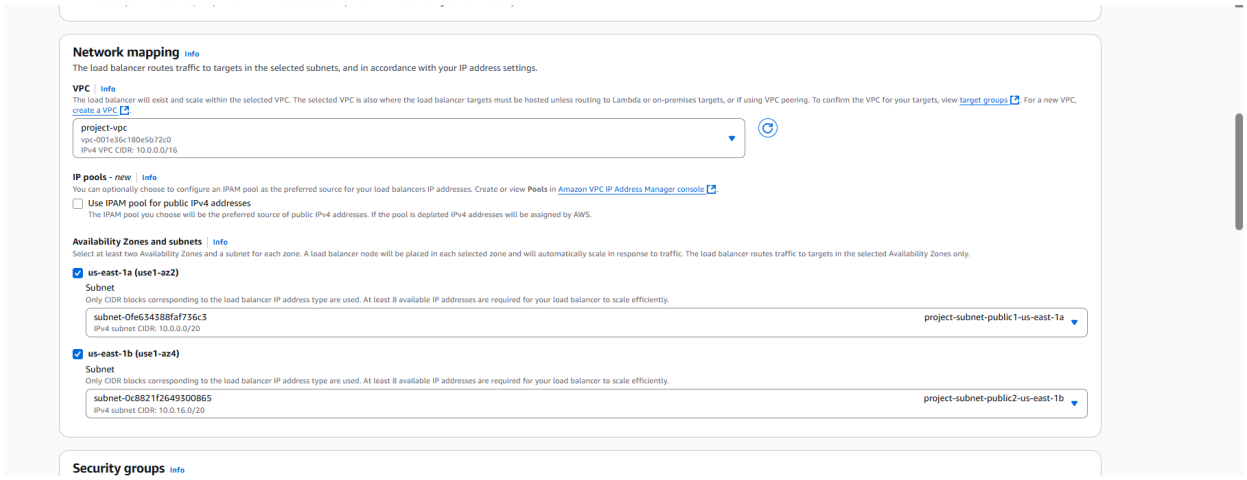

## 7. External Load Balancer & Auto Scaling

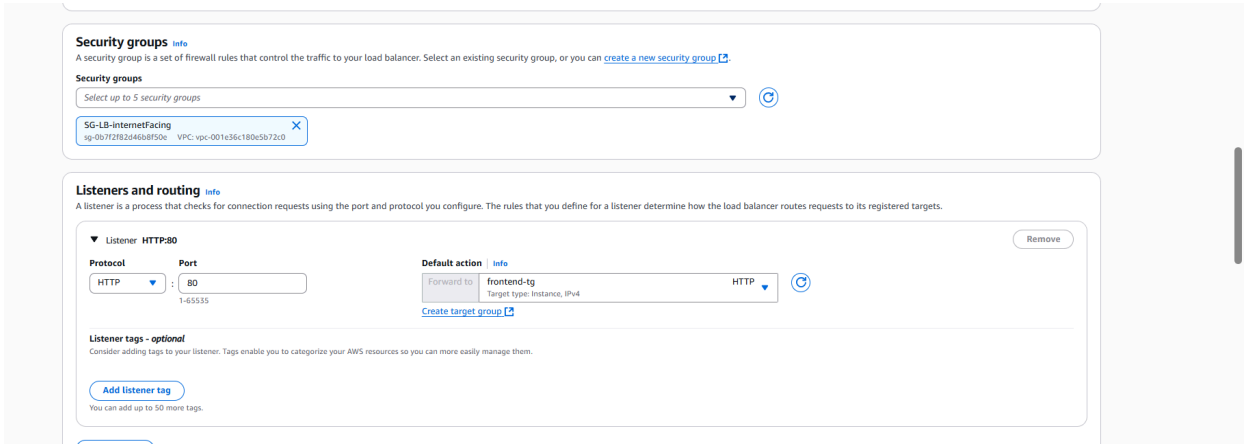
- **External ALB (Application Load Balancer) was deployed with listeners on HTTP/HTTPS.**
- **Mapped to frontend EC2 target group**
- **Configured with two public subnets**

