

3-Tier Web Architecture on AWS

ATYPON

Author: Ahmad Emad

Website: [Potfolio wesite](#)

YouTube Video: [Demonstartion](#)

Email: ahmademad995.ae@gmail.com

Objective Overview:

The objective of this deployment is to design and implement a secure, scalable, and high-availability 3-tier web architecture on AWS. This architecture ensures efficient load balancing, security, and performance optimization by distributing the application across multiple layers.

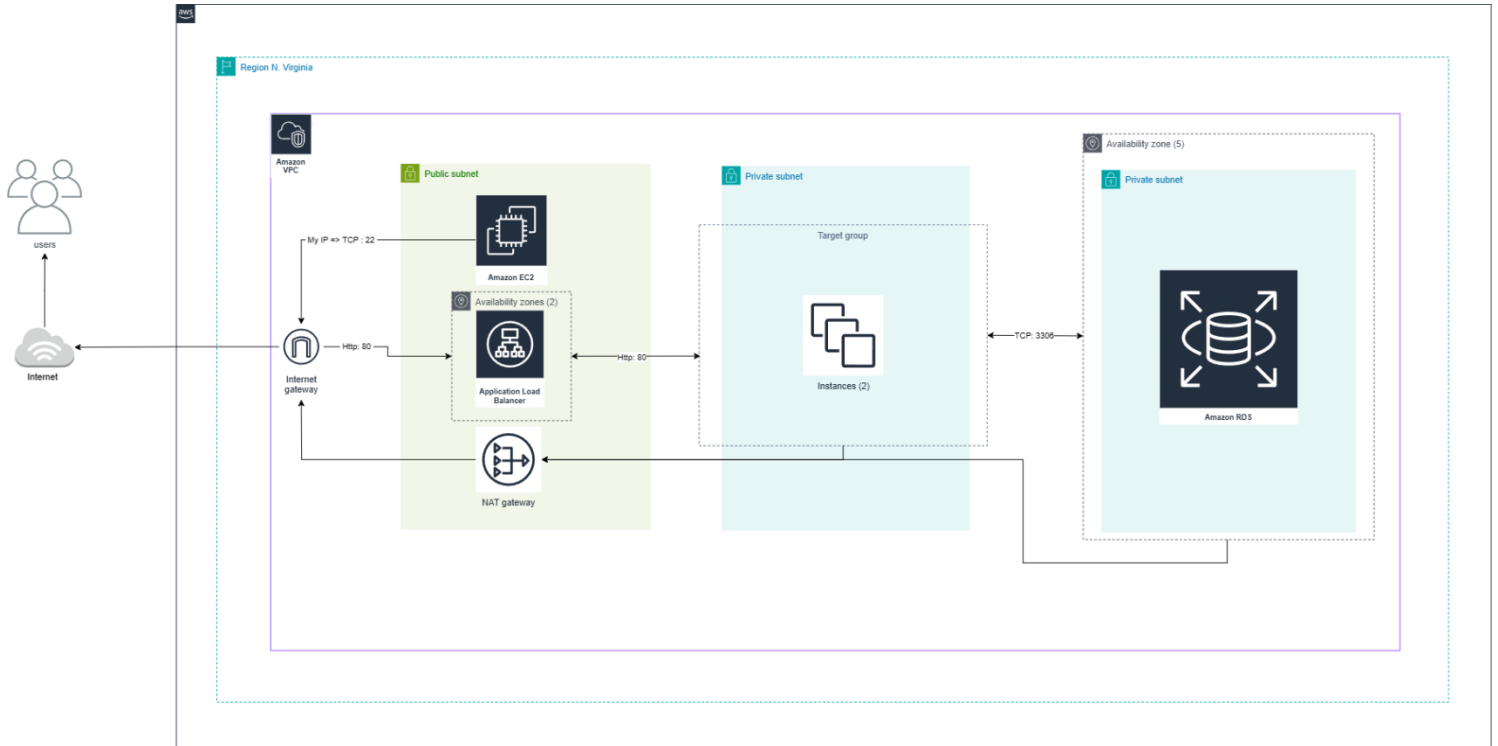
Table of Contents

Introduction	4
Network Diagram	4
Architecture	4
VPC	5
Atypon-Assignment-VPC	5
Details.....	5
Resource Map.....	5
Subnets	5
public_subnet-1	5
Description	5
Details.....	5
Route table	6
public_subnet-2	6
Description	6
Details.....	6
Route table	6
frontend_private_subnet.....	6
Description	6
Details.....	6
Route table	7
rds-ec2-db-subnet-group-1	7
Description	7
Details.....	7
Route table	7
Servers	8
Bastion_Host_Server.....	8
Description	8
Details.....	8
Security.....	8
Web_App_Server-1	8
Description	8
Details.....	8

