

جامعة محمد الخامس بالرباط
Université Mohamed V de Rabat



Cloud Project

By:

GUIGUI SALMA
MESKINI YASSIR
ELKAMEL ISMAIL

Overview

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



Introduction

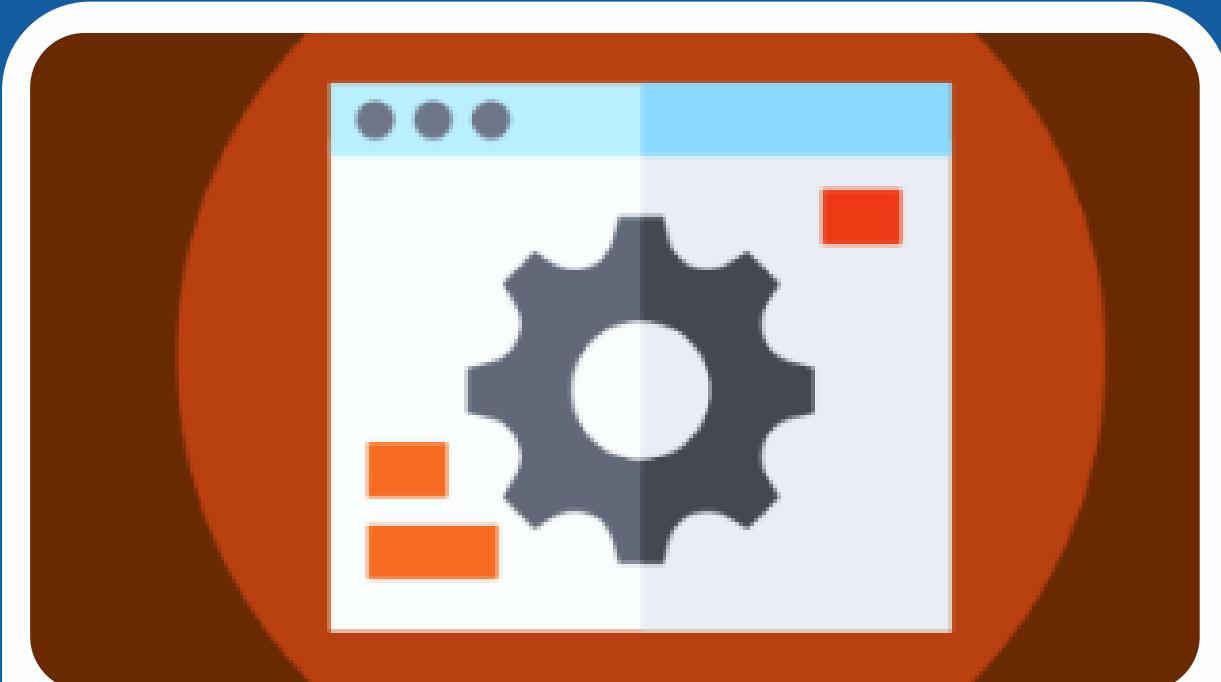
Cloud Provider



Three-Tier Architecture



WEB Tier

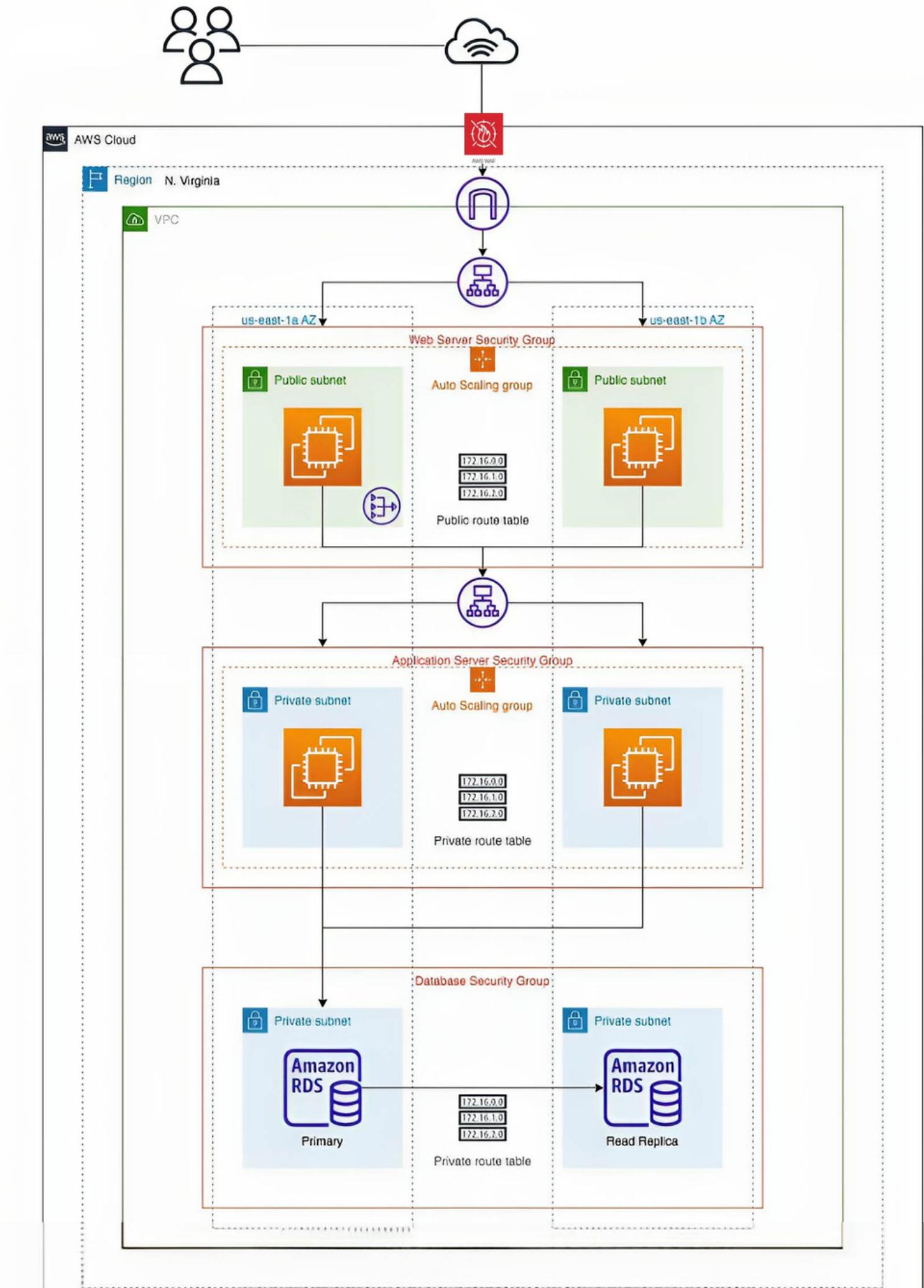


Application Tier



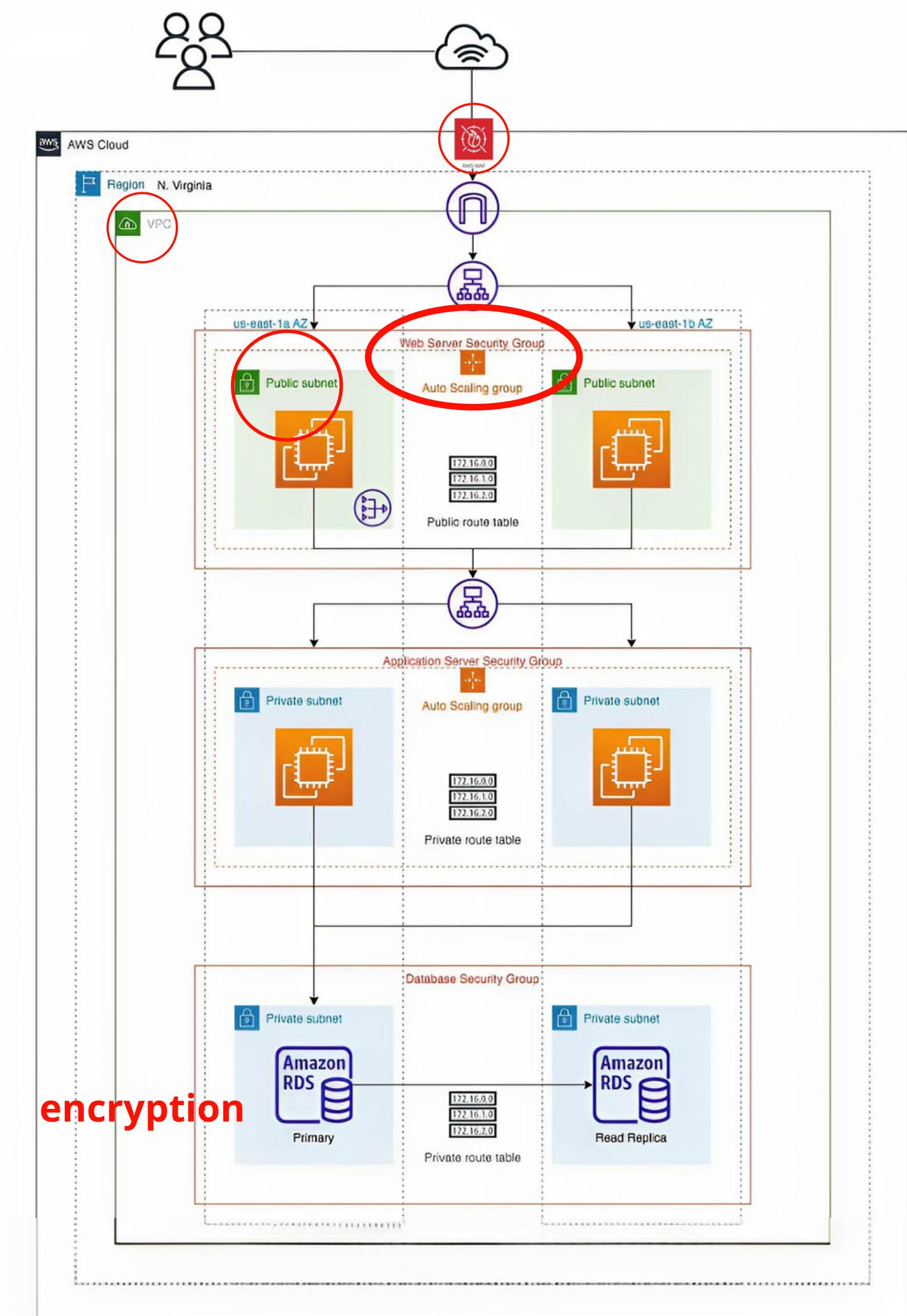
Database Tier

AWS Cloud Architecture



Security

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

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associati...
<input type="checkbox"/>	-	rtb-07f2a568a2b41f6e3	-
<input type="checkbox"/>	PrivateRouteTable-AZ1	rtb-092dd55ce32b170df	<u>subnet-0dd54c94647e33...</u>
