Disaster Tolerance for IaaS Built Upon Open Cloud Platform

Mr. Mitesh Patel[1] Prof. Ramesh Prajapati[2] Mr. Kaushal Jani[3]

[1,3] M.E. Student [2]Associate Professor

[1,2,3] Department of Computer Engineering

[1,3]Shree Saraswati Institute Of Engineering(058), Rajpur [2]Faculty of Engineering & Technology Rajpur

Abstract— The New advances of virtualization technology in Data Centre lead to the development of features such as High Availability, Disaster Recovery and Fault Tolerance. However, Infrastructure as a Service (IaaS) computing clouds that span across distributed areas require evens a more advanced mechanism. A Disaster Tolerance (DT) enablement solution that covers storage and VM migration in IaaS clouds computing. Technical aspects of implementation are highlighted, detailing the DT algorithm using cloud computing.

Key words: Virtualization, Cloud computing, Disaster Tolerant, Disaster Tolerance, Infrastructure as a Service.

I. INTRODUCTION

Disaster tolerance (DT) refers to the capability of a computing and data environment to survive a disaster (such as loss of communication components, loss of power and a human-made or natural catastrophe) and to continue to function, or to return to its functionality in a relatively short period of time. DT capability requires a distributed system with redundant elements that are physically separated on distances ranging from few buildings to continents.

Virtualization technology opened a new way to control and manipulate the operating systems that run inside the virtual machines (VM). Available techniques allow hypervisors to live migrate a VM between hosts preserving clients' connections in a transparent manner.

A. Infrastructure as a service (IaaS)

In this most basic cloud service model, cloud providers offer computers, as physical or more often as virtual machines, and other resources. The virtual machines are run as guests by a hypervisor, such as Xen or KVM. Management of pools of hypervisors by the cloud operational support system leads to the ability to scale to support a large number of virtual machines. Other resources in IaaS clouds include images in a virtual machine image library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. Amies, Alex; Sluiman, Harm; Tong IaaS cloud providers supply these resources on demand from their large pools installed in data centers. For wide area connectivity, the Internet can be used Orin carrier clouds – dedicated virtual private networks can be configured. Qiang Guo (July 2012). "Infrastructure as Service Cloud Concepts "Developing and Hosting Applications on the Cloud. IBM Press. ISBN 978-0-13-306684-5. To deploy their applications, cloud users then install operating system images on the machines as well as their application software. In this model, it is the cloud users who are responsible for patching and maintaining the operating systems and application software. Cloud providers typically bill IaaS services on 4 a utility computing basis, that is, cost will reflect the amount of resources allocated and consumed. IaaS refers not to a machine that does all the work, but simply to a facility given to businesses that offers user the leverage of extra storage space in servers and data centers. Examples of IaaS include: Amazon Cloud Formation (and underlying services such as Amazon EC2), Rackspace Cloud, Terre mark and Google Compute Engine.

II. LITERATURE SURVEY

It is important to have a deep understanding on the existing algorithm of Pre-copy and Post-copy method. In this chapter we have mentioned several research papers based on virtual machine migration methods, Optimization the migration of virtual computers, live migration of virtual machines, Eucalyptus open source Cloud-computing system, Disaster Recovery Planning: A Strategy for Data Security implemented by various people to understand the work done so far in this domain. This chapter gives us a detailed and extensive description of the work done by various people and the various methods implemented.

Currently, there are some works on the migration which can be referred to Pre-copy method in [2] [3] [4]. This method has three steps for migration a Virtual Machine: in the first step, the virtual machine memory pages are transferred in several rounds and then, in step two, the virtual machine CPU states are sent to the destination. After that instep three, the memory pages in source and destination are synched with each other. Also, Hines and Gopalan [5] present a Post-copy technique with optimization methods. In [6], the method of CR/TR has been presented, which aims to send Logs file instead memory pages toward the destination. Considering the benefits of Pre-copy approach, this is the main migration method, which is supported in mos. Hypervisors such as XEN and KVM. Thus, we used Precopy for sending memory pages and CPU states of virtual machines. However, Pre-copy approach has some short comings; one of these shortcomings is the lack of disk migration (transfer) algorithm. Hence, we cannot use default Pre-copy method in the non-shared disk environments, because the virtual machine disk must be transferred. In this condition, our method has a disk transmission algorithm which is not dependent on the shared disk and can be used in the above-mentioned environments. In addition, use of Pre-copy and other migration methods in Eucalyptuses impossible, because it has certain challenges; therefore, in our method, these challenges have been solved and this is an important difference between our method and that of others.

