Presented by:
- NAIYM Mohammed
- AIT BOUAZZA Zaynab
- EL KOURTI Houssam

SMARTLEARN

Towards a student-centric approach

TABLE OF CONTENTS

01

INTRODUCTION

The propose and objectives of the application

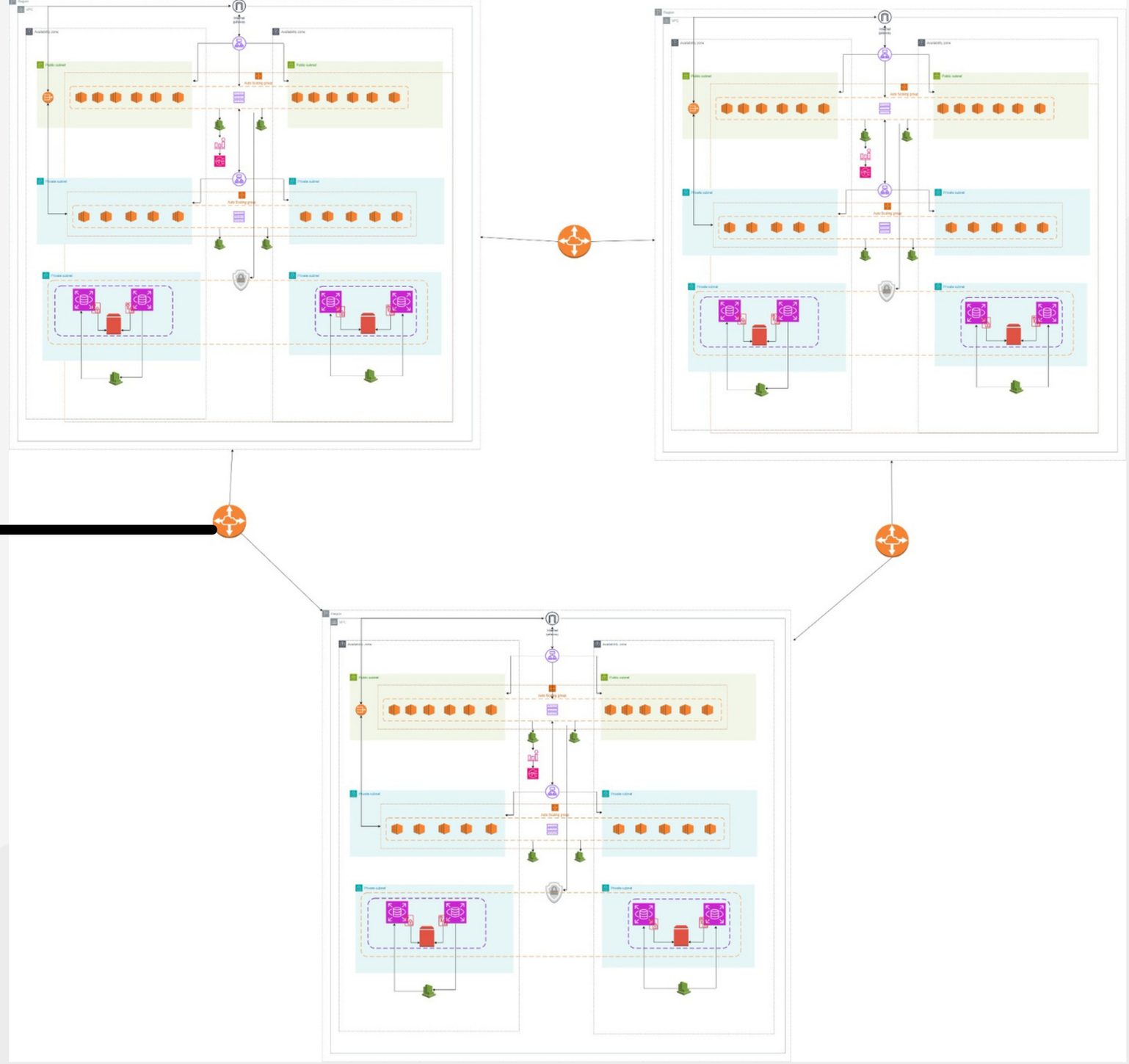
- Faciliter la communication efficace entre les étudiants et les professeurs.
- Permettant aux éducateurs d'évaluer et de prédire les performances des étudiants
- Infrastructure cloud sécurisée qui répondra à toutes les exigences de cette solution novatrice.

