International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4| ISSN: 2456-3307

Disaster Recovery and Active Backup of Linux Server

Suhas Kolte, Dr. Anup Gade
Tulsiramji Gaikwad Patil College of Engineering, Mohgoan, Nagpur, Maharashtra, India

ABSTRACT

Backup and disaster recovery are critical to the survival of your business; as in those without a solution will find themselves out of business when the inevitable disaster, be it technical failure, natural, or a malicious human, brings their systems down. It is therefore entirely logical that businesses should put in some time and energy towards finding a good backup and disaster recovery solution.. Included below you will find an analysis of industry trends and current debates. In this paper we provide a way to provide active backup to linux servers in situations of recovery. We also provide a real time system implementation for dealing with disaster recoveries. We also compare the time complexity for performing recovery on Cloud and cluster based linux servers. Experimental results show improvement in time requirement for different clusters.

Keywords : Disaster Recovery, Backup, Linux Servers

I. INTRODUCTION

The cyber threats that come from individuals, criminal groups, and even nation-states have grown and evolved over the years to the point where they represent a major business risk. Any business that foolishly ignores that risk, as did Sony, will reap a whirlwind of negative financial and personal consequences. Therefore, if sensitive data or log in credentials are stored on backup servers, that represents a large vulnerability for any company. In choosing a backup and disaster recovery solution, make sure good security practices are a top priority for both yourself and the potential solution provider.

Consolidation is a little more straightforward. Businesses have been reducing the number of data centers as well as physical pieces of hardware, replacing them with virtualization. This has had a number of benefits, but has presented challenges for backup and disaster recovery solutions. You will need to ensure that the solution you pick can handle virtual environments and will not slow or stop any virtualization plans. Backup and disaster recovery has come a long way since asking the secretary to copy the week's files onto a floppy disk and take it home for the weekend for safekeeping (although some businesses still follow this practice!). Although better than nothing, there are better ways to protect your business. On the other hand, you will need a way to choose the best fit for your company.

Our absolute dependence on information technology resources along with a number of catastrophic (e.g. Great East Japan earthquake, 9/11) and other events (human errors and failures, such as Amazon's EC2 service disruption [1]) have put Disaster Recovery (DR) in the spotlight. DR involves a set of practices and activities aiming at the integrity or the continuity of operation of the physical and virtual information technology assets of an organization, despite significant disruptive events. Particularly, DR practices are based on the continuous protection of resources (VM-image, VM-storage, storage, application), using a primary and a secondary datacenter connected through a Metropolitan, a Wide Area Network (MAN/WAN) or an inter-datacenter network. The secondary datacenter is ready to pick up work in case the primary one fails. In particular, DR life cycle has three main phases [2]: i) deployment, where the primary site and the secondary site(s) are set up for supporting DR; ii) synchronization, which is characterized by continuous data replication from the primary site to the secondary site; and iii) failover, referring to the recovery of the primary site at the backup.

II. RELATED WORK

The following sections explain the survey of various papers regarding this concern. Different methods that have been proposed for having data backup for Servers are given bellow.

In [2], Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, have proposed a novel data recovery service framework for cloud infrastructure, the Parity Cloud Service (PCS) provides a privacy-protected personal data recovery service. In this proposed framework user data is not required to be uploaded on to the server for data recovery. All the necessary server-side resources that provide the recovery services are within a reasonable bound. The advantages of Parity Cloud Service are that it provides a reliable data recovery at a low cost but the disadvantage is that its implementation complexity is higher.

In [3], Vijaykumar Javaraiah introduced a mechanism for online data backup technique for cloud along with disaster recovery. In this approach the cost of having the backup for Cloud platform has been reduced and also it protects data from disaster at the same time the process of migration from one cloud service provider to another becomes easier and much simpler. In this approach the consumers' are not dependent on the service provider and it also eliminates the associated data recovery cost. A simple hardware box is used that achieves all these at little cost.

