Strengthening Identity and Access Management with a Secure Architecture in AWS

Executive summary

500 Latam is a venture capital company with the mission of enhancing individuals and economies worldwide through entrepreneurship. Entirely focused on markets where technology, innovation, and capital can generate long-term value, thus driving economic growth.

The challenge

Previously, 500 Latam's workloads were spread across two separate accounts, which complicated identity management and resource access control. Additionally, their existing architecture showed vulnerabilities, including potential networking threats like unauthorized access to resources.

Why AWS?

AWS provides a combination of flexibility, security, auditing, management, and a comprehensive set of services that make it appealing for transitioning from single-account (or uncentralized multi-account) to centralized and secure governance of multi-account, multi-users environments, especially, for organizations seeking to leverage cloud infrastructure effectively and efficiently.

About Costumer

Figure 1 – 500 Latam Logo

The parent company stems from 500 Global, founded in 2010. In 2011, they consolidated 500 Latam in Mexico City, becoming one of the most active early-stage investment funds in the world.

> *"We have a mission: to help the most talented Spanish-speaking entrepreneurs in Latin America build successful companies".*

“Amazon Control Tower with Organizations.”

Amazon Control Tower simplifies the administration and governance of **multi-account** cloud environments in AWS, enabling organizations to maintain **security** and **efficiency** in their cloud operations.

The Solution

The most effective way to address this situation is to prepare a landing zone for configuring and governing a multi-account environment, as the task at hand involves diversifying workloads across different environments, such as Development, UAT, and Production.

AWS Control Tower plays a significant role in this challenge as we use it to automate the creation and initial configuration of accounts and resources. This ensures consistency in implementation and establishes AWS-recommended best practices, enhancing security and operational efficiency.

Additionally, with AWS Organizations, we have established a hierarchical organizational structure, allowing clear segmentation of accounts based on organizational units (OUs). This provides a solid foundation for resource management and policies.

Besides, it’s crucial to leverage IAM Identity Center as a centralized solution for identity management to simplify access and permission administration across accounts, providing a centralized layer for security and control.

On this journey, AWS Control Tower took on the responsibility of orchestrating and monitoring the multi-account environment, allowing us to proceed with the seamless migration of resources that flowed through an account to their respective environments.

In summary, these initiatives enabled us to assist in building a secure, multi-account (and three-tier) architecture for their workloads. The architecture strengthens identity and access control through the implementation of the Least Privilege principle, policies, roles, guardrails, as well as enhancing visibility and monitoring.

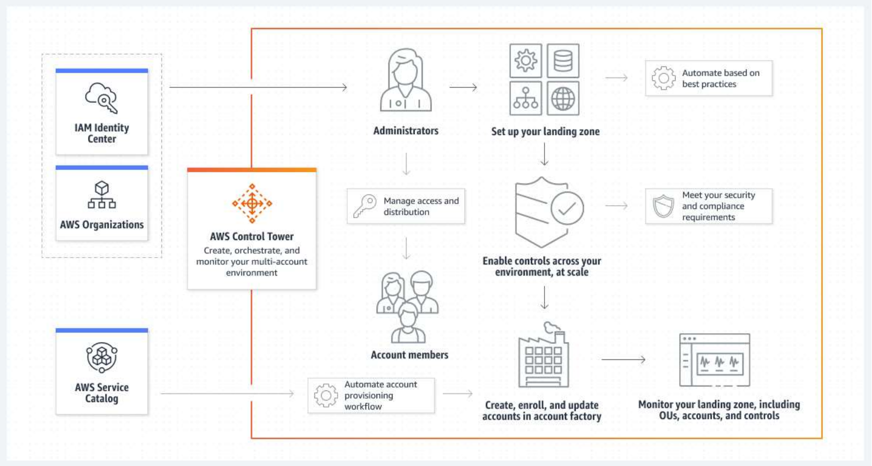

IAM Identity Center
AWS Organizations
AWS Service Catalog
AWS Control Tower
Create, orchestrate, and monitor your multi-account environment
Administrators
Set up your landing zone
Automate based on best practices
Manage access and distribution
Enable controls across your environment, at scale
Meet your security and compliance requirements
Account members
Automate account provisioning workflow
Create, enroll, and update accounts in account factory
Monitor your landing zone, including OUs, accounts, and controls

Figure 2 – AWS Control Tower

Best features of the Landing Zone

- **Organized Structure**
- **Security and Compliance**
- **Key Provisioning**
- **Identity Management**
- **Scalability and Flexibility**

Results and Benefits

We start with the implementation of a Landing Zone, aiming to plan a proper multicount management among the various organizations that were agreed upon for construction within the infrastructure environment and its different workloads. The use of a Landing Zone provides several benefits:

Organized Structure

Establishing an organizational structure in AWS by configuring organizational units in AWS Organizations. This facilitates the logical organization of accounts, which is crucial for the efficient and secure management of resources.

Security and Compliance

Provides automated configurations and controls that enable the implementation of consistent security and compliance policies across all accounts. This is essential to ensure a secure environment and comply with regulatory requirements.

Key Provisioning

AWS Control Tower automates the initial deployment of infrastructure according to AWS best practices. This includes the configuration of AWS Organizations, AWS accounts policies, and other key settings.