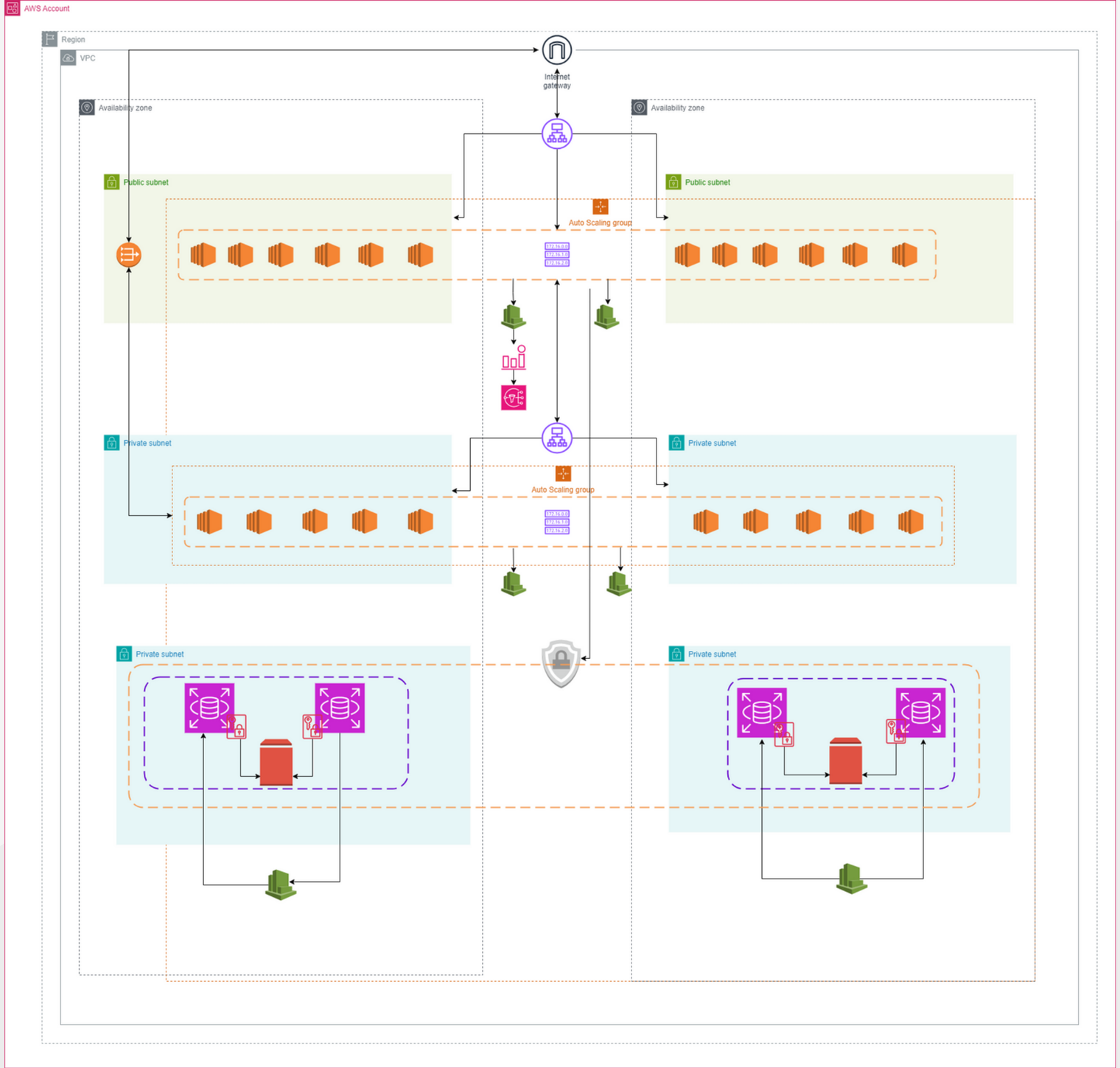
02

ARCHITECTURE OVERVIEW

The overall architecture of the application

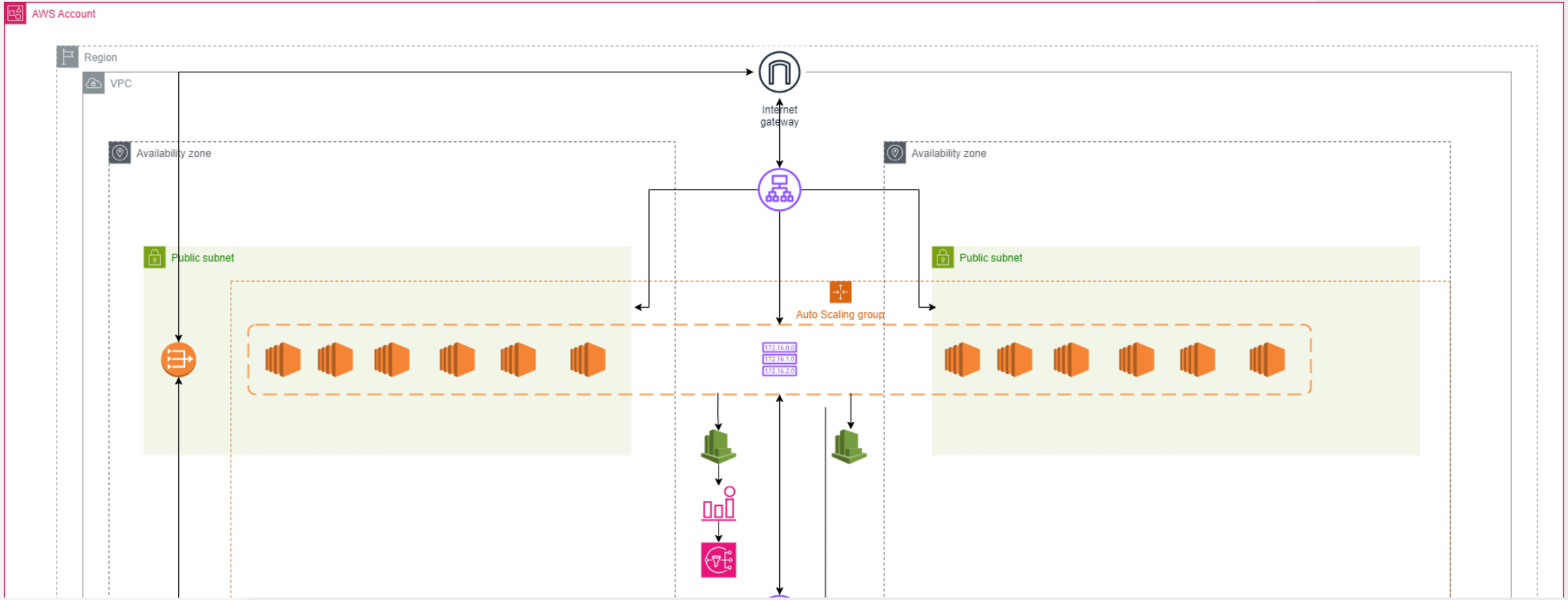
peering connection




AWS Account
Region
VPC
Internet gateway
Availability zone
Availability zone
Public subnet
Public subnet
Auto Scaling group
Private subnet
Private subnet
Auto Scaling group
Private subnet
Private subnet

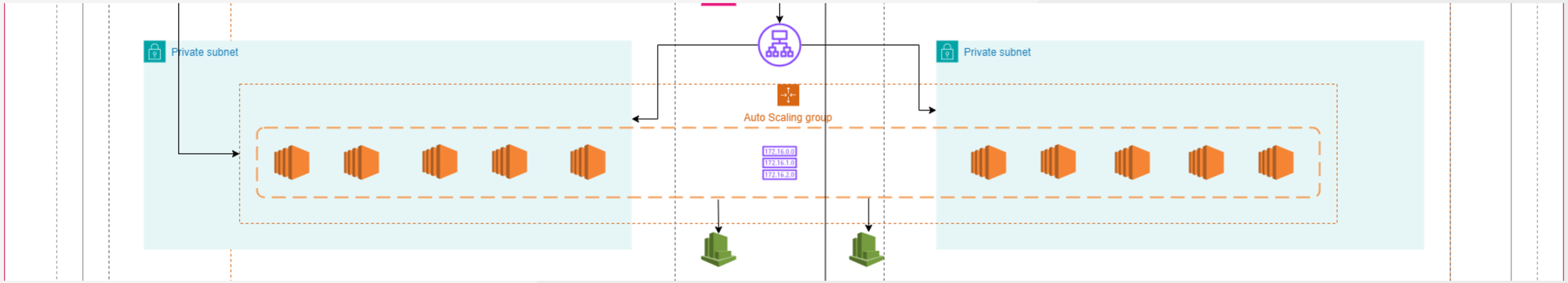
WEB TIER REQUIREMENTS

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


AWS Account
Region
VPC
Internet gateway
Availability zone
Availability zone
Public subnet
Public subnet
Auto Scaling group
172.16.0.0
172.16.1.0
172.16.2.0

