RCK LTD technical proposal for FishTank LTD

Migration of PETRA

Date: 01/02/2014

1. Introduction

Thank you for your invite to make a technical proposal concerning the migration of PETRA to cloud. This proposal has been prepared by RCK LTD with the detail of your soon to be legacy system in mind. The proposal provides a schematic outline of the migration to the cloud and the continued operation of PETRA, and its associated databases, on AWS. It also outlines costs including our services.

We at RCK LTD are glad that you found our initial proposal concerning FIshTank LTDs migration and operation to the cloud useful and look forward to securing and beneficial long-term relationship. We believe that the initial stages of our work together has been successful and we understand that PETRA is important to your business, and that the application should operate securely and consistently.

1 Proposal

1.1. Technical Overview

The initial stage of the project will be concerning assuring alignment with the feasibility tests that we have already conducted. This includes an outline of the number of staff required to man the successful migration and its ongoing operations.

Your current dependencies have been considered, including the various relationships between your WebServers, AppServers and Database. For instance, we understand that there isn't any extra functionality between the various WebServers and that we can consolidate their operations into a single cloud equivalent. The same is true for your AppServers and Databases. Efficiency and output is maintained by this consolidation and there is the opportunity to plan for a more diverse network if FishTank LTD consider that there should be. We also believe that there is potential for increased performance by taking advantage of the appropriate database hardware, including accounting for the high memory requirements. As such, and according to this proposal, memory would increase by 96 gigs.

The current function of your webservers would be dealt with by an Instance that has 8 CPU with 32GiB memory, and a network performance of up to 5 Gbps. Storage is on demand and can be fine-tuned if you have any forecasts as to what the usage might be.

There are some subtleties in terminology so hereon we will refer to the Instance that serves the same purpose as FishTank LTDs current web servers as WebInstances.

Concerning the various dependencies:

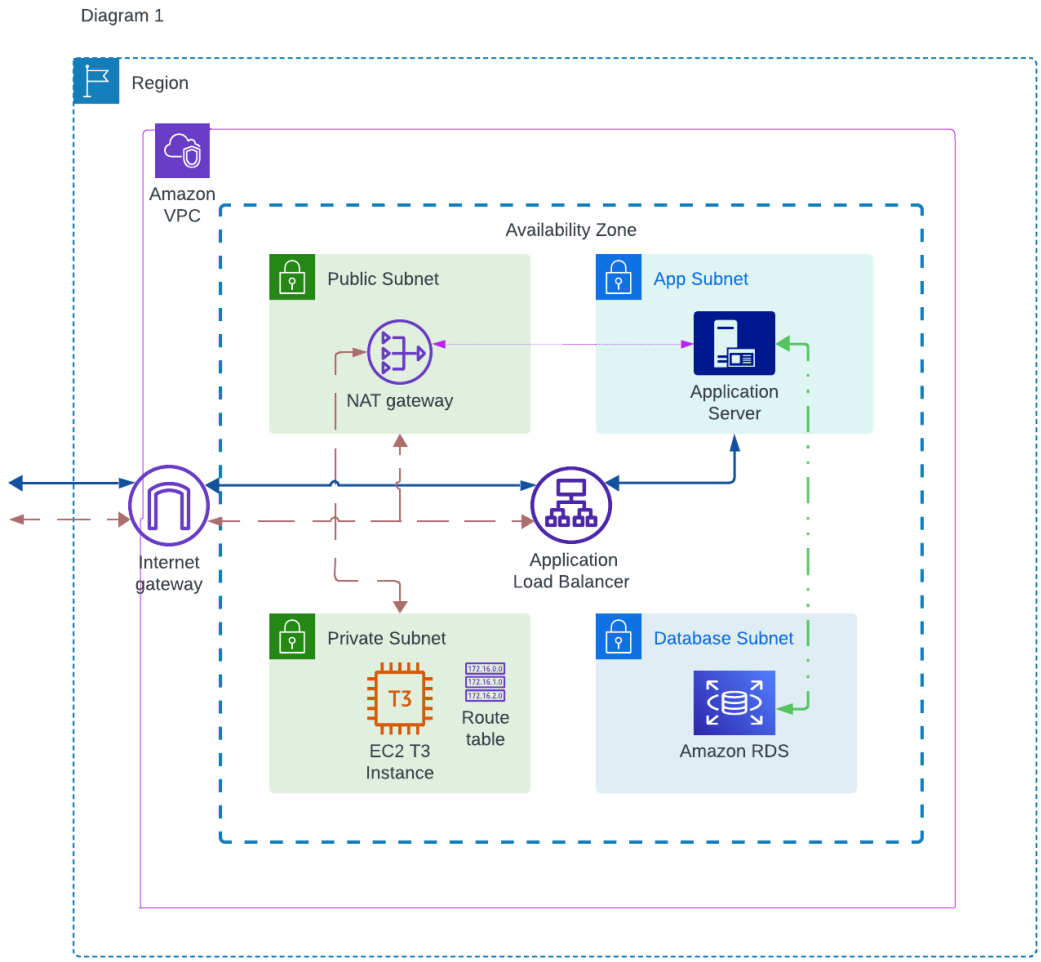
- WebInstances connecting to the internet will be filtered through a Network Address Translation (NAT).
- WebInstances communicating with the App will pass through a NAT gateway. Additional routing can be configured using a route table.
- Communication between AppServers and the Database is maintained through two subnets.

