جامعة محمد الخامس بالرباط
Université Mohamed V de Rabat

ENSIAS

Cloud Project

By:
GUIGUI SALMA
MESKINI YASSIR
ELKAMEL ISMAIL

Overview

- Introduction 01
- Cloud architecture 02
- Security measures 03
- Implementation 04
- Conclusion 05

Introduction

Cloud Provider

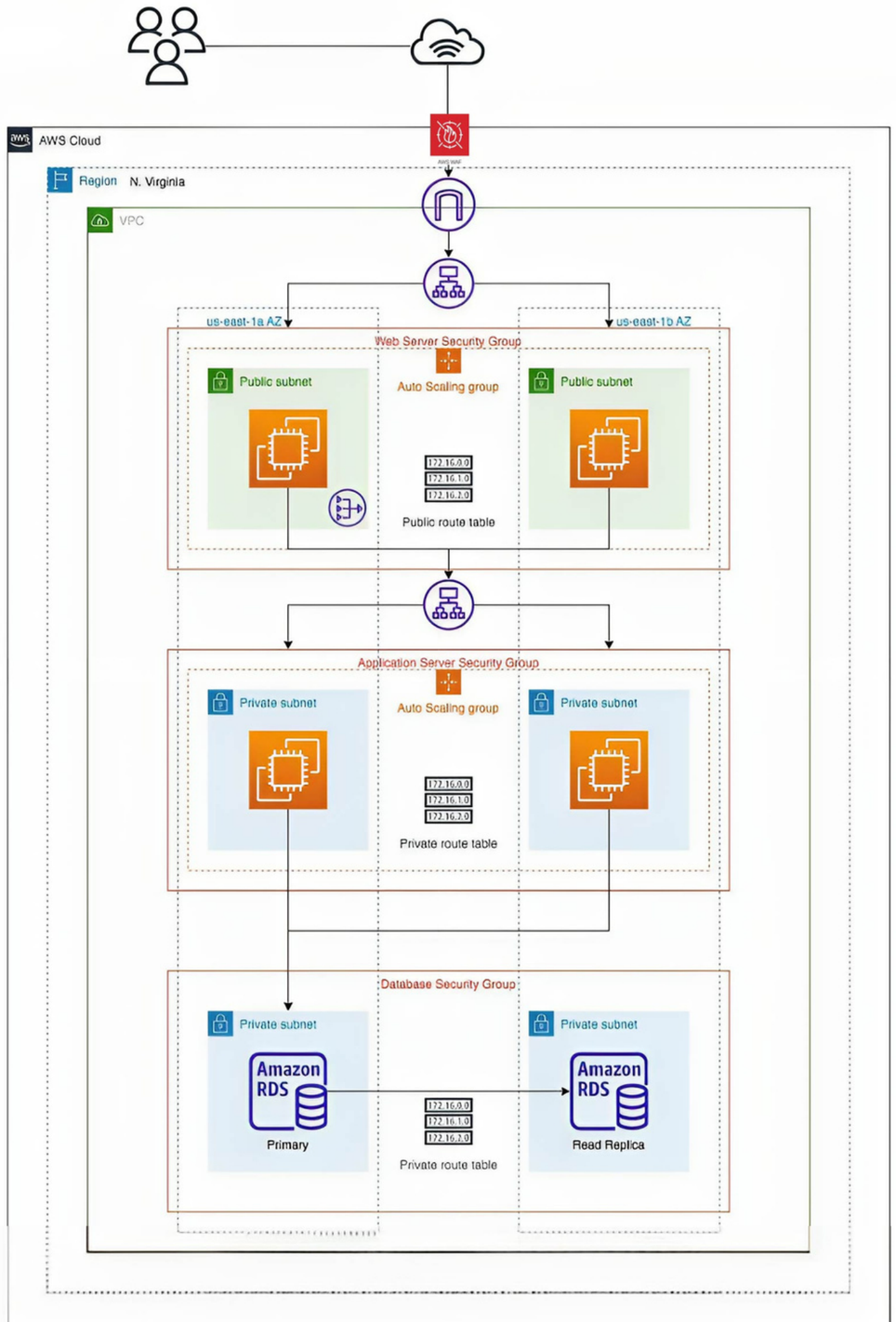
Three-Tier Architecture

WEB Tier

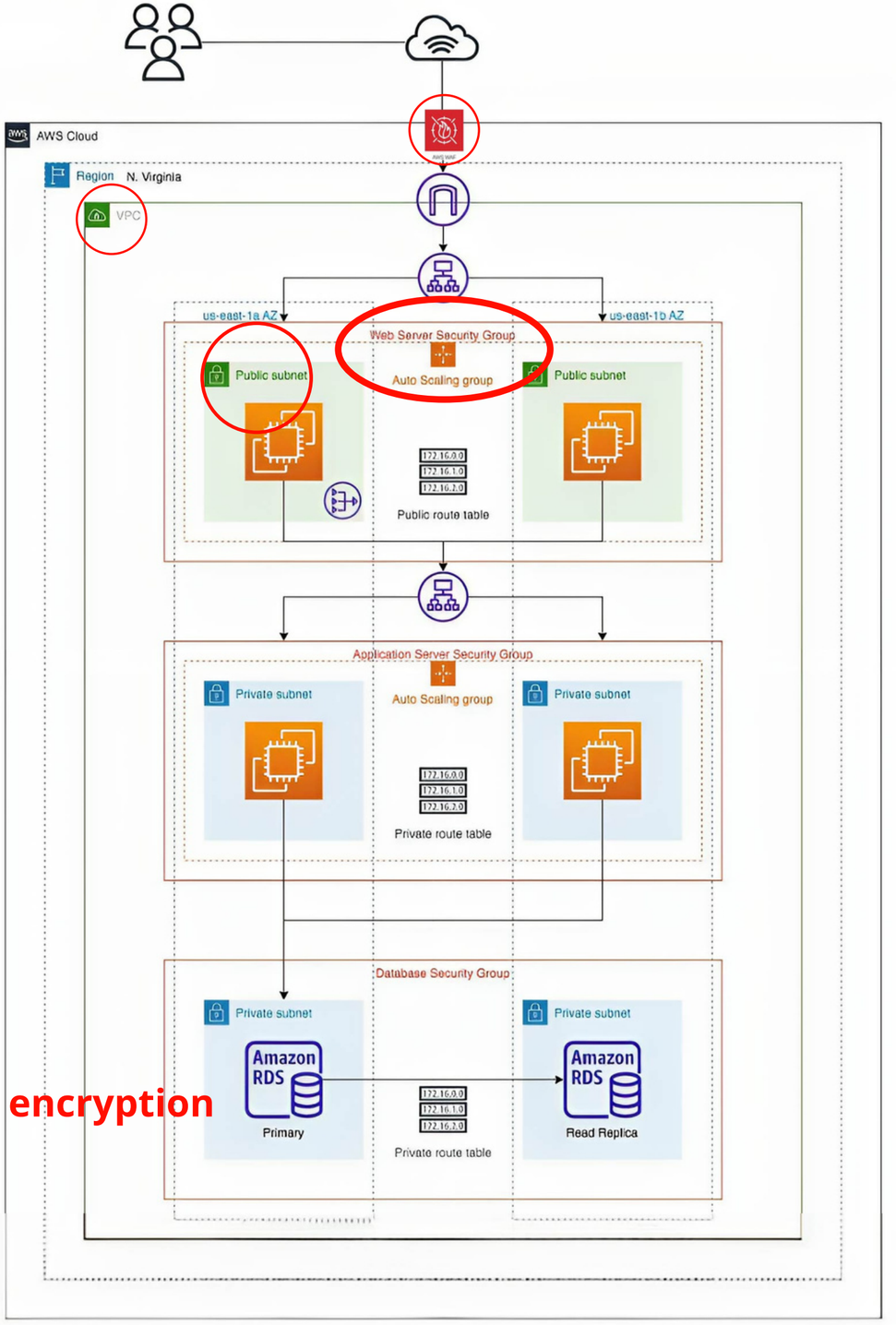
Application Tier

Database Tier

AWS Cloud Architecture



Security

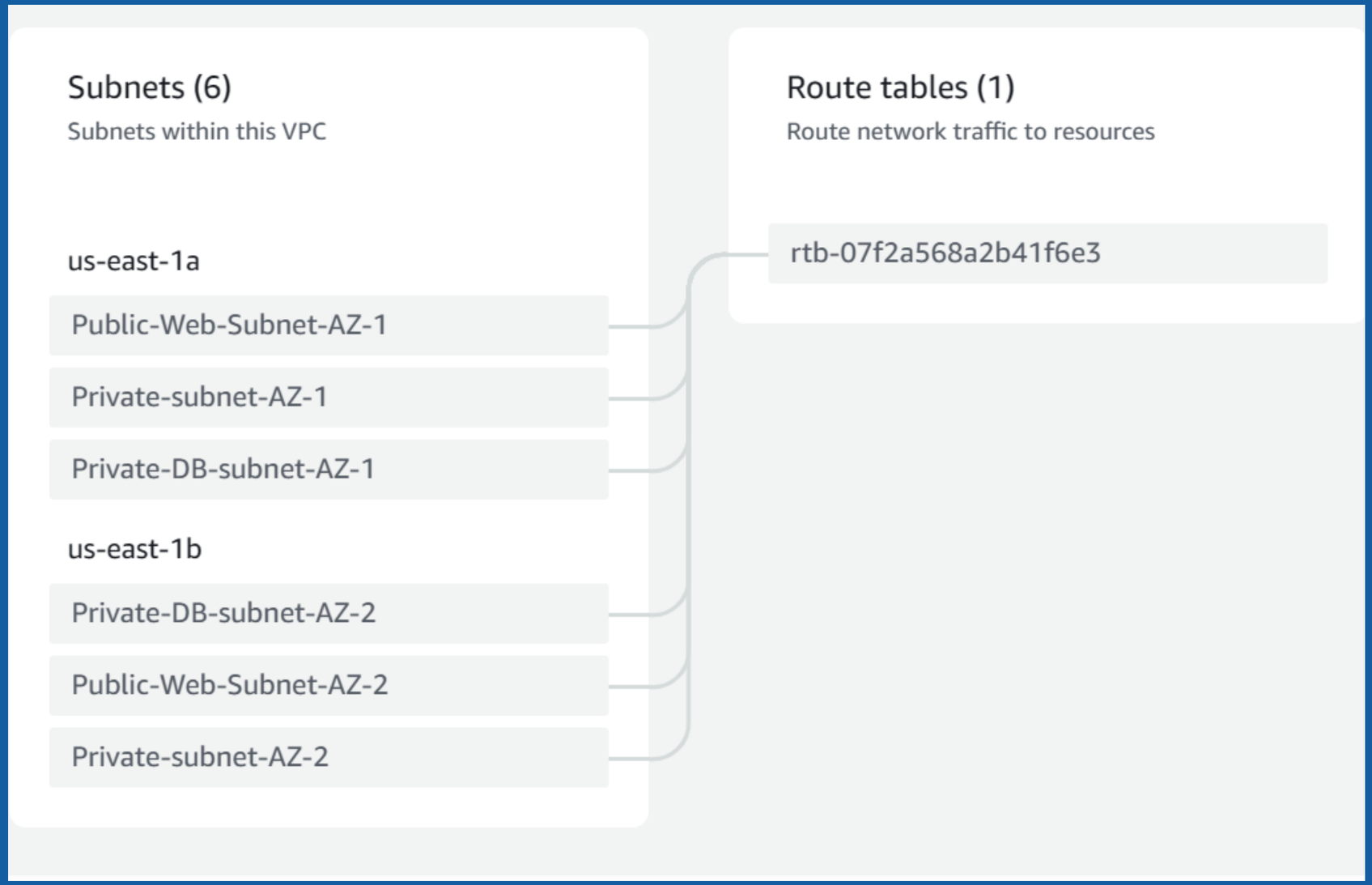

AWS Cloud
Region N. Virginia
VPC
us-east-1a AZ
us-east-1b AZ
Web Server Security Group
Public subnet
Auto Scaling group
Public subnet
Public route table
Application Server Security Group
Private subnet
Auto Scaling group
Private subnet
Private route table
Database Security Group
Private subnet
Amazon RDS
Primary
Private subnet
Amazon RDS
Read Replica
Private route table
encryption

INFORMATION ASSET	ASSET OWNER	RISK DETAILS	RISK CATEGORY
Student Data	Registrar's Office	Unauthorized access, Data breaches	Security, Privacy
System Availability	IT Department	DoS attacks	Availability
Operational Integrity	System Administrators	Insider threats	Security
