Cloud Computing

Designing A Cloud Solution

Group Number : 17

Submission Date : 29/11/2020

Lecturer Name : Dr Basel Magableh

Student 1

Name : Daragh Murnane

Student Number : C18427384

Student 2

Name : Philip Herweling

Student Number : C18470774

Student 3

Name : Patrick Moxham

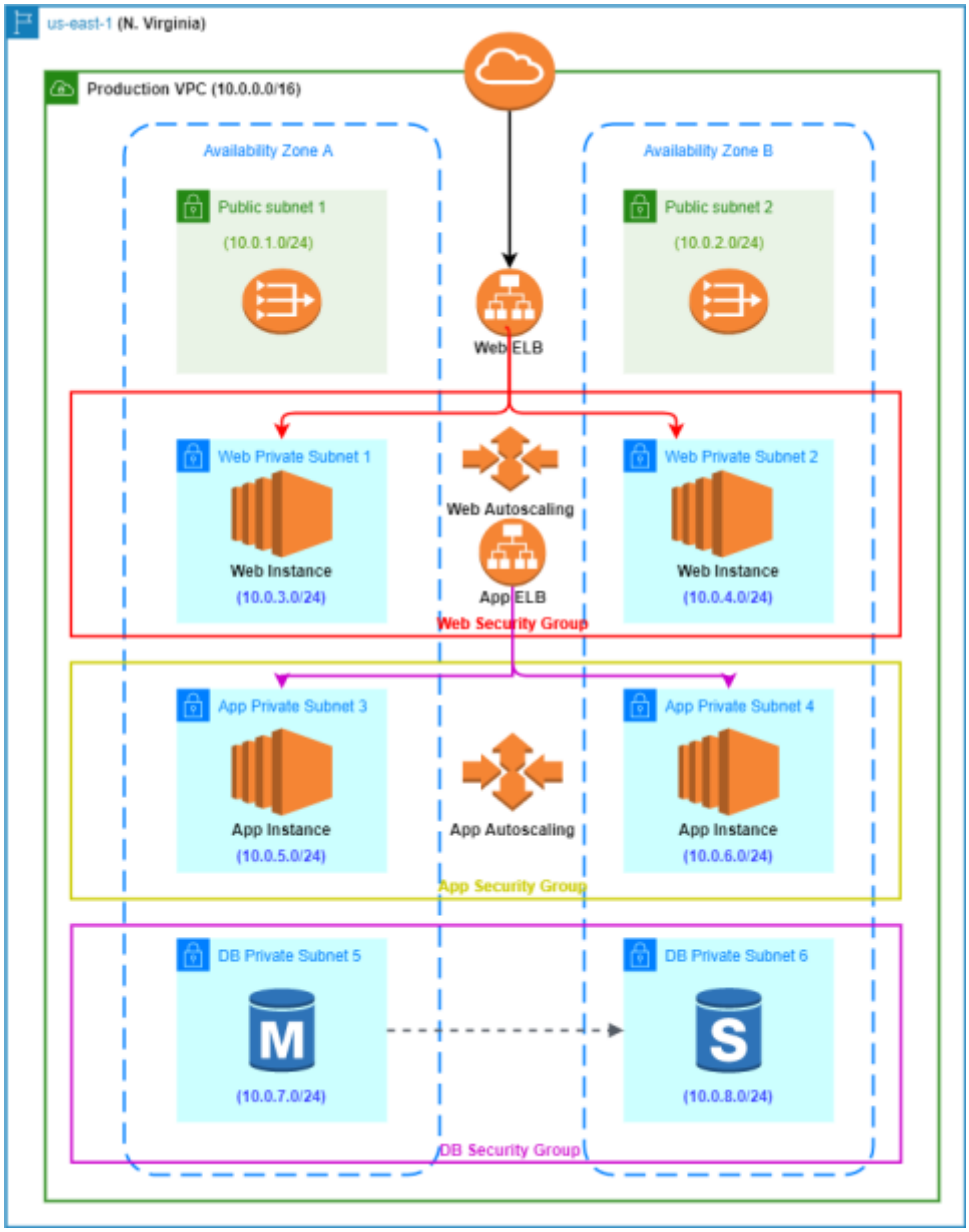
Student Number : C18480456

Table of Contents

Introduction 3
Solution – Identify the Potential Services needed and the purpose for each service 4
Solution – User Authentication 6
Solution – Network & Security 8
Solution – Web and Application Tiers 10
Solution – Business Continuity 12
Solution – Auditing 13
Conclusion 14

Introduction

The goal of this assignment was to bring together our previous work in the labs and design a cloud architecture solution for a medical company. To complete this project, we reviewed the detailed customer requirements as a group and discussed different solutions. Once everyone in the group was happy with the solution discussed we filled out the worksheets that were provided. Before we began filling out the worksheets, we completed an example of our architecture in draw.io.