In [4], Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki,Muzai Gakuendai, Inzai-shi, Chiba,Kazuo Ichihara, proposed the innovative file back-up concept HS-DRT, that makes use of an effective ultra-widely distributed data transfer mechanism and a high-speed encryption technology. This system consists of two sequences one is Backup sequence and other is Recovery sequence. The data to be backed-up is received In Backup sequence. The recovery sequence is used when there is a disaster or any data loss occurs the Supervisory Server (one of the components of the HSDRT) starts the recovery sequence. There are some limitations in this approach and due to which, this model cannot be declared as a perfect technique for Cloud back-up and recovery. Although this model can be used for movable clients such as laptops Smart phones etc. the data recovery cost is comparatively increased and also there is increased redundancy.

In [5], Giuseppe Pirr´o, Paolo Trunfio, Domenico Talia, Paolo Missier and Carole Goble proposed Efficient Routing Grounded on Taxonomy (ERGOT) which is fully based on the semantic analysis and does not focuses on time and implementation complexity. This system is based on the Semantics that provide support for Service Discovery in cloud computing. This model is built upon 3 components one A DHT (Distributed Hash Table) protocol second A SON (Semantic Overlay Network), and third A measure of semantic similarity among service description We makes a focus on this technique because it is not a simple back-up technique rather it provides retrieval of data in an efficient way that is totally based on the semantic similarity between service descriptions and service requests. ERGOT proposes a semantic-driven query answering in DHT-based systems by building a SON over a DHT but it does not go well with semantic similarity search models. The drawback of this model is an icreased time complexity and implementation complexity.

In [6], Eleni Palkopoulouy, Dominic A. Schupke, Thomas Bauscherty, proposed one technique that mainly focuses on the significant reduction of cost and router failure scenario i.e. (SBBR). It involves logical connectivity of IP that will be remain unchanged even after a router failure. The most important factor of this model is that it provides the network management system via multi-layer signaling. Additionally this model shows how service imposed maximum outage requirements that have a direct effect on the setting of the SBRR architecture (e.g. imposing a minimum number of network-wide shared router resources locations).The problem with model is that it is unable to include optimization concept with cost reduction.

In [7], Sheheryar Malik, Fabrice Huet, proposed the lowest cost point of view a model "Rent out the Rented Resources". This technique focuses on reducing the cloud service's monetary cost. It proposed a model for cross cloud federation which

consists of three phases that are 1) Discovery, 2) Matchmaking and 3) Authentication. This model is simply based on the concept of cloud vendors that rent the resources from different venture(s) and after virtualization, rents it to the clients as cloud services.

III. PROPOSED WORK

The proposed work is planned to be carried out in the following manner

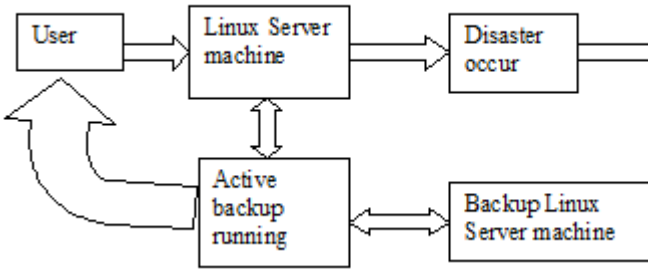

Fig.1:Basic system architecture

We present the Disaster Recovery that enables OpenShift-managed datacenter workloads, Virtual Machines (VMs) and Volumes, to be protected and recovered in another datacenter, in case of a disaster. The file system backup is an important strategy for data retention. In this project, we present an efficient, easy- to-use Backup and Disaster Recovery System for Linux Server. It supports full backup and regularly incremental backup to the server with very low cost and high throughout. The proposition of this Project is that an improvised process can successfully support disaster recovery activities in IT organizations. The project Focuses to build mainly "Disaster Recovery and Active Backup of Linux" Server which would maneuver, navigate and operate with minimum human intervention. This project aims at implementing to recover and protect a Linux Server in the event of a disaster. At the time of disaster automatically resume where it was running with the current configuration and current data so that the user should not scared of loss of machine in case of any disaster.

In this work, we describe a Disaster Recovery Layer (DRL) that we implemented for OpenShift [3] -based datacenters that enables Virtual Machines (VMs) and their data storage (volumes) to be protected and recovered in another datacenter, in case of a disaster, as shown in Figure 1. Our work has been performed in the context of the EU FP7 ORBIT project whose purpose was to develop technologies for the provision of business continuity as a service. Business continuity views an organization from a more general point of view, focusing on what needs to be done in order to keep the business running in the aftermath of a disaster, identifying triggering events, required procedures, involved entities (physical or virtual), and defining related priorities. Every successful business continuity strategy needs an effective DR plan and respective mechanisms.

