Impact of Multi-Cloud Infrastructure on Business Organizations to Use Cloud Platforms to Fulfill Their Cloud Needs

Karu Lal

Integration Engineer, Ohio National Financial Services, USA

E-mail for correspondence: karu021984@gmail.com

Received: Oct 04, 2016 **Accepted:** Nov 30, 2016 **Published:** Dec 31, 2016

Source of Support: Nil **No Conflict of Interest:** Declared

ABSTRACT

"Infrastructure as a Service" (IaaS) refers to utilizing various public cloud platforms by Multi-Cloud Infrastructure. This multi-cloud paradigm abstracts the differences between cloud providers so that applications and operational procedures can function in a manner that is uniform across all environments. This makes it possible for businesses to reap the benefits of the many capabilities cloud service providers offer while also avoiding the risks typically associated with depending on a single cloud service. It is becoming increasingly vital for enterprises to modernize their applications and seamlessly manage and control deployment and scale across environments. As a result, multi-cloud management of the underlying infrastructure is becoming increasingly important. Within the confines of this investigation, we have covered topics such as the relevance of the Multi-Cloud Infrastructure, its many benefits, drawbacks, and other issues. In addition, we have investigated the functions involved in the operation of multi-cloud infrastructure. This piece presents an overview of the multi-cloud infrastructure idea and discusses some recommended procedures.

Keywords: Multi-Cloud, Infrastructure as a Service (IaaS), Cloud Computing, Multi-Cloud Infrastructure

INTRODUCTION

When an enterprise runs its applications using cloud computing services from at least two different cloud providers, they are said to be using multi-cloud. Multi-cloud environments are an alternative to employing a single-cloud stack. These environments often consist of a combination of two or more public clouds, two or more private clouds, or some variety of both types. Because you can build a plan that leverages more than one vendor, you can select and choose the capabilities that are the most suitable for your business needs, which helps reduce the risk of being locked in by a single vendor. "Multi-cloud infrastructure" refers to a cloud environment enabling businesses to utilize two or more cloud platforms simultaneously. The public cloud is used frequently by multi-cloud infrastructure. To earn the ' Multi-cloud' label, an organization's cloud environment typically needs to use at least two different public cloud services. Every cloud in a multi-cloud architecture has the potential to fulfill the requirements of a specific service or application that an organization may require. Businesses can arrange their multi-cloud infrastructure in various ways, using a mix of private, public, and edge cloud services to satisfy specific business objectives. Multi-cloud strategies and multi-cloud solutions are becoming increasingly popular among businesses because they enable companies to operate apps exactly where they need them without introducing additional layers of complexity (Allison et al., 2015).

Multi-cloud solutions built on top of open-source technologies such as Kubernetes provide the flexibility and portability to migrate, construct, and optimize applications across different cloud computing environments. In addition, multi-cloud setups are compatible with DevOps development processes and other cloud-native application technologies that facilitate portability, such as containers and micro services architecture (Karthic et al., 2012). This makes them an attractive option for businesses. Anthos, the managed hybrid and multi-cloud platform offered by Google Cloud, is a great place to begin your multi-cloud adventure.

WHY IS MULTI-CLOUD INFRASTRUCTURE IMPORTANT?

Multi-cloud infrastructure lets companies employ many cloud platforms. The public cloud is used in multi-cloud infrastructure. A 'multi-cloud' cloud environment uses at least two public cloud services. Combining on premise

activities with apps and services on different public cloud platforms allows enterprises to maximize each vendor's benefits while minimizing their drawbacks (Desamsetti, 2016a). Companies use multi-cloud infrastructure to offload non-critical databases and information operations such as application stacks, message queues, load balancing, batch processing, and web traffic management. Different applications may be improved with cloud services unique to each provider when firms construct new software or modernize current ones (Artificial Intelligence best fits on Google Cloud). There may be Oracle Cloud-optimized enterprise apps.

Applications using a specific OS, like Microsoft Windows, may be best for a cloud like Microsoft Azure. Business factors like data gravity, restricted language management capabilities, or regional team preference may improve one cloud infrastructure platform. Each cloud provider has different services, benefits, and innovative capabilities. Indeed, public cloud providers differ in:

- Different kinds of cloud service portfolios
- A collection of tools that can assist with DevOps
- Various models of pricing
- Geographic locations and zoned areas of availability

It would help to have a consistent infrastructure and management stack for a Multi-Cloud Infrastructure. This stack must be able to be stacked on top of any physical infrastructure in any location from any cloud provider, and it must also be able to run all different types of applications, including both conventional and modern ones, in addition to a wide range of PaaS services (Desamsetti, 2016b). Put another way, multi-cloud infrastructure entails more than using several cloud providers. It is an operating paradigm that provides flexibility and consistency to any location, and it can run workloads on any cloud that a company needs. Infrastructure based on many clouds can assist in achieving greater operational efficiency in various settings. Having the freedom to do the following is part of this:

- Transfer apps between regions or nations beyond a single provider's capacity.
- Utilize diverse cloud services from many providers.
- Move workloads between providers if company strategy requires it.