Security.....	9
Web_App_Server-2	9
Description	9
Details.....	9
Security.....	9
Databases	10
database-1	10
Description	10
Details.....	10
Connectivity.....	10
Load Balancing.....	10
ELB.....	10
Description	10
Details.....	11
Resource Map.....	11
NAT gateways	11
NAT-Gateway	11
Description	11
Details.....	11
Conclusion.....	12

Introduction

Network Diagram



Architecture

The deployment consists of three distinct tiers:

1. **Presentation Tier (Web Layer & Access Layer)**
 - A **public-facing Application Load Balancer (ALB)** routes incoming traffic from the internet to EC2 instances in the public subnet. This ensures high availability and scalability by distributing user requests across multiple instances.
 - A **Bastion Host**, also deployed in the public subnet, provides secure SSH access to private instances, ensuring administrative access without exposing them to the internet.
2. **Application Tier** – EC2 instances in a private subnet handle business logic, ensuring that sensitive backend operations remain isolated from direct internet access. These instances communicate with the database tier while utilizing a NAT Gateway for outbound internet access when necessary.
3. **Database Tier** – An Amazon RDS instance is deployed in a private subnet for data storage and management. This enhances security by restricting direct internet exposure and allowing only the application tier to access it over TCP 3306.

VPC

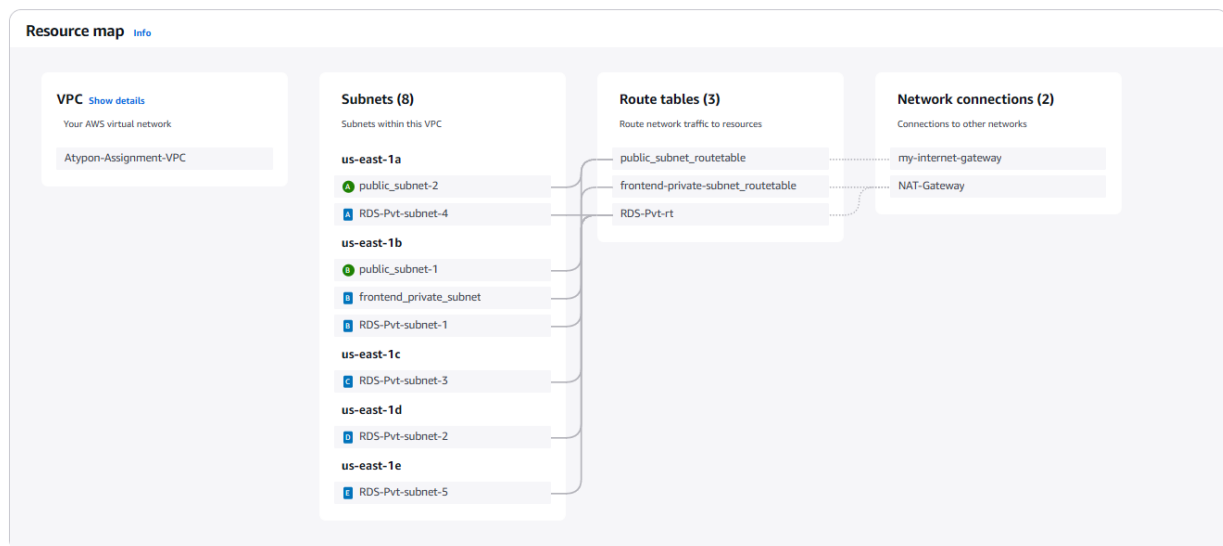
Atypon-Assignment-VPC

Details

IPv4 CIDR: 10.0.0.0/16

Default VPC: No

Resource Map



Subnets

public_subnet-1

Description

Public Subnet-1 is designed to host essential components of a 3-tier web architecture, including the Application Load Balancer (ALB), a NAT Gateway, and a Bastion Host. The ALB ensures efficient traffic distribution and routing to backend servers, while the NAT Gateway provides secure outbound internet access to instances in private subnets. The Bastion Host serves as a controlled entry point for system administrators to securely manage resources in the private network. This setup enables high availability, security, and scalability for the web application.

Details

IPv4 CIDR: 10.0.0.0/24

Availability Zone: us-east-1b

Route table

Route table: [rtb-0ae4b600a086bba74](#) / [public_subnet_routetable](#)

[Edit route table association](#)

Routes (2)	
<input type="text" value="Filter routes"/>	
< 1 >	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-0ad07e9869884a2b3

public_subnet-2

Description

The public_subnet-2 serves as one of the availability zones for the Application Load Balancer (ALB) in the AWS 3-tier architecture. Since the ALB requires at least two Availability Zones (AZs) for high availability, this subnet ensures fault tolerance by distributing incoming traffic across multiple zones, preventing single points of failure.