The main design goals of the Disaster Recovery Layer (DRL) were the following: efficient OpenShift integration, extensibility of the protection and restoration approaches, low-resource overhead, fast recovery and transparent operation. These goals where achieved through the completion of four major tasks:

- Extend the OpenShift cloud management platform so as to enable DR. The DRL framework is based on a number of autonomous components and extensions to OpenShift modules, whose functionalities are available through OpenShift's Horizon UI and command line interface.
- Develop mechanisms for the synchronization of VM state and data as well as for their recovery in case of a disaster. The DRL's extensible architecture allows easy and dynamic integration of protection, restoration and orchestration plug-ins that adopt new approaches (e.g., taking into account available bandwidth between sites) and serve (protect and recover) additional kind of resources.
- Enable accurate and in time detection of when and where a failure has occured over geographically distributed datacenter deployments. A robust and distributed disaster detection mechanism has been developed for this purpose, identifying datacenter disasters and alerting the DRL.

IV. EXPERIMENTAL RESULTS

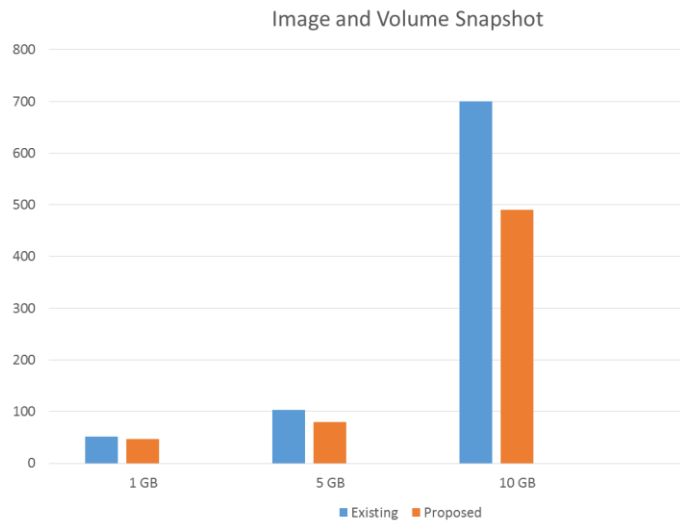

Fig 1: Image and Volume Snapshot

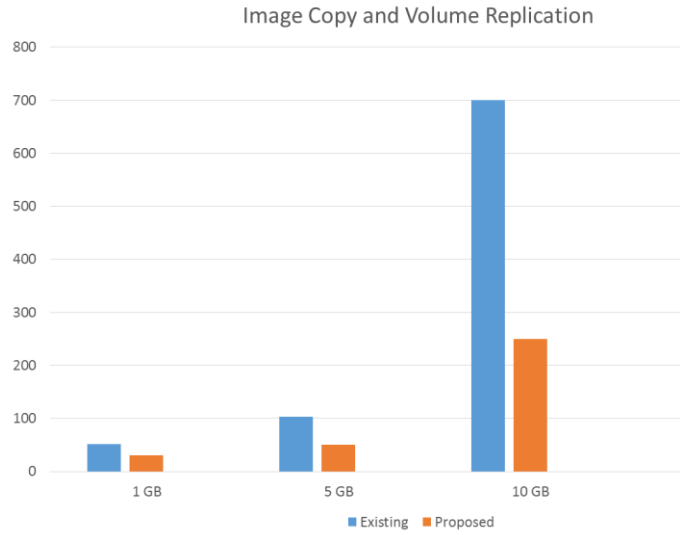

Fig 2 : Image and Volume Replication

V. CONCLUSION

In this paper we provide a way to provide active backup to linux servers in situations of recovery. We also provide a real time system implementation for dealing with disaster recoveries. In this work, we presented the Disaster Recovery Layer (DRL) for OpenShift-based datacenters, enabling the business continuity as a service concept. The DRL scheme being implemented and integrated with OpenShift, is extensible by design so as to easily incorporate new protection, restoration and orchestration policies. Two protection policies for VM images and two protection policies for persistent storage (volumes) were implemented, using either image/volume snapshot or image copy and volume replication. Replications policies are based on the continuous transfer of update data between the primary and backup datacenters.

