

oooo

Presented by:

- NAIYM Mohammed
- AIT BOUAZZA Zaynab
- EL KOURTI Houssam

SMARTLEARN

Towards a student-centric approach



TABLE OF CONTENTS

- Introduction
- Architecture Overview
- Security Consideration
- Implementation
- Conclusion



01

INTRODUCTION

The propose and
objectives of the
application



- Faciliter la communication efficace entre les étudiants et les professeurs.
- Permettant aux éducateurs d'évaluer et de prédire les performances des étudiants
- Infrastructure cloud sécurisée qui répondra à toutes les exigences de cette solution novatrice.

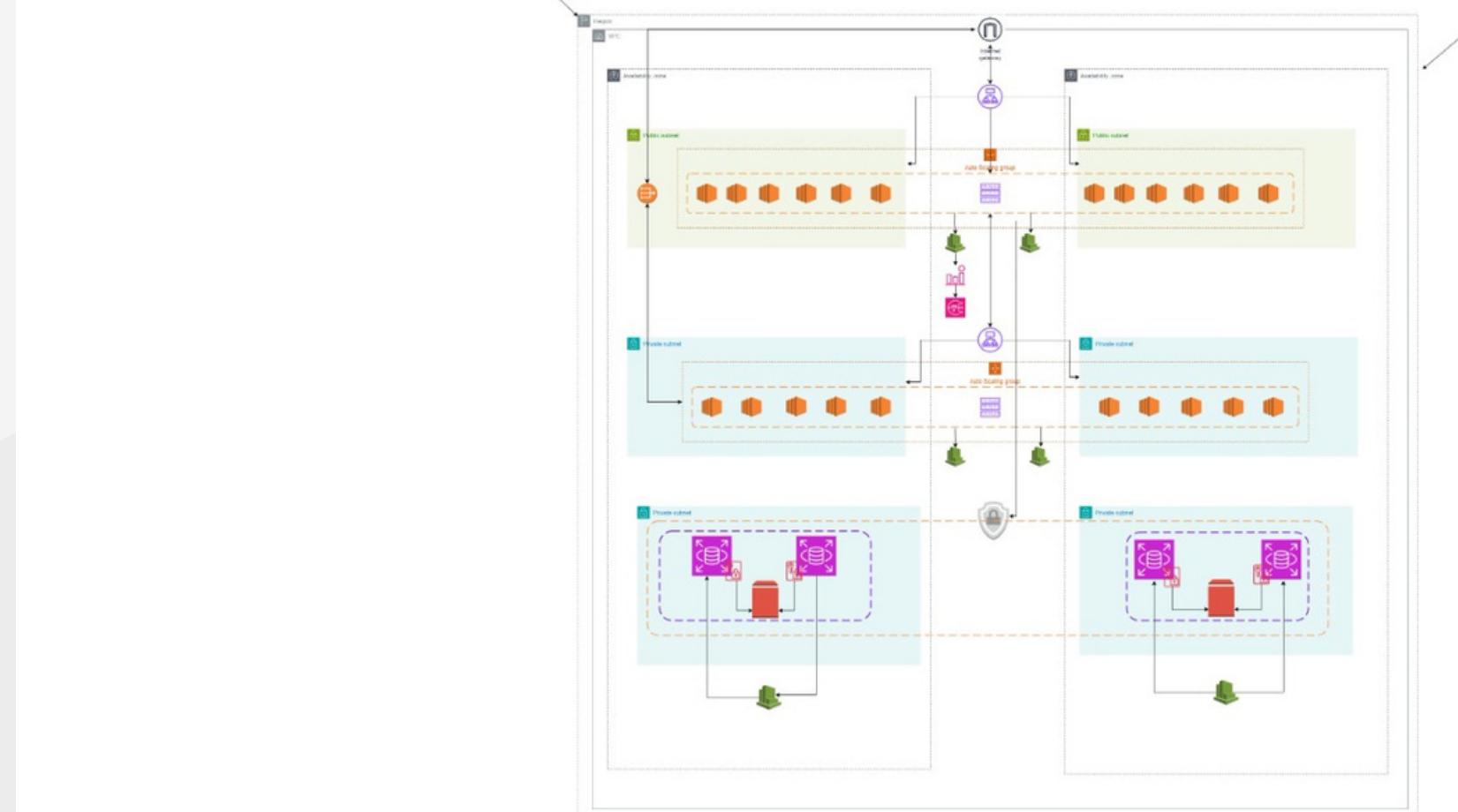
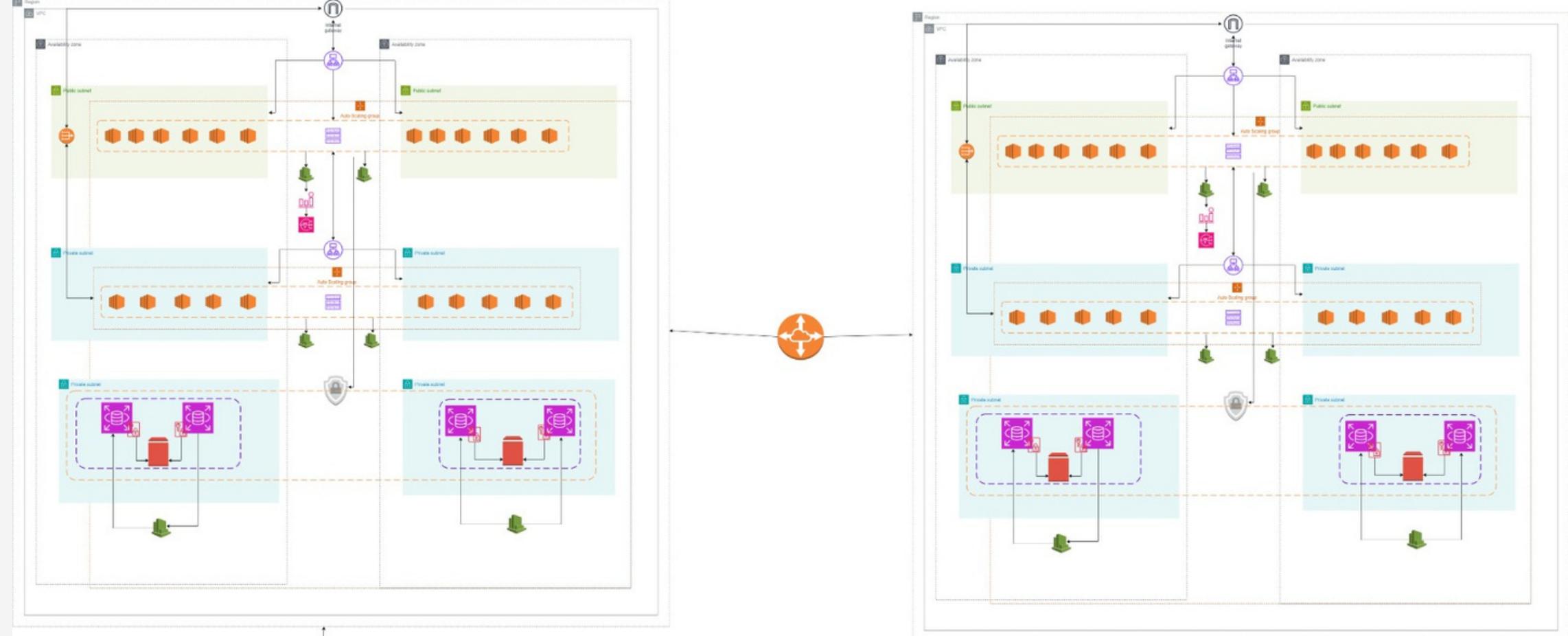