Data Integrity	Database Admins	Data loss due to disasters	Integrity

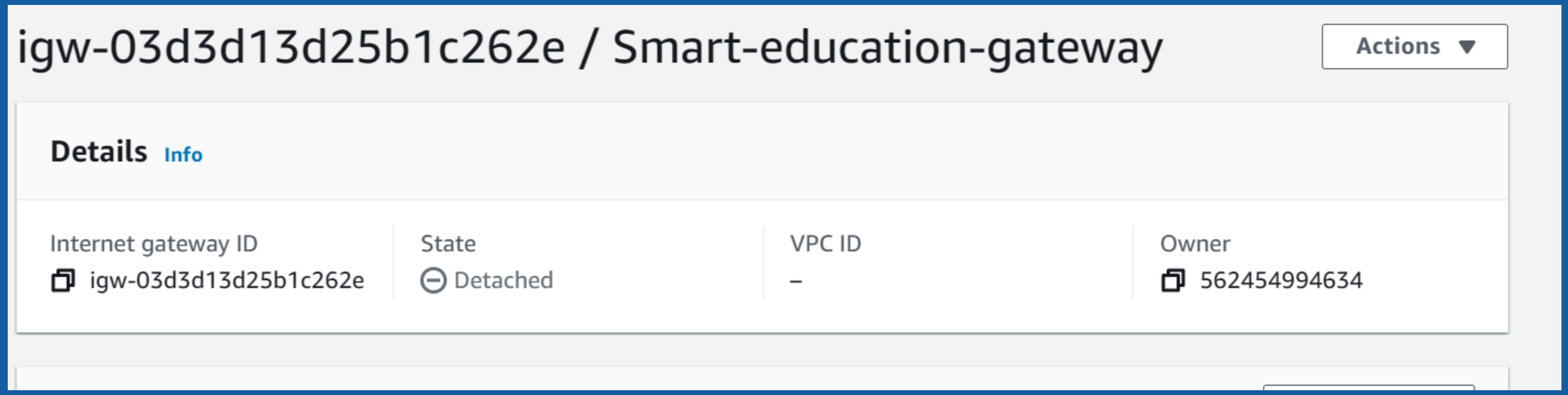
PROBABILITY RATING	IMPACT RATING	RISK TREATMENT	REMEDIATION TIMELINE	RISK OWNER
Medium	High	Encryption, Access Controls	1-3 Months	Data Protection Officer
Low-Medium	High	AWS Shield, Load Balancing	Ongoing	IT Security Manager
Medium	Medium	Least Privilege, Audit Trails	Ongoing	Chief Security Officer
Low	High	Regular Backups, Multi-AZ RDS	Ongoing	Database Manager

Implementation

Networking and Security


Subnets (6)
Subnets within this VPC
us-east-1a
Public-Web-Subnet-AZ-1
Private-subnet-AZ-1
Private-DB-subnet-AZ-1
us-east-1b
Private-DB-subnet-AZ-2
Public-Web-Subnet-AZ-2
Private-subnet-AZ-2
Route tables (1)
Route network traffic to resources
rtb-07f2a568a2b41f6e3

Name	Route table ID	Explicit subnet associati...
–	rtb-07f2a568a2b41f6e3	–
PrivateRouteTable-AZ1	rtb-092dd55ce32b170df	subnet-0dd54c94647e33...
Public-Route-Table	rtb-05a916f4cf759bf7b	2 subnets
–	rtb-034ca87242d35f035	–


igw-03d3d13d25b1c262e / Smart-education-gateway
Actions
Details Info
Internet gateway ID
igw-03d3d13d25b1c262e
State
Detached
VPC ID
–
Owner
562454994634

