Abbas *et al* *LGURJCSIT* 2018

LGURJCSIT
ISSN: 2519-7991

LGU R Journal for
Computer Sciences IT

Research Article

Vol. 2 Issue 2 April-June 2018

Review on Huawei Fusion Sphere Security

Sabir Abbas, Shan-e-Zahra

Department of Computer Science, Faculty of Information Technology, Lahore Garrison University, Lahore, Pakistan

sabirabbas065@gmail.com., shanezahra@lgu.edu.pk.

Abstract:

The cloud computing virtualization stage, services as another method for giving computing resources, gives clients available and financially savvy benefits, and brings hazards in the meantime. In this way, ensuring the privacy, trustworthiness, and accessibility of client information turns out to be significantly more basic to distributed computing frameworks. Huawei gives the virtualization stage security answers to confront the dangers and difficulties postured to the distributed computing framework. This article portrays the techniques and measures received by Huawei cloud computing virtualization stage to react to the security dangers and dangers to distributed computing frameworks. Huawei cloud computing virtualization stage is intended to give secure and solid server virtualization solutions for clients.

Keywords: *FusionSphere, Cloud Security, Cloud Computing, Huawei Architecture.*

1. INTRODUCTION

Created by Huawei, Fusion Sphere is a cloud-operating framework that addresses the issues of clients from an extensive variety of businesses. Fusion Sphere offers capable virtualization and resource pool management functions, far reaching cloud framework parts and devices, and open application programming interfaces (APIs).

It causes endeavors to on a level plane merge physical and virtual assets in server farms and vertically streamline benefit stages, encouraging the development and utilization of cloud computing stages. In July 2014, the extraordinary execution of Huawei's Fusion Sphere prompted Huawei turning into the main organization added to Gartner's Magic Quadrant for x86Server Virtualization Infrastructure amid that year. FusionSphere was likewise perceived as a cutting-edge item in developing markets [1][2]. FusionSphere incorporates OpenStack design to develop a product defined server farm ability and ideal robotized administration capacities, and backings business utilization of cloud-based telecom administrations [5].

What's more, FusionSphere is an open, deft, and solid cloud OS that means to encourage endeavors and bearers convey server virtualization, and in addition private, open, and half breed cloud administrations. In this manner, undertakings can utilize standard OpenStack design and APIs to pick unreservedly from OpenStack-based outsider items and administrations, making distributed computing less demanding [6] [8]. Here is the Architecture of FusionSphere: [1,2,3]

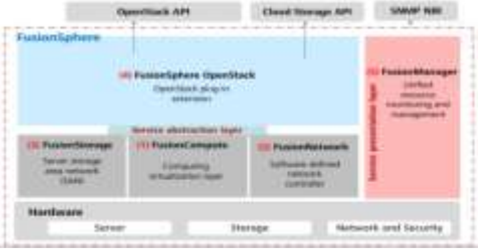

Figure No1: Architecture of fusion Sphere

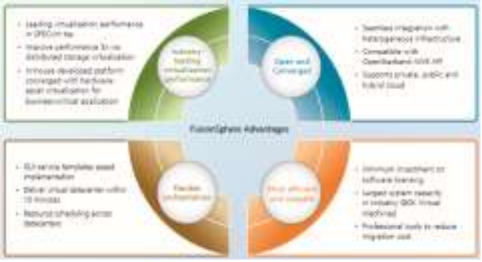

Figure No 2: Fusion Sphere Advantages

FUSIONSPHERE COMPONENTS

2. LITERATURE REVIEW

As a main cloud benefit mark, HUAWEI CLOUD HC is focused on furnishing clients with dependable and secure cloud administrations equipped for reasonable development, connecting the present to the future for ventures. HUAWEI CLOUD helps medium-and expansive measured endeavors address issues in cloud change and empowers the undertakings to exploit business openings later on. It helps little and medium-sized endeavors develop and anchors their future.