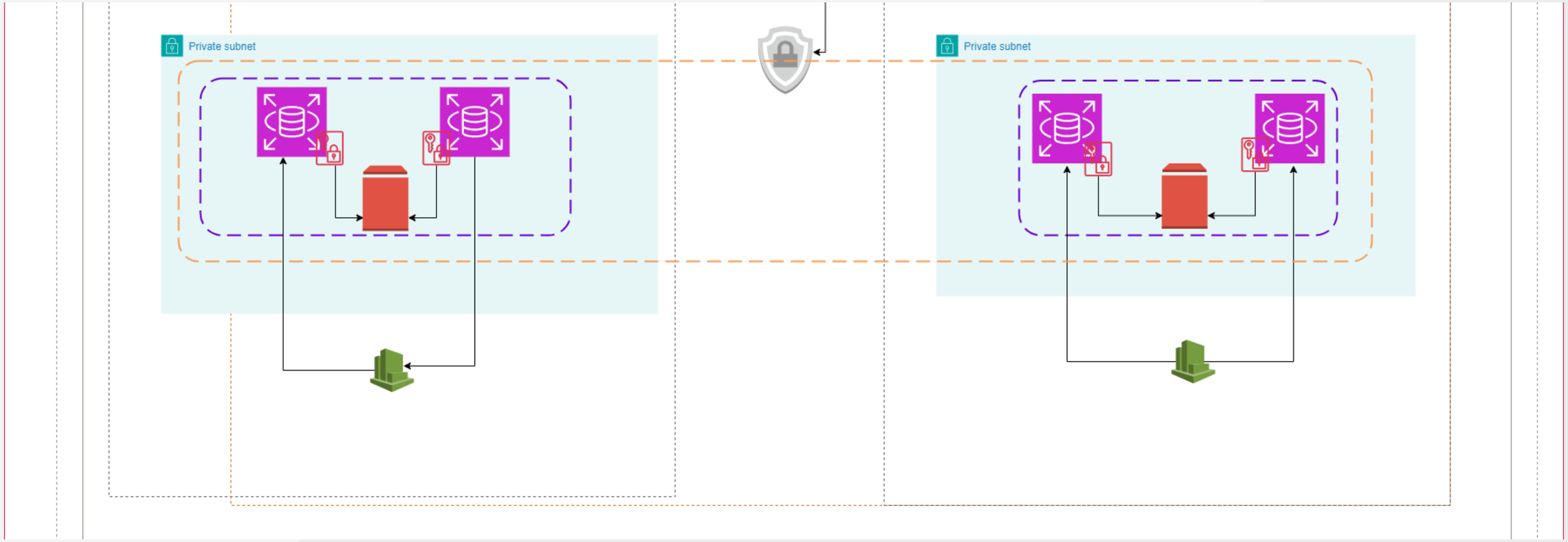
APPLICATION TIER REQUIREMENTS

Requirement	Solution
Architecture must be flexible and handle any peak in traffic or performance	- 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.


Private subnet
Private subnet
Auto Scaling group
172.16.0.0
172.16.1.0
172.16.2.0

DATABASETIER REQUIREMENTS

Requirement	Solution
Database needs consistent storage performance at 21,000 IOPS.	• 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.


Private subnet
Private subnet

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
Distributed Denial of Service (DDoS) Attack: Disruption of web services due to a DDoS attack.	- Web servers. - Online services.	- Lack of DDoS protection - Insufficient network capacity.	- DDoS mitigation tools. - Increased network capacity with high availability. - Usage of load balancers to distribute traffic.
Insufficient Authentication and Authorization: Unauthorized access to web resources due to weak authentication and authorization controls.	- User accounts. - Sensitive data.	- Weak password policies. - Inadequate role-based access controls.	- 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

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.	-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.

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

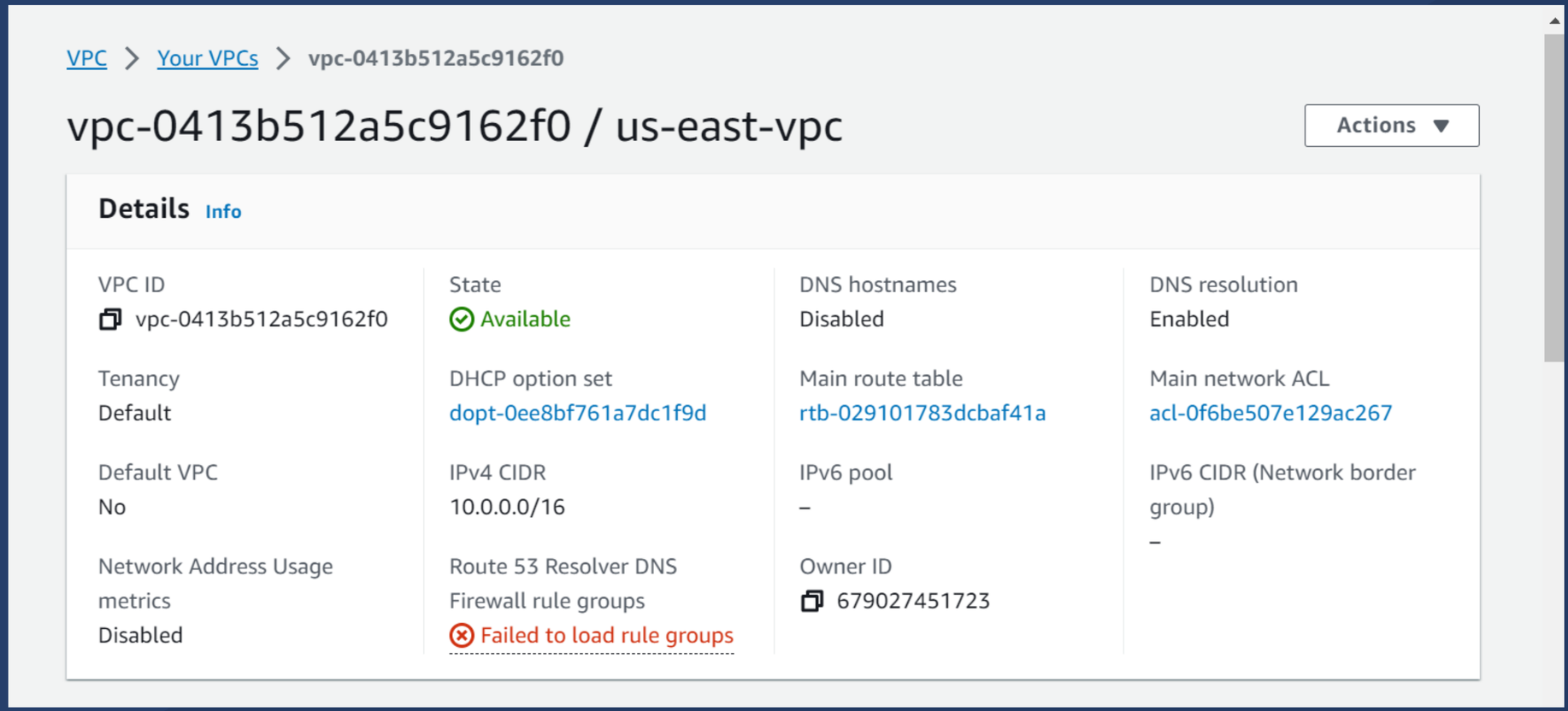
- Monitoring and logging tools configuration.
- Access to performance metrics.
- Log analysis and reporting.
- Read-only access to databases for monitoring purposes.
- Read-only access to storage

