Advanced IAM Security on AWS

AWS Security and Identity Management Case Study

Executive Summary

GoPanza is a company that develops an e-commerce SaaS platform focused on the digital transformation of grocery stores. Its platform uses artificial intelligence to provide shoppers with a convenient in-store shopping experience via mobile and desktop devices, with the ability to pick up their orders or have them delivered to their doorstep, allowing grocers to access the most efficient way for retailers to grow in the convenience economy.

The Challenge

GoPanza wants to migrate its Azure resources to AWS to take advantage of the significant benefits offered by AWS's advanced services and secure infrastructure. GoPanza's main goal **is** to create a robust and reliable infrastructure, improve the availability of the current architecture, and keep costs within the allocated budget. A crucial part of this challenge is strengthening identity and access management with a secure architecture, using specialized AWS tools and services. The transition to AWS requires rigorous identity and access management to ensure that only authorized people and services can interact with **GoPanza** resources.

Why AWS?

AWS offers a wide variety of services and solutions that can meet specific customer needs. With the right configuration, it is possible to obtain a powerful and low-cost architecture.

AWS infrastructure is robust, flexible, and scalable, with advanced security, high availability, and disaster recovery capabilities. Services such as Amazon RDS, Amazon ECS with Fargate, and Amazon OpenSearch not only improve operational efficiency and reduce costs, but combined with advanced tools such as AWS Organizations, AWS Control Tower, and AWS Identity and Access Management (IAM), they also strengthen security. These tools enable centralized and secure management of multi-account and multi-user environments, allowing customers to leverage cloud infrastructure more efficiently and focus on innovation and growth of their business.

About the customer

GoPanza digitally transforms brick-and-mortar grocery stores with its grocery e-commerce platform.

"Create an online store that complements your physical location, while adding tools to improve sales and margins."

GoPanza has twice been chosen as the "Platform of Excellence for Online Shopping" in MIDA's Consumer XRay in 2019 and 2020.

Their small but mighty team has more than 50 years of combined experience.

"Security and Identity Management".

It refers to protecting and controlling access to resources and data within an AWS environment, ensuring that only authorized users and services can access them.

This feature can be achieved through specific configurations and services such as AWS Identity and Access Management (IAM), AWS Organizations, and AWS Control Tower.

The Solution

To migrate **GoPanza** resources from Azure to AWS and build a robust, reliable, and resilient infrastructure, the IO Connect Services team conducted extensive research into the services AWS offers. It was critical to select the right services to meet the customer's specific infrastructure requirements.

A strategy was defined to replicate the infrastructure on AWS using services such as Amazon RDS for databases, Amazon ECS with Fargate for compute instances, and Amazon OpenSearch for search engines. The infrastructure had to adapt due to differences in the operation of some services, applying the best configuration for each one.

To address and improve the customer's current situation, the databases were moved to Amazon RDS instances with SQL Server, using a Multi-AZ deployment to ensure high availability. The use of automatic backups was recommended to ensure data availability and integrity, aligning with AWS best practices and recommendations.

Amazon ECS with Fargate was used to host the container-based application. AWS Fargate provides high availability through multiple hardware instances and auto-scaling based on customer needs, always ensuring high performance. To index and make data easier to access, Amazon OpenSearch was deployed. This service allows the creation and replication of instances in different availability zones with automatic scaling, ensuring the reliability of the data and the entire architecture.

In addition to the above, the IO Connect Services team combined managed database, compute, and search engine services with advanced governance and security tools, such as AWS Organizations, AWS Control Tower, and AWS Identity and Access Management (IAM). These tools allow for the implementation of granular access policies, multi-factor authentication, centralized account management, and continuous monitoring, ensuring a secure and well-managed environment.

"AWS Control Tower and AWS Organizations".

The joint deployment of AWS Control Tower and AWS Organizations offers numerous benefits, including simplified initial setup, automated compliance with security and governance best practices, and centralized management.

This provides a clear structure for policy and permissions management, ensuring that cloud resources are managed consistently and securely across the organization.

