Managing Multi-Cloud Deployments on Kubernetes with Istio, Prometheus and Grafana

Vivek Sharma
Assistant Professor,
GLA University, Mathura (UP), India
viveksharma.cea@gla.ac.in

2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS) | 978-1-6654-0816-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICACCS54159.2022.9785124

Abstract— **Today, Cloud-native is changing the way applications are constructed and being deployed. Traditionally, application development followed a waterfall and monolithic approach. Whereas cloud-native follows a microservices and agile approach. This cloud-native approach has many advantages over traditional approaches. However, relying on a single cloud vendor will create a number of issues like single-vendor dependency, the problem of reliability and availability, as no single cloud service provider has the best tools for everything. To remove this single-vendor dependency, Cloud-Architects use a multi-cloud environment. Multi-cloud refers to the use of many cloud providers and services in a single cloud network infrastructure. Multi-cloud environments are used to gain all benefits from different vendors like distribute computing resources, minimum downtime and high data availability. Organizations are using multi-cloud to increase their computing power and services availability for a business. In recent years, cloud service advances have led to a shift from private clouds to multi-tenant clouds and hybrid clouds. This multi-cloud will be a mixed environment that will take advantage of many infrastructure environments, such as private and public clouds.**

Keywords— Multi- Cloud; Grafana; Prometheus; Istio; Anthos; Kubernetes.

I. Introduction

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." - NIST (National Institute of Standards and Technology) [1].

This NIST cloud model promotes essentially five characteristics. On-demand availability, dynamic resource pooling, extensive network access, rapid elasticity, and measurable service are among these characteristics. Based on the need of services by end users. These services are classified into three service models like IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). There is also a deployment model, which classifies cloud architecture into four major clouds.

These are Private cloud, public cloud, Community cloud, Hybrid cloud or multi-cloud [2].

As the focus of organizations shifts from their On-Premise servers to subscription based-services and cloud-based technologies, they get into a situation where they have many decisions to take. As there are many problems with implementing their networking infrastructure on the cloud. Out of all the problems, their major concern will be whether they have to use a single cloud vendor service or they should go for a solution having multiple services offered by different cloud vendors. Fortunately, these options available to them are growing every day. As organizations try to decide what solution will work best for them, they will first need to understand the differences between single vendors cloud and multi cloud [4].

Single Vendor Cloud (Public or Private Cloud)

A single vendor cloud, which is owned or governed by a single entity (Organization). These clouds have benefits of secure networks for the integration of services and data security. The key characteristics of single vendor cloud is one-size-fits-all solution, which allows companies to use network services to integrate or working across multiple platforms. By having a single vendor cloud, entity can log into one single and unified system. Which allows them to move freely between applications that are designed to work concurrently. In this, they do not need to worry about transferring data or assets from one system to another. This transfer of data and assets from one system to another will allow cloud providers to troubleshoot any problems that emerge in the application, more effectively because they support the entire architecture.

Single-vendor cloud solutions are ideal for small business or startups, as they don't need to have any highly specific requirements for their business logic. Since they don't need any specific requirement for their application, they can get everything they may need from a single cloud vendor and can save significantly on implementation costs phase. For the large businesses, who have very specific requirements for their business need, can pay enough to convince the provider to design a customized solution for them. This approach will be expensive for a short term, but convenience of keeping everything (services and applications) within the same infrastructure can sometimes be worth the price and can be beneficial for the organizations. There are some pros and cons of a single cloud, defined as follows [2]:

978-1-6654-0816-5/22/$31.00 ©2022 IEEE

Table 1: Pros and Cons of Single- Vendor Cloud

Pros	Cons
Easy negotiation by having only a single entity to negotiate with.	Less power in price negotiations.
No finger-pointing between several vendors, as single vendor is solely responsible for any issue.	Dependence on the single vendor procedure in every case.
Easy procedure for support and services	Less freedom of choice for services.
Easy integration of services.	Vendor lock-in problem.
Less training is required for your own staff.	Training is required for every new service, which is also sometimes paid.
chances of compatibility issues will be less.	Not supportive for the technologies like operating systems, switches or protocols.
	Might be the issue of vendor lock- in like backup, disaster and recovery.