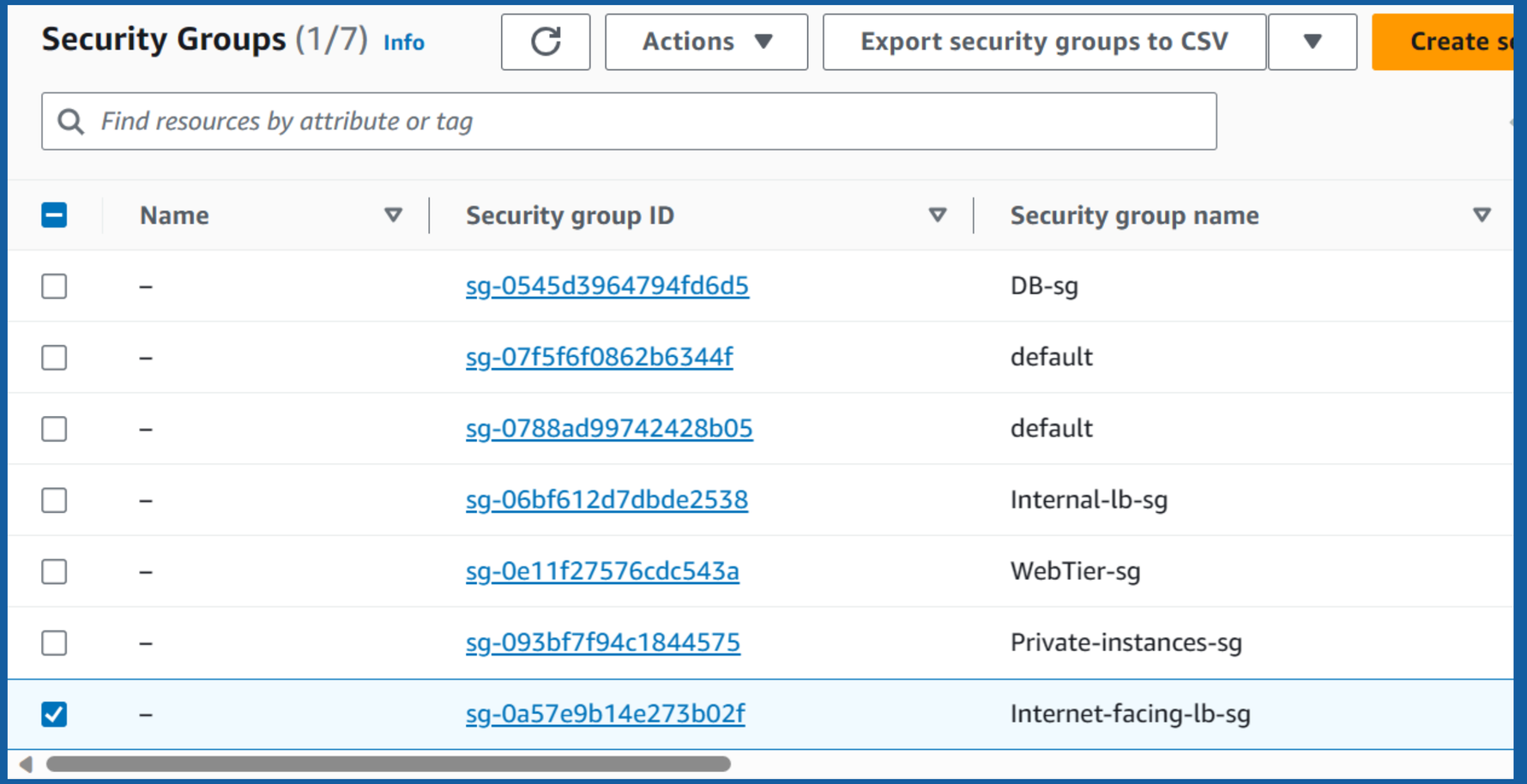
igw-03d3d13d25b1c262e / Smart-education-gateway

Actions

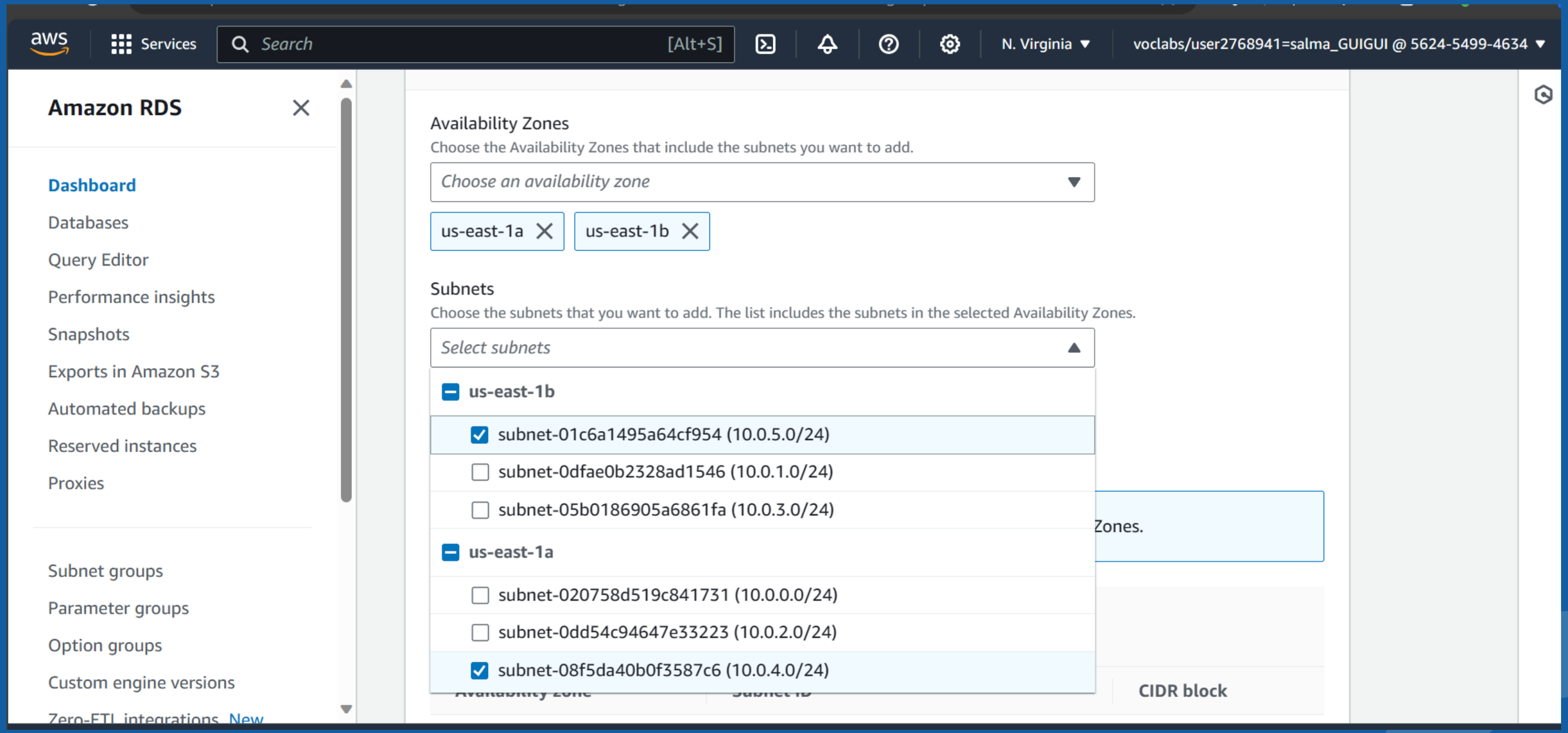
Details Info

Internet gateway ID	State	VPC ID	Owner
igw-03d3d13d25b1c262e	Attached	vpc-026dd6675978a80cb | smart-education-vpc	562454994634

	Name	NAT gateway ID	Connectivit...	State	State message
○	NAT-GW-AZ1	nat-0e9d8cd89f877f2b2	Public	Available	–
○	NAT-GW-AZ2	nat-0a8e864c20df137e6	Public	Available	–


Security Groups (1/7) Info
Actions
Export security groups to CSV
Create s
Find resources by attribute or tag
Name
Security group ID
Security group name
– sg-0545d3964794fd6d5 DB-sg
– sg-07f5f6f0862b6344f default
– sg-0788ad99742428b05 default
– sg-06bf612d7dbde2538 Internal-lb-sg
– sg-0e11f27576cdc543a WebTier-sg
– sg-093bf7f94c1844575 Private-instances-sg
– sg-0a57e9b14e273b02f Internet-facing-lb-sg