The Solution

A strategy was defined using AWS Organizations and AWS Control Tower to orchestrate the workload and integrate security solutions into a three-tier architecture, while AWS Identity and Access Management (IAM) was implemented to securely manage access to AWS resources.

Multi-Account Landing Zone and Governance

To meet account orchestration and governance requirements, a landing zone was deployed using AWS Organizations and AWS Control Tower. This landing zone makes it easy to set up and govern a multi-account environment, automating the initial creation and configuration of accounts and resources. This ensures consistency in deployment and establishes best practices recommended by AWS, improving security and operational efficiency.

Multi-Account Strategy

AWS Organizations enabled the establishment of a hierarchical organizational structure based on organizational units (OUs), providing a solid foundation for resource and policy management.

Orchestration and Monitoring

AWS Control Tower orchestrated and monitored the multi-account environment, enabling a seamless migration of resources from a single account to their respective segmented environments. This approach reduced the risk of vulnerabilities and threats and facilitated regulatory compliance by separating access to resources.

Based on the above, it was first necessary to create a multi-account structure with their respective Organizational Units (OUs) and the necessary configuration that consisted of the following:

- A landing zone at us-west-2 (Oregon)
- An organization with:
    - Management Account
    - Security OU with Log Archive and Audit Accounts
    - OU Dev with Dev Account
    - OU Prod with Prod Account
    - Current Account

AWS Organizations Terminology

- **Organization:** An entity that is created by combining a set of AWS accounts.
- **Invite:** The process of inviting another account to join an organization.
- Organizational Unit (OU): Serves as a container for accounts within a root.
- **Account:** A regular AWS account that contains all your AWS resources.
- **Root:** The parent container that houses all consolidated accounts in an organization.

The Solution

Identity and Access Management

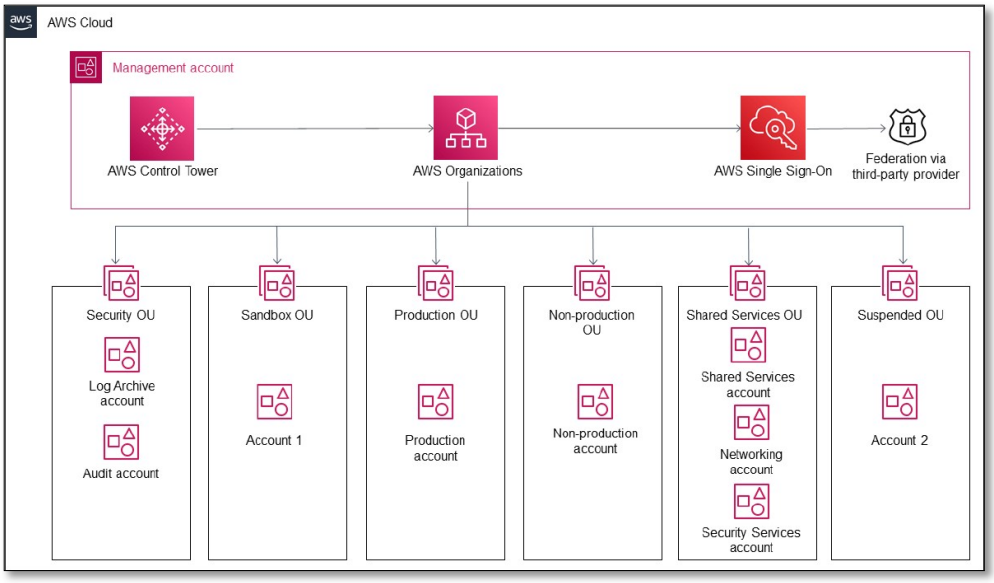
AWS Identity Access Management (IAM) was implemented as a centralized solution for identity management, simplifying access and permissions management across accounts. This provided a centralized layer for security and control, reinforcing the application of the principle of least privilege, policies, roles, and guardrails.

