ALPHA OMEGA INTEGRATION

CASE STUDY

Serverless Identity and Access Management (IAM) in AWS Cloud

aws partner network

Select Consulting Partner

Public Sector Partner

Overview

The Enterprise Cloud offerings and the Enterprise Business application offerings have matured significantly in the last 15 years. Many enterprise business applications and use cases have been migrated over multiple times to cloud services contributing to the mature Cloud-First architecture patterns. Rise of Serverless offerings add a radically different approach to Cloud-First architecture by forcing everything to be micro-services.

Alpha Omega Integration is a federal and commercial Cloud and System integrator with multiple digital transformations, cloud migrations, and enterprise modernization achievements under its belt. From High Performance Computing to Content Management, we have a success story for every critical use case across the spectrum.

American Institute of Architects is a premier Non-Government Organization (NGO) that provides membership and knowledge services to around 90,000 building architects across the world. In addition, more than 600,000 members of the Architecture, Engineering and Construction (AEC) community leverages AIA's services such as Contract Documents for industry standard contracts and forms. Alpha Omega has been a partner to AIA in its enterprise modernization and digital transformation efforts. This case study focuses on the IAM component of AIA IT infrastructure and how it benefitted from Cloud-First architecture and primarily use of Serverless Technologies.

Serverless – More than a Buzz word

Let's get our terminology clear: Serverless DOES involve servers. As a matter of fact, everything that runs on cloud runs on servers. The "less" part of the Serverless implies that, to run our applications, we don't need to manage servers (physical or virtual) or its configuration, patching, security or lifecycle. We get to focus on the application components (services) to be implemented and cloud vendors determine the right way to run them and scale them based on demand. It does induce a little bit of nervousness for the new adopters of Serverless since there are no "tangible" servers or virtual machines to manage. In addition, the orchestration of micro-

services in a Serverless world is little more complex than typical micro-services architecture. Despite these challenges, Serverless adoption has been exploding in enterprises and more recently in federal government due to its cost benefits, true scalability, and increase in service offerings from all three cloud providers.

Serverless services come in various forms, from individual function execution (AWS Lambda, Azure Functions) to the managed databases that scale horizontally (Google CloudSpanner DB) and everything in between. The real challenge lies in leveraging them for the right use case in an enterprise architecture.

Problem: IAM Hindering Business Scalability

AIA's legacy Identity and Access management infrastructure was implemented using JanRain and a Membership Management Commercial-off-the-Shelf (COTS) platform. The membership COTS platform was the source of identities as it managed the member and subscription lifecycle. JanRain managed the Delegated Authentication, Single-signon, and Access Management. Since the Membership COTS is the main source of identities and user profiles, every authentication request and part of authorization requests are delegated to it.

As the AIA's member base grew beyond 500K, the ability of Membership Management COTS to serve the IAM function with JanRain started to show cracks under the unpredictable and non-uniform workloads. The immediate remedy was to vertically scale Membership platform and JanRain servers. As the workload increased, improvements in capacity were minuscule compared to the capital investment needed. In addition, AIA has added new offerings for members and have deployed new custom applications that use the same IAM infrastructure. Although JanRain could theoretically scale to the demands of these additional users and applications, it was constrained by the membership platform's ability to scale and its lack of elasticity in underlying data center infrastructure.

Solution Possibilities - Think Cloud-First!

AIA's ongoing migration to AWS cloud was not only an opportunity for Alpha Omega to overhaul the IAM services, but also to rethink the potential solution in Cloud-First paradigm. Considering AIA's key IAM requirements such as scalability, maintainability, and speed to market at lower cost, it was easy to eliminate On-Premise IAM products due to long implementation times, upfront license costs, and specialty skills requirements. Open source IAM products, although may not incur license

costs, require specialized skillsets, thus adding to the implementation costs, and lower maintainability.

The option of an Identity-as-a-Service (IDaaS) platform was enticing due to speed to market and scalability features. Considering AIA's mid-size user base (currently standing at 600K) and simplicity of onboarding, authentication, and authorization workflows, the IDaaS wasn't cost effective considering investment in licenses and specialized skillsets.