- **Set up an internet-facing load balancer**

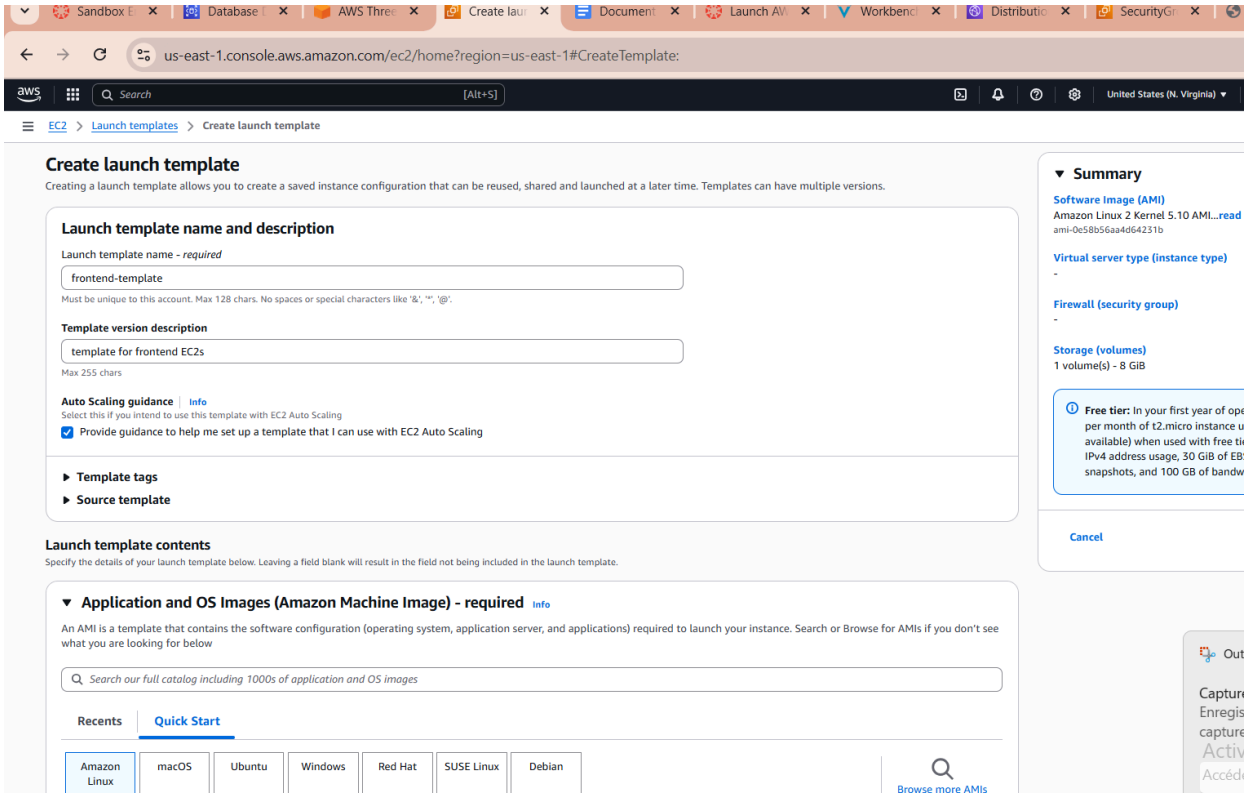


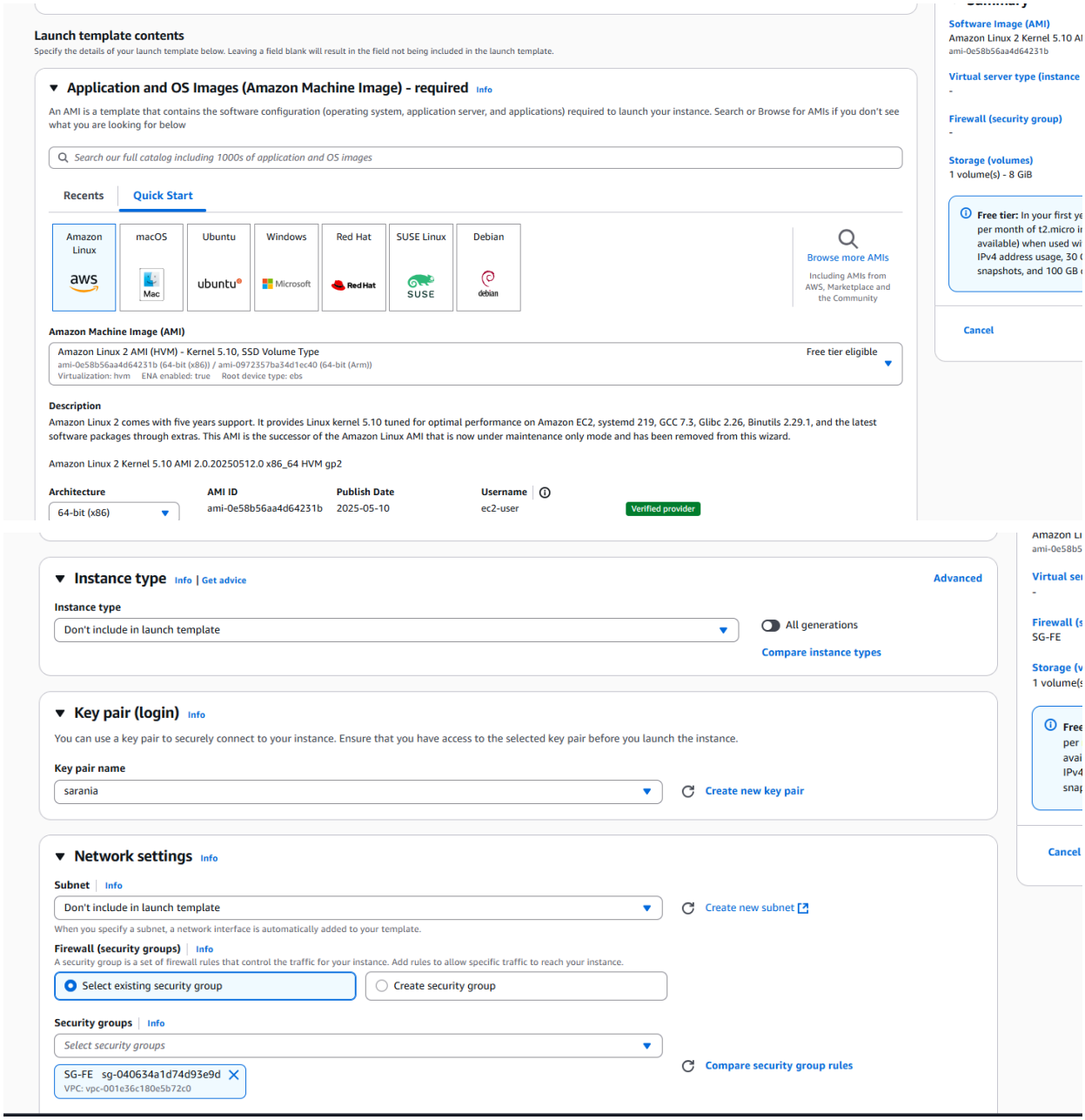

- **Setting its subnets to public**

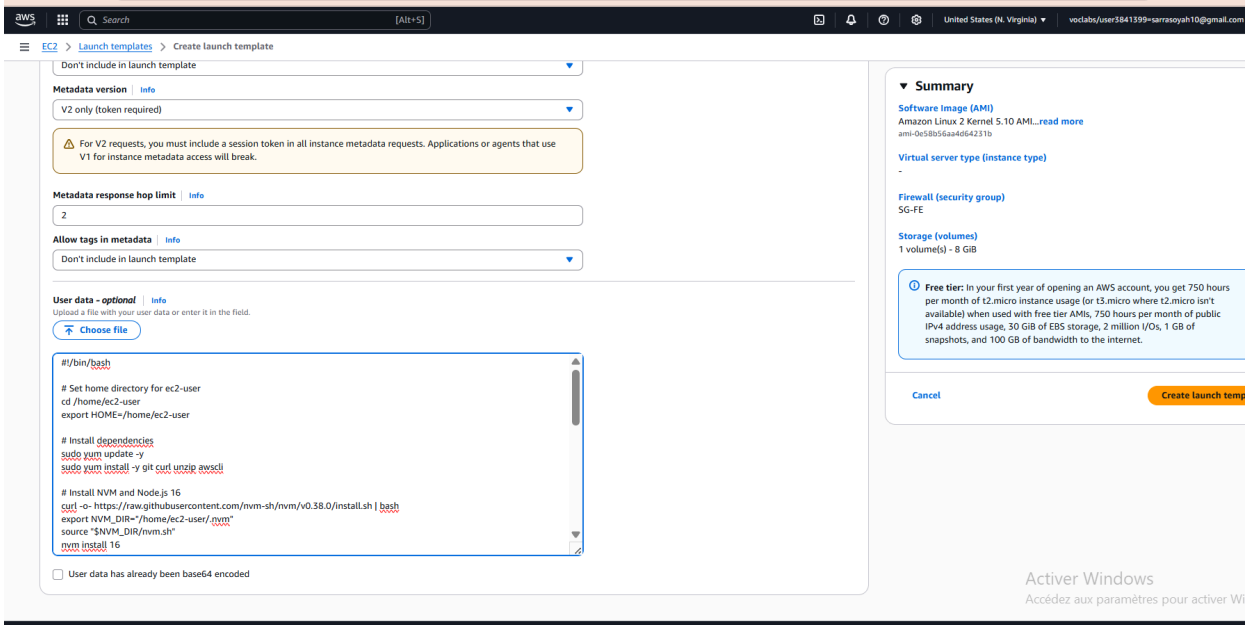




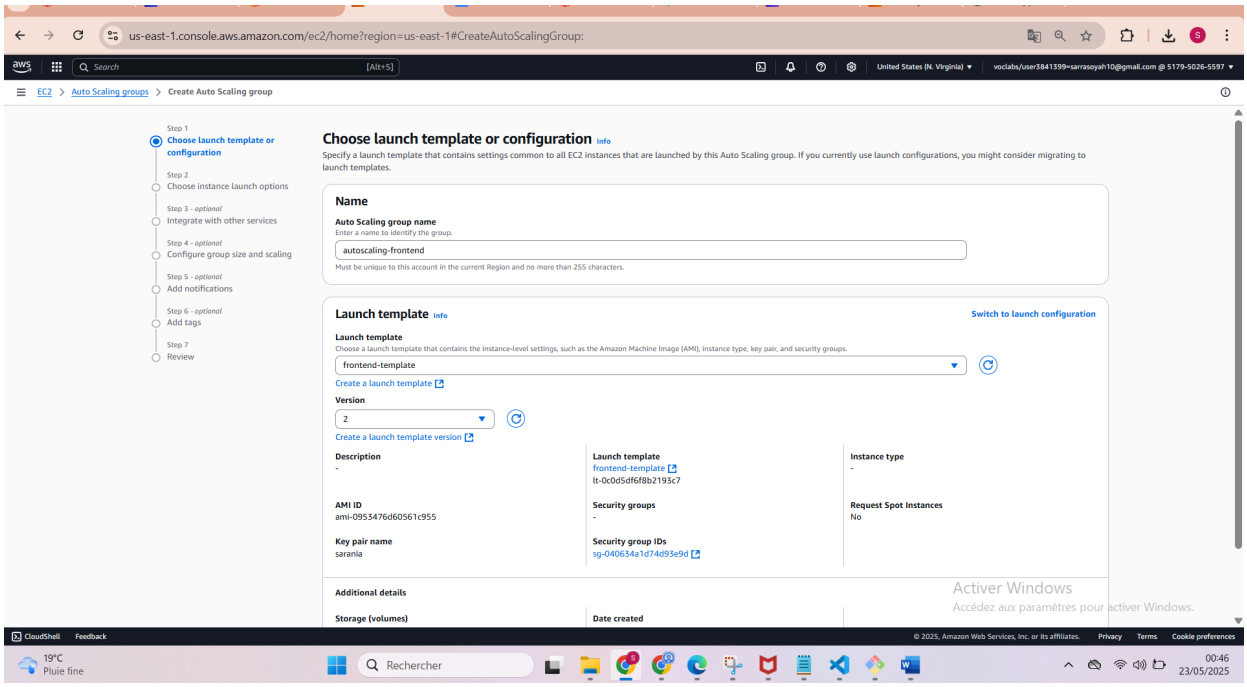

- **Template for frontend EC2s**

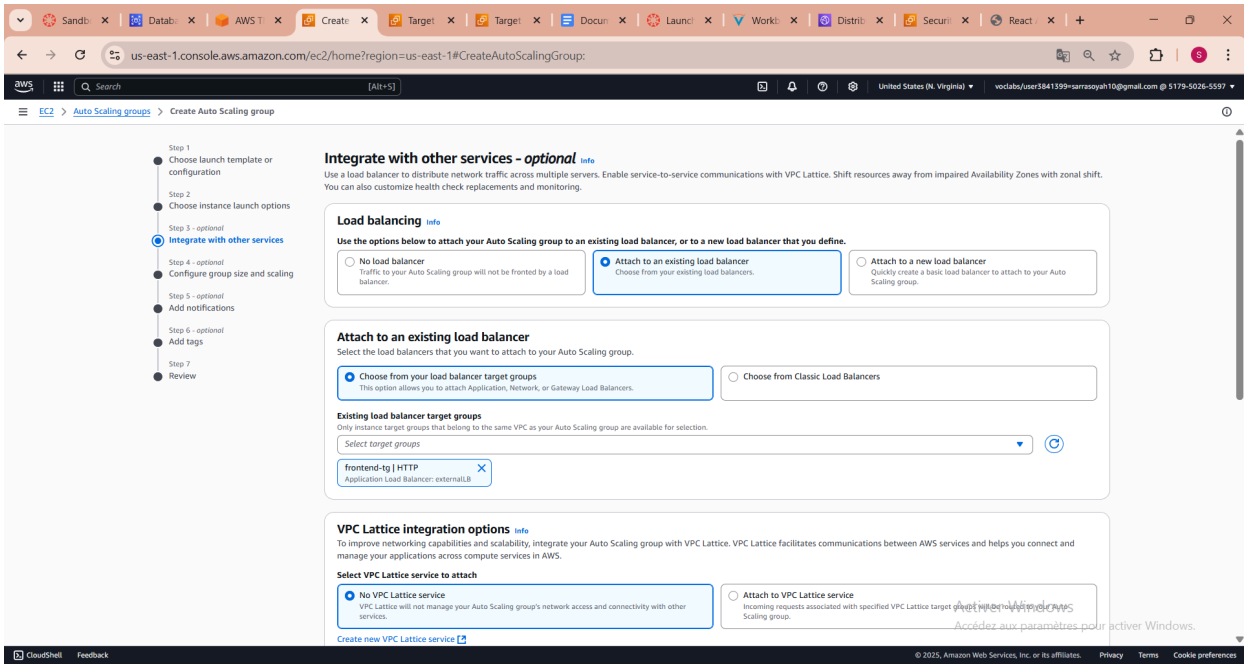


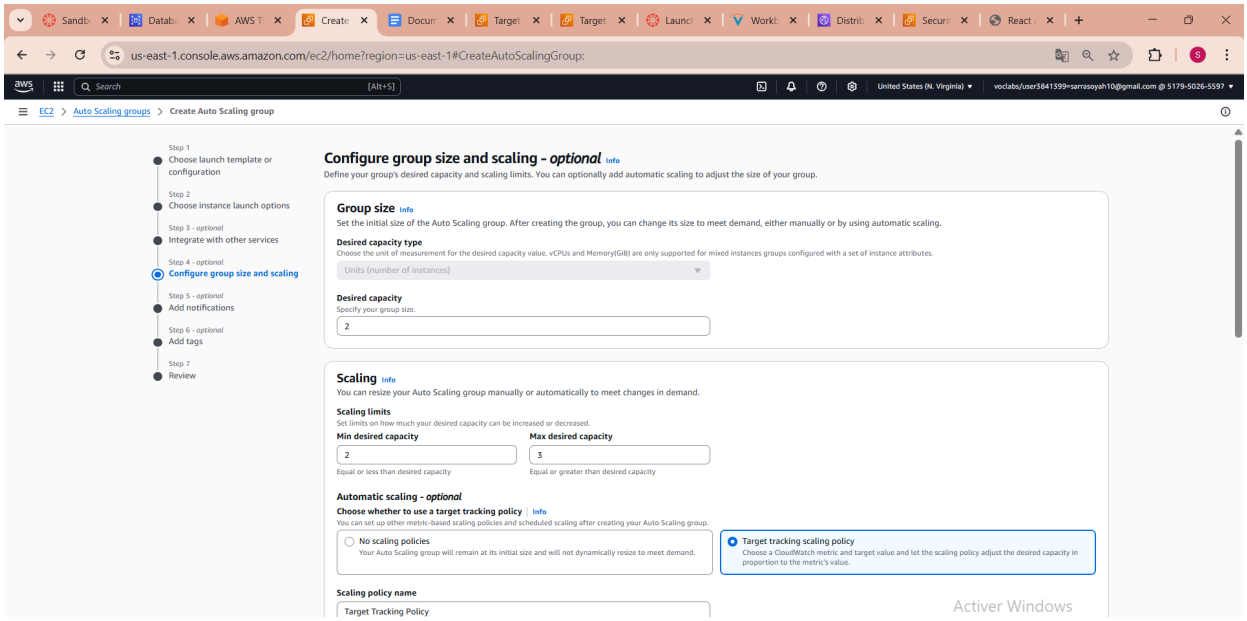

Launch template contents
Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.
Application and OS Images (Amazon Machine Image) - required Info
An AMI is a template that contains the software configuration (operating 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
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
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
64-bit (x86)
AMI ID
ami-0e58b56aa4d64231b
Publish Date
2025-05-10
Username
ec2-user
Verified provider
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AI
ami-0e58b56aa4d64231b
Virtual server type (instance
-
Firewall (security group)
-
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first ye
per month of t2.micro i
available) when used wi
IPv4 address usage, 30
snapshots, and 100 GB
Cancel
Instance type Info | Get advice
Advanced
Instance type
Don't include in launch template
All generations
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
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-FE sg-040634a1d74d93e9d
VPC: vpc-001e36c180e5b72c0
Compare security group rules
Amazon Li
ami-0e58b5
Virtual ser
-
Firewall (s
SG-FE
Storage (v
1 volume(s
Free
per
avai
IPv4
snap
Cancel

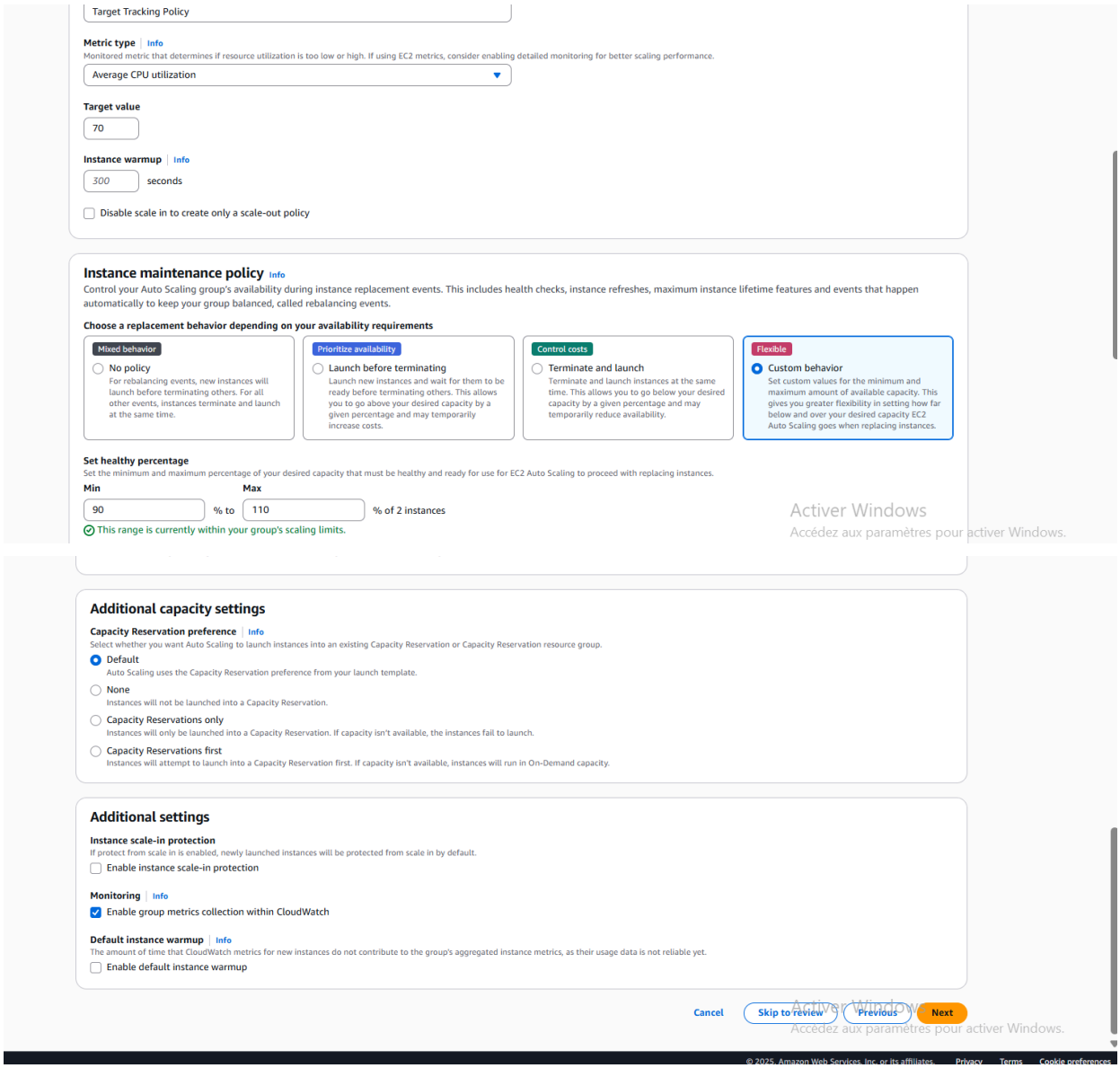



- **Configure auto scaling**

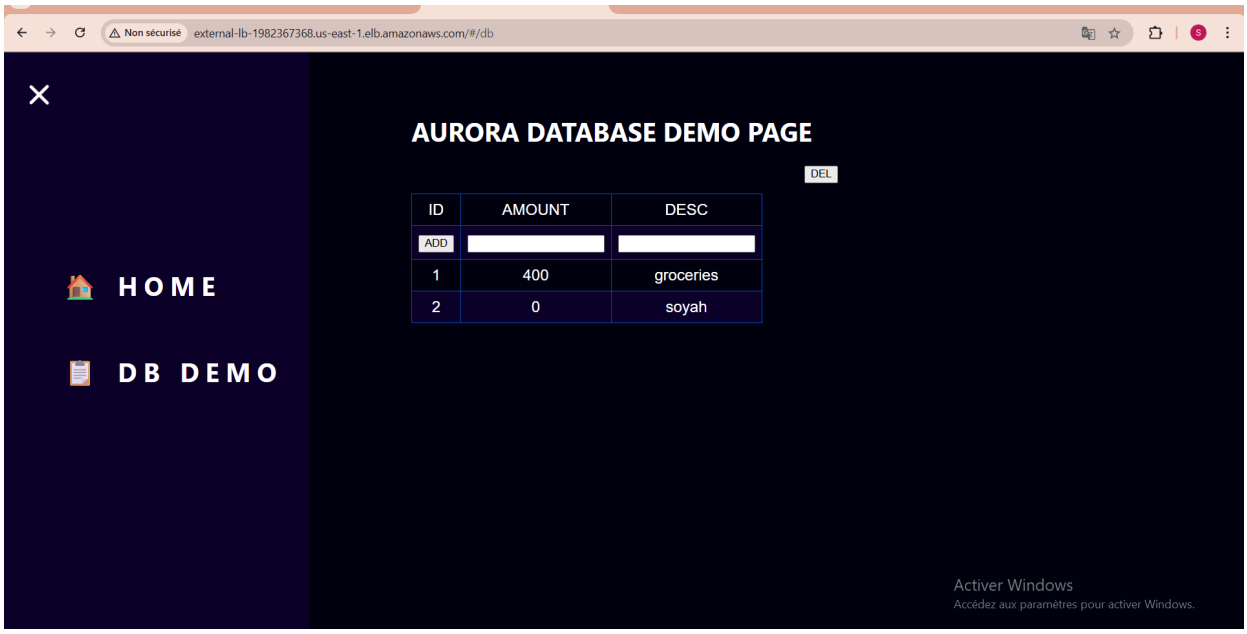



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateAutoScalingGroup:
EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template or configuration
Step 2
Choose instance launch options
Step 3 - optional
Integrate with other services
Step 4 - optional
Configure group size and scaling
Step 5 - optional
Add notifications
Step 6 - optional
Add tags
Step 7
Review
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
frontend-tg | HTTP
Application Load Balancer: externalLB
VPC Lattice integration options Info
To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.
Select VPC Lattice service to attach
No VPC Lattice service
VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.
Attach to VPC Lattice service
Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.
Create new VPC Lattice service
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateAutoScalingGroup:
EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template or configuration
Step 2
Choose instance launch options
Step 3 - optional
Integrate with other services
Step 4 - optional
Configure group size and scaling
Step 5 - optional
Add notifications
Step 6 - optional
Add tags
Step 7
Review
Configure group size and scaling - optional Info
Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.
Group size Info
Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.
Desired capacity type
Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.
Units (number of instances)
Desired capacity
Specify your group size.
2
Scaling Info
You can resize your Auto Scaling group manually or automatically to meet changes in demand.
Scaling limits
Set limits on how much your desired capacity can be increased or decreased.
Min desired capacity
2
Equal or less than desired capacity
Max desired capacity
3
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
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
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
90
% to
110
% of 2 instances
This range is currently within your group's scaling limits.
Activer 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
Activer Windows
Accédez aux paramètres pour activer Windows.
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

