INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 3)

Available online at: www.ijariit.com

A survey on design and implementation of out-of-band storage virtualization

Nikita Jain
jainnikita649@gmail.com
Kalinga University, Naya Raipur, Chhattisgarh

Sana Tak
sanatak06@gmail.com
Kalinga University, Naya Raipur, Chhattisgarh

ABSTRACT

Over the past several years, virtualization has evolved from a popular buzzword into a formidable strategic technology that many organizations have adopted and many others are strongly considering. This study paper revolves around the impact of virtualization at the various layers of storage stack. There is a rapid growth in the storage capacity, and hence the processing power in the respective enterprise's storage appliances coupled with the requirements for high availability and it needs a Storage Area Network (SAN) architecture for providing the storage and performance elements here. The Storage Virtualization provides us with a combination and management of storage resources for Storage Area Network with multiple servers as well as the storage devices. The main aim for storage virtualization is its necessity to be inexpensive and not affect the performance. This paper focus as on how virtualization helps security, Memory Management, Power Management and Disaster Recovery.

Keywords: *Storage, Performance, Virtualization, Network, Storage Virtualization, Storage Area Network (SAN), Network, Attached Storage (NAS), Server, Storage Device (Sub-System), Host, Virtual machine, Hypervisor.*

1. INTRODUCTION

The definition of the storage virtualization according to Storage Networking Industry Association (SNIA) [11] is as" the act of abstracting, hiding, or isolating the internal functions of a storage system or service from applications, host computers, or general network resources, for the purpose of enabling application and network-independent management of storage or data.

" Or"

The application of virtualization to storage services or device for the purpose of aggregating functions or devices, hiding complexity, or adding new capabilities to lower level storage resources." The technique of storage virtualization is very recent and useful in the utility of public interest. The study of weather forecasting, Genetic study, astrological study and another various discipline where a lot of unclassified data are required. These data are also not available to a single location or in single occupancy. Virtualization in storage is the very helpful approach for the detailed study of the concerns related to mankind. The networked storage technologies are very helpful for such need. Now we can't stick with a single vendor storage, and, different data center or cloud provider also have storage from a different vendor, so virtualization is required. Here a virtualized storage is a very handful technique to extend. At the same time, the main advantage of virtualization technique is resource sharing and isolation, which provides a path for QoS in storage allocation also.

Security

The study made by Benard O. Osero [8] and David G. Mwathi [8] on security implementation in virtualized network storage environment found that this system has all traditional software security issue because the service of virtualization is offered by hypervisor which is a software program. Their finding was that such system must have efficient resource sharing and isolation which should ensure the virtualization meaning. There is a high responsibility to ensure security here because in storage virtualization there is several logical machines so more risk of possible attacks.

Storage Management

Guangyan zhang et al. [2] were designed and implemented out-of-band virtualization for large SAN. This implementation was very robust to power failure. It incorporated existing legacy system. This technique was based on SLAS2 approach for scaling round robin stripped volume. Although their approach was able to manage

memory and power failure they didn' t provided security to the data stored on the infrastructure. Study on memory management approach in a virtual environment by xian chen et al. [4] has revealed many things like page sharing which was mostly implemented by self-sharing whose rate varies between platforms. Page size has also a significant influence on Linux than Windows platform. They have given a very nice approach to managing memory by the study on different OS and page sharing concept, but this approach was not solving the disaster recovery issue efficiently. The work of kai Qian et al. [9] on out-of-band storage virtualization system that supports thin provisioning. They introduced mapping metadata caching and lazy update technique that is very helpful for achieving least interaction overhead between metadata server and client. Their work was significantly able to address capital expense and power consumption along with the best mechanism for storage management and reclamation approach.

the access request. The use of Thin-store [9] ensures the proper disk utilization in the environment of storage area network where a pool of storage is available and management of unutilized sectors are poorly implemented. The multiprotocol switch [10] uses different protocols to make it capable of holding different approach for managing power requirements. The Enhanced Cloud Control and Security System (EC2S2) is totally host based add-on architecture which supports all kind of hardware and operating system platform. The proposed method provides an advanced protection against hypervisor related attacks and security against data stored on the physical device in the virtual environment from getting theft as well as unauthorized access. Our proposed method contains three concepts which are as follows:

1) Secure Storage Virtualization

2) Thin Provisioning

3) Multiprotocol Switch

Power Management

The proposal made by Huojun lno et al. [10] on multi-protocol switch using PCI Express (PCIe) protocol with PCIe switch fabric for I/O and switch virtualization achieved high bandwidth, low power as well as low latency multiprotocol switching. Their proposal is based on the fact that latency and I/O rate suffers due to legacy components. They have session establishing phase. This encrypted token along with proposed a technique to overcome it. But they didn' t encrypted{Token+Path} is passed to the hypervisor. Consider the security, isolation, and policy-based allocation.