Multi Vendors Cloud (Multi or Hybrid Cloud)

Multi-vendor cloud, the solution having multiple services offered by different cloud vendors [4]. This kind of solution is required, whenever the large businesses have highly specific requirements or their benefit from solution is far more than their expense on implementation. There is also a situation when a company has specific workload needs that only a certain vendor can provide. In these circumstances, either they go with predefined solutions provided by the current cloud vendor. This will lack that functionality which their industry demands. This situation becomes even more complicated when different departments of a company have their different IT needs.

For example, Software developers may need an application building environment while accounting needs a separate platform for doing their job effectively. To meet all these needs, companies must identify the best and economically suitable providers for each solution.

Solutions for these specific needs usually offer far more features and functionality compared to the single vendor predefined solution. This may be quite expensive and hard to integrate into a network, but the difference between the ideal solution and a compromised solution can often carry more significant changes in terms of revenue, missed opportunities and liability of compliance. Today’s multi cloud vendors solutions are generally easier to integrate and supportive than compared to those that were in the years past. This makes it a more viable option for any company that needs the improved performance. Even so, smaller companies with low and limited budgets may or may not be able to afford the implementation expenses.

Advantages of multi cloud vendors

1. **Innovation- The** multi-cloud environment enables you to innovate swiftly while taking use of each provider's finest offerings. This enables developers and architects to focus on innovation without worrying about the limitations of one vendor cloud over other vendor clouds. This way, developers get a legacy enterprise approach. Where vendors provide an opportunity to innovate through the features.

2. **Risk Mitigation -** The problem of outages doesn't occur often, but when this occurs this can cause major disruptions in service availability and reliability. A cloud solution tries to omit this problem, by having multiple geographic regions and more than one data centres in each region to increase availability and reliability of services. For small businesses having less hour’s uptime, this risk mitigation technique might work and cause less losses. But for a large organization having requirement of minimum downtime and high availability, a multi cloud approach will help. Multi cloud architecture reduces the risk of significant IT disasters by storing all of your assets in several cloud storages, allowing you to have a separate and totally independent clone of each application on some other vendor's cloud. This separate replica can be used in case the primary storage vendor cloud goes down.

3. **Minimum Vendor Lock-in -** In today’s world, dependency on a single vendor will be too risky for business. Because one vendor may not be able to provide all of your needed service levels for a certain service, you should shop around. In the worst case, the one who is responsible for service providing can go out of business or become your business competitor. Thus, by using multiple cloud vendors, organizations can minimize the problem of single vendor lock-in.

4. **Lower Latency -** To improve user experience and reduce service access latency. With a multi-cloud architecture, you may choose the regions and zones that are closer to your organisation and clients. The shorter the distance over which data must be transferred, the faster your application will reply. Every cloud provider has numerous areas throughout the world, and there is always a data centre that is closer to your consumers among them. By using a combination of these multiple cloud vendors, your application will get faster user experience with minimum latency.

5. **Negotiating Power -** A large firm with significant spending and consumption might take advantage of the various price choices available from several cloud vendors. This power of competition between multiple vendors allows organizations to increase their negotiating power. The various vendor options to pick the proper service that provides the most value and functionality.

Disadvantages of multi cloud vendors

There are a set challenges which concern the designing and managing a multi cloud architecture. Some of the major concerns or disadvantages of multi cloud architecture are:

