Overtime Lifecycle Environment



**Prepared By:**

Abdelrahman Mamdouh

Abdelrahman Hesham

Mirna Azmi

Nourelhoda Ashraf

Omar Hesham

Randa Osama

Reham Ashraf

Table of Contents

[Objective 2](#_Toc15284072)

[System Requirements 2](#_Toc15284073)

[Cloud Architecture 3](#_Toc15284074)

[Infrastructure Components 3](#_Toc15284075)

[VPC 3](#_Toc15284076)

[Bastion Server 3](#_Toc15284077)

[Orchestration Machine 3](#_Toc15284078)

[Routing Tables 3](#_Toc15284079)

[API Gateway 3](#_Toc15284080)

[Subnets 3](#_Toc15284081)

[NACLS 3](#_Toc15284082)

[Security Groups 3](#_Toc15284083)

[NAT 3](#_Toc15284084)

[Infrastructure as a code 4](#_Toc15284085)

[Cloud infrastructure diagram 5](#_Toc15284086)

[User Automated Creation 6](#_Toc15284087)

# Objective

We are required to develop a -Cloud Native- system that manages the overtime lifecycle according to the role of each system user.

The current system depends on two sub-systems “CATW” and “EES”, the users should update and insert the data in the two sub-systems, so we are required to create a single point data entry to decrease effort, time also minimize data error.

The new system is cloud native applied on AWS amazon web services trying to gain the max benefit from the AWS services such as RDS, Lambda………etc.

# System Requirements

* Orchestration Machine to manage RDS.
* Complete and secured cloud architecture.
* Service to handle single point data entry.
* Service to handle email approvals.
* Service for storage and archiving.

# Cloud Architecture

The infrastructure is built according to system requirements -security and networking- also to be easily using tunnels to access secured RDS.

## Infrastructure Components

### VPC

The virtual private cloud is created with CIDR range for IPV4 10.0.0.0/24.

All the infrastructure and the services are on the same region “us-east-1” USA Virginia.

### Bastion Server

The bastion server is the only component that exits in a public subnet and can be reached directly from the IGW.

A tunnel is created from the bastion to access RDS for development and testing.

### Orchestration Machine

The orchestration machine is the main machine used to handle RDSs also the machine can host other applications if needed.

The machine exits in a private subnet that can be only accessed using bastion server where the private key is installed.

SQL client is installed on the machine to manage the RDS.