2. DESIGN AND IMPLEMENTATION OF STORAGE VIRTUALIZATION

The existing solutions of storage virtualization have many problems [2,3,8]. To address those issues, we propose an architecture, Enhanced Cloud Control and Security System (EC2S2) that is the secure and efficient implementation of out-of-band storage virtualization. This method is targeted to provide security in the storage virtualization for VMs as well as proper storage and power management to get enhanced and efficient kind of infrastructure. It also provides proper isolation and integrity to the VM' s in the storage area network. This method uses cryptographic technology [8] by the file manager and assisted by minimal hardware support. It is incorporated with the cryptographic technique that uses session-based access and cross verification of the identity of the access request. The use of Thin-store [9] ensures the proper disk utilization in the environment of storage area network where a pool of storage is available and management of unutilized sectors are poorly implemented. The multiprotocol switch [10] uses different protocols to make it capable of holding different approach for managing power requirements. The Enhanced Cloud Control and Security System (EC2S2) is totally host based add-on architecture which supports all kind of hardware and operating system platform. The proposed method provides an advanced protection against hypervisor related attacks and security against data stored on the physical device in the virtual environment from getting theft as well as unauthorized access. Our proposed method contains three concepts which are as follows:

- Secure Storage Virtualization
- Thin Provisioning
- Multiprotocol Switch

2.1 Secure Storage Virtualization

Our system allows secure access control to the storage virtualization approach. The security is enabled by adding File server, Client component and SAN component [8]. These security components are based on cryptographic capabilities issued by file manager and verified by drivers with least hardware support. This technique provides secure communication link and allows encryption of data using SSL. The use of SSL imparts additional cryptographic security. This framework works as follows.

- VMs are making a request for a file to be accessed from the file server.
- File server encrypts and generates {Token+Path} and passes to the Client component.
- 3. The Client component and SAN component establish a session using asymmetric key cryptography. After establishing the session, the component server continues communication using symmetric key encryption. Once the session expires, each of the systems denies the symmetric key used for that session.
- Client component encrypts the token to be used in the session establishing phase. This encrypted token along with encrypted{Token+Path} is passed to the hypervisor.
- VM passes encrypted{Token+Path} to SAN component
- The token is validated and authenticated by SAN component and client component mutually.
- If token validation is successful then storage network is allowed to release file else operation will be denied.
- Once storage network is allowed, the file will be made available to the VM for that particular session. The entire process of key generation and cross-validation ensures that the identified user is authentic to be authorizing the access. Here the application of cryptographic technique identifies the valid users, then authenticate for the present session and finally authorizes the users to access the data. This helps in the securing of data.

2.2 Architecture of Thin-Store

Storage provisioning is the technique of allocating storage space to virtual machines, servers or any other computing device and it is deployed in compute layer. Thin-store [9] is based on the technique of provisioning, which ensures the ability of the system to utilize the resource intelligently in case of huge availability. Sometimes due to huge availability, design implementation doesn't' t bother about the management and unfortunately misuse the resource. So, we need to be much careful here. This technique is based on the bit-mapping to keep track of the unutilized blocks and sectors. The best part of this technique over other existing technique is that the overhead associated with the technique is very less and efficiently maps the available disk sectors. Thin store component of the proposed method comprises of four parts.

- Metadata Manager
- Address Mapper
- Storage Reclaimer
- Resource Monitor

Metadata Manager: The metadata manager plays a pivotal role in the management of metadata which is essential for virtualization and controls logical volume and mapping table. Metadata are mainly used for keeping a record of the entire mapping table, logical volume, updating of the data records etc. It also helps in the organization of storage resources like physical volume, volume groups, and logical volume. The integration with mapping metadata caching and lazy update technique, the performance of overall Thin-Store become very high.

Address Mapper: It is mainly aimed for load balancing and processes mapping request from the logical volume. It dynamically allocates a logical address to the application. The requirement of address mapper is also used to relate the logical address with the physical address by the address mapping technique. There are so many algorithms are used in the implementation of the address mapper viz. Hashing, Paging, Bit mapping technique. Among all techniques, Bit mapping is more advantageous because it has very less overhead.