<input type="checkbox"/>	Public-Route-Table	rtb-05a916f4cf759bf7b	2 subnets
<input type="checkbox"/>	-	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

 igw-03d3d13d25b1c262e

State

 Attached

VPC ID

[vpc-026dd6675978a80cb](#) |
[smart-education-vpc](#)

Owner

 562454994634

	Name	NAT gateway ID	Connectivit...	State	State message
<input type="radio"/>	NAT-GW-AZ1	nat-0e9d8cd89f877f2b2	Public	<input checked="" type="checkbox"/> Available	-
<input type="radio"/>	NAT-GW-AZ2	nat-0a8e864c20df137e6	Public	<input checked="" type="checkbox"/> Available	-

Security Groups (1/7) [Info](#) Actions ▾ [Export security groups to CSV](#) ▾ [Create security group](#)

Find resources by attribute or tag

<input type="checkbox"/>	Name	Security group ID	Security group name
<input type="checkbox"/>	-	sg-0545d3964794fd6d5	DB-sg
<input type="checkbox"/>	-	sg-07f5f6f0862b6344f	default
<input type="checkbox"/>	-	sg-0788ad99742428b05	default
<input type="checkbox"/>	-	sg-06bf612d7dbde2538	Internal-lb-sg
<input type="checkbox"/>	-	sg-0e11f27576cdc543a	WebTier-sg
<input type="checkbox"/>	-	sg-093bf7f94c1844575	Private-instances-sg
<input checked="" type="checkbox"/>	-	sg-0a57e9b14e273b02f	Internet-facing-lb-sg



Creation de notre DB



Services

Search [Alt+S]



N. Virginia ▾

voclabs/user2768941=salma_GUI @ 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-0dfaef0b2328ad1546 (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](#)

C

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.



