LGURJCSIT
Volume No. 1, Issue No. 4 (October- December), pp. 58-63

Review on Huawei Fusion Sphere Security

Sabir Abbas, Shan-e-Zahra, Noor-ul-Qamar

Abstract: The cloud computing virtualization stage is another method for giving computing resources that give clients available and financially savvy benefits, and bring hazards in 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 for confronting 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 also dangerous 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

Developed by Huawei, FusionSphere is a cloud operating system that meets the needs of customers from a wide range of industries. FusionSphere offers powerful virtualization and resource pool management functions, comprehensive cloud infrastructure components and tools, and open application programming interfaces (APIs).

It helps enterprises to horizontally consolidate physical and virtual resources in data centers and vertically optimize service platforms, facilitating the construction and use of cloud computing platforms. In July 2014, the outstanding performance of Huawei's FusionSphere led to Huawei becoming the only company added to Gartner's Magic Quadrant for x86Server Virtualization Infrastructure during that year. FusionSphere was also recognized as an up-and-coming product in emerging markets [1][2].

FusionSphere integrates OpenStack architecture to build up

a software-defined data center capability (including SDS and SDN) and optimal automated management capabilities, and supports commercial use of cloud-based telecom services (NFV and network function virtualization)[5].In addition, FusionSphere is an open, agile, and reliable cloud OS that aims to help enterprises and carriers deploy server virtualization, as well as private, public, and hybrid cloud services. Therefore, enterprises can use standard OpenStack architecture and APIs to choose freely from OpenStack-based third-party products and services, making cloud computing easier[6][8].Here is the Architecture of FusionSphere:[1]

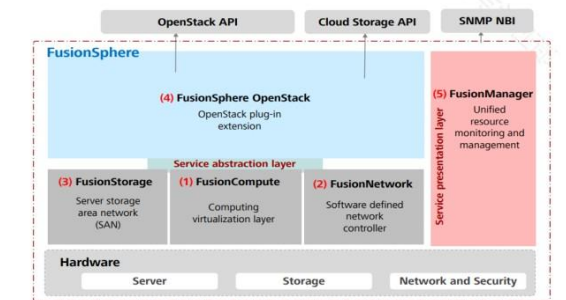

Fig 1: Architecture of fusion Sphere

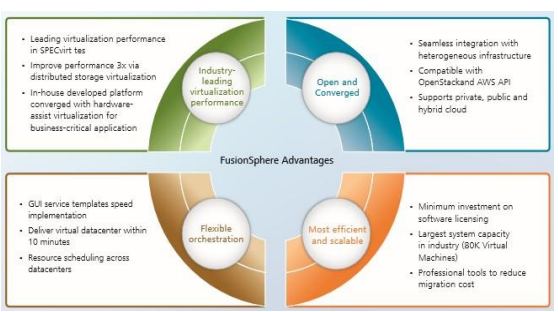

Fig 2: Fusion Sphere Advantages

FUSIONSPHERE COMPONENTS

2. LITERATURE REVIEW

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

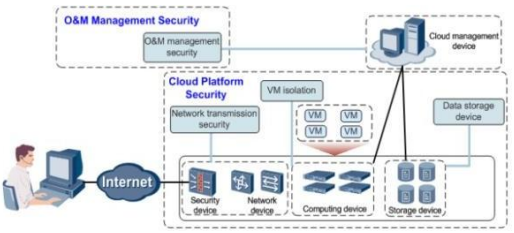

Figure 3: Structure of the virtualization platform security solution

Each layer of the security structure is described as follows:

2.1. 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 whether the system is under attacks or malicious operations are performed[2][9].

2.2. Account and Password Management

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

2.3. 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.

2.4. 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. A user can log in to the system only when the user name, password, and verification code they entered are correct. Note: 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].

2.5. 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.

2.6. 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]

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.

2.7. Security Against Malformed Packet Attacks

Because Fusion Manager interacts with end users on untrusted 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].

2.8. 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].

3. PROVEN SUCCESS

Huawei FusionSphere has served customers in 42 countries and regions around the globe, covering fields ranging from government and public utilities to telecommunications, energy, finance, transportation, health care, education, media, manufacturing and other industries. FusionSphere helps customers integrate and optimize their data centers and service platforms, improving system reliability and IT efficiency [5][6].

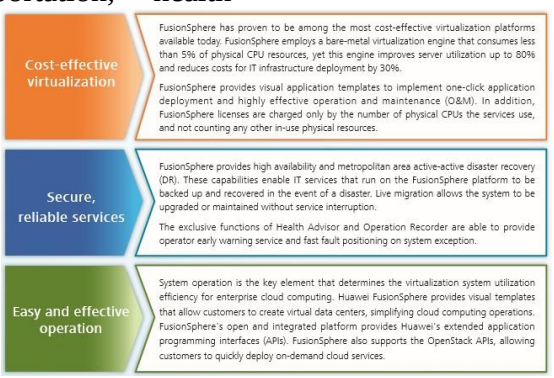

Fig 4:Proven Success of Fusion Sphere

4. CONCLUSION

Cloud Computing 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.

5. 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), 2010 Proceedings of PICMET'10:* (pp. 1-5). IEEE.

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

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

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

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

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