Storage Reclaimer: There is always some sector of the disks are getting occupied and some parts are getting freed. During this operation, there should be some intelligent responsibility taker to manage the recently freed space. For this act, Storage reclaimer takes the responsibility to manage free space. This helps thin provisioning an efficient approach to utilizing storage in the better manner.

Resource Monitor: It looks into the state of storage device and manages the storage spaces when its total capacity is about to finish. This component of ThinStore monitors the entire functionality of the system. This component is also responsible for the necessary updating of Address mapper. Routinely it keeps looking into all the functionality of the components.

2.3 Multiprotocol Switch

The basic architecture of storage virtualization consists of storage network i.e. SAN, NAS and DAS. Nowadays data centres are connected through a number of servers and switches for the fulfilment of client' s request. So, it is the first and foremost responsibility of the data centres are switches must be energy efficient with less delay. It requires a significant switching capacity for storage area network (SAN), cloud, internet and intranet. This storage network is connected to server via multiprotocol switch. The specialty of multiprotocol switch is that it reduces latency of the access as well as it makes system power efficient. The concept behind multiprotocol switch is that to reduce number of switches for different protocols. Normally, we require different number of I/O such as Ethernet, fibre channel or PCIe for interconnecting storage devices, server or other peripherals. This consumes a lot of power as well as imparts a large latency. Finally it affects the performance of the entire system. So, we are proposing a multiprotocol switch for handling such situation. The servers are connected to storage network by multiprotocol switch. This will make virtualization an effective for computing, storage and application. So, we have employed an intelligent switch to adopt various protocols like Ethernet over PCIe, PCIe over Internet or Fibre Channel over Ethernet. This switch is mainly employed due to making of an energy and latency efficient. The energy requirement of physical and control switch is very less as compared with the conventional Ethernet router. In this switching system, switch interface only sends and receives the multiprotocol packets in the PCIe signal format. The architecture of this switching system is based on CSMA-ST (Space Time-CSMA). This approach elevates switching capacity by improving transmission speed of CSMACD. The data and control of the switch are basically managed by two similar switch boards which are kept at the both end of Switch Access Card (SAC) inside the switching architecture. This approach provides more flexibility and more switching capacity due to separation of the data and control signal. The whole switching system makes it more scalable.

3. SECURITY ANALYSIS

In security analysis, we analyze the security efficiency of our method. The security level of our proposed method is very high due to public key cryptography. According to the study there are various security issues that should be considered while analyzing it.

- Isolation
- Application Security
- Computing Security
- Data Security

Isolation: The isolation of the individual existence of each VM hypervisor is required. So, the responsibility of hypervisor is a major role in the management of VMs. Here the use of session-based token and public key cryptography ensure the each VM' s request for the access is unique and can' t be interfered by someone else. In this way, the cryptographic technique incorporated with the existing hypervisor enables isolation of VMs.

Application Security: The cross verification of the session-based token ensure the application which requests the access to storage network are valid. The technique for cross verification is done mutually by SAN component and Client component on VM' s request. Once it is validated then only an application is allowed to access storage network. Thin-Store, based on thin provisioning manages the storage, maps logical address with the physical address as well as utilizes the unclaimed storage.

Computing Security: The architecture of the storage virtualization is in such a way that it needs different protocols are required to implement it fully. Each protocol requires their own computation, switches and becomes computational overhead as well as infrastructure cost. Uses of Multiprotocol switch and cross-validation of the token helps to enhance the computing security.

Data Security: Once the token is authenticated then only VMs are allowed to access the storage device. The use of asymmetric key cryptography ensures the most secure way to check the identification of the entity involved in the communication, till the public key is compromised. Once the identification is done through the public key cryptography, authentication and authorization are secure. In this way, it ensures the data security.

The analysis based on the security aspects ensures our system very much because the session based token used with different cryptographic technique helps to the efficient and effective identification, authentication as well as authorization.