Creation de notre DB


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2768941=salma_GUIGUI @ 5624-5499-4634
Amazon RDS
Dashboard
Databases
Query Editor
Performance insights
Snapshots
Exports in Amazon S3
Automated backups
Reserved instances
Proxies
Subnet groups
Parameter groups
Option groups
Custom engine versions
Zero-ETL integrations New
Availability Zones
Choose the Availability Zones that include the subnets you want to add.
Choose an availability zone
us-east-1a
us-east-1b
Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.
Select subnets
us-east-1b
subnet-01c6a1495a64cf954 (10.0.5.0/24)
subnet-0dfae0b2328ad1546 (10.0.1.0/24)
subnet-05b0186905a6861fa (10.0.3.0/24)
us-east-1a
subnet-020758d519c841731 (10.0.0.0/24)
subnet-0dd54c94647e33223 (10.0.2.0/24)
subnet-08f5da40b0f3587c6 (10.0.4.0/24)
Zones.
CIDR block

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

Backup

Backup retention period **Info**

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

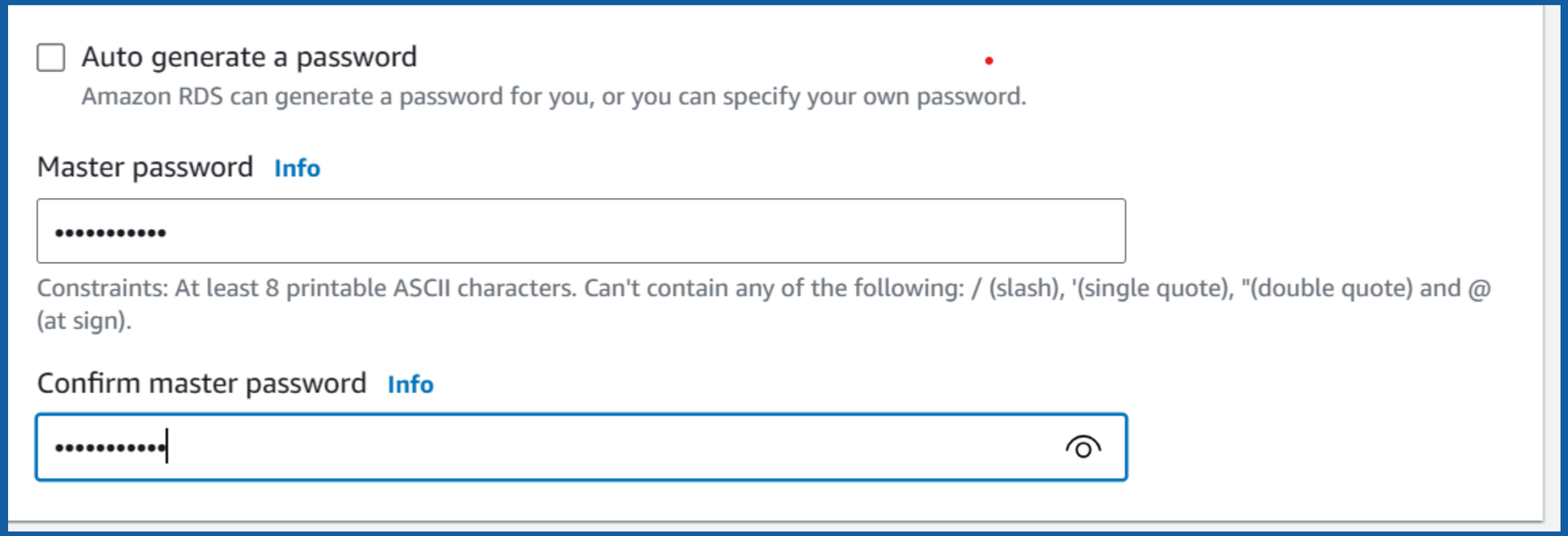
1 day

☑ 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**


Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password.
Master password Info
••••••••••••
Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).
Confirm master password Info
••••••••••••

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.

Network type Info

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

- (•) **IPv4**
  Your resources can communicate only over the IPv4 addressing protocol.
- ( ) **Dual-stack mode**
  Your resources can communicate over IPv4, IPv6, or both.

Virtual private cloud (VPC) Info

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

smart-education-vpc (vpc-026dd6675978a80cb)
6 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

Storage autoscaling

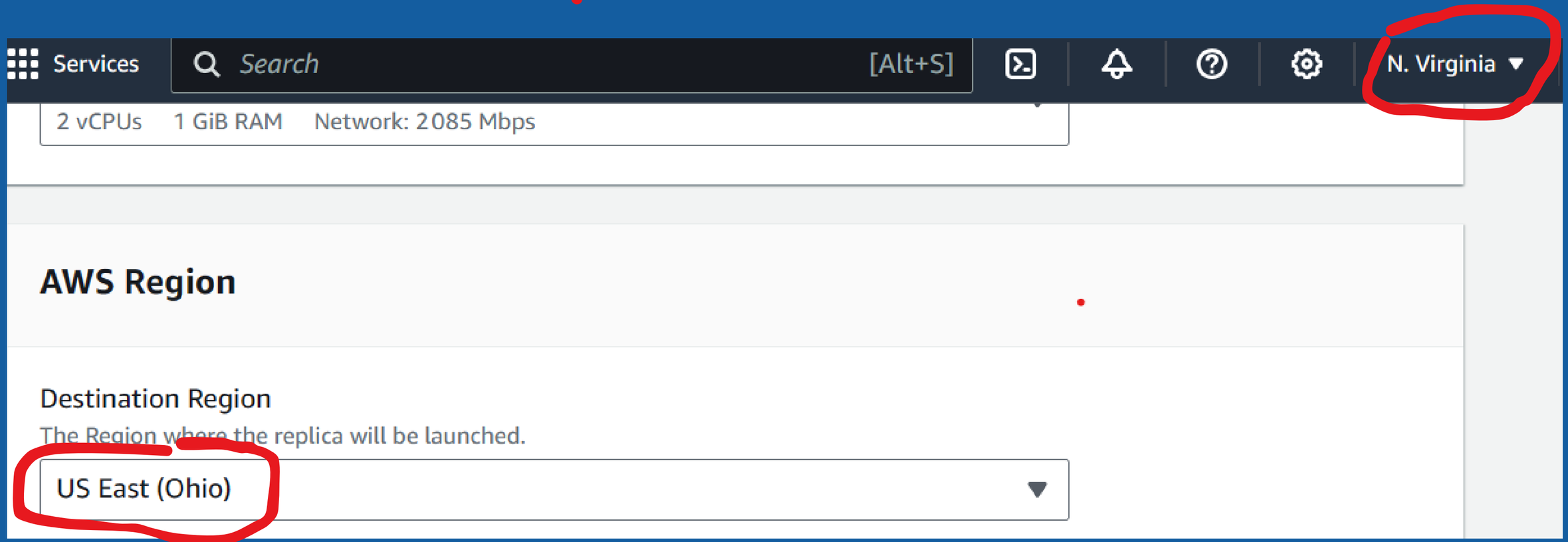
Info

Provides dynamic scaling support for your database's storage based on your application's needs.