# Final App:




## 8. Monitoring and Logging

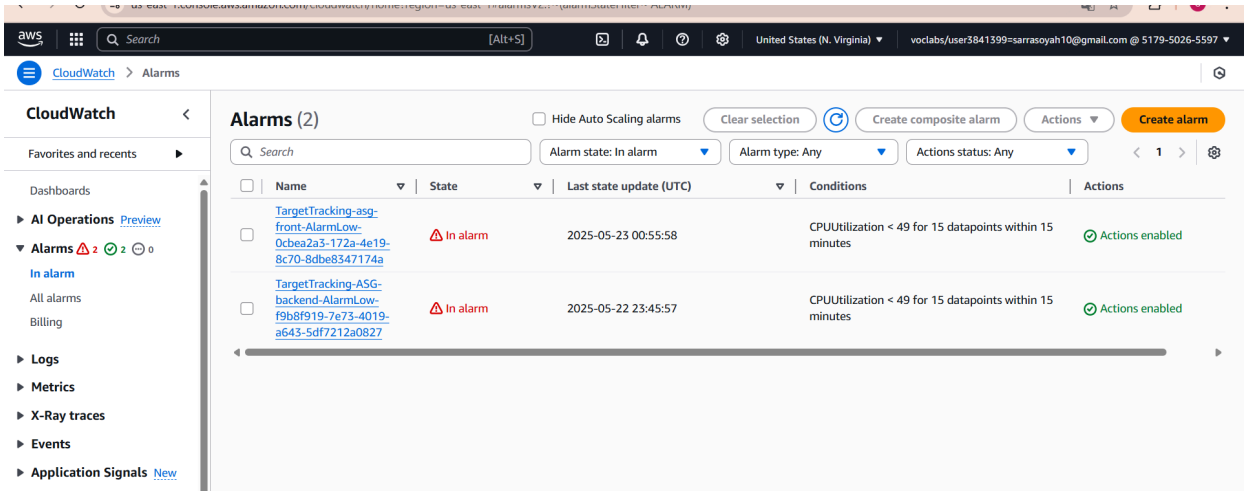
### 8.1 CloudWatch and CloudTrail

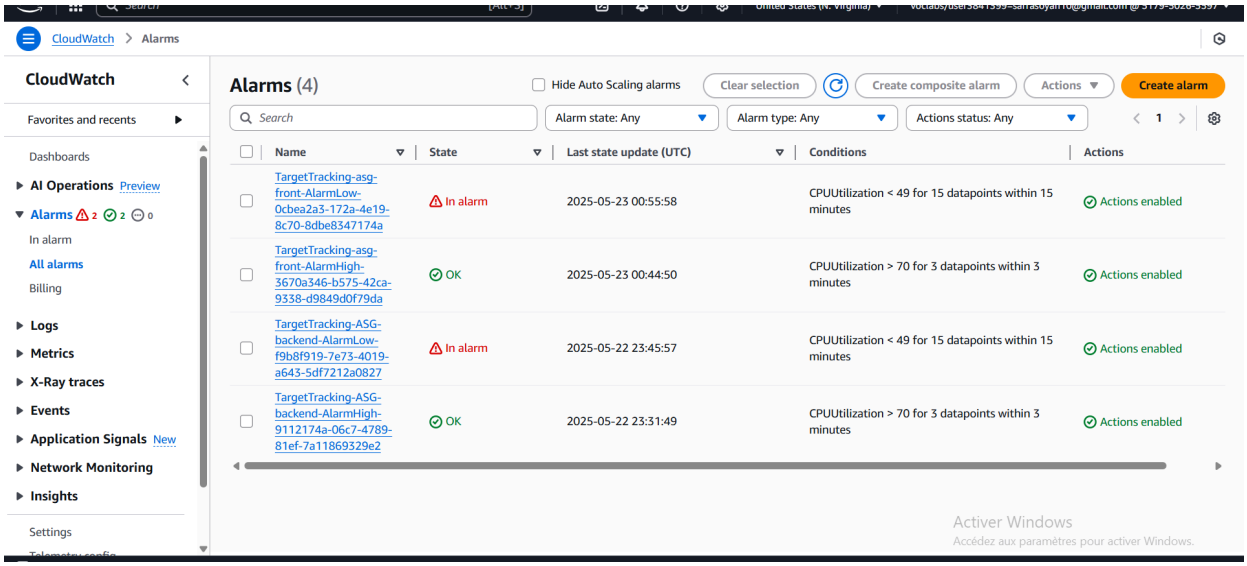
- **Enabled Amazon CloudWatch Logs for application and system logging**
- **Created CloudWatch Alarms:**
  - **Alert when CPU > 70%**
  - **Email notifications via SNS Topic and Subscription**
- **Enabled AWS CloudTrail to log all API activities, access attempts, and resource changes**

### 8.2 RDS Backups and Snapshots

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

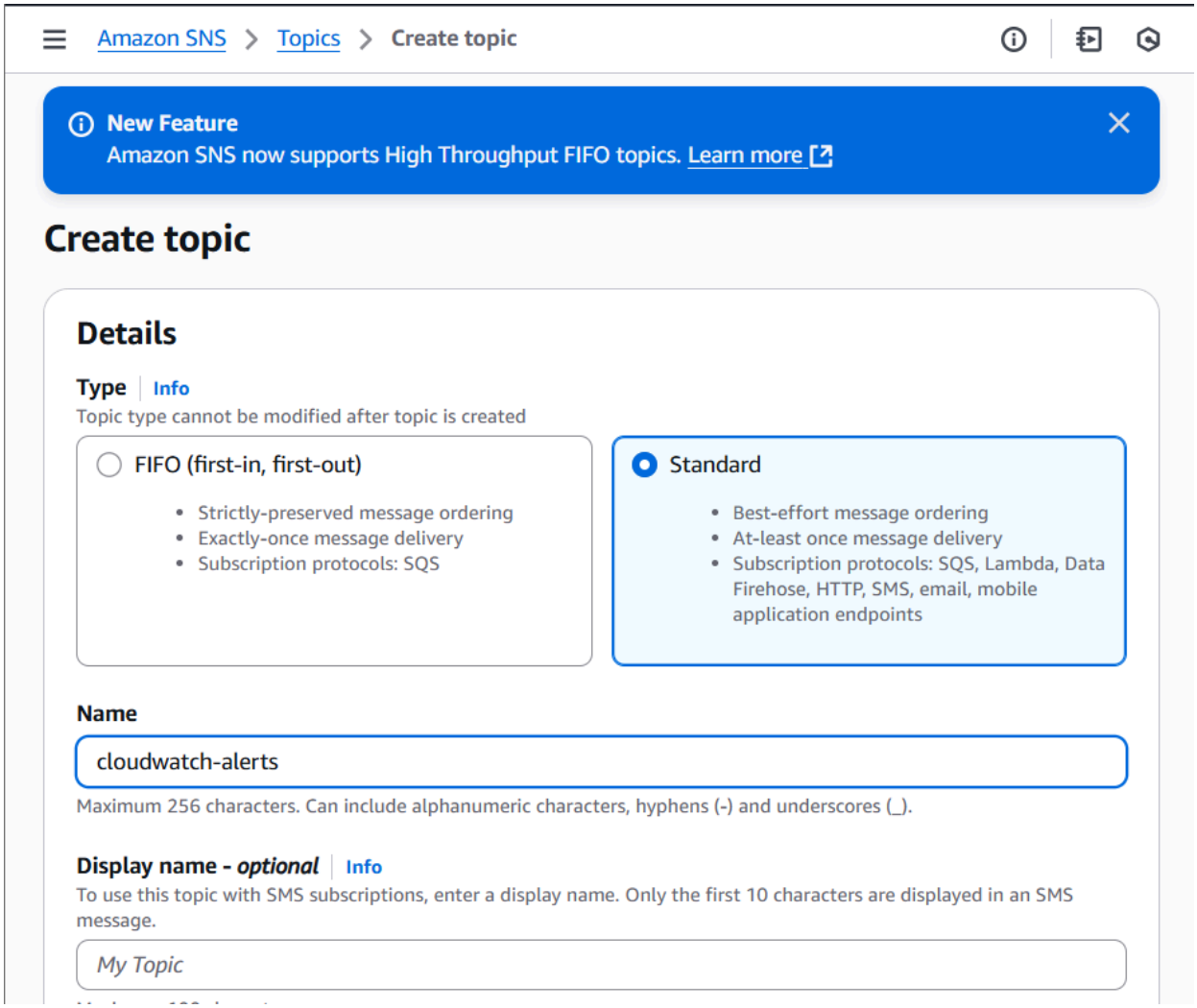
- **Backups can be restored to a point-in-time**