Details

IPv4 CIDR: 10.0.3.0/24

Availability Zone: us-east-1d

Route table

Route table: [rtb-0ae4b600a086bba74](#) / [public_subnet_routetable](#)

[Edit route table association](#)

Routes (2)	
<input type="text" value="Filter routes"/>	
< 1 >	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-0ad07e9869884a2b3

frontend_private_subnet

Description

The frontend_private_subnet is a private subnet that hosts two EC2 web servers, forming the web/application layer of the 3-tier architecture. These instances handle incoming traffic from the Application Load Balancer (ALB), process dynamic web content, and forward requests to the backend services.

Details

IPv4 CIDR: 10.0.1.0/24

Availability Zone: us-east-1b

Route table

Route table: [rtb-0ce43cabb5d612061 / frontend-private-subnet_routetable](#)

Edit route table association

Routes (2)

Filter routes

< 1 > ⚙

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-0ed8551a1e9966364

rds-ec2-db-subnet-group-1

Description

The rds-ec2-db-subnet-group-1 is a database subnet group that consists of five private subnets strategically distributed across multiple availability zones to enhance high availability and fault tolerance. This subnet group is specifically designed to accommodate a MySQL Amazon RDS instance, ensuring secure and isolated database operations while preventing direct internet exposure.

Details

rds-ec2-db-subnet-group-1

Subnet group details

VPC ID

[vpc-0a8ab36c450ed25dd](#)

ARN

arn:aws:rds:us-east-1:149536467998:subgrp:rds-ec2-db-subnet-group-1

Supported network types

IPv4

Description

Created from the RDS Management Console

Subnets (5)

Availability zone	Subnet name	Subnet ID	CIDR block
us-east-1a	RDS-Pvt-subnet-4	subnet-025d73d1d6b9e4958	10.0.5.128/25
us-east-1d	RDS-Pvt-subnet-2	subnet-0b19a44aae8b03a4d	10.0.4.128/25
us-east-1e	RDS-Pvt-subnet-5	subnet-071292047a97cbc8c	10.0.6.0/25
us-east-1c	RDS-Pvt-subnet-3	subnet-0fd86cc039081a9aa	10.0.5.0/25
us-east-1b	RDS-Pvt-subnet-1	subnet-0a70228e992d56fd8	10.0.4.0/25

Route table

Route table: [rtb-0efa90a76b77d229d / RDS-Pvt-rt](#)

Edit route table association

Routes (2)

Filter routes

< 1 > ⚙

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-0ed8551a1e9966364

Servers

Bastion_Host_Server

Description

The Bastion Host server is configured to accept only SSH connections from your specific IP address, ensuring secure and restricted access. Once connected to the Bastion Host, you can then securely access instances in the private subnet. This setup acts as a gateway, providing a controlled entry point for administrative tasks, while preventing unauthorized access to internal resources by limiting external connections to the Bastion Host.

Details

Platform details: Linux/UNIX

Subnet: [public_subnet-1](#)

Public IPv4 address: 18.208.173.9

Security

▼ Inbound rules

Q

Filter rules

<

1

>

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0a6be1ee838e9c53a	22	TCP	46.185.230.72/32	Bastion Host Security Group

<

>

▼ Outbound rules

Q

Filter rules

<

1

>

Name	Security group rule ID	Port range	Protocol	Destination	Security groups
-	sgr-08f120a32b9d44e62	All	All	0.0.0.0/0	Bastion Host Security Group

<

>

Web_App_Server-1

Description

Web_App_Server-1 is a server within the application tier of a 3-tier architecture. It handles the core business logic and serves the web application to users. This server processes requests from the front-end, typically interacting with databases and other back-end services. It runs application code, web frameworks, and APIs, ensuring seamless communication between the user-facing interface and the data layer. The Web_App_Server-1 is located in a private subnet for security, with traffic routed through the Application Load Balancer (ALB) in the public subnet.

Details

Platform details: Linux/UNIX

Subnet: [frontend_private_subnet](#)

Private IPv4 address: 10.0.1.8

Security

▼ Inbound rules						
<input type="text" value="Filter rules"/>						
Name	Security group rule ID	Port range	Protocol	Source	Security groups	
-	sgr-0097ae53db22a81f0	22	TCP	10.0.0.0/24	Web_App_SecurityGroup	
-	sgr-0dac918cd538cdd15	80	TCP	10.0.0.0/24	Web_App_SecurityGroup	

▼ Outbound rules						
<input type="text" value="Filter rules"/>						
Name	Security group rule ID	Port range	Protocol	Destination	Security groups	
-	sgr-02bf71f479eb8b945	All	All	0.0.0.0/0	Web_App_SecurityGroup	
-	sgr-00c7d3e25f420b860	3306	TCP	sg-072cfc7a565767f7b	ec2-rds-1	

Web_App_Server-2

Description

Web_App_Server-2 is created as an identical image (AMI) from Web_App_Server-1. This approach allows for quick scaling and redundancy by replicating the configuration and setup of Web_App_Server-1, ensuring both servers have the same environment, application, and configurations. Web_App_Server-2 can handle traffic in the same way as Web_App_Server-1, providing high availability and load balancing. It can automatically be added to the pool of application servers behind the Application Load Balancer (ALB), ensuring that if one server fails or needs maintenance, the other can take over seamlessly without disrupting service.