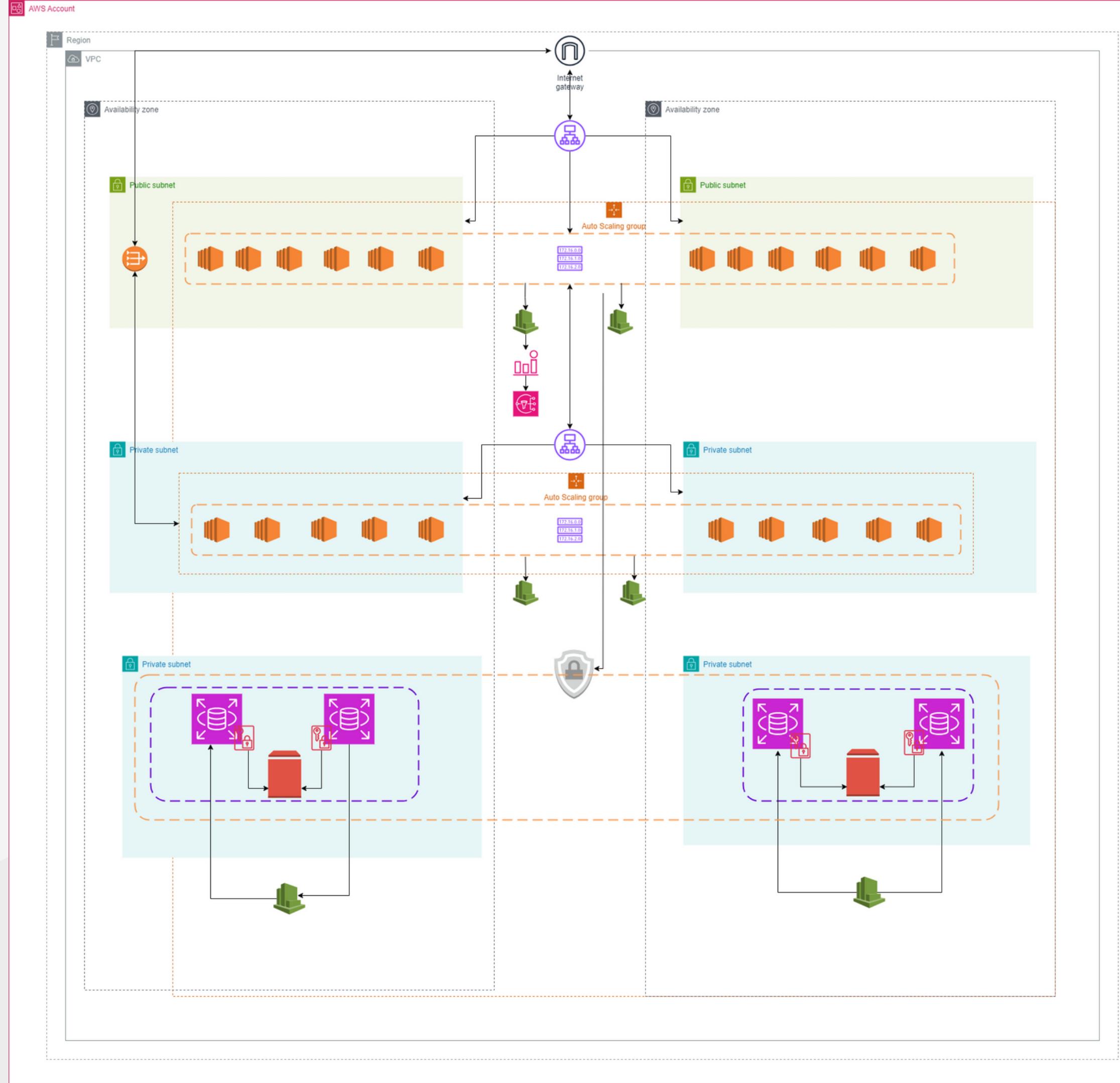
02

ARCHITECTURE OVERVIEW

The overall
architecture of the
application

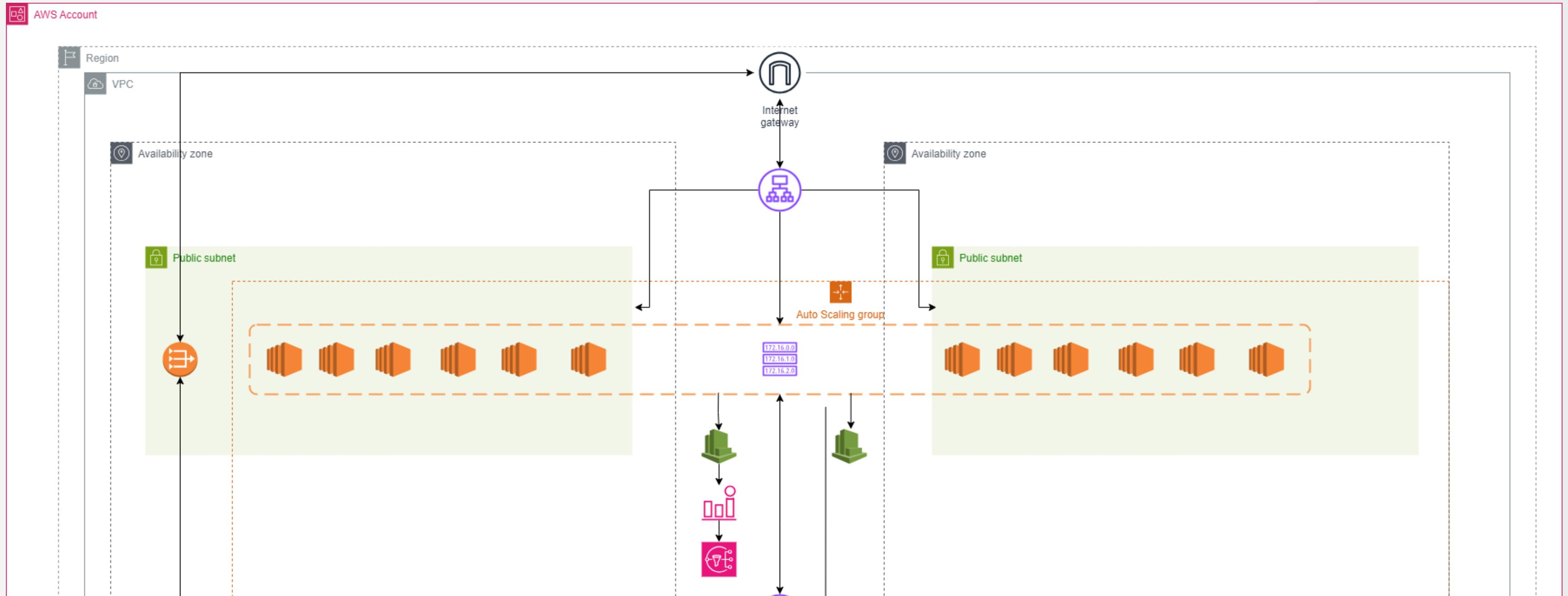
peering
connection





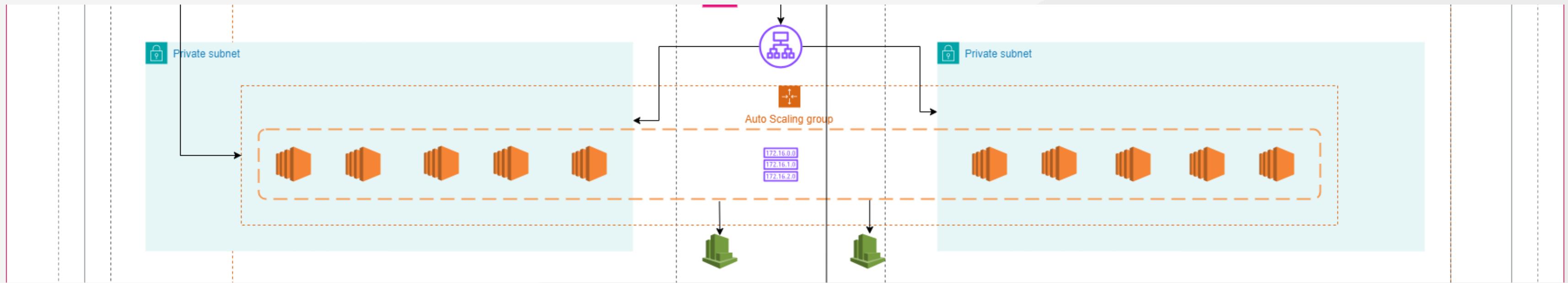
WEB TIER REQUIREMENTS

Requirement	Solution
Architecture must be flexible and handle any peak in traffic or performance	- Use AWS Auto Scaling - Use AWS Load Balancer
The overall acceptable incoming network bandwidth is between 300 Mbps and 750 Mbps.	Use Amazon CloudWatch to create the metric with the corresponding alarm
Application administrators want to be notified by email if there are more than 100 “400 HTTP errors” per minute in the application.	