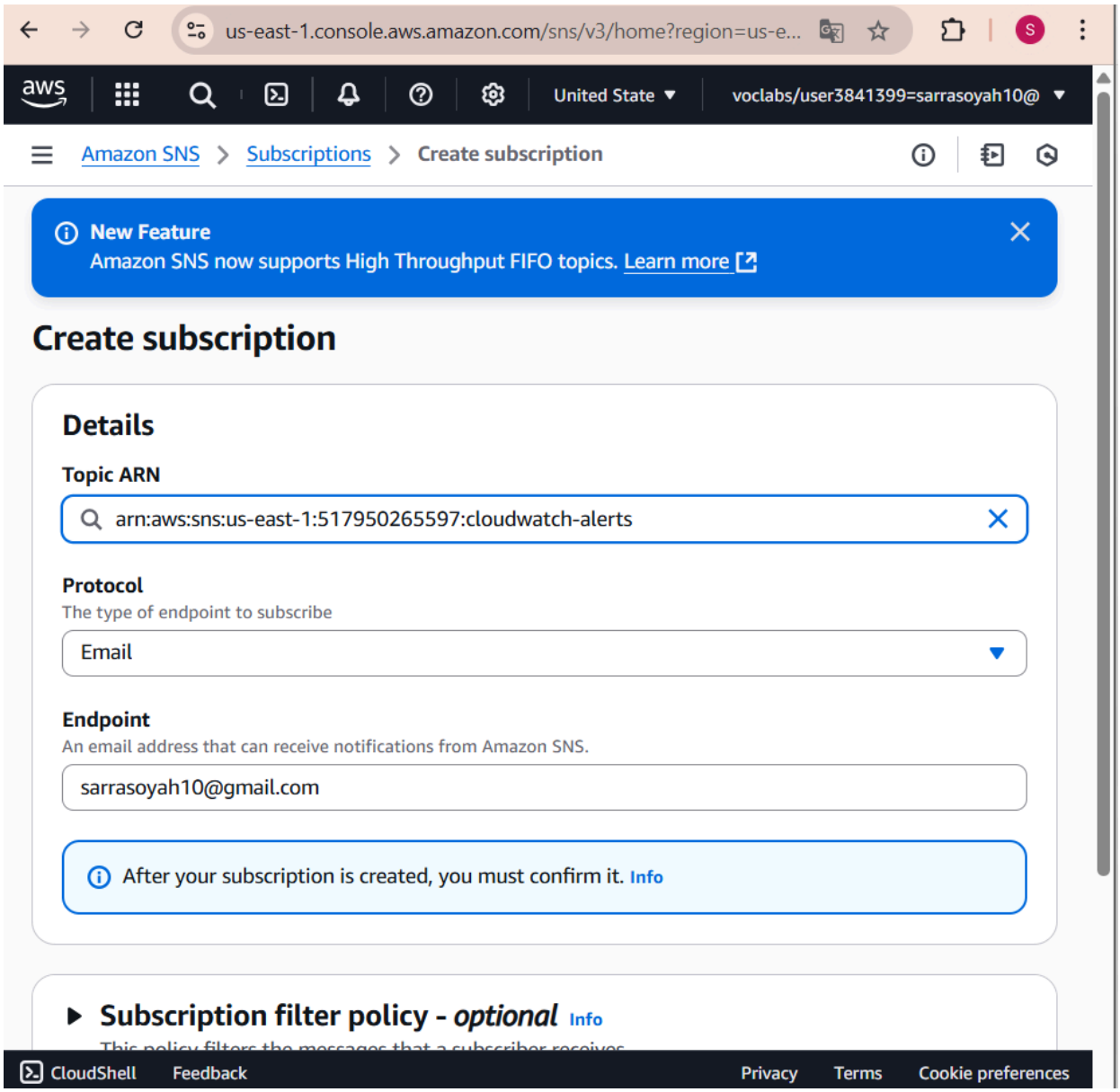




## Send notifications via Amazon SNS to a specified email address

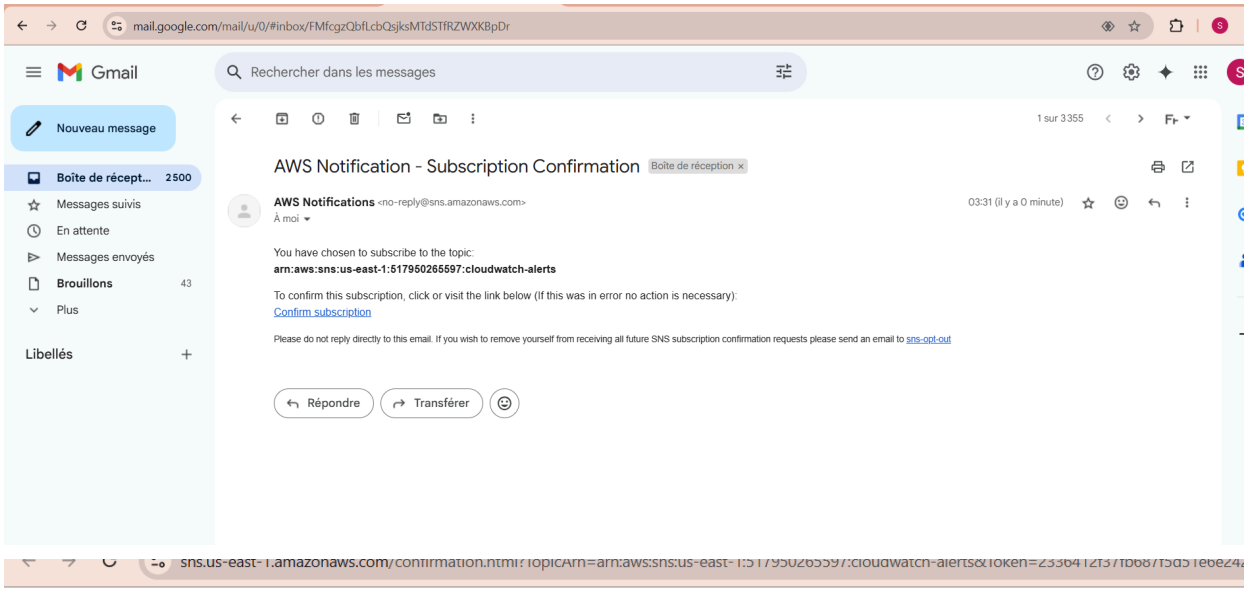
- **Topic Creation**



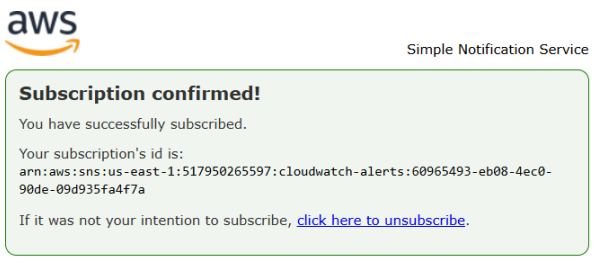

- **Subscription Creation**


us-east-1.console.aws.amazon.com/sns/v3/home?region=us-e...
United State
voclabs/user3841399=sarrasoyah10@
Amazon SNS
Subscriptions
Create subscription
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
Create subscription
Details
Topic ARN
arn:aws:sns:us-east-1:517950265597:cloudwatch-alerts
Protocol
The type of endpoint to subscribe
Email
Endpoint
An email address that can receive notifications from Amazon SNS.
sarrasoyah10@gmail.com
After your subscription is created, you must confirm it. Info
Subscription filter policy - optional Info
CloudShell
Feedback
Privacy
Terms
Cookie preferences

