© 2018 IJSRSET | Volume 4 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Disaster Recovery and Active Backup of Linux Server : A Review

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. This buyers guide hopes to reduce the amount of time and energy you spend finding the right solution by giving you a good starting point from which to begin your search. Included below you will find an analysis of industry trends and current debates. In this paper we provide a brief review of techniques that are available for disaster recovery on Linux and cloud servers.

Keywords : *Seed Block, Random number generator, Remote Server, Main Server, J-bit encoding*

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.

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 [1], Ms. Kruti Sharma has proposed a Seed Block Algorithm Architecture (SBA) and suggested a remote backup server. The remote Backup server is a replica of original cloud server which is physically situated at a remote location. This method is based on the concept of Exclusive-OR (XOR) operation of digital

computing. The whole mechanism consists of three main parts 1.The Main Cloud Server 2.Clients of the Cloud and 3.The Remote Server. The SBA uses a random number and a unique client id associated with each client.

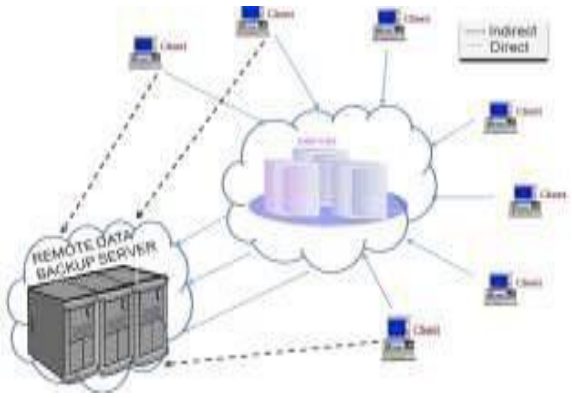

Fig. 1 Remote Backup Server and its Architecture

Whenever a new Client is get registered with the cloud its unique client id is get XOR with a random number. The result of this XOR operation is called as a Seed Block which will be used only for that particular client. Whenever a client stores any Data on to the Cloud it is saved in Cloud and at the same time it is XORed with its Seed Block and the resultant Data' is stored in the remote server. If any accidental data loss occurs in the main Cloud then in such cases the original data is recovered by XORing the Data' with the Seed Block of that particular client to obtain Data'' i.e. the original Data file.

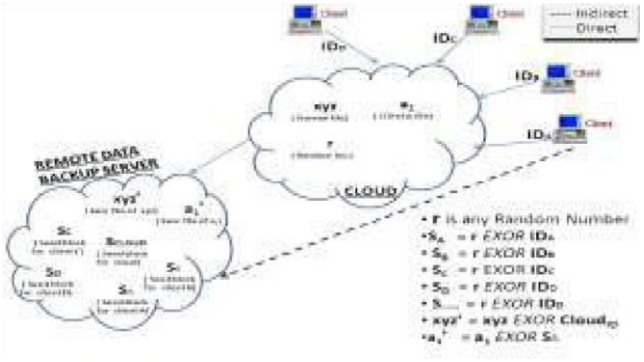

Fig. 2 Seed Block Algorithm and its Architecture.

This technique is fully capable of recovering the data files accurately in any data loss situation also at the same time it maintains data integrity. The disadvantage of this technique is that it is inefficient because the data files on the remote server uses the same space as in the main Cloud so in this way there is wastage of storage space. The storage space in the remote Server can be reduced by applying the compression techniques to achieve high efficiency.

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.

In [8], Lili Sun, Jianwei An, Yang Yang, Ming Zeng, suggested a technique in which there is a gradual increase in cost with the increase in data i.e. The Cold and Hot back-up strategy that performs backup and recovery on trigger basis of failure detection. In CBSRS (i.e. Cold Backup Service Replacement Strategy) recovery process, it is triggered when a service failure is detected and it will not be triggered when there is no failure i.e. when the service is available. The HBSRS (i.e. Hot Backup Service Replacement Strategy), is a transcendental recovery strategy for service composition that is used for dynamic network. During the implementation of process, the backup services remains in the activated state and the first returned results of services will be used to ensure the successful implementation of service composition.

III. EVALUATION AND DISCUSSION

The advantages and disadvantages of all the above discussed techniques are described in the Table-I. And due to the high applicability and need of backup process in many companies and enterprises, the role of a remote data back –up server with an efficient technique is very important and a hot research topic

Sr.no.	Approach	Advantage	Disadvantage
1	SBA[1]	Simple to implement	inefficient
2	Parity Cloud Service[2]	Reliable Privacy Low cost	High complexity
3	LINUX BOX[3]	Simple Low cost	High bandwidth, Complete server backup at a time
4	HSDRT[4]	Used for movable clients	Costly, Increased redundancy
5	ERGOT[]	Exact match retrieval, privacy	Increased complexity
6	Cold/Hot Backup Strategy[8]	Triggered only when failure detected	Cost increases as data increases

Table-I. Comparison between various techniques of Back-up and recovery

IV. CONCLUSION

All the above techniques tried to cover different issues of data backup and recovery for Cloud Computing such as maintaining the cost of implementation and implementation complexities as low as possible. However each one of the backup solution for Cloud Computing is unable to achieve all the issues of remote data back-up server with less storage space.

V. REFERENCES

[1] Ms. Kruti Sharma, Prof. Kavita R Singh, 2013 "Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing" International Conference on Communication Systems and Network Technologies IEEE.

[2] Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, 2011, "Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service," International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11.

[3] Vijaykumar Javaraiah, Brocade Advanced Networks and Telecommunication systems (ANTS), 2011,"Backupforcloud and Disaster Recovery for Consumers and SMBs," IEEE 5th International Conference, 2011.

[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.