Leveraging the cloud to drive exceptional digital customer experiences for Standard Bank

bbd case study

For Standard Bank, a large South African bank offering personal, business, wealth, insurance and corporate banking, BBD was tasked with creating a highly scalable platform that offers excellent digital customer experiences for their mobile virtual network operator (MVNO) project.

The platform, which includes client-facing portals, was built on the AWS cloud to leverage several of AWS' services to meet the various requirements of the project, including high uptime, scalability and security.

Objectives

- Above all else, ensure customers always have good digital experiences when interacting with the client-facing portals on the system
- Implement a platform that is scalable to meet demand
- Develop resilient software that has a high uptime
- Meet Standard Bank's standards on networking, user access, encryption, and compliance

Benefits

- Autoscaling capabilities enable the system to process thousands of requests per day without delay
- Hosting environment is designed to scale based on predefined metrics, ensuring a consistently performant system regardless of load
- A combination of tools allows the system to recover rapidly from stressed load, attacks and/ or failures with workload components to maximise the system's uptime
- User information and data is protected through various means including encryption and access control to meet the banking landscape's strict regulations
- Project outcomes reached in a fraction of the time enabled cost savings

Overview of the solution

With multiple channels within the bank reselling MVNO products, and with the demand for these products growing every day, Standard Bank challenged BBD to develop systems for their MVNO project.

The MVNO project ingests data from various sources and features client-facing portals. The systems to be developed needed to be always online, able to scale to meet demand and adhere to banking security standards.

To meet these requirements, the solution was built using AWS as the core cloud provider along with various AWS services.

Approach

Scalability

With the growing popularity of the MVNO offering, the influx of traffic is constantly increasing. It is important for the core applications to scale when needed. To achieve this, the code is hosted using two main methods:

- LAMBDA

LAMBDA forms part of the core the MVNO solution – driving the provisioning engine that processes all orders placed by the different consumers in the bank. The solution is built using AWS Step Function which provides state machines orchestrating LAMBDAs. LAMBDAs in turn ship with out-of-the -box autoscaling capabilities which helped the team to develop a system that can process thousands of requests per day without delay.

- EKS

With the power of EKS and Docker, the team was able to deliver a hosting environment that can scale based on predefined metrics. These metrics include CPU utilisation and memory consumption, among others. Metric breaches will trigger a scaling event which will allow consumers to always have a performant system to interact with regardless of the load thrown at it.

Uptime

To keep uptime as high as possible, the system needed to be built resilient and able to recover from stressed load, attacks and/ or failures with workload components. Creating resilience meant starting by creating visibility. To help create visibility of workload events, AWS Cloudwatch and AWS X-Ray were set up. Cloudwatch enabled the team to set up metrics based on various data points. In the event of a metric breach, an alarm is triggered to either perform a task or send out notifications (SNS) for component failures.

By utilising Canaries, the team can monitor critical endpoints on third-party APIs and report failures pro-actively.

To keep the lights on in our EKS clusters, the combination of ECR, Argo and Helm Charts were used. The Kubernetes control plane constantly monitors the health of all applications running on the EKS cluster, while Argo keeps the cluster state in sync with a Git repository (a GitOps approach). In the event of a pod failure, a new one will be created based on the pod definition, as specified in a Helm Chart. The new pod runs a container which pulls the specified image from ECR. This provides a self-healing solution in the event of a workload failing.

All AWS resource management is done with Terraform and the Serverless Framework. Terraform mitigates the risk of errors whilst provisioning new infrastructure, enabling a drastic reduction of time to recover infrastructure.

Scrutiny

Dealing with sensitive data means dealing with scrutiny. To protect user information, Standard Bank enforces strict standards on networking, user access, encryption, and compliance.

- User Access

To prevent malicious code from performing malicious activities on the Standard Bank's environments, all IAM roles are created by using a least privilege approach, whereby roles are created within a bounded set of permissions. This means that only assumed roles are used by services that require them. Any changes to IAM roles are monitored using CloudTrail, while user access to the AWS platform is closely controlled by Standard Bank's active directory.

- Encryption

With a major emphasis on the quality and application of encryption, the client required that two main types of encryptions are applied; encryption at rest, and encryption in transit. By utilising KMS keys, all assets are encrypted at rest where possible, while AWS Certificate Manager helps to manage certificates used to encrypt data in transit.

- Networking

By implementing VPCs connected to the Standard Bank's network through Transit Gateway, access to MVNO applications is limited. Additionally, all outside access is prohibited by the bank and requires a VPN connection.

- Compliance

Due to the sensitive nature of the banking environment, continuous compliance checks are done to make sure our environments comply as required by Standard Bank. Based on these needs, Prisma Cloud was configured to monitor compliance rules on all AWS environments, with simplified remediation using IaC. In the event of a breach, non-compliant config can be easily corrected on all environments. Changes to the environment are, as a result, also version controlled which promotes auditability of the systems.

Impact of BBD's partnership

Leveraging the power of AWS, BBD was able to achieve Standard Bank's goals for the project in a fraction of the time, which also led to great cost saving for them.

Due to the shared responsibility between AWS and BBD, risk on the project is further reduced, resulting in a confidence boost for both BBD's engineers and Standard Bank, as well as the ability to make changes to the system far easier.

Since the launch of the platform, the system has never failed under load, ensuring all customer interactions live up to the client's expectations of digital customer experiences. Furthermore, it is a testament to BBD's abilities within the cloud space and the maturity of the scaling capabilities of AWS.

With the selected combination of tools, customers can enjoy a platform that is always available, responsive and secure.