Solution – Identify the Potential Services needed and the purpose for each service

1. **Identity Access Management (IAM)**

IAM will allow the Medical Company to manage access to AWS services and resources securely. When the company uses IAM they can create users, groups and permissions to allow or deny users access to AWS resources.

2. **Amazon Virtual Private Cloud (VPC)**

VPC will allow the Medical Company to provision a logically isolated section of the AWS Cloud where they will be able to launch AWS resources in a virtual network. The VPC will host multi-tier web applications and will strictly enforce access and security restrictions between the Medical Company Web Servers, Application Servers and Database Servers.

3. **Amazon Elastic Compute Cloud (EC2)**

An Instance is a Virtual Server in the cloud, with Amazon EC2 the Medical Company will be able to set up and configure applications that run on the instance. It is designed to make web-scale cloud computing easier for developers.

4. **Amazon Simple Storage Service (S3)**

Amazon Simple Storage Service is an object storage service that offers scalability, data availability, security and performance. The Medical Company will use it to store and protect data regarding their website, application and database.

5. **Auto Scaling**

AWS Auto Scaling the Medical Company can maintain optimal performance and availability. This is a Service that monitors the users applications and automatically scales up or down the capacity to maintain availability. The servers in our project need to handle increases in traffic or may need to replace instances that have stopped unexpectedly, We create auto scaling groups to solve these issues

6. **Elastic Load Balancing (ELB)**

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets such as EC2 instances in our case. In our design we used an Application Load Balancer which is best suited for load balancing of HTTP and HTTPS traffic. ELB gives our application High Availability which will keep our applications running in the case of a failure.

7. **Relational Database Service (RDS)**

Amazon Relational Database Service makes it easy to set up, operate, and scale a relational database in the cloud. The Medical Company uses Microsoft SQL Server Standard Edition which is supported by Amazon RDS.

8. CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing and risk auditing of your AWS account. The Administrator can log, continuously monitor and retain account activity related to actions across the AWS infrastructure.

Detailed Requirements – Detailed Authentication

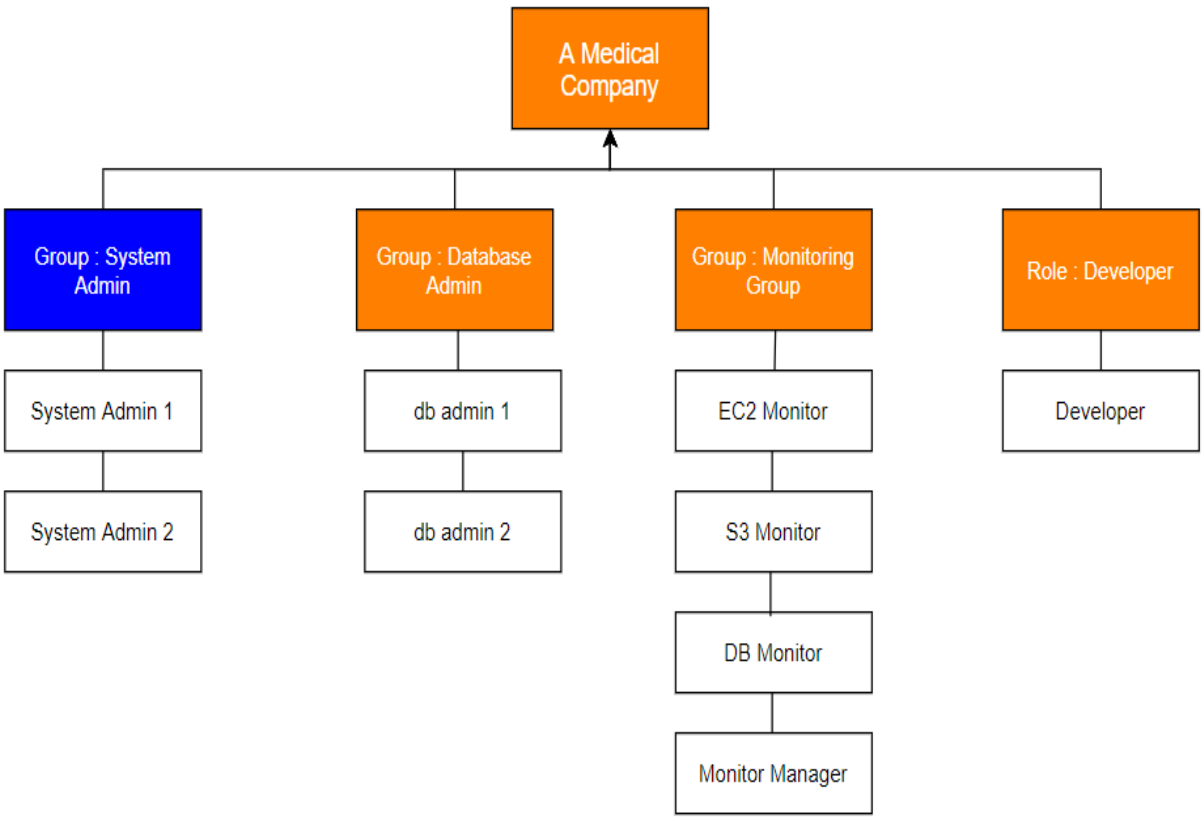
We reviewed the user requirements as a group and offered up different solutions on how to complete the following worksheets. It stated that there should be three user groups, to complete this we created a System Administrator Group with two users, Database Administrator Group with two users and a Monitoring Group with four users who would monitor EC2, RDS and S3.