Enable storage autoscaling

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

the Replica

The screenshot shows the AWS Lambda 'Create Function' wizard at the 'AWS Region' step. The top navigation bar includes 'Services', a search bar, and a region selector set to 'N. Virginia'. Below the bar, resource details are listed: '2 vCPUs', '1 GiB RAM', and 'Network: 2085 Mbps'. The main section is titled 'AWS Region' and contains a dropdown menu currently set to 'US East (Ohio)'. A red box highlights the 'US East (Ohio)' option, and another red box highlights the 'N. Virginia' region in the top bar.

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](#)

C Connect Instance state ▾ Actions ▾ Launch instances ▾

Find Instance by attribute or tag (case-sensitive)

< 1 >

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>	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

Specify the metric thresholds for the alarm.

Group samples by	Type of data to sample
Sample count	Network in
Alarm when	Bytes
>	1
Consecutive periods	Period
100	5 Minutes
Alarm name	
Network in 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

[s3://smart-education](#)

Succeeded

 6 files, 48.7 KB (100.00%)

Failed

 0 files, 0 B (0%)

Internal Load Balancing and Auto Scaling

Creating images

The screenshot shows the AWS Lambda console interface. At the top, there's a search bar labeled "Find Function by name or ARN (case-sensitive)" and a "Create new function" button. Below the search bar, there's a table with columns: Name, ARN, Handler, and Role. A single row is visible, representing a function named "HelloWorld" with the ARN "arn:aws:lambda:us-east-1:123456789012:function:HelloWorld". To the right of the table, there's a "Actions" dropdown menu with options: "Edit", "Delete", "Version history", "Logs", "Metrics", "CloudWatch Events", "CloudWatch Metrics", "CloudWatch Logs", "CloudWatch Metrics Insights", "AWS CloudTrail", "AWS X-Ray", "AWS Lambda Metrics", "AWS Lambda Metrics Insights", "AWS Lambda CloudWatch Metrics Insights", and "AWS Lambda CloudWatch Metrics Insights Insights".

Instances (1/1) Info

Connect Instance state Actions Launch Instances

Find Instance by attribute or tag (case-sensitive)

Name Instance ID Instance state Instance type

web-tier i-00ce14efba6ba5dc0 Running t2.micro

Connect View details Manage instance state

Instance settings Networking Security

Create image Create template from instance Launch more like this

Image and templates Monitor and troubleshoot

Instance: i-00ce14efba6ba5dc0 (web-tier)

Creating the target grp for our load balancer

✓ Successfully created the target group: **AppTierTargetGroup**. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the **Targets** tab. X

[EC2](#) > [Target groups](#) > AppTierTargetGroup

AppTierTargetGroup

[Actions ▾](#)



Introducing Automatic Target Weights (ATW) to increase application availability

Automatic Target Weights is achieved by turning on anomaly mitigation, which provides responsive, dynamic distribution of traffic to targets based on anomaly detection results. All HTTP/HTTPS target groups now include anomaly detection by default. [Learn more](#)

Creating the internal lb

targets, view your [target groups](#).

smart-education-vpc
vpc-026dd6675978a80cb
IPv4: 10.0.0.0/16

Mappings | [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones or the VPC are not available for selection.

us-east-1a (use1-az2)

Subnet

subnet-0dd54c94647e33223 Private-subnet-AZ-1 ▾

IPv4 address
Assigned from CIDR 10.0.2.0/24

us-east-1b (use1-az4)

Subnet

subnet-05b0186905a6861fa Private-subnet-AZ-2 ▾

IPv4 address
Assigned from CIDR 10.0.3.0/24

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

Remote

Protocol

Port

Default action

[Info](#)

HTTP

: 80

1-65535

Forward to

AppTierTargetGroup

Target type: Instance, IPv4

HTTP



[Create target group](#)

Load balancers (1)

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

Actions ▾ [Create load balancer](#) ▾

Filter load balancers < 1 > ⚙️

<input type="checkbox"/>	Name	DNS name	State	VPC ID	Available
<input type="checkbox"/>	app-tier-internal-lb	<input type="checkbox"/> internal-app-tier-internal-l...	Provisioning..	vpc-026dd6675978a8...	2 Available

Launch Template



Success

Successfully created [App-tierLaunchTemplate\(lt-0a1359f04c95f9613\)](#).

