MethodData

CASE STUDY

IBIWeb Single Sign On (SSO) Solution

Integrated Benefits Institute (IBI)

Introduction

IBI is the leading research organization in health and productivity, the Institute provides the data, research and tools professionals need to make sound decisions in how they invest in the health of their workforces. The project required the use of an Identity Provider (IdP) to broker Single Sign On (SSO) between their CRM and other 3rd party data providers. In addition, the solution needed to cater for SSO user management and ongoing maintenance.

IBI had a requirement for an intuitive and easy method for users that have successfully logged into the company's CRM (HubSpot), to be automatically logged into 3rd party provider portal, at the simple click of a button. The button click should redirect the user and log into the portal using SSO with the correct permissions and access levels based on their current membership types in their CRM The solution was to also facilitate automatic user management, meaning that when a user is created, updated or deleted in HubSpot, it should also automatically get created, updated or deleted in the Identity Provider (IdP) and the data provider.

Business Challenge

Other SaaS SSO solutions (including popular solutions such as Okta, OneLogin, and Azure Active Directory) were considered but turned out to be unfeasible due to the financial considerations of these services that typically bill on a per user per month basis. Using these solutions meant that costs would increase dramatically as the business scaled. The client also required users to be automatically managed in both the IdP and data provider based on user activity in their golden source: the HubSpot CRM.

AWS Solution

KeyCloak (an open-source software product allowing single sign-on with Identity and Access Management with SAML aimed at modern applications and services) was chosen as the SSO technology of choice. This would allow the app to be securely self-hosted in the AWS Cloud at a far more acceptable price-point, as it would allow the number of users to scale without incurring any additional monthly cost as their customer base grew.
AWS Services Used:

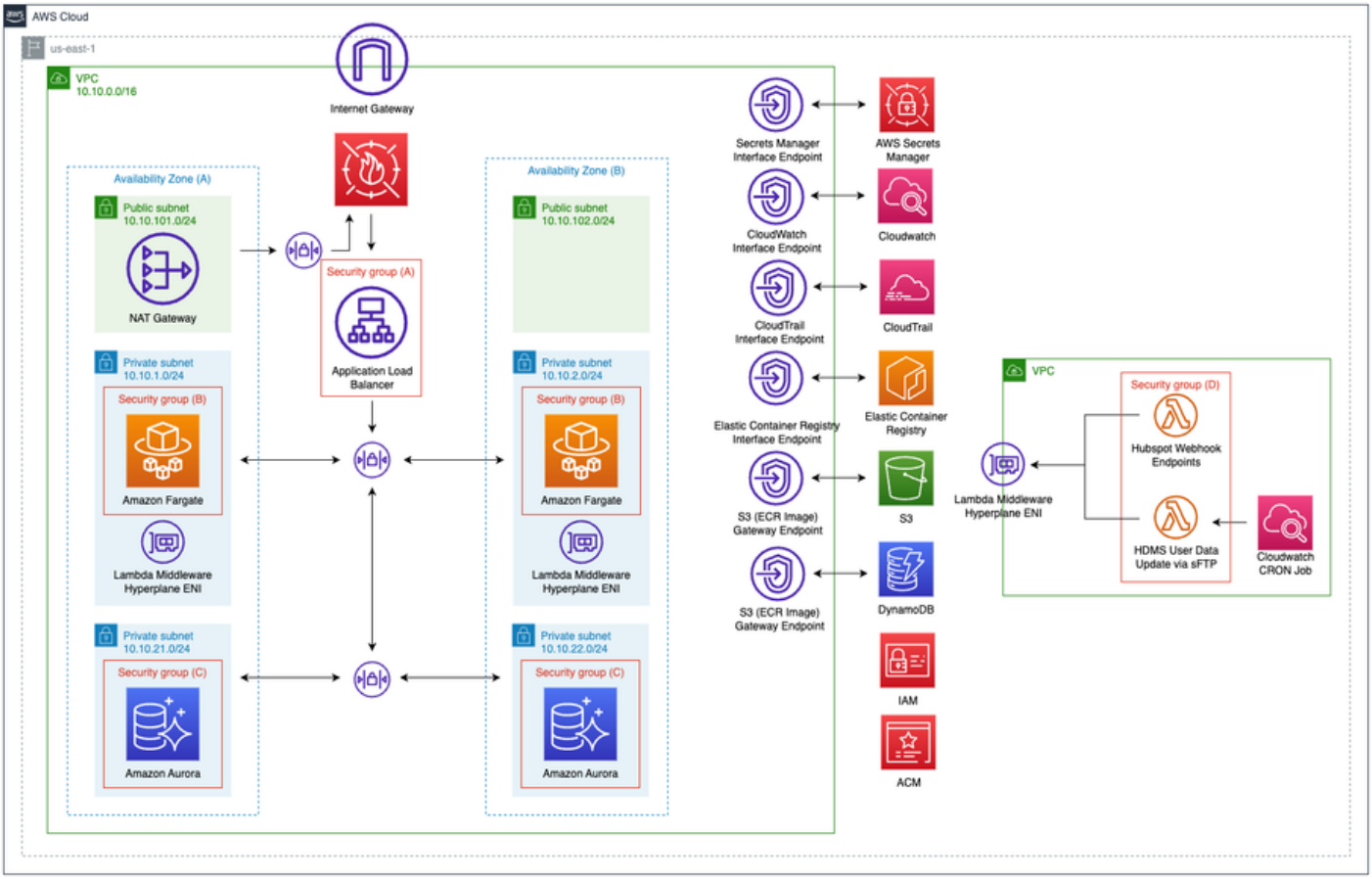
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Aurora Serverless v1 and v2
- AWS Fargate
- Amazon DynamoDB
- Amazon CloudWatch
- AWS CloudTrail
- AWS Config
- AWS Control Tower
- AWS Organizations
- AWS Well-Architected Tool
- Amazon Virtual Private Cloud (Amazon VPC)
- Amazon Route 53
- Amazon GuardDuty
- AWS Certificate Manager
- AWS ECS
- AWS Key Management Service (AWS KMS)
- AWS Secrets Manager
- Amazon RDS
- AWS IAM Identity Center
- AWS WAF
- AWS Lambda
- Amazon SNS
- Amazon S3
- AWS Fargate