We also reviewed the password policies and the permissions each user would have in the system. Administrators would require a require programmatic access and AWS Management Console access.

All other users should only have AWS Console Management Access, using a combination of username and password. The password policy was stated as follows.

1. Uppercase and 1 lowercase letter, 1 number, and 1 special character
2. Forced password change every 90 days
3. No re-use of previous three passwords

Solution – User Authentication



Group/Role #	Group/Role Name	Permissions
Group :	System Administrator	AWS Management Console Access, Programmatic Access
Group :	Database Administrator	AWS Management Console Access, Programmatic Access
Group :	Monitoring Group	AWS Management Console Access
Role:	Developer	AWS Management Console Access

Requirement	Solution
Should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character and a number.	Configure password policy using the following password policy options: • Minimum password length (set to 8). • Require at least one uppercase letter. • Require at least one lowercase letter. • Require at least one non alphanumeric character (special character). • Require at least one number.
Change passwords every 90 days and ensure that the previous three passwords can't be reused.	Configure password policy using the following password policy option: • Enable password expiration (set to 90 days). • Prevent Password reuse (set to 3).
All administrators require programmatic access.	Configure IAM policy by: • Create an access key (access key ID and a secret access key) for these users.
Administrator sign-in to the AWS Management Console requires the use of Virtual MFA.	Configure IAM Policy by : • Configure MFA devices for each administrator, which generates a six-digit authentication code. Assign the administrators to an MFA device.

Solution – Network & Security

VPC	Region	Purpose	Subnets	AZs	CIDR Range
1	us-east-1	Production	2 public 6 private	use1-az1 use2-az2	10.0.0.0/16
2	us-east-1	Development/Testing	2 public 6 private	use1-az1 use2-az2	10.0.0.0/16

As a group we decided our solution would contain 2 VPC's. One VPC for Production and one VPC for Development/Testing, each would contain 8 subnets spanning two availability zones to ensure high availability so that the application has minimum to no downtime. High availability will also ensure that in the case of a disaster the architecture can survive. As this is a Medical Company it is very important that there is no downtime in regard to the application.

Production VPC Subnet Solution

Subnet Name	VPC	Subnet Type- Public/private	AZ	Subnet Address
Public Subnet 1	**#1**	public	use1-az1	10.0.1.0/24
Public Subnet 2	**#1**	public	use2-az2	10.0.2.0/24
Web Private Subnet 1	**#1**	private	use1-az1	10.0.3.0/24
Web Private Subnet 2	**#1**	private	use2-az2	10.0.4.0/24
App Private Subnet 3	**#1**	private	use1-az1	10.0.5.0/24
App Private Subnet 4	**#1**	private	use2-az2	10.0.6.0/24
DB Private Subnet 5	**#1**	private	use1-az1	10.0.7.0/24
DB Private Subnet 6	**#1**	private	use2-az2	10.0.8.0/24