What are the benefits of Multi-Cloud Infrastructure?

Multi-cloud infrastructure systems provide consistent operations across a multi-cloud environment, including public cloud-native designs and hybrid cloud architectures (Khattak et al., 2015). With the flexibility to design, deploy, and administer from the data center out to the edge, organizations can architect the multi-cloud architecture that best matches their applications. This allows for the following benefits to be realized:

- Enables building, running, and managing contemporary apps on any cloud using a PaaS layer, Kubernetes runtime, and multi-cloud control plane.
- Enables building, running, and managing contemporary apps on any cloud using a PaaS layer, Kubernetes runtime, and multi-cloud control plane.
- Continuous monitoring of cloud resource configuration and benchmarks ensures real-time security and compliance posture visibility, aligning with industry standards and bespoke requirements.
- Optimized multi-cloud costs by allocating chargeback fees, tracking spending increases, and facilitating reservation and savings plan decision-making.
- Streamlined multi-cloud operations and automated governance policies without affecting DevOps teams.
- Enhanced Choice and Flexibility: Organizations can deploy cloud apps that best suit their needs and migrate them as needed while maintaining security and compliance.

Critical Components of Multi-Cloud Infrastructure

Now that we are familiar with the fundamentals of multi-cloud infrastructure, let's look at the essential parts of multi-cloud architecture.

Server load balancer

Server load balancing (SLB) is crucial to multi-cloud infrastructure. It redirects web traffic to various servers to balance loads. Using network-based, software-defined cloud systems, SLB may disperse increased web traffic over multiple servers. Larger companies must load balance across different regions. This is done with clever traffic distribution using global server load balancing (Lal, 2015). Hosted SLB solutions in private, public, or multi-cloud environments are preferred by most corporations.

An application server

For running apps, application servers are dedicated. Multicloud application servers let enterprises test, run, and host apps efficiently. Cloud servers meant for web pages may not be appropriate for demanding web apps. However, a multi-cloud architecture configured as an application server gives client organizations the processing power and memory to execute real-time applications. Multicloud application infrastructure can be customized to host certain apps or components.

Database server

Database management software runs on specialized database servers. Companies employ database servers to run necessary databases. Backend database applications commonly use multi-cloud-based database servers. Using the client-server network model, multi-cloud-augmented

database servers can meet client system data delivery needs. Database servers process massive amounts of data for large companies. Client-server architecture lets organizations process data in real time and better serve customers. File storage, processing, and retrieval can be done with multi-cloud database servers.

Server redundancy and backup

The most significant benefit of multi-cloud infrastructure is redundancy. Companies use multi-cloud for failover and recovery. SLB, database, and application tiers typically commission redundancy servers. Manufacturing environments are often secured with this 'redundant 3-tier architecture'.

Auto-scaling horizontally

Multicloud infrastructure has horizontal auto-scaling, allowing enterprises to scale their cloud resources. SLB or a similar technique assigns cloud resources to one or more cloud servers as the client needs. With horizontal auto-scaling, enterprises don't have to worry about cloud processing power or storage space running out, regardless of when a provider can complete their request.

How does Multi-Cloud Infrastructure Work?

Because leveraging numerous hyper-scale cloud providers in addition to on-premises infrastructure is becoming increasingly common, businesses need to find ways to simplify the complications brought about by this combination of resources. Every cloud service provider has its architecture, ground rules, and minimum system specifications. The following are the requirements for multi-cloud infrastructure solutions:

- Consistently manage apps irrespective of the location in which they are deployed.
- Enable the construction, movement, and execution of applications everywhere, including moving apps between public clouds without reworking the code.
- Maintain the safety of apps no matter where they are deployed.
- Enable the developer, and IT support to facilitate easy team collaboration.
- Create a pathway for migration to new cloud environments that is completely seamless so that adapting does not require refactoring.

To assist in increasing agility while limiting costs and risk, VMware has identified these five guiding principles for creating multi-cloud architecture. The following is an explanation of each of these best practices in multi-site cloud infrastructure:

- Ensure adaptability. Enable each application to be deployed to the cloud that best fits its needs to boost firm agility.
- Evolve without cost. Build an environment that supports application migration without refactoring to reduce expenses.
- Optimize resources fully. Create an ecosystem that gives developers and IT operators' significant skill leverage to reduce learning curves.
- Maximize automation investments. Create an environment that facilitates automation scaling across operations.

