A LOOK AT EDGELESS HYBRID-CLOUD INFRASTRUCTURE – AN OPTIMIZED SOLUTION FOR MULTI-SITE BACKUP, DISASTER RECOVERY AND HIGH AVAILABILITY

Ogbomo Efosa
Graduate Student
University of Cincinnati
Cincinnati, OH 45219, USA
ogbomoem@mail.uc.edu

Chengcheng Li, PhD
Associate Professor
University of Cincinnati
Cincinnati, OH 45220, USA
chengcheng.li@uc.edu

ABSTRACT

Cloud computing has been one of the major disruptive technology of this century changing the entire face of IT infrastructure across all spectrum. This has led to tremendous development, improvement and cost efficient means of securing IT infrastructures. Virtualization is the backbone driving the numerous cloud solutions and also making them marketable in the pay-as-you-use mechanism for all kind of deployment. This research is focus on improving the security and performance of cloud storage, backup and disaster recovery by evaluating the possibility of eliminating the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). A live synchronization between production and Disaster Recovery (DR) sites is presented. We considered the mechanism behind Virtual Machines (VM) and hypervisor interaction with physical memory on host computers and evaluated the ability of VM to read/write directly to a unified multiple storage locations. Dependencies, requirements and guidelines for implementing this solution would also be analyzed.

IT Research Symposium'19 Extended Abstracts, April 9, 2019, Cincinnati, Ohio, USA.

KEYWORDS

Virtualization; hypervisor; virtual-machines; disaster-recovery; virtual-storage; container; V-shadow.

INTRODUCTION

The increasing migration of critical services and business operations to the cloud, has led to the increase need and demand for more reliable and secure cloud infrastructure. And obviously, reliable data centers and critical applications as seen in health care, banking systems, stock exchange and other businesses, need an effective and efficient failure recovery mechanism to prevent against catastrophe, as just a few minute downtime cost most of these organizations huge amount of money.

Huge attention and several research have been carried out and still ongoing (as shown in the literature review section below) with a view of improving cloud backup and recovery. Most of these research helped to reduce backup and recovery time. We aim to eliminate the recovery time completely by analyzing virtualization storage, Network attached storage (NAS) and remote storage. Also, a review of how Virtual Machines (VMs) and containers write to memory will be conducted. And an evaluation of the possibility of these systems writing synchronously to multiple storage locations at the same time.

LITERATURE REVIEW

Cloud computing and several cloud services has been one of the major disruptive technologies of this century, changing the entire face of IT infrastructure across all spectrum. This has led to tremendous development, service improvement and cost efficient means of securing IT infrastructure, data centers, compute resources, IOT computing etc. Virtualization is the backbone driving the numerous cloud solutions and also making them marketable in the pay-as-you-use mechanism for all kind of deployment, Back-up and disaster recovery, big data analysis and so much more Modi and Acha, (2016); Silva, Kirikova and Alksnis, (2018).

Virtualization technology (Hypervisor and Container based) has enabled us to provide reliable infrastructures, ensure high availability and guaranteed better performance across mission critical applications both in government and at the enterprise level today by improving server utilization, reducing management cost and energy consumption Zhu, Jiang, Xiao and Li, (2011); Wu, Li, Wang, Jin and Chen, (2015). To maximize the numerous advantages of virtualization, Wu et al developed (VShadow); an efficient means of promoting physical machines into virtual machines (VMs) and enabling live migration processes in virtualization platforms as well.

Also, the concept and benefits of resource virtualization has been utilized in several other fields like smart factory “industry 4.0” Lu and Xu, (2018), IoT and Industrial IoT (I-IOT) with their throughput and latency compared by Batalla, Sienkiewicz, Latoszek, Krawiec, Mavromoustakis, and Mastorakis, (2016) and implemented in mobile edge computing (MEC) as well Hsieh, Lee, and Chen, (2018).

However, with the ever growing volumes of critical data on cloud data centers and the increasing dependencies on cloud infrastructure, Enterprises are exposed to a growing number and a wider variety of threats (known and currently devised – zero day exploits) and vulnerabilities Mugoh, Ateya, and Kasamani, (2012); LV and Rong, (2018); Dong, Zhu,Song, Li, Xiao, (2018)

As such, scheming adequate means of securing, deploying and managing cloud infrastructure becomes inevitable. Modi and Acha reviewed the various security challenges associated with virtualization, the inadequacy of different cloud firewalls, IDS/IPS techniques including machine learning techniques and AI, cloud security frameworks in general and identified research challenges, cloud IDS requirement which would help improve cloud security especially for the safe delivery of IoT.