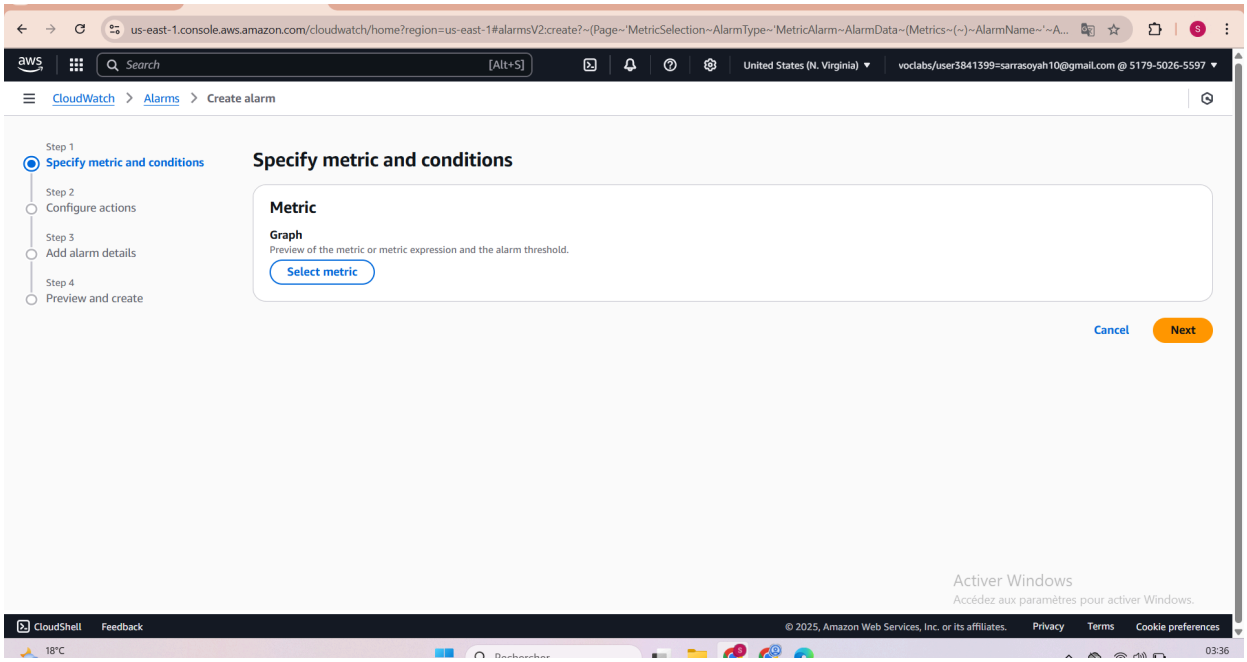
- **Output**

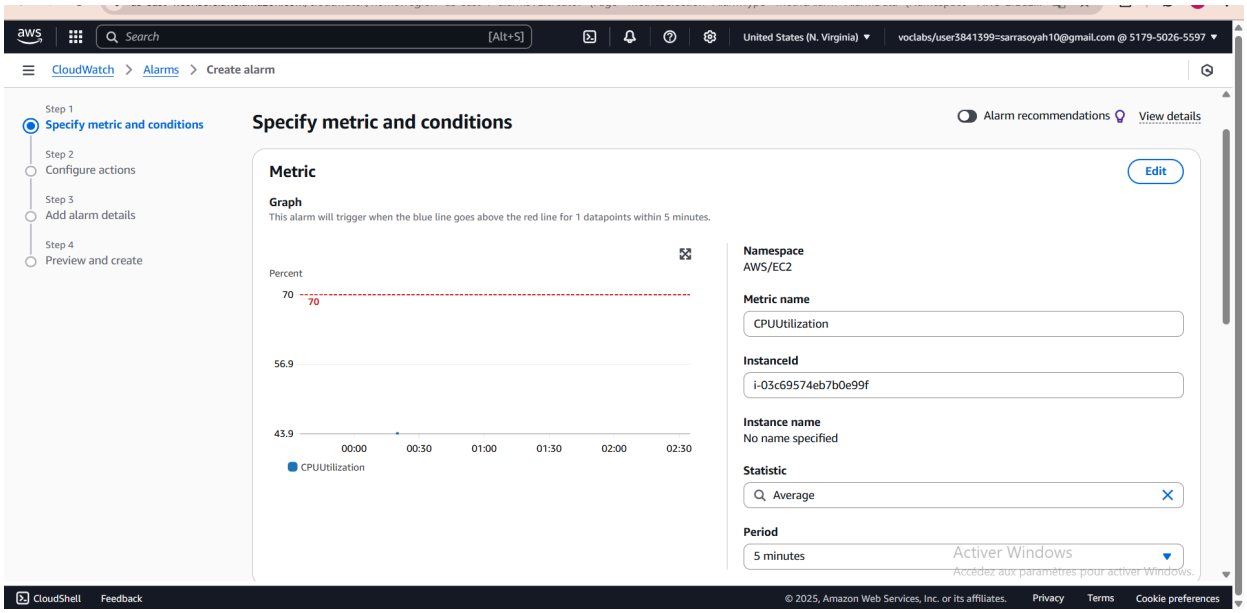


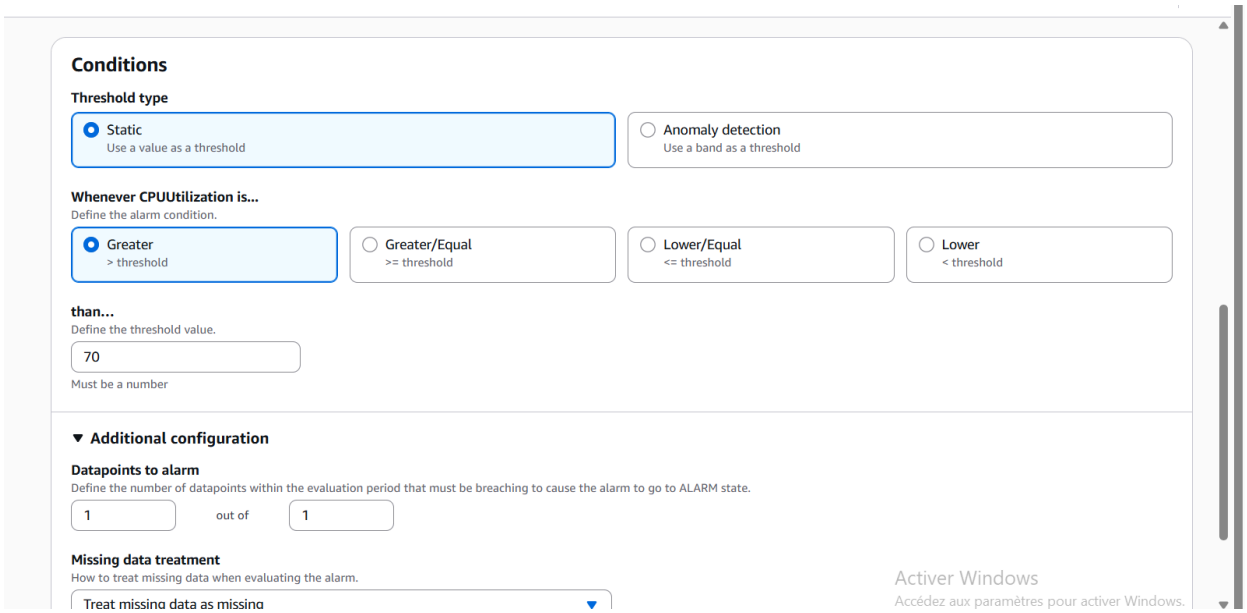


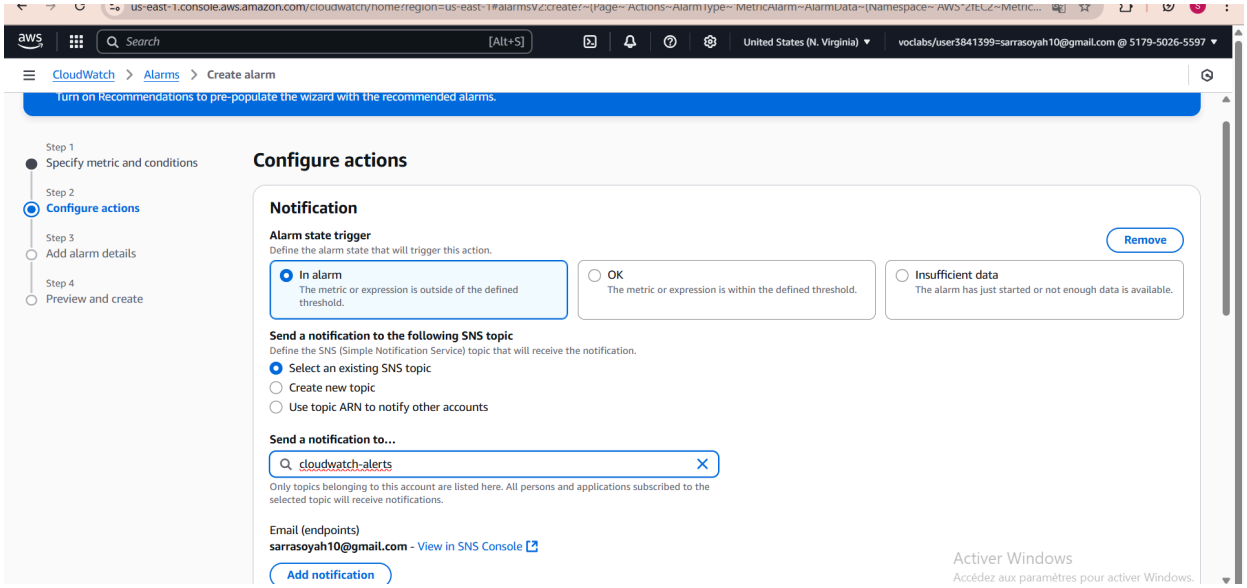



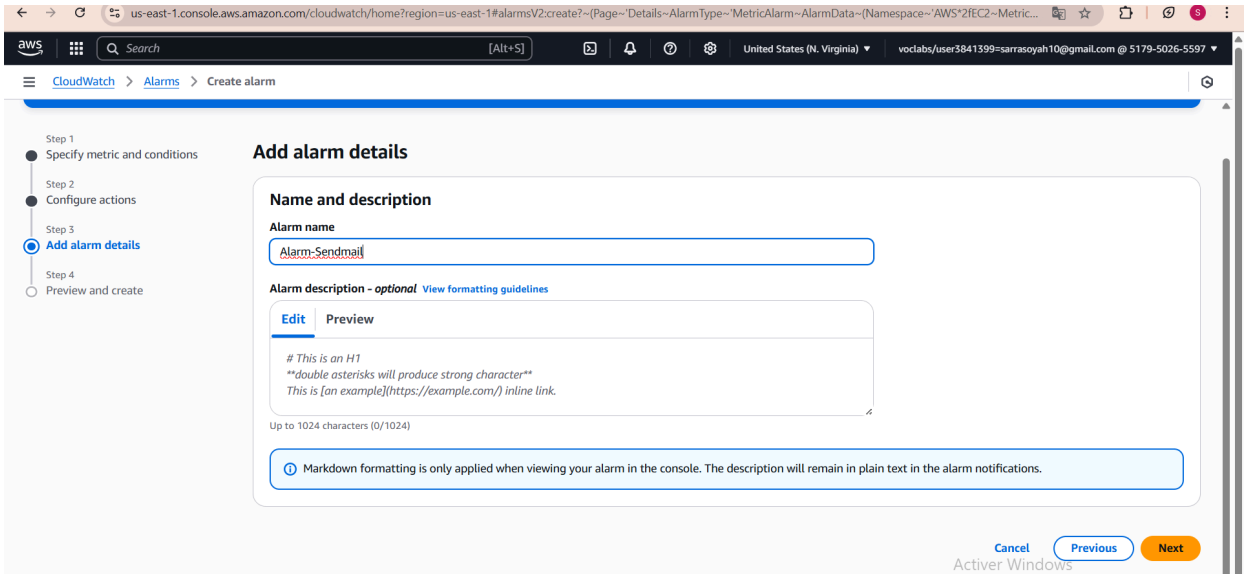

- **Alarm Creation**


us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'MetricSelection~AlarmType~'MetricAlarm~AlarmData~(Metrics~(~)~AlarmName~'~A...
Search
[Alt+S]
United States (N. Virginia)
voclabs/user3841399=sarrasoyah10@gmail.com @ 5179-5026-5597
CloudWatch
Alarms
Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add alarm details
Step 4
Preview and create
Specify metric and conditions
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
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
18°C
03:36

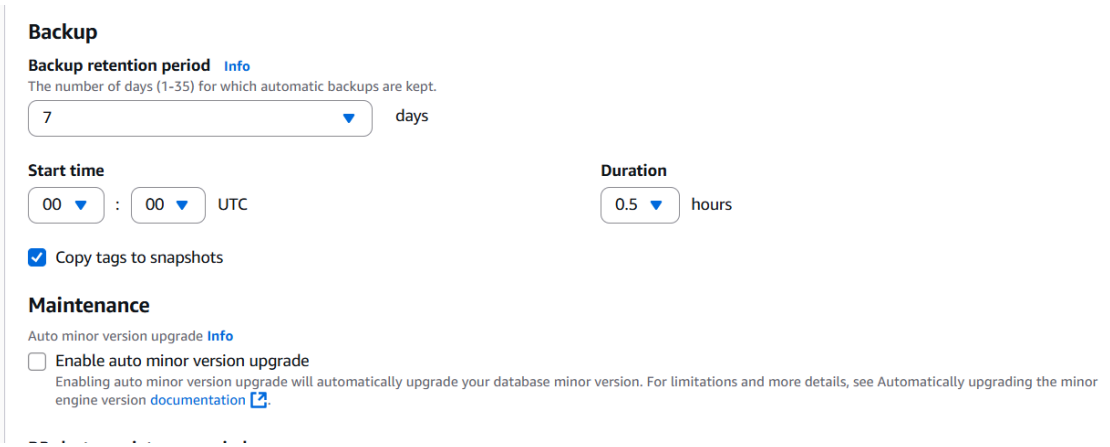

Search
[Alt+S]
United States (N. Virginia)
voclabs/user3841399=sarrasoyah10@gmail.com @ 5179-5026-5597
CloudWatch
Alarms
Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add alarm details
Step 4
Preview and create
Specify metric and conditions
Alarm recommendations
View details
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.
Percent
70
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.

