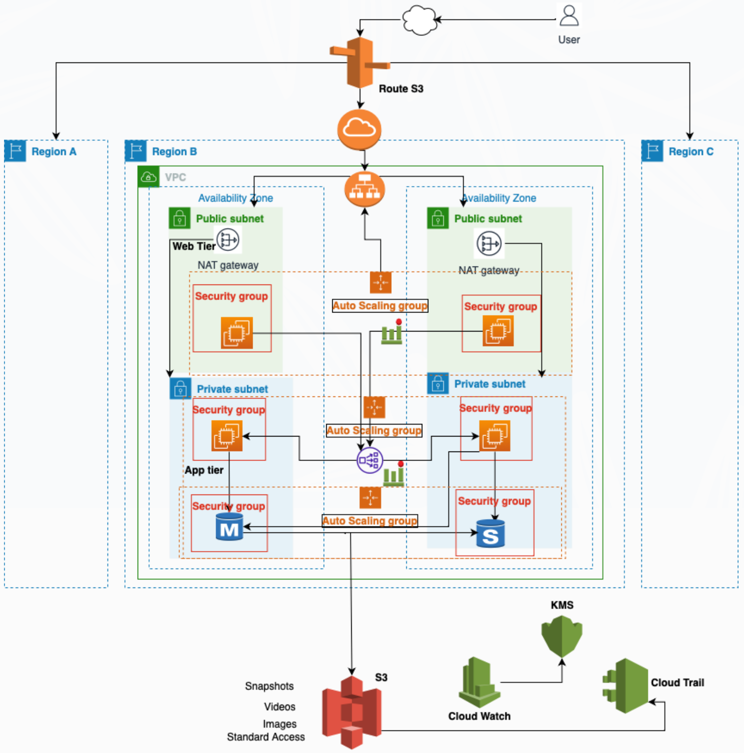
Group Midterm Project: Designing a Cloud Solution for TigerMed

Sravanth Revath Krishna Thatavarthi

Monika Tiyyagura

Trinath Sai Subhash Reddy Pittala

ARCHITECTURE PROPOSED



AWS Service Highlights

Amazon EC2:-

AWS compute service.

Auto-scaling optimizes instance count for performance.

Amazon RDS:-

Supports MS SQL server.

Features: High availability, durability, read replicas, medium read/write.

Used by NHS Digital, Moderna, Piedmont in healthcare.

Amazon Elastic Load Balancer:-

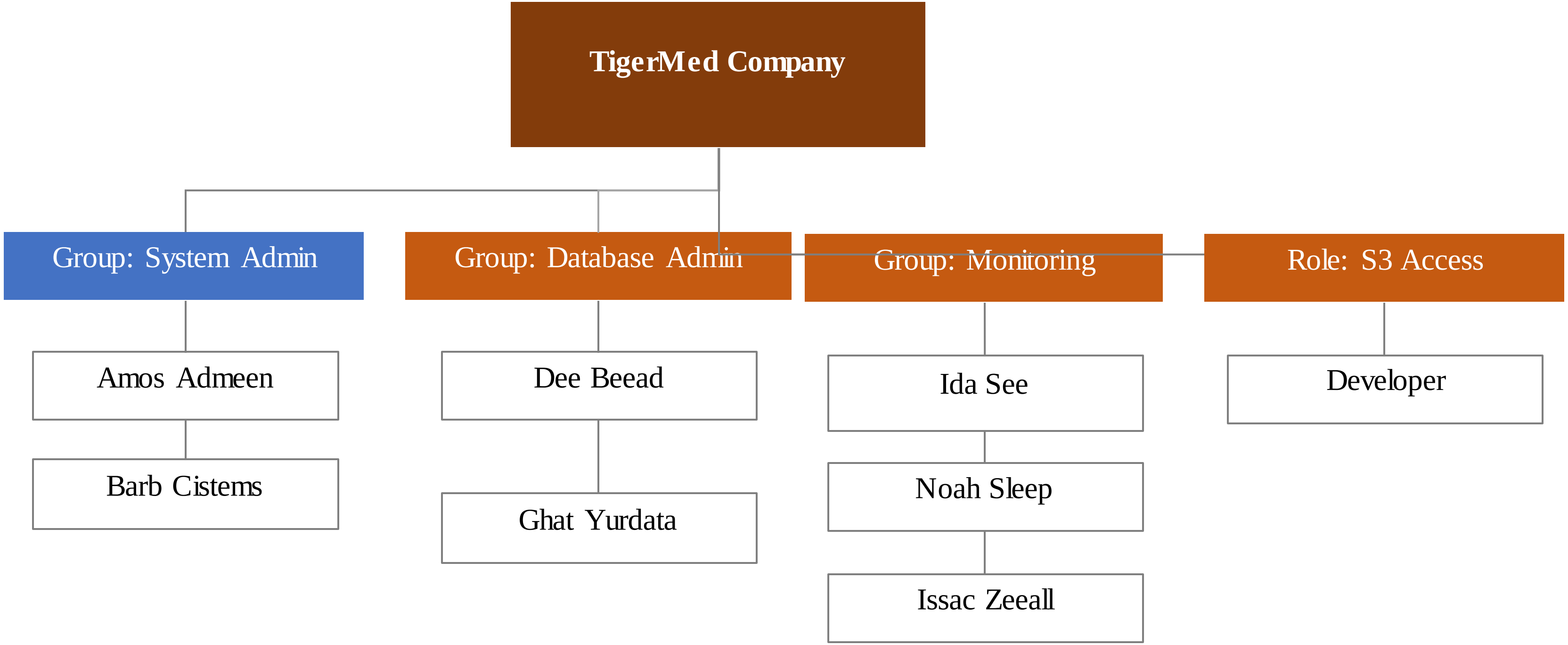
Application Load Balancer with health checks for HTTP/HTTPS.