Drawbacks of Multi-Cloud Infrastructure

A few disadvantages are associated with employing a multi-cloud strategy, which makes use of multi-cloud infrastructure supplied by various cloud service providers. However, a modern platform that supports many clouds can assist in finding solutions to these problems. A multi-cloud approach requires dependable connectivity to achieve high bandwidth low latency connectivity between on-premises workloads and users and cloud workloads and services. All major public cloud providers offer direct access for this high-quality connectivity need. Direct Connect for AWS, Cloud Interconnect for Google, and ExpressRoute for Azure. There are several connectivity chores to fulfill before operation or migrations can begin:

- Develop a multi-cloud connection with your chosen networking partner(s), starting with your on-premises data center.
- Set up a dedicated connection between the partner multi-cloud provider and the targeted cloud environments. Consult partner and cloud provider documentation for requirements and procedures.
- Install VMware SDDCs in cloud providers, ensuring non-overlapping IP address space for SDDC Management and application workload networks.
- Open proper HCX firewall ports on both on-premises and cloud firewalls.
- Install HCX Connector Appliance on-premises, activate, and couple with vCenter.
- On-premises vCenter login, HCX plugin configuration, site pairings to cloud HCX Managers, and on-premises resource Compute and Network Profiles.
- Connect the necessary HCX Service Mesh(s) to the VMware SDDCs in each cloud provider. Service mesh equipment will be deployed on cloud SDDCs.

Developer and operator skills are a significant barrier to multi-cloud architecture. Multiple clouds complicate operations. To use each cloud's innovation capabilities, new skills must be learned if it is run as a silo with its own development and operational model, taxonomy, and APIs. As firms go multi-cloud, many see higher labor expenses and lower efficiency (Thandeeswaran et al., 2012).

Meanwhile, operational risk rises. Different cloud settings make swiftly fixing performance concerns tougher for

app dev teams. Differences make it challenging to apply policies designed to ensure apps are always secure and compliant wherever they are deployed.

Best Practices for Multi-Cloud Infrastructure Management

Businesses may ensure the successful execution of their multi-cloud strategy over the long term by adhering to the best practices outlined in the following paragraphs. These five best practices must be followed when developing, implementing, and managing a multi-cloud environment for a company. Recommended Practices for the Management of Enterprise Multicloud Infrastructure:

Workload mapping

Correct workload mapping is essential for a successful multi-cloud strategy. Companies may easily map workloads to provide cloud services and infrastructure to the business teams and processes that need them (Gunasekhar et al., 2015). Correct mapping also helps the IT department design SLAs based on data protection, availability, uptime, latency, rapid scalability, batch processing, real-time streaming, and heavy-duty computing. Despite some overlap, multi-cloud and hybrid cloud are distinct concepts. Companies must evaluate public cloud, private cloud, hosting services, and hyper-converged infrastructure to create a long-term multi-cloud strategy.

Security centralization

Suppose a corporation establishes a multi-vendor, multi-geography IT infrastructure, and service level relationship without planning. If non-standard SLAs become the norm, supplying stakeholders with predictable, consistent, and agreeable business services becomes more accessible. A good multi-cloud roadmap should adopt a single, benchmarked, consistent set of SLAs for all resources, on-premise or in the cloud. Vendor consolidation aids enterprise-wide SLA implementation. The large number of heterogeneous IT resources in a multi-cloud context makes data security and privacy a priority. Thus, enterprise perimeter security—including apps, users, data sources, and endpoints—is complex. IT decision-makers must standardize and centralize security policies and consider partnering with a managed security service provider (MSSP) to integrate the business's security environment to reduce risks and improve cybersecurity.

Simplifying vendor management

Multicloud requires managing many technology vendors. Co-location, SaaS, cloud infrastructure, mobile apps, QA/testing teams, application development businesses, NOCs, SOCs, and managed service providers are all issues for the client. With effective vendor management, the company's multi-cloud infrastructure may become connected and segmented, increasing business risks and decreasing control (Jofre et al., 2014). Streamlining multi-cloud operations requires IT governance centralization. Enterprises need a multi-cloud management platform to deploy and de-provision cloud services, orchestrate them, monitor traffic, auto scale, and check availability and latency.

Rugged integration framework creation

Traditional IT ecosystems are adopting dynamic multi-cloud setups as remote work grows across businesses. Companies are implementing robust change management activities in 2021 to increase acceptance and usability. Organizations' IT departments prioritize customer satisfaction through fast-changing multi-cloud adoption. Multi-cloud integration is challenging due to the number of integration points between on-premise infrastructure, information storage, and third-party cloud-powered services and apps. Integration across many clouds takes a lot of work. However, several bespoke integration tools and APIs simplify the job.

Restoring from disaster

A company must overcome three challenges when implementing a multi-cloud disaster recovery strategy.