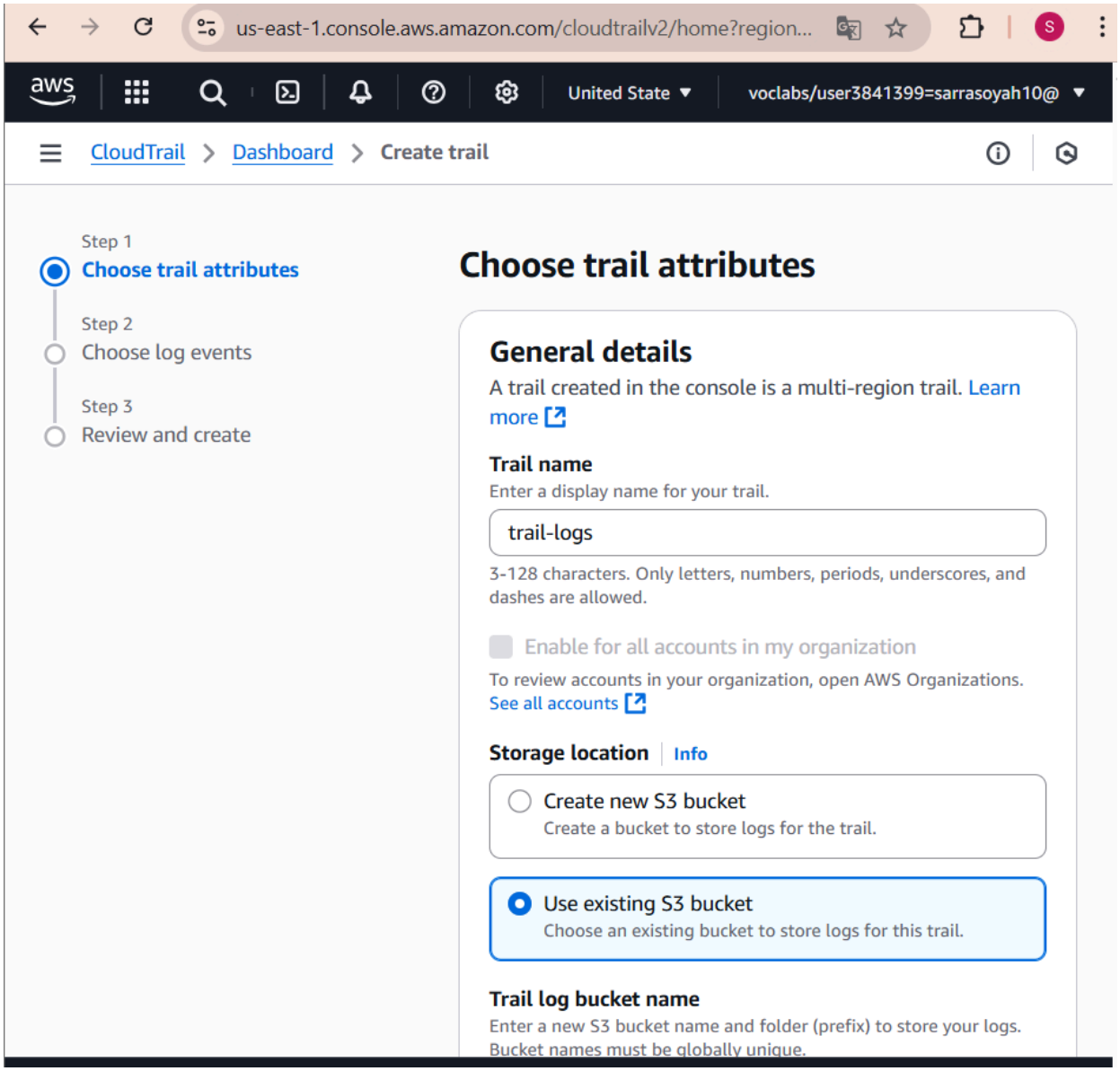

Search
[Alt+S]
United States (N. Virginia)
CloudWatch
Alarms
Create alarm
Turn on Recommendations to pre-populate the wizard with the recommended alarms.
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add alarm details
Step 4
Preview and create
Configure actions
Notification
Alarm state trigger
Define the alarm state that will trigger this action.
Remove
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.