Architecture - Server "Less" or "Full"

With a Cloud-First solution and AWS as a Cloud provider, choosing AWS Cognito User Pools was an obvious choice. Developing solutions around Cognito required a close look at the IAM needs of AIA, primarily:

- Reduce unwarranted load on the Membership COTS servers resulting from Authentication and Profile reads from integrated applications
- Provide faster response times, uniform Sign-on experience, and very high availability in the face of unpredictable peaks
- Scale the IAM capacity as the number of users grow and in turn implement true pay per use model
-

It was the last need statement that tilted the scale in the favor of Serverless for Alpha Omega's Cloud Architects.

> Alpha Omega's analysis of solutions alternatives concluded that a Serverless IAM solution provided an optimum mix of good return on investment, architectural simplicity, and required scalability. It also provided a true *pay as you go* model without any minimum license requirements and full control over IAM data.

Alpha Omega's "To-be" architecture leverages the Serverless backbone for IAM services using AWS Cognito, Lambda, DynamoDB, and Aurora MySQL Serverless. The new architecture directs authentication and authorization requests to Cognito, Lambda APIs, and AuroraDB. Cognito hold the user identity and password where as AuroraDB holds replicated User Profiles and Role information from membership COTS. The user profile and roles information is staged in DynamoDB until AuroraDB has completed replication. This ephemeral data staging allows authorization to work transparently during a tiny period of replication.

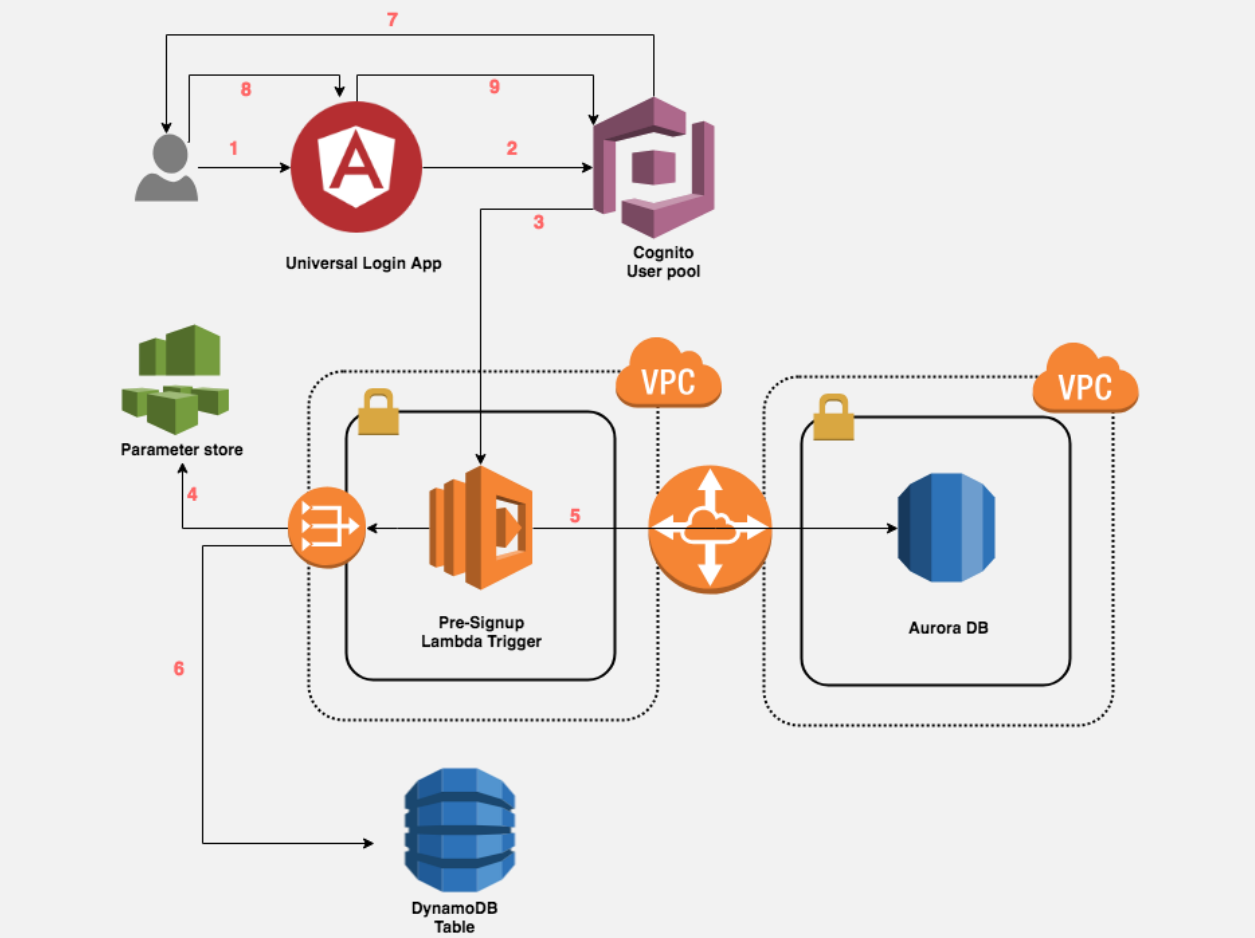
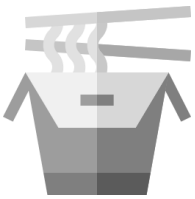