Vijay Kumar Javaraiah [7] presented an important problem in Cloud computing is data backup and disaster recovery in the event of network or cloud service provider failure. Most cloud service providers offer data backup at

All rights reserved by *www.ijsrd.com*

their premises at premium cost which might not be affordable by consumers and SMB's. Here we introduce a simple solution for this complex problem in the form of a mechanism for online data backup for cloud along with disaster recovery. This approach reduces the cost of the solution and not only protects data from disaster but also makes the process of migration from one cloud service provider to another, much simpler. This solution eliminates consumers' dependency on the service provider and also eliminates the associated data backup cost. A simple hardware box can do all these at little cost.

JUN-MING SHI1, HUA-JUN WANG2, HAN-YU LU3 [8] presented his paper analyzes realization principle of VxVM virtualization heterogeneity and VVR asynchronous replication, and brings forward a solution for the SAN virtualization. The paper introduces market requirement of storage virtualization heterogeneity, analyzes realization principle of VxVM virtualization heterogeneity and VVR asynchronous replication, and brings forward a solution for the SAN virtualization, implements heterogeneity, sites' difference of storage device, implements virtualization uniform management of SAN, it is high availability system with disaster tolerance function, so it can ensure effective stable operation of service of enterprise under any condition.

Yoshihisa Abe and Garth Gibson [9] presented Amazon S3-style storage is an attractive option for clouds that provides data access over HTTP/HTTPS. At the same time, parallel file systems are an essential component in privately owned clusters that enable highly scalable data intensive computing. In this work, we take advantage of both of those storage options, and propose pWalrus, a storage service layer that integrates parallel file systems effectively into cloud storage. Essentially, it exposes the mapping between S3 objects and backing files stored in an underlying parallel file system, and allows users to selectively use the S3 interface and direct access to the files.

III. WHAT IS DISASTER TOLERANCE SYSTEM?

A. Prevention

Designing and incorporating a proper disaster recovery plan is must to make cloud architecture efficient most. Nevertheless, the preventing data stored on cloud from collapsing or getting crashed is more important than managing the already collapsed one. Thus, preventive measures such as round the clock monitoring of cloud should be implemented. Monitoring, thus, is an important part of the cloud management that helps to prevent cloud from falling into the trap of disaster.

B. Preparedness

Even if you haven't left any loop behind in terms of prevention of your data on cloud, there are possibilities of unpredictable technical faults that can emerge anytime. Therefore, preparedness for such things should always be there no matter how secure or well protected your cloud is. If you are prepared for the worst, chances of restoring everything back and running operations smoothly increase gradually.

C. Response

An efficient disaster recovery plan is that, which starts functioning with agility and has quick response time. If your disaster recovery doesn't cater to the basic requirements at the time a cloud collapses, it means the plan lacks efficient tools that enable data to restore quickly.

D. Recovery

End result of a disaster recovery plan is that it should be able to restore everything at the earliest without any hassle. Thus, how well developed a disaster recovery plan is matter a loss.

IV. ARCHITECTURE OF DTS

In computing, iSCSI is an abbreviation of Internet Small Computer System Interface, an Internet Protocol (IP)-based storage networking standard for linking data storage facilities. By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances. ISCSI can be used to transmit data over local area networks (LANs), wide area networks (WANs), or the Internet and can enable location-independent data storage and retrieval. The protocol allows clients (called initiators) to send SCSI commands (CDBs) to SCSI storage devices (targets) on remote servers. It is a storage area network (SAN) protocol, allowing organizations to consolidate storage into data center storage arrays while providing hosts (such as database and web servers) with the illusion of locally attached disks. Unlike traditional Fiber Channel, which requires special-purpose cabling, iSCSI can be run over long distances using existing network infrastructure. In DTS we have used iSCSI for separating processing center (cluster controller and node controller) to storage and cloud controller. This will give shared storage for both primary and secondary to access client image snapshot when it need to be migrate for failover. Related works show it's give impressive performance and less consumption of time when use shared storage for live migration from any hypervisor.

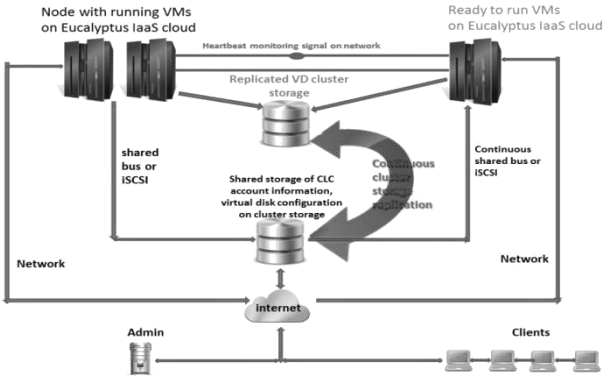

Fig. 1: Architecture of DTS

V. RESEARCH DETAIL

1) Find out what type of disasters
2) The goal of this project is to develop Disaster tolerance system for cloud provider

