International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 07 | July - 2021 ISSN: 2582-3930

Multi-Cloud and its Security

Deepali D. Ahir

M. E.S College of Engineering, Pune

Abstract -As the world is moving towards cloud computing, most of the enterprises started using a blend of existing IT infrastructure and diverse cloud models like multi-cloud, a hybrid cloud which gives cost savings, flexibility, performance, and scalability. With resources and services spread across multiple clouds, the attack surface is also multiplied. Now there are more services and resources to protect, and there are diverse ways to secure them because each cloud provider has its own set of services and ways to protect them. To protect the data and infrastructure, there is a need for continuous monitoring of the infrastructure for malicious activities, anomalous behaviours and the need to proactively calculate the security posture.To build security, different cloud providers offer different ways to secure your cloud resources and data, but with these blended environments, it is a challenge to learn and understand all these security tools and configuration options provided by different vendors. It will be a great help if we could find tools that provide a uniform interface to view and manage infrastructure across all clouds.

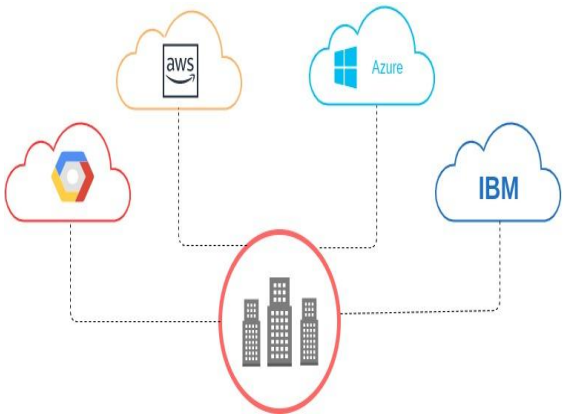
Key Words: Cloud computing, Multi-cloud, cloud providers, security challenges, AWS, GCP, Azure, Cloudquery, Steampipe

1.INTRODUCTION

Knowing the fact that a single cloud provider can not satisfy all the needs, enterprises started using different cloud services from different providers concurrently for service(Saas), infrastructure(Iaas), and platform (Paas) and making the most of the benefits. In multi-cloud, multiple cloud services are used from different vendors in a single heterogeneous architecture to optimize application and data performance along with the cost. It differs from a hybrid cloud where public, private deployment modes are typically used.

What is Multi-Cloud

In multi-cloud, more than one public cloud is used in a single network at one time. Figure 1 shows the use of different public clouds from different cloud vendors. Enterprises use this multi-cloud architecture to distribute their work load and to reduce the risk of data loss and downtime. Multi-cloud architecture improves the performance and overcomes the single cloud provider's unavailability thus avoiding the single point of failure[13].



Cloud Providers

In today's market, there are many cloud providers available like

- Google Cloud Platform(GCP)
- Microsoft Azure
- Amazon Web Services (AWS)
- Openstack
- Rackspace
- Vmware Cloud
- IBM Cloud

All of them provide cloud solutions with different features offered, some are better than others for certain tasks. These cloud providers offer many services that can benefit their customers, such as fast access to their data from any location, scalability, pay-for-use, data storage, data recovery, protection against hackers, on-demand security controls and use of the network and infrastructure facilities [3]. Using these providers enterprises can change their use of the CAPEX model to the OPEX.

After moving from capex to opex, enterprises can get many benefits like business strengthening, enhancing staff productivity, and delivering cost savings [4]. Also, it can enjoy the benefits of agility and scale while improving resiliency, availability, and performance[4].

But the major task is the selection of the best suitable cloud provider, selection of a cloud provider is a challenging task for the established enterprises with enormous data. It includes many factors like the business requirements, features provided by the cloud, the cost offered, and many more.