1. **Talent Recruitment and Management -** Finding the right individuals (such as developers, solution architects, and security experts) who are familiar with numerous cloud services, always willing to shift with the trend, and have experience managing and operating across multiple clouds is practically impossible as an organisation.
2. **Optimisation, Reporting and Cost Estimation- These** three tasks are highly valuable and integrated with each other. Although one can save costs and optimize the services by using multiple cloud vendors and consolidating them. However, each provider has their own set of fees for each service, making it difficult to correctly predict costs. Every time you encounter a cloud, you will need to create an estimate. You'll need a cross-account cost reporting solution to provide reports to properly manage the financial aspects of services across all clouds.
3. **Security Risks-** Security is also a major concern in multi cloud architecture, as there are always some loophole and incompatibility between two vendors. These problems can be minimized by using third party tools. Protecting a multi-cloud architecture, on the other hand, will always be more challenging than securing a solitary cloud.
4. **Operational Overhead/ Management -** In a single vendor cloud operational management is quite simple compared to the multi cloud. As a result of the multi-cloud infrastructure's dispersion across numerous clouds. The administrative responsibilities are patch management for operating systems, alert and respond to events, backup management and consolidation of logs. These tasks add additional layers of complexity to the architecture.

Whether it is latency or security of a multi cloud, there are always trade-offs between the convenience, value and timeline of cloud services.

II. Related Work

Anthos [3] is a product designed for multi cloud infrastructure management and application deployment. It offers the same basic features that Istio gives when it comes to visibility and multi-cloud service mesh and application service management. It is based on open-source technologies. That is pioneered by Google - including Kubernetes, Istio, and Knative. It ensures that on-premises and cloud environments are consistent. It aids in the rapid creation of applications.

Anthos on GKE, part of Anthos lets users take advantage of Google Kubernetes Engine [6] and cloud technology in their on-premises data centers and in the cloud [7]. Users get the same Google Kubernetes Engine experience with quick, simple and managed installation as well as upgrade validated by Google. GCP Console gives users a single pane of view for managing clusters across cloud environments and on-premises [8].

The three main features that Anthos offers that make it a competitive choice for businesses are:

- Consistent Kubernetes Experience: The ability to monitor the on-premises or a third party managed Kubernetes service and the Kubernetes cluster running on Google Cloud with the same single pane of glass with the cloud console. The OS, Kubernetes version, runtime and add-ons between Anthos GKE deployed in the different environments stay in sync with each other

- Secured Kubernetes Cluster: The Kubernetes version, OS and runtime are all kept up-to date with security patches and latest releases to mitigate security vulnerabilities, whether it’s the cluster running on user’s infrastructure or running in the cloud in Google’s data center are all managed by Google.

- Centralized multi-cluster management: It gives users the privilege to manage, monitor and enforce policies across all of GKE (Google Kubernetes Engine) clusters, whether in the on-premises or on the cloud, from Google Cloud Console.

Anthos early customer case studies:

Global enterprise customers are already using Anthos in a number of industries. As a software-based solution which is flexible and portable to build multi-cloud and hybrid environments.

For HSBC which is one of the largest financial and banking services organization in the world. A cloud managing solution will reduce the cost and complexity of big-data analytics is essential for its multi cloud strategy.

Darryl west, Group CIO in HSBC said these, “At HSBC, we needed a consistent platform to deploy both on-premises and in the cloud and Google Cloud’s software-based approach for managing hybrid environments provided us an innovative, differentiated solution that was able to be deployed quickly for our customers.”

Many businesses already have infrastructure and software in place, but they want the flexibility to expand in the cloud in the long term. Google is collaborating actively with its partners to support these customers, introducing over 30 software, hardware, and system integration partners who are ready to assist customers get started with Anthos right away.

Kip Compton, Senior Vice President of Cloud Platforms and Solutions at Cisco said that, “We know that hybrid and multi-cloud approaches represent the future for many of our customers”. “Our customers want to develop and deploy their applications anywhere - on-prem, in the public cloud, or in multiple public clouds - seamlessly and securely [15]. We’re excited to make that possible by integrating Cisco’s industry-leading data center, networking, and security technologies with Anthos and growing our partnership with Google Cloud.”

Siemens, Europe's largest industrial manufacturer, is looking forward to the insights Google Kubernetes Engine On-Prem will provide in their complicated, hybrid environment. Martin Lehofer, Head of Research, Siemens said this, “Anthos is a great gift for us. It gives us a unified management view of our hybrid deployment and a consistent platform to run our workloads across environments” [16].