Desired capacity

Specify your group size.

2

Scaling Info

You can resize your Auto Scaling group manually or automatically

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

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



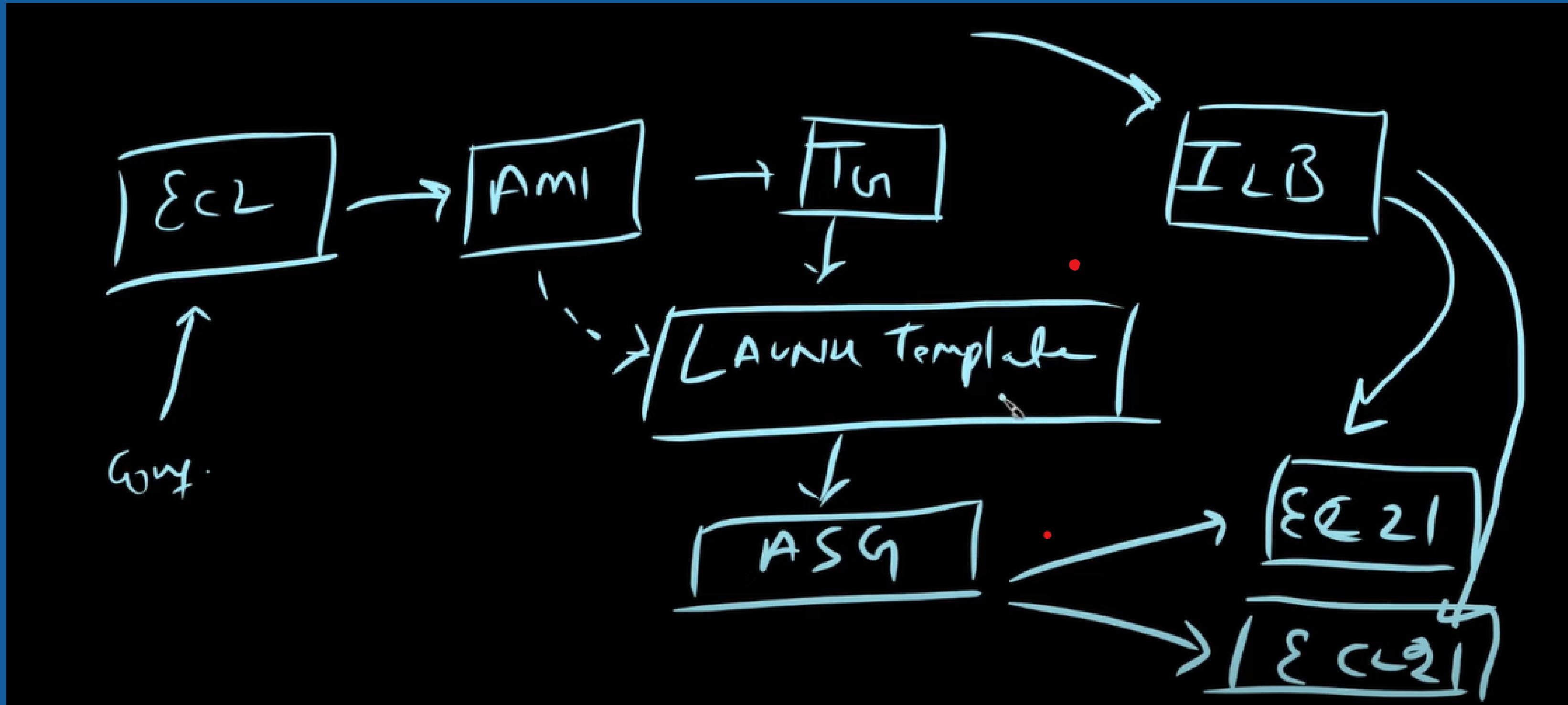
Instances



[AppTierSG](#)

[App-tierLaunchTemplate](#) | Version Default 2

what we did



Web Tier Instance Deployment

Creating a webtier Ec2 instance

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-026dd6675978a80cb (smart-education-vpc)
10.0.0.0/16