Also functions as Network Load Balancer.

Supports TCP/UDP at network layer.

- Amazon IAM – Identity Access Management
- Amazon CloudTrail
- Amazon VPC
- Amazon KMS – Key Management Service
- Amazon S3
- Auto Scaling
- NAT Gateway – Network Access List
- Auto Scaling
- Amazon CloudWatch

Identity and Access Management



User Authentication

Group/Role #	Group/Role Name	Permissions
Group	System Admin	Comprehensive AWS access, excluding database and monitoring tools. Includes AWS Management Console and IAM groups.
Group	Database Admin	Exclusive access to AWS RDS and associated database operations.
Group	Monitoring	Dedicated access to monitoring services: CloudWatch and CloudTrail.
Role	S3 Access	Full read/write permissions for S3 Buckets.

User Authentication

<table>
<tr><th>Requirement</th><th>Solution</th></tr>
<tr><td>Passwords should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character, and a number</td><td>AWS IAM Custom Password Policy:
◦ Require at least one uppercase letter from Latin alphabet (A–Z)
◦ Require at least one lowercase letter from Latin alphabet (a–z)
◦ Require at least one non-alphanumeric character ! @ # $ % ^ &amp; * ( ) _ + - = [ ] { } | '
◦ Require at least one number</td></tr>
<tr><td>Passwords must be changed every 90 days; the last three passwords cannot be re-used</td><td>Additional requirements for the IAM Password policy:
◦ Enable password expiration - [expiration of 90 days]
◦ Prevent password reuse - [maximum of 3]</td></tr>
<tr><td>All administrators require programmatic access</td><td>◦ Create IAM groups that give programmatic access to administrators.
◦ Create IAM roles for administrative access that may be connected to any user who requires programmatic access on a need-only basis.</td></tr>
<tr><td>Administrator sign-in to the AWS Management Console requires the use of Virtual MFA</td><td>All members of the 'Admin' groups must have Multi-Factor Authentication (MFA) enabled for access.</td></tr>
</table>

Network Architecture

VPC	Region	Purpose	No of Subnets	No of AZs	VPC CIDR Range
1	US East(North Virginia)	Production Environment	4	2	10.0.0.0/16
1	US East(North Virginia)	Development Environment	4	2	10.1.0.0/16
1	US East(North Virginia)	Testing Environment	4	2	10.2.0.0/16
2	Europe(London)	Production Environment	4	2	11.0.0.0/16
2	Europe(London)	Development Environment	4	2	11.1.0.0/16
2	Europe(London)	Testing Environment	4	2	11.2.0.0/16
2	Asia Pacific(Tokyo)	Production Environment	4	2	12.0.0.0/16
2	Asia Pacific(Tokyo)	Development Environment	4	2	12.1.0.0/16
2	Asia Pacific(Tokyo)	Testing Environment	4	2	12.2.0.0/16