- WebInstances accessing the internet for administrative purposes will be filtered through a NAT, employing Identity-Based Policies and Network Access Control Lists (NACLs) for an added layer of security.
- AppServers accessing the internet for administrative purposes will also be filtered through a NAT using an Identity-Based policy.
- Database access to the internet for administrative tasks will be filtered through a NAT with an identity-based policy. Additionally, the load balancer facilitates API port access, which can be configured using NACLs.
- Active Directory can be hosted on the WebInstances, with routing managed by its respective route table.

The WebInstance is kept in a private subnet to assure extra security. Unless your specification changes, its booted with Windows or can have different web servers installed on it. Furthermore, the Network Access Control List Meaning can add an extra layer of security with rules that acts like a firewall. This extra layer will be important in securing the operation of PETRA. Furthermore, there is to plan for emergencies and disasters, as was outlined in our initial proposal.

As an initial sketch the network (Diagram 1):

Diagram 1



Having one web server in private subnet and the app server in the app subnet assures extra security. The NAT gateway as route to the internet, matches the functionality of FishTank LTDs current network arrangements. A load balancer can increase accessibility to a database which should satisfy 3389 Database Internet RDP port, for administrators use.

The chosen option for the Database is RDS which means that AWS will manage scaling, database backups, software patches, software installs, and OS patches. One we receive a specification from FishTank LTD we can fine tune the type of control that FishTank want over the database. Service maintenance agreements can be updated according with demand and the initial outline of costs includes an around the clock service, at a limit of 35 hours per week, with one dedicated person at any one time to match the requirements and operation of PETRA.

2.2. Cost

2.2.1 Upfront and Migration Cost

Description	Amount
Planning and Testing Migration – 24/7 Onsite and Remote Service	£6125
Impact Assessment	£4000
AWS Database Migration – maximum of 1 month migration period	£ 809.48
Total	**£10,934]**

2.2.2. Ongoing Monthly Cost

Description	Amount
AWS EC2 (WebInstance) – Windows Server, 32GB, Performance: Up to 5GB	£1153.43
AWS EC2 (AppServer) – Windows Server, 16 CPU, 64GB, Performance: up to 10GB.	£913.05
AWS RDS SQL Server – 16 CPU, Memory: 128 GiB, On Demand Utilization	£ 6600.57
RCK LTD Service Management – On-going management of the service to spec	£6600
Total	**£15,267.05]**