Migration: Migrating data from on-premise workloads and systems to a multi-cloud ecosystem makes disaster recovery difficult. To avoid data loss during this uncertain period, all levels must plan carefully for business continuity and network availability.

Multicloud: Even in 2021, when multicloud is gaining popularity, on-premise or single-cloud systems have disaster recovery plans. Multiple dynamic characteristics make expanding disaster recovery measures for multi-cloud setups difficult. These include workload, scalability, geographical coverage, data type, deployment types like IaaS and SaaS, infrastructure services like private cloud, public cloud, and hosting, and cloud service suppliers like AWS and Azure.

Evolving environments: Multicloud environments are adaptable and scalable. Thus, the company's infrastructure must, too. Continuous delivery and integration help streamline fast-changing IT needs.

Conclusion

The primary reason why businesses utilize multi-cloud architecture is to mitigate the risk of experiencing data loss or downtime due to the failure of a localized or single-vendor component. A multi-cloud infrastructure not only helps eliminate the risk of being locked in by a single vendor but also delivers far-reaching commercial and technological goals, such as better pricing competitiveness, faster speed, larger capacity, and additional features.

Because of its increased data sovereignty, it makes it possible for businesses to achieve ideal performance levels and reduce latency. By utilizing a multi-cloud infrastructure, companies can position their servers and other associated resources in the geographic region that is most convenient for their end customers. The security ecosystems of today's leading cloud infrastructure providers offer cutting-edge levels of protection. Cloud companies implement security solutions and best practices that are on par with, and sometimes even superior to, those utilized by the industry's most prestigious enterprise data centers. As a result, most customers no longer view worries about data security as a valid reason to avoid adopting multi-cloud architecture.

A multi-cloud infrastructure can generate large volumes of data regarding its availability, performance, resource utilization, downtime, traffic patterns, usage correlations, and other trends when robust process automation and integration measures are implemented, in addition to the appropriate use of cloud management solutions. Because of the rapid and high-volume information collection, management teams can go beyond routine network monitoring and instead collect in-depth insights to improve the performance of their organizations, departments, and groups.

REFERENCES

Allison, M., Turner, S., & Allen, A. A. (2015). Towards interpreting models to orchestrate IaaS multi-cloud infrastructures. *The Institute of Electrical and Electronics Engineers, Inc.(IEEE) Conference Proceedings.*, 80-85. https://doi.org/10.1109/ICCSE.2015.7250222

Desamsetti, H. (2016a). A Fused Homomorphic Encryption Technique to Increase Secure Data Storage in Cloud Based Systems. *The International Journal of Science & Technoledge*, *4*(10), 151-155.

Desamsetti, H. (2016b). Issues with the Cloud Computing Technology. *International Research Journal of Engineering and Technology (IRJET), 3*(5), 321-323.

Gunasekhar, T., Rao, K. T., Reddy, V. K., Kiran, P. S., & Rao, B. T. (2015). Mitigation of Insider Attacks through Multi-Cloud. *International Journal of Electrical and Computer Engineering*, *5*(1), 136-141.

Jofre, J., Velayos, C., Landi, G., Giertych, M., Hume, A. C., Francis, G., & Oton, A. V. (2014). Federation of the BonFIRE multi-cloud infrastructure with networking facilities. *Computer Networks, 61*, 184. https://doi.org/10.1016/j.bjp.2013.11.012

Karthic, C. D., Sujatha, S., & Praveenkumar, V. (2012). A Dynamic Cloud Discovery Framework for Deploying of Scientific Computing Services over a Multi-cloud Infrastructure. *Journal of Artificial Intelligence (Faisalabad), 5*(4), 161.

Khattak, H. A. K., Abbass, H., Naeem, A., Saleem, K., & Iqbal, W. (2015). Security concerns of cloud-based healthcare systems: A perspective of moving from single-cloud to a multi-cloud infrastructure. *The Institute of Electrical and Electronics Engineers, Inc.(IEEE) Conference Proceedings.*, 61-67. https://doi.org/10.1109/HealthCom.2015.7454474

Lal, K. (2015). How Does Cloud Infrastructure Work? *Asia Pacific Journal of Energy and Environment*, *2*(2), 61-64. https://doi.org/10.18034/apjee.v2i2.697

Thandeeswaran, R., Subhashimi, S., Jeyanthi, N., & Durai, M. A. S. (2012). Secured Multi-Cloud Virtual Infrastructure with Improved Performance. *Cybernetics and Information Technologies, 12*(2), 11-22.

--0--

SOCIAL SCIENCE RESEARCH NETWORK
2171 Monroe Avenue, Suite 203, Rochester, NY 14618, USA
http://www.ssrn.com/en/
AJTP Link: https://www.ssrn.com/link/American-Journal-Trade-Policy.html