RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Cloud Migration Whois Service

RIPE NCC Database Team

Sander Buskens | 29 October 2020 | RIPE 81

Proof of Concept

- Company Cloud First Strategy
- Migrate whois Release Candidate environment to the cloud as a Proof of Concept
- Aims:
  - Find out changes needed in whois architecture for moving to cloud
  - Demonstrate feasibility to community
  - Handle production load

Advantages

- More flexibility, resizing and provisioning services can be done very quickly
  - Easier to scale up and down
  - Cost optimisation
  - Focus on feature development rather than infrastructure/environment maintenance
- Operational improvements
  - Use managed services for common infrastructural components
- Disaster recovery
  - RIPE Database hosted in different physical locations
  - Failover to internal servers in the event of a cloud outage
- Improve availability

Amazon Cloud

- AWS is the biggest cloud provider
- Large number of services provided by AWS
- Company supports AWS
  - In-house production experience with AWS
  - Engineers have prior AWS experience
  - Cloud Team: representatives from various disciplines within the RIPE NCC working on cloud migration initiatives
  - AWS implementation partner
  - Validation sessions with AWS Solution Architects to discuss best practices on Cloud principles and best-fit AWS services
  - Cloud training

Legal Considerations

- Data classification
  - There is a lot of personal data in the RIPE database
- Amazon Legal Framework has been reviewed
- RC Data dummification improved as result of review
  - Improved descr and org-name attribute dummification ("PII Privacy Leak in descr: attributes", https://ripe80.ripe.net/presentations/39-RIPE-Database-and-GDPR-final.pdf)
- Whois RC services and data reside in the European Region

Security

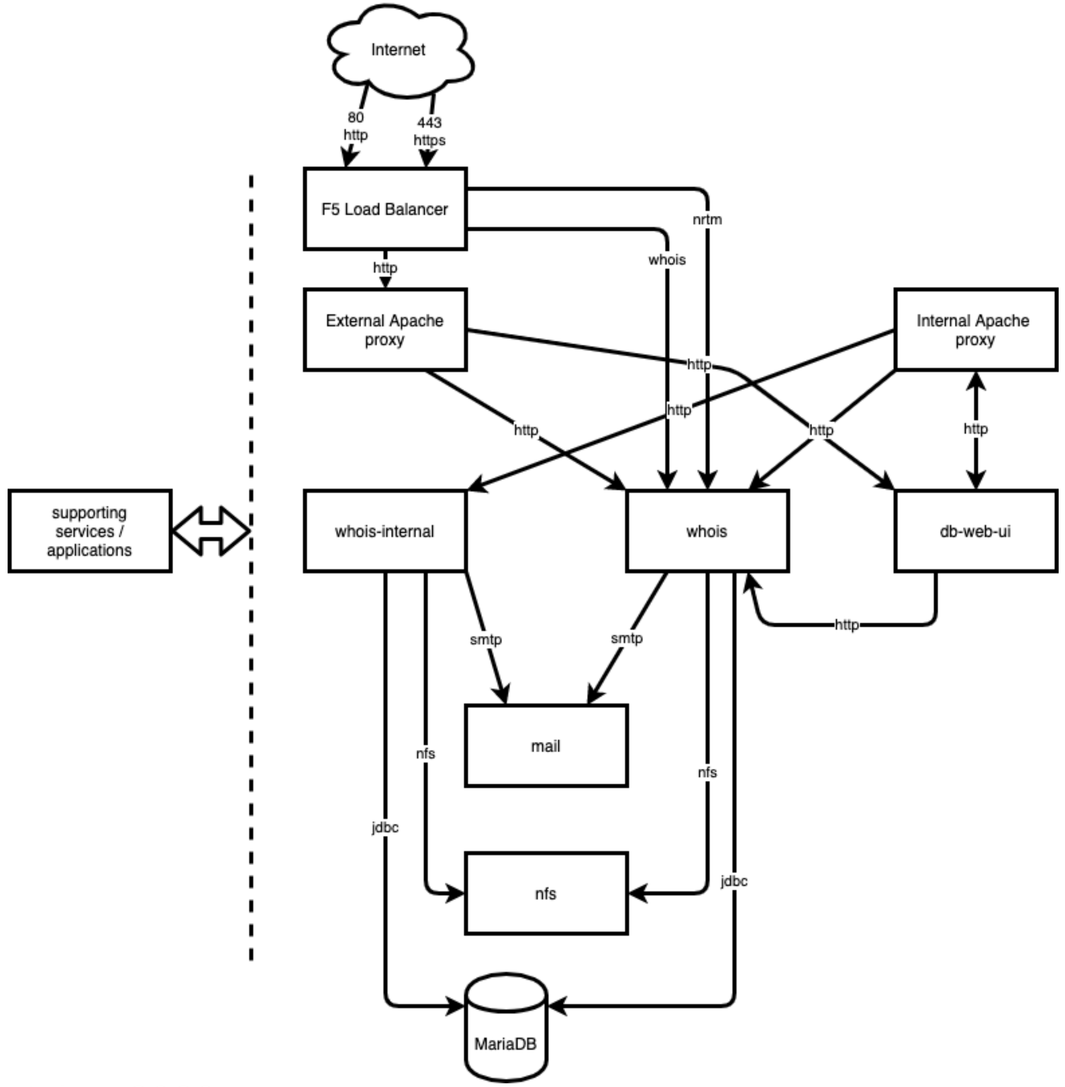
- Data encryption
- Pentesting
- Secure code reviews
- Network security
- Secure secrets and credentials management
- Audit trail on infrastructure changes
- AWS Shared Security Responsibility Model