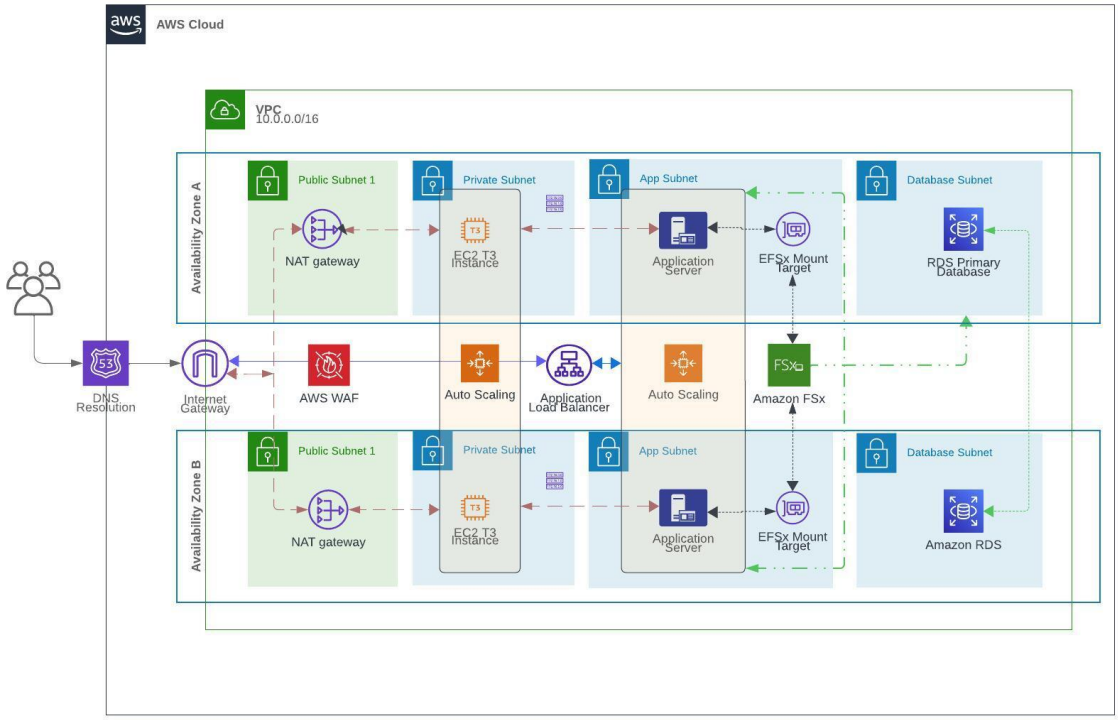
2.2.3. Total Year Cost

Our estimate for the total yearly cost of the migration and operation of PETRA on AWS Cloud, including RCK LTDs services in managing and maintaining the change is **£194,138.60.**

3. Concerning further outlay: AWS Well Architected Framework

The technical overview and quote match FishTank LTD's current on-site arrangement in the cloud and keep the costs of the migration to the cloud and continued operations to an absolute minimum.

The current proposal includes the migration of the web servers, windows application servers, MS SQL Server and include an increase in RAM. There are, however, some other recommendations that can be made regarding the evolution of Fishtank LTD's AWS architecture as concerning the well architected framework which includes the pillars of Operational Excellence, Performance Efficiency, Reliability, Sustainability, Security and Cost Optimization.



The further outlay would include an architecture that spans across two Availability Zones for increase resilience. This would assure improved fault tolerance, geographical distribution, and disaster recovery. If one availability zone fails, your application would continue to run in another availability zone, assuring that there isn't a single point of failure. Improvements in distribution wouldn't be assumed but measured. It should be the case your Manchester office will be served the application at reduced latency. There are, of course, costs associated with launching and maintaining the new instances and further data transfer costs.

We also propose to move to AWS FSx for Windows file system so as to manage directories that would otherwise be managed by FishTank LTD after an AMI install in the private subnet. This reduces maintenance overheads and increases scalability. There's no need to manage images and updates on of the instance and costs could potentially be reduced by scaling back as per demand (i.e. you'd only pay for what is process). Encryption can be at rest and / or in transit. CloudWatch and CloudTrail can be integrated in order to monitor performance and access. In essence, technicians and developers can continue to operate with their current knowledge and working practices.

The Application Load balancer and Auto-Scaling Group further increase availability and aid in improving security. In the new schemata the Application Load Balancer has been paired with a WAF to help prevent common web exploits that could affect application availability or consume excessive resources.

The Application Load Balancer itself improves the security of the application tier by ensuring that SSL/TLS cipher protocols are always used. Desync protection is based on the http_desync_guardian library, which would protect against HTTP vulnerabilities due to Desync.

Furthermore, Route53 has would be added to resolve domain names to IP address, improving the performance and security of the application by keeping your DNS resolution within the network.

There's also the potential further refinement with predefined security policies for TLS listeners in order to meet compliance and security standards. AWS Certificate Manager (ACM) or AWS Identity and Access Management (IAM) can be used to manage server certificates.

All three tiers can benefit from these changes. Furthermore, we can recommend creating and chaining security groups which work at the instance level for an extra layer of protection.

You'll note that Amazon RDS is proposed as a database solution. The Microsoft SQL server can be migrated to RDS so as to increase availability and reduce maintenance overheads.

3. Conclusion

Thank you for the opportunity to tender for the contract to migrate and operate PETRA on AWS Cloud. The proposal includes a proposed initial architecture and a plan for progressing to improve the architecture as according to well architected principles. We look forward to further discussions as to specification and timeframes so as to fine tune our service. We look forward to hearing from you.