

nib group - Case Study

Red Queen Platform enablement project

Project Overview

nib commenced their Amazon Web Services (AWS) journey in early 2015, determining that AWS was the target IaaS platform of choice by completing a Proof of Concept process. Following the PoC, a business case to transition the digital footprint of nib's business to AWS was approved to proceed and the AWS migration program commenced in earnest in December 2015.

In March 2016, nib realised further specialist assistance was required to mature the AWS environment and ensure the platform incorporated the appropriate controls to adhere with its governing standards and guidelines. nib needed the AWS environment to provide greater flexibility and efficiency by enabling automated environment builds including automated DR and High Availability testing.

In April 2016, CMD Solutions was engaged to perform an AWS platform review and enablement project focused on building in the necessary security compliance controls. The project was structured to provide nib with confidence that the appropriate controls had been embedded into the platform, and that nib could provide the necessary regulatory bodies with evidence that Red Queen Platform does not present any significant vulnerabilities.

The major challenges faced by nib at the outset of the enablement project were:

- Digital innovation initiatives were hampered by a lack of platform automation and standardised patterns
- Each business unit was focused on their own project requirements and not the overarching platform requirements
- The cross functional application delivery teams needed to migrate the existing .NET apps to AWS but there was no detailed migration plan or repeatable platform patterns to use
- The AWS Platform had not been matured and needed work to align with nib's guiding principles and standards
- nib didn't have strong AWS architectural skills and experience in undertaking large scale migrations or securing AWS implementations

Business Context The project set out to achieve the following objectives:

- Reduce operational overhead by creating an automated platform that is simple to manage
- Reduce risk by adopting a highly secure and resilient architecture
- Provide business flexibility by scaling the platform resources to dynamically meet demand
- Achieve lower operational costs in comparison to the existing on premise model

Technology Context

The IT operations team at nib realised they needed a more efficient and scalable platform that was also secure and resilient. The team had an emerging DevOps capability however additional expertise in relation to ensuring the platform had all of the necessary security controls built into each environment and its automated processes was required.

Technology and Toolsets:

AWS:

- Internal developed tool for standard deployment 'Sceptre'
- Multiple VPCs, AZs, Subnets, Security Groups, Restricted traffic
- Automated CloudFormation stacks
- Full H/A auto-scaled architecture
- EC2 Container Service
- Elastic Beanstalk
- IAM
- RDS PostgreSQL
- Cloudwatch
- CloudTrail
- Config
- Trusted Advisor

Third Party Tools:

- KMS / S3 for Secrets management
- GitHub Enterprise
- GitHub Enterprise
- BuildKite
- Sumo logic
- CloudFlare for CDN and WAF

Our Role

The CMD Solutions team were engaged to review the existing AWS platform, business objectives, and to form a target state architecture. The team performed a gap analysis and formed a strategic roadmap to help nib transform from the current platform state to a mature, production ready environment. CMD Solutions followed through from the initial advisory and design work to implementation and support activities designed to ensure the nib team were ready to meet the BAU delivery demands placed on the platform.

Delivery Outcomes

Summary of Key Outcomes & Benefits

CMD Solutions achieved the following **outcomes**:

- The CMD team created highly available, resilient AWS design patterns based on finance and insurance industry experience
- Production grade security controls and processes were implemented
- A scalable architecture that can be increased without compromising security controls, using automated infrastructure deployment processes was designed and implemented
- A highly available design across three AWS availability zones has improved the resiliency and availability of the application services
- An efficient platform has been created using a consumption based pay-as-you-go model
- A strong risk and compliance posture has been formed

The following **benefits** were delivered as a result of the project:

- Faster time to market for new applications
- Scalable architecture supporting business growth initiatives
- Enterprise security controls embedded into the infrastructure as code automation improved the organisational risk profile
- Efficient and secure infrastructure platform

The following operational **risks** were reduced as a direct result of the project:

- CMD designed and implemented a solution that provides High Availability and Business Continuity with security controls built into the platform using a low cost consumption based model
- Threats posed by external intruders, malicious insiders and malicious code have been mitigated through the use of high availability and secure architecture for each solution component. This design has ensured the platform is fault tolerant and resilient by avoiding any single point sensitivities and embedding security controls at all layers of the solution