2. Why use Multi-cloud architecture

A multi-cloud architecture combines different services from different cloud providers so that they can distribute their workloads across multiple cloud environments and can get the best out of them. For example, one cloud provider is best in faster data transfer and the other gives better data security, it is an enterprise choice to choose one suitable for their business goals. Following are the reasons why enterprises choose multi-cloud architecture:

Flexibility

Choosing the best suitable cloud platform across multiple cloud providers with different options available gives you more flexibility.

Scalability

It is the ability to increase or decrease IT resources depending on the business need, using the multi-cloud.

Cost

Instead of extending infrastructure, enterprises can start using virtual data centers without any addition of the hardware. This saves space as well as the cost of hardware.

Disaster Avoidance

There are many reasons for failure like it can be because of human errors, sometimes it can be because of calamity. If you have multiple cloud domains that can bypass downtime and ensure to have computing resources available.

3. Managing Security in Multi-Cloud

When an enterprise uses multi-cloud , its security is the biggest task to handle. Each cloud provider you add, adds more attack surfaces and pushes the enterprise towards more risk. All public clouds work on a shared responsibility model, where security of the cloud is the responsibility of the provider but the security in the cloud is the responsibility of the customer. This means that customers have to make sure that they understand the configuration of each service well, and that they configure the services according to best practices. With multiple services spread across multiple clouds, it is a lot of data/policies to decipher, understand and implement. Moreover each cloud has its own user interface and command line tools, adding to the already steep learning curve for cloud adoption.

So it is crucial to have properly defined security policies and the distribution of these policies among multi-cloud environments.

Security Challenges in Multi-Cloud

1. DIfferent nomenclature followed by different cloud providers. Example: a machine in AWS is an EC2 instance, whereas it is called a Compute VM in Azure. In GCP "Service principal" is an important part of Identity and Access Management, but it is an alien term for AWS.
2. The use of multiple security tools generates a dissociate security posture. AWS has aws CLI, GCP has gcloud, and Azure has az CLI tool and powershell.
3. Even the compliance standards like CIS have different set of compliance checks spread across different services for AWS/GCP/Azure.
4. Defining a unified approach for security management among all the cloud providers is a complex task
5. Lack of visibility across the threat landscape can impede threat investigation and response times.

To overcome these challenges many commercial solutions are available in the market where they provide a unified security approach for all the cloud services. Many open source solutions are also available which configure, analyze, manage and solve multi-cloud security challenges.

Open-source tools for multi-cloud security

1. **Cloudquery(Uptycs)**

Cloudquery is the product of United State based IT firm Uptycs founded in 2016. It provides multi-cloud security by monitoring the configuration policies of enterprise cloud resources and data [5].

What is Cloudquery and how does it work?

- Cloudquery is the extension of osquery, those who are familiar with osquery can easily understand cloudquery [5].
- It has a single place to manage data across AWS, Azure, and GCP cloud providers [5].
- It eases the monitoring and visualization of enterprise cloud resources [5].
- It has an interface similar to SQL, so no need to understand different tools provided by cloud providers as SQL is very known to everyone [5].
- It can create scheduled queries to collect data from cloud providers and send it to the configured destination [5].
- It conducts real-time inspections and does comprehensive analysis [5].

2. **Steampipe**

Steampipe is an open-source tool of Turbot, Newyork, USA. It provides a command-line interface(CLI) that solves issues related to cloud resources and services.

How Steampipe works

- The main goal of steampipe is to simplify the workflow for the cloud, it reveals cloud configuration into a high-performance relational database [6].
- With Steampipe SQL tables act as complex cloud resources like security groups, databases, etc.[6].
- When any user writes a SQL query, Steampipe converts it into API calls, these calls get executed in real-time cloud services APIs [6].

- Data that will be fetched as a result of query execution is stored into the tables using PostgreSQL, which allows users to do many tasks just like any other database table [6].

3. Cloudquery(Cloudquery.io)

This open-source tool converts cloud infrastructure into queryable SQL tables for easy monitoring and security [7]. It provides support for different cloud providers mainly Aws, Azure, GCP, and Okta [7].