### Routing Tables

### API Gateway

### Subnets

### NACLS

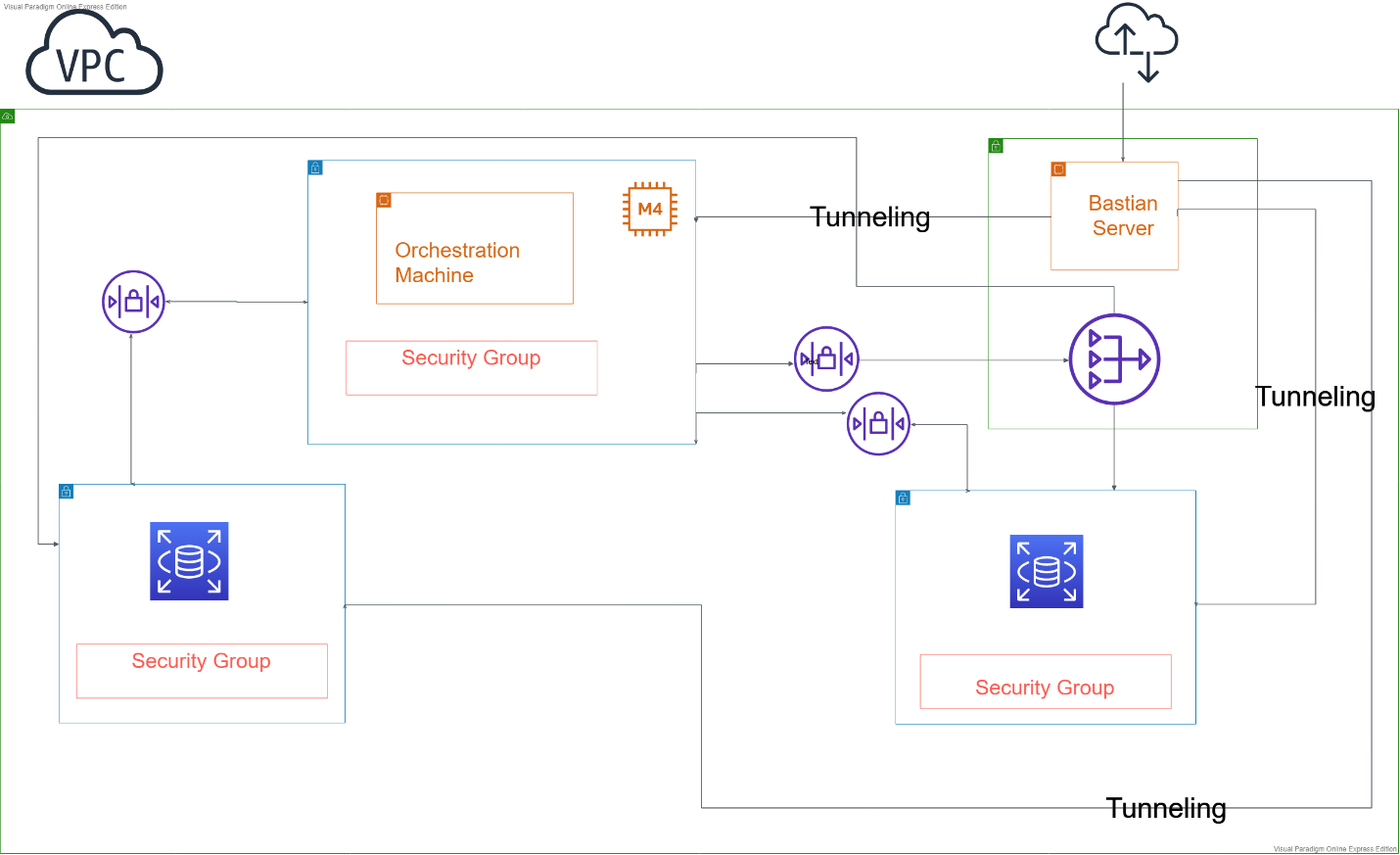
### Security Groups

### NAT

## Infrastructure as a code

Terraform tool is used in creating infrastructure, the tool uses AWS CLI inserted credentials to verify the account and specify the user creating infrastructure

## Cloud infrastructure diagram



## User Automated Creation

## Cost

We are a team of 7 individuals we’re divided into 2 teams, team 1 developers of 4 and team 2 architecture of 3.  
  
As an architecture team at first we sketched the design of the project architecture then we implemented what is designed on the AWS console using one of the team account.   
  
As developers team they tried their trial codes using eclipse (JAVA programming language) on their personal accounts before integrating all on same account.  
-Region:  
 VPC🡪 N.Virginia

Bucket 🡪N.Virginia

-CIDERS & I/P addresses:  
 1)VPC 🡪10.0.0.0/24  
 2) Subnets

Orch-VM 🡪10.0.0.128/28  
Dev2-RDS🡪10.0.0.16/28  
Networking RDS 🡪 10.0.0.64/26  
Dev1-RDS 🡪10.0.0.0/28

TEST1-RDS 🡪10.0.0.32/28  
TEST2-RDS 🡪10.0.0.48/28  
3) NAT gateway 🡪10.0.0.70

-NACLS:  
 1) DEV-RDS  
inbound:

|  |
| --- |
|  |
| **Rule #** | **Type** | **Protocol** | **Port Range** | **Source** | **Allow / Deny** |  |
|  | | | | | |  |
| 1 | MySQL/Aurora (3306) | TCP (6) | 3306 | 10.0.0.133/32 | ALLOW |  |
| 2 | MySQL/Aurora (3306) | TCP (6) | 3306 | 10.0.0.126/32 | ALLOW |  |

Outbound:

|  |
| --- |
|  |
| **Rule #** | **Type** | **Protocol** | **Port Range** | **Destination** | **Allow / Deny** |  |
|  | | | | | |  |
| 1 | ALL TCP | TCP (6) | 0 - 65535 | 0.0.0.0/0 | ALLOW |  |

2) Public-Networking

Inbound:

| **Rule #** | **Type** | **Protocol** | **Port Range** | **Source** | **Allow / Deny** |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | |  |
| 1 | ALL TCP | TCP (6) | 0 - 65535 | 0.0.0.0/0 | ALLOW |  |

Outbound:

|  |
| --- |
|  |
| **Rule #** | **Type** | **Protocol** | **Port Range** | **Destination** | **Allow / Deny** |  |
|  | | | | | |  |
| 1 | ALL TCP | TCP (6) | 0 - 65535 | 0.0.0.0/0 | ALLOW |  |

3) TEST-RDS  
Inbound:

| **Rule #** | **Type** | **Protocol** | **Port Range** | **Source** | **Allow / Deny** |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | |  |
| 1 | MySQL/Aurora (3306) | TCP (6) | 3306 | 10.0.0.133/32 | ALLOW |  |
| 2 | MySQL/Aurora (3306) | TCP (6) | 3306 | 10.0.0.126/32 | ALLOW |  |

Outbound:

| **Rule #** | **Type** | **Protocol** | **Port Range** | **Destination** | **Allow / Deny** |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | |  |
| 1 | ALL TCP | TCP (6) | 0 - 65535 | 0.0.0.0/0 | ALLOW |  |

4) ORCH-VM  
inbound:

| **Rule #** | **Type** | **Protocol** | **Port Range** | **Source** | **Allow / Deny** |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | |  |
| 1 | SSH (22) | TCP (6) | 22 | 10.0.0.126/32 | ALLOW |  |
| 2 | ALL TCP | TCP (6) | 0 - 65535 | 0.0.0.0/0 | ALLOW |  |

Outbound:

| **Rule #** | **Type** | **Protocol** | **Port Range** | **Destination** | **Allow / Deny** |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | |  |
| 1 | ALL TCP | TCP (6) | 0 - 65535 | 0.0.0.0/0 | ALLOW |  |

-We used in the cloud:  
 1)2 EC2  
 2)3 Lambda  
 3)SES  
 4)1 RDS  
 5) 1 S3   
 6) API Gateway  
 7) 1 EBS  
 8)1 NAT  
 9) Internet Gateway  
 10) 2 route tables  
 11)6 subnets (5 private & 1 public)  
 12)Tunneling  
  
Difficulties we encountered:  
 As architecture team:

We had issues to connect to the Bastion server and some security issues we solved some by security groups and NACLs.  
We had issues in creating Bastion Server itself as we realized later it is just an EC2 we special characterization.  
We had issues with connect the VPC to the internet and the solution was NAT.  
We did not know how to make swap memory, so we searched and the issue is solved.  
We were encountered be suitable inbound and outbound rules for the NACls, we discussed and solve the issue.  
  
As developers:  
 Left for the developers team  
Design:  
  
Flow of data and operation:

