**Digital Futures Data Engineering Academy**

**Case Study part 2 (Project W5 d4)**

**Technical Design**

**Introduction**

The purpose of this document is to provide a detailed AWS cloud migration strategy and pricing estimate for the client, Fishtank Ltd. The scope of the migration will cover the technical design and cloud infrastructure for a single client application and possible dependencies. The client will use this document over the next few weeks to get their first production workload running on AWS.

**Client Application**

PETRA is a CRM application based on Microsoft’s commercial of the shelf dynamic CRM platform but is heavily customised for client needs. It is constantly used during a working week by over 5,000 users across the UK: sales, HR, Fulfilment departments.

At a high-level PETRA is a standard three-layer-application comprising of Web, Application, and Database. The platform runs on Microsoft Windows Server 2008 and the database is Microsoft SQL Server 2012, both of which are out of extended support with Microsoft.

The current firewall rules of the three layers are listed below:

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Source | Destination | Comment |
| 443 | WebServers | Internet | Webservers use HTTPS to the internet |
| 9000 | WebServers | AppServers | PETRAweb talks to PETRAapp over port 9000 |
| unknown | AppServers | Database |  |
| 3389 | Webservers | Internet | RDP port, for administrators use |
| 3389 | AppServers | Internet | RDP port, for administrators use |
| 3389 | Database | Internet | RDP port, for administrators use |

The client’s current assets are listed below:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset Tags | Description | Operating System | CPU | Memory | Storage |
| S002, S003, S004, S005 | WebServer 1-4 | Windows Server 2008 | 2GB | 4GB | 30GB |
| S006, S007, S008, S009 | AppServer 1-4 | Windows Server | 4GB | 8GB | 100GB |
| S012, S013 | Database | MS SQL Server 2012 | 8GB | 16GB | 1TB |

**Cloud Architecture Diagrams**

Network Architecture (Figure 1)

A screenshot of a computer

Description automatically generated

Security (Figure 2)

A diagram of a security group

Description automatically generated

Client Application (Figure 3)

A screenshot of a computer diagram

Description automatically generated

Automation (Figure 4)

A diagram of a cloud watch

Description automatically generated

**Cloud Architecture Description**

The previous page displays the visual element of the cloud architecture. The resulting infrastructure will capture the workflow of the client’s current system, PETRA, and its dependencies. Design diagrams were split into multiple sections for increased visibility, and outline network architecture, security, client application model, and automation.

Figure 1

The foundation of the infrastructure utilises AWS availability zones with redundancy and disaster recovery in mind. High availability is achieved by having copies of the cloud PETRA system distributed over multiple availability zones. If a disaster hit a resource or availability zone, then the load balancers will ensure traffic is routed to the correct resources. The client is equipped with an AWS virtual private cloud to house their network with both public and private subnets for internet access and housing the computing instances, respectively. The client will replace their current active directory with AWS’ route 53 DNS service so users can access the internet gateway into the VPC. From there, the NAT gateways and NACLs will handle traffic into the private subnets. Conversely, when traffic needs to be routed to the internet, the public subnets is equipped with a route table. The private subnet is responsible for housing the sensitive resources such as web servers, application servers, and the database.

Figure 2

Five security precautions have been taken to protect the client’s system:

* Amazon Shield to protect against DDOS attacks.
* Network Access Control Lists to filter traffic entering the private subnets.
* Security Groups to isolate resource layers, putting sensitive resources further away from potential attackers.
* Identity and Access Management to give users access to only resources they need at certain times. In other words, to rule out misuse within the organisation.
* Private subnet to ensure sensitive resources are not accessible from the outside.

Figure 3

**The cloud architecture includes multiple availability zones, but only one availability zone is presented for increased visibility of the inner resources**. Getting into the core structure of the system, the architecture design presented mimics the original structure of the client’s application. The core of the system resides within the private subnet and, in there, the three-layer structure of the application can be seen. From left to right there is, the web servers, the application servers, and the database. Since there are two availability zones, there are two copies of the system. More specifically, there are two copies of the database where one is the primary “writer” database, and the other is a secondary “read replica” database. In the original system, the client has three groups of assets (shown in the 2nd table). The web servers in the private subnet use T3-small EC2 instances with Windows machine image because the original web servers run on Windows operating system and requires 2GB CPU with 30GB storage. The application servers in the private subnet use T3-medium EC2 instances with Windows machine image for similar reasons as the web servers but require 4GB with 100GB storage. An AWS EBS is attached to each instance with the required storage capacity. In each subnet, there is an AWS Aurora Database instance with the required 1TB storage capacity. The client may use migration services to swap the underlying Microsoft SQL Server for Aurora for efficiency.

Figure 4

The final diagram shows how the compute and database instances can be monitored by AWS Cloudwatch to trigger Event Bridge to launch and terminate resources as needed to combat against unexpected system failures or a sudden increase in traffic. The desired operating level for resources can be set in Cloudwatch and Event Bridge setting to customise how many instances are running. Autoscaling helps increase resources to manage increased demand or failure, and autoscaling can reduce active resources to reduce operational cost by terminating unused resources.

**Page 4**

Single page summary of pricing – total costs, comprising of annual AWS fees and cloud support.

**Total cost = 271,649.1 USD**

**AWS annual cost = 195,583.80 USD**

**Cloud consulting cost = 76,065.30 USD**

AWS annual cost can be found broken down in the appendix, detailing purchase of the Network infrastructure, security and automation components, and the core application components.

The cloud consulting costs are broken down as follows:

£1000 solution architect

£ 650 server migration engineer

£ 750 db migration engineer

£ 250 2x

£ 350 3x

£3k x 20 = £60k = 76,065.30 USD

20 days (4 weeks) is the assumed duration of the support needed.

**Appendix**

Export of pricing from AWS calculator.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Detailed Estimate | |  |  |  |  |  |  |
| Group hierarchy | Region | Description | Service | Upfront | Monthly | First 12 months total | Currency |
| My Estimate | Europe (London) | | VPN Connection | 0 | 11292 | 135504 | USD |
| My Estimate | Europe (London) | | Network Address Translation (NAT) Gateway | 0 | 73 | 876 | USD |
| My Estimate | Europe (London) | | Public IPv4 Address | 0 | 3.65 | 43.8 | USD |
| My Estimate | Europe (London) | | Amazon CloudWatch | 0 | 1.2 | 14.4 | USD |
| My Estimate | Europe (London) | | Amazon EventBridge | 0 | 0 | 0 | USD |
| My Estimate | Europe (London) | | Amazon Route 53 | 0 | 0 | 0 | USD |
| My Estimate | Europe (London) | | AWS Shield | 0 | 3000 | 36000 | USD |
| My Estimate | Europe (London) | | Amazon EC2 | 0 | 67.16 | 805.92 | USD |
| My Estimate | Europe (London) | | Amazon EC2 | 0 | 47.012 | 564.14 | USD |
| My Estimate | Europe (London) | | AWS Database Migration Service | 0 | 1047.46 | 12569.52 | USD |
| My Estimate | Europe (London) | | Amazon Aurora MySQL-Compatible | 0 | 263.53 | 3162.36 | USD |
| My Estimate | Europe (London) | | Amazon Aurora MySQL-Compatible | 0 | 263.53 | 3162.36 | USD |
| My Estimate | Europe (London) | | Amazon EC2 | 0 | 47.012 | 564.14 | USD |
| My Estimate | Europe (London) | | Amazon EC2 | 0 | 67.16 | 805.92 | USD |
| My Estimate | Europe (London) | | Amazon Elastic Block Store (EBS) | 0 | 39.31 | 471.72 | USD |
| My Estimate | Europe (London) | | Amazon Elastic Block Store (EBS) | 0 | 86.63 | 1039.56 | USD |