Subnet [Info](#)

subnet-020758d519c841731 Public-Web-Subnet-AZ-1
VPC: vpc-026dd6675978a80cb Owner: 562454994634 Availability Zone: us-east-1a
IP addresses available: 250 CIDR: 10.0.0.0/24

Create new subnet

Auto-assign public IP [Info](#)

Enable

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

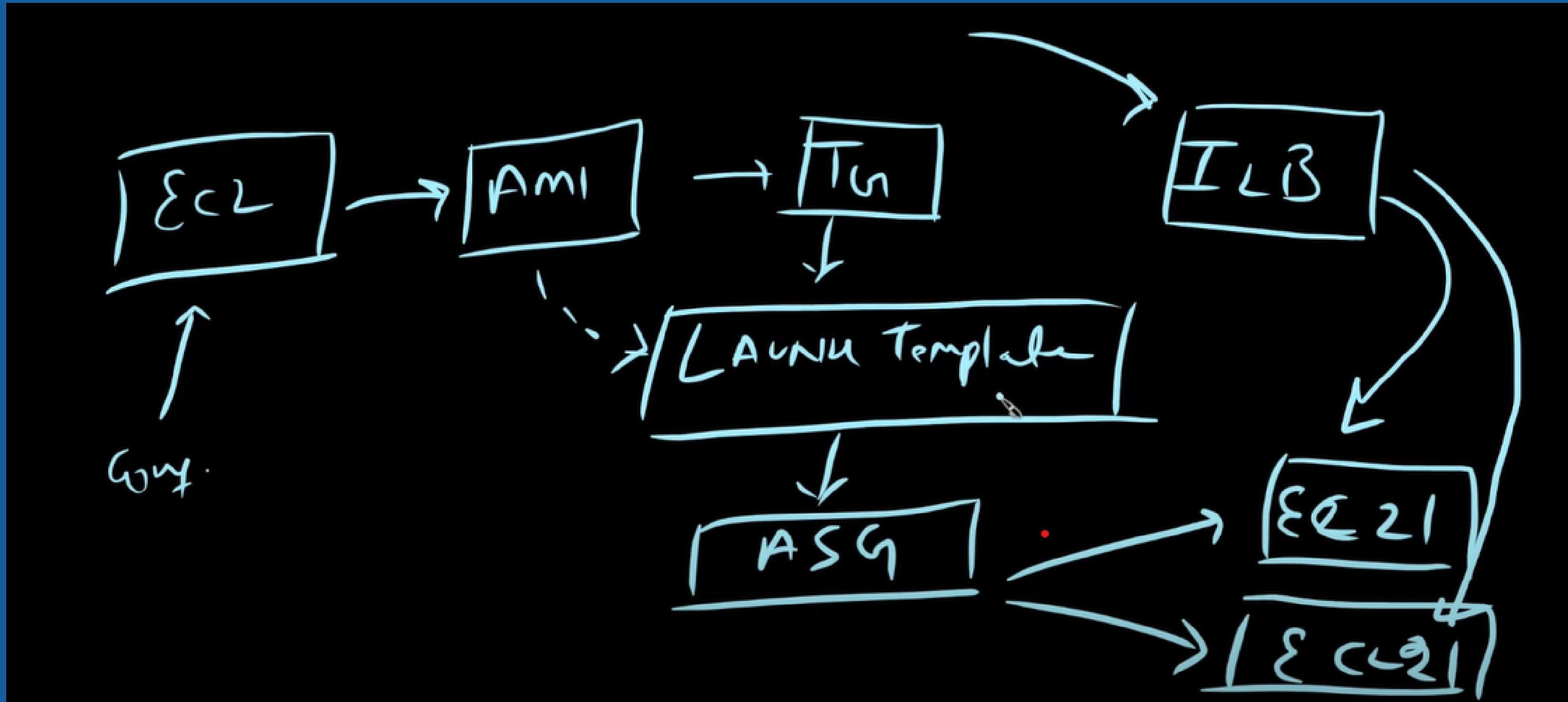
Common security groups [Info](#)

Select security groups

WebTier-sg sg-0e11f27576cdc543a

Compare security group rules

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 access the front end through the DNS of the Web-tier-Load-balancer

additional features

AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Describe web ACL and associate it to AWS resources