4. PERFORMANCE ANALYSIS

In the performance analysis, we analyze the performance of our method and compare results with the existing system. We setup a PC with 2.4GHz Intel quad-core CPU and 4GB RAM with Linux and Xen3.3.1 for virtualization system. We have taken two segate 7400rpm SATA HDD of 500GB each and created two guest domains D1 and D2. Here each of the domains was allocated a single dedicated processor core. Depending on the test type we can change the size of the RAM for the guest domain, and it can vary from 128MB to 1GB. There are various monitoring tools such as iostat, xentop etc can be used. The performance analysis is measured based on the I/O per second (IOPS) request and CPU utilization. After running this technique in the system, we found some of the great advancement with respect to response time and throughput.

iSCSI TARGET PERFORMANCE RESULTS

Here we have analyzed the performance of different targets. With the aspect of features, both SCSI Target Subsystem (SCST) and Linux I/O Target (LIOT) are the more advanced features than SCSI Target Framework (STGT) and iSCSI Enterprise Target (IET). IET' s performance is not going to measure here, because it is now unsupported. Thus it is out of the consideration. So, now performance comparison is between SCST, LIOT, and STGT. These three targets are running on three different virtual machines. Here three different test cases were performed, these are :

- Only writing on the disk
- Only reading from the disk
- Read and write in parallel on the same disk.

This performance test was conducted with the help of Flexible I/O (FIO) tool. Flexible I/O (FIO) is a tool to measure I/O performance of different storage types. While comparing the features of SCST and LIOT, each has its own benefits in their own way. In an aspect of performance, it is clear that LIOT is best one. Next to LIOT is SCST and STGT. But here in the Figure 5.3.B, noticeable thing is that STGT' s performance is better than other two. This is happening because it is only requesting Read Access which is mostly available and frequently observed. These frequently accessed data are serviced by the cache, not from the disk. So STGT shows better performance. This approach is not suitable in case of writing because writing requests are distinct every times. So the possibility of fetching data from the cache is very less. Thus Write performance is the good option to consider while measuring the performance. LIOT should be chosen as iSCSI target in this SAN, Because of its performance, since it is included in almost all Linux distributions hence support are available for LIOT in QEMU/KVM, libvirt, and open stack. This makes LIOT target configuration very reliable, easy and stable. In case of SCST, it does not come with Linux Kernel, so it takes more time and effort to implement and configure and also stability is not guaranteed, because it is externally patched to the LINUX kernel.

Remarks

The experimental results provide these important findings. Random read and write operation in vSAN significantly high with respect to regular disk performance. (II) Cloud service providers can improve their storage efficiency by implementing thin provisioning on their storage resources.

Customers can purchase or rent the storage, based on their expected need rather than just the whole investment. (IV) When we need to place multiple virtual disks in a single physical storage, these virtual disks should be co-located nearly whose accesses are temporally dependent on each other. It will result in best performance. (V) The smaller size of virtual disks is mostly preferred because it has less seek on disk and gives better throughput. (VI) It is the best practice of placing the sequentially accessed virtual disk in the outer zone of the disk to achieve better performance.

5. CONCLUSION AND FUTURE WORK

The purpose of this paper is to study different possibilities of designing of a storage area network (SAN) and to get an optimized solution for it. There are different protocols available for storage area networks such as iSCSI, SCSI, FC, FCIP and FCoE. Based on the study, iSCSI is recommended as the best-suited protocol for the SAN. Hence, iSCSI is used to enable communication between storage server(Target)and client(Initiator) in this SAN design. The main advantages of virtualization in SAN are for efficient utilization of hardware, replication, and scalability of storage and possibility of live migration. In this paper, we presented a design and implementation of storage virtualization with security and efficiency. The mechanism includes thin provisioning, the inclusion of multiprotocol switch along with cryptographic technique. Using the proposed method, one can achieve energy efficient and low latent storage virtualized environment. The use of thin provisioning advances the system to achieve better disk utilization and the multiprotocol switch makes the system energy efficient as well as cryptographic technique makes it secure. By the security and performance analysis, we found that our method is providing better result over the existing solution. Here, Disaster recovery is not considered and SAN solution is not implemented to the open stack for the cloud storage. The future study based on this paper can be integrating with the open stack to provide better cloud services.

6. REFERENCES

[1] B. Li, J. Shu, and W. Zheng, Design and implementation of a storage virtualization system based on scsi target simulator in san," Tsinghua Science & Technology, vol. 10, no. 1, pp. 122- 127, 2005.

[2] G. Zhang, J. Shu, W. Xue, and W. Zheng, " Design and implementation of an out-of-band virtualization system for large sans," Computers, IEEE Transactions on, vol. 56, no. 12, pp. 1654-1665, 2007.

[3] J. Guo-song and H. Xiao-ling, " Design and implementation of iscsi out-of-band storage virtualization," in Intelligence Science and Information Engineering (ISIE), 2011 International Conference on, pp. 378-381, IEEE, 2011.

