THE BASE TALPA NETWORK CASE STUDY

Name of the customer: Talpa Network

Start date of the project: 8th July 2019

Date when the project entered production: 1st November 2020

End date of the project: Active development in progress

About the Customer

Talpa Network is the new name for the Dutch company in which John de Mol has consolidated his Dutch multimedia activities. Talpa Network consists of Talpa TV (SBS6, Net5, Veronica and SBS9), Talpa Radio (538, Sky Radio, Veronica and Radio 10), Talpa Social (Social1nfluencers), Talpa Digital (KIJK, JUKE and VoetbalTV), Talpa Events, and the e-commerce division (Vakantie Veilingen, Actievandedag and Ticketscout). All these companies are supported by Talpa Media Solutions, Talpa Platform, and Talpa Creative. This extensive network makes the Dutch multimedia company relevant and desirable for both consumers and advertisers.

Customer Challenge

The onboarding process for new projects on AWS was a very slow process for Talpa Network; infrastructure was not standardized and centralized. Some of the project environments were hosted in a single AWS account; maintaining this kind of mixed infrastructure became a real challenge for the company.

As a fast-growing company, Talpa Network needed a fast, secure, standardized, and centralized infrastructure for each new project. Each project consists of multiple environments and uses standardized platform tools for planning, development, testing, logging, and monitoring. The solution had to be integrated with the existing tooling of choice and all projects needed to be part of the centralized organization structure within a single AWS Organization.

AWS available solutions were considered versus building a custom solution from scratch to be tailored for the Talpa were considered as options and Talpa already had Solution Architects with hands-on experience building custom "Landing Zone" solutions for managing multiple accounts.

Later one was chosen as it represented a better fit to internal organization, way of working, and tooling in use.
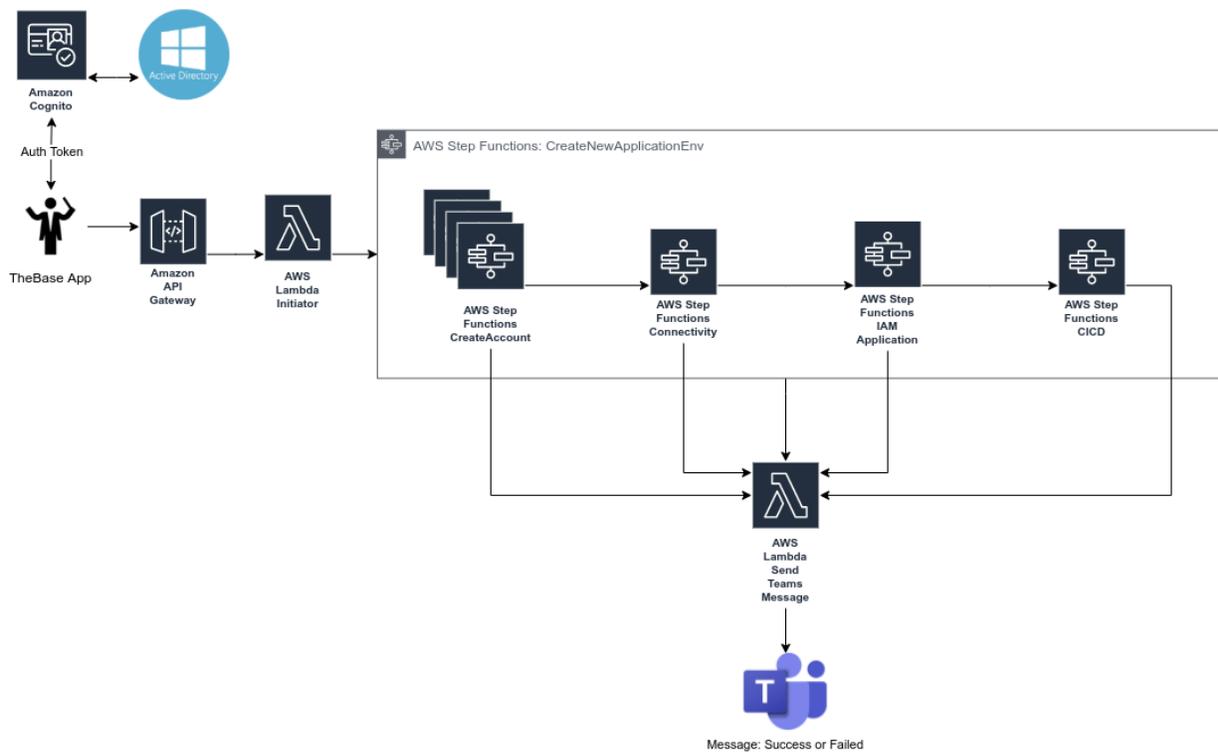
The Solution

The solution was to build a "one-stop shop" for provisioning and configuring accounts. The product "The Base" is an automated solution for provisioning the Development, Test, Acceptance, and Production project environments. Each created AWS account has strictly defined and centrally managed networking, securely connected to all existing internally used tooling related to CI/CD, monitoring, dashboarding, documentation, project management, and code quality assurance services authorized against an Active Directory. AWS available services like AWS Config and AWS Guard Duty are preconfigured for each project environment for security analysis, audit, and threat detection and managed on a central level.

Backend services are delivered entirely with AWS serverless components (API Gateway, AWS Lambda, AWS Step Functions) and authorized with Cognito.

The developed workflow is a controlled and monitored process with integrated notifications for events of interest. DynamoDB is used for storing inventory information about deployed environments.

The Lambda functions are written in Python, using a serverless framework; infrastructure is described in CloudFormation templates.

Results and Benefits

The Base represents an excellent example of collaboration and co-creation between Levi9 and Talpa, leveraging expertise, existing knowledge, and hands-on building tailored and optimized solutions entirely based on serverless.

With this solution, the onboarding of new projects in the company became an automated process, simpler and faster. The creation of Development, Test, Acceptance and Production accounts takes less than an hour. Each account is aligned to internal standards and has all tools for CI/CD, monitoring, code quality assurance pre-deployed in it.

The solution led to a shift of the focus of the development teams to solve business problems instead of provisioning infrastructure and managing it.

The automated workflow also delivers the following benefits:

- Compliant infrastructure based on Talpa Network Security policy

- Centralized identity management

- Integration with existing tooling in use

- Improved security with real-time monitoring and automated actions