FinChamps

FourCo facilitates FinChamps' migration to AWS and increases compliance on security, reliability and control.

The Challenge

In 2021, as requirements at FinChamps for new banking customers became stricter, there arose a need to move the SaaS stack to AWS Cloud.

Hans Pragt, Founder and Director of FinChamps:

"At FinChamps, we develop software for filing in the financial world. Think of banks, health insurers, energy suppliers, as well as legal professionals and debt collection organizations. In 2020, two banks decided to equip their special management departments with our web-based package, "CaseControl". Since falling behind on a loan or mortgage often involves sensitive personal information, we were faced with additional stricter requirements from both the AFM and the German BAFIN in the field of security and reliability. To meet these requirements, we had no choice but to say goodbye to our then hosting provider and make the move to AWS."

FinChamps had its hosting with a Dutch ISP, where virtual machines were purchased. The decision to move to AWS was a logical step, but FinChamps couldn't do it alone. Hans: *"It quickly became apparent that we didn't have enough in-house expertise to fully utilize all of the possibilities and functionalities that AWS offers. In our search for an organization that could support us in this endeavor, we evaluated various consultancy agencies and ultimately chose FourCo because we felt they had the necessary expertise to support us effectively while also being small enough to provide us with personal attention."*

The Activities

The transition to AWS was a significant change for the FinChamps team. In addition to setting up the infrastructure, FourCo provided guidance to the software team on containerizing the software stack, configuring a git environment, creating deployment pipelines and participating in security meetings during the onboarding project with a large European banking system that chose FinChamps. Alongside the implementation, FinChamps also decided to entrust the support and management of the AWS environment to FourCo under an SLA.

The Setup

Bas Smit of FourCo: *"Given the privacy-sensitive nature of the data stored in the banking application, we worked with the customer to create an AWS Landing Zone that ensures development, test, and production environments are separated at the AWS account level.*

For large customers, it was also necessary to provide dedicated hosting within their own AWS account, with access granted to cloud administrators through a ‘break glass’ procedure."

<u>Containerization</u>

In the previous hosting environment, services such as the web server and application server were installed directly on the virtual machine, which carried the risk of development and production environments diverging. In consultation with FinChamps, the development team containerized the application, hosting it in AWS using the AWS container service ECS and locally with Docker Compose. Container image building is fully automated via Git(hub) Pipelines.

THE AWS STACK

The SaaS stack in AWS consists of the following Serverless services

- AWS Application Load balancers and Web Application Firewall for secure and high available network access
- AWS Elastic Container Service based on Fargate (AWS ECS) for application hosting
- AWS Aurora Relational Database System (AWS Aurora RDS) as database
- AWS Simple Storage Service (AWS S3) for document and file storage

<u>Low/No-Ops</u>

An important cost component in the total cost of ownership (TCO) of an application stack is the periodic management of a server environment. By choosing Serverless services from AWS where possible, the amount of operational work is minimized.

Additionally, by declaring the entire architecture using Infrastructure as Code based on AWS CDK, new (dedicated) customer environments can be consistently deployed with limited lead time

Availability and disaster recovery

'CaseControl' is a business-critical application. It is essential to have a robust Disaster Recovery (DR) solution that is periodically tested. While the application is already highly available at the primary location across three availability zones, an additional fallback location was deemed necessary.

"The Disaster Recovery (DR) solution was built by creating a shadow environment in another AWS region that is virtually in sync with the primary environment and meets the following requirements:

- Located within the EU due to GDPR regulations.
- Acceptable latency from the EU sites to the DR region.
- Recovery Point Objective (RPO) and Recovery Time Objective (RTO) times of less than 2 hours.
- Meets the same standards regarding audits, security, privacy, etc."

Security and Encryption

Encryption at rest and in transit is crucial when hosting financial applications, especially given the stringent requirements that must be met to ensure compliance. To meet these requirements, specific AWS Key Management Service configurations were implemented, which were then encoded into the Infrastructure as Code. This approach ensured that the same policies were consistently applied throughout the entire stack

Secure communication

A module in the application stack involves the secure exchange of files between the SaaS application and on-premises customer systems. To ensure secure communication and message signing, a PGP framework was established in collaboration with the system bank. Additionally, all incoming and outgoing communication from the platform is screened by Web Application Firewalls

Security Event and Incident Management

One of the requirements of the AWS platform is to monitor security events. To achieve this, a selection has been made from the AWS CloudTrail audit log, which is processed in dashboards and alerts. A subset of events is monitored, including:

- Successful or failed logins on AWS console, CLI, and API
- Changes to firewall rules (Security Groups)
- Changes related to database access
- Modifications or stops to the Audit Log
- Mutations on IAM policies and roles
- Customizations related to AWS user account credentials.

Implementation process and methodologies

The infrastructure was constructed using the Kanban method, which was applied to several phases of the implementation process, including:

- Initial setup of the AWS environment and deployment of the Landing Zone
- Design and establishment of infrastructure blueprint for hosting
- Parallel processing of tasks
    - Construction and acceptance of reference implementation based on the design
    - Guiding application developers on containerization and CI/CD
- Adjustment of necessary controls for the SIEM
- Attendance at weekly project and security meetings with the end customer teams of the system bank and providing evidence for compliance teams
- Conducting pre- and post-GoLive Disaster Recovery tests and delivering results.

Guidance and knowledge transfer

A crucial aspect of our collaboration is the intensive knowledge transfer and guidance provided to the FinChamps technical team. Through hands-on work, comprehensive documentation, and code reviews, we have enabled them to work independently with their AWS environment and the CI/CD setup.

Furthermore, even after the migration, FourCo remains involved in maintaining and updating the AWS infrastructure, as well as supporting ongoing development.

Working Together

Hans Pragt about the collaboration: *" The collaboration over the past 2 years has taught us that we made the right choice. It has been a pleasant, open, and proactive collaboration with predictable costs. Perhaps the best evidence of our success is the fact that in a recent pentest conducted by one of our clients, zero findings were reported!"*

About FinChamps

FinChamps, an organization of leaders from the financial world, supported by progressive software developers with years of experience in credit management, debt collection, fraud, special management and other financial applications.

Contact:
Hans Pragt, Director,
hp@FinChamps.com
www.finchamps.nl

FinChamps

About FourCo

We are proud of our highly experienced, professional team and loyal customers. We strive to deliver the best cloud and infrastructure solutions for our customers. We are open and honest professionals and enjoy working with our clients as part of their team.

Contact:
Arjen van Wijngaarden, Partner
arjen@fourco.nl
www.fourco.nl

FOURCO