Web ACL details

Resource type
Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

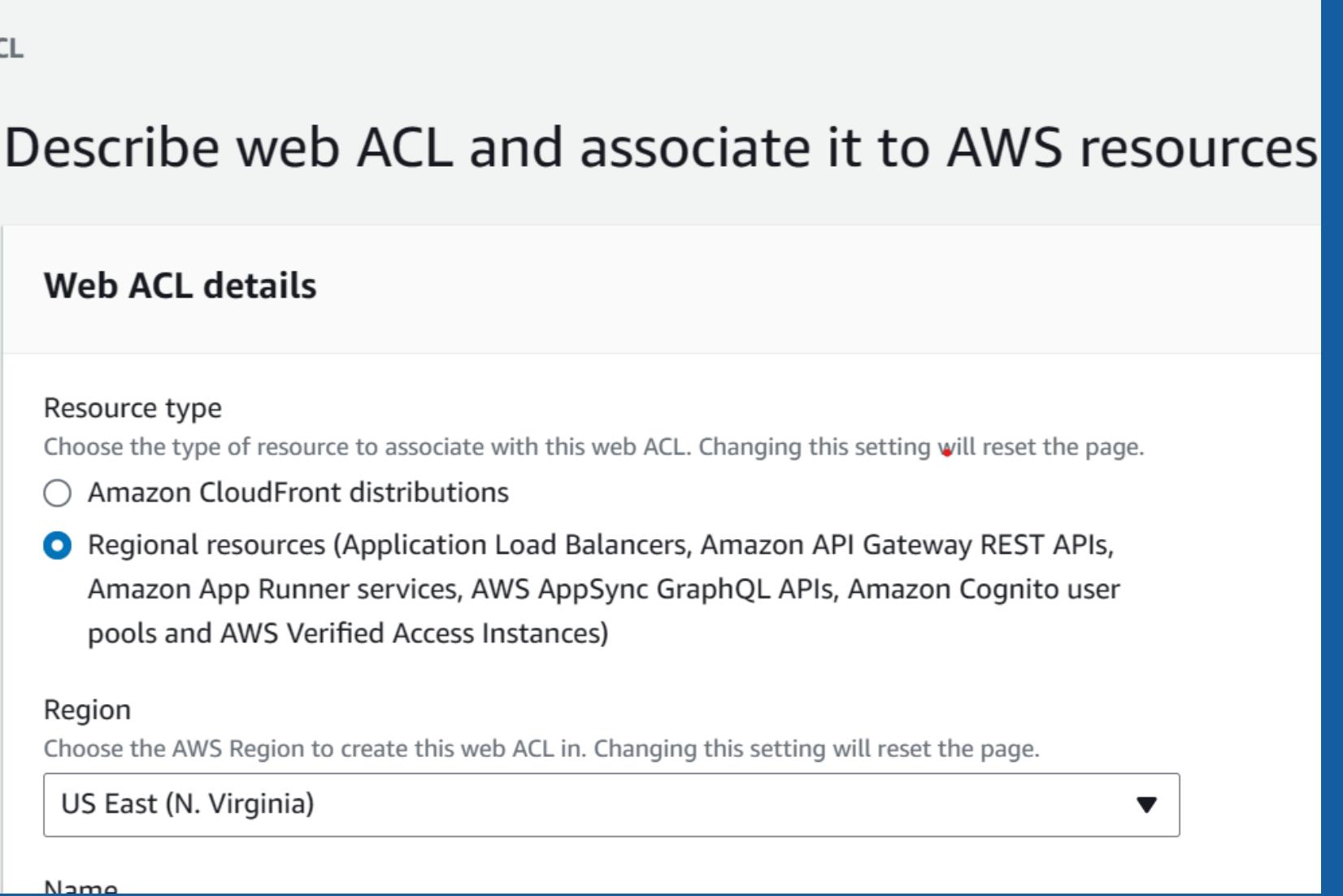
Amazon CloudFront distributions

Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, Amazon App Runner services, AWS AppSync GraphQL APIs, Amazon Cognito user pools and AWS Verified Access Instances)

Region
Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

US East (N. Virginia) ▾

Name



+ Region(Recovery site)

+ Acess Control

