TRILIO

Trilio

Customer Case Study

A Major Bank

Executive Summary

This case study is about a large Latin American Financial Services organization. For the last four decades this organization has been actively involved in the construction of Colombia and has become an important benchmark in the country's financial sector.

They have a comprehensive portfolio of products and services that meets the needs of individuals, companies, and various sectors such as mining and energy, with constant innovation and exclusive offers for each segment.

They are a team of more than 17,300 people, with over 19.3 million clients in Latin America, nearly 500 branches and approximately 2,700 ATMs.

In addition to Colombia, they have operations in Panama, Costa Rica, Honduras, El Salvador, and Miami, in the United States.

Customer Challenges

Like all other organizations in the Financial Services Industry, they must adhere to strict regulatory compliance requirements.

Like many of their peers leveraging the scale and flexibility of Kubernetes-based applications, the customer (via several Red Hat ARO and Google GKE clusters) deployed their cloud-native applications in a hybrid and multi-cloud environment providing them with significant agility.

All of the aforementioned presented a unique set of challenges for data protection and recovery. The organization required a solution with comprehensive backup and recovery attributes:

- Flexible and Agnostic - The ability to support diverse private, public and hybrid cloud platforms and infrastructure such as multiple cloud storage environments; without having to make any changes to their applications.
- Cloud Native – Designed for Kubernetes, to provide support for the customer's dynamic, ever-evolving microservice-based applications and infrastructure.
- Control – Ability to select 'what to backup', or 'what to restore' at an application-level.
- Mobility and Agility - Migrating applications and data to secondary clusters in case of a disaster; Capable of seamless application movement to different clusters for organizational or performance purposes.
- SLA / Compliance - Ensured that their data is always secure and easily recoverable in the event of any disruption. Aiding in the ability to meet required regulatory compliance standards.

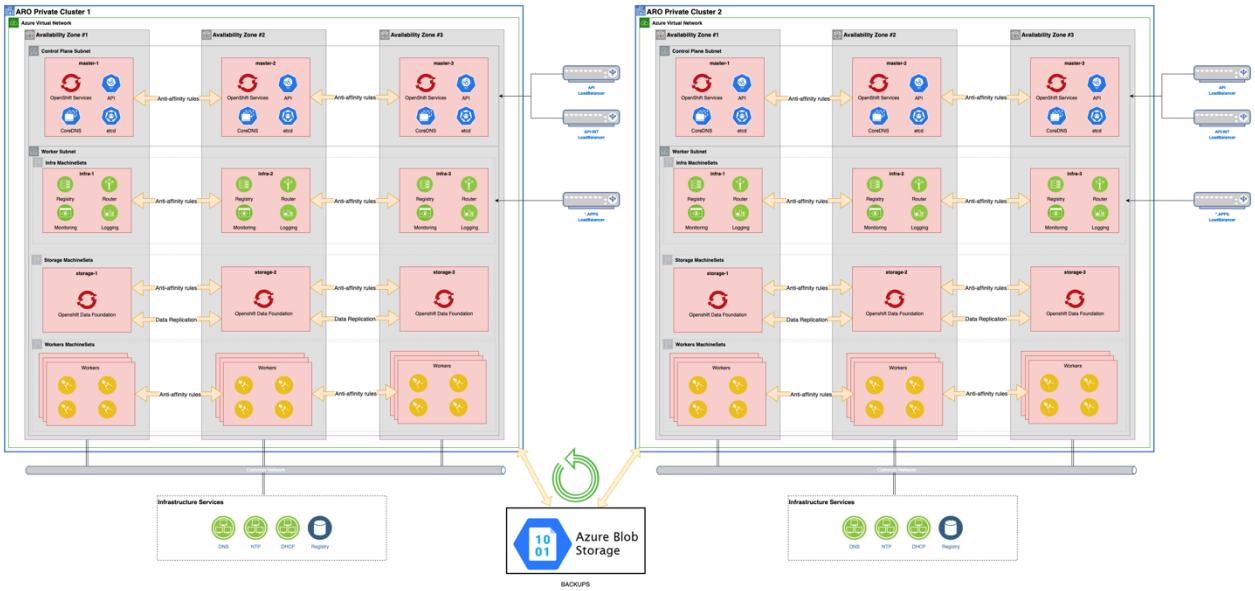
Customer's Implementation Journey

Prior to our engagement, the customer was using a legacy-based solution which prohibited operational scale and created multiple inefficiencies through:

- The combination of scripts and manual work.
- Processes that were highly prone to human error.
- Lack of skill set. A select few employees had the skills to only do lengthy recovery tasks, impacting the business negatively and creating a pessimistic view of the IT organization.