04

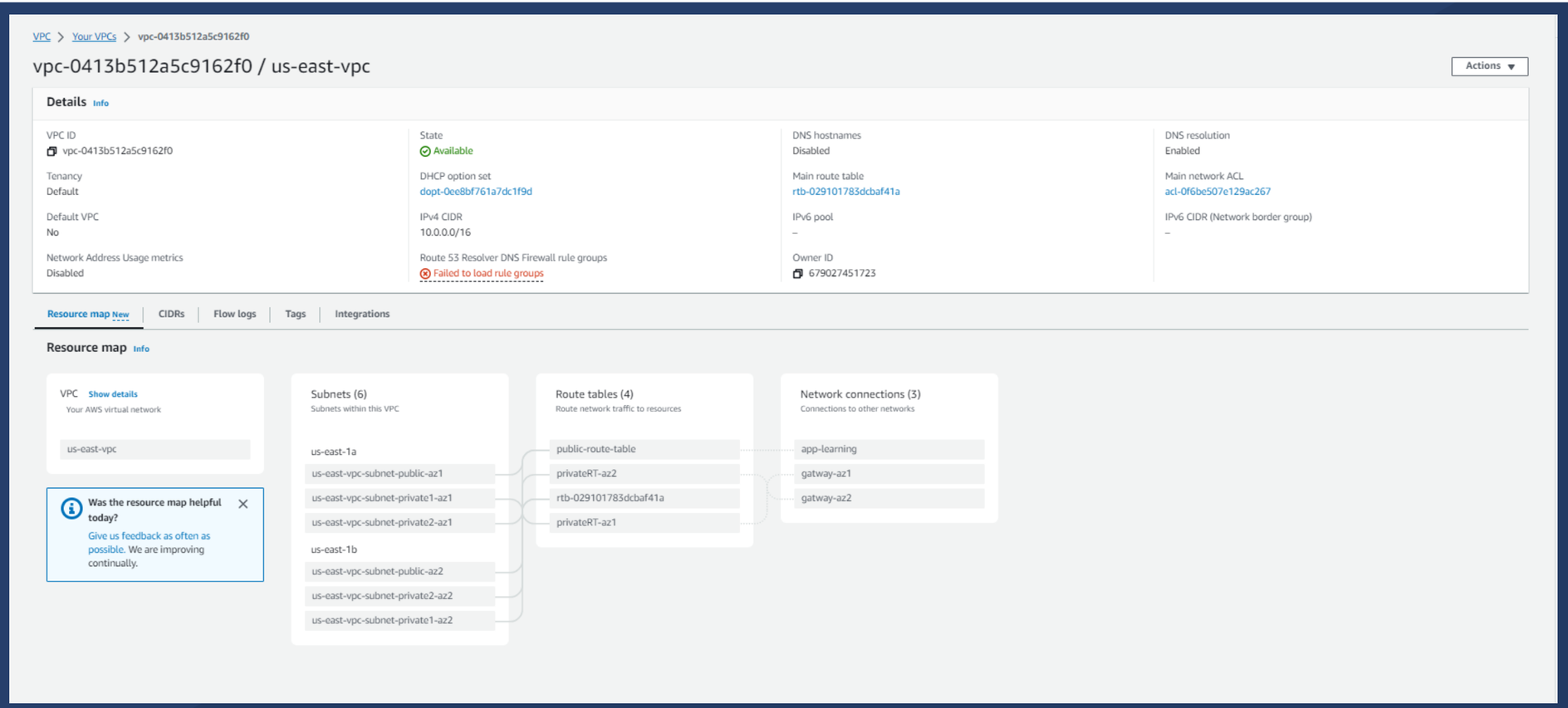
IMPLEMENTATION

Implementation in AWS

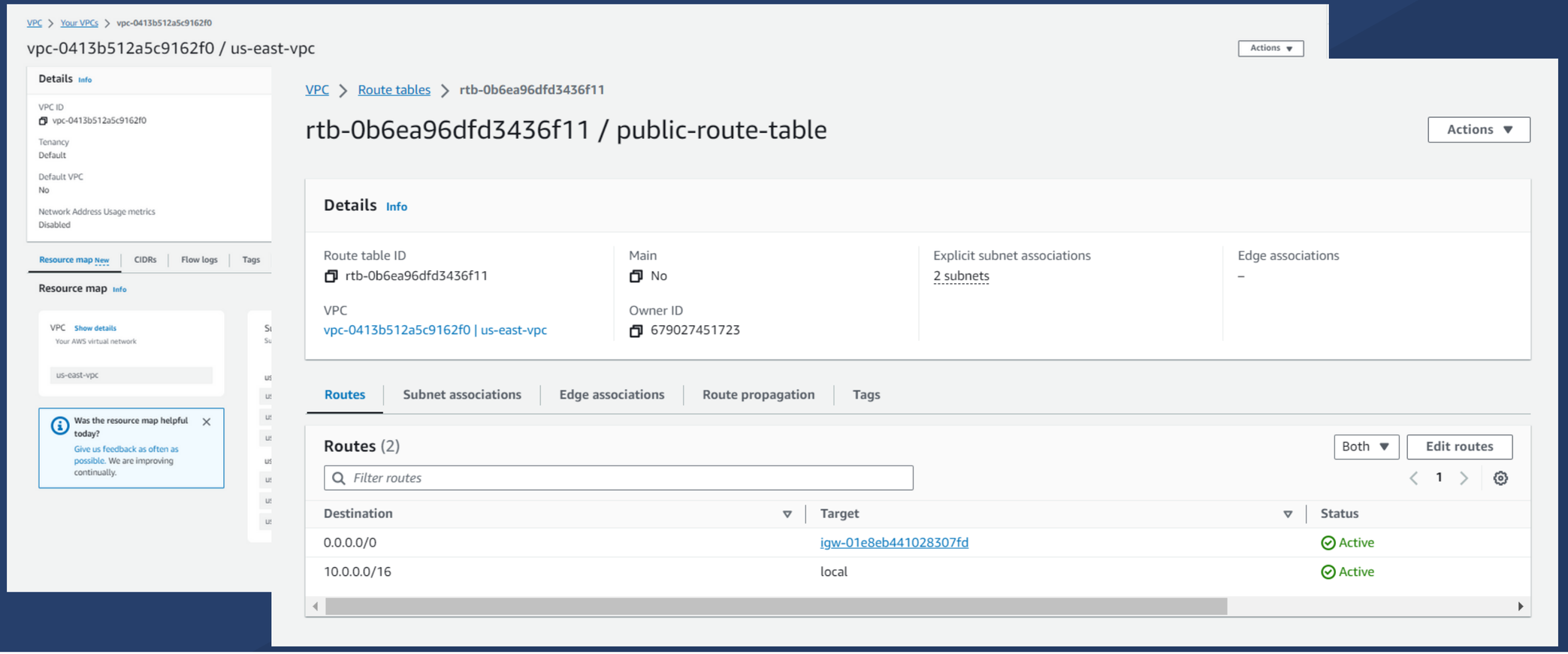
VPC


VPC > Your VPCs > vpc-0413b512a5c9162f0
vpc-0413b512a5c9162f0 / us-east-vpc
Actions
Details Info
VPC ID
vpc-0413b512a5c9162f0
State
Available
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-0ee8bf761a7dc1f9d
Main route table
rtb-029101783dcbaf41a
Main network ACL
acl-0f6be507e129ac267
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
Failed to load rule groups
Owner ID
679027451723