III. Proposed Work

To take the advantages of multi-cloud, like negotiation, risk mitigation and lower latency in the cloud. We use the multi-cloud architecture design using Kubernetes, Istio, Grafana and Prometheus. Each component provides compatibility and transparency between different cloud vendors [14]. VPN connection is used to connect two clusters running on Cloud vendors infrastructure.

Multi-cloud architecture using kubernetes provides ability to transfer or recreate workloads across different clouds [9]. This ability allows application to sustain in the condition of infrastructure failure and disaster recovery. It also automates various manual processes, enables Horizontal scaling, Automates rollouts and rollbacks.

In this architecture, Istio will provide a number of key capabilities across a network of services. It provides traffic management, observability and security to the services mesh. In this architecture, two or more kubernetes clusters running a remote configuration are connected to the Istio control plane, later in which Envoy can then form a mesh network across multiple clusters[11].

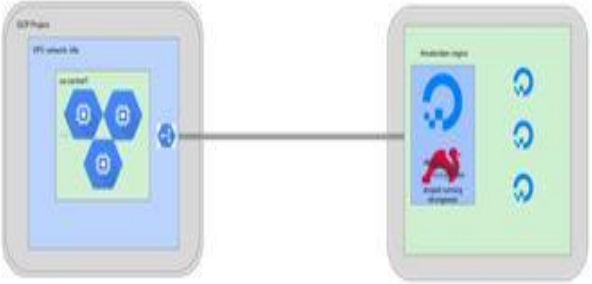

Figure 1: Architecture Overview

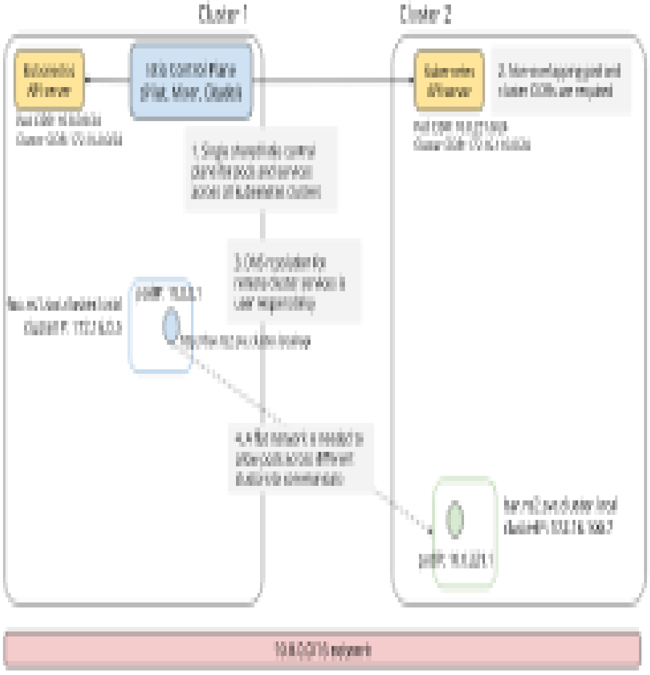
Cluster 1
Cluster 2
Kubernetes API server
Istio Control Plane (Pilot, Mixer, Citadel)
Kubernetes API server
2. Non-overlapping pod and cluster CIDRs are required
1. Single shared Istio control plane for pods and services across all kubernetes clusters
3. DNS resolution for remote cluster services is user responsibility
4. A flat network is needed to allow pods across different clusters to communicate
10.0.0.0/16 network

Figure 2: Istio mesh spanning across multiple Kubernetes clusters having direct network access to remote pods over VPN connection

In the proposed approach, two service foo and bar running on two different pods inside different kubernetes clusters, are connected through a secure VPN connection [10].