Use Amazon CloudWatch to monitor application's logs for HTTP errors and configure an alarm to trigger an SNS (Simple Notification Service) notification via email to the application administrators if the error count exceeds 100 per minute
Web Tier instances should be tagged as “Key=Name” and “Value=web-tier”	Use the Amazon EC2 console to create tags for instances



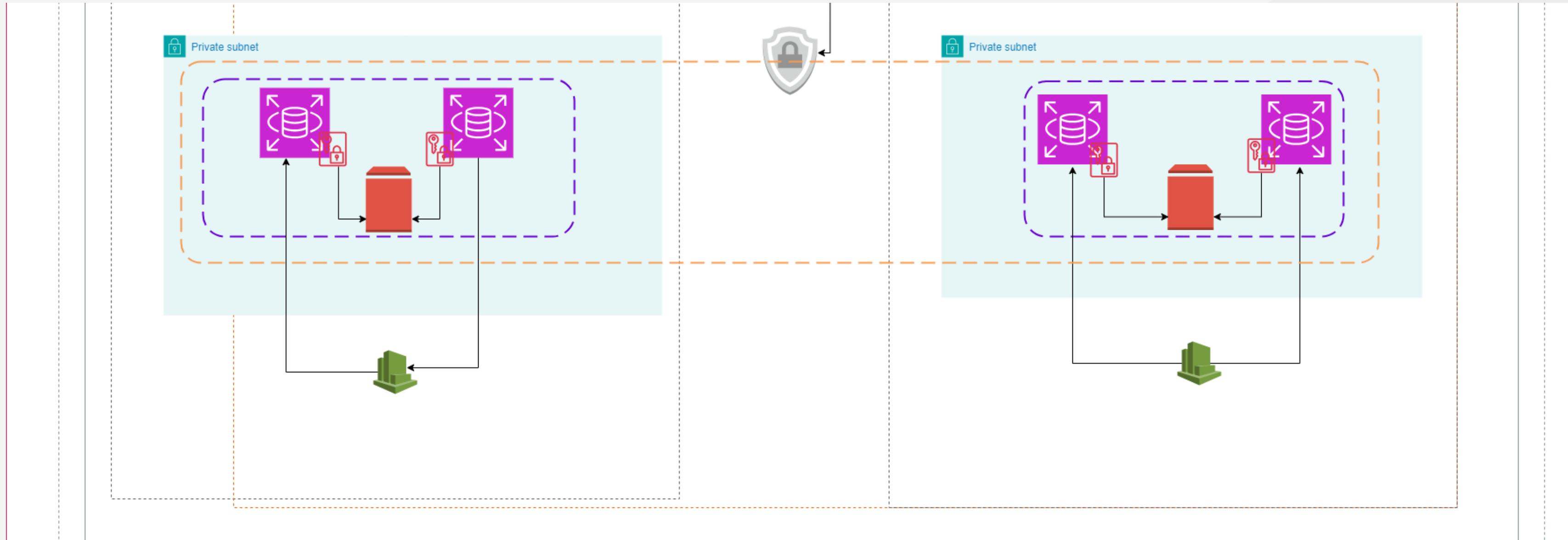
APPLICATION TIER REQUIREMENTS

Requirement	Solution
Architecture must be flexible and handle any peak in traffic or performance	<ul style="list-style-type: none">- Use AWS Auto Scaling- Use AWS Load Balancer
Server capacity should be between 50% and 60%	Set up autoscaling group with target utilization of 50-60% and configure the group to add remove instances as needed to maintain that utilization
Overall memory and CU utilization should not go above 80% and 75% respectively or below 30% for either	Use Amazon CloudWatch to create this metric and a corresponding alarm
Internet access is required for patching and updates without exposing the servers	Use a NAT gateway in a public subnet of the VPC to allow outbound internet access for the patching server and other resources in the private subnets
Application Tier instances should be tagged as "Key-Name" and "Value=app-tier"	Use the Amazon EC2 console to create tags for our Instances.