Application Characteristics

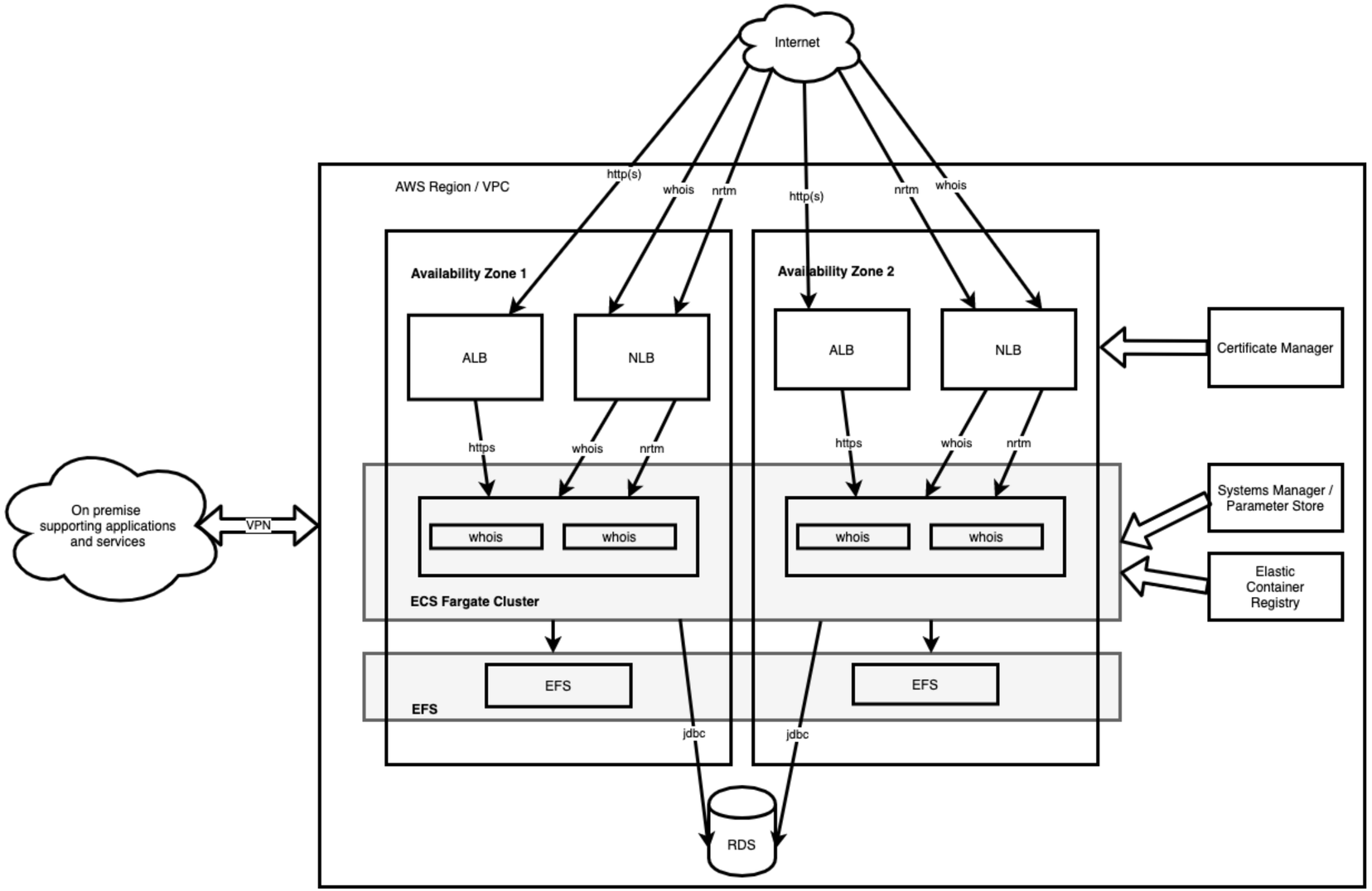
- Java based
- Read intensive
  - ~1000 queries per second
  - ~1 update per second
- MariaDB database size
  - ~100GB storage