The organization realized they needed to find an easier way to protect their applications and remove these operational inefficiencies and complexity from the architecture in a non-disruptive manner.

Customer's ARO Architecture Diagram



The Selection Process

The customer evaluated multiple options in the market and down-selected two vendors, then continued with a deeper evaluation and decided on performing an extensive PoC with Trilio. This successful exercise resulted in the selection of Trilio as the ideal solution and partner of choice.

Below are key capabilities that resulted in this selection:

- **Multi-cloud Management** - Our hybrid multi-cluster cloud-native solution helped them overcome their previous limitations. From a single pane of glass, the organization can now monitor, observe and manage the data protection of all of their cloud-native applications.
- **Cloud Agnostic** - The public cloud is very resilient but at times, not enough. Trilio provided the customer with improved disaster recovery capabilities that help ensure the continuity of applications running in an OpenShift cluster, reducing the risk of downtime in the event of a disaster, and providing optimal RTOs.
- **Automated** - Trilio provided them with an automated disaster recovery test solution, making it easier to assess their disaster recovery plan and ensure that it was effective. Additional automation and operating efficiencies can be achieved in the future by integrating Trilio with other solutions such as Ansible or Red Hat Advanced Cluster Management (RHACM).
- **DevOps and GitOps Friendly** - Trilio and its APIs integrate with existing tools and workflows, making it easier to combine with their existing infrastructure and manage applications and namespaces by teams and tenants.
- **Time & Resource Savings through Native Control** - Our "Inclusions" feature allowed the customer to cherry-pick only what they needed to protect and protect only that application's data and metadata to an external remote backup target, saving network bandwidth and storage at the same time. The "Exclusions" feature allowed them to exclude some PVs used for logs and did not need safekeeping, as they were moved somewhere else by a different tool.
- **Ease of Use** - The intuitive nature of the Trilio solution allowed for many in the organization to quickly adopt data protection when and where needed. All tests in this case study were successfully performed in the Trilio User Interface. Furthermore, the customers expressed their appreciation that all could have been completed in the CLI if required.
- **Meta Data Support** - The ability to capture and recover metadata is a crucial step in the ability to recover an application. Our state-of-the-art "Transformations" feature allowed the customer to modify any metadata object when executing a recovery procedure (configmaps for example). This aids in the ability to re-orchestrate a point-in-time into other clouds, clusters, etc.
- **Ransomware Protection** - Leveraging the National Institute of Security and Technology's (NIST) Cybersecurity Framework, Trilio will help to prevent future ransomware attacks through application-level encryption and immutability; Trilio integrates with the S3 object locking mechanism, so no modification of the backups are allowed for a determined period of time.

Deployment and Next Steps

- The solution was deployed in a test environment in 5 minutes. Full configuration in the customer's environment took less than 3 hours.
- The customer ran numerous tests, including local backup and recovery, migration and disaster recovery to other ARO clusters, Metadata only backup/recoveries, and verified that Trilio for OpenShift met their expectations and use cases.
- At the time Azure Disk storage for OpenShift was in "tech preview" therefore the customer was reluctant to deploy in a production. Since Trilio supports any CSI storage environment with snapshot capabilities we suggested the customer use Red Hat OpenShift Data Foundation (ODF) for the Persistent Volumes' storage, while Red Hat finalized their support for Azure Disk. This temporary use of ODF accelerated adoption and deployment into production much sooner.
- The customer is now automatically protecting applications and data, of both Red Hat OpenShift and GKE in ARO without the need of specialists.
- The resource savings are significant as the organization has gone from days and hours to minutes for recovery.

About Trilio

Trilio is a leader in Cloud-Native Data Protection for OpenStack and Kubernetes environments. Since 2013, Trilio has been on a mission to give tenants more control over their ever-changing, growing, complex, and scalable cloud-based architectures. Today, Trilio is trusted by businesses all around the world to protect their cloud-based Applications in a way that's easily recoverable and requires little-to-no central IT administration.

TRILIO

TRILIO.IO