[4] X. Chen, W. Chen, P. Long, Z. Lu, and Z. Wang, " Semma: Secure efficient memory management approach in virtual environment," in Advanced Cloud and Big Data (CBD), 2013 International Conference on, pp. 131-138, IEEE, 2013.

[5] X. Xiang, H. Yu, and J. Shu, "Storage virtualization based asynchronous remote mirror," in Grid and Cooperative Computing, 2009. GCC'09. Eighth International Conference on, pp. 313-318, IEEE, 2009.

[6] A, A. Faris, M. A. Shrud, and A. H. Kharaz, Towards an efficacious storage performance in virtualized environment," in Complex, Intelligent, and Software Intensive Systems (CISIS), 2013 Seventh International Conference on, pp. 243-249, IEEE, 2013.

[7] J. W. Choi, D. I. Shin, Y. J. Yu, H. Eom, and H. Y. Yeom, " Towards high-performance san with fast storage devices," ACM Transactions on Networking, Architecture, and Storage (NAS), 2011 6th IEEE International Conference on, pp. 1-10, IEEE, 2011

[8] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1113

[9] K. Qian, L. Yi, and J. Shu," This store: Out-of-band virtualization with thin provisioning," in Networking, Architecture and Storage (NAS), 2011 6th IEEE International Conference on, pp. 1-10, IEEE, 2011

[10] H. Luo, J. Y. Hui, and A. G. Fayoumi, " A low power and delay multi-protocol switch with io and network virtualization," in High-Performance Switching and Routing (HPSR), 2013 IEEE 14th International Conference on, pp. 35-42, IEEE, 2013.

[11] Storage Networking Industry Association." http://www.snia.org/"

[12] Ahmad, " Easy and efficient disk i/o workload characterization in vmware esx server," in Workload Characterization, 2007. IISWC 2007. IEEE 10th International Symposium on, pp. 149-158, IEEE, 2007.

[13] Ahmad, J. M. Anderson, A. M. Holler, R. Kambo, and V. Makhija, "An analysis of disk performance in vmware esx server virtual machines," in Work-load Characterization, 2003. WWC-6. 2003 IEEE International Workshop on, pp. 65-76, IEEE, 2003.

[14] D. Anderson, "Task force on network storage architecture: network attached storage is inevitable," in System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference on, vol. 1, pp. 725-vol, IEEE, 1997.

[15] H. Guo, J. Zhou, L. Yang, and S. Yu, "A design study for network-based storage systems and performance evaluation," in Networks, 2002. ICON 2002. 10th IEEE International Conference on, pp. 156-161, IEEE, 2002.

[16] W. Y. H. Wang, H. N. Yeo, Y. L. Zhu, T. C. Chong, T. Y. Chai, L. Zhou, and J. Bitwas, "Design and development of ethernet-based storage area network protocol," Computer Communications, vol. 29, no. 9, pp. 1271-1283, 2006.

[17]. R. D. Chamberlain and B. Shands, "Direct-attached disk subsystem performance assessment," in snapi, pp. 71-78, IEEE, 2007.

[18] Patel, K. Sendhil Kumar, N. Singh, K. Parikh, and N. Jaisankar, " Data security and privacy using data partition and centric key management in cloud," in Information Communication and Embedded Systems (ICICES), 2014 International Conference on, pp. 1-5, IEEE, 2014.

[19] Z. Qiang, C. Dong, W. Yunlong, and D. Zhuang, "The out-of-band virtualization model of network storage based on trusted computing," in Natural Computation (ICNC), 2010 Sixth International Conference on, vol. 8, pp. 4354-4357, IEEE, 2010.

[20] Y. Guang, Z. Jingli, and L. Chao, "Implementation and performance evaluation of an iscsi-based storage virtualization," in Networking, Architecture, and Storage, 2007. NAS 2007. International Conference on, pp. 273-274, IEEE,2007.

[21] Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, "Managing security of virtual machine images in a cloud environment," in Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 91-96, ACM, 2009.

[22] V. Aravindan, "Performance analysis of an iscsi block device in virtualized environment," 2014.

[23] Sugumaran, B. B. Murugan, and D. Kamalraj, "An architecture for data security in cloud computing," in Computing and Communication Technologies (WCCCT), 2014 World Congress on, pp. 252-255, IEEE, 2014.

[24] F. S. Al-Anzi, A. A. Salman, N. K. Jacob, and J. Soni, "Towards robust, scalable and secure network storage in cloud computing," in Digital Information and Communication Technology and it's Applications (DICTAP), 2014 Fourth International Conference on, pp. 51-55, IEEE, 2014.