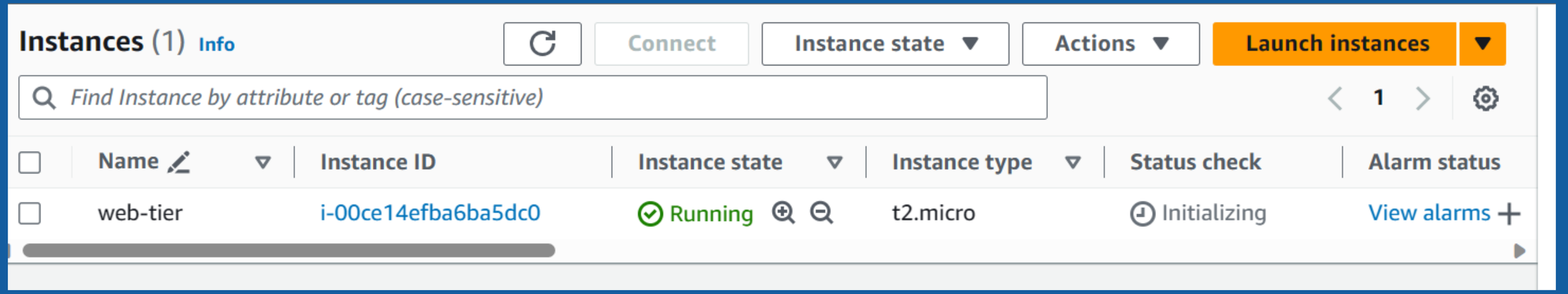
- [x] Enable storage autoscaling

  Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

the Replica

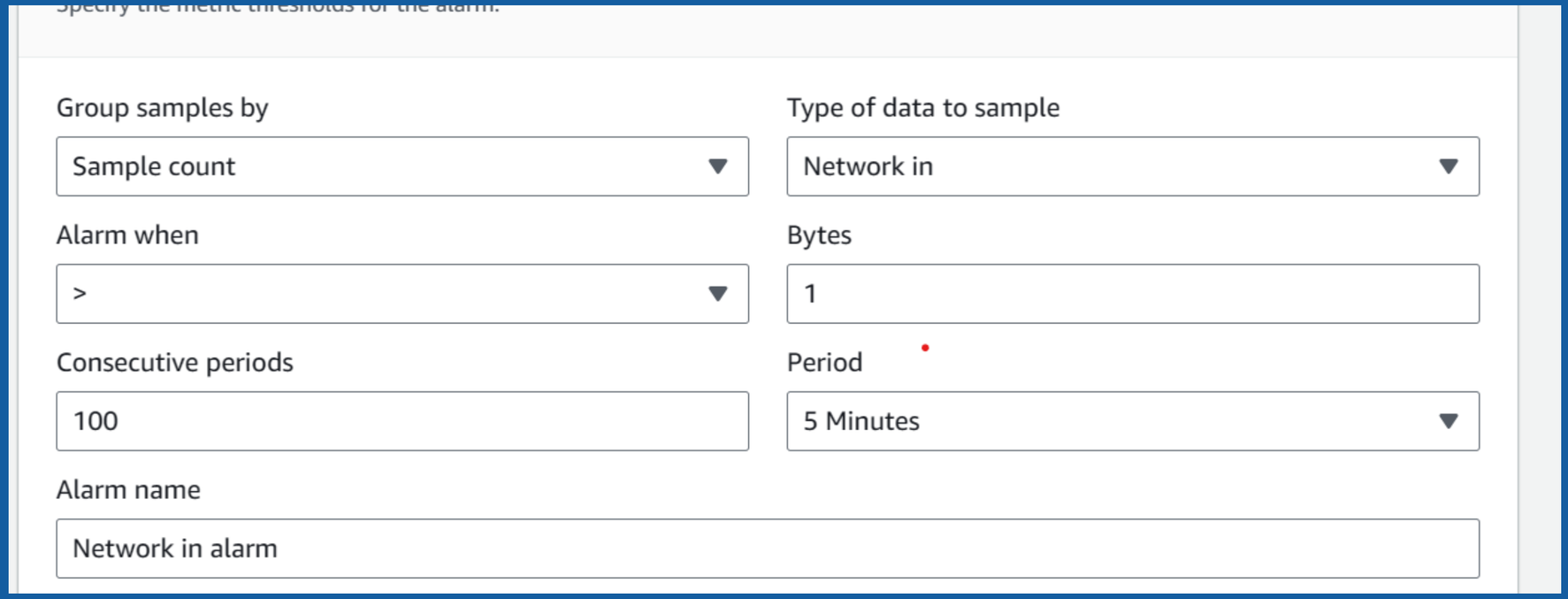

Services
Search
[Alt+S]
N. Virginia
2 vCPUs
1 GiB RAM
Network: 2085 Mbps
AWS Region
Destination Region
The Region where the replica will be launched.
US East (Ohio)

App Tier Instance Deployment


Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
web-tier
i-00ce14efba6ba5dc0
Running
t2.micro
Initializing
View alarms

Application administrators want to be notified by email if there are more than 100 “400 HTTP errors” per minute in the application.