DATABASE TIER REQUIREMENTS

Requirement	Solution
Database needs consistent storage performance at 21,000 IOPS.	<ul style="list-style-type: none">• Use Amazon RDS with Elastic Block Store (EBS), and configurate it with the provisionned IOPS storage type (21,000)• Use Amazon CloudWatch to regulary monitor and adjust the provisionned IOPS as needed.
availability is a requirement	Use Amazon RDS with Multi-AZ deployment for automatic failover and data redundancy.
No change to the database schema can be made at this time.	With Amazon RDS, there's no need to modify the existing schema during provisioning or migration.



03

SECURITY CONSIDERATION

Security Measures and
considerations



RISK ASSESSMENT PLAN

**Modèle d'évaluation des risques
ISO 27001 :**

- évaluer et gérer les risques liés à la sécurité de l'information au sein d'une organisation
- Pour établir, mettre en œuvre, maintenir et améliorer continuellement un système de gestion de la sécurité de l'information (SMSI).

APP TIER REQUIREMENTS

Risk	Asset	Vulnerability	Risk Treatment
Code Injection: Unauthorized execution of code within the application.	- Application logic. - User data.	- Lack of input validation. - Insufficient code review processes.	- Input validation. - Secure coding practices. - Regular code reviews.
Privilege Escalation: Unauthorized elevation of user privileges.	- User accounts. - Sensitive data.	- Weak access controls. - Unmonitored privilege changes.	- Regular access reviews. - Least privilege principle.
Physical Attacks: Physical damage to servers and infrastructure	- Servers. - Hardware infrastructure.	- Lack of physical security measures.	- Physical access controls. - Surveillance.

WEB TIER REQUIREMENTS

Risk	Asset	Vulnerability	Risk Treatment
<p>Distributed Denial of Service (DDoS) Attack: Disruption of web services due to a DDoS attack.</p>	<ul style="list-style-type: none">- Web servers.- Online services.	<ul style="list-style-type: none">- Lack of DDoS protection- Insufficient network capacity.	<ul style="list-style-type: none">- DDoS mitigation tools.- Increased network capacity with high availability.- Usage of load balancers to distribute traffic.
<p>Insufficient Authentication and Authorization: Unauthorized access to web resources due to weak authentication and authorization controls.</p>	<ul style="list-style-type: none">- User accounts.- Sensitive data.	<ul style="list-style-type: none">- Weak password policies.- Inadequate role-based access controls.	<ul style="list-style-type: none">- Multi-factor authentication.- Strong password policies.- Regular access reviews.

DATABASE TIER REQUIREMENTS

Risk	Asset	Vulnerability	Risk Treatment
Data Breach: Unauthorized access leading to exposure of sensitive data.	- Sensitive customer data.	- Weak authentication. - Insufficient access control. - Unencrypted data in transit.	- Implement strong access controls. - Encrypt sensitive data at rest and in transit. - Regularly monitor and audit access logs.
Data Loss: Accidental or intentional deletion or corruption of data.	- Critical data.	- Lack of data backup. - Inadequate version control.	- Implement backup and recovery procedures. - Use versioning for critical data. - Regularly test data recovery processes.
Insider Threats: Malicious actions by employees or trusted entities.	- Sensitive data. - Intellectual property.	- Lack of employee training. - Excessive user privileges.	- Employee training. - Principle of least privilege. - User behavior analytics
Malware: Malicious software compromising application integrity	- Application data. - Sensitive files.	- Unpatched software. - Lack of antivirus measures.	- Regular patch management. - Antivirus software.
Account Hijacking: Unauthorized access to user accounts.	- User accounts. - Access credentials.	- Weak passwords. - Phishing attacks.	- Multi-factor authentication. - Strong password policies.
Phishing: Deceptive attempts to obtain sensitive information.	- User credentials. - Sensitive information.	- Lack of user awareness. - Insufficient email security.	- Security awareness training. - Email filtering.
Man-in-the-Middle (MitM) Attacks: Intercepting and manipulating communication between parties.	- Data transmitted over networks. - User credentials.	- Unencrypted communication. - Compromised network devices.	- Encryption. - Secure communication protocols.



PASSWORDS POLICIES

0000

0000

PASSWORDS POLICIES

Requirement	Solution
Should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character, and a number.	Implement a password policy that requires users to use a combination of these types of characters in their passwords.
Change passwords every 90 days and ensure that the previous three passwords can't be reused.	<ul style="list-style-type: none">-Set up a password expiration policy in the system.-Implement a password history feature in the system to keep track of the previous passwords used by a user.
Administrator sign-in to the Management Console requires the use of Virtual MFA	Set up Virtual MFA for each administrator in the system. This would require administrators to use a virtual MFA device to generate a code as part of the sign-in process.