Prerequisites

1. Two or more running kubernetes clusters having version 1.13 or above.

2. Single shared istio control plane for pods and services across all kubernetes clusters.

3. Non-overlapping pods and cluster CIDRs are required.

4. DNS resolution for remote cluster services

5. VPN network to allow pods across different clusters to communicate.

Grafana, an open source metric analytics & visualization suite[12]. It allows you to visualize, query, alert-on metrics data. Also, create, share, and explore dashboards with your team. Prometheus, a system monitoring and alerting open source toolkit[13].

IV. Conclusion

This architecture will solve the problem of managing multi cloud deployments and distributed micro services with a single control plane and enables DevOps teams to provision, and secure their micro services without necessarily the knowledge of the underlying platform. With this architecture of micro services, DevOps teams get better traffic management, more secure communication channels, high availability, reliability and many more. There is also an enhanced risk management as, migrating the traffic to only a specific version of the backend based on custom headers.

There is also mutual TLS between two different micro services. We get a complete bird's eye view of the running micro services. We also get a more secure and easy working architecture with features like circuit breaking, to automatically switch to another version of the micro service, in case an existing version gets timed out. Custom plug-ins and custom CRDs lets operators integrate and monitor custom services with Grafana and custom metrics and instrumentation with Prometheus. All of these features extend to and are of extreme value to operators managing Multi-Cloud and Hybrid Cloud environments.

References

[1] NIST, NIST Cloud Computing Program - NCCP. https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp.

[2] Centric Consulting. Pros and Cons of a Multi-Cloud Strategy. https://centricconsulting.com/blog/pros-and-cons-of-a-multi-cloud-strategy/.

[3] Google Cloud, Anthos| Google Cloud. https://cloud.google.com/anthos.

[4] Stratoscale.com. https://www.stratoscale.com/blog/it-leadership/cloud-clouds-choose-single-multi-cloud-approach/.

[5] Istio, Shared control plane (single-network). https://istio.io/docs/setup/install/multicluster/shared-vpn/.

[6] D. Jaramillo, D. V. Nguyen, and R. Smart, "Leveraging microservices architecture by using Docker technology," in SoutheastCon 2016, 2016, pp. 1–5.

[7] "Microservices," martinfowler.com. [Online]. Available: https://martinfowler.com/articles/microservices.html. [Accessed: 01-Oct-2018].

[8] N. Dragoni et al., "Microservices: Yesterday, Today, and Tomorrow," in Present and Ulterior Software Engineering, M. Mazzara and B. Meyer, Eds. Cham: Springer International Publishing, 2017, pp. 195–216.

[9] "Docker - Build, Ship, and Run Any App, Anywhere." [Online]. Available: https://www.docker.com/. [Accessed: 01-Oct-2018].

[10] "Kubernetes," Kubernetes. [Online]. Available: https://kubernetes.io/. [Accessed: 24-Jan-2018].

[11] L. A. Vayghan, M. A. Saied, M. Toeroe, and F. Khendek, "Deploying Microservice Based Applications with Kubernetes: Experiments and Lessons Learned," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 970–973.

[12] A. Balalaie, A. Heydarnoori, P. Jamshidi, "Microservices Architecture Enables DevOps: Migration to a Cloud-native Architecture", IEEE Software, vol. 33, no. 3, pp. 42-52, 2016.

[13] Jenkins, [online] Available: https://jenkins-ci.org/

[14] G. Caire, F. Leal, P. Chainho, R. Evans, F. Garijo, J. Gomez, J. Pavon, P. Kearney, J. Stark, and P. Massonet. Agent oriented analysis using MESSAGE/UML. In M. Wooldridge, P. Ciancarini, and G. Weiss, editors, Second International Workshop on Agent-Oriented Software Engineering (AOSE-2001), pages 101–108, 2001.

[15] Turnbull, J.: The Docker Book: Containerization is the new virtualization James Turnbull (2014).

[16] Binz, T., Breitenbücher, U., Kopp, O., Leymann, F.: TOSCA: Portable Automated Deployment and Management of Cloud Applications. In: Advanced Web Services. Pp. 527–549. Springer (2014).