cloudWatch Alarm



connecting to the RDS from my instance

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 298
Server version: 5.7.12 MySQL Community Server (GPL)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> create DATABASE webappdb;
Query OK, 1 row affected (0.01 sec)
```

uploading code to our S3 bucket

Upload succeeded
View details below.

Upload: status

Close

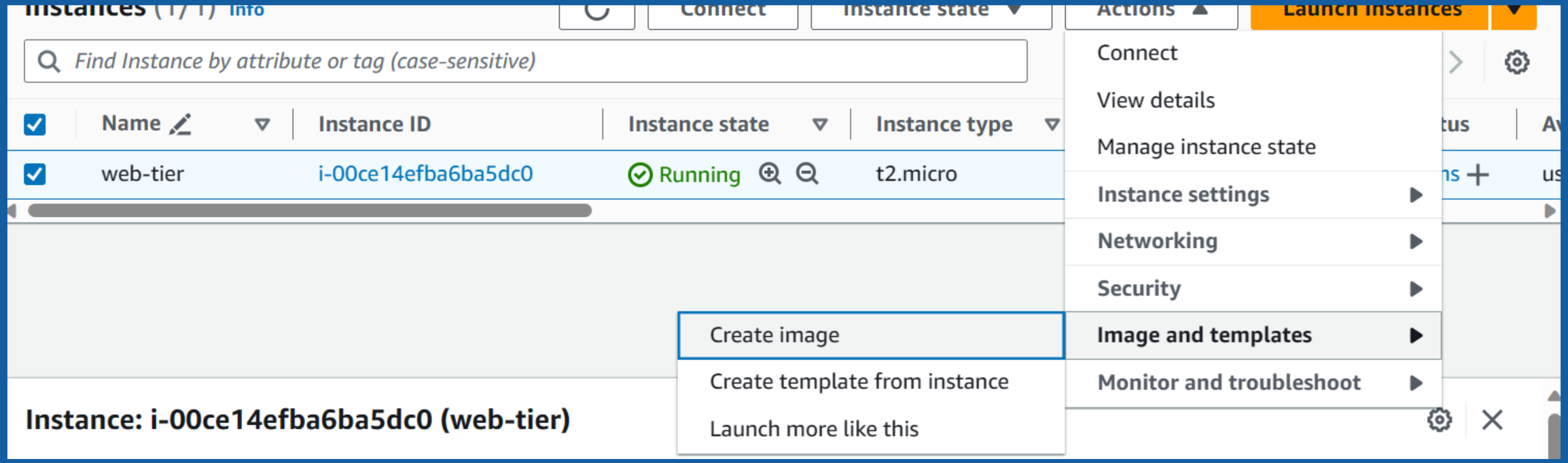
The information below will no longer be available after you navigate away from this page.

Summary

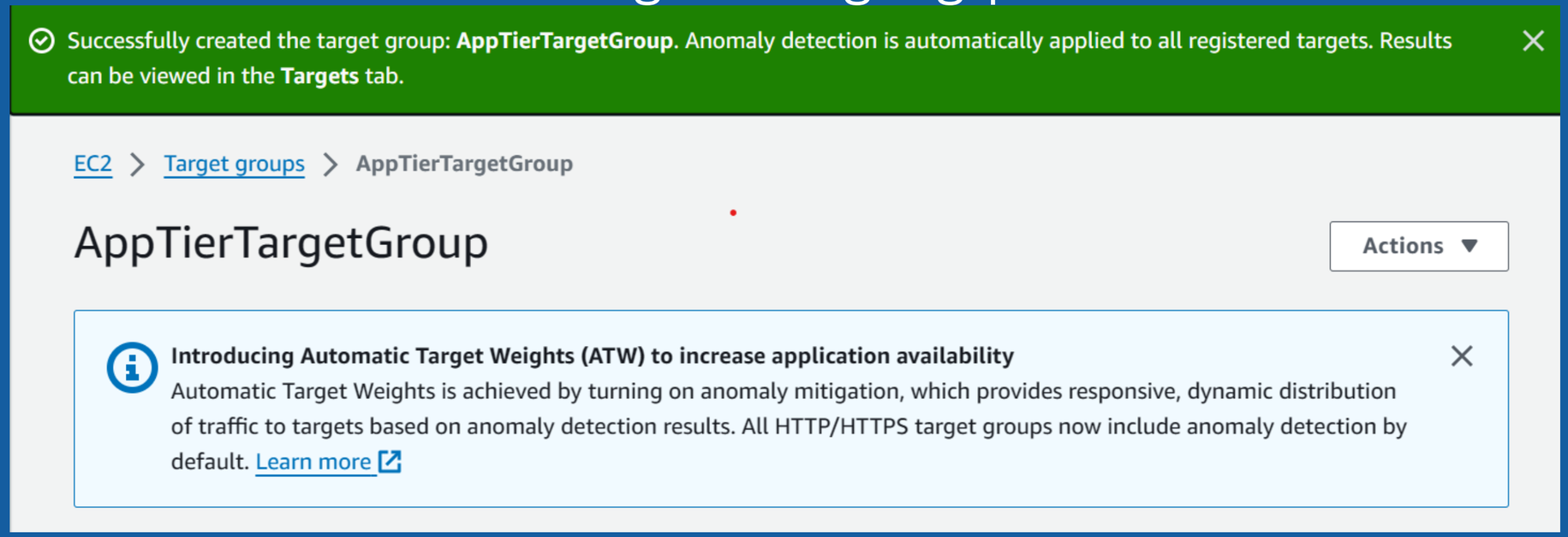
Destination	Succeeded	Failed
s3://smart-education	6 files, 48.7 KB (100.00%)	0 files, 0 B (0%)

Internal Load Balancing and Auto Scaling

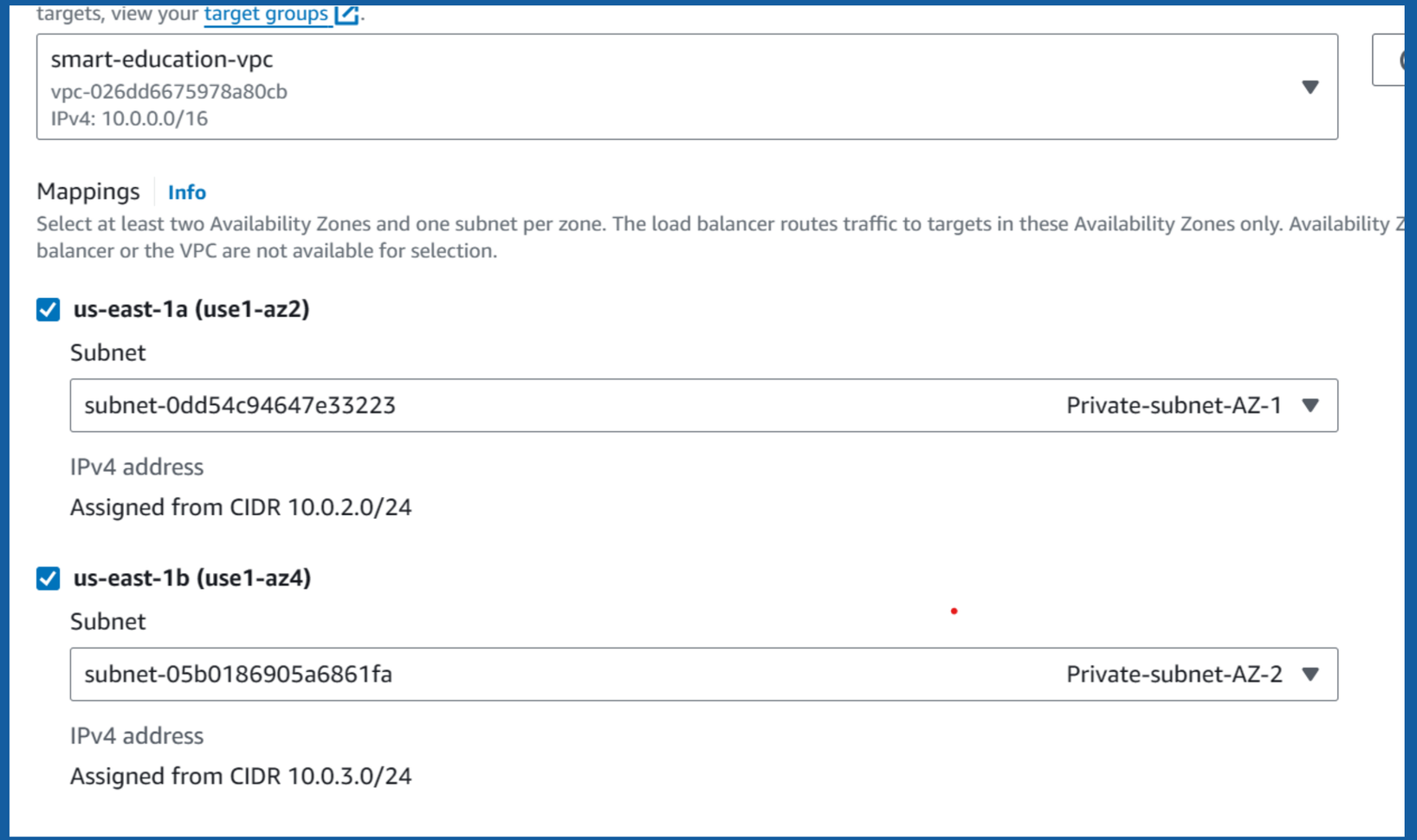
Creating images



Creating the target grp for our load balencer



Creating the internal lb



Security groups

Select up to 5 security groups