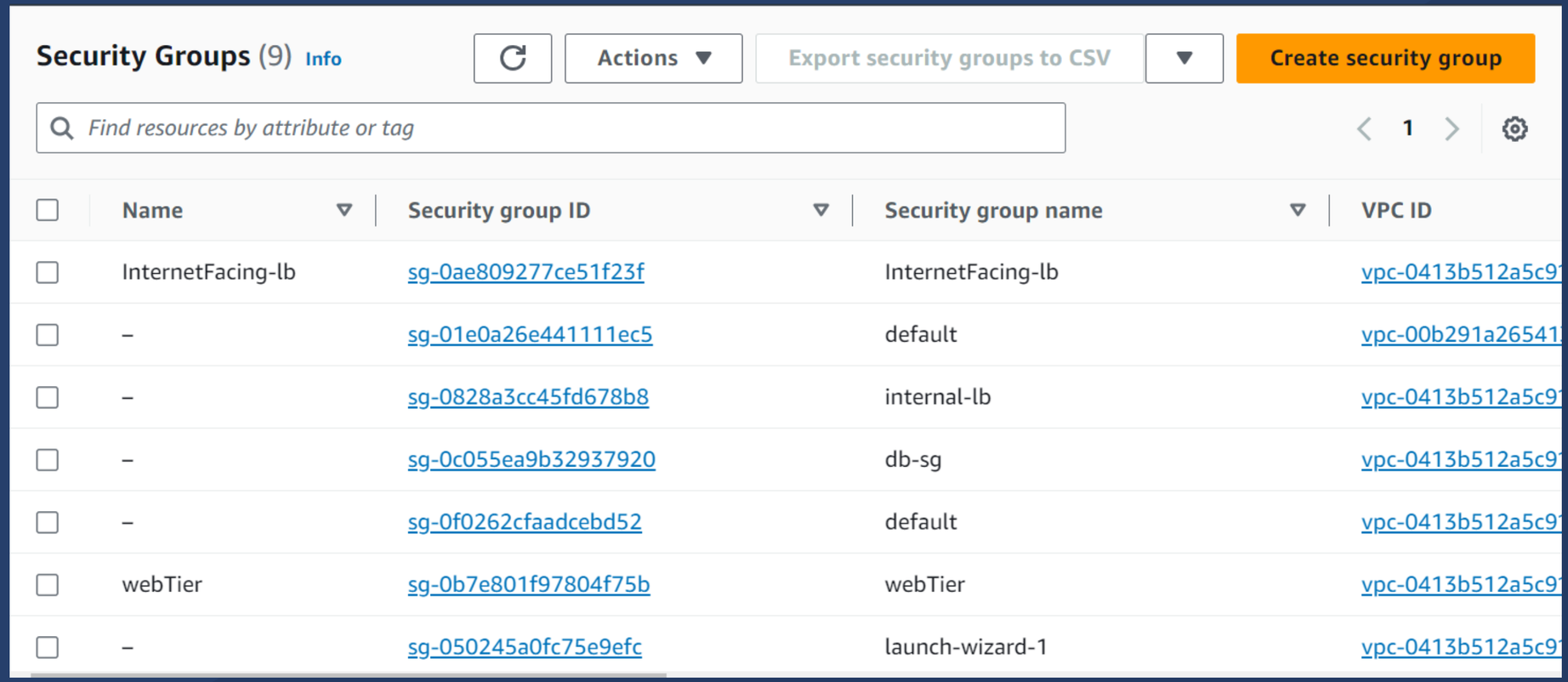
SUBNET AND ROUTE TABLES



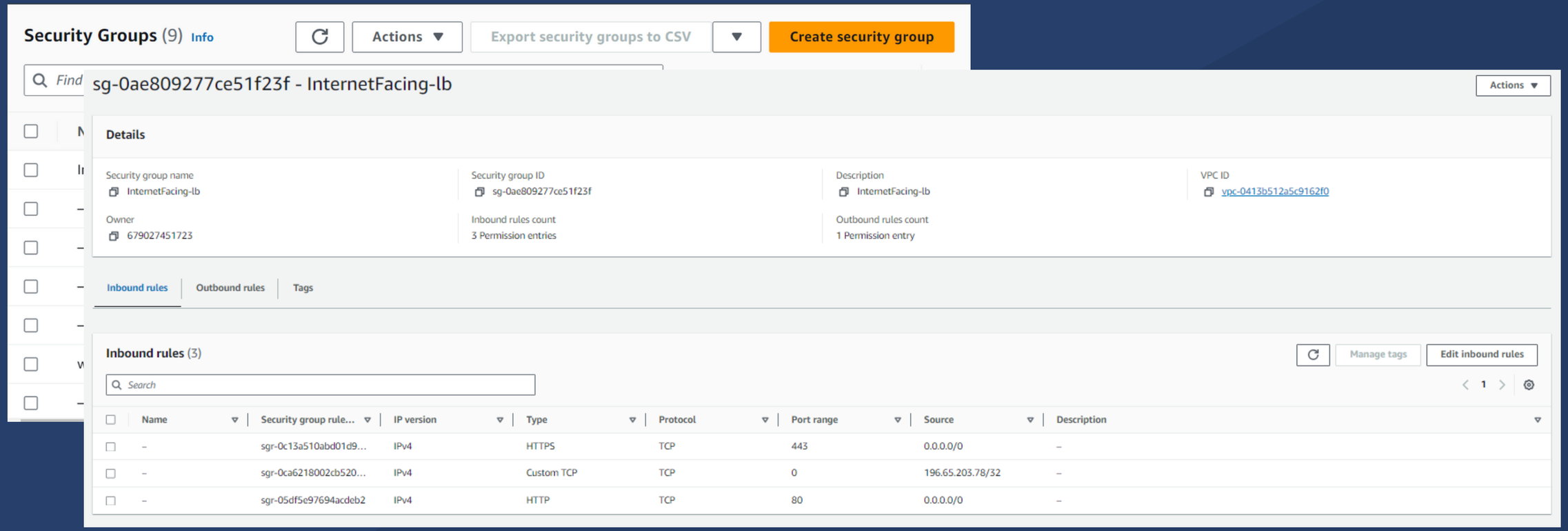
SUBNET AND ROUTE TABLES



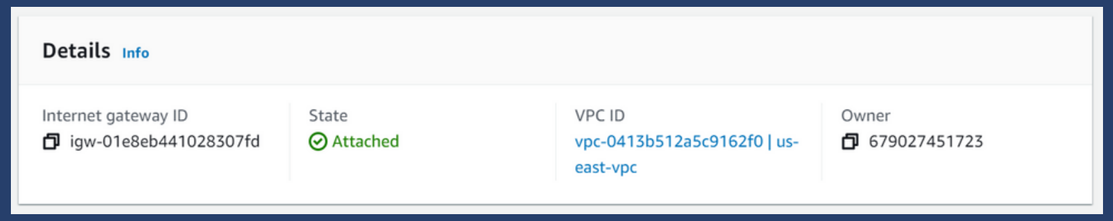
SECURITY GROUPS

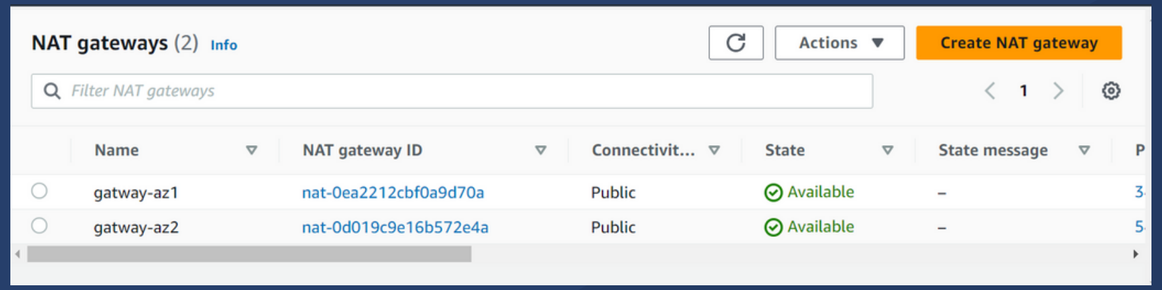