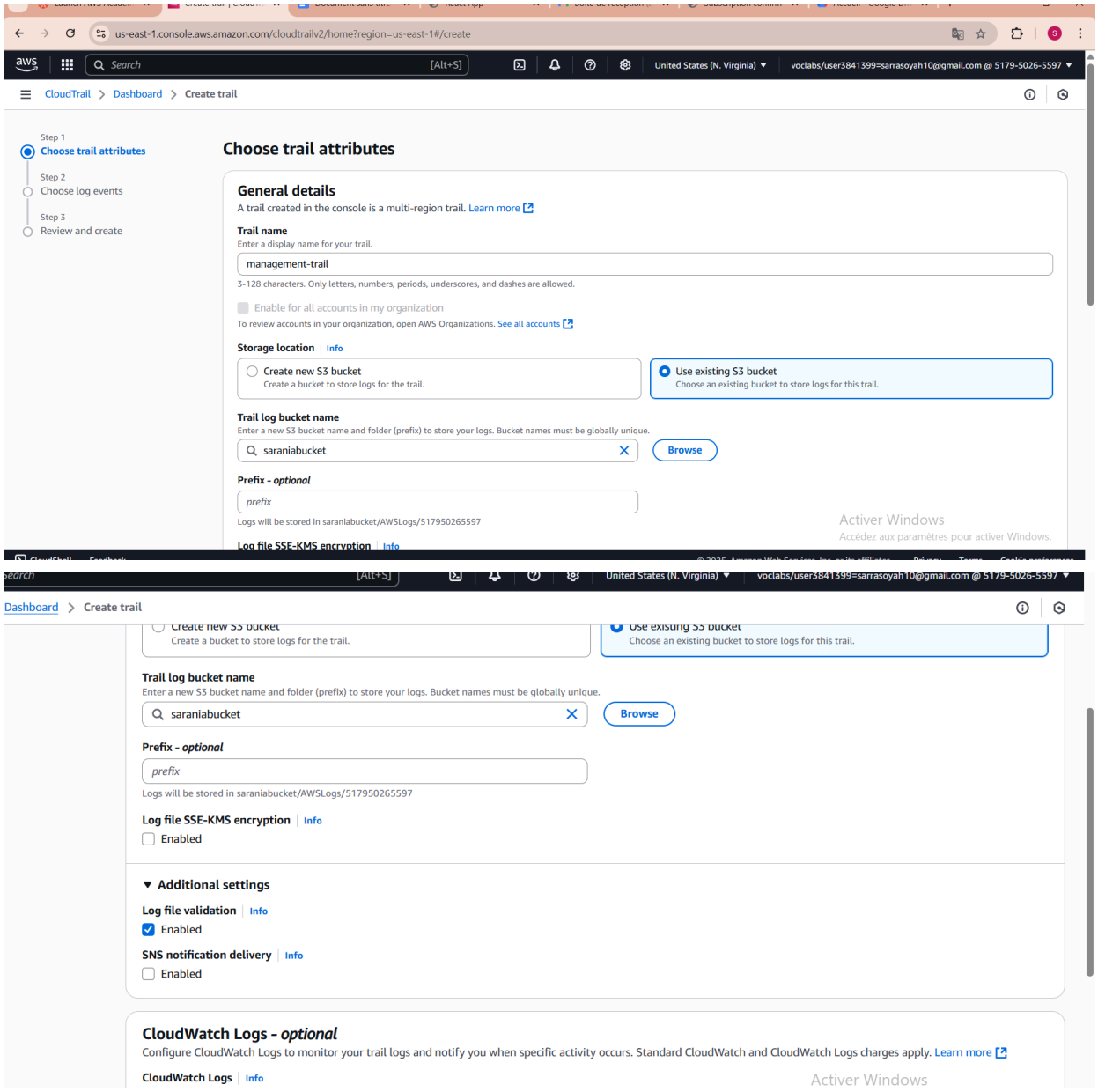


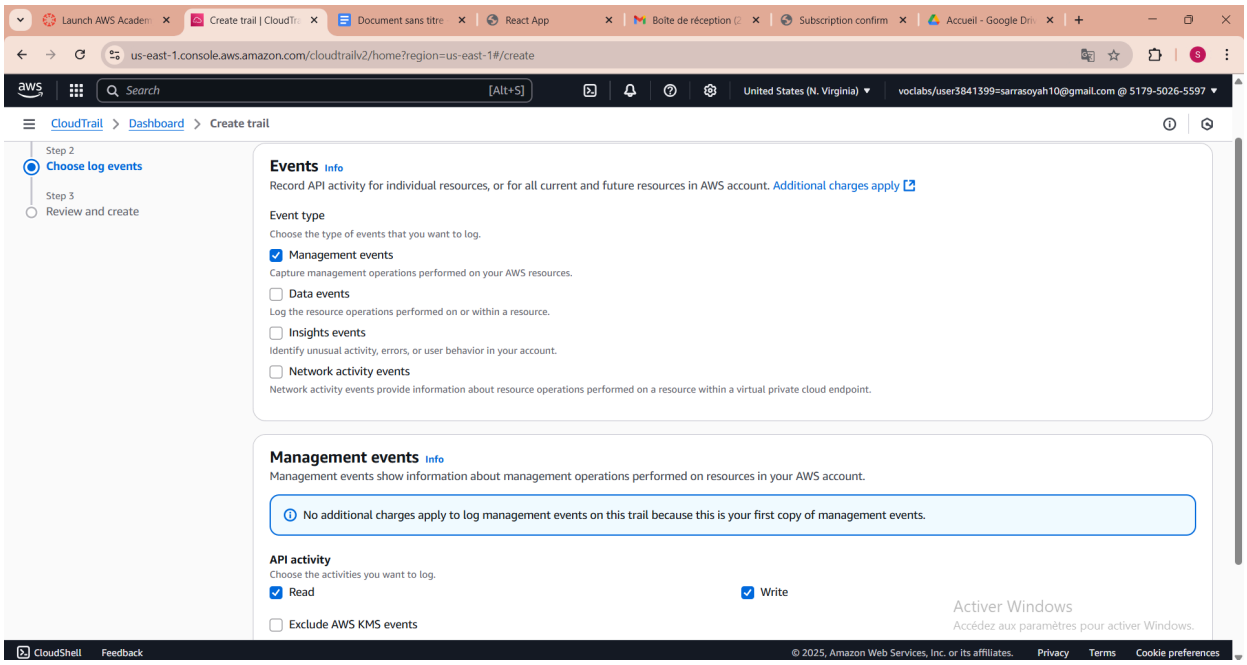

- **Enable backup in RDS :**

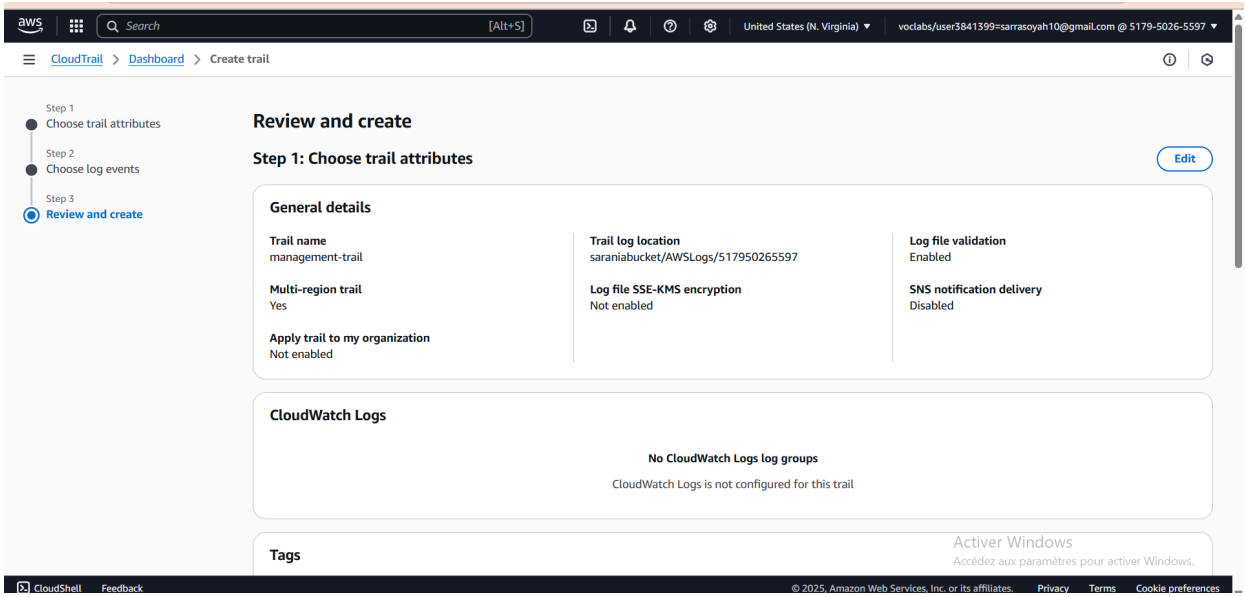


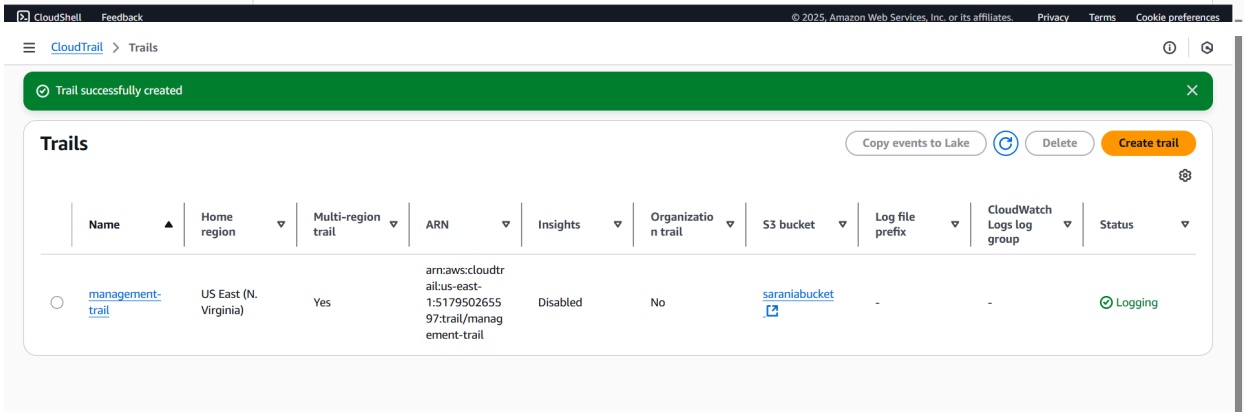

- **Cloudtrail creation:**

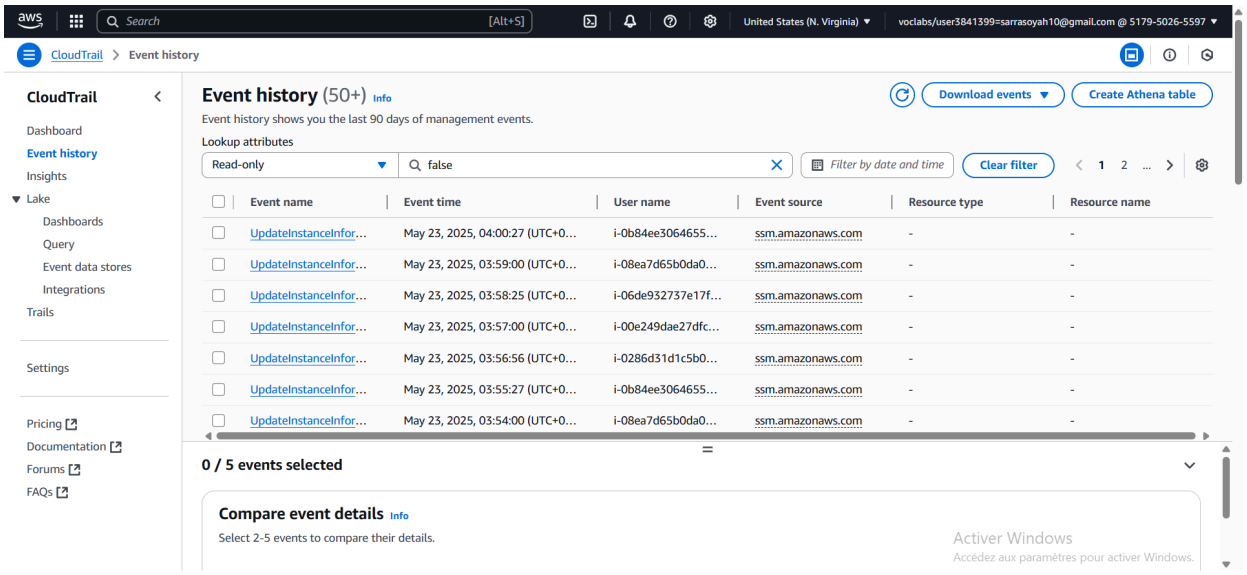

us-east-1.console.aws.amazon.com/cloudtrailv2/home?region...
United State
voclabs/user3841399=sarrasoyah10@
CloudTrail
Dashboard
Create trail
Step 1
Choose trail attributes
Step 2
Choose log events
Step 3
Review and create
Choose trail attributes
General details
A trail created in the console is a multi-region trail. Learn more
Trail name
Enter a display name for your trail.
trail-logs
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
Search
[Alt+S]
United States (N. Virginia)
voclabs/user3841399=sarrasoyah10@gmail.com @ 5179-5026-5597
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.
management-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.
saraniabucket
Browse
Prefix - optional
prefix
Logs will be stored in saraniabucket/AWSLogs/517950265597
Log file SSE-KMS encryption Info
Activer Windows
Accédez aux paramètres pour activer Windows.
Dashboard
Create trail
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.
saraniabucket
Browse
Prefix - optional
prefix
Logs will be stored in saraniabucket/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


Launch AWS Academ
Create trail | CloudTra
Document sans titre
React App
Boîte de réception (2
Subscription confirm
Accueil - Google Driv
us-east-1.console.aws.amazon.com/cloudtrailv2/home?region=us-east-1#/create
aws
Search
[Alt+S]
United States (N. Virginia)
voclabs/user3841399=sarrasoyah10@gmail.com @ 5179-5026-5597
CloudTrail > Dashboard > Create trail
Step 2
Choose log events
Step 3
Review and create
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.
No additional charges apply to log management events on this trail because this is your first copy of management events.
API activity
Choose the activities you want to log.
Read
Write
Exclude AWS KMS events
Activer Windows
Accédez aux paramètres pour activer Windows.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Search
[Alt+S]
United States (N. Virginia)
voclabs/user3841399=sarrasoyah10@gmail.com @ 5179-5026-5597
CloudTrail > Dashboard > Create trail
Step 1
Choose trail attributes
Step 2
Choose log events
Step 3
Review and create
Review and create
Step 1: Choose trail attributes
Edit
General details
Trail name
management-trail
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Trail log location
saraniabucket/AWSLogs/517950265597
Log file SSE-KMS encryption
Not enabled
Log file validation
Enabled
SNS notification delivery
Disabled
CloudWatch Logs
No CloudWatch Logs log groups
CloudWatch Logs is not configured for this trail
Tags
Activer Windows
Accédez aux paramètres pour activer Windows.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudTrail > Trails
Trail successfully created
Trails
Copy events to Lake
Delete
Create trail
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




## 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.**