HUAWEI CLOUD holds fast to benefit limits and the three "don't" (we don't create applications, we don't contact clients' information, and we don't make value venture). Huawei teams up with clients for joint advancement, constantly making qualities for clients and accomplices. As of February 2018, HUAWEI CLOUD has 100 cloud benefits under 14 classifications and more than 60 arrangements particularly suited for the assembling, social insurance, web based business, Internet of Vehicles, SAP, HPC, and IoT segments, serving countless undertakings. In July 2017. HUAWEI CLOUD has been exceedingly perceived by the British Standards Institution and won the CSA STAR gold decoration accreditation. In April 2017. Huawei issued open cloud systems and discharged Service Stage, the primary open cloud benefit suite intended for Cloud Native application engineers, and will discharge 10 situation particular cloud benefit arrangements inside the year.

In March 2017. Huawei built up Cloud BU and put in excess of 2000 faculty out in the open mists, discharged 54-cloud administrations including 10 classifications, and turned into the principal Asian platinum individual from the OpenStack Foundation at the OpenStack's Board of Directors meeting. In December 2016. Huawei wound up one of the principal group of merchants whose distributed computing administration capacities are perceived by the Ministry of Industry and Information Technology (MIIT) and Huawei open cloud benefit was regarded as the propelled benefit. In November 2016. Huawei was respected as one of "Solid Performers" without precedent for The Forrester Wave™: Public Cloud Platforms in

China, Q4 2016. In May 2016. Huawei was very prescribed to people in general cloud advertise in Europe in Forrester-Brief-China's Clouds come to Europe. The report accentuated Huawei's driving position in China's open cloud advertise. In January 2016. Huawei turned into the gold board chief of OpenStack. In 2015, HUAWEI CLOUD passed the level-3 security insurance validation, discharged undertaking cloud benefits in China, and participated with universal telecom bearers on the advancement of open mists. In 2014 Huawei ended up one of the primary bunch of cloud specialist organizations that passed the ISO 27001 validation, the most broadly utilized confirmation in the data security field. In 2013, Huawei discharged cloud OS FusionSphere and turned into the brilliant individual from the OpenStack Foundation. In November 2010. Huawei distributed computing system was propelled out of the blue.

3. METHODOLOGY:

Huawei provides the virtualization platform security solution to face the threats and challenges posed to the cloud computing system.

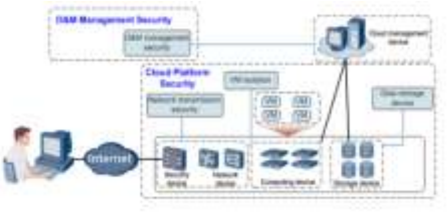

Figure No 3: virtualization platform structure

Each layer of the security structure is described as follows:

3.1. Log security management

Administrators can view logs to ascertain system running status and operation records, thereby auditing user behaviors and locating problems. An operation log records the operation a user has performed on the system, for example, logging in to the system, logging out of the system, or creating a VM, as well as the result of the operation. The operation logs can help administrators check whetk2her the system is under attacks or malicious operations are performed [2][9][14].

3.2. Account and password management

On Fusion Manager, administrators can change user passwords periodically to ensure password security.

3.3. Rights management

Fusion Manager provides comprehensive rights management functions. User permissions are controlled by organization and domain [2]. This helps isolate the data of different organizations and domains and secure the internal resources of the system.

3.4. Web security management

The framework supports against web application assaults, for example, SQL infusion and cross-website scripting. A realistic confirmation code is required on the login page. On the web-based login page, the framework creates an irregular confirmation code [11][12]. A user can log in to the system only when the user name, password, and verification code they entered are correct. On first login, users are not required to enter the verification code. However, if they enter an incorrect password, they will be asked to enter the verification code during the next login attempt. The web management system is automatically locked if no user activity is detected in a preset period of time [2][8][13].

3.5. Data security management

Essential security settings are executed to guarantee secure working of databases. The accompanying security-related measures are gone up against a PostgreSQL database:

1. Logs operations performed on the PostgreSQL database.
2. Prevents remote access to the database.
3. Backs up information to reestablish the database in case of a database disappointment.

3.6. OS security management

The Fusion Manager system uses a SUSE Linux OS. Basic security settings are configured to protect the security of the SUSE Linux OS, including: [10][15][16]

1. Disables unnecessary services, such as Telnet and FTP services.
2. Hardens the secure shell (SSH) service.
3. Controls the access permission on files and directories.
4. Records operation logs.