- Application is mostly very read intensive with limited writes to database.

Current Architecture



Cloud Architecture



The Migration Process

- Building up AWS environment
- Scripting AWS infrastructure provisioning using Terraform
- Containerising whois and supporting applications
- Integrating continuous deployment pipeline into GitLab
- Load testing with production loads to properly size the environment and validate the capacity required
  - Performed extensive functional and load testing of AWS RC environment
  - Load test set created from one hour of regular whois production requests and running that against AWS environment
  - Analysed findings per run, tweaked MariaDB settings, resized RDS instance (cpu, memory) and re-ran load test number of times to find optimal instance size and settings to achieve similar performance characteristics to current production setup

Cost Optimisation

- Aim to improve availability and reliability of whois while keeping costs under control
  - Cost areas: RDS, Fargate, network traffic and storage
  - Tuned and sized environment for optimal capacity versus operating costs required
  - Use reserved instances to lower operating costs
  - Experiment with running non production environments (dev, test) only during office hours (will save additional costs for not running services while they're not actively being used)
- Internal cost review
- Cost forecasts for budgeting

Next Steps

- Try it out at https://rc.db.ripe.net/db-web-ui
- Work in progress
  - IPv6
  - Failover
    - Setup hot standby read-only failover whois environment on premise at RIPE NCC
  - Preserve client IP for personal object accounting
  - Availability
  - Move fulltext search index into managed ElasticSearch

Production Rollout

- Expect first half of 2021
- An implementation plan will be prepared for production rollout
  - Expect no query downtime
  - Anticipate minimal update downtime

Questions

sbuskens@ripe.net

References

- AWS security processes whitepaper
  - https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
- Activity Plan 2020
  - https://www.ripe.net/publications/docs/ripe-735
- Our Approach to the Cloud (by Kaveh Ranjbar)
  - https://labs.ripe.net/Members/kranjbar/our-approach-to-the-cloud