0000

ACCESS RIGHT

- Group System Administrator
- Group Data Base Administrator
- Group Monitor



GROUP SYSTEM ADMINISTRATOR

- Infrastructure as Code (IaC) deployment tools.
- Compute resources management.
- Networking configuration.
- Full access to databases.
- Storage management.
- Identity and access management.





GROUP DATA BASE ADMINISTRATOR

- Database creation and management.
- Database optimization and performance tuning.
- Database backup and recovery.
- Limited access to compute resources.
- Read-only access to storage.





GROUP MONITOR

- Monitoring and logging tools configuration.
- Access to performance metrics.
- Log analysis and reporting.
- Read-only access to databases for monitoring purposes.
- Read-only access to storage



04

IMPLEMENTATION

Implementation in
AWS

VPC

VPC > Your VPCs > vpc-0413b512a5c9162f0

vpc-0413b512a5c9162f0 / us-east-vpc

Actions ▾

Details		Info	
VPC ID	<input type="button" value="vpc-0413b512a5c9162f0"/>	State	Available
Tenancy	Default	DHCP option set	dopt-0ee8bf761a7dc1f9d
Default VPC	No	IPv4 CIDR	10.0.0.0/16
Network Address Usage metrics	Disabled	Route 53 Resolver DNS	Failed to load rule groups
		Firewall rule groups	
		Owner ID	<input type="button" value="679027451723"/>
		DNS hostnames	Disabled
		Main route table	rtb-029101783dcbaef41a
		IPv6 pool	-
		IPv6 CIDR (Network border group)	-
		DNS resolution	Enabled
		Main network ACL	acl-0f6be507e129ac267



SUBNET AND ROUTE TABLES

VPC > Your VPCs > vpc-0413b512a5c9162f0

vpc-0413b512a5c9162f0 / us-east-vpc

Actions ▾

Details		Info	
VPC ID	vpc-0413b512a5c9162f0	State	Available
Tenancy	Default	DHCP option set	dopt-0ee8bf761a7dc1f9d
Default VPC	No	IPv4 CIDR	10.0.0.0/16
Network Address Usage metrics	Disabled	Route 53 Resolver DNS Firewall rule groups	Failed to load rule groups
DNS hostnames			
Disabled		Enabled	
Main route table			
rtb-029101783dcba41a		acl-0f6be507e129ac267	
IPv6 pool			
-		-	
Owner ID			
679027451723			

Resource map New | CIDRs | Flow logs | Tags | Integrations

Resource map Info

VPC Show details Your AWS virtual network
us-east-vpc

Was the resource map helpful today? Give us feedback as often as possible. We are improving continually.

Subnets (6) Subnets within this VPC

- us-east-1a
 - us-east-vpc-subnet-public-az1
 - us-east-vpc-subnet-private1-az1
 - us-east-vpc-subnet-private2-az1
- us-east-1b
 - us-east-vpc-subnet-public-az2
 - us-east-vpc-subnet-private2-az2
 - us-east-vpc-subnet-private1-az2

Route tables (4) Route network traffic to resources

- public-route-table
- privateRT-az2
- rtb-029101783dcba41a
- privateRT-az1

Network connections (3) Connections to other networks

- app-learning
- gatway-az1
- gatway-az2

```
graph LR; sub1[Subnets (6)] --- sub1a[us-east-1a]; sub1 --- sub1b[us-east-1b]; sub1a --- sub1a1[us-east-vpc-subnet-public-az1]; sub1a --- sub1a2[us-east-vpc-subnet-private1-az1]; sub1a --- sub1a3[us-east-vpc-subnet-private2-az1]; sub1b --- sub1b1[us-east-vpc-subnet-public-az2]; sub1b --- sub1b2[us-east-vpc-subnet-private2-az2]; sub1b --- sub1b3[us-east-vpc-subnet-private1-az2]; sub2[Route tables (4)] --- rtb1[public-route-table]; sub2 --- rtb2[privateRT-az2]; sub2 --- rtb3[rtb-029101783dcba41a]; sub2 --- rtb4[privateRT-az1]; sub3[Network connections (3)] --- nc1[app-learning]; sub3 --- nc2[gatway-az1]; sub3 --- nc3[gatway-az2]; style sub1 fill:#f0f0f0; style sub2 fill:#f0f0f0; style sub3 fill:#f0f0f0; style sub1a fill:#e0e0e0; style sub1b fill:#e0e0e0; style sub1a1 fill:#e0e0e0; style sub1a2 fill:#e0e0e0; style sub1a3 fill:#e0e0e0; style sub1b1 fill:#e0e0e0; style sub1b2 fill:#e0e0e0; style sub1b3 fill:#e0e0e0; style rtb1 fill:#e0e0e0; style rtb2 fill:#e0e0e0; style rtb3 fill:#e0e0e0; style rtb4 fill:#e0e0e0; style nc1 fill:#e0e0e0; style nc2 fill:#e0e0e0; style nc3 fill:#e0e0e0;
```



SUBNET AND ROUTE TABLES

The screenshot displays two AWS VPC management interfaces side-by-side.