How cloudquery works

- cloudquery fetches, monitors, and normalizes cloud infrastructure into SQL database once [7].
- This SQL database can be queried to extract more information to detect security and compliance failures.
- This way it extracts different disband APIs which enables security, cost, governance,compliance policies with SQL [7].
- It can be extended to more resources [7].

4. ScoutSuite

ScoutSuite is a CNCF Sandbox project [10]. It is an open-source multi-threaded security audit tool for cloud environments.ScoutSuite is developed by a security consultant and is written in Python [8].It provides support for AWS, Azure, GCP, Alibaba, and Oracle Cloud.

How ScoutSuite works

- It collects configuration data from cloud providers for manual exploration and brings out risk areas using APIs exhibited by cloud providers [8].
- After completing a security audit it provides a comprehensive vision of attack surfaces automatically [8].

5. Cloud Custodian

Cloud Custodian is an open-source tool that merges different tools used by enterprises for cloud management into a single tool [9]. It is used to manage AWS, Azure, and GCP [10].

How Cloud Custodian works

- First, it requires writing all the policies into a YAML file [10].
- Policies describe the resource type on which each policy will run, set of filters that control resources and it also includes a mode that controls policy execution [10].
- With Cloud custodian, it is easy to set rules and validate[10]

6. Security Monkey

It is the open-source product of Netflix which monitors, notify and describes security breaches. It works on AWS, GCP, OpenStack [11].

How Security Monkey works

- It browses through all the cloud services, accounts, regions [11] .
- It remembers the previous states and can tell you what changed and when [11].

Security Monkey has three technical components : Watcher responsible for monitoring, Notifier which alerts users when an item has changed and Auditor executes business rules at odds with configuration to check the risk [12].

4. CONCLUSION

Multi-cloud gives more flexibility and reliability in many ways and hence enterprises are going for multi-cloud deployments. These deployments pose a challenge to security professionals as they have to get acquainted with the nomenclature and tool sets of multiple cloud providers. They need to learn and understand many tools provided by different cloud providers, and understand the best ways to configure their services. Implementing the compliance standards is also a daunting task because they have different compliance checks for different cloud providers.

To overcome the security challenges incorporated with multi-cloud many open source tools are available as discussed above with their own pros and cons. Without any doubt, these tools provide better usability by providing uniform access to multi-cloud configuration.These tools also have the ability to extend their functionality to suit specific needs.Enterprises using multi-cloud environments will benefit from using above mentioned open source tools to secure their cloud infrastructure. It will help customers by easing out the learning curve, as they won't need to learn and master multiple tools. Plus less number of tools also mean easier software lifecycle and dependency management. Overall, a unified view and single page of glass to look at and manage all your cloud infrastructure is a great boon for customers going for multi-cloud deployments.

REFERENCES

1. "How To Ensure Flexibility in a Hybrid Multicloud Strategy" by Veritas http://www.veritas.com/cloud
2. https://www.vmware.com/topics/glossary/content/multi-cloud-management
3. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications
4. Rory Duncan "A *multi-cloud* world requires a *multi-cloud security* approach Computer Fraud & *Security* 27 May 2020 Volume 2020, Issue 5 (Cover date: May 2020)Pages 11-12"
5. https://www.uptycs.com/product-opensource-cloudquery
6. https://steampipe.io/blog/introducing-steampipe
7. https://docs.cloudquery.io/
8. https://github.com/nccgroup/ScoutSuite
9. https://cloudcustodian.io/docs/index.html
10. https://github.com/cloud-custodian/cloud-custodian
11. https://github.com/Netflix/security_monkey
12. https://netflixtechblog.com/announcing-security-monkey-aws-security-configuration-monitoring-and-analysis-1f2bfb001708

13. Danilo Ardagna, "Cloud and Multi-cloud Computing: Current Challenges and Future Applications"

BIOGRAPHIES

Deepali D. Ahir received M.E degree in 2013 from Savitribai Phule Pune University. She works as an Asst. Professor in M.E.S College of Engineering, Pune