Internal-lb-sg
sg-06bf612d7dbde2538 VPC: vpc-026dd6675978a80cb

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 to its registered targets.

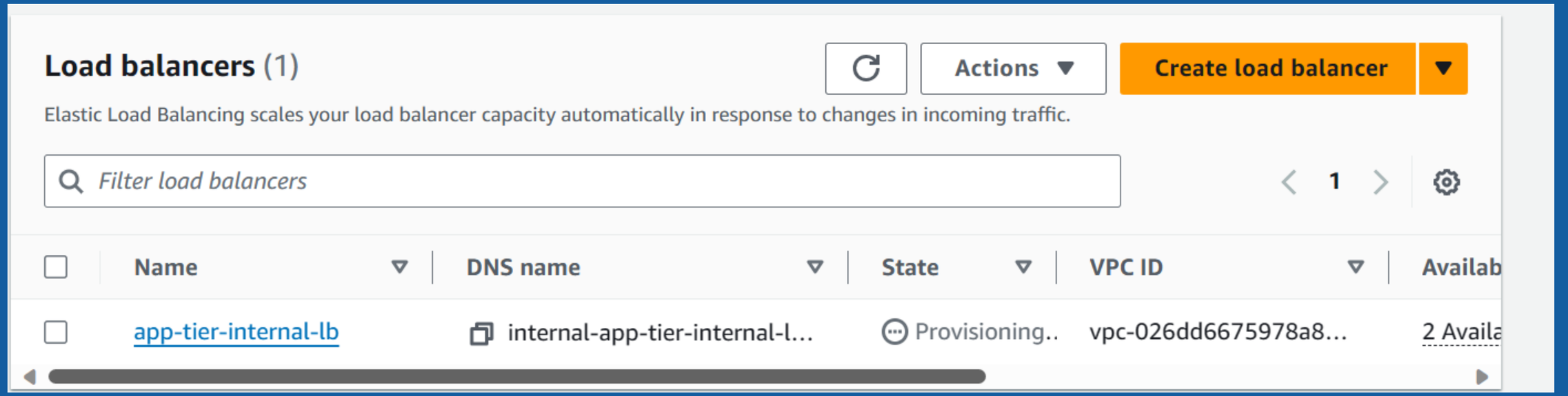
▼ Listener **HTTP:80**

Protocol: HTTP : Port: 80
1-65535

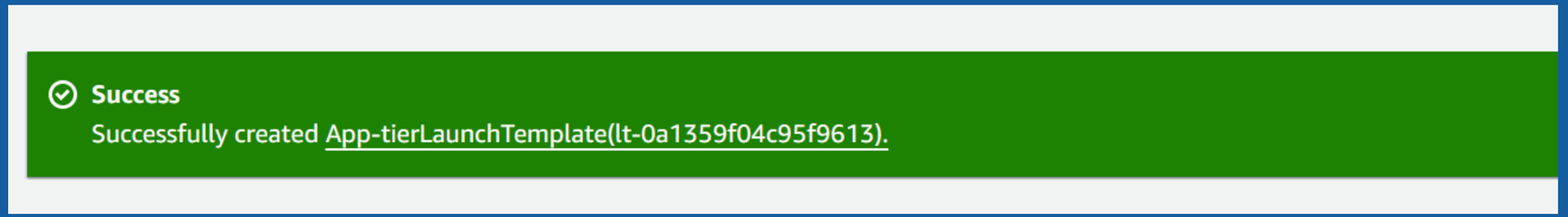
Default action Info

Forward to: AppTierTargetGroup HTTP
Target type: Instance, IPv4

Create target group


Load balancers (1)
Actions
Create load balancer
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.
Filter load balancers
1
Name
DNS name
State
VPC ID
Availab
app-tier-internal-lb
internal-app-tier-internal-l...
Provisioning..
vpc-026dd6675978a8...
2 Availa

Launch Template



Desired capacity

Specify your group size.

2

Scaling Info

You can resize your Auto Scaling group manually or automaticall

Scaling limits

Set limits on how much your desired capacity can be increased o

Min desired capacity