Left Panel (VPC Details):

- VPC ID:** vpc-0413b512a5c9162f0
- Tenancy:** Default
- Default VPC:** No
- Network Address Usage metrics:** Disabled

Right Panel (Route Table Details):

- Route table ID:** rtb-0b6ea96dfd3436f11
- Main:** No
- VPC:** vpc-0413b512a5c9162f0 | us-east-vpc
- Owner ID:** 679027451723
- Explicit subnet associations:** 2 subnets
- Edge associations:** -

Bottom Section (Routes):

Destination	Target	Status
0.0.0.0/0	igw-01e8eb441028307fd	Active
10.0.0.0/16	local	Active



SECURITY GROUPS

Security Groups (9) [Info](#) Actions ▾ Export security groups to CSV ▾ [Create security group](#)

Find resources by attribute or tag < 1 >

<input type="checkbox"/>	Name	▼	Security group ID	▼	Security group name	▼	VPC ID
<input type="checkbox"/>	InternetFacing-lb		sg-0ae809277ce51f23f		InternetFacing-lb		vpc-0413b512a5c91
<input type="checkbox"/>	-		sg-01e0a26e441111ec5		default		vpc-00b291a26541
<input type="checkbox"/>	-		sg-0828a3cc45fd678b8		internal-lb		vpc-0413b512a5c91
<input type="checkbox"/>	-		sg-0c055ea9b32937920		db-sg		vpc-0413b512a5c91
<input type="checkbox"/>	-		sg-0f0262cfaadceb52		default		vpc-0413b512a5c91
<input type="checkbox"/>	webTier		sg-0b7e801f97804f75b		webTier		vpc-0413b512a5c91
<input type="checkbox"/>	-		sg-050245a0fc75e9efc		launch-wizard-1		vpc-0413b512a5c91



SECURITY GROUPS

Security Groups (9) [Info](#)

[C](#) Actions ▾ Export security groups to CSV ▾ [Create security group](#)

Find sg-0ae809277ce51f23f - InternetFacing-lb [Actions](#) ▾

Details	
Security group name InternetFacing-lb	Security group ID sg-0ae809277ce51f23f
Owner 679027451723	Description InternetFacing-lb
	Inbound rules count 3 Permission entries
	Outbound rules count 1 Permission entry

[Inbound rules](#) [Outbound rules](#) [Tags](#)

Inbound rules (3)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0c13a510abd01d9...	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
-	sgr-0ca6218002cb520...	IPv4	Custom TCP	TCP	0	196.65.203.78/32	-
-	sgr-05df5e97694acdeb2	IPv4	HTTP	TCP	80	0.0.0.0/0	-



INTERNET GATWAY

Details [Info](#)

Internet gateway ID igw-01e8eb441028307fd	State Attached	VPC ID vpc-0413b512a5c9162f0 us-east-vpc	Owner 679027451723
--	--------------------------------	---	---------------------------------------

NAT gateways (2) [Info](#)

Name	NAT gateway ID	Connectivit...	State	State message	P
gatway-az1	nat-0ea2212cbf0a9d70a	Public	Available	-	3
gatway-az2	nat-0d019c9e16b572e4a	Public	Available	-	5

[VPC](#) > [NAT_gateways](#) > [nat-0ea2212cbf0a9d70a](#)

nat-0ea2212cbf0a9d70a / gatway-az1

Actions ▾

Details [Info](#)

NAT gateway ID nat-0ea2212cbf0a9d70a	Connectivity type Public	State Available	State message Info -
NAT gateway ARN arn:aws:ec2:us-east-1:679027451723:natgateway/nat-0ea2212cbf0a9d70a	Primary public IPv4 address 34.197.191.211	Primary private IPv4 address 10.0.0.16	Primary network interface ID eni-003f09268e021d335
VPC vpc-0413b512a5c9162f0 / us-east-vpc	Subnet subnet-0f3c1234a5128276d / us-east-vpc-subnet-public-az1	Created Monday, 1 January 2024 at 02:21:10 GMT+1	Deleted -



DATA BASE SUBNET

RDS > Subnet groups > db-subnet-group

db-subnet-group

Subnet group details	
VPC ID	vpc-0413b512a5c9162f0
ARN	arn:aws:rds:us-east-1:679027451723:subgrp:db-subnet-group
Supported network types	IPv4
Description	db-subnet-group



SECURITY GROUPS

Security Groups (9) [Info](#)

[C](#) Actions ▾ Export security groups to CSV ▾ [Create security group](#)

Find sg-0ae809277ce51f23f - InternetFacing-lb [Actions ▾](#)

Details	
Security group name InternetFacing-lb	Security group ID sg-0ae809277ce51f23f
Owner 679027451723	Description InternetFacing-lb
	Inbound rules count 3 Permission entries
	Outbound rules count 1 Permission entry

[Inbound rules](#) [Outbound rules](#) [Tags](#)

Inbound rules (3)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0c13a510abd01d9...	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
-	sgr-0ca6218002cb520...	IPv4	Custom TCP	TCP	0	196.65.203.78/32	-
-	sgr-05df5e97694acdeb2	IPv4	HTTP	TCP	80	0.0.0.0/0	-