Identity Security

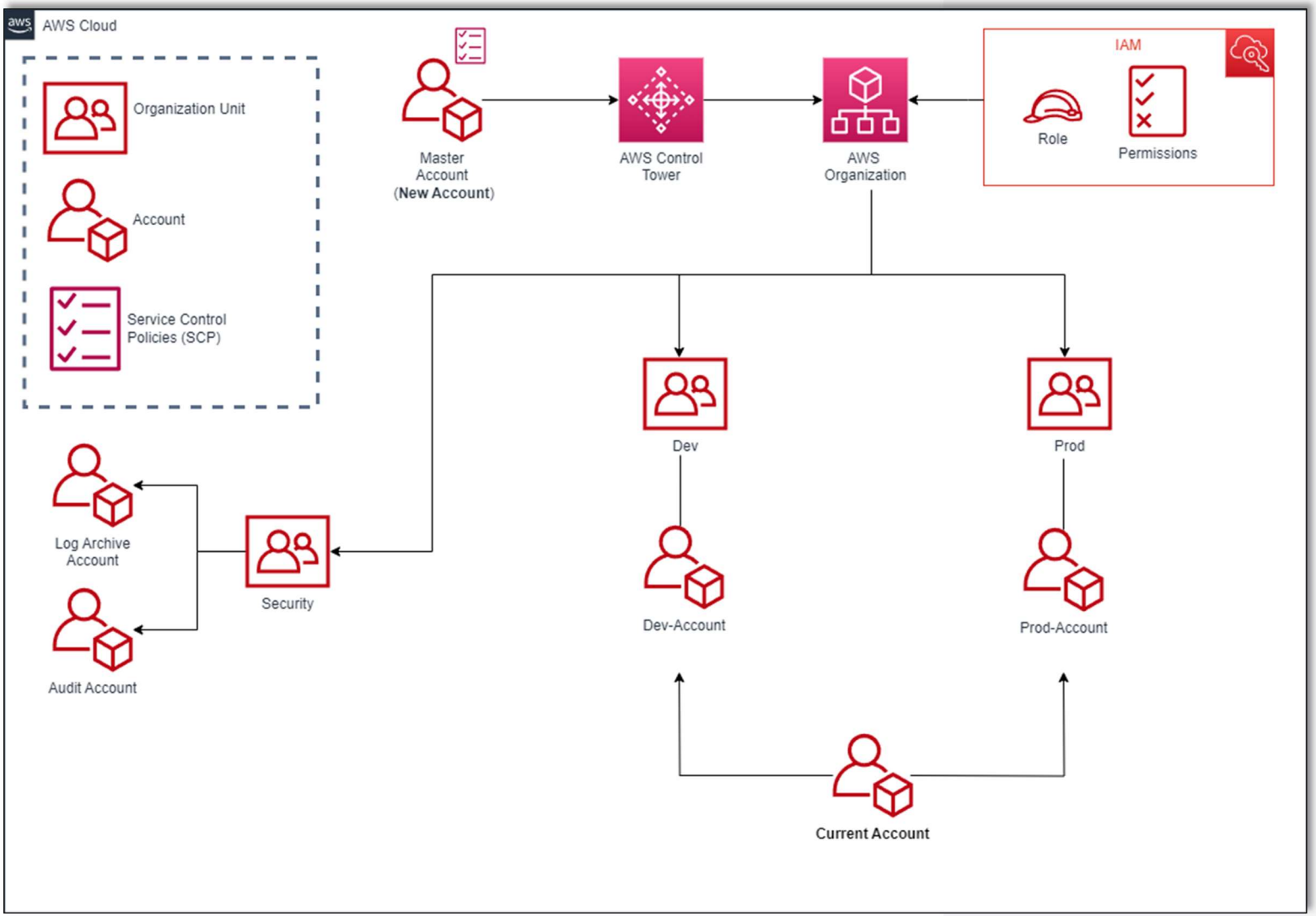
AWS IAM Identity Center (formerly AWS Single Sign-On) was used as the primary tool to manage the environment, helping to securely create or connect workforce identities and centrally manage access across AWS accounts and applications. A crucial hierarchy was established for working on infrastructure and using least privileges based on user level.

Level Structure:

1. **Root User:** Creates administrative users and grants them permissions to access their environments. It also gives access to administrative users to create additional users themselves.
2. **Administrative Users:** They have permissions to create users within the account, manage roles, and create groups with pre-attached permissions.
3. **Environment-Specific Users:** Work agents who can have read and/or write permissions only on the necessary services, such as Amazon RDS, Amazon ECS, or Amazon OpenSearch.