VI. REFERENCES

1. Disaster Recovery Layer for Distributed OpenShift Deployments L. Toms; P. Kokkinos; V. Anagnostopoulos; O. Feder; D. Kyriazis; K. Meth; E. Varvarigos; T. Varvarigou IEEE Transactions on Cloud Computing
2. Unified human and robot command for disaster recovery situations Carlos Ibarra Lopez; James Kuczynski; Holly A. Yanco 2017 IEEE International Symposium on Technologies for Homeland Security (HST)
3. Information Technology Disaster Recovery process improvement in organization Dinesh Alawanthan; Magiswary Dorasamy; Murali Raman 2017 International Conference on Research and Innovation in Information Systems (ICRIIS) Year: 2017
4. Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki,Muzai Gakuendai, Inzai-shi, Chiba,Kazuo Ichihara, 2010, "Performance Evaluation of a Disaster Recovery System and Practical Network System Applications," Fifth International Conference on Systems and Networks Communications, pp 256-259.
5. Giuseppe Pirro, Paolo Trunfio , Domenico Talia, Paolo Missier and Carole Goble, 2010, "ERGOT: A Semantic-based System for Service Discovery in Distributed Infrastructures," 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing.
6. Eleni Palkopoulouy, Dominic A. Schupke, Thomas Bauscherty, 2011,"Recovery Time Analysis for the Shared Backup Router Resources (SBRR) Architecture", IEEE ICC.
7. Sheheryar Malik, Fabrice Huet, December 2011, "Virtual Cloud: Rent Out the Rented Resources," 6th International Conference on Internet Technology and Secure Transactions,11-14 ,Abu Dhabi, United Arab Emirates.
8. Lili Sun, Jianwei An, Yang Yang, Ming Zeng, 2011, "Recovery Strategies for Service Composition in

Dynamic Network," International Conference on Cloud and Service Computing

9. YUeno, N.Miyaho, and S.Suzuki, , 2009, "Disaster Recovery Mechanism using Widely Distributed Networking and Secure Metadata Handling Technology", Proceedings of the 4th edition of the UPGRADE-CN workshop, pp. 45-48.
10. Xi Zhou, Junshuai Shi, Yingxiao Xu, Yinsheng Li and Weiwei Sun, 2008, "A backup restoration algorithm of service composition in MANETs," Communication Technology ICCT 11th IEEE International Conference, pp. 588-591.
11. M. Armbrust et al, "Above the clouds: A berkeley view of cloud computing," http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/ /EECS-2009-28.pdf.
12. F.BKashani, C.Chen,C.Shahabi.WSPDS, 2004, "Web Services Peer to Peer Discovery Service ," ICOMP.
13. P.Demeester et al., 1999, "Resilience in Multilayer Networks," IEEE Communications Magazine, Vol. 37, No. 8, p.70-76.
14. S. Zhang, X. Chen, and X. Huo, 2010, "Cloud Computing Research and Development Trend," IEEE Second International Conference on Future Networks, pp. 93-97.
15. T. M. Coughlin and S. L. Linfoot, 2010, "A Novel Taxonomy for Consumer Metadata," IEEE ICCE Conference.
16. K. Keahey, M. Tsugawa, A. Matsunaga, J. Fortes, 2009, "Sky Computing", IEEE Journal of Internet Computing, vol. 13, pp. 43-51.
17. M. D. Assuncao, A.Costanzo and R. Buyya, 2009, "Evaluating the Cost- Benefit of Using Cloud Computing to Extend the Capacity of Clusters," Proceedings of the 18th International Symposium on High Performance Distributed Computing (HPDC 2009), Germany.
18. Wayne A. Jansen, 2011, "Cloud Hooks: Security and Privacy Issues in Cloud Computing, 44th Hawaii International Conference on System Sciences.Hawaii.
19. Jinpeng et al, 2009, "Managing Security of Virtual Machine Images in a Cloud Environment", CCSW, Chicago, USA.
20. Ms..Kruti Sharma,Prof K.R.Singh, 2012, "Online data Backup And Disaster Recovery techniques in cloud computing: A review", IJEIT, Vol.2, Issue 5.