All rights reserved by *www.ijsrd.com*

3) Study different solutions that can give tolerance to cloud Venders
4) When disaster occur control goes to secondary datacenter
5) Failover and failback system
6) Transparent to client
7) Estimate RPO and RTO

A. RPO AND RTO

1) A "recovery point objective" or "RPO", is defined by business continuity planning. It is the maximum tolerable period in which data might be lost from an IT service due to a major incident. The RPO gives systems designers a limit to work to. For instance, if the RPO is set to 4 hours, then in practice, offsite mirrored backups must be continuously maintained- a daily offsite backup on tape will not suffice. Care must be taken to avoid two common mistakes around the use and definition of RPO. Firstly, BC Staff use business impact analysis to determine RPO for each service- RPO is NOT determined by the extant backup regime. Secondly, when any level of preparation of offsite data is required, rather than at the time the backups are offsite- the period during which data is lost very often starts near the time of the beginning of the work to prepare backups which are eventually offsite.
2) The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
3) It can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users. Decision time for user's representative is not included.
4) The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points.
5) In accepted business continuity planning methodology the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the business continuity planner). The RTOs are then presented to senior management for acceptance.
6) The RTO attaches to the business process and not the resources required supporting the process.
7) The RTO and the results of the BIA in its entirety provide the basis for identifying and analysing viable strategies for inclusion in the business continuity plan. Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO. This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTOs
8) The "O" in RTO stands for objective, not mandates. In reality, tactics are often selected that will not meet the RTO. In this instance the RTO will not be met but should still remain an objective of future strategy revision.

VI. CONCLUSION

Client use cloud instance for many purpose for as parallel rendering, web server or for file sharing etc, any of this instance have specific software for fulfill this requirement and services. When disaster occur client loss their data but with proper DT plan cloud vender can able to backup all instance image at another site(backup site) and so disaster harm to only processing center. With backup data all client transparently able to get back their instances by split cloud infrastructure in two part datacenter and processing center of replicated and connect via iSCSI protocols with any continuous replication scheme.

VII. RERERENCES

[1] Sh.Z. Rad, M.S. Javan, and M.K, Akbari, "A survey on virtual machine migration methods and performance evaluations", First CSUT Conference on Computer, Communication, Information Technology (CSCCIT), Tabriz, Iran, 2011,IEEE.
[2] C.P. Sapuntzakis, R. Chandra, B. Pfaff, J. Chow, M.S. Lam, and M. Rosenblum, "Optimization the migration of virtual computers", In Proceeding of 5th USENIX Symposium on Operating Systems Design and Implementation (OSDI-02),December 2002.
[3] C. Clark, K. Fraser, S. Hand, J.G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, "Live migration of virtual machines", In Proc. of the second USENIX Symposium on Networked Systems Design and Implementation (NSDI), Boston, MA,USA, May 2005.
[4] R. Bradford, E. Kotsovinos, A. Feldmann, and H. Schioberg ,"Live wide-area migration of virtual machines with local persistent state",VEE'07, June 2007.
[5] M. R. Hines and K. Gopalan, "Post-copy based live virtual machine migration using adaptive pre-paging and dynamic self-ballooning", Proceeding of the 2009 ACM SIGPLAN/SIGOPS International Conf. on Virtual Execution Environments, Binghamton University (State University of New York), Feb2009.
[6] H. Liu, H. Jin, X. Liao, L. Hu, and C. Yu, "Live migration of virtual machine based on full system trace and replay", in Proceedings of the 18th International Symposium on High-performance Distributed Computing (HPDC'09), 2009,pp.101–110.
[7] Vijay Kumar Javaraiah Brocade Communications Bangalore, India" Backup for Cloud and Disaster Recovery for Consumers and SMBs"2012.
[8] A Method for Implementing Application Disaster Tolerance based on VxVM Virtualization Intelligent Storage, engin jun-ming shi1, hua-jun wang2, han-yu lu3 1,2College of Information Engineering, Chengdu University of Technology, Chengdu 610059, China 3Department of Computer and Information Engineering, Guizhou University, Guiyan 550003, China 2010 IEEE.
[9] pWalrus: Towards Better Integration of Parallel File Systems into Cloud Storage Yoshihisa be and Garth Gibson -Department of Computer Science Carnegie Mellon University Pittsburgh, PA, USA 2010 IEEE

All rights reserved by *www.ijsrd.com*

[10] Cloud Computing Services with VMware Virtualization - Cloud Infrastructure, http://www.vmware.com/solutions/cloud-computing/.
[11] Amazon Simple Storage Service API reference, API version 2006-03-01, 2006.
[12] http://enterprisesecurity.symantec.com/PDF/AxentPDFs/RiskMgmt.pdf
[13] http://en.wikipedia.org/wiki/Eucalyptus
[14] http://en.wikipedia.org/wiki/Hypervisor
[15] http://www.eucalyptus.com

All rights reserved by *www.ijsrd.com*