Figure 1: Alpha Omega's Serverless Architecture on AWS provides true elasticity per unit increase in user base

The uniform Authentication experience is delivered through the APIs running on top of this backbone with UX delivered by Angular6 application served through AWS S3 and CloudFront.

Takeaway

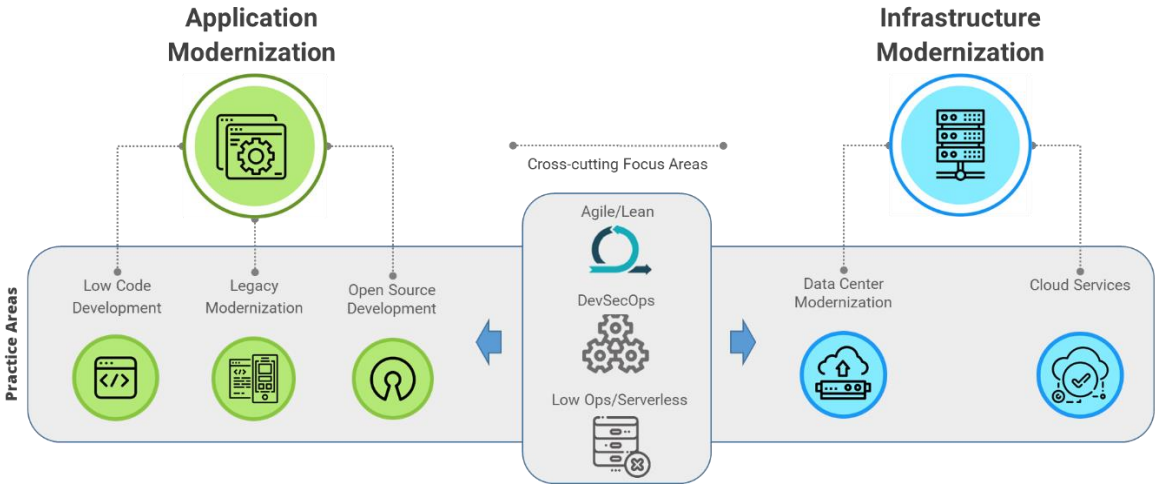


The Serverless Cloud offerings have brought a paradigm shift in Cloud-First architecture. They require a whole new way of thinking of how traditional use cases such as workflows, security, and data management can be architected so that they do not impede true potential of serverless services. Alpha Omega's Enterprise Modernization practice offers proven and mature Serverless Architectural patterns for most common and not-so common use cases. We invite you to engage with us to get onboard with Serverless revolution.

ALPHA OMEGA INTEGRATION

CREATING NEW POSSIBILITIES

Alpha Omega Integration is a technology firm with special focus on cloud first modernization. Headquartered in Tyson Corner VA, Alpha Omega provides Cloud Architecture, Application Modernization, Serverless Implementation, Legacy Operations & Maintenance (O&M), and Data Center modernization services. Our customers include Federal Agencies such as Dept. of State, Dept. of Defense, National Oceanic and Atmospheric Administration (NOAA), Dept. of Agriculture (USDA), and non-governmental organizations such as American Institute of Architects (AIA).



Alpha Omega's Disruptive Innovation Group (DIG) manages multiple Practice Centers under our Application and Infrastructure Modernization practice. Our Agile Lean practices, DevOps toolset, and Low Ops/Serverless focus area span across our services providing efficient cloud ready architecture to our customers.

Alpha Omega is a Select AWS Consulting partner.