3.7. Security against malformed packet attacks

Because Fusion Manager interacts with end users on un trusted networks, it may be vulnerable to malformed packet attacks. Fusion Manager has been fully tested using tools, such as Codenomicon and xDefend, on its capability of defending against malformed packet floods, ensuring the security of the Fusion Manager system during interaction with end users [3][10][15].

3.8. Data Backup

In the Fusion Sphere solution, one or more copies of backup data are stored so that data is not lost and services are not affected even if storage devices such as hard disks become faulty. The system performs a bit- or byte-based verification on data stored in disks, and distributes verification information to each disk in a disk array. During the distribution, the system makes sure that a data block and its verification information are stored on different disks. In this way, damaged data can be reconstructed based on other data blocks and corresponding verification information after a disk is damaged [4].

4. PROVEN SUCCESS

Huawei Fusion Sphere has served clients in 42 nations and locales around the world, covering fields going from government and open utilities to broadcast communications, vitality, finance, transportation, social insurance, instruction, media, producing and different enterprises. FusionSphere enables clients to incorporate and enhance their server farms and administration stages, enhancing framework ependability and IT efficiency [5][6].

Cost-effective virtualization
Secure, reliable services
Easy and effective operation

Figure No 4: Proven Success of Fusion Sphere

5. CONCLUSION

CC systems can face traditional Security threats from external network like IP attacks, OS and software loopholes, Virus, SQL injection, Phishing, Zero-day attacks and from intranet include Ever-changing attacks pose difficulties for prevention, Worms and viruses are spread through loopholes if patches and virus database are not upgraded to the latest version, causing tremendous security threats, Confidential information disclosure happens frequently because of unauthorized Internet access activities, Convenient mobile device access challenges intranet security and Data leakage and virus spreading occurs due to the lack of peripheral management. So the Huawei fusion sphere provides the virtualization platform security solution to face the threats and challenges posed to the cloud computing system. Fusion sphere manager manages the cloud security in all aspects.

6. REFERENCES

[1] Nakai, Y., & Tanaka, Y. (2010, July). Chinese company's IPR strategy: How Huawei Technologies succeeded in dominating overseas market by Sideward-Crawl Crab Strategy. In *Technology Management for Global Economic Growth (PICMET),* IEEE. *Proceedings of PICMET'10:* (pp. 1-5).*2010*

[2] Winkler, V. J. (2011). *Securing the Cloud: Cloud computer Security techniques and tactics*. Elsevier.

[3] Wei, J., Zheng, Z., & Liu, S. (2006). *U.S. Patent Application No. 11/549,186*.

[4] Liu, S., Wei, J., & Li, C. (2007). *U.S. Patent Application No. 11/697,601*.

[5] Huawei FusionCloud DataCenter Virtualization Solution: http://enterprise.huawei.com/en/products/itapp/cloud-platform-software/cloud-platform-s/hw-127115.htm

[6]Huawei FusionSphere: http://enterprise.huawei.com/en/solutions/IT-solutions/server-consolidation/hw-133186.htm

[7] Sabahi, F. Cloud computing security threats and responses. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on* (pp. 245-249).

[8] Huawei, Z., & Ruixia, L. A scheme to improve security of SSL. In Circuits, Communications and Systems, 2009. PACCS'09. Pacific-Asia Conference on (pp. 401-404).

[9] Horne, D. (2001). U.S. Patent Application No. 09/996,671.

[10] Kaufman, L. M. (2009). Data security in the world of cloud computing. IEEE Security & Privacy, 7(4).

[11] (CC) Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2012. Version 3.1 Revision 4.

[12] (CEM) Common Methodology for Information Technology Security Evaluation. September 2012. Version 3.1 Revision 4.

[13] ISO/IEC TR 19791, Information technology–Security techniques–Security assessment of operational systems, ISO/IEC, April(2010).

[14] (ISO/IEC) 15408, Common Criteria for Information Technology Security Evaluation

Part 1, 2, 3, Version 3.1 R4, Common Criteria, September(2012).

[15] (ISO/IEC 18045), Common Methodology for Information Technology Security Evaluation, Version 3.1 R4, Common Criteria, September (2012).

[16] CESG, http://www.cesg.gov.uk, February 10(2013). The Common Criteria, http://www.commoncriteriaportal.org, (2013).

[17] KISA(Korean Internet Security Agency), http://kisec.kisa.or.kr/kor/main.jsp, (2013).