Details

Platform details: Linux/UNIX

Subnet: frontend private subnet

Private IPv4 address: 10.0.1.135

Security

▼ Inbound rules

< 1 >

Name	Security group rule ID	Port range	Protocol	Source	Security groups
–	sgr-0097ae33db22a81f0	22	TCP	10.0.0.0/24	Web_App_SecurityGroup
–	sgr-0dac918cd538cdd15	80	TCP	10.0.0.0/24	Web_App_SecurityGroup

◀ ▶

▼ Outbound rules

< 1 >

Name	Security group rule ID	Port range	Protocol	Destination	Security groups
–	sgr-02bf71f479eb8b945	All	All	0.0.0.0/0	Web_App_SecurityGroup
–	sgr-00c7d3e25f420b860	3306	TCP	sg-072cfc7a565767f7b	ec2-rds-1

◀ ▶

Databases

database-1

Description

Database-1 is a MySQL RDS instance configured to serve the web application through port 3306. It spans across five Availability Zones, ensuring high availability, fault tolerance, and improved disaster recovery capabilities. This setup allows the database to maintain consistent performance and resilience, as traffic can be routed to healthy nodes in the event of an outage or failure in one Availability Zone. The MySQL RDS instance is securely located in a private subnet, providing database services to the Web App Servers while maintaining a strong security posture.

Details

Engine: MySQL Community

Region: us-east-1b













Port: 3306

Subnet group: [rds-ec2-db-subnet-group-1](#)

Connectivity

Resource 1: [Web App Server-1](#)

Resource 2: [Web App Server-2](#)

Connected compute resources (2) Info							 Actions 
Connections to compute resources that were created automatically by RDS are shown here. Connections to compute resources that were created manually aren't shown.							
<input type="text" value="Filter by compute resources"/>							 1  
Resource identifier 	Resource type 	Availability Zone 	VPC security group 	Compute resource security group 	Connected proxy 		
i-009101e29810bf337	EC2 instance	us-east-1b	rds-ec2-1	ec2-rds-1	-		
i-0d69c1035803a3fa9	EC2 instance	us-east-1b	rds-ec2-1	ec2-rds-1	-		

Load Balancing

ELB

Description

The Elastic Load Balancer (ELB), configured with the Application Load Balancer (ALB) type, distributes incoming traffic to two web application servers using a round-robin algorithm. This load balancing method ensures that each server receives an approximately equal share of traffic, optimizing resource utilization and preventing any single server from being overwhelmed.

Details

Load balancer type: Application

Availability Zones: [public_subnet-1](#) [public_subnet-2](#)

DNS name: [ELB-1859305876.us-east-1.elb.amazonaws.com](#)

Load balancing algorithm: Round robin

Target group: [Web_App_Server-1](#) [Web_App_Server-2](#)

Resource Map



NAT gateways

NAT-Gateway

Description

The NAT Gateway provides secure outbound internet access for the web servers and the MySQL RDS instance while keeping them in a private subnet. This allows the web servers to download necessary updates, communicate with external services, and perform maintenance tasks without exposing them directly to the internet. Similarly, the RDS instance can reach external repositories for database patching and updates while remaining isolated from direct internet access. The NAT Gateway is deployed in a public subnet and routes traffic from private subnets to the internet, ensuring a secure and controlled network environment.

Details

Primary private IPv4 address: 10.0.0.203

Subnet: [public_subnet-1](#)

Conclusion

This 3-tier web architecture is designed for high availability, security, and scalability. The public subnet hosts the ALB, NAT Gateway, and Bastion Host, ensuring efficient traffic management, controlled administrative access, and secure outbound connectivity. The application tier consists of multiple Web App Servers that handle business logic and scale dynamically using a round-robin load balancing strategy. The database tier features a MySQL RDS instance with multi-AZ deployment for fault tolerance and data reliability. The NAT Gateway enables secure external communication for the web servers and database without exposing them to direct internet access.

To deploy the application, rsync was used to synchronize project files across the web servers, ensuring consistency across instances. Web_App_Server-2 was created by taking an AMI (Amazon Machine Image) of Web_App_Server-1 and launching a new instance from that image, ensuring an identical setup for seamless scaling and redundancy. Additionally, the website was configured to display the private IP address of the instance serving each client request, allowing for visibility into which backend server is handling the traffic. This setup enhances performance monitoring, debugging, and overall system reliability.