Implementation

A comprehensive collection of AWS accounts were created via **AWS Control Tower** in accordance with **AWS best practices**. These included (but are not limited to) separate Management, Audit, Logging, Security, Production and Development Accounts.

Furthermore, Terraform and Terragrunt was used as infrastructure as code platform to automatically deploy and maintain all AWS infrastructure via code. We made use of an **AWS quick start guide** to ensure best practices for KeyCloak deployment and extended the security due diligence by making sure all application, network and environment security best practices were followed. This was accomplished by locking down and minimizing traffic through Firewalls, Security Groups and NACLs, and by making use of internal VPC Endpoints. **AWS Secrets Manager** and **ACM** was both used to ensure secure communication and encryption at every available layer.

Building and implementing the middleware SSO user management and self-hosted IdP solution was straight forward and we didn't encounter any major obstacles here. Our team gained tremendous insight on how SSO SAML 2.0 works in the progress.



Results / Outcome

The final outcome was a comprehensive, secure, and affordable SSO solution that scales in performance, and not in cost, while the client's business grows. At the time of writing ~5000 users were added to the SSO solution which would have cost ~$5000 p/m if conducted through an equivalent SaaS platform. Our solution averages about ~$500 p/m which results in a 10x cost saving for our customer. As an added bonus, our solution also manages SSO Users through middleware hosted in AWS on behalf of the customer and their 3rd party data provider at virtually no additional cost.

TCO Analysis

The following cost factors were analyzed, quoted, and approved before development started:

For CapEx purposes:

- AWS Infrastructure setup and configuration through cloud formation
- Solution and Middleware implementation and Development cost

For OpEx purposes:

- AWS Infrastructure costs
- AWS Business Support costs
- Partner maintenance and continuous support

Lessons Learned

Utilizing infrastructure as code from the beginning of the project ensured that we could constantly inspect, improve, and redeploy our infrastructure at speed. Re-deployments were seamless and provided reproducible and consistent results. It now provides us with the opportunity to reproduce this solution, with best practices included by default, for any number of customers in the future.

AWS Control Tower and Organizations turned a complex, multi-account organization and resource infrastructure construct into one which is simple and accomplished with just a few clicks. The multi-account setup is used to isolate different aspects of the project and therefore enforce security. It enabled the team to learn about, and quickly deploy best practices that we could rely on.

The guidance and insight provided by working through the AWS Well Architected Framework and Well Architected Tool were extremely valuable to the entire team. We were able to discover areas that required more attention, verify that parts of the solution were following best practices, and gain insight into aspects of the project we had not yet even considered. While we did make use of the Well Architected Tool towards the end of the project, we will be using it in future projects as a 'check-in' tool that will be used throughout development. Apart from providing guidelines and educational resources, it jump-starts the process of making use of and learning about, best practices in every aspect of the project.

As this is a security solution, the team was exposed to, and implemented, many security best practices - making full use of KMS and at-rest/in-transit encryption, implementing VPC Endpoints for AWS Service communication, and leveraging security-oriented services like WAF and GuardDuty to name a few. These are learnings our team, can now take into all future projects.
An area of improvement for the team as they enter into future projects, is the order in which architectural improvements were made. Many of the architectural changes altered the flow of data within the solution - for example adding VPC Endpoints to AWS services. This resulted in previous network security measures (such as security groups and NACLs) being obsolete in the evolved deployment. Time was spent continuously tweaking the network security as the architecture evolved, however, this process would be better left to the end of the infrastructure development process to lock down the final version of the infrastructure.

Conclusion

This custom SSO solution enables IBI's customers to use a single password for logging into their private content on HubSpot, and for clicking through to the analytics provider content. Even better, is that this results in an overall better user experience for IBI's end-users at a 10th of the cost of a traditional SaaS SSO solution. In addition, it automatically manages and synchronizes all these users across both the systems, saving IBI valuable time and money by not having to manually create and update users in multiple systems. Due to the complexity and high security requirement of the project, our team gained significant experience in AWS tools which will serve us well on our next projects.