Development/Test Subnet Solution

Subnet Name	VPC	Subnet Type- Public/private	AZ	Subnet Address
Public Subnet 1	**#2**	public	use1-az1	10.0.1.0/24
Public Subnet 2	**#2**	public	use2-az2	10.0.2.0/24
WebDev Private Subnet 1	**#2**	private	use1-az1	10.0.3.0/24
WebDev Private Subnet 2	**#2**	private	use2-az2	10.0.4.0/24
AppDev Private Subnet 3	**#2**	private	use1-az1	10.0.5.0/24
AppDev Private Subnet 4	**#2**	private	use2-az2	10.0.6.0/24
DBDev Private Subnet 5	**#2**	private	use1-az1	10.0.7.0/24
DBDev Private Subnet 6	**#2**	private	use2-az2	10.0.8.0/24

Solution – Web and Application Tiers

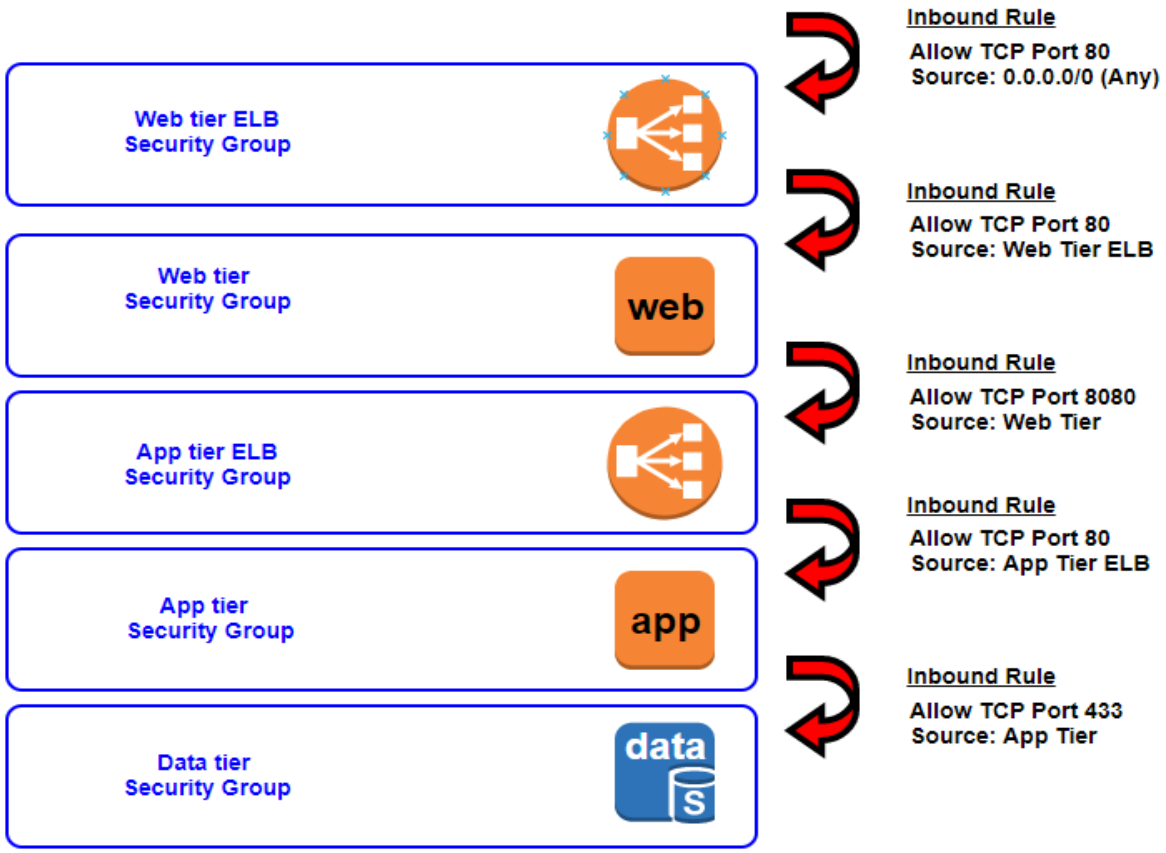
Tier	Tag	OS	Type	Size	Justification	# of instances	User Data?
Web	Key = Name Value= web-tier	MS Windows	t3	medium	General purpose instance CPU:2 Memory: 4Gb	2-4	Yes
App	Key = Name Value = app-tier	MS Windows	t3	xlarge	General purpose instance CPU:4 Memory: 16Gb	2-4	Yes
DB	Key = Name Value = db-tier	MS Windows	db.t3	2xlarge	General purpose instance CPU:8 Memory: 32Gb	1 Primary 1 Standby	No