GoPanza Control Tower and Organizations Architecture



AWS Control Tower Features

- **Landing Zone:** Multi-account environment designed with security and compliance best practices.
- **Bead Factory:** Enables self-service to set up and provision new accounts.
- **Preventive and Detective Guardrails:** Pre-packaged governance rules for security, operations, and compliance, applicable to specific accounts or the entire enterprise
- **Mandatory and Optional Barriers:** They define whether to allow access, changes, and restrictions on AWS services.
- **Control Panel:** It provides real-time information about the AWS environment (number of OUs, number of accounts provisioned, guardrails enabled, and their status).

Results and Benefits

Deploying AWS Identity and Access Management (IAM), AWS Organizations, and AWS Control Tower in GoPanza's cloud environment has provided several significant benefits, improving both security and operational efficiency.

These advanced tools have enabled the company to not only strengthen its security infrastructure, but also streamline identity management and access control centrally. The specific benefits and tangible results obtained through this implementation are detailed below:

Benefits of AWS Identity and Access Management (IAM):

- **Granular Access Control:** Allows you to define detailed policies to control who can access which resources and under what conditions.
- **Multi-factor authentication (MFA):** Adds an extra layer of security through multi-factor authentication.
- **Role and Permissions Management:** Facilitates the creation of roles with specific permissions, optimizing security and administration.
- **Auditing and Monitoring:** Provides activity logging and access monitoring to detect and respond to suspicious activity.

Results:

- Significant improvement in security with a 50% reduction in unauthorized access.
- Increase operational efficiency with simplified permissions management.

Benefits of AWS Organizations:

- **Centralized Account Management:** Allows you to organize and manage multiple AWS accounts from a single location.
- **Service Control Policies (SCPs):** Implements policies at the organizational level to ensure compliance with best practices and security requirements.
- **Billing Consolidation:** Simplify financial management by consolidating billing from multiple accounts.
- **Resource Segmentation and Organization:** Facilitates the segmentation of resources into organizational units (OUs) for more effective management.

AWS IAM Features

- **Authentication:** Allows you to create and monitor users, groups, and roles, verifying assets, individuals, services, and applications within your AWS account.
- **Authorization:** Access is managed by policies and permissions.
- **Granular Permissions:** Set up specific permissions for different groups based on their needs.
- **Cross-Account Shared Access:** Allows you to designate access between multiple AWS accounts without sharing credentials.
- **AWS Organizations:** Facilitates fine-grained control of multiple accounts by grouping them and assigning permissions.
- **Identity Federation:** Integrates access with other identity providers.

Results and Benefits

Results:

- Increased administrative efficiency with a 30% reduction in account management time.
- Improved organizational security, with a lower likelihood of human error and improper access.

Benefits of AWS Control Tower:

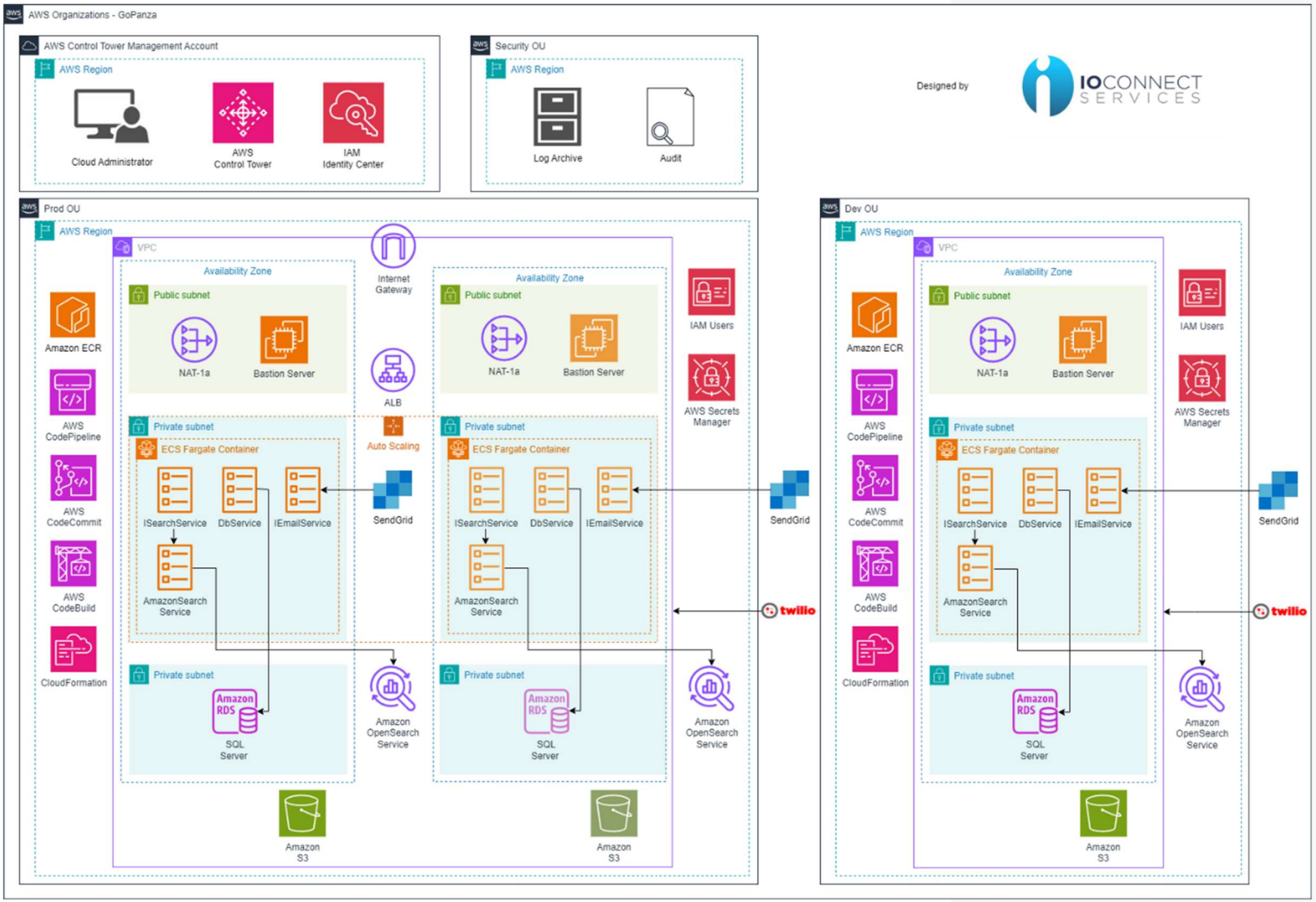
1. **Initial Setup Automation:** Simplifies the creation and configuration of a multi-account environment following best practices.
2. **Automatic Compliance:** Ensures that all accounts automatically follow predefined policies and controls.
3. **Monitoring and Alerting:** Provides tools to monitor compliance and receive alerts on potential issues.
4. **Security Guardrails:** Implements security and governance controls that protect the integrity of cloud infrastructure.

Results:

- 40% reduction in initial setup and start-up time for new accounts.
- 70% improvement in adherence to security and compliance policies, with fewer incidences of non-compliance.
- Increased visibility and control of the infrastructure with proactive alerts, improving incident response.

Implementing these services together has ensured a secure, well-managed, and efficient cloud environment, making it easier to manage identities and access resources in a centralized and consistent manner.

GoPanza High Level Solution Diagram



Next Steps

GoPanza now has a robust infrastructure with high availability and auto-scaling, as well as centralized and secure identity and access management. However, to fully consolidate your business in the AWS cloud and take full advantage of the platform's capabilities, you need to consider implementing new advanced capabilities and services.

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 specialized in Information Technology Consulting Services. All our team members have one thing in common: our enthusiasm for technology and our passion for excellence in customer service. We provide services throughout North America, LATAM, and Europe. We are headquartered in the New York metropolitan area, and we also have offices in Guadalajara, Mexico and Madrid, Spain.

IOCONNECT SERVICES