Subnets

Subnet Name	VPC	Subnet Type (public/private)	AZ	Subnet CIDR Range
US-web-a	#1	Public	us-east-1a	10.0.0.0/24
US-web-b	#1	Public	us-east-1b	10.0.2.0/24
US-app-a	#1	Private	us-east-1a	10.0.1.0/24
US-app-b	#1	Private	us-east-1b	10.0.3.0/24
EU-web-a	#2	Public	eu-west-2a	11.0.0.0/24
EU-web-b	#2	Public	eu-west-2b	11.0.2.0/24
EU-app-a	#2	Private	eu-west-2a	11.0.1.0/24
EU-app-b	#2	Private	eu-west-2b	11.0.3.0/24

VPC in AWS: Network Control & Security:

- VPCs provide enhanced control over cloud network configurations, enabling deployments across various regions and availability zones.
- By ensuring isolation of networking resources, VPCs significantly boost security measures.
Utilizing multiple VPCs enables distinct environments tailored for each target product deployment region.
- To enhance availability and durability, two Availability Zones (AZs) are used within each region. This approach ensures continuous operation even if one AZ experiences issues.

Subnet Name	VPC	Subnet Type (Public/private)	AZ	Subnet Type (Public/private)
ap-web-a	#3	Public	Ap-northeast-1a	12.0.0.0/24
ap-web-b	#3	Public	Ap-northeast-1b	12.0.2.0/24
ap-web-a	#3	Private	Ap-northeast-1a	12.0.1.0/24
ap-web-b	#3	Private	Ap-northeast-1b	12.0.3.0/24

Web and Application Tiers

Tier	Tags	OS	Instance Type	Size	Justification	No of instances	User Data? Y/N
Web	**Key**:name **Value**:web-tier	MS Windows	t3.medium	2cpu/4gb memory	At an affordable price, T3 instances provide the maximum performance the memory client needs.	2	N
App	**Key**:name **Value**:app-tier	MS Windows	t3.xlarge	4cpu/16gb memory	At an affordable price, T3 instances provide the maximum performance the memory client needs.	2	N
DB	**Key**:name **Value**:web-tier	MS Windows	db.t3.2xlarge	8cpu/32gb memory	At an affordable price, T3 instances provide the maximum performance the memory client needs.	2	Y

AWS Security

Service	Encryption	Details
Web-tier-sg	HTTP, HTTPS	Accessible from Anywhere
RDS	TDE (Transparent Data Encryption)	Data encryption/decryption with storage
EC2-RDS Connection	SSL/TLS	Data encrypt in transit
S3	SSE AES-256	Server-side encryption by AWS
VPC	Security, NACL	Subnets & VPC are secured

Application Load Balancers & ELB Service: Enhancing Performance and Resilience:

- Application Load Balancers efficiently distribute incoming traffic across multiple EC2 instances within an auto-scaling group, ensuring equal load distribution.
- The ELB service fortifies the architecture's resilience. Even in the face of resource failures, it ensures consistent and high-quality service delivery.

Load Balancer	Name	External/Internal	Subnets	SG Name*	Rule	Source
Web Tier	web-elb	external	us-east-web,ap-northeast-web,eu-west-web	web-elb-sg	HTTP, HTTPS	anywhere
App Tier	app-elb	internal	us-east-app,ap-northeast-app,eu-west-app	app-elb-sg	HTTP, HTTPS,TCP	Web-elb

Instance Tier	SG Name*	Rule	Source
Web Tier	web-tier-sg	HTTP, HTTPS	Anywhere
App Tier	app-tier-sg	Receives requests from load balancers in app tier on port 443	Web-tier-sg

Answering Questions

- ➢ *What do you need for a high availability environment?*

Consideration has been given to high availability for both single-region and multi-region setups. We've set up extra web and app instances and balanced their loads using an application load balancer to maintain high availability within one region. We've incorporated an auto-scaling group to adjust EC2 instances across different regions. We selected AWS RDS for its Availability Zone (AZ) deployment features. This configuration ensures high availability for our web, app, and database instances.

- ➢ *What do you need to configure automatic scaling?*

Launch template:

- AMI, Instance type and Security group.
- Auto Scaling group.
- Elastic Load Balancers (Optional).
- Scaling policies (Optional)

Auditing

- Every account needs to enable AWS CloudTrail, and it should be utilized in all supported regions.
- A centralized logging account with very restricted access stores the AWS CloudTrail logs.
- Set up a trail or event stream directing events to a chosen AWS S3 bucket to ensure logs are saved securely.
- Clients will get the necessary monitoring and operational insights from Amazon CloudWatch to review, adjust, and refine their infrastructure for maximum cost-effectiveness and efficiency.
- With this data, alerts can be set up to notify when servers become overloaded or when there are unused resources.
- Amazon Cloud Trail provides users the ability to log, oversee, and monitor account actions.

Thank You