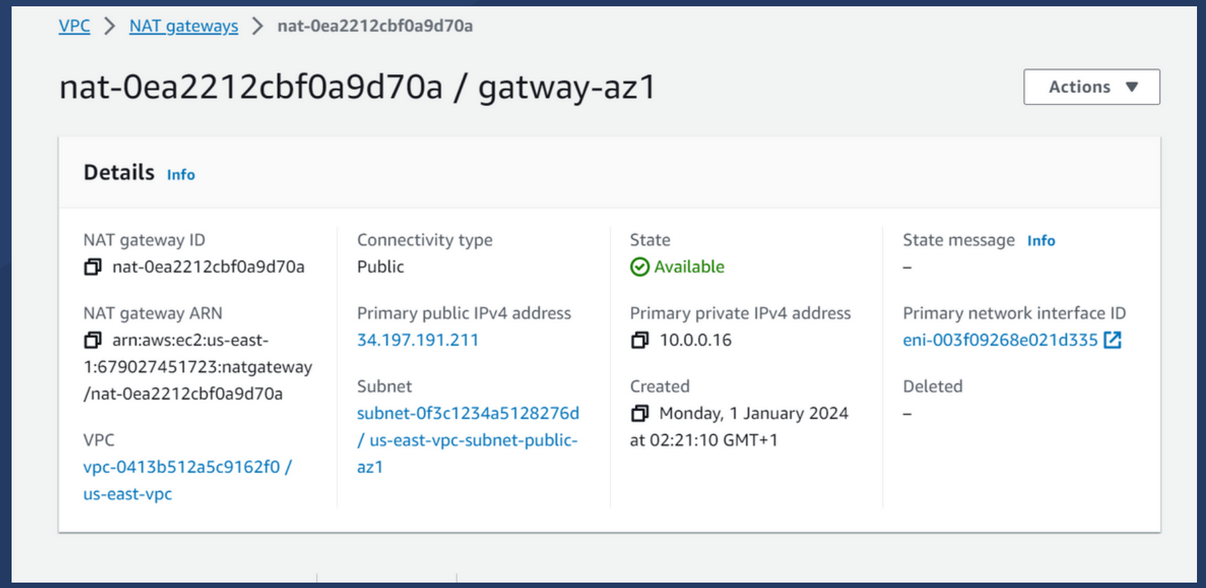
SECURITY GROUPS



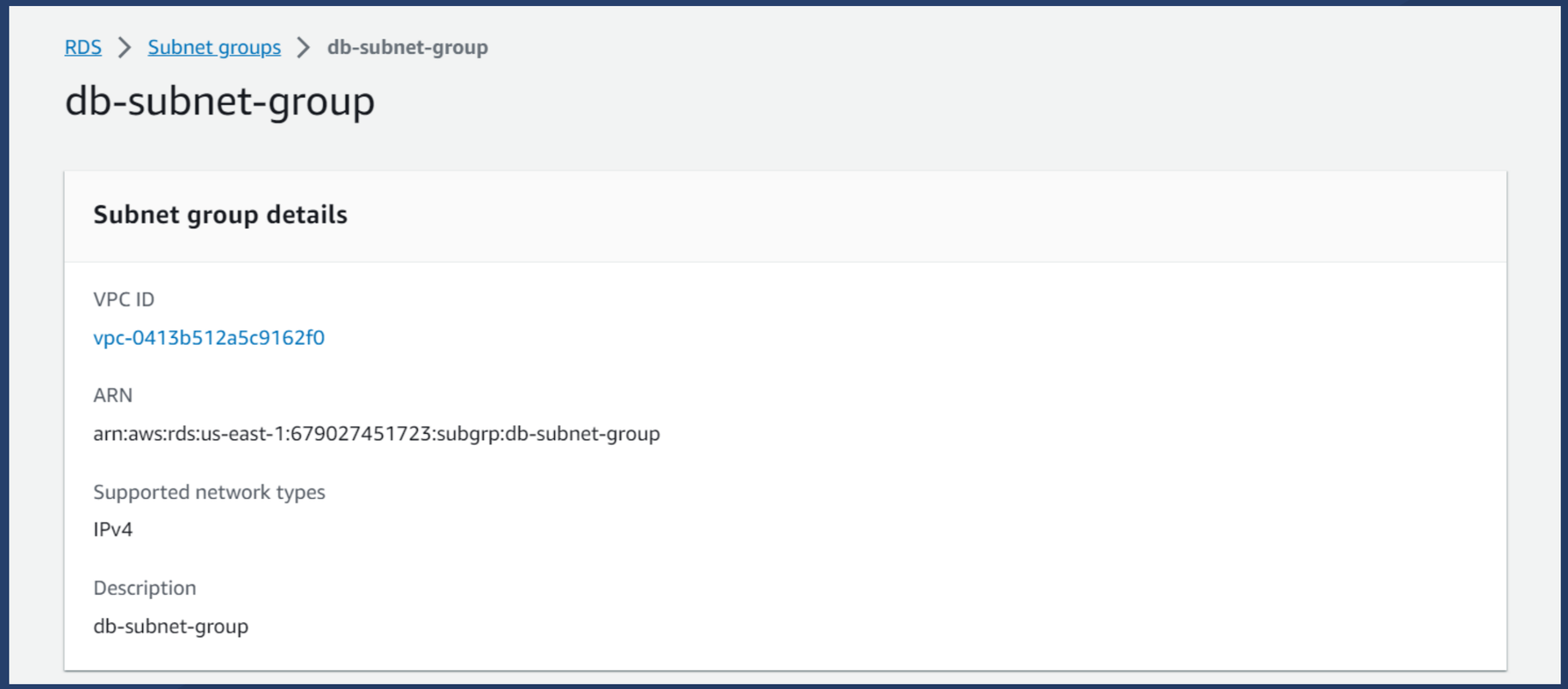
INTERNET GATWAY



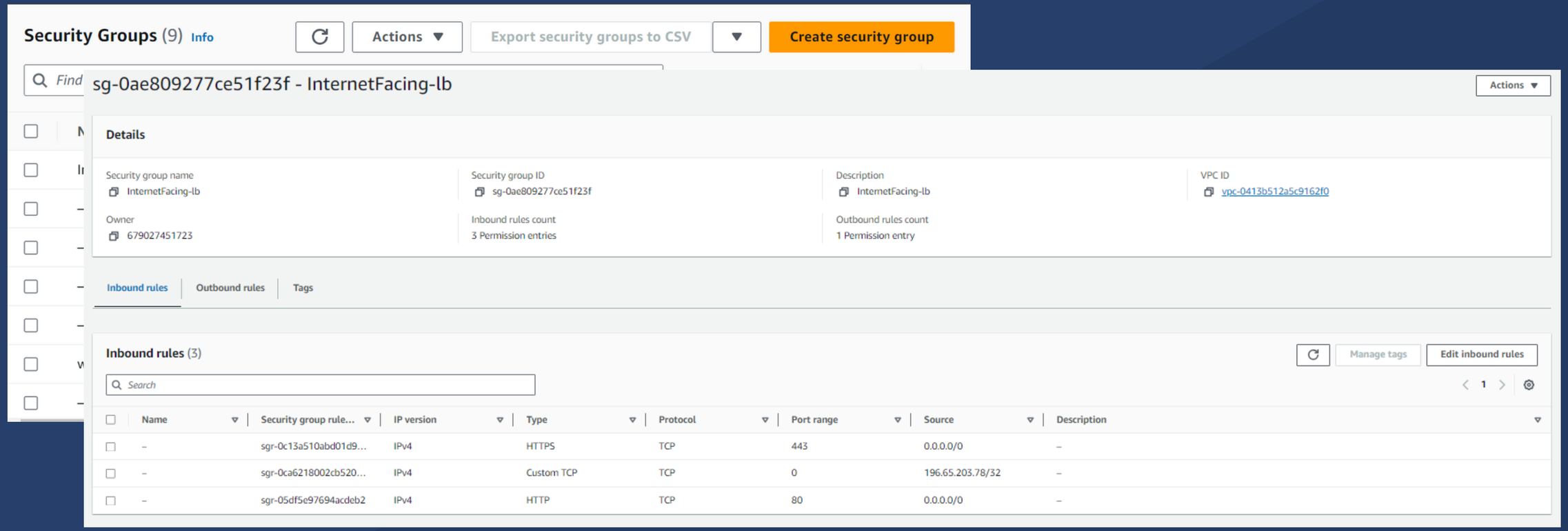




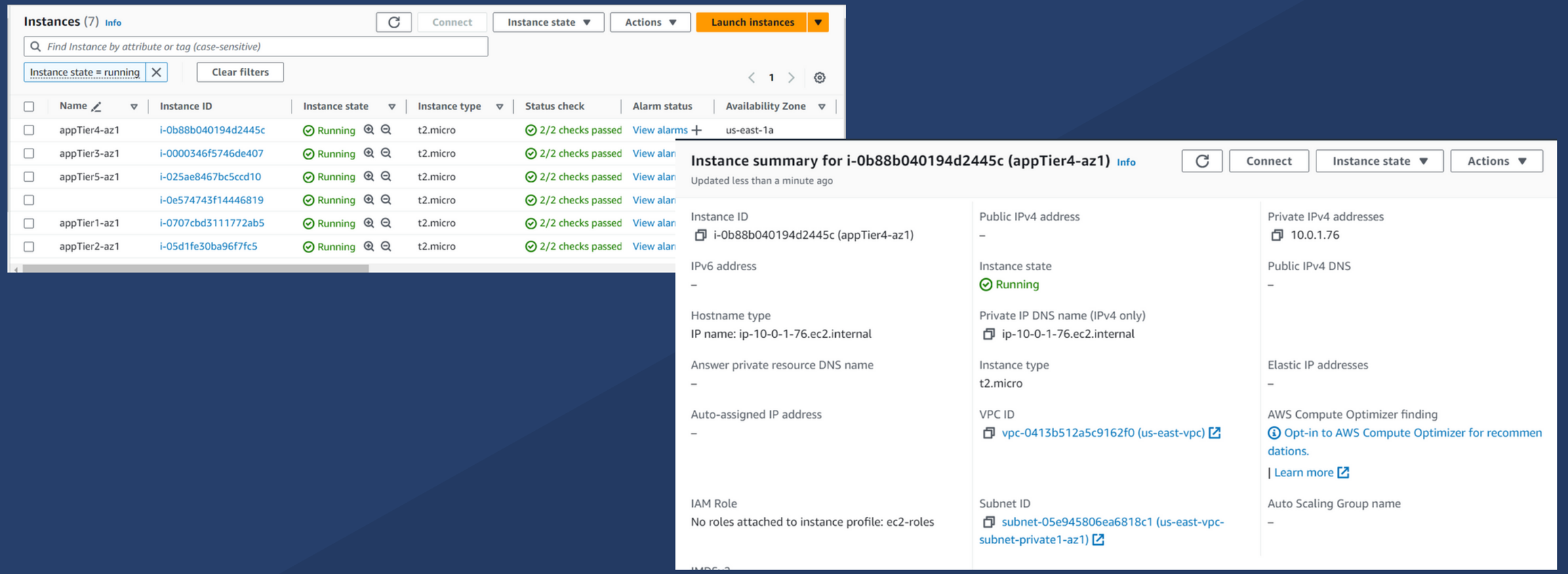
DATA BASE SUBNET



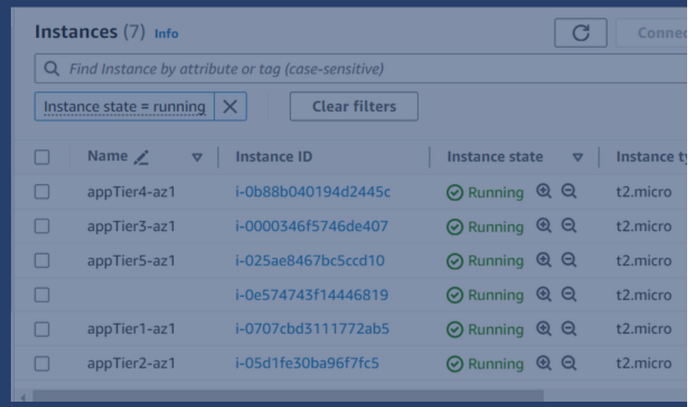