EC2 INSTANCES

Instances (7) [Info](#)

[C](#) [Connect](#) [Instance state ▾](#) [Actions ▾](#) [Launch instances ▾](#)

Find Instance by attribute or tag (case-sensitive)

[Instance state = running](#) [X](#) [Clear filters](#)

<input type="checkbox"/>	Name ✎	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	appTier4-az1	i-0b88b040194d2445c	Running Q Q	t2.micro	2/2 checks passed View alarms +	View alarm	us-east-1a
<input type="checkbox"/>	appTier3-az1	i-0000346f5746de407	Running Q Q	t2.micro	2/2 checks passed View alarm	View alarm	
<input type="checkbox"/>	appTier5-az1	i-025ae8467bc5ccd10	Running Q Q	t2.micro	2/2 checks passed View alarm	View alarm	
<input type="checkbox"/>		i-0e574743f14446819	Running Q Q	t2.micro	2/2 checks passed View alarm	View alarm	
<input type="checkbox"/>	appTier1-az1	i-0707cbd3111772ab5	Running Q Q	t2.micro	2/2 checks passed View alarm	View alarm	
<input type="checkbox"/>	appTier2-az1	i-05d1fe30ba96f7fc5	Running Q Q	t2.micro	2/2 checks passed View alarm	View alarm	

Instance summary for i-0b88b040194d2445c (appTier4-az1) [Info](#)

Updated less than a minute ago

Instance ID i-0b88b040194d2445c (appTier4-az1)	Public IPv4 address -	Private IPv4 addresses 10.0.1.76
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-10-0-1-76.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-1-76.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address -	VPC ID vpc-0413b512a5c9162f0 (us-east-vpc)	Learn more Learn more
IAM Role No roles attached to instance profile: ec2-roles	Subnet ID subnet-05e945806ea6818c1 (us-east-vpc-subnet-private1-az1)	Auto Scaling Group name -



EC2 INSTANCES

Instances (7) [Info](#)

[Find Instance by attribute or tag \(case-sensitive\)](#)

[Instance state = running](#) [Clear filters](#)

Name	Instance ID	Instance state	Instance type
appTier4-az1	i-0b88b040194d2445c	Running	t2.micro
appTier3-az1	i-0000346f5746de407	Running	t2.micro
appTier5-az1	i-025ae8467bc5ccd10	Running	t2.micro
	i-0e574743f14446819	Running	t2.micro
appTier1-az1	i-0707cbd3111772ab5	Running	t2.micro
appTier2-az1	i-05d1fe30ba96f7fc5	Running	t2.micro

Instance type

c5.2xlarge

Family: c5 8 vCPU 16 GiB Memory Current generation: true

On-Demand Windows base pricing: 0.708 USD per Hour

On-Demand RHEL base pricing: 0.47 USD per Hour

On-Demand Linux base pricing: 0.34 USD per Hour

On-Demand SUSE base pricing: 0.44 USD per Hour

Instance type

t3.medium

Family: t3 2 vCPU 4 GiB Memory Current generation: true

On-Demand SUSE base pricing: 0.0979 USD per Hour

On-Demand Windows base pricing: 0.06 USD per Hour

On-Demand Linux base pricing: 0.0416 USD per Hour

On-Demand RHEL base pricing: 0.1016 USD per Hour

Running

Create IP DNS name (IPv4 only)
ip-10-0-1-76.ec2.internal

Instance type
micro

Instance ID
vpc-0413b512a5c9162f0 (us-east-vpc)

Subnet ID
subnet-05e945806ea6818c1 (us-east-vpc-private1-az1)

Elastic IP addresses

AWS Compute Optimizer finding
[Opt-in to AWS Compute Optimizer for recommendations.](#)

[Learn more](#)

Auto Scaling Group name



TARGET GROUP

EC2 > Target groups

Target groups (1) [Info](#)

Actions [Create target group](#)

Filter target groups

< 1 > [Edit filters](#)

<input type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer
<input type="checkbox"/>	appTier	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/appTier/56789	80	HTTP	Instance	None associated

Target type: Instance
Protocol : Port: HTTP: 80
Protocol version: HTTP1
VPC: [vpc-0413b512a5c9162f0](#)

IP address type: IPv4
Load balancer: [None associated](#)

2 Total targets: 0 Healthy, 0 Unhealthy, 0 Anomalous

0 Unused, 0 Initial, 0 Draining

[Distribution of targets by Availability Zone \(AZ\)](#)
Select values in this table to see corresponding filters applied to the Registered targets table below.

[Targets](#) [Monitoring](#) [Health checks](#) [Attributes](#) [Tags](#)

Registered targets (2) [Info](#)

[Anomaly mitigation: Not applicable](#) [Edit](#) [Deregister](#) [Register targets](#)

Filter targets

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Anomaly detection result
<input type="checkbox"/>	i-0bd266a5093b6e282		80	us-east-1b	Unused	Target group is not co...	Normal
<input type="checkbox"/>	i-0e574743f14446819		80	us-east-1a	Unused	Target group is not co...	Normal



05

CONCLUSION

Importance of well
designed and secure
architecture



THANK YOU