Identity Management

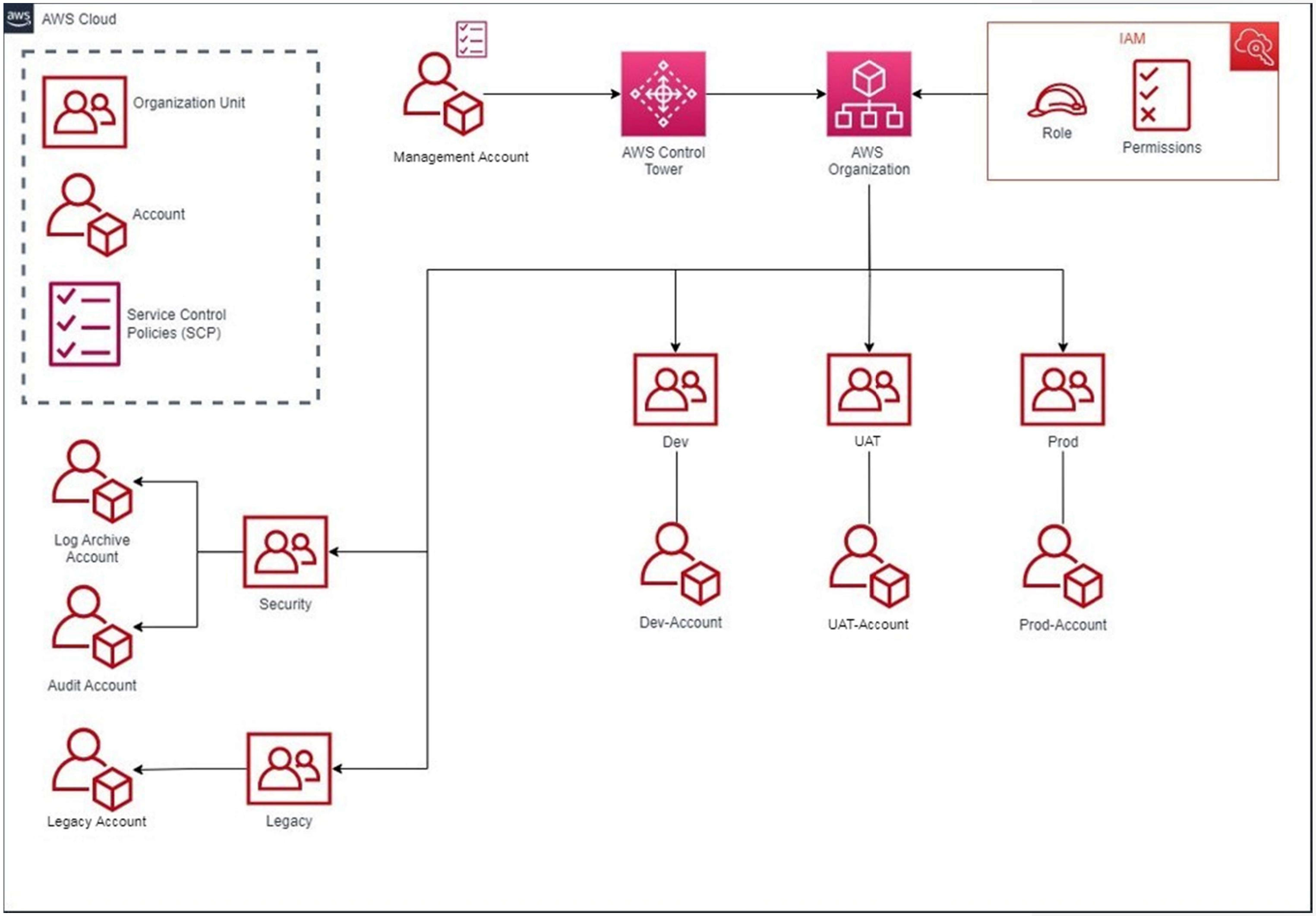
Facilitates centralized identity management through the configuration of IAM Identity Center. This simplifies access and permission management across accounts, which is crucial in a multi-account environment.

Scalability and Flexibility

Provides a scalable and flexible foundation that allows for the addition of new accounts, adoption of new practices, and adaptation as requirements and infrastructure evolve.

500 Latam

High level solution diagram



Next Steps

This is not the first time that ***500 Latam*** has worked with AWS services, as they had their workloads in the cloud. However, they are pleased with the project and are now looking to implement new functionalities into their infrastructure, such as high-level CI/CD integration, for the complete consolidation of their business on the AWS Cloud.

Organized Infrastructure

This solution provides optimal multi-account management, flowing through environment distribution for distinct types of workloads.

Security and Compliance

Ability to implement security and compliance policies across all accounts for a regulatory requirement.

Scalability and Flexibility

You can add different accounts through organizations and apply best practices to each one at any time. Highly flexible.

About IO Connect Services

IO Connect Services is a company specializing in Information Technology Consultancy Services. All our team members have one thing in common: our enthusiasm for technology and our passion for customer service excellence. We provide services in all North America, LATAM and Europe. Our headquarters are in NYC metropolitan area, and we also have offices in Guadalajara, Mexico and Madrid, Spain.