SECURITY GROUPS



EC2 INSTANCES



EC2 INSTANCES



Instance type

c5.2xlarge

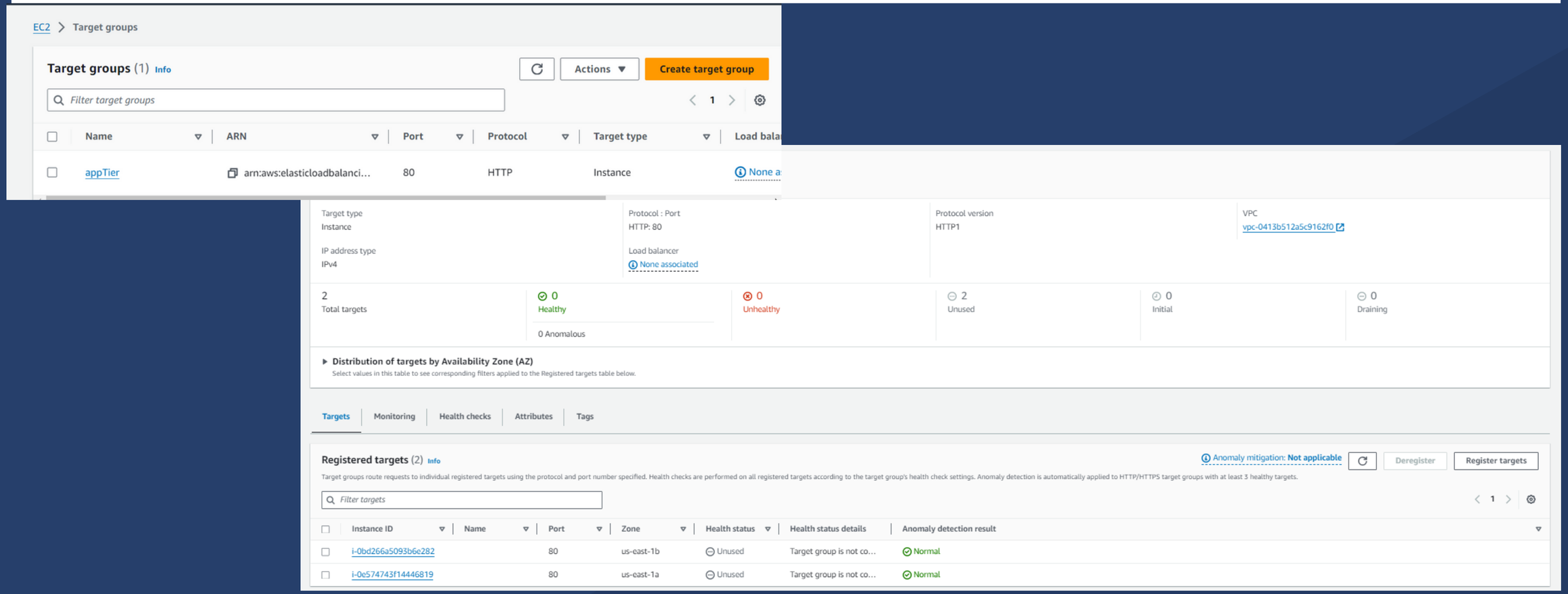
Family: c5 8 vCPU 16 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.708 USD per Hour
On-Demand RHEL base pricing: 0.47 USD per Hour
On-Demand Linux base pricing: 0.34 USD per Hour
On-Demand SUSE base pricing: 0.44 USD per Hour

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

TARGET GROUP



05

CONCLUSION

Importance of well designed and secure architecture

THANK YOU