After reviewing a Medical Company's current architecture, we discussed how we would replicate this in AWS. Each tier has MS Windows as their OS. The web tier needs t3.medium as it two CPU's and 4GB of memory, The App Tier needs t3.xlarge as it needs four CPU's and 16GB of Memory, The Database Tier Requires db.t2.2xlarge as it needs 8 CPU's and 32GB of Memory. For the database tier we designed our architecture to have one primary database and one standby, this ensures high availability as these two instances will perform synchronous data replication. Both the Web-Tier and Application-Tier need to have IIS installed this is installed through the user data.

Load Balancer	Name	External/ Internal	Subnets	SG Name *	Rule	Source
For Web Tier	web-elb	External	Public Subnet 1 Public Subnet 2	web-elb-sg	Receive requests from the Internet	0.0.0.0/0 ::/0 (any)
For App Tier	app-elb	Internal	Web Private Subnet 1 Web Private Subnet 2	app-elb-sg	Receive requests from web tier server	web-tier-sg

Instance Tier	SG Name*	Rule	Source
Web Tier	web-tier-sg	Receives requests from the web tier Elastic Load Balancer	web-tier-elb
App Tier	app-tier-sg	Receives requests from the application tier Elastic Load Balancer	App-tier-elb
Database Tier	db-tier-sg	Receives requests from the application servers	App-tier-sg

As a group our discussion focused on Security Group Chaining. We created a Security Group Chaining Diagram as a group to show how our security groups interact with each other.



Solution – Business Continuity

Tier	OS	Type	Size	Configuration Name*	Role	Security Group
Web	Windows	t3	medium	WebTier	Developer	Web Security Group
App	Windows	t3	xlarge	AppTier	Developer	App Security Group

Tier	Launch Configuration*	Group Name	Group Size	VPC	Subnets	ELB	Tags
Web	WebTier	WebTier	Minimum Capacity : 2 Maximum Capacity : 4	Production VPC	Public Subnet 1 Public Subnet 2	Application Load Balancer	Key = Name Value = web-tier-elb
App	AppTier	AppTier	Minimum Capacity: 2 Maximum Capacity: 4	Production VPC	Web Private Subnet 1 Web Private Subnet 2	Application Load Balancer	Key = Name Value = app-tier-elb

As a group we discussed the Business Continuity for the Medical Company. We agreed that the web and app tiers should be resilient and if a server becomes unavailable it will be replaced by a new server. The database tier also should support Multi-AZ deployment and we did this by creating a primary database and a standby database as we discussed above. To ensure that the architecture could handle doubling the number of servers to support rapid growth, we set the minimum capacity to 2 and the maximum capacity to 4.

Solution – Auditing

Administrators must be able to track every AWS service-related action in the account. With CloudTrail as I have mentioned above the administrators will be able to log, continuously monitor and retain account activity

1. **Compliance Aid**

AWS CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards by providing a history of activity in your AWS account

2. **Security Analysis**

The Administrators can perform security analysis and detect user patterns.

3. **Data Exfiltration**

The Administrators can detect data exfiltration by collecting activity data on S3 objects. Data exfiltration occurs when malware or a malicious actor carries out an unauthorised data transfer from a computer.

4. **Operational Issue Troubleshooting**

The Administrators can troubleshoot operational issues by leveraging the AWS API call history produced by AWS CloudTrail. They can quickly identify the most recent changes made to resources in the environment.

5. **Unusual Activity Detection**

The Administrators can detect any unusual activity by enabling CloudTrail insights. They can then quickly alert and act on operational issues.

6. **Data Events**

Data events provide insights into the resource operations performed on or within the resource. Administrators can log API actions on Amazon S3 objects and receive detailed information such as the AWS account, IAM user role and IP Address of the user.

7. **Management Events**

This provides Administrators insight into the management operations performed on resources in the AWS account. Administrators can log actions such as creation, deletion and modification of EC2 instances.

Conclusion

Overall, we feel as a group that this assignment has greatly improved our understanding of Cloud Computing and AWS. We were able to research more services that AWS offers and create a solution together as a group for a Medical Company. This assignment has further developed our communication skills and teamwork skills which will be vital in the future in securing employment.

Although it was tougher to complete this group project without seeing the other group members face to face I felt we met this challenge head on and came out with greater time management and creative thinking skills.