2

Equal or less than desired capacity

Max desired capacity

2

Equal or greater than desired capacity

EC2 > Auto Scaling groups

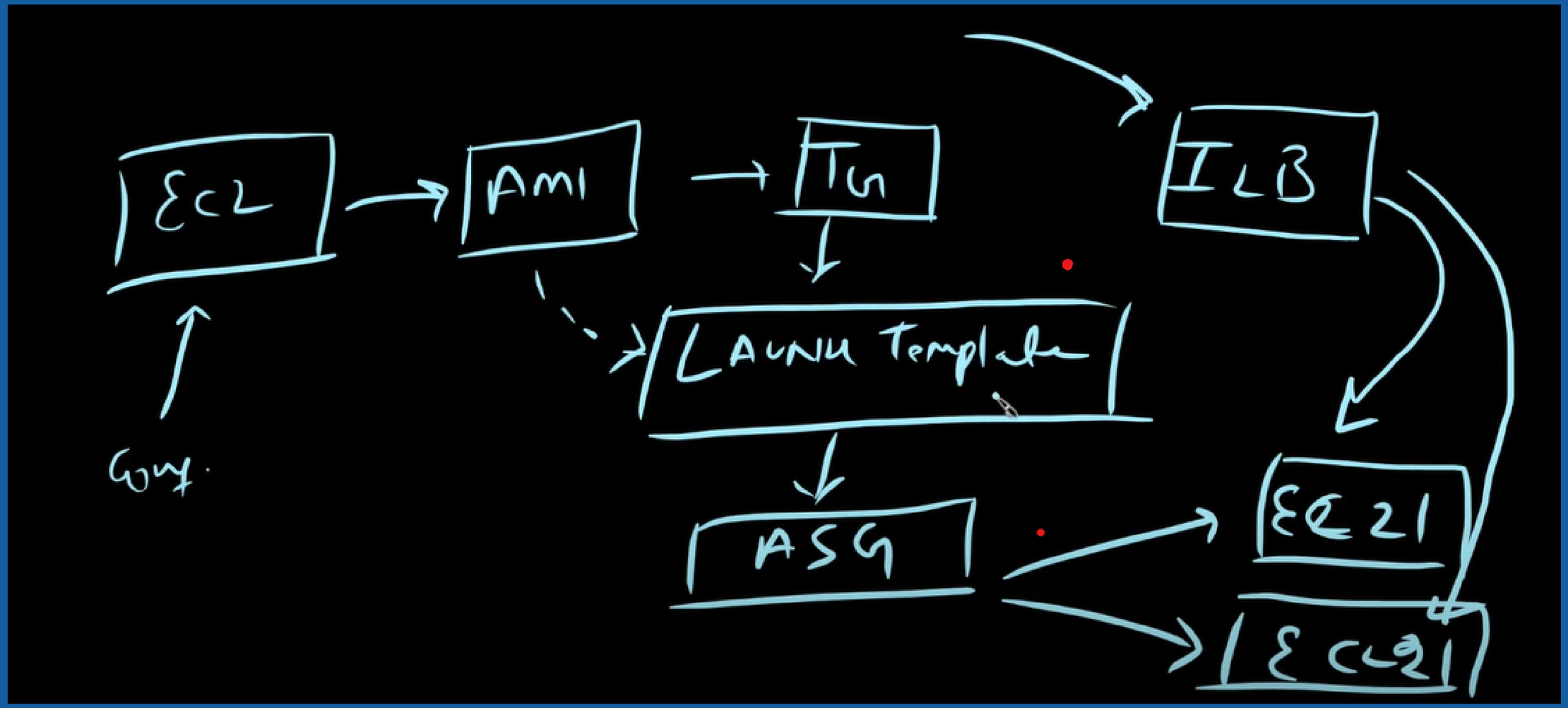
Auto Scaling groups (1) Info

Launch configurations | Launch templates | Actions | Create Auto Scaling g

Search your Auto Scaling groups

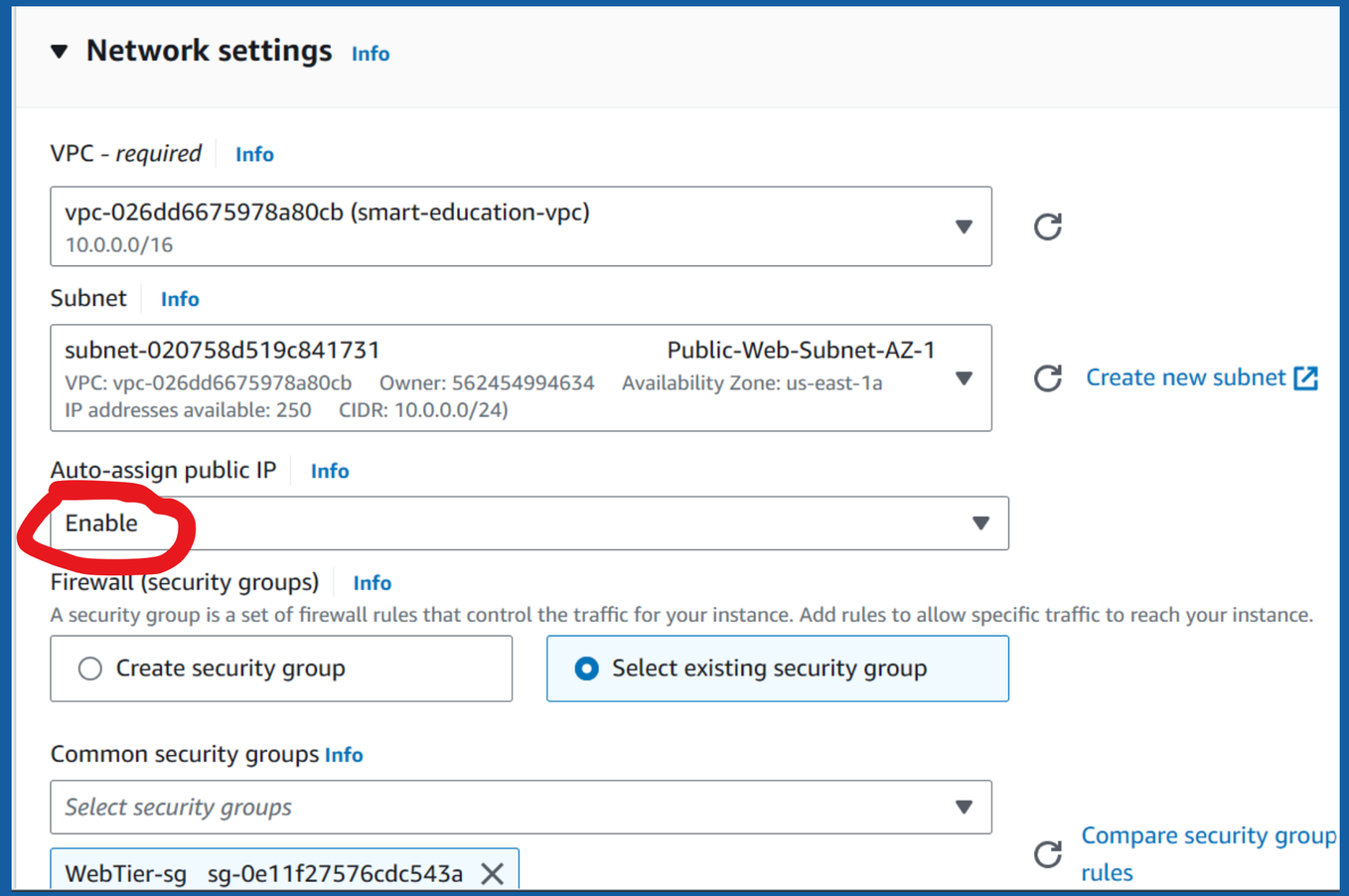
Name	Launch template/configuration	Instances
AppTierSG	App-tierLaunchTemplate | Version Default	2

what we did

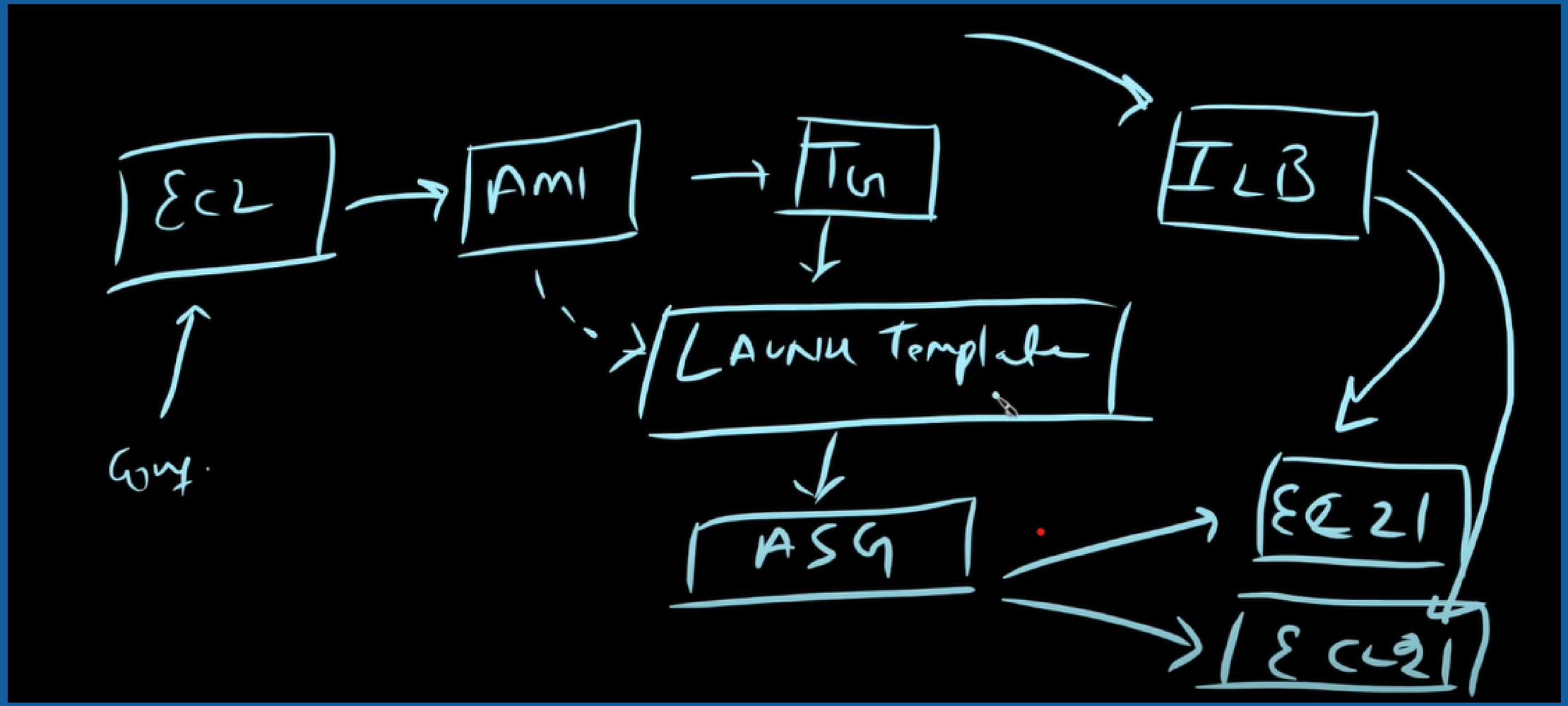


Web Tier Instance Deployment

Creating a webtier Ec2 instance

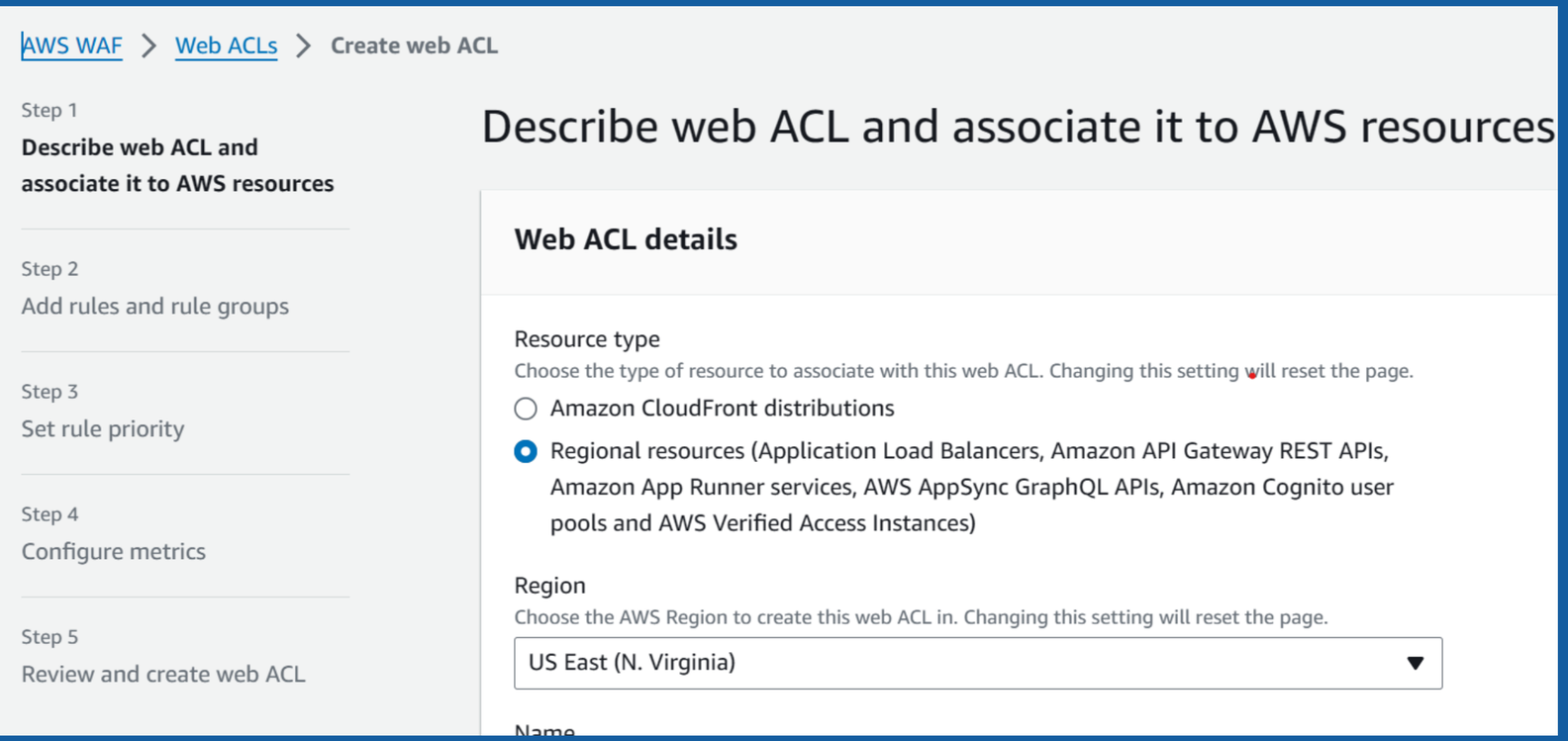


We redo the same but now an extarnal load balencer and an autoscaling grp for the Web Tier



At the end we should be able to acess the front end throught the DNSof the Web-tier-Load-balencer

additional features



+ Region(Recovery site)

+ Acess Control


THANK
YOU