The cloud platform and infrastructure is very dynamic and boundless (IoT), as such current security assessment methods has some limitations. LV and Rong proposed a security assessment model specifically for cloud platforms using “stochastic game nets”.

Other methods seems to accept the fact that security expert would always be on the losing side to hackers and activist – especially with the rise of zero-day exploits, ransom ware and other natural disaster by focusing their effort on mitigating exploits and these unforeseen circumstances. For example Zhu et al proposed a method for optimizing hypervisor-based-fault-tolerance (HBFT) which greatly improve the synchronization time between primary VMs and backup VMs to ensure no data loss and major downtime is experience during any of the various disaster recovery scenarios.

To ensure reliability and resiliency, data needs to be replicated in several geographical locations to mitigate against disasters on multiple company site and at the same time take into considerations several factors including RTO and RPO (Sengupta and Annervas, 2014).

METHOD

This research is focus on evaluating the possibility of eliminating the RPO and RTO in the Disaster Recovery (DR) systems completely by proposing a live and seamless synchronization between production and DR sites. At this initial stage of the research, we would consider the mechanism behind VM and hypervisor interaction with physical memory on host computers and then evaluate the ability of VM to read/write directly to a unified multiple storage locations (which might be at different geographical locations). Dependencies, requirements and guidelines for implementing this solution would also be analyzed

RESULTS AND DISCUSSION

The research assistants to help review other research papers and methodology on improving virtual storage technology. The software engineers to design the software and its interface for interacting with user and some devices and cloud accounts on AWS and Azure for analysis and troubleshooting.

PROPOSED CONTRIBUTION OF WORK

This research will be focusing on the improvement on the security and the performance of cloud storage, backup and disaster recovery. The evaluation should be a success by seeing the possibility of eliminating the Recovery Point Objection and Recovery Time Objective. The ability of the VM to read/write directly to a unified multiple storage locations will also be tested. Dependencies, requirements and guidelines for implementing this solution would also be analyzed.

REFERENCES

Modi, C., & Acha, K. (2017). Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: A comprehensive review. Journal of Supercomputing, 73(3), 1192-1234. doi:10.1007/s11227-016-1805-9

da Silva, V. G., Kirikova, M., & Alksnis, G. (2018). Containers for virtualization: An overview. Applied Computer Systems, 23(1), 21-27. doi:10.2478/acss-2018-0003

Zhu, J., Jiang, Z., Xiao, Z., & Li, X. (2011). Optimizing the performance of virtual machine synchronization for fault tolerance. IEEE Transactions on Computers, 60(12), 1718-1729. doi:10.1109/TC.2010.224

Programming, 45(1), 45-66. doi:10.1007/s10766-015-0385-2

Lu, Y., & Xu, X. (2018). Resource virtualization: A core technology for developing cyber-physical production systems.Journal of Manufacturing Systems, 47, 128-140. doi:10.1016/j.jmsy.2018.05.003

Batalla, J. M., Sienkiewicz, K., Latoszek, W., Krawiec, P., Mavromoustakis, C. X., & Mastorakis, G. (2018). Validation of virtualization platforms for I-IoT purposes. Journal of Supercomputing, 74(9), 4227-4241. doi:10.1007/s11227-016-1844-2

Hsieh, H., Lee, C., & Chen, J. (2018). Mobile edge computing platform with container-based virtualization technology for IoT applications. Wireless Personal Communications, 102(1), 527-542. doi:10.1007/s11277-018-5856-5

Mugoh, L., Lukandu Ateya, I., & Shibwabo Kasamani, B. (2012). Intelli-restore as an instantaneous approach for reduced data recovery time. Journal of Systems Integration (1804-2724), 3(3), 3-16. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=84631692&site=ehost-live

Lv, J., & Rong, J. (2018). Virtualisation security risk assessment for enterprise cloud services based on stochastic game nets model. IET Information Security, 12(1), 1-8. doi:10.1049/iet-ifs.2017.0038

Dong, J., Zhu, H., Song, C., Li, Q., & Xiao, R. (2018). Task-oriented multilevel cooperative access control scheme for environment with virtualization and IoT. Wireless Communications & Mobile Computing, , 1-11. doi:10.1155/2018/5938152

Sengupta, S., & Annervaz, K. M. (2014). Multi-site data distribution for disaster recovery—A planning framework.Future Generation Computer Systems, 41, 53-64. doi:10.1016/j.future.2014.07.007

Wu, S., Li, Y., Wang, X., Jin, H., & Chen, H. (2017). Vshadow: Promoting physical servers into virtualization world.International Journal of Parallel